**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验指导书 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

学生姓名 张晓彤 学号 2019051119

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 午～ 11 月 9 日 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. **实验器件、仪器和设备**

计算机2台，交换机一台。

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

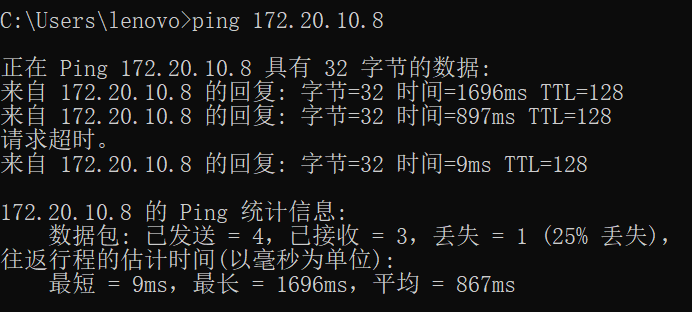
3、分析PING、TRACERT、ARP命令的工作过程

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. **实验步骤**
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。

将主机A和主机B连到同一个WiFi热点上，将主机A的掩码255.255.255.240和B的ip地址172.20.10.8进行运算，其处于同一个子网内，用主机A 172.20.10.3 ping 主机B 172.20.10.8



**ping的原理：**

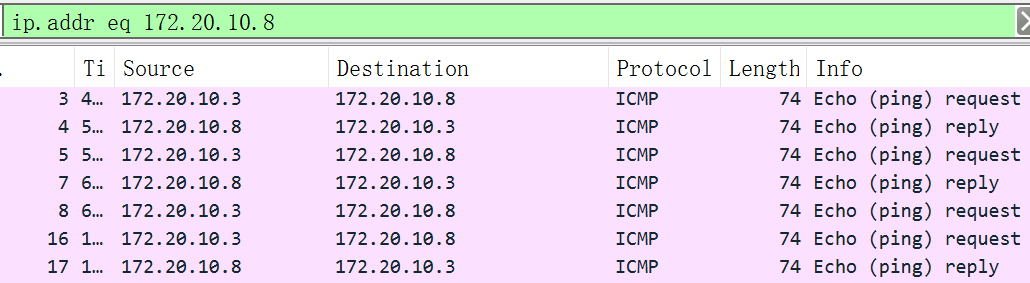
①构建一个固定格式的ICMP请求数据包，然后由ICMP协议将这个数据包连同目的地址一起交给IP 层协议，IP层协议将本机IP地址作为源地址，加上一些其他的控制信息，构建一个IP数据包，并在一个映射表中查找出目的IP地址所对应的物理地址(MAC地址：这是数据链路层协议构建数据链路层的传输单元——帧所必需的)，一并交给数据链路层。后者构建一个数据帧，目的地址是IP层传过来的物理地址，源地址则是本机的物理地址，还要附加上一些控制信息，依据以太网的介质访问规则，将它们传送出去。

②主机B收到这个数据帧后，先检查它的目的地址，并和本机的物理地址对比，如符合，则接收;否则丢弃。接收后检查该数据帧，将IP数据包从帧中提取出来，交给本机的IP层协议。同样，IP层检查后，将有用的信息提取后交给ICMP协议，后者处理后，马上构建一个ICMP应答包，发送给主机A，其过程和主机A发送ICMP请求包到主机B一模一样。

**Wireshark捕获到ICMP数据包：**

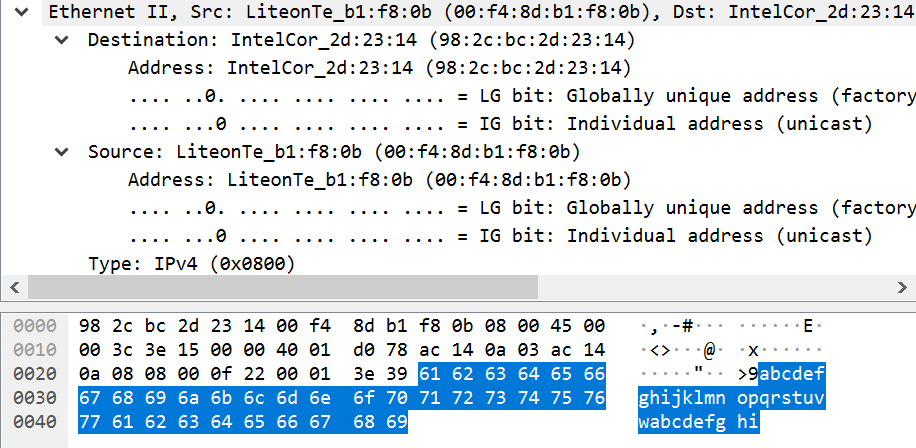
主机A四次请求request，主机B三次响应reply

第三次请求超时了，所以主机B没有应答



**以太数据帧：**

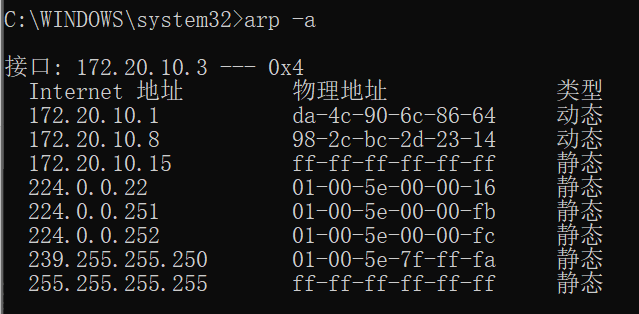
**格式：**

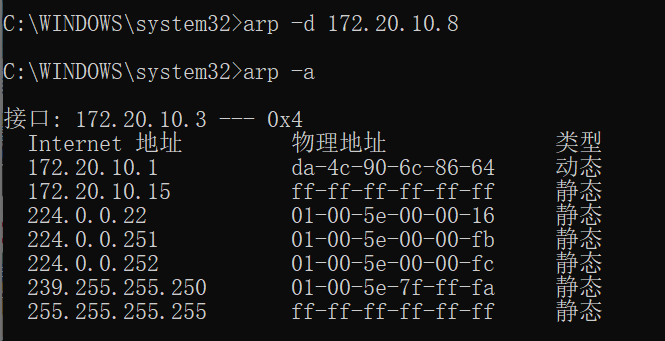


|  |  |
| --- | --- |
| Ethernet II | 以太网是当今现有局域网采用的最通用的通信协议标准。属于链路层协议  它由6个字节的目的MAC地址，6个字节的源MAC地址，2个字节的类型域为Frame Header  接下来是46--1500 字节的数据和4字节的帧校验  类型域用于标示封装在这个Frame里面数据的类型 |
| Src:/Source:/Address:  LiteonTe\_b1:f8:0b (00:f4:8d:b1:f8:0b) | 源地址帧 6 字节，网卡牌子：LiteonTe  前3个字节(00:f4:8d)为组织唯一标识符OUI：由厂家向IEEE购买  后3个字节(b1:f8:0b)为扩展标识符，由厂家指派  MAC地址封装在网卡的芯片中间，是唯一的地址 |
| Dst:/Address:/Destination Intelcor\_2d:23:14(98:2c:bc:2d:23:14) | 源地址帧 6 字节，网卡牌子：Intelcor  前3个字节(98:2c:bc)为组织唯一标识符OUI  后3个字节(2d:23:14)为扩展标识符 |
| LG bit: Globally unique address (factory default) | 全局唯一地址（厂家默认） |
| IG bit: Individual address (unicast) | 单播地址、本地管理地址 |
| Type: IPv4 (0x0800) | 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。  字段为 0x0800 时，表示将数据交付给 IP 协议 |
| FCS校验帧序列 | 抓包软件抓到的是去掉前同步码、帧开始定界符、FCS之外的数据，wireshark把8字节的前序和4字节的FCS都过滤了。  网卡接收到一个帧，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。  Wireshark抓到的帧，是FCS校验通过的帧，而帧尾的FCS会被硬件去掉，所以没有FCS。另一方面，wireshark也不会抓到FCS校验失败的帧。  wireshark报文长度大小：14（以太类型头）＋20（ip头）＋（实际数据） |
| 蓝色选中部分为数据段 | 在经过物理层和逻辑链路层的处理之后，包含在帧中的数据将被传递给在类型段中指定的高层协议。该数据段的长度最小应当不低于46个字节，最大应不超过1500字节。如果数据段长度过小，那么将会在数据段后自动填充（Trailer）字符。相反，如果数据段长度过大，那么将会把数据段分段后传输。  此时ping传送32字节，抓包并没有显示填充字节，原因如上格所写 |

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）；**

查看：

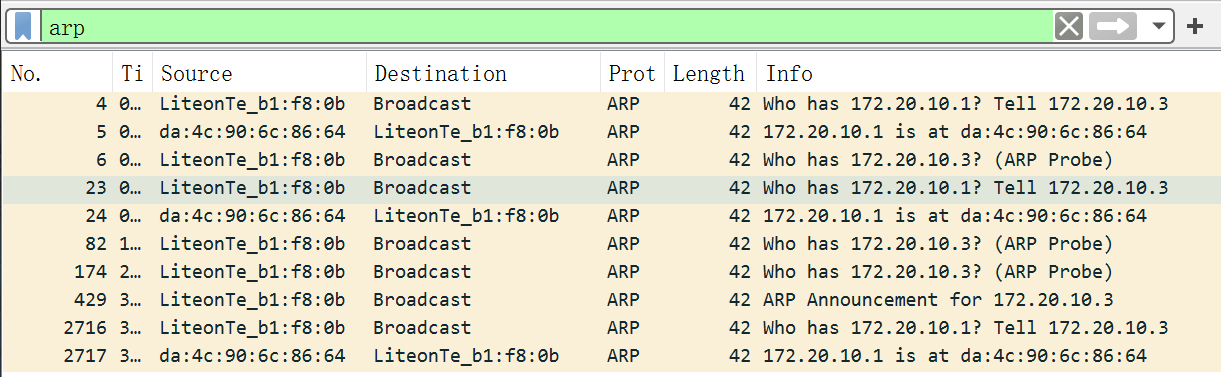
删除：

**ARP映射表**：缓存同一网段设备IP地址和MAC地址的映射，用于数据帧的转发。设备通过ARP解析到目的MAC之后，将会在自己的ARP映射表中增加IP地址到MAC地址的映射表，以用于后续到同一目的地数据帧的转发。

**静态**ARP表项：静态ARP表项通过手工配置（通过对应设备的IP地址与MAC地址绑定命定进行）和维护。不会被老化，也不会被动态ARP表项覆盖。

**动态**ARP表项：动态ARP表项由ARP协议通过ARP报文自动生成和维护，可以被老化，可以被新的ARP报文更新，也可以被静态ARP表项所覆盖。当到达老化时间或接口关闭时会删除相应的动态ARP表项。

* **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；**



4为本机的**广播的ARP协议**，目的在于找寻网关的172.20.10.1的MAC地址，5为网关172.20.10.1回复给172.20.10.3其MAC地址。

