1.due day:20221108（周二）22点。

2.至ftp服务器“作业/班级/20221104第五次实验[截止20221108-2200]”，届时未下载到，视未提交。

3.文件名：学号姓名.doc,如“23094202张三.doc”

**实验4-1:P+Ethernet+ARP**

# 1 实验目的

查看IPv4封装、Ethernet帧封装、ARP协议的工作过程，了解各字段含义及功能。

# 2 实验内容及要求

使用之前实验中用到的虚拟机环境，cmd下，host OS ping Geust OS,或反之。

在host OS上，启用wireshark抓包，过滤协议写icmp就能看到了！！

cmd下执行操作，

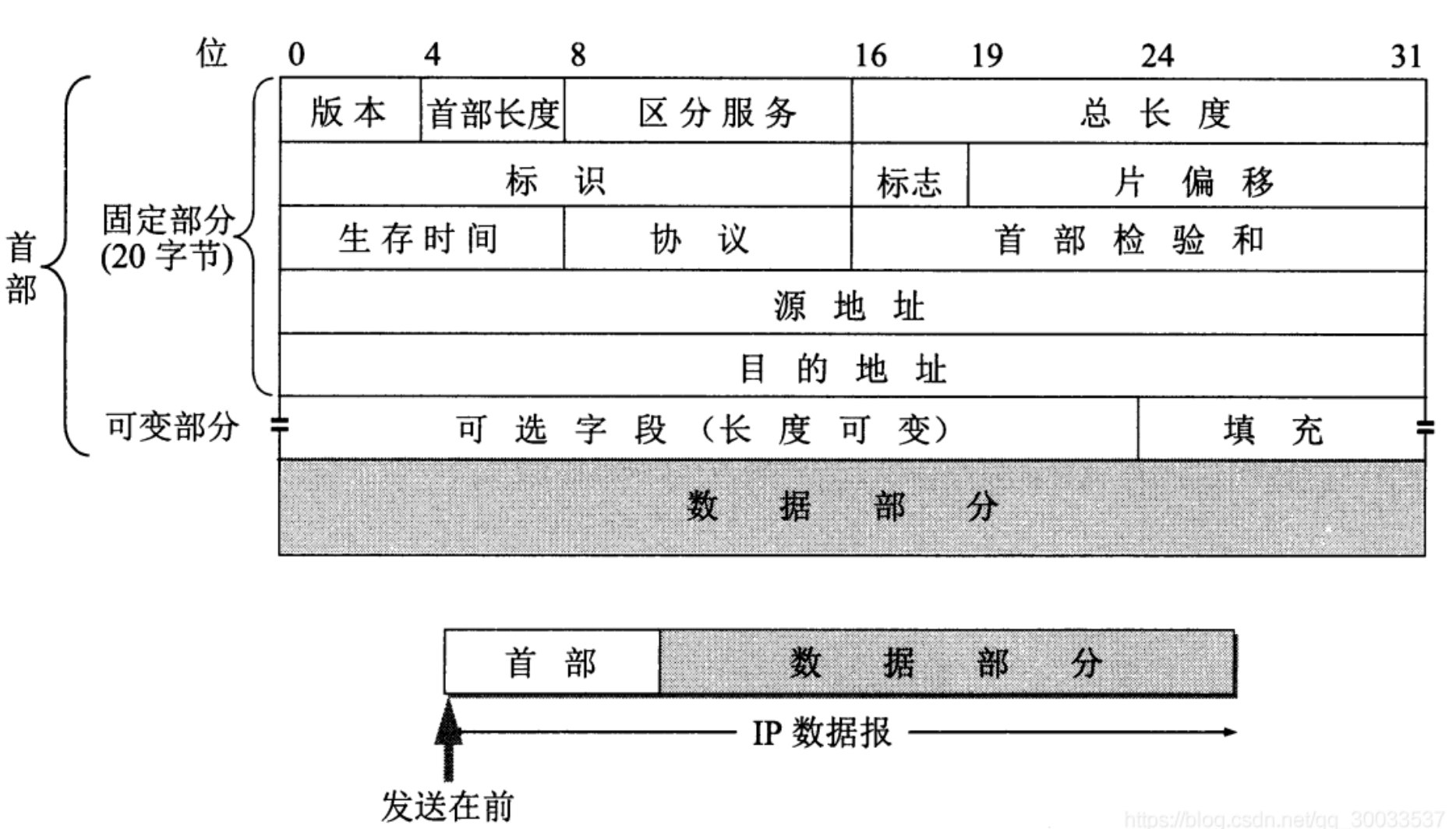
Host ping Guest，则在Host上启用wireshark抓包。

Guest ping Host，则在Guest上启用wireshark抓包。

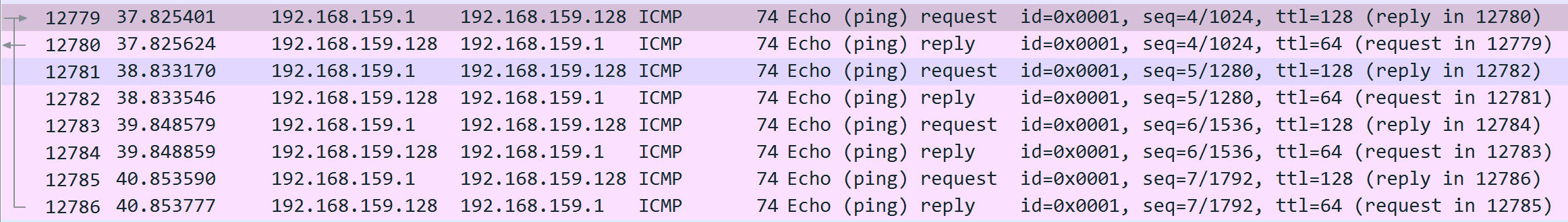
## (1)关于IPv4 header:

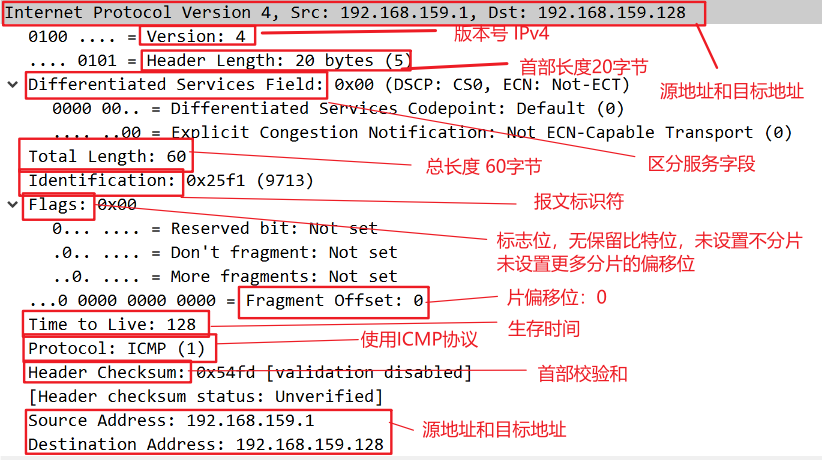
### a.逐字段的含义。

总概况：



ICMP即是捕获ping命令的数据包：

报文各字段内容及对应如下：



从网络上查阅到各个字段的含义如下：

1. 版本：占4位。指IP协议是IPv4还是IPv6，通信双方的版本必须一致。
