**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 验证型 实验地点

学生姓名 林晓旭 学号 2019051121

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 3 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. **实验原理**

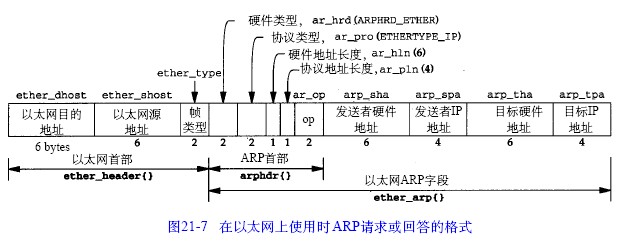
**网络嗅探器**

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**



**其他协议数据包格式见教材**。

1. **实验过程**
2. 安装Wireshark
3. 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。

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）；
* 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；
* 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；
* 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。

4、IP协议分析

* 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;
* 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。

1. 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。
* 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。

**【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？

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？

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？

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）。

5、通过下面实验**理解网关**

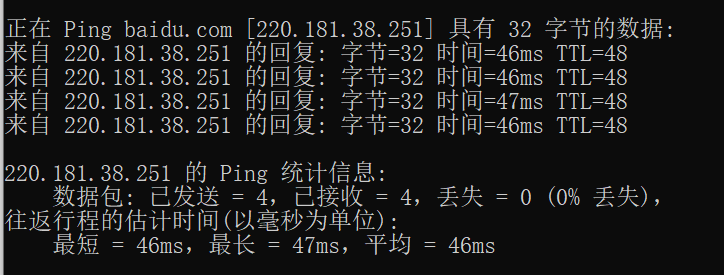
假设主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析。

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。

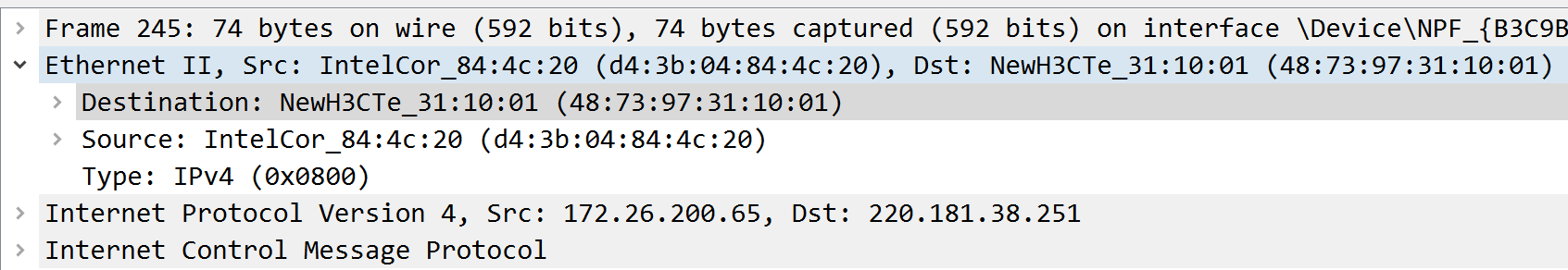
针对上述情况，分别将主机的网关设置为本机地址，观察测试结果，并分析原因。

**四、实验结果**

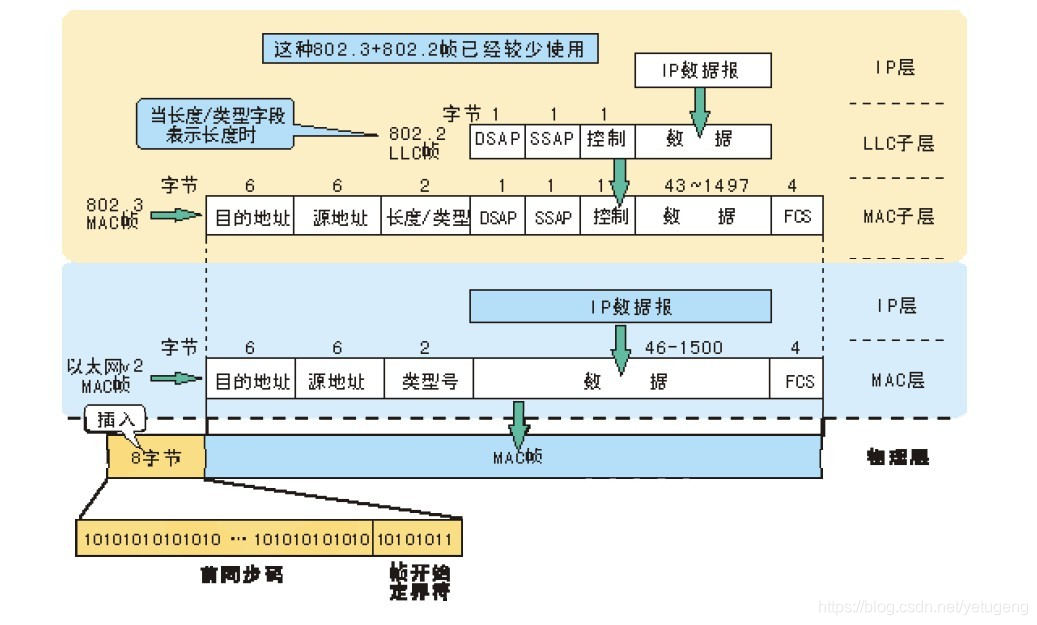
2、以太网协议分析：

使用ping命令向ip地址为220.181.38.251发送ICMP报文  
 

用wireshark抓包



发现以太网数据帧中，首先头部字段是属于ethernet V2协议，包括了目的主机MAC地址、源主机MAC地址以及封装的网络层协议类型TYPE。



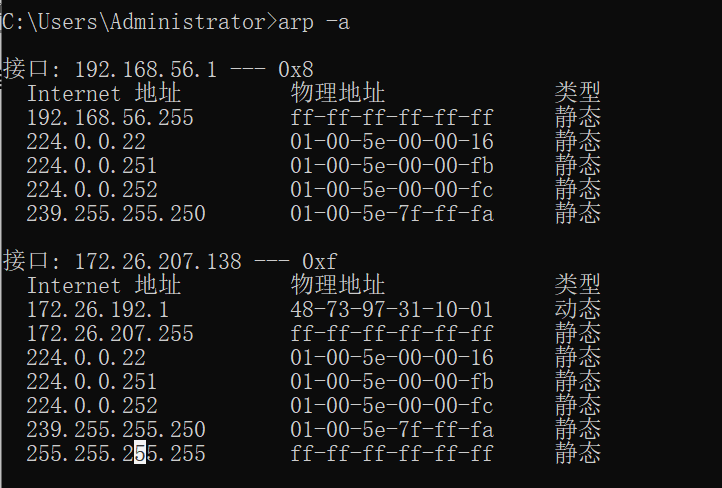
但是明明在Ethernet V2协议报文中，在目的MAC地址前面还有7个字节的前同步码和1个字节的真帧开始界定符以及在报文末尾还有4个字节的帧检验序列FCS。为什么wireshark捕获不到呢？

首先，前同步码是用来使接收端的适配器在接受MAC帧时能够迅速调整时钟频率，使它和发送端的频率相同。前同步码为7个字节，1和0交替。而帧开始界定符用来表明数据部分的开始。由于Ethernet V2采用曼切斯特编码，每一个码元的正中间都会有电压的转换，所以当适配器发现某个时刻本该有电压转换而却没有，则可以判断以太网数据帧的结束。

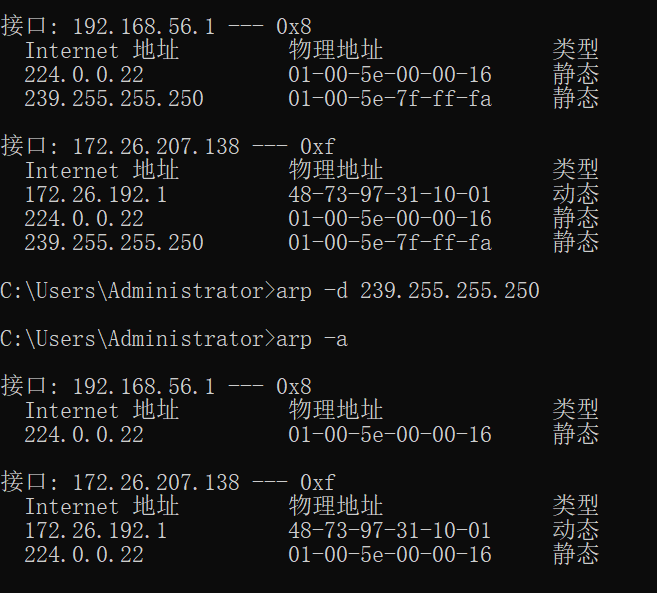
在网卡先要去挑签到同步码和帧开始界定符，然后对帧进行CRC校验，因为数据链路层不是可靠协议，所以在校验失败时会丢弃该帧，如果校验正确，就判断帧的目的MAC地址是否在自己的接受范围内（目的MAC地址、广播地址、多播地址），如果符合则交由设备驱动程序进行处理。所以在使用抓包软件抓到的数据包时去掉前同步码、帧开始界定符以及序列校验序列FCS之外的数据。

