**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 数据链路层和网络层协议分析 指导教师 潘冰

实验项目编号 07 实验项目类型 实验地点 计算机网络实验室

学生姓名 贺萱 学号 2019054616

学院 智能科学与工程学院 系 专业 信息安全

实验时间2021年 11月2日上午～11月15日下午温度 ℃湿度

1. **实验目的**
2. 理解链路层、网络层主要协议格式，以及协议的工作原理
3. 理解网关和子网掩码概念
4. 学会利用网络嗅探器（如**Wireshark**）分析协议格式和协议的工作过程
5. 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。
6. **实验内容**
7. 用嗅探器捕获数据包。
8. 分析以太网帧、ARP协议、IP协议、ICMP协议格式
9. 分析PING、TRACERT、ARP命令的工作过程
10. 通过修改主机的网关为指定默认网关、本机IP地址或不设置网关，观察ping的结果，用嗅探器捕获数据包并分析。
11. **主要仪器设备**

**仪器：**两台具有网络功能的PC 机

**实验环境：**局部网环境

1. **实验原理**

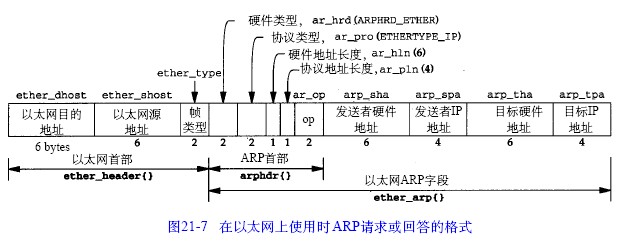
**1、网络嗅探器**

Wireshark是一个网络数据包分析软件。通过该软件可以获取网络数据包，并能进行统计分析网络数据包数据。运行Wireshark时需要将网卡设为**混合模式**。

如果在交换环境里对其他主机进行嗅探，需要对交换机端口进行映射。

**2、协议**

以太网上使用的ARP协议格式



1. **实验步骤**
2. **安装Wireshark**

Wireshark软件在之前的实验中就已经安装成功并使用，这里不做过多赘述

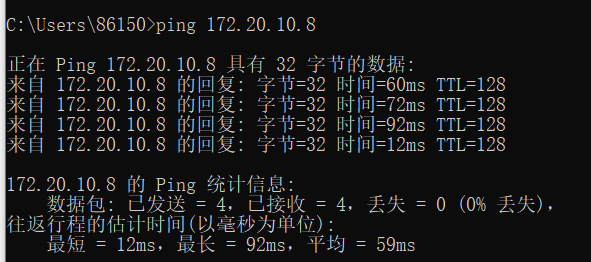
1. **以太网协议分析**

从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。

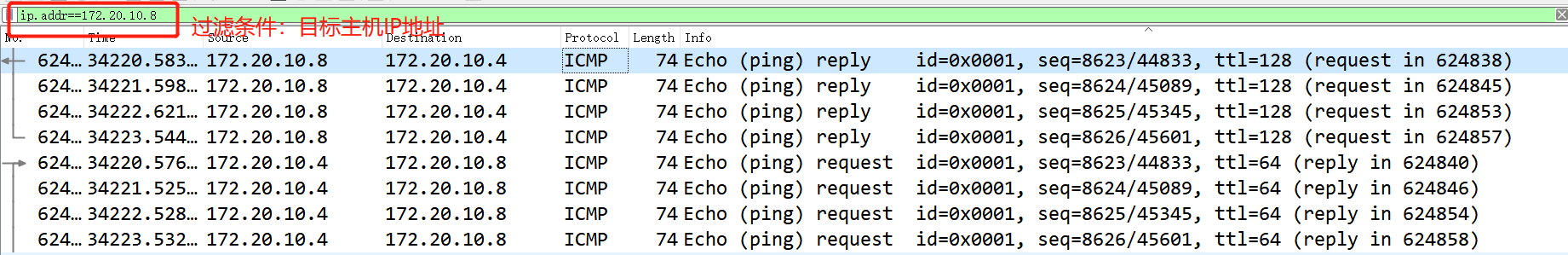
主机A：IP地址172.20.10.4

主机B：IP地址172.20.10.8

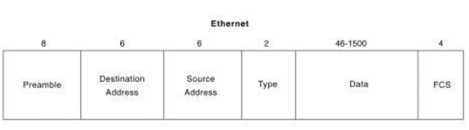
**主机Aping主机B**



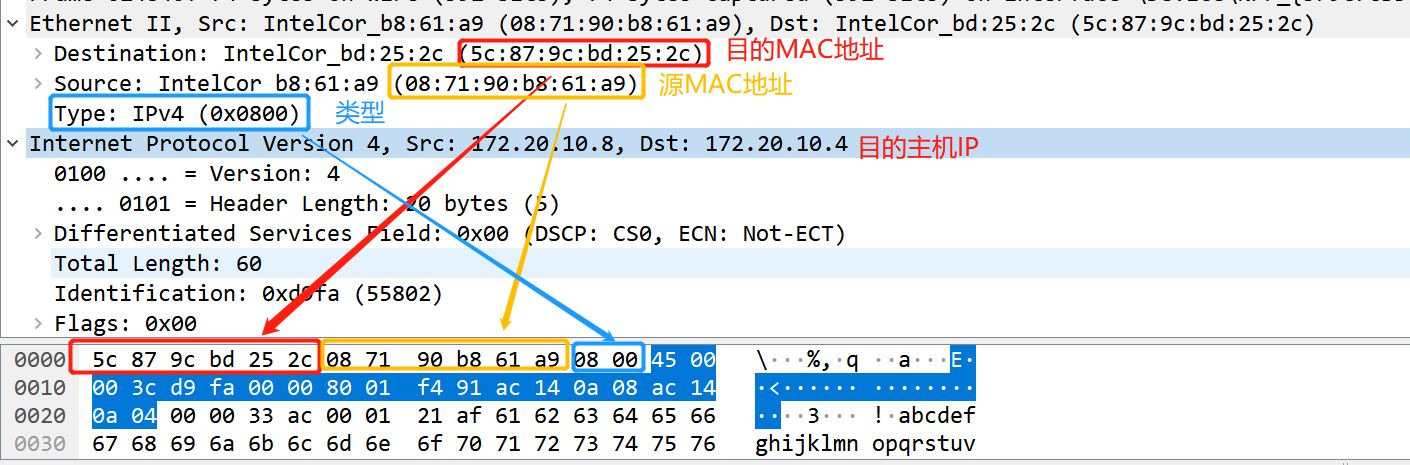
**Wireshark捕获数据包**

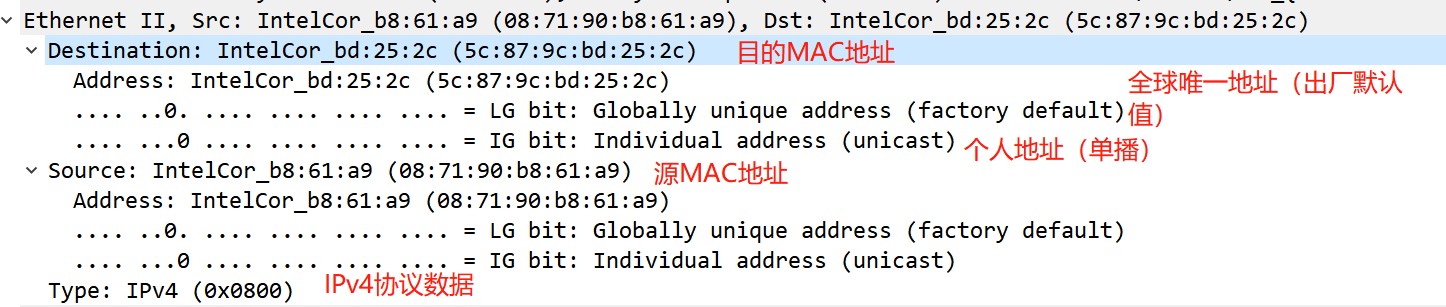


以太网数据帧格式：



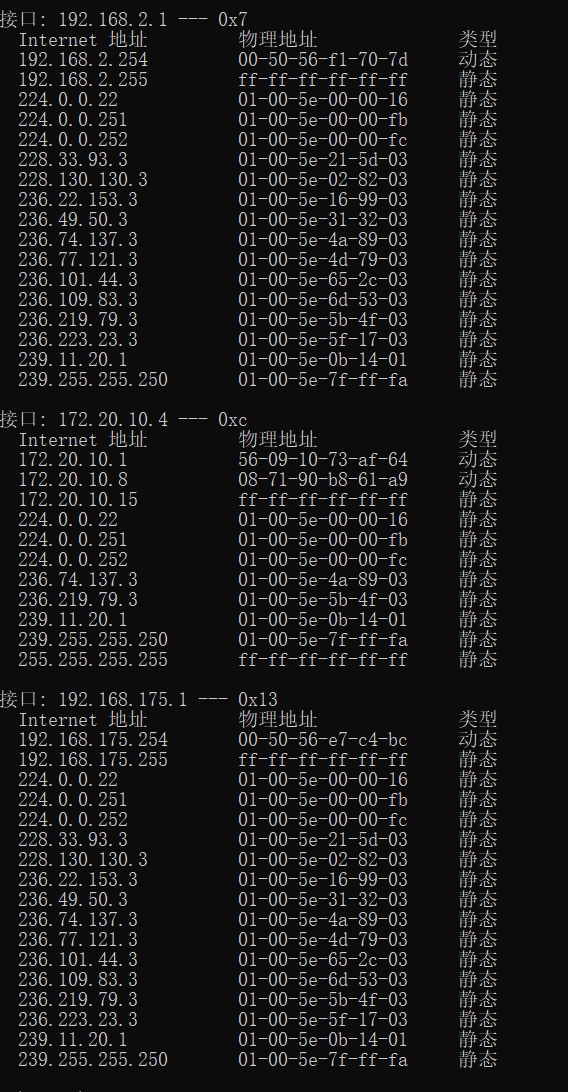
根据以太网帧格式对应可知





1. **ARP协议分析**
2. **进入DOS窗口，用arp – a 查看本机上的ARP表的情况，然后用 arp –d B 删除B的记录（如果有的话）；**

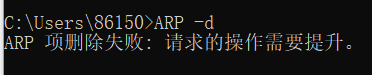
**arp -a：**通过询问当前协议数据，显示当前 ARP 项。如果指定 inet\_addr，则只显示指定计算机的 IP 地址和物理地址。如果不止一个网络接口使用 ARP，则显示每个 ARP 表的项。



