【实验名称：ARP消息分析实验】

学生姓名：李雪菲 合作学生：无

实验地点：济事楼330 实验时间：2025-05-08

【实验目的】

1. 验证地址解析协议(ARP)完成地址解析的过程
2. 验证ARP报文结构
3. 验证显示和清除终端ARP缓存器内容的命令

【实验原理】

1. 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。

二、ARP协议

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。但这个目标MAC地址是如何获得的呢？它就是通过地址解析协议获得的。

三、ARP报文

ARP报文的总长度为64字节。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软件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 = 42 bytes；而真正发包时为了保证以太网帧的最小帧长为64bytes，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60bytes。比以太网帧的最小帧长扫了4bytes，原因是因为wireshark抓包时不能抓到数据包最后的CRC 字段。

【实验设备】

1.一台电脑

2.cisco packet tracer 仿真软件

3.wireshark 软件

【实验步骤】

1.分析在Packet tracer中ARP报文情况

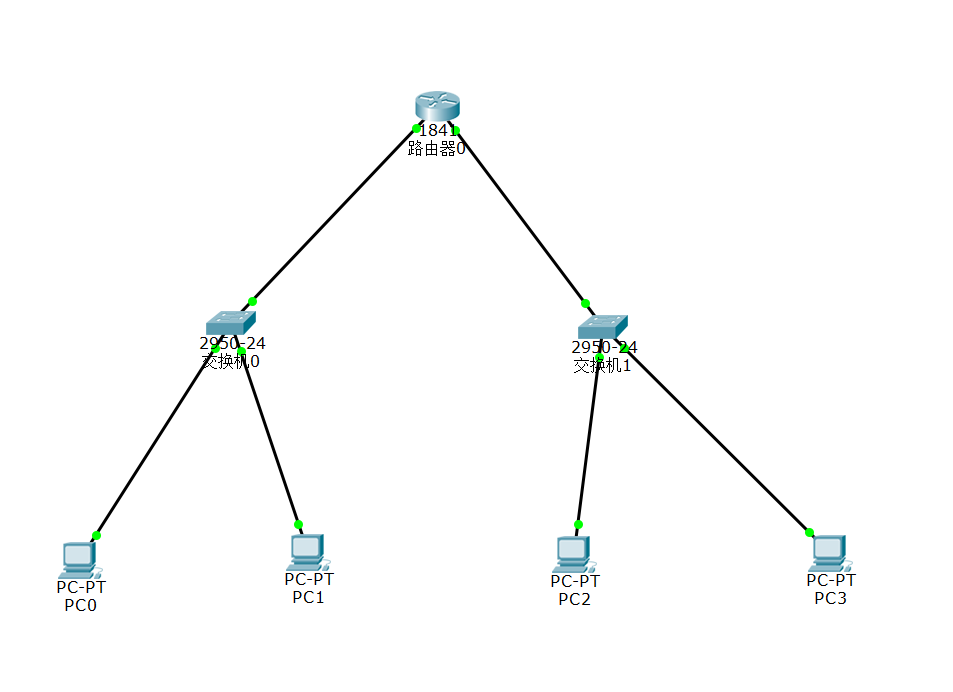
2.查看ARP报文各字段内容，并解读

3.查看本机的ARP内容

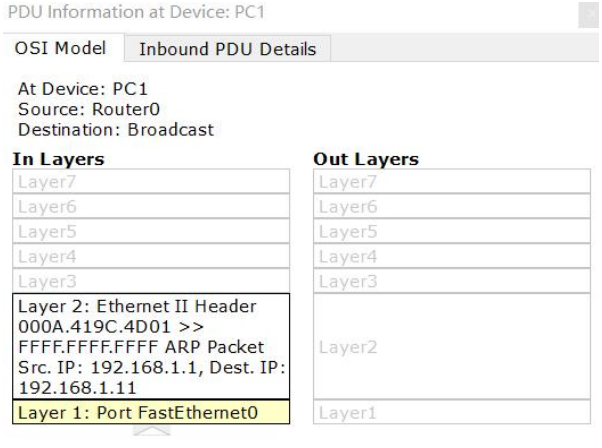
4.用WireShark抓取ARP数据包，并分析各字段信息内容

【实验现象】

一、在Packet tracer中ARP报文情况



抓取ARP报文并且分析报文



At Device: Router1：显示该信息来自 Router1 设备。

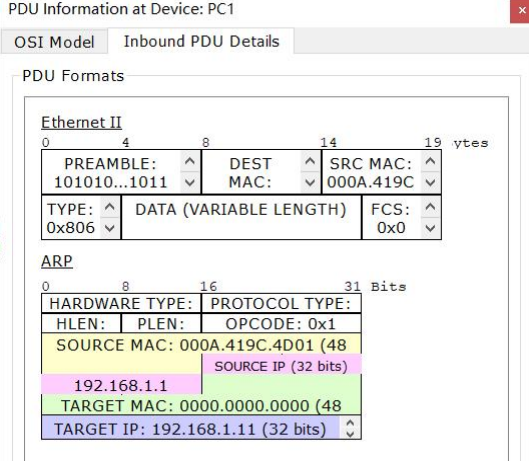
Source：PC1：数据包源自 PC1。

