****



**WireShark DHCP实验报告**

**学院： 智能与计算学部**

**专业： 计算机科学与技术**

**姓名： 陈秋澄**

**学号： 3022244290**

**2024年4月15日**

我按照文件要求自己进行了相关操作，在终端输入相关指令，用wireshark进行抓包。



图1-a 操作佐证a

在filter处输入bootp筛选出捕获到的DHCP记录如下图所示：

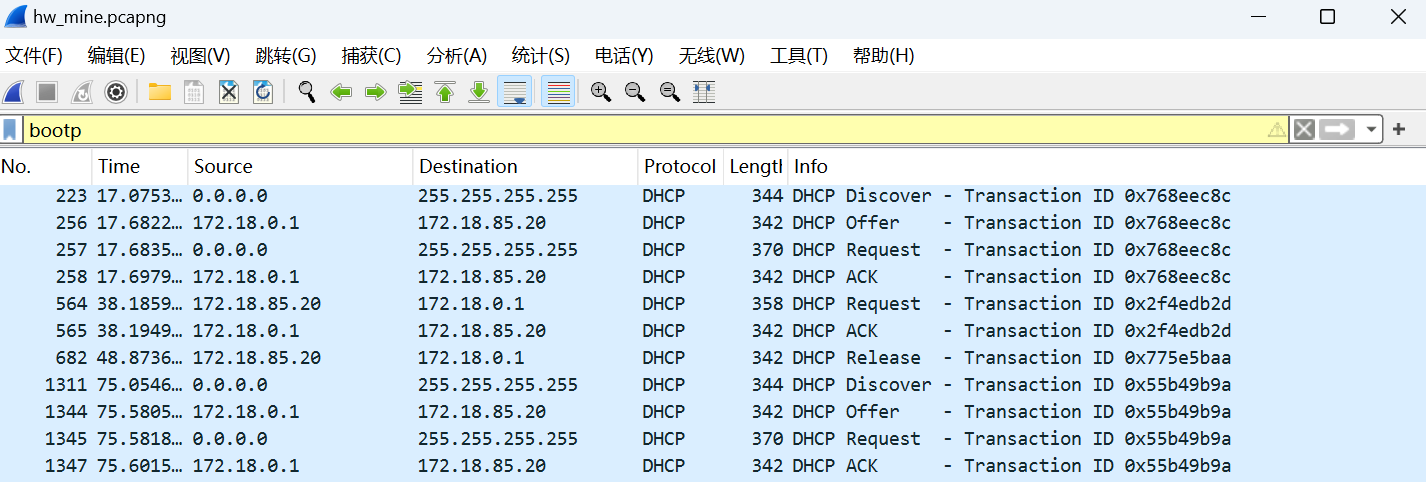
****

图1-b 操作佐证b

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

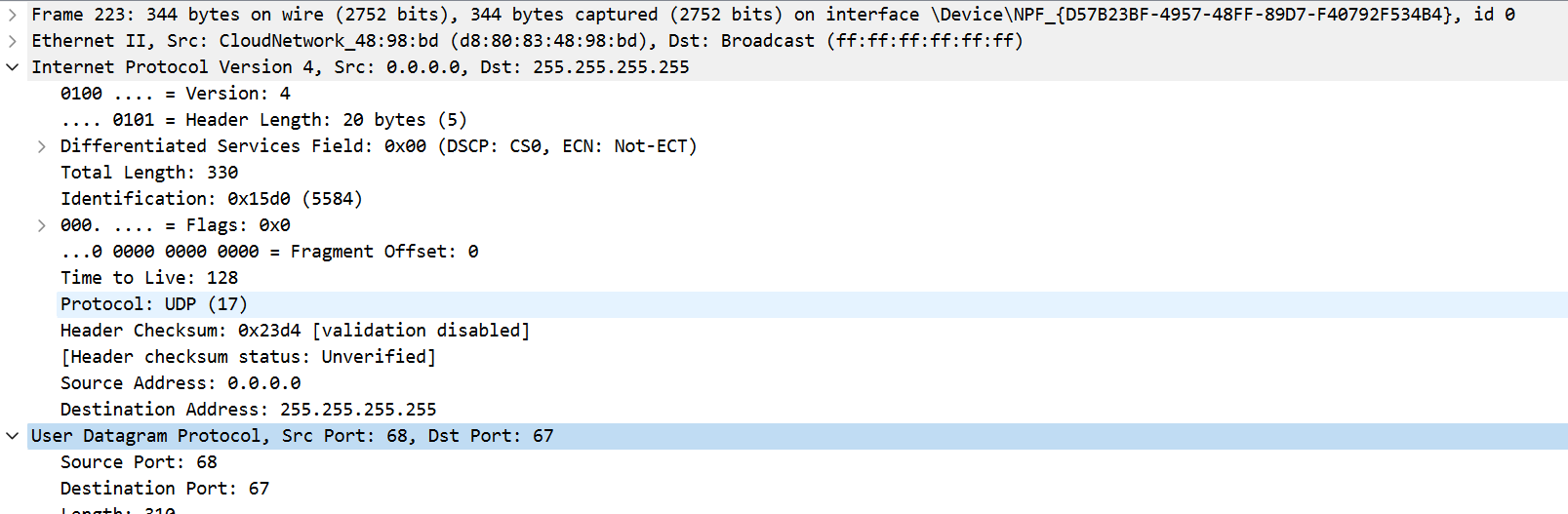
DHCP消息通过UDP发送，原因是使用的协议是UDP，如下图所示：

图2 Question 1佐证

