



湖南大学  
HUNAN UNIVERSITY

# 课程实验报告

课 程 名 称: 计算机网络

实验项目名称: Wireshark 软件使用与 ARP 协议分析

专 业 班 级: 计科 1902

姓 名: 樊一鸣

学 号: 2019028010212

指 导 教 师: 罗辉章

信息科学与工程学院

# 一、实验题目

学习 Wireshark 的基本操作, 抓取和分析有线局域网的数据包; 掌握以太网 MAC 帧的基本结构, 掌握 ARP 协议的特点工作过程

# 二、实验内容

使用 Wireshark 抓取局域网的数据包并进行分析:

- 1. 学习 Wireshark 基本操作: 重点掌握捕获过滤器和显示过滤器。
- 2. 观察 MAC 地址: 了解 MAC 地址的组成, 辨识 MAC 地址类型。
- 3. 分析以太网帧结构: 观察以太网帧的首部和尾部, 了解数据封装成帧的原理。
- 4. 分析 ARP 协议: 抓取 ARP 请求和应答报文, 分析其工作过程。

# 三、实验原理

## 3.1 以太网 MAC 帧格式

本实验基于使用最广泛的有线局域网 (以太网 Ethernet II), 以太网的帧结构如表 1.1-1 所示。其中, MAC 地址 (Media Access Control Address, 媒体存取控制位址) 或称物理地址 (Physical Address), 用于在网络中标识网卡。MAC 地址的长度为 48 位(6 个字节), 通常表示 12 个 16 进制数, 如: 00-16-EA-AE-3C-40。其中前 3 个字节的 16 进制数 00-16-EA 代表网络硬件制造商的编号、即组织唯一标志符(OUI), 它由 IEEE 分配; 而后 3 个字节的 16 进制数 AE-3C-40 代表该制造商所生产的某个网络产品(如网卡)的系列号。

表 1.1-1 以太网帧格式

前导字符	目的 MAC 地址	源 MAC 地址	类型	IP 数据报	帧校验
8 字节	6 字节	6 字节	2 字节	46-1500 字节	4 字节

## 3.2 ARP 协议及数据报格式

地址解析协议 (Address Resolution Protocol, ARP), 主要作用是将 IP 地址解析为 MAC 地址。当某主机或网络设备要发送数据给目标主机时, 必须知道对方的网络层地址 (即 IP 地址), 而且在数据链路层封装成帧时, 还必须有目标主机 (或下一跳路由器) 的 MAC 地址。本实验重点观察最简单的情形: 同一个网段内, 主机 A 要向主机 B 发送信息时, ARP 解析的过程 (主机 A 和 B 不在同一网段的情况请参阅课本相关内容)。

ARP 报文结构如图 1.1-1 所示, ARP 报文总长度为 28 字节, MAC 地址长度为 6 字节, IP 地址长度为 4 字节。每个字段的含义如下:

- 硬件类型: 指明了发送方想知道的硬件接口类型, 以太网的值为 1。
- 协议类型: 表示要映射的协议地址类型。IP 地址的类型值为 0x0800。
- 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。在以太网中, 它们的值分别为 6 和 4。
- 操作码 (op): 用来表示这个报文的类型, ARP 请求为 1, ARP 响应为 2, RARP 请

求为 3，RARP 响应为 4



图 1.1-1 ARP 报文结构示意图

3.3 实验方法及手段

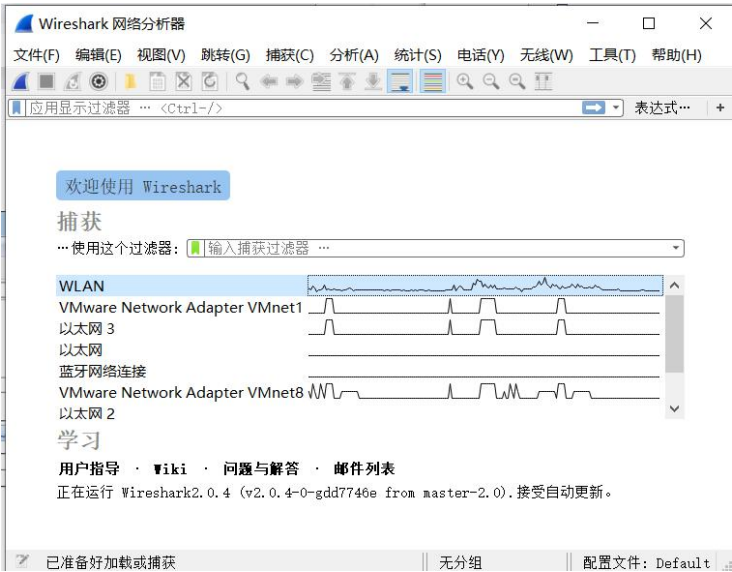
使用 Wireshark 软件在有线局域网中捕捉相关网络操作的数据包，运用观察对比、计算验证、分析统计等方法，掌握以太网 MAC 帧和 IP 数据报的结构以及 ARP 协议的工作原理。

