**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

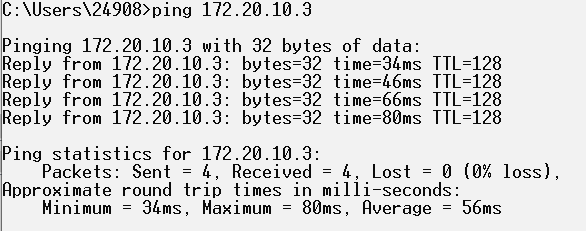
实验项目编号 7 实验项目类型 验证 实验地点 计算机网络实验室

学生姓名 袁霖 学号 2019051099

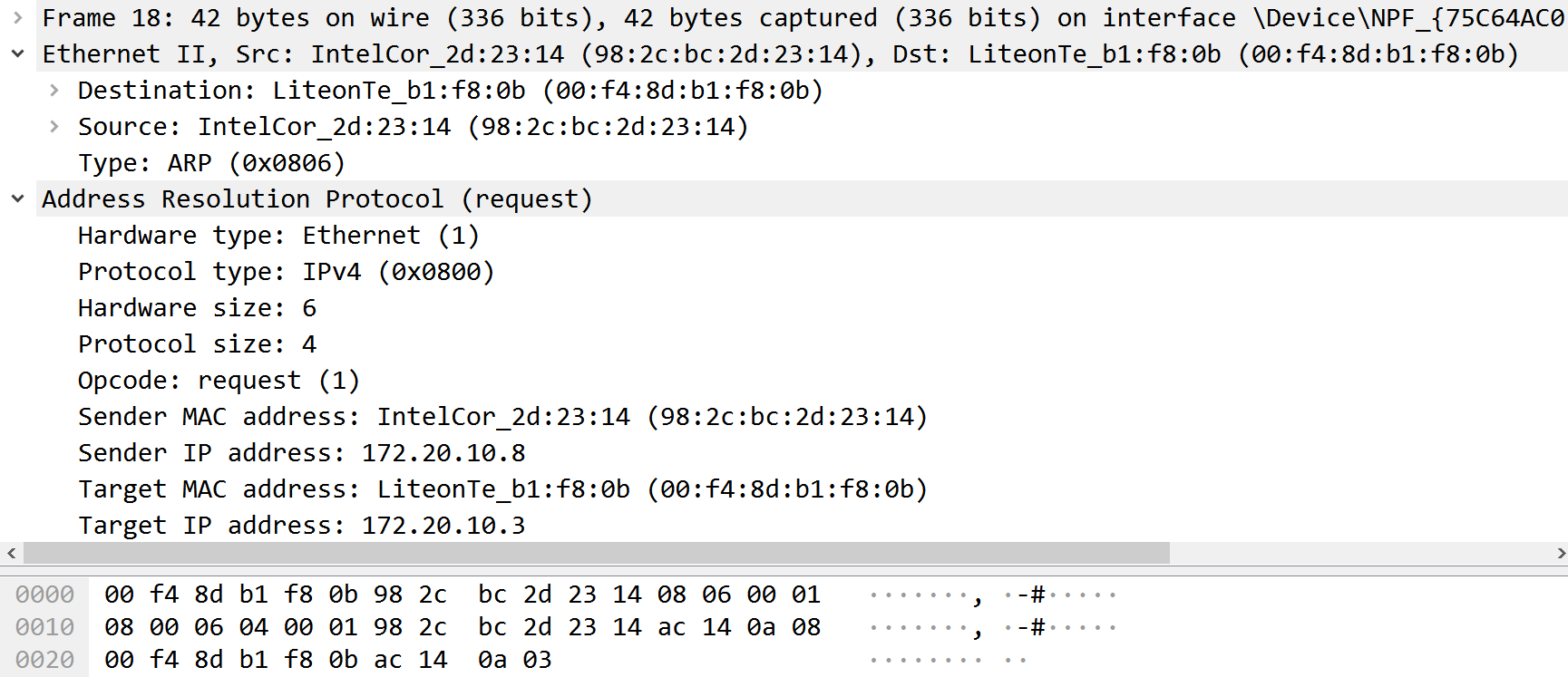
学院 智能科学与工程 系 专业 信息安全

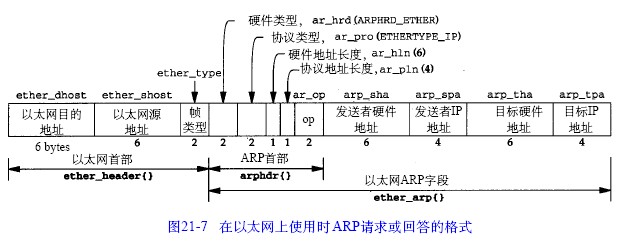
实验时间 2021 年 11 月 2 日 上 午～ 11 月 6 日 下 午

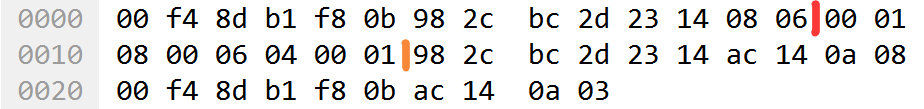
1. **实验目的**
2. 理解链路层、网络层主要协议格式，以及协议的工作原理
3. 理解网关和子网掩码概念
4. 学会利用网络嗅探器（如**Wireshark**）分析协议格式和协议的工作过程
5. 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。
6. **实验内容**
7. 用嗅探器捕获数据包。
8. 分析以太网帧、ARP协议、IP协议、ICMP协议格式
9. 分析PING、TRACERT、ARP命令的工作过程
10. 通过修改主机的网关为指定默认网关、本机IP地址或不设置网关，观察ping的结果，用嗅探器捕获数据包并分析。
11. **实验步骤（过程、结果截图）**
12. **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**



以下为捕获到的以太数据帧：







由上图所示：红色分割线左边是以太网的首部部分，右边是以太网的ARP字段，其中的红色分割线与橙色分割线之间时ARP首部部分。

对应着上图的ARP协议格式，可以得到MAC帧各字段的含义：



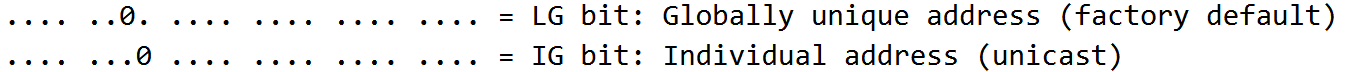
**以太网目的地址（MAC地址） 以太网源地址（MAC地址） 帧类型（ARP） 硬件类型（Ethernet(1)）**



**协议类型（IPv4）硬件地址长度 协议地址长度 操作码 发送方MAC地址 发送方IP地址**



**目标MAC地址 目标IP地址**



在以太网目的地址及源地址中均有以上两个bit位。

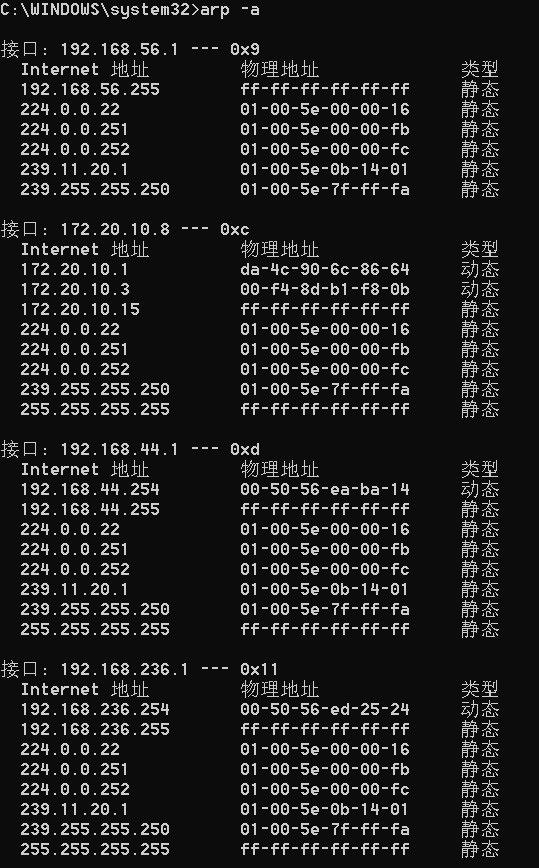
其中，LG bit对应着MAC地址的第7位，它为0表示的是全局管理地址且不可以重复，而为1表示的是管理上统治本地的地址，用于区别于其他设备。

而IG bit对应着MAC地址的第8位，它用于区分单播、组播、广播地址。当它为0时，代表一个实际设备的MAC地址，当值为1时，表示它是一个组播或广播地址。可以看到，这条ARP请求报文是单播的，它是利用单播轮询的方式来保证主机的IP--MAC映射的有效性。

帧类型字段是用来标志上一层使用的是什么协议。

1. **ARP协议分析**

①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）（需要以管理员的身份运行）



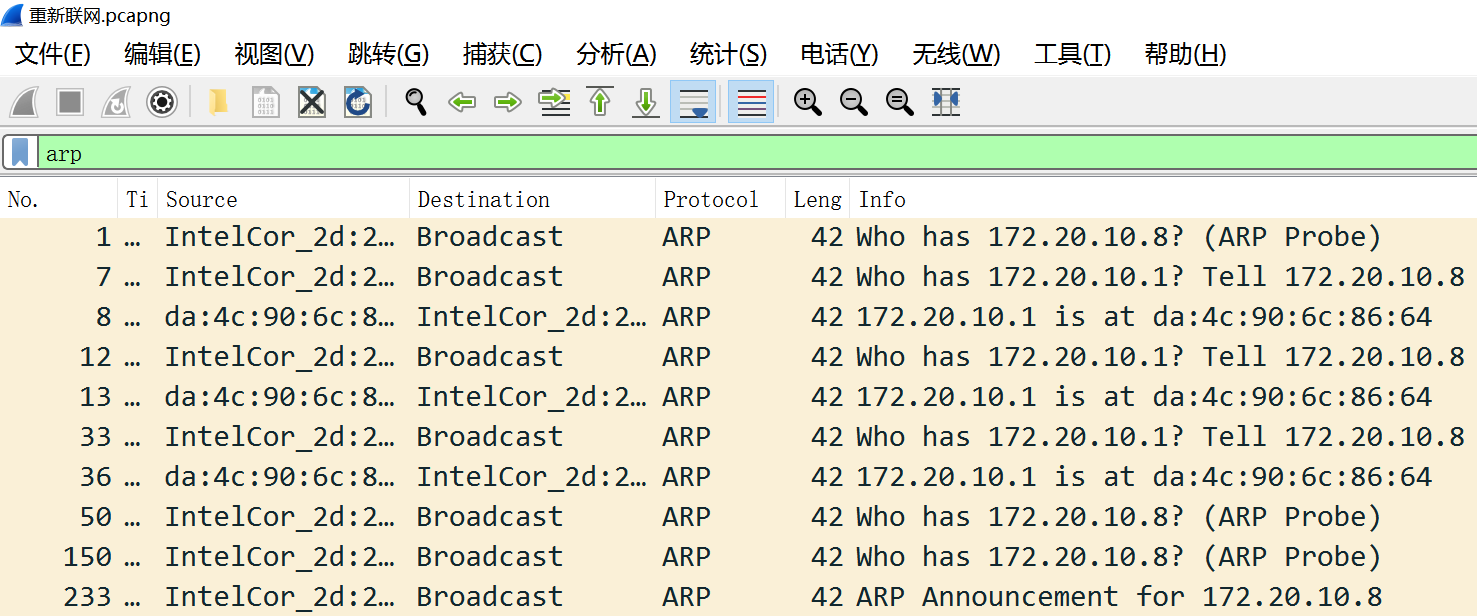
有主机B（IP地址为172.20.10.3）的记录，删除之。



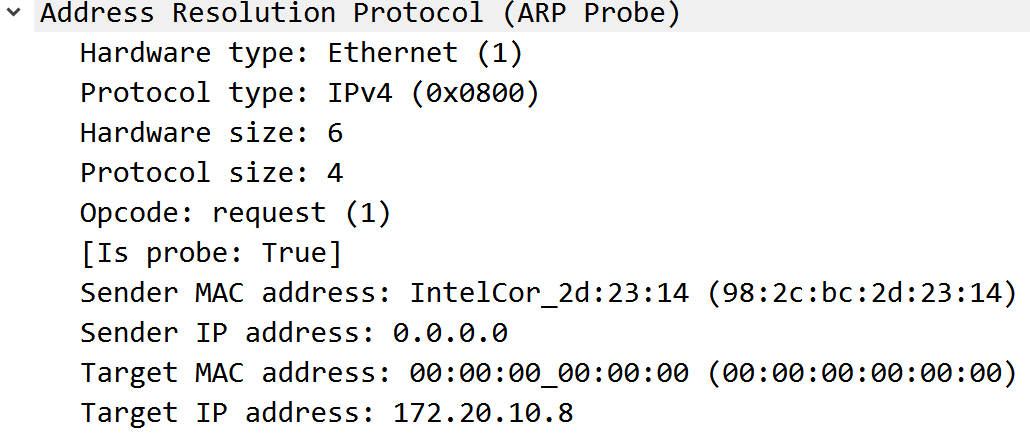
②运行Wireshark程序

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

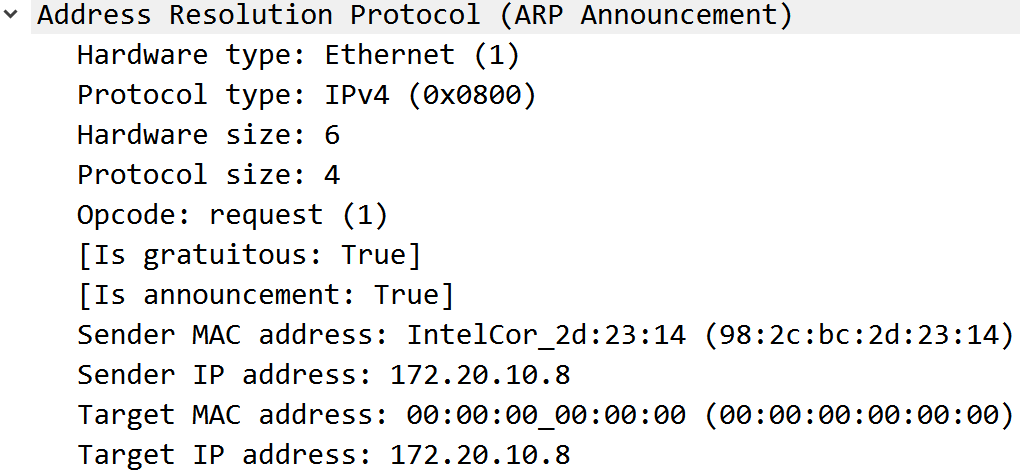
可以捕获到ARP报文，通过下图可以看出，捕获到了4种ARP报文，分别为ARP Probe，ARP Announcement，ARP request，ARP reply：



