实验报告：ARP 实验四

课程名称：计算机网络实践　**年级：**大二　**上机实践成绩：**

指导教师：章玥　**姓名：**邱吉尔

学号：10235101533　**上机实践日期：2024/12/9**

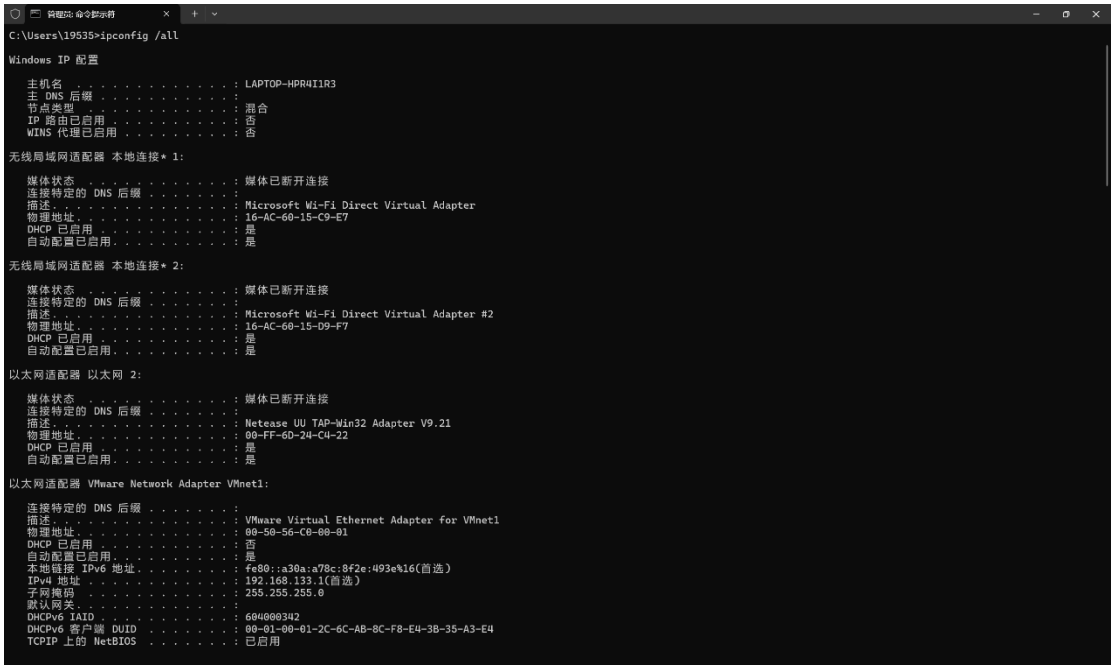
一、目的

1. **学会通过 Wireshark 获取 ARP 消息**
2. **掌握 ARP 数据包结构**
3. **掌握 ARP 数据包各字段的含义**
4. **了解 ARP 协议适用领域**

