**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 实验七 实验项目类型 实验地点

学生姓名 李芷靖 学号 2019051114

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

**相关知识理解：**

1. 子网掩码

子网掩码的主要功能是告知网络设备，一个特定的 IP 地址的哪一部分是包含网络地址与子网地址，哪一部分是主机地址。网络的路由设备只要识别出目的地址的网络号与子网号 即可做出路由寻址决策，IP 地址的主机部分不参与路由器的路由寻址操作，只用于在网段中唯一标识一个网络设备的接口。将子网掩码和 IP 地址作"与"操作后， IP 地址的主机部分将被丢弃，剩余的是网络地址和子网地址。例如，一个 IP 分组的目的 IP 地址为：10.2.2.1，若子网掩码为：255.255.255.0，与之作"与"运算得：10.2.2.0，则该网络设备认为该 IP 地址的网络号与子网号为：10.2.2.0。

1. 默认网关

在Internet中的网关一般是指用于连接两个或者两个以上网段的网络设备，通常使用路由器（Router）作为网关。在TCP/IP网络体系中，网关的基本作用是根据目的IP地址的网络号与子网号，选择最佳的出口对IP分组进行转发，实现跨网段的数据通信。

1. ARP协议

在以太网（Ethernet）中，一个网络设备要和另一个网络设备进行直接通信，除了知道目标设备的网络层逻辑地址（如IP地址）外，还要知道目标设备的第二层物理地址（MAC 地址）。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。在一次ARP的请求与响应过程中，通信双方都把对方的MAC地址与IP地址的对应关系保存在各自的ARP表中，以在后续的通信中使用。ARP表使用老化机制，删除在一段时间内没有使用过的IP与MAC地址的映射关系。

1. 以太网协议分析

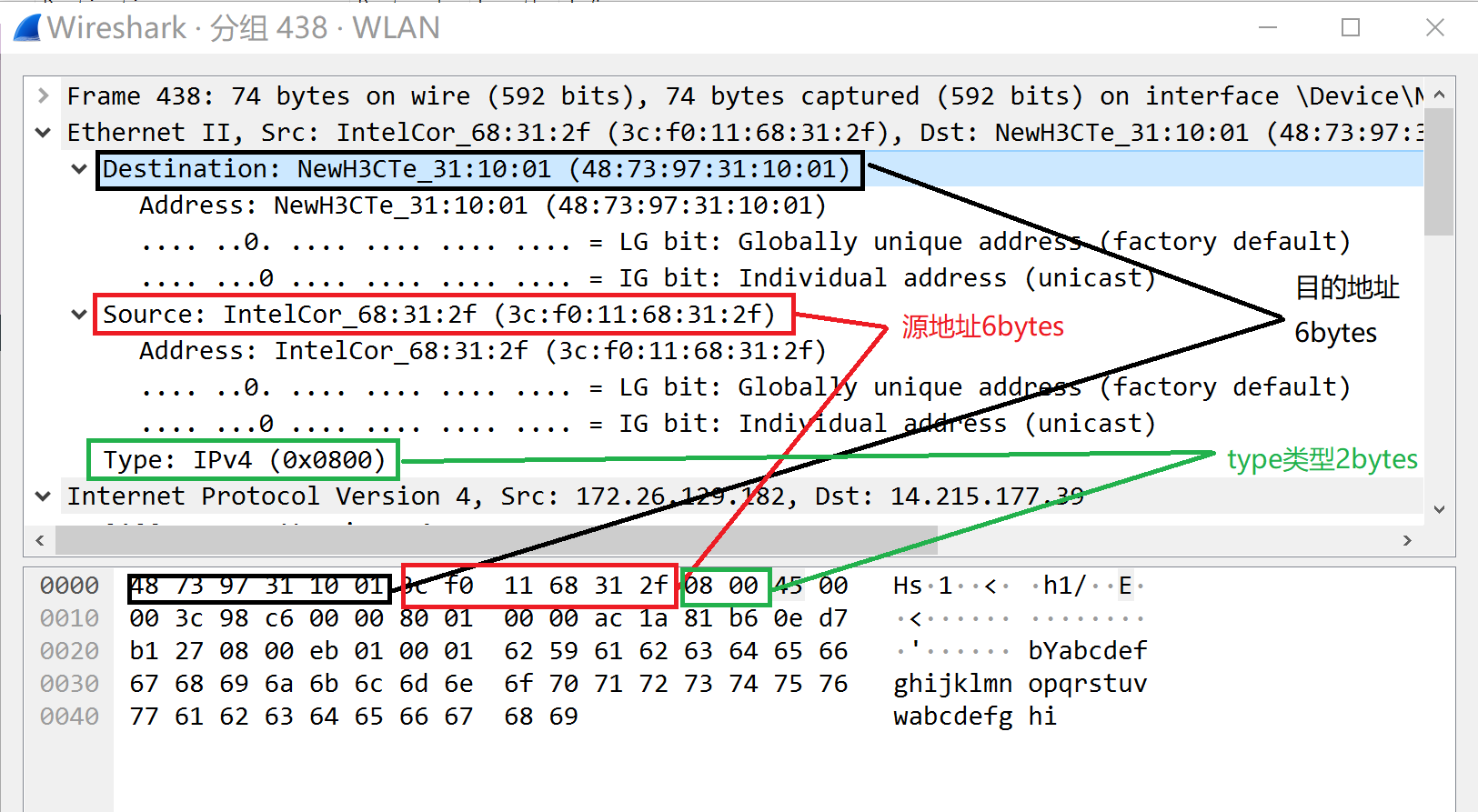
原理：

(1) 局域网(LAN)是在一个小的范围内，将分散的独立计算机系统互联起来，实现资源的共享和数据通信。局域网的主要的特点是：地理分布范围小、数据传输速率高、误码率低和协议简单等。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 目的地址DMAC | 源地址SMAC | 帧类型/长度TYPE/LEN | 数据DATA | 帧校验FCS |
| 6 bytes | 6 bytes | 2 bytes | 46-1500 bytes | 4 bytes |

(2)以太网中传输的数据包通常被称为“帧”，以太网的“帧”结构如下：

(3)数据链路层将不可靠的物理层转变为一条无差错的链路，涉及的数据单位是帧(frame)，高层的协议数据被封装在以太网帧的数据字段发送。使用网络协议分析软件可以捕获各种协议数据包，通过查看这些协议数据包中数据链路帧的各字段可以分析网络协议的内部机制。

分析：

目标地址和源地址（Destination Address & Source Address）：表示发送和接收帧的工作站的地址，各占据6个字节。其中，目标地址可以是单址，也可以是多点传送或广播地址。  
 类型（Type）或长度（Length）：这两个字节在Ethernet II帧中表示类型（Type），指定接收数据的高层协议类型。而在IEEE 802.3帧中表示长度（Length），说明后面数据段的长度。

经查阅网上资料得知。图中数据可以发现看不到前导包与校验（FCS），因为网卡进来的数据是已经校验正确的数据包，会相应的处理掉了前导包和FCS，数据不正确的包已经被丢弃了。

分析数据可以得出：

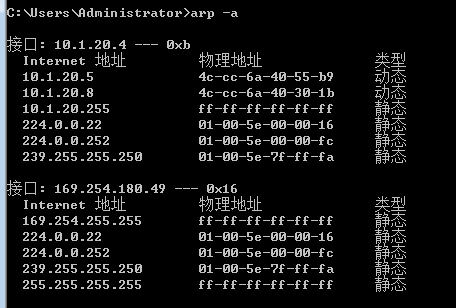
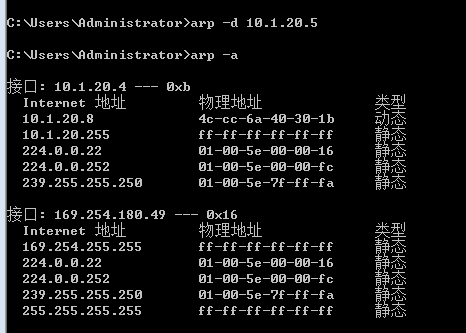
* Ethernet II是目的mac地址在前，源mac地址在后。
* 数据是由mac为48:73:97:31:10:01 ⇒ 3c:f0:11:68:31:2f的设备，mac填充为高位字节在前。
* DATA装载的是IPv4协议。除了IPv4类型之外还分别有IPv4(0x0800)、ARP(0x0806)、RARP(0x0835)、IPv6(0x86DD)
* Wireshark接收到的数据包均为网卡校验正确的数据包，所以没有了前导包与校验(FCS)数据。

主机检查帧头中的目的MAC地址，如果目的MAC地址不是本机MAC地址，也不是本机侦听的组播或广播MAC地址，则主机会丢弃收到的帧。如果目的MAC地址是本机MAC地址，则接收该帧，检查帧校验序列（FCS）字段，并与本机计算的值对比来确定帧在传输过程中是否保持了完整性。如果检查通过，就会剥离帧头和帧尾，然后根据帧头中的Type字段来决定把数据发送到哪个上层协议进行后续处理。

1. ARP协议分析

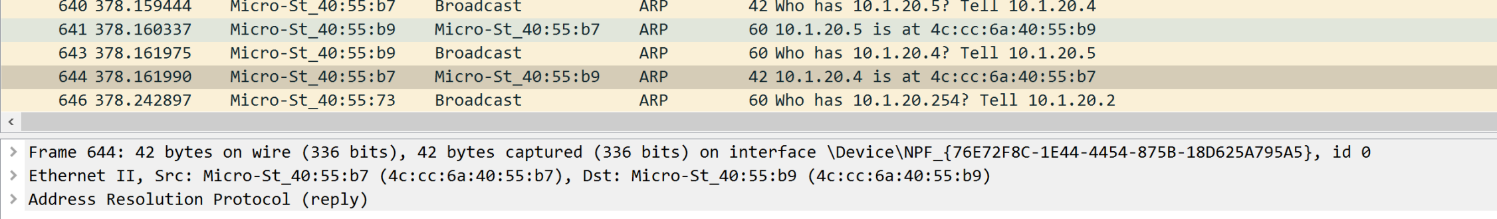
* 进入DOS窗口，用arp – a 查看本机上的ARP表的情况，然后用 arp –d B 删除B的记录（如果有的话）；

