**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

学生姓名 陈星池 学号 2019051102

学院 智能科学与工程学院 系 专业 信息安全

实验时间 年 月 日 午～ 月 日 午 温度 ℃湿度

1. **实验目的**

1、 理解链路层、网络层主要协议格式，以及协议的工作原理

2、 理解网关和子网掩码概念

3、 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

4、 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。

1. **实验内容**

1、 用嗅探器捕获数据包。

2、 分析以太网帧、ARP协议、IP协议、ICMP协议格式

3、 分析PING、TRACERT、ARP命令的工作过程

4、 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。

1. **实验环境**

计算机2台，交换机一台。

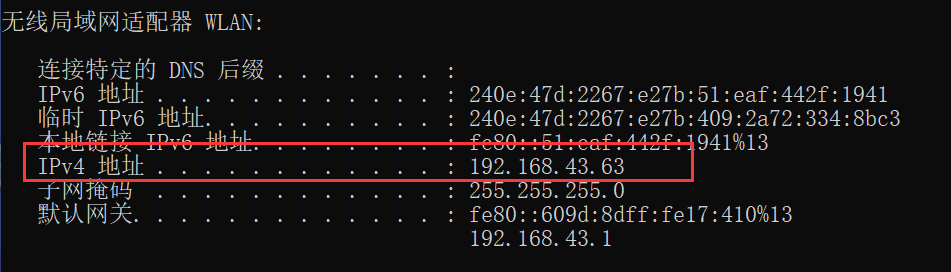
1. **实验步骤**

**1、以太网协议分析**

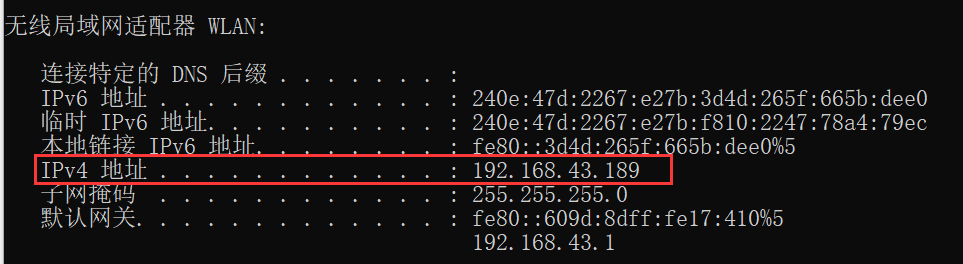
从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。

实验时，我与19软工李敏同学的电脑都连接我的热点

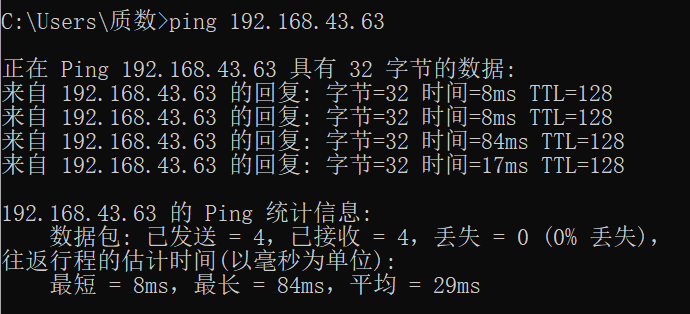
19软工李敏同学的IP地址为192.168.43.63



我的IP地址为192.168.43.189

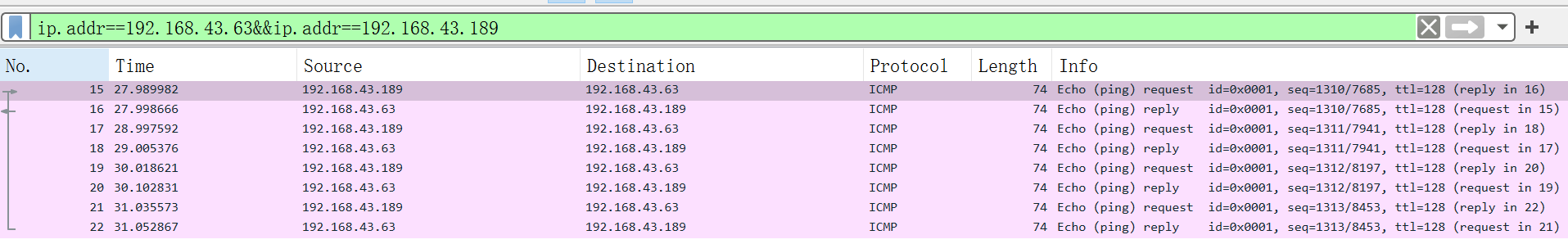


我的电脑ping她的电脑结果为

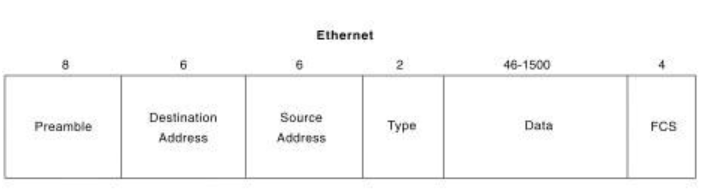


在wireshark上捕获到数据包为，过滤器：

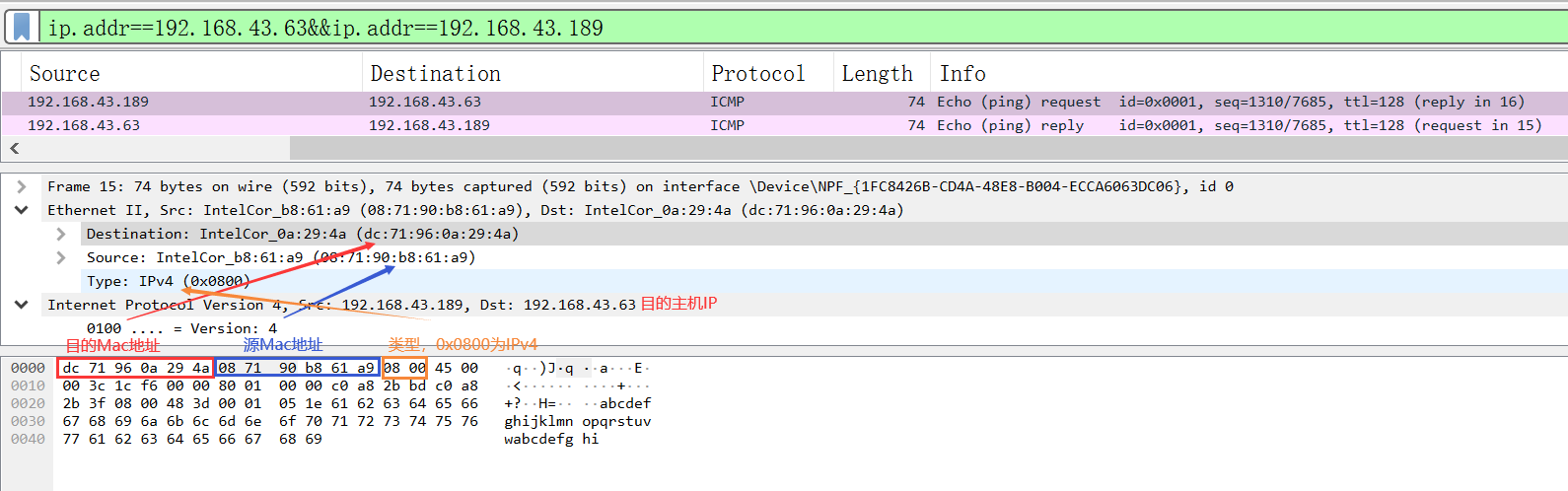
ip.addr==192.168.43.63&&ip.addr==192.168.43.189

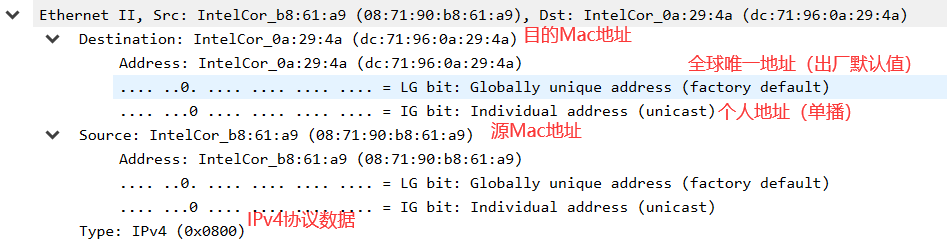


以太网数据帧：



根据以太网帧格式对应可知



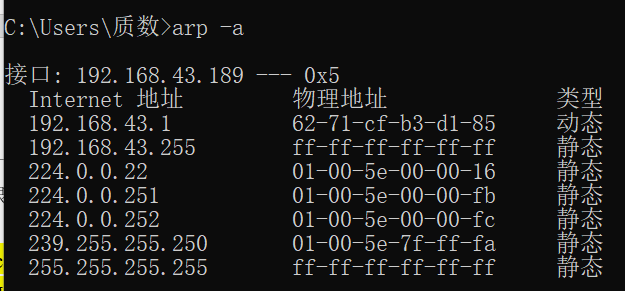


**2、ARP协议分析**

本实验与19信安贾熙妮一起做，连接我的热点，我的IP地址为192.168.43.189，她的IP地址为192.168.43.115

|  |  |
| --- | --- |
| 我的主机 |  |
| 19信安贾熙妮的主机 |  |

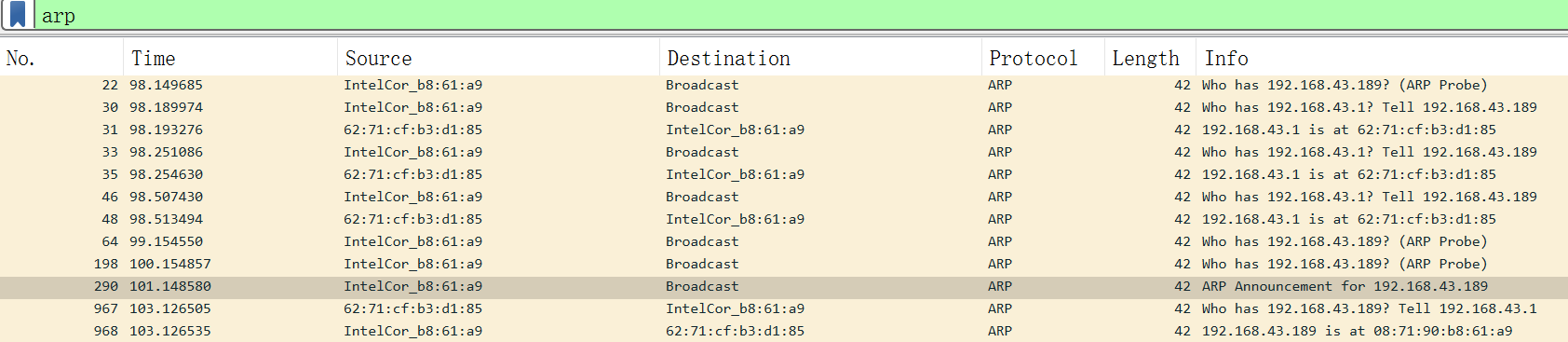
* 进入DOS窗口，用arp – a 查看本机上的ARP表的情况，然后用 arp –d B 删除B的记录（如果有的话）；