Destination：Broadcast：这是一个广播包，目标是所有设备

Layers：

Layer 1：物理层，数据包通过相同的 FastEthernet0/1 端口发送出去。

Layer 2：数据链路层，显示了 Ethernet II 帧头信息。此时源 MAC地址为 000E.8FAC.8302，目标 MAC 地址为 0002.1722.CDCA。ARP 响应的源 IP 为 192.168.2.1，目标 IP 为 192.168.2.13。



Ethernet II：

Preamble（前导码）：起始部分为 101010...1011，这部分用于同步网络设备之间的时钟频率，以确保数据的正确解读。

Destination MAC（目标 MAC 地址）：为 FFFF.FFFF.FFFF，这是一个广播地址，表示该 ARP 请求被发送到所有设备。

Source MAC（源 MAC 地址）：为 0002.1722.CDCA，这是发送该请求的设备的物理地址。

Type（类型）：0x806，表示这个帧携带的数据是 ARP 协议的数据。

Data（数据）：数据部分是可变长度的，包括 ARP 请求的具体内容。

FCS（帧检验序列）：为 0x0，用于错误检测的帧尾，虽然在此图示中显示为 0，实际操作中由网络设备计算并添加。

ARP：

Hardware Type（硬件类型）：0x1，表示这是以太网（Ethernet）。

Protocol Type（协议类型）：0x0800，表示上层协议是 IP。

HLEN（硬件地址长度）：0x06，表示硬件地址（MAC 地址）的长度为 6 字节。

PLEN（协议地址长度）：0x04，表示协议地址（IP 地址）的长度为 4 字节。

Opcode（操作码）：0x01，表示这是一个 ARP 请求（请求 MAC 地址）。

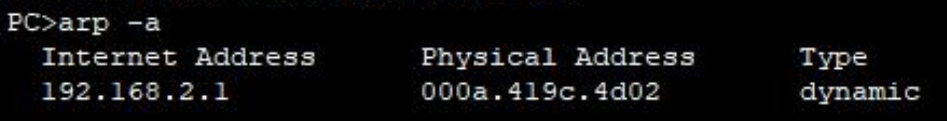
Source MAC Address：0002.1722.CDCA，请求方的物理地址。

Source IP Address：192.168.2.13，请求方的 IP 地址。

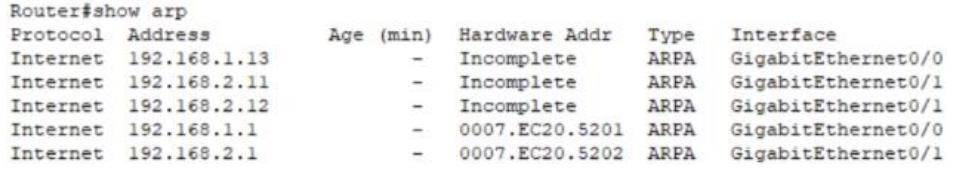
Target MAC Address：0000.0000.0000，目标方的 MAC 地址在请求时未知，因此全为 0。