23、24和2716、2717同样。

过程如下：1. A发送一个ARP request（广播包，目的MAC全1），LAN中的所有主机（不考虑VLAN）都会收到这个ARP request。携带自己的IP地址和MAC地址和目的主机的IP地址。

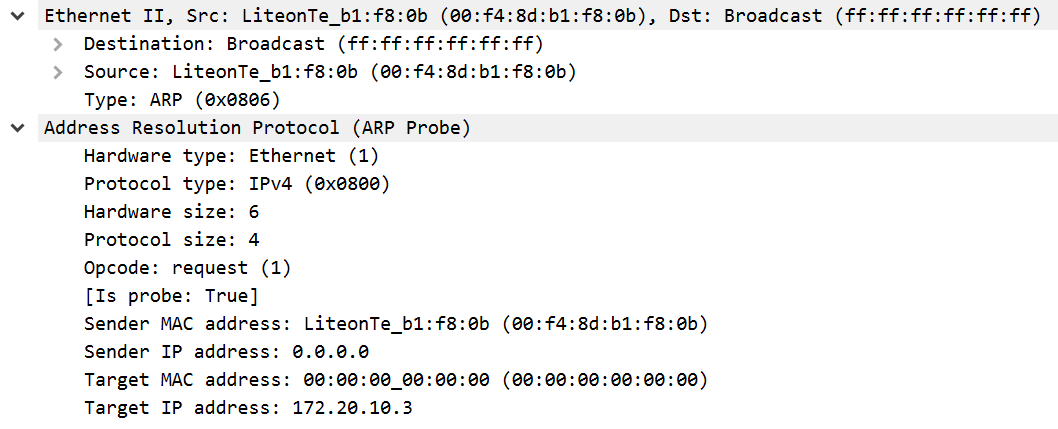
2. B收到了这个ARP request后，发现ARP request询问的IP地址是自己，B做如下事:1）更新自己的ARP映射，即把A主机的MAC地址映射到A的IP地址上。2）给主机A发送ARP reply（单播）

3. A收到B发来的ARP reply，更新自己的ARP映射

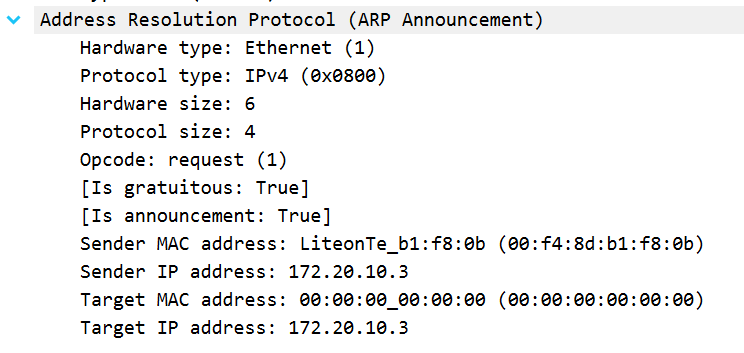
4. 此时A知道了B的MAC地址，B也知道A的MAC地址，A和B可相互通信。但某个时刻其中一个主机的MAC地址-IP地址映射会过期，就再次重复1到3的过程。

6、82、174为**免费ARP**，一种特殊的ARP报文，该报文中携带的目标IP地址是本机IP地址，报文源MAC地址是本机MAC地址，报文的目的MAC地址是广播地址。

**免费ARP**：确定其它设备的IP地址是否与本机的IP地址冲突。当其它设备收到免费ARP报文后，如果发现报文中的IP地址和自己的IP地址相同，则给发送免费ARP报文的设备返回一个ARP应答，告知该设备IP地址冲突。



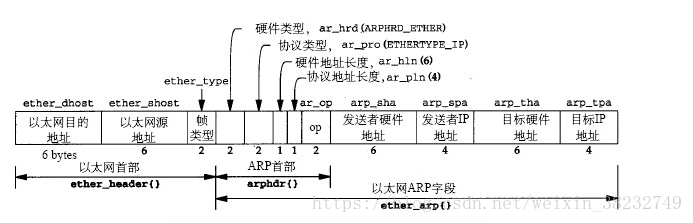
429为**ARP announcement 协议通告**，用于昭示LAN本机要使用某个IP地址了，是一个Sender IP和Target IP填充的都是本机IP地址的ARP request。这会让LAN(VLAN)中所有主机都会更新自己的ARP cache，将IP地址映射到发送者的MAC地址。



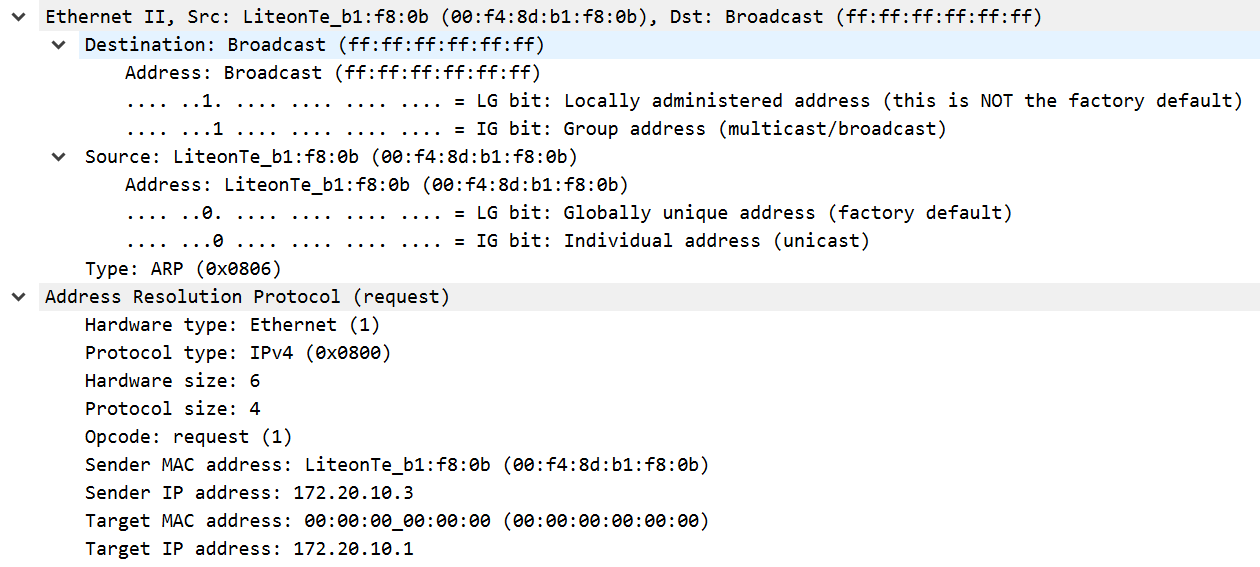
**查询默认网关的地址**：网关是一个网络到另一个网络的关口，一个网络一个网关，所以它的作用就是把网络A和网络B连接起来，使之A网络中的机器能够和B网络中的机器进行通信。

跨子网通信需要默认网关的转发，而要和默认网关通信，就需要获得其MAC地址。

ARP协议报文格式：



以No.4数据包为例：



目标IP地址

目标MAC地址

发送端IP地址

发送端MAC地址

操作码，为1表示是个ARP请求包

协议长度

硬件地址长度

协议类型

硬件类型

网络层，ARP请求包

上层协议为ARP

源地址为本机MAC地址

目的地址全1，为广播地址

链路层

硬件类型：表示硬件地址的类型。它的值为1表示以太网地址；

协议类型：表示要映射的协议地址类型。它的值为0x0800即表示IP地址；

硬件地址长度和协议地址长度分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上IP地址的ARP请求或应答来说，它们的值分别为6和4；