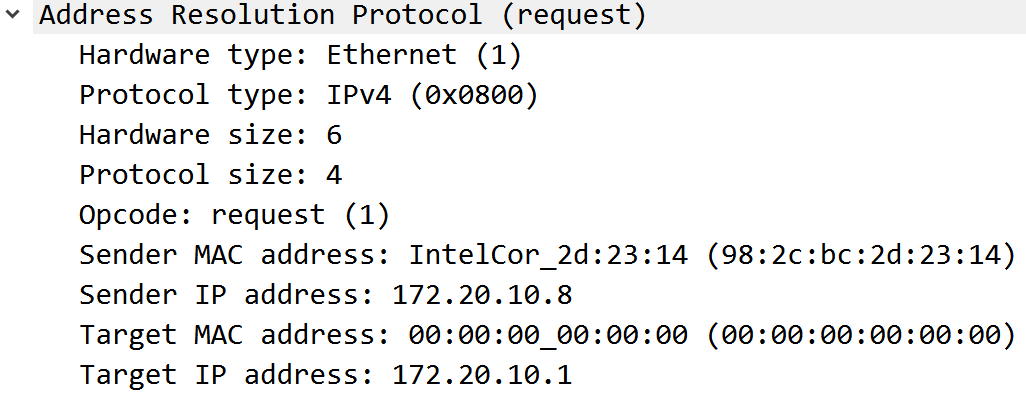
* 1. ARP probe：用于检测IP地址冲突。
     1. Sender MAC address：源主机的MAC地址
     2. Sender IP addres：为0，这是为了避免对其它主机的ARP缓存造成污染。当其它主机已经使用了候选的IP地址时，就不会影响到它的正常通信。
     3. Target MAC address：由于不知道候选IP地址是否被利用，因此就更没有IP地址对应的MAC地址，故填充为0
     4. Target IP address：候选IP地址，当有主机利用该IP地址时，就可以发回一个应答报文



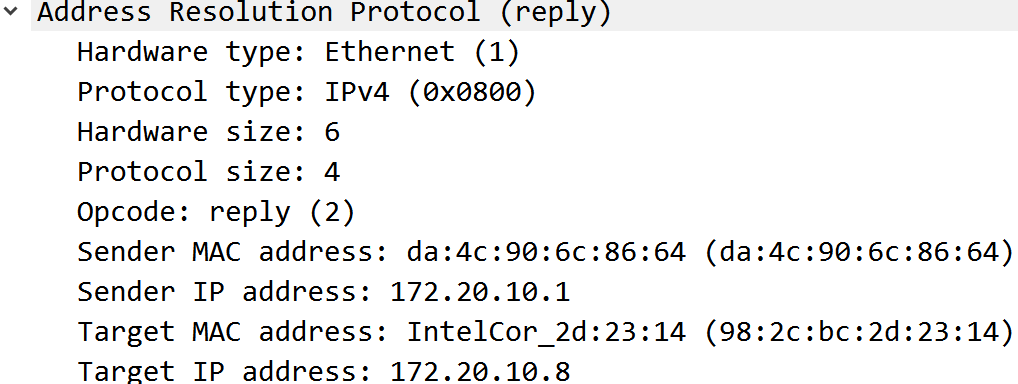
* 1. ARP Announcement：用于告诉所有在同一个LAN（或VLAN）的主机，本机要使用候选的IP地址了。
     1. Sender MAC address：源主机的MAC地址
     2. Sender IP addres：候选IP地址
     3. Target MAC address：为0，让同一个LAN（或VLAN）的主机都更新ARP缓存，将候选IP地址映射到发送者的MAC地址
     4. Target IP address：候选IP地址



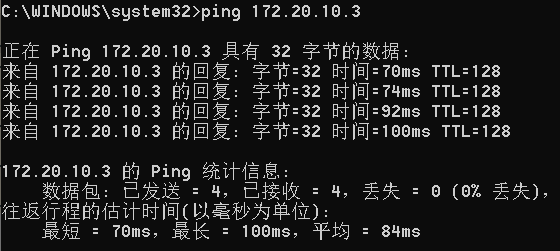
* 1. ARP request：用于获取默认网关的MAC地址，并将源主机的IP地址与MAC地址告诉默认网关，用于更新默认网关的ARP缓存表
     1. Sender MAC address：源主机的MAC地址
     2. Sender IP addres：源主机的IP地址
     3. Target MAC address：为0，不知道默认网关的MAC地址，故填充为0
     4. Target IP address：默认网关的IP地址



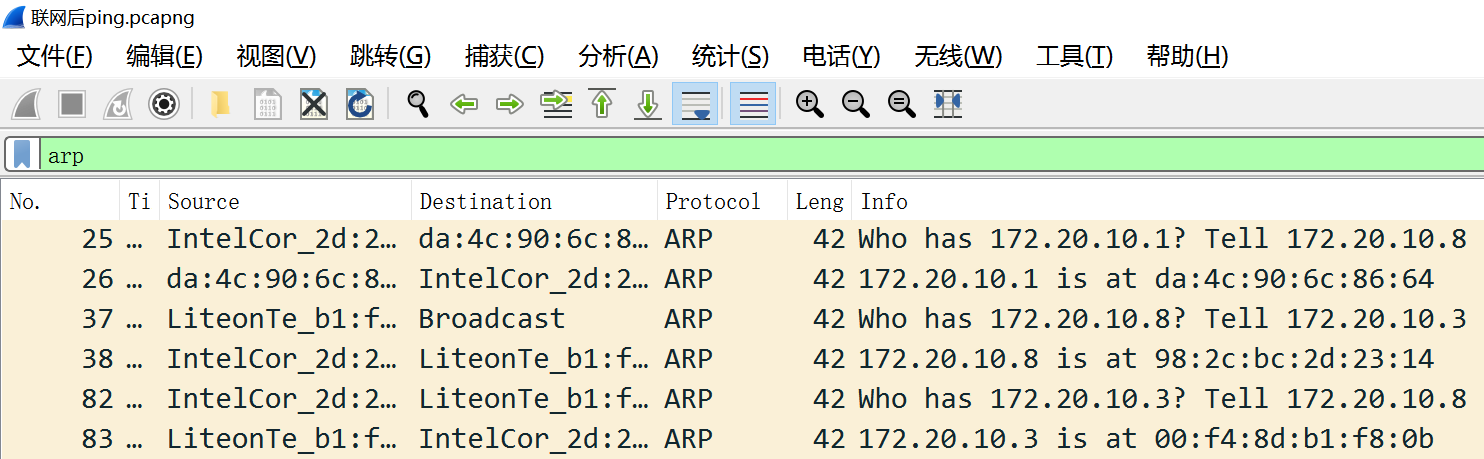
* 1. ARP reply：将默认网关的MAC地址返回给源主机，用于更新源主机的ARP缓存表
     1. Sender MAC address：默认网关的MAC地址
     2. Sender IP addres：默认网关的IP地址
     3. Target MAC address：源主机的MAC地址
     4. Target IP address：源主机的IP地址



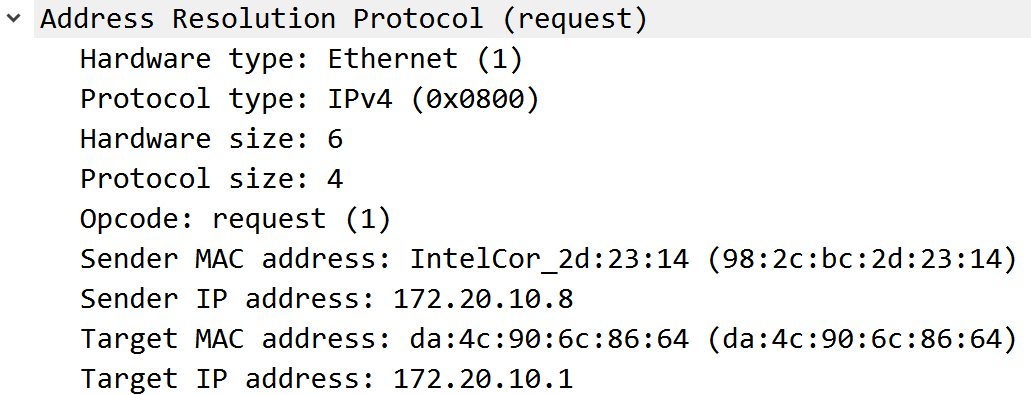
④从主机A上向主机B发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义

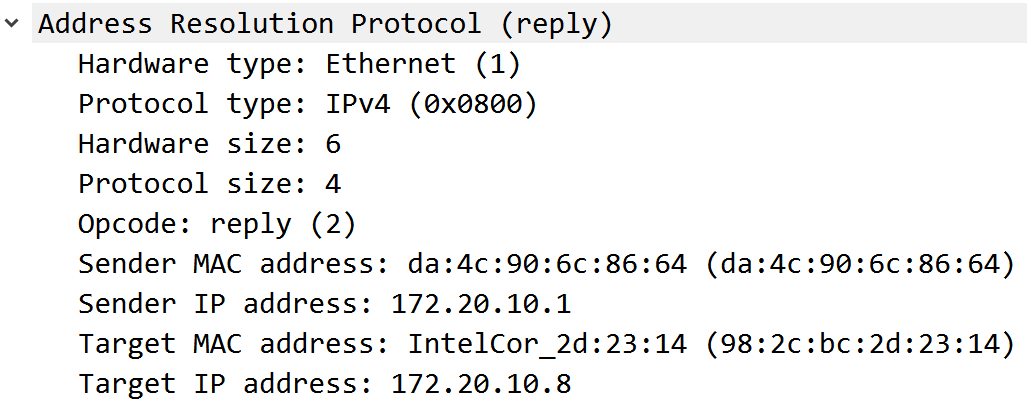


由下图可知，可以捕获ARP报文。可以看到，本主机（172.20.10.1）先向默认网关发送了ARP request报文，并收到了ARP reply。随后，目的主机（172.20.10.3）广播了一条ARP request报文，用于请求本主机的MAC地址，而本主机发送了一个ARP reply来回应。然后，本主机向目的主机发送了ARP request报文，目的主机又回应了一个ARP reply报文。



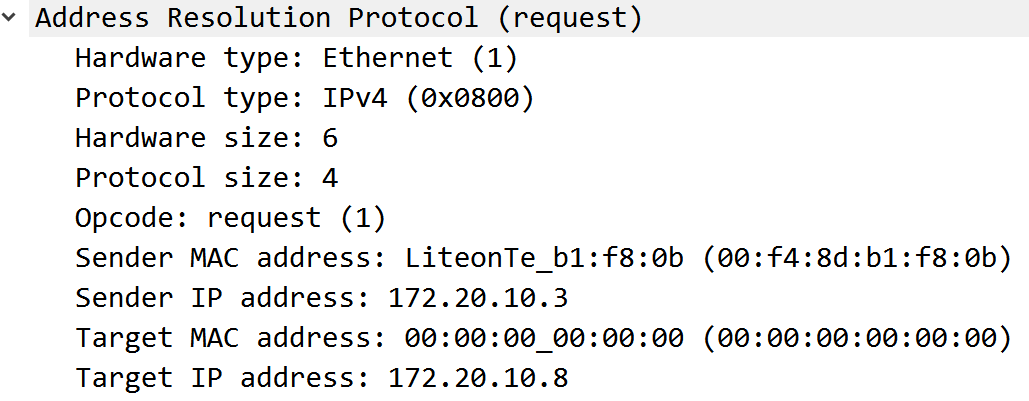
1. 对于第一对ARP请求与应答报文：本主机利用单播的方式向默认网关发送了一条ARP request，默认网关随后发送了一条单播的ARP reply。原因可能是这是ARP老化机制的一种，即单播轮询：每隔一段时间，本主机都需要向ARP缓存表中的其它主机发送单播请求，来询问其MAC地址与IP地址的映射关系是否还有效，这用于维护ARP缓存表的实时性。

