**暨南大学本科实验报告专用纸**

课程名称 计算机网络 指导教师 潘冰 成绩

实验项目名称 数据链路层和网络层协议分析 实验项目编号

实验项目类型 验证 实验地点 计算机网络实验教室 学院 专业 智科院19级信息安全

学生姓名 李媛 学号 2019050385

实验时间 2021 年 11 月 1 日

**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。

**2.【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。

**3.【实验环境】**

计算机2台，交换机一台。

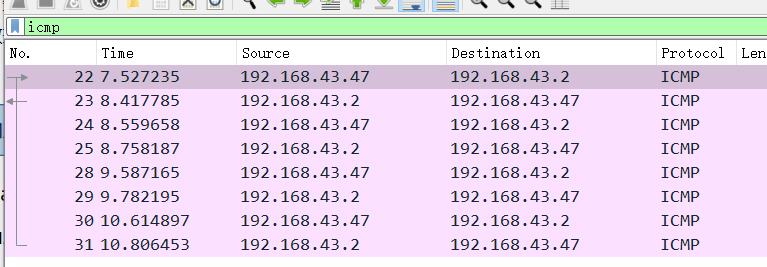
**4.【实验步骤以及分析过程】**

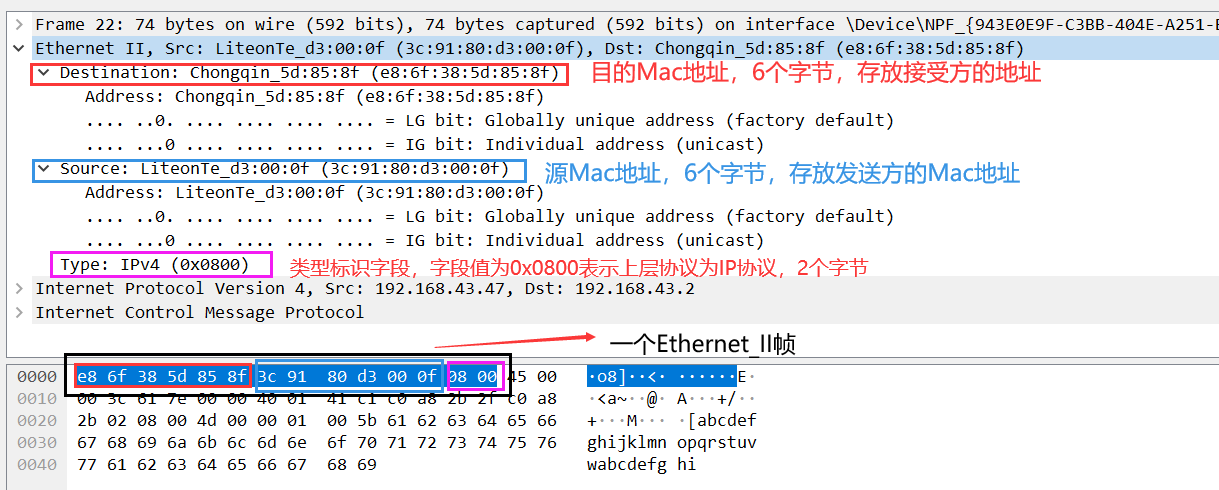
1. 安装Wireshark
2. 以太网协议分析

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。

实验过程：

* 将主机A与B连接到同一个局域网互相ping通，分析其中一份ICMP报文的以太网帧格式如下：





如图，以太网帧中包含了目的主机的mac地址，源主机mac地址，以及TYPE类型字段，致命上一层（网络层）使用的是什么协议，在这里0x800指明了icmp使用的网络层协议为IP协议

* **思考，IG位和LG位有什么特殊的含义？**

去查阅资料，得出答案：IG位对应MAC的第8位，用于区分单播地址和组播地址，众所周知，只有单播地址的前24位代表厂家，且第一个字节的最后一位是0，组播地址第一个字节的最后一位是1，广播地址属于特殊的组播地址，其MAC地址是48个1，因此也可以理解为，广播地址在MAC上标识同一种设备。抓包结果中的unicast也是单播的意思。观察这条报文，IG位是0，说明是进行的单搏。

而LG位的作用就没那么常用了，在日常生活中几乎见不到。LG位是MAC地址的第7位，它的作用就是做一个特殊标识，如果有关部门或者政府想让这个设备“特殊”一点，可以把这一位置为1，用来区别于其他设备。

总结上文意思即是：一般主机发送数据帧有三种方式：单播、组播、广播。三种发送方式的帧的D.MAC字段有些区别。单播时，MAC地址的第一个字节的第8个比特位为0；组播时，第一个字节的第8个比特位为1；广播时，48个比特位全为1，即表示为FF-FF-FF-FF-FF。

* **思考，为什么报文里没有8字节的前序和4字节的FCS？**

前序：由0、1间隔代码组成，用来通知目标站作好接收准备。以太网帧则使用8个字节的0、1间隔代码作为起始符.在帧的前面插入（硬件生成）的 8 字节中，第一个字段共 7 个字节，是前同步码，用来迅速实现 MAC 帧的比特同步。第二个字段 1 个字节是帧开始定界符表示一帧实际开始。

FCS：循环冗余校验字段，用来对数据进行校验，如果校验结果不正确，则将数据丢弃。该字段长4字节。

为什么在wires hark报文里面捕获不到这12个字节呢？

通过查阅资料，得出答案：

是因为wireshark把这2个都给过滤了。

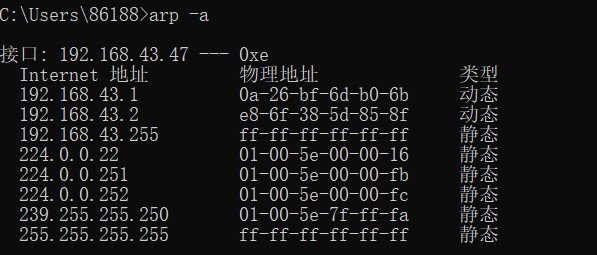
在物理层上网卡要先去掉前导同步码和帧开始定界符，然后对帧进行CRC检验，如果帧校验和错，就丢弃此帧。如果校验和正确，就判断帧的目 的硬件地址是否符合自己的接收条件（目的地址是自己的物理硬件地址、广播地址、可接收的多播硬件地址等），如果符合，就将帧交“设备驱动程序”做进一步处 理。这时我们的抓包软件才能抓到数据，因此，抓包软件抓到的是去掉前导同步码、帧开始分界符、FCS之外的数据，因此，在报文里看不到前序也看不到末尾的FCS

1. ARP协议分析

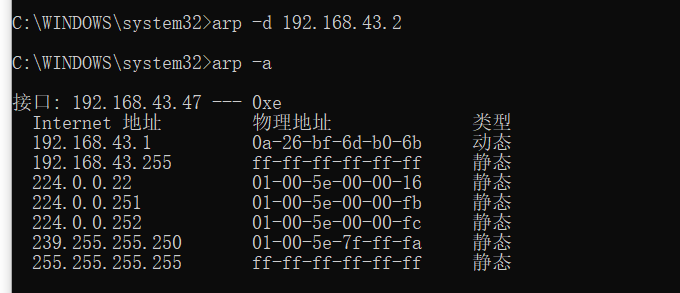
实验过程：

* 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 查看本机上的ARP表的情况，如图，存在B（192.168.43.2）的地址记录：

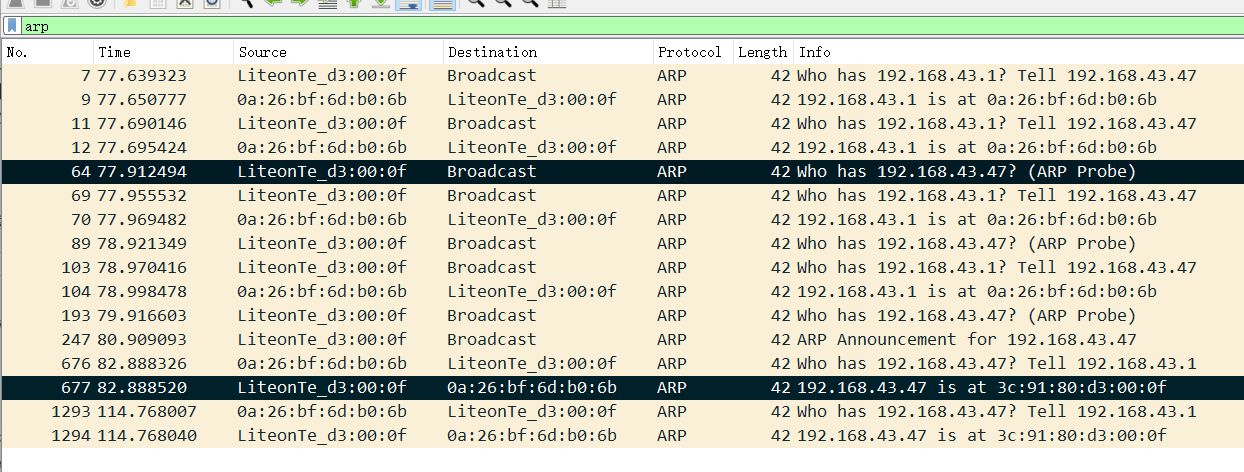


arp –d B 删除B的记录；



* 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；

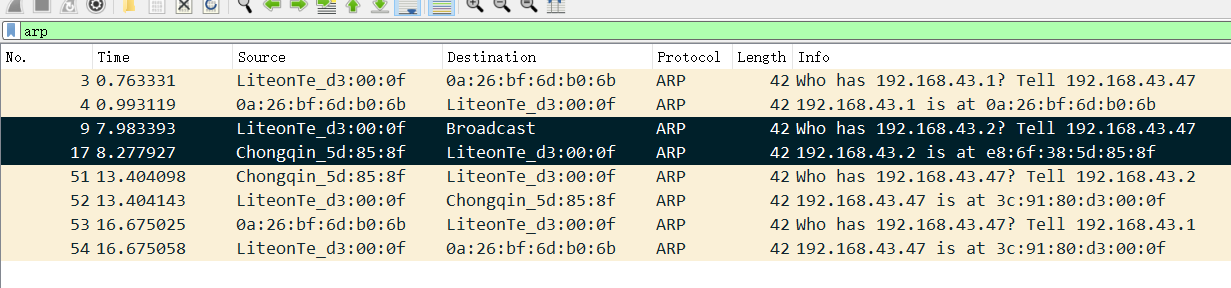
能捕获到ARP报文，如下图：



可以观察到，网线断开一分钟后，再联网收到了两种广播报文，一种是询问默认网关192.168.43.1的mac地址，另一种是询问自身192.168.43.47的mac地址。不排除这些报文有一些是同局域网里另一台主机发送的广播报文的可能，也可能是因为，网线连接需要一些数据通信，首先要知道网关的mac地址的，所以会先发送一条广播报文先去寻找默认网关

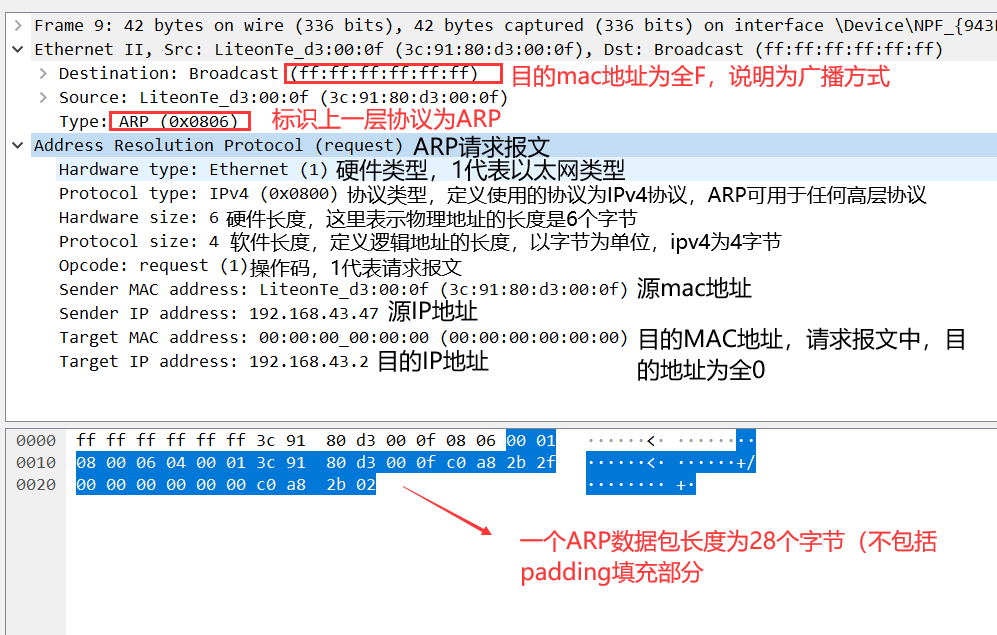
* 从主机A上向主机B发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义

能捕获到ARP报文：



分析ApingB：

1. 主机A 192.168.43.47想知道主机B 192.168.43.2的mac地址，在局域网内发送广播ARP报文，询问谁是192.168.43.2，截获到的广播ARP报文分析如下图：

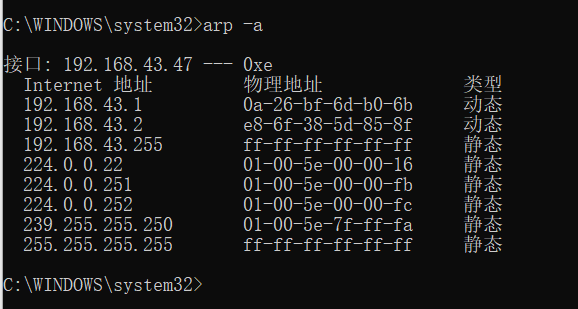


1. 主机B 192.168.43.47收到请求报文，并进行响应，响应ARP报文格式分析如下图：



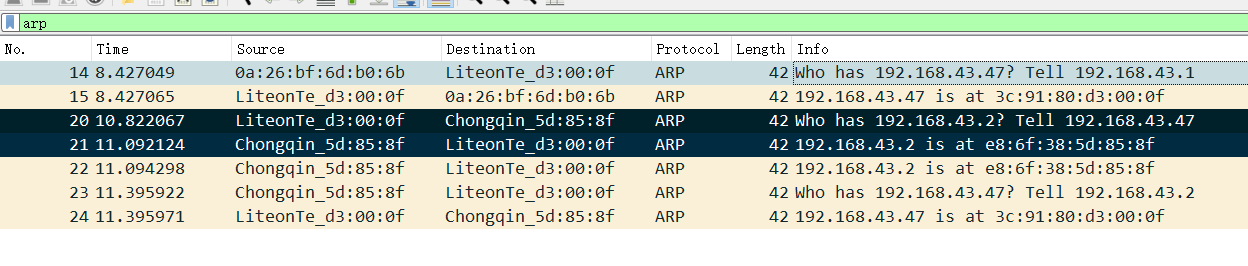
* 通过arp - a 查看ARP表的更新情况，记录此时能否看到B对应的MAC地址；

