**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

实验项目编号六实验项目类型 验证型 实验地点计算机网络实验室

学生姓名 张诗宇 学号 2019054001

学院 智能科学与工程 系 专业 信息安全

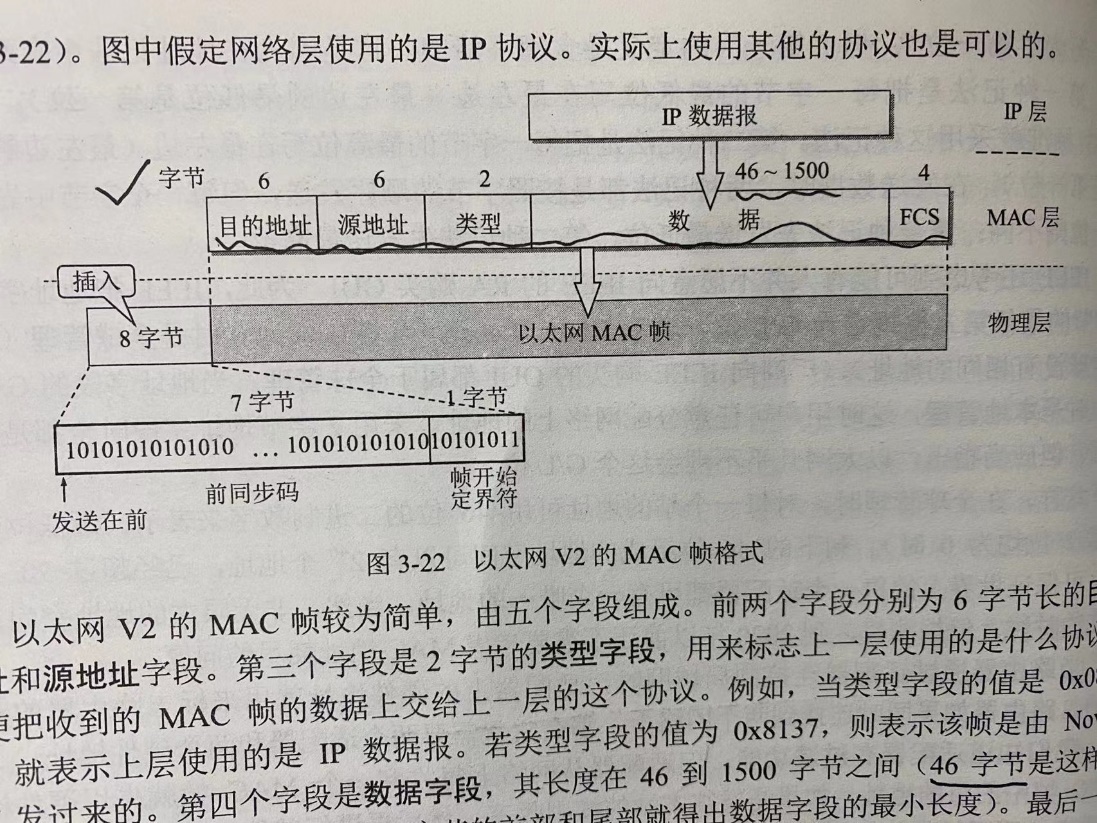
实验时间 2021 年 11 月 1 日 上 午～ 11 月 15 日 下 午

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. **实验环境**

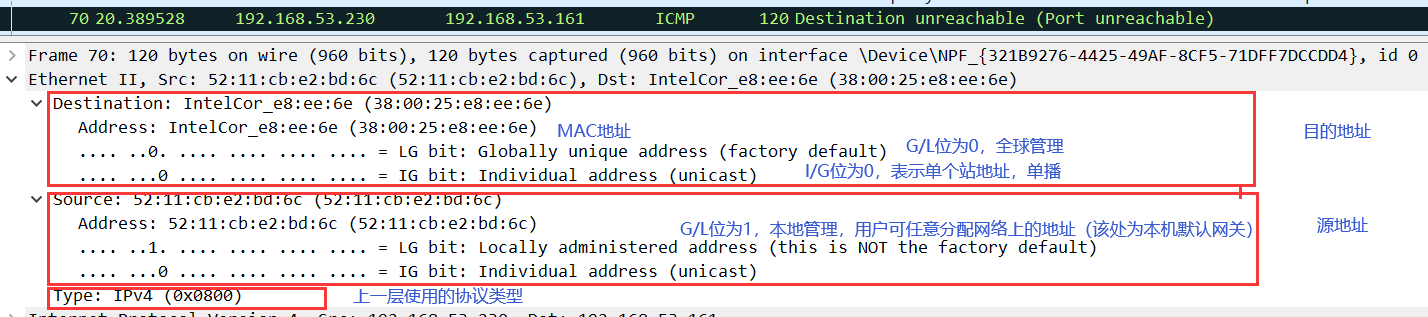
计算机2台

1. **实验步骤**
2. 安装Wireshark
3. 以太网协议分析

以太网MAC帧格式如下：



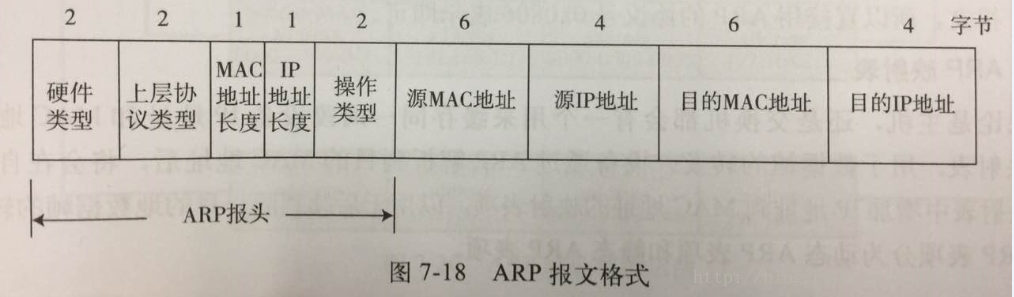
从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。