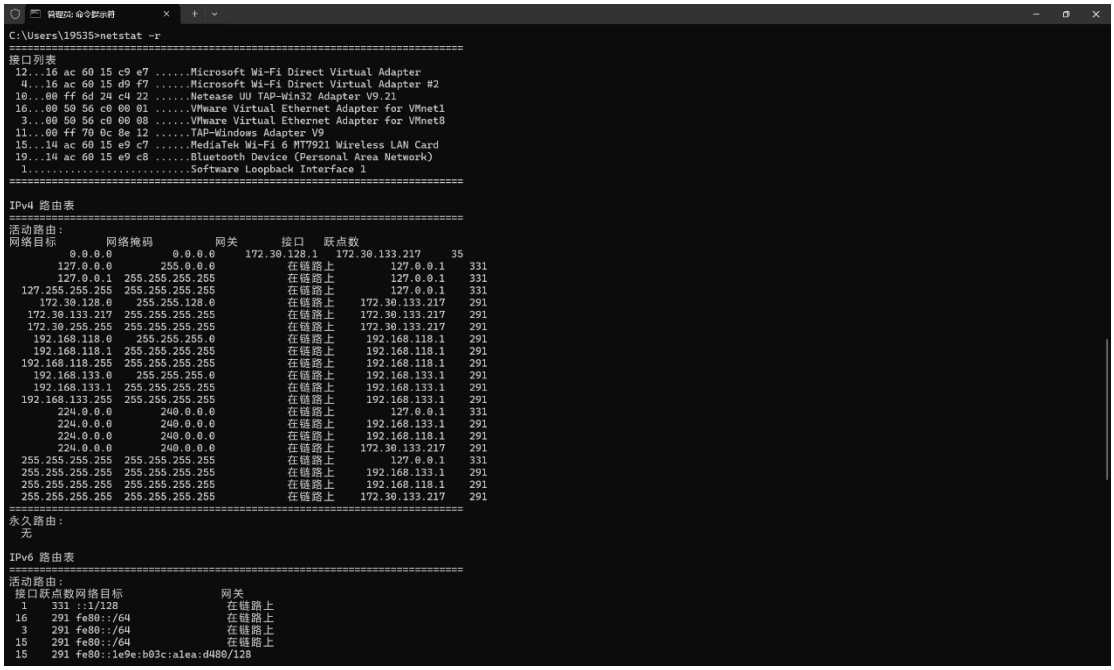
二、实验步骤

1. **捕获 Trace**

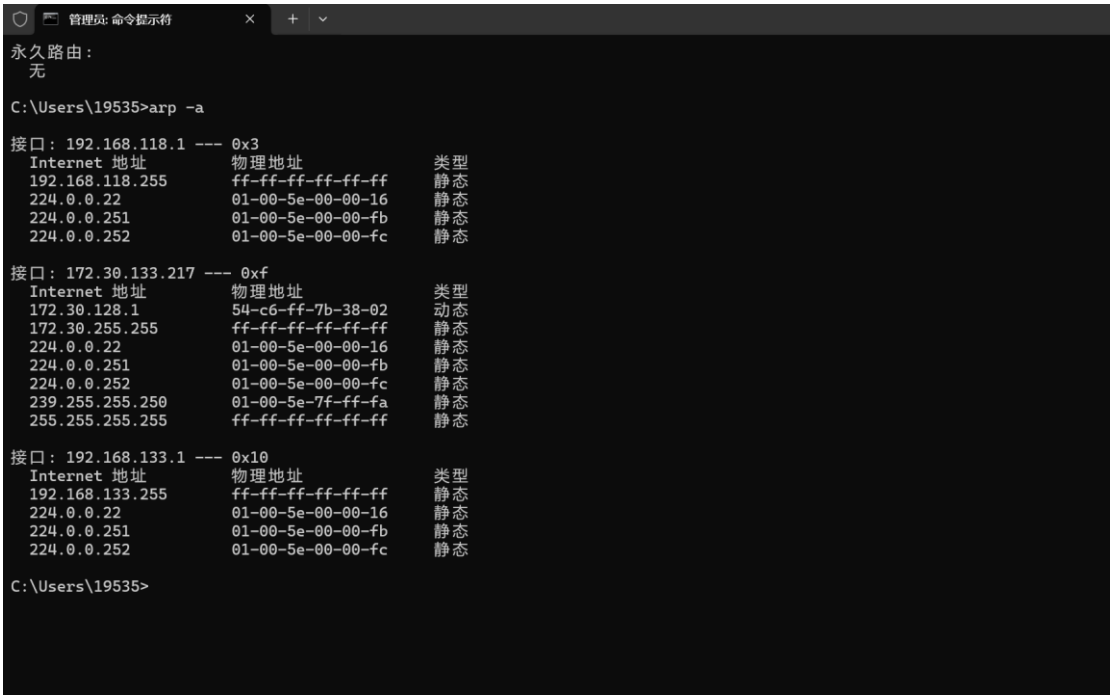
ipconfig /all:



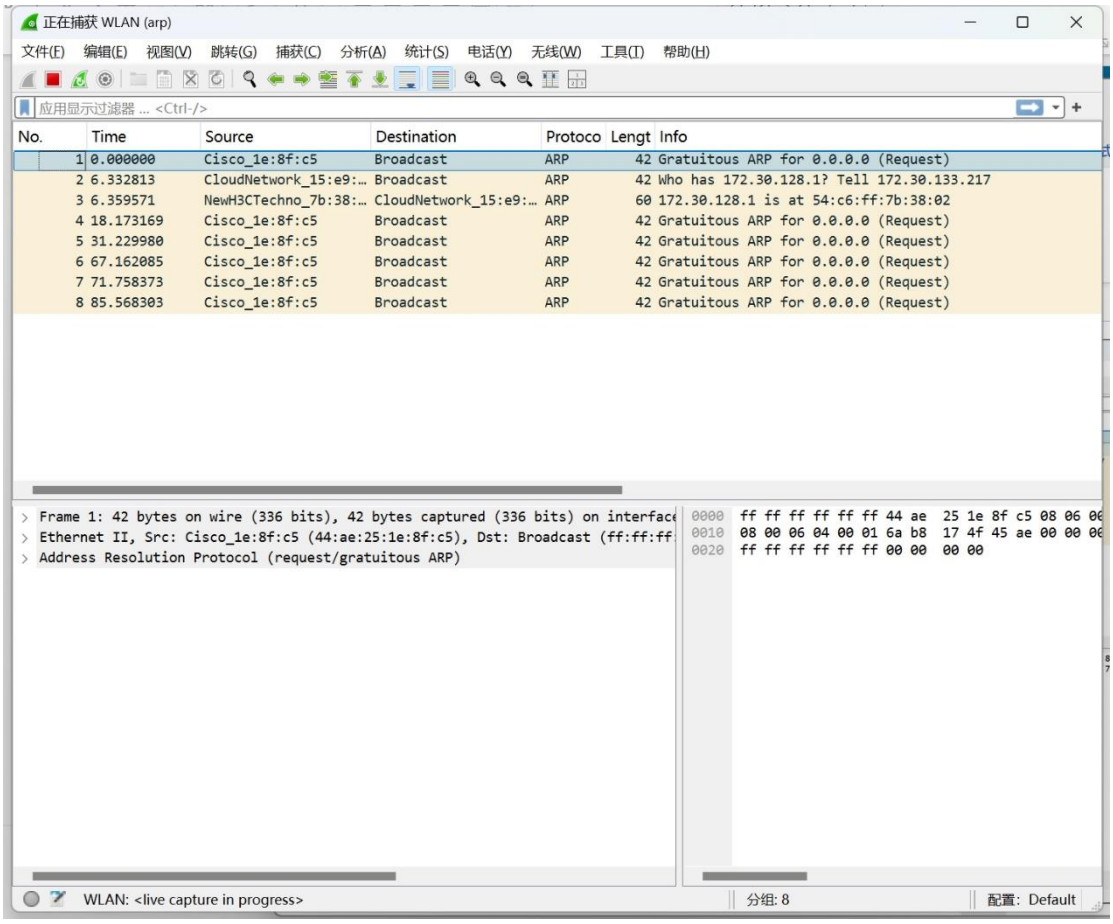
netstat -r:


管理员: 命令提示符
C:\Users\19535>netstat -r
接口列表
12...16 ac 60 15 c9 e7 ......Microsoft Wi-Fi Direct Virtual Adapter
4...16 ac 60 15 d9 f7 ......Microsoft Wi-Fi Direct Virtual Adapter #2
10...00 ff 6d 24 c4 22 ......Netease UU TAP-Win32 Adapter V9.21
16...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
3...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
11...00 ff 70 0c 8e 12 ......TAP-Windows Adapter V9
15...14 ac 60 15 e9 c7 ......MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
19...14 ac 60 15 e9 c8 ......Bluetooth Device (Personal Area Network)
1...........................Software Loopback Interface 1
IPv4 路由表
活动路由:
网络目标 网络掩码 网关 接口 跃点数
0.0.0.0 0.0.0.0 172.30.128.1 172.30.133.217 35
127.0.0.0 255.0.0.0 在链路上 127.0.0.1 331
127.0.0.1 255.255.255.255 在链路上 127.0.0.1 331
127.255.255.255 255.255.255.255 在链路上 127.0.0.1 331
172.30.128.0 255.255.128.0 在链路上 172.30.133.217 291
172.30.133.217 255.255.255.255 在链路上 172.30.133.217 291
172.30.255.255 255.255.255.255 在链路上 172.30.133.217 291
192.168.118.0 255.255.255.0 在链路上 192.168.118.1 291
192.168.118.1 255.255.255.255 在链路上 192.168.118.1 291
192.168.118.255 255.255.255.255 在链路上 192.168.118.1 291
192.168.133.0 255.255.255.0 在链路上 192.168.133.1 291
192.168.133.1 255.255.255.255 在链路上 192.168.133.1 291
192.168.133.255 255.255.255.255 在链路上 192.168.133.1 291
224.0.0.0 240.0.0.0 在链路上 127.0.0.1 331
224.0.0.0 240.0.0.0 在链路上 192.168.133.1 291
224.0.0.0 240.0.0.0 在链路上 192.168.118.1 291
224.0.0.0 240.0.0.0 在链路上 172.30.133.217 291
255.255.255.255 255.255.255.255 在链路上 127.0.0.1 331
255.255.255.255 255.255.255.255 在链路上 192.168.133.1 291
255.255.255.255 255.255.255.255 在链路上 192.168.118.1 291
255.255.255.255 255.255.255.255 在链路上 172.30.133.217 291
永久路由:
无
IPv6 路由表
活动路由:
接口 跃点数 网络目标 网关
1 331 ::1/128 在链路上
16 291 fe80::/64 在链路上
3 291 fe80::/64 在链路上
15 291 fe80::/64 在链路上
15 291 fe80::1e9e:b03c:a1ea:d480/128