Ping成功后，A主机和B主机都会将对方的mac地址写入字节的arp缓存表中，方便下一次寻找对方的物理地址时直接从arp路由表中寻找，因此，是会看到对应的mac地址的，如下图：



* 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；

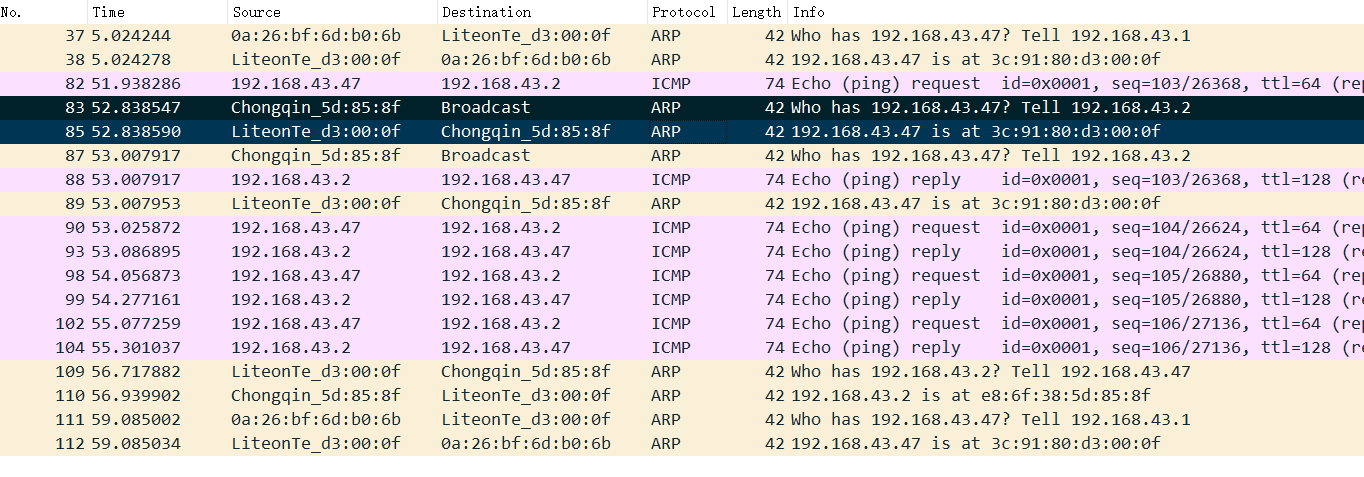
此时可以捕获到arp报文，但是捕获不到A主机发送的广播报文，都是arp的单播报文（为了保证ARP缓存表的实时有效）：



* 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。

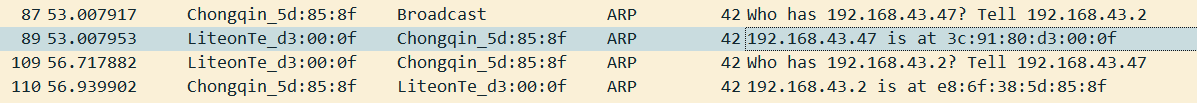
从上面的arp缓存表可以知道，对方主机的mac缓存是动态映射，是不会一直存在本机的arp缓存表上，一般来说，如果5分钟主机间没有任何通信，对方的mac地址在本机的缓存记录就会失效并且删除。

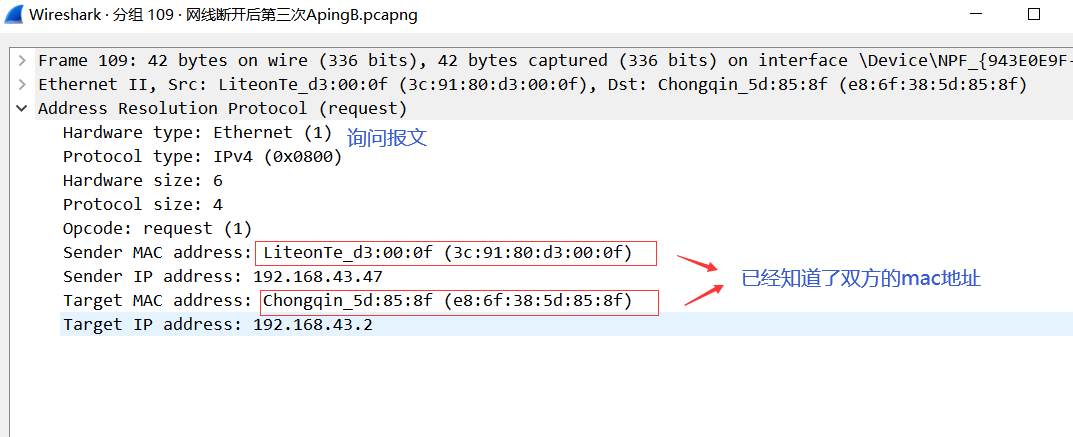
所以断开五分钟后，A ping B时，A的缓存表没有B的mac地址，需要再一次在局域网里发布广播ARP报文去询问B的mac地址，如下图，能捕获到arp广播报文（黑色记号标记的数据包）：



* **思考，关于特殊ARP协议包的疑惑和分析？**

在实验的过程中看到了很多奇怪的arp单播报文，例如：





87-89已经知道了通过arp广播报文知道了192.168.43.47的mac地址，为什么109-110还需要发送一条单播报文给192.168.43.47，要求它再返回它的mac地址呢？

通过查阅资料得到了答案：在RFC1122 中定义了四种用于刷新 ARP 缓存条目的机制，其中的第二种 Unicast Poll （单播轮询）就是定时向 ARP 缓存条目中的主机发送点到点（单播）的 ARP 请求报文，假如在 N 次连续超时时间过后，都没有收到对应主机的 ARP响应报文，则将此条目从 ARP 缓存中删除。

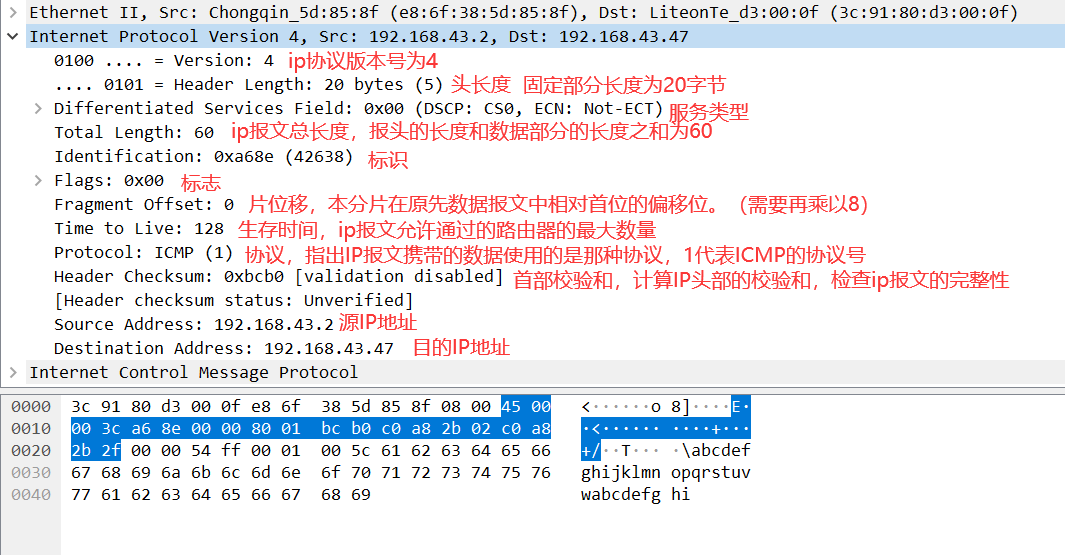
广播ARP和单播ARP是相辅相成的。当一个主机第一次想去获取同一网络中某个设备的MAC地址，由于此时主机不知道设备的MAC地址，所以只能广播ARP请求，以便于这个ARP请求能被设备收到；当第一个过程走完之后（其实就是主机收到了设备的ARP应答），双方都知道对方的IP--MAC映射，也会在自己的ARP表中生成这个映射；由于ARP老化机制第二种--单播轮询，主机会定期向设备发送点到点的单播ARP请求报文，用来确认对方是否存在，确认这条ARP缓存是该更新（主要是更新老化定时器）还是删除，同时，使用单播还可以减少网络中的ARP报文数量，所以说，一系列的单播报文就是为了确认IP--MAC映射是否还有效,以保证ARP缓冲表的实时性和有效性。

4、IP协议分析

实验过程：

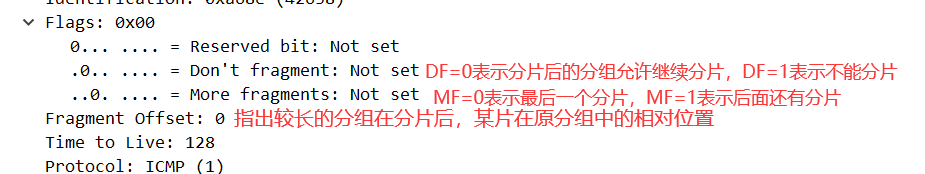
* 从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较;