**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?**

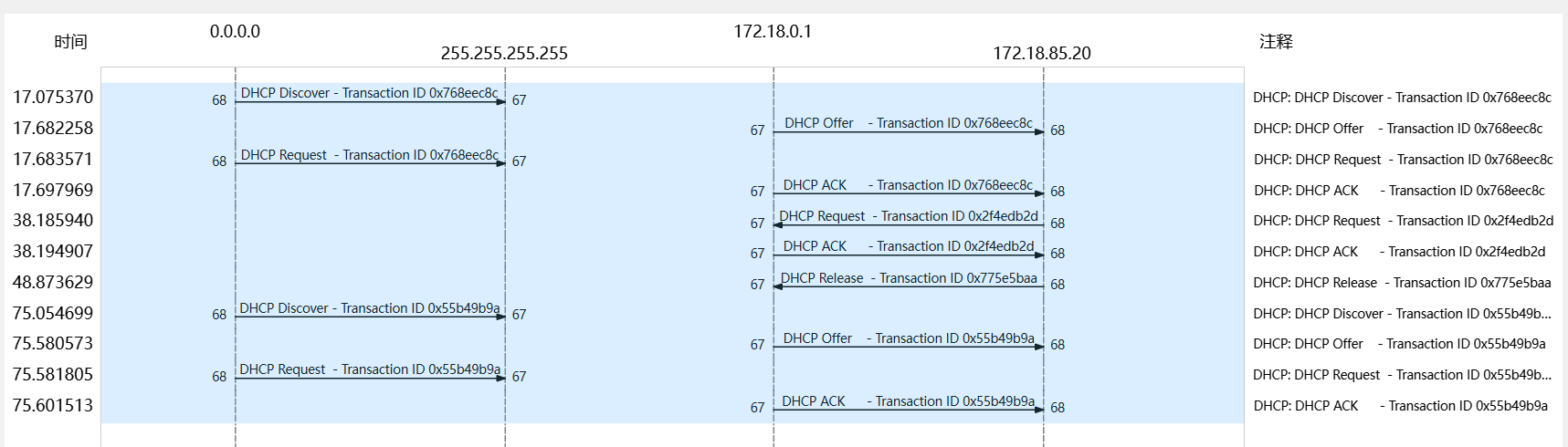


图3-a Question 2 timing datagram

四个交换包的顺序是：首先用户端发送Discover，广播DHCP发现报文；接着DHCP服务器发送Offer，收到发现报文后提供租约；接着客户端Request，选择一个服务器提供后请求租用（同样请求中允许服务器单播回复，其中仍然包括我的网卡 MAC 地址）；最后DHCP服务器发送ACK确认响应，正是所要请求的参数。从图中可以看出我电脑DHCP发现和 DHCP 请求都是68 端口发出，而服务器DHCP 提供和 DHCP 响应都是 67 端口发出。顺序为：Discover，Offer，Request，ACK，如下图所示。端口号是否与本实验作业中给出的示例相同。

