Andrew Becker

Professor Melissourgos

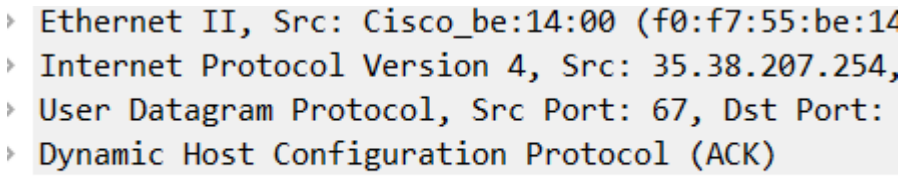
10/25/23

CIS 337 01

Wireshark Lab:

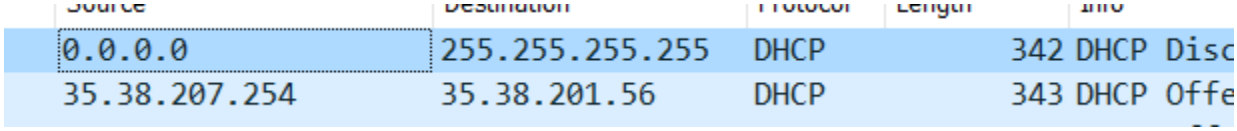
DHCP v8.1

1. Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?



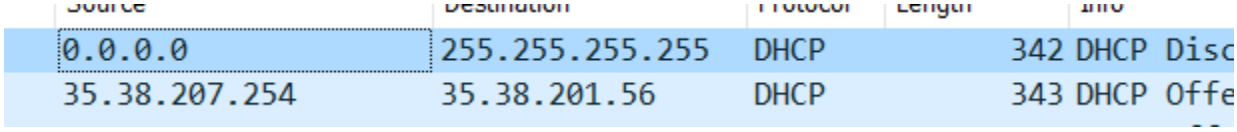
UDP

2. What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.



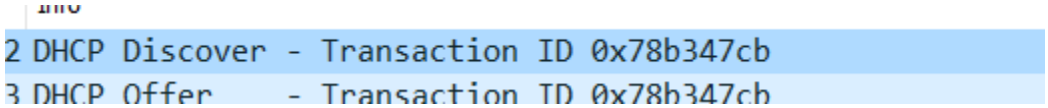
0.0.0.0. defines an IP block containing all possible IP addresses

3. What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.



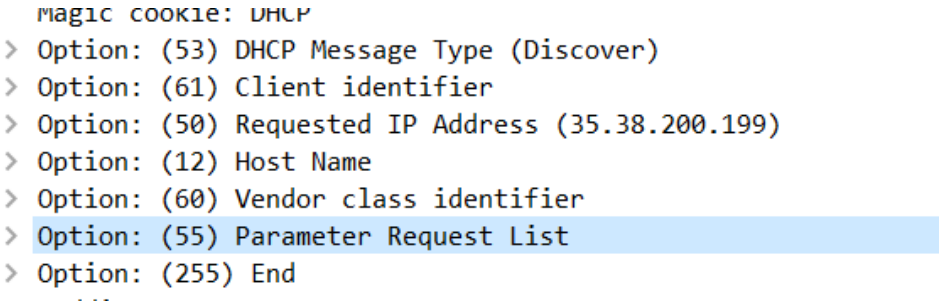
255.255.255.255 it is a "local broadcast," instructing any IP stack seeing that address to process the packet locally.

4. What is the value in the transaction ID field of this DHCP Discover message?



0x78b347cb

5. Now inspect the options field in the DHCP Discover message. What are five pieces of information (beyond an IP address) that the client is suggesting or requesting to receive from the DHCP server as part of this DHCP transaction?



DHCP message type, Client identifier, Hostname, Vendor class identifier, Parameter request list

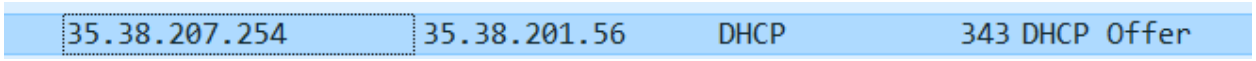
6. How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-5 above?

The transaction ID in this DHCP OFFER is the same as the transaction ID that was used for the earlier DHCP DISCOVER message

7. What is the *source* IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain.

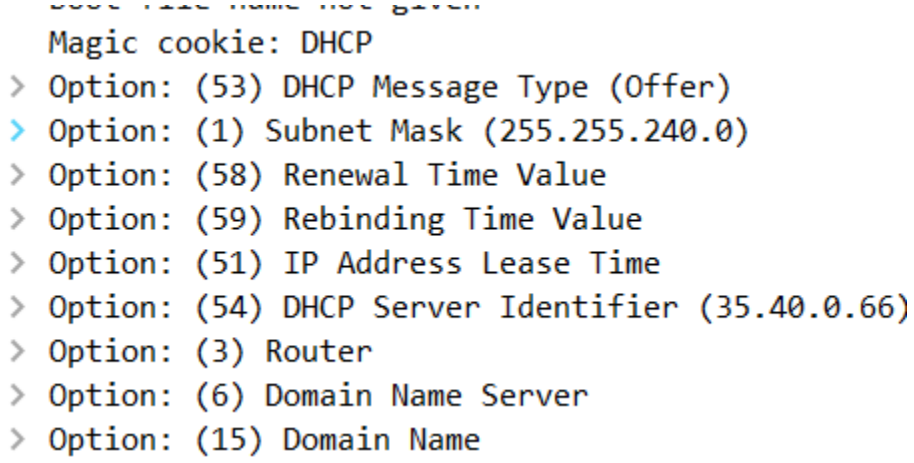
35.38.201.56 ; This was the IP that was given to us by the DHCP server

8. What is the *destination* IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain. [If you really want to dig into this, consult the DHCP RFC, page 24.]