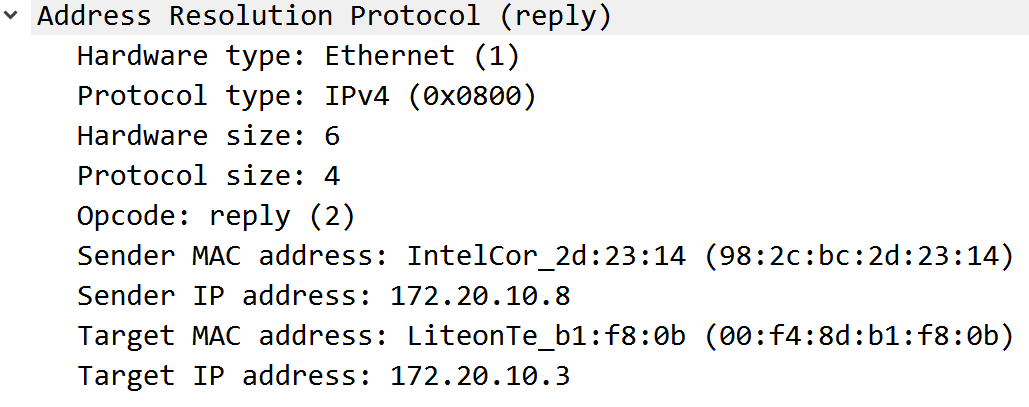




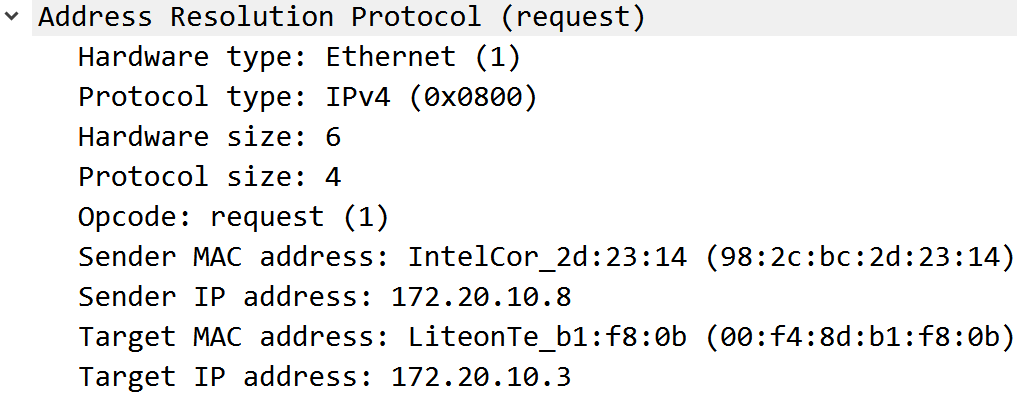
1. 对于第二对ARP请求与应答报文，目的主机（172.20.10.3）利用广播的方式发送了一条ARP request报文，用于请求本主机（172.20.10.8）对应的MAC地址，而本主机利用单播的方式向目的主机发送了一条ARP reply报文。原因是目的主机不知道本主机的MAC地址，而当目的主机需要向本主机发送数据报时又需要用到MAC地址，因此需要通过广播的方式让同一局域网中的主机都收到这个ARP request报文，来保证本主机能收到并发回MAC地址，这同时也能让本主机更新自己的ARP缓存表。在进行完这一轮请求与应答后，双方都知道了对方的IP--MAC映射，并将它写入到ARP缓存表中。

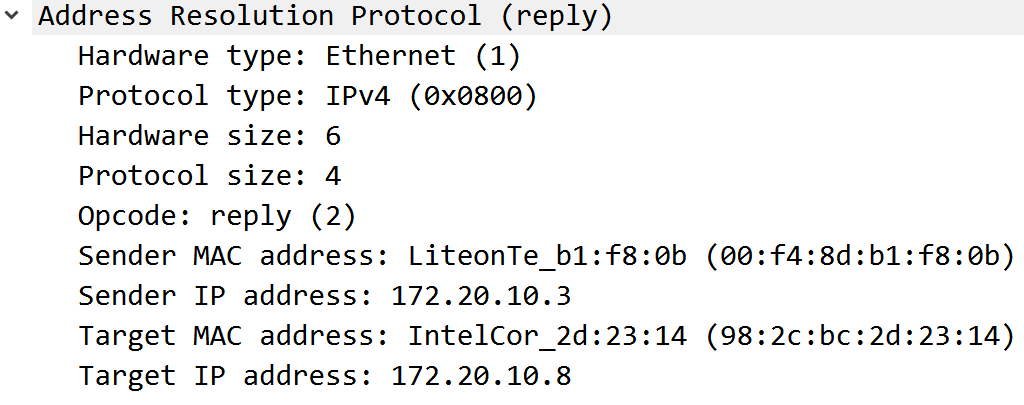
由于请求方不知道目的主机的MAC地址，因此Target MAC address填充0，当同一局域网主机的IP地址与Target IP address相同时，则会接收，否则就丢弃。





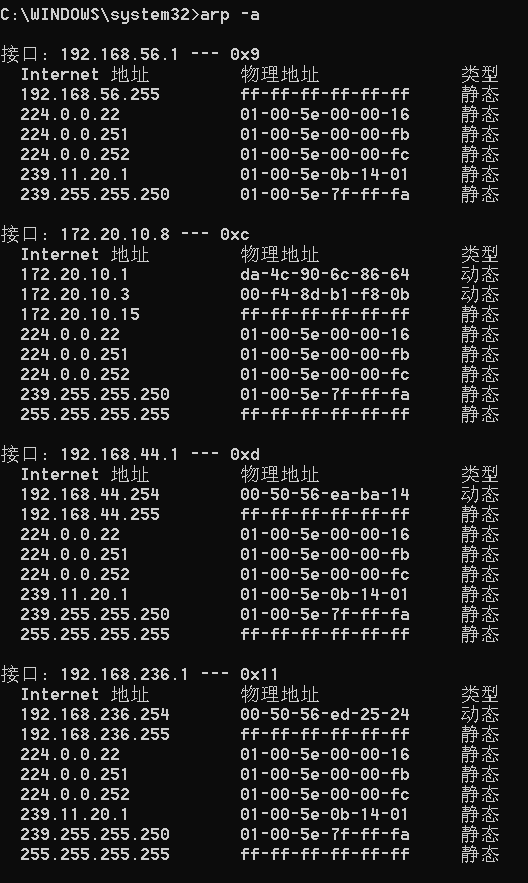
1. 对于第三对ARP请求与应答报文，本主机（172.20.10.8）向目的主机（172.20.10.3）单播了一条ARP request报文，随后目的主机又向本主机回应了一条ARP reply报文。这原因可能与第一对ARP请求与应答报文相同。此时，双方都已经拥有了对方的IP--MAC映射，每隔一段时间后都需要重新发送一次ARP请求来确保ARP缓存表的实时性与有效性。同时，采用单播的方式可以减少网络中数据包的数量，从而避免了拥塞的情况。





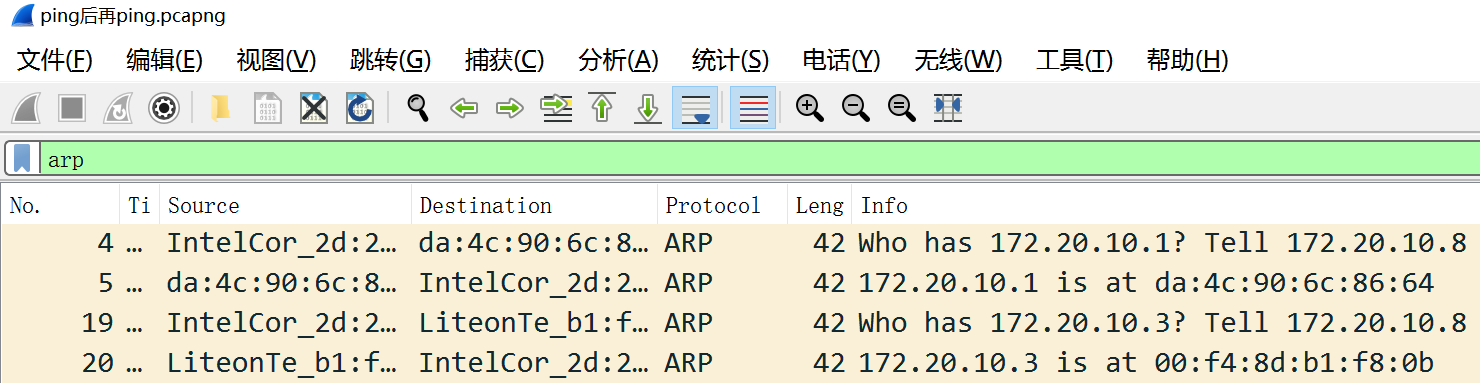
⑤通过arp - a 查看ARP表的更新情况，记录此时能否看到B对应的MAC地址

由下表所示，ARP缓存表中重新加入了目的主机（172.20.10.3）的IP--MAC映射



⑥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

由下图所示，此时仍然可以捕获到ARP报文，但是都是单播轮询维持本机ARP缓存表有效性的报文，而没有询问对方MAC地址的广播ARP报文。说明此时本机与目的主机都在ARP缓存表中存有了对方的IP--MAC映射关系。

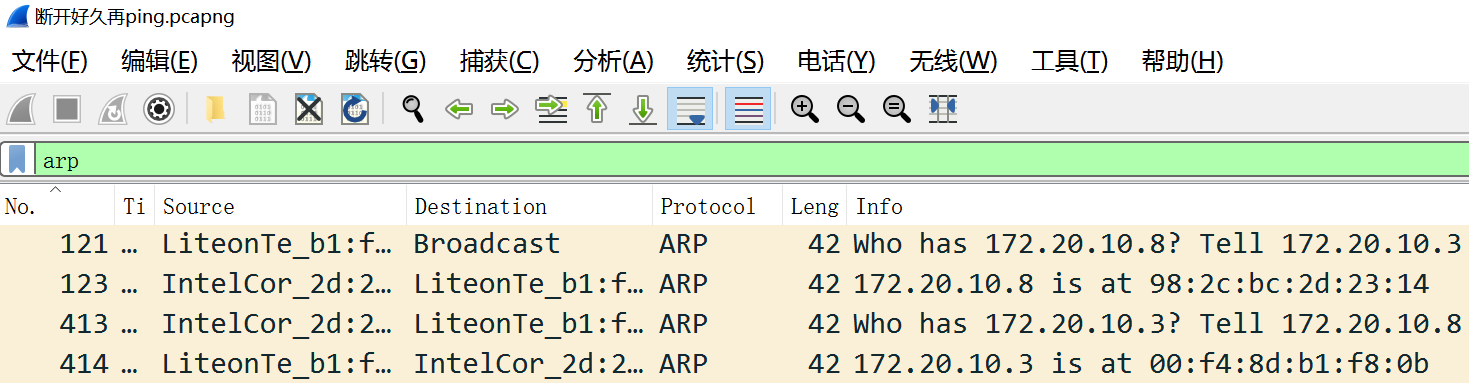


⑦主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文

由下图所示，还可以收到ARP报文。

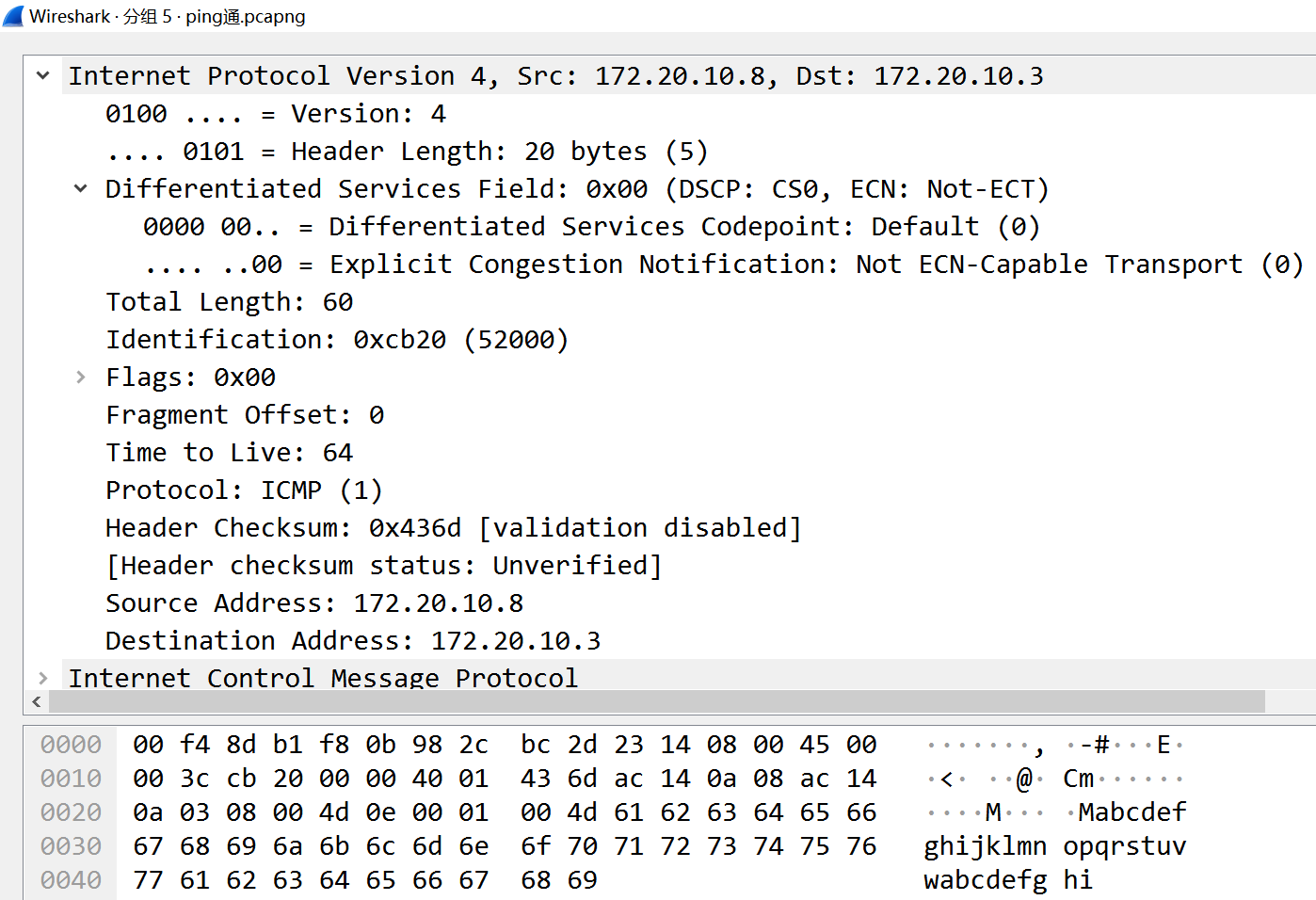
对于第一对ARP请求与应答报文，原因是断开数据通信的时间过长，超过了映射地址项目的生存时间，故目的主机中将本主机的IP--MAC地址映射删除。当目的主机需要向本主机发送数据报时，无法在ARP缓存表中找到本主机的IP--MAC地址映射，故需要重新在局域网中发送一条广播ARP request请求报文来获取本主机的MAC地址，并将自己的IP地址及MAC地址告诉本主机。而本主机在收到ARP request报文后再做出单播的应答报文。