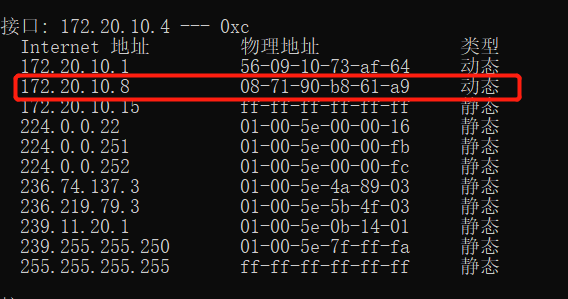
arp -a参数的作用就是当需要了解网络设备对应的MAC地址时，可以在命令提示符中输入arp -a参数回车，读取与IP地址对应的MAC地址关系表。

从图中可以看出，不止一个网络接口在使用ARP协议，ARP协议是解决同一个局域网上的主机或路由器的IP地址和硬件地址的映射问题，从图中可以看出IP地址所对应的物理地址，他们是意一对应的关系

**arp -d：**参数的含义就是删除 inet\_addr指定的主机。inet\_addr可以是通配符 \*，以删除所有主机。



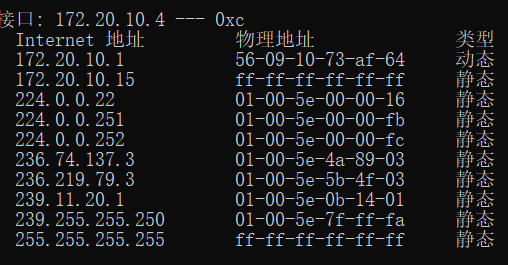
在使用arp-d命令时，出现“ARP项删除失败：请求的操作需要提升。”字样，是因为权限不够导致，参考网络资料后，以管理员身份进入cmd即可解决



从图中可以看出有主机B的IP地址，调用arp -d命令删除记录



再执行arp -a命令显示，验证是否成功删除

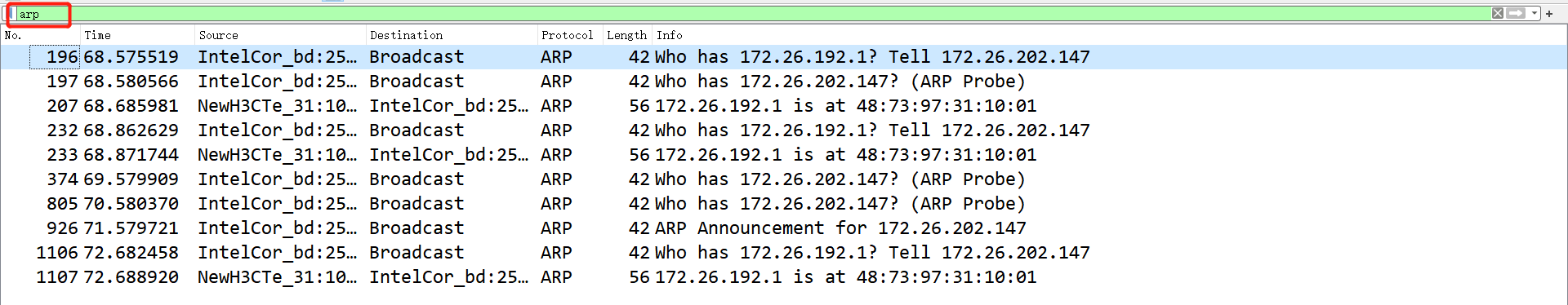


从图中看出，成功删除目标主机记录

**（2）运行Wireshark程序；**

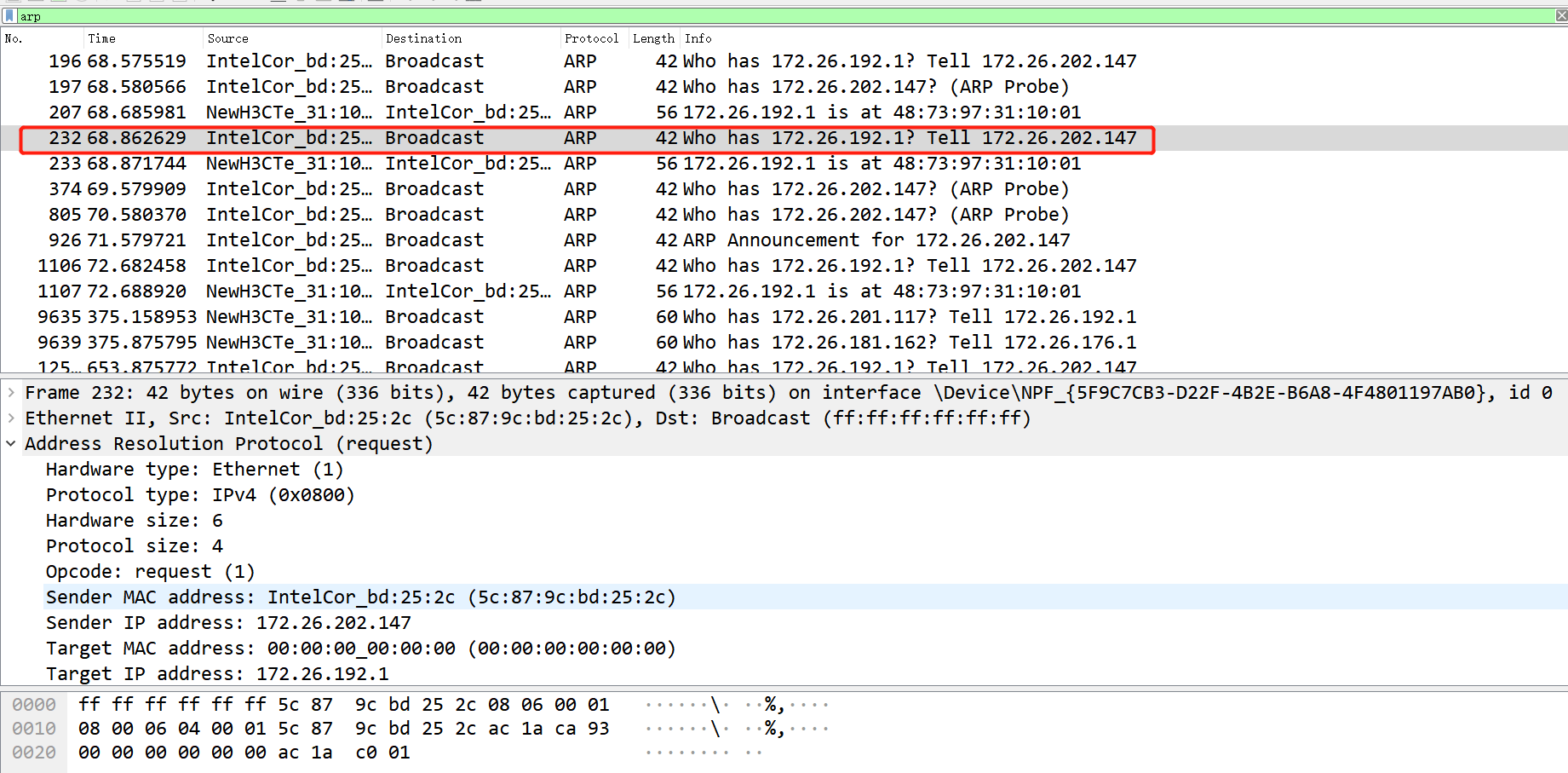
**（3）把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；**

断网1分钟后，再联网，可以捕获到ARP报文，捕获数据如下



**请求包：**

选中报文

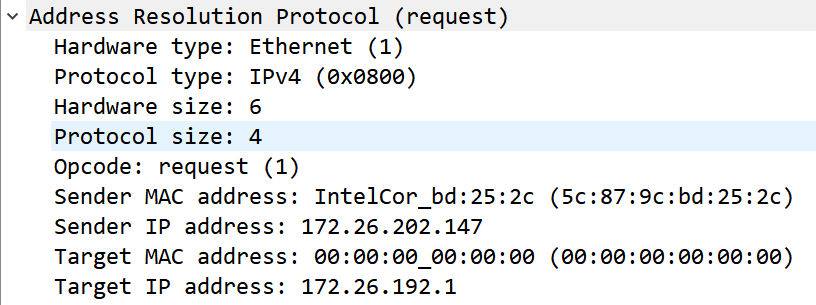




以上内容表示这是第 1 帧数据包的详细信息。其中，该包的大小为 42个字节。



以上内容表示以太网帧头部信息。其中源 MAC 地址为 5c:87:9c:bd:25:2c，目标 MAC 地 址为 ff:ff:ff:ff:ff:ff（广播地址）。这里的目标地址为广播地址，是因为主机 PC2 不知道 PC1 主机的 MAC 地址。这样，局域网中所以设备都会收到该数据包。



Address Resolution Protocol (request) 表示该包是一个请求包

Hardware type: Ethernet (1) 硬件类型，值为1表示以太网地址

Protocol type: IPv4 (0x0800) 协议类型

Hardware size: 6 硬件地址长度

Protocol size: 4 协议长度

Opcode: request (1)  操作码该值为 1，表示是个 ARP 请求包

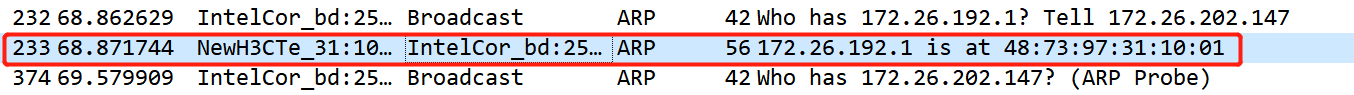
Sender MAC address: IntelCor\_bd:25:2c (5c:87:9c:bd:25:2c)   发送端 MAC 地址

Sender IP address: 172.26.202.147 发送端 IP 地址

Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00) 目标 MAC 地址

Target IP address: 172.26.192.1   目标 IP 地址

**响应包：**

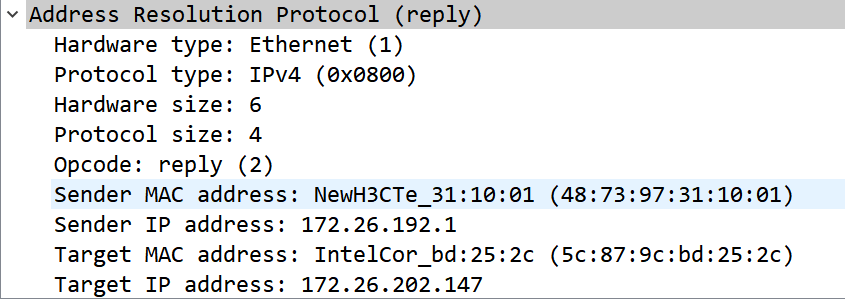




以上信息表示这是第二个数据包的详细信息。其中，该包的大小为 56个字节



 以上内容是以太网帧头部的信息。其中，源 MAC 地址为 48:73:97:31:10:01 ，目标 MAC 地址为 5c:87:9c:bd:25:2c。从该行信息中，可以知道 PC2 获取到了 PC1 主机的 MAC 地址。 这样就可以正常通信了