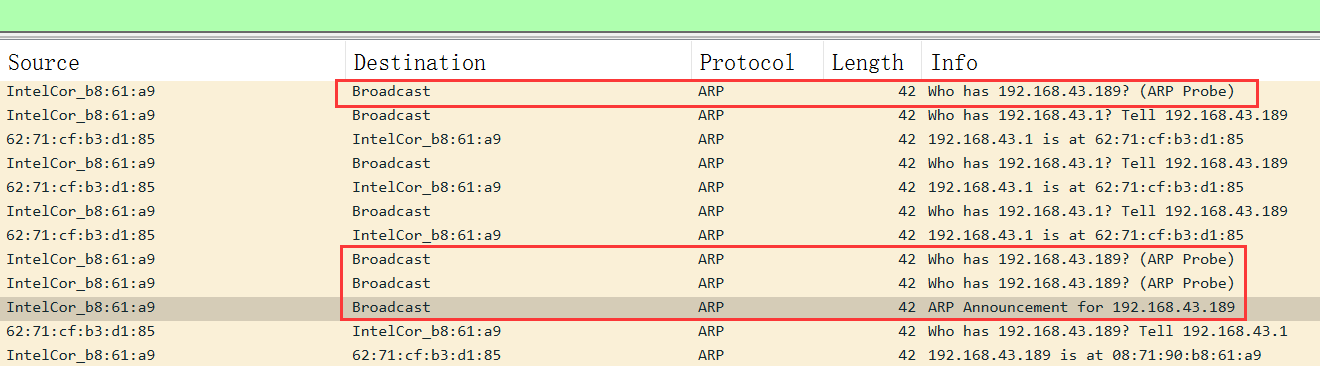
可以看出没有192.168.43.115的记录

* 运行Wireshark程序；
* 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；

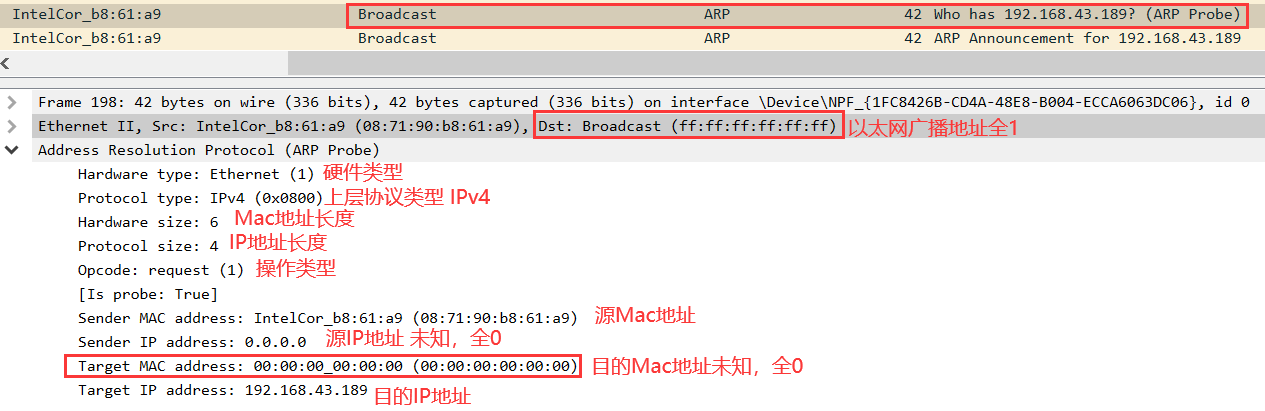
能捕获到ARP报文



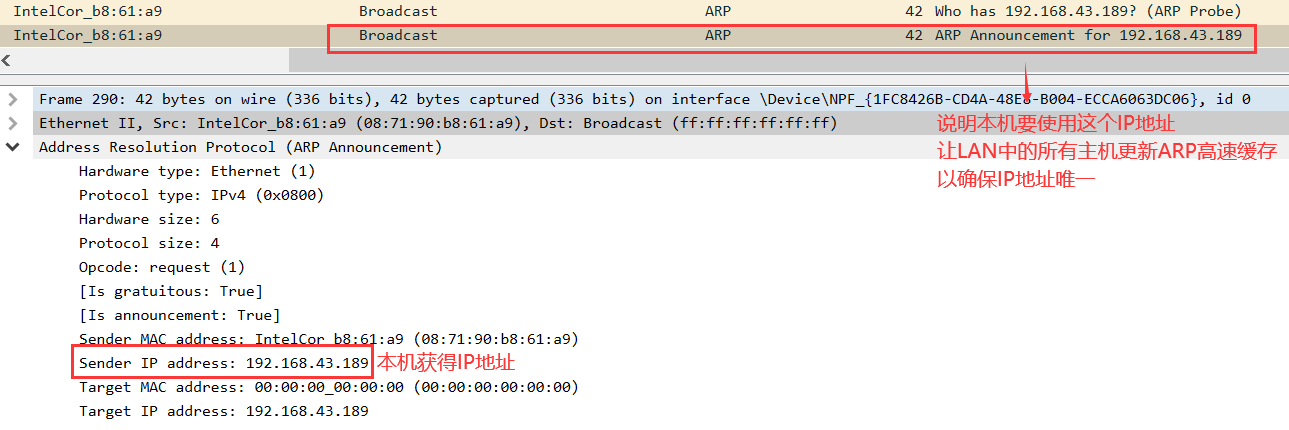
首先广播我的IP地址，以确保分配的IP地址不冲突



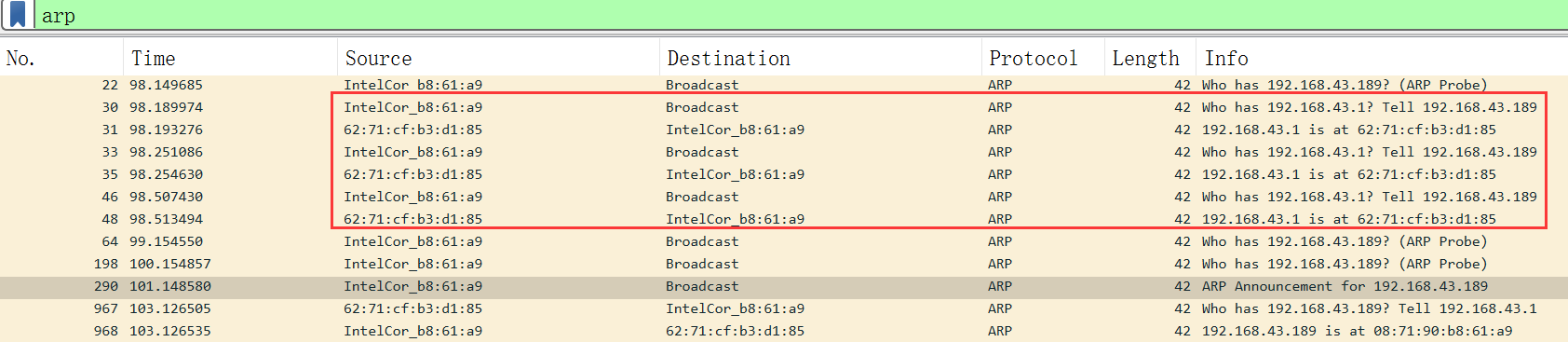
广播ARP



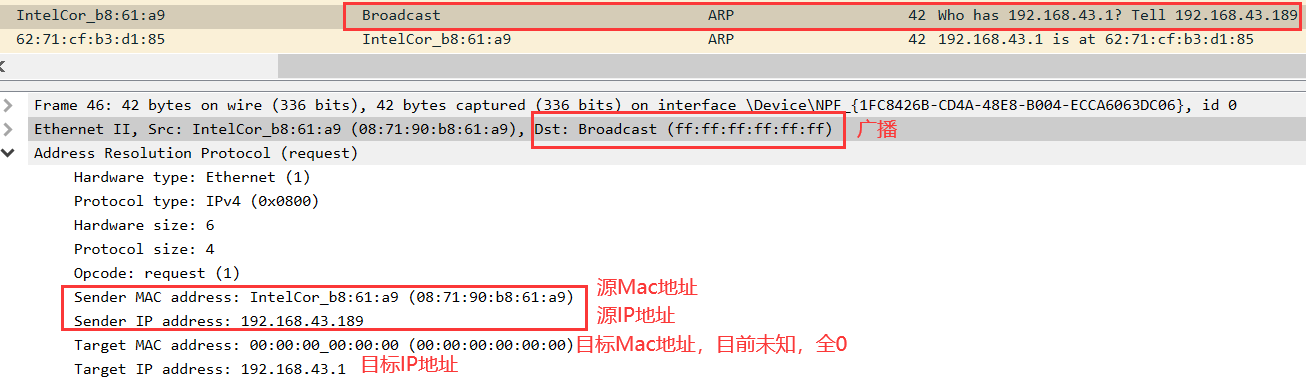
响应ARP



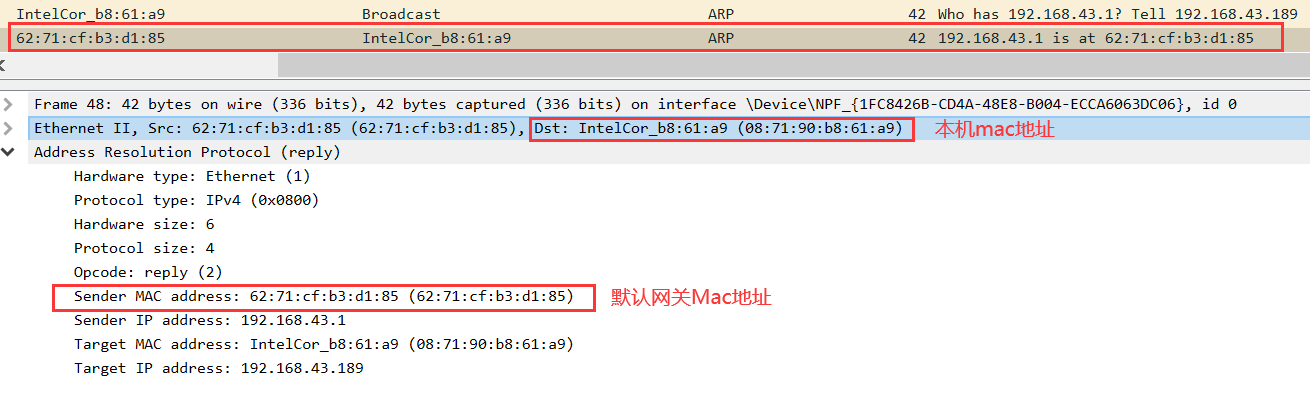
当目的IP地址和本机IP地址不在同一个网段，就需要将数包发送给默认网关，这时需要知道默认网关的MAC地址，因此广播寻找默认网关的MAC地址