2. 首部长度：占4位。以4B为单位，最大值为60B。默认情况下首部长度看成20B，此时不使用任何选项（即可选字段）。
3. 总长度：占16位。指首部和数据之和的长度，以1B为单位，因此数据报最大长度为216-1=65535B。以太网的最大传送单元（MTU）为1500B，因此当一个IP数据包封装成帧时，数据包总长度一定不能超过数据链路层的MTU值。
4. 标识：占16位。它是一个计数器，每产生一个数据报就加1，但它并不是“序号”（IP是无连接服务）。当一个数据报长度超过网络的MTU时，必须分片，此时每个数据报片都复制一次标识号以便能重装成原来的数据报。重装数据报是在目的端主机完成的。
5. 标志：占3位。目前只有前两位有效，即MF和DF。MF=1表示后面还有分片；MF=0表示这是最后一个分片。DF=0允许分片；DF=1不允许片。
6. 片偏移：占13位。指明了每个分片相对于原始报文开头的偏移量，以8B为单位，即每个分片的长度必须是8B的整数倍。
7. **生存时间（TTL）：占8位。报文经过的每个路由器都将此字段减1，当此字段等于0时，丢弃该报文，确保报文不会永远在网络中循环。**
8. **协议：占8位。指出携带的数据应交给那个传输层协议，值为6表TCP；值为17表示UDP。**
9. 首部检验和：占16位。只检验数据报首部，不检验数据部分。
10. 源地址：占32位。表示发送方的IP地址。
11. 目的地址：占32位。表示接收方的IP地址。