I/G位为1时表示组地址，用来进行多播/广播。

1. ARP协议分析

ARP报文格式如下图所示



硬件类型：表示硬件地址的类型（其中，值为1表示以太网地址）

上层协议类型：表示要映射的协议地址类型（其中，0x0800表示IP地址，其他还可能是ICMP/IGMP）。

硬件地址长度：指出该报文中硬件地址的长度（ARP报文中，它的值为6）。

协议地址长度：指出该报文中协议地址的长度（ARP报文中，它的值为4）。

op：操作字段，共有4种类型（1.ARP请求，2.ARP应答，3.RARP请求，4.RARP应答）。

源mac地址：发送方设备的硬件地址。

源ip地址：发送方设备的IP地址。

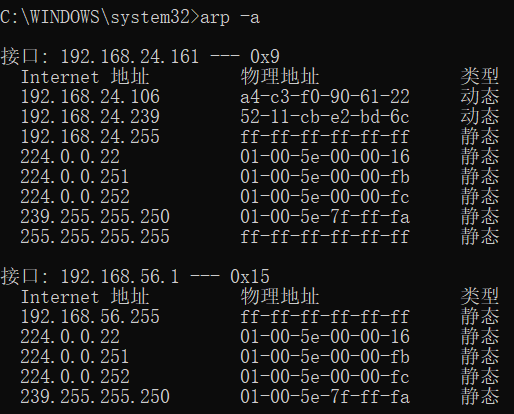
目的mac地址：接收方设备的硬件地址。

目的ip地址：接收方设备的IP地址。

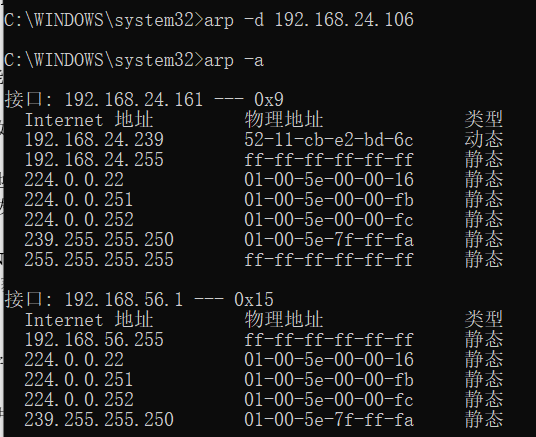
主机A：192.168.24.161

主机B：192.168.24.106

* 进入DOS窗口，用arp – a 查看本机上的ARP表的情况

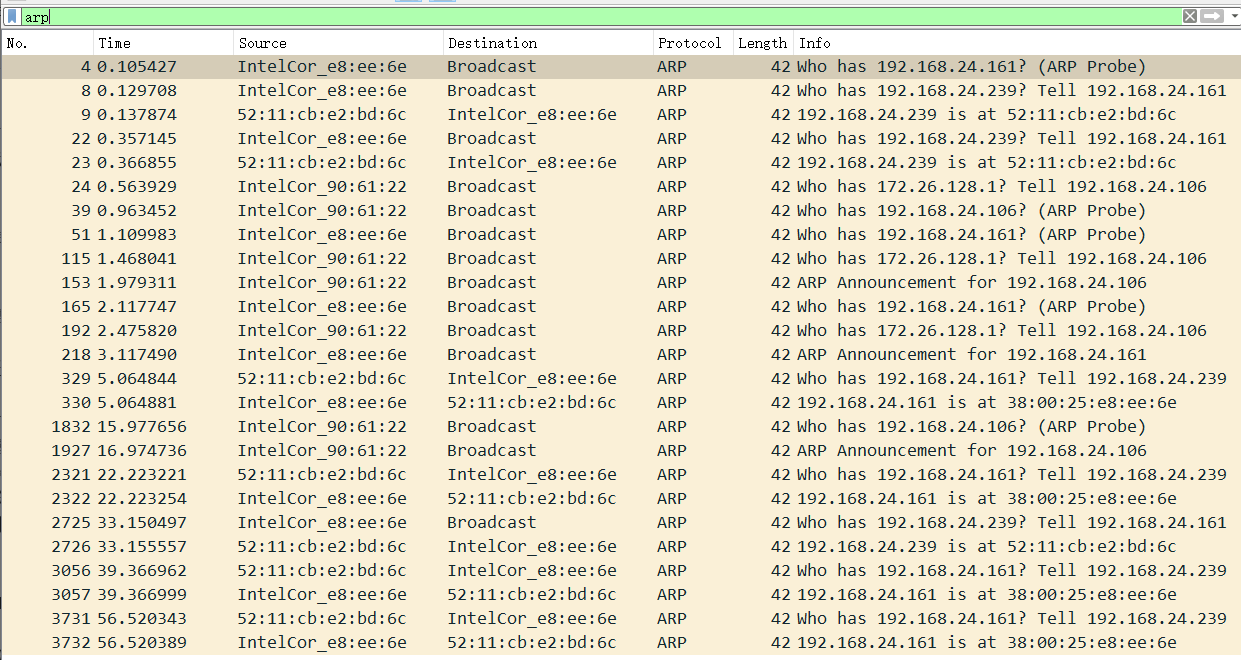