两台主机A，B为一组进行实验，查看A主机上的ARP表的情况，并且将A主机上的ARP表中的B记录删除



* 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；

捕获ARP报文：

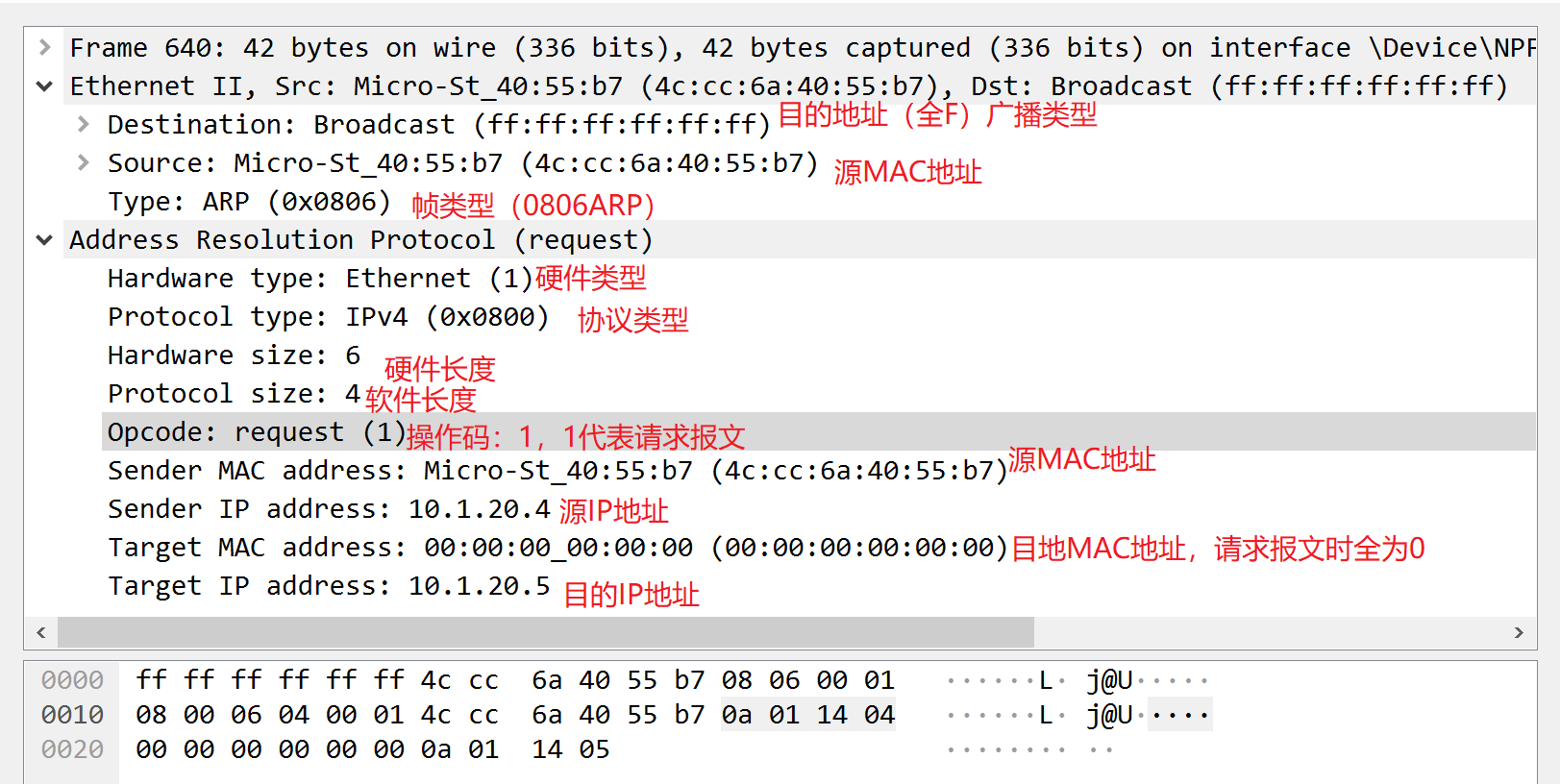
可以捕获到ARP报文

* 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；

ARP报文直接封装在数据链路帧中， ARP分组被封装在以太网的帧中。注意，分析报文时帧中的类型字段指出此帧所携带的数据是ARP报文。

分析ARP报文：

请求报文：

当PC1发送的ARP请求报文，以广播报的形式发送到局域网后，当pc2检测到IP地址与自己的IP相同，就会发送给PC1响应报文。

对于ARP响应包来说，源IP，目地IP，源MAC，目地MAC都是知道的。

响应报文：

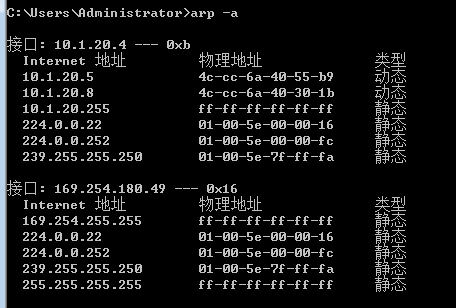
ARP响应的数据包和请求的数据包不同之处在于：

-用于响应的数据包的操作码（Opcode）现在是2，表明这是一个用于响应的数据包；

-发送方的MAC地址和IP地址变成了目标MAC地址和IP地址；

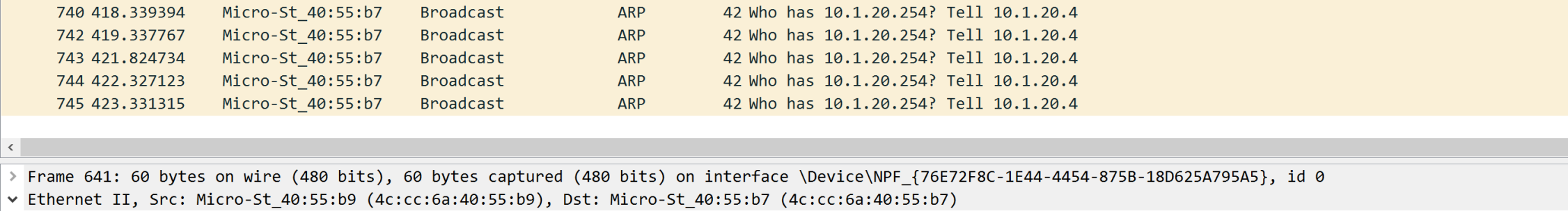
-响应数据包中的内容都是可用的，也就是说我们已经获取了B主机的MAC地址，即4c:cc:6a:40:55:b9，那么接下来就可以正常通信了。

* 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；



再次查看主机A的ARP表，又可以查看到B对应的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；
* 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。



当主机A的ARP表上又可以查看到B对应的MAC地址时，再次从主机A上向主机B发PING检测报文此时可以捕获到ARP报文，反之主机B上向主机A发PING检测报文，也能能捕获ARP报文；只不过在主机A上之捕获到广播请求报文，而没有响应报文。ARP缓存表有生存时间，存在一定的时间段内不进行两主机之间的同行，动态ARP缓存会失效，需要重新进行添加MAC地址后进行通信，生存时间不固定，在实验中我们尝试了五分钟内两主机不相互通信，但缓存表中信息并没有删除，还是能捕获到ARP报文。所以可能是该缓存表的生成时间比五分钟要长。

查阅资料得知，ARP协议中存在一个免费的ARP协议数据包，这个数据包是以广播的形式发出的，这样一来，网络上的所有主机都能收到它。

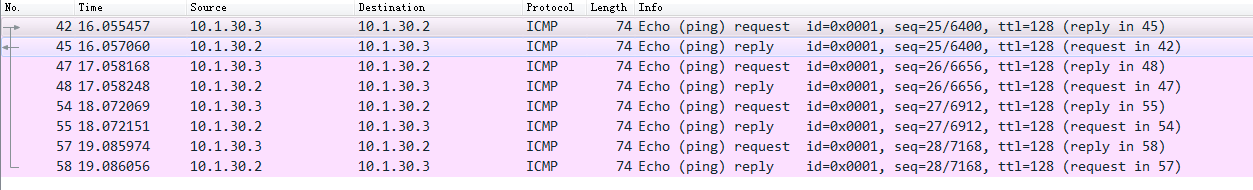
接下来，发现发送方的IP地址和接收方的IP地址是一致的。网络中的其它主机收到这个数据包之后，它会让这些主机使用新的IP和MAC地址映射关系来更新它们的ARP表。由于这个ARP数据包是源主机未经请求主动发出的，并导致了目标主机更新了ARP缓存，所以称之为免费的ARP。

