

TELEMATICS

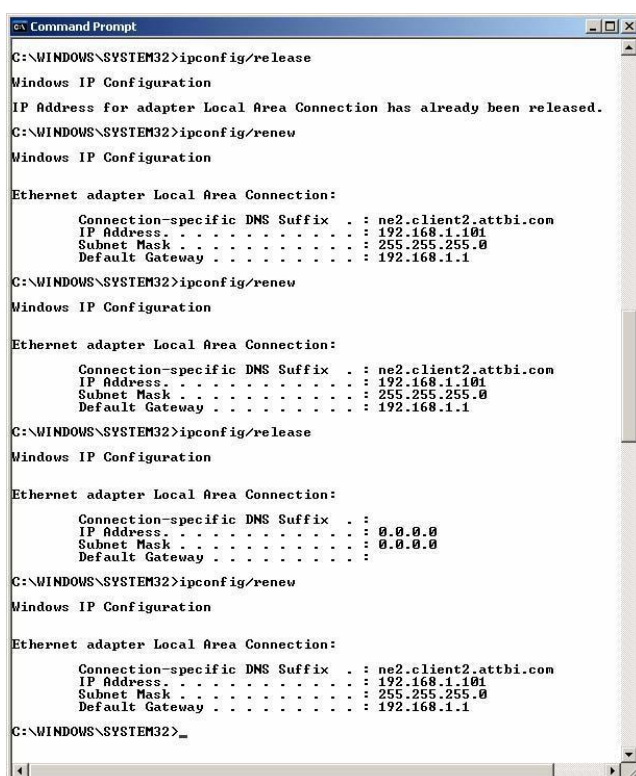
Based on *Computer Networking: A Top-Down Approach, 6th ed.*, J.F. Kurose and K.W. Ross

Laboratorio Wireshark: DHCP,

En esta práctica de laboratorio, echaremos un vistazo rápido a DHCP. Recuerde que DHCP se utiliza ampliamente en redes LAN cableadas e inalámbricas corporativas, universitarias y domésticas para asignar dinámicamente direcciones IP a hosts (así como para configurar otra información adicional de red).

Esta práctica de laboratorio es breve, ya que solo examinaremos los paquetes DHCP capturados por un host. Si también tiene acceso administrativo a su servidor DHCP, es posible que desee repetir esta práctica de laboratorio después de realizar algunos cambios en la configuración (como el tiempo de concesión). Si tiene un router en casa, lo más probable es que pueda configurar su propio servidor DHCP.

1. DHCP Experiment and ARP analysis



```
C:\WINDOWS\SYSTEM32>ipconfig/release
Windows IP Configuration
IP Address for adapter Local Area Connection has already been released.
C:\WINDOWS\SYSTEM32>ipconfig/renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>ipconfig/release
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . :

C:\WINDOWS\SYSTEM32>ipconfig/renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : ne2.client2.attbi.com
    IP Address. . . . . : 192.168.1.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\WINDOWS\SYSTEM32>
```

Para observar DHCP en acción, ejecutaremos varios comandos relacionados con DHCP y capturaremos los mensajes DHCP intercambiados como resultado de la ejecución de estos comandos.

Comencemos abriendo la aplicación de símbolo del sistema en Windows. Como se muestra en la Figura 1, teclee "ipconfig /release". El ejecutable de ipconfig está en C:\windows\system32. Este comando libera su dirección IP actual, de modo que la dirección IP de su host pasa a ser 0.0.0.0.

TELEMATICA

(NOTA: Para sistemas Linux debes mirar el comando “dhclient”

<http://www.computerhope.com/unix/dhclient.htm>)

Figure 1 Command Prompt window showing sequence of ipconfig commands that you should enter.

1. Inicia Wireshark y comience la captura de paquetes de Wireshark.
2. Ahora regrese al símbolo del sistema de Windows y teclee "ipconfig /renew". Esto le indica a su host que obtenga una nueva configuración de red, incluida una nueva dirección IP. En la Figura 1, el host obtiene la dirección IP 192.168.1.108
3. Espere hasta “ipconfig /renew” haya terminado. Entonces vuelve a teclear el mismo comando “ipconfig /renew” otra vez.
4. Cuando el segundo “ipconfig /renew” termine, teclea el comando “ipconfig/release” para liberar la dirección IP que previamente se nos había asignado al equipo.
5. Finalmente, vuelve a teclear “ipconfig /renew” de nuevo para conseguir una nueva dirección IP para el equipo.
6. Para Wireshark.

(CAPTURA1)

Ahora echemos un vistazo a la ventana resultante de Wireshark. Para ver solo los paquetes DHCP, vete al campo de filtro y teclea "dhcp". Vemos en la Figura 2 que el primer comando ipconfig renew hizo que se generarán cuatro paquetes DHCP: un paquete DHCP Discover, un paquete DHCP Offer, un paquete DHCP Request y un paquete DHCP ACK.

