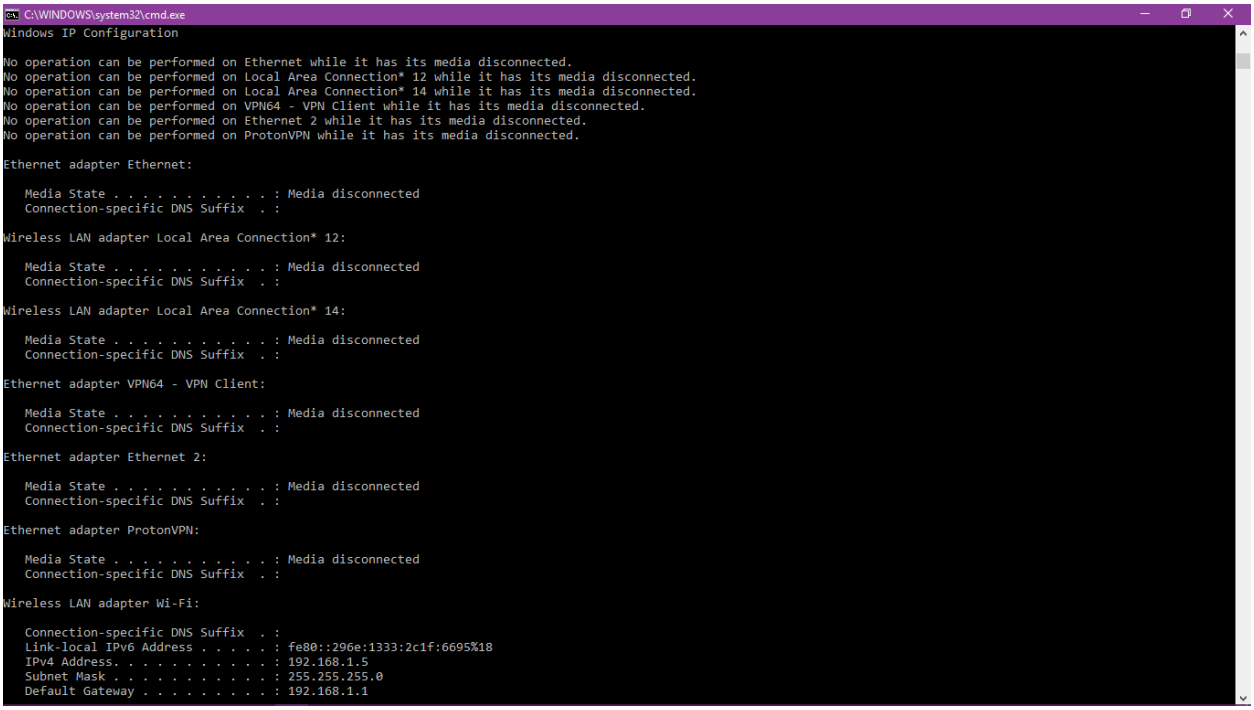
BAYANI, Femo Steven Felicisimo

2015-07104

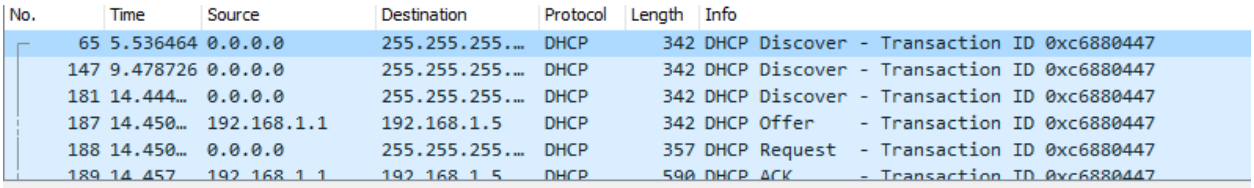
Wireshark Lab 9: DHCP

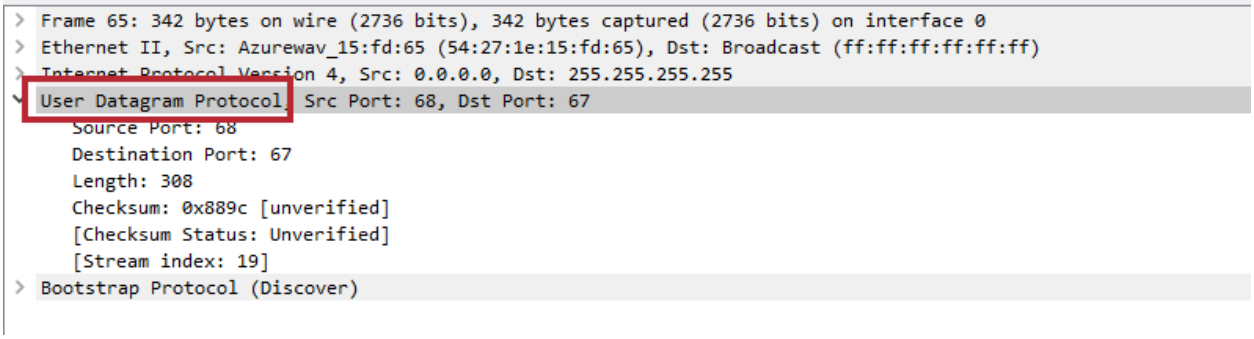
CMSC 138



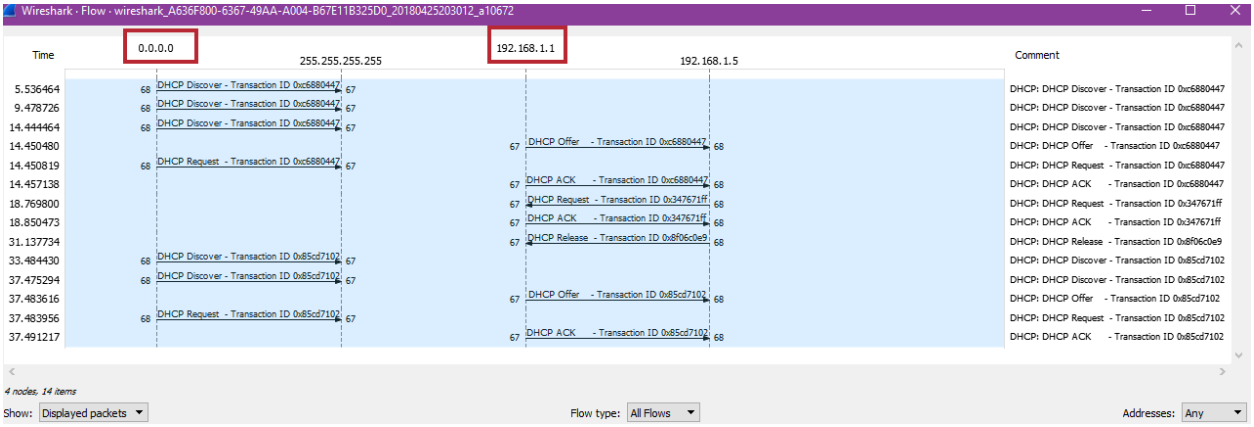
1. Are DHCP messages sent over UDP or TCP?

DHCP messages are sent over **UDP**.