1. IP协议分析

IP协议数据包格式

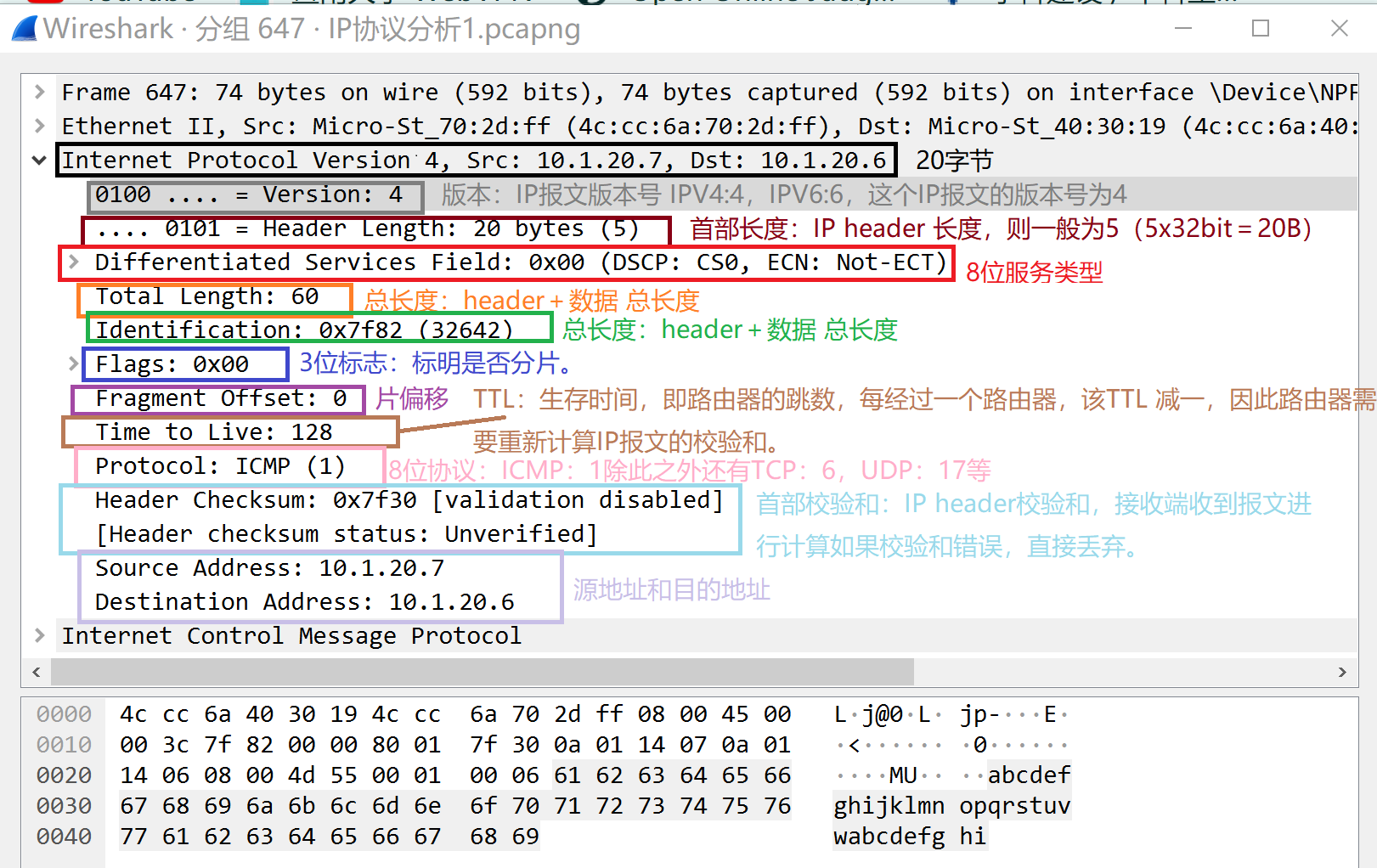
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4位版本 | 4位首部长度 | 8位服务类型 | 16位总长度（字节数） | |
| 16位标识 | | | 3位标志 | 13位片偏移 |
| 8位生存时间（TTL） | | 8位协议 | 16位首部检验和 | |
| 32位源IP地址 | | | | |
| 32位目的IP地址 | | | | |
| 选项（如果有） | | | | |
| 数据 | | | | |

* 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;

从主机A上向主机B发PING检测报文。

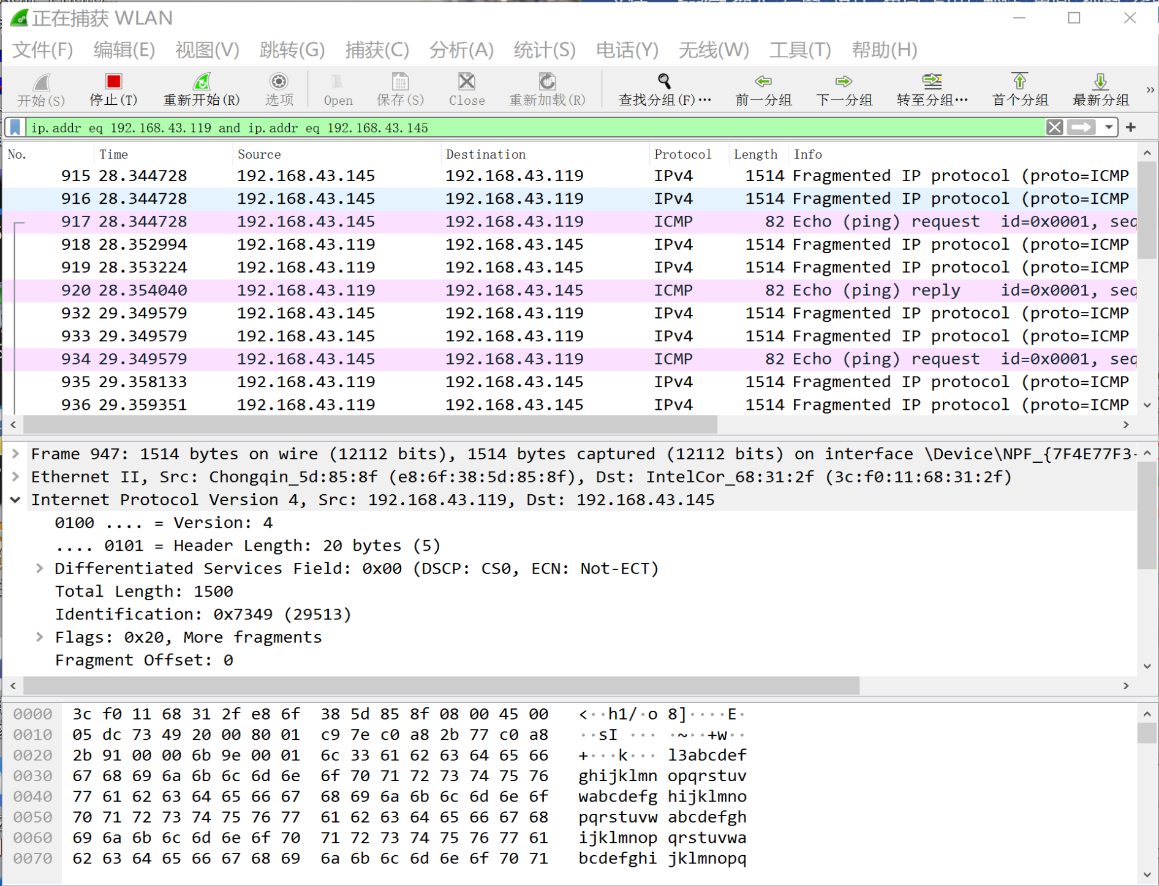
分析IP数据包：



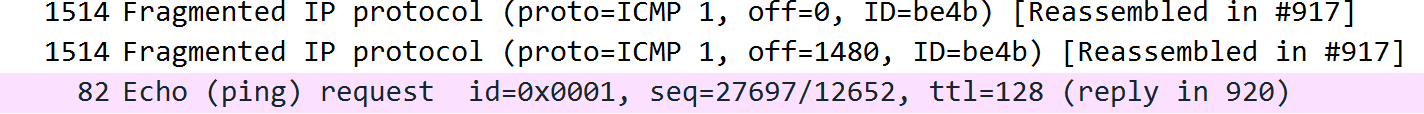
请求报文和响应报文基本一致，因为是在同子网主机通信，所以TTL在两种报文中显示的都是128，IP字段的TTL值不变，说明目的主机到源主机的数据报没有经过一个路由器。

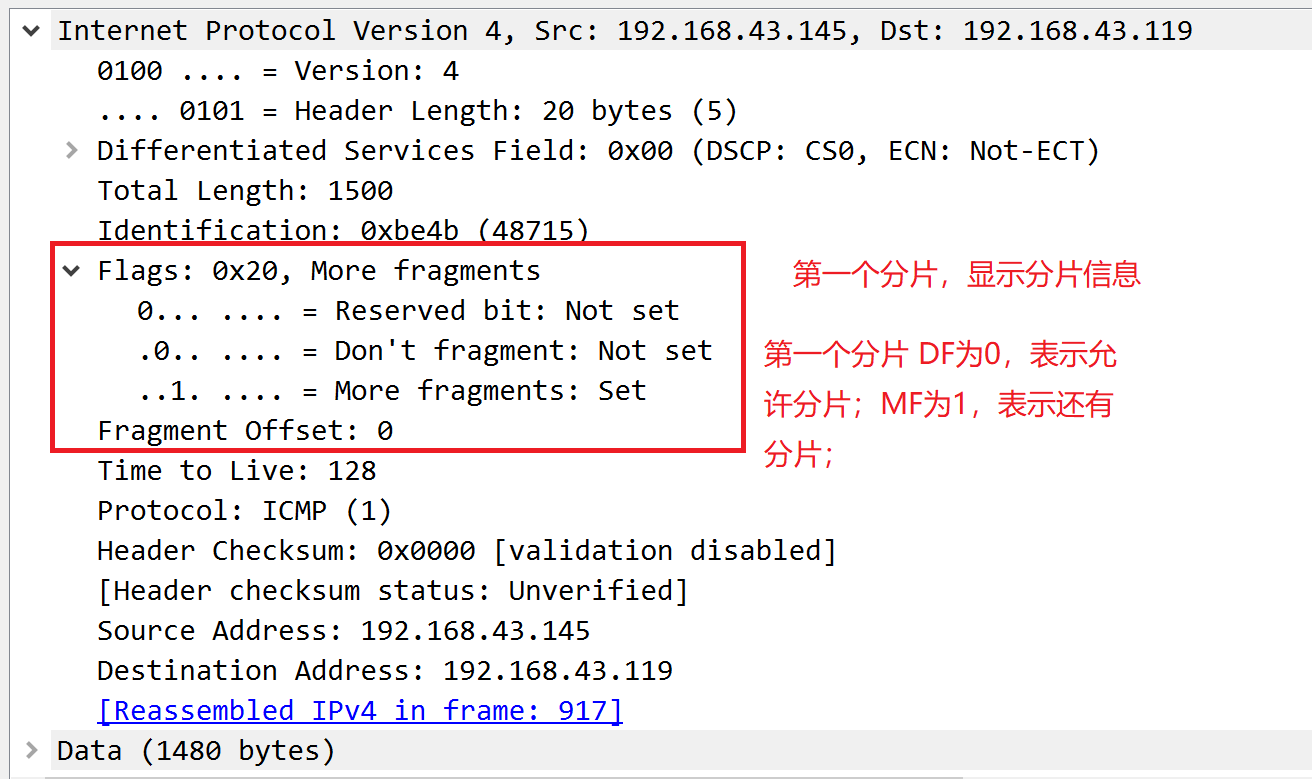
* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析**分片和重组**过程。

