**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 指导教师 潘冰

实验项目编号 实验项目类型 实验地点 b402

学生姓名 胡靖 学号 2019053753

学院 智能科学与工程学院 系 专业 软件工程

实验时间2021 年11月2日 上 午～11月9日上午 温度 ℃湿度

1. **实验目的**

* 理解链路层、网络层主要协议格式，以及协议的工作原理
* 理解网关和子网掩码概念
* 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
* 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程

1. **实验内容**

* 用嗅探器捕获数据包
* 分析以太网帧、ARP协议、IP协议、ICMP协议
* 分析PING、TRACERT、ARP命令的工作过程
* 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

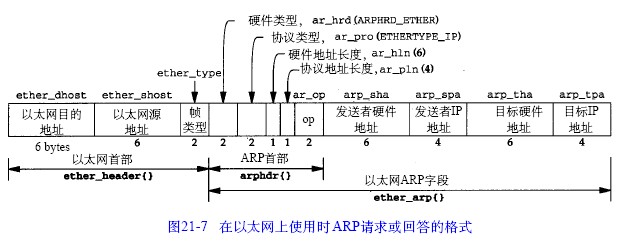
1. **实验原理**

**1**、**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。**

**2、协议**

以太网上使用的ARP协议格式



1. **实验环境**

主机一台，Macbook一台，软路由做主路由，wifi路由器设置为AP模式做有线中继让所有设备位于软路由的网段下

1. **实验步骤**

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，以捕获以太数据帧，记录并分析MAC帧各字段的含义

|  |  |  |
| --- | --- | --- |
| 设备 | IP地址 | MAC地址 |
| 软路由 | 192.168.2.1 | 6a-27-19-a7-5b-b2 |
| AP | 192.168.2.160 | 18-f2-2c-f3-a5-af |
| 主机A | 192.168.2.203 | 2a-16-10-1a-0b-5b |
| 主机B | 192.168.2.173 | 00-e0-4c-68-19-e2 |

