CS 315: Computer Networks Lab
Spring 2023-24, IIT Dharwad
Assignment-9

Wireshark Lab: DHCP

March 17, 2025

Lab Instructions

- Mark your attendance before leaving the lab.
- Handle the lab resources with utmost care.
- Please go through the following exercises in today's lab.
- It is recommended that you complete all the following exercises during the lab slot itself.
- If you face any difficulties, please feel free to seek help online or from your peers or TAs.
- After finishing all exercises, please carry your solutions with you (via email/pen drive) for future reference, and delete the files from the desktop.

Introduction

In this lab, we'll take a quick look at the Dynamic Host Configuration Protocol, DHCP. Recall that DHCP is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts, as well as to configure other network configuration information.

As we've done in earlier Wireshark labs, you'll perform a few actions on your computer that will cause DHCP to spring into action, and then use Wireshark to collect and then the packet trace containing DHCP protocol messages.

Part 0: Paste a screenshot of your system IP address, using `ipconfig` (on Windows) or `ifconfig` (on Mac and Linux), and fill out this Google form to submit the details of your system. The same system must be used to attempt all exercises of this lab.

Gathering a Packet Trace

In order to collect a trace that will contain all four DHCP message types, we'll need to take a few command line actions on a Mac, Linux or PC.

On a Mac:

1. In a terminal window/shell enter the following command:

```
% sudo ipconfig set en0 none
```

Where `en0` (in this example) is the interface on which you want to capture packets using Wireshark. You can easily find the list of interface names in Wireshark by choosing Capture->options. This command will de-configure network interface `en0`.

2. Start up Wireshark, capturing packets on the interface you de-configured in Step 1.
3. In the terminal window/shell enter the following command:

```
% sudo ipconfig set en0 dhcp
```

This will cause the DHCP protocol to request and receive an IP address and other information from the DHCP server.

4. After waiting for a few seconds, stop Wireshark capture.

On a Linux machine:

1. In a terminal window/shell, enter the following commands:

```
sudo ip addr flush en0
sudo dhclient -r
```

where en0 (in this example) is the interface on which you want to capture packets using Wireshark. You can easily find the list of interface names in Wireshark by choosing Capture -> Options. This command will remove the existing IP address of the interface, and release any existing DHCP address leases.

2. Start up Wireshark, capturing packets on the interface you de-configured in Step 1.
3. In the terminal window/shell, enter the following command:

```
sudo dhclient en0
```

where, as with above, `en0` is the interface on which you are currently capturing packets. This will cause the DHCP protocol to request and receive an IP address and other information from the DHCP server.

4. After waiting for a few seconds, stop Wireshark capture.

On a Windows:

1. In a command-line window enter the following command:

```
> ipconfig /release
```

This command will cause your PC to give up its IP address.