Target IP Address：192.168.2.1，目标方的 IP 地址，即发送方希望获取 MAC 地址的 IP 地址。

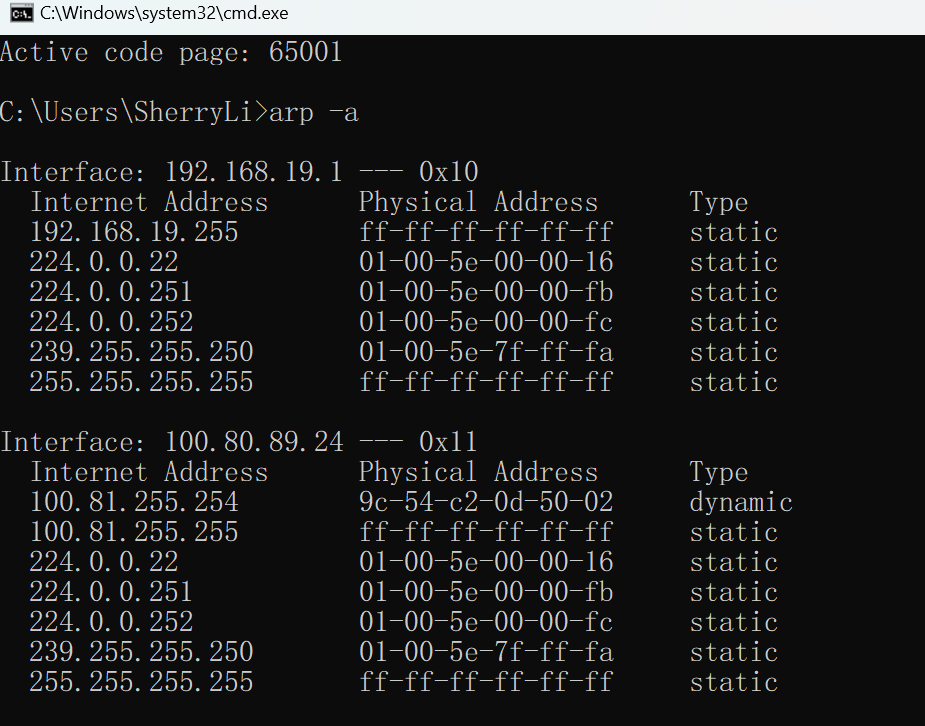
查看终端的ARP命令



当前路由器 Router 的 ARP 表



1. 本机的ARP内容



1. 接口：192.168.178.1 --- 0x2

IP 地址 192.168.178.255：这是一个子网广播地址，MAC 地址为 ff-ffff-ff-ff-ff，标记为静态，表示这个地址是用于广播消息到本地网络上的所有设备。

IP 地址 224.0.0.22，224.0.0.251，224.0.0.252：这些都是多播地址，对应的 MAC 地址以 01-00-5e 开头，根据多播 IP 到 MAC 地址映射的标准来设定，也都是静态条目。

IP 地址 239.255.255.250：同样是一个多播地址，用于特定的多播服务，如 SSDP（简单服务发现协议），MAC 地址同样为静态。

2. 接口：100.81.138.91 --- 0x6

IP 地址 100.81.255.254：这个地址可能是该接口的默认网关或者某个特定服务的地址，MAC 地址为 9c-54-c2-0d-50-02，标记为动态，表示这个地址是从网络上动态学习的。

IP 地址 100.81.255.255：这是该子网的广播地址，用于广播消息到这个特定子网的所有设备，MAC 地址为 ff-ff-ff-ff-ff-ff，标记为静态。