arp -a:

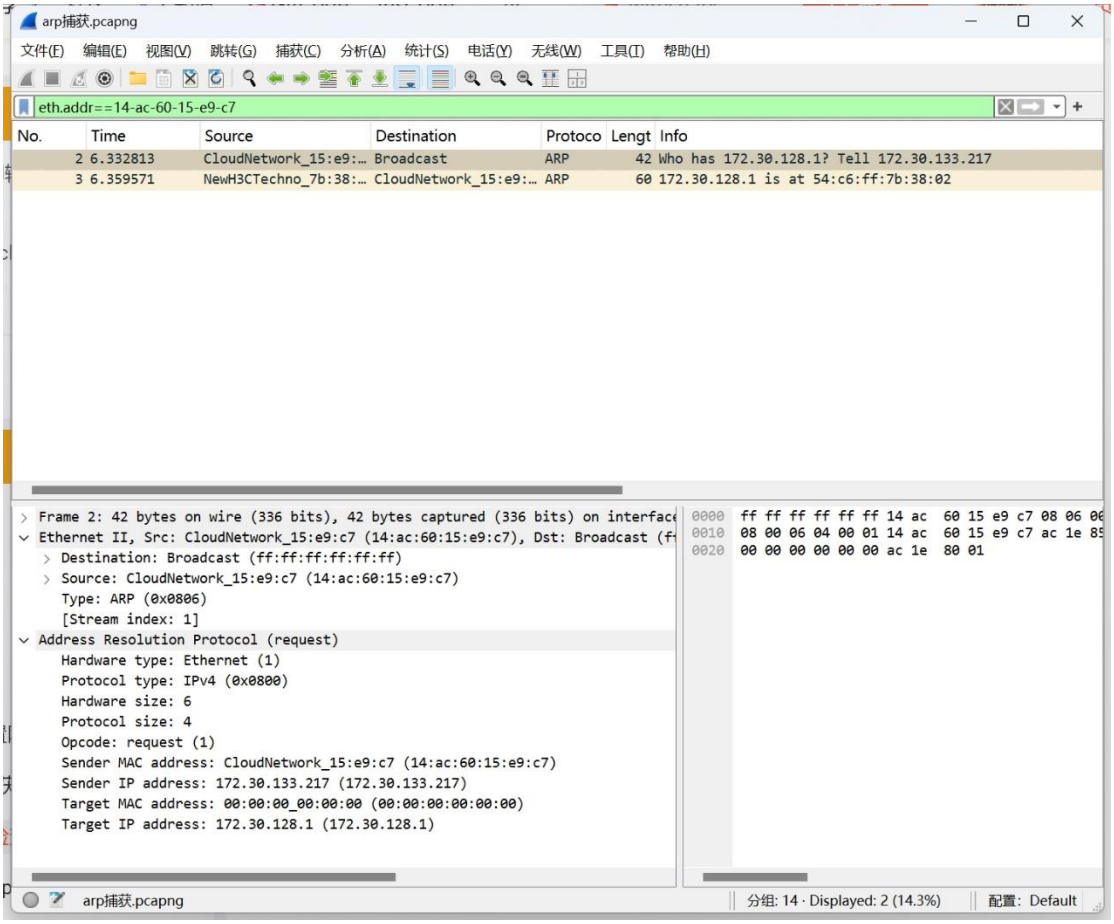

管理员: 命令提示符
永久路由:
无
C:\Users\19535>arp -a
接口: 192.168.118.1 --- 0x3
Internet 地址 物理地址 类型
192.168.118.255 ff-ff-ff-ff-ff-ff 静态
224.0.0.22 01-00-5e-00-00-16 静态
224.0.0.251 01-00-5e-00-00-fb 静态
224.0.0.252 01-00-5e-00-00-fc 静态
接口: 172.30.133.217 --- 0xf
Internet 地址 物理地址 类型
172.30.128.1 54-c6-ff-7b-38-02 动态
172.30.255.255 ff-ff-ff-ff-ff-ff 静态
224.0.0.22 01-00-5e-00-00-16 静态
224.0.0.251 01-00-5e-00-00-fb 静态
224.0.0.252 01-00-5e-00-00-fc 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态
255.255.255.255 ff-ff-ff-ff-ff-ff 静态
接口: 192.168.133.1 --- 0x10
Internet 地址 物理地址 类型
192.168.133.255 ff-ff-ff-ff-ff-ff 静态
224.0.0.22 01-00-5e-00-00-16 静态
224.0.0.251 01-00-5e-00-00-fb 静态
224.0.0.252 01-00-5e-00-00-fc 静态
C:\Users\19535>

