School of Computer Science and Cybersecurity

CUC

Lab Report #

|  |  |
| --- | --- |
| Lab Name | Wireshark Lab5:DHCP |
| Course Name | Computer Networks |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | 赵婧宇 | Student ID | 201711123028 |

|  |  |
| --- | --- |
| Partners |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | 2019.06.18 | Lab Location | #48 |

|  |
| --- |
| Notes： |

**Section I Introduction**

Prepares the reader to understand the whole experiment.

|  |  |
| --- | --- |
| **Must Have:**  1. Clearly stated purpose of the experiment  2. Important background and/or theory | **May include:**  1. Description of specialized equipment  2. Justification of experiment's importance |

In this lab, we’ll take a quick look at DHCP. 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).

**Section II Methods & Materials**

Can be lists or even "refer to lab manual" where appropriate.

**Section III Procedure & Results**

Describes ACTUAL process, especially changes from planned method.

|  |
| --- |
| * **number** and **title** tables and graphs correctly and clearly * draw attention to key points in tables or graphs with a sentence * provide sample calculation only * state key result in sentence form |

**DHCP Experiment**

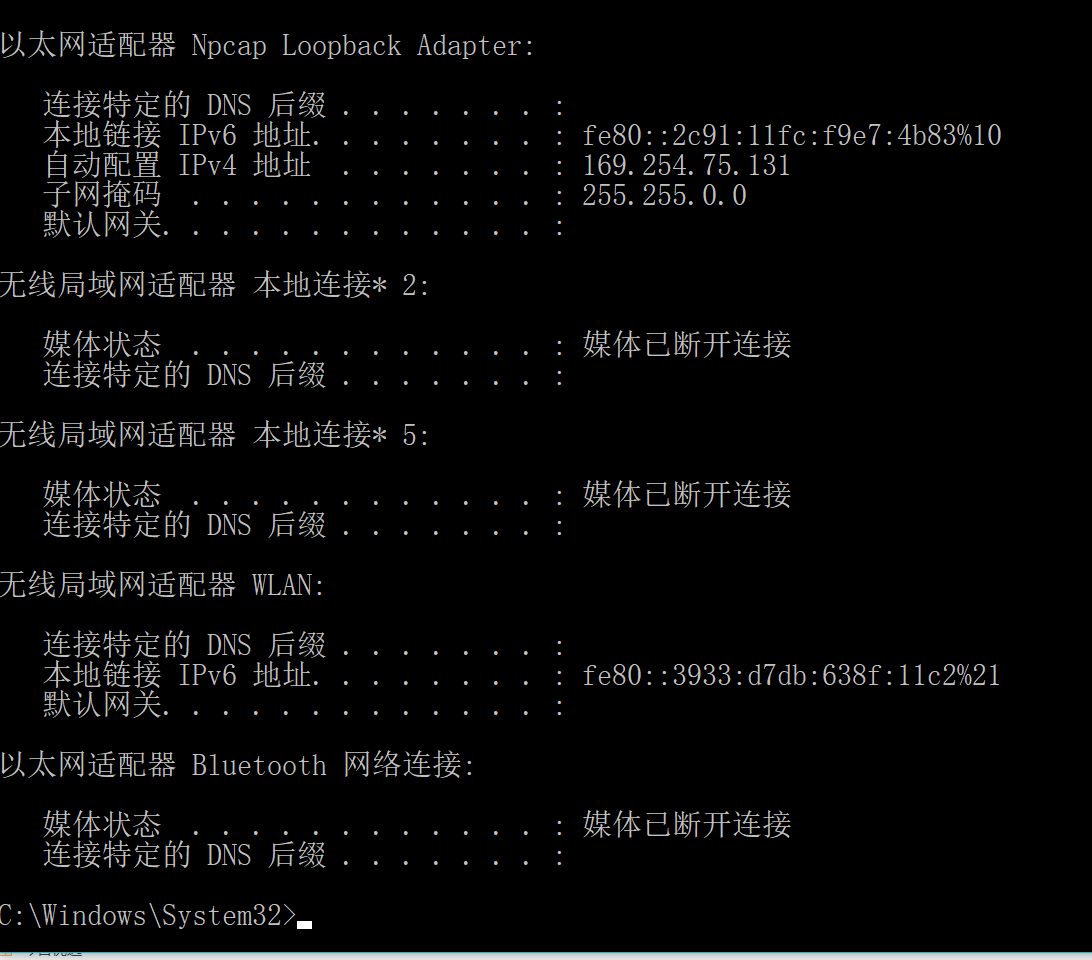
In order to observe DHCP in action, we’ll perform several DHCP-related commands and capture the DHCP messages exchanged as a result of executing these commands. Do the following:

Begin by opening the Windows Command Prompt application (which can be found in your

Accessories folder). As shown in Figure 1, enter “ipconfig /release”. The executable for

ipconfig is in C:\windows\system32. This command releases your current IP address, so that

your host’s IP address becomes 0.0.0.0.



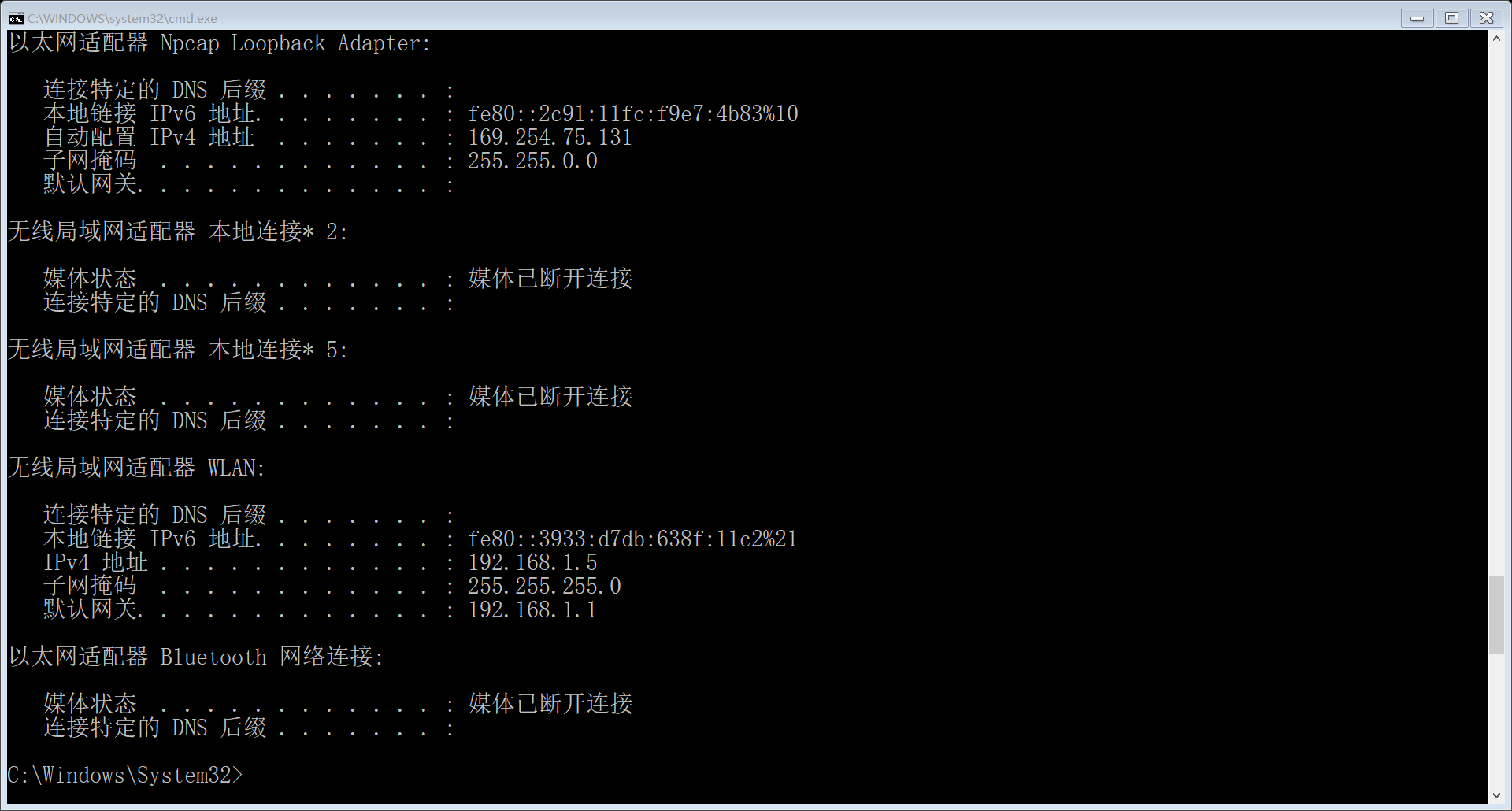
1. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and