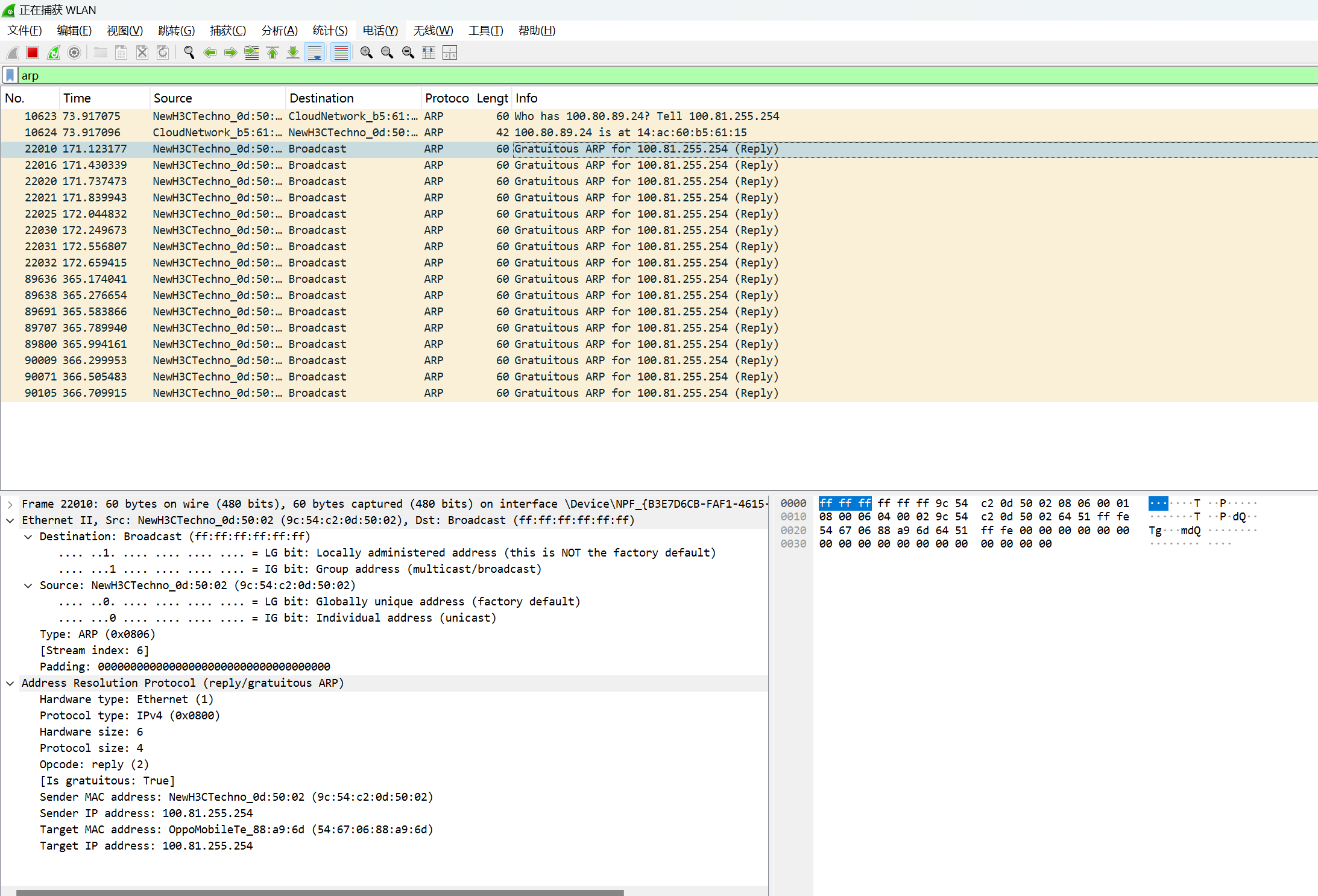
其余 IP 地址：包括多播地址和广播地址，与第一个接口的描述相同。

3. 接口：192.168.216.1 --- 0x1b