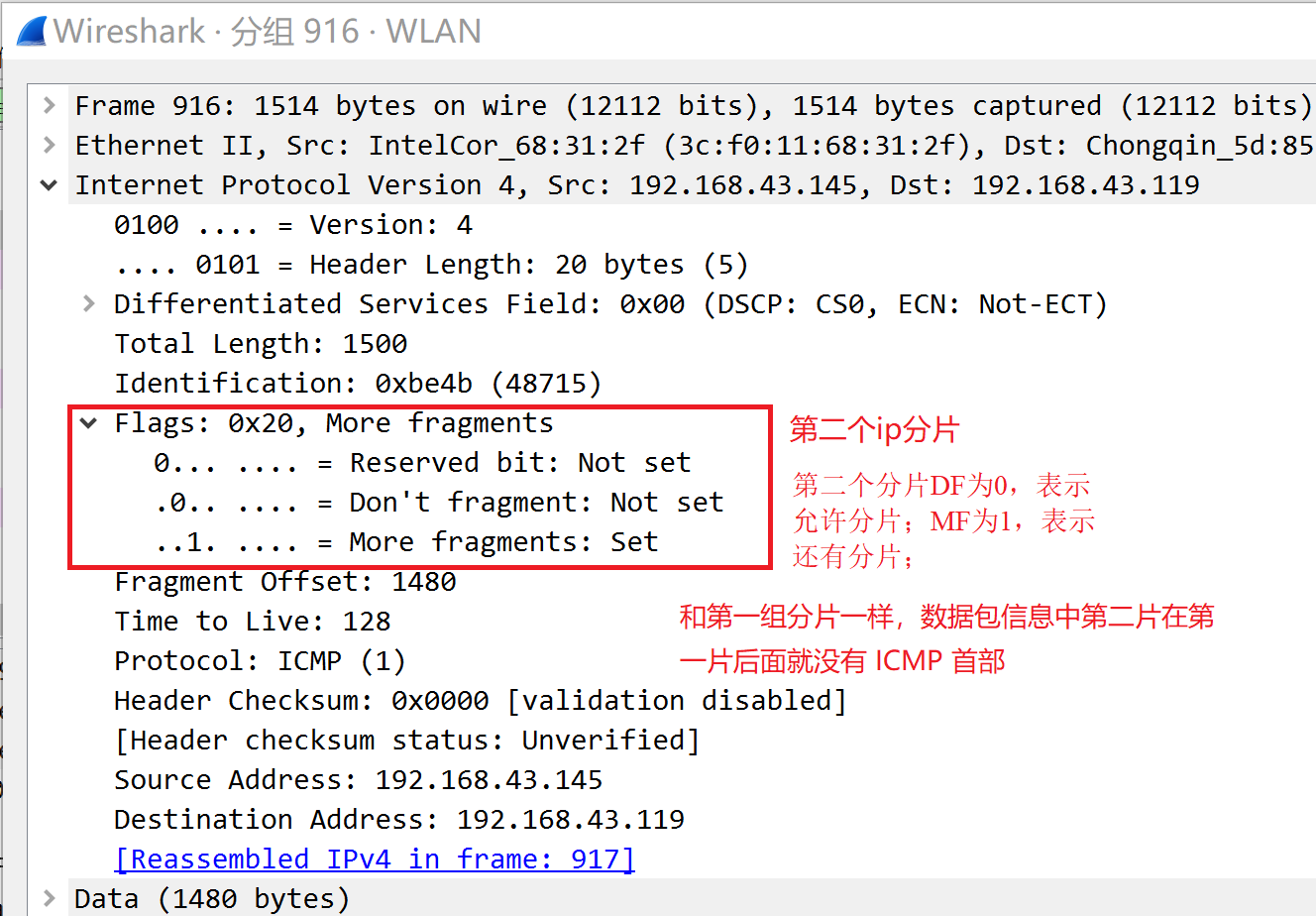
通过课本知识学习得知，链路层通常对可传输的每一个帧的最大长度都有上限。为了使超过此上限的ip数据报能够正常传输，IP引入了“分片”和“重组”。

对同一子网下另一主机发送ping -l 3000命令，因为数据包长度自定义超过了规定长度，所以能够捕获到IP分片信息。

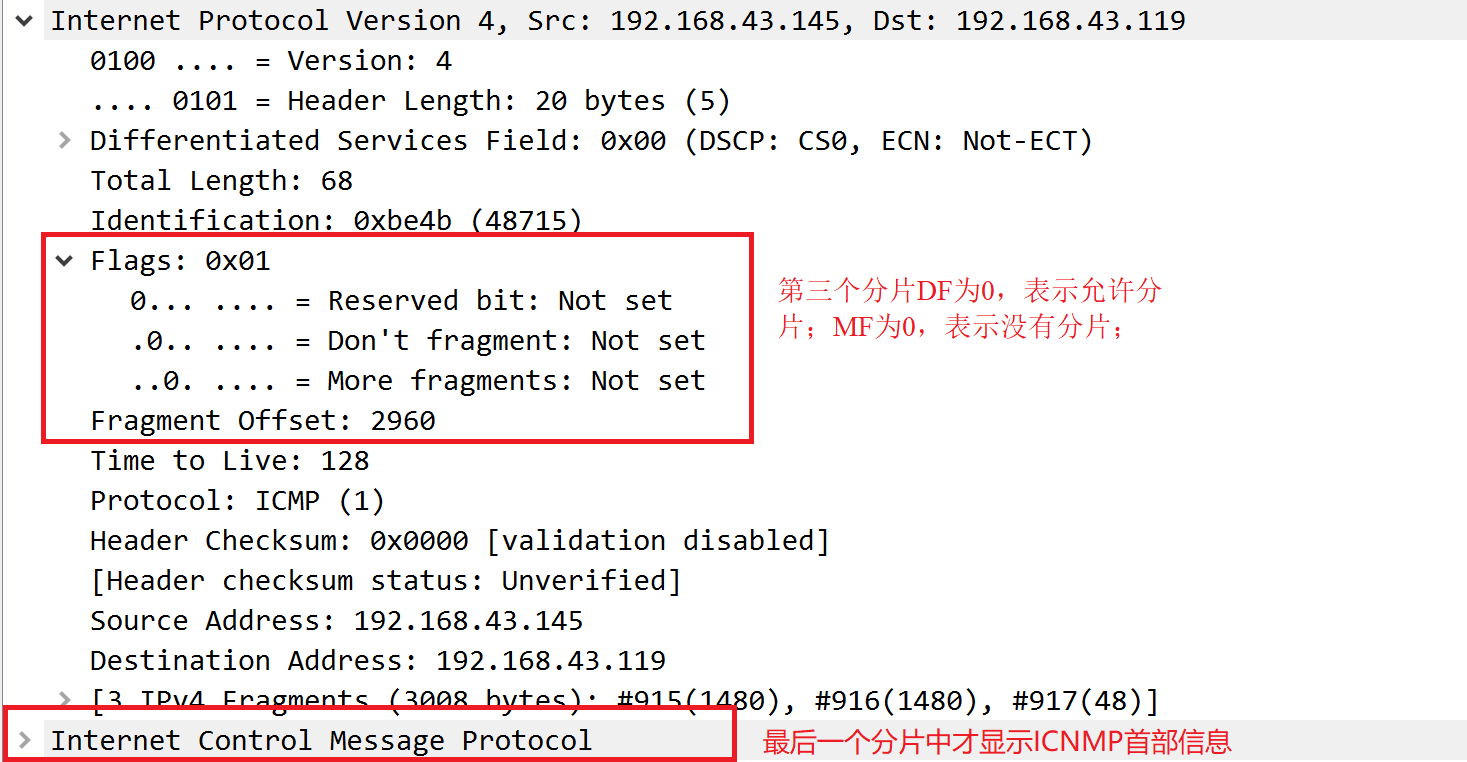
以太网数据链路层能传输的最大报文长度1500B(不包含帧头部)，当超过这个MTU值时，需要对IP数据包进行分片。使用命令 ping -l 3000 10.10.87.122，-l 指定数据长度为3000bytes,抓包看到数据包被分为了3个分片，前两个分片是IP 数据包，最后一个分片是ICMP数据包。IP数据包的长度都是1500，其中20字节是IP头部，1480是数据长度；ICMP类型数据包的IP数据长度是68（20+8+40），其中20字节是IP头部信息，8字节是ICMP头部信息，40字节是数据长度。



第一个分片 DF为0，表示允许分片；MF为1，表示还有分片；数据部分偏移为0；

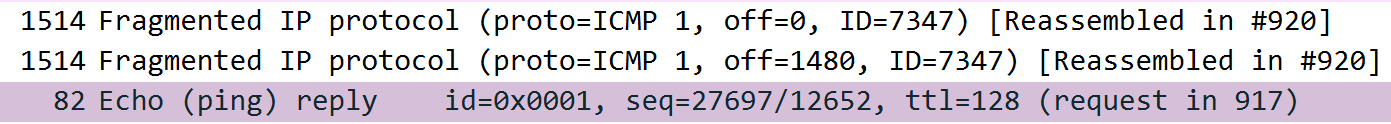


第二个分片DF为0，表示允许分片；MF为1，表示还有分片；数据部分偏移为185，单位为8字节，表示偏移了185\*8=1480字节；



第三个分片DF为0，表示允许分片；MF为0，表示没有分片；数据部分偏移为370，偏移了2960字节。

以上就是一组IP数报分片发送，路由器只做分片不做重组



接收器标识匹配使用外国和当地的互联网地址，协议号，和识别领域的片段。接收器将重组从片段数据与同时使用的片段偏移和多个片段标志相同的ID。当接收机接收的最后一个片段（其具有的“更多片段”标志设置为0），它可以通过乘以最后一个片段的八个偏移，并加入最后一个片段的数据的大小来计算的原始数据有效载荷的长度，。