操作类型（OP）：1表示ARP请求，2表示ARP应答；

发送端MAC地址：发送方设备的硬件地址；

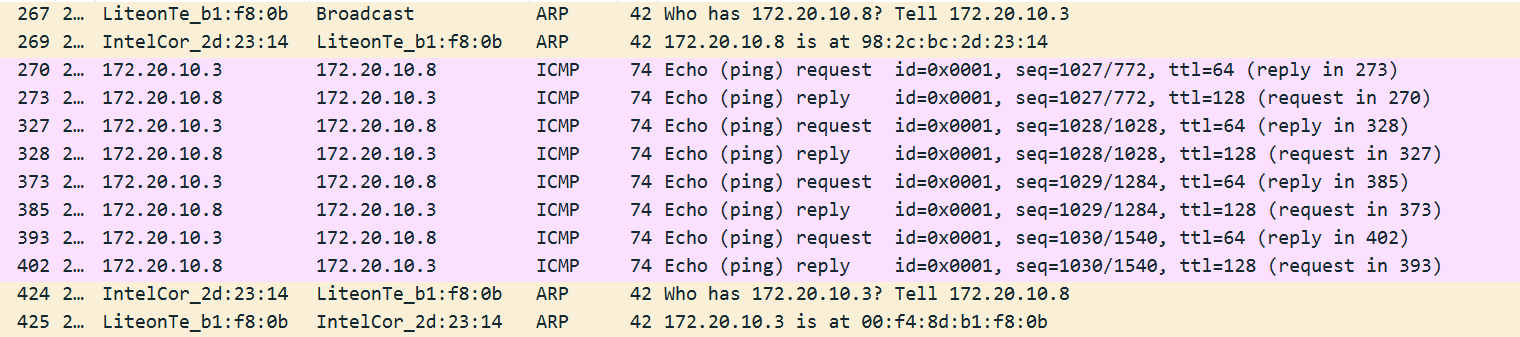
发送端IP地址：发送方设备的IP地址；

目标MAC地址：接收方设备的硬件地址。

目标IP地址：接收方设备的IP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；**

此时能捕获ARP报文，267为本机寻找主机B 172.20.10.8 的MAC地址的广播请求信息，269为主机B的单播应答信息携带自己的MAC地址。得到主机B的ip地址和mac地址的映射之后，才发送icmp数据包。

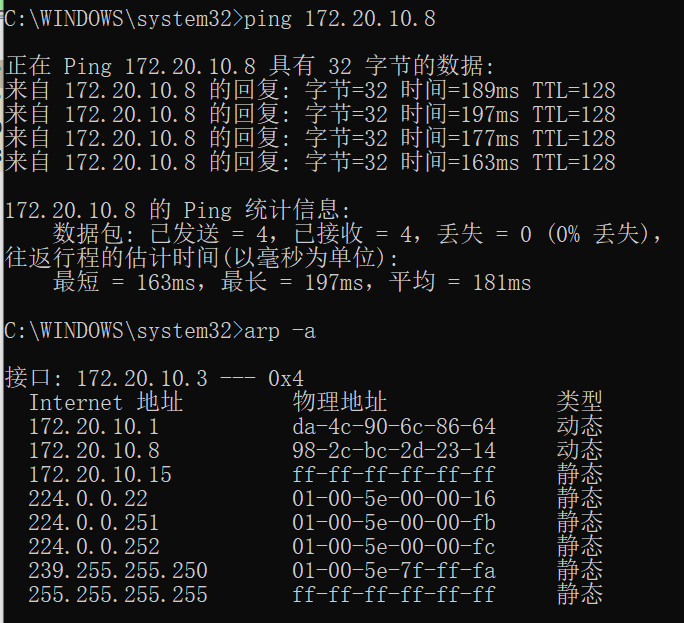


在检测报文发送完毕之后又出现的ARP报文。该ARP报文为单播发送。

查找后续发送arp的原因：初始猜测为arp老化，需重新寻找mac地址，但查阅资料发现，arp通常在电脑的老化时间应该是20分钟。但是在此期间，需要不断的刷新arp。也就是说arp的刷新会依靠arp报文的发送来刷新。但是这个时候，arp报文的发送，作用在于确认对端是否还在线，而不是要去寻找对端的mac地址。所以可以直接指定mac地址以及ip地址，如果对端在线，那么本端则刷新arp缓存。

* **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；**

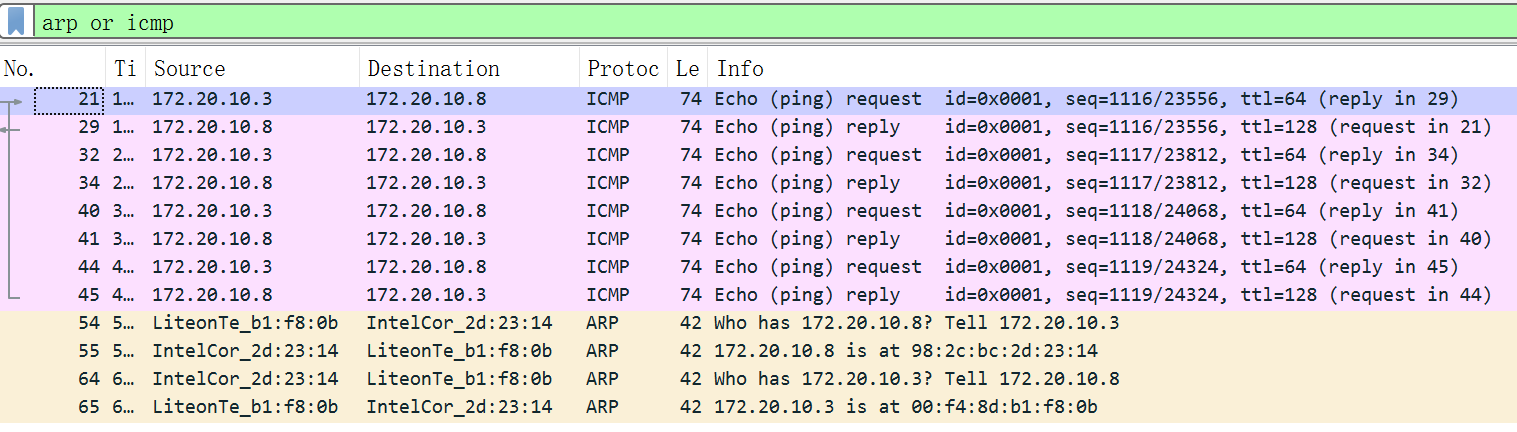
再次出现主机B对应的MAC地址。证明上文中的ARP协议更新了ARP映射地址表。本机A添加了主机B的IP地址和MAC地址的映射。



* **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；**

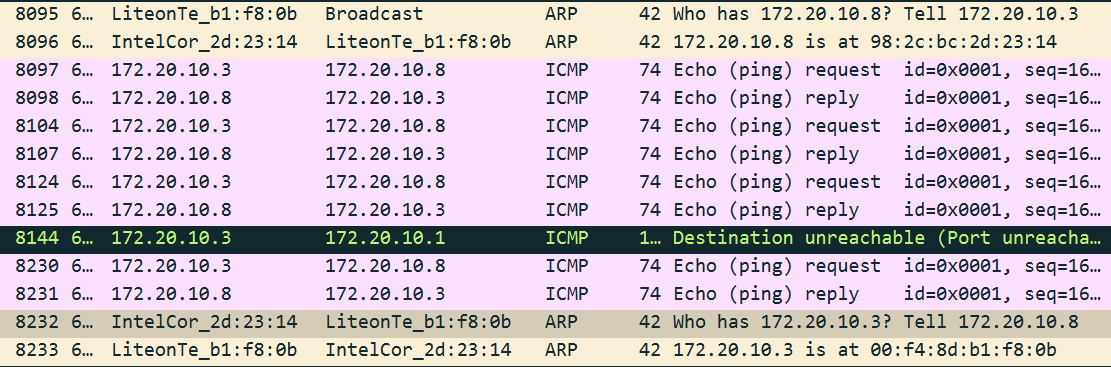
此时在ICMP之前已无捕获ARP报文，ICMP之后捕获的ARP报文原因见前文描述。

经过第一次的ping操作，本机ARP地址映射表上已经有与主机B的IP地址所对应的MAC地址了，再次发送ping报文时，从本机ARP地址映射表中得到其MAC地址，故不需要通过ARP协议在局域网中进行广播寻找其MAC地址了。



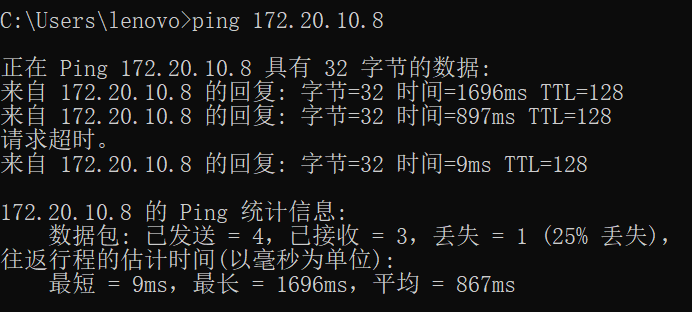
* **主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。**

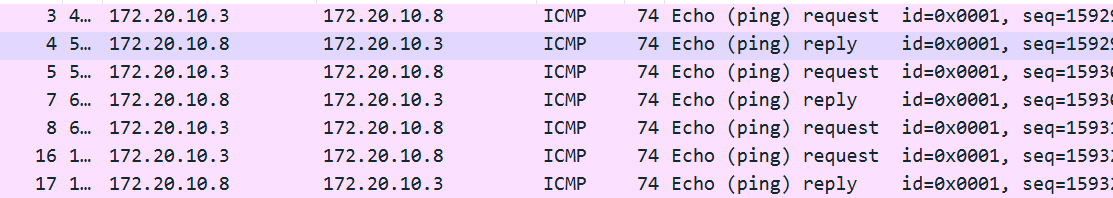
此时可以捕获ARP报文，本主机会发广播请求MAC地址，证明此时ARP地址映射表中已经没有主机B的IP地址和MAC地址的映射了，其原因是5分钟主机A上和主机B停止进行任何数据通信，而之前得到的映射是动态ARP表项，故地址到达老化时间或接口关闭，删除了相应的动态ARP表项。