用 arp –d B 删除B的记录（需用管理员模式）；（主机B也将A的记录删除）

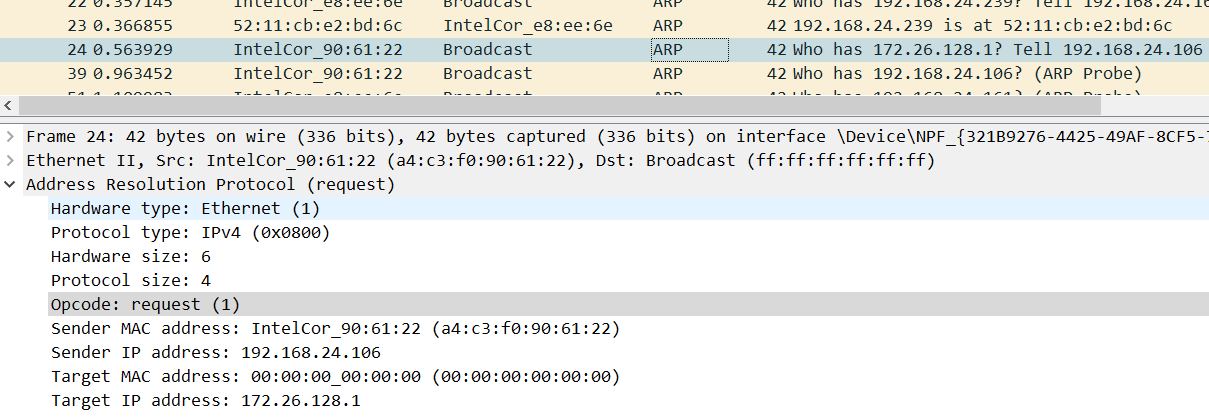


* 运行Wireshark程序；
* 把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；

此时可以捕获到ARP报文



分析ARP字段含义：



ARP请求

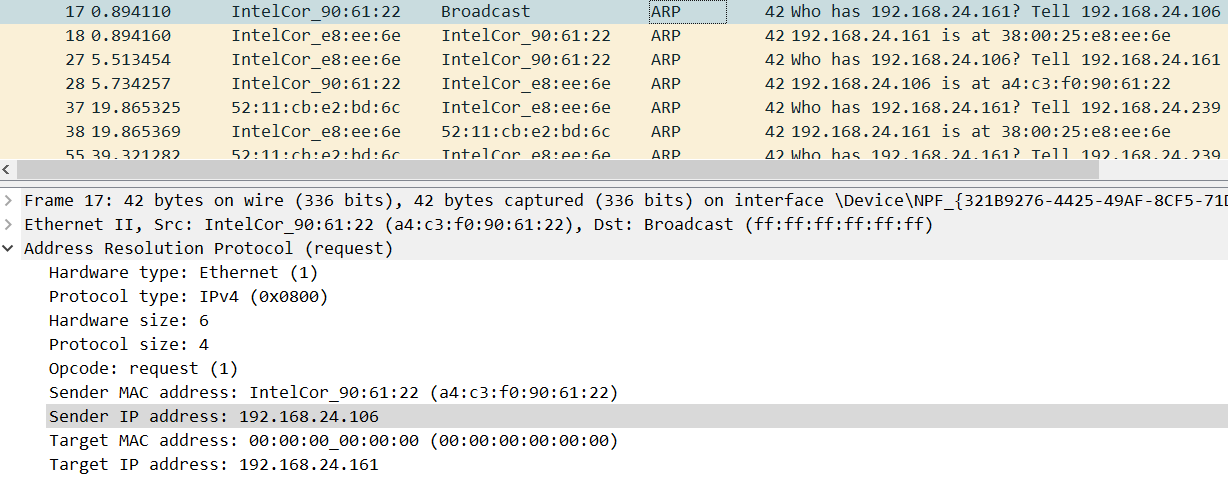
源地址

目的地址

以太网地址

IPv4协议

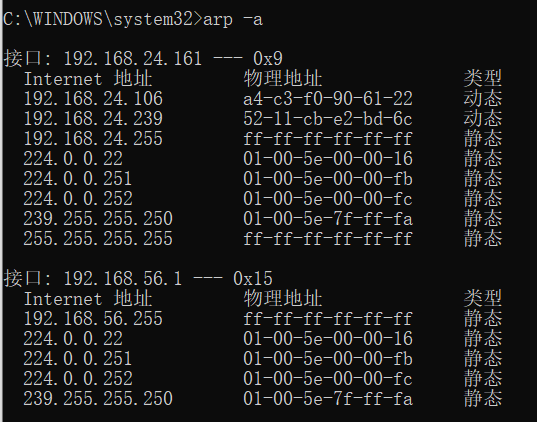
* 从主机B上向主机A发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；



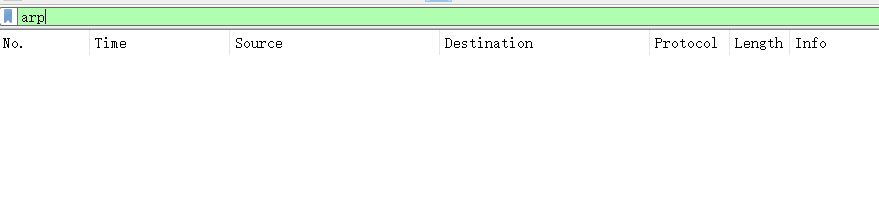
此时能捕获ARP报文。由于之前主机B将A的记录删除，此时B的ARP缓存中没有A的记录，所以ARP先在本局域网上广播发送一个ARP请求分组；主机A的IP地址与ARP请求分组中要查询的IP地址一致，于是收下这个ARP请求，并向主机B发送ARP响应分组。

