Wireshark Lab 1 —— DHCP

Kangyan XU

Brief Abstract

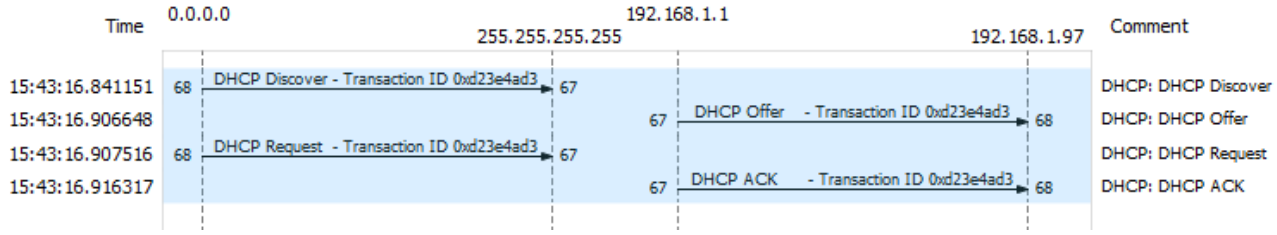
This report analyzes the process of a host getting its own IP address from a DHCP server, using the Wireshark. This report also includes the answers to some detailed questions on DHCP.

Questions

1. Are DHCP messages sent over UDP or TCP?

A: UDP. Without knowing the server, TCP handshake cannot be processed.

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?



A: Each packet's source and destination port numbers are labeled in the datagram (67 and 68). The port numbers are same because in DHCP, both client side and server side are well-known port number.

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

A: Client MAC address.

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

A: As mentioned in RFC 2131, chp3, "DHCP Message Type" option must be included in every message and define the type. Type 1 is referred to the discover message and type 3 is referred to the request message.

```
▾ Option: (53) DHCP Message Type (Discover)
      Length: 1
      DHCP: Discover (1)
```

```
▾ Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
```

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?

A:
The four messages have Transaction ID: 0xd23e4ad3

```
Transaction ID: 0xd23e4ad3
```

The second set has Transaction ID: 0x1d3e3a96

```
Transaction ID: 0x1d3e3a96
```

According to the definition in RFC 2131, Transaction ID is used to associate messages and responses between a client and a server.

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.

No.	Time	Source	Destination	Protocol	Length	Info
84	15:43:16.841151	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover
85	15:43:16.906648	192.168.1.1	192.168.1.97	DHCP	342	DHCP Offer
86	15:43:16.907516	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request
87	15:43:16.916317	192.168.1.1	192.168.1.97	DHCP	342	DHCP ACK

A: Use 0.0.0.0 cause not knowing its IP, use 255.255.255.255 to broadcast.
Source and destination IP addresses are labeled in the snapshot above.

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

A: 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.

A: 192.168.1.97
In DHCP Offer and DHCP ACK:

```
Your (client) IP address: 192.168.1.97
```

In DHCP Request:

```
Option: (50) Requested IP Address (192.168.1.97)
    Length: 4
    Requested IP Address: 192.168.1.97
```

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?

A: Relay agent IP address is 0.0.0.0
There is no relay agent in my experiment.

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

A: According to A Top-Down Approach, chp4.4, this allows a host to learn its subnet mask and the address of its first-hop router (often the default gateway).

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?

A: No.

```
Option: (50) Requested IP Address (192.168.1.97)
    Length: 4
    Requested IP Address: 192.168.1.97
```

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

A: The lease time is used to determine how long the IP address will be valid.

```
Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (259200s) 3 days
```

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?

A: To return the client's allocated IP address.
There is no acknowledgement.
If the message is lost, the server will take back the address when the lease time is over.

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.	Time	Source	Destination	Protocol	Length	Info
83	15:43:16.794557	Sagemcom_a2:	Broadcast	ARP	60	Who has 192.168.1.97? Tell 192.168.1.1
84	15:43:16.841151	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xd23e4ad3
85	15:43:16.906648	192.168.1.1	192.168.1.97	DHCP	342	DHCP Offer - Transaction ID 0xd23e4ad3
86	15:43:16.907516	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xd23e4ad3
87	15:43:16.916317	192.168.1.1	192.168.1.97	DHCP	342	DHCP ACK - Transaction ID 0xd23e4ad3
90	15:43:16.923642	Dell_a0:	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.97

A: No ARP packets sent or received during the DHCP packet-exchange period.

There is high probability that the timeline regarding to ARP is in wrong order. So the purpose of these frequent ARPs could be getting other side's MAC address so that the broadcast is not needed and unicast is applied during the DHCP packet-exchange period.