软路由：

文本

描述已自动生成

AP路由器：

图形用户界面

描述已自动生成

主机A：

图片包含 图形用户界面

描述已自动生成

主机B：



文本

描述已自动生成

从A主机向B主机发送PING检测报文

日历

低可信度描述已自动生成

捕获的ICMP报文如下：

图形用户界面, 文本, 应用程序

描述已自动生成

以太网数据帧如下：



上面截图中显示了链路层协议，在一行Ethernet II中，Src表示源地址即主机A的MAC地址，Dst表示目的地址即主机B的MAC地址。

对于Destination和Source中地址字段的第一个字节的最低位为I/G，当I/G比特为0是表示单个站地址，为1时表示组地址。



第一个字节的最低第2位规定为G/L位，当G/L=1，表示本地管理，G/L=0，表示全球唯一管理（默认）。





Type为0x0800指IPv4协议，而0x86dd IPv6协议数据，0x809B AppleTalk协议数据，0x8138 Novell类型协议数据等。

3、ARP协议分析

* 进入DOS窗口，用arp -a查看本主机上的ARP表的情况，然后用arp -d删除B的记录

主机A的ARP表：

文本

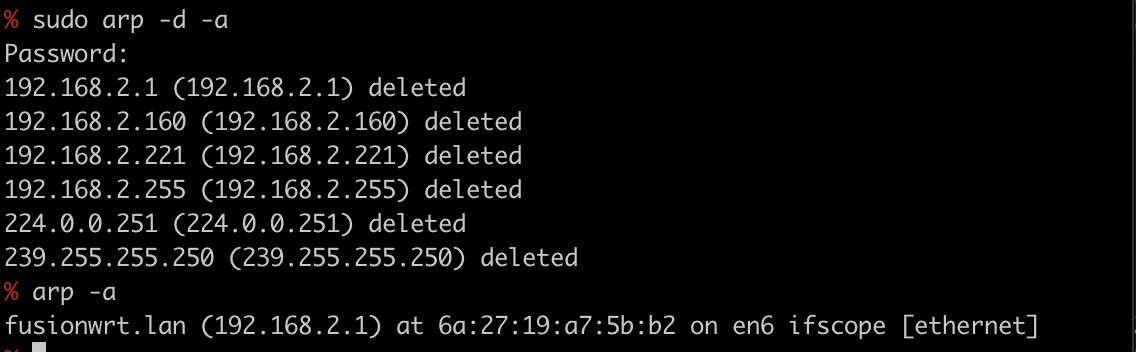
描述已自动生成

主机B的ARP表：

文本

描述已自动生成

删除主机B的ARP表：

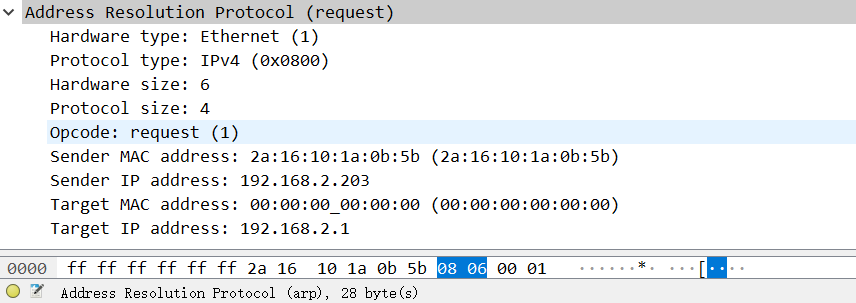


* 运行Wireshark程序
* 把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义

表格

描述已自动生成

标红的第一句的ARP报文段如下



Hardware type：硬件类型，值为1表示以太网地址

Protocol type：上层协议类型，映射IP地址时的值如图0x0800

Hardware size：MAC地址长度

Protocol size：IP协议地址长度

Opcode：操作类型，指定本次ARP报文类型，1表示ARP请求报文，2标识ARP应答报文

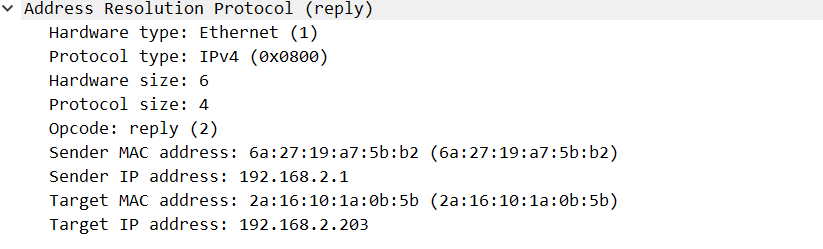
Sender MAC address：源MAC地址

Sender IP address：源IP地址

Target MAC address：目的MAC地址，表示接收方设备的硬件地址，在请求报文中改字段全为0，即00:00:00:00:00:00，表示任意地址

Target IP address：目的IP地址，表示接收方的IP地址

第二句的ARP报文段如下



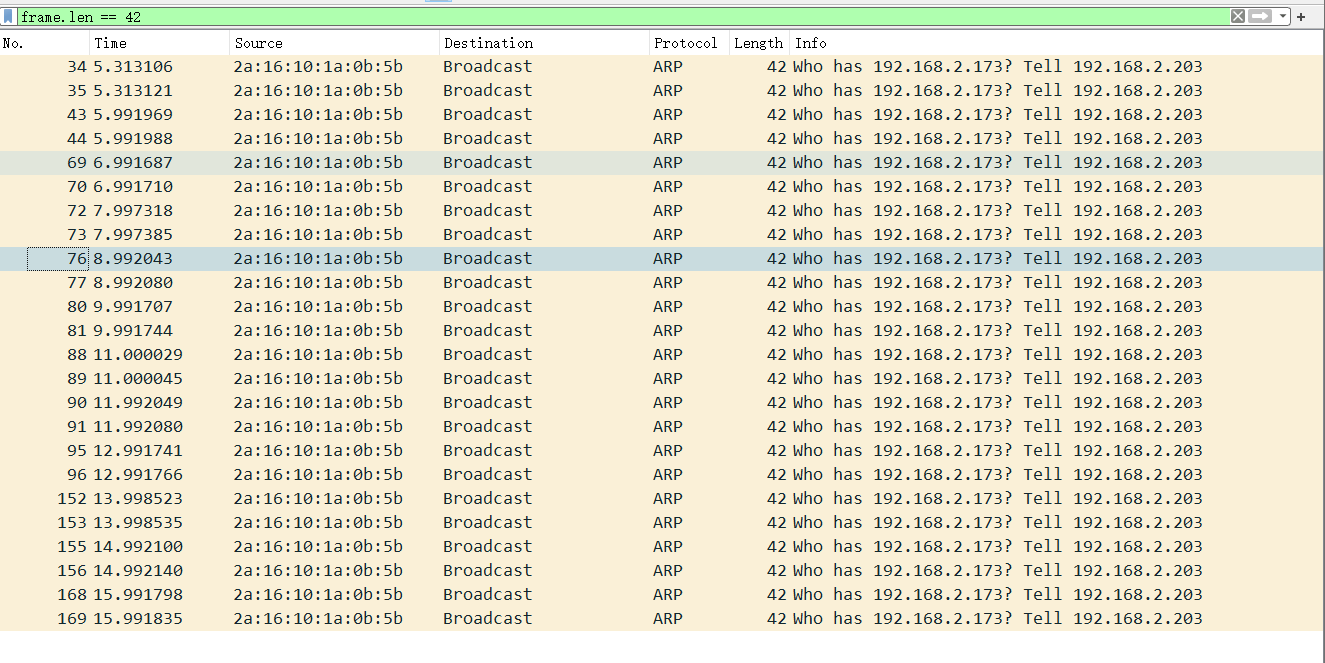
这一段是ARP应答报文，应答给之前发出请求报文的主机

* 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

图片包含 图形用户界面

描述已自动生成

此时发送PING检测报文，发现无法访问主机B，查看wireshark捕获到得ARP报文字段



此时发现全部都是ARP请求报文，以广播的形式发送出去，应该是没有收到主机B的应答

* 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；

一些文字和图案

描述已自动生成

查看ARP表，确实有看到B的MAC地址，同时还有软路由和AP路由器的MAC地址，是因为主机A发送ARP请求报文的时候应该是经过AP路由器在发给软路由最终才被主机B接收到并发送ARP应答报文，因为中间经过很多层，所以主机A在给主机B发送PING检测报文的时候两次都超时了