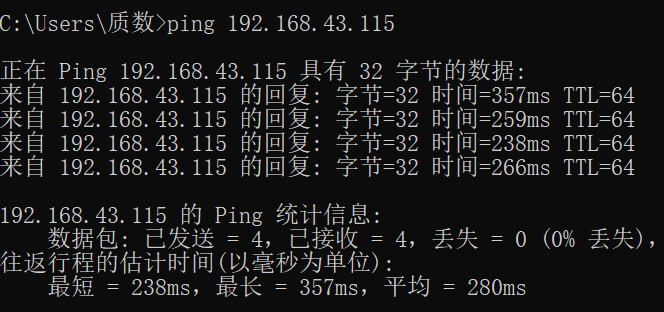
ARP广播寻找默认网关MAC地址



ARP响应找到默认网关MAC地址



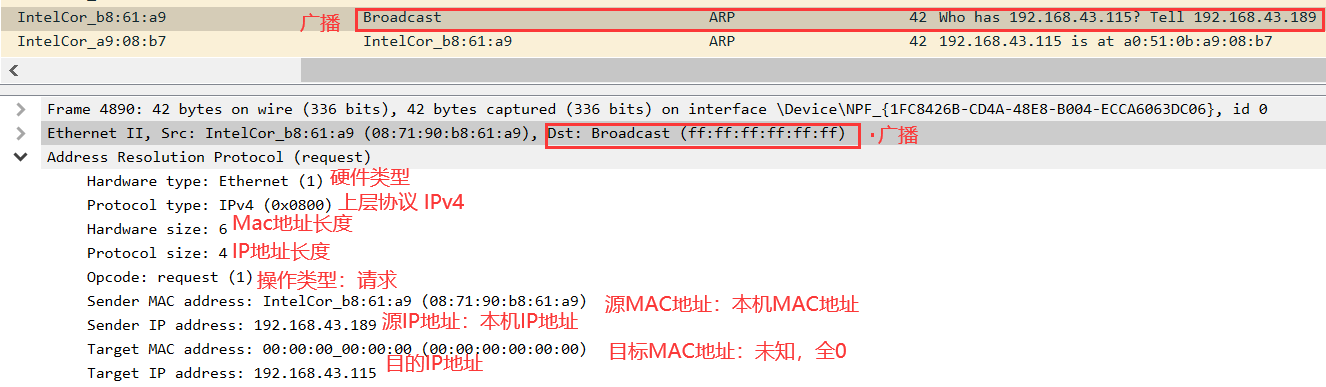
* 从主机A上向主机B发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；



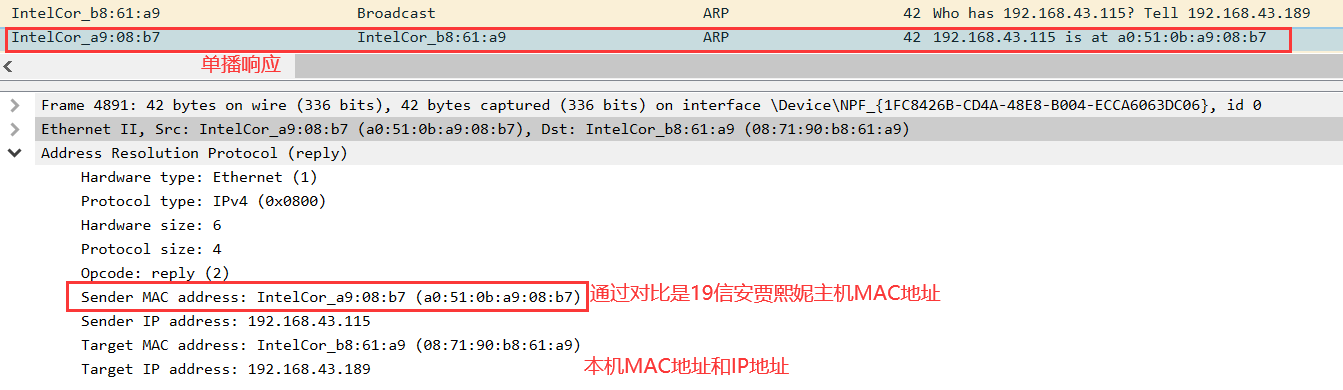
能捕获到ARP报文



因ARP高速缓存中没有IP地址192.168.43.115映射到Mac地址的信息，所以进行广播

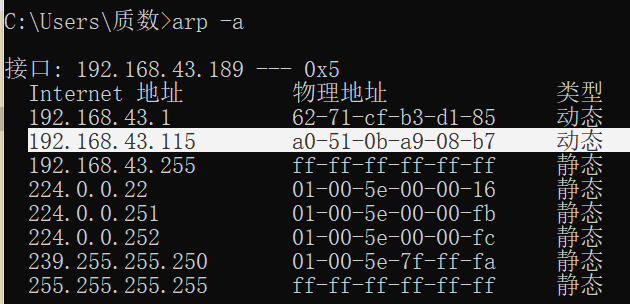


单播响应，由得到的MAC地址可知主机A、B处于同一网络，因此响应主机MAC地址



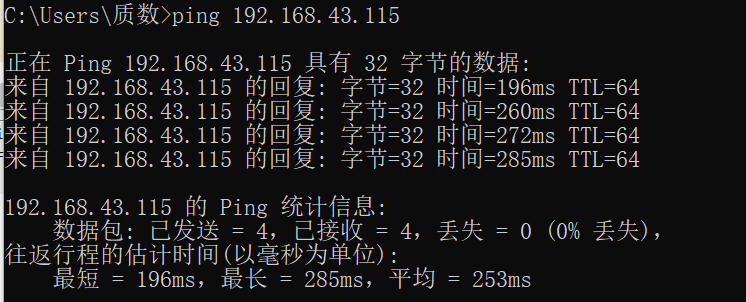
* 通过arp - a 查看ARP表的更新情况，记录此时能否看到B对应的MAC地址；

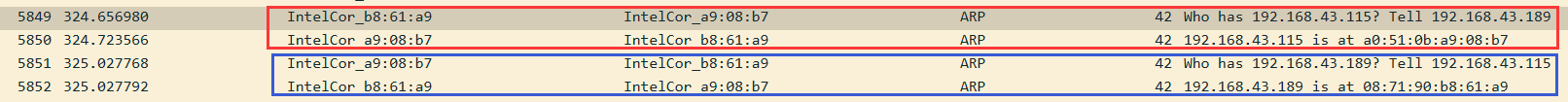
此时更新增加了主机B的IP地址和MAC地址



* 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；

A ping B

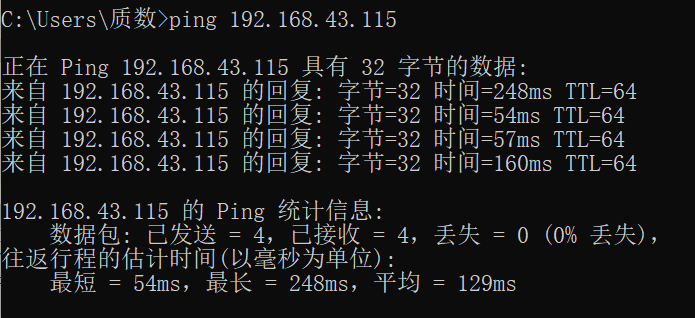


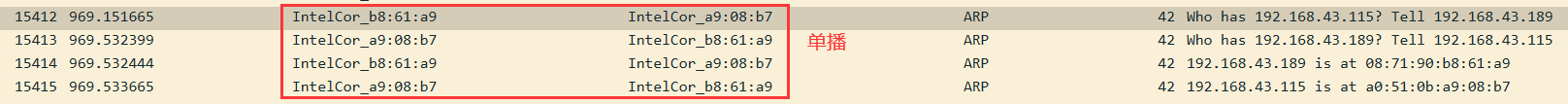


当ARP表更新后，理论上不再使用广播查找目的MAC地址，即不需要再发送ARP数据包，而从高速缓存中就可得到IP地址到MAC地址的映射，但通过wireshark却捕获到了单播ARP包，通过查询得知通常ARP单播请求是用来验证ARP表中的cache是否有效。

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。

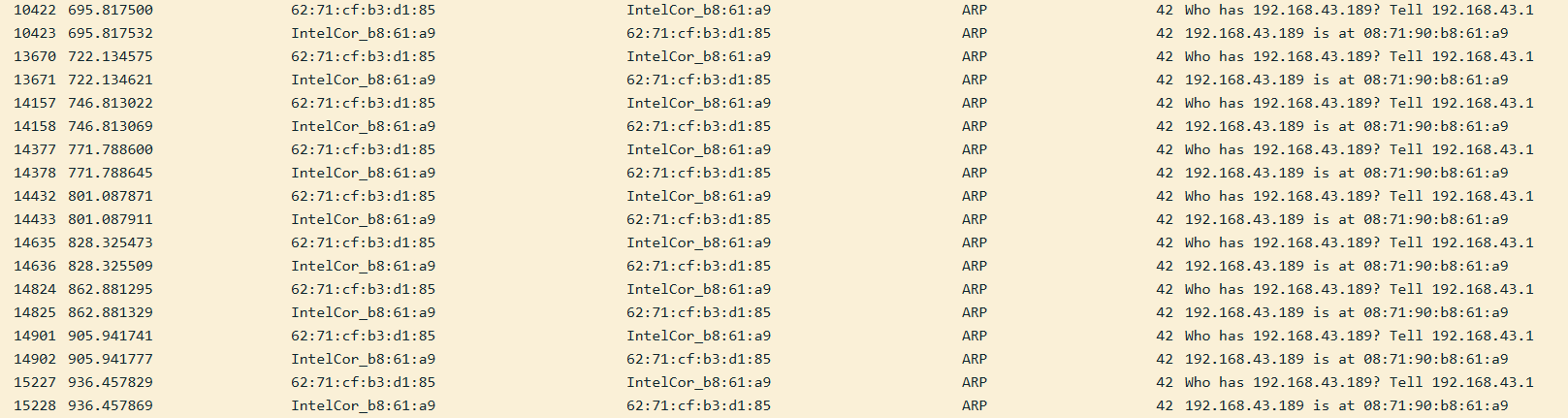
* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。





与上一步相似，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。

在做以上实验过程中，发现不断捕获到主机和默认网关之间的单播请求和响应包



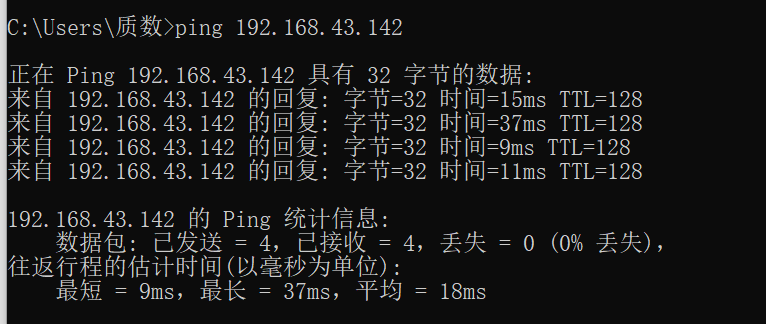
通过查询得知，这与单播轮询有关，通过定期向远端主机发送点对点ARP请求，主动轮询远端主机，如果连续N次轮询都没有收到ARP应答，则删除该表项。用来确保我的IP和网关有效，使我的主机联网且能与其他网络主机通信。