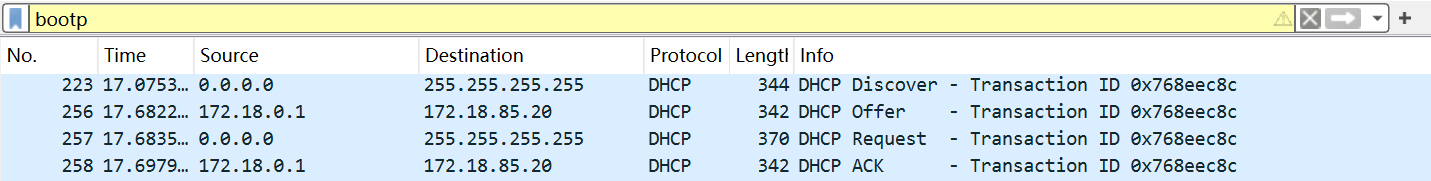


图3-b Question 2佐证b

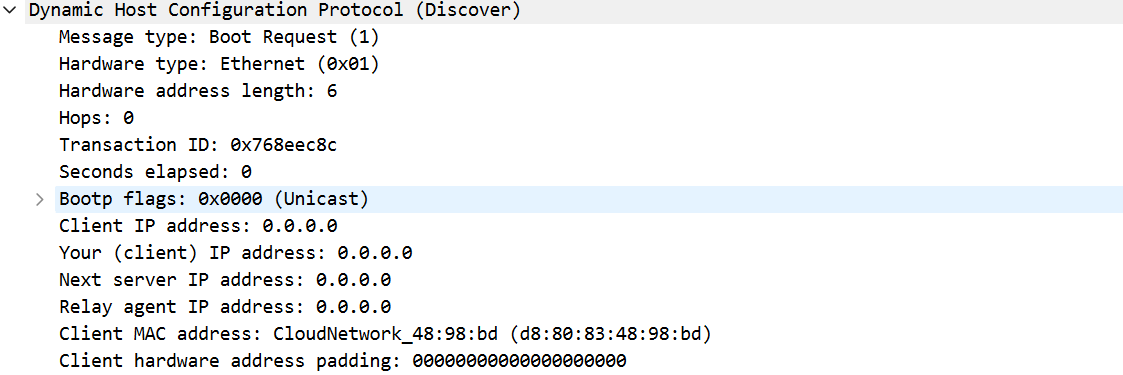


图3-c Question 2佐证c

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

主机的链路层地址是：CloudNetwork\_48:98:bd (d8:80:83:48:98:bd)，如下图所示：

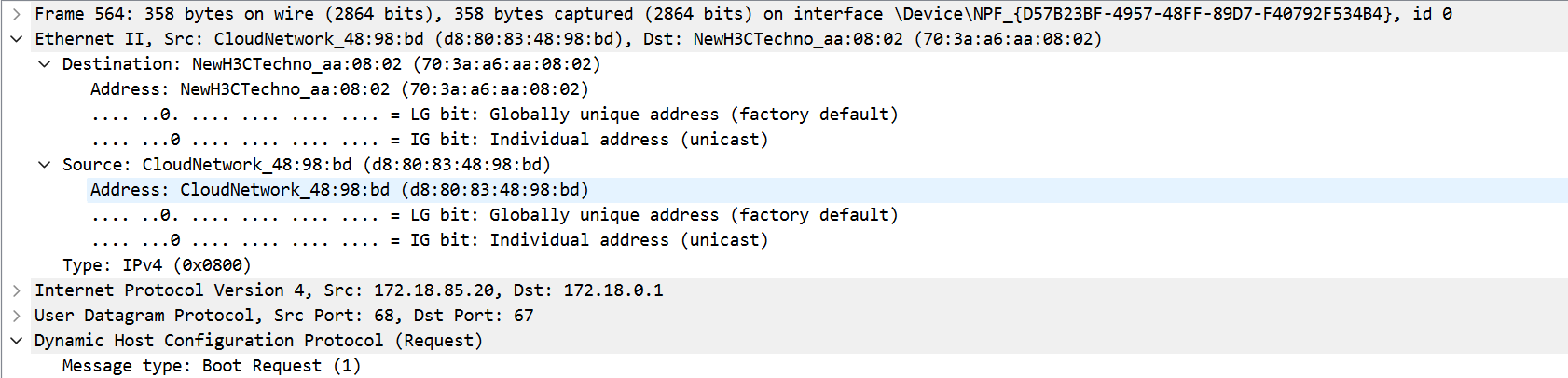


图4 Question 3佐证

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