* 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

表格

描述已自动生成

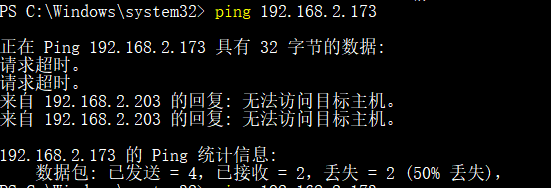
如上图，主机A给主机B发送PING报文，并且捕捉到了ARP报文

图形用户界面, 文本, 应用程序

描述已自动生成

这里主机A并没有发送ARP广播报文，只是给主机B发送了ARP请求报文，是为了确定主机B的ip地址是否有变化，主机B的IP地址没有变化，所以主机B直接发送应答报文

* 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



表格

描述已自动生成

过5分钟之后，主机A会先发一个ARP报文确定自己的IP地址是否发送变化，然后给主机B发送PING检测报文时，发送请求超时的现象，然后主机A又会进行ARP广播报文的发送，至于超时我认为应该是主机B处于待机状态，网络也没有连通（虽然接着网线）

4、IP协议分析(这部分是第二天测试的，因为前一晚发现软路由温度过高关了软路由，第二天重启之后AP路由器无法接收到软路由信号，等到修好之后主机A、主机B以及路由器AP的ip发生了变化)

|  |  |  |
| --- | --- | --- |
| 设备 | IP地址 | MAC地址 |
| 软路由 | 192.168.2.1 | 6a-27-19-a7-5b-b2 |
| AP | 192.168.2.159 | 18-f2-2c-f3-a5-af |
| 主机A | 192.168.2.202 | 2a-16-10-1a-0b-5b |
| 主机B | 192.168.2.173 | 00-e0-4c-68-19-e2 |

* 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

日历

低可信度描述已自动生成

捕获到的ICMP报文，从中可以查看IP数据包

表格

描述已自动生成

查看从主机A给主机B发送PING检测报文时的IP数据报如下：

图形用户界面, 文本, 应用程序

描述已自动生成

对于其中的每一个字段进行分析如下：

Version：版本字段，占4位，指的是IP协议的版本，上图显示为4即当前的IP协议版本号为4（IPv4）

Header Length：首部长度，占4位，单位为4字节，这里表示首部长度占5个4位字节即20字节

Differentiated Services Field：区分服务，占8字节，一般情况不使用该字段，图上就并未使用

Total Length：总长度，占16位，表示为首部长度+数据长度，这里的总长度为60字节，因此数据长度为40字节

Identification：标识，占16位，用来产生IP数据报的表示，通常分片时用，这里因为IP数据报总长度不足以分片，并未使用

Flags：标志，占3位，只有最后两位有意义。最后一位MF，如果MF=1表示后面“还有分片”，MF=0表示最后一个分片；倒数第二位DF，如果DF=0表示分片后的分组允许继续分片，DF=1表示不能分片。上图表示分片后的分组允许继续分片以及这是最后一个分片

Fragment offset：片偏移，占13位，指出较长的分组在分片后，某片在原分组中的相对位置，并且是以8个字节为偏移单位，这里为0表示没有偏移即第一个分片

Time to Live：生存时间，占8位，记为TTL（Time To Live），指示数据报在网络中可通过的路由器数的最大值，这里为128表示可以通过128个路由器寻找目的主机，超过128个路由器发送的数据报将被丢弃