3、ARP协议分析

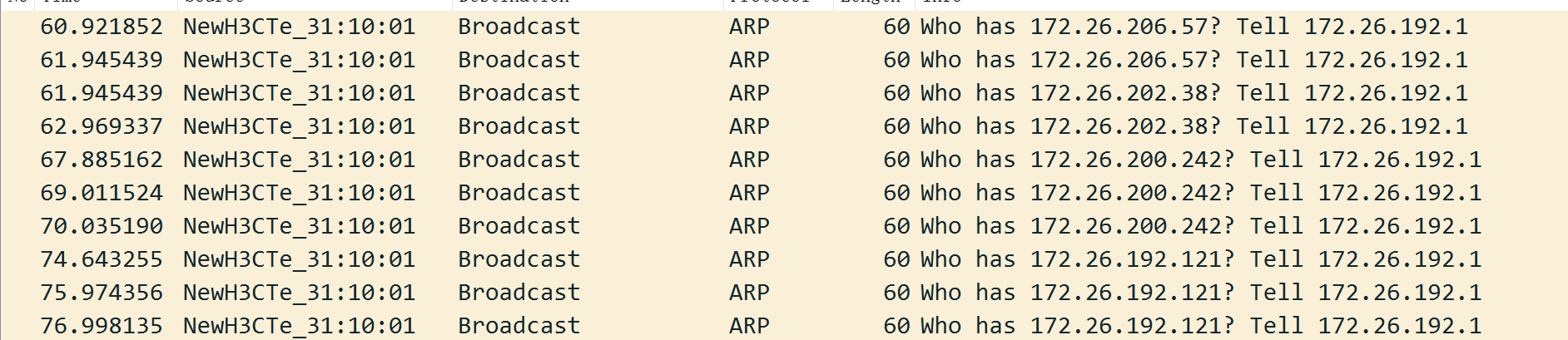
首先通过在命令行输入arp -a来查看本机的arp表，arp表的作用是用于缓存ip到mac地址的映射关系。



