CS 315: Computer Networks Lab
Spring 2022-23, IIT Dharwad
Assignment-9
Wireshark Lab: DHCP
March 07, 2023

Lab Instructions

- Please leave your bags on the Iron shelf near the SP16 entrance.
- Login to the Ubuntu OS on your machine. The login credentials are as follows:
    - Username: user
    - Password: 123456
- Mark your attendance in the attendance sheet 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.

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.

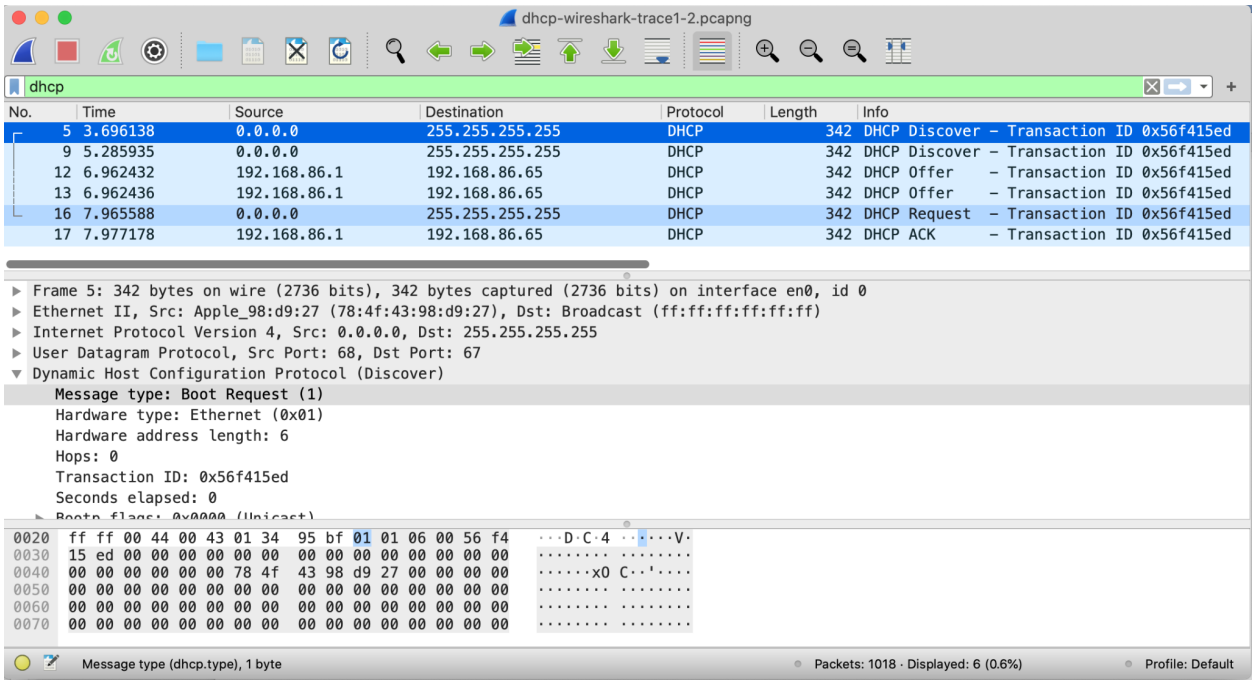
2. Start up Wireshark.
3. In the command-line window enter the following command:

```
> 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, you should 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.



DHCP Questions

Let's start by looking at the DHCP Discover message. Locate the IP datagram containing the first Discover message in your trace. Answer the following questions.

1. Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?
2. What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.

3. What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.
4. What is the value in the transaction ID field of this DHCP Discover message?
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?

Now let's look at the DHCP Offer message. Locate the IP datagram containing the DHCP Offer message in your trace that was sent by a DHCP server in the response to the DHCP Discover message that you studied in questions 1-5 above.

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

It would appear that once the DHCP Offer message is received, that the client may have all of the information it needs to proceed. However, the client may have received OFFERs from multiple DHCP servers and so a second phase is needed, with two more mandatory messages – the client-to-server DHCP Request message, and the server-to-client DHCP ACK message is needed. But at least the client knows there is at least one DHCP server out there! Let's take a look at the DHCP Request message, remembering that although we've already seen a Discover message in our trace, that is not always the case when a DHCP request message is sent.

Locate the IP datagram containing the first DHCP Request message in your trace, and answer the following questions.

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

Locate the IP datagram containing the first DHCP ACK message in your trace, and answer the following questions.

15. What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.
16. What is the destination IP address used in the datagram containing this ACK message. Is there anything special about this address? Explain.
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?
18. For how long a time (the so-called “lease time”) has the DHPC server assigned this IP address to the client?
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?

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).