选择A ping B时的一份ICMP报文中的ip数据包分许如下图：



可以看到，这份IP数据包是没有选项部分的，总长度为60字节，20字节为报文头部长度，40字节为数据部分的长度

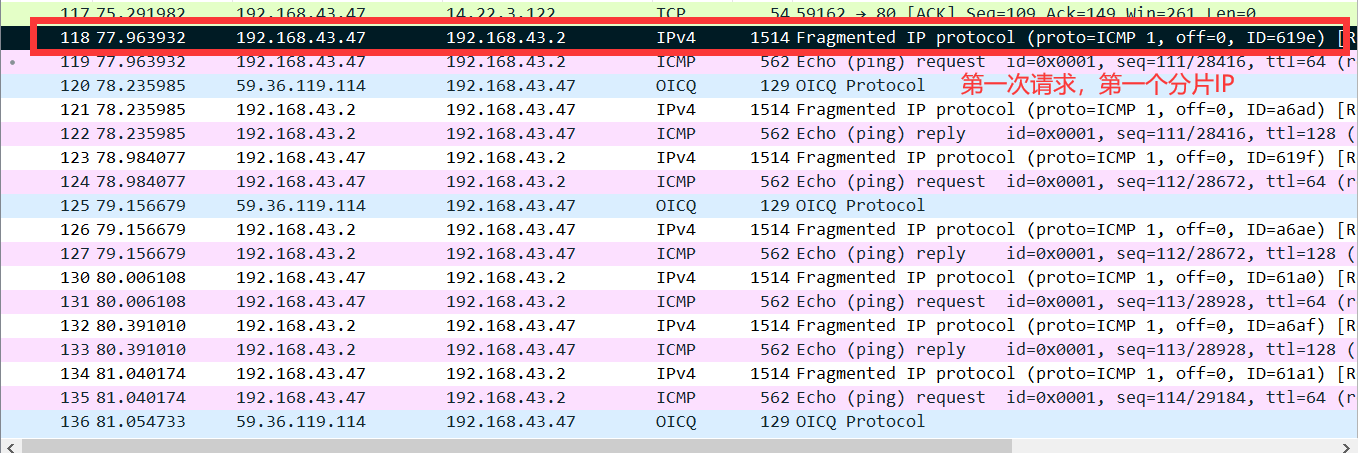
对标志位详细分析：

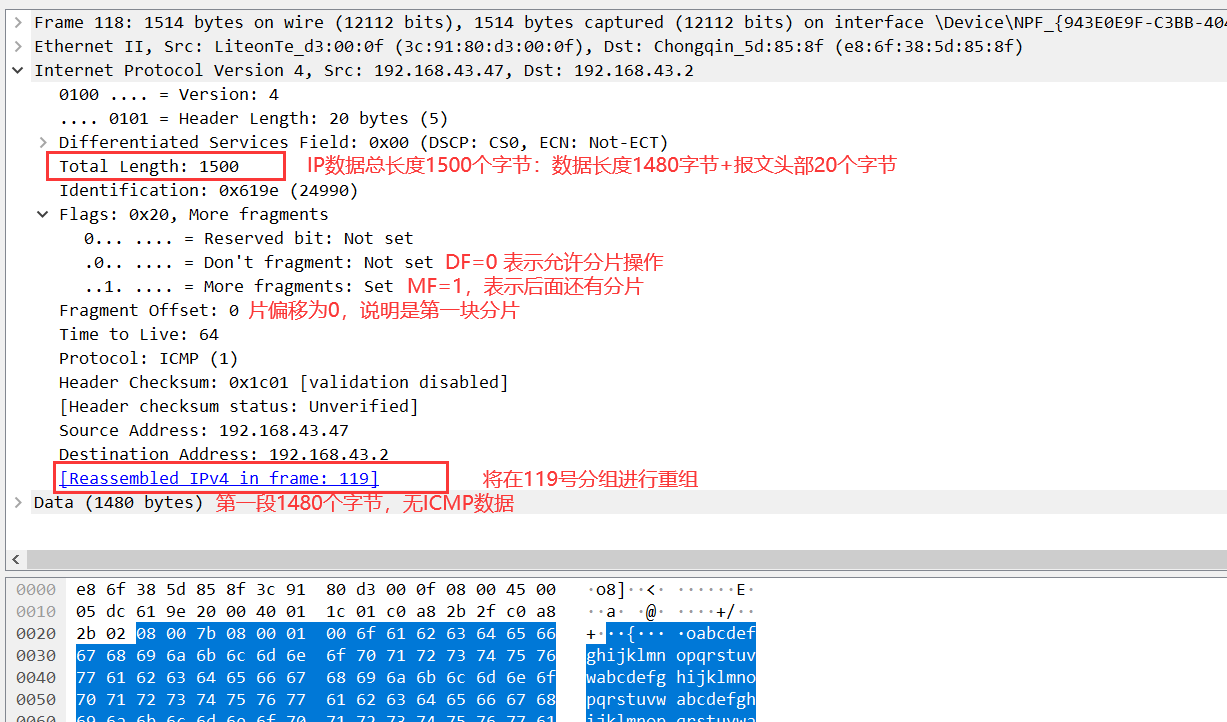


可见，此份ip数据报是允许分片的，他的后面没有分片，它的片偏移是0，说明这份IP数据包并没有超过MTU，没有被分片

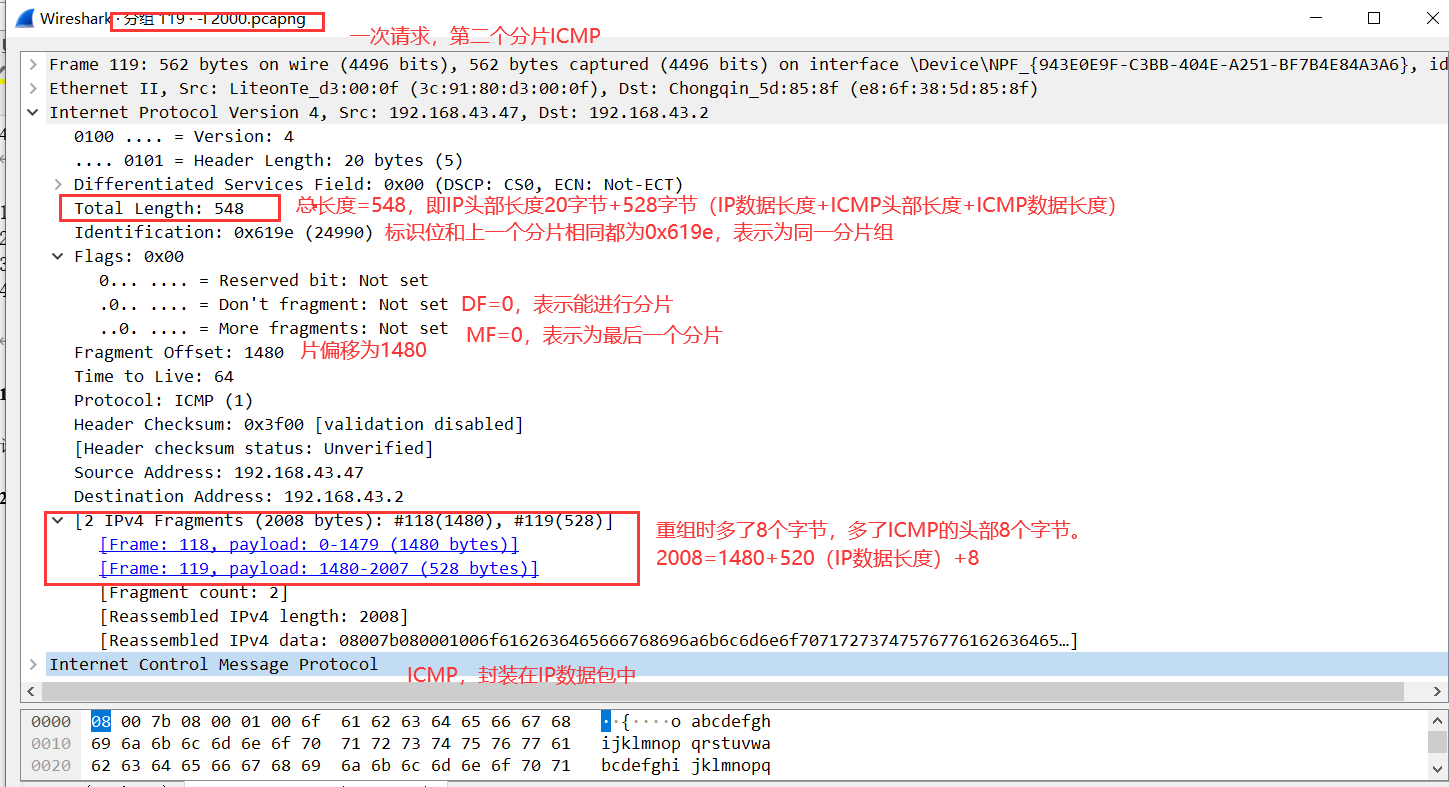
* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析**分片和重组**过程。

如下图，分析第一次请求，第一个分片IP：





分析第二个分片重组：



分析如上所示，第二块分片片偏移为1480，总长度为548字节。可以观察到接下来的8个ICMP的数据包都是进行了同样的分片操作对IP数据包进行分片以及重组。

1. ICMP协议分析

通过ping和tracet命令，了解ICMP协议的使用。

了解ICMP：

1. ICMP允许主机或路由报告差错情况和提供有关异常情况。ICMP是因特网的标准协议，但ICMP不是高层协议，而是IP层的协议。通常ICMP报文被IP层或更高层协议（TCP或UDP）使用。一些ICMP报文把差错报文返回给用户进程。

2. ICMP报文作为IP层数据报的数据，加上数据报的首部，组成数据报发送出去。

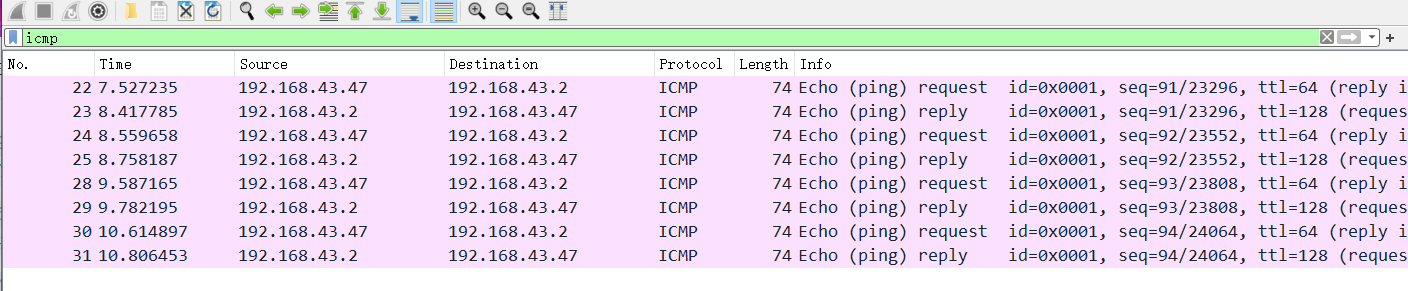
3. ICMP报文的种类有两种，即ICMP差错报告报文和ICMP询问报文。

4. ICMP报文的前4个字节是统一的格式，共有三个字段：即类型，代码和检验和。8位类型和8位代码字段一起决定了ICMP报文的类型。

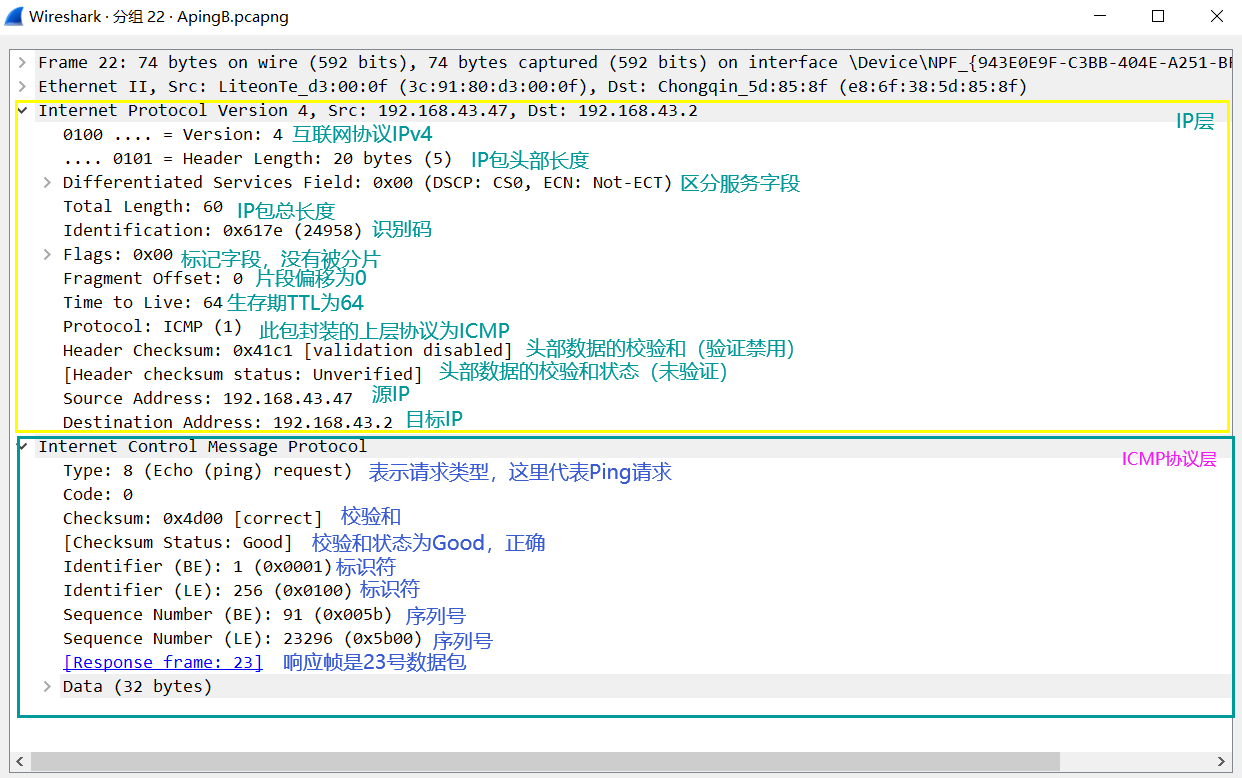
实验过程：

* 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。

ApingB成功ping通，截获ICMP数据包如下:

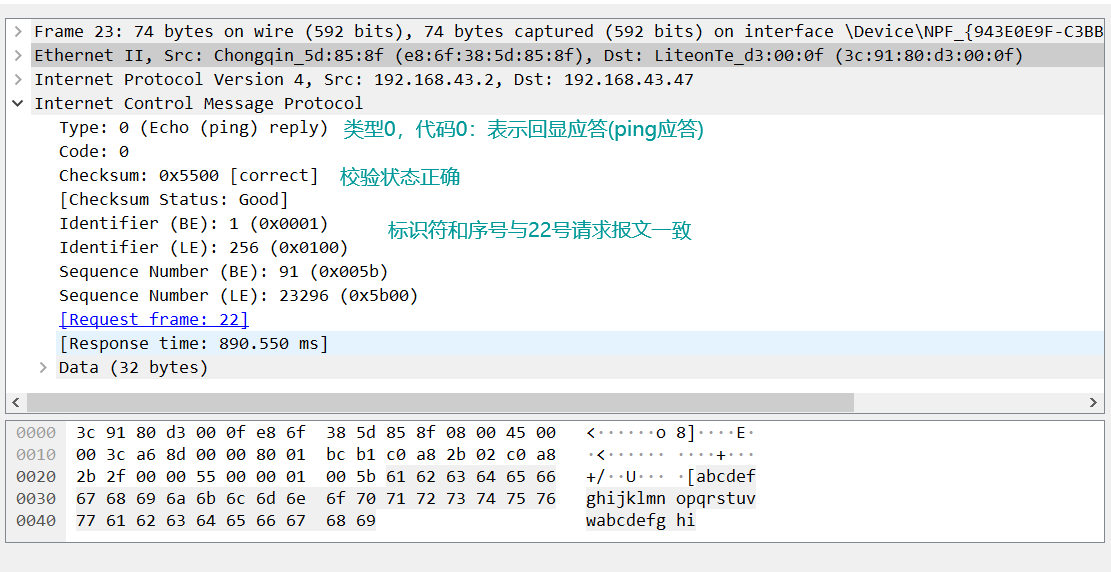


其中22-23为一对请求响应的ICMP数据包，ping程序中的ICMP包都是回显请求，属于ICMP两类报文格式中的询问报文。其中，分析22号数据包如下：



可以看到Type中，类型8，代码0：表示回显请求(ping请求)。Ping程序是为了测试另一台主机是否可达。该程序发送一份ICMP回显请求报文给主机，并等待返回ICMP回显应答。

接下来观察23号回应报文：

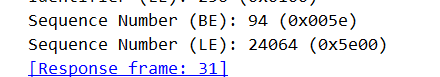


可以看到，Type值变成了0，代表ping的应答报文。“标识”和“序号”用于匹配请求与应答。，相同的标识和序号代表了对22这个请求的回答

同时还可以观察到，序列号从1开始，每发送一次新的回显请求就加1。ping程序打印出返回的每个分组的序列号，有助于允许我们查看是否有分组丢失，失序或重复。

24-25包序列号为92：

28-29包序列号为93：

30-31包序列号为94：

* + - * **思考，如果返回差错信息，是怎么体现差错信息的？**

ICMP差错报告报文共有5种

1> 终点不可达：终点不可达分为:网络不可达，主机不可达，协议不可达，端口不可达，需要分片但DF比特已置为1，以及源路由失败等六种情况，其代码字段分别置为0至5。当出现以上六种情况时就向源站发送终点不可达报文。

说明：

端口不可达：UDP的规则之一是：如果收到UDP数据报而且目的端口与某个正在使用的进程不相符，那么UDP返回一个ICMP不可达报文。

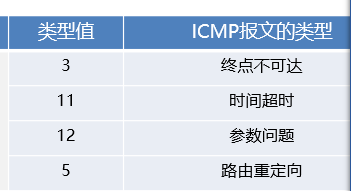
2> 源站抑制：当路由器或主机由于拥塞而丢弃数据报时，就向源站发送源站抑制报文，使源站知道应当将数据报的发送速率放慢。

3> 时间超过：当路由器收到生存时间为零的数据报时，除丢弃该数据报外，还要向源站发送时间超过报文。当目的站在预先规定的时间内不能收到一个数据报的全部数据报片时，就将已收到的数据报片都丢弃，并向源站发送时间超过报文。

4> 参数问题：当路由器或目的主机收到的数据报的首部中的字段的值不正确时，就丢弃该数据报，并向源站发送参数问题报文。

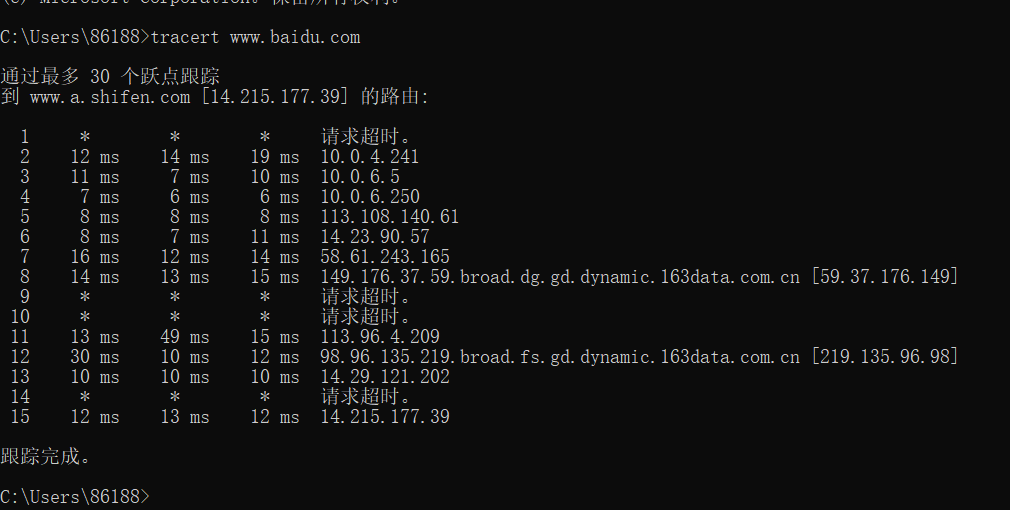
5> 改变路由（重定向）路由器将改变路由报文发送给主机，让主机知道下次应将数据报发送给另外的路由器。

