

# Análisis del Tráfico DHCP con Wireshark

Vamos a analizar el tráfico DHCP que hay entre un cliente y un servidor cuando este último quiere conectarse a la red.

Tenemos instalado un Windows server que nos está sirviendo de servidor DHCP, con una pool que abarca entre 192.168.100.10 y 192.168.100.25.

Tenemos además un cliente al cual vamos a borrar y renovar su configuración de adaptador de red para simular que es un equipo que nunca se ha conectado a la red previamente.

También borraremos la entrada de la concesión de la IP para la MAC del cliente en el servidor, así podremos analizar el proceso de configuración dinámica al completo.

1. Borramos la configuración de red con `ipconfig /release`, y la renovamos con `ipconfig /renew` para que el cliente vuelva a solicitar una nueva dirección IP al servidor DHCP.

```
C:\Users\Mañana>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : 
    Vínculo: dirección IPv6 local. . . : fe80::c8a4:18b7:a056:fe0e%11
    Dirección IPv4 de configuración automática: 169.254.254.14
    Máscara de subred . . . . . : 255.255.0.0
    Puerta de enlace predeterminada . . . . . : 

Adaptador de túnel isatap.{D5A7DE48-1BD1-4EE1-96A8-33C941E90A42}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : 

C:\Users\Mañana>ipconfig /renew

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . : cordeiro.local
    Vínculo: dirección IPv6 local. . . : fe80::c8a4:18b7:a056:fe0e%11
    Dirección IPv4. . . . . : 192.168.100.10
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 

Adaptador de túnel isatap.cordeiro.local:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . : cordeiro.local
```

2. En una segunda maquina conectada a la red tenemos abierto wireshark para capturar los paquetes que se mueven en ella. Filtramos por DHCP, y una vez lanzamos `ipconfig /renew` en el cliente empezamos a capturar paquetes del protocolo.

Podemos observar 4 paquetes:

- a. DISCOVER: Se envia del cliente (temporalmente 0.0.0.0) al broadcast, ya que no conoce la red, de esa manera llegara a cualquier equipo dentro de ella, para descubrir si hay algun servidor dhcp.
- b. OFFER: Lo manda el servidor nuevamente al broadcast, ya que el cliente aun no tiene IP, ofreciendole una de las direcciones disponibles dentro de la pool.
- c. REQUEST: Lo manda el cliente al broadcast, solicitando la IP que le ha ofrecido el servidor.
- d. ACK: Finalmente se termina la transacción con un paquete del servidor al broadcast, “reconociendo” que la dirección IP sugerida se asociara con la MAC del cliente para llevar a cabo la configuración automatica.

dhcp						
No.	Time	Source	Destination	Protocol	Length	Info
13	29.884345263	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x459b5576
14	29.884824662	192.168.100.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x459b5576
15	29.885008848	0.0.0.0	255.255.255.255	DHCP	368	DHCP Request - Transaction ID 0x459b5576
17	29.887416496	192.168.100.1	255.255.255.255	DHCP	344	DHCP ACK - Transaction ID 0x459b5576

# Paquete Discover

## Podemos encontrar:

- El tipo de paquete dentro del protocolo DHCP, Discover.
- IP del cliente: 0.0.0.0.
- MAC del cliente: 00:0c:29:4c:97:34.
- IP solicitada: 192.168.100.10, su anterior dirección, probablemente porque quede algun dato en caché.

```

> Frame 13: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_4c:97:34 (00:0c:29:4c:97:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x459b5576
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: VMware_4c:97:34 (00:0c:29:4c:97:34)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
    Length: 1
    DHCP: Discover (1)
  > Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: VMware_4c:97:34 (00:0c:29:4c:97:34)
  > Option: (50) Requested IP Address (192.168.100.10)
    Length: 4
    Requested IP Address: 192.168.100.10
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

# Paquete Offer

## Podemos encontrar:

- El tipo de paquete dentro del protocolo DHCP, Offer.
- IP del cliente: 192.168.100.10, la que le esta ofreciendo.
- MAC del cliente: 00:0c:29:4c:97:34.
- IP ofrecida: 192.168.100.10, la primera disponible en la pool.
- Mascara de subred: 255.255.255.0.
- Lease: 2h.
- Dirección del servidor DHCP: 192.168.100.1.
- Nombre de dominio del servidor: cordeiro.local.

