1 – El protocolo DHCP

DHCP (Dynamic Host Configuration Protocol) es un protocolo de la capa de aplicación. Este nos permite conectar un equipo a la red de forma automática (la manera manual equivalente es la configuración TCP/IP que hacemos en Packet Tracer, por ejemplo). De esta forma, el equipo se encargará de iniciar un proceso en el que acabe obteniendo la configuración TCP/IP para poder comunicarse con otros elementos de la red.

Podemos ver la utilidad de este protocolo con un sencillo ejemplo:

Imaginamos una gran empresa con cientos de ordenadores. En lugar de que un técnico tenga que configurar cada uno de ellos, es mucho más sencillo que al conectarlos a la red obtengan de forma automática su configuración TCP/IP gracias al protocolo DHCP.

Sin embargo, este protocolo tiene más ventajas a parte de la automatización de la conexión, como el aprovechamiento de direcciones IP, la facilidad de la conectividad y la minimización de los errores de configuración.

2 – Cómo funciona

El protocolo DHCP se basa en el modelo ciente/servidor, en el que un cliente espera recibir la información de la configuración TCP/IP, y un servidor es el que la proporciona (ambos estarán conectados a la red y el servidor tendrá instalado el servicio DHCP).

Un ejemplo que podemos observar fácilmente, ocurre al configurar nuestro teléfono móvil como punto de acceso WiFi. Nuestro smartphone, no sólo actúa como punto de acceso, sino que también proporciona una dirección IP al cliente por DHCP, por lo que nuestro teléfono se habrá convertido en una especie de servidor DHCP. Este, además, es un proceso que ocurre en cualquier router cuando se conecta un nuevo dispositivo.

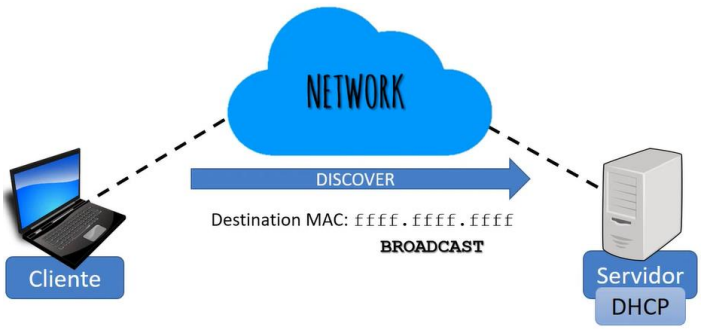
2.1 – DHCP handshake

Para que un servidor le proporciona la configuración TCP/IP al cliente tiene que suceder antes un proceso de 4 fases de intercambio de información entre ellos: el DHCP handshake (o DORA, por las siglas de este proceso)

1 – Discover

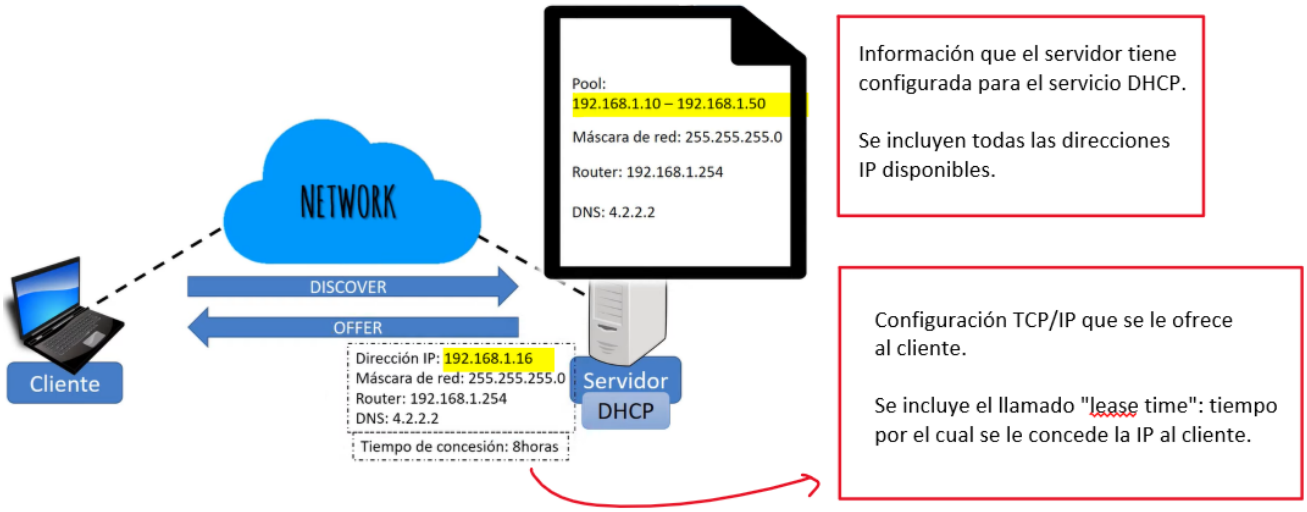
Cuando el cliente con el DHCP activado en su configuración de red, se conecta a la red, envía un mensaje DHCP de tipo discover, en el que intentará descubrir si existe un servidor DHCP en la red que le pueda ofrecer una dirección IP.