主机B收到主机A的ARP响应分组后，就在其ARP缓存中写入主机A的IP地址到硬件地址的映射。为减少通信量，主机A收到主机B的请求分组时，就会在其ARP缓存中写入B映射。发送一次数据报，双方的地址映射都会被存入对方的ARP高速缓存中。

* 通过arp - a 查看ARP表的更新情况，此时能看到B对应的MAC地址；



* 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；



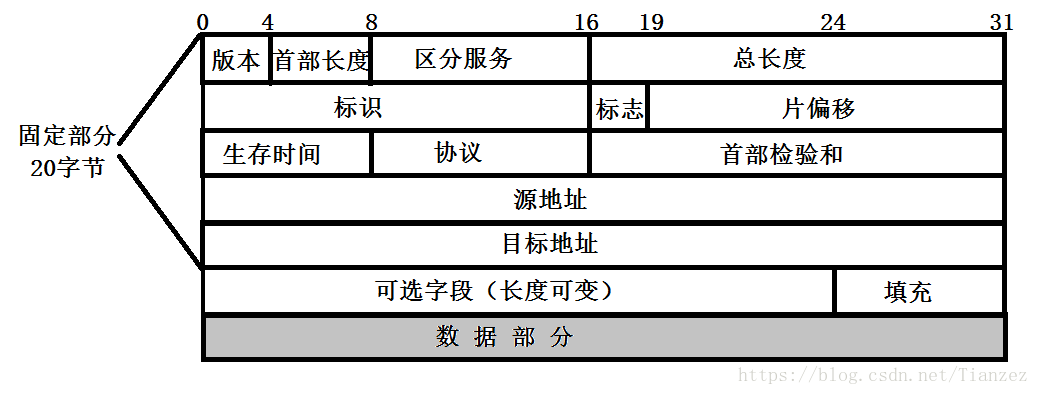
此时主机B的ARP告诉缓存中已经有了主机A的记录，直接就可以找到主机A的MAC地址，不再需要ARP。

* 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。

5分钟后不可以捕获到ARP报文，15分钟后再次捕获能捕获ARP报文。这是因为超过了生存时间，ARP会将这段时间未使用的记录删除，再次发出ping命令，双方需要重新建立地址映射记录。

1. IP协议分析

IP数据包格式如下图：



版本:占4位,指IP协议的版本.通信双方使用的IP协议版本必须一致。

首部长度:占 4 位,可表示的最大十进制数值是15。

区分服务:占 8 位,用来获得更好的服务。一般情况下都不使用这个字段

总长度:总长度指首部及数据之和的长度,单位为字节。

标识 (Identification):占 16位。当数据报由于长度超过网络的 MTU 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的标识字段中。相同的标识字段的值使分片后的各数据报片最后能正确地重装成为原来的数据报。

标志 (Flag):占3 位,但目前只有2位有意义. 标志字段中的最低位记为 MF(More Fragment).MF=1即表示后面"还有分片"的数据报.MF=0表示这已是若干数据报片中的最后一个.标志字段中间的一位记为DF(Don't Fragment),意思是"不能分片",只有当 DF=0时才允许分片.

片偏移:占 13位.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。

生存时间:占 8位,生存时间字段常用的英文缩写是TTL(Time To Live),其表明数据报在网络中的寿命。路由器在每次转发数据报之前就把TTL值减1.若TTL值减小到0，就丢弃这个数据报，不再转发。

协议:占 8 位。协议字段指出此数据报携带的数据是使用何种协议,以便使目的主机的IP层知道应将数据部分上交给哪个处理过程。

首部检验和:占 16位。这个字段只检验数据报的首部,但不包括数据部分。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。

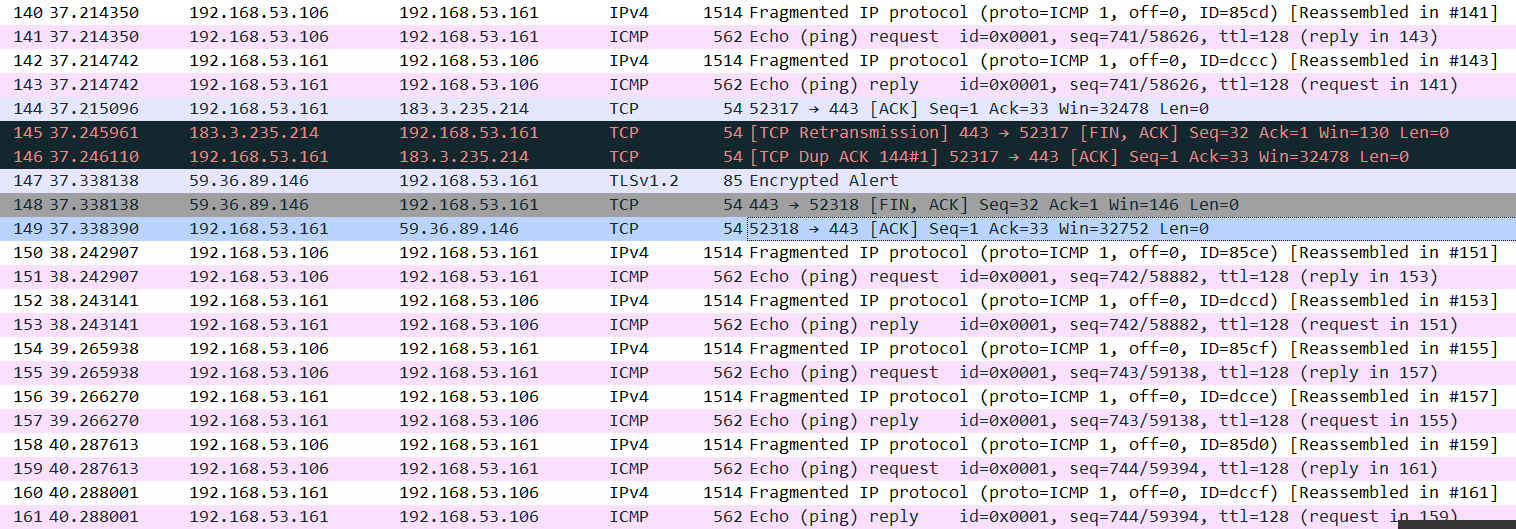
源地址:占32位.