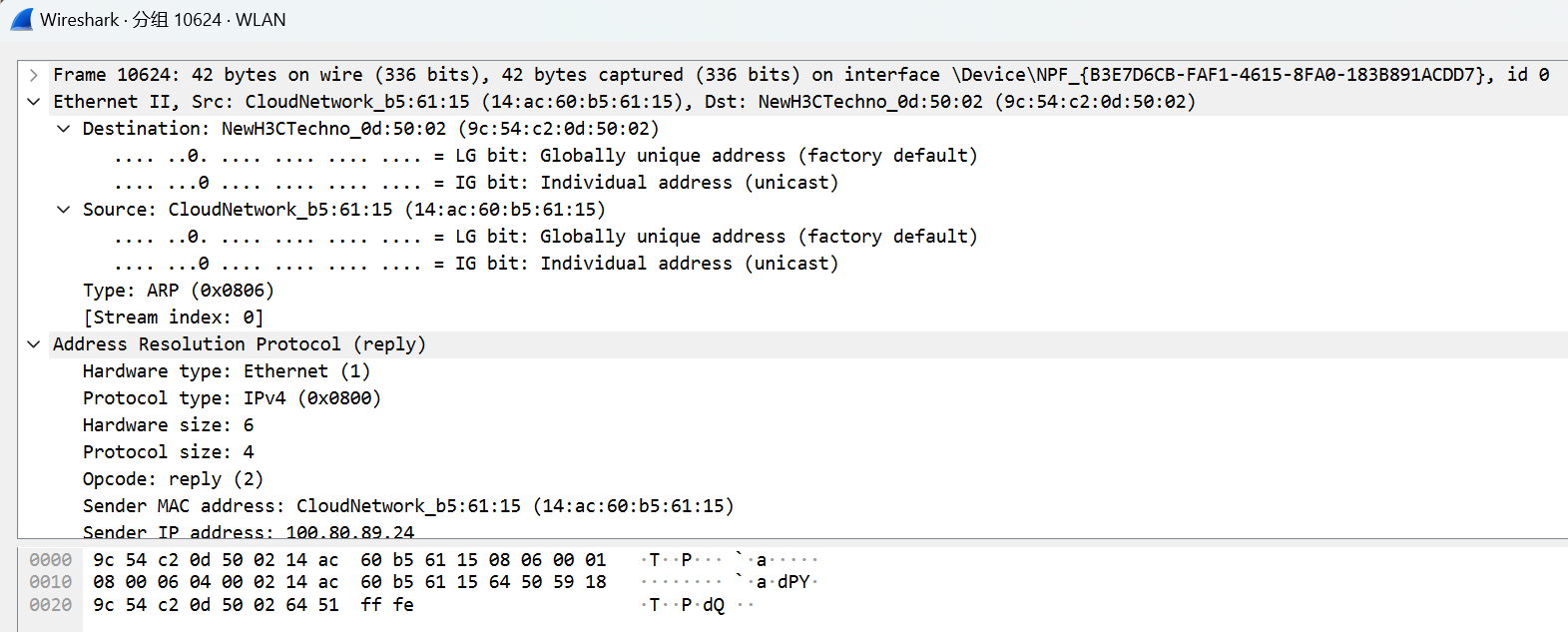
IP 地址 192.168.216.255：这是该子网的广播地址，用于广播消息到这个特定子网的所有设备，MAC 地址为 ff-ff-ff-ff-ff-ff，标记为静态。