DHCP的discover信息与request信息的区别如下所示：

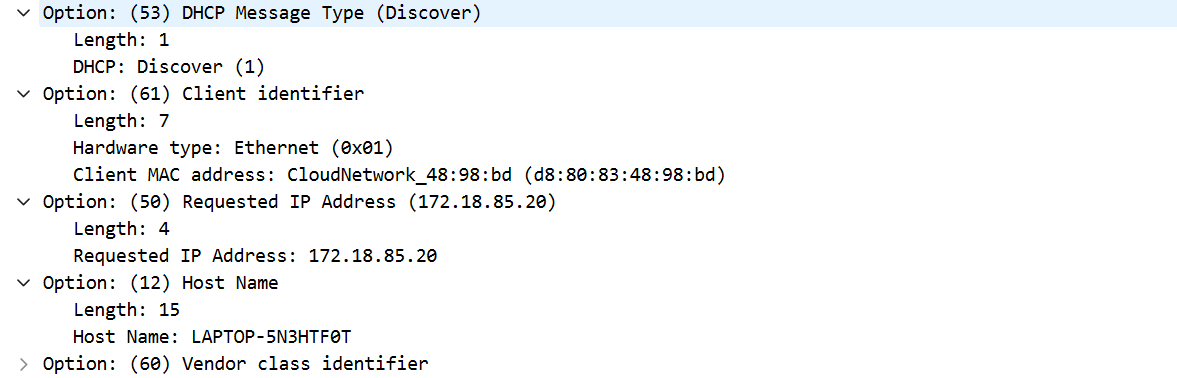


图5-a Question 4佐证a

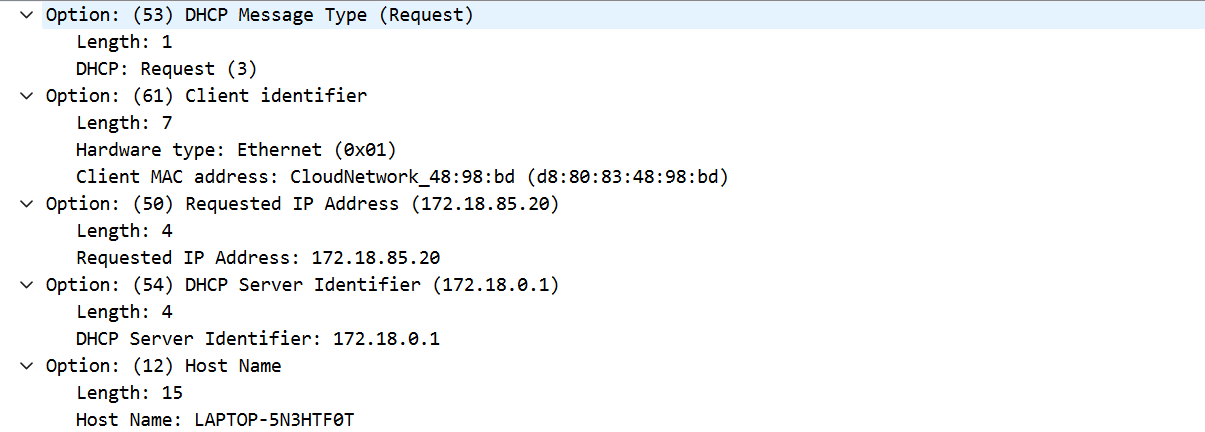


图5-b Question 4佐证b

由上两图可以看出二者在前四个Option上不同，其中最重要的是Option(54)即服务器标识，因为考虑到DHCP一开始是使用广播，所以是没有服务器的信息的，即在发现时是没有服务器的IP地址，只有到Request的时候有服务器IP地址的。但是使用DHCP首部字段中的有一个选项字段（即Option(53)）也可以将二者区分开来。