目的地址:占 32位.

* 从主机B上向主机A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;

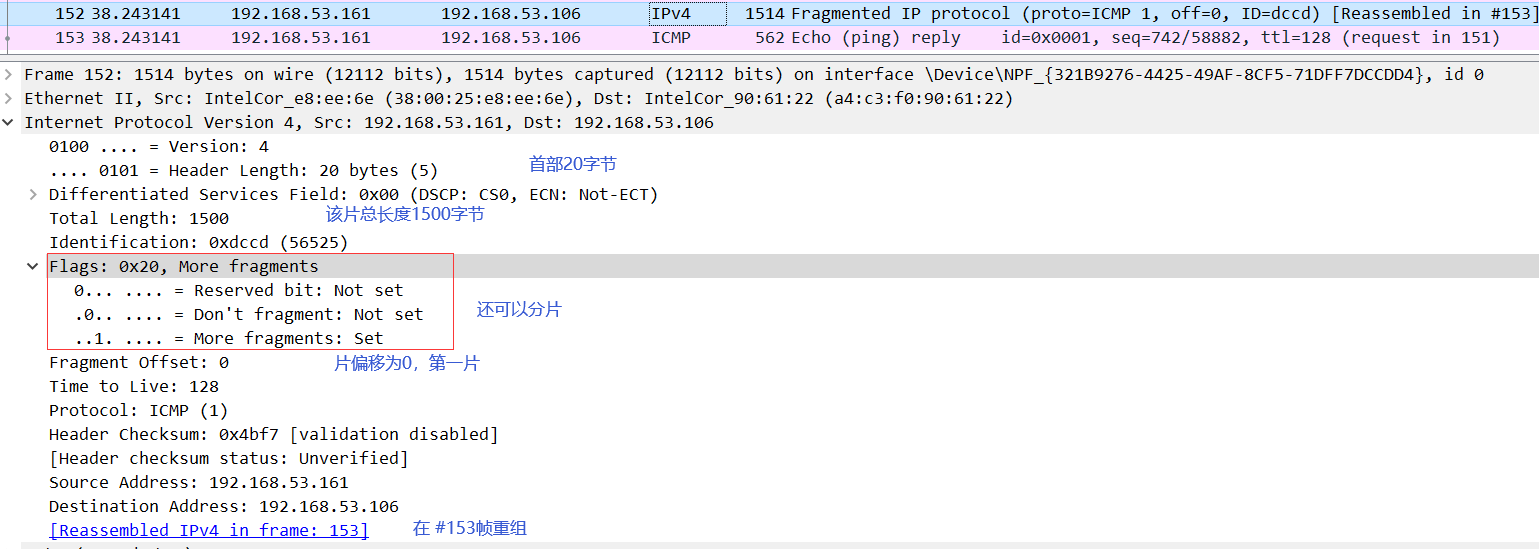


* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析**分片和重组**过程。

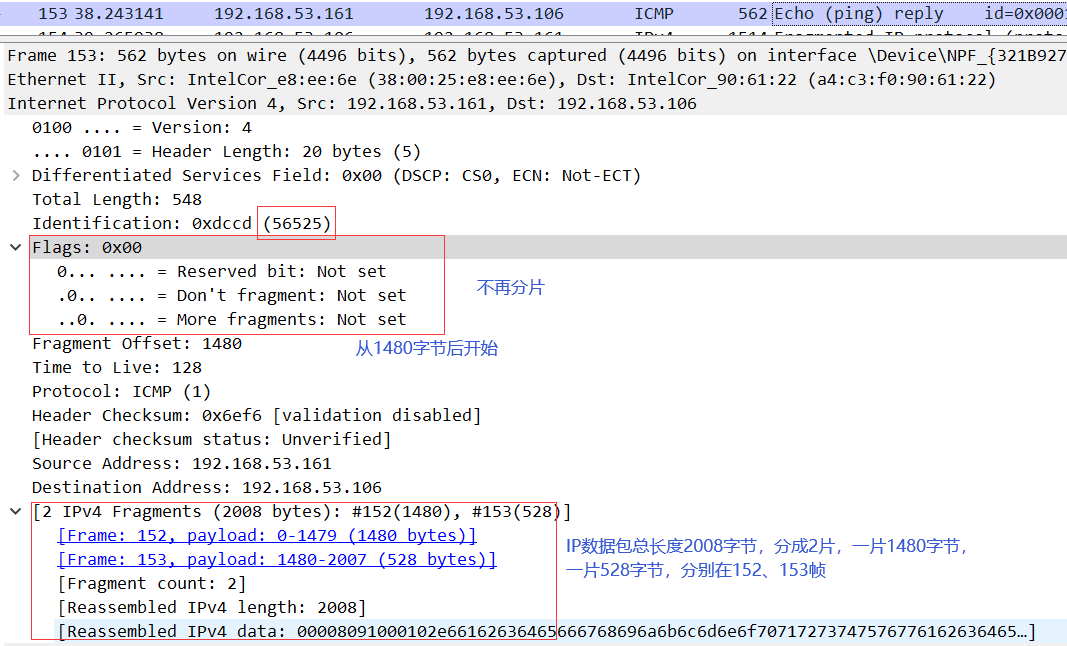


数据包被分成2片，4个数据包共8片。

第一片：



第二片：



数据包总长度多出的8字节时ICMP的首部。

1. ICMP协议分析

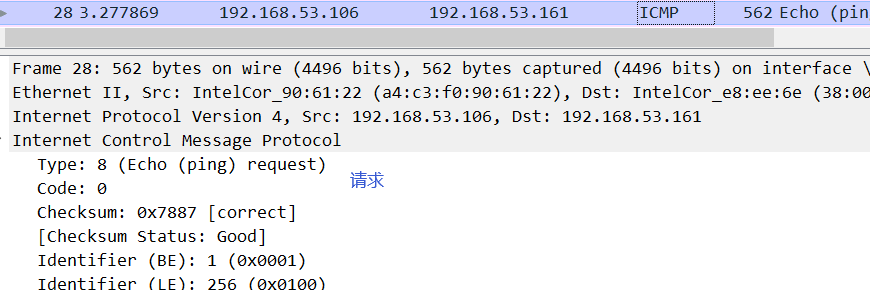
ICMP报文格式：

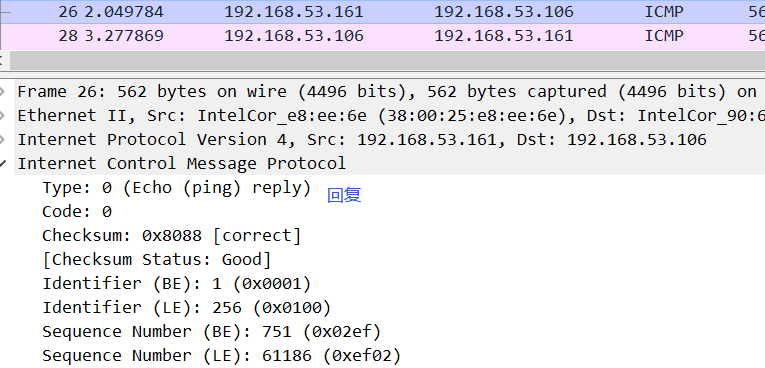




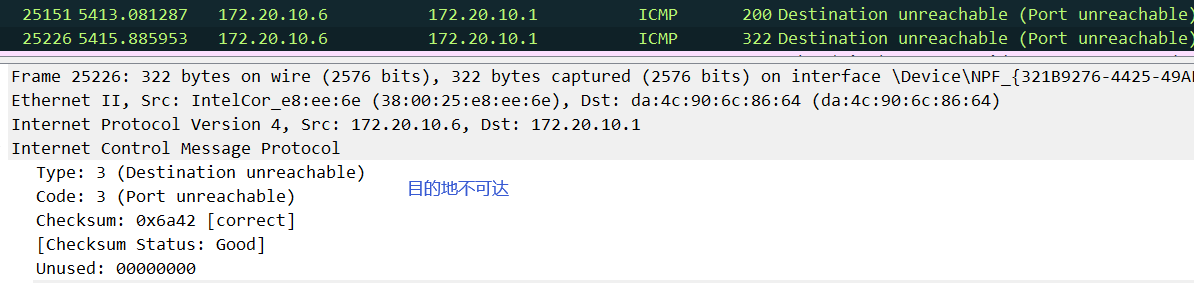
通过ping和tracet命令，了解ICMP协议的使用。

* 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。



Tracert工作原理：

Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