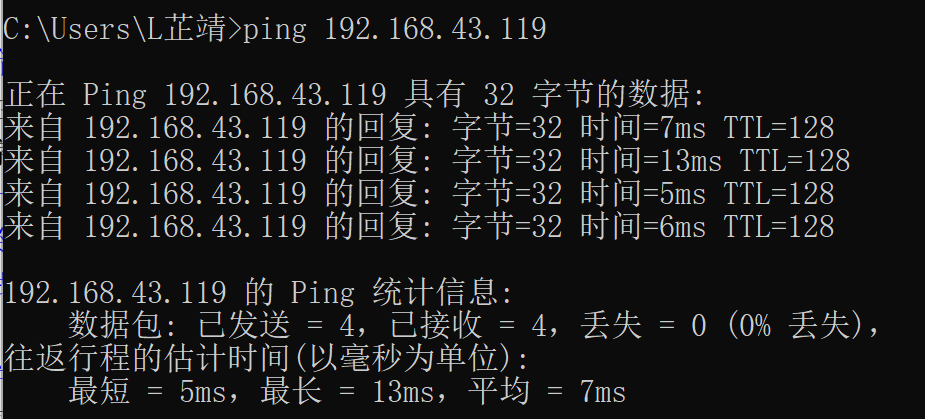
1. ICMP协议分析

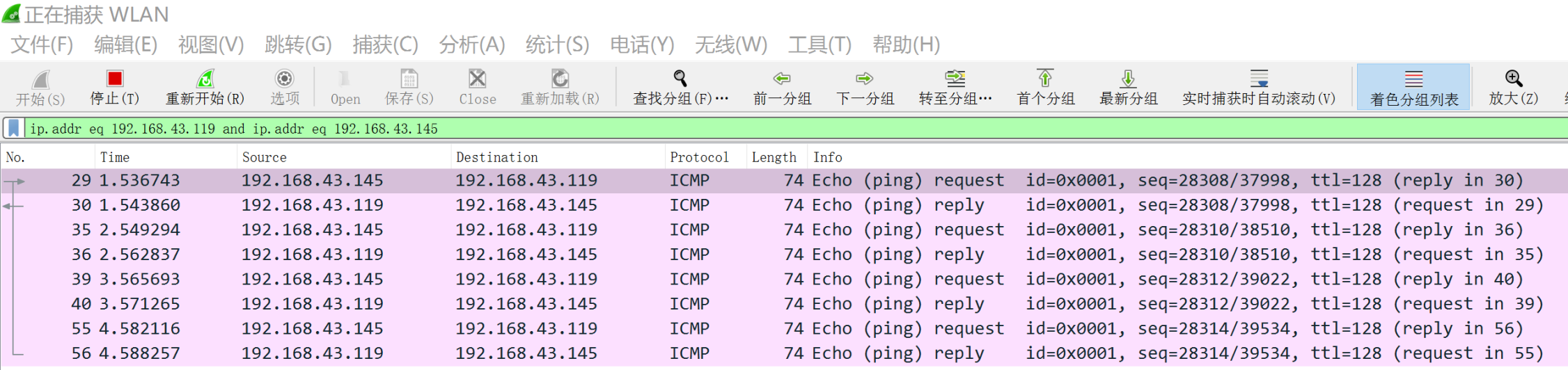
ICMP用于IP主机、路由器直接传递控制信息，控制信息是指网络通不通、主机是否可达、路由是否可用等网络本身信息。ICMP本身不传输用户信息。

ICMP报文格式：

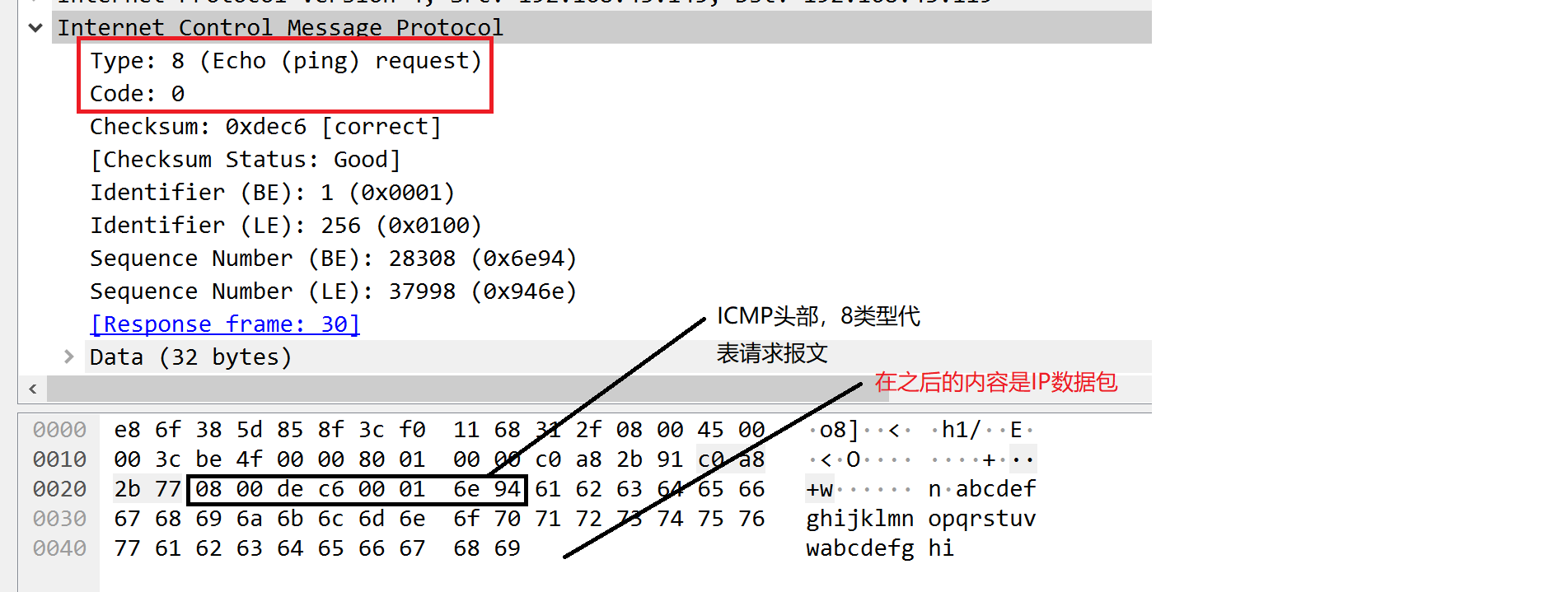
|  |  |  |
| --- | --- | --- |
| 类型 | 代码 | 校验和 |
| 首部其他部分 | | |
| 数据 | | |

* 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A向主机B发送PING报文主机A能够捕获到ICMP请求数据包和应答数据包

获取一个请求报文



* 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。

ICMP报文的种类分为两种：一种是差错报告报文，另一种是查询报文。

(1)差错报告报文

类型值为3时：表示终点不可达

类型值为4时：表示源点抑制

类型值为5时：表示改变路由(Redirect）

类型值为11时：表示超时

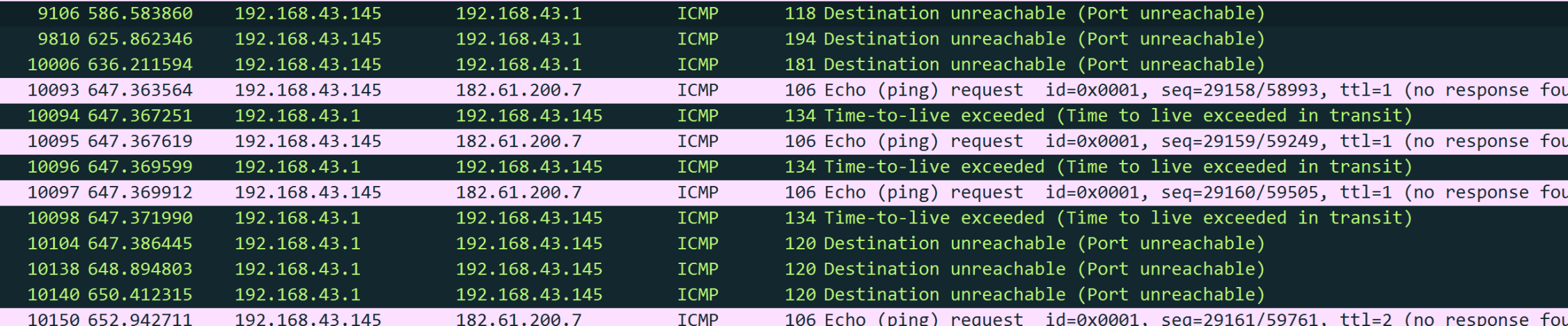
类型值为12时：表示参数问题

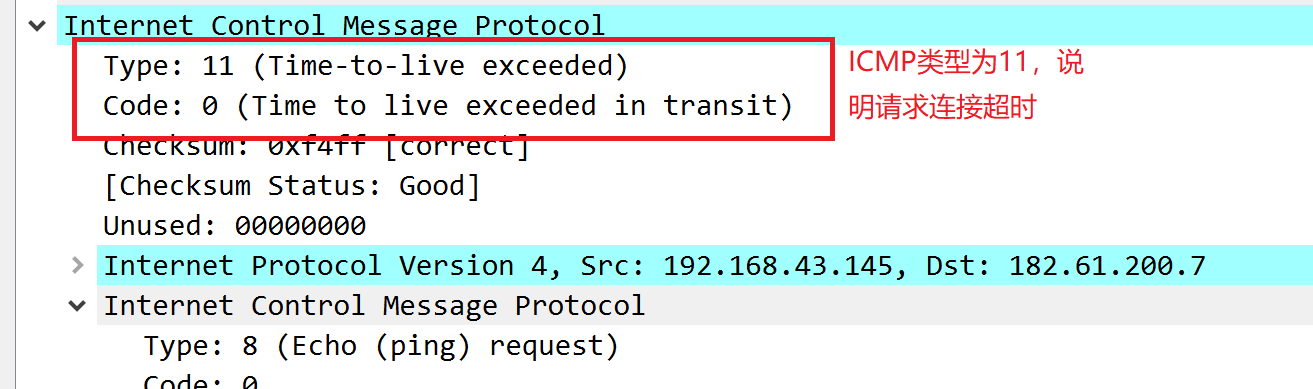
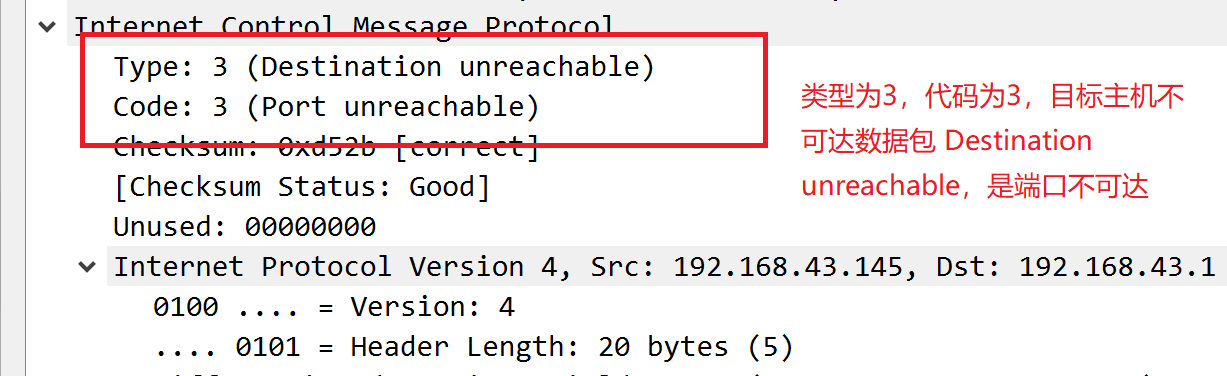
(2)询问报文