Address Resolution Protocol (reply) 以上内容表示这里一个 ARP 响应包

Hardware type: Ethernet (1) 硬件类型

Protocol type: IPv4 (0x0800) 协议类型

Hardware size: 6 硬件地址长度

Protocol size: 4 协议地址长度

Opcode: reply (2) 操作码为2，表示该包是ARP响应包

Sender MAC address: NewH3CTe\_31:10:01 (48:73:97:31:10:01) 发送端MAC地址

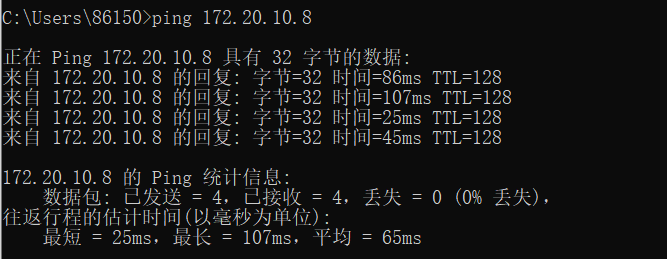
Sender IP address: 172.26.192.1 发送端IP地址

Target MAC address: IntelCor\_bd:25:2c (5c:87:9c:bd:25:2c) 目标MAC地址

Target IP address: 172.26.202.147目标IP地址

1. **从主机A上向主机B发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；**

从主机A向主机B发PING检测报文



运行wireshark进行捕捉，根据观察，此时可以捕获ARP报文，报文如下

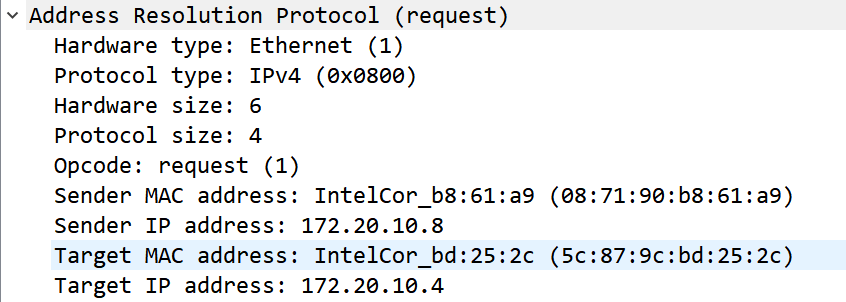




以上信息表示这是数据包的详细信息。其中，该包的大小为 42个字节



以上内容表示以太网帧头部信息。其中源 MAC 地址为 08:71:90:b8:61:a9，目标 MAC 地址为 5c:87:9c:bd:25:2c（广播地址）。



Address Resolution Protocol (request) 以上内容表示这里一个 ARP 请求包

Hardware type: Ethernet (1) 硬件类型

Protocol type: IPv4 (0x0800) 软件类型

Hardware size: 6 硬件地址长度

Protocol size: 4 软件地址长度

Opcode: request (1) 操作码该值为 1，表示是个 ARP 请求包

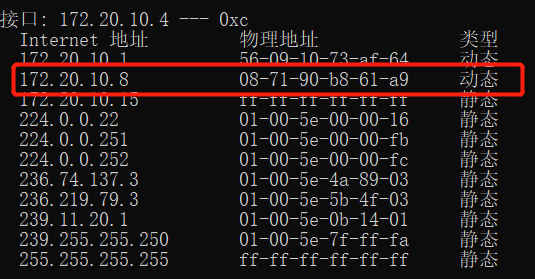
Sender MAC address: IntelCor\_b8:61:a9 (08:71:90:b8:61:a9) 发送端MAC地址

Sender IP address: 172.20.10.8 发送端IP地址

Target MAC address: IntelCor\_bd:25:2c (5c:87:9c:bd:25:2c) 目标MAC地址

Target IP address: 172.20.10.4 目标IP地址

1. **通过arp - a 查看ARP表的更新情况，记录此时能否看到B对应的MAC地址；**

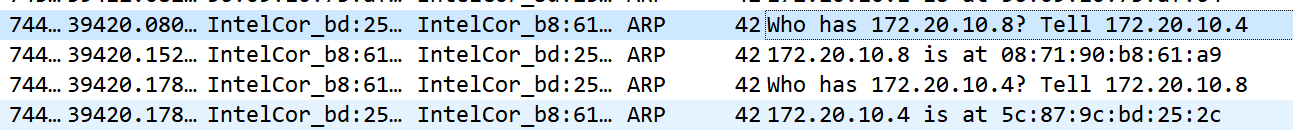


此时可以根据主机B的IP地址看到主机B对应的MAC地址，并与B的物理地址比较，相同

1. **再次从主机A上向主机B发PING检测报文，或者再次从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文；**

主机A再次向主机B发PING检测报文

此时能捕获到ARP报文，捕获报文如下：



当ARP表更新后，理论上不再使用广播查找目的MAC地址，即不需要再发送ARP数据包，而从高速缓存中就可得到IP地址到MAC地址的映射，但通过wireshark却捕获到了单播ARP包，通过查询得知通常ARP单播请求是用来验证ARP表中的cache是否有效

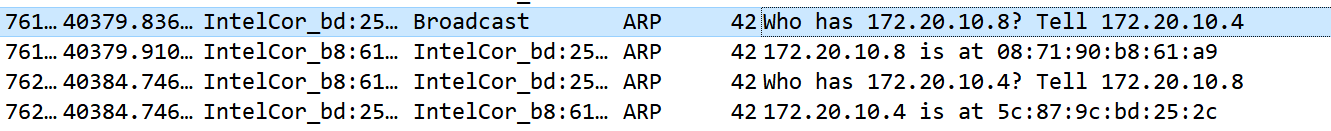
当确认有效之后，ping的后几个包并没有捕获到相应ARP数据包

这里主机A并没有发送ARP广播报文，只是给主机B发送了ARP请求报文，是为了确定主机B的ip地址是否有变化，主机B的IP地址没有变化，所以主机B直接发送应答报文

1. **主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。**

5分钟后，主机A再次向主机B发PING检测报文

此时仍然可以捕获到ARP报文，捕获报文如下：

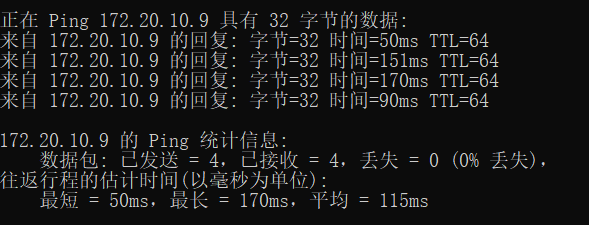
观察发现，与上一步结果相似，捕获到单播的ARP数据包，用于验证ARP表中的cache是否有效，说明cache中仍有该映射，不需要广播。

1. **IP协议分析**
2. **从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较;**

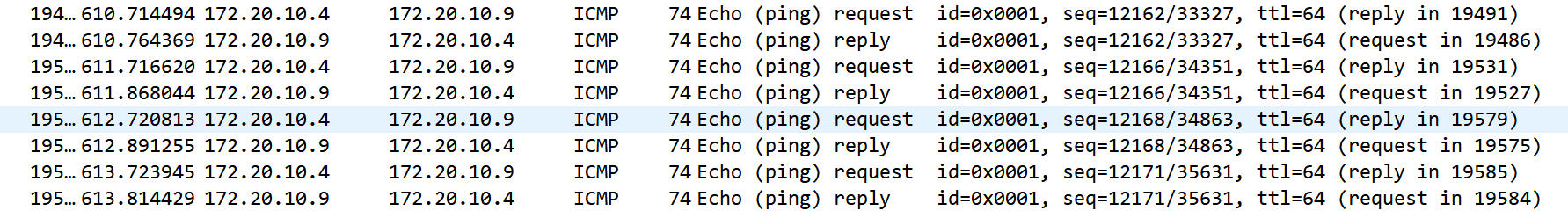
主机A：IP地址：172.20.10.4

主机B：IP地址：172.20.10.9

主机A向主机B发PING检测报文



捕获IP数据包如下：



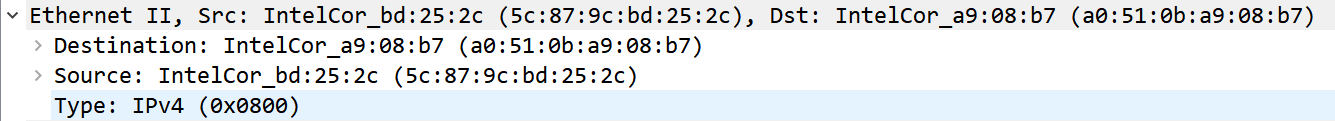
分析字段含义：

**请求帧：**





Frame字段用于概括整个以太网帧的重要信息

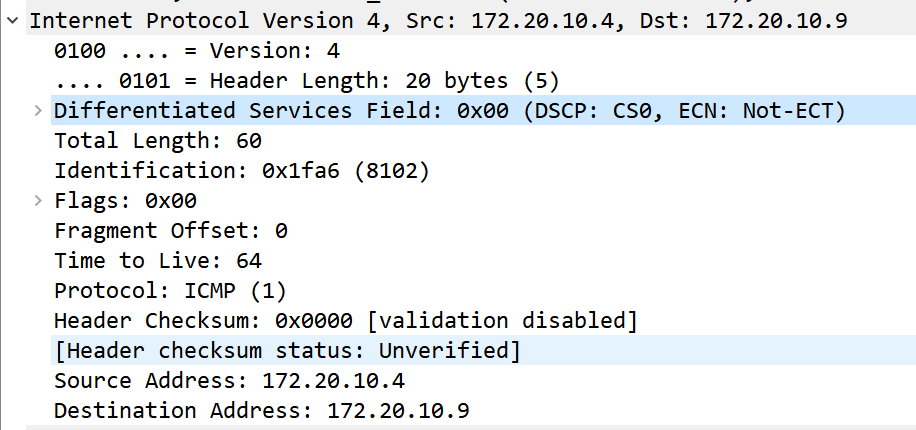


Ethernet II, Src: IntelCor\_bd:25:2c (5c:87:9c:bd:25:2c), Dst: IntelCor\_a9:08:b7 (a0:51:0b:a9:08:b7)