### b.对(执行ping命令)所捕获的IP报文而言，该 IPv4 header 中 protocol type 字段的值是几？

是1

1. 请查阅教材，若 IP data 部分封装的是 TCP 报文，那IP首部中 protocol type 的数值是多少？

是6

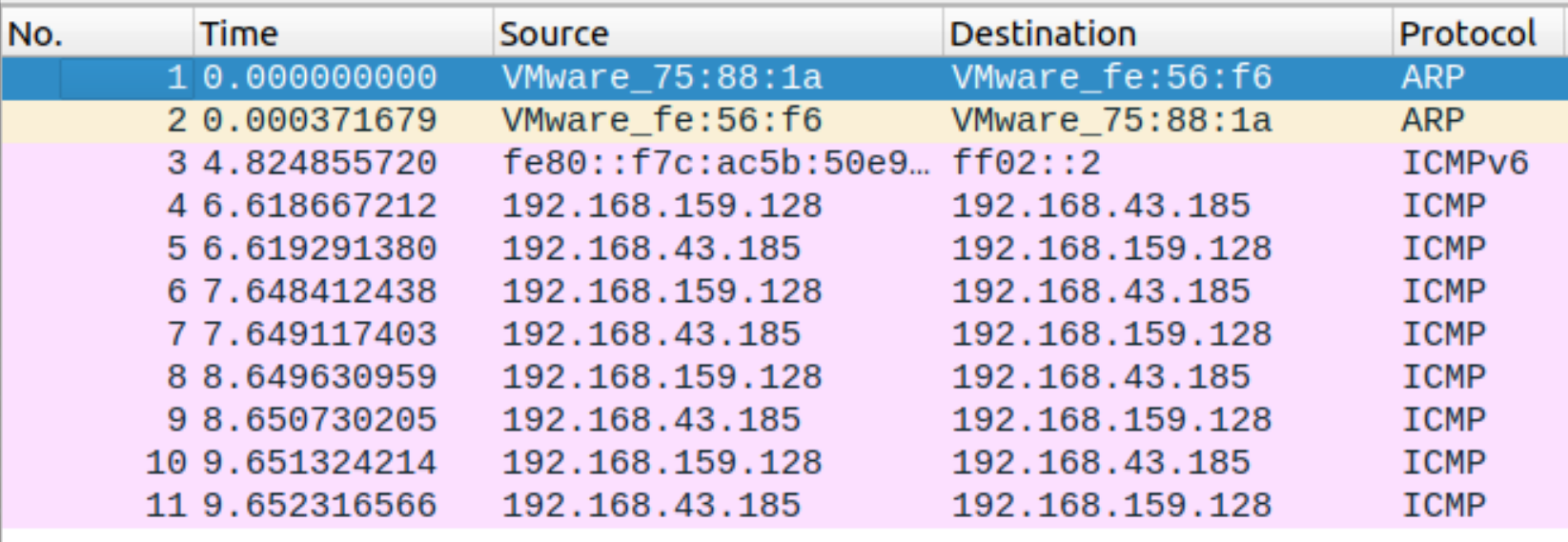
1. 若封装的是 UDP 报文，protocol type 字段的数值是多少？

是17

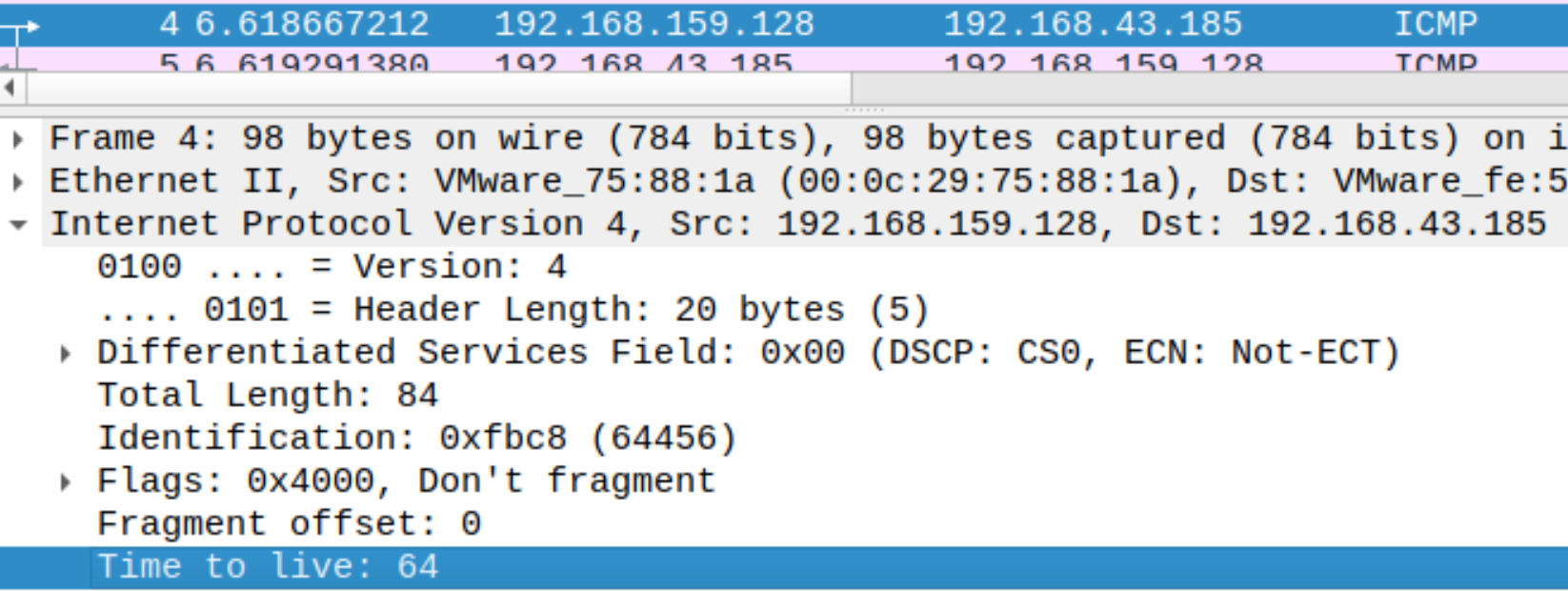
### c.两种操作：从host ping guest、从guest ping host，分别捕获的IP数据包首部中的TTL字段值相同吗？