对于第二对ARP请求与应答报文，是与第一对报文间隔了一段时间后才发出的，是ARP的单播轮询方式，用于保证双方ARP缓存表的IP--MAC地址映射的实时性。



1. **IP协议分析**

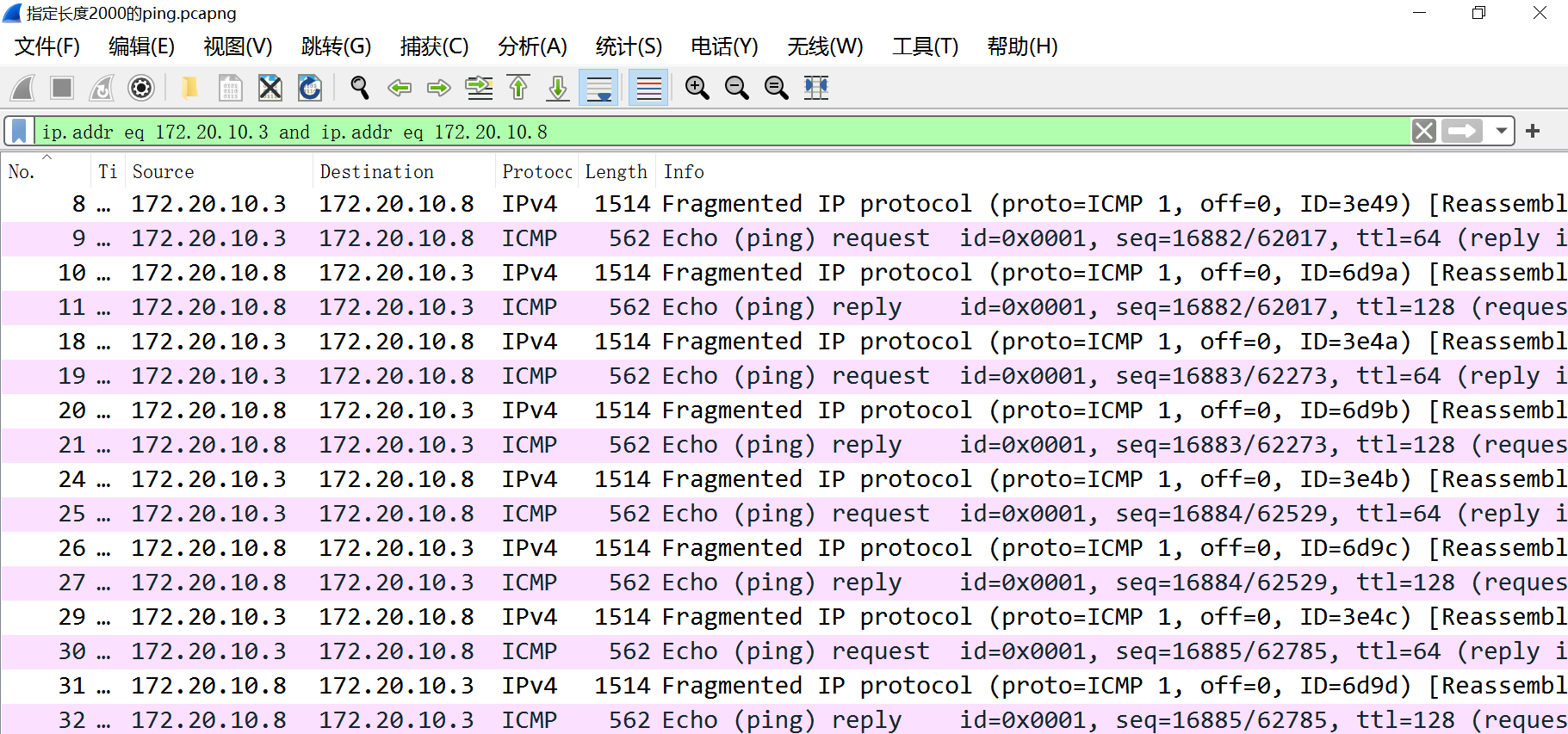
①从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较



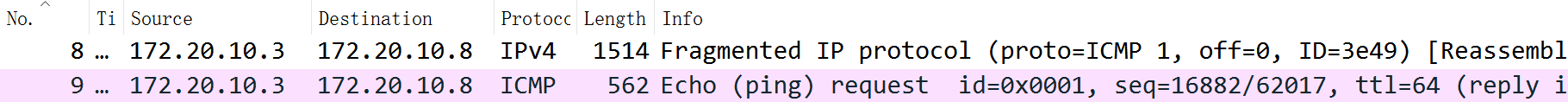
1. Version：占4位，IP协议的版本号。只有版本号相同才可以获取数据
2. Header Length：占4位，首部长度。首部长度一个单位表示4字节。可表示的最小值是5（0101），即5\*4=20字节；最大值是15个单位（1111），即15\*4=60字节。
3. Differentiated Services：占8位，区分服务。IPV4一般情况下不使用.
4. Total Length：占16位，总长度（首部长度+数据长度）。IP数据报最大长度为2^16-1=65535字节（一般不会直接被数据链路层封装，需要分片后封装）。总长度不可以超过最大传送单元MTU（即MAC帧中数据字段的最大长度）
5. Identification：占16位，标识。在分片时需要用来产生IP数据报的标识，是一个计数器，而不是序号。
6. Flags：占3位，标志，只有两位有意义。
   1. 最低位MF（More Fragment）：1表示后面还有分片；0表示最后一个分片
   2. 中间位DF（Don't Fragment）：1表示不能分片；0表示分片后的分组允许继续分片
7. Fragment Offset：占13位，片偏移。表示较长的分组在分片后，某片在原分组中的相对位置。以8个字节为偏移单位。
8. Time To Live：占8位，生存时间。单位不是秒，是数据报在网络中可通过的路由器数的最大值。当TTL=0时，如果报文还没有被接收，那么会利用ICMP协议发送错误信息，并将该数据报丢弃。
9. Protocol：占8位，协议。封装的上一层的协议，以便接收方将数据交给对应的协议进行处理。
10. Header Checksum：占16位，首部校验和。路由器只检验数据部分，采用的是反码算数运算法，而不是采用CRC检验码。
11. Source Address：占4字节，源地址。
12. Destination Address：占4字节，目的地址。