begin Wireshark packet capture.

2. Now go back to the Windows Command Prompt and enter “ipconfig /renew”. This

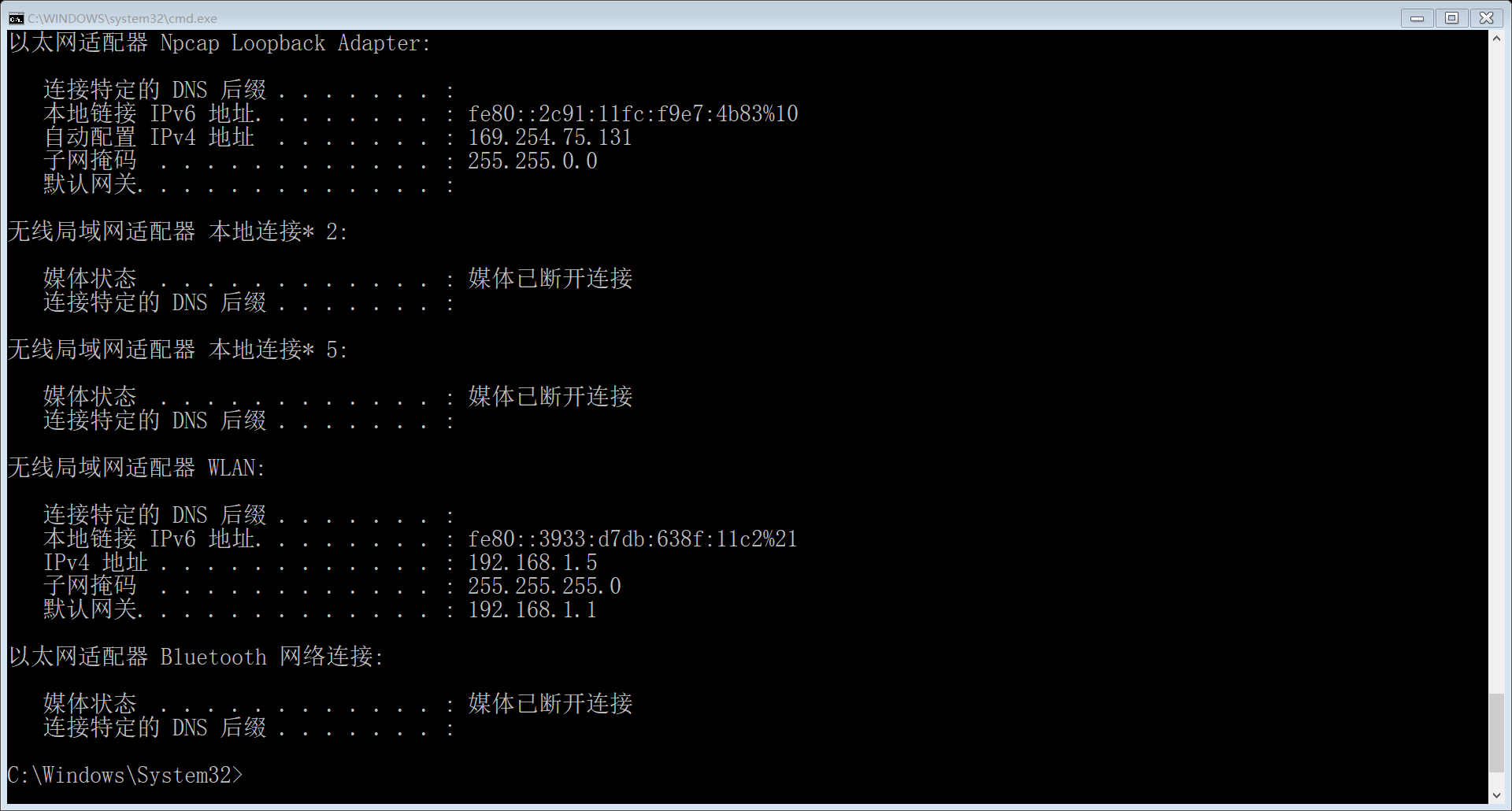
instructs your host to obtain a network configuration, including a new IP address. In