Protocol：协议，占8位，指出此数据报携带的数据使用何种协议，以便目的主机的IP层将数据部分上交给那个协议处理，这里表示的是ICMP协议

Header Checksum：首部校验和，占16位，用于检验数据报的首部

Source Address：源IP地址

Destination Address：目的IP地址

书上的IP数据包的格式如下：

图片包含 日程表

描述已自动生成

可以看出刚刚捕获的IP数据报和书上的格式完全一样，仅仅是确实了可变部分

* 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

主机A给主机发送2000字节的数据：

电脑萤幕

中度可信度描述已自动生成

通过wireshark抓包获得的数据报信息如下：

表格

描述已自动生成

标红部分为主机A给主机B发送PING检测报文的阶段，查看第一个数据报捕获的IP数据报如下：

图形用户界面, 应用程序, Word

描述已自动生成

可以看到IP数据报总长度为1500字节，因此数据部分的长度为1480字节，最后一个红框进行了标记

第二个红框显示了标识位，后面分片重组将依据这个标识位，

第三个红框中DF=0表示能分片，MF=1表示还有分片

第二数据报捕获的IP数据报如下：

图形用户界面, 文本, 应用程序

描述已自动生成

这里的数据报总长度为548字节，除去ICMP首部8个字节，就是原始数据的520字节，加上之前的1480字节正好为2000字节

最后一个红框中展示了改分片的偏移为1480字节

5、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

从主机A想主机B发PING检测报文，捕获ICMP请求数据包和应答数据包如下：

表格

描述已自动生成

查看其中的具体数据：ICMP请求数据包

图片包含 图形用户界面

描述已自动生成

Type：类型，占一字节，标识ICMP报文的类型，图中类型8表示发送(ping)请求

Code：代码，占一字节，标识对应ICMP报文的代码，与类型字段一起共同标识了ICMP报文的详细类型。

Checksum：校验和，这是对包括ICMP报文数据部分在内的整个ICMP数据报的校验和，以检验报文在传输过程中是否出现了差错

Identifier：标识，占两个字节，用于标识本ICMP进程

Sequence number：序号，与标识一起用于匹配请求和应答

ICMP应答数据包

形状

描述已自动生成

这里的Type=0表示回显应答

ICMP数据包数据格式如下：

表格

描述已自动生成

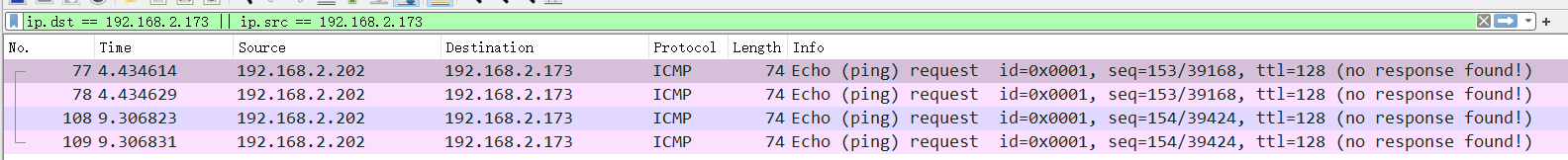
因此捕获的ICMP请求数据包和应答数据包满足ICMP数据包标准格式

后面尝试捕获返回差错信息的ICMP报文：让主机B处于休眠状态，主机A给主机B发送PING检测报文

文本

描述已自动生成

捕获的ICMP报文如下：



图片包含 图形用户界面

描述已自动生成

发送了PING检测报文但是并未检测到目标主机，控制台显示请求超时，而wireshark并未捕捉到应答数据包，这是因为主机B处于休眠状态，网络不通

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

使用tracert命令跟踪局域网内的主机会导致跟踪路径过段导致测试结果没有意义，因此选择其他主机作为跟踪对象，这里选择自己购买的云服务器进行跟踪，

文本

描述已自动生成

图形用户界面, 应用程序, 表格, Excel

描述已自动生成

Type=8时的ICMP响应数据包格式：此时表示请求回显，即发送Ping请求

图形用户界面, 文本, 应用程序

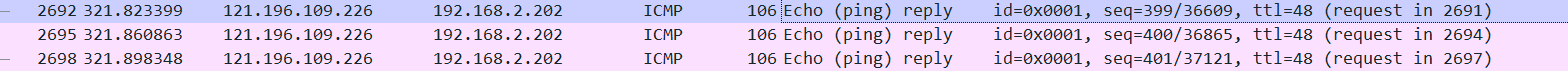
描述已自动生成

Type=11时的ICMP响应数据包格式：此时表示Code=0，表示TTL超时

图形用户界面, 文本, 应用程序

描述已自动生成

Type=0时的ICMP响应数据包格式：此时表示回显应答，即Ping应答



形状

低可信度描述已自动生成

【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：经过测试A能捕获到ARP报文的情况是给其他主机发送PING检测报文的情况，如果对本主机自己发送PING报文，将不能捕获到ARP报文