Conclusion

The process that a host obtains its IP address from the DHCP server is well illustrated in the Wireshark. The DHCP packet-exchange includes four steps: discovery, offer, request and acknowledgement, the transaction ID does not change in this period. The host does not accept the IP address offered by DHCP server immediately, only after another request and acknowledgement process, the IP address can be settled, meanwhile a lease time is set in the acknowledgement.

The Wireshark is a good tool to analyze, the flow graph is clear, the details of the packets also very complete.

Screen Shots

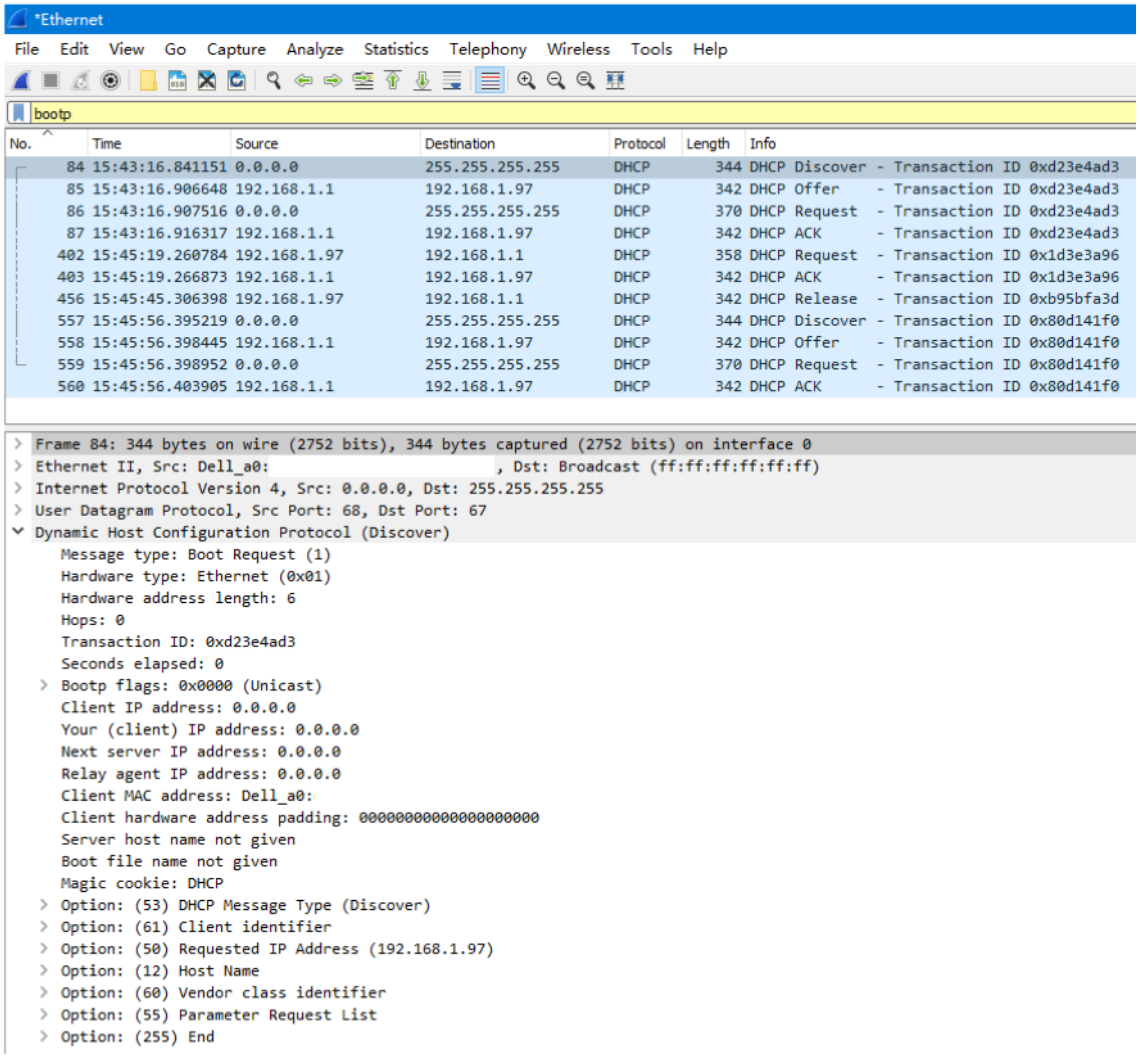


Figure1 Wireshark Window showing DHCP Discover Message

Sept.23 2019