Figure 1, the host obtains the IP address 192.168.1.108



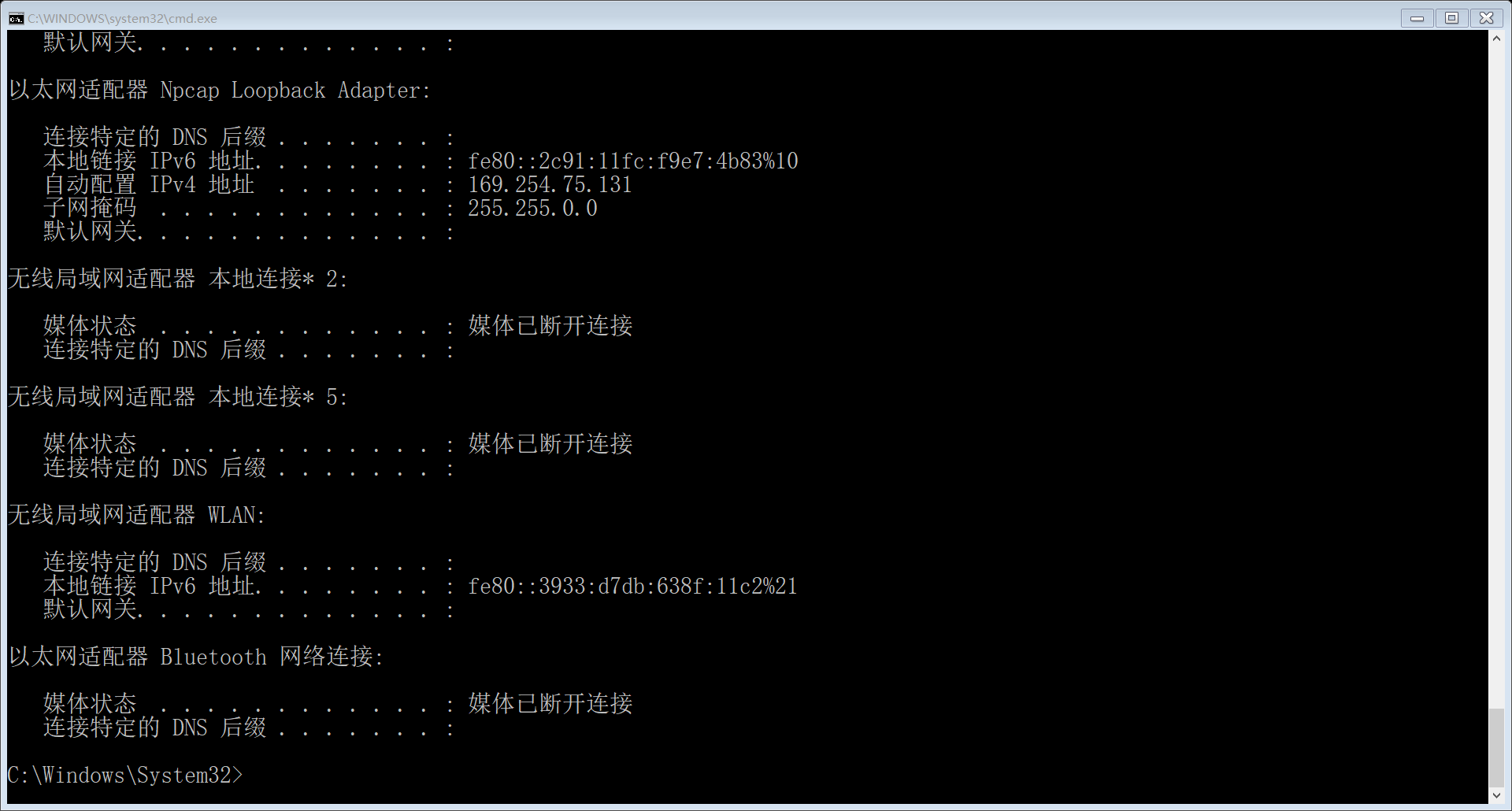
3. Wait until the “ipconfig /renew” has terminated. Then enter the same command

“ipconfig /renew” again.

