Aaron Dardik

Lab 1

EE450

Abstract: In this lab we investigate Dynamic Host Configuration Protocol (DHCP) and gain experience with the WireShark application. We investigate the Discover-Offer-Request-ACK sequence of communications and learn how the server assigns a temporary IP to the client. Additionally, we gain experience with understanding packets and analyzing their contents.

1 ) The DHCP payload is being sent using the UDP transport protocol.

A close-up of a sign

Description automatically generated with low confidence

2) The source IP address is 0.0.0.0 which indicates that it is a placeholder IP for “this host.”

A screenshot of a computer

Description automatically generated with medium confidence

3) The destination IP used in the datagram containing the discover message is 255.255.255.255. This represents the broadcast address, or place to send messages to every device on the network.

A screenshot of a computer

Description automatically generated with low confidence

4) The transaction ID field contains the hexadecimal 0x9108eafb.

A picture containing text, screenshot, font, line

Description automatically generated

5) An additional 5 pieces of information that the client is requesting from the DHCP are: DHCP message type, client identifier, host name, vendor class identifier and parameter request list.

A screenshot of a computer

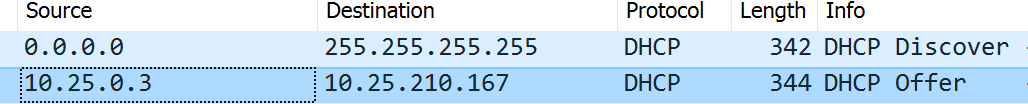
Description automatically generated with medium confidence

6) The ‘Offer’ message is in response to the ‘Discovery’ message sent. We know this as the DHCP protocol has 4 steps – the first is the discovery step and this is followed by the offer step. By knowing the protocol we know that this ‘offer’ is in response to ‘discovery.’ Additionally as the client listens on port 68, and the ‘Offer’ message lists the destination port as 68 we know the message is being sent to the client.

A screenshot of a computer screen

Description automatically generated with low confidence

7) The source IP address in the ‘Offer’ message is 10.25.0.3 which signifies ‘no unique collection / private network.’



8) As the broadcast bit is cleared to 0, the message should be sent to the IP address specified in the ‘yiaddr’ field – as stated in the DHCP RFC. This address is 10.25.210.167 which is in a private non-routable range.

A picture containing text, font, screenshot, number

Description automatically generated

9) The DHCP server provides the client with information including: DHCP message type, DHCP server identifier, subnet mask, router and domain name server.

A screenshot of a computer

Description automatically generated

10) The destination port in the first DHCP request message in the trace is port 67. The source port is 68.

A picture containing text, font, white, typography

Description automatically generated

11) The source IP address in the IP datagram containing the request message is 0.0.0.0 which is the default / placeholder IP address for “this host.”



12) The destination IP used in the datagram containing the request message is 255.255.255.255. This represents the broadcast address, or place to send messages to every device on the network.



13) For the request message the Transaction ID is 0x9108eafb which is the same as the Transaction ID for the Discover and Offer messages.

A picture containing text, font, screenshot, line

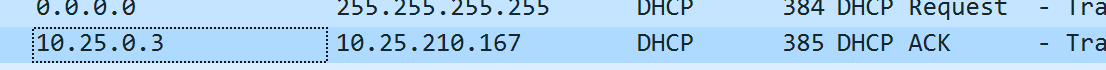
Description automatically generated

14) In the earlier “Discover” message, the parameter request list is, by tag number: (1), (3), (6), (15), (31), (33), (43), (44), (46), (47), (119), (121), (249), (252). This is the same as the ‘parameter request list’ here in the Request message.

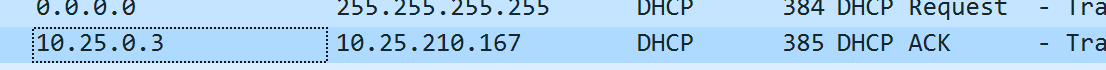
A screenshot of a computer screen

Description automatically generated with low confidence

15) The source IP address for the datagram containing the ACK message is 10.25.0.3 which represents ‘no unique location / private network.’



16) The destination IP for this ACK message is 10.25.210.167 which is in a private non-routable range. This is the same as the destination address used in the Offer Message as this is the address the server has provided for the client (us).



17) Your (client) IP address.

A picture containing text, font, screenshot, white

Description automatically generated

18) The IP address lease time is 30 minutes.

A picture containing text, font, screenshot, white

Description automatically generated

19) The IP address of the first hop router is 10.25.0.3. Wireshark calls this the ‘Relay Agent IP Address’ which connects DHCP packets between clients and servers not on the same physical subnet.

A screen shot of a computer

Description automatically generated with low confidence