Destination: IntelCor\_a9:08:b7 (a0:51:0b:a9:08:b7) 目的MAC地址

Source: IntelCor\_bd:25:2c (5c:87:9c:bd:25:2c) 源MAC地址

Type: IPv4 (0x0800) 上层类型帧，可知是IPv4



Internet Protocol Version 4, Src: 172.20.10.4, Dst: 172.20.10.9

0100 .... = Version: 4 版本IPv4

.... 0101 = Header Length: 20 bytes (5) 首部长度

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) 服务标识符

Total Length: 60 总长度

Identification: 0x1fa6 (8102) 标识符

Flags: 0x00 标识

Fragment Offset: 0 片内偏移

Time to Live: 64 生存期

Protocol: ICMP (1) 上册协议ICMP

Header Checksum: 0x0000 [validation disabled] 首部校验和

[Header checksum status: Unverified]

Source Address: 172.20.10.4 源IP

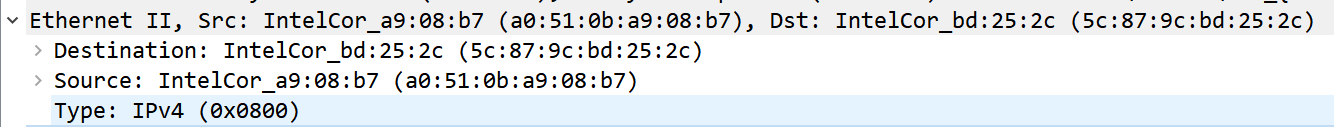
Destination Address: 172.20.10.9 目标IP

**响应帧：**





Frame字段用于概括整个以太网帧的重要信息

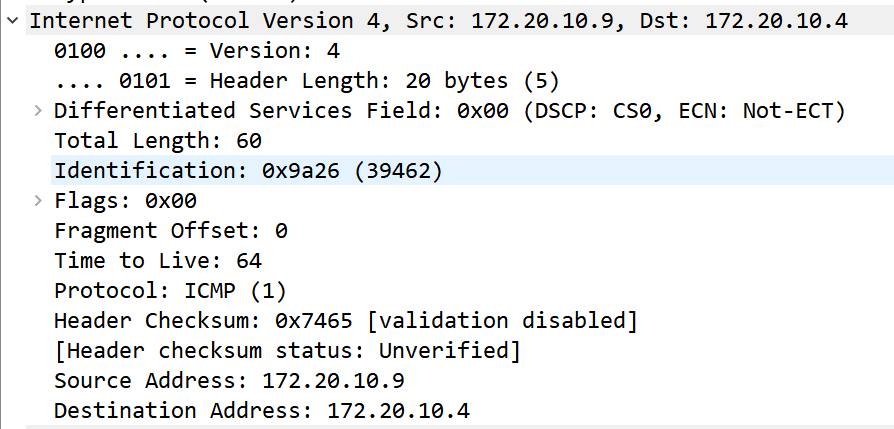


Ethernet II, Src: IntelCor\_a9:08:b7 (a0:51:0b:a9:08:b7), Dst: IntelCor\_bd:25:2c (5c:87:9c:bd:25:2c)

Destination: IntelCor\_bd:25:2c (5c:87:9c:bd:25:2c) 目标MAC地址

Source: IntelCor\_a9:08:b7 (a0:51:0b:a9:08:b7) 源MAC地址

Type: IPv4 (0x0800) 上层类型帧，可知是IPv4



Internet Protocol Version 4, Src: 172.20.10.9, Dst: 172.20.10.4

0100 .... = Version: 4 版本号4

.... 0101 = Header Length: 20 bytes (5) 首部长度20

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60 总长度60

Identification: 0x9a26 (39462) 标识符

Flags: 0x00 标识，没有分片

Fragment Offset: 0 段偏移为0

Time to Live: 64 生存时间

Protocol: ICMP (1) 上层协议ICMP

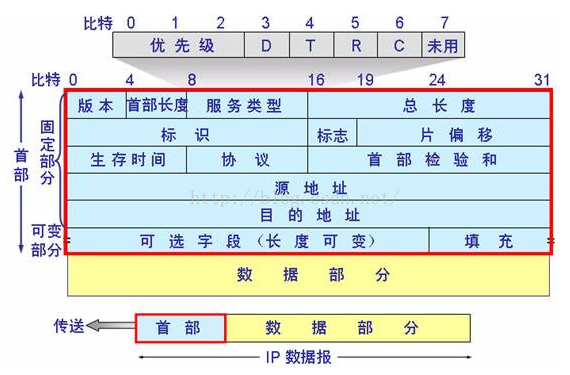
Header Checksum: 0x7465 [validation disabled] 首部校验和

[Header checksum status: Unverified]