图片包含 日历

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成

具体原因是：主机已经保存了自己IP地址和MAC地址的映射，因此不需要发送ARP报文来确认。

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：ping 127.0.0.1时，数据包并没有到达网口，因此捕获不到ICMP报文，同时ping本机的时候，虽然用这种方法来判断网卡是否正常工作，但实际上并没有发送到网卡，两种方式都是经过环路来进行处理的

图形用户界面, 应用程序

描述已自动生成

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：信息“Request timed out”是因为所经过的路由器的路由表中具有到达目标的路由，而目标因为其他原因不可到达，这是就会出现“Request timed out”，具体原因如下：目标主机不在线、防火墙拦截、IP安全策略限制、网关设置错误。以下是目标主机不在线的例子

文本

描述已自动生成

而信息“Destination Host Unreachable”表示目标主机不存在或者没有和对方建立连接，并且目标主机不存在于本主机的路由表中。以下是目标主机不存在的例子：

文本

描述已自动生成

不知道为何在windows下两种情况显示相同，但是实际上它们有着很大的区别

4、请通过实验验证：

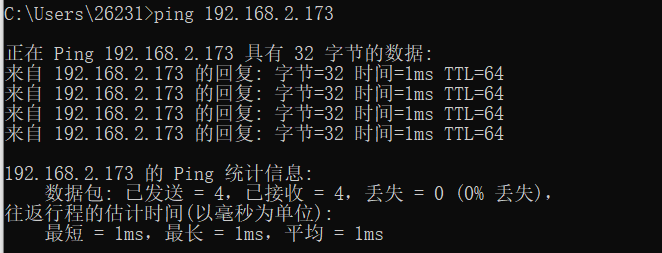
* + 主机如果不设置“网关”，同一网段内的主机是否相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。