**3、IP协议分析**

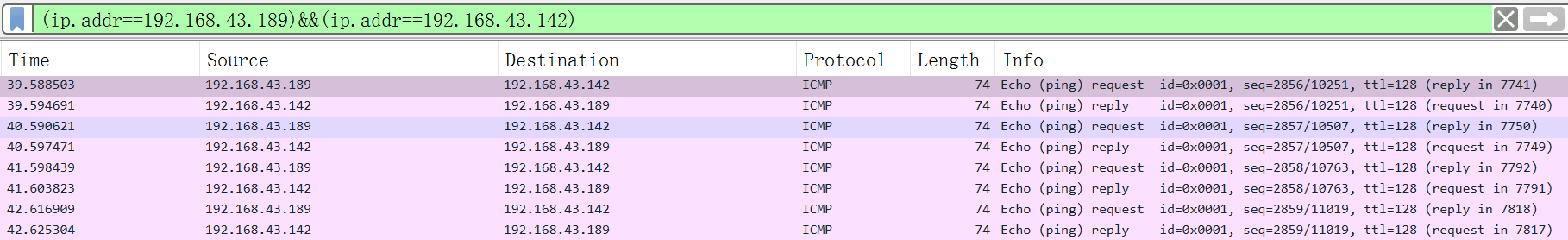
实验时我的IP地址为192.168.43.189，19信安贺萱的IP地址为192.168.43.142

* 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;

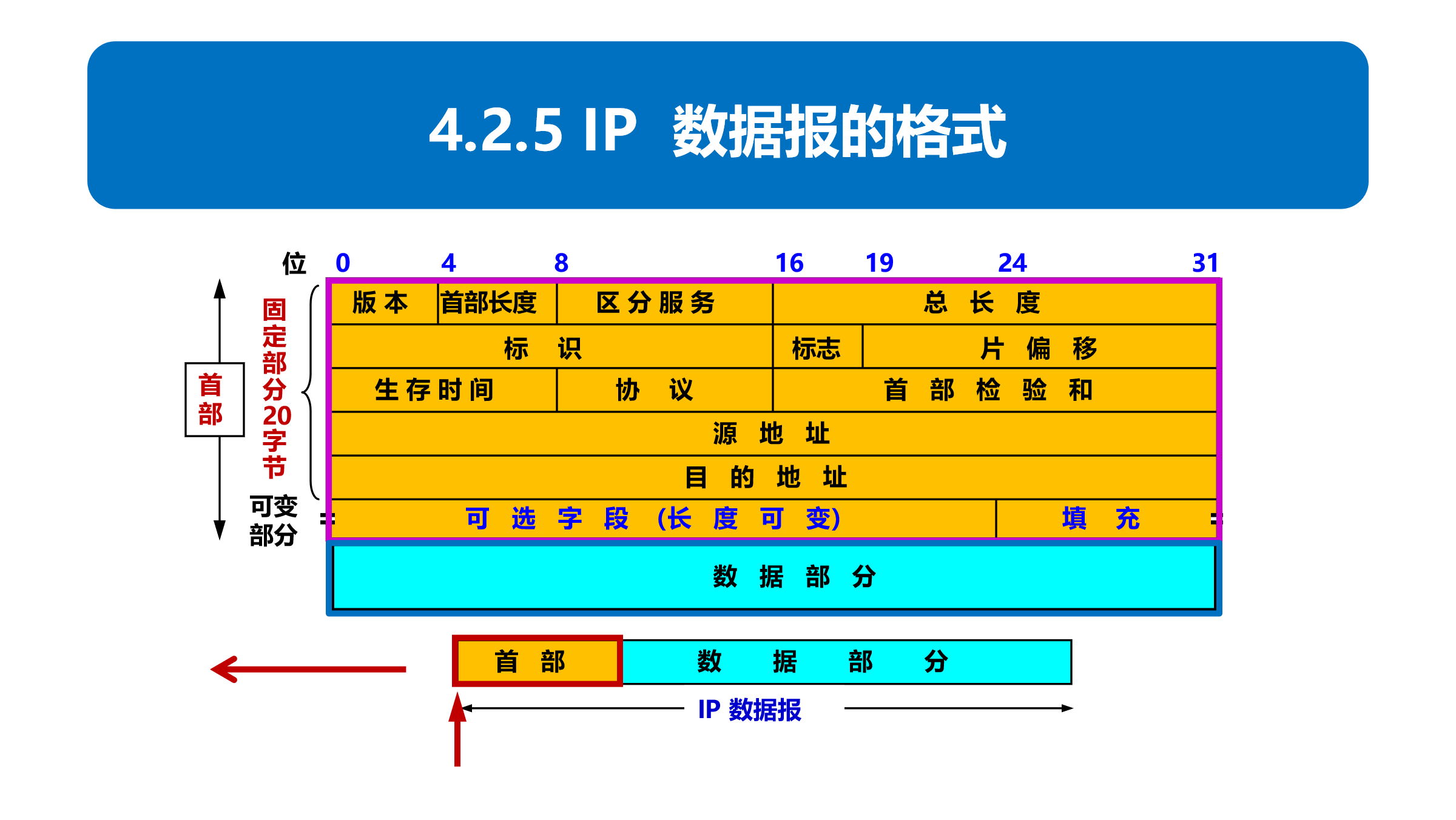
过滤器输入(ip.addr==192.168.43.189)&&(ip.addr==192.168.43.142)，



得到相应请求和相应ICMP报文



由ppt得IP数据包格式为

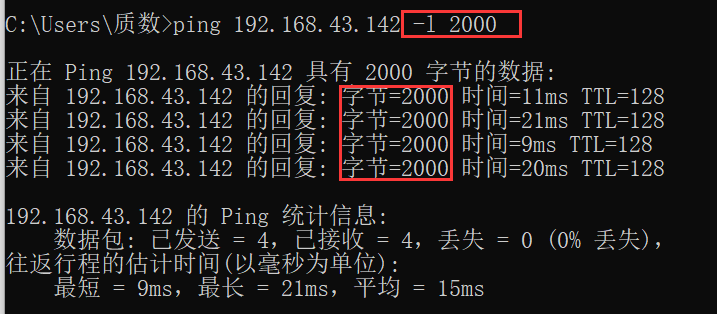


具体分析IP数据包：

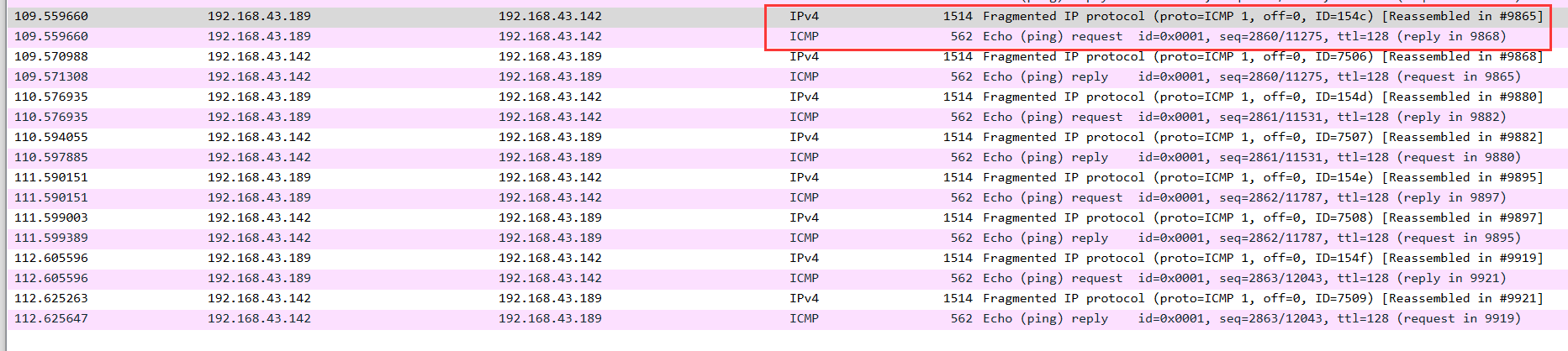


可以看出首部固定部分与IP数据包格式一一对应

* 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。



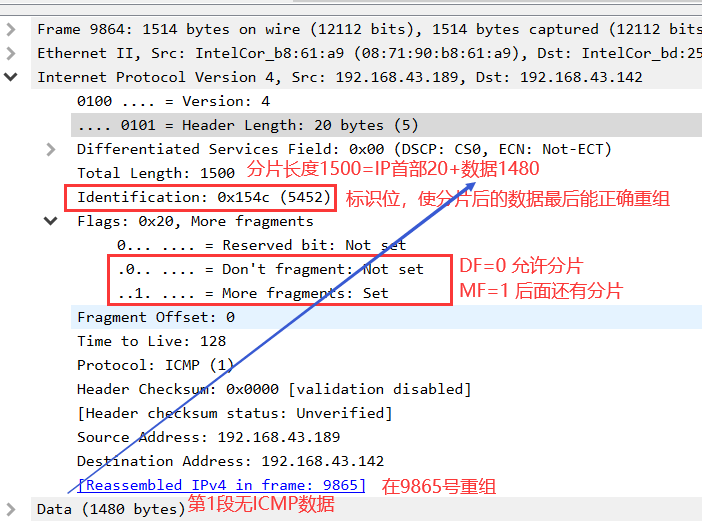
Wireshark捕获到分片数据包



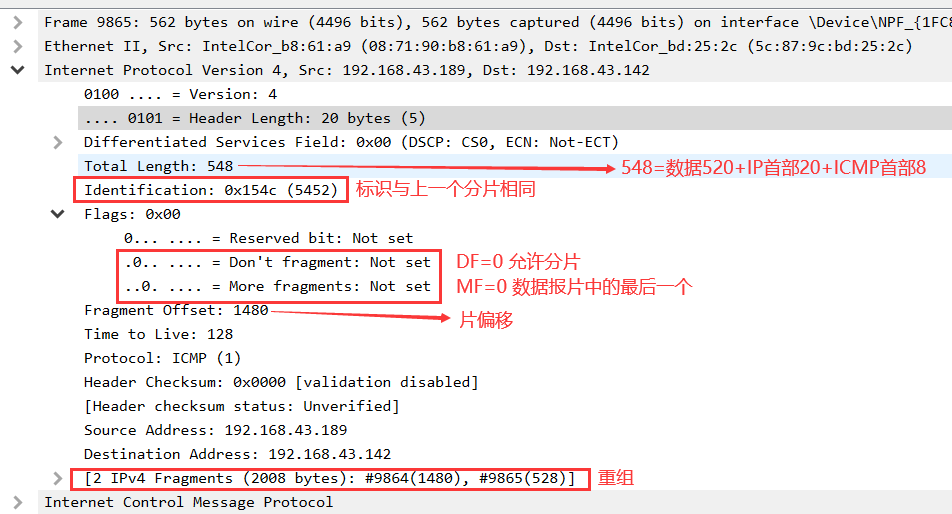
具体分析一次分片和重组的过程：



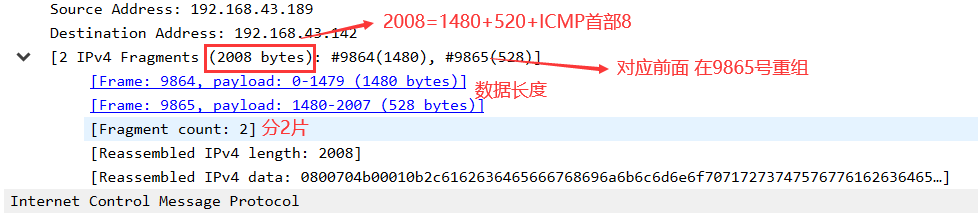
第一个分片：



第二个分片：



重组：

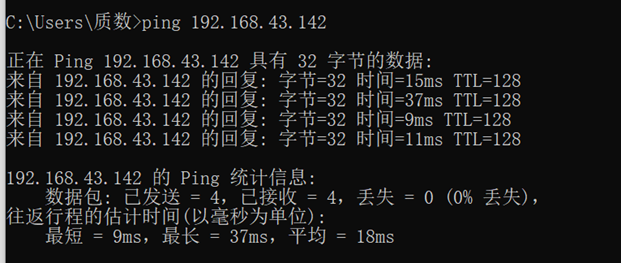


将2000字节长度的数据分为2片，数据长度分片为1480+520，通过相同的标识位重组数据，重组的数据会带上首部信息，因此原本2000长度的数据最后为2008，详细分析见图。

