**《计算机网络》Wireshark实验**





**Wireshark-DHCP**

**学 号 3020205015**

**姓 名 石云天**

**学 院 未来技术学院**

**专 业 计算机科学与技术**

**年 级 2020**

**任课教师 周晓波**

**2023 年 4 月 27日**

# 一、报告摘要

本次实验通过在Windows命令行输入ipconfig命令，捕获并分析通过WLAN接入校园网时的DHCP数据包的相关信息。实验结果说明，DHCP采用UDP进行数据传输，源端口号与目的端口号分别为68与67。DHCP Discover与DHCP Request报文通过DHCP Message Type字段进行区分，分别为1与3。Translation ID字段在DHCP连接建立过程中保持一致，用于区分不同的连接建立过程。在DHCP数据包中，源IP地址为0.0.0.0，目的IP地址为255.255.255.255或DHCP服务器的IP地址。本次实验中DHCP服务器的IP地址为172.23.0.1，DHCP Offer信息中分配给主机的IP地址为172.23.193.31.通过分析捕获到的DHCP数据包，可以了解到DHCP协议的相关特性与工作过程。此外，在本次实验中未发现中继代理的存在。

# 二、任务要求

1. Are DHCP messages sent over UDP or TCP?

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?

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

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

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?

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.

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

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.

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?

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

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?

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

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? which the measured data differs from the idealized behavior of TCP that we’ve studied in the text.

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.

# 三、实验结果与分析

首先根据实验要求，在Windows命令行下输入ipconfig相关命令，可以得到以下操作截图。（注：本次实验中为使用有线网接入校园网，因此本地连接断开，在实验过程中通过WLAN接入校园网，本次实验通过此条路径抓包与实验）抓包路径情况如下图1：