答：手动设置IP地址和子网掩码，将默认网关不填

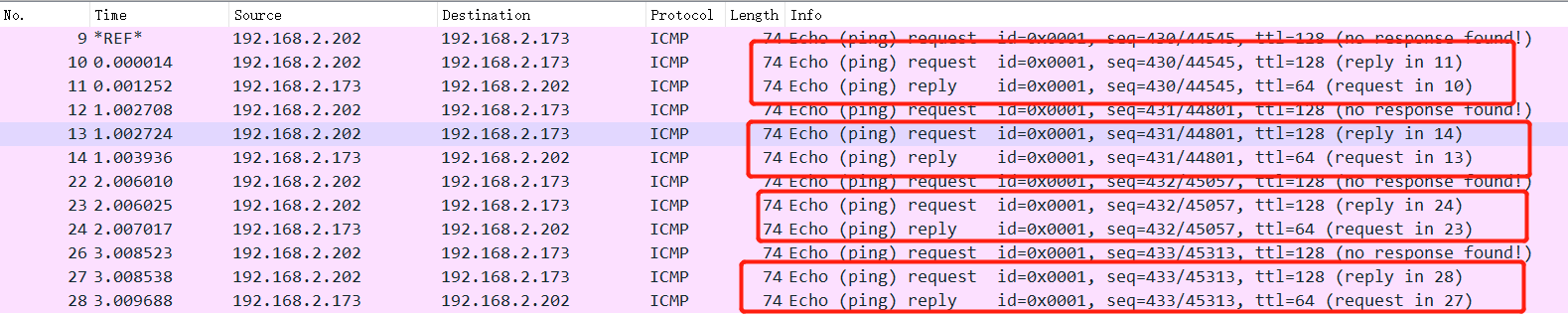
图形用户界面

描述已自动生成

接着用主机A向主机B发送PING检测报文：

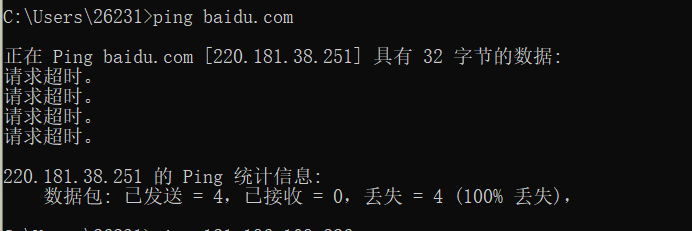


收到8个ICMP数据包，2个ARP数据包如下：



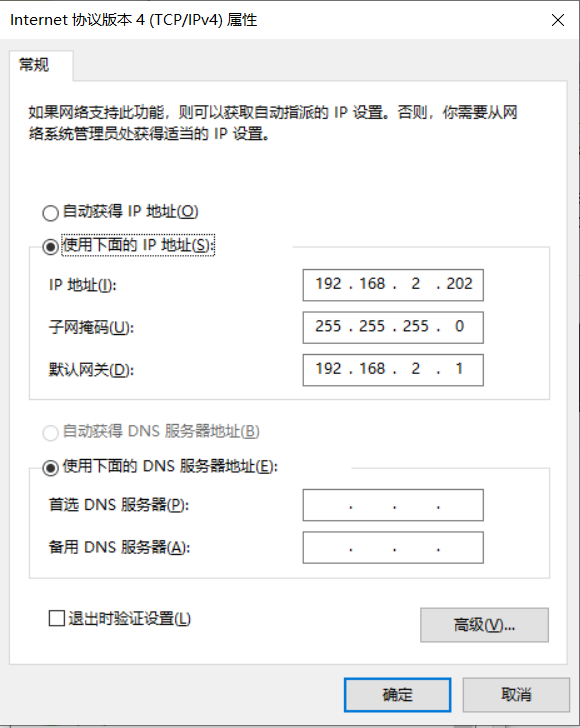


从主机A向百度发送PING检测报文：请求超时

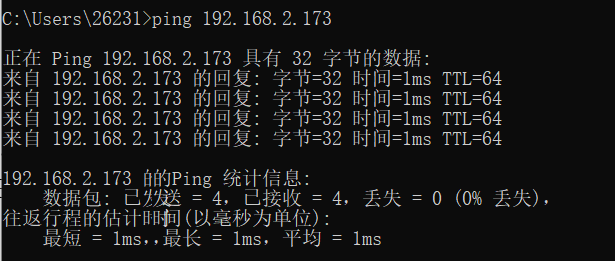


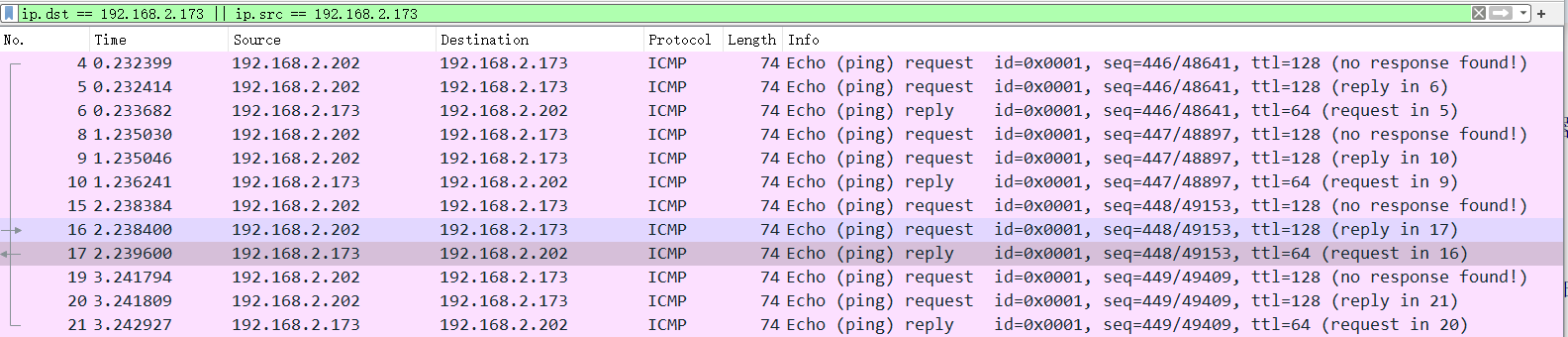
* + 主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

为主机A手动设置网关：

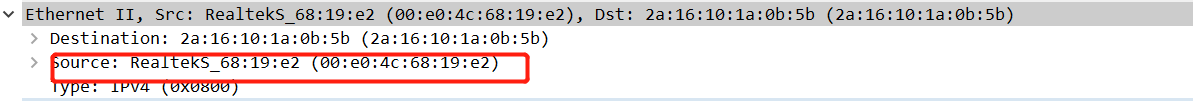


使用主机A向主机B发送PING检测报文：





可以看到主机B的MAC地址：



主机A向其他网段的主机发送PING检测报文：

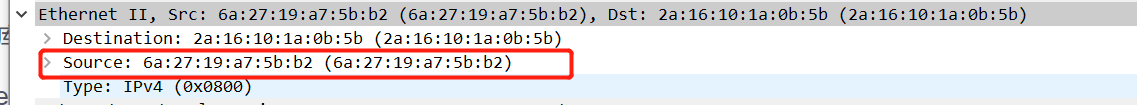
图片包含 文本

描述已自动生成

表格

描述已自动生成

此时可以看到网关（软路由）的MAC地址：



5、通过下面实验**理解网关**

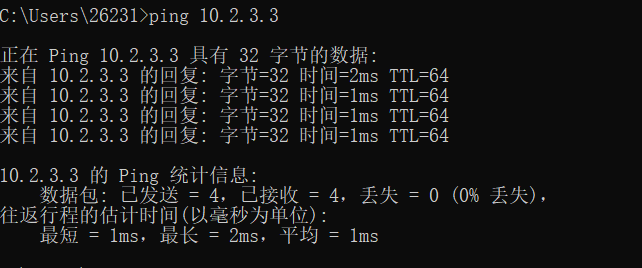
* 假设主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析