其余 IP 地址：包括多播地址和广播地址，与前面的接口描述相同。

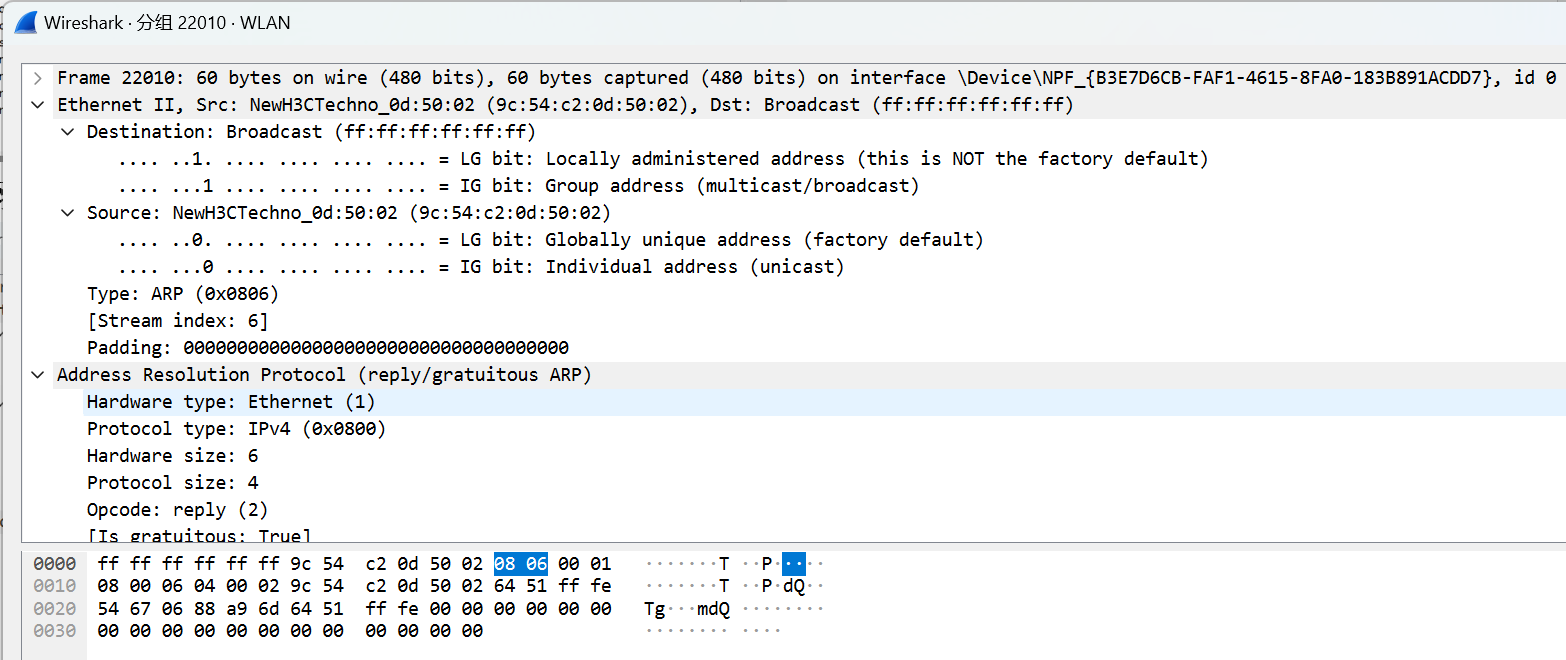
1. 用WireShark抓取ARP数据包



请求报文



响应报文



【分析讨论】

1. ARP 表的初步观察

在使用 arp -a 命令查看 ARP 表时，可以看到本机已知的网络设备的 IP 地址和 MAC 地址列表。这显示了当前设备已经学习到的网络内部的 IP 到 MAC 地址映射。

2. 清除 ARP 缓存后的变化

执行 arp -d 清除 ARP 缓存后，再次使用 arp -a 查看 ARP 表时，表中内容减少或显示为空。清除 ARP 缓存后，本机删除了所有动态学习的 IP 到 MAC 地址映射。这表明 ARP 缓存是动态的，设备通过网络通信实时更新这些信息。

3. ARP 缓存自动恢复

一段时间后，再次使用 arp -a 命令，发现 ARP 表已经重新填充了一些条目。这说明操作系统和网络设备在网络活动中自动重新学习了 IP 到 MAC 的映射这可能通过 ARP 请求和响应，或通常的网络交互过程自动完成。