Source Address: 172.20.10.9 源IP地址

Destination Address: 172.20.10.4 目标IP地址

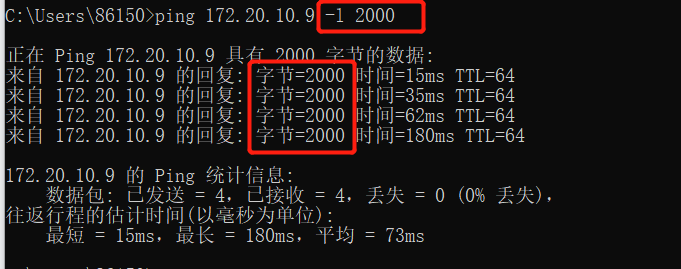
**IP数据包格式**



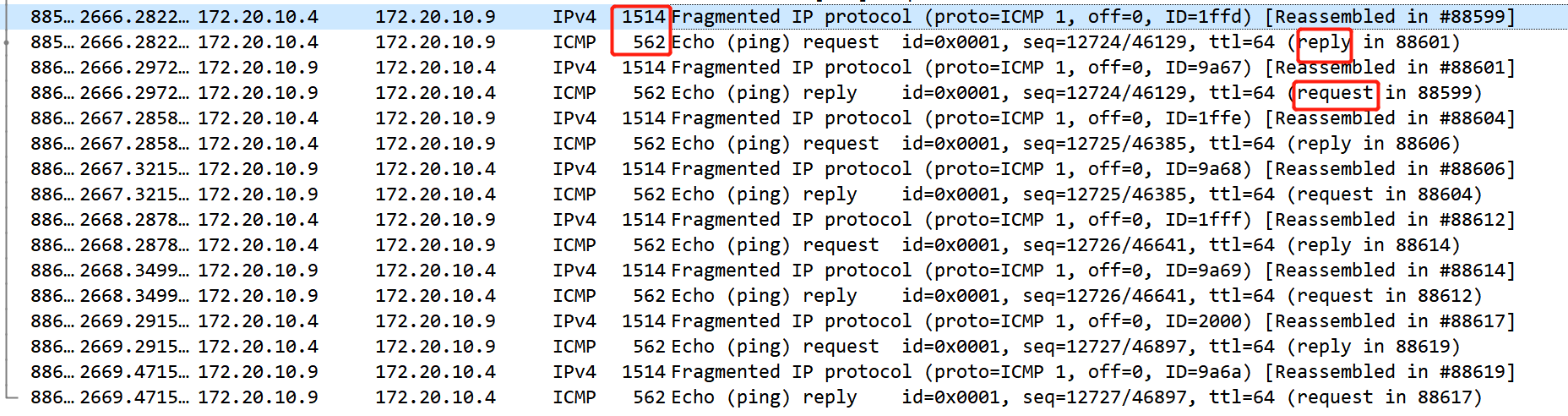
可以看出无论是请求帧还是响应帧首部固定部分都与IP数据包格式一一对应

1. **使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析分片和重组过程。**

主机ApingB



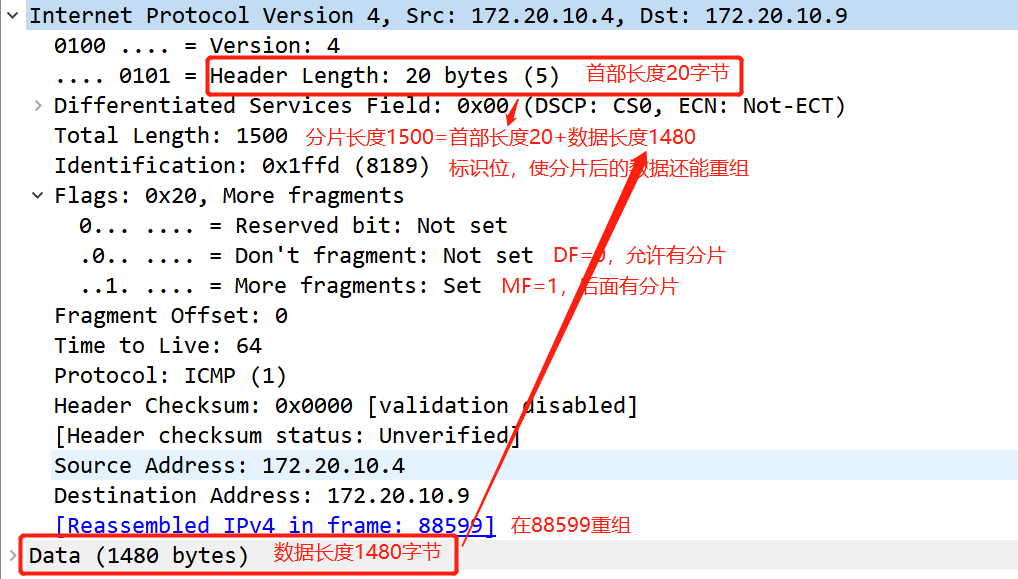
Wireshark捕获数据如下：



从图中观察可知数据包被分成两片，下面具体分析分片和重组情况：

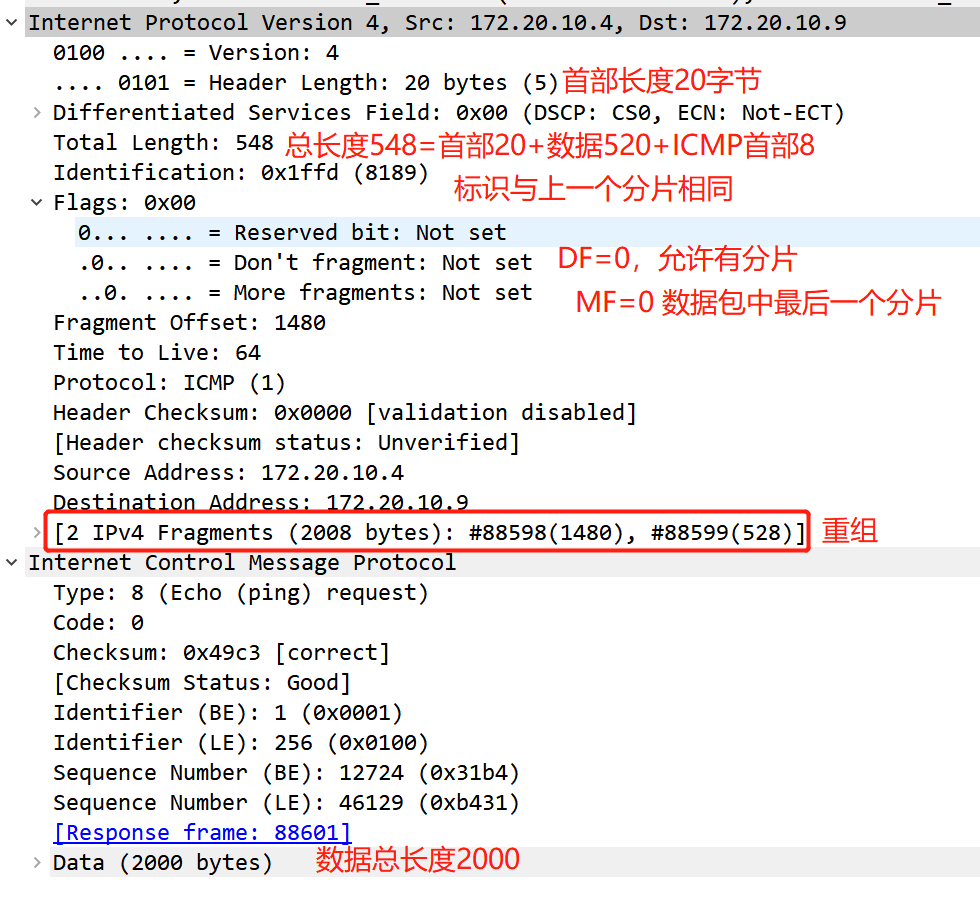
**第一个分片：**



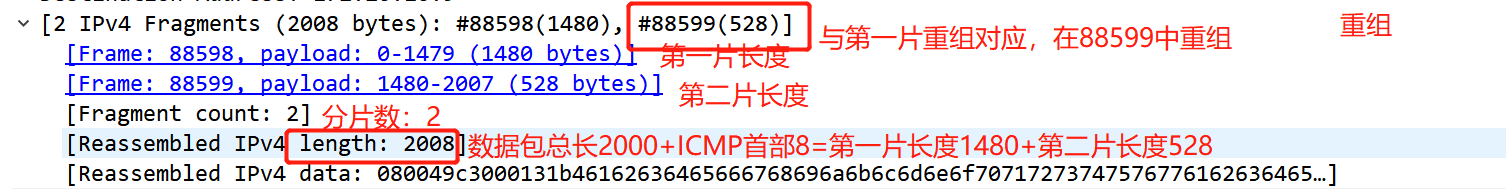


**第二个分片：**





**重组：**



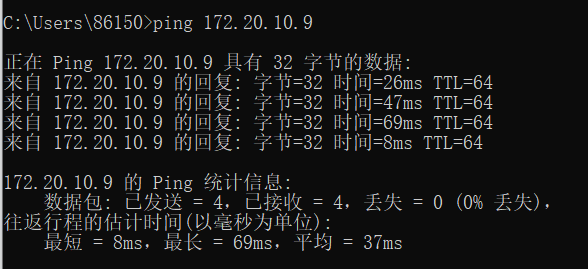
在传输2000字节长度数据时，会将数据分为2片，数据长度分片为第一片长度1480+第二片520，在第二片中通过相同的标识位重组数据，重组的数据会带上ICMP首部信息，因此原本2000长度的数据最后为2008，详细分析见图。

1. **ICMP协议分析**

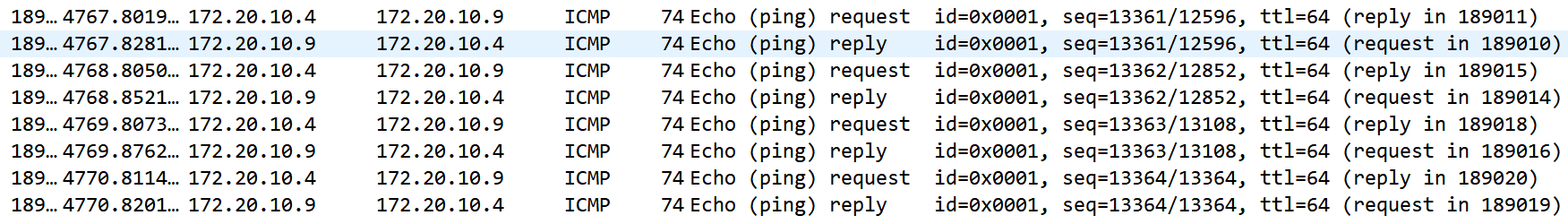
通过ping和tracet命令，了解ICMP协议的使用。

1. **从主机A上向主机B发PING检测报文，捕获ICMP请求数据包和应答数据包，记录并分析各字段的含义，并与ICMP数据包格式进行比较；如果返回的差错信息，请分析是由于什么差错引起的。**

主机Aping主机B

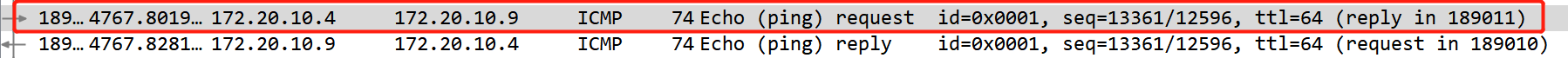


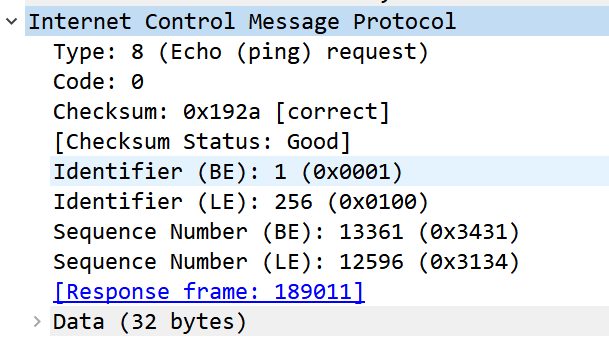
Wireshark捕获数据如下：



记录并分析各字段含义：

**请求包：**





Internet Control Message Protocol

Type: 8 (Echo (ping) request) 类型8，根据类型可知为请求报文

Code: 0 代码为0

Checksum: 0x192a [correct] 检验和

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 13361 (0x3431) 序列号，和应答包中序列号类型相同

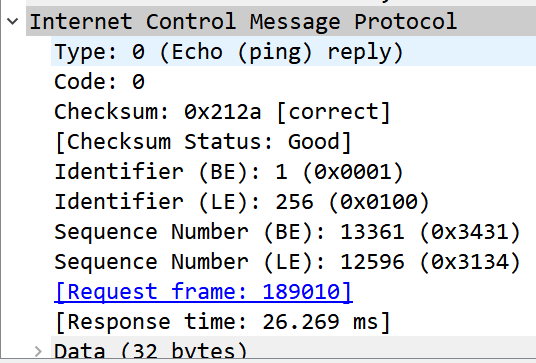
Sequence Number (LE): 12596 (0x3134)

[Response frame: 189011] 响应帧为189011帧

Data (32 bytes) 数据长度32字节

**应答包：**





Internet Control Message Protocol

Type: 0 (Echo (ping) reply) 类型0，根据类型可知为响应报文

Code: 0 代码为0

Checksum: 0x212a [correct] 校验和

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence Number (BE): 13361 (0x3431) 序列号，和请求包中序列号相同

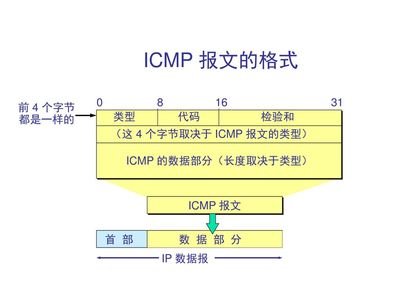
Sequence Number (LE): 12596 (0x3134)

[Request frame: 189010] 请求帧为189010

[Response time: 26.269 ms] 响应时间

Data (32 bytes) 数据长度32字节

**ICMP数据包格式**



可以看出无论是请求包还是响应包报文格式都与ICMP数据包格式一一对应

实验过程中并未返回差错信息

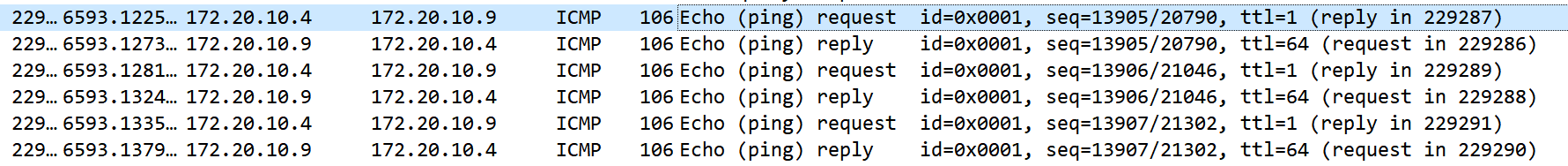
1. **使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。**