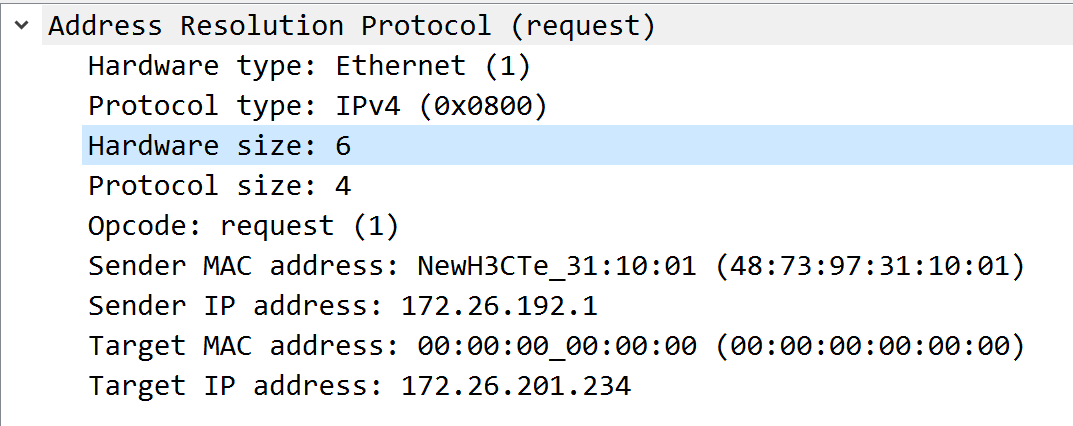
可以通过arp -d [ip address]来删除arp表中的某一项



把网线断开一分钟后再联网当然能捕获到arp。



首先是arp request报文



Hardware type用来标识数据链路层的协议，这里数据链路层使用了ethernet协议，所以值为1

Protocol type用来标识网络层协议，这里网络层协议使用IPV4协议，所以值为0x0800

Hardware size用来标识硬件地址的字节长度，所以值为6

Protocol size用来标识协议地址的字节长度，IPV4的地址由32为，即4个字节长度

Opcode标识arp数据包类型，request报文为1，reply 报文为2

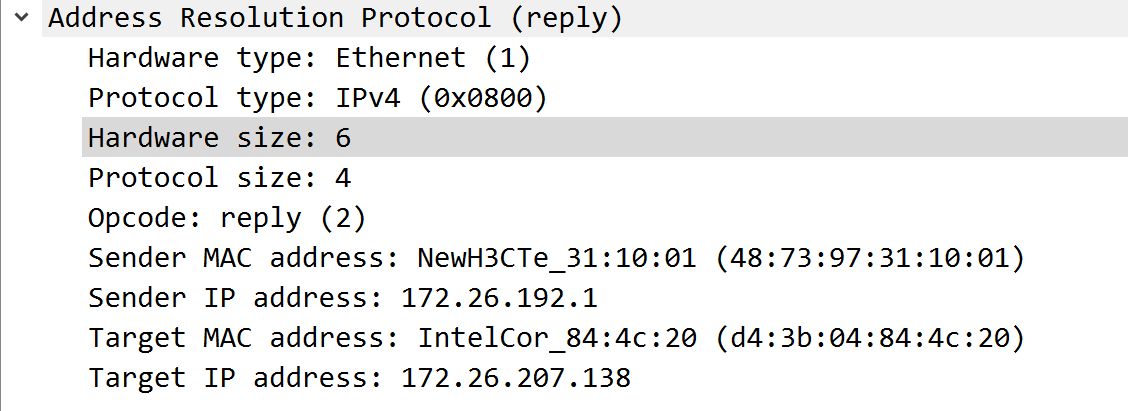
Sender MAC address标识该arp报文发送者的MAC地址

Sender IP address标识该arp报文发送者的IP地址

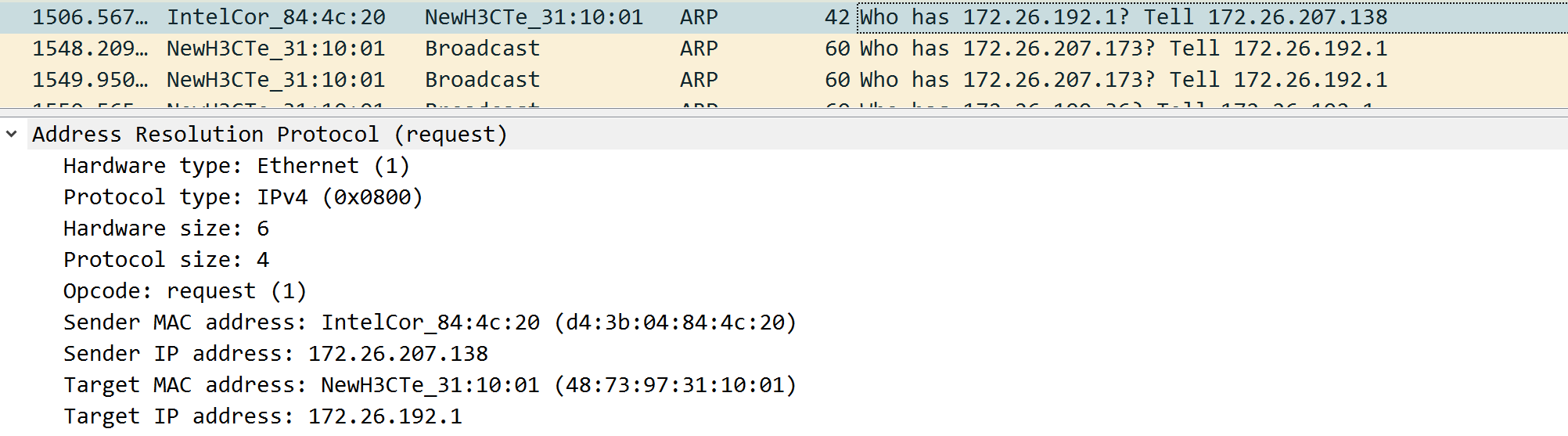
Target MAC address标识目的MAC地址

Target IP address标识目的IP地址

Arp reply报文大同小异

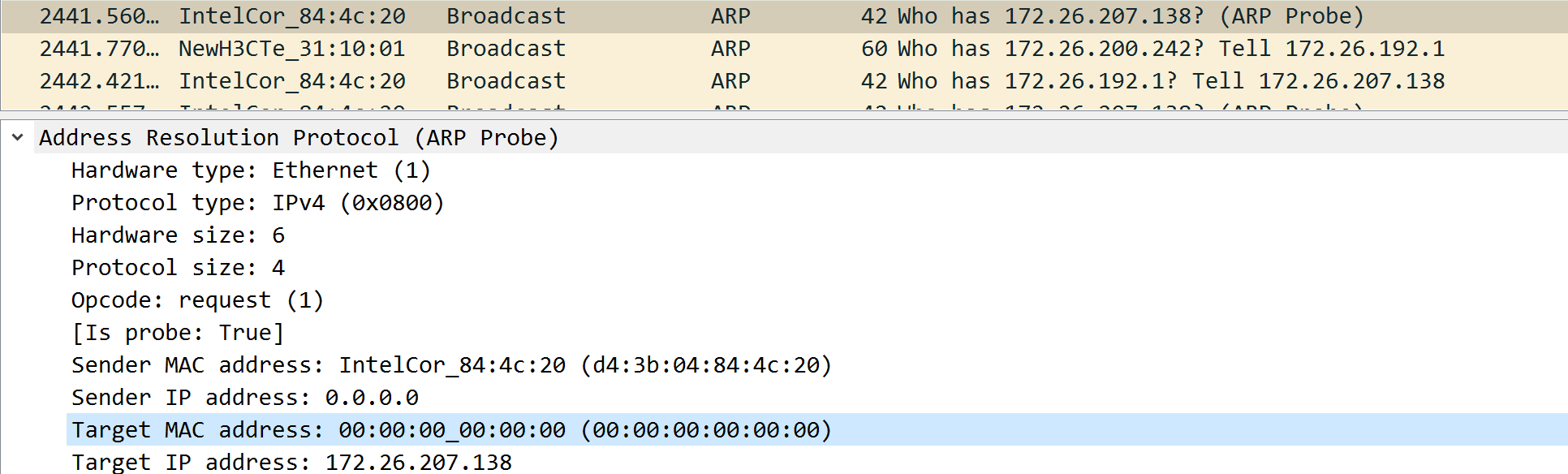


在用wireshark抓包时，意外的发现了竟然有arp request报文以单播的形式进行发送。

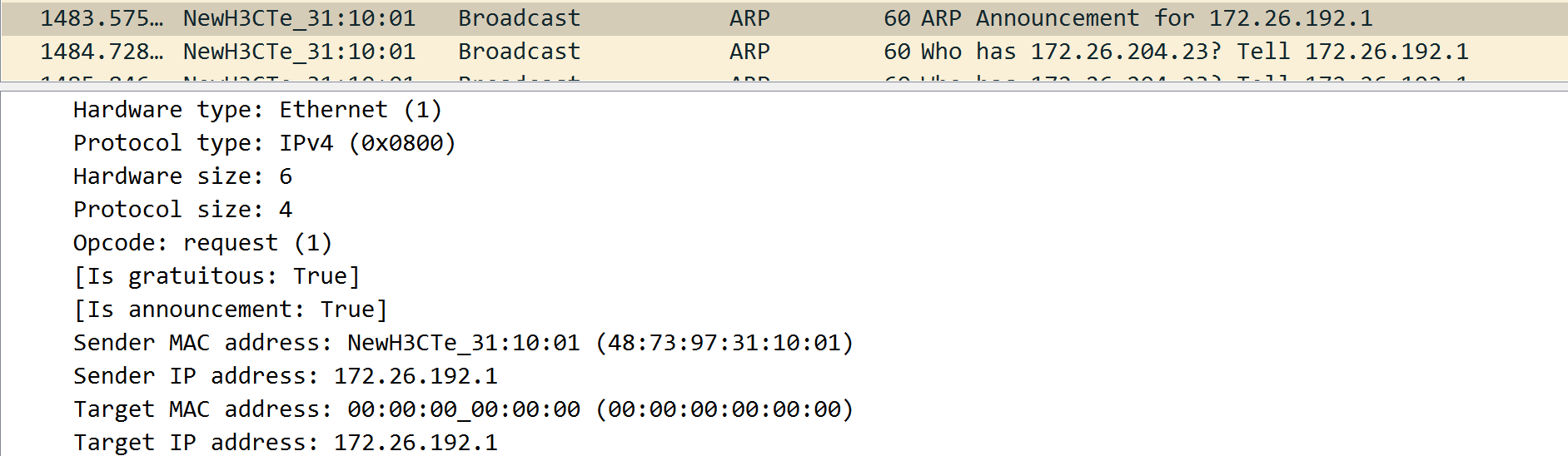


经查阅资料后知道了，这样的arp request报文的目的是来维护arp表中映射的有效性（时效性），也就是说保证arp表中的ip-mac对是正确的。

还有一种比较比较特殊的arp request报文如下

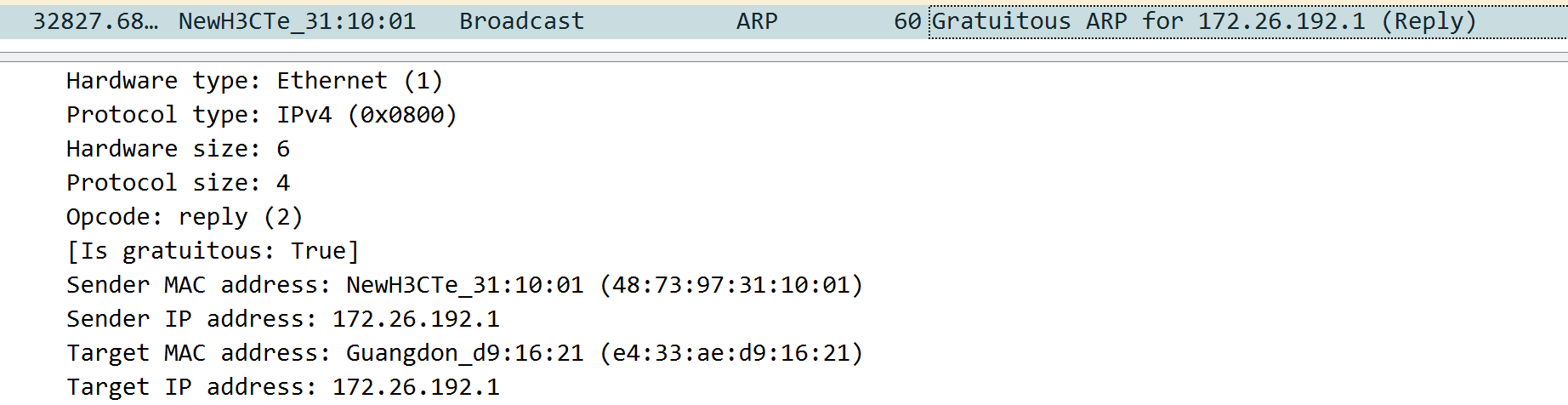


这类报文叫做ARP probe报文。顾名思义就是探测IP地址的ARP报文。这类报文只指明了Sender MAC address以及Target IP address，目的是用来检测IP冲突。Sender IP address设计为空的原因是以免别的主机将Sender的MAC-IP映射给缓存，不想给别的主机缓存的原因是源主机的IP尚未确定，如果出现了IP冲突，显然源主机就要换个IP。



当发送ARP probe报文后没有收到别的主机回复后，源主机就会发送一个ARP announcement来声明本机的IP地址。

还有一种奇怪的arp reply报文



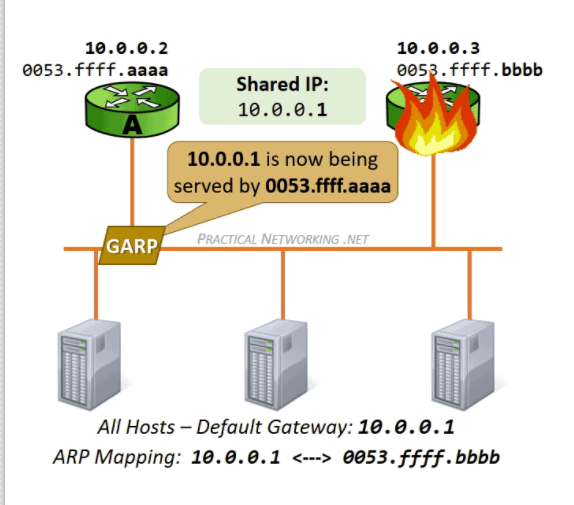
一般来说，arp reply报文是以单播的形式发出去，但是这个arp是以广播的形式发送。根据主机缓存arp表的原理（主机收到arp request或者arp reply报文后会将报文中的sender ip和sender mac给写入或覆写至本机的arp缓存表中）。在上图中，172.26.192.1是网关IP地址，我猜测这样做的目的和前面的arp announcement一样，都是用来声明自身的IP地址。因为主机不会缓存Target 的MAC和IP，所以Target Mac可以是任意值，而Target IP设为本机IP是这个报文不需要回应。

将sender IP和target IP相同的arp报文称作gratuitous arp（免费arp）：

就比如上文所提到的报文就是典型的gratuitous arp报文。Gratuitous arp报文是一类不需要回应的报文。

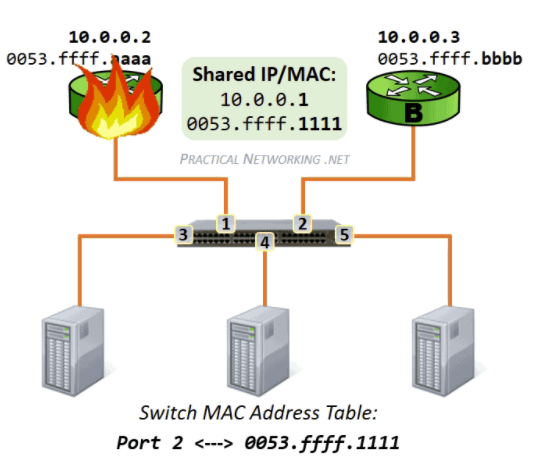
其作用主要有三种：

1. 更新别的主机的MAC-IP映射。如果有一个主机换了MAC地址，但是又保留了原来的IP，那么此时需要通过广播gratuitous arp报文来提醒别的主机去更新ARP缓存表。比如说一个虚拟机换了一个新的物理实体，那么此时虚拟机的IP未变，而MAC地址变了。
2. 声明一个节点的存在。就相当于先前所说的ARP announcement，这里不在阐述。
3. 冗余。

（1）、当两个有各自MAC地址的物理设备共同使用一个IP地址。  


当一个物理设备发生故障时（着火），那么另一个设备就广播一个gratuitous报文来提醒别的主机将发送至该IP的报文来数据链路层上发送个另一个MAC地址设备。

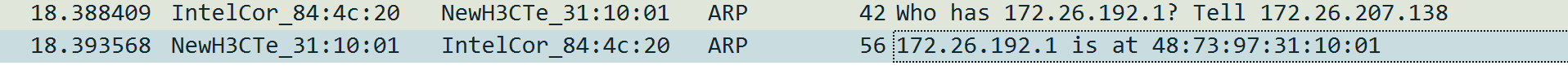
（2）当两个物理设备共同使用同一个IP地址且同一个MAC地址



当一台设备发生故障的时候，虽然说背的主机不用跟新ARP缓存表，但是还是需要另一台设备发送gratuitous报文来提醒交换机更新MAC-端口表（交换机更新MAC-端口表是根据每个MAC帧的Souce MAC address来构建的）