将主机A和主机B连到同一个交换机上，分别设置主机A和主机B的IP地址如下：





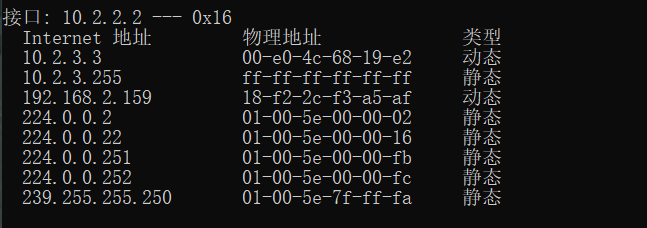
A主机向B主机发送PING检测报文：请求成功



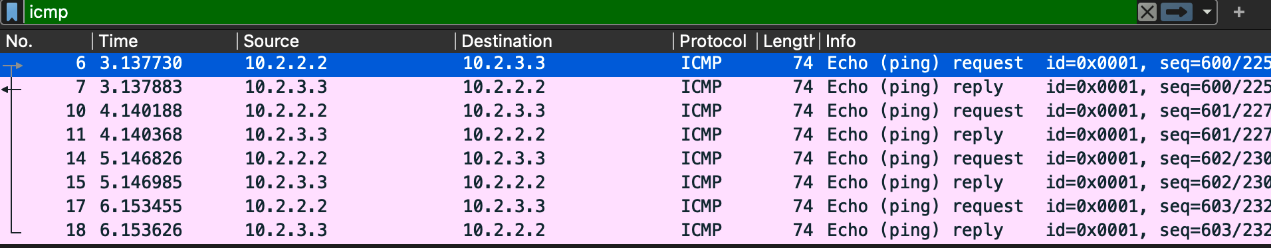
从A主机捕获到ICMP请求和应答报文



查看ARP



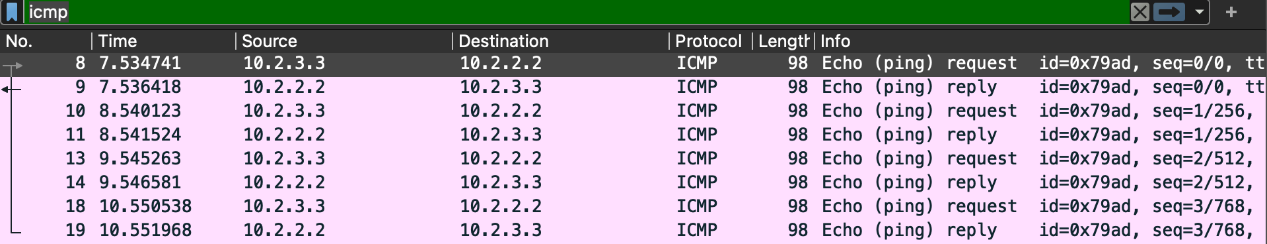
B主机同样捕获到ICMP请求和应答报文



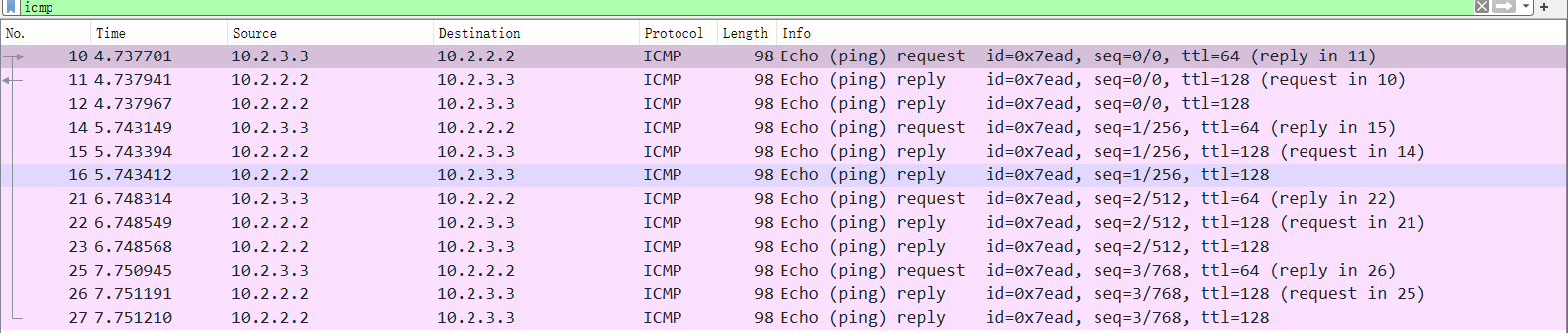
从B主机向A主机发送PING检测报文：请求成功



B主机捕获到ICMP请求和应答报文



A主机同样捕获到ICMP请求和应答报文



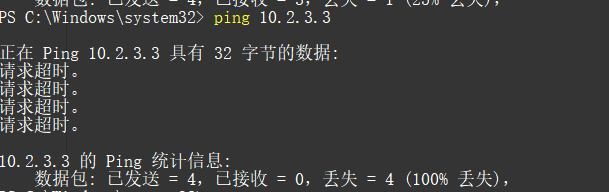
分析：从主机A给主机B发送PING检测报文，主机A的子网掩码与主机B相与之后发现主机B与主机A处于同一个网段，因此主机B会给主机A发送应答报文，两台主机可以通信；主机B给主机A发送PING检测报文

* 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。