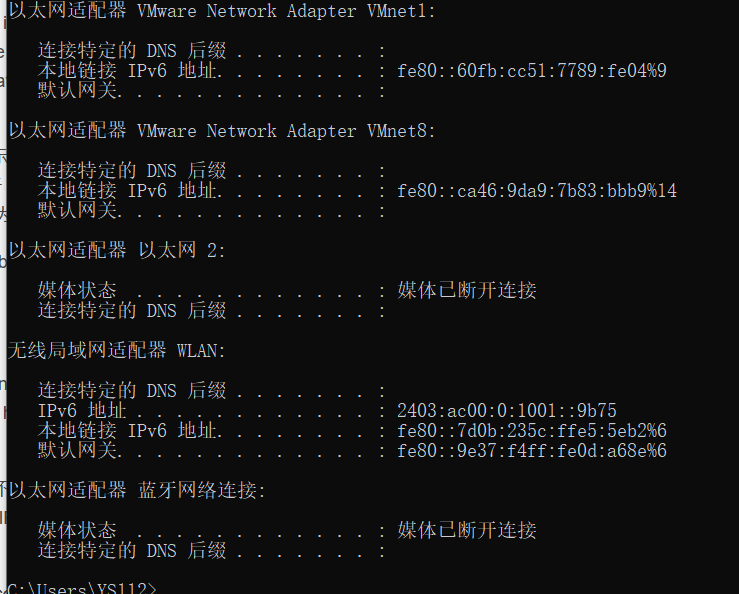


图1 抓包路径截图

接下来进行抓包，通过“bootp”进行筛选后得到以下捕获情况，见下图2：

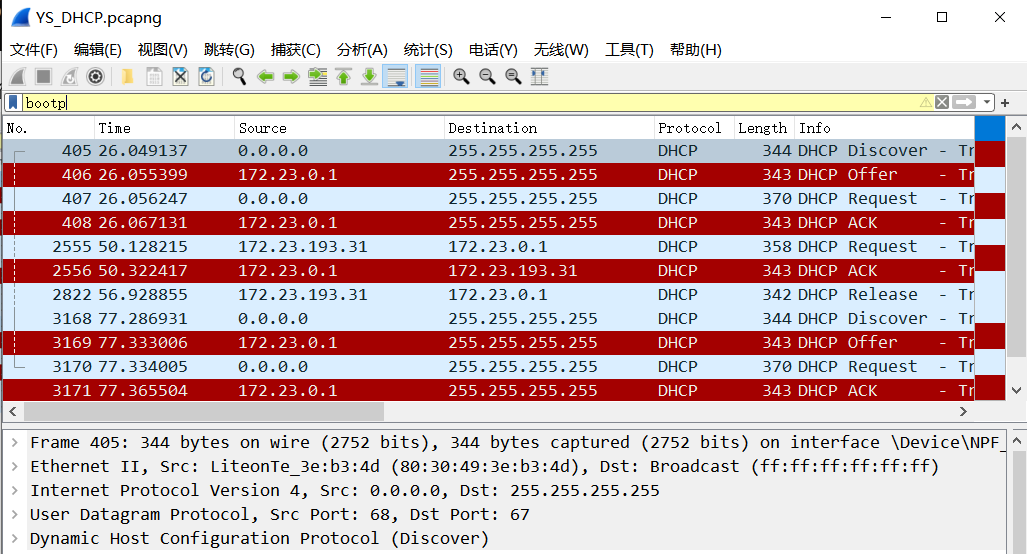


图2 捕获情况

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

DHCP采用UDP进行数据传输，理由见下图3（已用红色标注）：

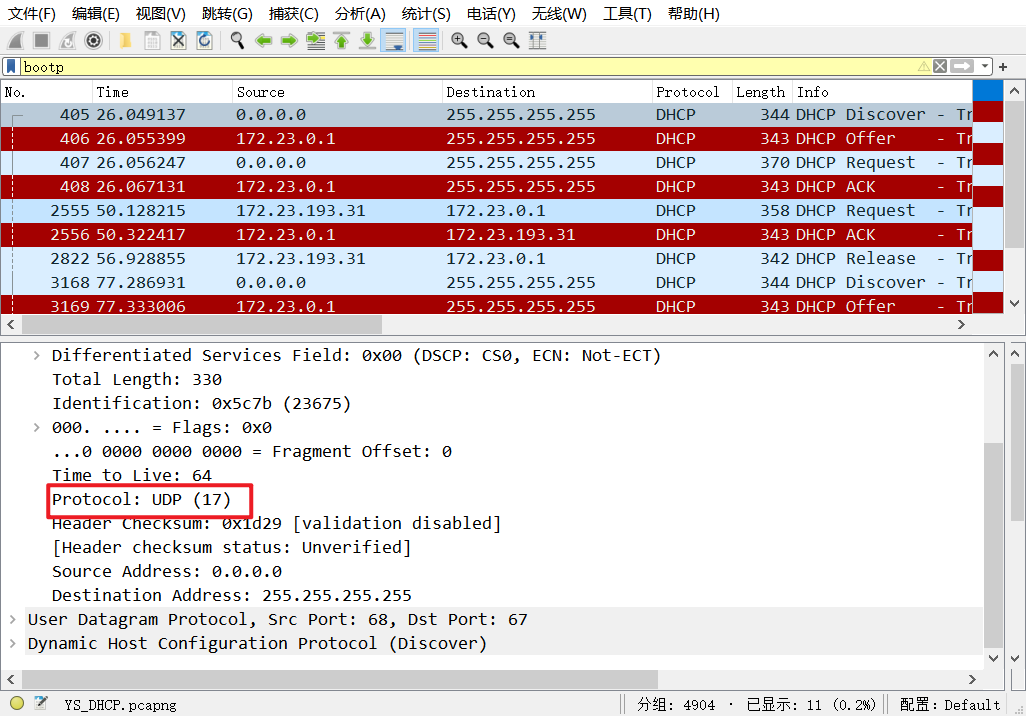


图3 UDP传输

**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?**

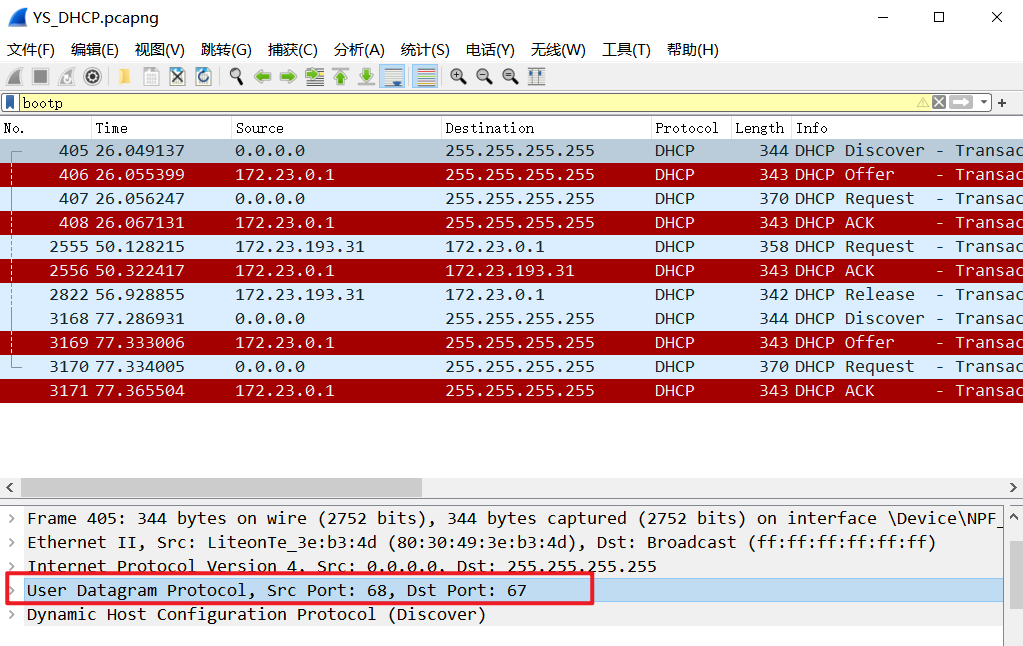


图4 端口信息

由前四个报文的图示信息可知示意图中的源端口号与目的端口号，与示例所用端口号一致，为68与67号端口。

|  |  |  |
| --- | --- | --- |
| 数据包 | 源端口号 | 目的端口号 |
| DHCP Discover | 68 | 67 |
| DHCP Offer | 67 | 68 |
| DHCP Request | 68 | 67 |
| DHCP ACK | 67 | 68 |