四、实验步骤

(一) WireShark 基本使用

1. 运行 WireShark 软件：

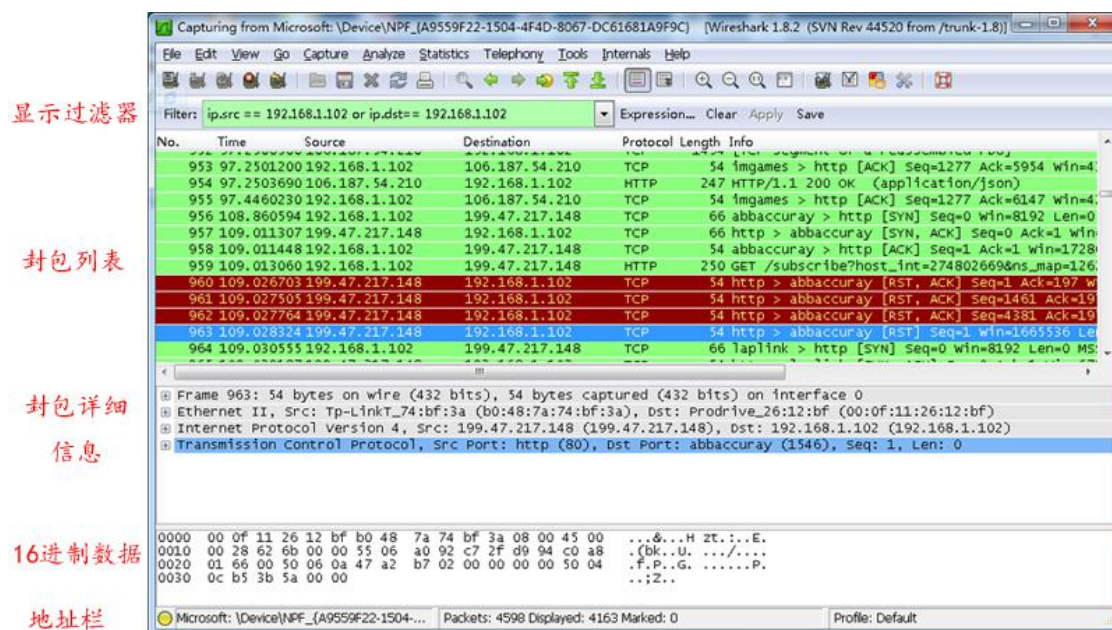
软件启动界面



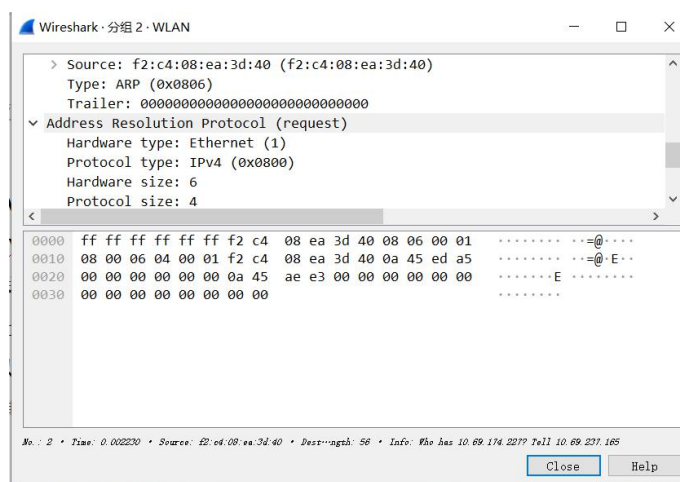
抓包操作：点击左上角蓝色按钮



窗口信息如下



2. 包中详细信息的查看：双击想要查看的封包，然后可以查看到其中的详细信息。



## (二) 观察 MAC 地址

启动 Wireshark 捕捉数据包，在命令行窗口分别 ping 网关和 ping 同网段的一台主机，分析本机发出的数据包。重点观察以太网帧的 Destination 和 Source 的 MAC 地址，辨识 MAC 地址类型，解读 OUI 信息、I/G 和 G/L 位。