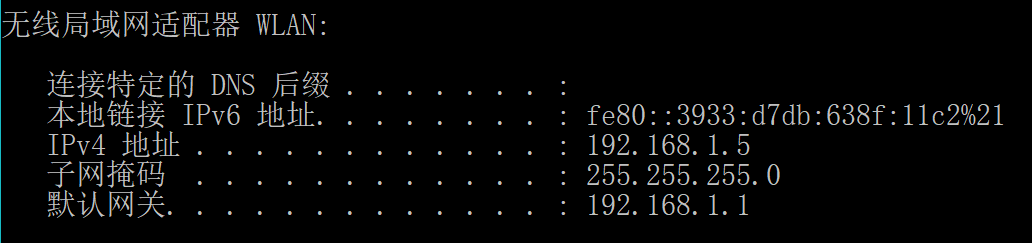


4. When the second “ipconfig /renew” terminates, enter the command “ipconfig/release” to

release the previously-allocated IP address to your computer.

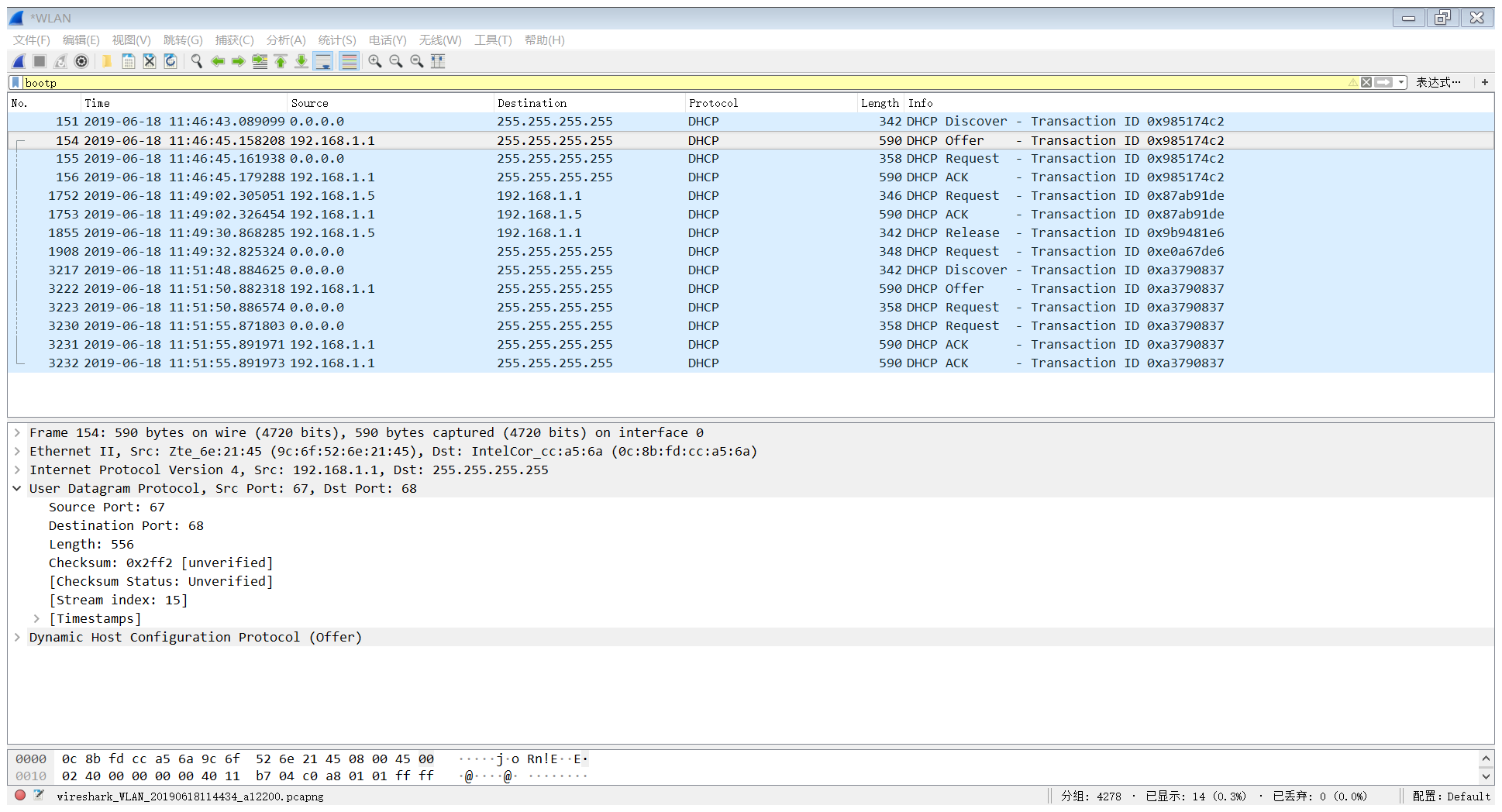


5. Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.



6. Stop Wireshark packet capture.

Now let’s take a look at the resulting Wireshark window. To see only the DHCP packets, enter into the filter field “bootp”. (DHCP derives from an older protocol called BOOTP. Both BOOTP and DHCP use the same port numbers, 67 and 68. To see DHCP packets in the current version of Wireshark, you need to enter “bootp” and not “dhcp” in the filter.) We see from Figure 2 that the first ipconfig renew command caused four DHCP packets to be generated: a DHCP Discover packet, a DHCP Offer packet, a DHCP Request packet, and a DHCP ACK packet.