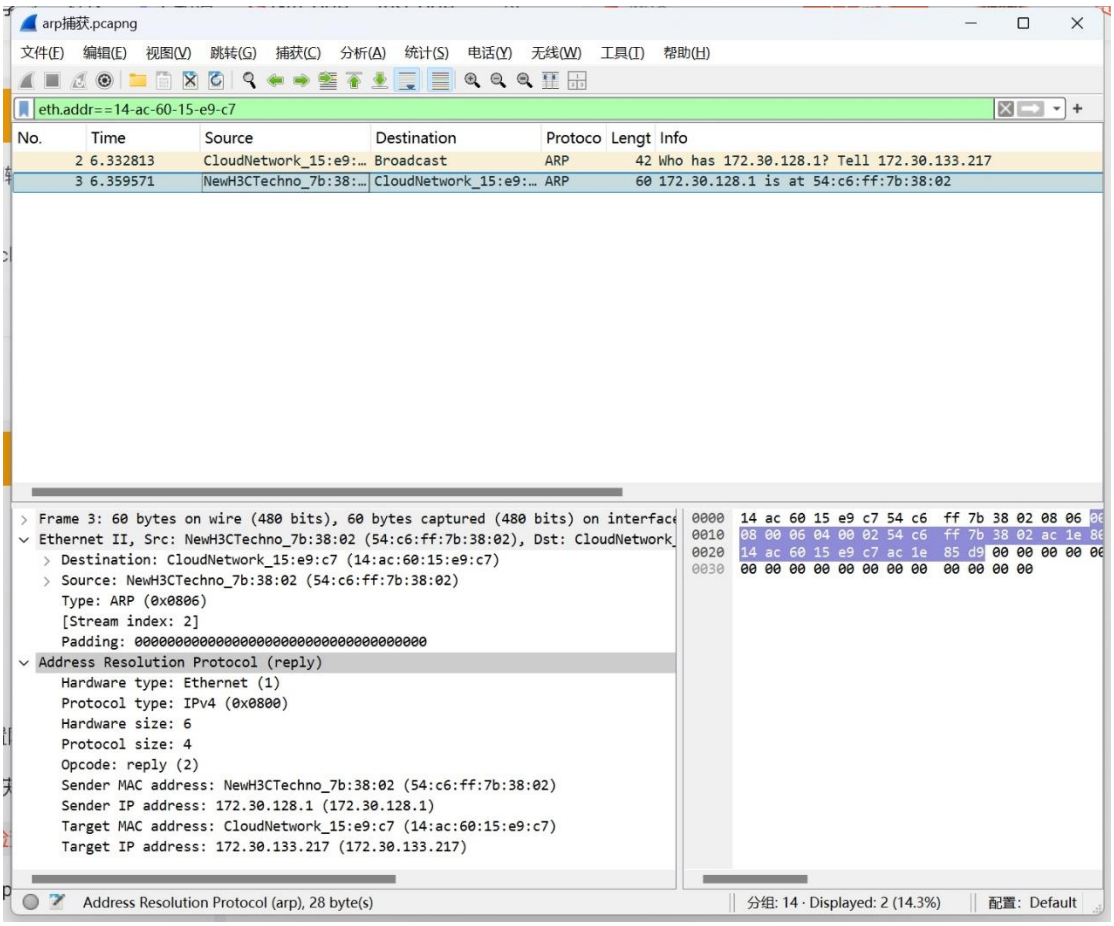
arp 报文：



2. 分析 Wireshark 捕获到的 arp 报文：

①通过语句“eth.addr==01:02:03:04:05:06”的形式，在 wireshark 中设置过滤器，找出与自己 mac 地址相关的 arp 报文。 Arp 报文包括请求报文和应答报文，仔细分析两种报文的格式。


arp捕获.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
eth.addr==14-ac-60-15-e9-c7
No. Time Source Destination Protoco Lengt Info
2 6.332813 CloudNetwork_15:e9:... Broadcast ARP 42 Who has 172.30.128.1? Tell 172.30.133.217
3 6.359571 NewH3CTechno_7b:38:... CloudNetwork_15:e9:... ARP 60 172.30.128.1 is at 54:c6:ff:7b:38:02
Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
Ethernet II, Src: CloudNetwork_15:e9:c7 (14:ac:60:15:e9:c7), Dst: Broadcast (ff