**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?**

第一组四个信息的Transaction-ID是：0x768eec8c；

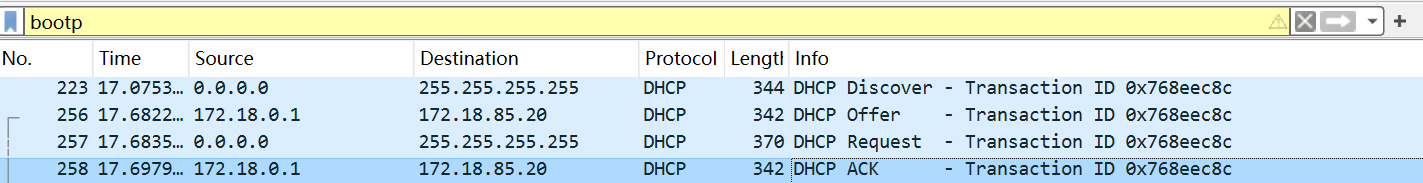


图6 Question 5佐证

Transaction-ID是一个随机生成的值，当客户端请求和服务器一样使才会认为有效，这是一个安全性保证的措施，即用来区分不同交互的组。

**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.**

主机如果没有IP地址，IP数据报的值是0.0.0.0，目的地址广播地址为255.255.255.255，服务器使用其作为源的实际IP地址。

第1、3个消息的目的IP地址都是255.255.255.255，可以看出是在广播信息；

客户端发送的两次信息（Discover和Request）的IP地址都是0.0.0.0，因为此时客户端还没有IP地址；

DHCP服务器发送的两次信息（Offer和ACK）的IP地址是其在当前局域网下的IP地址，即为172.18.85.20；

上述结果如下图所示：

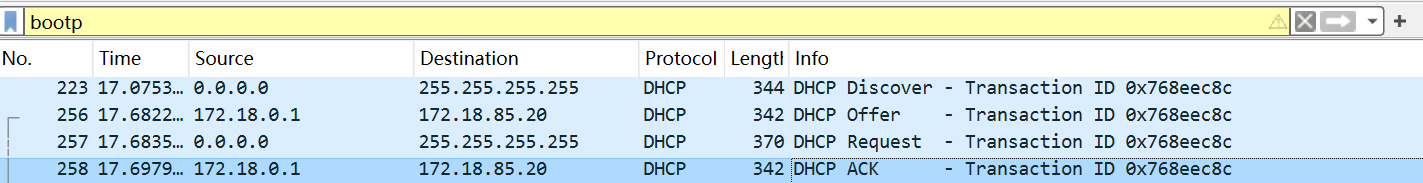


图7 Question 6佐证

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

我的DHCP服务器的IP地址是172.18.0.1，如下图所示：