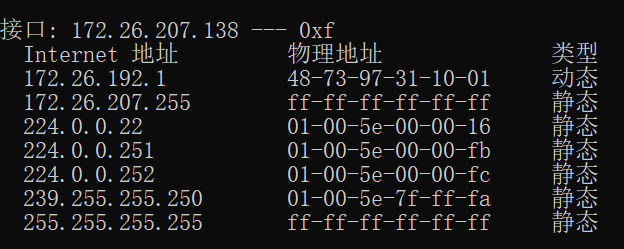
当用主机ping baidu.com时，





主机先会检查ping的目标IP地址是否与本机是在同一网段中，如果不是则用需要将IP数据包发送至默认网关。这是如果没有缓存网关的MAC地址的话，就需要发送ARP请求报文来获取网关的MAC地址。

在ping之后查看arp缓存表



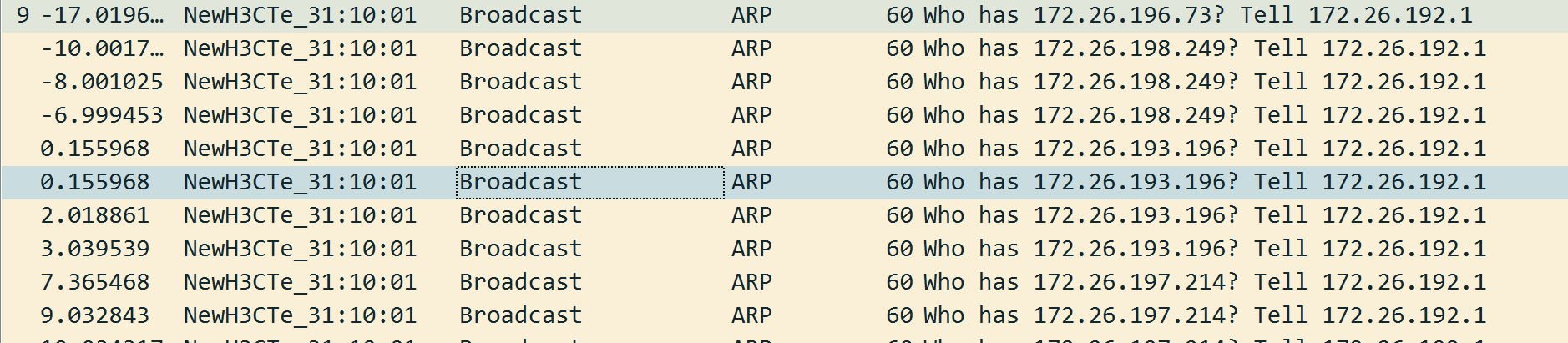
发现缓存表中缓存了网关IP的MAC地址，且注册位动态条目。

动态条目与静态条目的区别时，动态条目有老化事件而静态条目没有。

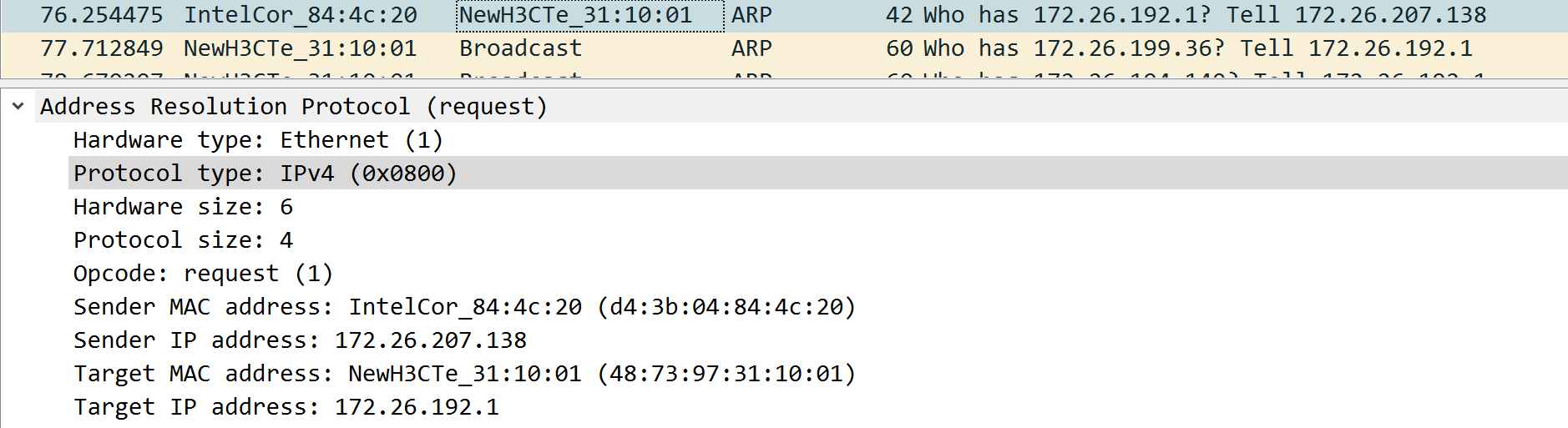
当主机一段时间（2 mins）内没有收到来自动态条目IP的ARP报文后，会将该动态条目丢弃。每一收到同态条目IP的ARP报文都会刷新该条目的生存时间（2 mins）。

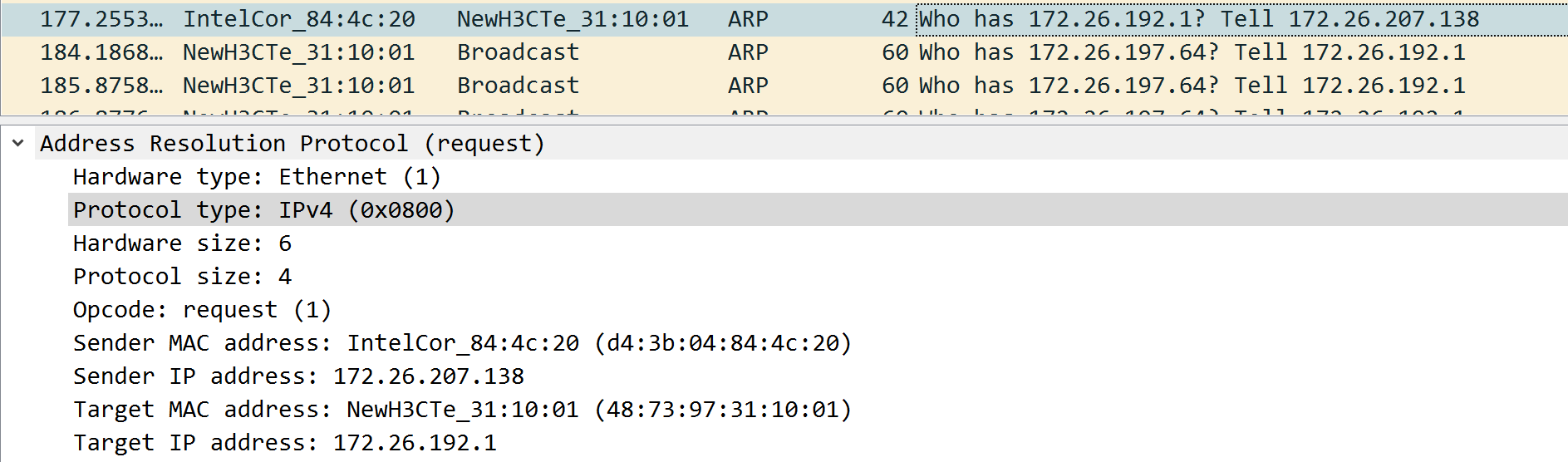
一些主机会设置最大动态条目数量，规定ARP表中最多存在多少个动态条目，当动态条目满了且有新的动态条目需要注册时，会丢弃老的同台条目。

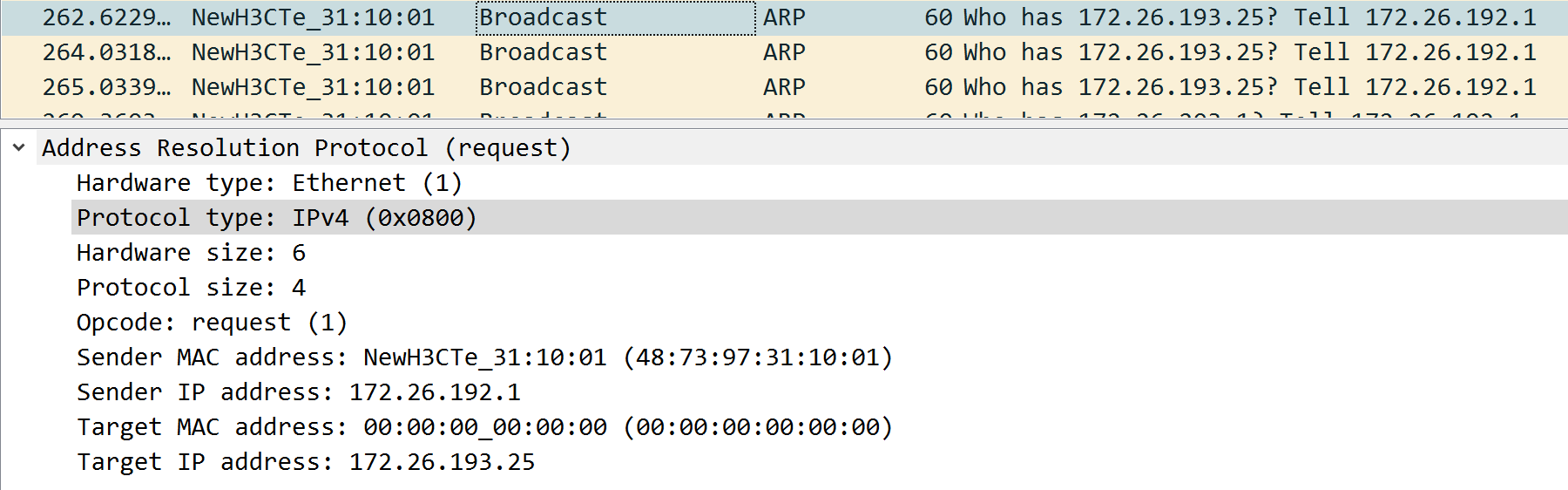
再执行一次相同的ping命令，因为arp缓存表中有对应网关IP的表项，所以无需再发arp请求报文。