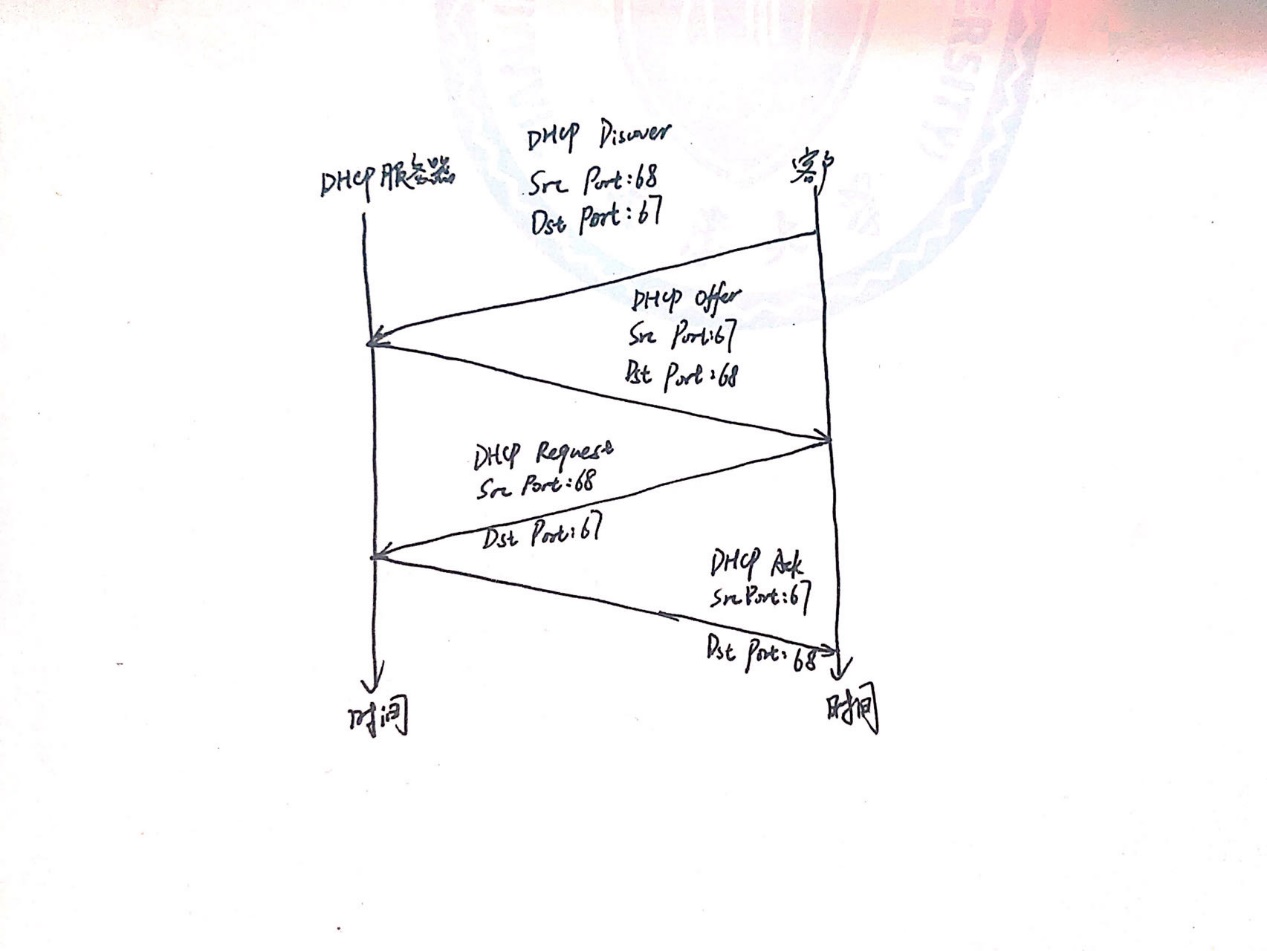


图5 手绘传播图

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

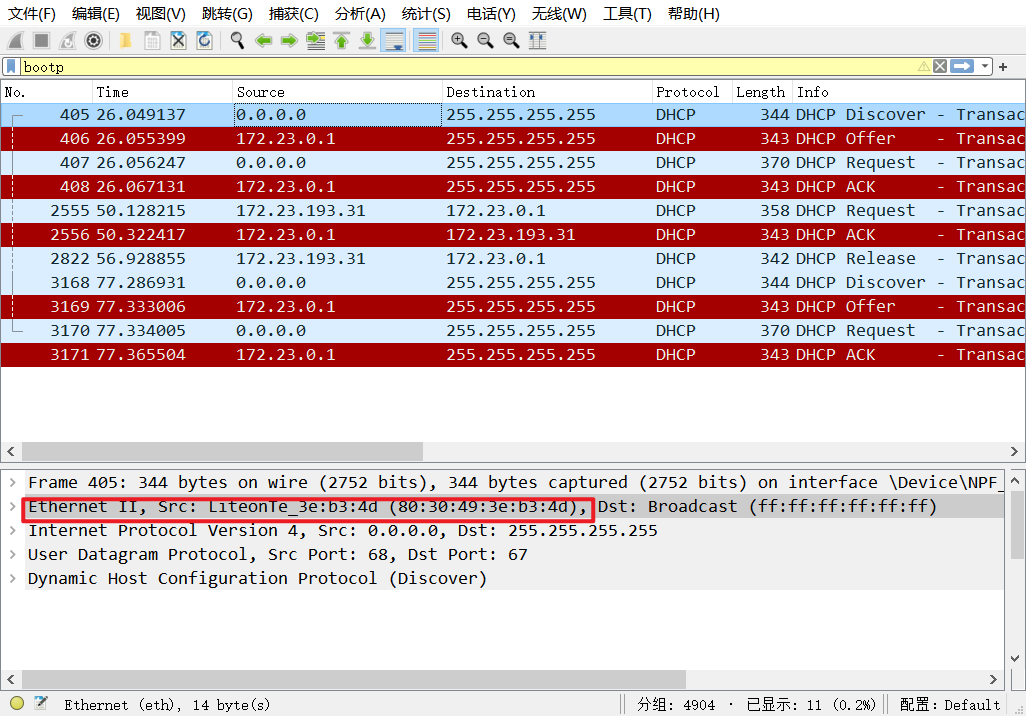


图6 以太网地址信息

由图可知，以太网地址：80:30:49:3e:b3:4d。

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