(step1 并不必要)

**Step1:** Ping baidu.com: 在命令行中使用命令 ping baidu.com，得到数据如下，可以看到我们 ping 的 baidu.com 的 IP 地址是 220.181.38.251

```
C:\Users\fanyi>ping baidu.com
```

正在 Ping baidu.com [220.181.38.251] 具有 32 字节的数据:

来自 220.181.38.251 的回复: 字节=32 时间=28ms TTL=48

来自 220.181.38.251 的回复: 字节=32 时间=26ms TTL=48

来自 220.181.38.251 的回复: 字节=32 时间=26ms TTL=48

来自 220.181.38.251 的回复: 字节=32 时间=32ms TTL=48

220.181.38.251 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 26ms, 最长 = 32ms, 平均 = 28ms

然后在 wireshark 中筛选出目的地址: ip.dst==220.181.38.251, 发现如下四个数据包

No.	Time	Source	Destination	Protocol	Length	Info
484	2.726359	10.68.137.99	220.181.38.251	ICMP	74	Echo (ping) request id=0x0
702	3.742485	10.68.137.99	220.181.38.251	ICMP	74	Echo (ping) request id=0x0
963	4.753683	10.68.137.99	220.181.38.251	ICMP	74	Echo (ping) request id=0x0
1205	5.765997	10.68.137.99	220.181.38.251	ICMP	74	Echo (ping) request id=0x0

> Frame 484: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{0AC3A15F-C...}

> Ethernet II, Src: IntelCor\_c6:6a:97 (d0:ab:d5:c6:6a:97), Dst: NewH3CTe\_d4:70:02 (44:1a:fa:d4:70:02)

> Internet Protocol Version 4, Src: 10.68.137.99, Dst: 220.181.38.251

> Internet Control Message Protocol

0000 44 1a fa d4 70 02 d0 ab d5 c6 6a 97 08 00 45 00 D...p... ..j...E.

0010 00 3c e8 b4 00 00 40 01 00 00 0a 44 89 63 dc b5 .<....@. ...D.C..

0020 26 fb 08 00 4d 56 00 01 00 05 61 62 63 64 65 66 &...MV... ..abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

P:筛选出的数据包

MAC 地址格式详解:





以太网帧的 Destination 和 Source 的 MAC 地址: 目的地址是 (44:1a:fa:d4:79:02) 说明 baidu.com 他服务器的 MAC 地址就是 (44:1a:fa:d4:79:02), 而查询本机的 MAC 地址是 D0-AB-D5-C6-6A-97, 与数据包中的相符。

```

▼ Ethernet II, Src: IntelCor_c6:6a:97 (d0:ab:d5:c6:6a:97), Dst: NewH3CTe_d4:70:02 (44:1a:fa:d4:70:02)
  > Destination: NewH3CTe_d4:70:02 (44:1a:fa:d4:70:02)
  > Source: IntelCor_c6:6a:97 (d0:ab:d5:c6:6a:97)
  Type: IPv4 (0x0800)

无线网络适配器 WLAN:

连接特定的 DNS 后缀 . . . . . : 
描述. . . . . : Intel(R) Wireless-AC 9560 160MHz
物理地址. . . . . : D0-AB-D5-C6-6A-97
DHCP 已启用. . . . . : 是
自动配置已启用. . . . . : 是
IPv6 地址. . . . . : 2001:250:4402:1119::64c (首选)
  
```

P: MAC 地址

Baidu.com 的 MAC 地址分析: OUI: 44:1a:fa (<http://www.my-ip.club/oui-info/44-1A-FA>), 通过查询这个 OUI (OUI 与厂商有关), 可以看到它是新华三技术公司的产品。

**OUI: 44-1A-FA**

Vendor: New H3C Technologies Co., Ltd  
 Address1: 466 Changhe Road, Binjiang District  
 Address2: Hangzhou Zhejiang 310052  
 Address3: CN