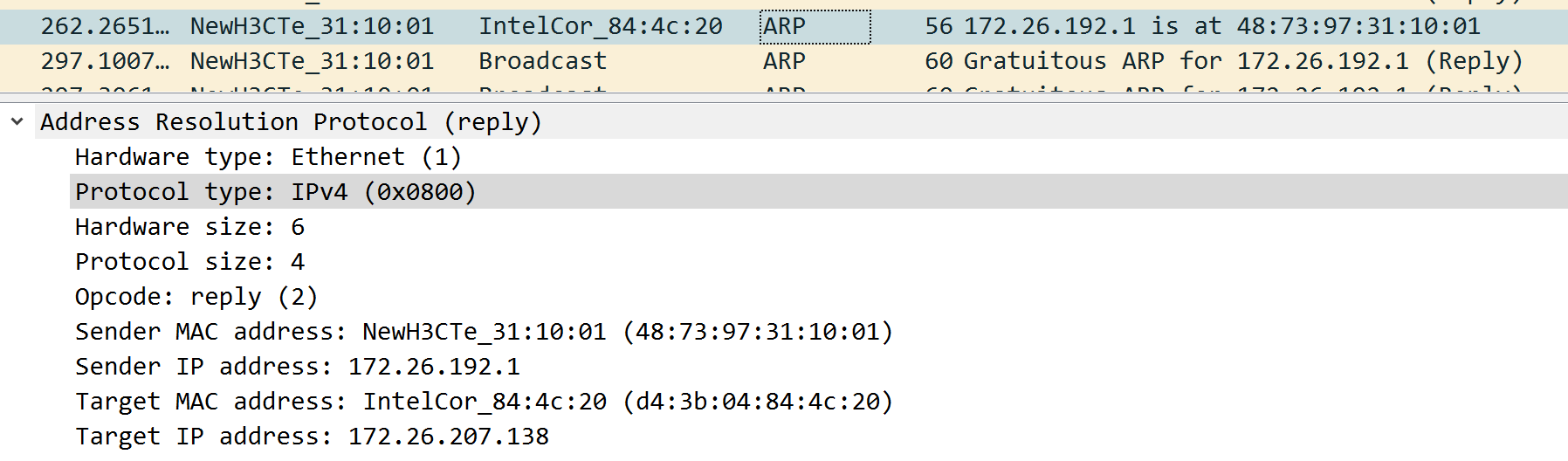
再过一段时间发相同的ping命令，发现主机并没有发arp请求报文。经过探究，原因如下，







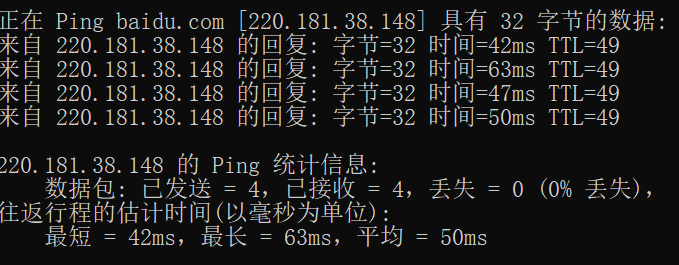
本主机每个一段时间（80-100s）就会发送一个单播的arp请求报文来检查arp缓存表中关于网关IP的动态条目是否可用。所以网关就会发送给本机一个arp回应报文



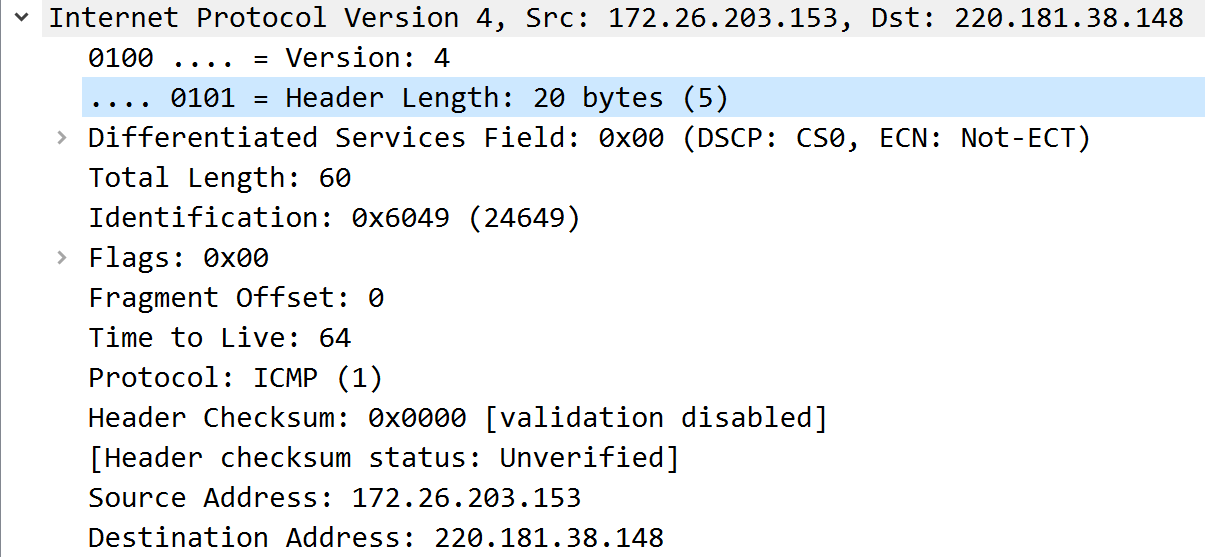
从而使网关IP所在的动态条目的生存时间刷新。

1. IP协议分析

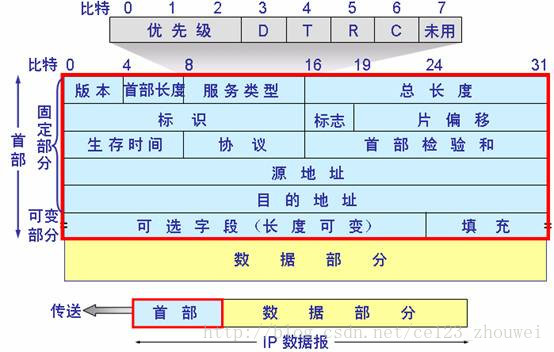
向IP地址为220.181.38.148发出PING命令检测报文



用Wireshark抓包，查看IP数据包的格式



IP数据包格式：



先根据抓包结果与IP数据包格式进行对比分析：

首先说明IP数据包有头部和数据部分组成，其中头部固定部分占20各字节，可选部分的长度可变但是字节大小一定要是4的倍数，不足用0填充。以下对各字段含义进行说明  
（1）、版本字段指示当前数据包遵循IP协议的版本，抓包结果在这个字段的值是4，表示使用IPV4协议。

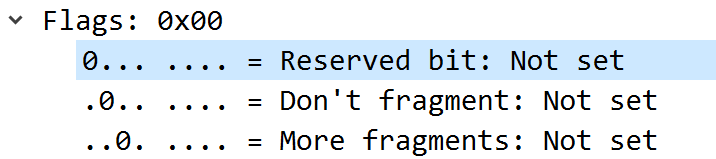
（2）、首部长度表示IP数据包首部的字节长度，值得注意是这里以4字节为单位。这也是要求IP首部的字节长度要为4倍数的原因，不然就无法表示首部长度。可见IP数据包最长可达60字节。抓包结果在这个字段的值是4，表示IP头部长20字节。

（3）、服务类型占8位,用来获得更好的服务.这个字段在旧标准中叫做服务类型,但实际上一直没有被使用过.1998年IETF把这个字段改名为区分服务DS(Differentiated Services).只有在使用区分服务时,这个字段才起作用. PING过程并没有使用区分服务，所以抓包结果在这个字段的值是0。

（4）、总长度表示IP数据包的长度，包括首部长度和数据部分长度，以字节为单位。这个字段占16个字节，所以IP数据包最大长度为65535字节。此外，网络层下的数据链路层有着自己的帧格式以及最大传送单元MTU(Maximum Transfer Unit),在以太网传输协议中，数据帧数据部分的长度需要在46-1500字节范围内，不足的需要填充，超过的需要进行分片。