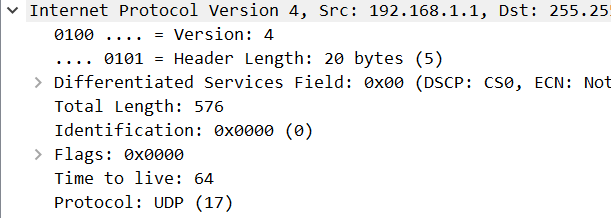


**Section IV Discussion**

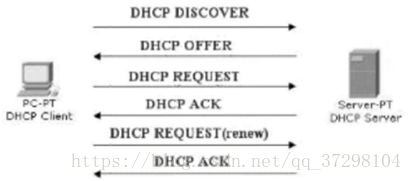
Answer the questions in the section [what to hand in] of the lab guide, includes two aspects:

1. Are DHCP messages sent over UDP or TCP?

Answer: Over UDP



1. 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?

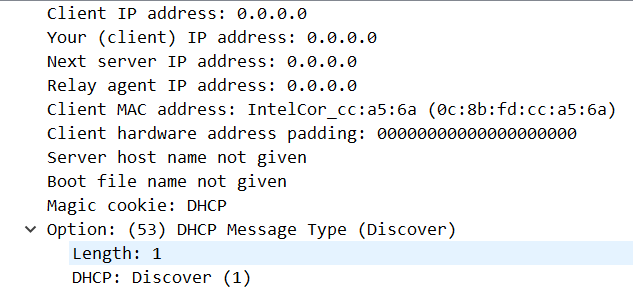


1. What is the link-layer (e.g., Ethernet) address of your host?



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

Answer: From DHCP Message Type.



1. 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?

Answer:

The Transaction-ID of the first four:

The second set:



Because DHCP data used to distinguish different groups

1. 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.