Al final, con este proceso lo que se está haciendo es un broadcast, en el que el cliente enviará una dirección MAC con la dirección de broadcast.



2 – Offer

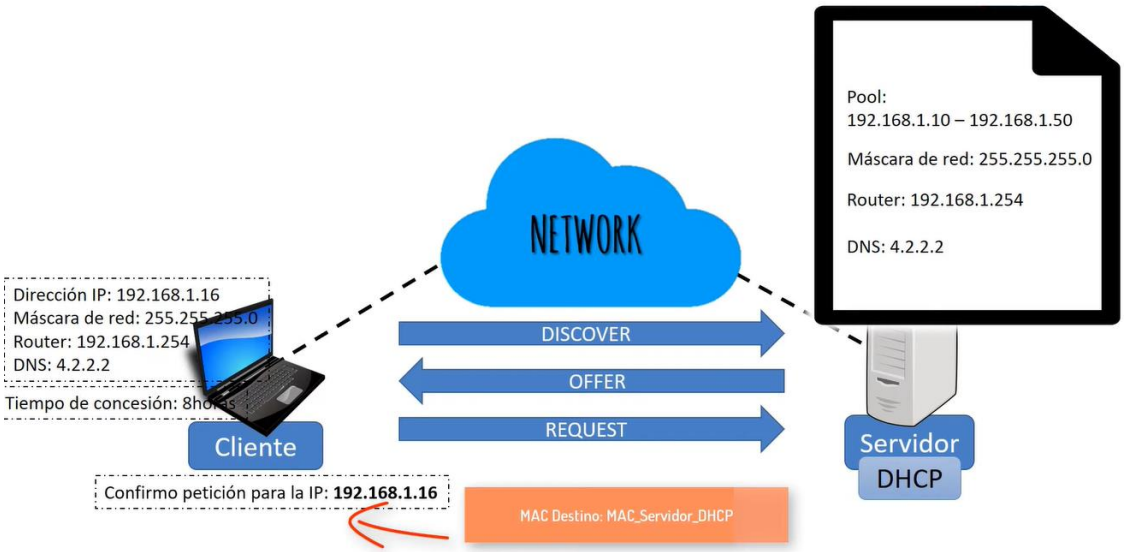
Una vez que el mensaje discover llega al servidor DHCP, este buscará una dirección IP libre dentro de la información que tiene asignada del servicio DHCP.