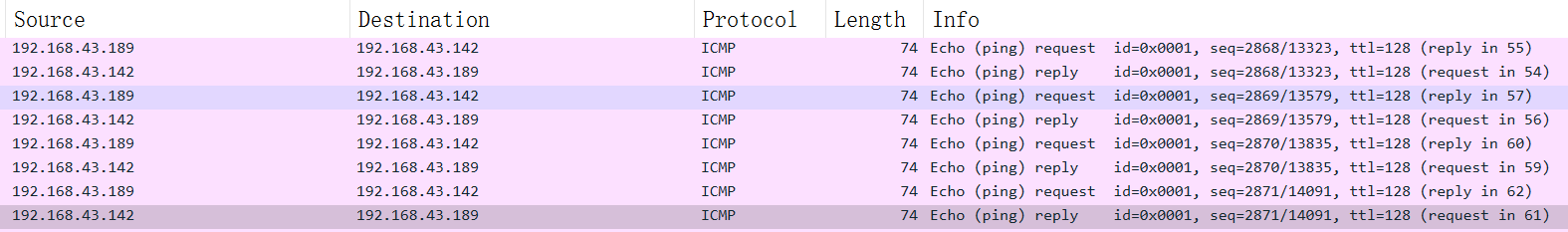
**4、ICMP协议分析**

通过ping和tracet命令，了解ICMP协议的使用。

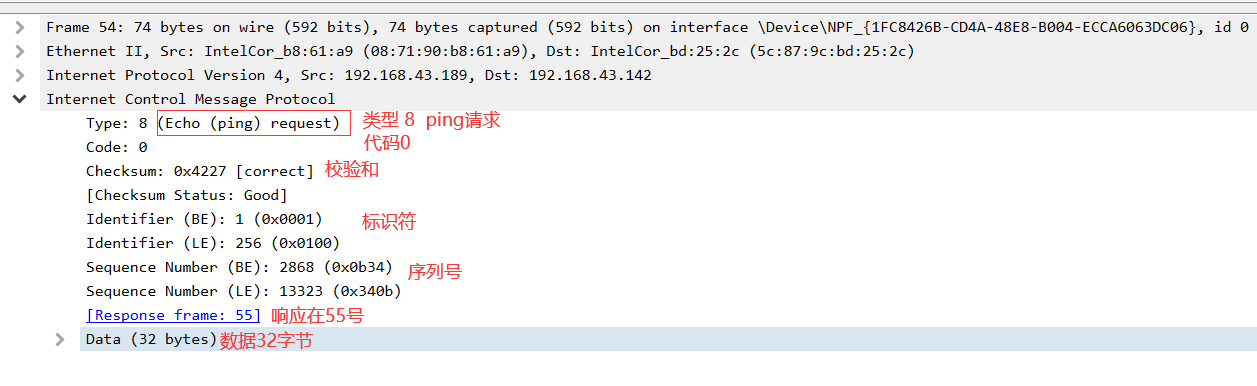
* 从主机A上向主机B发PING检测报文，捕获ICMP请求数据包和应答数据包，记录并分析各字段的含义，并与ICMP数据包格式进行比较；如果返回的差错信息，请分析是由于什么差错引起的。



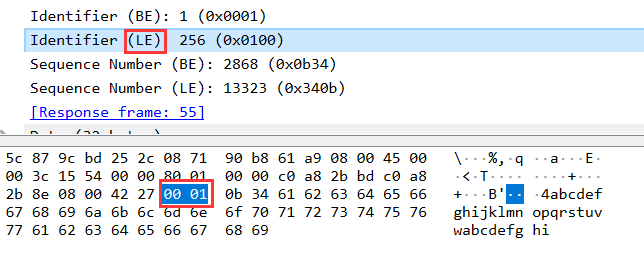
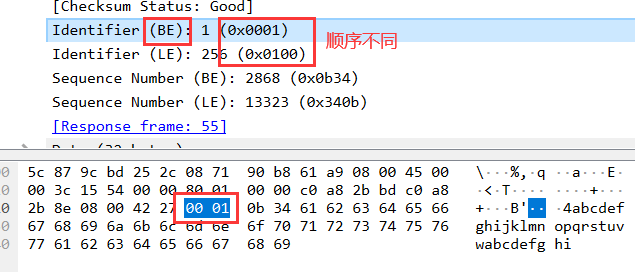
ping后wireshark捕获的ICMP数据包



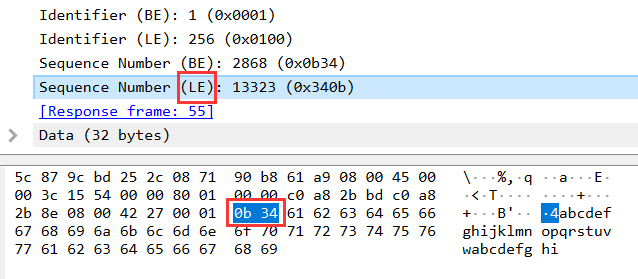
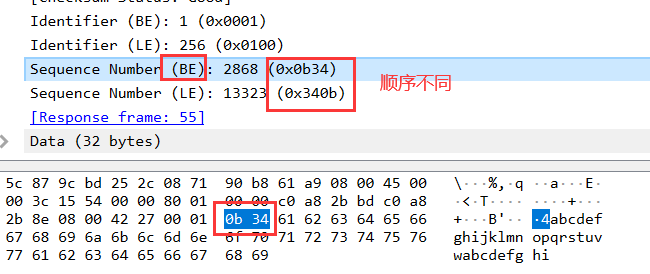
请求数据包分析



发现与ICMP数据包格式相比，Identifier和Sequence Number多了BE和LE的区别



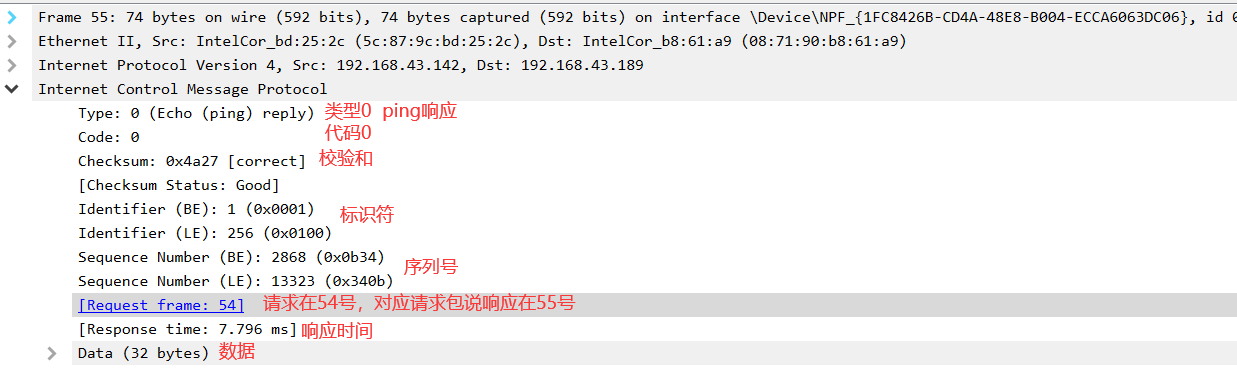
Identifier BE和LE对应的值相同但0x0001和0x0100顺序不同



Sequence Number BE和LE对应的值相同，0x0b34和0x340b顺序不同

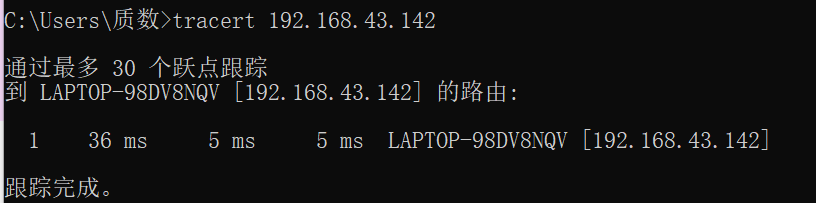
因为Windows是序列号的低位优先字节顺序，而Linux是大端格式，因此Windows为LE：little-endian byte order，Linux为BE：big-endian

应答数据包分析：

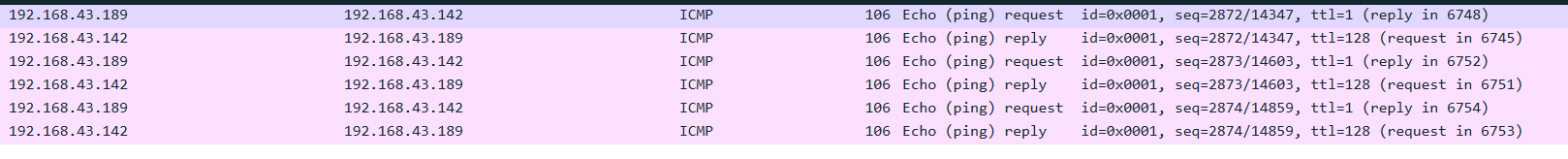


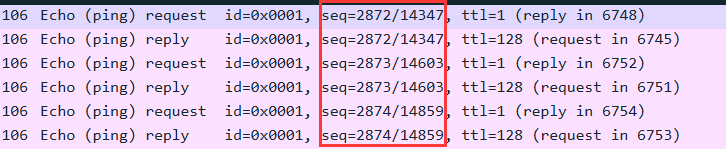
* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。