首先，tracert送出一个TTL是1的IP 数据包到目的地，当路径上的第一个路由器收到这个数据包时，它将TTL减1。此时，TTL变为0，所以该路由器会将此数据包丢掉，并送回一个「ICMP time exceeded」消息（包括发IP包的源地址，IP包的所有内容及路由器的IP地址），tracert 收到这个消息后，便知道这个路由器存在于这个路径上，接着tracert 再送出另一个TTL是2 的数据包，发现第2 个路由器...... tracert 每次将送出的数据包的TTL 加1来发现另一个路由器，这个重复的动作一直持续到某个数据包 抵达目的地。当数据包到达目的地后，该主机则不会送回ICMP time exceeded消息，一旦到达目的地，由于tracert通过UDP数据包向不常见端口(30000以上)发送数据包，因此会收到「ICMP port unreachable」消息，故可判断到达目的地。

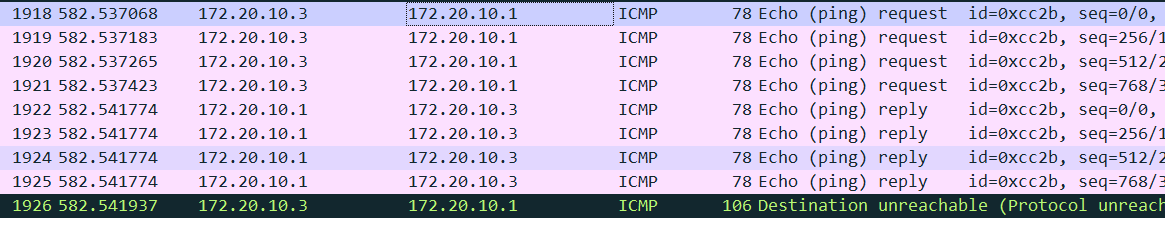
tracert 有一个固定的时间等待响应(ICMP TTL到期消息)。如果这个时间过了，它将打印出一系列的\*号表明：在这个路径上，这个设备不能在给定的时间内发出ICMP TTL到期消息的响应。然后，Tracert给TTL记数器加1，继续进行。

