

1) UDP, as seen in the packet header.

2) Yes, port 68 & 67 respectively

"DHC"

3) 98:SF:d3:EC:C8:a0

4) flags: for discover option(53) is "350101"
for request option(53) is "350103"
So type 1 is request, & type 3 is discover

5) 1st set: 0x598710c7
2nd Set: 0x2c3e5d45

I imagine they have a 2 fold purpose

1) to track acknowledgements.
2) to allow for some parallelism in the
DHCP server. (Again, tracking purposes.)
B) it is a broadcast IP in the
dest. & a placeholder for 'self' in the
Source field
(null)

Destination is 255.255.255.255
for all 4 messages.

Source is 0.0.0.0 for Disc. & Request
and 10.123.0.1 for Offer & ACK.

7) It's within the router @ 10.123.0.1

8) There's a 'your IP Address' field in the
BootP protocol.

IP offered: 10.123.11.37

9) "Relay agent IP Address: 0.0.0.0"

My relay Addr is also null.

10) The DHCP server doesn't have to be

the same as the router, so this adds a spot into the protocol.
As for the subnet, it's to set that setting for the client.

11) This is in the 'Your IP' line, just like 8.

The client does accept the IP by requesting it back from the DHCP server.

This is in Option (50)

12) The lease time is used to tell the client when to renew its IP & other info. This also releases IPs from the in-use pool. Mine, @ USC, is 8 hours.

13) The Release message tells the DHCP Server that the IP that the Client was using is available for other clients. If the Release packet is dropped the DHCP won't reassign that IP until the lease is up.

14) Yup! They identify the new device on the network to the DHCP Server, and vice-versa.