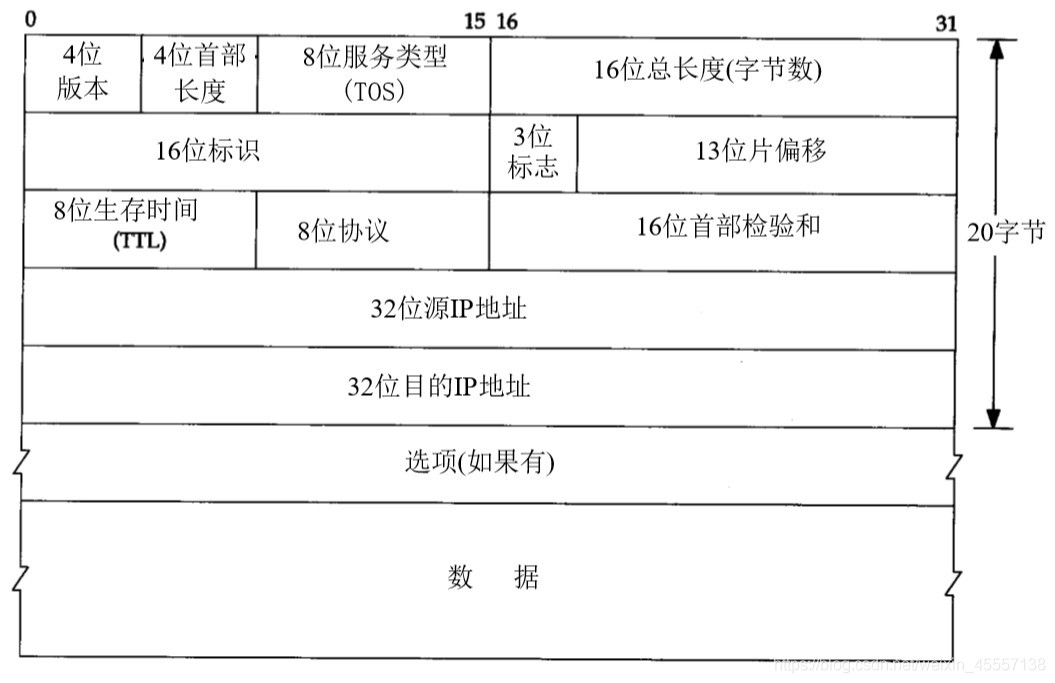
**4、IP协议分析**

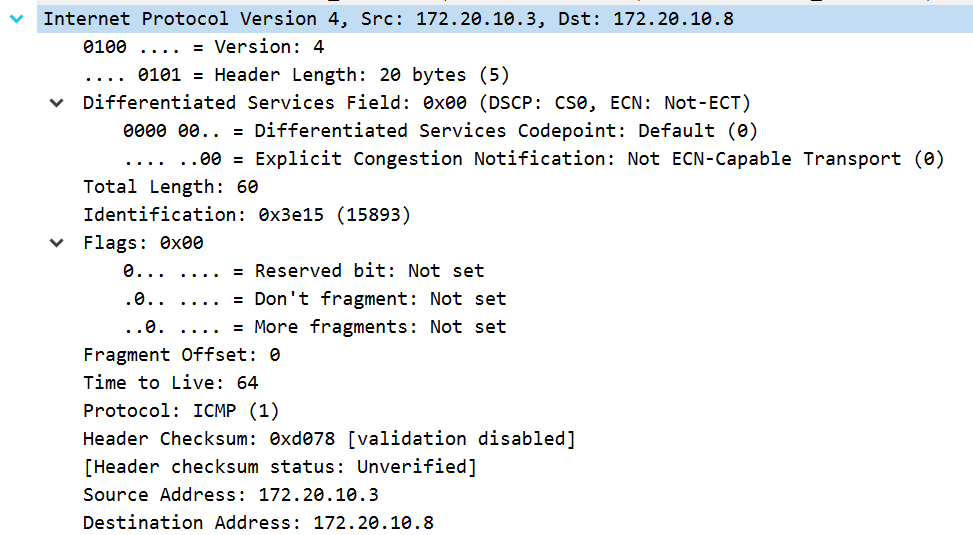
* **从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较;**





选择No.3的icmp报文：icmp报文基于IP协议。





目的IP地址

源IP地址

首部校验和

不进行分片

协议

存活时间

分段偏移

保留位

标志

标识符

总长度

服务类型

首部长度20个字节

版本号

版本Version:4 这里指的是IPv4

首部Header Length:20 bytes:IPv4的首部是固定的，就是20字节。

区分服务：占8位，只有在使用区分服务时，这个字段才起作用

总长度Total Length:60,代表IP报文总长度，报文总长度不能超过1500字节，否则需要分片。1500字节的限制是以太网在**数据链路层**带来的。IP数据部分最大长度1480，头部20字节。

标识：占16位，IP软件在存储器中维持一个计数器，每产生一个数据报，计数器就加1，并将此值赋给标识字段

Don’t fragment:为1表示不能被分割，为0表示可以。

More fragments:表示没有后一个分片。

片偏移：占13位，片偏移指出：较长的分组在分片后，某片在原分组中的相对位置。也就是说，相对用户数据字段的起点，该片从何处开始。片偏移以8个字节为偏移单位。这就是说，除了最后一个分片，每个分片的长度一定是8字节（64位）的整数倍。

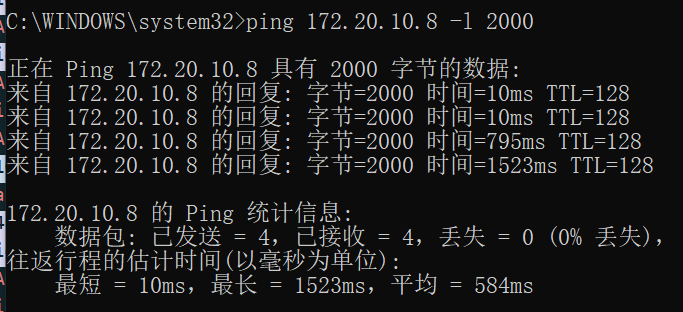
生存时间Time to live:代表还剩余多少跳被丢弃，即还可以经过多少个路由器，两边都是64。设置该字段的目的在于防止网络环路。

Protocol:上层的协议，比如tcp,udp，icmp。

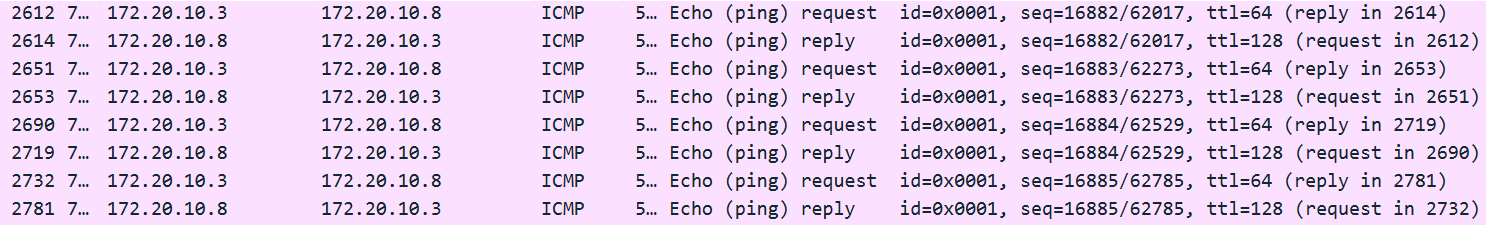
首部校验和：16位，这个字段只检验数据报的首部，但不包括数据部分

Source，Destination:源地址,目的地址。

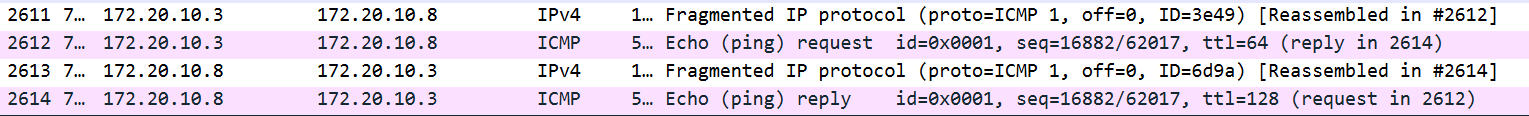
* **使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析分片和重组过程。**