差错报文报告差错的方式是通过Type类型值字段(8字节)进行报告的，常见的差错报告类型值有以下：

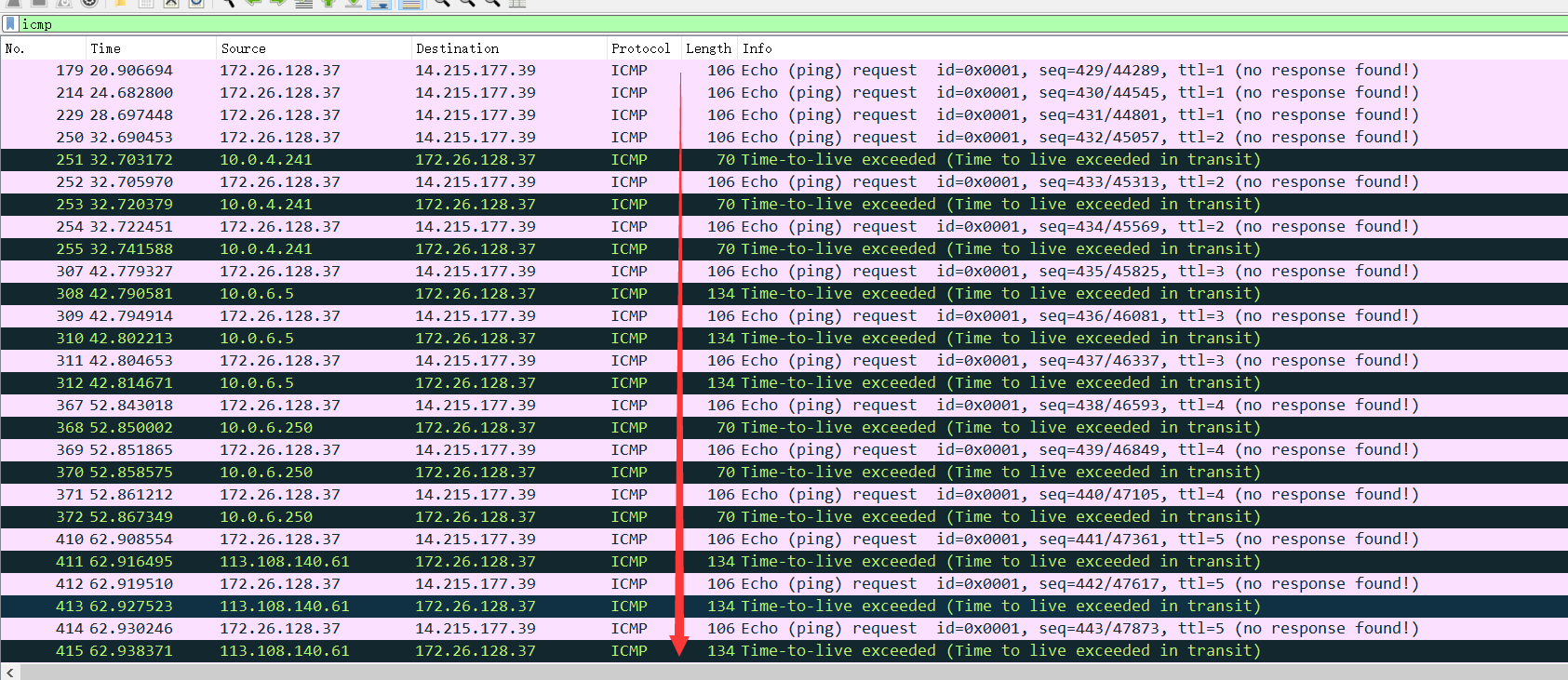


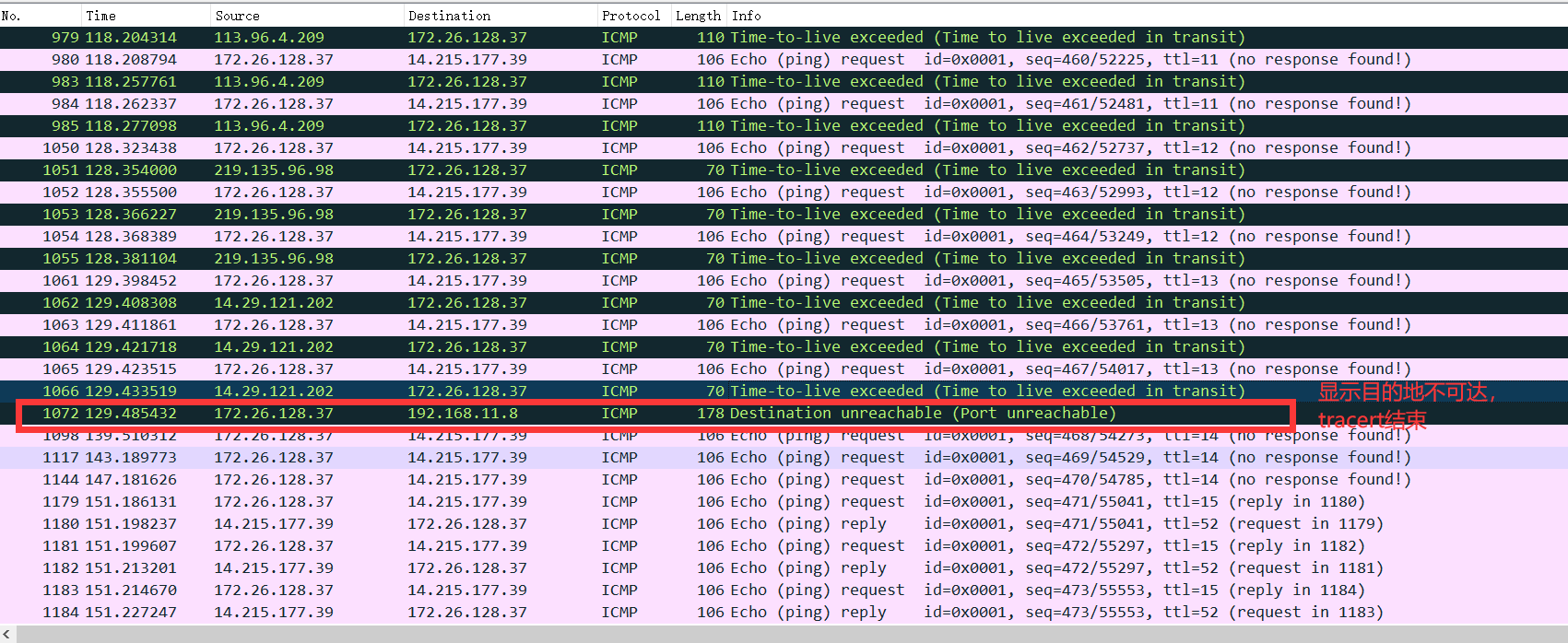
* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。

Tracert 百度网址：



截获到的ICMP报文：

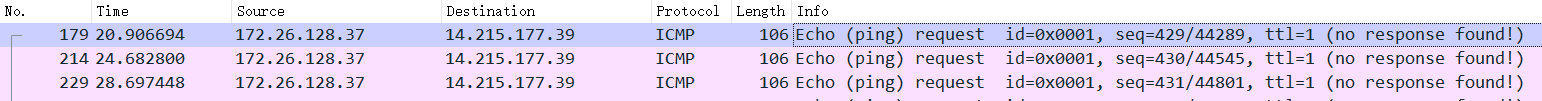


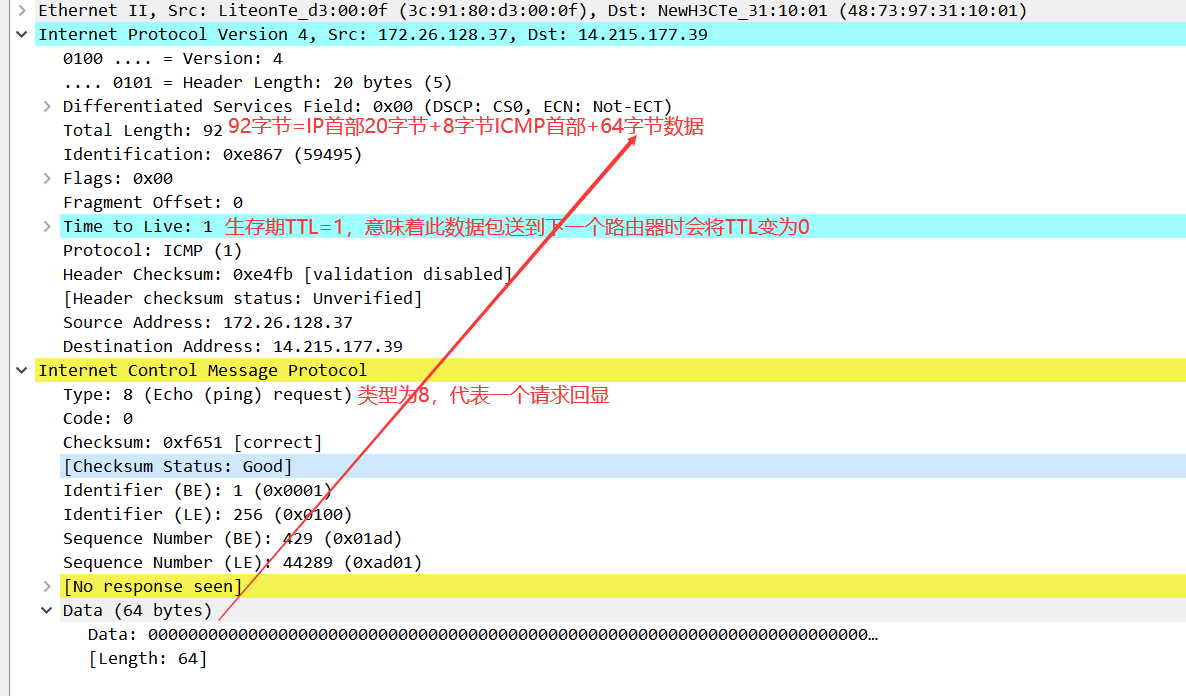


观察报文，从179号包开始跟踪路由，直到1072号包判断到达目的地，详细分析：

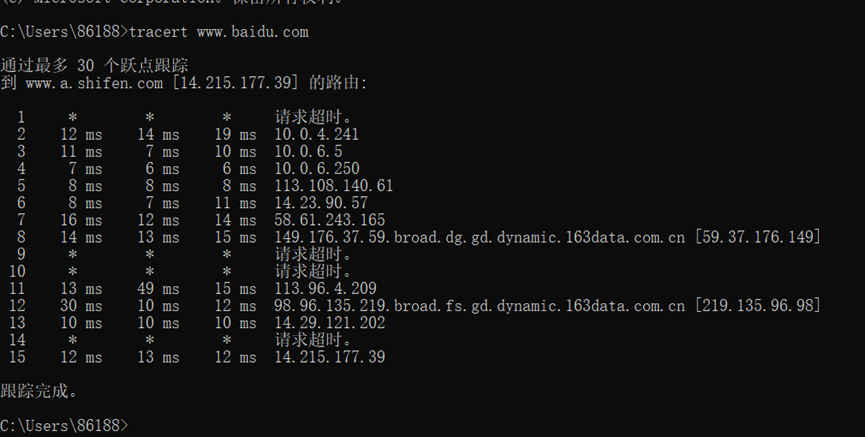
* 首先，tracert送出一个TTL是1的IP 数据包到目的地

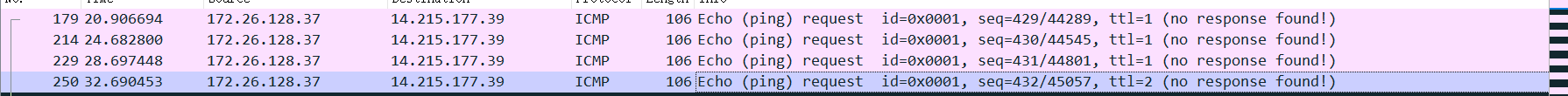
分析179号包：（type=8）





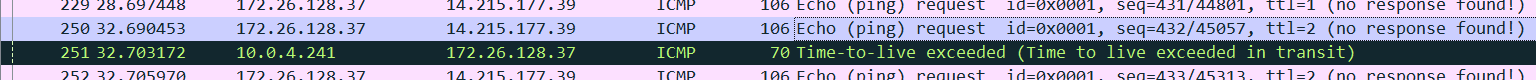
* tracert 有一个固定的时间等待响应(ICMP TTL到期消息)。如果这个时间过了，它将打印出一系列的\*号表明：在这个路径上，这个设备不能在给定的时间内发出ICMP TTL到期消息的响应。然后，Tracert给TTL记数器加1，继续进行。所以跟踪到的第一个路由设备超时，等不到回应，因此输出 \*，并且TTL+1，所以250包是ttl=2的请求回显类的ICMP报文