Records found: 1

P: OUI 查询结果

I/G (IndividualGroup)位: 因为 4 化为 16 进制为 0100, 因此他的 IG 位为 0, 表示为单播地址, 如果 I/G 位为 1, 则为多播地址

G/L 位: G/L 位为 1, 是本地管理地址, 是网络管理员为了加强自己对网络管理而指定的地址。如果 G/L=0, 则是全局管理地址, 由 IEEE 分配。

**Step2:** ping 网关: 多播地址, 本地管理地址

输入在 cmd 中输入 ipconfig, 可以看到目前的默认网关是 10.72.121.254

```

无线网络适配器 WLAN:

连接特定的 DNS 后缀 . . . . . : 
本地链接 IPv6 地址. . . . . : fe80::dc73:6679:7c3:c4c%3
IPv4 地址. . . . . : 10.72.120.170
子网掩码. . . . . : 255.255.254.0
默认网关. . . . . : 10.72.121.254
  
```

在 cmd 中 ping 自己的网关, 同时使用 Wireshark 进行捕获。MAC 地址为: b40931648d02

```
> Frame 48: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface  
v Ethernet II, Src: IntelCor_c6:6a:97 (d0:ab:d5:c6:6a:97), Dst: HuaweiTe_64:8d:02  
  > Destination: HuaweiTe_64:8d:02 (b4:09:31:64:8d:02)  
  > Source: IntelCor_c6:6a:97 (d0:ab:d5:c6:6a:97)  
    Type: IPv4 (0x0800)  
> Internet Protocol Version 4, Src: 10.72.120.170, Dst: 10.72.121.254  
> Internet Control Message Protocol
```

```
C:\Users\fanyi>ping 10.72.121.254 -t  
  
正在 Ping 10.72.121.254 具有 32 字节的数据:  
来自 10.72.121.254 的回复: 字节=32 时间=4ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=5ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=3ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=4ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=5ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=3ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=3ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=4ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=10ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=5ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=6ms TTL=254  
来自 10.72.121.254 的回复: 字节=32 时间=7ms TTL=254
```

因为 mac 地址是 b40931648d02，因此 OUI 是 b4:09:31，查询这个 OUI 的详细信息如下，可以看出他的生产厂商是华为。

I/G (IndividualGroup)位:因为 b 化为 16 进制为 1011，因此他的 IG 位为 1，表示为多播地址。

G/L 位: G/L 位为 0，是全局管理地址。

## OUI: B4-09-31

Vendor: HUAWEI TECHNOLOGIES CO.,LTD

Address1: No.2 Xin Cheng Road, Room R6,Songshan Lake Technology Park

Address2: Dongguan 523808

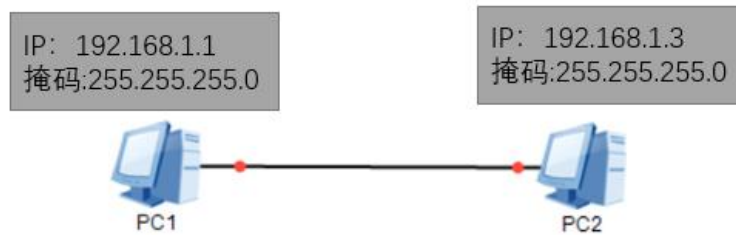
Address3: CN

Records found: 1

Last Update: 2022/04/20 04:44:16

### Step3:ping 同网段的一台主机

首先要通过网线连接另一台主机，通过配置两台主机的 IP 地址让其在同一网段下，两条主机的拓扑结构图和配置的 IP 如下。



使用 ping 命令，去 ping 台主机：抓包结果如下

IP2peer.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ip.dst==192.168.1.3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=
3	1.011750	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=
5	2.027552	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=
7	3.040847	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=
9	4.057421	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=
15	5.070899	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=
17	6.086999	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
> Ethernet II, Src: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36), Dst: 00:e1:99:01:53:68 (00:e1:99:01:53:68)

MAC 地址分析：MAC 地址为:00e199015368

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
 > Ethernet II, Src: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36), Dst: 00:e1:99:01:53:68 (00:e1:99:01:53:68)  
 > Destination: 00:e1:99:01:53:68 (00:e1:99:01:53:68)  
 > Source: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36)  
 Type: IPv4 (0x0800)  
 > Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3  
 > Internet Control Message Protocol