Host ping guest：TTL=128

Guest ping host：



Request 报文如下：TTL=64，不同



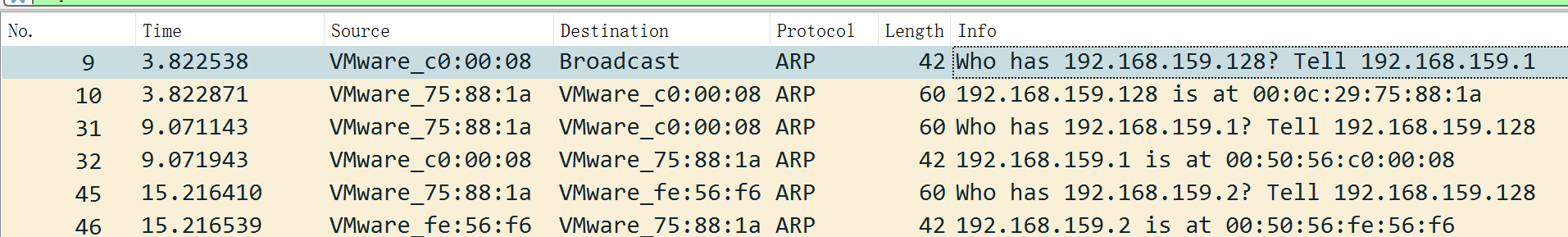
## (2)关于ARP:

(为了能触发ARP工作，在host OS的命令行/cmd模式下，要先清空arp缓存表。先使用 arp-a 查看 arp 缓存；再用命令“arp-d”删除缓存中的 IP 与 mac 的绑定”，请查阅arp命令。）