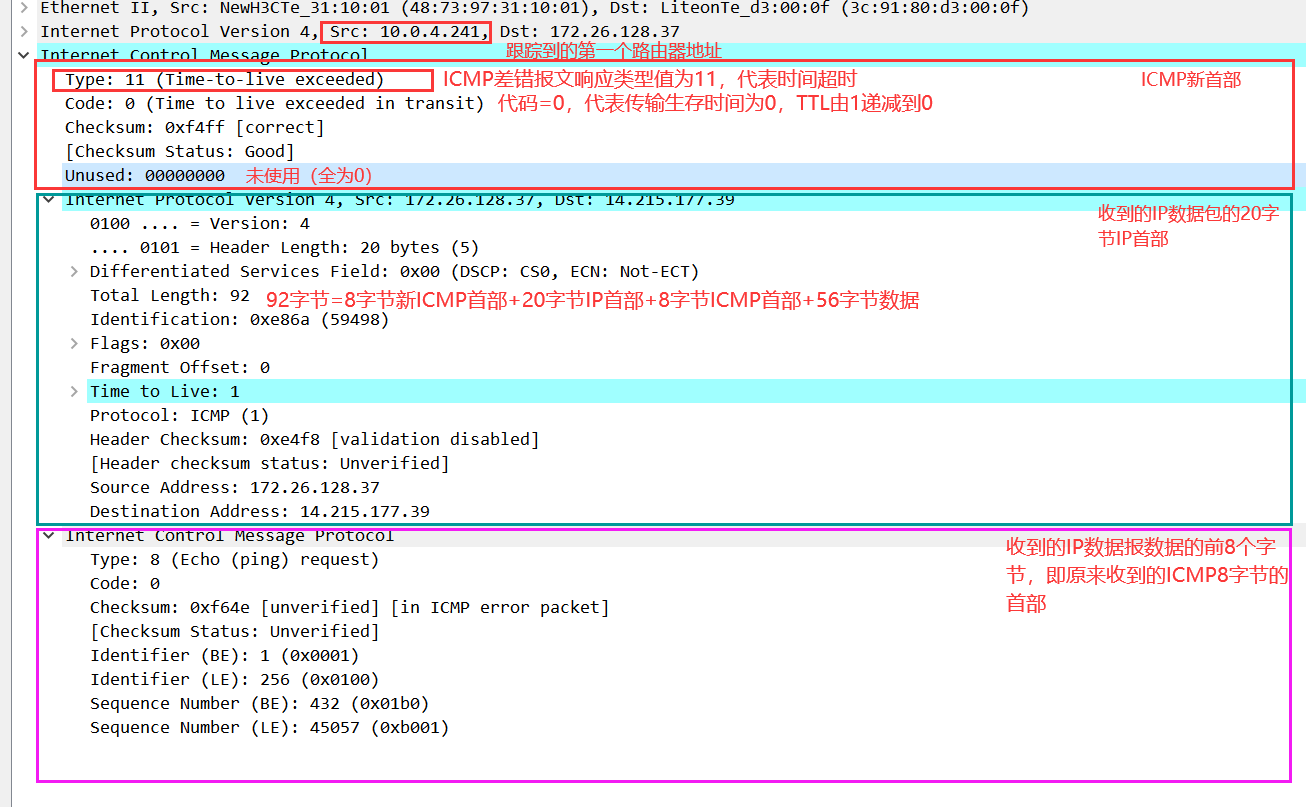




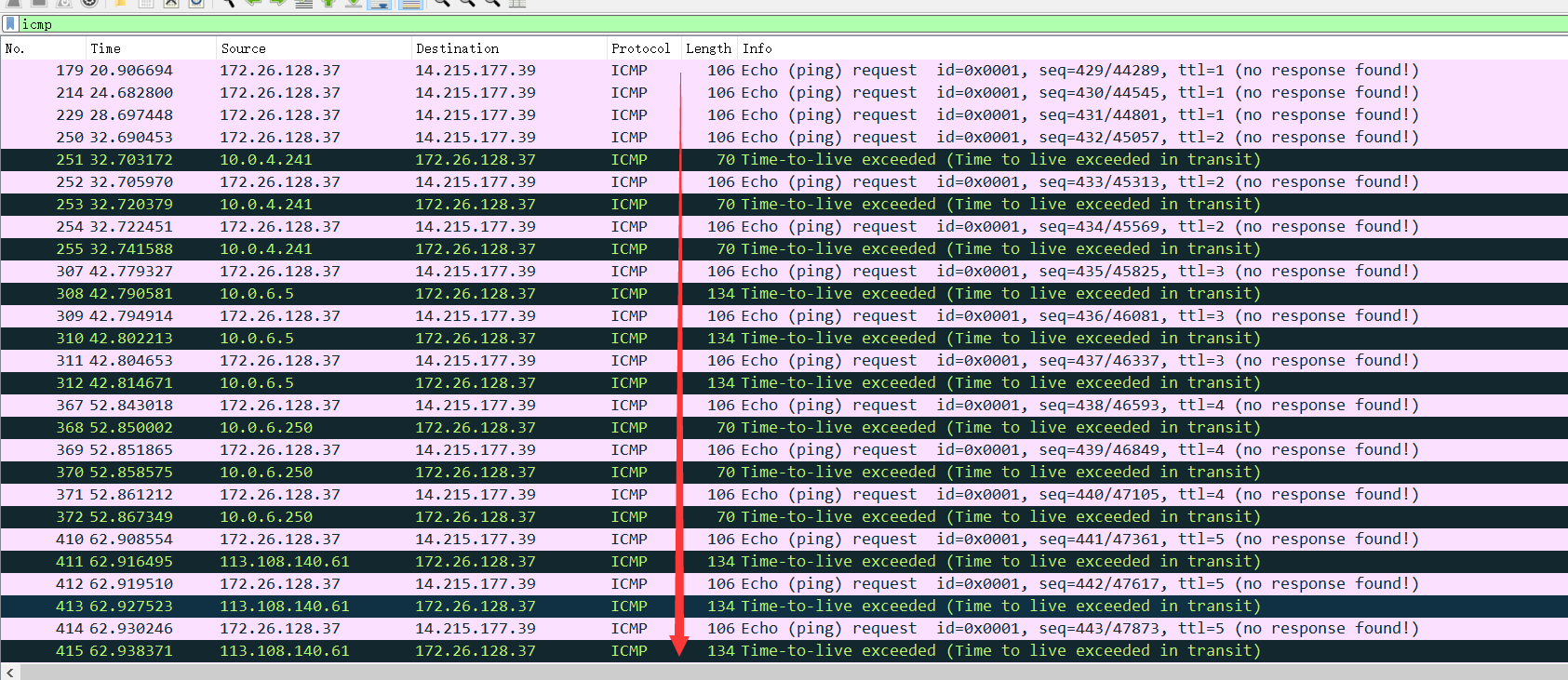
* 当路径上的第一个路由器收到这个数据包时，它将TTL减1。此时，TTL变为0，所以该路由器会将此数据包丢掉，并送回一个「ICMP time exceeded」消息（包括发IP包的源地址，IP包的所有内容及路由器的IP地址）

分析251响应报文（它是第一个响应报文）：（type=11）

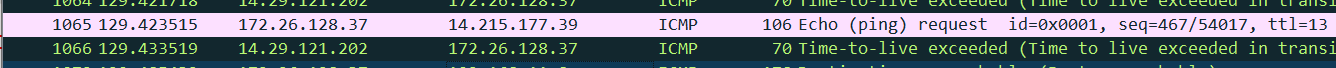




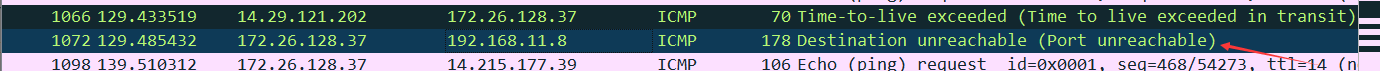
* tracert 收到251数据包的「ICMP time exceeded」这个消息后，便知道这个路由器存在于这个路径上，接着tracert 再送出另一个TTL是2 的数据包，发现第2 个路由器...... tracert 每次将送出的数据包的TTL 不断加1来发现另一个路由器，，在第二跳返回TTL超时，这个重复的动作一直持续到某个数据包 抵达目的地。



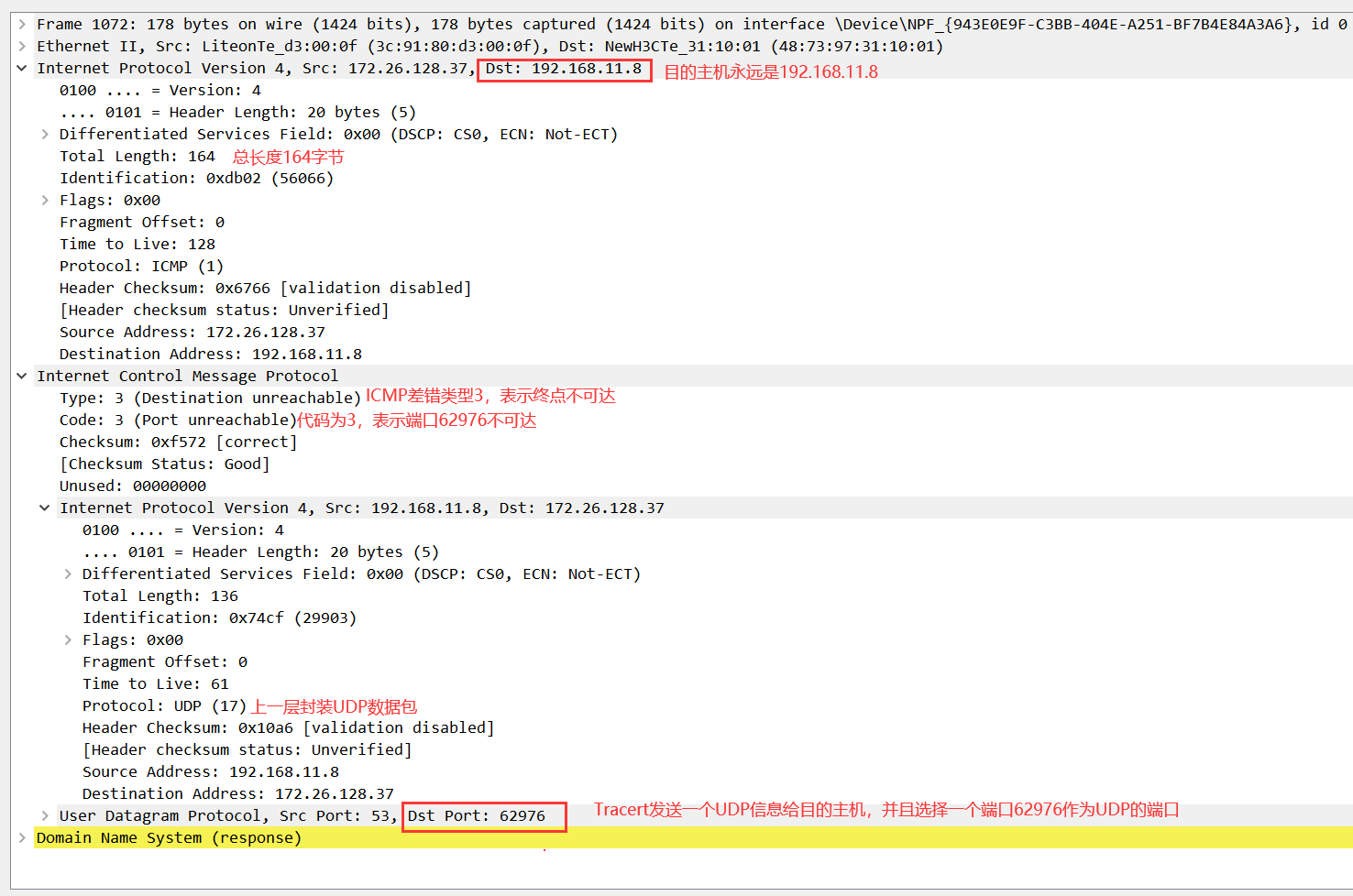
可以看到TTL不断加一并且不断收到「ICMP time exceeded」响应报文，如此重复，直到1065包发送了一个TTL=13的数据包后收到了「ICMP port unreachable」消息



* 数据包到达目的地后，该主机则不会送回ICMP time exceeded消息，一旦到达目的地，由于tracert通过UDP数据包向不常见端口(30000以上)发送数据包，因此会收到「ICMP port unreachable」消息，故可判断到达目的地。



对应报文1072号：



可以看到，此时到达了目的主机，但是计算机并不能知道，于是，Tracert还同时发送一个UDP信息给目的主机，并且选择一个很大的值作为UDP的端口，使主机的任何一个应用程序都不使用这个端口。（这里选择了端口号62976作为UDP端口），因此， UDP模块就产生一个“端口不可到达”的错误，这时就能判断到达目的地了，tracert跟踪结束。

* **思考，如何总结tracert跟踪流程：**

1. 首先发送一个TTL为1的UDP报文，当到达第一个路由器时TTL减1变为0，路由器就不再转发这个数据了，而直接丢弃，并且发送一个ICMP“超时”信息给源主机，并告知自己的IP地址；

2. 之后再发送一个TTL为2的报文，在第二跳返回TTL超时，这个过程不断进行，直至到达目的地；

3. 在目的地，由于数据报中使用了无效的端口号（缺省为33434），目的主机会返回一个ICMP目的地不可达消息，该tracert操作结束。

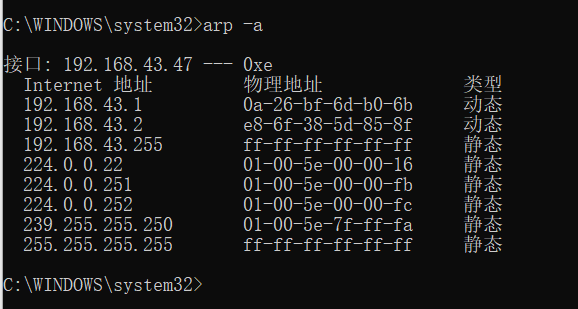
在上述过程中，tracert记录下每一个ICMP TTL超时消息的源地址，从而获得报文到达目的地所经过的网关的IP地址。

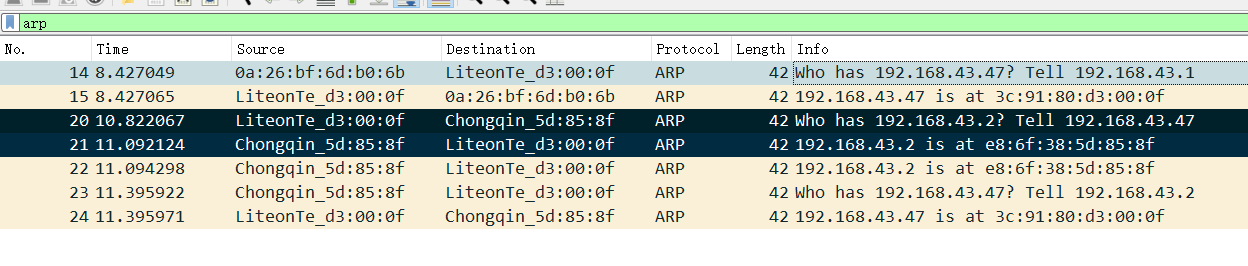
**5.【思考题】（分析原因并通过实验验证）**

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？

答：如果主机的ARP高速缓存里存有目标主机的IP以及其对应的mac地址，那么与目标主机通信的时候会先在本机的arp高速缓存中找到对应的mac地址后，就不需要arp广播报文，不需要在局域网中广播查找目标主机的mac。所以说A有时能捕获ARP报文，有时不能捕获到。