主机Atracert主机B



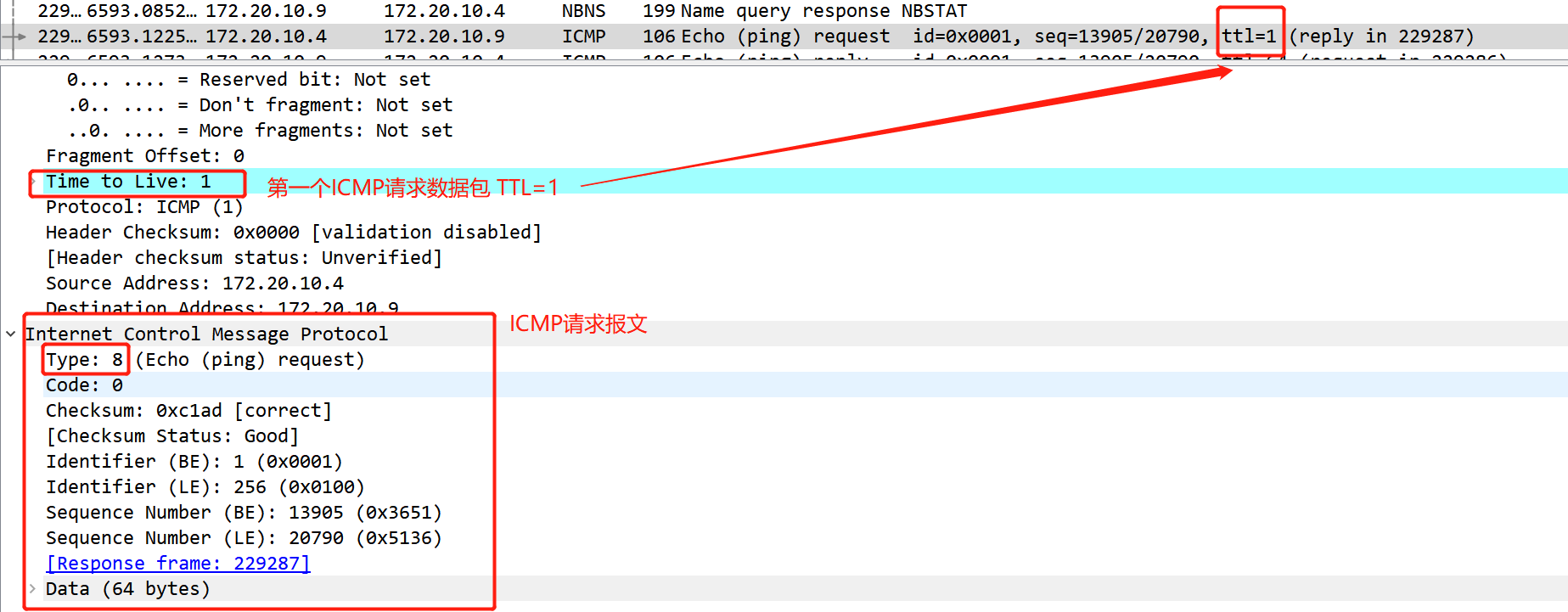
在同一路由器下，共发送三个探测包，tracert通过seq识别返回的包

wireshark捕获数据如下：

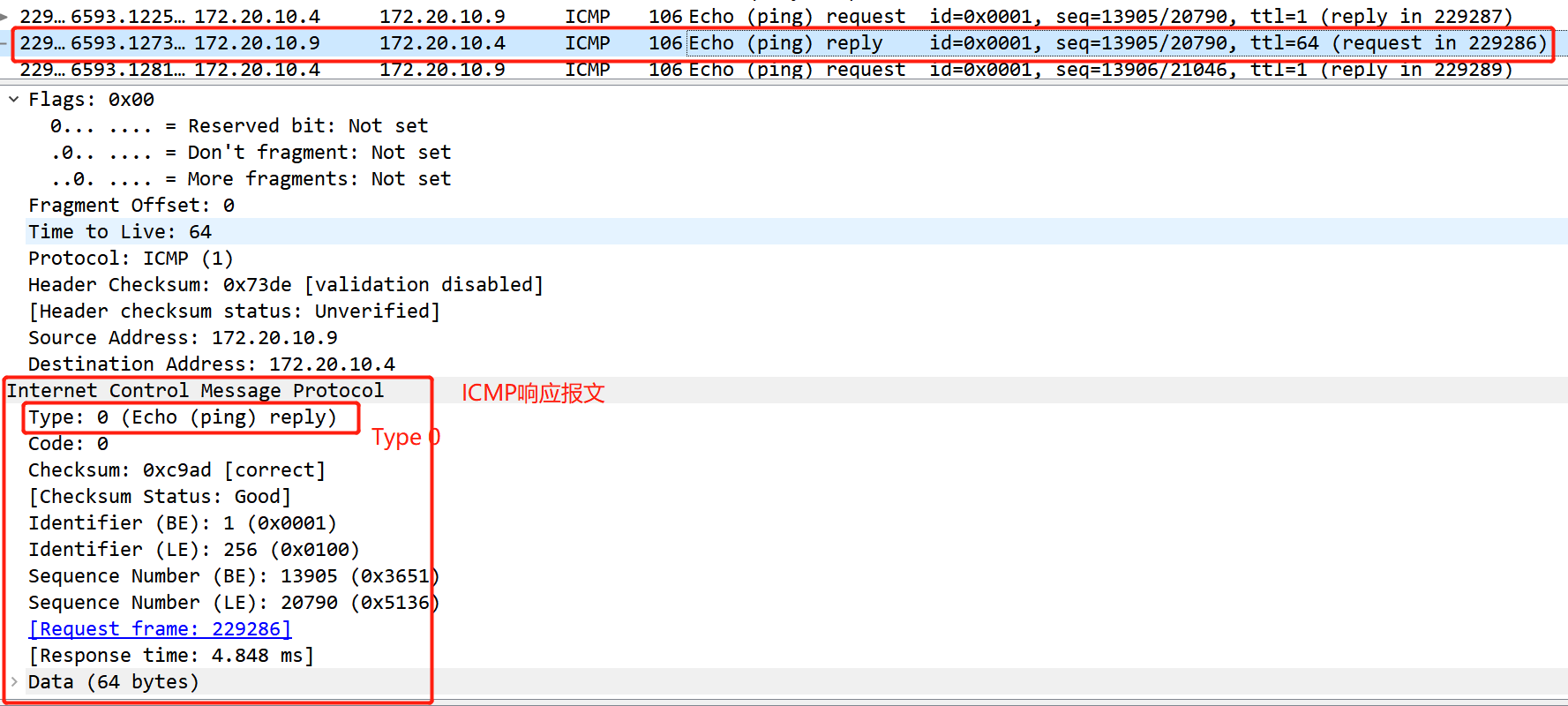


可以看出Tracert命令与ping命令都使用了ICMP协议

类型8、代码0：回射请求。



类型0、代码0：回射应答。



类型11、代码0：超时。

通过以上对数据报的解析，我们看到Tracert命令通过控制IP报文的生存期（TTL），实现路由跟踪提供路由器到目的地址的每一跳的信息。TTL等于1的ICMP回显请求报文被首先发送，路径上的第一个路由器将会丢弃该报文并且发送回ICMP超时错误消息的报文。TTL=x，每到一个路由器TTL-1，当TTL-1=0时，该路由器返回一个ICMP超时差错报文，从而获取该路由器的信息。主机依次发送TTL=2,TTL=3,……的ICMP回应请求报，知道最后一个请求报到达目的主机时TTL=1，目的主机不执行TTL-1的操作，直接返回ICMP请求应答数据包。

**（五）思考题**

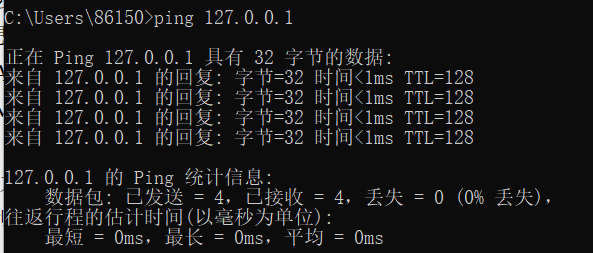
1、在ARP包分析实验过程中，为什么A有时能捕获ARP报文，有时却不能捕获ARP报文？

当主机A想要向本地LAN上的主机B发送IP数据报时，首先检查其ARP缓存中是否有主机B的IP地址。如果在ARP缓存中找到相应的MAC地址，则无需发送ARP请求，此时无法捕获ARP消息；如果没有缓存，则需要广播并发送ARP请求数据包，此时将捕获ARP消息。

在ARP报文分析实验中，通过ARP - a检查ARP表，如果ARP表中没有主机B的IP地址到MAC地址的映射记录，则可以捕获ARP广播消息。当更新ARP表后添加主机B的信息时，无法捕获ARP广播消息，只能捕获ARP单广播消息来确认缓存映射是否仍然有效。

2、为什么运行ping 127.0.0.1时，不能捕获到ICMP报文？如果运行ping 本机IP地址能收到报文吗？ 为什么？

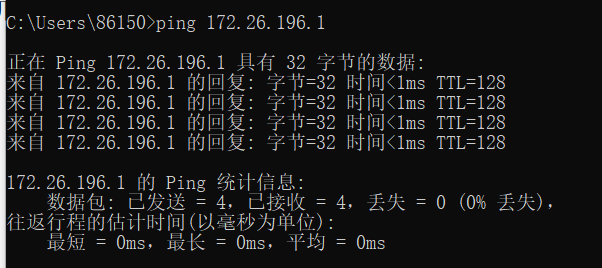
127.0.0.1表示本机回环地址，ping它是不经过网卡的，都是通过环路来处理的所以无法捕获到ICMP报文



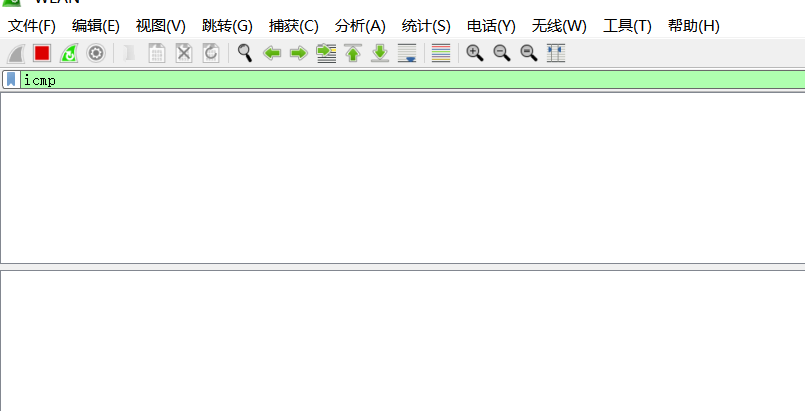
此时wireshark没有捕获到任何ICMP报文

如果运行ping本机的IP也是收不到报文的，因为ping本机IP时在IP协议栈就进行了回环，因此不能捕获到icmp报文。

本机IP地址：172.26.196.1



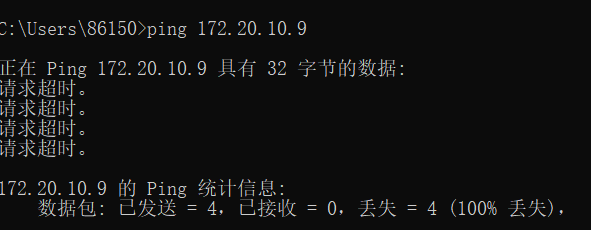
此时wireshark上仍然没有捕获到任何ICMP报文



3、在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

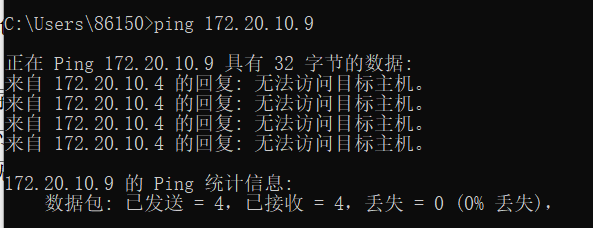
Request timed out：请求超时，是ping的数据包具有到达目标的路由，但因其他原因不可到达。可能由以下情况引起:开启防火墙拦截、安全限制、不在同一网段内即使路由存在也无法找到地址等。