类型值为8或者0时：表示回送(Echo)请求或应答

类型值为13或14时：表示时间戳(Timestamp)请求或应答

Tracert跟踪www.baidu.com





实验结果与查阅资料总结：

1.对于携带ICMP差错报文的数据报，不再产生ICMP差错报文。

如果主机A发送了一个ICMP的数据报文给主机B，数据在传输过程中经过其中一个路由器出现错误，由于该路由器已经接收到一个ICMP数据报文，所以不会再产生一个ICMP差错报文。

2.对于分片的数据报，如果不是第一个分片，则不产生ICMP差错报文

对于主机A发送了一个分片的数据，如果路由设备或主机接收到的分片数据不是第一个分片数据，不会产生ICMP差错报文。

3.对于具有多播地址的数据报，不产生ICMP差错报文

如果一个ip地址是一个广播地址的话，不会产生ICMP差错报文。

4.对于具有特殊地址如（127.0.0.0或0.0.0.0）的数据报，不产生ICMP差错报文

Tracert工作原理

1. 从源地址发出一个UDP探测包到目的地址，并将TTL设置为1；
2. 到达路由器时，将TTL减1；
3. 当TTL变为0时，包被丢弃，路由器向源地址发回一个ICMP超时通知（ICMP Time Exceeded Message），内含发送IP包的源地址，IP包的所有内容及路由器的IP地址；
4. 当源地址收到该ICMP包时，显示这一跳路由信息；
5. 重复1～5，并每次设置TTL加1；
6. 直至目标地址收到探测数据包，并返回端口不可达通知（ICMP Port Unreachable）；
7. 当源地址收到ICMP Port Unreachable包时停止traceroute。
8. 思考题
9. 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：当A的ARP缓存表中没有B的MAC地址时，主机A会通过广播方式寻找B的MAC地址，所以能捕获得到ARP报文，当A的ARP缓存表中已经有了B的缓存地址了，就不用通过ARP协议去寻找B的MAC地址，也就不会捕获到ARP报文了。

1. 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：ping是对两个TCP/IP系统连通性进行测试的基本工具，他只利用ICMP回显请求和回显响应报文，而不用经过传输层（TCP/IP）。所以，只要弄清楚ping命令发送时是否有经过网卡，即可知道是否能捕获到ICMP报文。

localhost解析地址为127.0.0.1，运行ping 127.0.0.1时，IP输出函数会先检查地址是否是环回地址（不属于任何一个有类别地址类，它代表设备的本地虚拟接口）。127.0.0.1是回环地址，且数据包不经过网卡，所以ping 127.0.0.1时捕获不到ICMP。

在ping本机IP地址是，通过判断该地址是否是回环地址，广播多播地址后，会将本机地址交给环回驱动程序处理，环回驱动程序返回给ip输入函数，所以也是不经过网卡，所以也不能捕获到ICMP数据包。

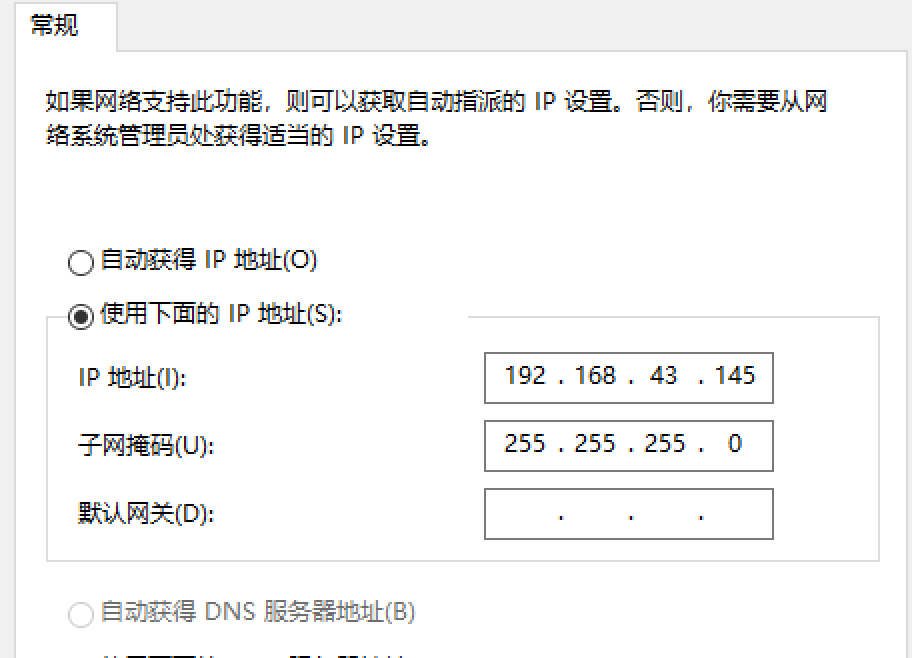
1. 在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

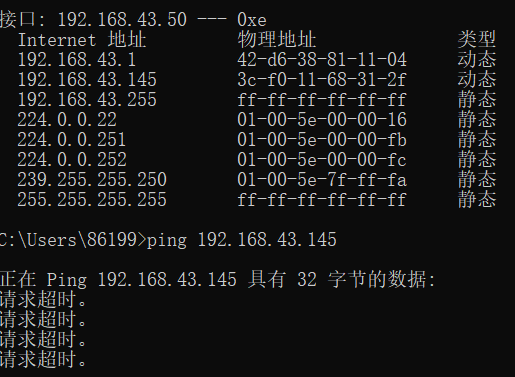
答：返回信息“Request timed out”请求超时，这说明对方无法接受发送过来的数据。可能是本地的TCP/IP协议或者是本地网关地址出现了问题，可以先ping自己来检查是否是本地出现了问题，然后ping一些域名网站，查看DNS是否正常。也有可能是路由器配置问题或者是目标主机网络不存在（IP地址错误）。

返回信息“Destination Host Unreachable”目标主机不能到达，信息说明对方主机不存在或者没有跟对方建立连接，路由表中连到达目标的路由都没有。出现这类错误的可能是1、 局域网使用DHCP动态分配IP地址时，DHCP出现故障或者失，DHCP失效或者出现故障时，客户机无法分配到IP地址，系统只有自设IP地址，而IP地址的自动设置往往会分配到不同的子网，因此会出现“Destination Host Unreachable”。2、子网掩码设置错误，如果子网掩码不是系统自动生成的，则在计算时一定细心。3、路由表返回错误信息这种情况一般是在“Destination Host Unreachable”前面加上IP地址，说明本地计算机与外部网络连接没有问题，但与某台主机连接存在问题。

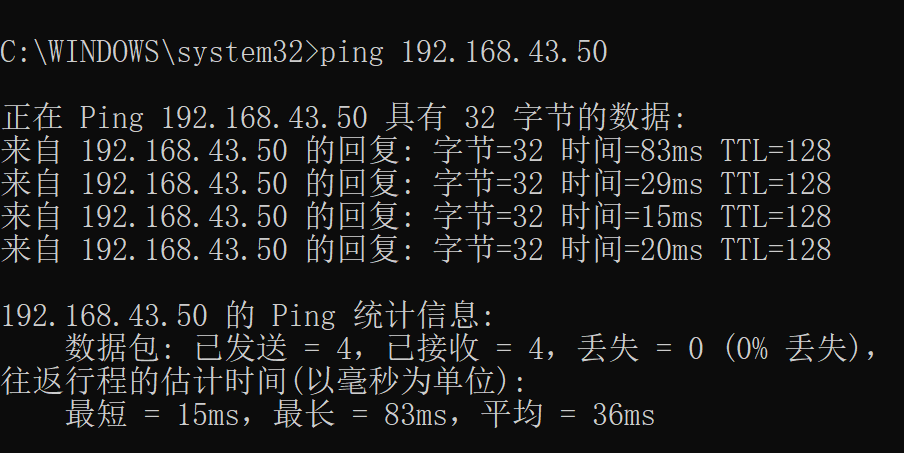
1. 请通过实验**验证**：

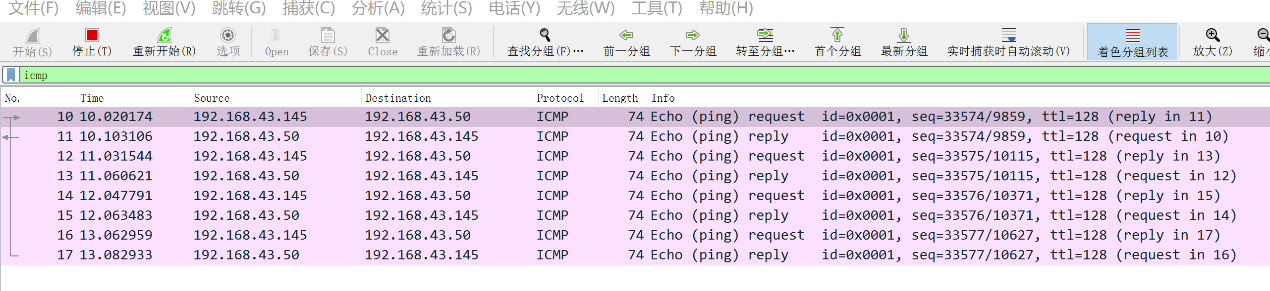
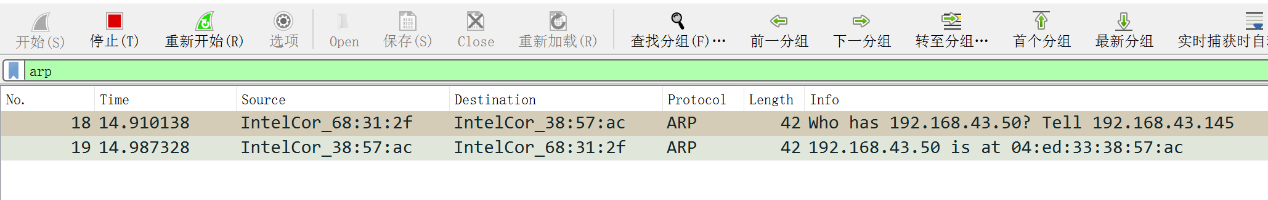
主机如果不设置“网关”，同一网段内的主机可以相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。