②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

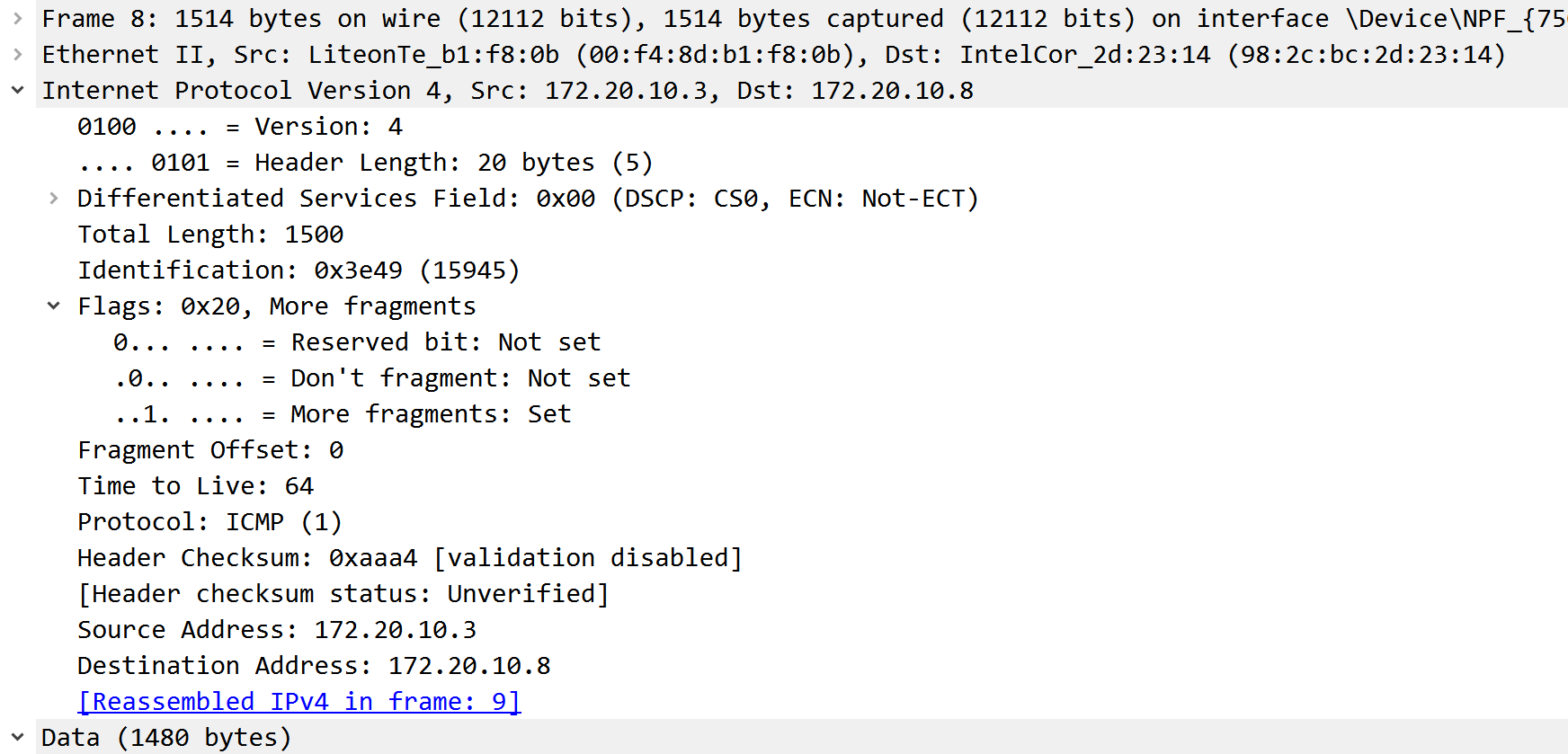
利用Wireshark捕获到的数据包如下：



对于第一次ping request，有两个分片，如下所示：

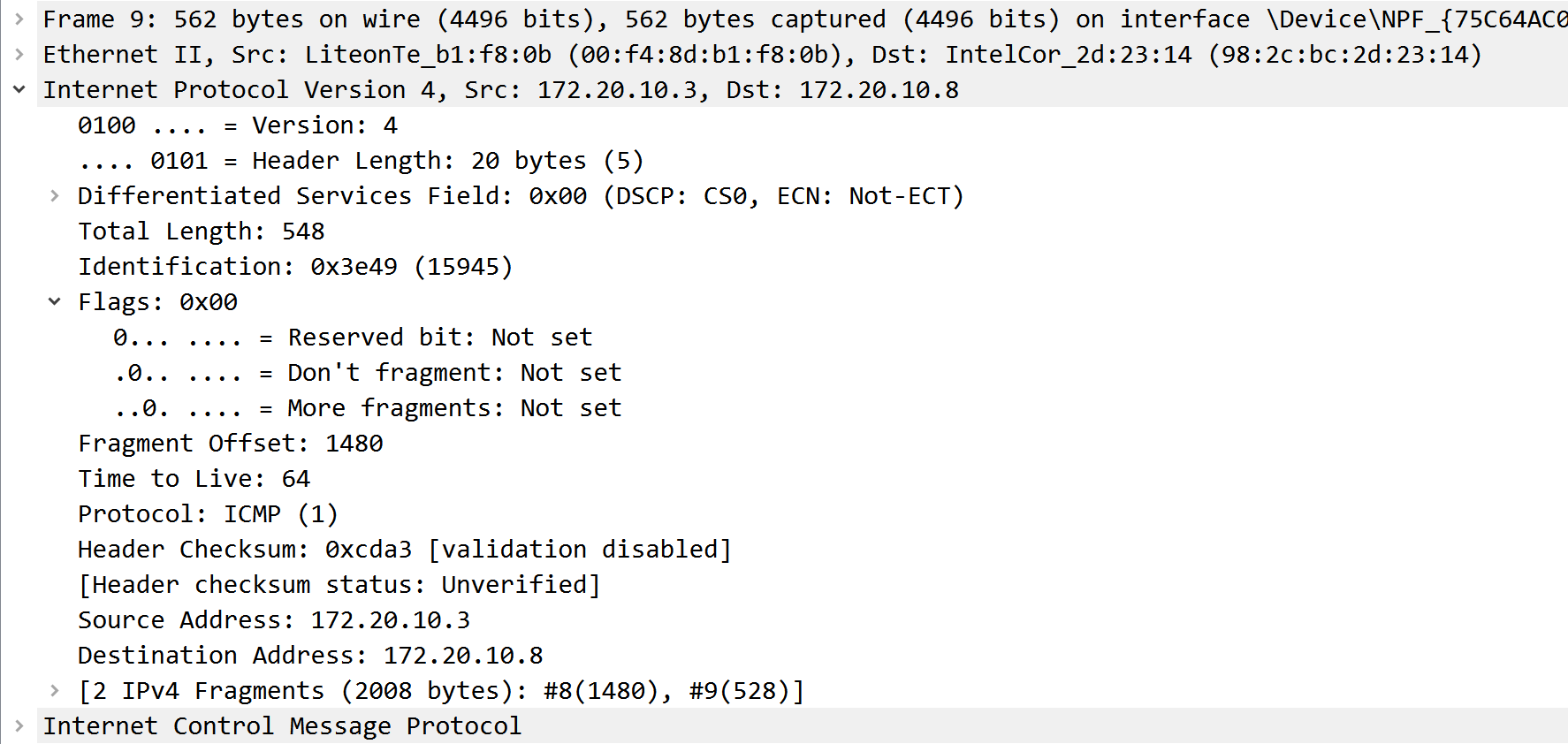


第一个分片如下图所示：



1. 数据帧长度：1514=IP数据报总长度：1500+以太网帧头部：14。实际上该MAC帧长度应该为1518字节（还有4字节的FCS），但是这4字节没有统计，只显示了关键字节
2. IP数据报首部长度：20（Header Length）
3. IP数据报总长度：1500（Total Length）
4. 标志：DF=0，可以继续分片；MF=1，后面还有分片
5. 在9号分组重组
6. 第一个分组数据部分有1480个字节，并且不含ICMP数据

第二个分片如下图所示：





1. 数据帧长度：562字节
2. IP数据报首部长度：20字节
3. IP数据报总长度：548=IP head:20+ICMP head:8+DATA:520
4. 标志：DF=0，可以继续分片；MF=0，这是最后一个分片
5. 两次分组传输的数据长度：2000字节
6. 为什么8号数据+9号数据=1480+528=2008，多了8字节？答：因为ICMP的首部还有8个字节

**分析IP数据报分片和重组过程：**

IP数据报分片：

由于需要执行ping -l 2000命令，即需要传送2000字节大小的数据包。由于2000字节已经超过了数据链路层的最大传输单元：1500字节，因此需要进行分片。

对于第一个分片：由于数据链路层一次最多能传输1500字节的数据，同时还要包括20字节的IP数据报首部，因此在第一个分组中只能传送1500-20=1480字节的数据。而第一个分片的MAC帧长度为1518字节=MAC帧首部:14+IP数据报首部:20+数据:1480+FCS:4。

对于第二个分片：在传送完1480字节的数据后，还剩下2000-1480=520字节的数据需要传送，同时还要注意加上8字节的ICMP首部。因此，第二个分片的MAC帧长度为566字节=MAC帧首部:14+IP数据报首部:20+ICMP首部:8+数据:520+FCS:4。

IP数据报分片步骤：

IP数据报在分片之前，其标志位为0，片偏移为0。

1. 检查DF标志位，若为1则表示不能分片，该数据报将被丢弃，并返回一个ICMP错误给发送方；若为0则表示可以分片
2. 基于MTU值，将数据字段分成多个部分。除了最后的数据部分外，所有新建的数据字段长度必须为8字节的倍数，否则将不能通过片偏移来定位分片的相对位置
3. 分好的数据部分都被放入一个IP数据报中，这些数据报的标识位相同，表示是由同一个IP数据报分片而来，并有片偏移来标识该片在原分组中的相对位置。最后一个分片的MF位为0，其余分片MF位为1
4. 对于可选字段，其选项类型的高位字节决定了这个信息是被复制到所有分片数据报还是只复制到第一个数据报
5. 设置新的数据报的首部长度及总长度
6. 重新计算报文的首部校验和

IP数据报重组：

接收方可以根据IP数据报的标识位来判断这些分片是不是来自同一个IP报文，具有同一个标识位的分片将会重组在一起。同时，接收方还需要根据片偏移来判断某个分片相对整个包的位置。其次，还需要根据MF标志位来判断是否还有新的分片。利用这些信息，接收方就能对IP数据报进行重组。

IP数据报重组步骤：

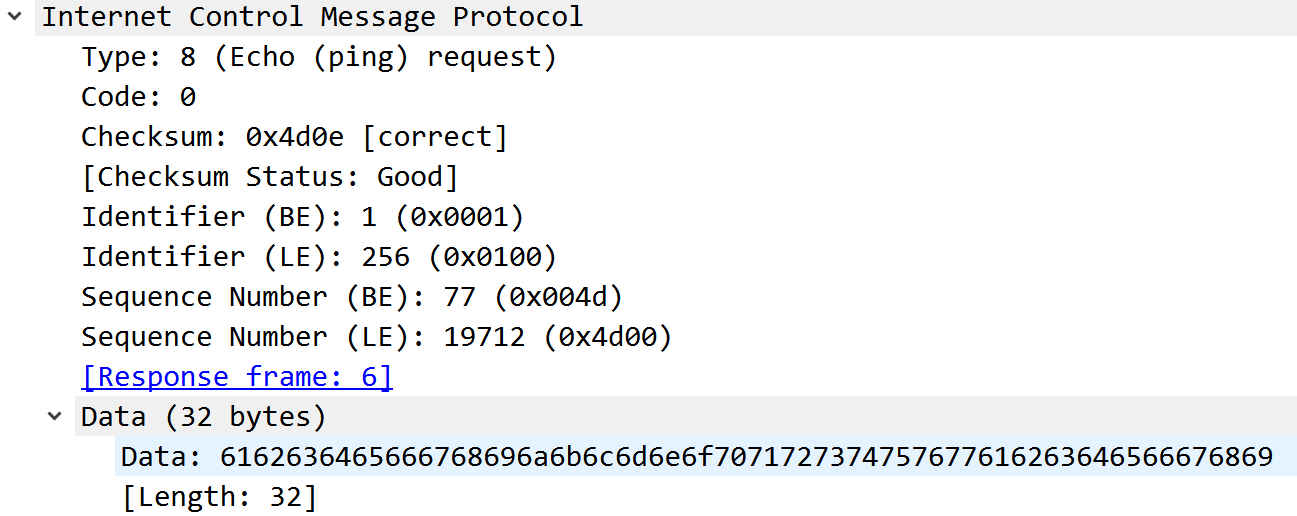
1. 接收方在收到第一个分片时就分配一个存储缓冲区，并启动一个计时器
2. 定位某一个数据报所属的分组
3. 在所属分组的位置插入该分片
4. 判断数据报的所有分片是否被全部接收
5. 若在重组完成前计时器移除，则删除该数据报的所有内容
6. **ICMP协议分析**

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。

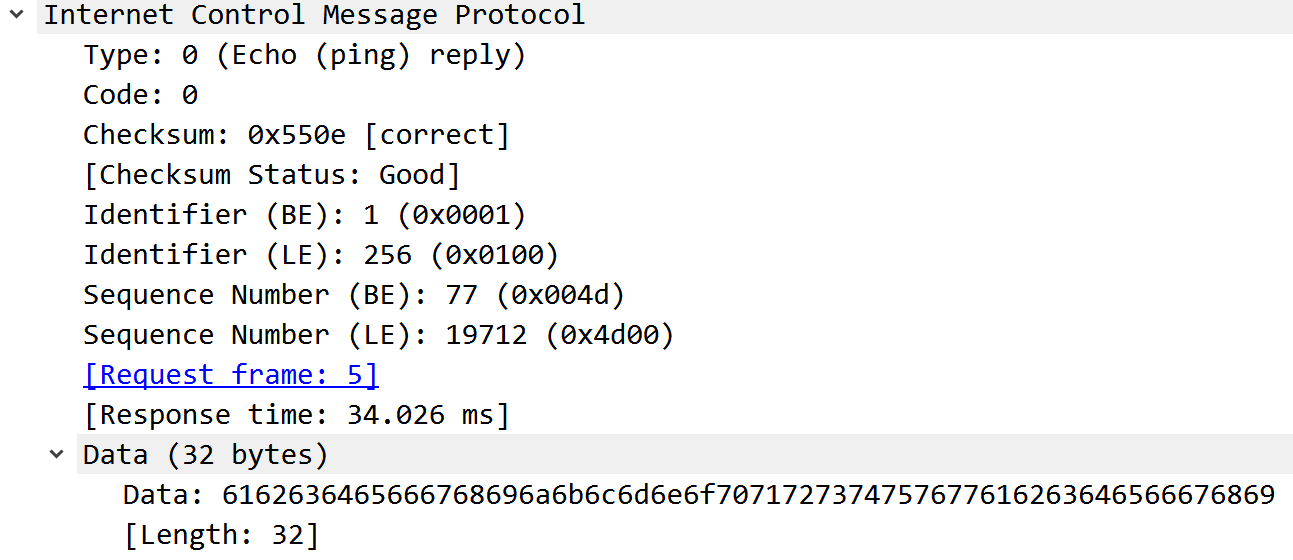
ICMP数据报格式分析：

1. **ping通的报文**

请求报文：



响应报文：

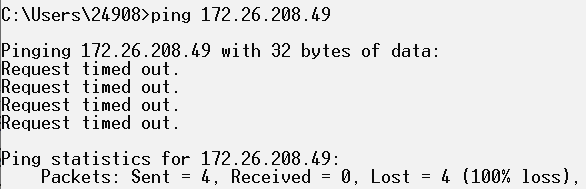


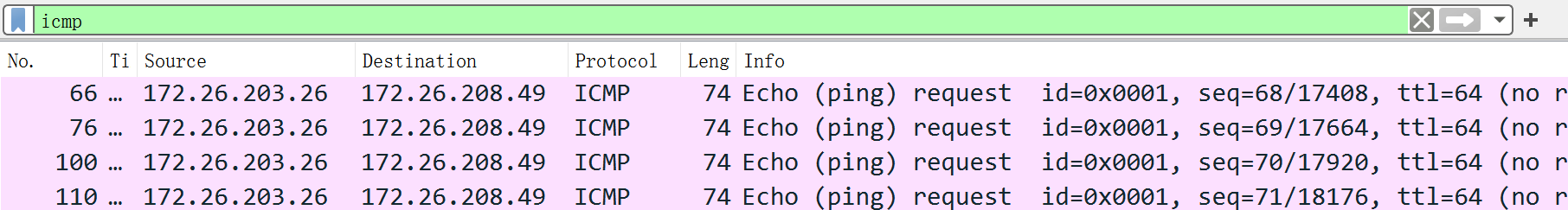
* 1. 类型(Type)：占8位，表示生成的错误报文。
  2. 代码(Code)：占8位，进一步地限定生成的ICMP报文。该字段用来查找产生错误的原因。
  3. 校验和(CheckSum)：占16位，对整个报文（首部和数据）按二进制反码运算求校验和。
  4. ID值与序列号(Identifier, Sequence Number)：占4字节，该4字节取决于ICMP的报文类型。
  5. 数据部分(Data)：长度取决于类型和代码域部分。

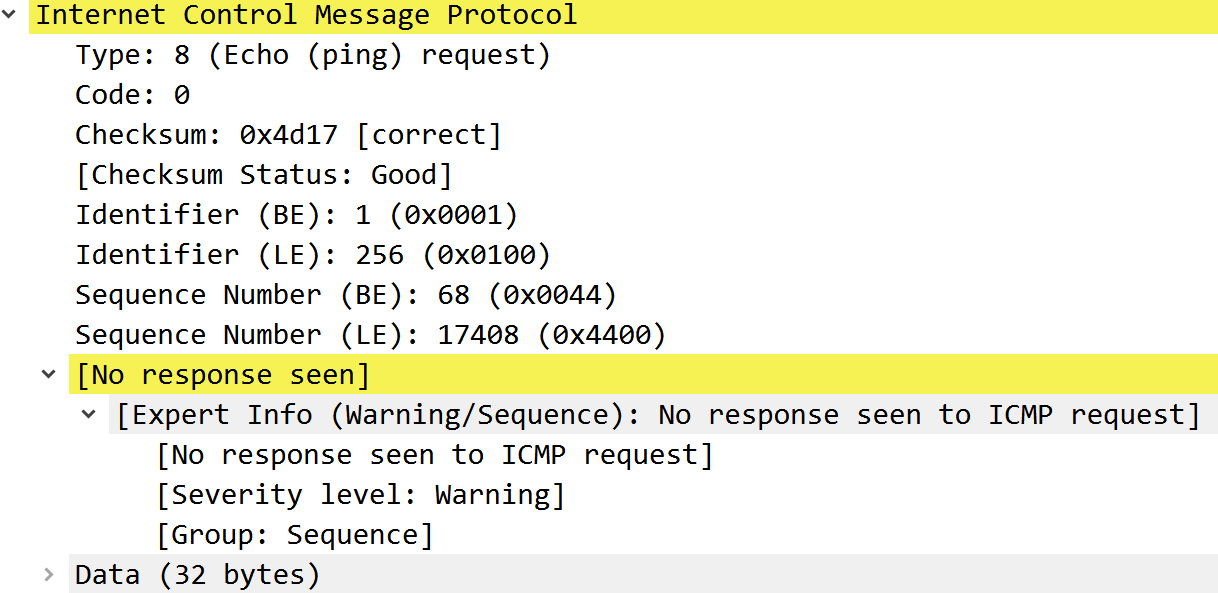
1. **分析返回的差错信息**
   1. 对方关机/没有连接网络/网络连接出现问题/防火墙禁ping：request time out