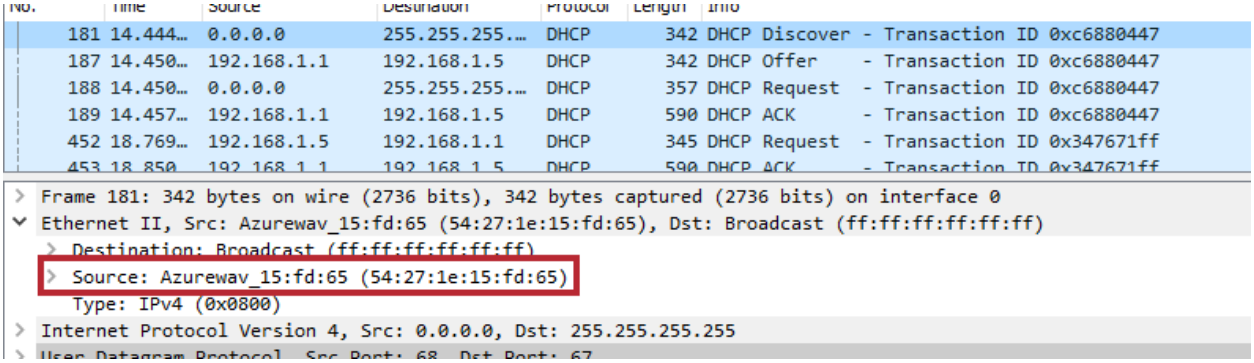


2. Draw a timing diagram illustrating the sequence of the first four-packet. Discover/Offer/Request/Ack DHCP exchange between client and server. For each packet, indicate the source and destination port numbers.