当目的主机开启防火墙、安全限制、不在同一网段内，都出现以下情况：



Destination Host Unreachable：目的主机不可达，是ping的数据包没有到达目的地址的路由。可能由以下情况引起：对方没有开机或者开机后没有接入对应的广播域、目的IP地址不存在、没有对应访问的路由等。

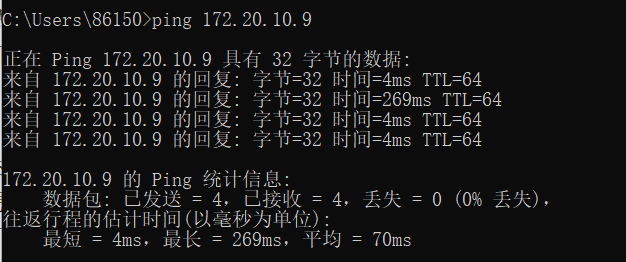
当对方没有开机、没有接入对应广播域、目的IP地址不存在、没有对应访问的路由时，都出现以下情况：



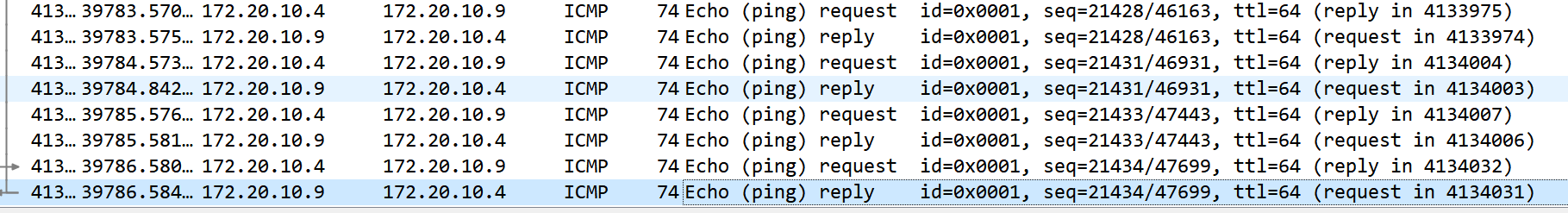
4、请通过实验**验证**：

**主机如果不设置“网关”，同一网段内的主机可以相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。**

主机Aping主机B



获得8个ICMP数据包



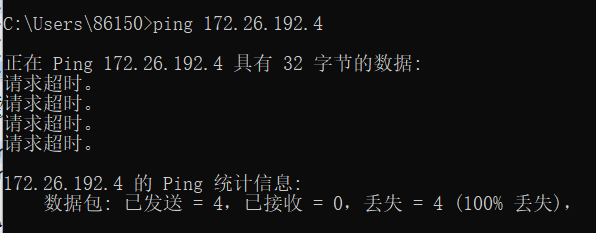
获得2个ARP数据包



**不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。**

将主机B连接校园网，此时主机B的IP地址为172.20.10.4

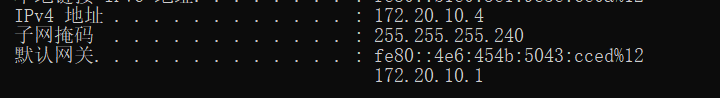
主机Aping主机B



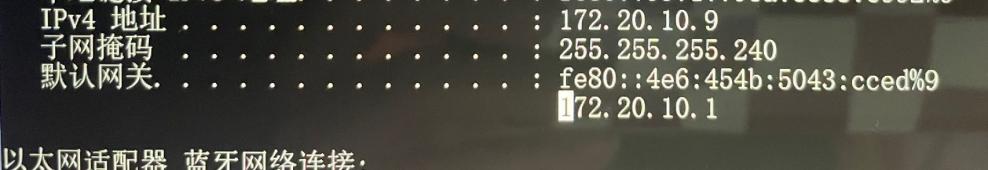
此时wireshark中不管是ICMP还是ARP协议都没有捕获到任何数据包

主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。

主机A网关

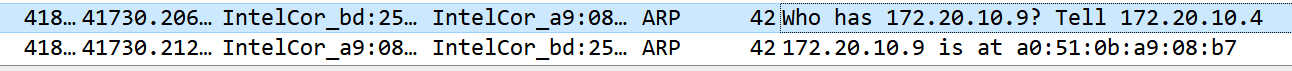


主机B网关

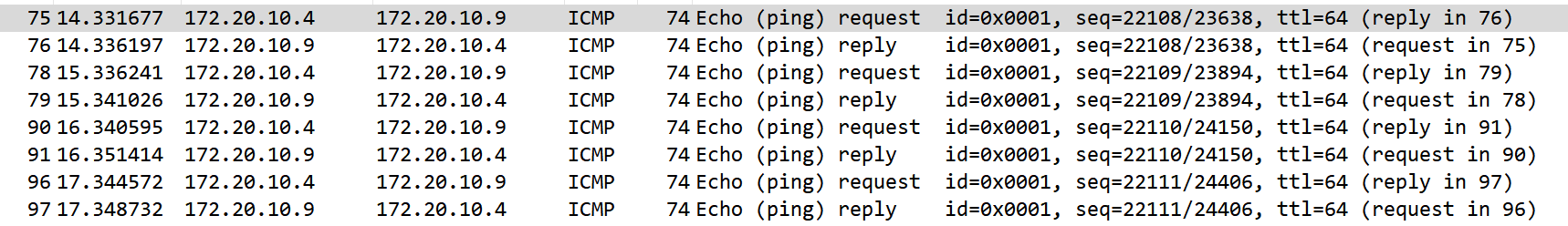


主机Aping主机B

2个ARP数据包



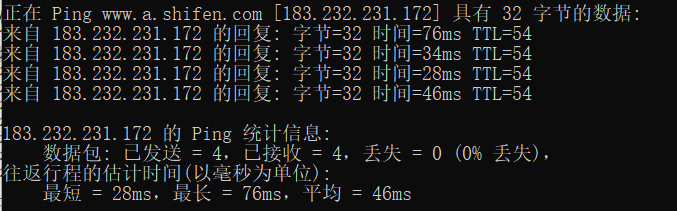
8个ICMP数据包

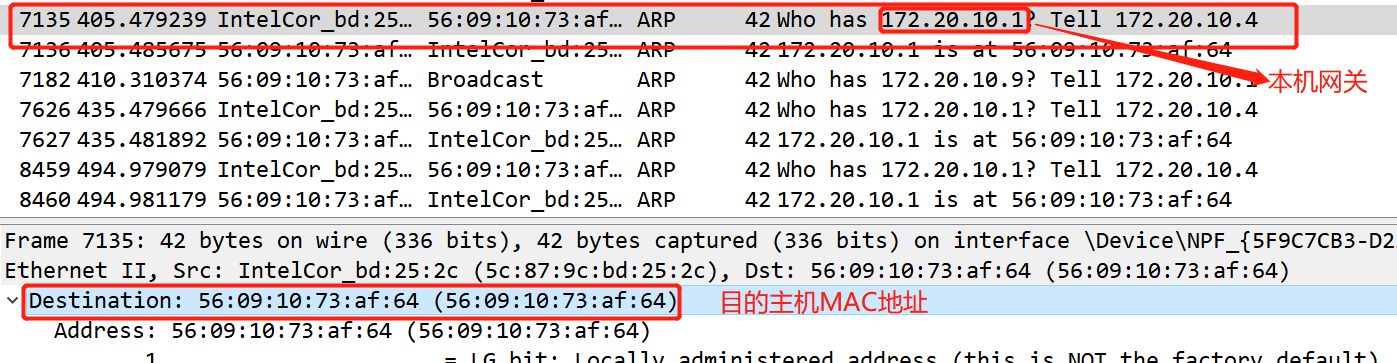


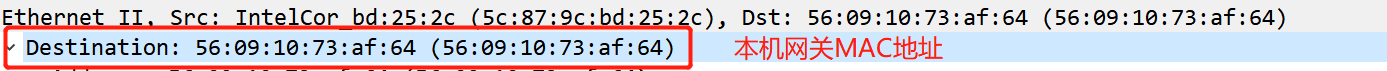
**不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。**