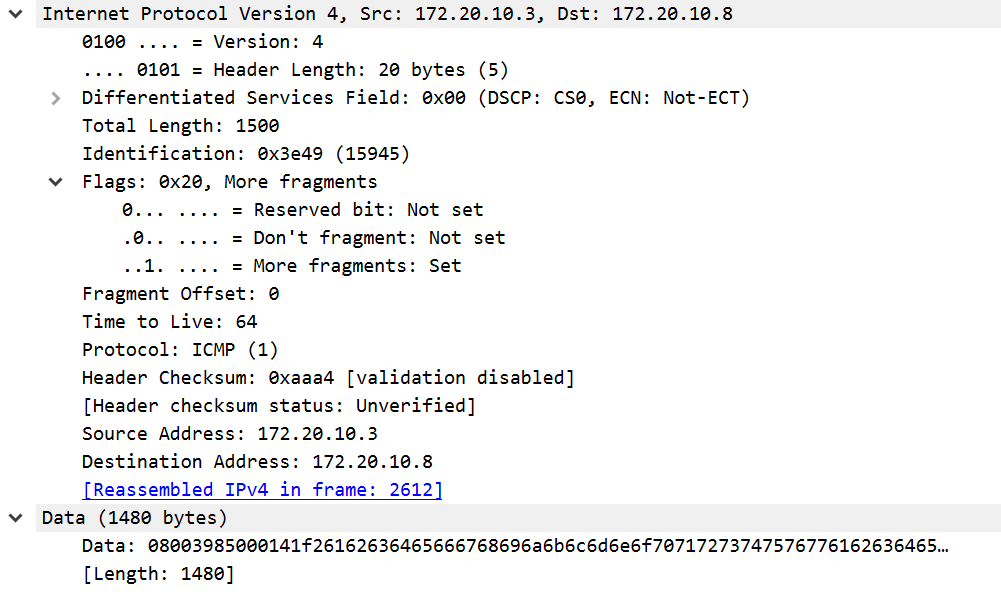
全部ICMP协议：



捕获IP分片：



2611:IPv4

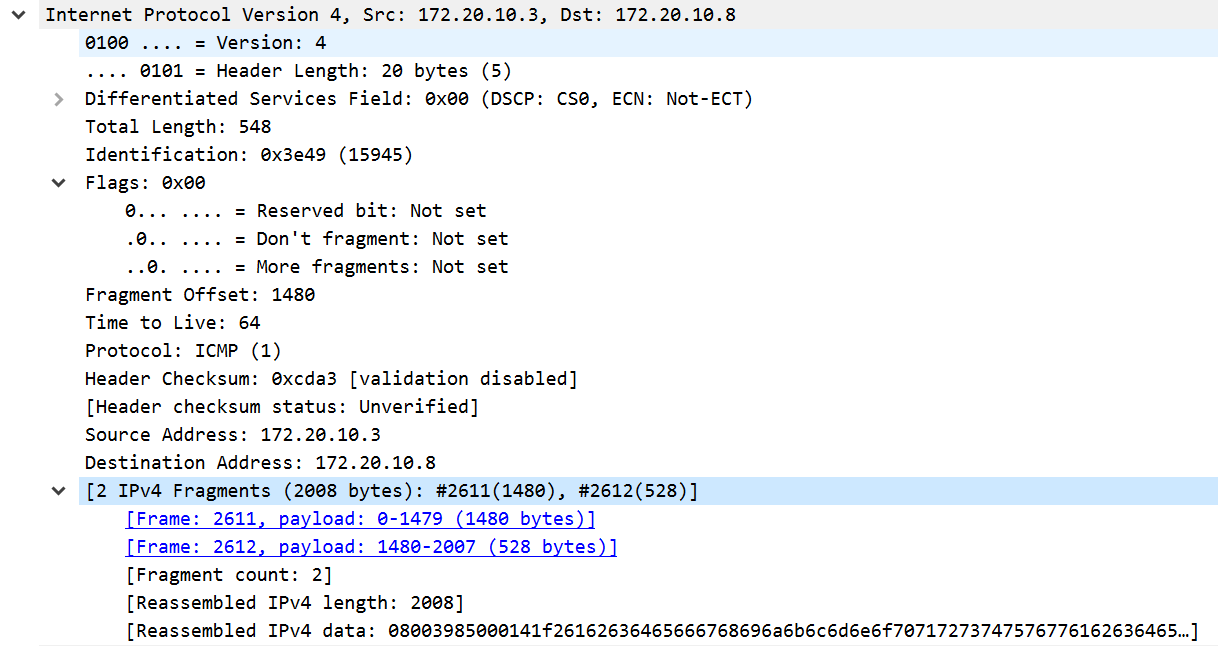


数据长度为1480字节，加上IP头部20字节，到达最大报文长度1500字节

片位移为0，这是第一个分片

表示这个数据包有后一个分片

2612:ICMP



片位移为1480，这是第二个分片，也是最后一个分片

表示这个数据包没有后一个分片

IP首部占用20个字节，ICMP首部占8个字节，所以捕获ICMP包大小最大为1472字节。

1480=1452+20(IP首部)+8(ICMP首部)、528+1472=2000

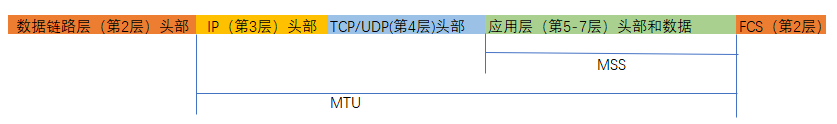
最大传输单元和最大报文大小：

1480=1514-14-20（以太网帧大小-数据链路层头部-IP头部）

最大传输单元（MTU）：指由IP包头和数据部分组成的IP数据包长度。

最大报文长度（MMS）：是指TCP报文段内数据净载的最大长度，也即上层协议交付给TCP的每个数据单元的最大长度。

一般以太网MTU都为1500, 所以在以太网中, 往往TCP MSS为1460(需要减去IP数据包头的大小20Bytes和TCP数据段的头20Bytes)



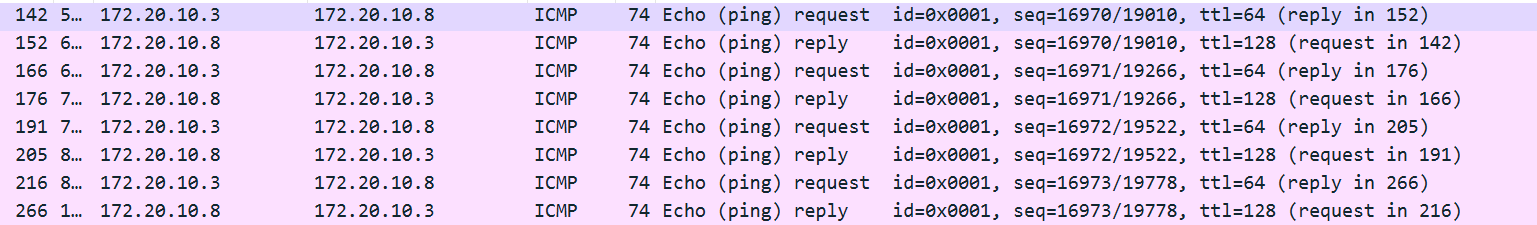
1. ICMP协议分析

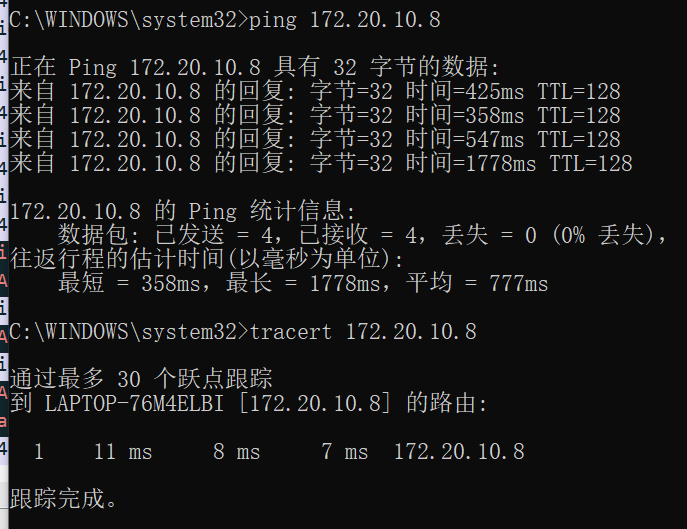
通过ping和tracet命令，了解ICMP协议的使用。

* 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。

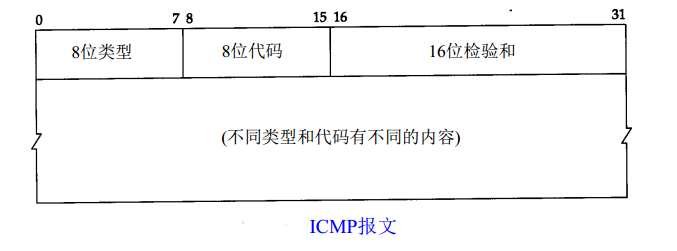
捕获8个icmp数据包（请求4个，应答4个）

ping监测通讯信息是否可达，不可达就通讯断开，交换机发送5次，windows发送4次，用到了ICMP协议。产生错误的原因：目的主机有防火墙，ping不回去，目的主机拒绝接受ICMP，不应答，或路由器路由表有问题。