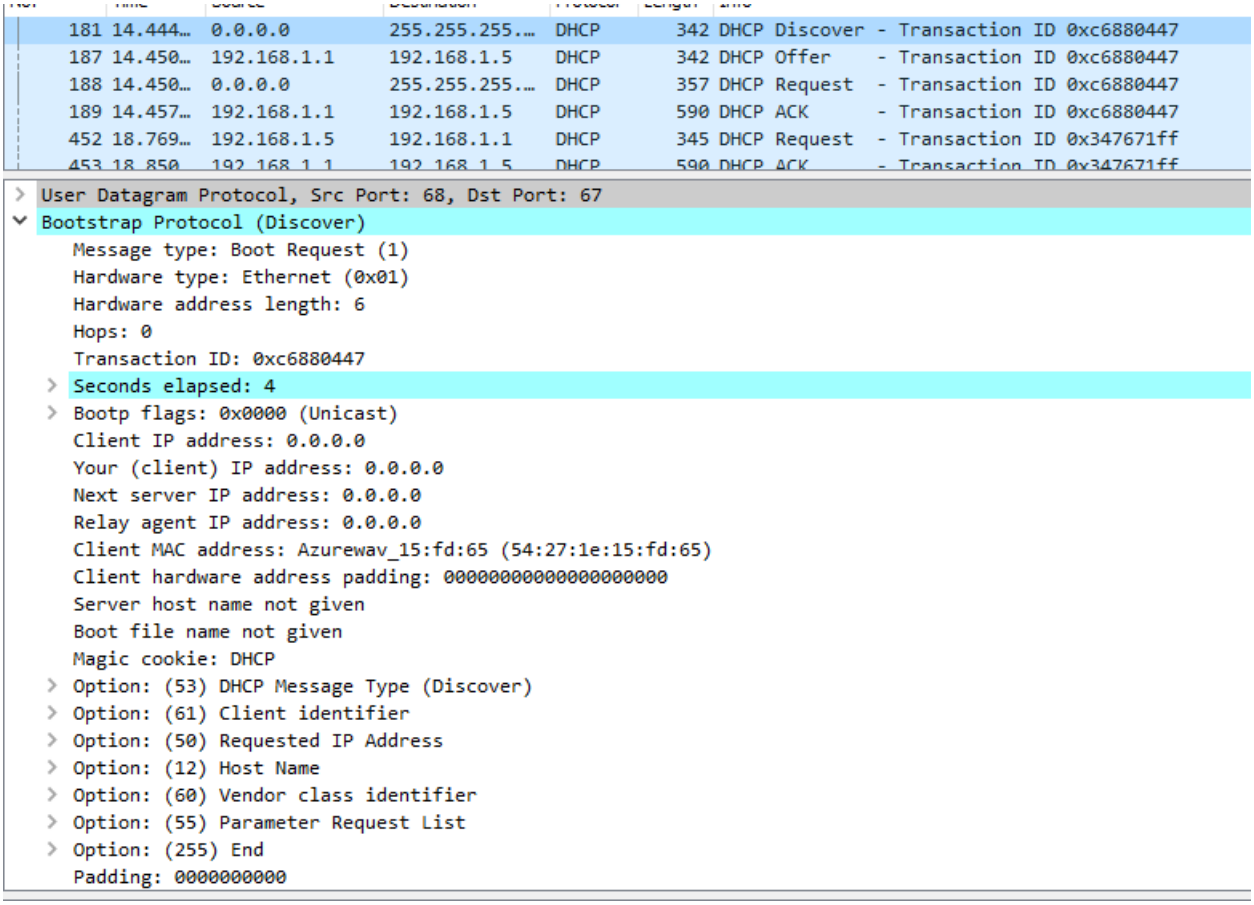


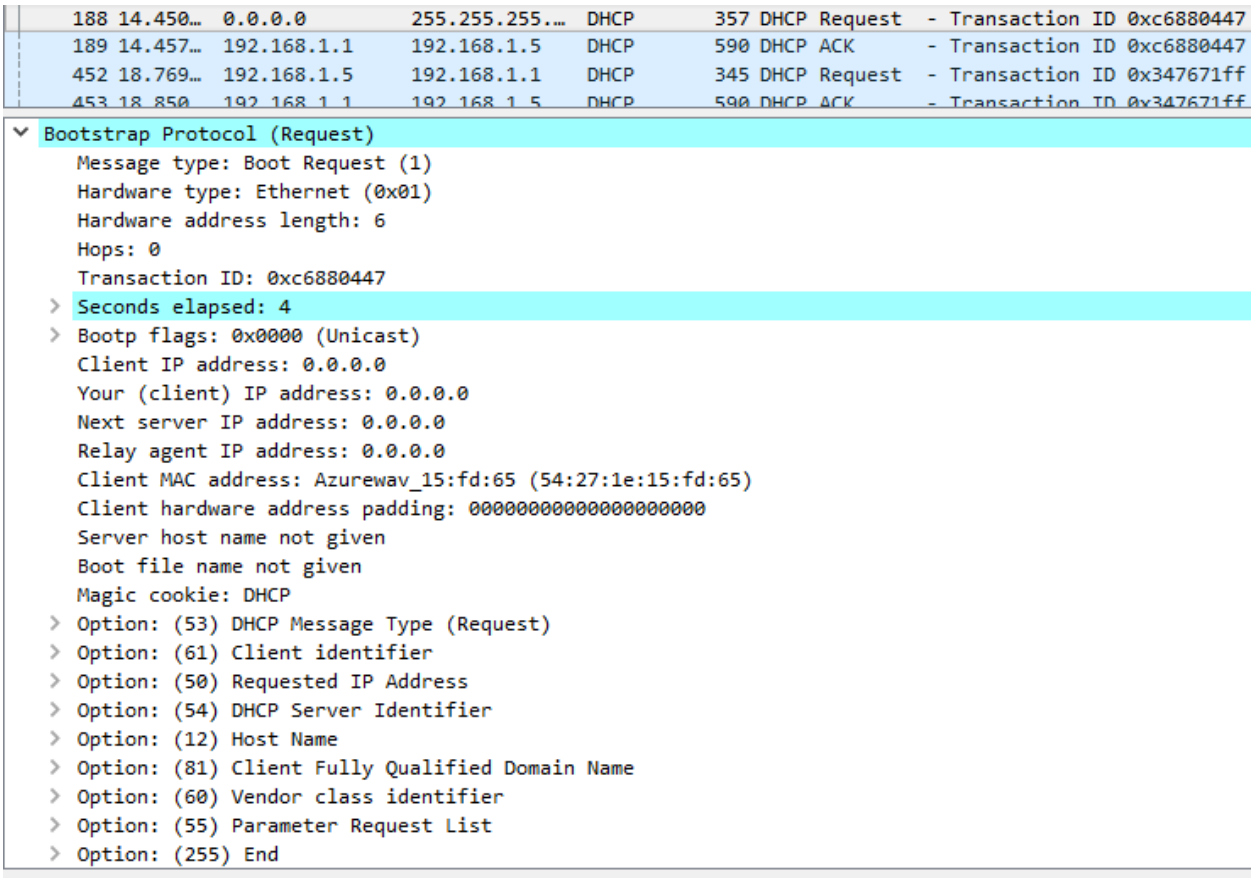
3. What is the data link layer (e.g. Ethernet) address of your host?

The data link layer address of my host is **54:27:1e:15:fd:65**.