差错出现原因：路由表中有目的主机的路由，但是因为其他原因不可达

以下就是目的主机关机的情况：Wireshark只能捕获request数据包，但是没有reply







* 1. 局域网使用DHCP动态分配IP地址时出现故障或失败/子网掩码手动设置/路由表返回错误信息

差错出现原因：路由表中没有目的主机的路由

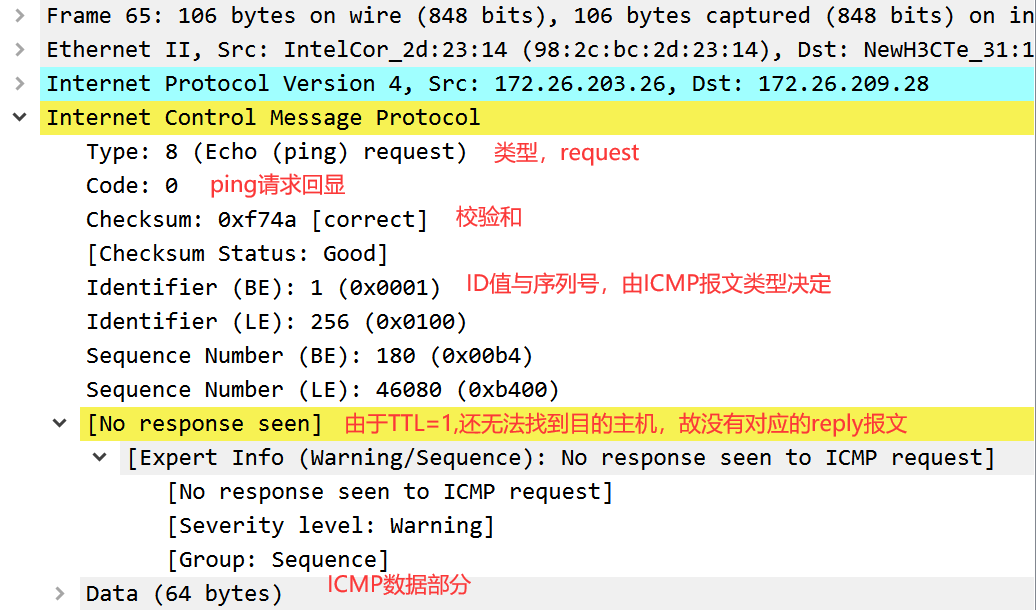
②使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8 request,type=0 reply,type=11连接超时）。分析tracert工作原理。

1. **分析不同类型的ICMP响应数据包格式**

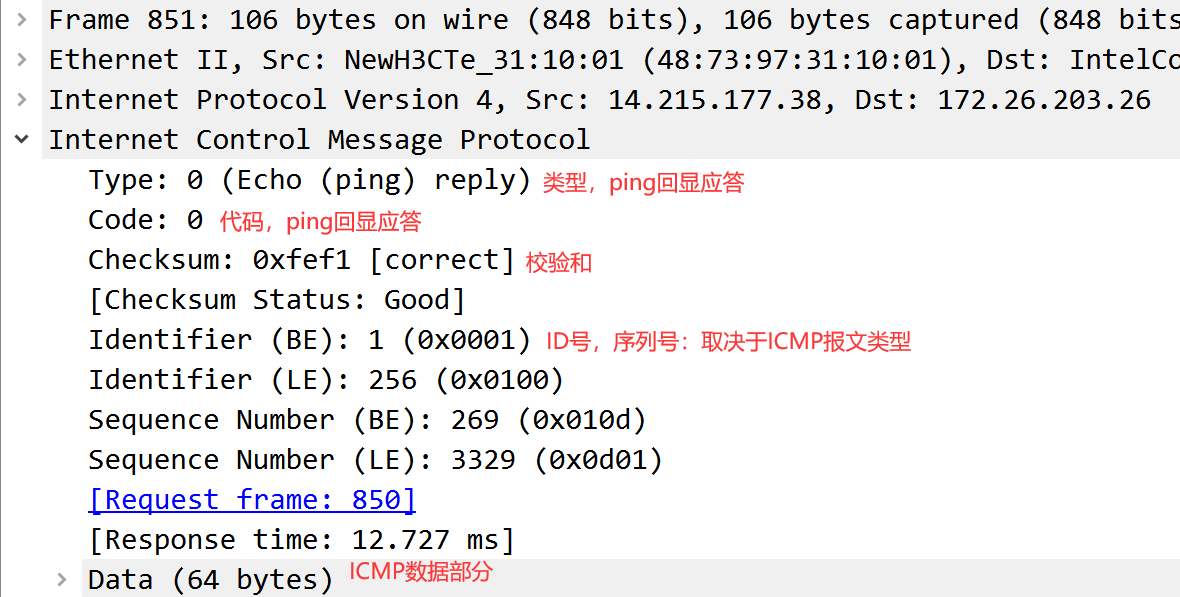
**由于request与reply类型的报文前文以分析过，故不再赘述，只分析传输期间生存时间为0的报文**

* 1. **tracert www.baidu.com**

1. type=8，request



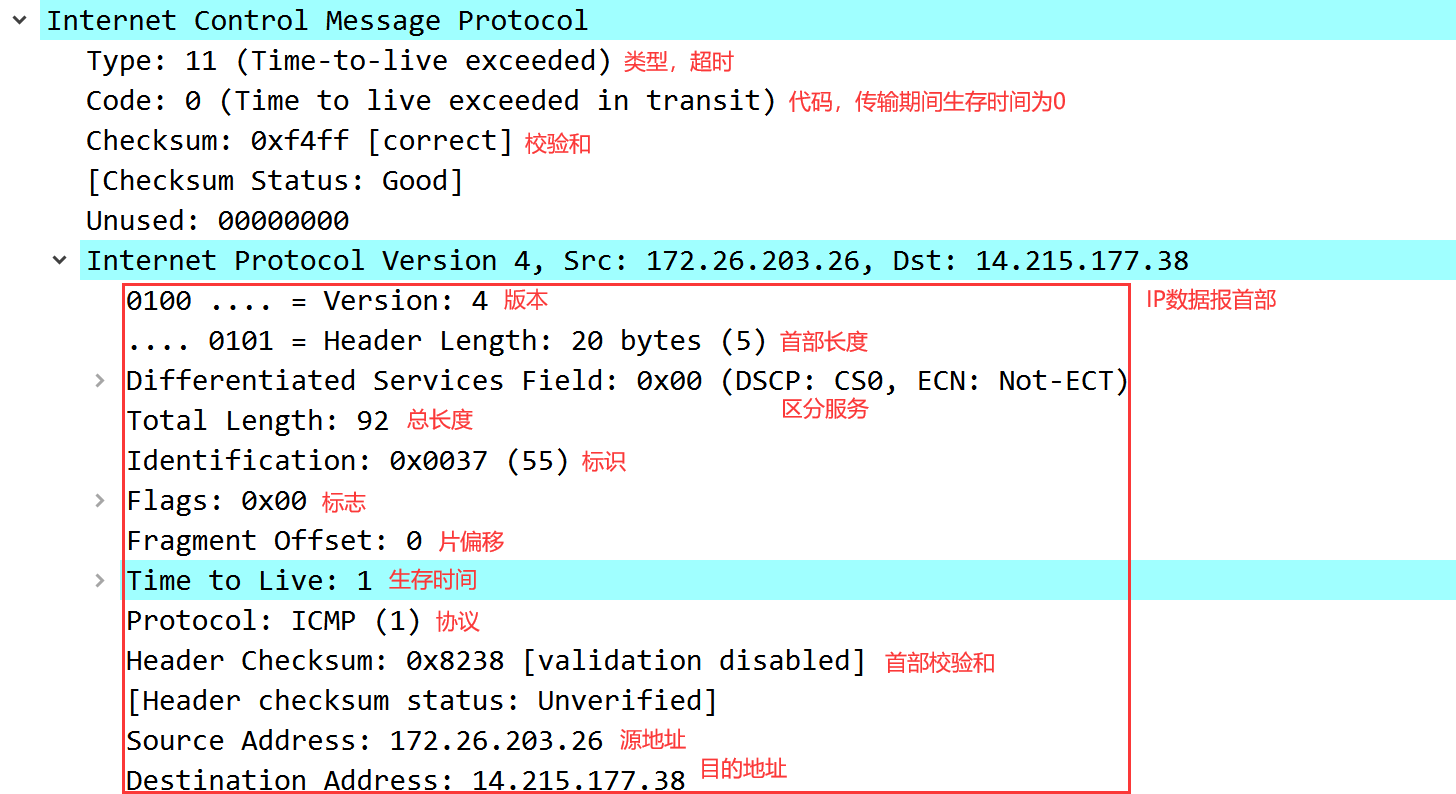
1. type=0，reply



1. type=11，time-to-live exceeded

由下图可以看出，ICMP的差错报告报文的格式为：ICMP差错报告报文的前8个字节+收到的需要进行差错报告的IP数据包的首部+该IP数据报数据字段的前8个字节

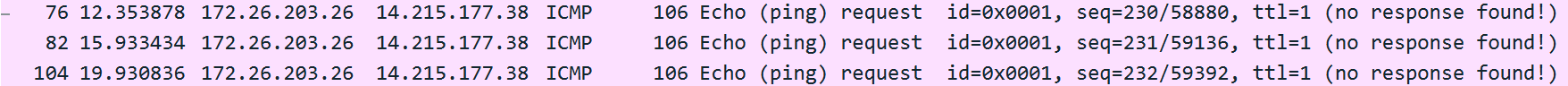
而本次实验收到的IP数据报数据字段的前8个字节就是需要进行差错报告的ICMP报文的前8个字节。





**2 . 分析tracert的工作原理**

1. 从源地址发出三个ICMP请求回显（ICMP Echo Request）数据包到目的地址，并将TTL值设置为1。由于此时并不能达到目的地址，因此该request不会有对应的reply。

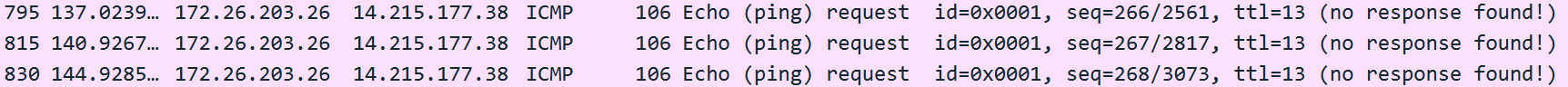


1. 当该数据报到达经过的第一个路由器时，TTL数会减1变为0，故该路由器会丢弃该数据报，并向源点发送时间超过报文。

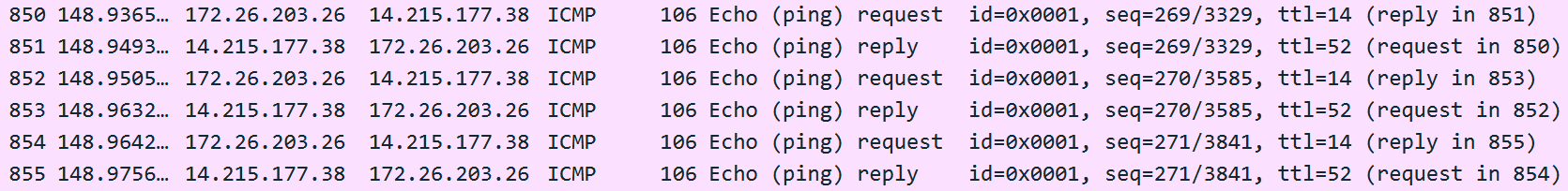




1. 重复以上两个步骤，同时每次源地址发送的ICMP请求的TTL值都加1。本次实验直到TTL=13时还报文还不能达到目的主机



1. 当TTL=14时，目的地址收到了ICMP数据报，并返回ICMP的回应答复（ICMP Echo Reply），当源地址收到应答包后，就停止tracert。



1. **思考题**
2. 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？

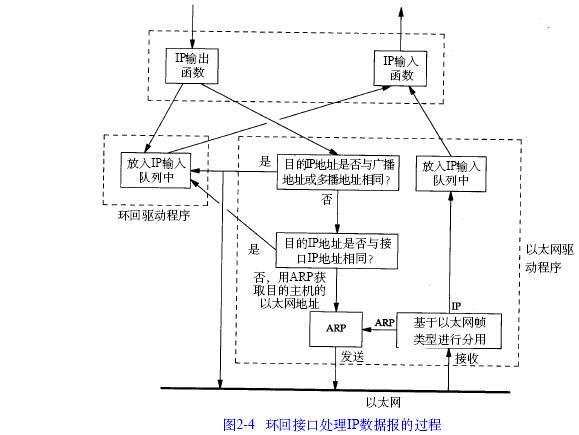
答：ARP缓存表中的每一个IP--MAC地址映射都有一定的生存时间，只要目的主机的IP--MAC地址映射还在生存时间内，源主机就不需要通过广播ARP request的方式来获取目的主机IP地址对应的MAC地址。因此有时候会捕获不到ARP报文。而当ARP缓存表中没有目的主机的IP--MAC地址映射或该地址映射失效是，就能捕获到ARP的广播报文。