因此他的 OUI 是:00-E1-99

因为 0=000b,因此 I/G=0,G/L=0

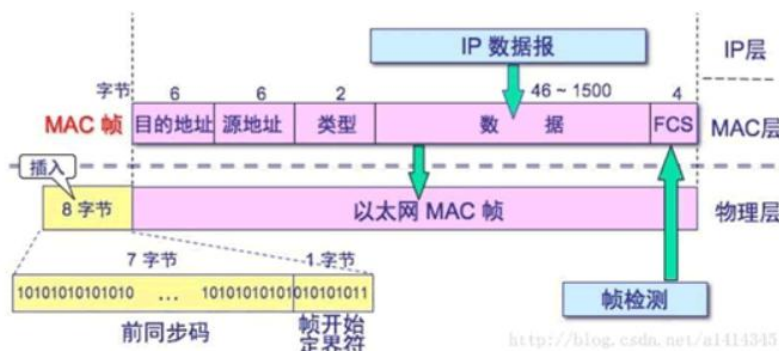
I/G (IndividualGroup)位:为 1, 是单播地址

G/L 位: 是全局管理地址

### (三) 分析以太网的帧结构

以太网帧结构如下图：从下图可以看出以太网 MAC 帧分为目的地址，源地址，类型，IP 数据包和 FCS(帧检测序列) 五个部分





选择其中一个数据包，点击 Ethernet II 展开（图 1.1-9），查看 MAC 帧的各个字段

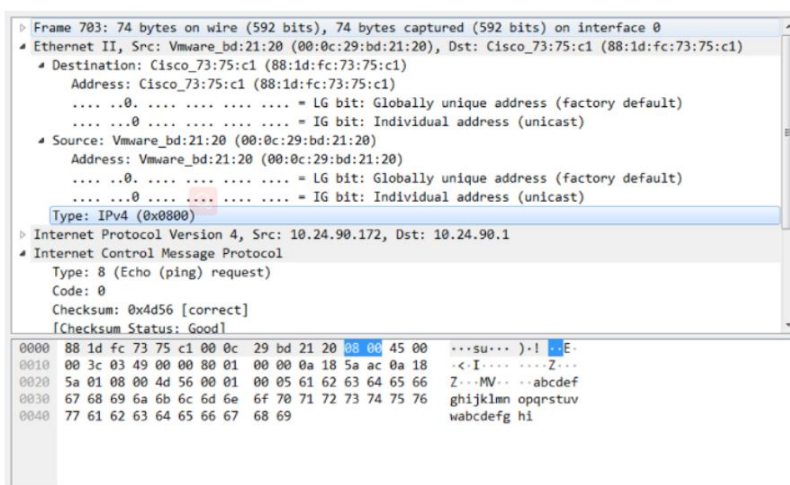
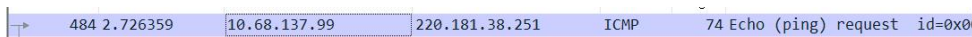


