**【实验名称】：**ARP消息分析实验

**学生姓名：2151133**孙韩雅

**实验地点：**济事楼330 **实验时间：**2023-11-27

**【实验目的】**

了解ARP协议的历史、概念以及原理，学会分析ARP数据包。

**【实验原理】**

1.ARP出现原因

ARP协议是“Address Resolution Protocol”（地址解析协议）的缩写。其作用是在以太网环境中，数据的传输所依懒的是MAC地址而非IP地址，而将已知IP地址转换为MAC地址的工作是由ARP协议来完成的。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的MAC地址的。在以太网中，一个主机和另一个主机进行直接通信，必须要知道目标主机的MAC地址，它是通过地址解析协议获得的。

所谓“地址解析”就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。

2.ARP映射方式

2.1.静态映射

静态映射的意思是要手动创建一张ARP表，把逻辑（IP）地址和物理地址关联起来。这个ARP表储存在网络中的每一台机器上。例如，知道其机器的IP地址但不知道其物理地址的机器就可以通过查ARP表找出对应的物理地址。这样做有一定的局限性，因为物理地址可能发生变化：

（1）机器可能更换NIC（网络适配器），结果变成一个新的物理地址。

（2）在某些局域网中，每当计算机加电时，他的物理地址都要改变一次。

（3）移动电脑可以从一个物理网络转移到另一个物理网络，这样会时物理地址改变。要避免这些问题出现，必须定期维护更新ARP表，此类比较麻烦而且会影响网络性能。

2.2.动态映射

动态映射时，每次只要机器知道另一台机器的逻辑（IP）地址，就可以使用协议找出相对应的物理地址。已经设计出的实现了动态映射协议的有ARP和RARP两种。ARP把逻辑（IP）地址映射为物理地址。RARP把物理地址映射为逻辑（IP）地址。

3.ARP原理及流程

在任何时候，一台主机有IP数据报文发送给另一台主机，它都要知道接收方的逻辑（IP）地址。但是IP地址必须封装成帧才能通过物理网络。这就意味着发送方必须有接收方的物理（MAC）地址，因此需要完成逻辑地址到物理地址的映射。而ARP协议可以接收来自IP协 议的逻辑地址，将其映射为相应的物理地址，然后把物理地址递交给数据链路层。

3.1.ARP请求

任何时候，当主机需要找出这个网络中的另一个主机的物理地址时，它就可以发送一个ARP请求报文，这个报文包好了发送方的MAC地址和IP地址以及接收方的IP地址。因为发送方不知道接收方的物理地址，所以这个查询分组会在网络层中进行广播。

3.2.ARP响应

局域网中的每一台主机都会接受并处理这个ARP请求报文，然后进行验证，查看接收方的IP地址是不是自己的地址，只有验证成功的主机才会返回一个ARP响应报文，这个响应报文包含接收方的IP地址和物理地址。这个报文利用收到的ARP请求报文中的请求方物理地址以单播的方式直接发送给ARP请求报文的请求方。

4.ARP协议报文字段抓包解析

4.1.报文格式

硬件类型：16位字段，用来定义运行ARP的网络类型。每个局域网基于其类型被指派一个整数。例如：以太网的类型为1。ARP可用在任何物理网络上。

协议类型：16位字段，用来定义使用的协议。例如：对IPv4协议这个字段是0800。ARP可用于任何高层协议。

硬件长度：8位字段，用来定义物理地址的长度，以字节为单位。例如：对于以太网的值为6。

协议长度：8位字段，用来定义逻辑地址的长度，以字节为单位。例如：对于IPv4协议的值为4。

操作码：16位字段，用来定义报文的类型。已定义的分组类型有两种：ARP请求（1），ARP响应（2）。

源硬件地址：这是一个可变长度字段，用来定义发送方的物理地址。例如：对于以太网这个字段的长度是6字节。

源逻辑地址：这是一个可变长度字段，用来定义发送方的逻辑（IP）地址。例如：对于IP协议这个字段的长度是4字节。目的硬件地址：这是一个可变长度字段，用来定义目标的物理地址，例如，对以太网来说这个字段位6字节。对于ARP请求报文，这个字段为全0，因为发送方并不知道目标的硬件地址。