设置主机A的IP地址和子网掩码：

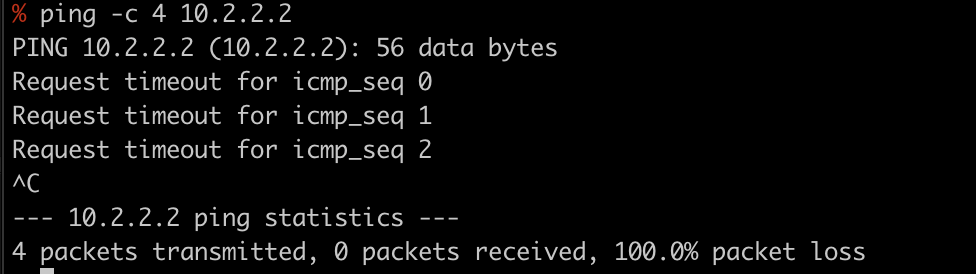


主机A给主机B发送PING检测报文：请求超时

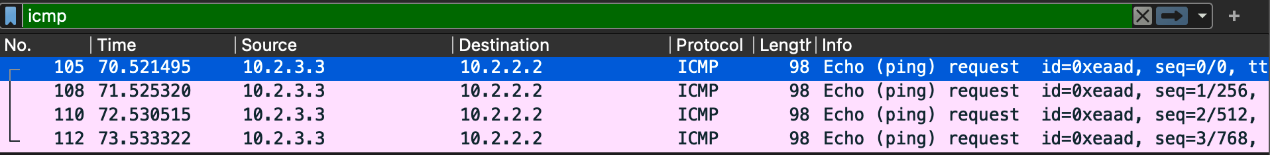


主机A和主机B都不能捕获到ICMP报文

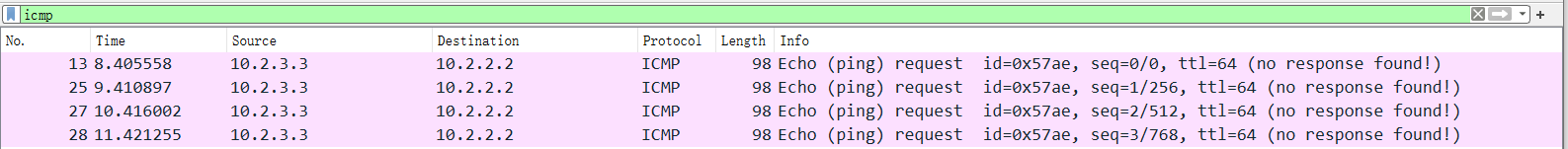
主机B给主机A发送PING检测报文：请求超时



主机B捕获到了ICMP请求报文：



主机A同样捕获到了ICMP请求报文：



此时发现虽然主机B给主机A发送了ICMP请求报文，但是并没有收到主机A给主机B的应答报文

分析：从主机A给主机B发送PING请求报文时，主机A的子网掩码与主机B的IP地址相与计算发现主机B和主机A并不在一个网段，因此主机A并没有向主机B发送信息，所以捕获不到ICMP请求报文；相反主机B给主机A发送PING请求报文时，主机B的子网掩码和主机A的IP地址做相与计算发现主机A在主机B的网段里面，因此主机B会给主机A发送请求报文，但是当主机B给主机A发送应答报文的时候，通过子网掩码与主机B的IP地址相与发现主机B和主机A不在一个网段，因此不会发送应答报文