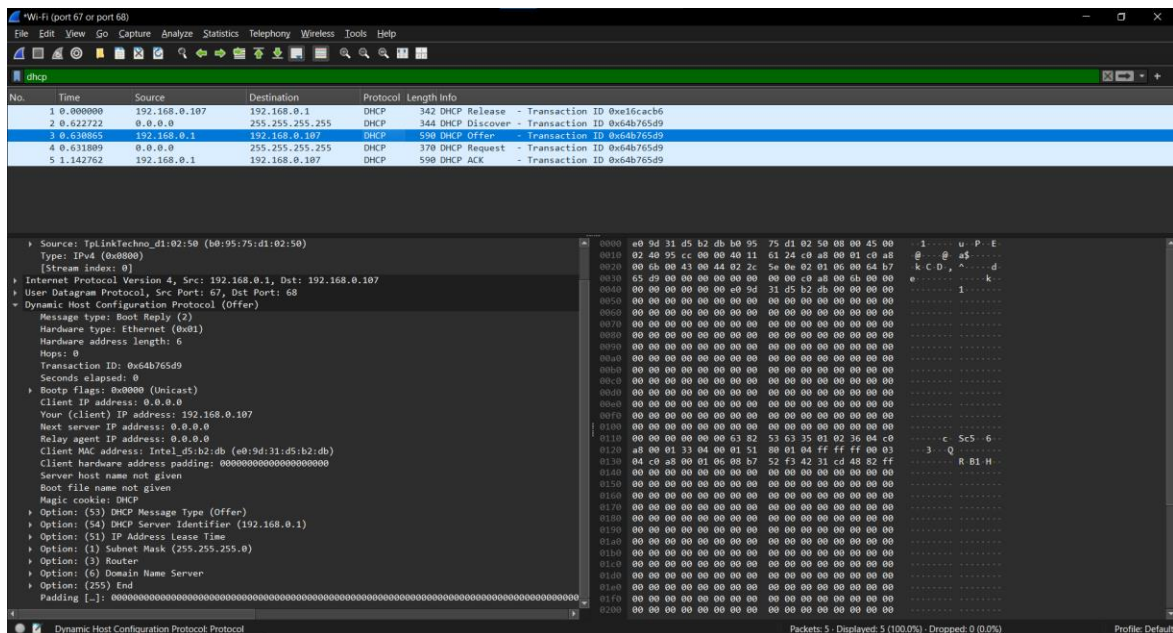


- ## DHCP Discover



The image displays a Wireshark packet capture of a DHCP transaction. The top pane shows a list of packets, with packet 5 selected. The middle pane shows the packet details for the selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (Request). The bottom pane shows the packet bytes in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.107	192.168.0.1	DHCP	342	DHCP Release - Transaction ID 0xe16cacb6
2	0.622722	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x64b765d9
3	0.630855	192.168.0.1	192.168.0.107	DHCP	590	DHCP Offer - Transaction ID 0x64b765d9
4	0.631899	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x64b765d9
5	1.142762	192.168.0.1	192.168.0.107	DHCP	590	DHCP ACK - Transaction ID 0x64b765d9

**Packet 5 Details:**

- Ethernet II, Src: Realtek (08:00:00:00:00:00), Dst: Realtek (08:00:00:00:00:00)
- 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: 0x64b765d9
  - 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: Intel\_05:b2:2d: (e0:0d:31:d5:b2:db)
  - Client hardware address padding: 000000000000000000000000
  - Server host name not given
  - Boot file name not given
  - Magic cookie: DHCP
  - Options: (53) DHCP Message Type (Request)
  - Option: (61) Client identifier
  - Option: (50) Requested IP Address (192.168.0.107)
  - Option: (54) DHCP Server Identifier (192.168.0.1)
  - Option: (12) Host Name
  - Option: (61) Client Fully Qualified Domain Name
  - Option: (60) Vendor class identifier
  - Option: (55) Parameter Request List
  - Option: (255) End

**Packet 5 Bytes:**

```

0000 ff ff ff ff ff ff 0d 31 d5 b2 db 00 00 45 00 .....107.E
0010 81 64 52 14 00 00 00 11 67 6c 00 00 00 00 ff ff ..DR.....107
0020 ff ff 00 44 00 43 01 50 54 de 01 01 06 00 64 b7 ...D.C.P.T...d
0030 65 d9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040 00 00 00 00 00 e0 5d 31 d5 b2 db 00 00 00 00 .....107
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0110 00 00 00 00 00 00 63 82 53 63 25 01 83 34 07 01 .....c.SCS...
0120 e0 5d 31 d5 b2 db 32 04 c0 a8 00 66 36 04 c0 a8 ...1.2...K6...
0130 00 01 0c 0f 4c 41 50 54 4f 50 2d 55 31 44 37 41 ...LAPT.OP-UID7A
0140 46 54 4a 51 12 00 00 00 4c 41 50 54 4f 50 2d 55 ...FTJQ...LAPTOP-U
0150 31 44 37 41 46 54 4a 3c 08 4d 53 46 54 20 35 2e ...1D7ATJQ.NSIT.5.
0160 30 3f 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 ...07...h.../w...
0170 fc ff .....
  
```

**Summary:** The packet capture shows a DHCP transaction where a client (0.0.0.0) requests an IP address from a server (192.168.0.1). The server responds with a DHCP ACK, indicating that the client's request was successful.

[illegible]

To capture DHCP packets, you need to **force a device to request a new IP**.

We can do it by using ipconfig /release

```
C:\WINDOWS\system32>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet 6 while it has its media disconnected.
No operation can be performed on OpenVPN Data Channel Offload for Surfshark while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.
No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Unknown adapter wintunshark0:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter vEthernet (Default Switch):

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::950d:3229:c585:800%75
    IPv4 Address. . . . . : 172.17.112.1
    Subnet Mask . . . . . : 255.255.240.0
    Default Gateway . . . . . :

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::17ac:ab1b:859d:6837%21
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Ethernet 6:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Unknown adapter OpenVPN Data Channel Offload for Surfshark:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :
```

The Dynamic Host Configuration Protocol (DHCP) is used to assign IP addresses to devices automatically. The process follows four steps known as DORA:

### 1) DHCP Discover (Client → Broadcast)

When a device (PC, phone, etc.) connects to a network, it doesn't have an IP address.

It sends a DHCP Discover message to find available DHCP servers.

This message is broadcasted (sent to all devices in the network) since the client doesn't know the DHCP server's IP.

### 2) DHCP Offer (Server → Broadcast)

A DHCP server receives the Discover request and offers an IP address to the client.

The server sends a DHCP Offer message with an available IP address and other network details like subnet mask, gateway, and DNS.

### 3) DHCP Request (Client → Broadcast)

The client accepts the offered IP by sending a DHCP Request message.

This message is also broadcasted because there may be multiple DHCP servers, and the client wants to inform everyone which server's offer it is accepting.

### 4) DHCP Acknowledge (Server → Unicast)

The DHCP server confirms the assignment by sending a DHCP Acknowledge (ACK) message.

The client can now use the assigned IP address to communicate in the network.