目的逻辑地址：这是一个可变长度字段，用来定义目标的逻辑（IP）地址，对于IPv4协议这个字段的长度为4个字节。

4.2.ARP报文总长度

ARP报文的总长度为64字节。首先要知道帧的概念 帧是在数据链路层传输的数据格式，比如以太网v2，以太网IEEE802.3和PPP等。所以Wireshark抓到的帧是包含帧头的，即包含以太网v2的帧头，长14 bytes；而ARP数据包的长度固定为28 bytes；帧总长度=帧头+网络层包头+传输层报文头+应用数据；而ARP请求中ARP包已经是最高层，之上没有传输层和应用层，所以总长度为：帧总长度=帧头+ARP包头=14+28=42bytes；而真正发包的时为了保证以太网帧的最小帧长为64 bytes，会在报文里添加一个padding字段，用来填充数据包大小。使用wireshark抓包时，抓到的包为60 bytes。比以太网帧的最小帧长扫了4 bytes，原因是因为wireshark抓包时不能抓到数据包最后的CRC字段。

CRC字段是为了校验以太网帧的正确性。在数据包填充完成后，回去通过算法计算一个值放到数据包的CRC字段中。当接受端收到数据包后，会同样使用算法计算一个值，然后和CRC字段的值进行对比，查看是否相同。如果不同则证明数据包被更改，如果相同则证明数据包并未被更改。