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: CloudNetwork_15:e9:c7 (14:ac:60:15:e9:c7)
Type: ARP (0x0806)
[Stream index: 1]
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: CloudNetwork_15:e9:c7 (14:ac:60:15:e9:c7)
Sender IP address: 172.30.133.217 (172.30.133.217)
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 172.30.128.1 (172.30.128.1)
0000 ff ff ff ff ff ff 14 ac 60 15 e9 c7 08 06 00
0010 08 00 06 04 00 01 14 ac 60 15 e9 c7 ac 1e 85
0020 00 00 00 00 00 00 ac 1e 80 01
arp捕获.pcapng
分组: 14 · Displayed: 2 (14.3%)
配置: Default

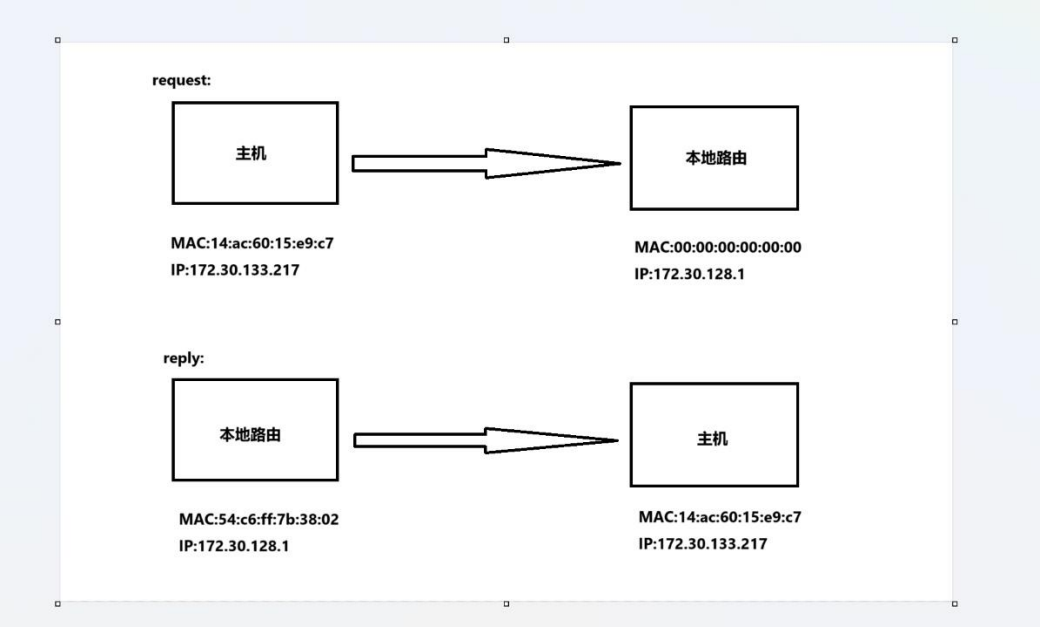


No.2 为请求报文，No.3 为应答报文

请求报文的 Sender MAC address 和 Sender IP address 是本机地址，而应答报文的 Target MAC address 和 Target IP address 是本机地址