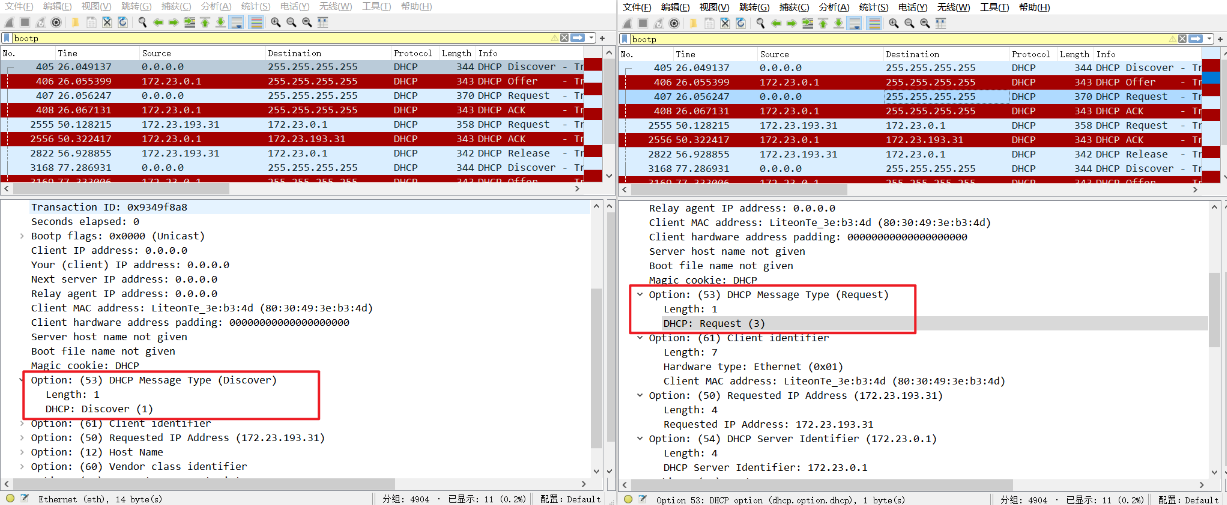


图7 报文信息

区分DHCP Discover与DHCP Request两个报文，可以利用DHCP Message Type这个标志位，DHCP Discover为1，DHCP Request为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?**