4.3.报文封装

ARP报文直接封装在数据链路帧中。注意，帧中的类型字段指出此帧所携带的数据是ARP报文。

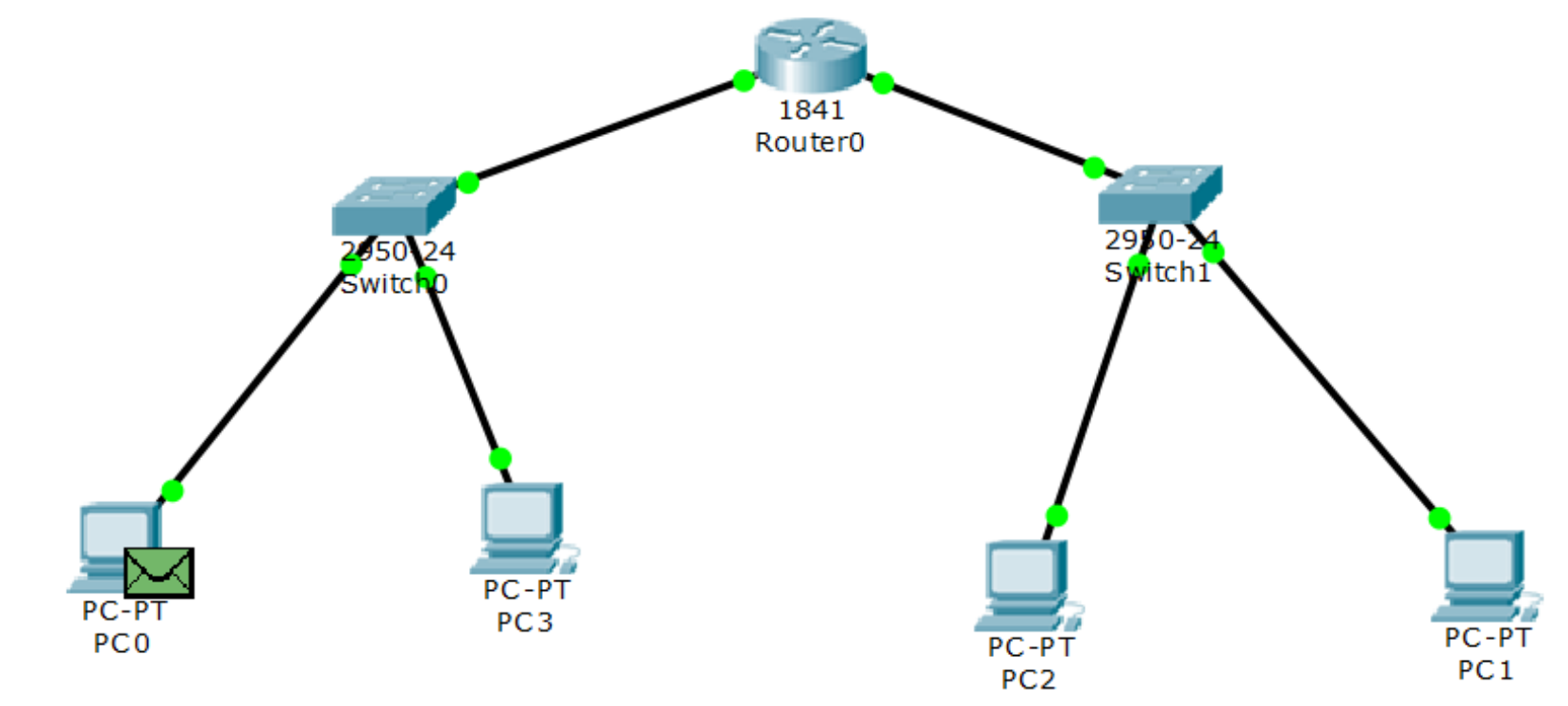
**【实验设备】**

HUAWEI MateBook X Pro（安装有Cisco Packet Tracer与Wireshark抓包分析工具）

【**实验步骤**】

1.查看本机的ARP内容。

2.规划网络地址连接线路：



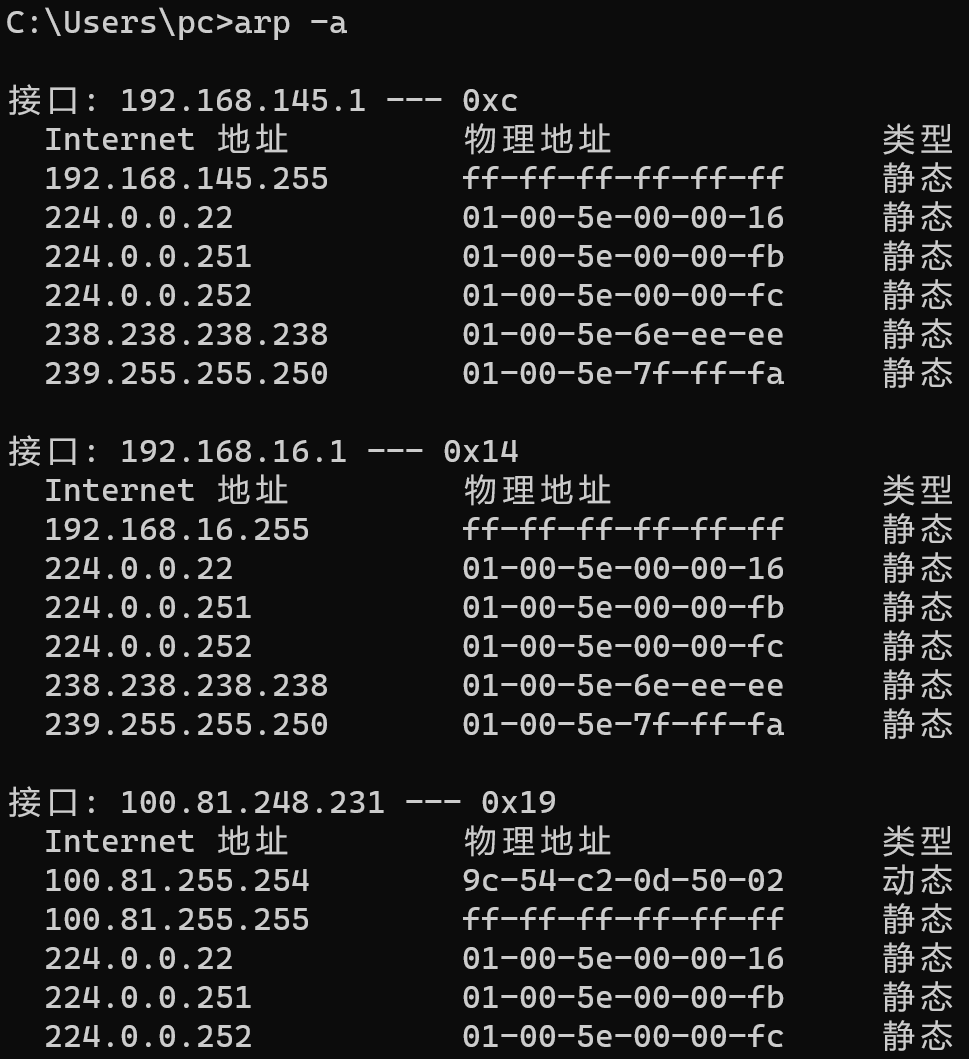