图 1.1-9 以太网帧结构展开界面

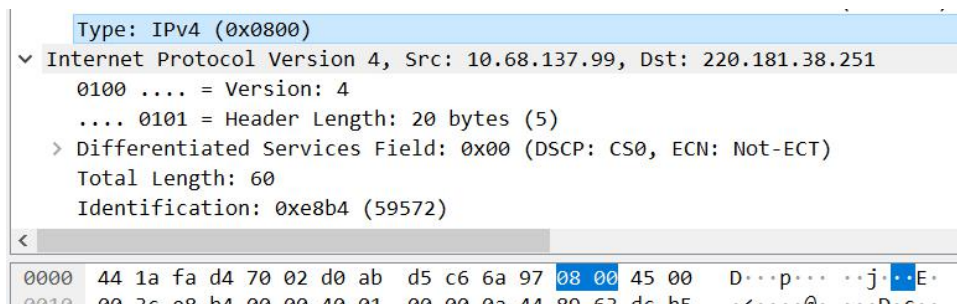
这里选择了 ping 向百度的第一个报文：



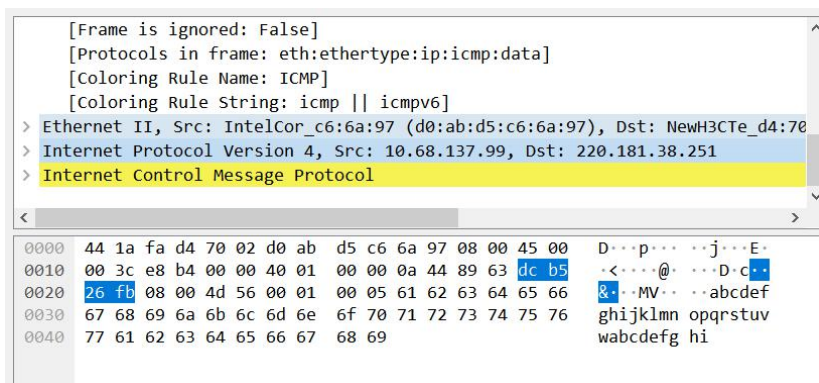
①首先看前 12 个字节，其中前 6 个代表的是源 MAC 地址，后 6 个字节代表目的 IP 地址。

0000	44 1a fa d4 70 02 d0 ab d5 c6 6a 97 08 00 45 00
0010	00 3c e8 b4 00 00 40 01 00 00 0a 44 89 63 dc b5
0020	26 fb 08 00 4d 56 00 01 00 05 61 62 63 64 65 66
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040	77 61 62 63 64 65 66 67 68 69

②第 13 和 14 个字节是类型，当其为 0x0800 的时候交付给 IP 协议



③14 个字节之后的内容是封装了 IPv4 协议的内容



④从上面的数据中，我们发现没有找到以太网帧结构的 FCS 和前序 8 字节，通过查阅资料得知，以太网将这两个结构过滤了

在物理层上网卡要先去掉前导同步码和帧开始定界符，然后对帧进行 CRC 检验，如果帧校验和错，就丢弃此帧。如果校验和正确，就判断帧的目的硬件地址是否符合自己的接收条件（目的地址是自己的物理硬件地址、广播地址、可接收的多播硬件地址等），如果符合，就将帧交“设备驱动程序”做进一步处理。这时我们的抓包软件才能抓到数据，因此，抓包软件抓到的是去掉前导同步码、帧开始分界符、FCS 之外的数据。 --引用自 [csdn 博客](#)

#### (四) ARP 协议分析

清空缓存方式：使用管理员身份打开 cmd，执行如命令 arp -d

管理员: 命令提示符

```
Microsoft Windows [版本 10.0.19044.1645]
(c) Microsoft Corporation. 保留所有权利。

C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>arp -a

接口: 10.68.23.189 --- 0x3
    Internet 地址      物理地址      类型
    10.68.0.1          44-1a-fa-d4-70-02 动态
    10.69.255.255      ff-ff-ff-ff-ff-ff 静态
    224.0.0.22         01-00-5e-00-00-16 静态

接口: 192.168.136.1 --- 0x4
    Internet 地址      物理地址      类型
    192.168.136.255    ff-ff-ff-ff-ff-ff 静态
    224.0.0.22         01-00-5e-00-00-16 静态

接口: 192.168.81.1 --- 0x6
    Internet 地址      物理地址      类型
    192.168.81.255     ff-ff-ff-ff-ff-ff 静态
    224.0.0.22         01-00-5e-00-00-16 静态

接口: 192.168.1.1 --- 0xb
    Internet 地址      物理地址      类型
    192.168.1.255      ff-ff-ff-ff-ff-ff 静态
    224.0.0.22         01-00-5e-00-00-16 静态
```

1. 使用 CTR + F 命令（其语法见图 1.1-10），清空本机的 ARP 缓存，开启 Wireshark，ping 本机的同网段地址，在显示过滤器条框中输入“CTR”，观察捕获的 ARP 报文的各个字段，分析请求/响应的过程。

Ping 192.168.1.3 捕获到的信息如下

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	f8:b4:6a:14:02:36	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.1
2	0.002061	00:e1:99:01:53:68	f8:b4:6a:14:02:36	ARP	60	192.168.1.3 is at 00:e1:99:01:53:68
3	0.002070	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=64
4	0.004207	192.168.1.3	192.168.1.1	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
5	1.012858	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376, ttl=64
6	1.014961	192.168.1.3	192.168.1.1	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
7	2.027668	192.168.1.1	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=64

分析 ARP 执行过程：

①首先查看第一条报文，看到目标地址 ping 的 IP 地址，但是现在没有找到的物理地址。

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface  
> Ethernet II, Src: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
▼ Address Resolution Protocol (request)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: request (1)  
Sender MAC address: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36)  
Sender IP address: 192.168.1.1  
Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
Target IP address: 192.168.1.3