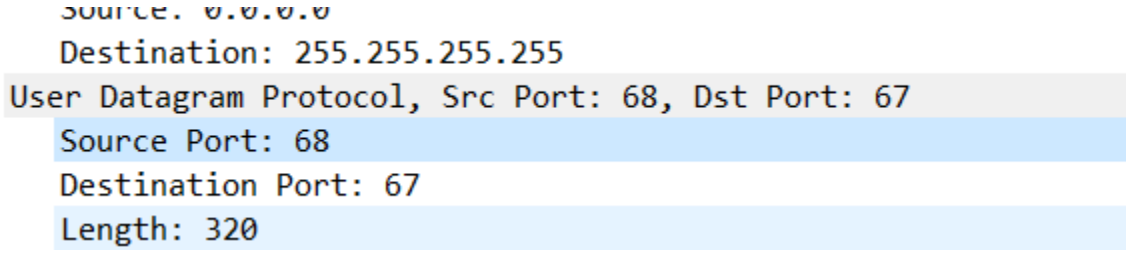
35.38.207.254 ; This is the domain server that is giving us our IP address

9. Now inspect the options field in the DHCP Offer message. What are five pieces of information that the DHCP server is providing to the DHCP client in the DHCP Offer message?



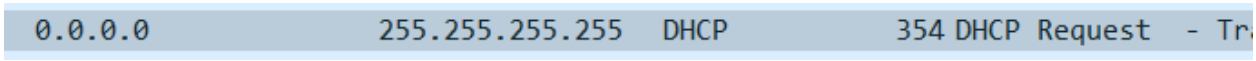
Subnet mask, Renewal Time Value, IP address lease time, DHCP server identifier, Domain name server

10. What is the UDP source port number in the IP datagram containing the first DHCP Request message in your trace? What is the UDP destination port number being used?



Source Port: 68, Destination port: 67

11. What is the source IP address in the IP datagram containing this Request message? Is there anything special about this address? Explain.

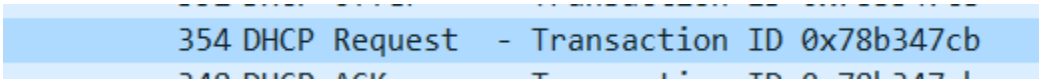


0.0.0.0. defines an IP block containing all possible IP addresses

12. What is the destination IP address used in the datagram containing this Request message. Is there anything special about this address? Explain.

255.255.255.255 it is a “local broadcast,” instructing any IP stack seeing that address to process the packet locally.

13. What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages?



Yes the transaction ID is the same as the Discover and Offer messages

14. Now inspect the options field in the DHCP Discover message and take a close look at the “Parameter Request List”. The DHCP RFC notes that“The client can inform the server which configuration parameters the client is interested in by including the 'parameter request list' option. The data portion of this option explicitly lists the options requested by tag number.”

What differences do you see between the entries in the 'parameter request list' option in this Request message and the same list option in the earlier Discover message?

```
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (43) Vendor-Specific Information
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (119) Domain Search
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (252) Private/Proxy autodiscovery
```

The parameter request list is asking for the Subnet mask, router, Domain name server, domain name, perform router discovery, static route, vendor-specific information, NetBIOS over TCP/IP Name Server, NetBIOS over TCP/IP Node type, NetBIOS over TCP/IP Scope, Domain search, classless static route

15. What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.

```
35.38.207.254    35.38.201.56    DHCP    348 DHCP ACK    - T
```

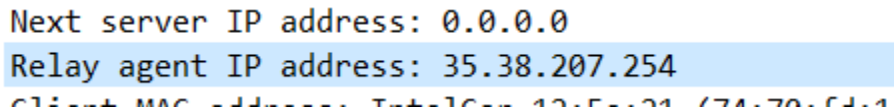
35.38.201.56, This is the IP we were given for the OFFER message

16. What is the destination IP address used in the datagram containing this ACK message. Is there anything special about this address? Explain.

```
35.38.207.254    35.38.201.56    DHCP    348 DHCP ACK    - T
```

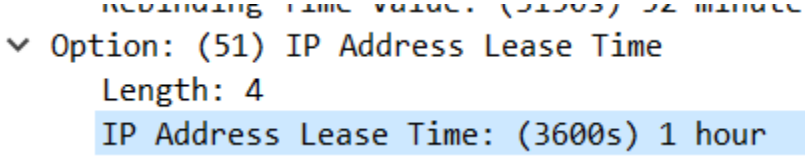
35.38.207.254, This is the same destination server address that offered the IP to us

17. What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address?



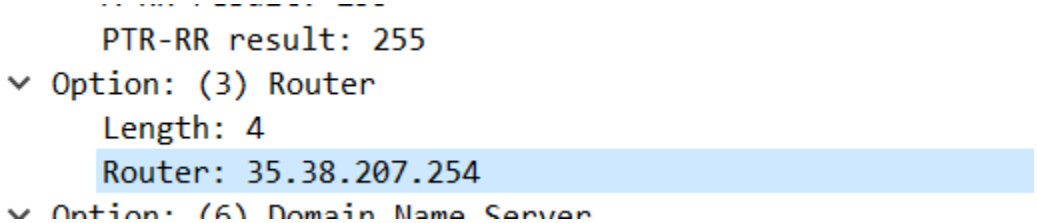
Relay agent IP address: 35.38.207.254

18. For how long a time (the so-called “lease time”) has the DHCP server assigned this IP address to the client?



1 Hour

19. What is the IP address (returned by the DHCP server to the DHCP client in this DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet?



35.38.207.254