3 – Request

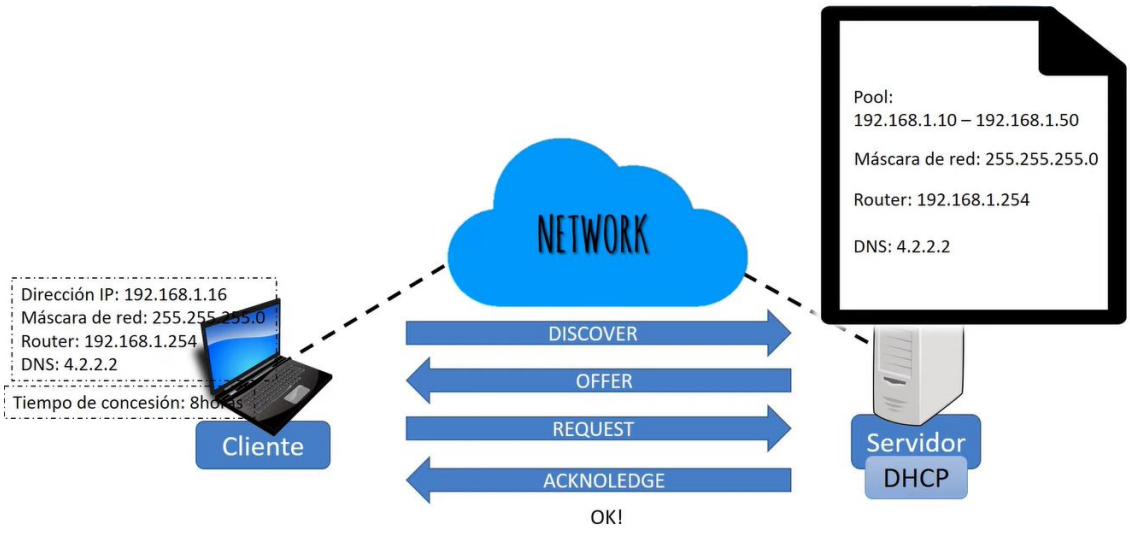
El cliente, al recibir la información proporcionada por el servidor, responderá con un mensaje de HCP request, en el que confirmará al servidor DHCP que se asignará la dirección IP concedida.

Esta vez, el cliente incluirá en el mensaje request la dirección MAC destino del servidor, que habrá aprendido con el anterior mensaje, por lo que esto ya no es una trama tipo broadcast, sino unicast.



4 – Acknowledge (ACK)

El servidor responde con un ACK, confirmando la concesión de la dirección IP.



3 – Práctica

Se comprobará el proceso del handshake DHCP en una máquina virtual con Windows 10 (para facilitar el tráfico de red).

1 – ipconfig /release

Para empezar, se desconectará esta máquina de la red. Entonces, dentro de la CMD se escribirá el comando “ipconfig /release” para que renuncie a su dirección IP. Así, pasará a tener la IP 0.0.0.0.

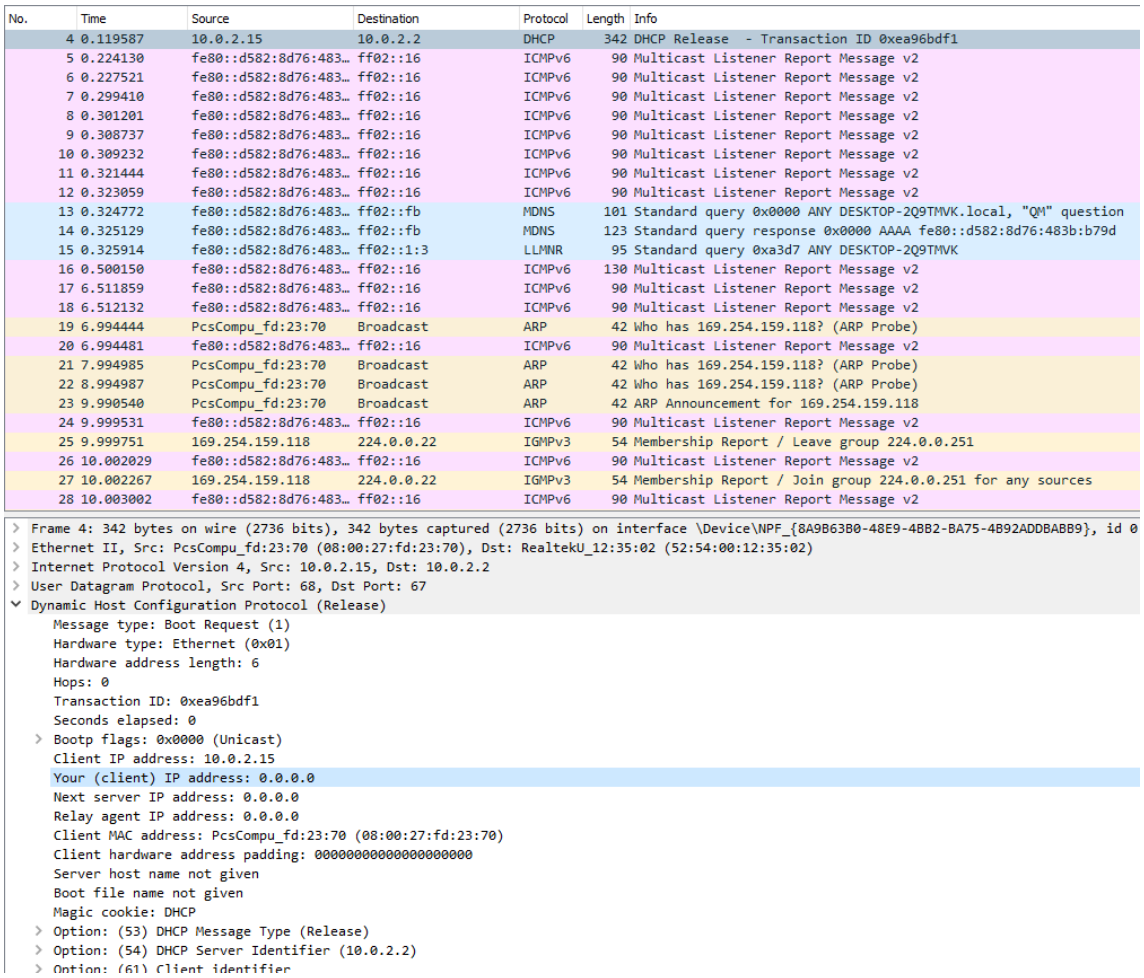
```
C:\Users\Sergio>ipconfig /release

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::d582:8d76:483b:b79d%5
   Puerta de enlace predeterminada . . . . . :
```