物理地址全零

目标地址

②ARP 会将报文广播到本网段的所有主机，如果找到对应的 IP 就会返回相应的 ARP 报文，从截获的第二条报文可以发现，报文中携带了 192.168.1.3 的物理地址信息

Wireshark · 分组 2 · 以太网

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface  
> Ethernet II, Src: 00:e1:99:01:53:68 (00:e1:99:01:53:68), Dst: f8:b4:6a:14:02:36  
▼ Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: 00:e1:99:01:53:68 (00:e1:99:01:53:68)  
Sender IP address: 192.168.1.3  
Target MAC address: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36)  
Target IP address: 192.168.1.1

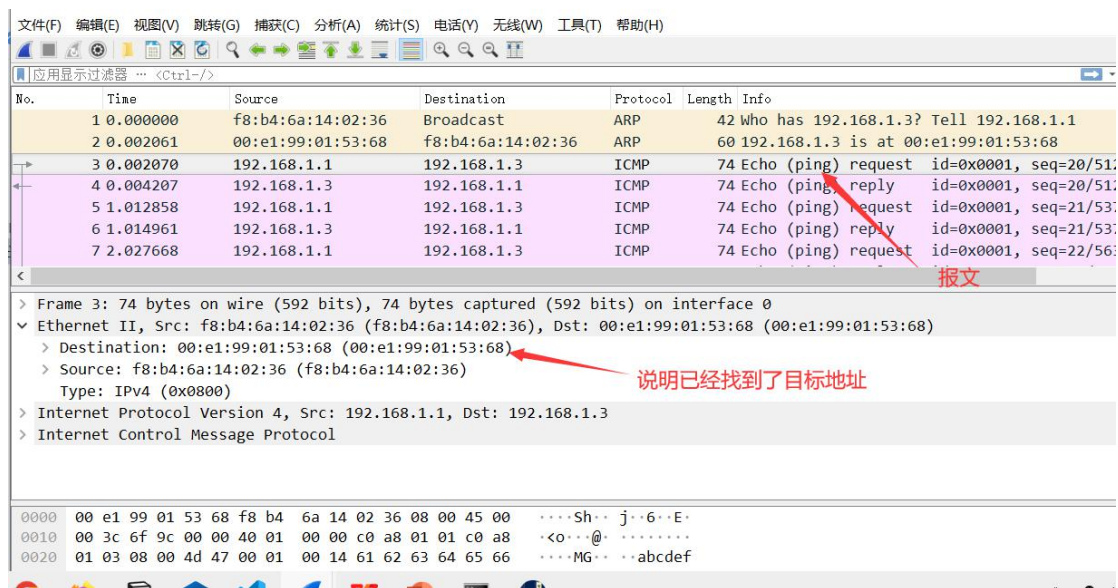
携带了物理地址信息

来自目标地址

0000	f8 b4 6a 14 02 36	00 e1 99 01 53 68	08 06 00 01	..j..6.. ..Sh....
0010	08 00 06 04 00 02	00 e1 99 01 53 68	c0 a8 01 03	..... ..Sh....
0020	f8 b4 6a 14 02 36	c0 a8 01 01 55 55	55 55 55 55	..j..6.. ..UUUUUU
0030	55 55 55 55 55 55	55 55 55 55 55 55		UUUUUUUU UU

之后的 ICMP 报文中，发现本机已经找到了另一台主机的 MAC 地址





这时再查看 arp 缓存信息，可以看到已经有了 192.168.1.3 的物理地址。

接口: 192.168.1.1 --- 0xb		
Internet 地址	物理地址	类型
192.168.1.3	00-e1-99-01-53-68	动态
192.168.1.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.251	01-00-5e-00-00-fb	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态

总结：主机 A ping 主机 B 过程

第一步：主机 A 发送广播报文； 第二步：主机 B 收到报文，对照自己的 IP 地址，发现是符合的，就返回 ARP 广播报文，携带其 MAC 地址信息； 第三步：主机 A 收到 B 的报文，将 B 的 IP 地址和物理地址映射存到本地 ARP 缓存中； 第四步：主机 A 向主机 B 发送 ICMP 报文。