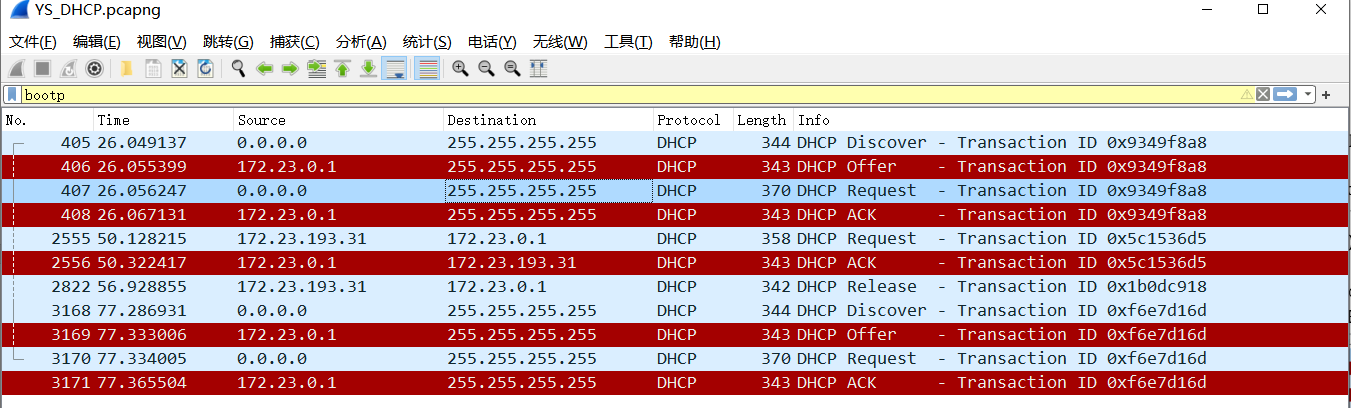


图8 DHCP数据包信息

前四个DHCP数据包的Translation ID是一致的，如下表：

|  |  |
| --- | --- |
| 数据包 | Translation ID |
| DHCP Discover | 0x9349f8a8 |
| DHCP Offer | 0x9349f8a8 |
| DHCP Request | 0x9349f8a8 |
| DHCP ACK | 0x9349f8a8 |

第二次传输的DHCP数据包（Request与ACK）的Translation ID均为0x5c1536d5。使用Translation ID的意义：每次建立DHCP连接均需要四次握手，而这四次握手的Translation ID均一致，表明他们均处于同一次连接建立过程中，不同的Translation ID避免不同连接建立时数据包相互混淆。

**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.**

DHCP messages (Discover/Offer/Request/ACK DHCP)的源IP地址与目的IP地址如下图9所示：

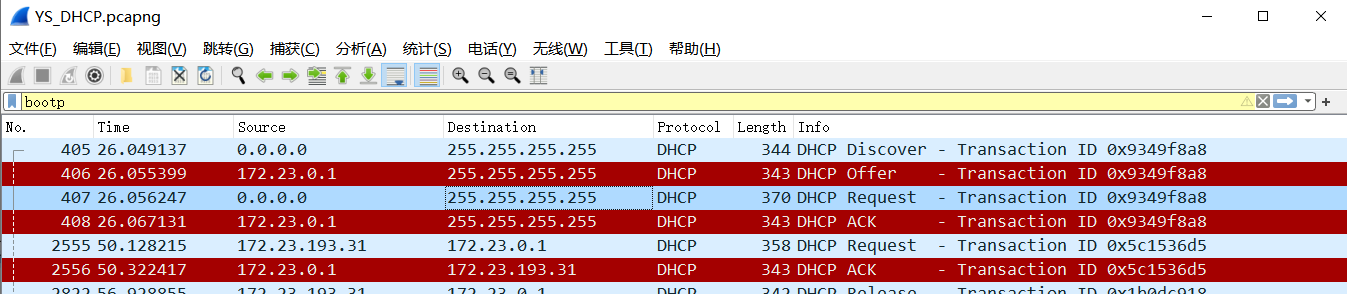


图9 源IP与目的IP地址

|  |  |  |
| --- | --- | --- |
| 数据包 | 源IP | 目的IP |
| DHCP Discover | 0.0.0.0 | 255.255.255.255 |
| DHCP Offer | 172.23.0.1 | 255.255.255.255 |
| DHCP Request | 0.0.0.0 | 255.255.255.255 |
| DHCP ACK | 172.23.0.1 | 255.255.255.255 |