且二者的 Opcode 字段不相同

②画出你的计算机和本地路由间 ARP 的请求和应答数据包，标记出请求和应答，为每个数据包给出发送者和接受者的 MAC 和 IP 地址。



③分析报文，回答问题：

a. 什么样的操作码是用来表示一个请求？应答呢？

操作码=1 表示一个请求，操作码=2 表示一个应答

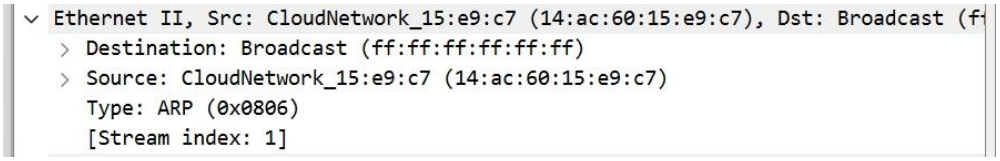
b. 一个请求的 ARP 的报头有多大？应答呢？

两者都是 28 字节

c. 对未知目标的 MAC 地址的请求是什么值？

00:00:00:00:00:00

d. 什么以太网类型值说明 ARP 是更高一层的协议？



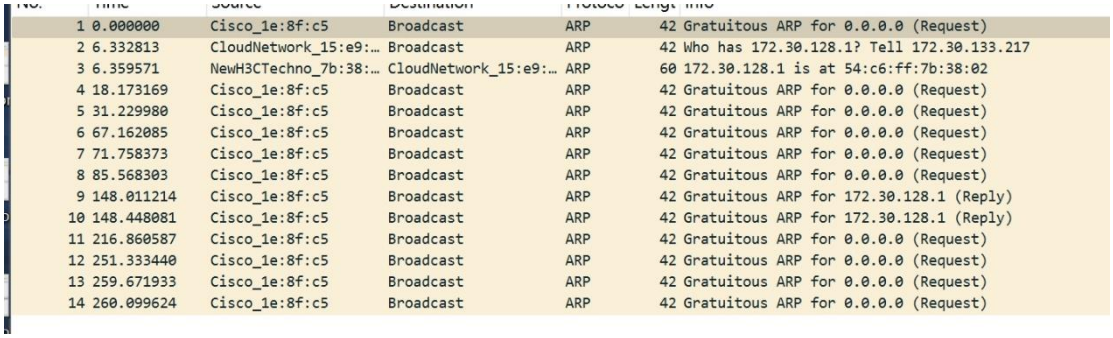
0x0806

e.ARP 应答是广播吗？

不是，是单播的，只发送给请求的地址

三、在完成本实验后，思考下列问题：

去除过滤器，我们发现还有更多的 arp 报文。请研究这些额外的 arp 报文中，有什么其他的功能作用。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
2	6.332813	CloudNetwork_15:e9:…	Broadcast	ARP	42	Who has 172.30.128.1? Tell 172.30.133.217
3	6.359571	NewH3CTechno_7b:38:…	CloudNetwork_15:e9:…	ARP	60	172.30.128.1 is at 54:c6:ff:7b:38:02
4	18.173169	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
5	31.229980	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
6	67.162085	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
7	71.758373	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
8	85.568303	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
9	148.011214	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
10	148.448081	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 172.30.128.1 (Reply)
11	216.860587	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
12	251.333440	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
13	259.671933	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
14	260.099624	Cisco_1e:8f:c5	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)

可以看到更多的 ARP 报文 info 是 Gratuitous ARP for……，即为免费 ARP，其主要作用是：

i. 起到一个宣告作用。以广播的形式将数据包发送出去，不需要得到回应，只为了告诉其他计算机自己的 IP 地址和 MAC 地址。

ii. 可用于检测 IP 地址冲突。当一台主机发送了免费 ARP 请求报文后，如果收到了 ARP 响应报文，则说明网络内已经存在使用该 IP 地址的主机。

iii. 可用于更新其他主机的 ARP 缓存表。如果该主机更换了网卡，而其他主机的 ARP 缓存表仍然保留着原来的 MAC 地址。这时，可以发送免费的 ARP 数据包。其他主机收到该数据包后，将更新 ARP 缓存表，将原来的 MAC 地址替换为新的 MAC 地址。