Mientras se ejecutaba este comando, se escuchaba el tráfico de red con Wireshark:

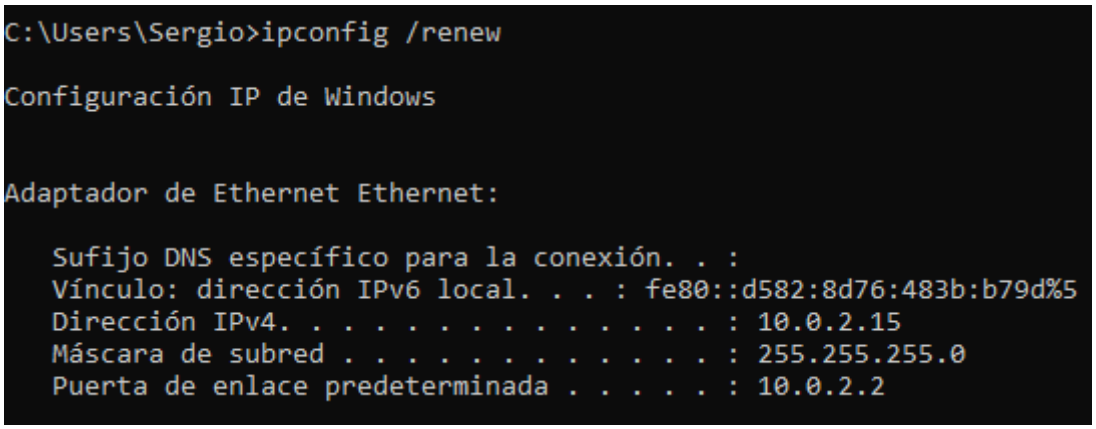


No.	Time	Source	Destination	Protocol	Length	Info
4	0.119587	10.0.2.15	10.0.2.2	DHCP	342	DHCP Release - Transaction ID 0xea96bdf1
5	0.224130	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6	0.227521	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
7	0.299410	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
8	0.301201	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
9	0.308737	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
10	0.309232	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
11	0.321444	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
12	0.323059	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
13	0.324772	fe80::d582:8d76:483…	ff02::fb	MDNS	101	Standard query 0x0000 ANY DESKTOP-2Q9TMVK.local, "QM" question
14	0.325129	fe80::d582:8d76:483…	ff02::fb	MDNS	123	Standard query response 0x0000 AAAA fe80::d582:8d76:483b:b79d
15	0.325914	fe80::d582:8d76:483…	ff02::1:3	LLMNR	95	Standard query 0xa3d7 ANY DESKTOP-2Q9TMVK
16	0.500150	fe80::d582:8d76:483…	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
17	6.511859	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
18	6.512132	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
19	6.994444	PcsCompu_fd:23:70	Broadcast	ARP	42	Who has 169.254.159.118? (ARP Probe)
20	6.994481	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
21	7.994985	PcsCompu_fd:23:70	Broadcast	ARP	42	Who has 169.254.159.118? (ARP Probe)
22	8.994987	PcsCompu_fd:23:70	Broadcast	ARP	42	Who has 169.254.159.118? (ARP Probe)
23	9.990540	PcsCompu_fd:23:70	Broadcast	ARP	42	ARP Announcement for 169.254.159.118
24	9.999531	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
25	9.999751	169.254.159.118	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.251
26	10.002029	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
27	10.002267	169.254.159.118	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
28	10.003002	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