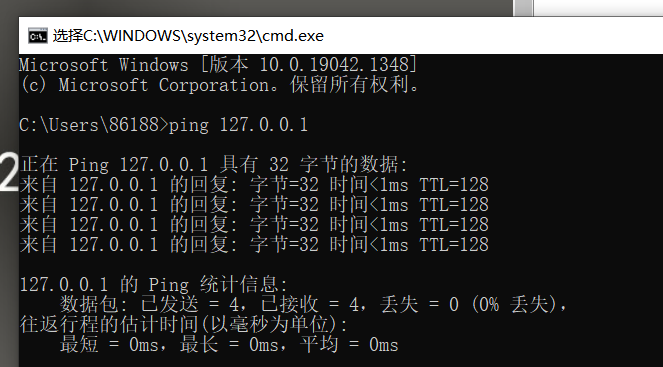
例如：查看本机的arp表，存在主机192.168.43.2的mac地址，此时再ping，捕获不到arp的广播报文了



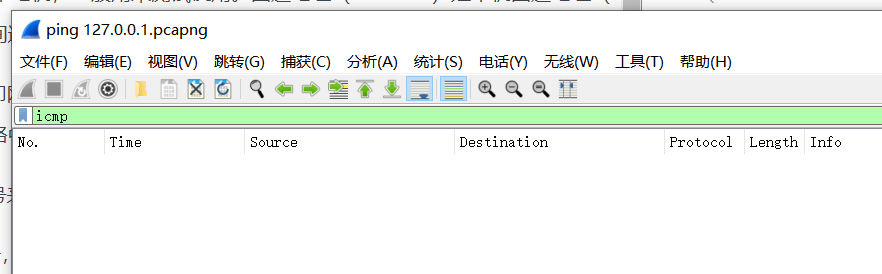


2、为什么运行ping 127.0.0.1时，不能捕获到ICMP报文？如果运行ping 本机IP地址能收到报文吗？ 为什么？

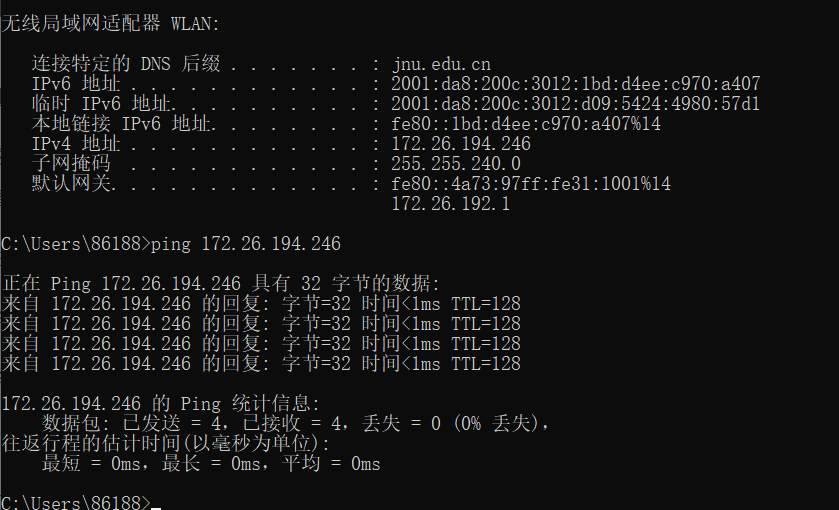
答：ping127.0.0.1 并用wireshark捕获如下：



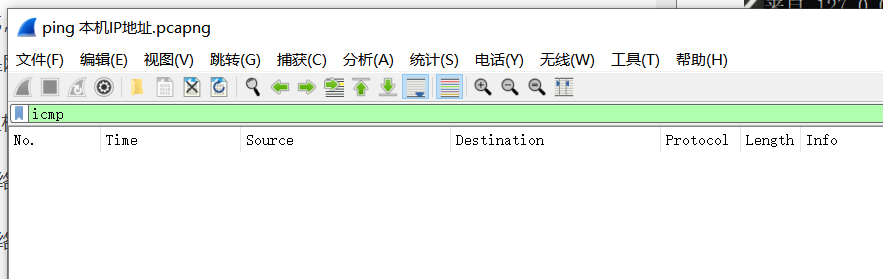
Ping127.0.0.1捕获不到ICMP报文：



Ping本机IP：



用wireshark捕获报文，发现也无法捕获到ICMP报文：



分析：

ping 127.0.0.1：127.0.0.1是回送地址，指本地机，一般用来测试使用。回送地址（127.x.x.x）是本机回送地址（Loopback Address），即主机IP堆栈内部的IP地址，主要用于网络软件测试以及本地机进程间通信，无论什么程序，一旦使用回送地址发送数据，协议软件立即返回，不进行任何网络传输。

也就是说，ping127.0.0.1这条命令是不经过网卡的，ping本地回环是测试tcp/ip协议栈，在协议栈的IP层就进行了回环，所以是捕获不到ICMP报文的。它能ping通，同时说明了我的TCP/IP协议栈没问题

Ping 本机地址：ping本地IP地址时，数据报从网卡协议的最顶层（应用层）接收数据，然后到传输层，其次是IP层，当数据报达到IP层的时候，IP层检测到数据包的目的主机本机，那么就会将数据包送回环回接口，然后送回本机。以上的几个层次，都成一个IP协议栈（自上往下），ping本机就可以测试IP协议栈（网卡协议）是否正常。

和ping127.0.0.1类似，数据报最后在IP栈回环，因此是不能捕获到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？

答：

Request timed out(包从主机出去了)：主要是主机路由表中具有到达目标的路由，且arp广播，最终有找到arp到达路由的下一跳mac地址，而因为其他中间原因不可到达或者目标设置防火墙等原因没有回应，这时候会出现超时。例如：ping 不同网段并不存在的主机

Destination host Unreachable (包无法从主机出去)：主要是路由表中具有到达目标的路由，且arp广播，最终没有找到arp到达路由的下一跳mac地址，则会出现目标不可达。例如：ping 相同网段并不存在的主机

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。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。

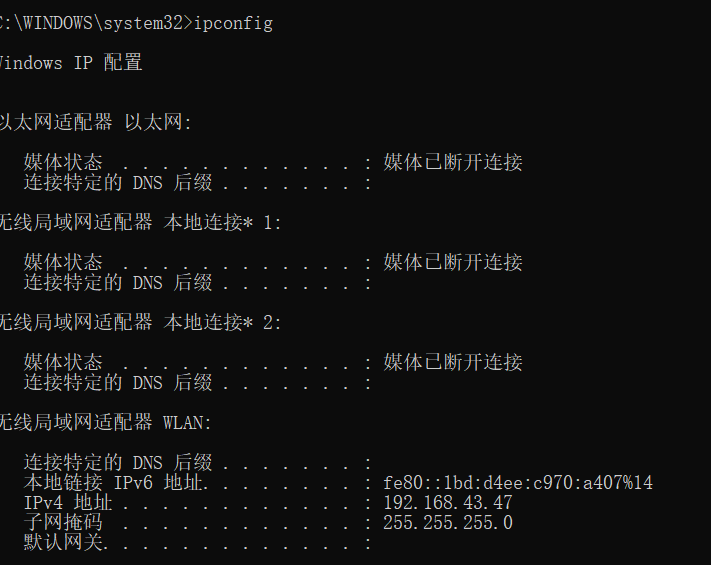
主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

答：

实验过程：

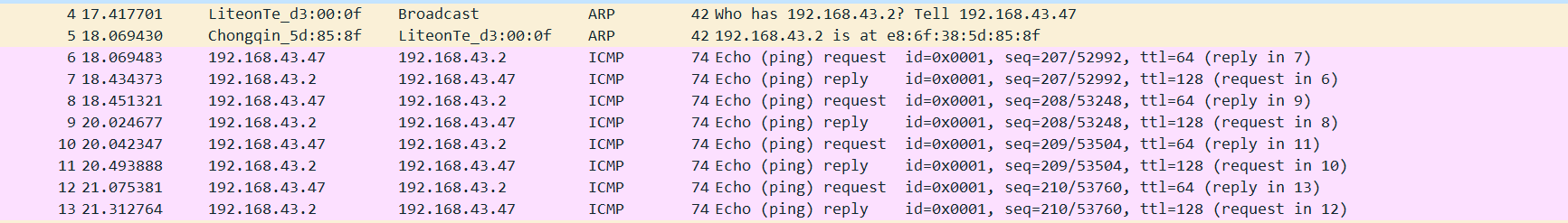
* 将两台主机连接到同一个数据热点，实现两台主机处于同一网段中
* 不设置“网关”，同一网段内的主机可以相互通信

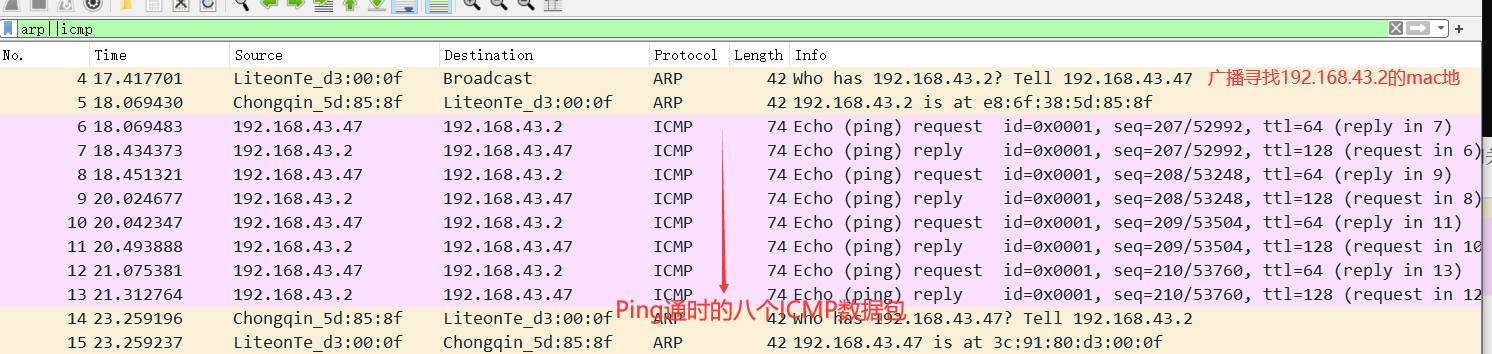
主机A不设置网关：



主机B不设置网关，IP地址为：192.168.43.2，子网掩码：255.255.255.0 默认网关：无

ApingB，可以ping通，捕获8个ICMP数据包，2个ARP数据包如下：





通过上面的报文，其中5号数据包是主机B的arp响应报文，里面包含了B的mac地址。

通过观察可以发现，主机A和B处于同一个局域网中，所以，A的广播报文在局域网内发布并且是可以得到B的回应的，是不需要去询问默认网关的mac地址，所以A和B自然可以ping通

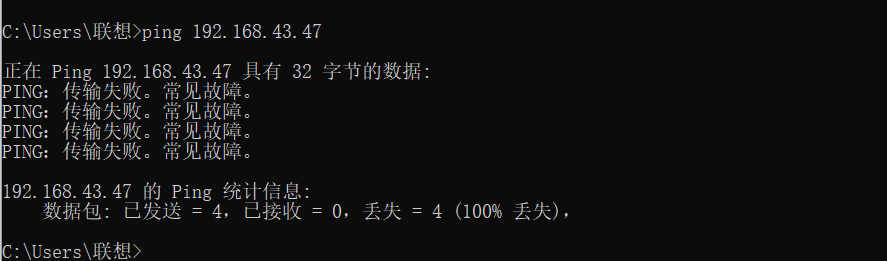
* 不设置“网关”，不同网段内的主机不可以相互通信

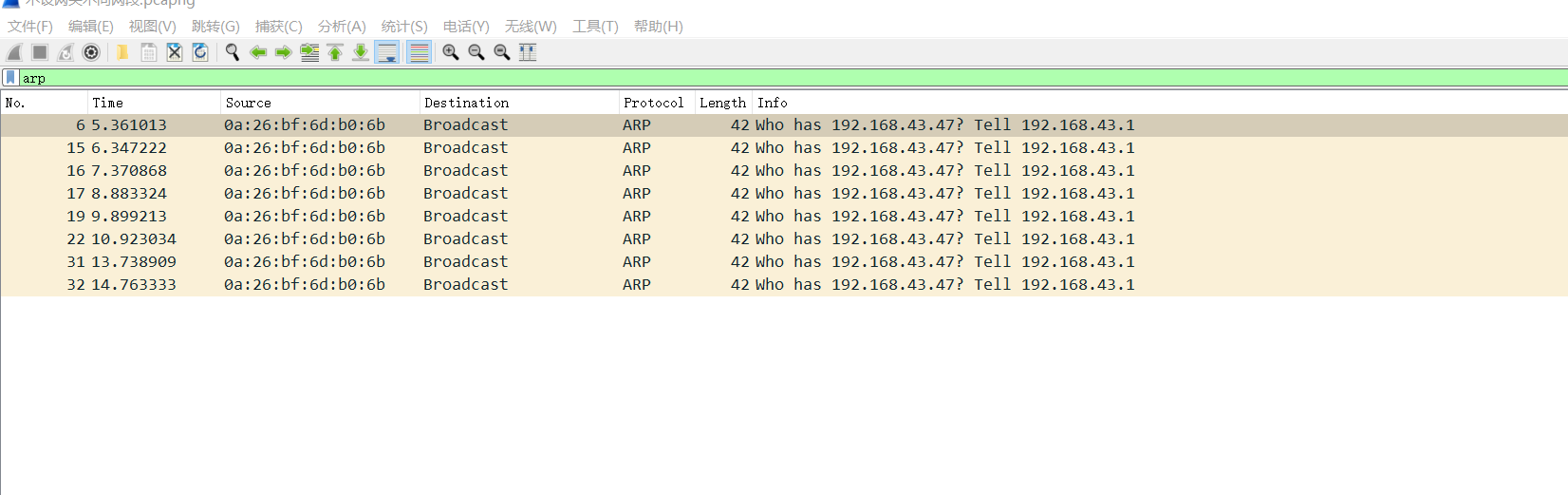
主机A配置不变，修改主机B的IP地址，其他不变：



此时主机B的子网掩码与IP地址与运算得到B的网络号是192.168.28，而主机A还在原来的网络号192.168.43的网段中，不同局域网内的主机痛信是要经过网关转发的。由于两个网段没有设置默认网关所以主机A和B是无法通信的，如下图：