3.用WireShark抓取ARP数据包。

4.查看ARP报文字段内容，并解读。

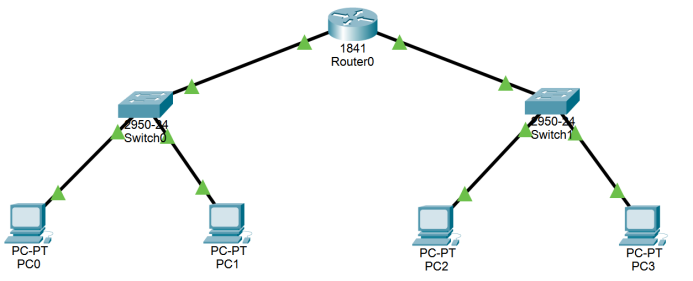
5.分析在Packet tracer中ARP报文情况。

**【实验现象】**

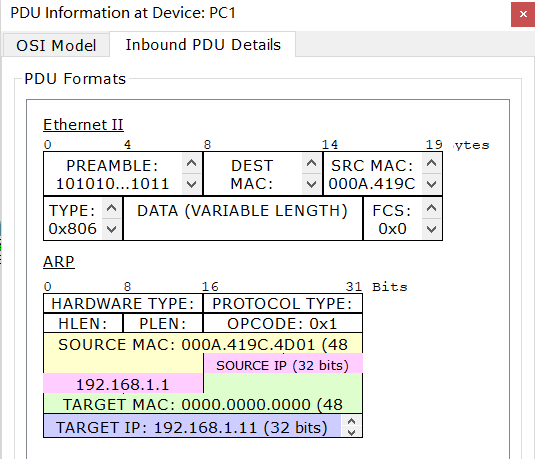
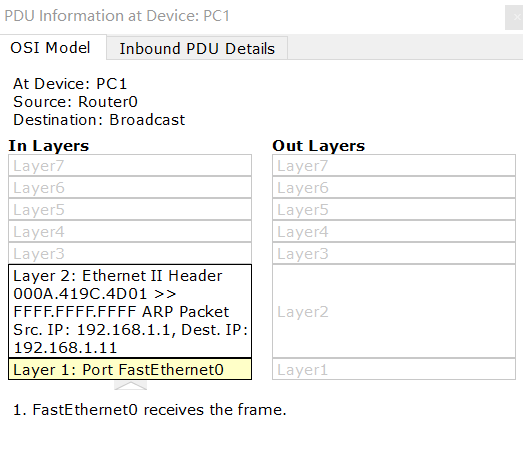
1.查看本机的ARP内容：