2. Start up Wireshark.

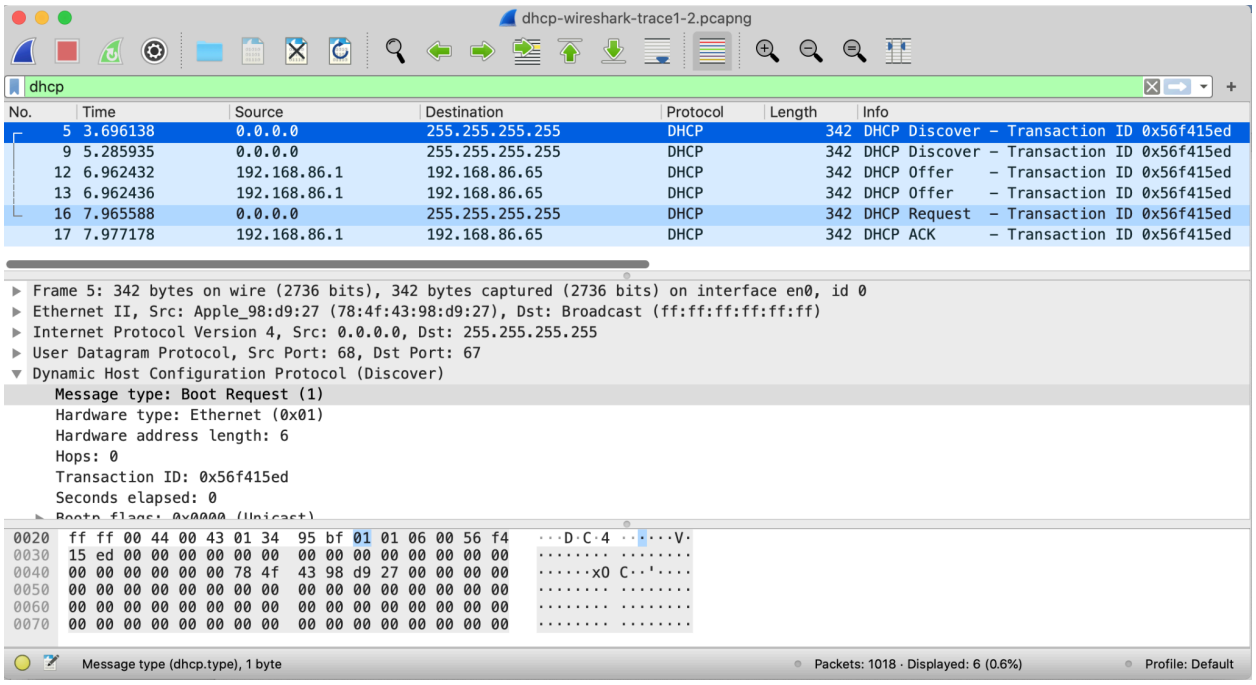
3. In the command-line window enter the following command:

   ```
   > ipconfig /renew
   ```

   This will cause the DHCP protocol to request and receive an IP address and other information from a DHCP server.

4. After waiting for a few seconds, stop Wireshark capture.

After stopping Wireshark capture in step 4, take a peek in your Wireshark window to make sure you've actually captured the packets that we're looking for. If you enter "dhcp" into the display filter field (as shown in the light green field in the top left of Figure 1), your screen (on a Mac) should look similar to Figure 1.



Part 1: DHCP Questions

1. What is the Transaction ID in a DHCP Discover message? Which system generates this identifier? What is its significance?

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

3. What are the source and destination IP addresses in a DHCP Discover message? Why are they this way?

4. What is the “Requested IP address” field in a DHCP Discover packet, and how does it impact the DHCP Offer?

5. What is the MAC address in the DHCP Discover packet, and why is it crucial in the DHCP process?

6. How do you know that this Offer message is being sent in response to the DHCP Discover message?

7. What is the client-assigned and next-hop IP address in the DHCP Offer packet, and how do they assist in routing?

8. Explain the Lease time, Renewal time, and Rebinding time in DHCP. How do they ensure IP continuity?

9. Which DHCP options are included in the 'Parameter Request Lists' of a DHCP Discover packet, and answered in the DHCP Offer packet?

10. In the DHCP Discover and Request packets, the client IP address is 0.0.0.0, so on what basis does the DHCP server know from where the request has been raised?

11. What is the broadcast IP address used in the DHCP communication, and why is it significant?

12. Which transport layer protocol and its standard port number is used for DHCP ACK message exchange?

13. What are the source and destination port numbers in DHCP ACK message?

14. What is unique about the source and destination IP addresses in the DHCP ACK message?

Submission Details

- Write your answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers (with screenshots, if necessary).

References

- https://superuser.com/questions/1614467/why-does-dhcp-server-prefer-unicasting-over-broadcasting-and-at-what-cost
- https://forum.networklessons.com/t/introduction-to-dhcp/970/71?u=lagapidis
- https://networkengineering.stackexchange.com/questions/11120/how-dhcp-offer-unicast-works?rq=1
- https://notes.networklessons.com/dhcp-offer-message-sent-as-broadcast