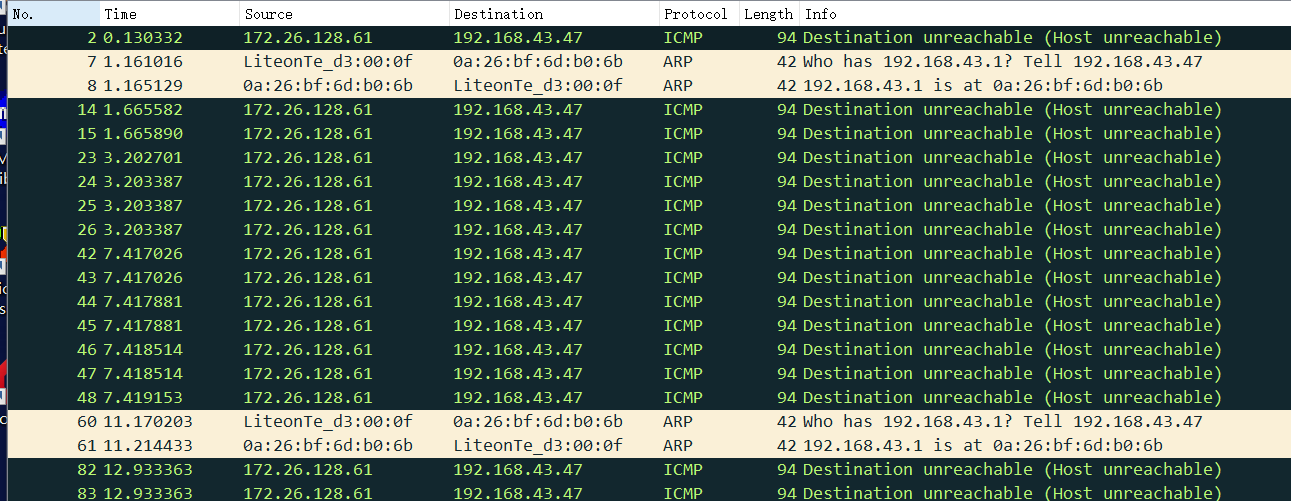
BpingA：





观察报文，主机B在自己的局域网里发布了8条广播ARP询问报文询问A的mac地址，由于B不再A的子网中，所以他收不到广播报文，所以A的广播报文没有主机响应。得不到B的mac地址，所以ping不同

ApingB也是同理，只有ARP广播报文：

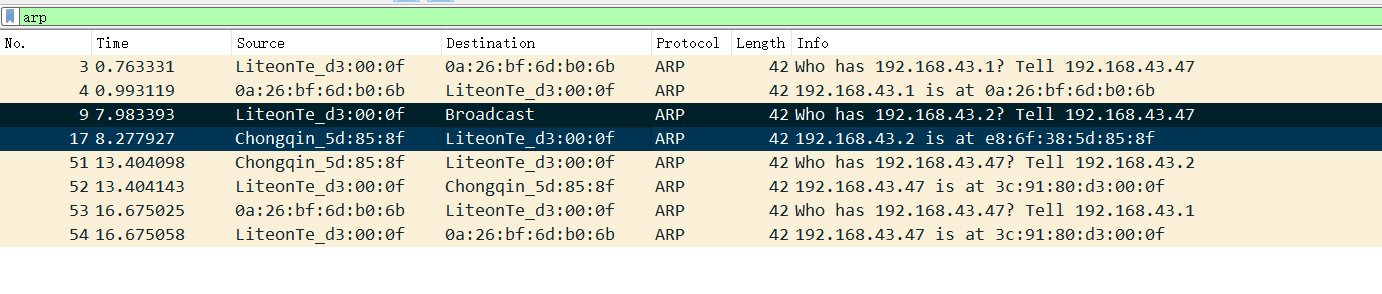


* 设置“网关”，同一网段的主机通信

主机A ip：192.168.43.47 子网掩码：255.255.255.0 默认网关：192.168.43.1

主机B IP：192.168.43.2 子网掩码：255.255.255.0 默认网关：192.168.43.1

ApingB，很明显，A和B就在一个局域网里面，可以ping通，捕获报文如下：

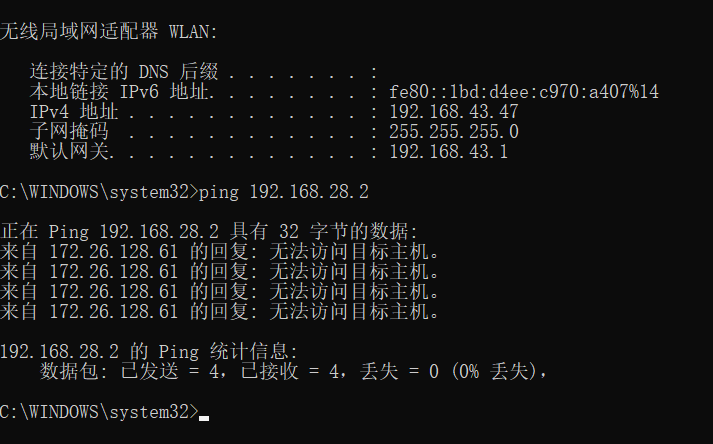


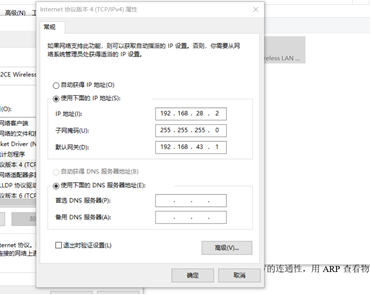
可以看到，嗅探器捕获到ARP的广播报文以及响应报文（9和17号数据包），能看到对方主机B的MAC地址

* 设置网关后，不同网段的主机之间通信需要网关转发

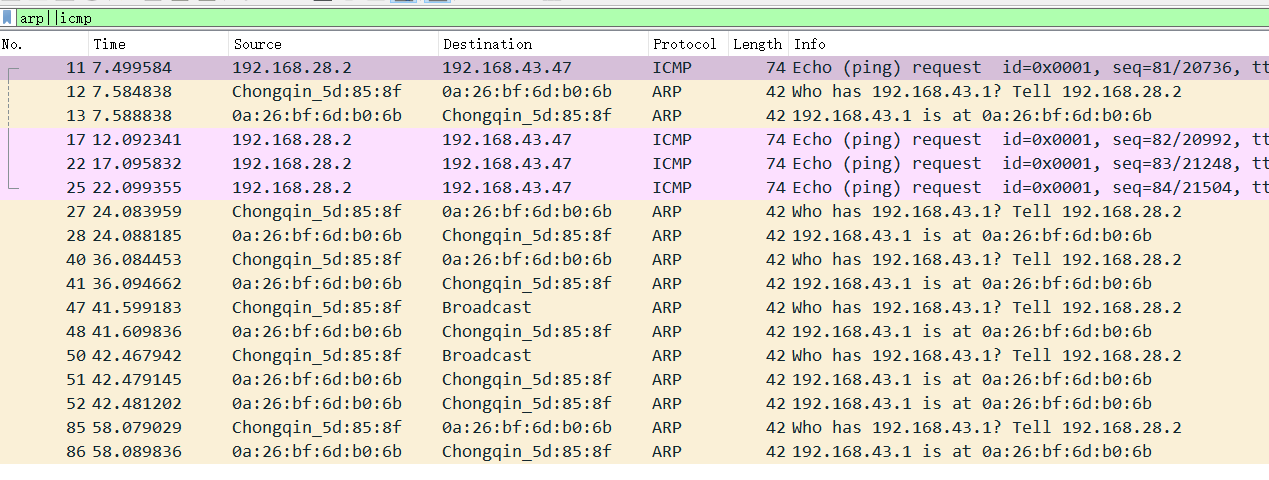
主机A ip：192.168.43.47 子网掩码：255.255.255.0 默认网关：192.168.43.1

主机B IP：192.168.28.2 子网掩码：255.255.255.0 默认网关：192.168.43.1





BpingA：虽然通过B和A不在同一个网段中，但是由于B和A都有自己的默认网关，BpingA的时候会向自己的默认网关询问A的地址，再由网关转发，这样B就会得到A的mac地址，所以他们可以ping通。捕获的wireshark截图如下：



我们可以从arp里看到发给自己默认网关的arp广播/单播报文，可以看到本机的mac地址和网关的mac地址（ARP广播获知网关的MAC），捕获不到目的主机的mac地址（因为是由网关封装转发并回复的）。

* 思考，所以网关是什么？它的作用是什么？那默认网关和其他网关又是什么呢？

通过实验可以看到，网关实质上是一个网络通向其他网络的IP地址。

在没有路由器的情况下，两个网络之间是不能进行TCP/IP通信的，即使是两个网络连接在同一台交换机(或集线器)上，TCP/IP协议也会根据子网掩码判定两个网络中的主机处在不同的网络里。而要实现这两个网络之间的通信，则必须通过网关。如果网络A中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络B的网关，网络B的网关再转发给网络B的某个主机。所以说，只有设置好网关的IP地址，TCP/IP协议才能实现不同网络之间的相互通信。网关的IP地址是具有路由功能的设备的IP地址，具有路由功能的设备有路由器、启用了路由协议的服务器(实质上相当于一台路由器)、代理服务器(也相当于一台路由器)。

什么是默认网关？一台主机可以有多个网关，默认网关的意思是一台主机如果找不到可用的网关，就把数据包发给默认指定的网关，由这个网关来处理数据包。现在主机使用的网关，一般指的是默认网关。如图是实验中的193.168.43.1就是一个具有路由功能的IP地址，即为默认网关。

因此，只有设置了网关，不同网段的主机才可以通信

* 思考，设置网关时不同网段的主机通信的完整流程是怎样的呢？为什么可以看到本机的mac地址和网关的mac地址却捕获不到目的主机的mac地址？

通过实验总结不同网端通信的流程如下：

1. 查找路由表。网络号不同的情况下，需要查找路由表，一旦匹配到路由条目，则把IP包发给这条路由条目的下一台跳，如果路由表前几条都没有匹配到，那么就去最后一跳万能路由，即默认网关

2. 发现网关硬件接口MAC。网关肯定是和本机属于同一网段，可以从ARP缓存中或者ARP广播获知网关的MAC。

3. 主机将ARP请求封装在以太帧中，发给默认网关。Ping包发给网关

4. 网关硬件接口接受以太网帧。

5. 网关路由转发。网关解出ARP请求的目的IP属于另一个网段，查找路由表，查找通往目的IP的下一跳IP。根据本地ARP缓存表或者ARP广播获知目的IP地址的MAC地址，然后将IP包添加以太网帧头，发送出去。

6. 发送封装了ARP应答的单播帧。目标主机收到封装了此ARP的广播帧后，剥掉帧的MAC头，取出ARP报文，从ARP报文取出目的IP，匹配自己的IP，然后发送封装了ARP应答的单播帧

7.默认网关解析局域网net\_B的单播帧，识别ARP应答，将此ARP应答封装二层MAC头，构造源主机所在局域网的单播帧并发送

8. 主机收到此ARP的单播帧后，剥掉帧的MAC头，解析ARP应答报文，从ARP报文取出目的IP，匹配自己的IP，更新本机ARP表。

至此，不同网段中的host\_A与host\_B可以通信，整个流程结束。

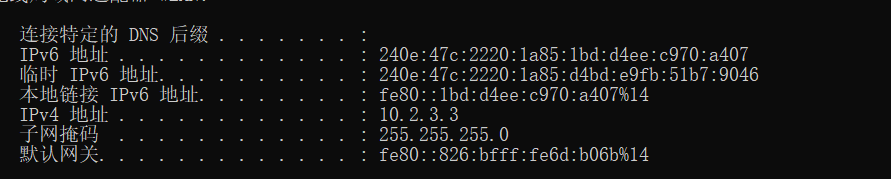
5、通过下面实验**理解网关。**

**【给的两种IP地址都在同一网段，于是将第一种设为了不同网段】**

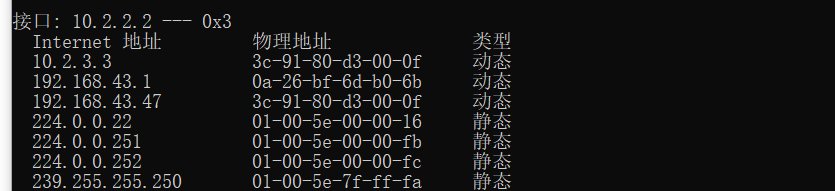
* 假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/24，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析。

实验过程

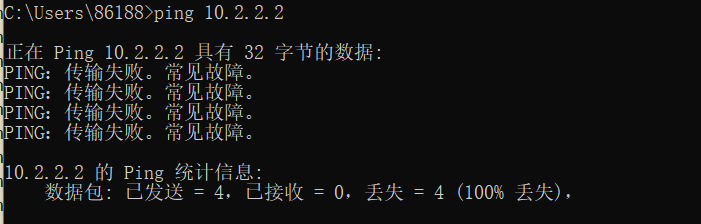
10.2.3.3/24 主机B的配置



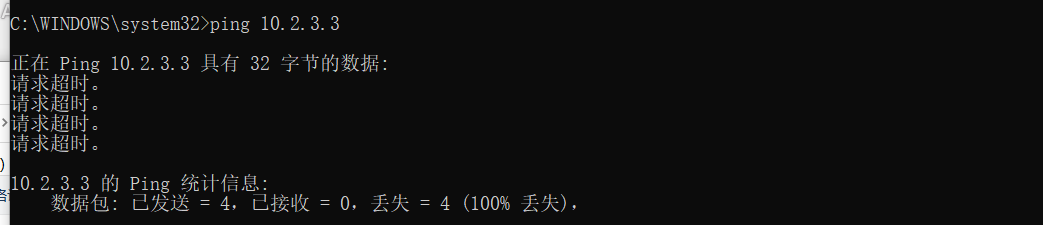
10.2.2.2/24 主机A的配置：



B ping A：



A ping B：

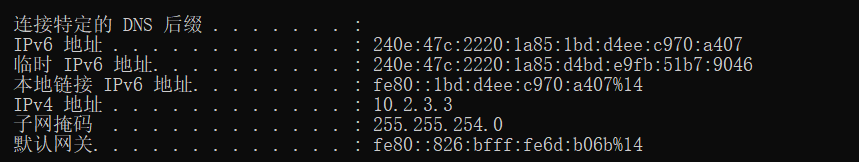


结论和分析：结果A和B无法ping通。A的网络号为10.2.2，主机B的网络号为10.2.3.3，由于没有网关，A和B又不在同一个局域网中，根据思考题4中的分析可知，AB是无法通信的，实验结果正确