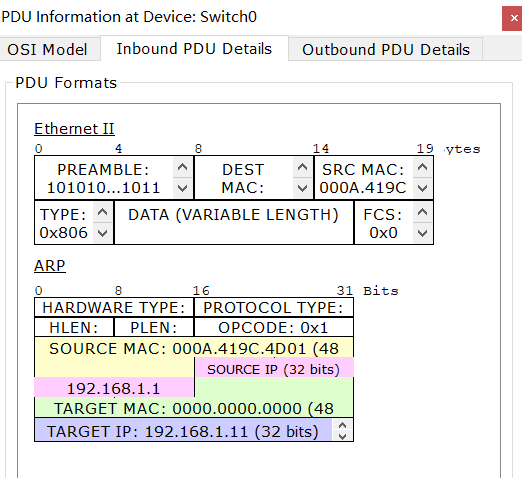
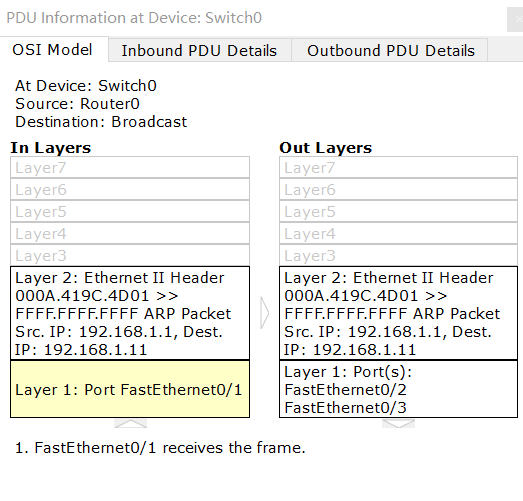
2.规划网络地址连接线路，配置DHCP动态IP：



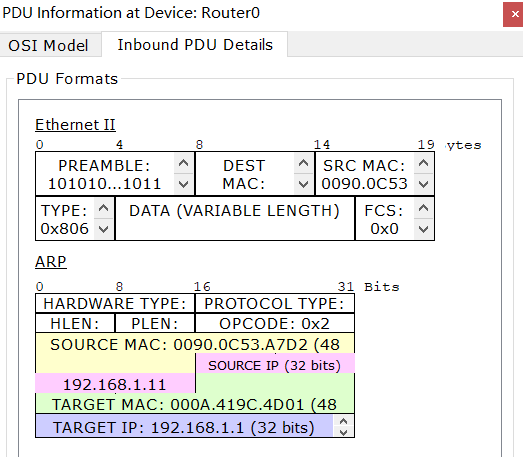
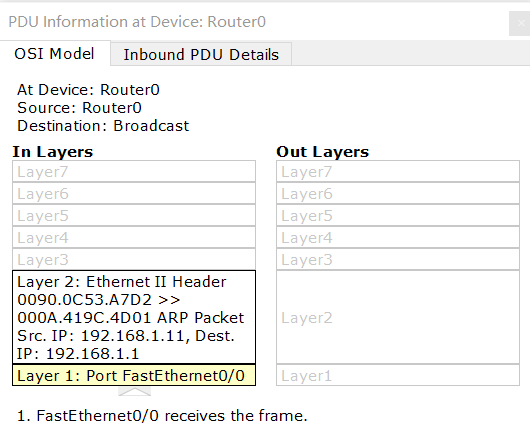
3.PC1产生ARP报文：