不设置网关，但主机A和B在同一网段下

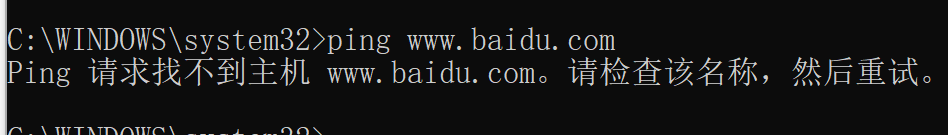
第一次试验中，已经将两主机设置在同一网段中，但主机A的防火墙没有开放，所以主机A能ping主机B。但主机B不能ping主机A。

将两台主机防火墙都打开后进行试验：



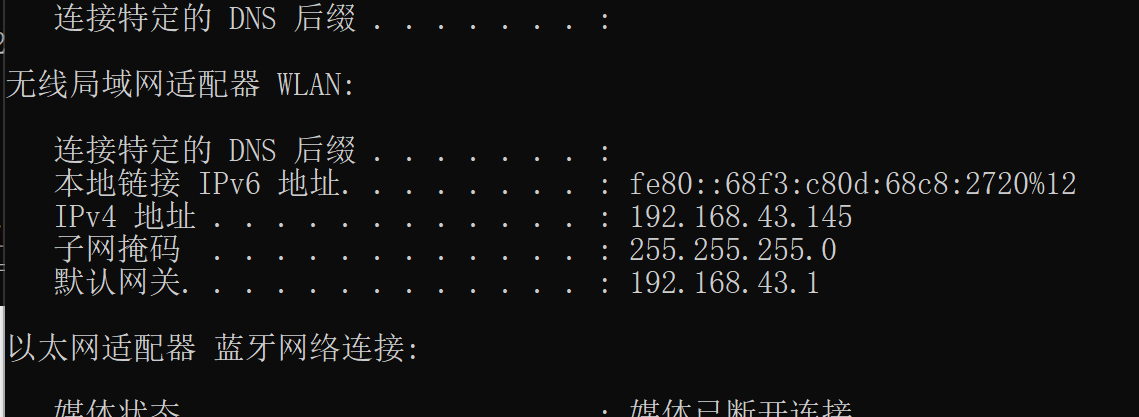
 

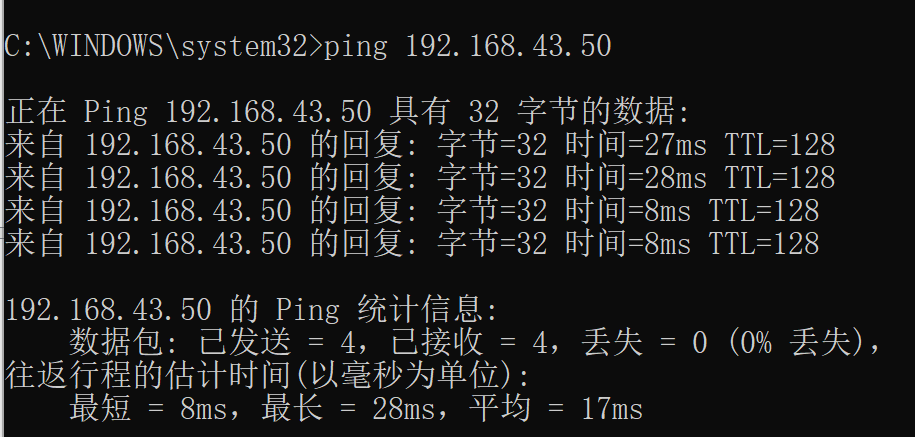
A主机ping B主机，两主机之间能够相互通信，并且可以捕获8个ICMP数据包，2个ARP数据包

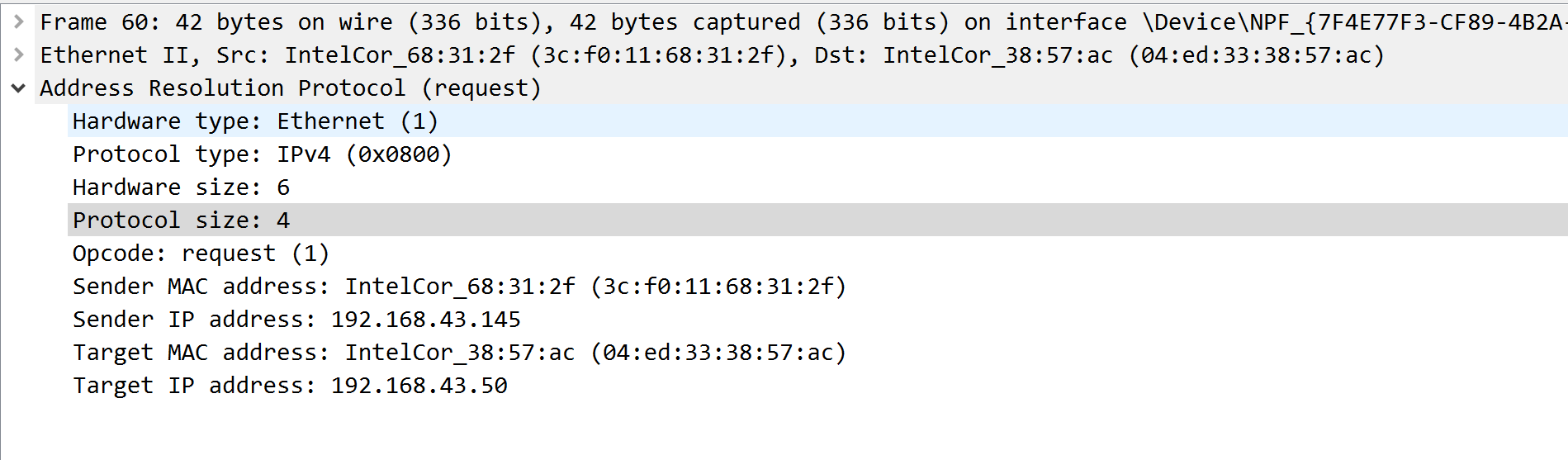


在ping不同网段ip地址时，不能进行相互通信显示“目的主机不可达”，用嗅探器捕获不到任何信息。

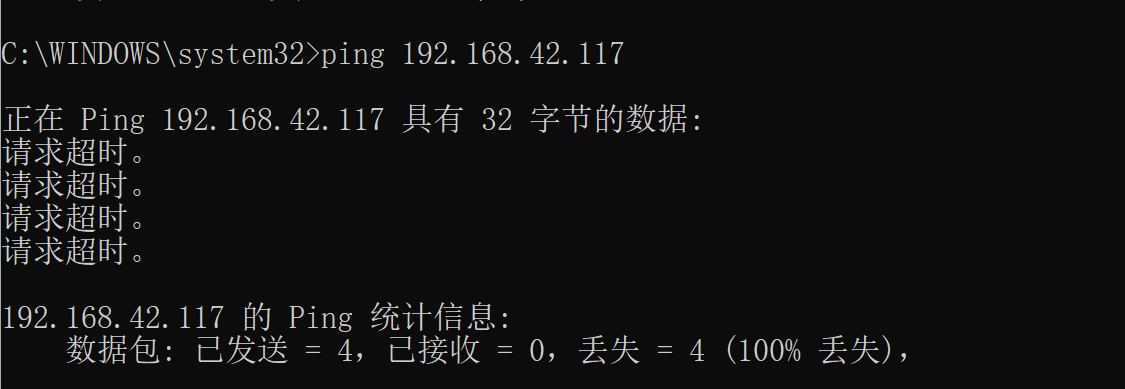
主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