实验时我的IP地址为192.168.43.189，19信安贺萱的IP地址为192.168.43.142



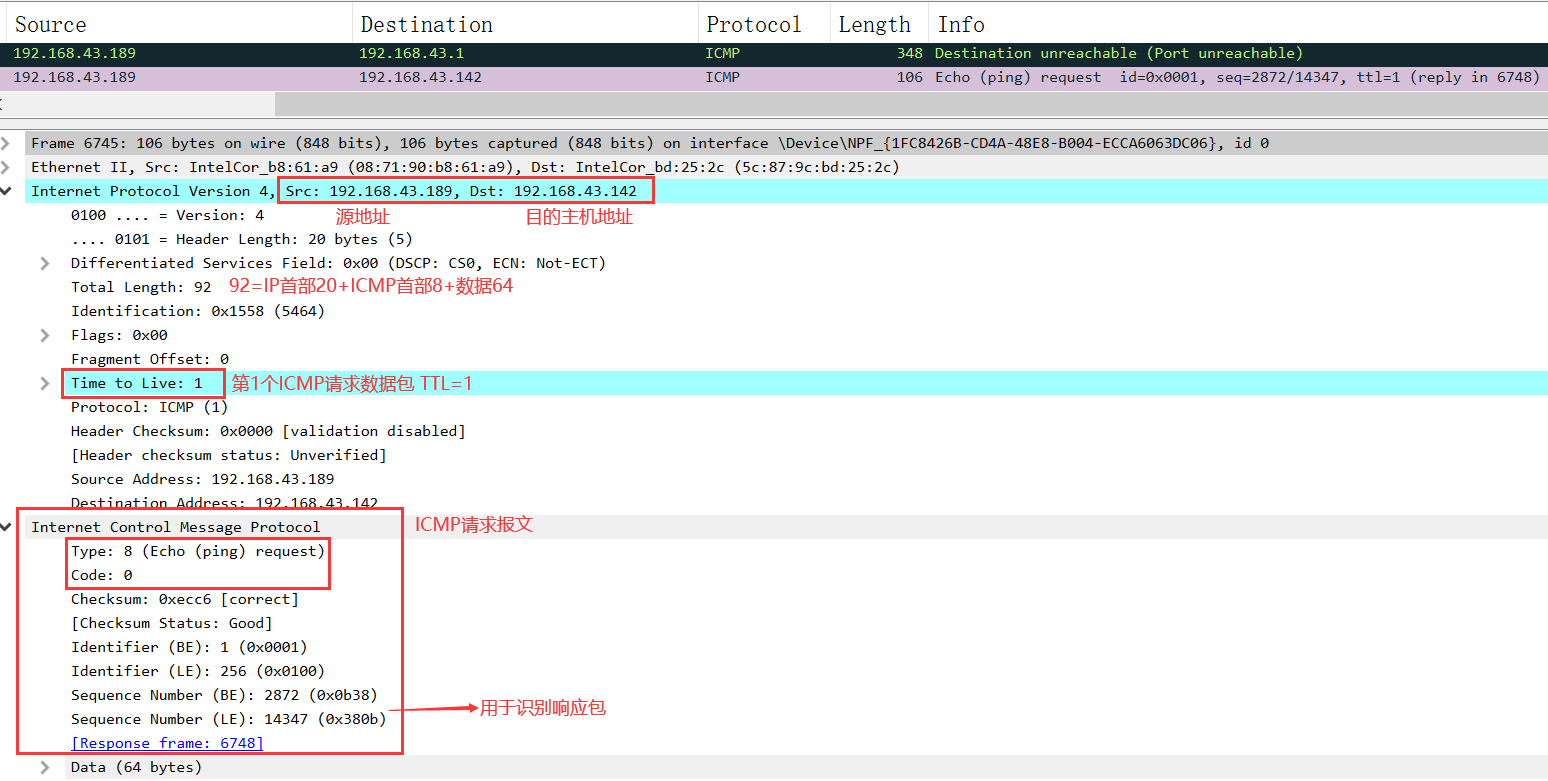
仅需一跳，则说明在同一路由器下，共发送三个探测包，tracert通过seq识别返回的包