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：Wireshark只能抓取经过网卡的流量

1. ping 127.0.0.1不能捕获到ICMP协议报文，因为ping 127.0.0.1时直接将数据包放入IP输入队列中，数据包是不经过网卡的，因此可以用来检查TCP/IP协议栈是否正常

2.ping 本机IP地址也不可以捕获到ICMP协议报文，因为当目的IP地址与本地IP地址相同时，会将数据包直接放入IP输入队列中，而不需要经过网卡



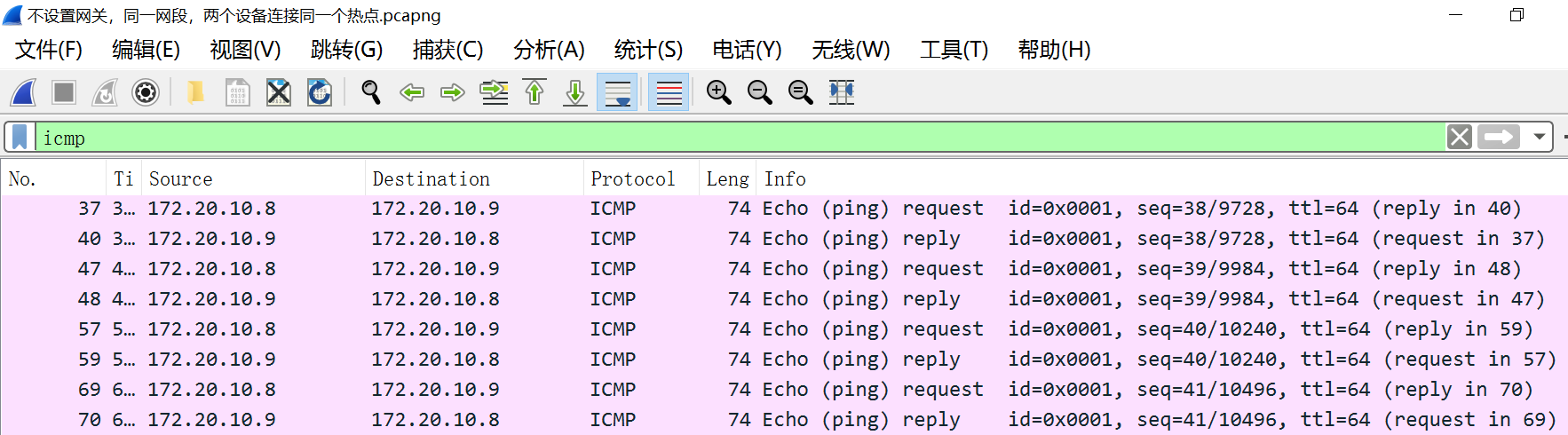
1. 在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

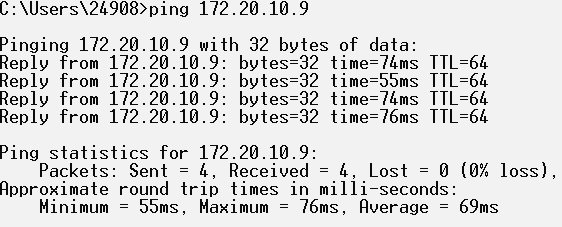
答：

* 1. 返回Request timed out的原因为：有目的主机路由，但是由于其他原因不可达：
     1. 防火墙拦截
     2. 跨网段IP地址冲突
     3. 没有回程路由，同网段可能是子网掩码错误
     4. 回程路由指向其它的IP地址
  2. 返回Destination Host Unreachable的原因为：没有目的主机路由，即对方主机不存在或没有建立连接：
     1. 局域网使用DHCP动态分配IP地址时，DHCP出现故障或失败
     2. 子网掩码手动设置错误
     3. 路由表返回错误信息

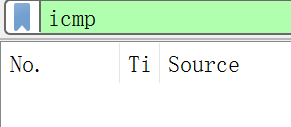
1. 请通过实验**验证**：

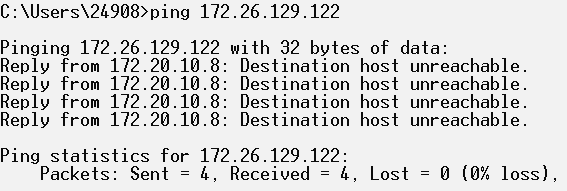
主机如果不设置“网关”，同一网段内的主机可以相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。