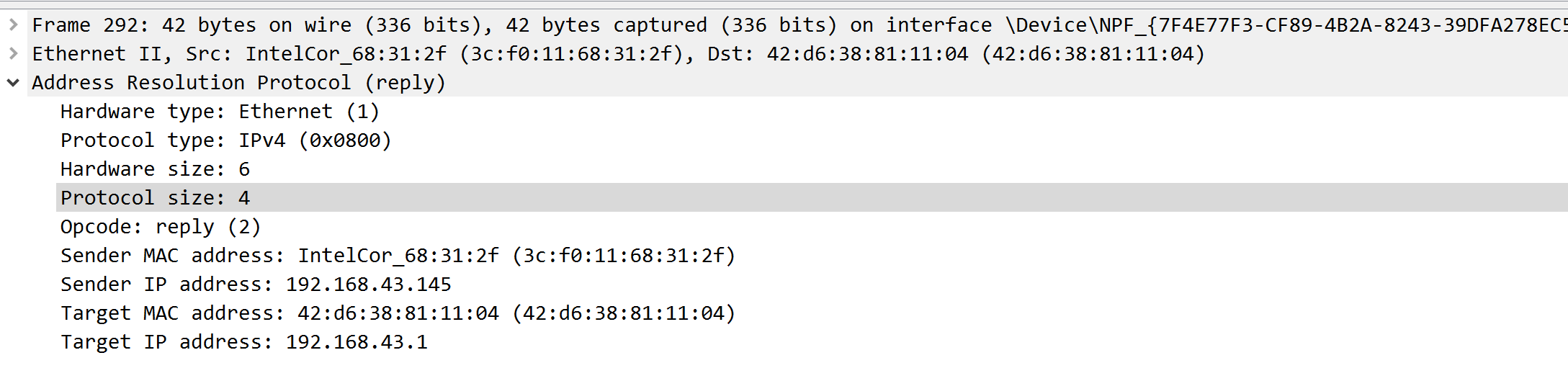
主机A和B设置相同默认网关。

主机Aping主机B，能够进行通信，



并且能在捕获到的ARP数据包中观察到目的主机B的MAC地址。

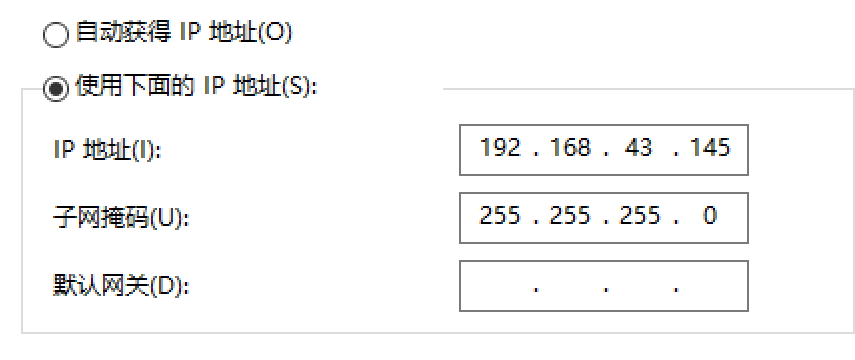
当主机Aping不同网段上的另一主机地址时，不能相互通信，

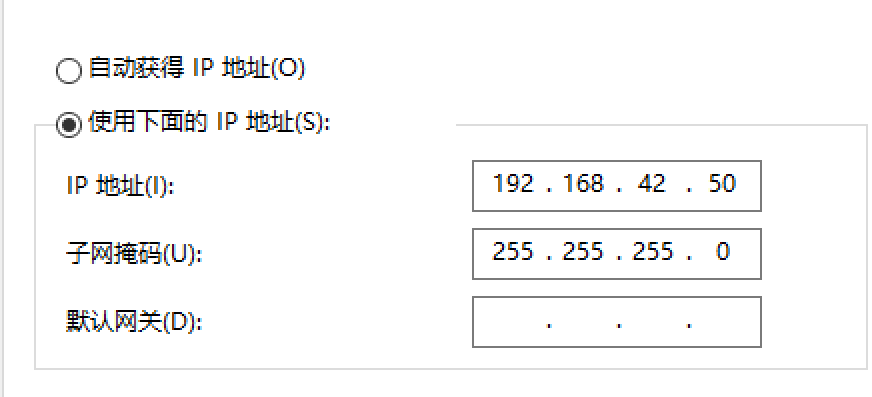


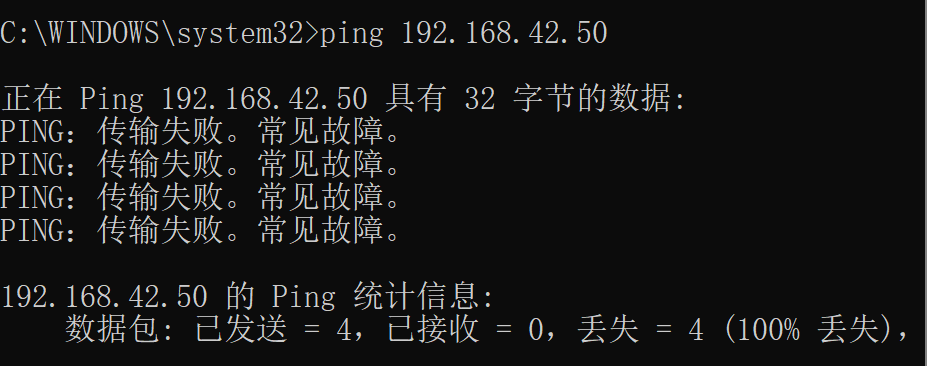
但是在捕获到的ARP不能看到目的主机的MAC地址，但是能看到网关的MAC地址。

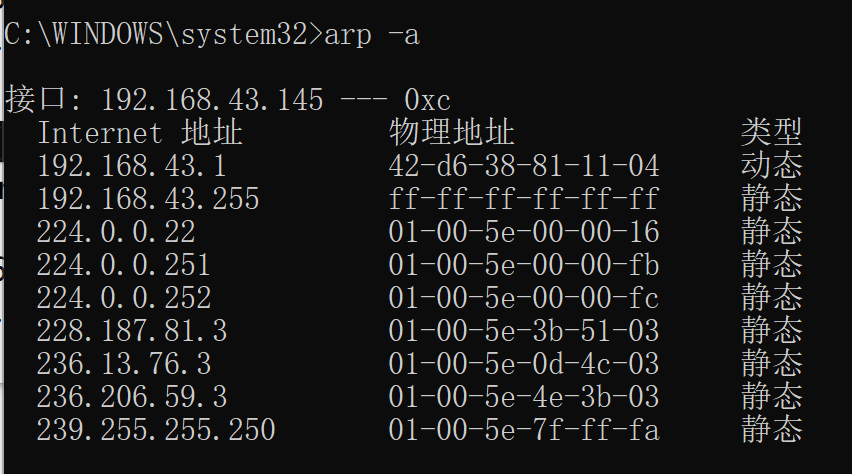
1. 通过下面实验**理解网关**

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设置IP地址

主机B设置IP地址

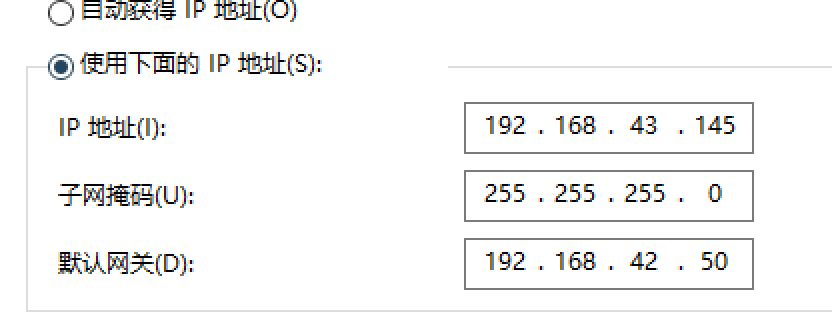
主机Aping主机B失败

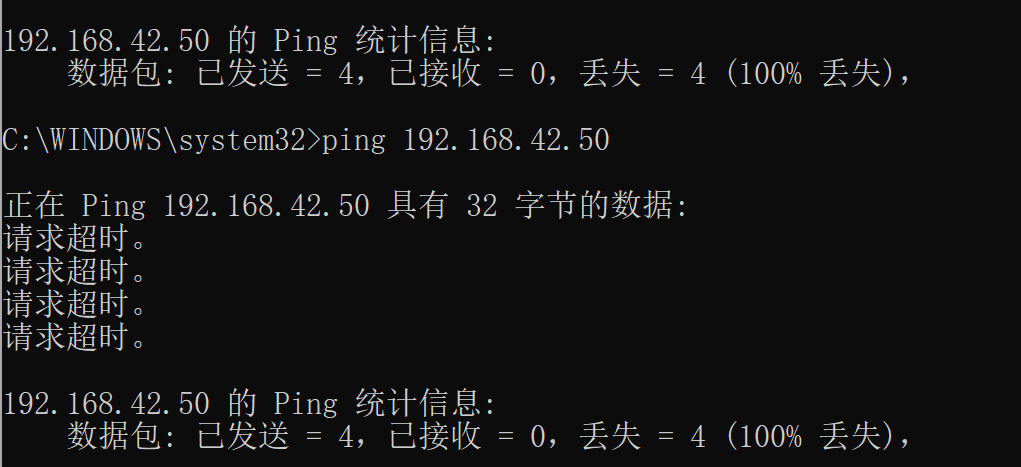
主机A中的ARP缓存表并没有主机B的MAC地址缓存。

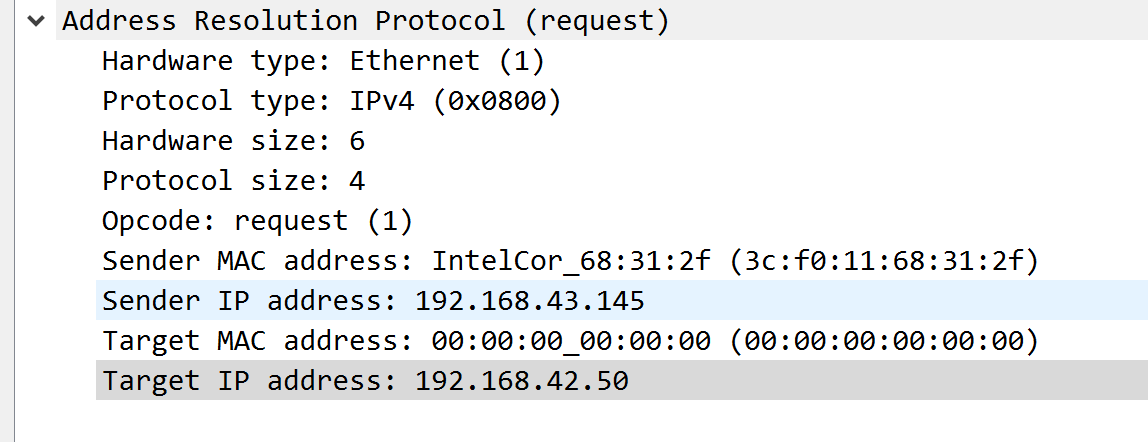
分析：这时两个PC机都使用是C类地址，不在同一个网段，也即是他们的网络地址不同，根据TCP/IP协议的规范，不在同一网络中的PC机不可以直接通信，必须借助网关 ，但此时都没有设定自己的网关，数据包不知道往哪儿发送，就丢弃了，故不能ping通。

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。

A设置网关，B不设置网关

将A的网关设置为主机B的IP地址一样。

主机Aping主机B不能通信。

在ARP数据包中只能观察到网关的MAC地址。

分析： 这时两个PC机都使用是C类地址，不在同一个网段，也即是他们的网络地址不同。设定的PCA的网关为PCB的IP地址，当PCA想要跟PCB通信时，发现PCB跟自己不再同一个网段，然后只能把数据发给自己的网关了（192.168.42.50），当PCA的网关收到数据后，按常理应该把数据发给网关的下一个跳 或则发给其他以PCA的 网关为网关的主机，但是这时只有PCA的以这个IP地址为网关，所以此时网关就不知道把数据发给谁了，就只好丢弃了。故两边就不能ping通。