如图，删除主机到虚拟机的arp缓存



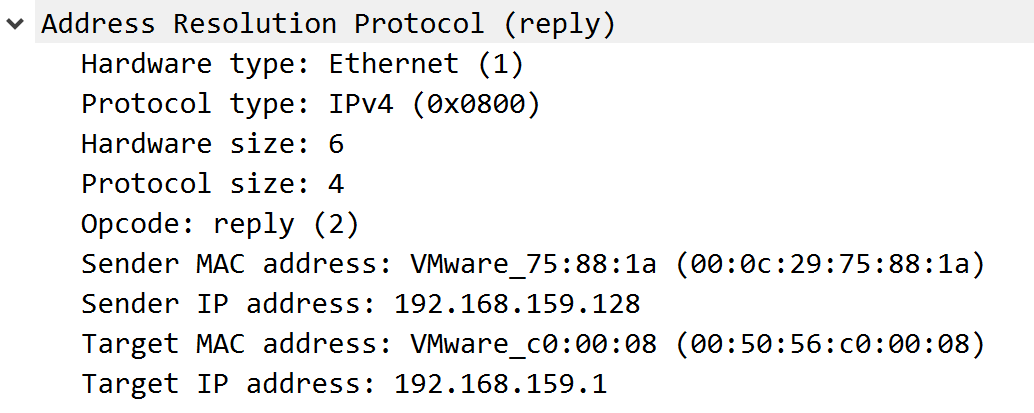
抓包的报文如图所示：



Request报文：



Reply报文：



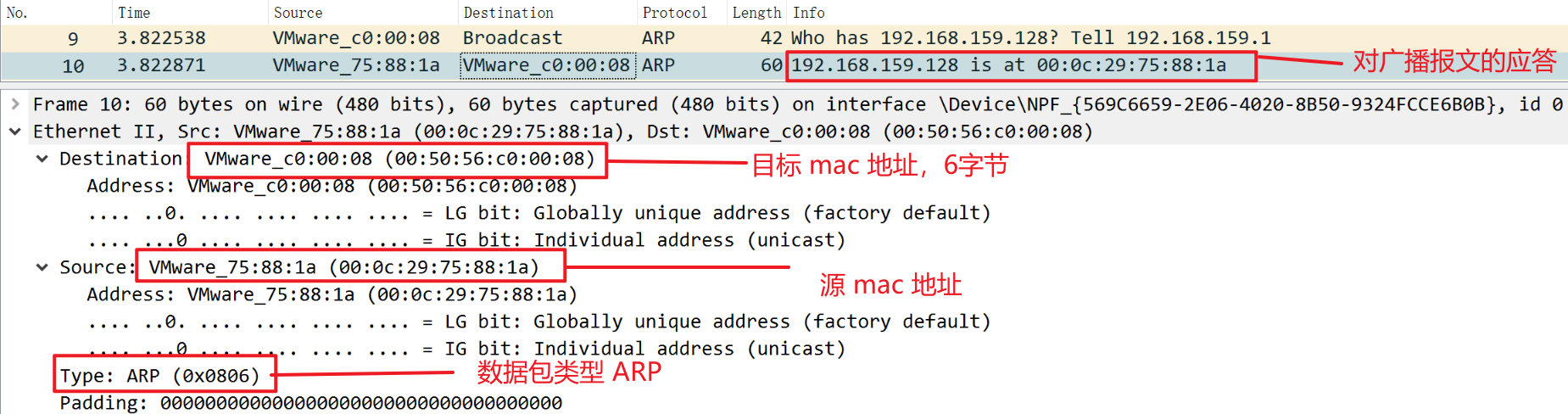
### ARP报文中，哪个字段用来区分该报文是 ARP Request 还是 ARP Reply?