Observamos que se produce un DHCP release, en el que observamos la dirección IP 0.0.0.0.

2 – ipconfig /renew

Asignamos al equipo una nueva dirección IP mediante el comando “ipconfig /renew” en la CMD. En este momento se producirá el DHCP handshake que nos proporcionará una nueva configuración TCP/IP automáticamente tal y como se explicó anteriormente.



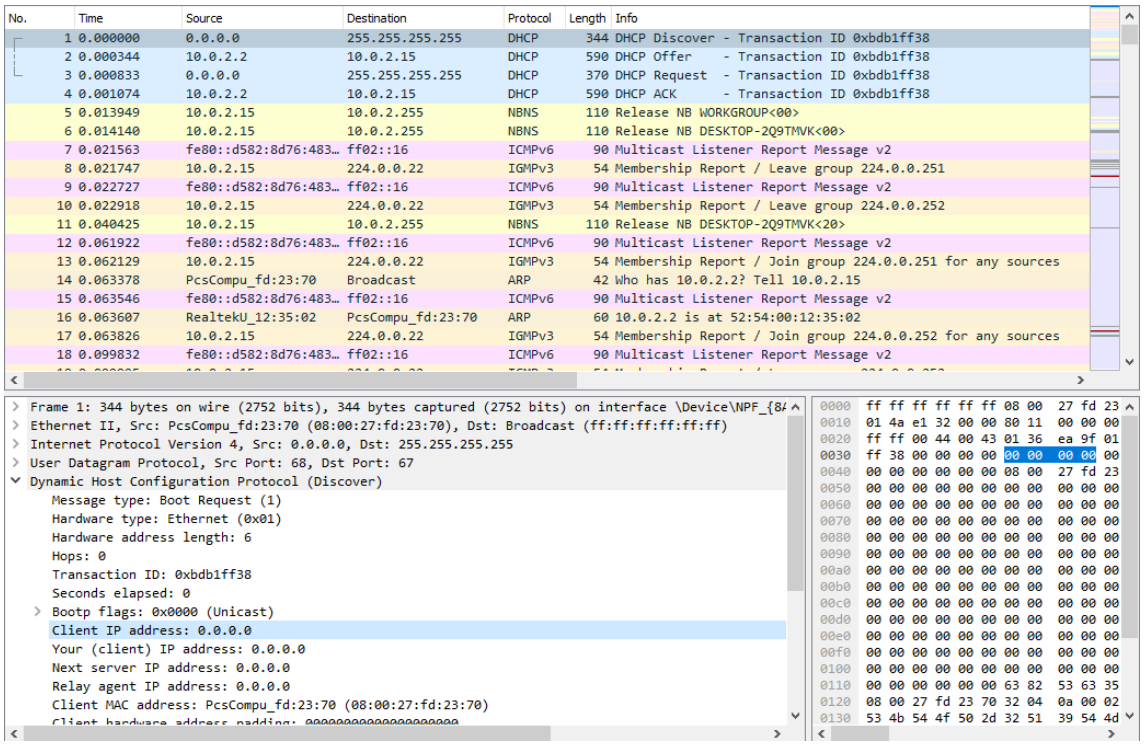
```
C:\Users\Sergio>ipconfig /renew

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::d582:8d76:483b:b79d%5
   Dirección IPv4. . . . . . . . . . . . : 10.0.2.15
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.0.2.2
```