Answer: The broadcast method used by the IP datagram in the four message exchanges.

|  |  |  |
| --- | --- | --- |
|  | Source | Destination |
| Discover | 0.0.0.0 | 255.255.255.255 |
| Offer | 192.168.1.1 | 255.255.255.255 |
| Request | 0.0.0.0 | 255.255.255.255 |
| Ack | 192.168.1.1 | 255.255.255.255 |

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

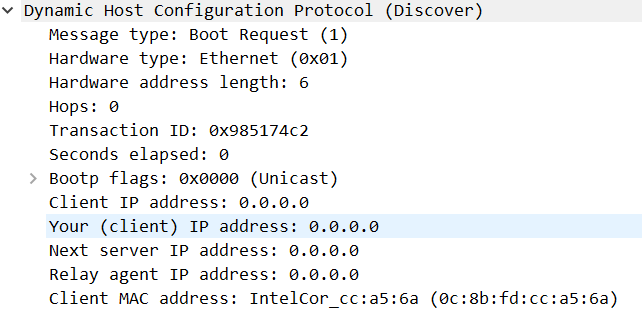
Answer: 192.168.1.1

1. 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.

Answer: 192.168.1.5. In the DHCP offer



1. 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?

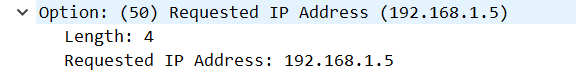
Answer: 0.0.0.0

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

Answer: When the client starts the IP configuration after receiving the last ACK, set the subnet mask and network administrator.

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?

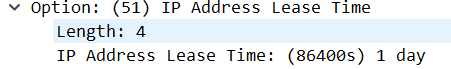
Answer: Request Address: 192.168.1.5



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

Answer: The unused IP address DHCP server needs to be recycled, because the IP address market is limited, so as to avoid the phenomenon of insufficient use of IP address.

My lease time is 1 day.

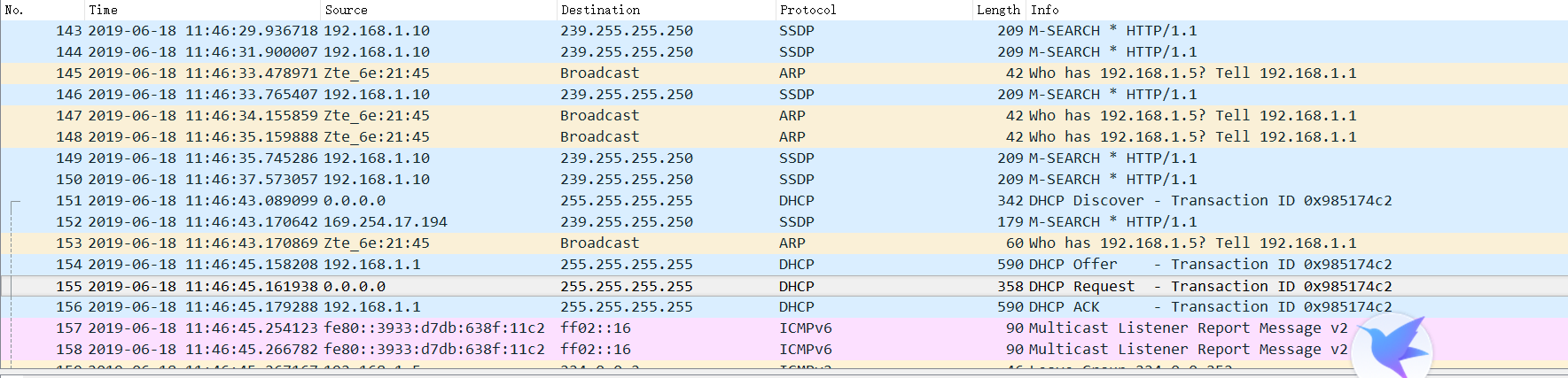


13. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?

Answer: The purpose of the DHCP release message is to release the leased IP address, and the DHCP server does not issue the receiving confirmation of the client DHCP request. If the release message is lost, the IP is reclaimed.

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.

Answer: ARP packets have been sent.



Broadcast to check if there are IP conflicts.

**Section V Conclusion**

States what is known as a result of the experiment.

|  |  |
| --- | --- |
| **Must do:**  1. State what's known  2. Justify that statement | **May do:**  1. State significance of findings  2. Suggest further research |

Release the current IP address, wireless network immediately interrupted.

Understand the process of DHCP IP address assignment.