Opcode，1表示request，2表示reply

### ARP Request 报文所在 Ethernet 帧中的目的MAC地址是什么？这个地址是什么意思？

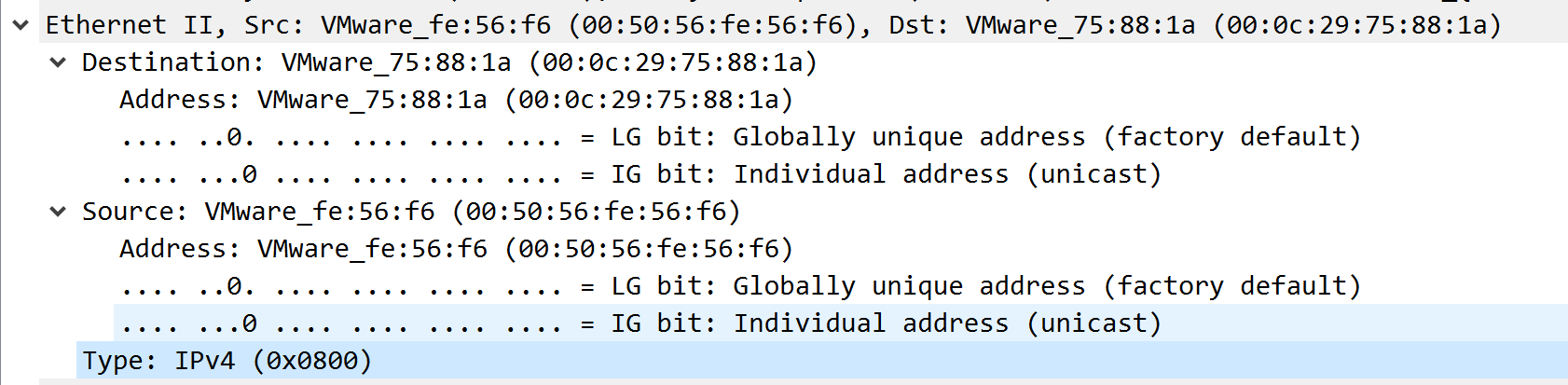


### c．与 ARP reqeust 报文对应的 ARP reply 报文，其所在的 Ethernet 帧的首部中各字段的值是什么？



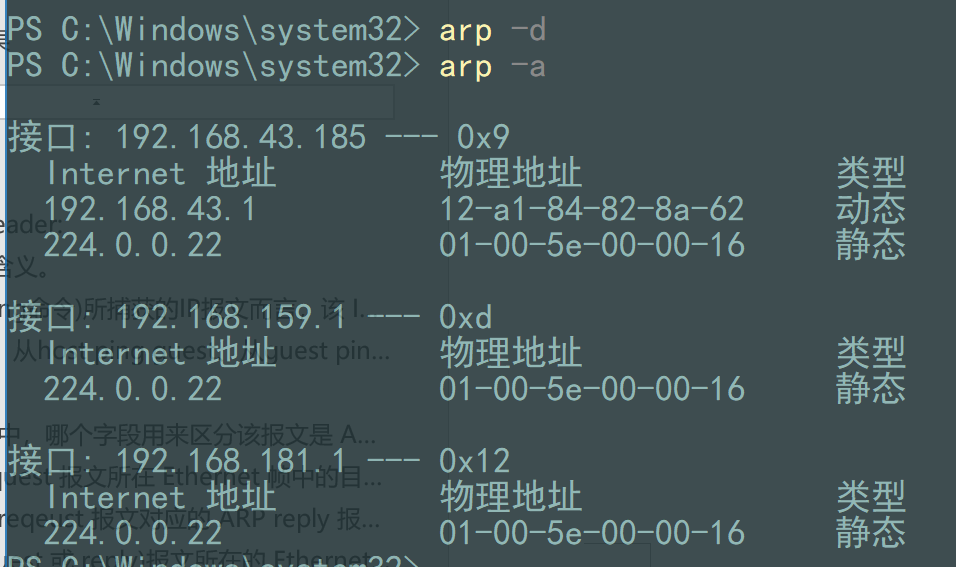
### ARP(request 或 reply)报文所在的 Ethernet 帧中的 protocol type 字段是？