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

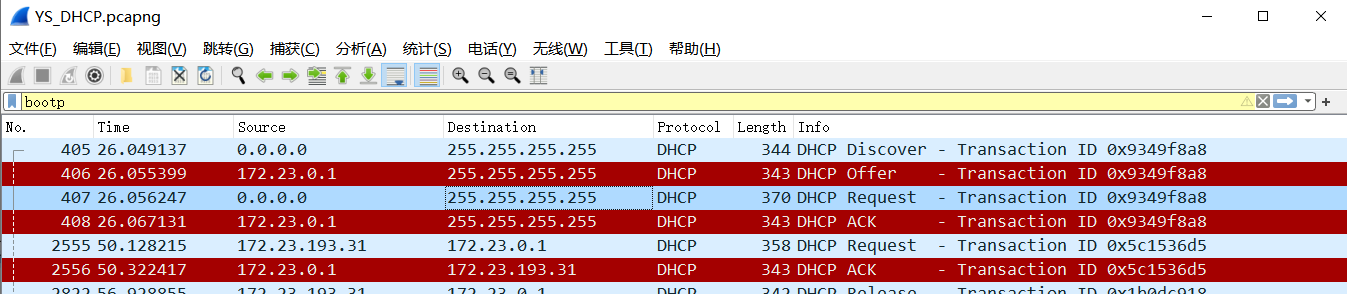


图10 IP地址

由上图知：DHCP服务器的IP地址为172.23.0.1。

**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.**

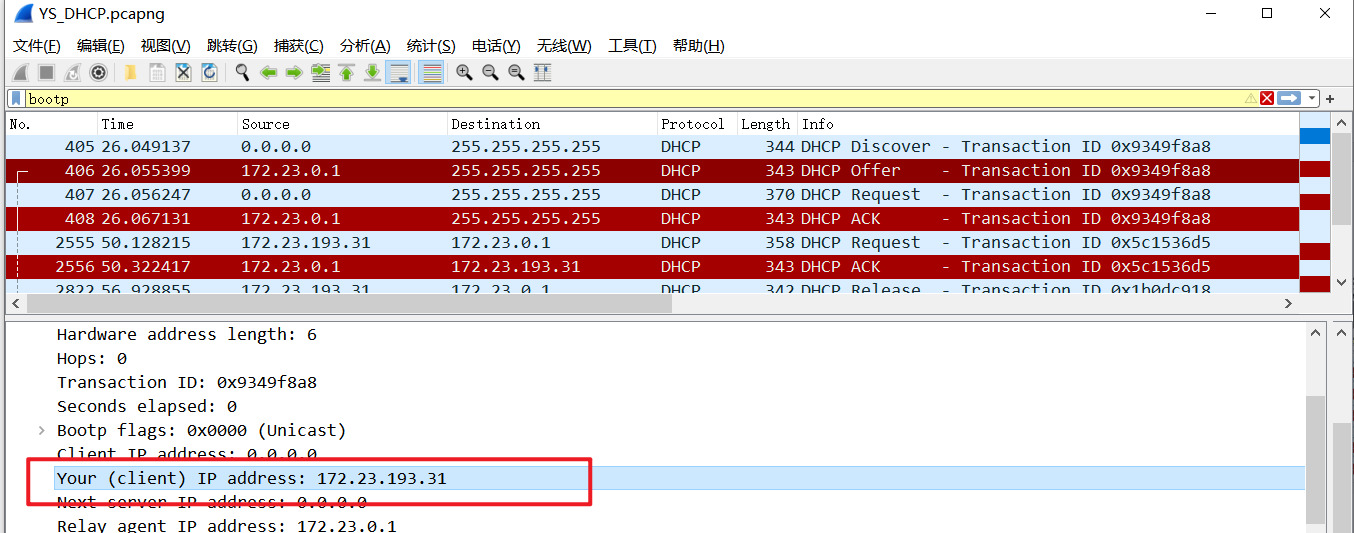


图11 分配的IP地址

由上图知，分配的IP地址为172.23.193.31，DHCP ACK 中会包含此IP地址。

**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?**

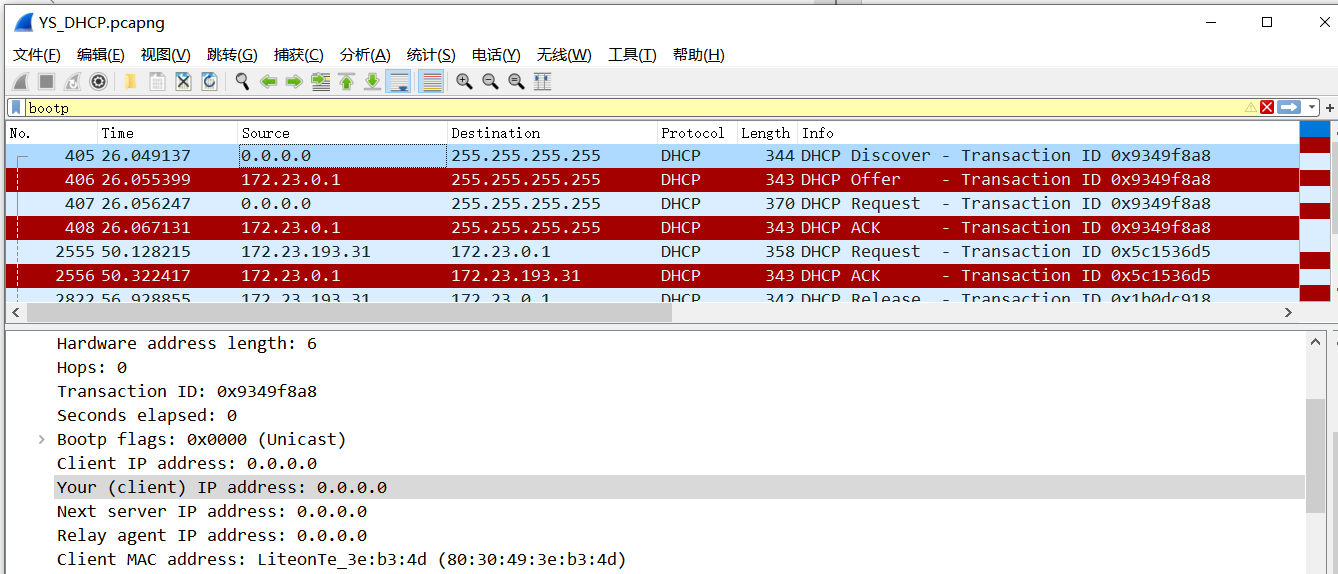


图12 中继代理

Trace中的Relay agent IP address值为0.0.0.0，表示无中继代理。如上图所示，Relay agent IP address值为0.0.0.0，说明本次实验中无中继代理。