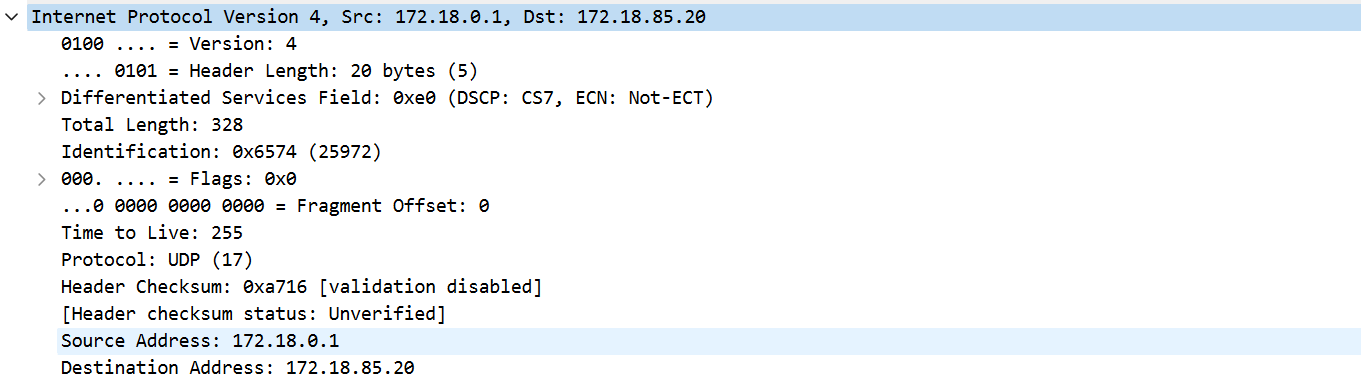
****

图8 Question 7佐证

**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.**

分配给我的IP地址是172.18.85.20，可以在Offer信息中看到，如下图所示：

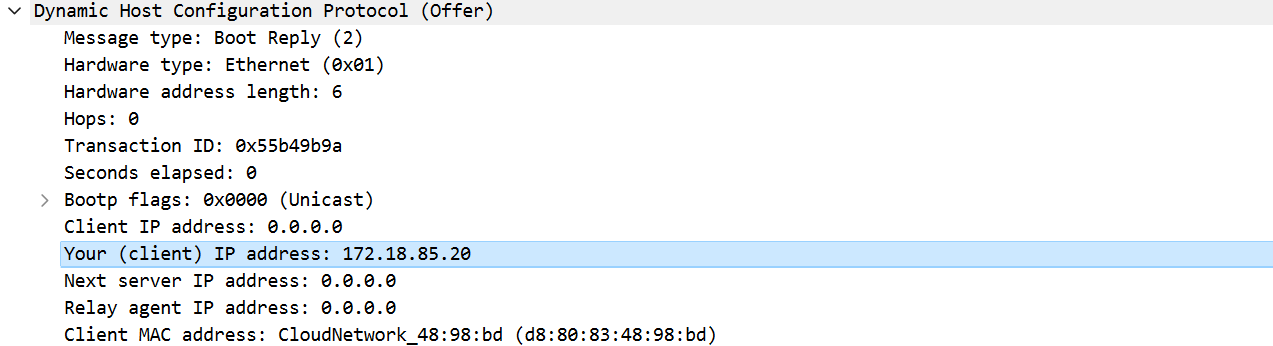


图9 Question 8佐证

**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?**

可以看出在四条信息中，中继代理的IP地址都是0.0.0.0，表示没有使用DHCP中继。如下图所示：

在我的实验中也没有使用中继代理：

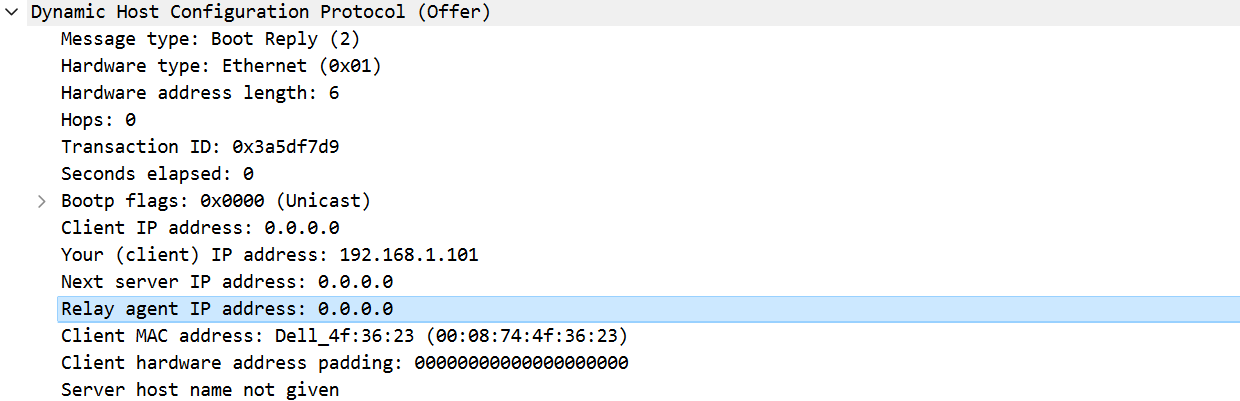


图10 Question 9佐证

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

提供了路由器的IP，在我们得到路由器的IP地址之后，发送请求可以直接向路由器发送，起到了中间代理的作用；

提供了子网掩码，告诉我们当前获取的子网的大小以及客户端应该使用哪个子网掩码，方便以后的配置。

客户端可以在完成了 Discover - Offer - Request - ACK 交互后可以配置掩码和网关；如果有多个DHCP 服务器，客户端可以收到多个服务器提供，所以客户端可以在这些服务器提供里选择优越的位置，IP地址和网络掩码是重要的决策依据。