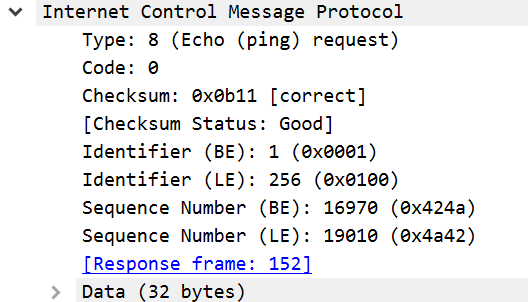


ICMP报文格式：





142 ：ICMP请求数据包：



识别码：BE表示用内存低位是数据高位

LE表示内存中低位是数据低位

数据部分

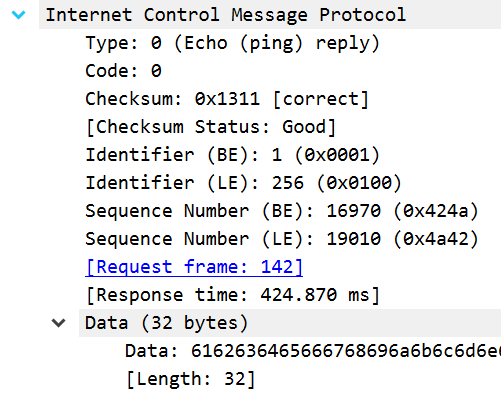
校验和

代码：8位字段，记录发送特定类型的ICMP报文的原因

报文类型

数据部分：包括差错报文的数据部分携带的信息可以找出引起差错的原始报文，查询报文的数据部分携带了基于查询数据的额外信息

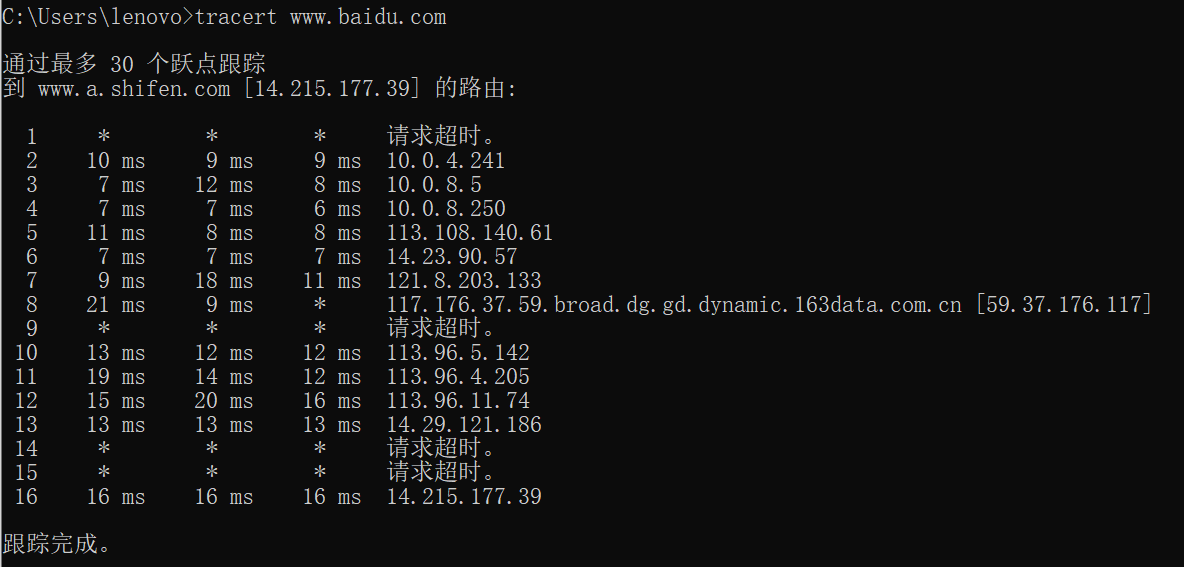
152：ICMP应答数据包：



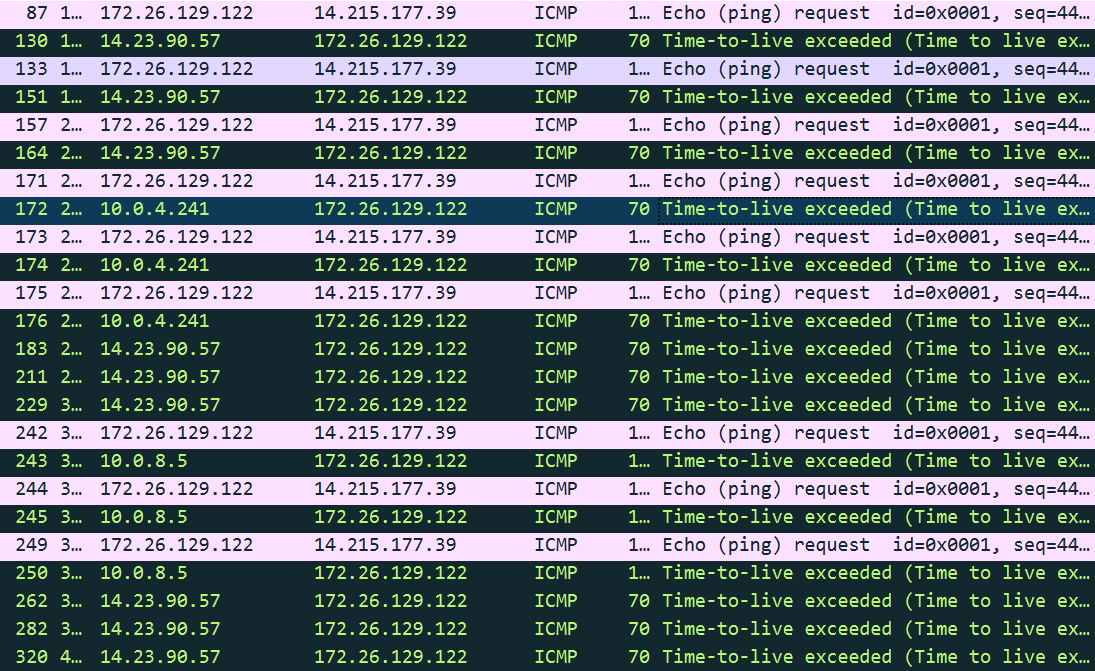
* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。

Type=8和type=0的ICMP响应数据包格式见上文。

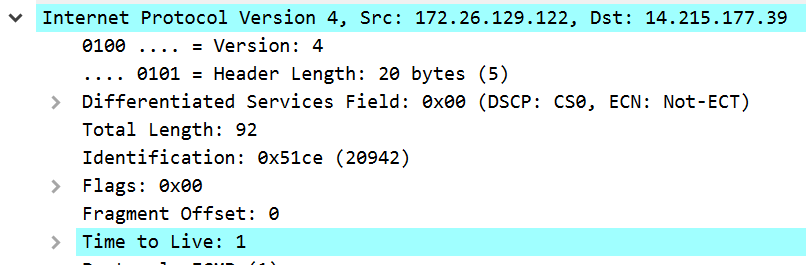
tracert www.baidu.com:



捕获数据包：

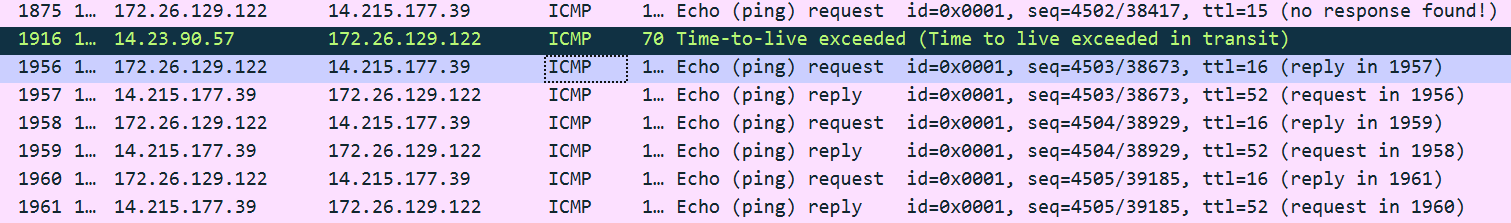


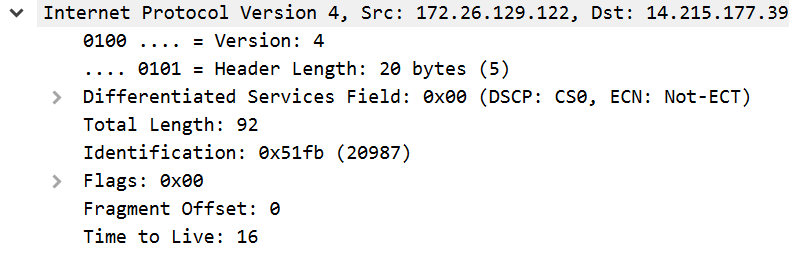
tracert 命令：先发送 TTL 为 1 的回应数据包，当数据包上的 TTL在路由器收到后TTL自动减1 ，一旦某个路由器将TTL减1后，等于了0，路由器应该将“ICMP Time Exceeded”的消息发回源计算机，源计算机就根据收到的信息判断达到的路由器和所用时间。

No87icmp请求：

下次再次发送数据包时，将TTL递增 1，继续上述测试，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL过期的数据包，这在 Tracert 实用程序中看不到，我们会显示请求超时的请求信息。请求消息会发三次（使用相同的ttl值），若没有reply消息返回，就把ttl加1，继续发出。直到最后终端的响应为止。

最后一次：捕获数据包：



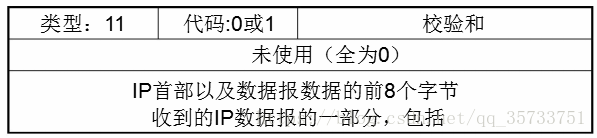
No1956：

可见ttl=16，一共经过16个节点，与tracert所得的结果个数相同

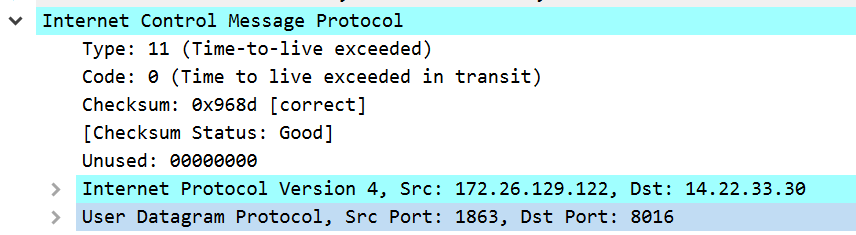


Type=11的icmp数据包:no130：

超时报文格式：



当主机A给主机B发送一个数据报文时，该数据报文在网络中会有一个TTL生存时间字段，就是数据报文每经过一台路由器,TTL字段值就会减1,当路由器收到数据报文后TTL字段值减1后为0的话，那么该路由器就会把数据报丢弃并向主机A发回一个ICMP超时报文，这种机制有效的防止了路由环路，也就是解决了数据报在路由器之间一直转圈的问题。



IP首部

以及数据包前8个字节

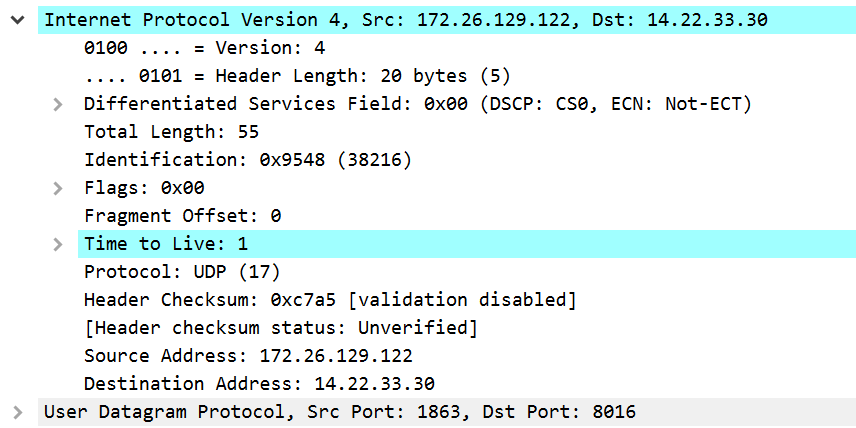
未使用

校验和状态是好的

校验和：表示校验和是正确的

代码

类型



1. **实验小结**

**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？**

一开始通信时能够捕获到添加主机B的MAC地址的ARP报文，但短时间再一次请求通信时，主机ARP地址映射表中含有目的主机的IP及其对的MAC地址，则无需广播寻找，此时不需要在发送ARP报文，可能捕获不到。但是一段时间后动态ARP表项会老化或被更新，又需要发送arp报文。所以有时候能捕获，有时候不能。