（5）、标识字段占16位。主机IP软件中会维持一个计数器，每产生一个IP数据报就会将计数器的值加1并将值赋给这个字段。当一个IP数据包要进行分片操作时，标识会被复制到所有的分片数据包中。在进行数据包重组过程中，主机根据标识字段将数据包进行合并。

（6）、标志字段一共由3位，其中最高位是保留位，次高位为DF（Don’t Fragment）位，当DF=0时才可以对数据包进行分片操作。最低位位MF(More Fragment)位，当MF=1时标识在这个数据包之后还有被分片的数据包。MF=0时这是分片数据包中的最后一个。



（7）、片偏移地段占13位，标识该数据包在原组中的偏移量，以8字节位单位。也就是说分片长度一定是8字节的整数倍。

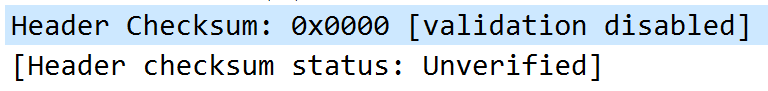
（8）、生存时间字段占8位，标识数据包在网络中的存活时间。一开始的存活时间是以秒位单位，由于现在网络中的转发速度太快了，以秒位单位太长了。所以现在生存时间以路由转发次数为单位。每当数据包经过一个路由器转发后，生存时间减1。当生存时间为0时，该数据包会被丢弃。



（9）、协议字段一共占8位，表示上层协议类型。以便目标主机知道将IP数据包上交给哪个过程进行处理。



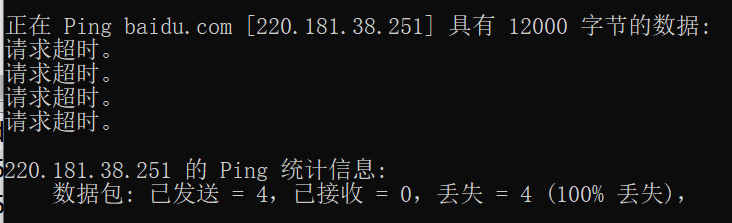
（10）、首部校验和字段占16位，只用来进行检验IP首部字段，不包括数据部分。这是因为数据报每经过一个路由器,都要重新计算一下首都检验和 (一些字段,如生存时间,标志,片偏移等都可能发生变化),不检验数据部分可减少计算的工作量.



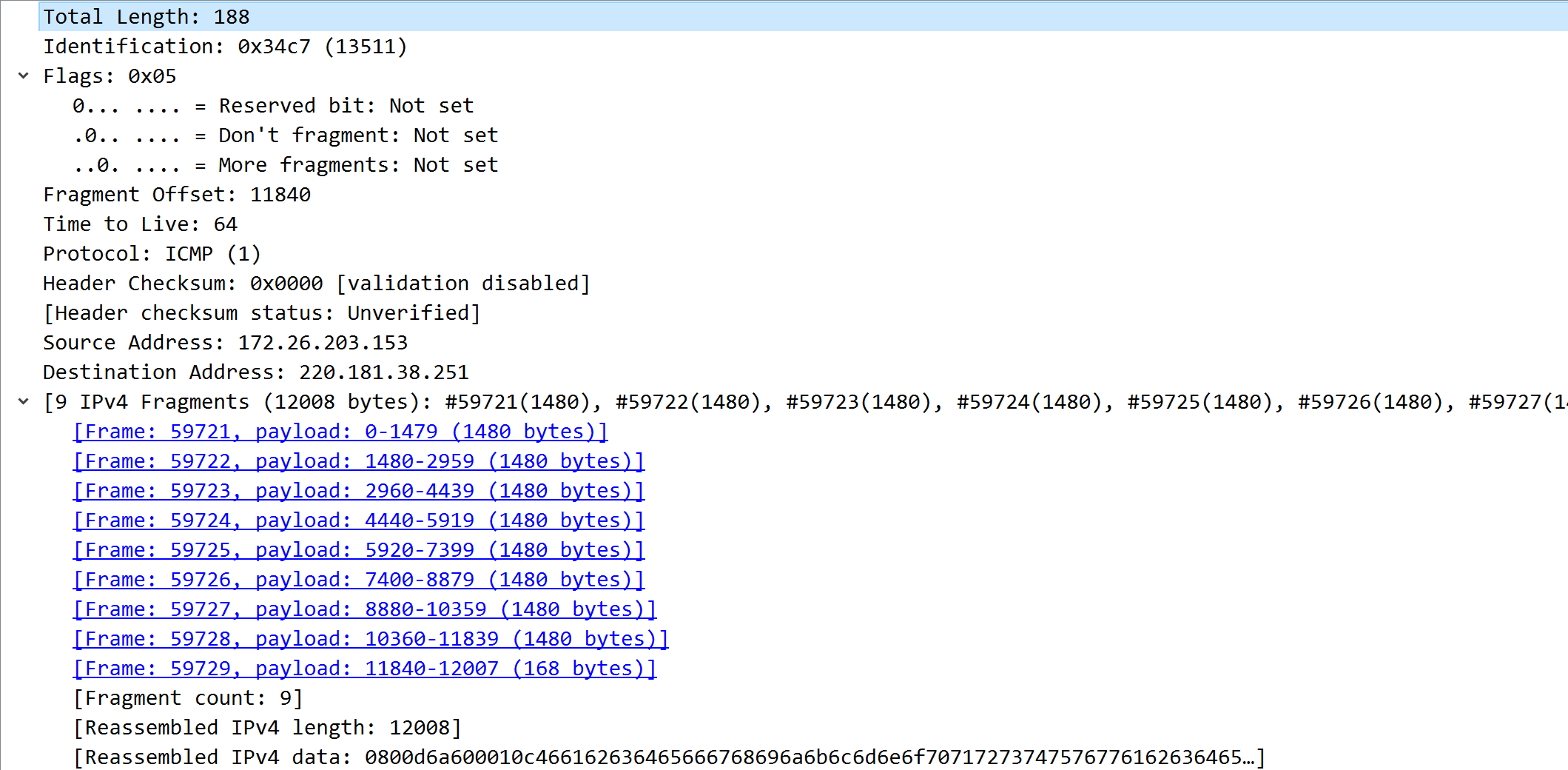
这是本机发送的IP数据包，Checksum为0的原因是操作系统将计算校验和的任务交由网卡来完成，所以在Wireshark在截获发由网卡的数据包时，校验和还是还没有被计算。Validation disabled表示禁用校验，原因同上。因为校验和是在网卡进行计算，是发生在数据包被WireShark截获之前，所以当前的校验和并没有意义，也就不去验证。

（11）、源地址和目标地址就是源主机和目的主机的IP地址，占32位。

用ping命令发送12000字节的数据包



用wireshark抓包，下图展示其中一个IP数据包格式。

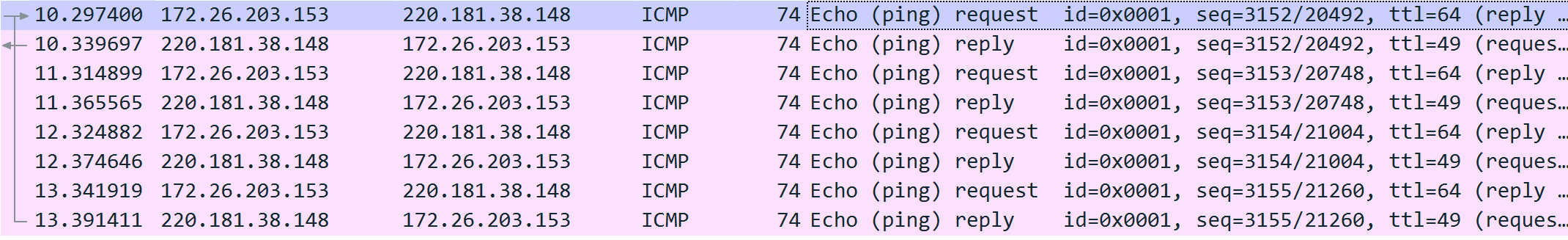


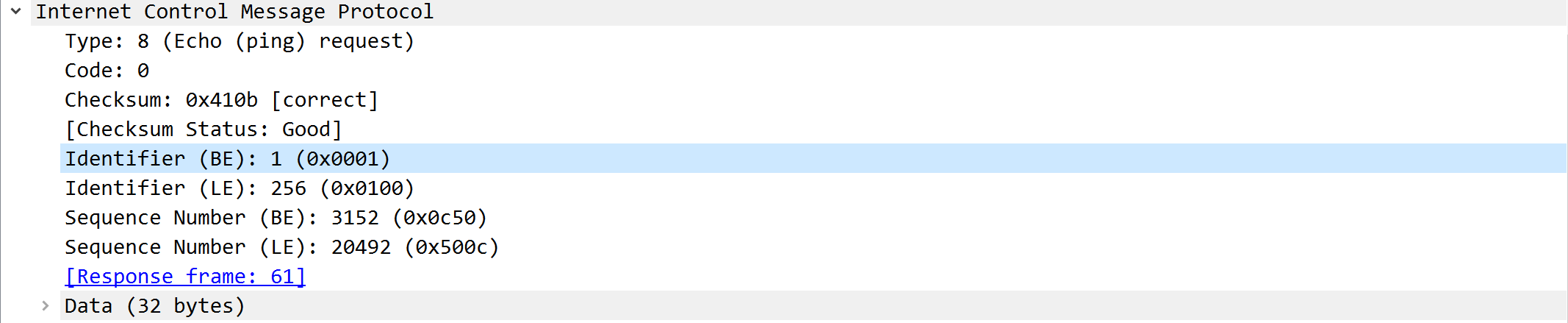
可见，WireShark抓取的IP数据包的首部是分片末尾IP数据包的首部。因为，最后一个分片数据长度位168字节，加上首部的20个字节，恰好是188字节（Total Length=188）。且标志位MF也为0表示是最后一个分片。该12000字节的数据，一共被分成了9个IP数据包。在以太网写一下，一个数据帧的数据部分最多1500字节，且IP首部最少占20个字节，所以一个IP数据包的数据部分最大1480个字节。12000=1480\*8+160。多出来的8个字节是ICMP报文头部的字节数。