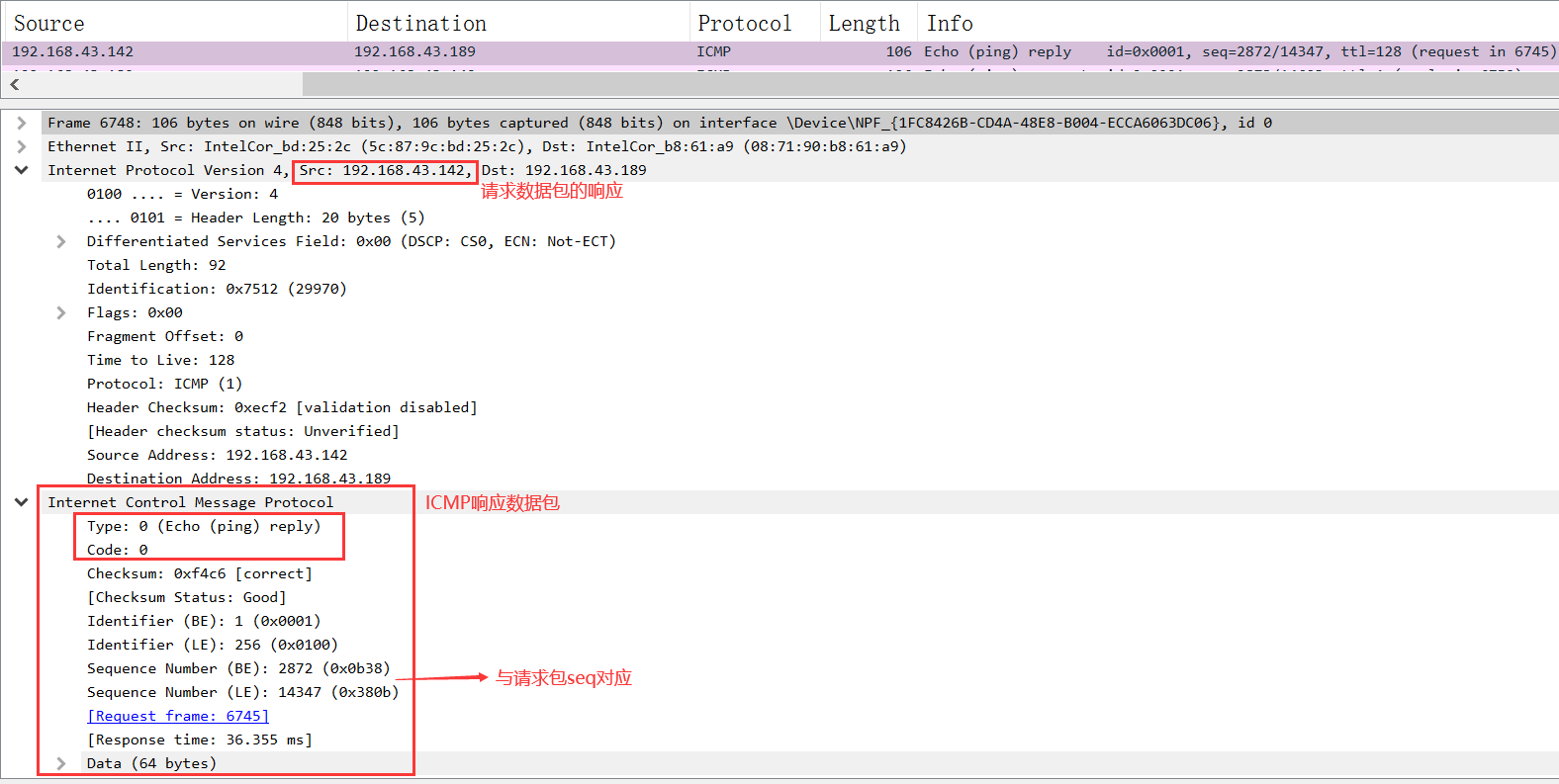


ICMP数据包type=8，请求

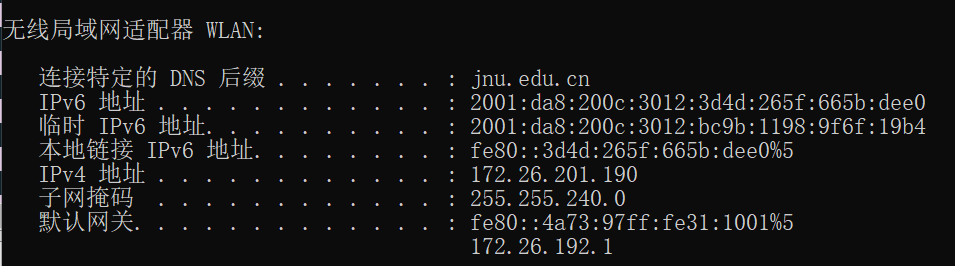
可以看出Tracert命令与ping命令都使用了ICMP协议



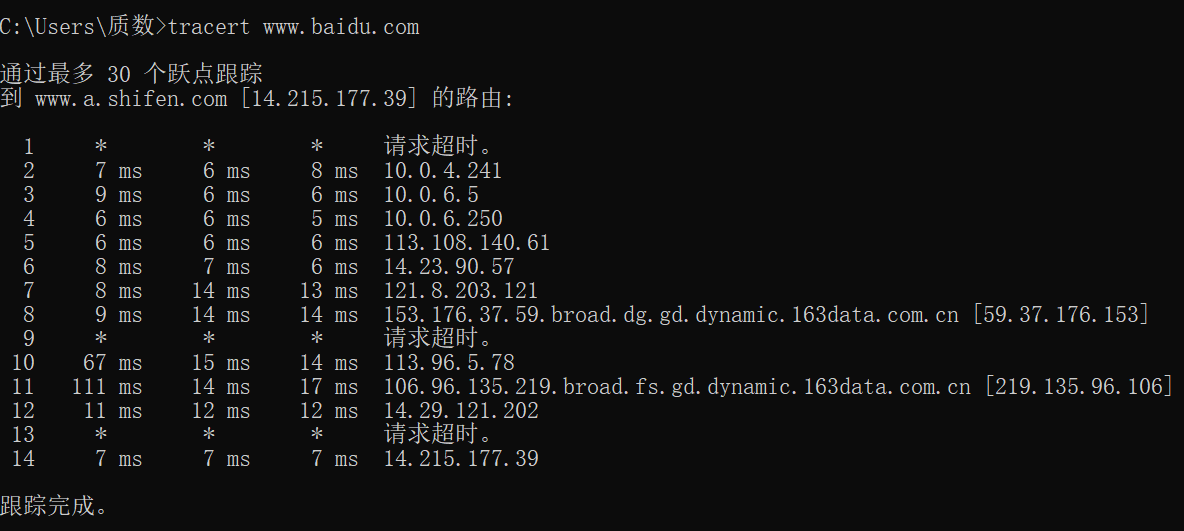
ICMP数据包type=0，响应



为捕获失败的情况，此时连接的为校园网JNU-Secure，我的IP为172.26.201.190

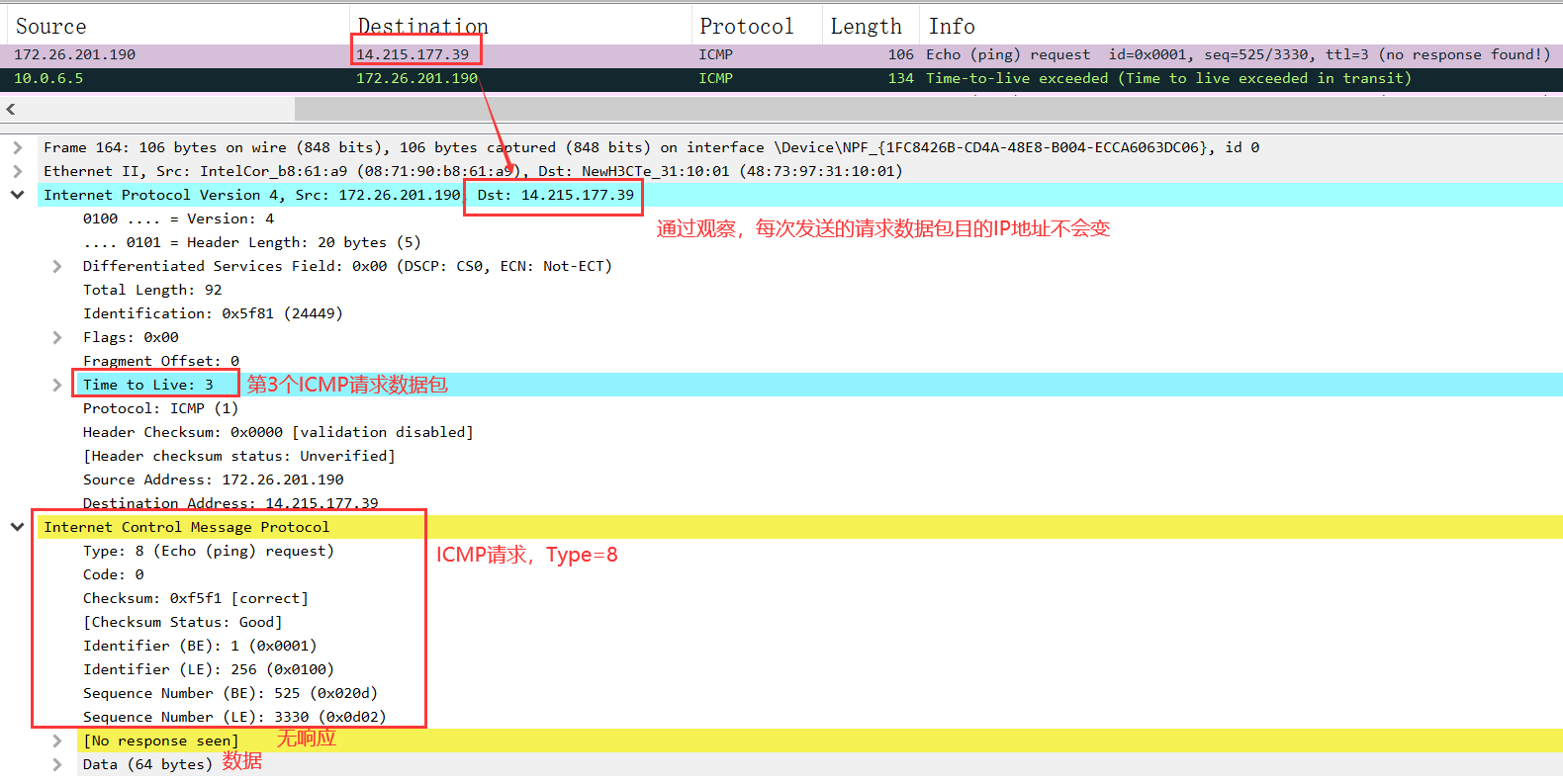


tracert [www.baidu.com](http://www.baidu.com)



存在请求超时的情况，在wireshark上捕获相应数据包

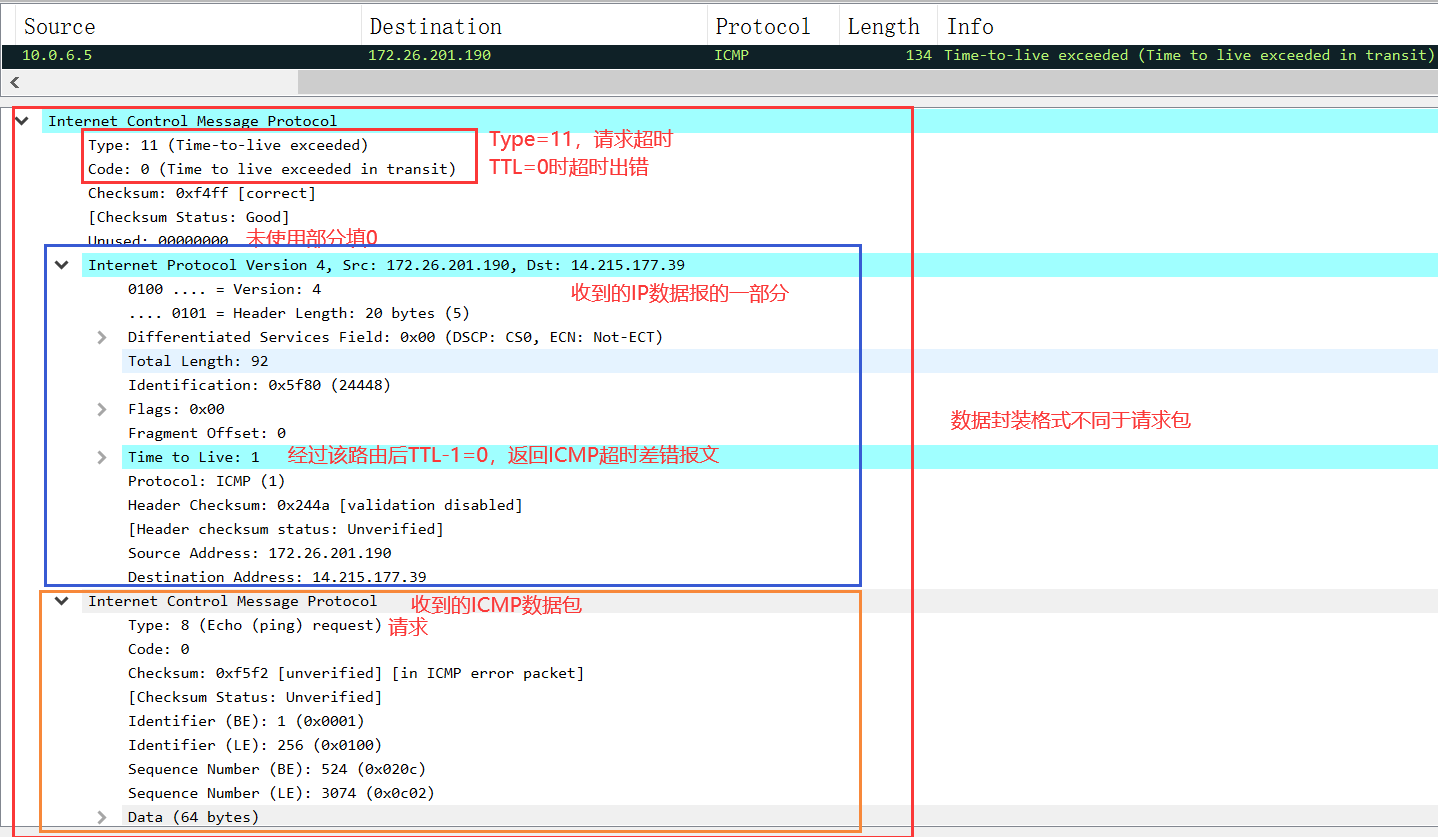
第3个ICMP请求数据包，TTL=3



其数据封装格式为

|  |
| --- |
| IP数据包 |
| ICMP数据包 |

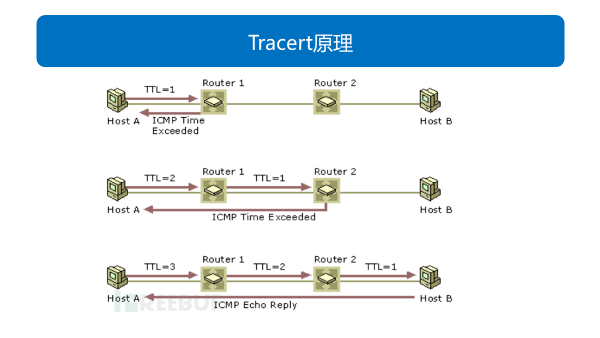
第3个ICMP请求数据包的响应



其数据封装格式为

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | 类型 | 代码 | 校验和 | |
| 未使用部分 |
| 收到的IP数据包的一部分，包括IP首部和数据包数据的前8字节 |

tracert工作原理：



主机A向主机B发送ICMP请求包，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。

**【思考题】（分析原因并通过实验验证）**

* **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？**

**分析：**

当主机A要向本局域网上某台主机B发送IP数据报时，就先在其ARP高速缓存中查看有无主机B的IP地址。若在ARP高速缓存中查出其对应的MAC地址，则无需发送ARP请求，此时捕获不到ARP报文；若无缓存，则需广播发送一个ARP请求分组，此时捕获到ARP报文。

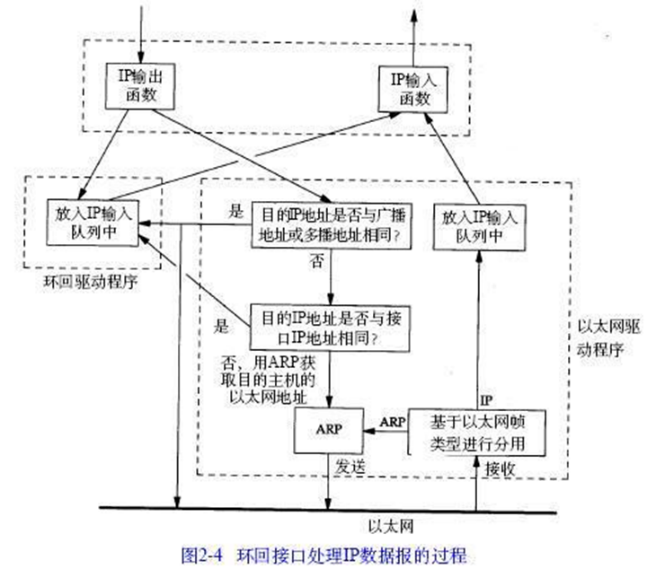
**验证：**

在ARP包分析实验过程中，通过arp -a查看ARP表，当ARP表无主机B的IP地址到MAC地址映射记录时，可以捕获到ARP广播报文，当ARP表更新后增加主机B的信息后，捕获不到ARP广播报文，只能捕获ARP单播报文，用于确认该缓存映射是否仍有效。

* **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？**

**分析：**

运行ping 127.0.0.1时，不能捕获到ICMP报文，因为127.0.0.1用于本机环回测试,若主机发送一个目的地址为环回地址的IP数据报，则本主机中的协议软件就处理数据报中的数据，而不会把数据报发送到任何网络。



由该图得到环回接口处理IP数据报流程为：

IP输出函数首先检查地址是否为环回地址：

①若是环回地址，直接交给环回驱动程序处理，返回IP输入函数；

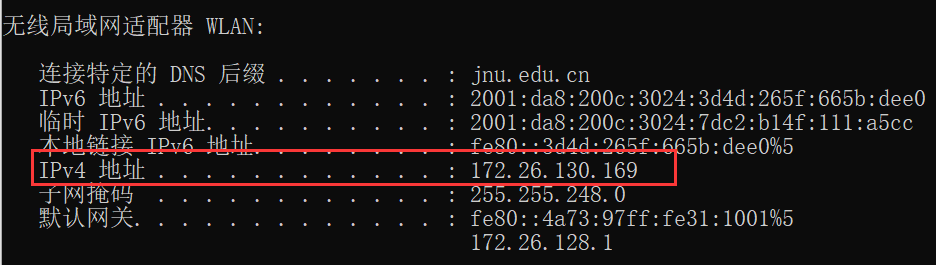
②若不是环回地址，判断目的IP地址是否与广播地址或多播地址相同，若相同也交给还回驱动程序处理；