IPv4

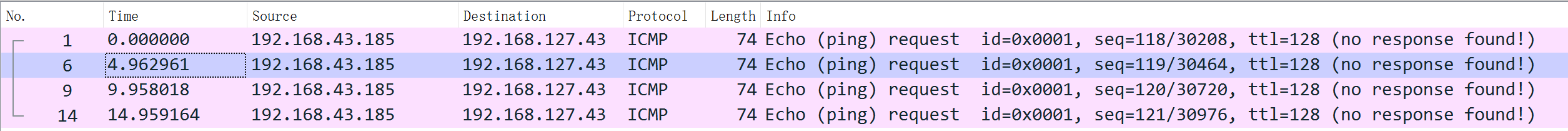


## (3)在 host 上 ping 一个(在 Host 和 Guest 上都)不存在的私有IP地址，ARP Query 和 Reply 报文的 ethernet 帧首部的目的 MAC 和各字段，分别是什么？

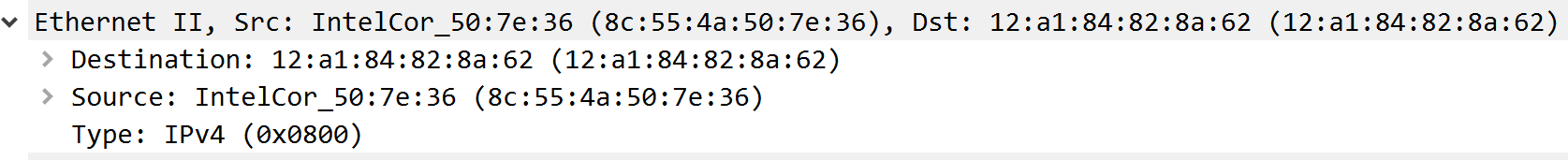
首先清空缓存



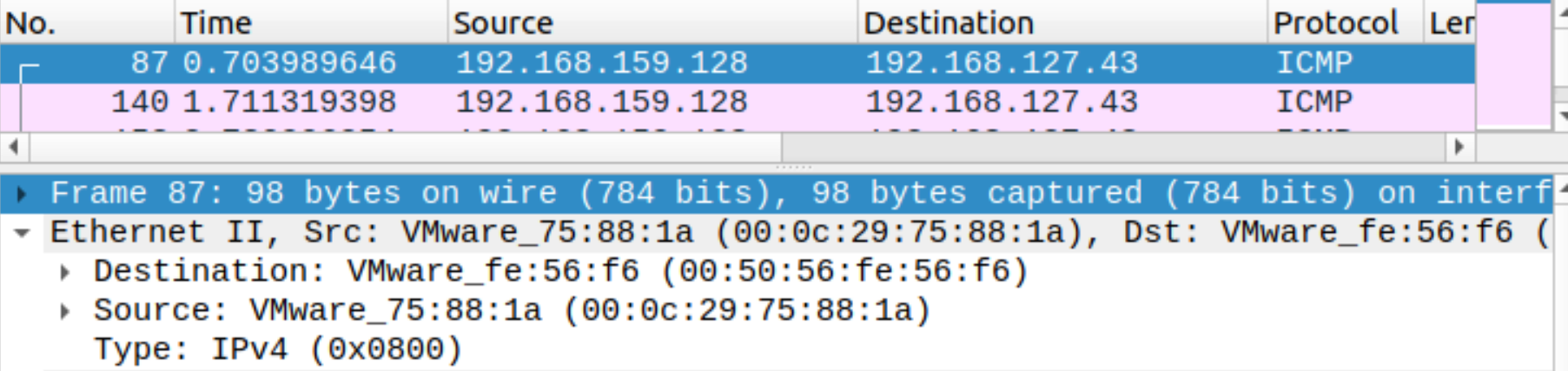
报文如图，发送4个request报文但没有回复。



源地址是自己，目标地址是对方IP



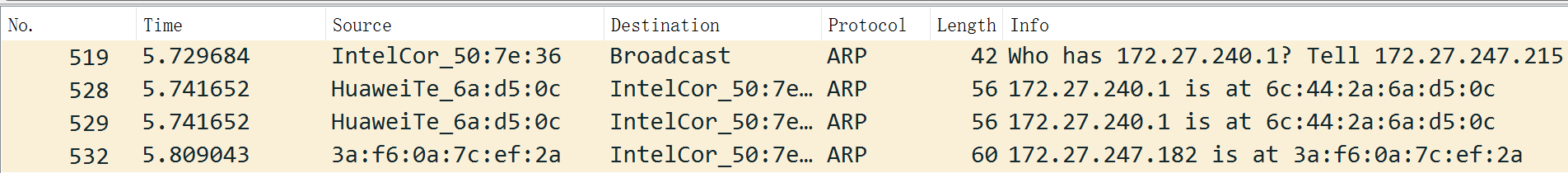
虚拟机ping：



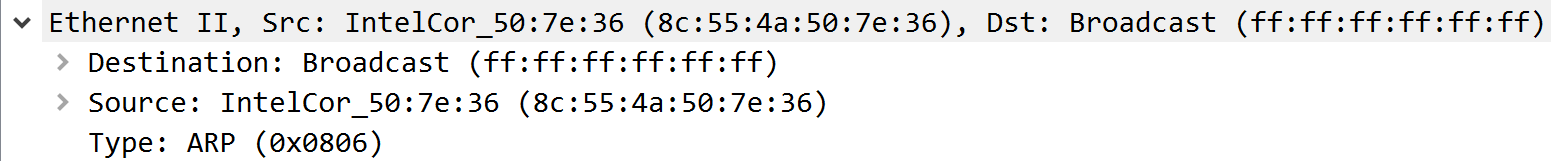
源地址是自己，目标地址是虚拟机的网卡，通过网卡进入外界。

## (4)在 host 上 ping www.bjfu.edu.cn、在 guest 上 ping www.bjfu.edu.cn,包含 ARP Query 和 Reply 报文的ethernet 帧首部各字段，分别是什么？给出合理的解释或判断。你的host OS所在的