1. ICMP协议分析

首先ICMP报文分为查询报文和差错报文。

使用ping并用wireshark抓包





分析ICMP报文格式：

TYPE字段占1个字节，表示报文类型。其中8表示此报文为回显请求报文。如果是回显回应报文则是0。

CODE字段占1个字节，用来进一步细分报文类型。

具体来说，需要共同考虑TYPE和CODE字段才能决定该ICMP报文的含义。

Checksum字段占2个字节，是ICMP报文的校验和

ICMP报文的前4个字节是固定的。

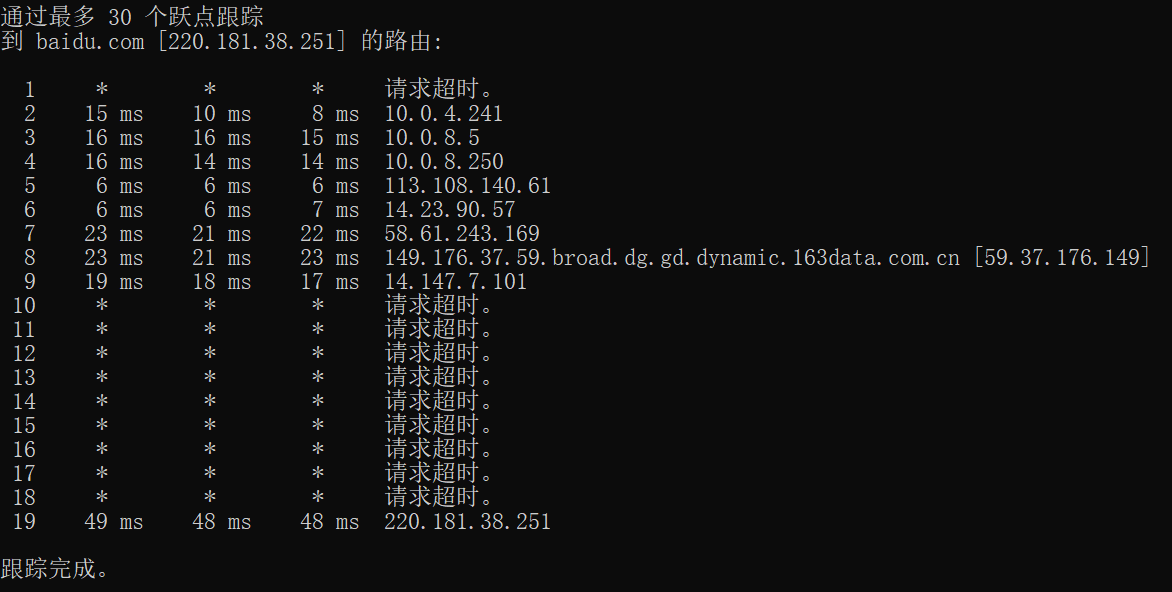
Identifier字段占2个字节，用来标志发送该ICMP报文的进程标识符

在抓包中发现由BE和LE两种表示，分别是大端(Big Encodian)和小端(Little Encodian)表示。其中大端表示将高字节放在内存的低地址；小端表示将低字节放在内存的低地址。实验主机使用的是大端表示。

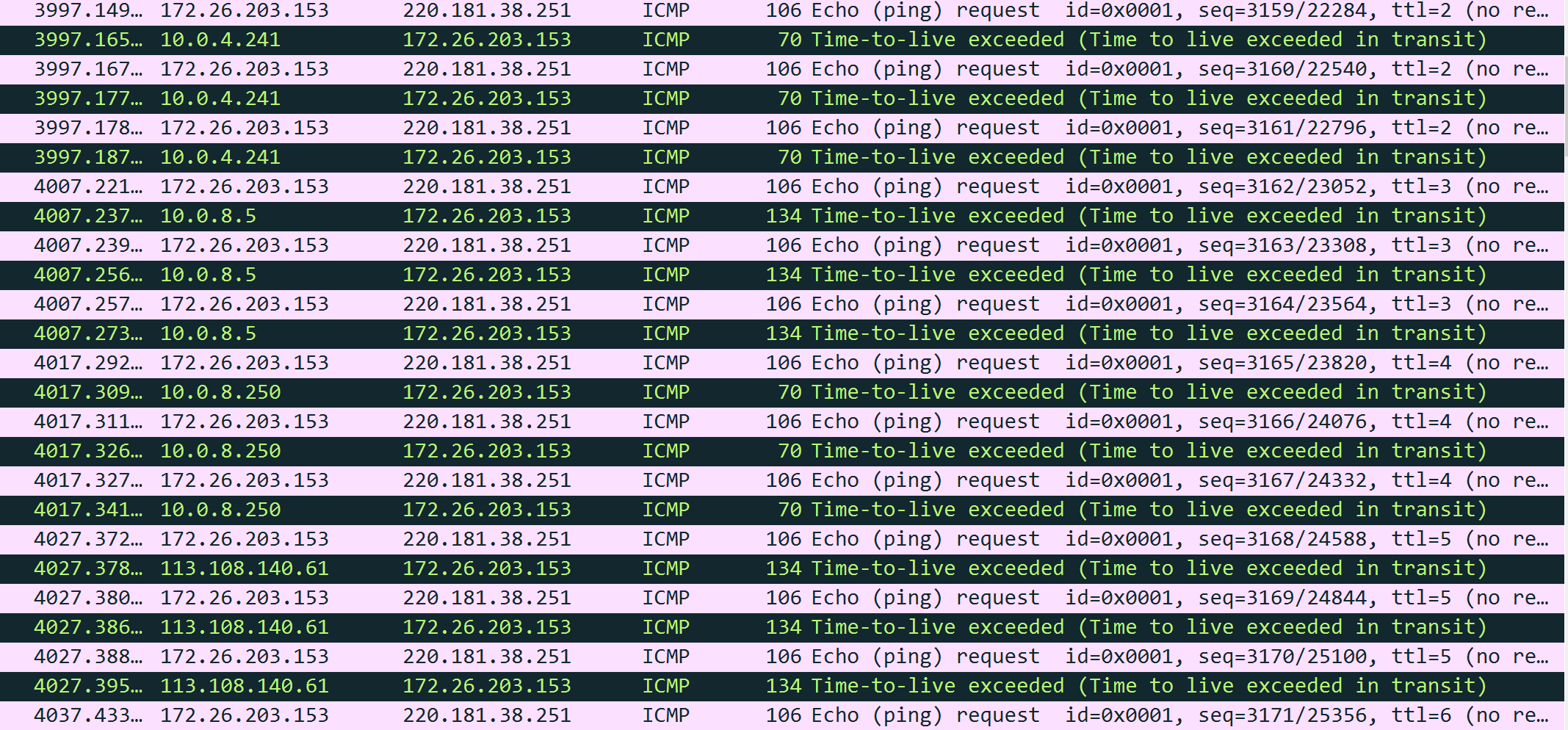
Sequence Number字段占两个字节。每发送一个ICMP报文，Sequence Numver就会增加1。Sequence Number可以用来跟踪ICMP报文的后续情况（有没有回复等）。

一次ping命令会让主机发送4个ICMP Request报文。当目标主机收到ICMP Request报文后，会发送ICMP Reply报文。主机可以通过计算发送ICMP Request报文以及收到ICMP Rely报文的时间差来反映网络情况，可以通过ICMP报文中包含的TTL来反映源IP与目的IP之间的网络距离。

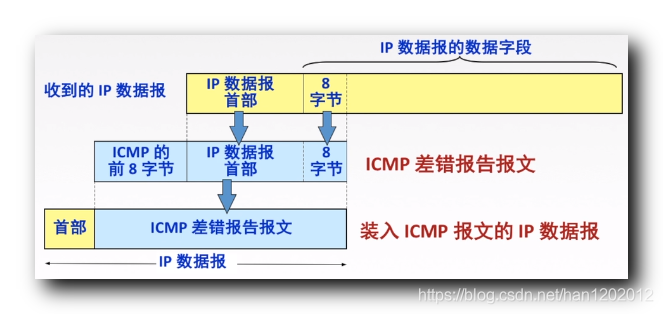
使用tracert命令来获得两IP节点之间的路由路径



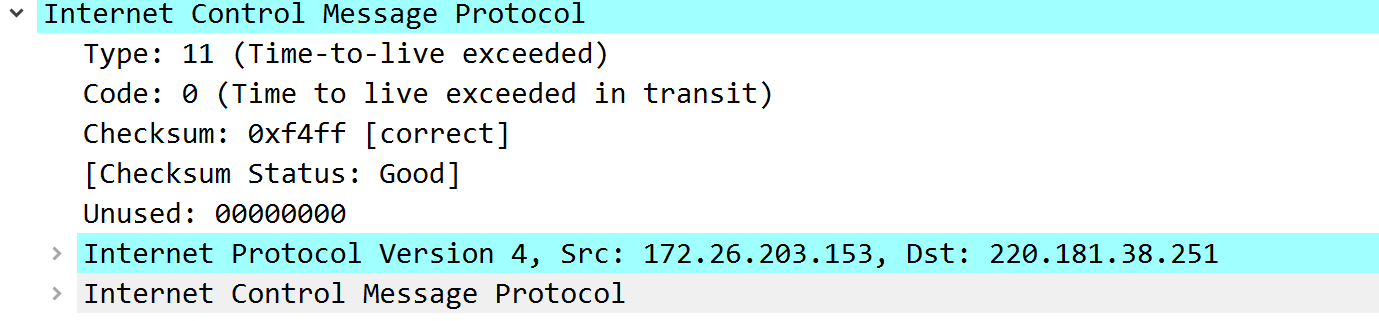
用wireshark抓包



可见当我们使用tracert命令时，主机会发送TTL从1开始递增的ICMP回显请求报文，每个TTL发送三次，直至收到目标主机所发送的ICMP回显回应报文。总所周知，当一个路由节点收到TTL为1的IP数据包且当前节点并不是路由节点时，会将这个IP数据包丢弃并发送一个ICMP差错报文至原来的IP主机。