总之，路由器行向客户端指示其默认网关是什么。子网掩码行告诉客户端应该使用哪个子网掩码。

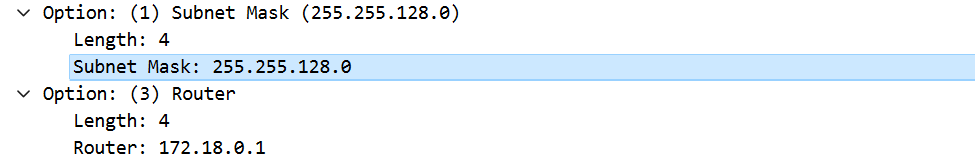


图11 Question 10佐证

**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?**

客户端接收了此IP地址，因为发送了Request请求，我们要请求的IP就是DHCP申请出来的Offer中的那个IP地址，如下图所示：

Offer的截图：

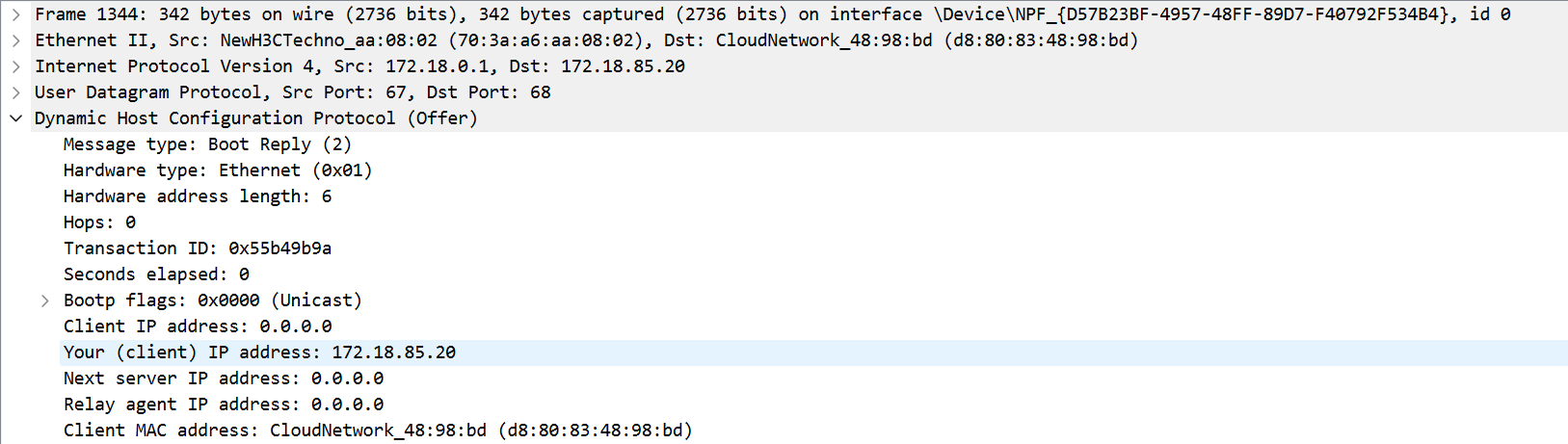


图12-a Question 11佐证a

Request的截图：

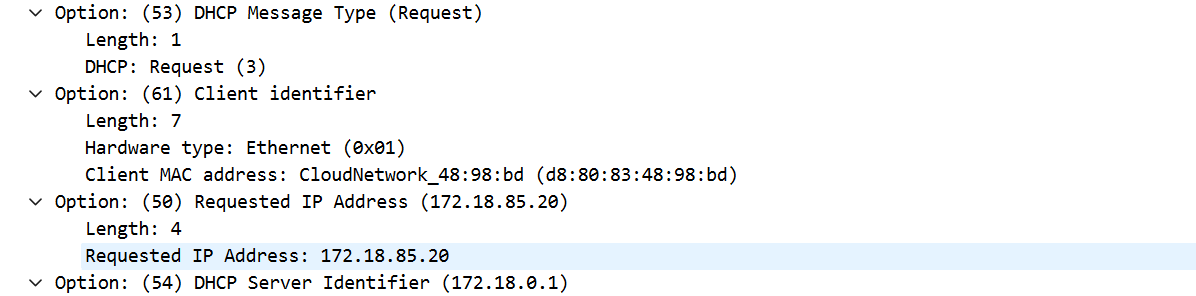
****

图12-b Question 11佐证b

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

租约时间是DHCP服务器分配IP的时间量给客户的地址，即在租约期间，DHCP服务器不会分配IP提供给客户端给另一个客户端，除非它是由客户端释放的。一旦租约时间已过，DHCP服务器可以重复使用该IP地址以提供给另一个客户。