Mientras se ejecutaba este comando, se escuchaba el tráfico de red con Wireshark:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xbdb1ff38
2	0.000344	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction ID 0xbdb1ff38
3	0.000833	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xbdb1ff38
4	0.001074	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction ID 0xbdb1ff38
5	0.013949	10.0.2.15	10.0.2.255	NBNS	110	Release NB WORKGROUP<00>
6	0.014140	10.0.2.15	10.0.2.255	NBNS	110	Release NB DESKTOP-2Q9TMVK<00>
7	0.021563	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
8	0.021747	10.0.2.15	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.251
9	0.022727	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
10	0.022918	10.0.2.15	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
11	0.040425	10.0.2.15	10.0.2.255	NBNS	110	Release NB DESKTOP-2Q9TMVK<20>
12	0.061922	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
13	0.062129	10.0.2.15	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
14	0.063378	PcsCompu_fd:23:70	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.15
15	0.063546	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
16	0.063607	RealtekU_12:35:02	PcsCompu_fd:23:70	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
17	0.063826	10.0.2.15	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
18	0.099832	fe80::d582:8d76:483…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

```
> Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{8A
> Ethernet II, Src: PcsCompu_fd:23:70 (08:00:27:fd:23:70), 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
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xbdb1ff38
    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: PcsCompu_fd:23:70 (08:00:27:fd:23:70)
    Client hardware address padding: 00000000000000000000
```

```
0000  ff ff ff ff ff ff 08 00  27 fd 23
0010  01 4a e1 32 00 00 80 11  00 00 00
0020  ff ff 00 44 00 43 01 36  ea 9f 01
0030  ff 38 00 00 00 00 00 00  00 00 00
0040  00 00 00 00 00 00 08 00  27 fd 23
0050  00 00 00 00 00 00 00 00  00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00
0110  00 00 00 00 00 00 63 82  53 63 35
0120  08 00 27 fd 23 70 32 04  0a 00 02
0130  53 4b 54 4f 50 2d 32 51  39 54 4d
```

Prestamos especial atención al DHCP handshake:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xbdb1ff38
2	0.000344	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction ID 0xbdb1ff38
3	0.000833	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xbdb1ff38
4	0.001074	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction ID 0xbdb1ff38

Observamos los 4 pasos: discover, offer, request y acknowledge.