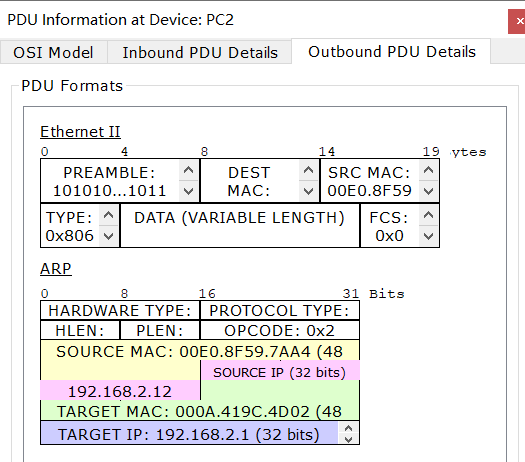
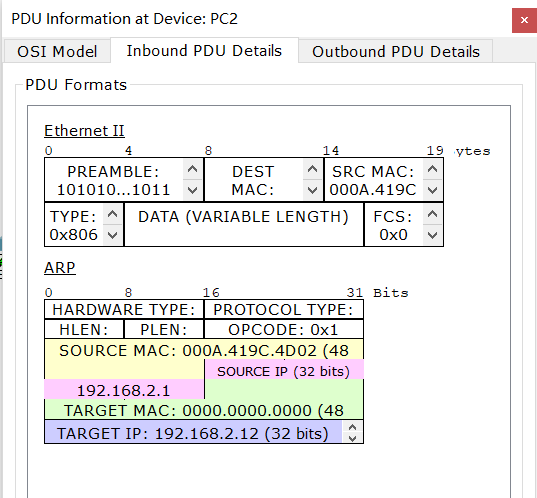
在交换机处转发：



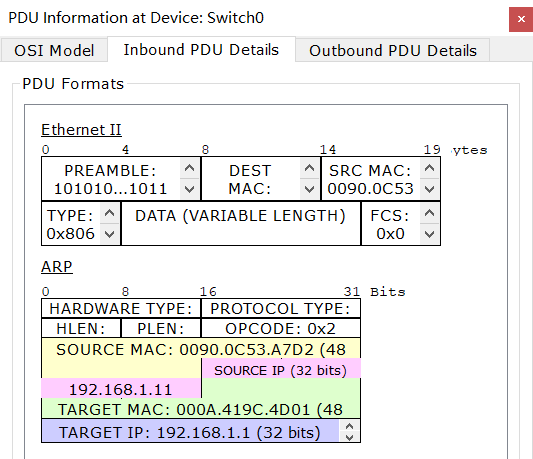
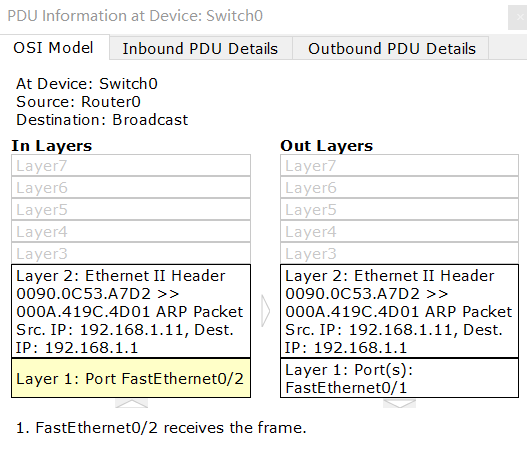
交换机发送报文给路由器：



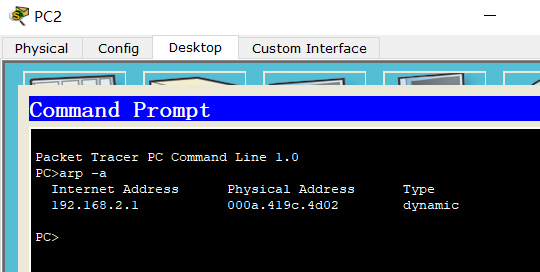
4.路由器向另一个交换机发送数据包，并由交换机转发。PC2得到响应，通过交换机返回给路由器：



