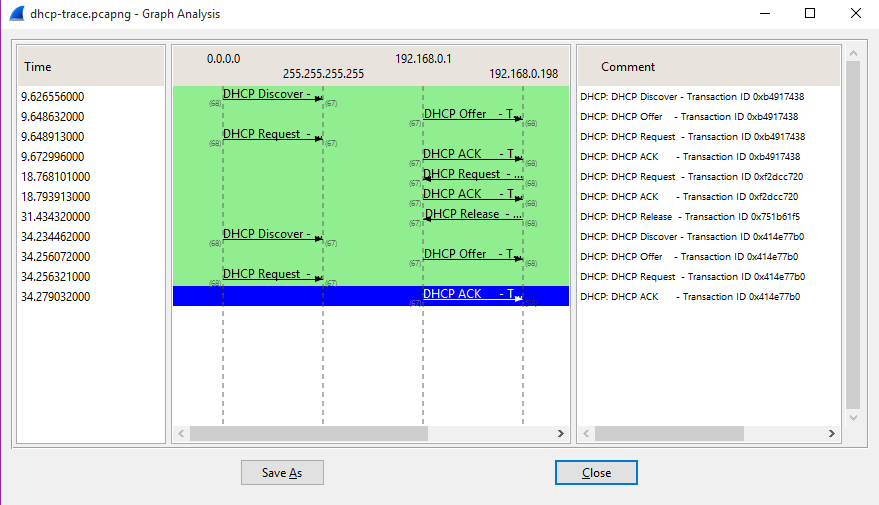
Wireshark Lab: DHCP

Brent Berghmans 1334252

**1. Are DHCP messages sent over UDP or TCP?**

The DHCP messages are being sent over UDP.

**2. Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?**



|  |  |  |
| --- | --- | --- |
| **DHCP Sequence** | **Source Port** | **Destination Port** |
| Discover | 68 | 67 |
| Offer | 67 | 68 |
| Request | 68 | 67 |
| Ack | 67 | 68 |

These ports are the same as the ports in the assignment trace.

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

The link-layer address of my host is: *bc:85:56:a0:a2:e9*

**4. What values in the DHCP discover message differentiate this message from the DHCP request message?**

|  |  |  |
| --- | --- | --- |
| **Option Number** | **DHCP Discover** | **DHCP Request** |
| 53 | DHCP: Discover (1) | DHCP: Request (3) |
| 54 | / | DHCP Server Identifier:  192.168.0.1 |
| 81 | / | Flags 0x00  A-RR result: 0  PTR-RR result: 0  Client name: pc |

**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 (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?**

The transaction ID of the first 4 DHCP messages is: 0xb4917438

The transaction ID of the second set DHCP messages is: 0xf2dcc720

I assume the purpose of this transaction ID field is to differentiate the different sets of requests, because of the underlying layer being UDP, there is no stream, they are just “random” packets coming from somewhere. So to know which packet belongs to which “set” we need some sort of identification, that identification is being provided by the transaction-id field.

**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 DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.**

|  |  |  |
| --- | --- | --- |
| **Message No.** | **Source** | **Destination** |
| 153 | 0.0.0.0 | 255.255.255.255 |
| 154 | 192.168.0.1 | 192.168.0.198 |
| 155 | 0.0.0.0 | 255.255.255.255 |
| 156 | 192.168.0.1 | 192.168.0.198 |

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

The IP address of my DHCP server is 192.168.0.1

**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 server offers me the IP address 192.168.0.198 in the DHCP Offer message

Option: (t=53,l=1) DHCP Message Type = DHCP Offer

**9. In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?**

My relay agent’s IP is 0.0.0.0, this indicates that there is no relay agent active.

**10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.**

The subnet mask tells which subnet is available, the router line defines what IP address should be used to make connection to the internet.

**11. In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client’s response to the first server OFFER message, does the client accept this IP address? Where in the client’s RESPONSE is the client’s requested address?**

In the client Request response message, option 50 defines the IP address that the client is requesting. In my case, this IP address is the same as the one in the DHCP offer.

This is also the case in the assignment trace.

**12. Explain the purpose of the lease time. How long is the lease time in your experiment?**

The lease time in my experiment was 1 hour.

The purpose of the lease time is that IP addresses that aren’t being used anymore, automatically get released. If we would not do this every requested IP address will stay occupied and eventually all the IP addresses will be used up.

**13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment 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 that is currently in use. It frees up this IP address so it can be used in future DHCP requests.

There is no acknowledgement for an release. If a DHCP release message was lost, the IP address will not be released until the lease time has timed out.

**14. 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**

No there were no ARP packets sent during a DHCP exchange period, only before and after packet-exchange periods.