```

> Frame 14: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_d2:f7:56 (00:0c:29:d2:f7:56), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
- Dynamic Host Configuration Protocol (Offer)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x459b5576
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.100.10
  Next server IP address: 192.168.100.1
  Relay agent IP address: 0.0.0.0
  Client MAC address: VMware_4c:97:34 (00:0c:29:4c:97:34)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  - Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
  - Option: (58) Renewal Time Value
    Length: 4
    Renewal Time Value: 1 hour (3600)
  > Option: (59) Rebinding Time Value
  - Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: 2 hours (7200)
  - Option: (54) DHCP Server Identifier (192.168.100.1)
    Length: 4
    DHCP Server Identifier: 192.168.100.1
  - Option: (15) Domain Name
    Length: 15
    Domain Name: cordeiro.local
  > Option: (6) Domain Name Server
  > Option: (255) End
```

# Paquete Request

## Podemos encontrar:

- El tipo de paquete dentro del protocolo DHCP, request.
- IP del cliente: 0.0.0.0, aún sin IP
- MAC del cliente: 00:0c:29:4c:97:34.
- IP solicitada: 192.168.100.10, la ofrecida por el servidor.
- Dirección del servidor DHCP: 192.168.100.1.
- Nombre de equipo del servidor: WIN-K2CFHS36N2I.

```

> Frame 15: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_4c:97:34 (00:0c:29:4c:97:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
- Dynamic Host Configuration Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x459b5576
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: VMware_4c:97:34 (00:0c:29:4c:97:34)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
- Option: (53) DHCP Message Type (Request)
  Length: 1
  DHCP: Request (3)
- Option: (61) Client identifier
  Length: 7
  Hardware type: Ethernet (0x01)
  Client MAC address: VMware_4c:97:34 (00:0c:29:4c:97:34)
- Option: (50) Requested IP Address (192.168.100.10)
  Length: 4
  Requested IP Address: 192.168.100.10
- Option: (54) DHCP Server Identifier (192.168.100.1)
  Length: 4
  DHCP Server Identifier: 192.168.100.1
- Option: (12) Host Name
  Length: 15
  Host Name: WIN-K2CFHS36N2I
- Option: (81) Client Fully Qualified Domain Name
  Length: 18
  > Flags: 0x00
```

# Paquete ACK

## Podemos encontrar:

- El tipo de paquete dentro del protocolo DHCP, ACK.
- IP del cliente: 192.168.100.10, la ofrecida y solicitada, que se asignara en la tabla ARP a la MAC del cliente.
- MAC del cliente: 00:0c:29:4c:97:34.
- IP ofrecida: 192.168.100.10, la primera disponible en la pool.
- Mascara de subred: 255.255.255.0.
- Lease: 2h.
- Dirección del servidor DHCP: 192.168.100.1.

```
▶ Frame 17: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface eth0, id 0
▶ Ethernet II, Src: VMware_d2:f7:56 (00:0c:29:d2:f7:56), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 67, Dst Port: 68
▼ Dynamic Host Configuration Protocol (ACK)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x459b5576
  Seconds elapsed: 0
▶ Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.100.10
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: VMware_4c:97:34 (00:0c:29:4c:97:34)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▼ Option: (53) DHCP Message Type (ACK)
  Length: 1
  DHCP: ACK (5)
▼ Option: (58) Renewal Time Value
  Length: 4
  Renewal Time Value: 1 hour (3600)
▼ Option: (59) Rebinding Time Value
  Length: 4
  Rebinding Time Value: 1 hour, 45 minutes (6300)
▼ Option: (51) IP Address Lease Time
  Length: 4
  IP Address Lease Time: 2 hours (7200)
▼ Option: (54) DHCP Server Identifier (192.168.100.1)
  Length: 4
  DHCP Server Identifier: 192.168.100.1
▼ Option: (1) Subnet Mask (255.255.255.0)
  Length: 4
  Subnet Mask: 255.255.255.0
▼ Option: (81) Client Fully Qualified Domain Name
  Length: 3
```