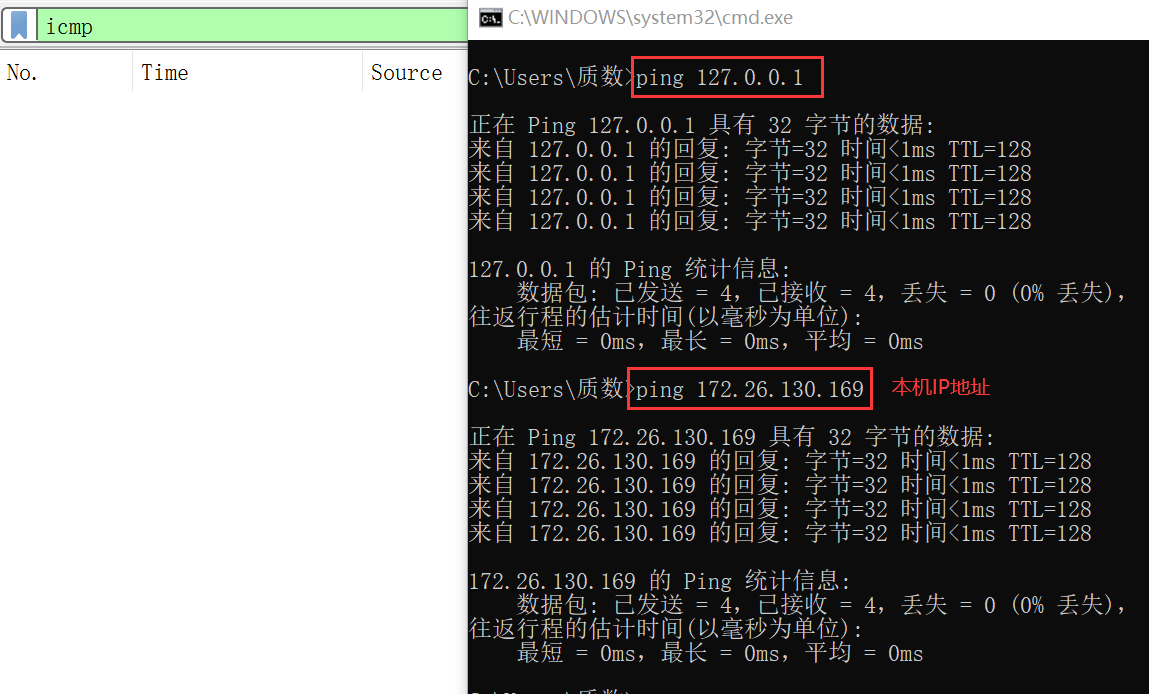
③若不是广播或多播地址，判断目的IP地址是否与本机接口IP地址相同，若是本机IP地址，则放入环回驱动程序，若不是则用ARP获取MAC地址

由以上过程可知运行ping 本机IP地址交由环回驱动程序处理，不经过以太网，也不能捕获到ICMP报文

**验证：**

验证实验时我的IP地址如下





验证证明两种情况都不能捕获到ICMP报文

* **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？**

**分析:**

“Request timed out”是ping的数据包具有到达目标的路由，但到达不了返回的路由。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。

“Destination Host Unreachable” 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。

**验证：**

“Request timed out”

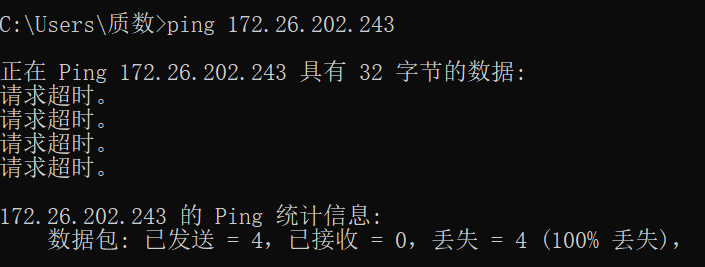
防火墙开启：

我的IP地址

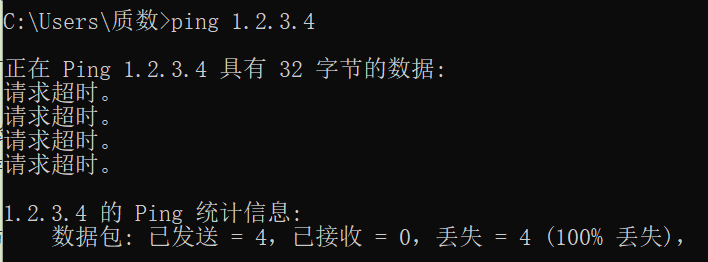


19信安贾熙妮的IP地址





不在同一网段内

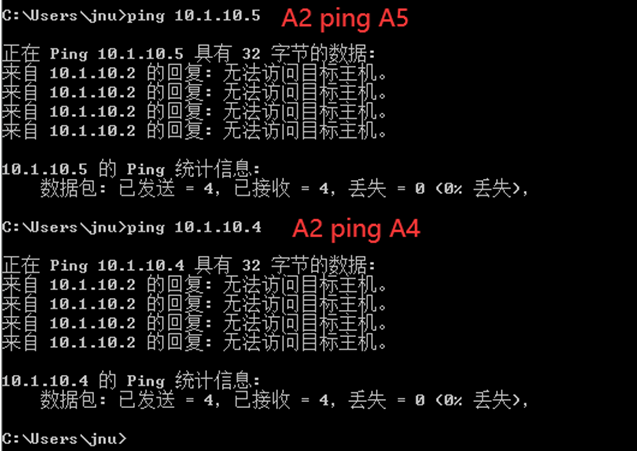


“Destination Host Unreachable”

当我的电脑连接我的热点，我的IP地址为192.168.43.189时，在前面实验19信安贺萱和我连接同一热点的IP地址为192.168.43.142，但做验证实验时已知无人连接该热点，因此无人接入对应的广播域，此时该IP地址不存在，ping时出现无法访问目标主机的情况。



想到在做实验5、6时，不在同一VLAN下的主机也互相ping不通，显示无法访问目标主机，原因是不在同一广播域



* 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。**

同一网段内的主机不需要通过网关通信，因此不设置网关没有影响

我与19信安贺萱的主机同时连接我的热点，手动配置不设置网关

|  |  |
| --- | --- |
| 主机A |  |
| 主机B |  |

|  |  |
| --- | --- |
| A ping B |  |
| 8个ICMP数据包 |  |
| 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。**

|  |  |
| --- | --- |
| A |  |
| B |  |

|  |  |
| --- | --- |
| A ping B |  |
| Wireshark |  |

不设置网关，不同网段的主机不能通信

**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。**

|  |  |
| --- | --- |
| A |  |
| B |  |

|  |  |
| --- | --- |
| A ping B |  |
| 8个ICMP数据包 |  |
| ARP数据包 | 根据捕获到的ARP数据包可知，不是广播，能看到对方主机的MAC地址 |

**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）。**

**能通信：**

|  |  |
| --- | --- |
| A |  |
| B  baidu.com的IP地址 |  |

|  |  |
| --- | --- |
| A ping B |  |
| ICMP数据包 |  |
| ARP数据包 | ARP数据包能看到网关的MAC地址 |

**不能通信：**

|  |  |
| --- | --- |
| A |  |
| B |  |

|  |  |
| --- | --- |
| A ping B |  |
| ICMP数据包 |  |
| ARP数据包 | ARP数据包能看到网关的MAC地址 |

* 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。**

主机A：00001010.00000010. 00000010. 00000010

主机B: 00001010.00000010. 00000011. 00000011

地址掩码11111111.11111111.11111110.00000000 (255.255.254.0）

|  |  |
| --- | --- |
| A网络地址计算 | 00001010.00000010. 00000010. 00000010  11111111.11111111.11111110.00000000  ----------------------------------------------------与运算  00001010.00000010. 00000010.00000000  网络地址为10.2.2.0/23 |
| B网络地址计算 | 00001010.00000010. 00000011. 00000011  11111111.11111111.11111110.00000000  ----------------------------------------------------与运算  00001010.00000010. 00000010.00000000  网络地址为10.2.2.0/23 |

可得主机A和B的网络地址相同，不设置网关A与B也能通信，理论上可以互相ping通

实验时

|  |  |
| --- | --- |
| 主机A  配置 |  |
| 主机B  配置 |  |

|  |  |
| --- | --- |
| A ping B |  |
| B ping A |  |

理论分析可以ping通，实际却没有ping通，在ARP表中有对应的物理地址 ，考虑实验前未修改IP地址时没有测试两台主机的连通性，未排除接线原因，等下次实验有机会再安装wireshark尝试寻找原因。

**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和B的地址掩码不同，A与 B通信时用A的地址掩码计算网络地址，B与 A通信时用B的地址掩码计算网络地址，具体计算过程如下：

主机A：00001010.00000010. 00000010. 00000010

主机B: 00001010.00000010. 00000011. 00000011

A与 B通信时：A、B网络地址不同

|  |  |
| --- | --- |
| A网络地址计算 | 地址掩码：11111111.11111111.11111111.00000000  00001010.00000010. 00000010. 00000010  11111111.11111111.11111111.00000000  ---------------------------------------------------与运算  00001010.00000010. 00000010.00000000  网络地址为10.2.2.0/24 |
| B网络地址计算 | 地址掩码：11111111.11111111.11111111.00000000  00001010.00000010. 00000011. 00000011  11111111.11111111.11111111.00000000  ---------------------------------------------------与运算  00001010.00000010. 00000011. 00000000  网络地址为10.2.3.0/24 |

B与 A通信时：A、B网络地址相同

|  |  |
| --- | --- |
| A网络地址计算 | 地址掩码：11111111.11111111.11111110.00000000  00001010.00000010. 00000010. 00000010  11111111.11111111.11111110.00000000  ---------------------------------------------------与运算  00001010.00000010. 00000010.00000000  网络地址为10.2.2.0/23 |
| B网络地址计算 | 地址掩码：11111111.11111111.11111110.00000000  00001010.00000010. 00000011. 00000011  11111111.11111111.11111110.00000000  ---------------------------------------------------与运算  00001010.00000010. 00000010. 00000000  网络地址为10.2.2.0/23 |

A ping B时，计算得到的A,B网络地址不同，又因为未设置网关，A向B发送的请求包B接收不到，因此此时ping不通。

B ping A时，通过计算A和B的网络地址相同，B可以向A发送请求包，A向B发送响应包时计算得AB不在同一网络，又未设置网关，无法发送响应包给B,因此也ping不通。

以上两种情况虽然都是ping失败，但显示的错误信息应不同。

验证:

|  |  |
| --- | --- |
| 主机A  配置 |  |
| 主机B  配置 |  |

|  |  |
| --- | --- |
| A ping B |  |
| B ping A |  |

1. **实验总结**

本次实验通过以太网协议分析，可知目的主机IP地址不会变，而以太网协议中的目的MAC地址若不需要路由器转发则为目的主机的MAC地址，否则为对应网关硬件地址。

通过ARP协议分析实验进一步理解掌握ARP协议的工作过程，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，在捕获数据包过程发现不断捕获到主机和默认网关之间的单播请求和响应包，这与单播轮询有关，用来确保我的IP和网关有效，使我的主机联网且能与其他网络主机通信。

通过IP协议分析实验，对IP协议格式有进一步熟悉，同时对分片和重组过程有了进一步掌握。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，实验中对wireshark的ICMP数据包Identifier（BE）、Identifier（LE）、Sequence number(BE)、Sequence number(LE)感到疑惑，通过查询得知是wireshark根据Windows和Linux系统设置的，对应数值不变，只是表达方式改变，其中Windows为LE：little-endian byte order，Linux为BE：big-endian。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。

通过思考题的分析和验证，对能否捕获ARP报文的情况进行了总结分析，同时对环回驱动程序有了进一步了解，知道ping 127.0.0.1和本机IP地址不能捕获到报文的原因。同时，对ping过程中出现ping不通的情况进行了原因分析和验证，并对“网关”有了进一步理解。在同一网段不设置“网关”即可通信，但不同网段通信必须设置“网关”，对于最后一道思考题遗留的问题还需下次实验查找原因。