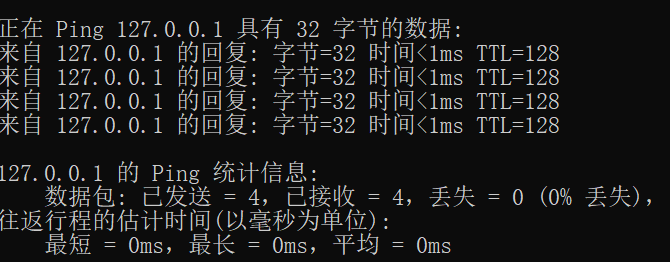


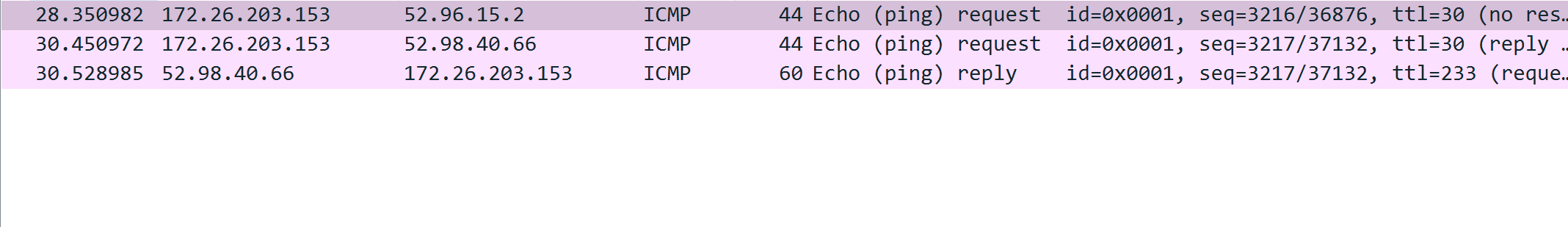
上图说明了ICMP差错报文的组成方式。是由原来IP数据包的首部字段+原来IP数据包的数据字段的前8个字节作为ICMP差错报文的数据部分，



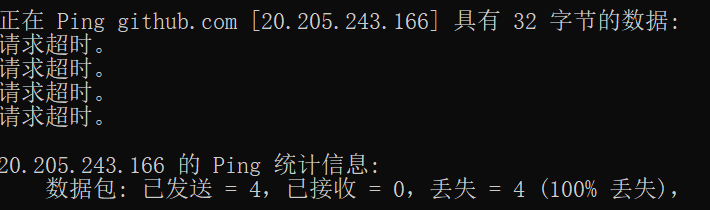
ICMP差错报文的TYPE为11表示IP数据包的TTL超时了。Code为0表示是在传输过程中TTL超时。

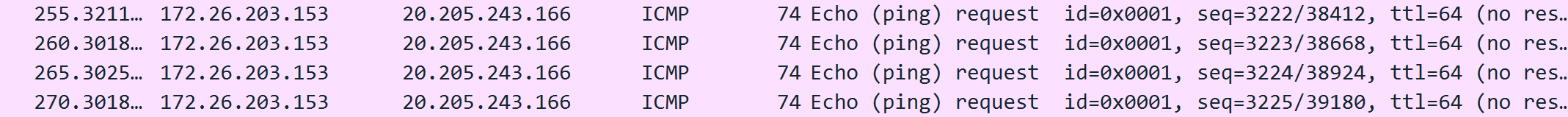
1. **实验总结**
2. ARP报文的主要目的时用来查询IP-MAC对应关系，所以当本机的ARP缓存表中缓存了需要的IP-MAC关系时自然就不需要使用ARP报文来获取一个IP的MAC地址。
3. 127.0.0.1是回环地址，目的地址为回环地址的IP数据包并不会经过网卡发送，而wireshark只能截获发送给网卡的报文，所以wireshark捕获不到。



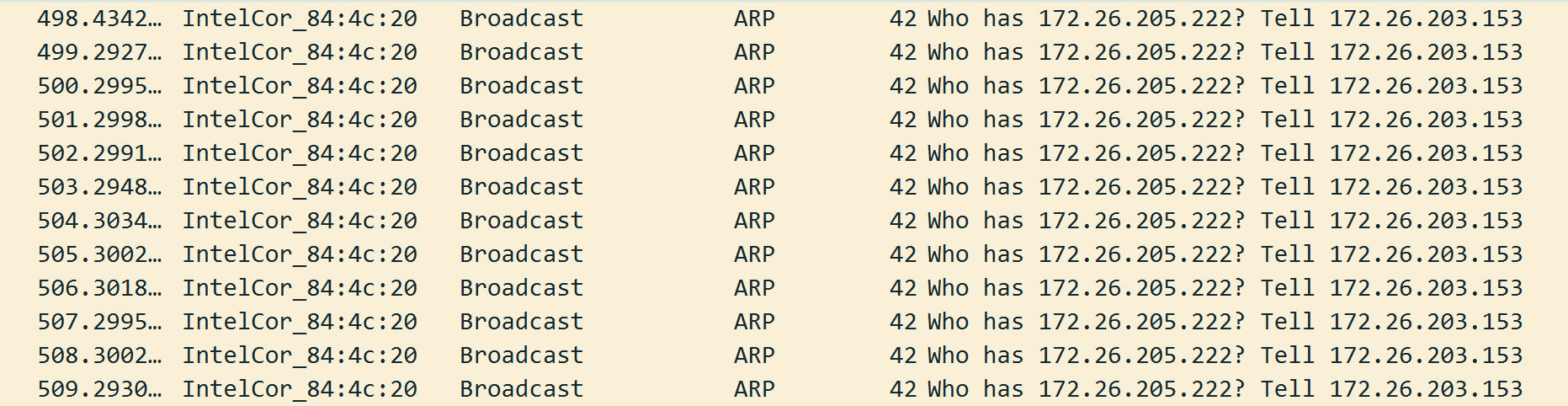


1. 当ping出现request timeout的原因是主机发出的ICMP request报文没有收到回应。





当ping出现destination host unreachable的原因是主机无法解析ping命令的IP地址。即无法获得该IP地址对应的MAC地址。这样连ICMP报文的发不出去。



1. 当ping同一网段的主机时，主机会直接该网段广播请求该目的主机IP的MAC地址，不需要经过网关。8个ICMP报文分别是源主机发出的4个ICMP Request报文和目的主机发出的4个ICMP Reply报文。两个ARP报文分别是源主机发出了广播ARP报文和目的主机发出的单播ARP报文。

当ping不同网段的主机时，主机首先需要将数据包发送至网关，再由网关向其他网段发送。所以主机需要请求网关IP的MAC地址。在这种情况下如果没有设置网关IP，连ARP报文都无法构建，自然不行。

1. 主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23，两台主机均不设置网关。这种情况是能ping的通的。

主机A所处网段是10.2.2.0，主机所处网段也是10.2.2.0，根据上文的分析，两台主机是ping德通的。

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。这种情况是ping不同的。

此时，主机A所处网段是10.2.2.0，主机B所处网段为10.2.2.0，虽然他们同属一个网段，但是ping不ping得通给看ping具体的工作流程。

（1）、

当主机A去ping主机B时，首先将主机B的IP地址与自己的子网掩码进行位与操作，此时主机A认为主机B的网段是10.2.3.0，和自己的网段不同，所以主机A认为需要经过网关发送，但是网关并没有设置，所以ping不通。

此时ping显示的错误是目的地不可达。

（2）、

当主机B去ping主机A时，首先将主机A的IP地址与自己的子网掩码进行位与操作，姿势主机B认为主机A的网段是10.2.2.0，是与自己处于同一个网段，所以会直接向网段广播请求主机A的MAC地址（通过ARP协议），那么由于确实是在同一网段，主机B是能得到主机A的MAC地址的，从而主机B能成功地发送ICMP Request报文而主机A能成功地收到主机B发送的ICMP报文。

但是，当主机A想向主机B发送ICMP Reply报文时就会出现（1）中的情况，所以无法发送ICMP Reply报文。

此时ping显示的错误是请求超时。

当将主机A、B的网关设置成它们各自的IP地址时，主机A、B之间是能相互ping通的。

（1）、

当主机A去ping主机B时，发现不是同一网段，就会将数据包发给网关，也就是主机A本身。主机A再通过路由机制来将数据包发送至主机B。

（2）、

主机B去ping主机A同理。