1 – Discover

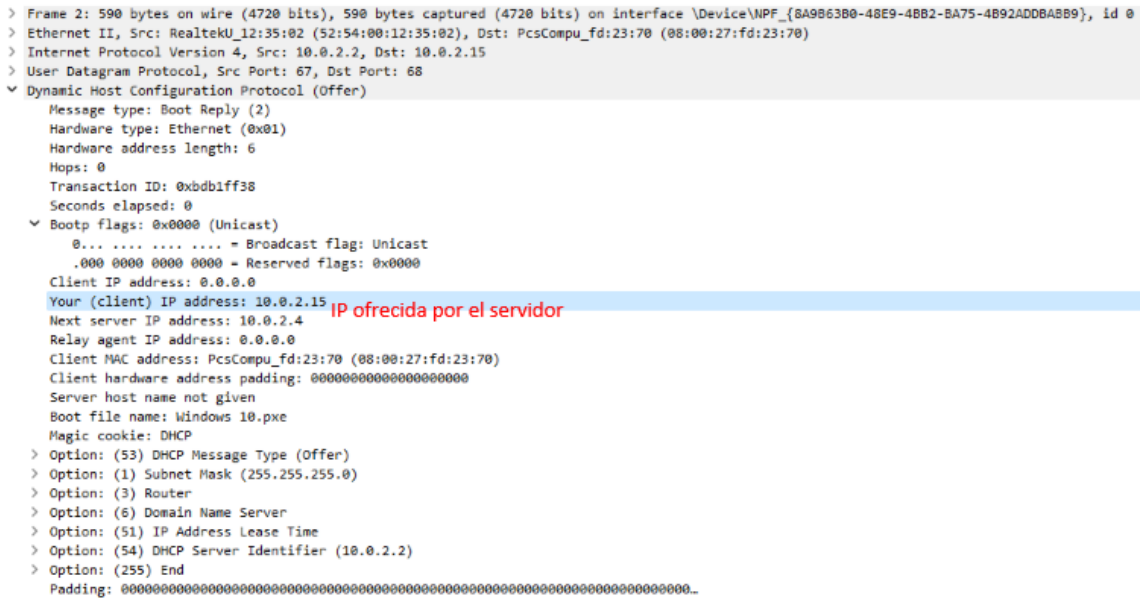
```
> Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{8A9B63B0-48E9-4BB2-BA75-4B92ADDBABB9}, id 0
> Ethernet II, Src: PcsCompu_fd:23:70 (08:00:27:fd:23:70), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xbdb1ff38
    Seconds elapsed: 0
  v Bootp flags: 0x0000 (Unicast)
      0... .... .... .... = Broadcast flag: Unicast
      .000 0000 0000 0000 = Reserved flags: 0x0000
    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: PcsCompu_fd:23:70 (08:00:27:fd:23:70)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (10.0.2.15)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

Broadcast

Client IP

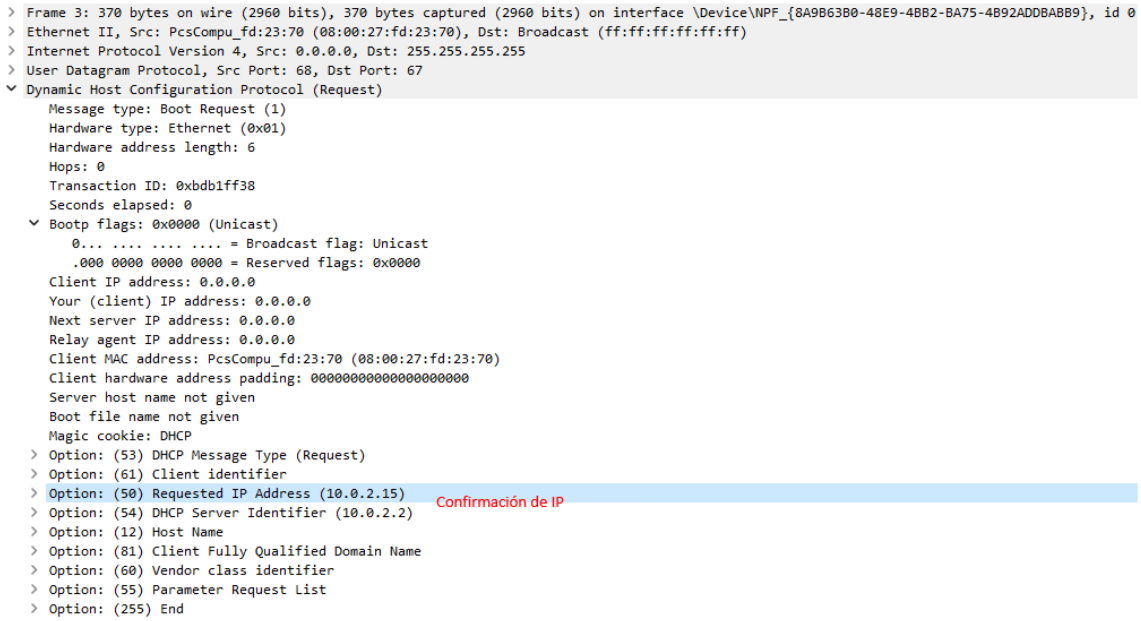
El cliente con IP 0.0.0.0 realiza el broadcast.

2 – Offer



El servidor ofrece la IP “10.0.2.15”.

3 – Request



El cliente confirma la IP ofrecida por el servidor “10.0.2.15”.

4 – Acknowledge

```
> Frame 4: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{8A9B63B0-48E9-4BB2-BA75-4B92ADDBABB9}, id 0
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_fd:23:70 (08:00:27:fd:23:70)
> Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xbdb1ff38
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 10.0.2.15
    Your (client) IP address: 10.0.2.15
    Next server IP address: 10.0.2.4
    Relay agent IP address: 0.0.0.0
    Client MAC address: PcsCompu_fd:23:70 (08:00:27:fd:23:70)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name: Windows 10.pxe
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (51) IP Address Lease Time
  > Option: (54) DHCP Server Identifier (10.0.2.2)
  > Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000000000000000000000000000…
```