在我的实验中，租赁期是1天，如下图所示。

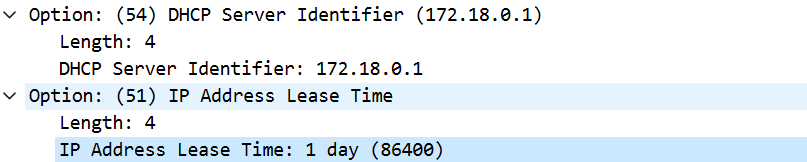


图13 Question 12佐证

**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?**

主动告知DHCP服务器客户端要离开了，DHCP服务器在收到消息之后可以把分配出去的资源回收并将资源重新分配。

DHCP服务器不会发送向客户端发回确认DHCP释放消息的消息。

如果客户的DHCP发布消息丢失了，那么DHCP分配的资源可能需要等到租赁到期的时候才能进行回收。

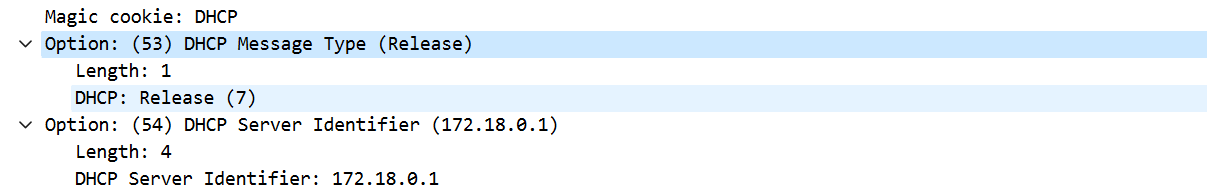


图14 Question 13佐证

**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.**

如下图所示，有ARP包被发送和收到；

这些ARP包的用途是DHCP服务器发出了ARP请求，把提供的IP地址分配给客户端，DHCP服务器会针对提供的IP地址发出ARP包请求以确保该IP地址没有被另一客户端使用，即广播检测IP使用的MAC地址，查看是否发生冲突。

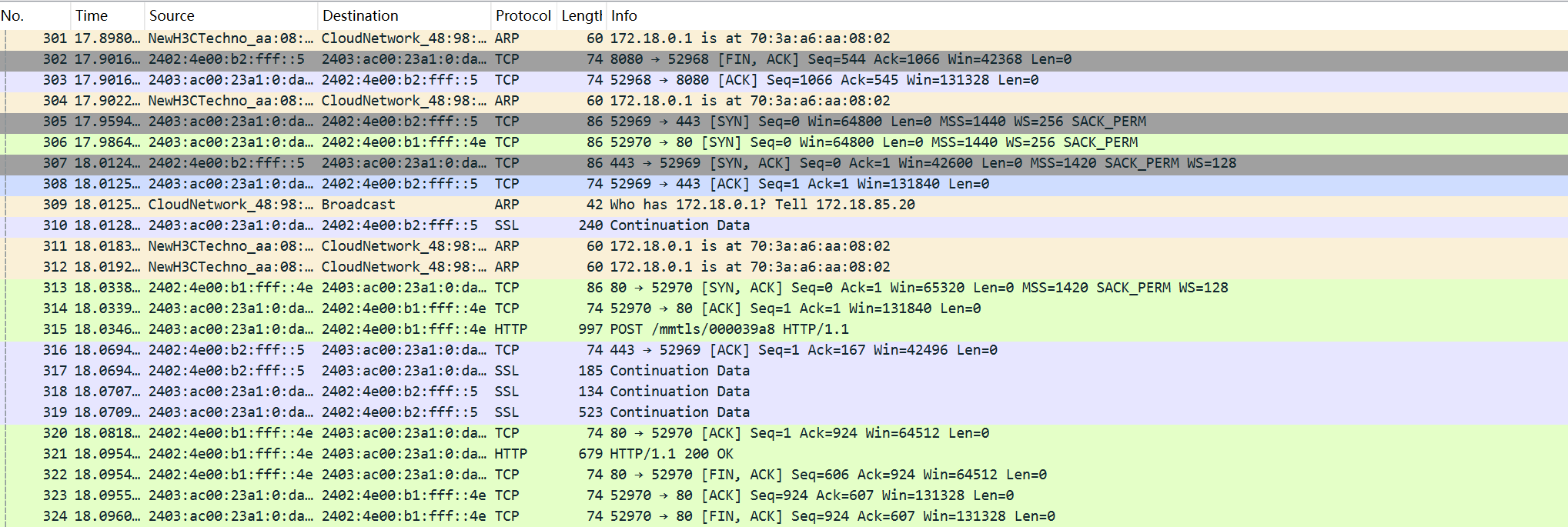


图15 Question 14佐证