**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？**

①127.0.0.1是本机的环回地址。ping 127.0.0.1时，不需要经过网卡，这是用来测试TCP/IP协议栈的，在IP层就进行了回环，不能捕获ICMP报文。

②ping 本机IP地址不能收到报文。因为数据报从网卡协议的最顶层（应用层）接受数据到传输层到IP层，数据报到达IP层的时候，IP层会检测数据包的目的主机为本机，会将数据包送回环回接口，然后送回本机。以上几个层次自上而下构成一个IP协议栈，通过ping本机可以测试IP协议栈（网卡协议）是否正常。

**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？**

Destination Host Unreachable：目标主机不可达。返回该信息的原因可能如下：①局域网使用DHCP动态分配IP地址时，DHCP出现故障或者失败。②子网掩码设置错误。③路由表返回错误信息，本地系统没有到达所需目标的路由，或者远程路由报告没有目的地的路由（Reply From <IP address>:~）。④没有指明网关，无法发送出去。

Request timed out：请求超时。此消息表示在1秒的默认时间内没有收到Echo Reply消息。造成该情况的原因可能如下：网络堵塞，设置了防火墙使ICMP包被过滤，ARP请求失败，路由错误或未返回信息丢弃，对方关机，目的主机到源主机不可达但源主机与目的主机可通信等。

**4、请通过实验验证：**

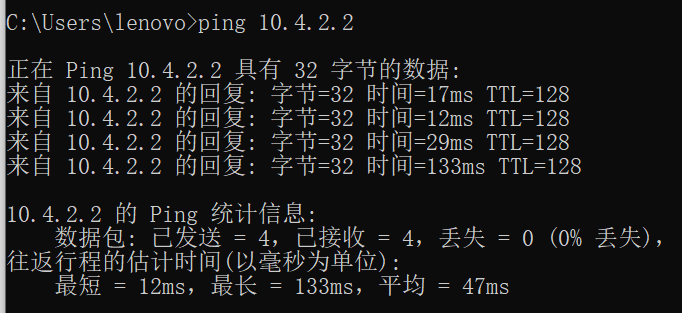
**主机如果不设置“网关”，同一网段内的主机可以相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。**

配置本机地址为10.4.3.3，另一台主机配置ip地址为10.4.2.2，子网掩码均为255.255.254.0，不设置网关。此时IP地址分别与子网掩码进行与运算得到均为10.4.2.0，两个主机同属于一个网段。

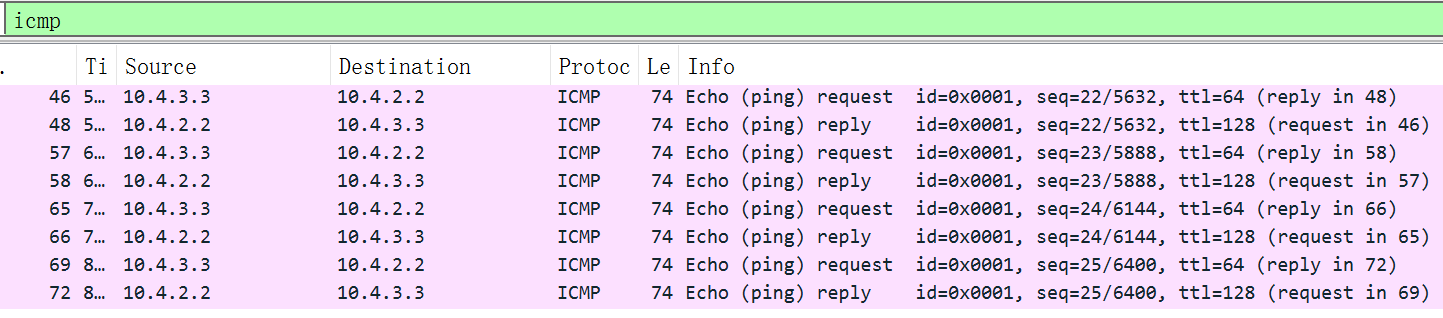
同网段主机通信：主机A与主机B通信，主机A首先要封装需要发给主机B的数据包，主机A能得到自己的IP地址和MAC地址，主机B的IP地址。主机A需要获得主机B的MAC地址。这时主机A就通过比较上面已经封装好的源IP和目标IP，通过子网掩码计算，发现源IP和目标IP恰好在同一个IP网络内。

获取主机B的MAC地址：首先主机A就向本网段发一个ARP请求，这个ARP请求包中包括主机A的源IP地址，源MAC地址，目标主机B的IP地址，而目标MAC地址为广播MAC地址（全部为1），整个局域网的所有主机都能收到这个请求MAC地址的数据包。在主机B收到此ARP请求后，构建一个包括自己的MAC地址的ARP回应包，回应给主机A。此时完成封装。

主机A向网络内发出这些数据包，因为目标地址在本网段，所以本网段所有主机都能收到这个数据包，不需要通过网关转发，最后只有真正的目标主机B能够打开这些数据包。 此时相互ping可通。



捕获的数据包：

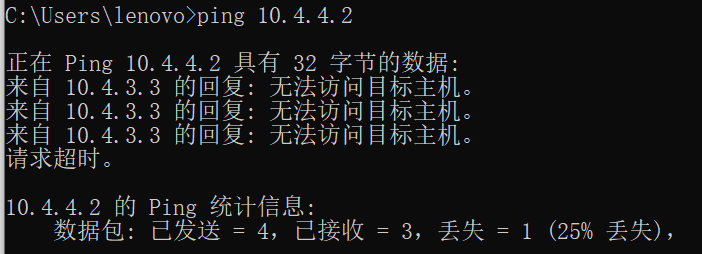


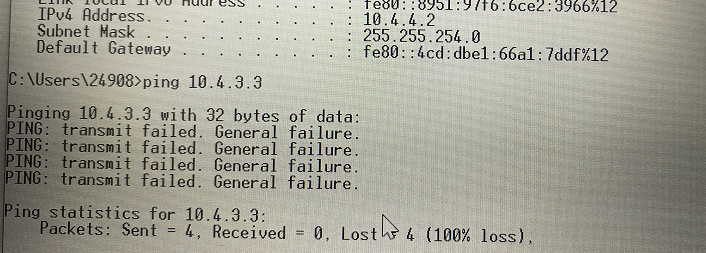
**不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。**

配置本机地址为10.4.3.3，另一台主机配置ip地址为10.4.4.2，本机子网掩码为255.255.254.0，不设置网关。此时IP地址分别与本机子网掩码进行与运算得到10.4.2.0和10.4.4.0，两个主机不属于同一个网段。

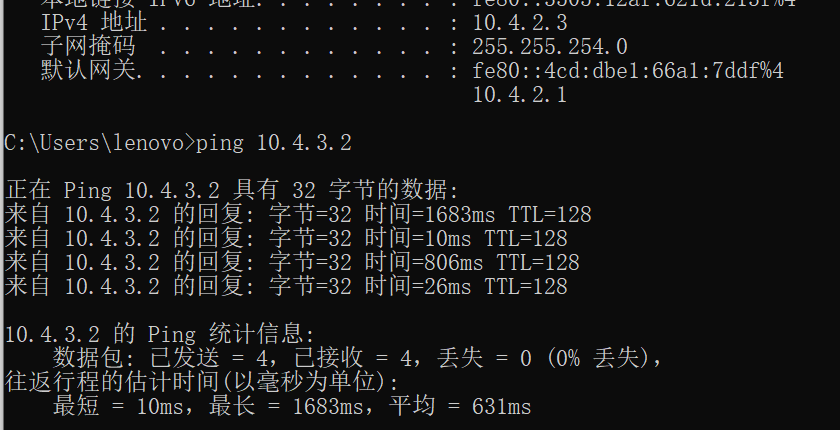
显示目的主机不可达，不同网段通信需要经过网关转发获得下一级的MAC地址，而此时不设置网关，则找不到目标主机的MAC地址，则提示无法访问目的主机。

不同网段通信：主机A在准备发向主机B的数据中，封装好自己的IP地址和MAC地址和目标主机B的IP地址。主机A用ARP去广播请求网关MAC地址，因为网关和本机在同一网段，网关能够收到这个ARP请求并能正确回应给主机A，这时主机A在数据包中封装好自己的IP地址和MAC地址，同时也封装好目标主机B的IP地址和网关的MAC地址，把数据包从网卡发出去，因为目标MAC是网关的，所以网关收到这个数据包后，发现目标MAC是自己，而目标IP却是别人，所以它不可以再往上打开这个数据包，它要做的工作就是把这些数据包发给下一跳路由器（如果网关自身就是一台路由器的话），如果网关是一台普通PC，那么它就发给路由器，让路由器把这些数据包正确传输到远程目标网络，到达远程网络后，它们的网关再将数据包发给数据包中的目标。