TELEMATICA

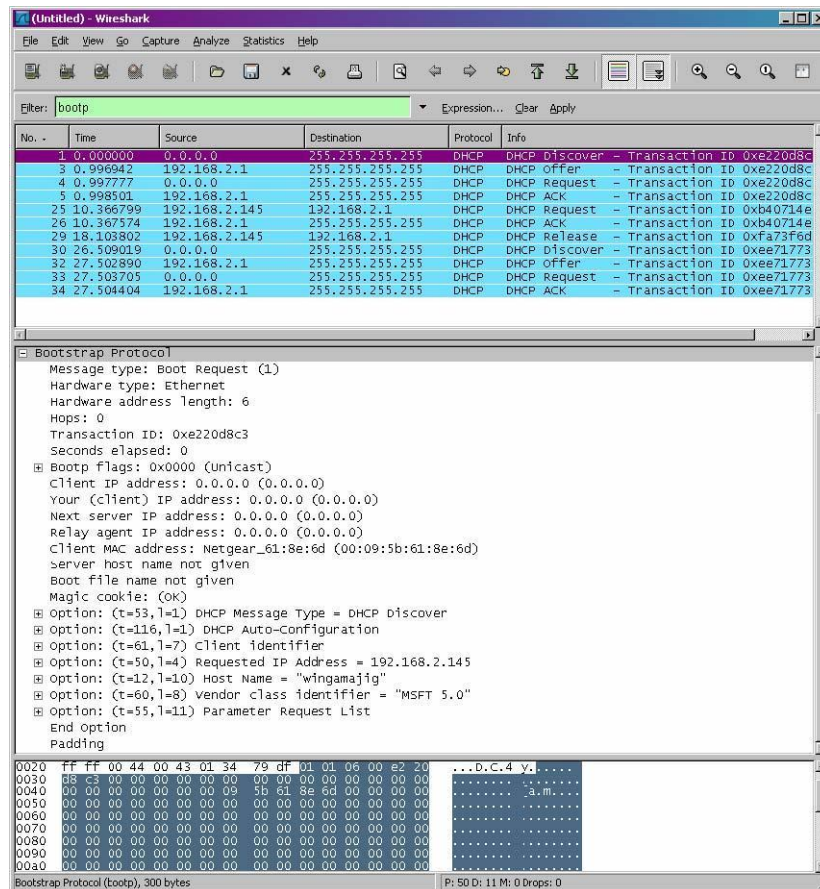


Figure 2 Wireshark window with first DHCP packet – the DHCP Discover packet – expanded.

Debes tener una captura de pantalla de la ventana del símbolo del sistema similar a la Figura 1 anterior para obtener esa captura. Intenta responder las siguientes preguntas:

1. ¿Los mensajes DHCP se envían a través de UDP o TCP?
2. Dibuja un esquema de temporización que ilustre la secuencia del primer intercambio de DHCP de descubrimiento/oferta/solicitud/ACK de cuatro paquetes entre el cliente y el servidor. Para cada paquete, indique los números de puerto de origen y destino.
3. ¿Cuál es la dirección de la capa de enlace (por ej., Ethernet) de su host?, la MAC
4. ¿Qué valores en el mensaje DHCP Discover diferencian éste del mensaje de DHCP Request?
5. ¿Cuál es el valor del campo Transaction-ID en cada una de los primeros cuatro mensajes DHCP (Discover/Offer/Request/ACK)? ¿Cuál es el valor del campo Transaction-ID en el segundo conjunto de (Request/ACK) de los mensajes DHCP? ¿Cuál es el propósito del campo Transaction-ID?
6. Un host usa DHCP para obtener una dirección IP, entre otras cosas. ¡Pero la dirección IP de un host no se confirma hasta el final del intercambio de los cuatro mensajes! Si la dirección IP no se configura hasta el final del intercambio de los cuatro mensajes, ¿qué valores se utilizan en los datagramas IP en el intercambio de los cuatro mensajes? Para

TELEMATICA

cada uno de los cuatro mensajes DHCP (discover/offer/request/ACK de DHCP), indique las direcciones IP de origen y destino que se transportan en el datagrama IP.

7. ¿Cuál es la dirección IP del servidor DHCP?
8. ¿Qué dirección IP ofrece el servidor DHCP a su host en el mensaje DHCP Offer? Indique qué mensaje DHCP contiene la dirección DHCP ofrecida.
9. Explique el propósito de añadir información del router y la máscara de subred en el mensaje DHCP Offer.
10. Explique el propósito del campo "lease time". ¿Cuánto dura ese "lease time"?
11. ¿Cuál es el propósito del mensaje de DHCP Release? ¿El servidor DHCP emite un ACK de DHCP request del cliente? ¿Qué sucedería si se pierde el mensaje de DHCP Release del cliente?