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

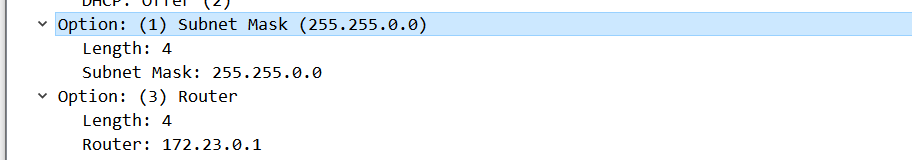


图13 DHCP Offer报文

在DHCP Offer报文中，Subnet Mask为子网掩码，用以指明一个IP地址的那些位标识的是主机所在的子网，Router指明该子网中路由器的IP地址。

**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?**

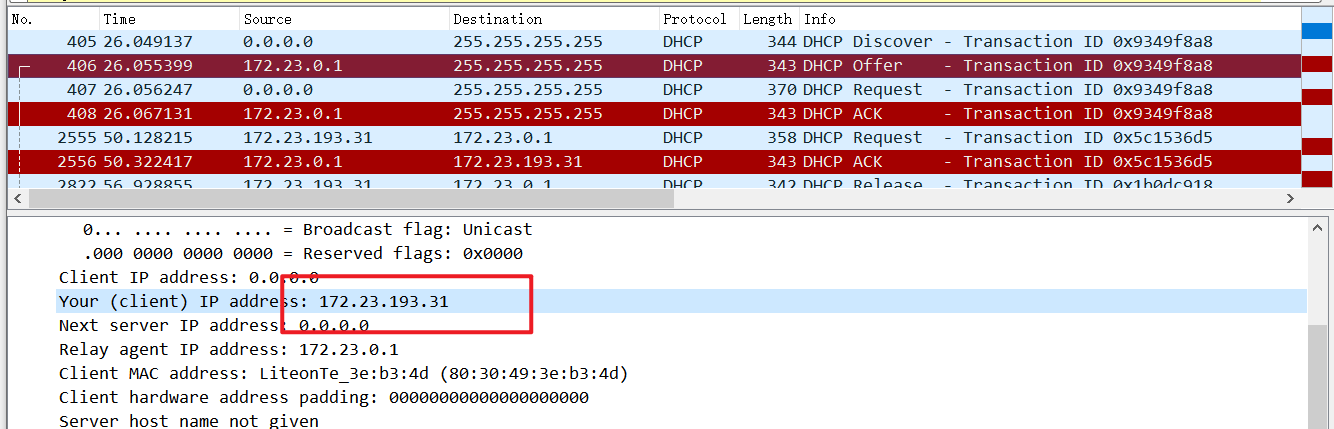


图14 需要的IP地址

需要的IP地址可通过上图中Your (client) IP address（已用红色标注）得到：172.23.193.31。

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

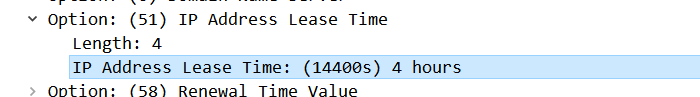


图15 lease time

lease time为IP地址租用期，表示该IP地址的有效时间量，便于DHCP服务器回收管理IP地址，由上图知，lease time为4小时。

**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? which the measured data differs from the idealized behavior of TCP that we’ve studied in the text.**

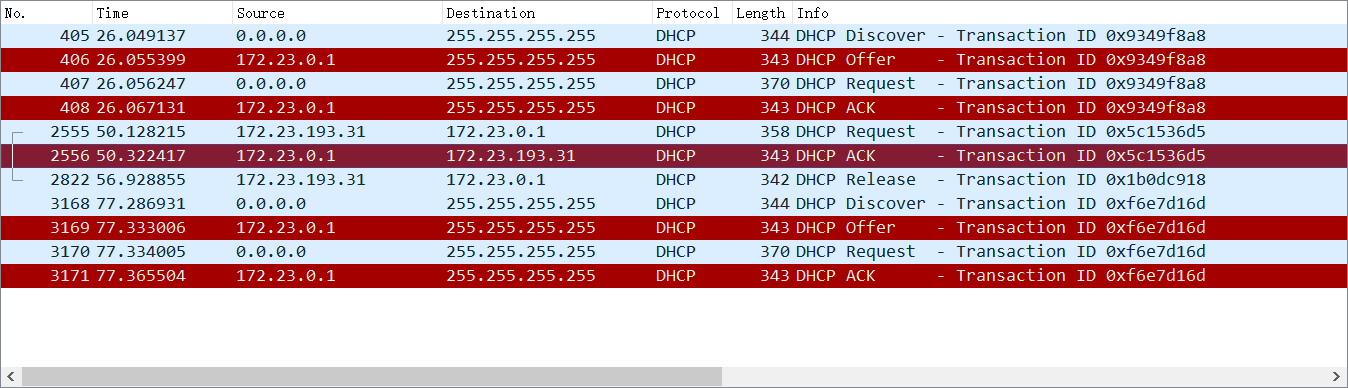


图16 DHCP Release

DHCP Release作用：当DHCP客户端不再需要使用分配IP地址时（一般出现在客户端关机、下线等状况）就会主动向DHCP服务器发送RELEASE请求，告知服务器用户不再需要分配IP地址，请求DHCP服务器释放对应的IP地址；