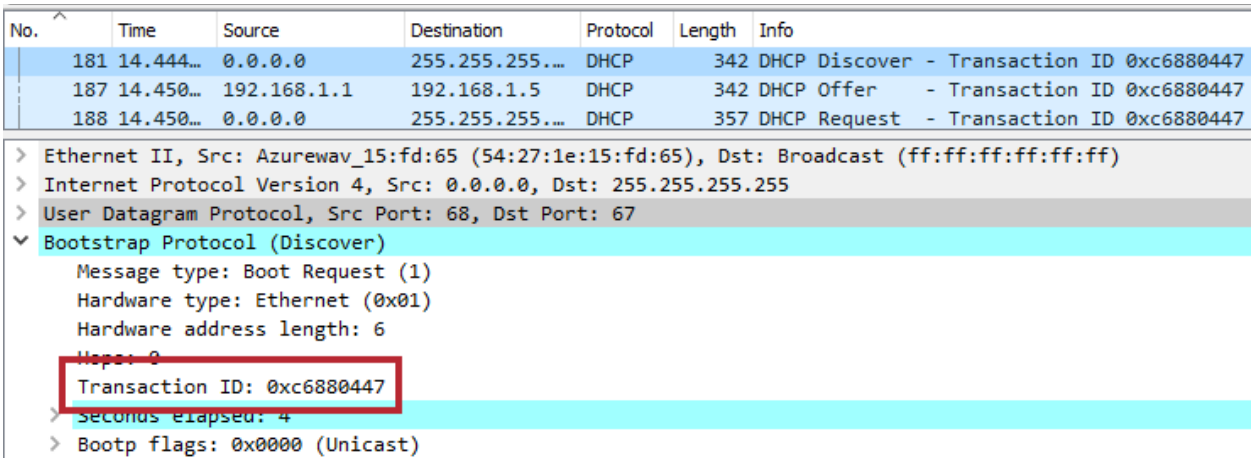
4. What values in the DHCP Discover message differentiate this message from the DHCP Request message?
   - DHCP Message Type
   - Request has DHCP Server Identifier
   - Request has Client Fully Qualified Domain Name


181 14.444… 0.0.0.0 255.255.255.… DHCP 342 DHCP Discover - Transaction ID 0xc6880447
187 14.450… 192.168.1.1 192.168.1.5 DHCP 342 DHCP Offer - Transaction ID 0xc6880447
188 14.450… 0.0.0.0 255.255.255.… DHCP 357 DHCP Request - Transaction ID 0xc6880447
189 14.457… 192.168.1.1 192.168.1.5 DHCP 590 DHCP ACK - Transaction ID 0xc6880447
452 18.769… 192.168.1.5 192.168.1.1 DHCP 345 DHCP Request - Transaction ID 0x347671ff
User Datagram Protocol, Src Port: 68, Dst Port: 67
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xc6880447
Seconds elapsed: 4
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: Azurewav_15:fd:65 (54:27:1e:15:fd:65)
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
Option: (12) Host Name
Option: (60) Vendor class identifier
Option: (55) Parameter Request List
Option: (255) End
Padding: 0000000000