**不同网段之间能通信**

本机ping 百度







通过wireshark可以看到本机网关的MAC地址

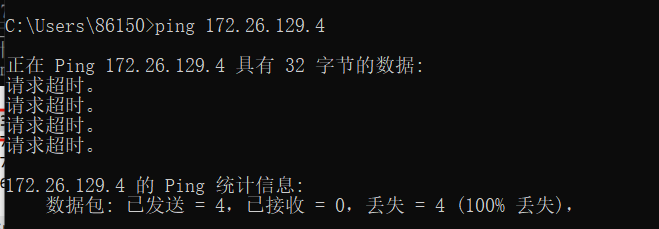
利用arp -a命令进行验证

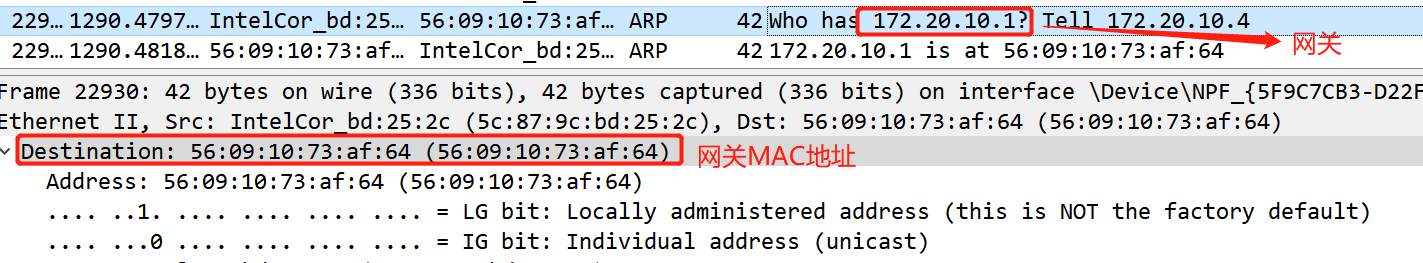


经对比相同

**不同网段之间不能通信**

主机Aping主机B，主机B连接校园网





通过wireshark可以看到本机网关MAC地址

5、通过下面实验**理解网关**

**假设主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析。**

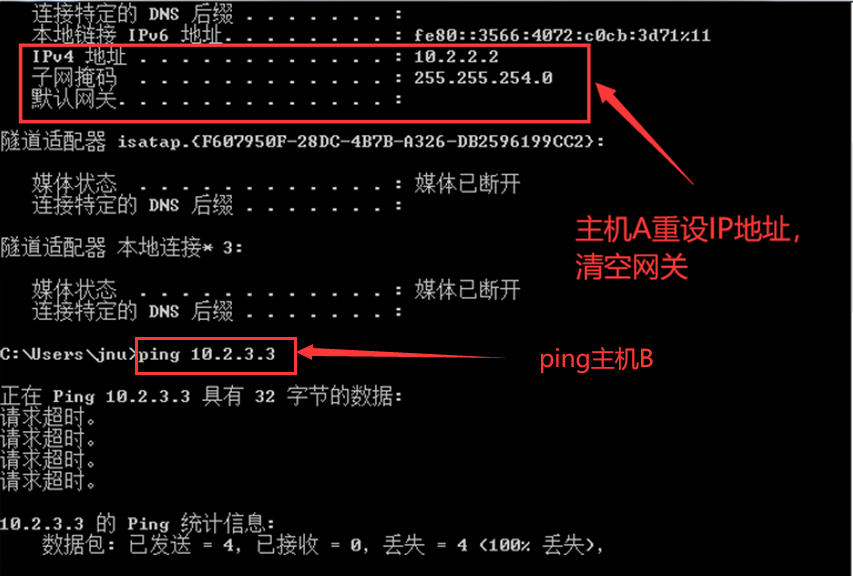
这个实验是利用计算机网络实验室的计算机完成的：

主机A的IP地址——10.2.2.2 子网掩码：255.255.254.0

主机B的IP地址——10.2.3.3 子网掩码：255.255.254.0

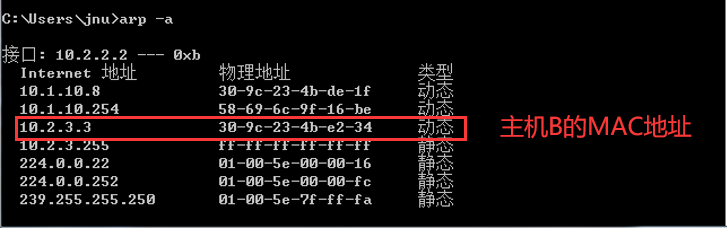
A和B的网关都清空

**（1）修改IP地址和子网掩码后主机A ping主机B:**

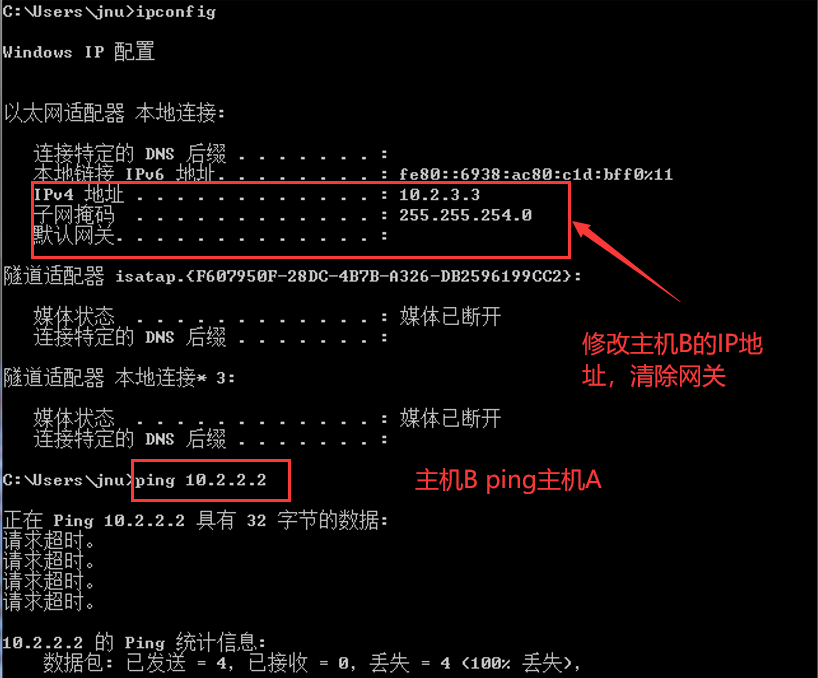


arp -a查看物理地址：

发现新增了主机B的物理地址：

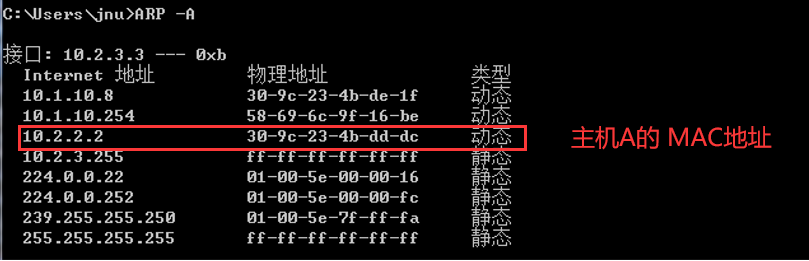


**（2）主机B ping主机A：**



arp -a查看物理地址：

发现新增了主机B的物理地址：



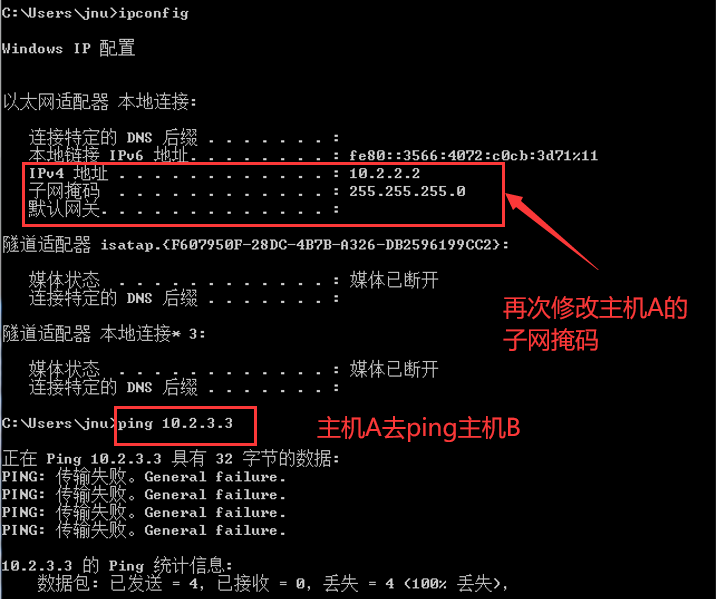
**假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/23，两主机不设置网关，分别在主机A和主机B上用ping测试与对方的连通性，用ARP查看物理地址。对测试结果进行分析。**

主机A的IP地址——10.2.2.2 子网掩码：255.255.255.0

主机B的IP地址——10.2.3.3 子网掩码：255.255.254.0

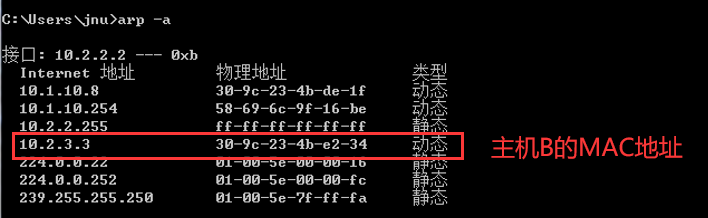
主机A的网关发生了变化：

**（1）修改子网掩码后，主机A去ping主机B：**

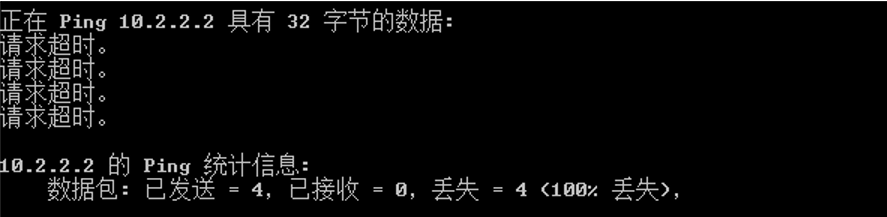


arp -a查看物理地址：

发现新增了主机B的物理地址：

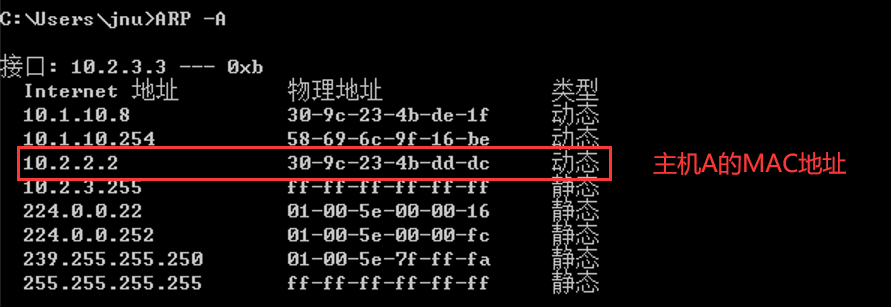


**（2）主机B ping主机A：**



arp -a查看物理地址：

发现新增了主机A的物理地址：



1. **实验总结**

本次实验通过以太网协议分析，掌握了以太网数据帧含义以及MAC帧各个字段的含义，熟练运用wireshark了解分析目的主机和源主机的MAC地址。

通过ARP协议分析实验进一步理解掌握ARP协议的工作过程，可以通过相关命令arp -a查询、arp -d删除ARP数据，掌握ARP报文各字段含义，并通过分析wireshark捕获的数据包掌握了不同情况下的广播和单播，同时体会到ARP高速缓存的作用，若存在缓存记录就不需要进行广播查找，响应时一般为单播。

通过IP协议分析实验，对IP协议格式字段含义有进一步熟悉，同时对分片和重组过程有了进一步掌握，会将较大的数据在传输时进行分片，后重组，最后的数据长度要大于数据长度，因为增加了8位ICMP首部字段。

通过ICMP协议分析实验，对ICMP协议格式和工作过程有了进一步掌握，通过wireshark分析ICMP各个字段的含义，同时也通过实验对tracert命令的原理有进一步理解和掌握，分析不同type类型的ICMP响应数据包格式，发现数据封装方式的不同。

通过对思考问题的分析和验证，总结并分析ARP报文是否能被捕获。同时对环回驱动有了进一步的了解，知道Ping 127.0.0.1和本地IP地址不能捕获消息的原因。同时，对Ping过程中Ping失败的原因进行了分析和验证，进一步了解了“网关”。同一网段的通信不设置网关，不同网段的通信必须设置网关。