1. **思考与总结**
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？

当ARP高速缓存中有目的主机的地址映射记录时，不再需要通过ARP寻找目的MAC，也就捕获不到ARP报文。而ARP高速缓存中没有目的主机的地址映射时，就需要通过ARP找到目的主机的物理地址。

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？

因为127. 0.0.1表示本机回环地址，ping 127.0.0.1是不经过网卡的，是通过环路来处理的。而ping本机IP地址是需要经过网卡的，因此能捕获到ICMP报文。



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？

Request timed out：

a.对方已关机

b.对方与自己不在同一网段内，通过路由也无法找到对方

c.对方确实存在，但设置了ICMP数据包过滤（比如防火墙设置）

可以用带参数 -a 的Ping命令探测对方是否存在，如果能得到对方的NETBIOS名称，则说明对方是存在的，是有防火墙设置，如果得不到，多半是对方不存在或关机，或不在同一网段内。

d.错误设置IP地址

Destination host Unreachable：

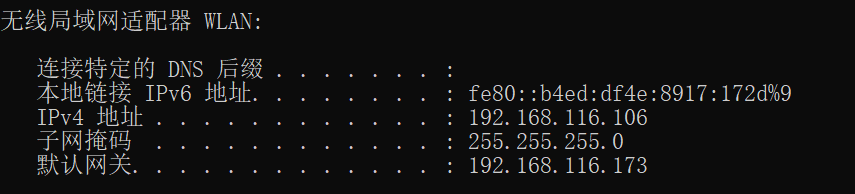
对方与自己不在同一网段内，而自己又未设置默认的路由，或者网络上根本没有这个地址；网线出了故障。

“destination host unreachable”和 “time out”的区别：如果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，这时候会出现“time out”，如果路由表中连到达目标的路由都没有，那就会出现“destination host unreachable”。

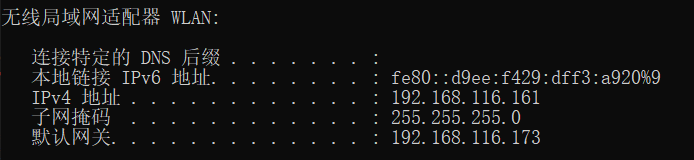
1. 请通过实验**验证**：

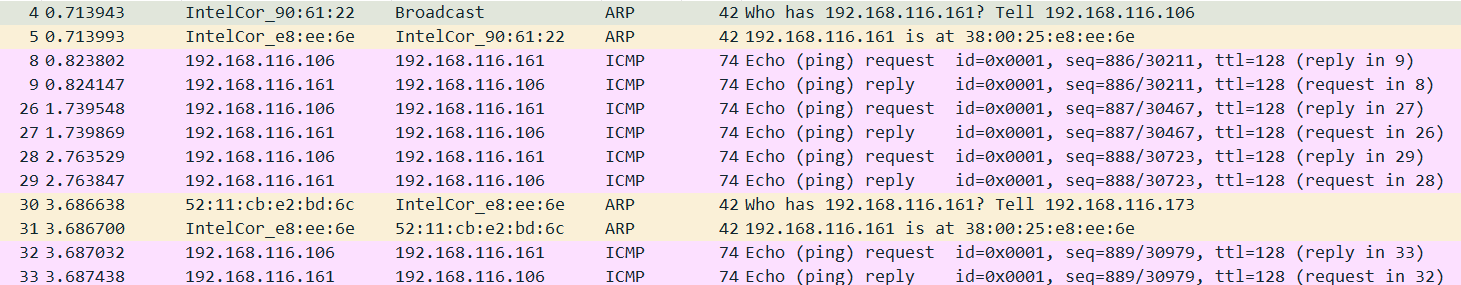
主机如果不设置“网关”，同一网段内的主机可以相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。

主机A：



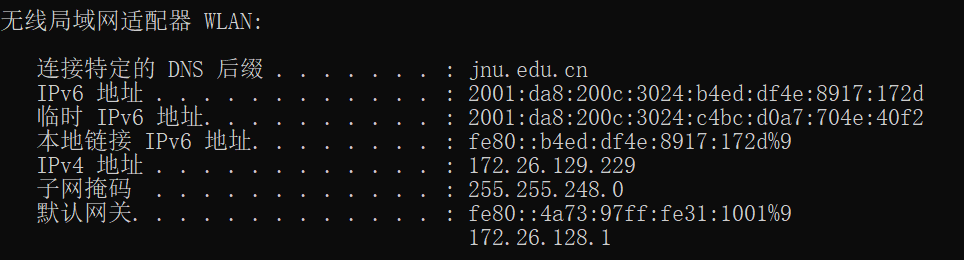
主机B



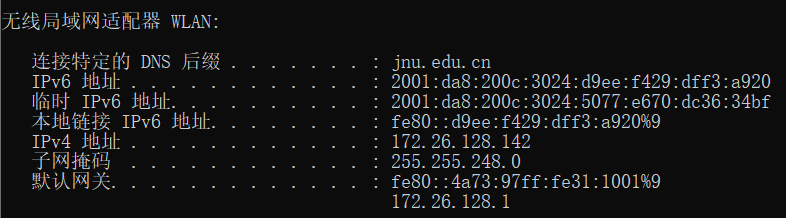


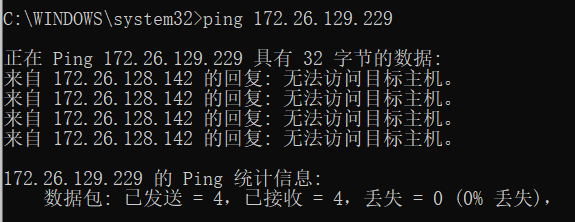
不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。