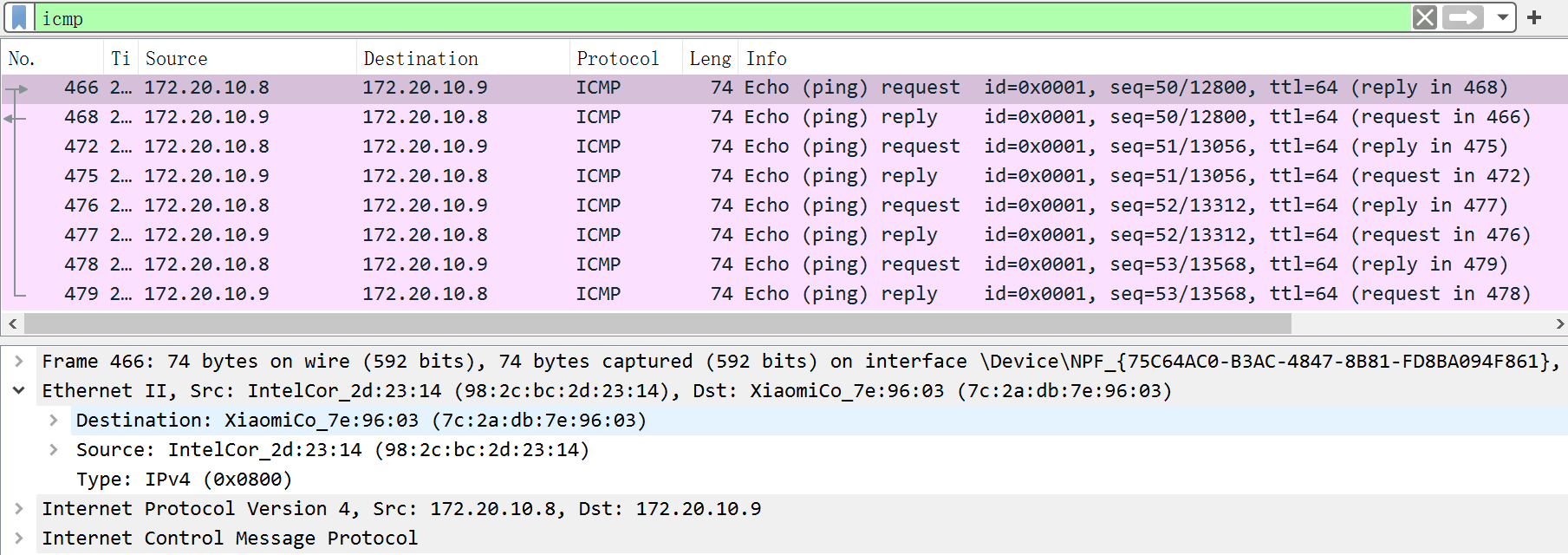


不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。





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）。

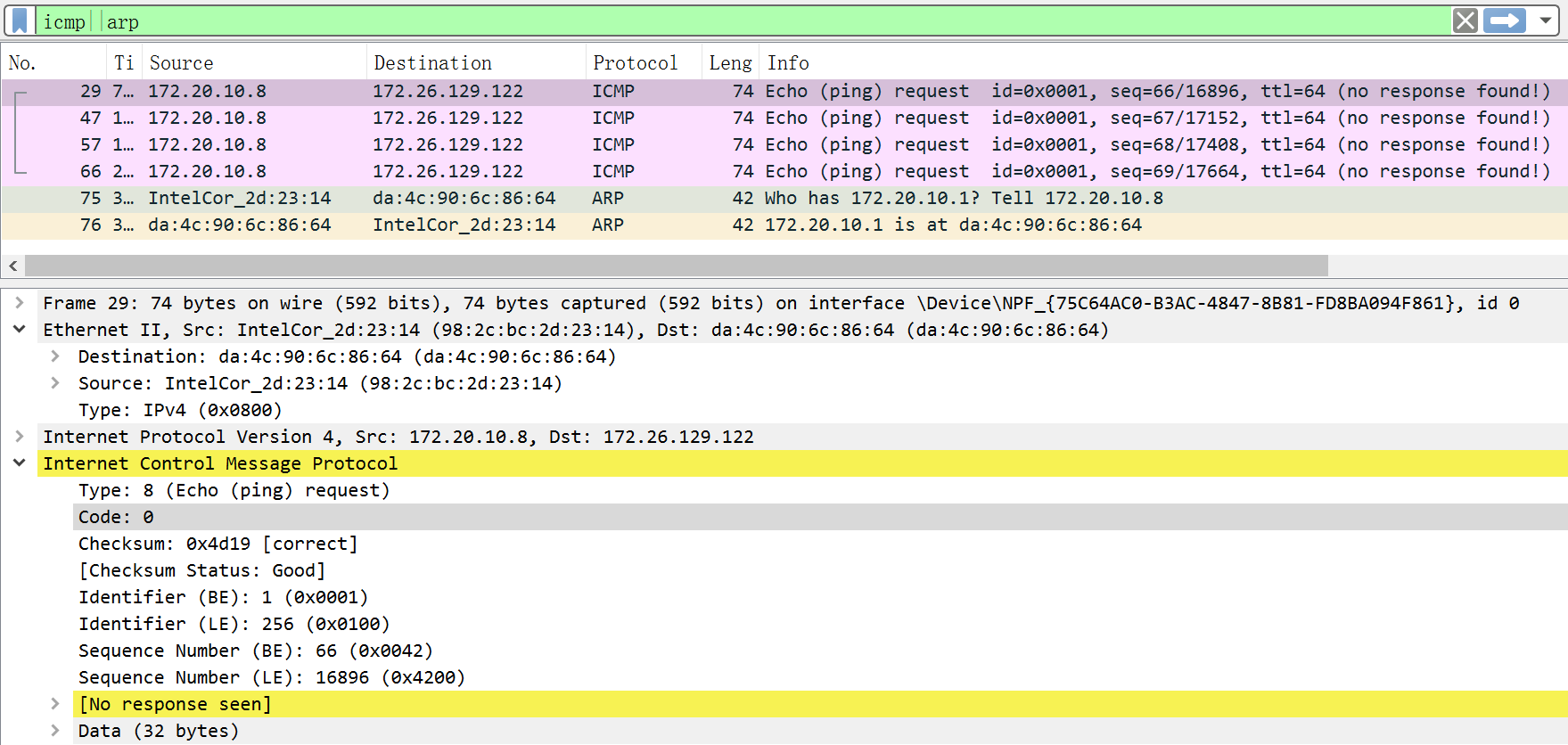


图 1主机间不能通信

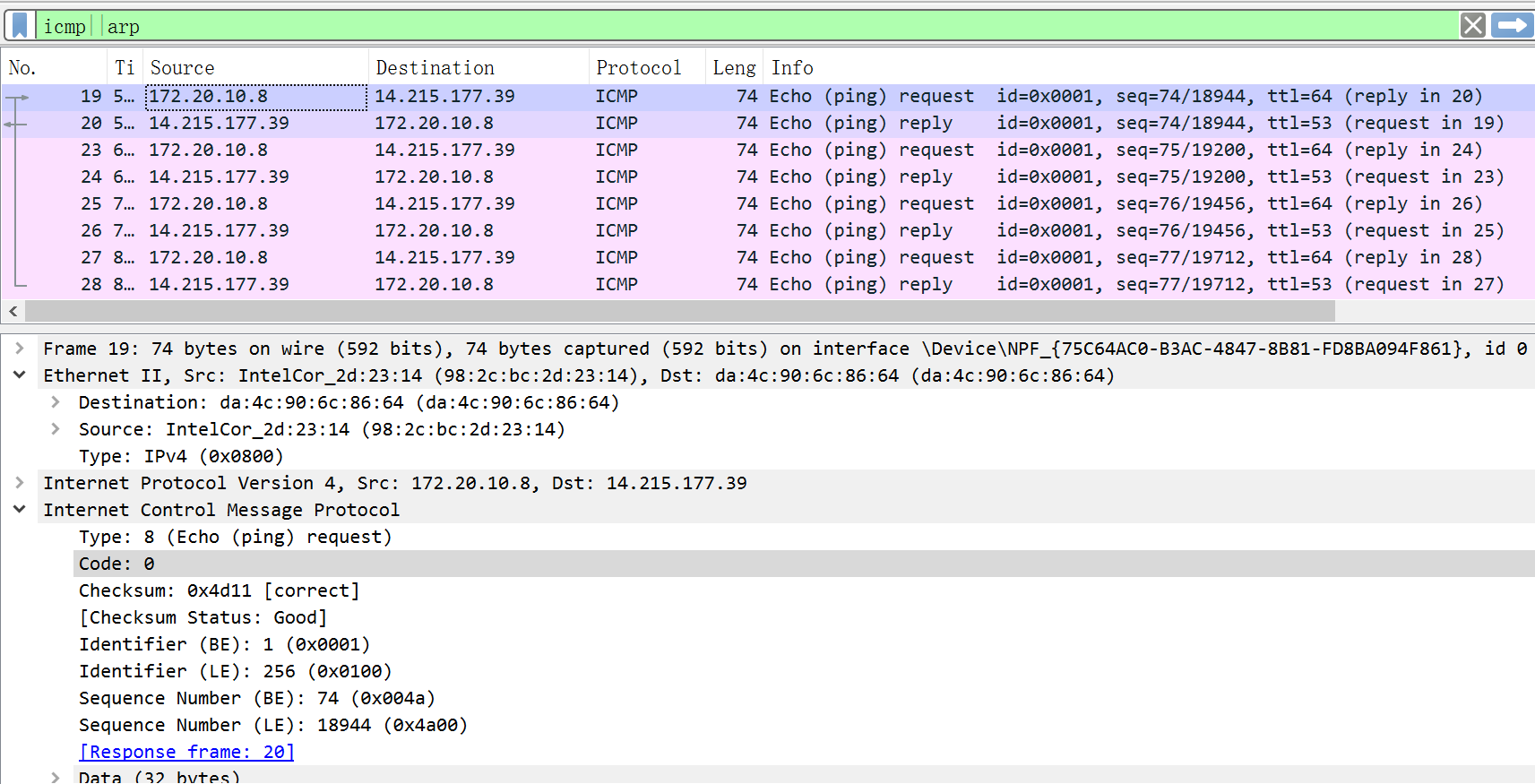


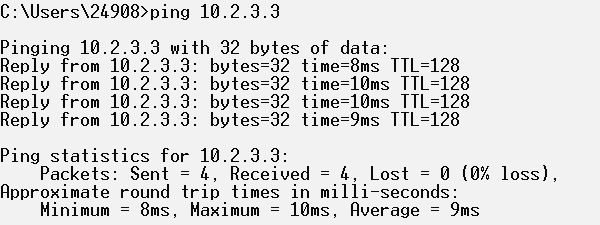
图 2主机之间可以通信

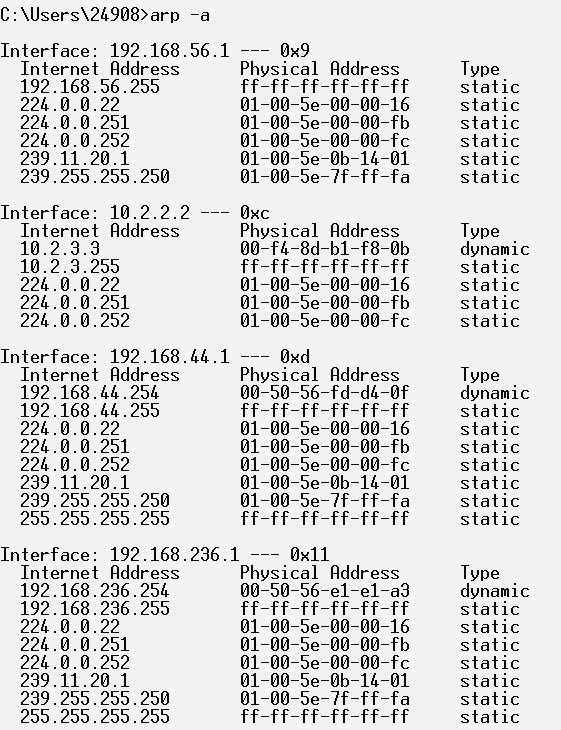
1. 通过下面实验**理解网关**

**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。**

答：当A ping B时，需要将B的IP地址和A的子网掩码进行与运算，并将计算的结果作为B所在的网段，再将IP数据报发送到该网段。经计算得：IPB:10.2.3.3&A子网掩码:255.255.254.0=10.2.2.0，则主机A会将IP数据报发送到网段10.2.2.0中，由于主机B也在该网段中，因此可以收到该request报文。同时，当B需要将其reply报文发送给A时，需要将IPA:10.2.2.2&B子网掩码:255.255.254.0=10.2.2.0，并将reply报文发送到该网段中。由于主机A就在该网段中，因此也可以收到reply报文。故主机A和主机B是连通的。

通过观察ARP缓存表也可以观察得出主机A中关于主机B的IP--MAC映射是正确的



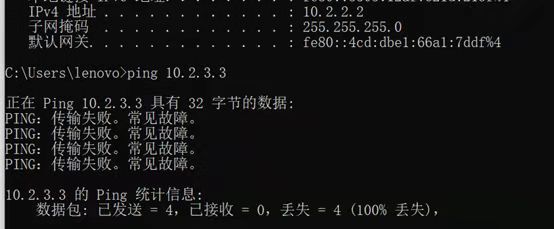


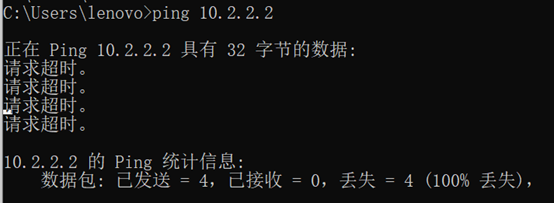
6781883775c01d8f275221b9c316bd6

**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。**

答：当A ping B时，需要将B的IP地址和A的子网掩码进行与运算，并将计算的结果作为B所在的网段，再将IP数据报发送到该网段。经计算得：IPB:10.2.3.3&A子网掩码:255.255.255.0=10.2.3.0，则主机A需要将IP数据报发送到网段10.2.3.0中。由于主机A所在的网段为10.2.2.0，将数据报发送到网段10.2.3.0中需要经过路由器。由于没有设置网关，故数据报无法转发到网段10.2.3.0中，因此Wireshark只能捕获到4个request报文而收不到reply报文，从而产生传输失败的故障。

当B ping A时，需要将A的IP地址和B的子网掩码进行与运算，并将计算结果作为A所在的网段，再将IP数据报发送到该网段中。经计算得：IPA:10.2.2.2&B子网掩码:255.255.254.0=10.2.2.0，则主机B需要将IP数据报发送到网段10.2.2.0中，由于主机B就在该网段中，因此B向A发送request报文A可以收到。而当A收到request报文后，就需要向B发送reply报文。但是由上文分析，A的报文是发送不到B的，因此应当会出现请求超时的错误。

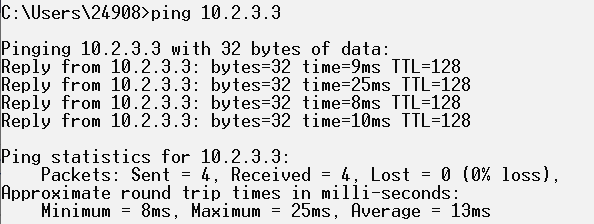


****

**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。**

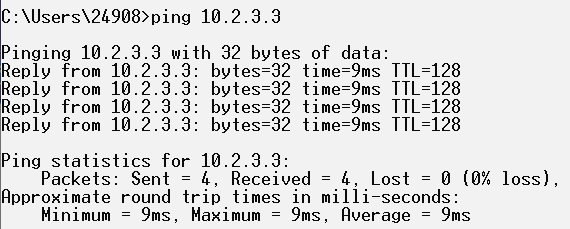
1. **主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23**

由上文可知，这种情况下主机A与主机B在同一网段下，且自身的IP地址与对方的子网掩码相与后得到的网络号仍为自身的网络号，因此不需要通过网管进行转发，而是直接将数据报发送给目的主机即可。因此该情况下两台主机都可以相互ping通。



1. **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**

由上文可知，源主机与目的主机不在同一个网段中。当源主机需要向目的主机发送数据报时，需要先将自身的IP地址与自身的子网掩码相与，再将目的主机的IP地址与自身的子网掩码相与，并将两次计算得到的网络号相比较：如果相同则说明两主机在同一网段，源主机直接向目的主机发送数据报即可；若不相同则说明两主机不在一个网段，需要通过网关进行转发。因此在这种情况下A和B也是可以ping通的。



1. **总结**
2. **以太网协议总结**
   1. 当网卡接收到一个帧时，第一步就是计算FCS，并与接收到的帧尾的FCS进行对比，如果一致则接收，如果不一致则丢弃。而Wireshark抓到的帧，都是FCS校验通过的帧，而帧尾的FCS会被硬件丢掉，所以利用Wireshark捕获数据包是无法查看FCS的。同时，Wireshark也抓不到FCS校验失败的帧。
   2. MAC帧在传送时使用的源地址和目的地址都是MAC地址，这两个MAC地址都写在MAC帧的首部中。
   3. MAC地址一共有48位。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。
3. **ARP协议总结**
   1. ARP协议也存在单播请求的情况，目的是主机定期确认ARP缓存表中的IP--MAC映射还是否有效，以决定这条ARP缓存是应该更新还是删除。同时，利用单播的方式请求不仅可以减少网络中ARP报文的数量，还可以保证ARP缓存表的实时性和有效性。
   2. 当一个主机第一次想获得同一网络中某设备的MAC地址是，会使用广播ARP请求的方式，来保证该设备一定能收到这个ARP的请求报文。这个操作就能使得双方都知道了对方的IP--MAC映射，就能在ARP缓存表中缓存该条映射。
   3. Gratuitous ARP：主机发送一个目标IP为自己IP的ARP请求，主要有以下两个作用：
      1. 主机用于确定当前网络中是否有IP地址与自己的IP地址一样的主机，此时如果收到了应答报文，则说明有IP地址相同的主机，这时则会提醒用户发生了IP地址冲突；若没有收到应答报文，则说明没有IP地址冲突
      2. 主机的MAC地址发生了变化（修改了MAC地址，或者更换了网卡），此时广播的ARP请求可以让LAN（或VLAN）中的所有主机更新ARP请求方的IP和MAC映射关系
      3. Gratuitous ARP在发现IP地址冲突后什么也不能做，此时就需要ACD（Address Conflict Detection）地址冲突检测机制来解决这个问题
   4. 地址冲突检测（ACD）：ACD定义了ARP probe和ARP announcement两种包，都是ARP请求，但是填充内容不同
      1. 网卡启动（或从睡眠状态恢复，或链接建立）是，会发送一个ARP probe。主机不会立即发送ARP probe，单个网卡也不会连续发送ARP probe，避免造成拥塞
      2. 发送主机可能收到ARP reply或者ARP probe。若收到ARP reply则说明候选IP地址已经有主机使用，此时会提示发送主机出现了IP地址冲突；若收到Target IP地址为候选IP的ARP probe，则说明另外一个主机也想要使用同一个候选IP地址，此时两个主机都会提示出现了IP地址冲突
      3. 若上述两种ARP包都没有收到，则说明候选IP地址可用。主机会发送一个ARP announcement来告诉同一LAN（或VLAN）的其它主机这个候选IP被使用，从而让其它主机更新ARP缓存
      4. 与Gratutious ARP不同，在系统运行期间ACD是一直运行的
      5. 当提示IP地址发生冲突后，需要进行地址冲突处理：
         1. 放弃该候选IP地址
         2. 再发送一个ARP announcement报文，如果冲突仍然存在则放弃该候选IP
         3. 无视冲突，继续使用该候选IP地址
4. **IP协议总结**
   1. IP数据报首部的首部长度与可变部分有关。如果没有可变部分，则首部固定长为20字节，就没有必要设置首部长度。由于首部长度最小可以表示5\*4=20字节，最大可以表示15\*4=60字节，因此IP数据报最多可以扩展60-20=40个字节。
   2. 为什么IP数据报的最大长度为2^16-1=65535字节，但是一般不会这么长，需要分片？答：因为数据链路层中MAC帧的长度有限制，MAC帧数据字段长度为46-1500字节，加上14字节的帧首部和4字节的FCS，MAC帧的长度范围为64-1518字节。
   3. IP软件在存储器中维持一个计数器。当每产生一个数据报时，计数器就加1，并将此值赋值给标识字段。这个标识不是序号，因为IP协议是无连接服务，因此数据报不存在按序接收的问题。当数据报由于长度超过网络的MTU（最大传送单元）而必须分片时，这个标识字段的值就被复制到所有的数据报分片的标识字段中。相同的标识字段的值使分片后的各数据报分片最后能重装为原来的数据报。
   4. 标志：接收方需要将分片重组，故对MF为敏感；中间结点可能需要再次进行分片，故对DF位敏感。作用：用来找path MTU，提高效率。
   5. 只有目的节点可以对分片进行重组，而路由器不可以。中间设备可能只能看到部分分片，故不能承担重组的工作，而且重组再分组的效率低。
   6. IP协议向上封装多种协议，向下屏蔽多种物理网络存在的差异。
   7. 若某个分片丢失，则整个IP包都会被丢弃，网络层也不会重传。
   8. 片偏移以个字节为偏移单位，因此所有分片的数据字段长度都必须为8个字节的倍数
5. **ICMP协议总结**
   1. Windows的tracert命令与Linux的traceroute命令不同，当目的主机收到ICMP数据报之后，会向源主机发送回显应答报文，而traceroute命令返回的是ICMP终点不可达的差错报告报文
   2. ICMP协议的差错报告报文格式是：ICMP差错报告报文的前8个字节+收到的需要进行差错报告的IP数据包的首部+该IP数据报数据字段的前8个字节

**暨南大学本科实验报告专用纸(附页)**