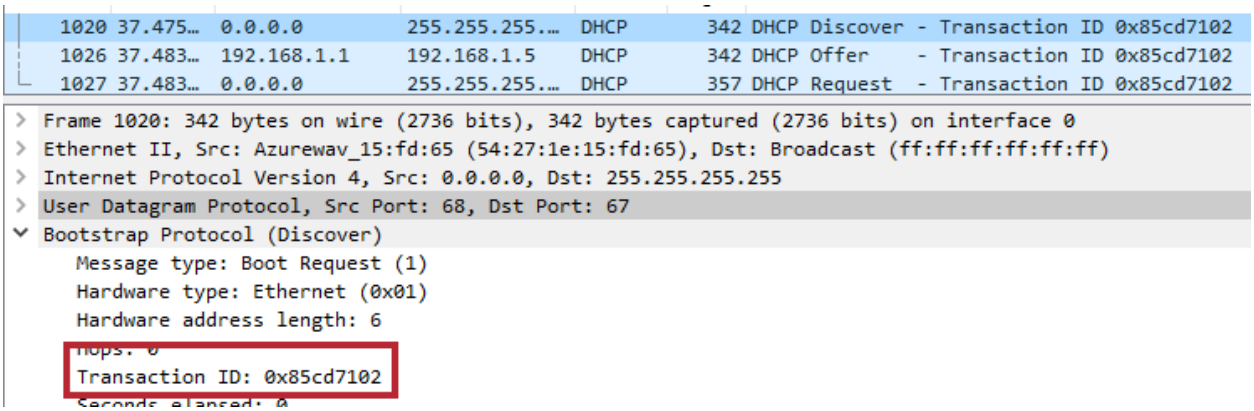


5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set of DHCP messages? What is the purpose of the Transaction-ID field?

All the four DHCP messages have the same Transaction ID: **0xc6880447**.



The second set of DHCP messages all have the same Transaction ID: **0x85cd7102**.



The Transaction ID field is different from each set of messages so that the host can differentiate different requests.

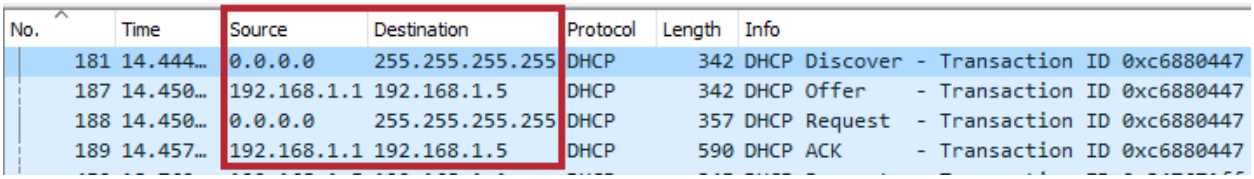
6. A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange. If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