主机A：

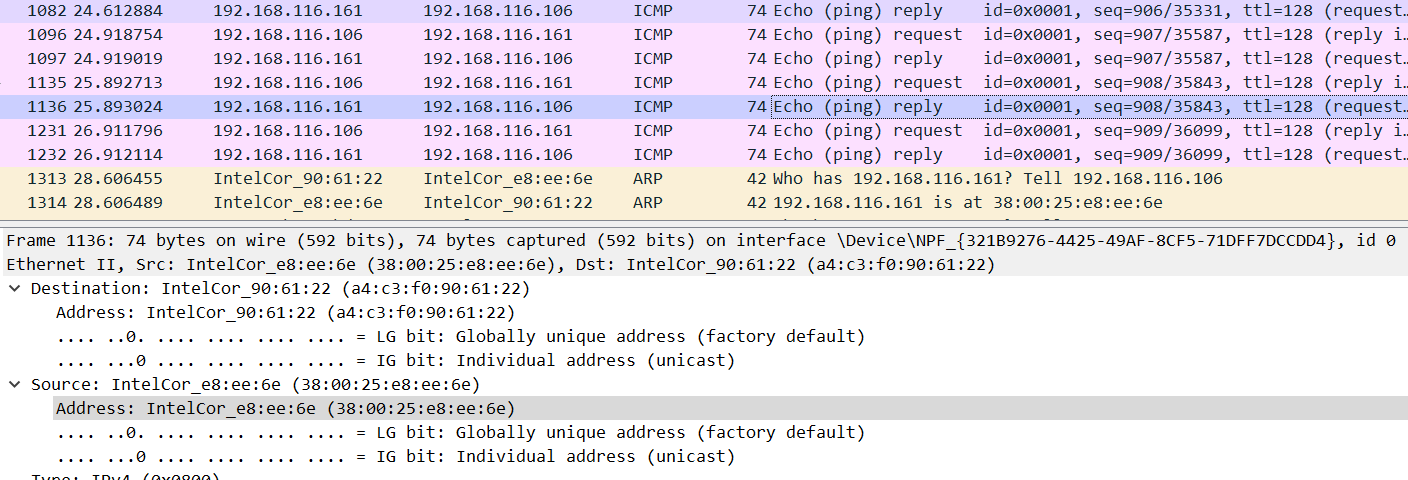


主机B：





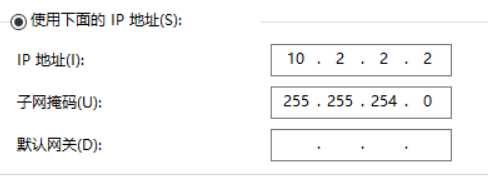
主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。

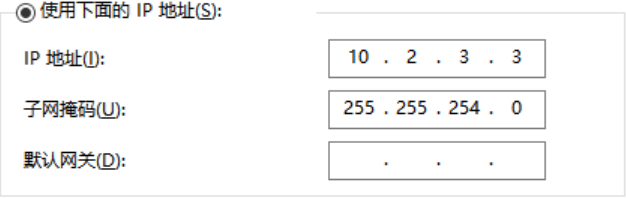


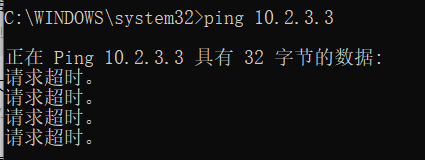
不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

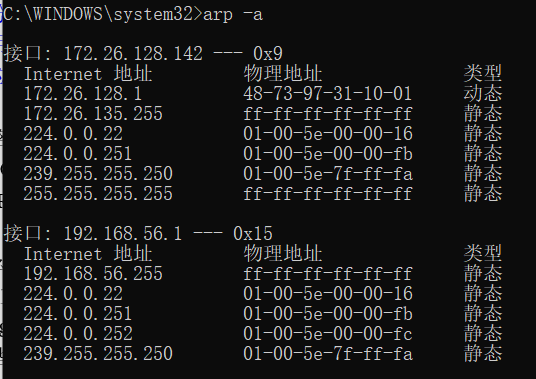
1. 通过下面实验**理解网关**

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。

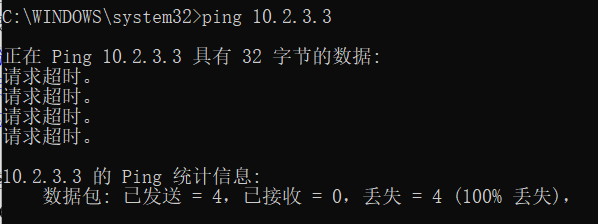


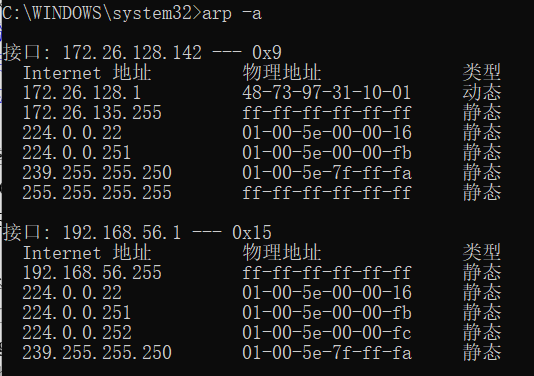






假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/23，两主机不设置网关，分别在主机A和主机B上用ping测试与对方的连通性，用ARP查看物理地址。对测试结果进行分析。





**暨南大学本科实验报告专用纸(附页)**