是的；

如果DHCP Release丢失，那么DHCP服务器不知道客户端已完成IP地址配置，还会持续为客户端动态分配IP地址，将会造成资源浪费。

**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.**

存在ARP，见下图17。ARP为地址解析协议，根据IP地址获取物理地址。主机发送信息时将包含目标IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址，收到返回信息后将该IP地址与物理地址存入本机ARP缓存中并保留一定时间，在下次请求时直接查询ARP缓存以节约资源。

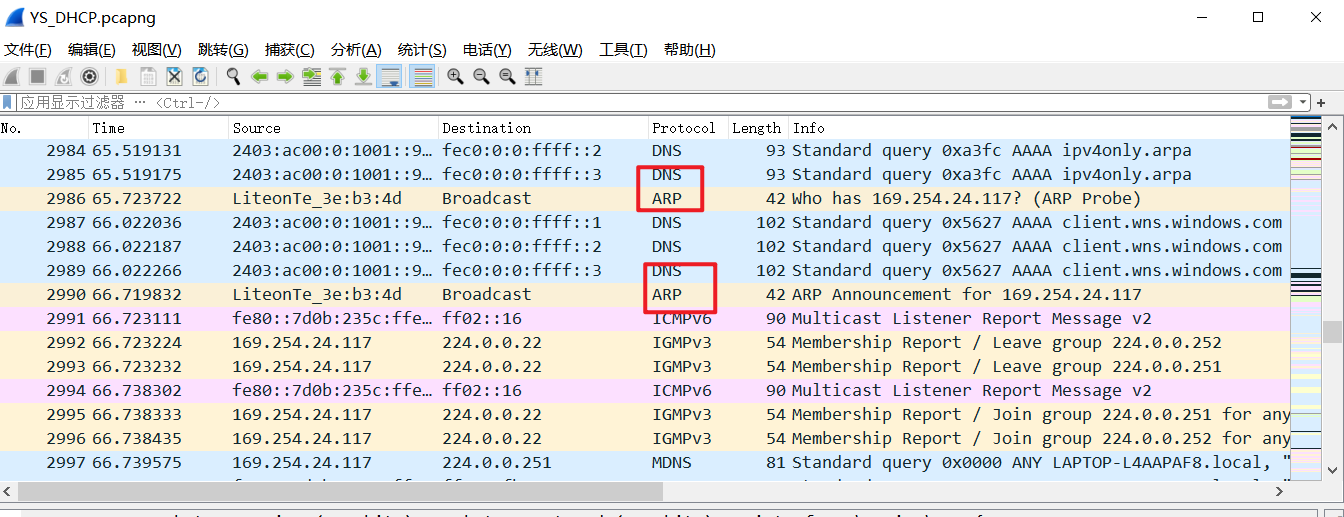


图17 ARP

# 四、总结

在本次实验中，首先在Windows命令行下输入ipconfig相关命令，获取本地连接信息截图。随后，使用Wireshark工具进行抓包，并通过筛选“bootp”以获取DHCP（动态主机配置协议）的捕获情况。

在实验过程中，我遇到了一些问题和困难。首先，由于笔记本电脑未使用有线网接入校园网，因此本地连接是断开的，只能通过WLAN接入校园网进行实验。这导致了在抓包过程中可能会出现丢包或者数据包不完整的情况，影响了分析与解读数据的准确性。对于DHCP协议的各个字段和报文格式的理解也是一项挑战，在分析数据时，需要了解DHCP报文的各个字段的含义和作用，如报文类型、Transaction ID等，并与实验要求进行对比，以解决各个问题。这需要我对DHCP协议有较为深入的了解，并且需要仔细观察和分析数据。对于Wireshark工具的使用也有了进一步的掌握与理解，Wireshark是一款功能强大的网络抓包工具，在使用过程中，需要注意过滤器的设置、抓包条件的选择、数据包的解析等，以确保获取到准确的抓包数据。在本次实验完成后，我对DHCP协议的工作机制、报文格式和字段含义有了更加深入的了解。通过对数据的分析，我学会了如何从中获取有关DHCP报文的信息，如报文类型、Transaction ID、源IP地址、目的IP地址等，并且能够回答实验中提出的问题。

总而言之，本次实验使我更加熟悉了DHCP协议的工作原理以及使用Wireshark工具进行网络抓包的方法，但在此过程中也面临了一些问题和困难，我仍需要继续提升网络协议分析能力与抓包技能，以更好地应对日后的挑战。