Command
Prompt

```

C:\ Command Prompt
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
Tunnel adapter Local Area Connection* 3:

Connection-specific DNS Suffix . . . . .
IPv6 Address . . . . . : 2001:0:d5c:5a30:3450:13fc:bb4a:30da
Link-local IPv6 Address . . . . . : fe80::3450:13fc:bb4a:30da%19
Default Gateway . . . . . : . . . . .

Tunnel adapter isatap.{1752A370-1B9A-4AAF-82C7-830FE405F1BB}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
C:\Users\forre>ipconfig/release

Windows IP Configuration

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 2 while it has its media disconnect ed.

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . . . .
Link-local IPv6 Address . . . . . : fe80::50f0:9a43:de5a:d5df%2
Default Gateway . . . . . : . . . . .

Ethernet adapter Bluetooth Network Connection 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
Tunnel adapter Local Area Connection* 3:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
C:\Users\forre>ipconfig /renew

Windows IP Configuration

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 2 while it has its media disconnect ed.

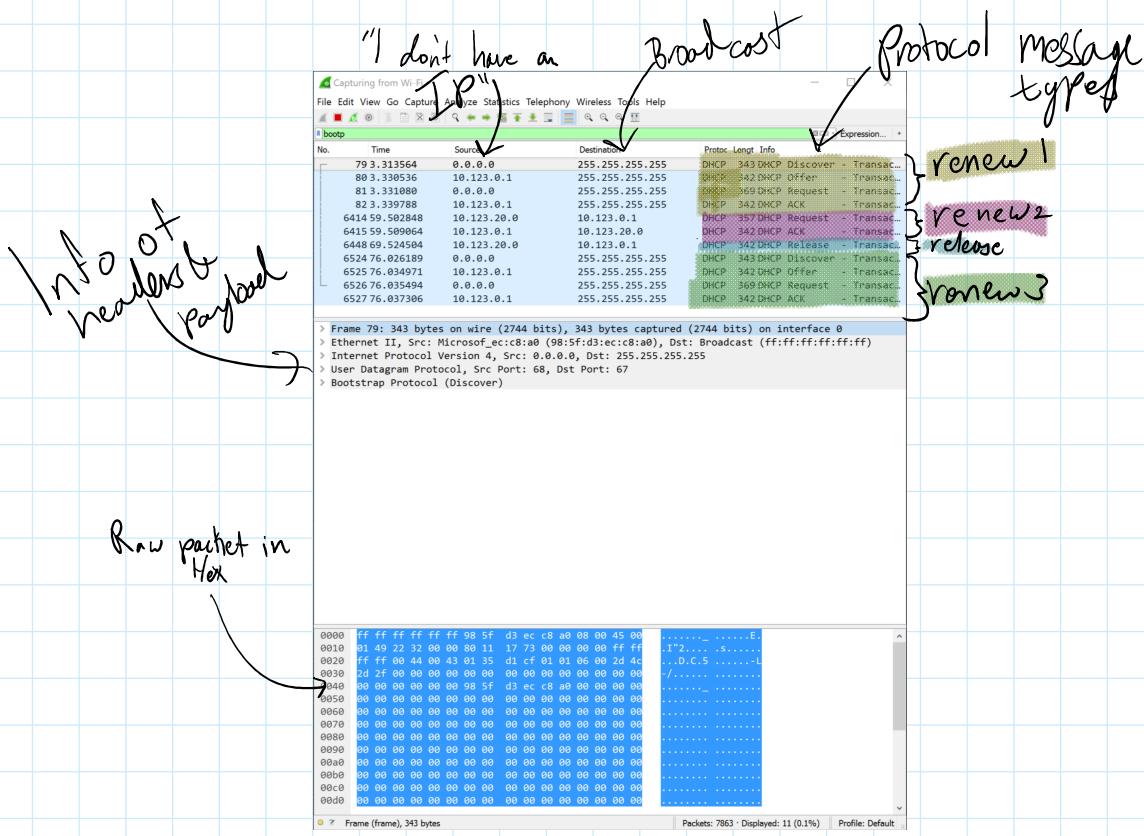
Wireless LAN adapter Local Area Connection* 2:

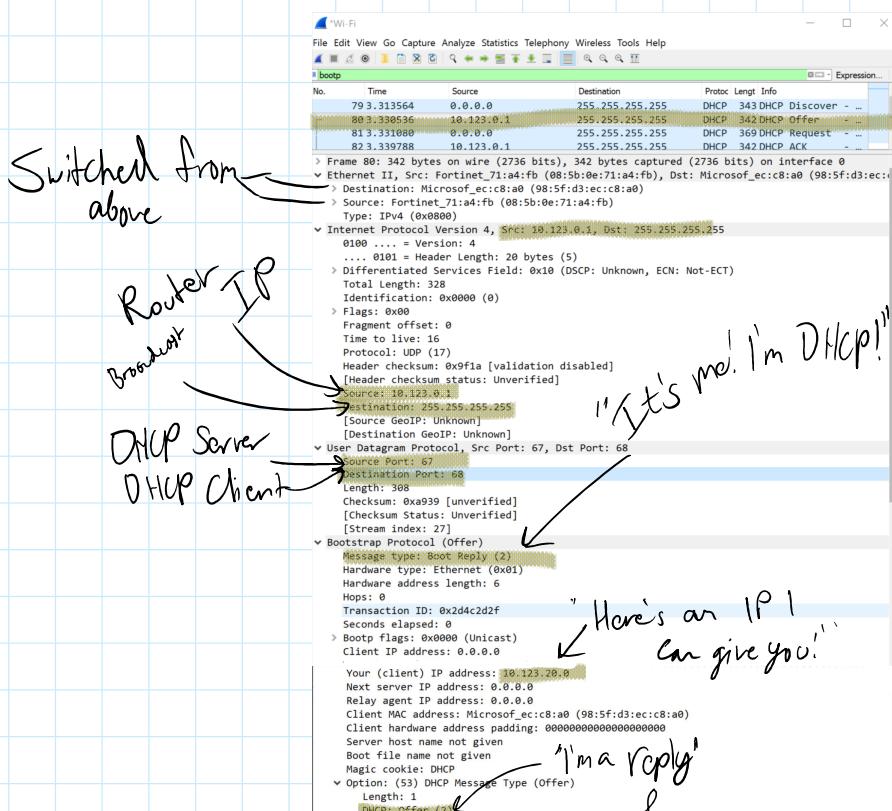
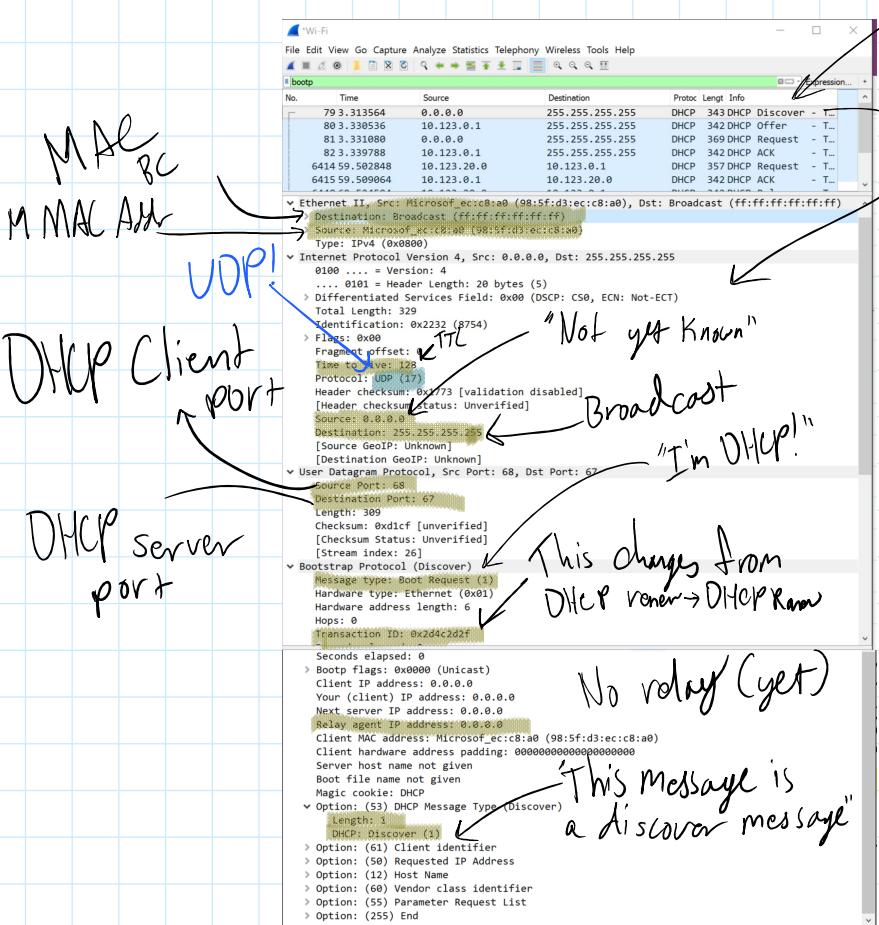
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . .
Wireless LAN adapter Wi-Fi:

```

Abdullah

So, I did the lab & later saw the "print and annotate" part. Thus, the following shows what I recall as necessary info. The actual data will be different than the above answers, however, as I had to re-run the sniffer to get screenshots.





Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
v Option: (53) DHCP Message Type (Offer)
 Length: 1
 DHCP: Offer (2)
v Option: (54) DHCP Server Identifier
 Length: 4
 DHCP Server Identifier: 10.123.0.1
v Option: (51) IP Address Lease Time
 Length: 4
 IP Address Lease Time: (28800s) 8 hours
> Option: (1) Subnet Mask
> Option: (3) Router
> Option: (6) Domain Name Server
> Option: (58) Renewal Time Value
> Option: (59) Rebinding Time Value
> Option: (2) Time Offset
> Option: (255) End
Padding: 00000000

Text item (text), 4 bytes | Packets: 9228 · Displayed: 11 (0.1%) | Profile: Default