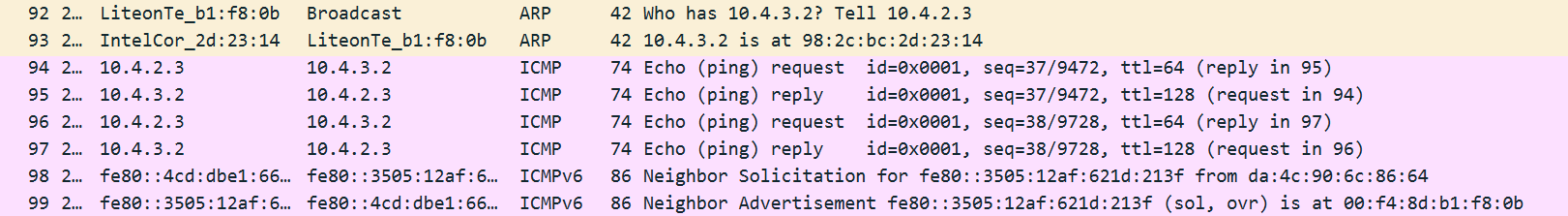
本机：

另一台主机：

**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。**



捕获数据包：获取对方主机的MAC地址为98:2c:bc:2d:23:14

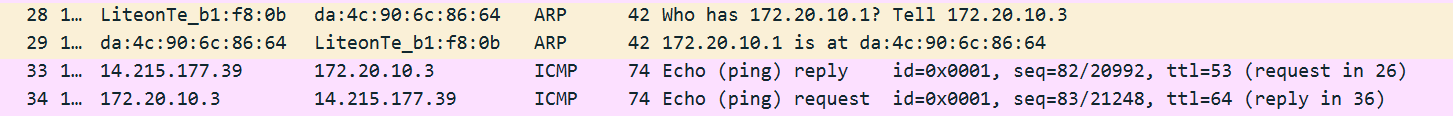


**不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。**

Ping [www.baidu.com](http://www.baidu.com)：为能通信的不同网段的主机之间通信



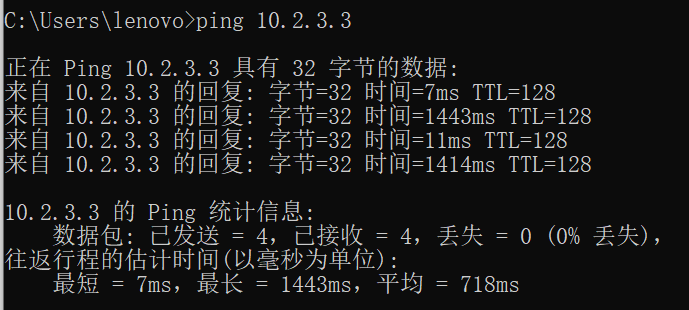
看到本网关的MAC地址为da:4c:90:6c:86:64

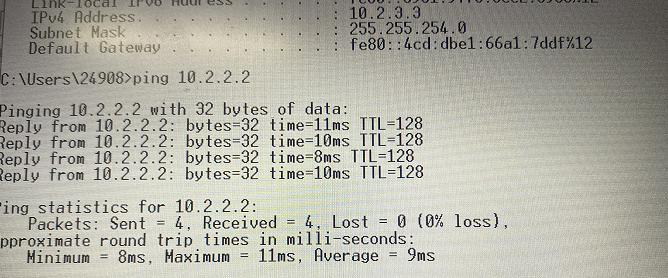


总结：在网段通信时，数据包中的地址就是源IP，目标IP，源MAC，目标MAC，根本用不到网关。当检测到需要把数据包发到远程网络时，目标MAC就必须改变了，在还没有出内网时，目标MAC必须写成网关的MAC地址发出去，当网关收到时，再把目标MAC地址改成下一跳的MAC地址发出去，同时源MAC地址要始终保持为发出端口的MAC地址（回应报文可以依靠它路由回去），而源IP及目标IP不曾改变（用于判断收到数据包的本机IP和数据包IP是否一致，若一致不转发），就算到达了公网上，目标MAC仍然在不断改变着，直到最后，这个数据包到达目标IP的网络。

**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。**

本机：

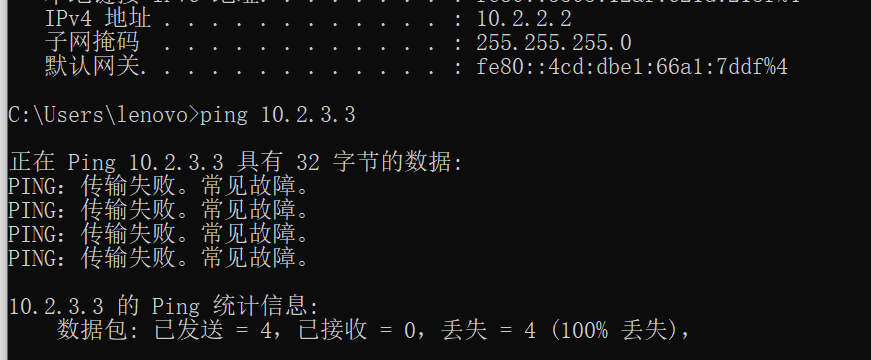
另一主机：

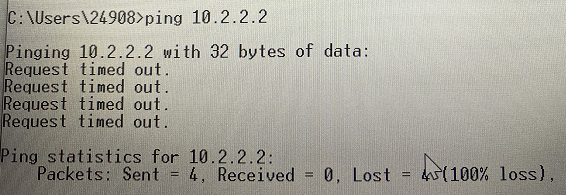
本机arp：

配置本机地址为10.2.2.2，另一台主机配置ip地址为10.2.3.3，网络号均为23位，本主机子网掩码为255.255.254.0，不设置网关。此时IP地址分别与本机子网掩码进行与运算得到均为10.2.2.0，两个主机同属于一个网段。故本机获取另一台主机的MAC地址不需要网关，只需向本网段发一个ARP请求，本网段上的主机匹配后即可返回应答。此时arp表上也有10.2.3.3对应的映射。

**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。**

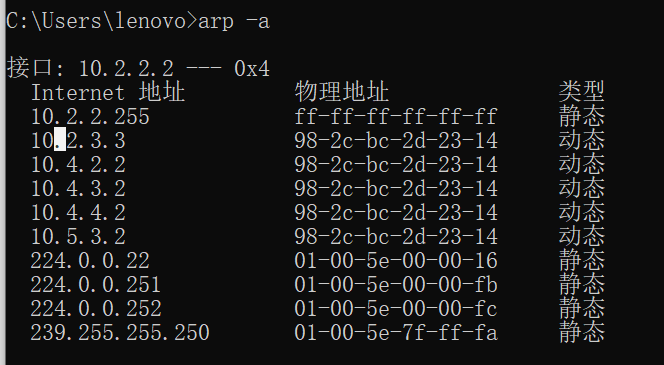
配置本机地址为10.2.2.2，另一台主机配置ip地址为10.2.3.3，网络号分别为24位和23位，则子网掩码分别为255.255.255.0和255.255.254.0，不设置网关。此时**IP地址分别与本机的子网掩码进行与运算**得到分别为10.2.2.0和10.2.3.0，两个主机不同属于一个网段。所以通信失败，**且无对方的物理地址**。

本机：

另一台主机：

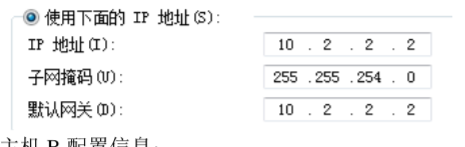
结果另一台主机ping本机后查看本机arp，找到主机B。

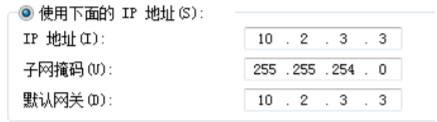
过程：主机B将对方的IP地址与自己的子网掩码进行与运算，发现对方的和自己的在同一个网段上（10.2.2.0），所以B在这个网络上广播获得A的物理地址，并向A发送报文，但A不能回复，故B上显示请求超时。因为B能向A发送报文，故双方主机均能添加对方MAC地址。

Arp：

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。

**网络号相同：**

本机：

另一台主机：

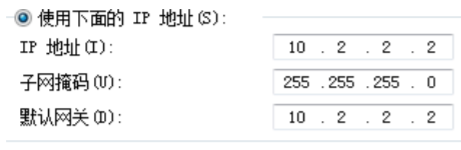
实验前删除前面的arp信息。

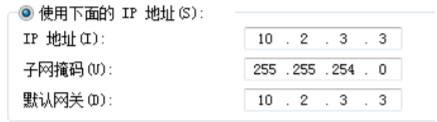
相互之间可以ping通，且本机和主机B的arp表上均再次出现对方的MAC地址。

捕获数据包：捕获到两部主机的arp广播请求对方MAC地址的数据包。

结果分析：目的主机A (10.2.2.2）和目的主机B(10.2.3.3）各自将对方的IP地址与自己的子网掩码进行与运算，发现对方的都和自己在同一个网段(10.2.2.0)上，所以能够不通过网关通信，通过ARP获取对方MAC地址。

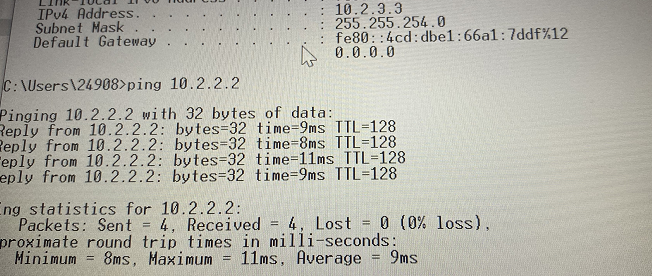
**网络号不同：**

本机：

另一台主机：

实验前删除前面的arp信息。

本机：

另一台主机：

此时能ping通。本机和主机B的arp表上均再次出现对方的MAC地址。并且捕获到两部主机的arp广播请求对方MAC地址的数据包。

结果分析:主机A将目的主机B的IP地址与自己的子网掩码进行与运算之后，得到的网络号为10.2.3.0，与自己的网络号(10.2.2.0）不一样。所以当源主机企图向其他网络的主机进行通信的时候，无法直接通信时，就要将IP分组转发给默认网关，由默认网关转发给其他的路由器，这样ARP仍然能够获得目标主机的MAC地址。而实验中设置的默认网关为本机ip地址，所以能在本机捕获到默认网关寻找给其他的路由器的arp报文。