Discover: 0.0.0.0 -> 255.255.255.255

Offer: 192.168.1.1 -> 192.168.1.5

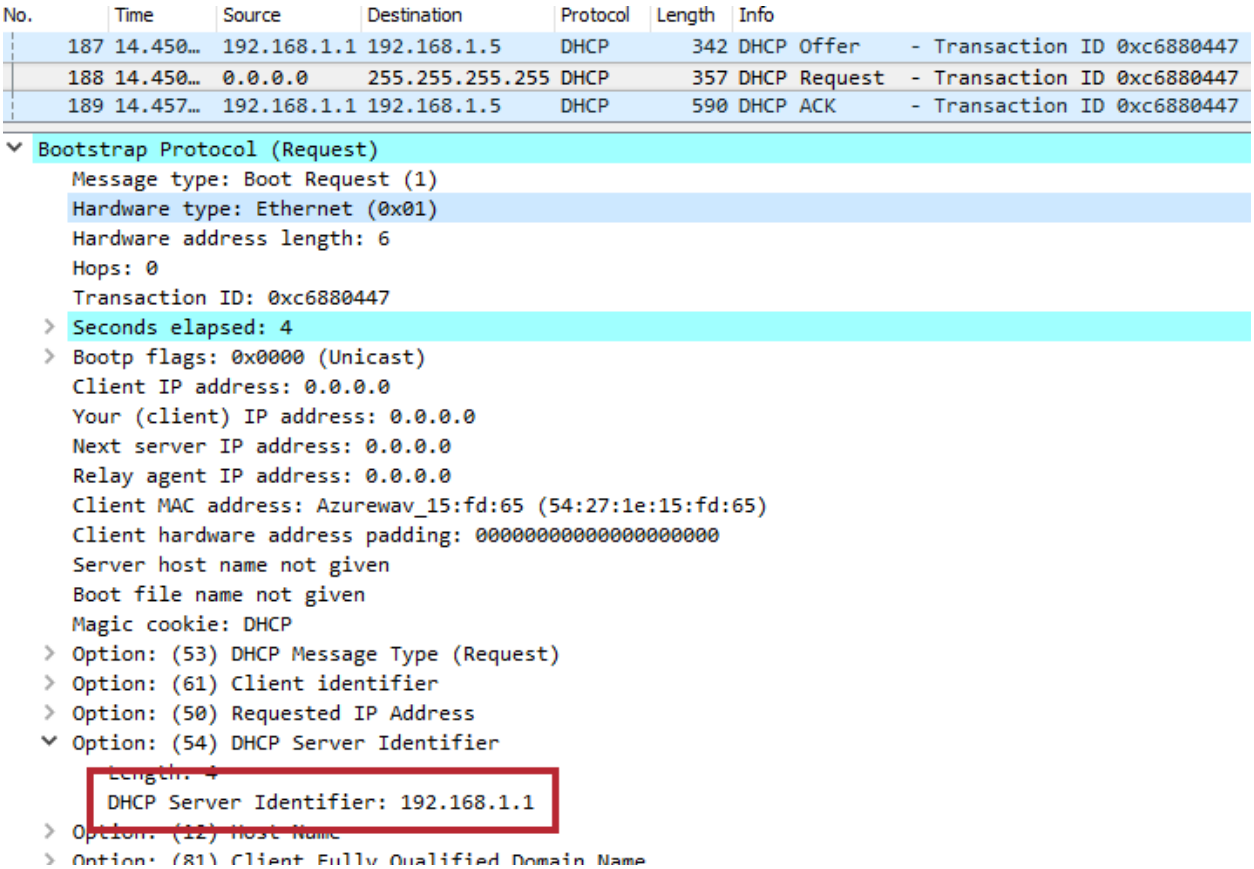
Request: 0.0.0.0 -> 255.255.255

ACK: 192.168.1.1 -> 192.168.1.5



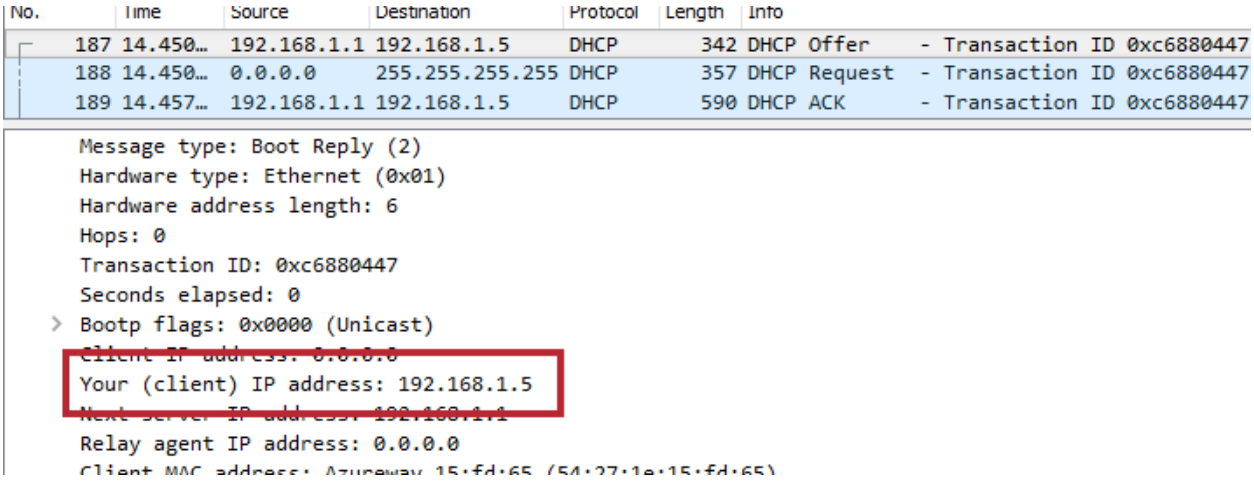
7. What is the IP address of your DHCP server?

The IP address of my DHCP server is **192.168.1.1**.



8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

The IP address that the DHCP server is offering to my host is **192.168.1.5**.