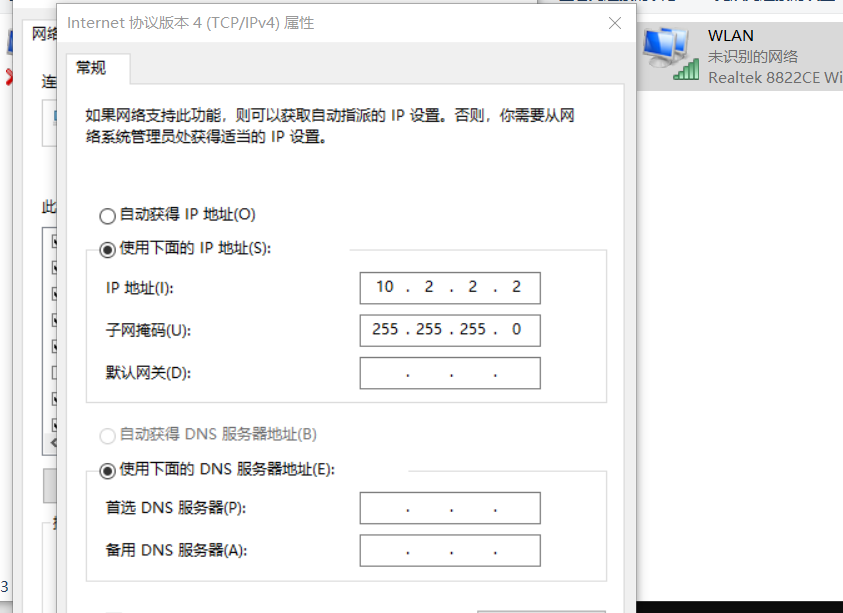
* 假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/23，两主机不设置网关，分别在主机A和主机B上用ping测试与对方的连通性，用ARP查看物理地址。对测试结果进行分析。

实验过程：

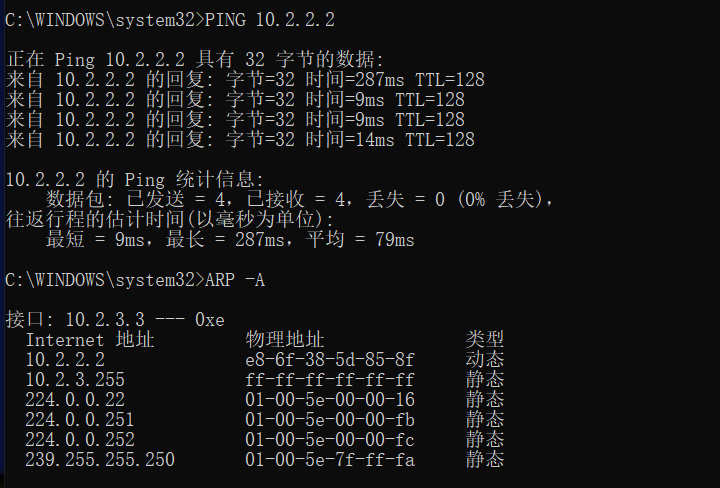
10.2.3.3 主机B的配置

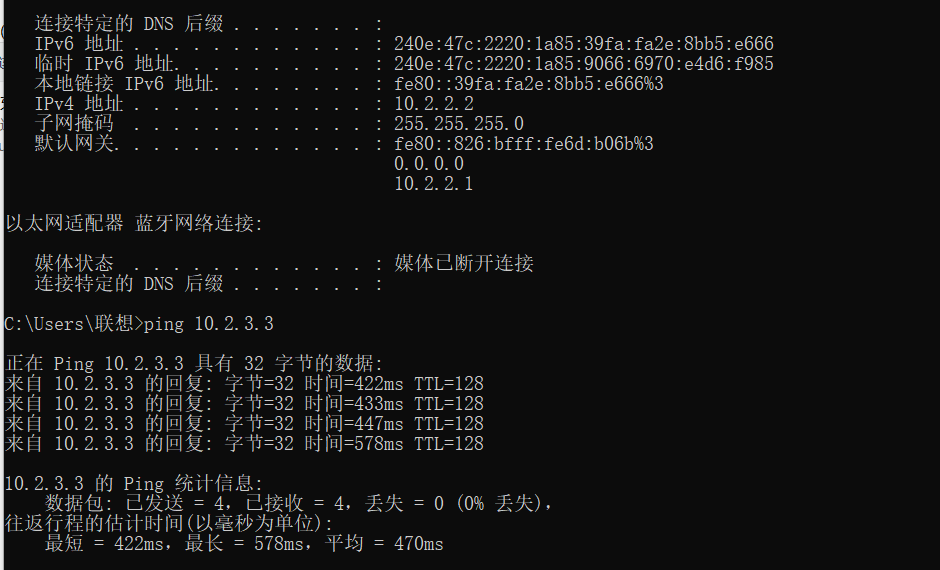


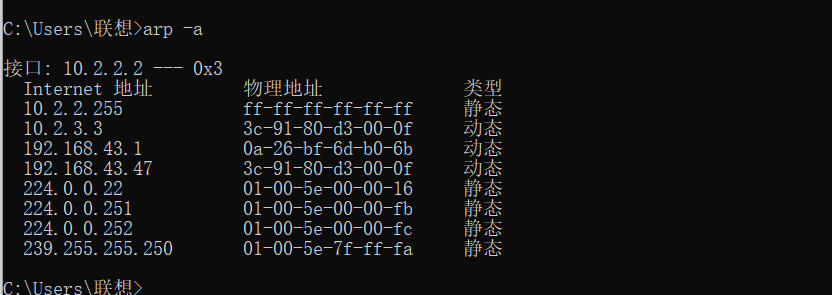
10.2.2.2 主机A的配置：

****

BpingA,可以ping通，arp -a查看，存在A的Mac地址：

 ApingB,可以ping通，arp -a查看，存在B的Mac地址：





结论和分析：A的IP地址和子网掩码相与得到A的子网掩码是10.2.2，B的IP地址和子网掩码相与得到B的子网掩码也是10.2.2，说明A和B处于同一个网段中，所以AB不需要经过网关就可以相互ping通

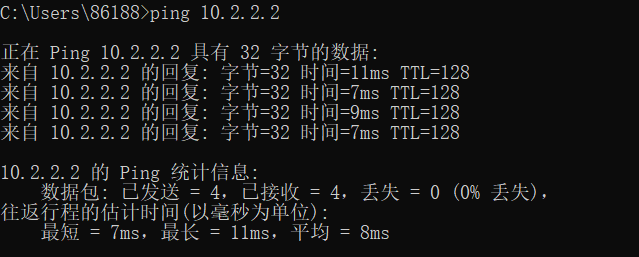
* 针对上述情况，分别将主机的网关设置为本机地址，观察测试结果，并分析原因。

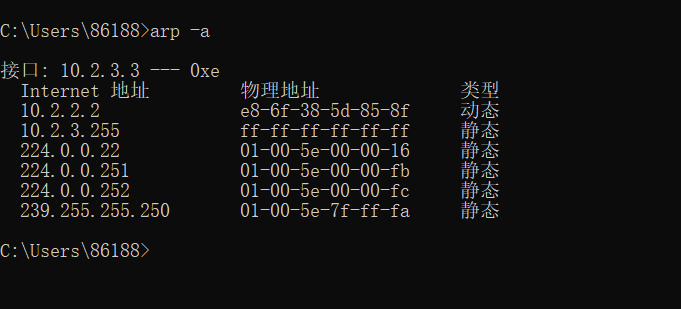
设置：

10.3.3.3 主机B的配置：10.2.3.3 网掩码：255.255.254.0 默认网关：10.2.3.1

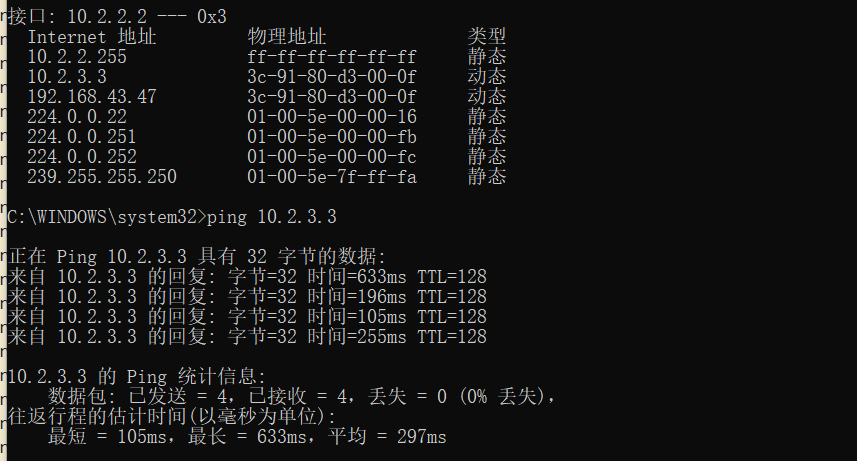
10.2.2.2 主机A：ip：10.2.2.2 子网掩码：255.255.255.0 默认网关：10.2.2.1

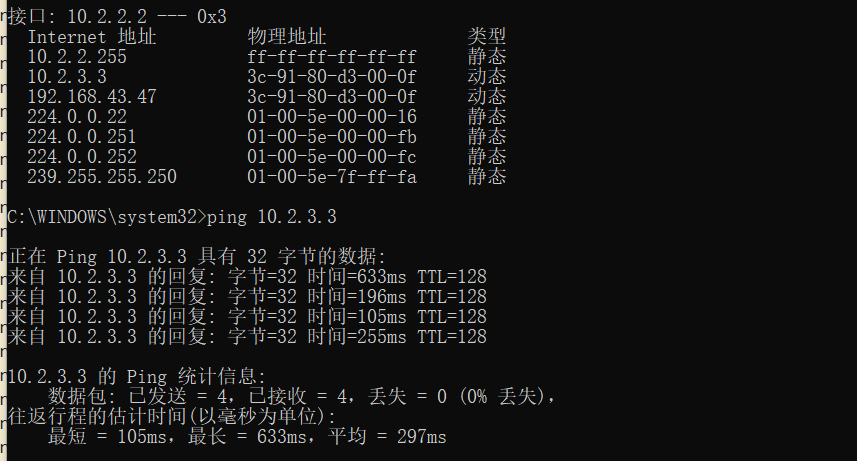
B ping A，可以ping通，查看arp -a，存在A的mac地址：





A ping B,也可以ping通，A的ARP表中也有B的地址：





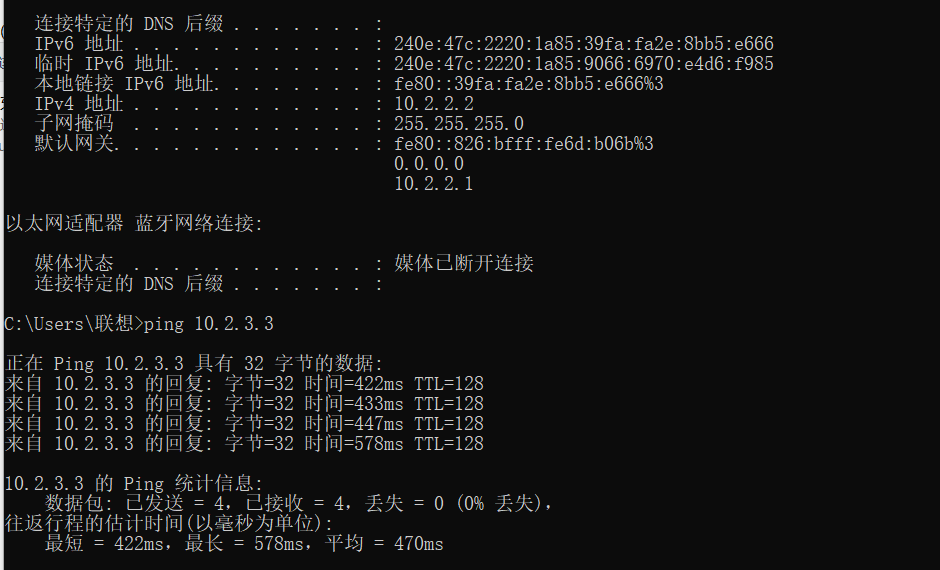
分析：A和B处于同一网段，这时默认网关没有作用，AB自然可以ping通

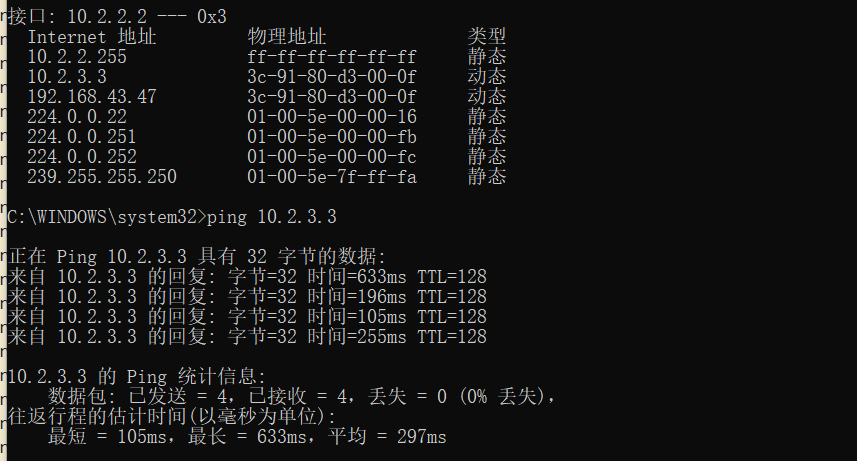
设置：

10.3.3.3 主机B的配置：10.2.3.3 网掩码：255.255.255.0 默认网关：10.2.3.1

10.2.2.2 主机A：ip：10.2.2.2 子网掩码：255.255.255.0 默认网关：10.2.2.1

结果AB仍旧可以ping通，通过ipconfig可以发现AB的默认网关都更改了，而且多了一个0.0.0.0的默认网关，产生了一个新的局域网，A的ipconfig显示如下：B的也一样





分析：不同网段设置网关，结果是ping通了。可能是因为，新建立了两个局域网10.2.2和10.3.3，分别设置了两个默认网关在两个局域网中。相互ping时10.2.2的默认网关转发请求至10.3.3，所以可以相互ping通。

对网关的详细理解请看第4题。

**6.【实验小结】**

通过本次实验，对数据链路层以太网帧的传播形式和原理有了深刻的认识。也进一步了解网络层中的IP,ARP,ICMP的作用，以及我还了解了主机和主机之间实现通信的过程。除此之外，对与什么是网关，网关是如何得到对方的mac地址最终实现通信的这个过程有了深刻的理解和体会。实验过程进行了思考并且认真求证，对我受益匪浅，除了在最后思考第五题，对于新设置的不同网关仍旧可以通信仍存在疑惑。