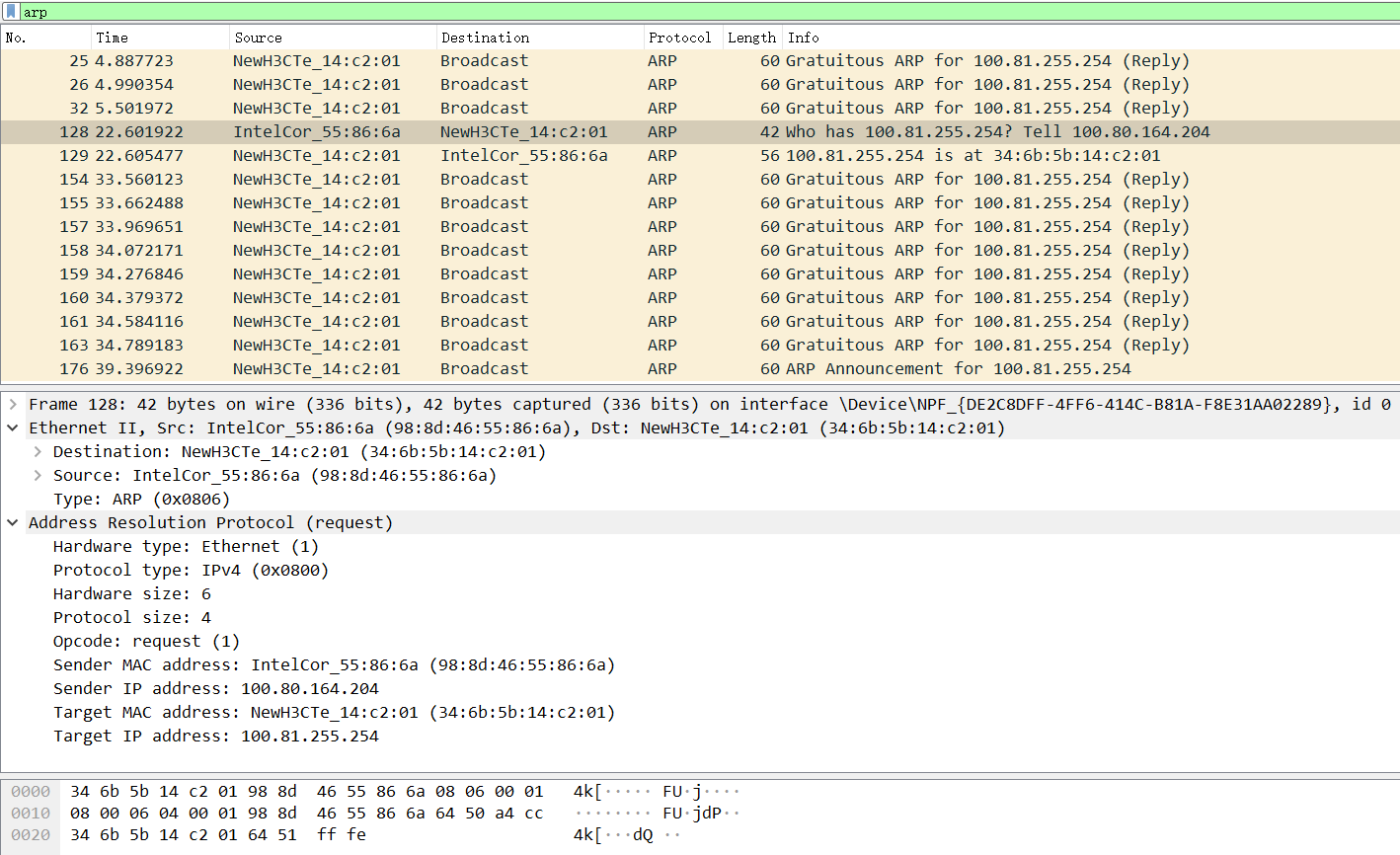
路由器接收到，表明请求ARP成功：



5.查看终端的ARP命令：



6.WireShark抓取ARP报文：



**【分析讨论】**

在使用WireShark进行分析的过程中，我发现ARP报文的发送方发送了一个ARP请求，请求目标主机的MAC地址。然后，目标主机收到ARP请求后，回复一个ARP应答，将自己的MAC地址告知发送方。通过这样的过程，发送方就能够知道目标主机的MAC地址，进一步实现了IP地址到MAC地址的映射。

ARP协议在局域网中扮演着非常重要的角色，它通过建立IP地址和MAC地址之间的映射关系，实现了数据包的正确转发。在实际网络环境中，ARP协议的正常工作对于保证网络的正常通信至关重要。