Host上ping：



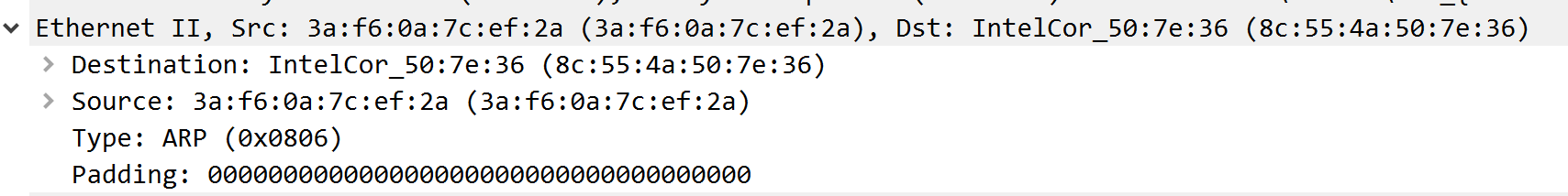
Query：



源端口是自己的端口，因为不知道目标端口的MAC地址，所以使用广播方式。

Type是ARP。

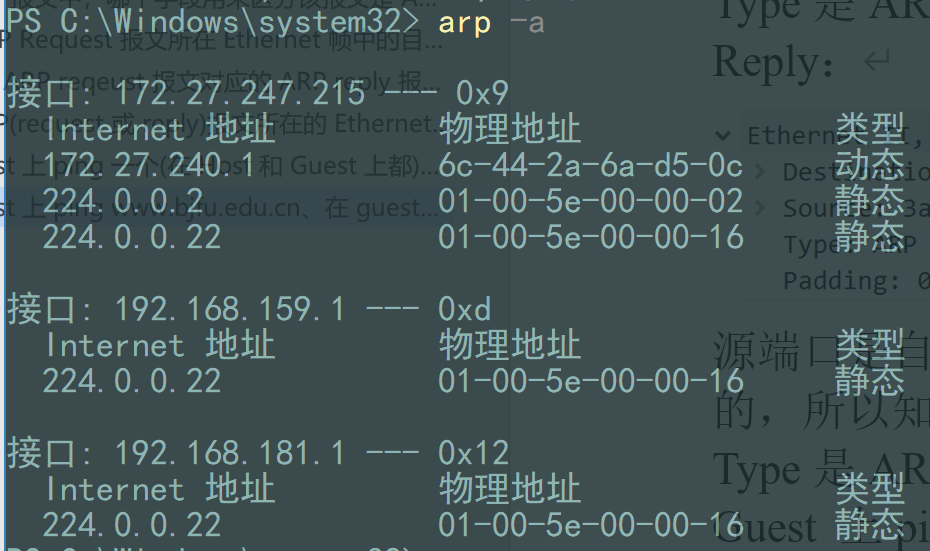
Reply：



源端口是自己的MAC地址，目标端口是query的源端口，因为ARP是单播回复的，所以知道了要回复的端口号之后就直接发送一条单播报文了。

Type是ARP。

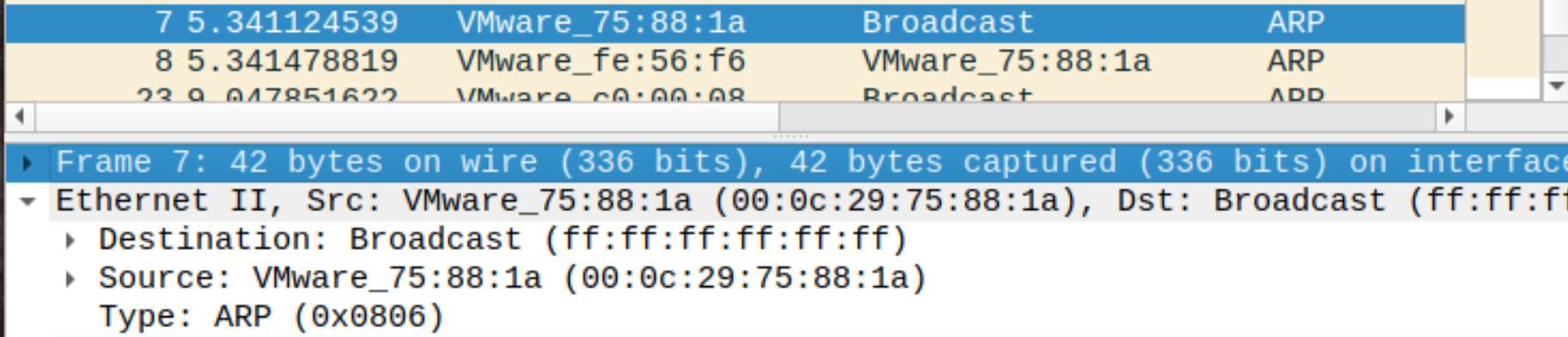
查看缓存，确实多了172.27.240.1这个IP地址及其所对应的MAC地址。



Guest 上ping：

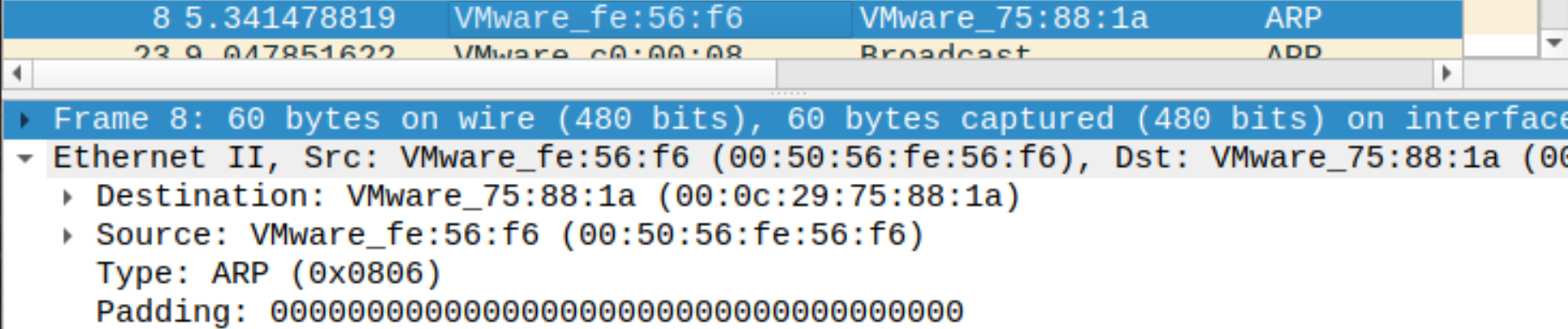
Request：

目标端口仍然是广播地址，但是src用的是自己的虚拟网卡，上面实体主机写的就是intelCor，说明实体机装的是Intel的网卡。



Reply：

Src和实体机也不一样，感觉可能是因为是虚拟机，所以得先进入虚拟机的网关，由虚拟机的网关做处理后再回送机器上的目标端口。



# 3实验提交

截图(wireshark 中的 packet)，并就所捕获报文的截图，对报文结构或工作过程加以文字说明。