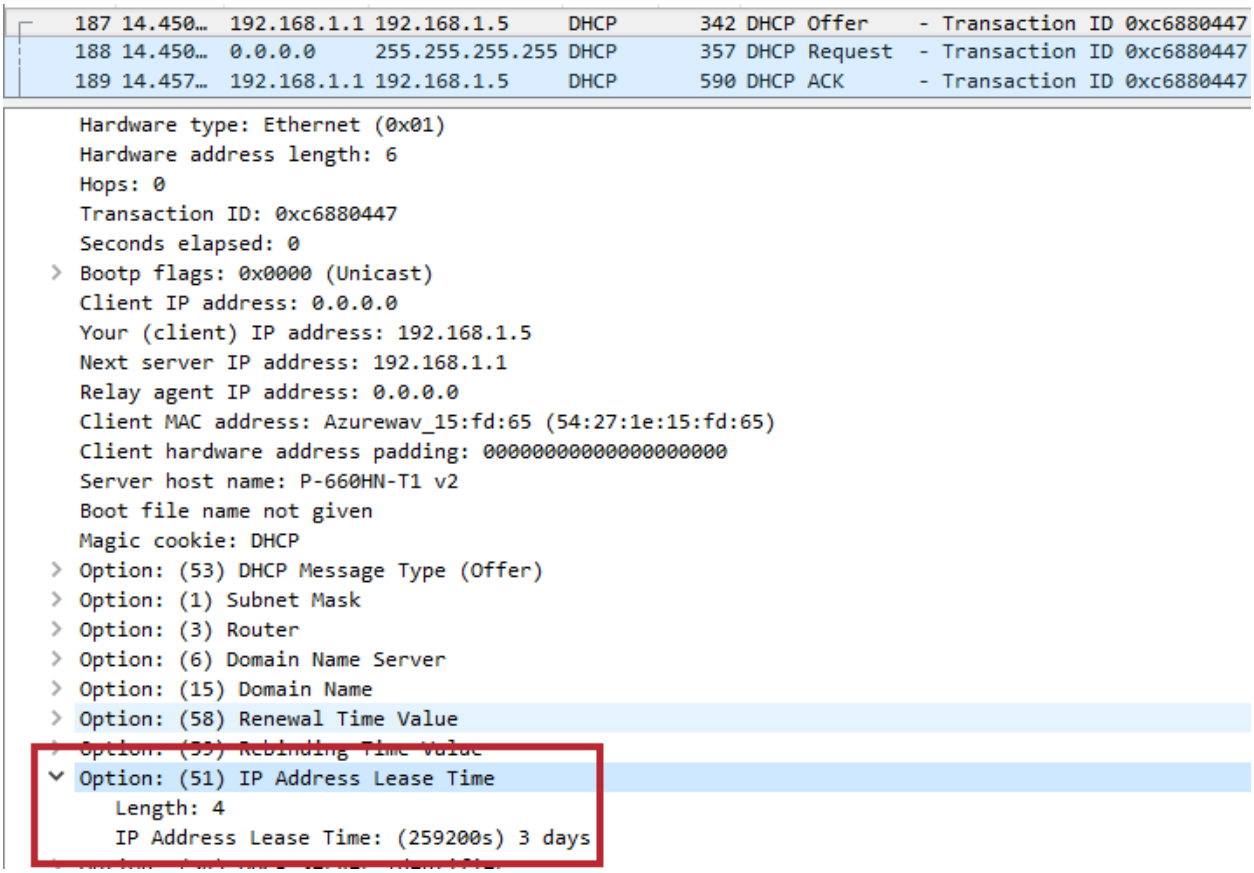


9. Is there a relay agent between the host and the DHCP server? If yes, what is the IP address of the relay agent? If none, how did you know there is none?

10. Explain the purpose of the router and subnet mask lines in DHCP offer message.
11. Explain the purpose of the lease time. How long is the lease time in your experiment?

The purpose of the least time is to tell the client how long it can use the IP address until it is reassigned a new IP address.

The lease time in my experiment is **2959200 seconds or 3 days**.



12. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgement of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

The purpose of the DHCP release message is to release the IP address back to the server.

There is no acknowledgement from the DHCP server that the DHCP request has been received.

If the message is lost, the client releases the IP address, but the server will not reassign that address until the client's lease on the address expires.

13. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet exchange period? If so, explain the purpose of those ARP packets.

Yes, there were ARP packets sent.

The purpose of these ARP packets are used to recognize and find the IP addresses of other machines in the network.