2. 使用 CTR + F 命令，清空本机的 ARP 缓存。开启 Wireshark，ping 与本机网段不同的 IP 地址或域名，观察捕获的 ARP 报文的各个字段，分析请求/响应的过程。

Ping 一个不存在的地址，例如 192.168.1.5

```

C:\ 管理员: 命令提示符 - ping 192.168.1.5

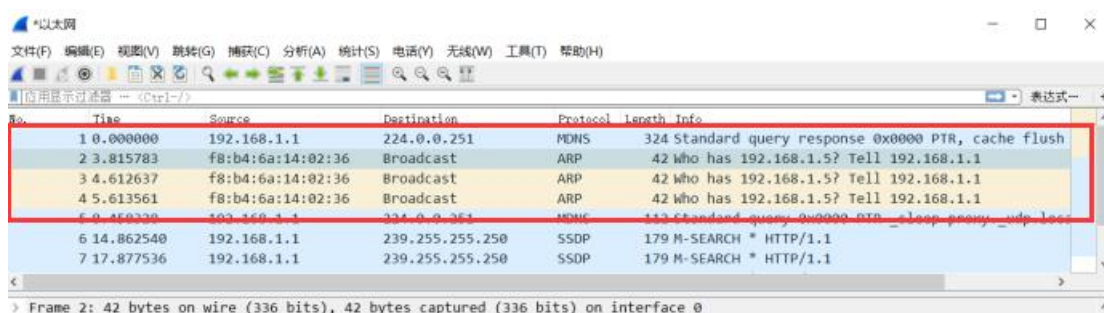
Microsoft Windows [版本 10.0.19044.1645]
(c) Microsoft Corporation。保留所有权利。

C:\WINDOWS\system32>arp -d

C:\WINDOWS\system32>ping 192.168.1.5

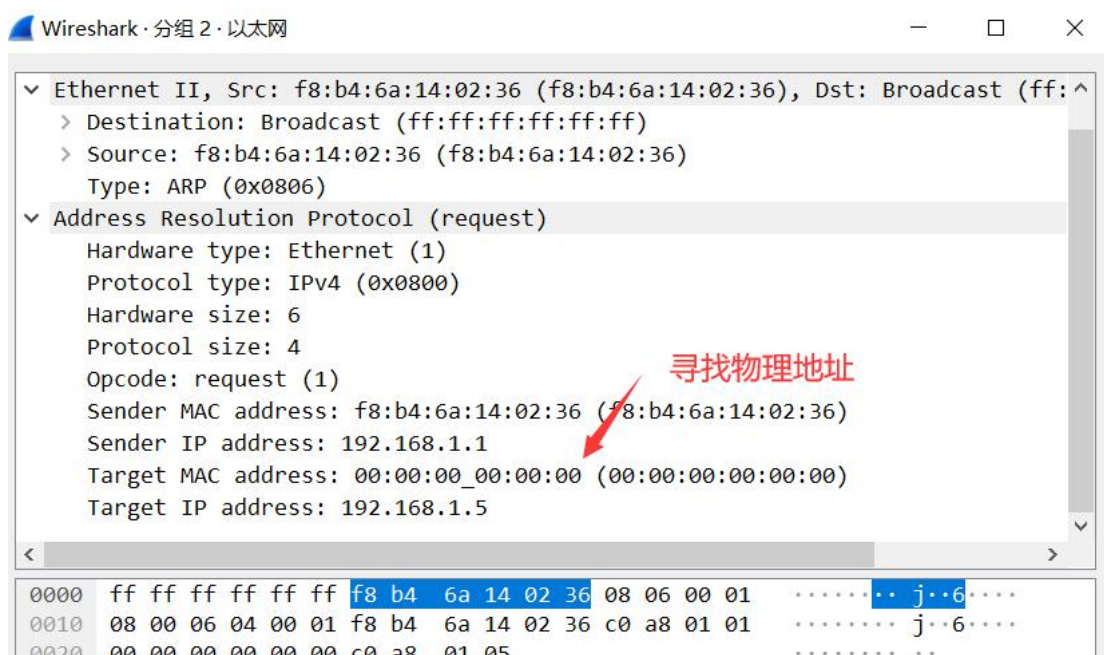
正在 Ping 192.168.1.5 具有 32 字节的数据:
来自 192.168.1.1 的回复: 无法访问目标主机。
请求超时。
  
```

截获的报文如下



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.1	224.0.0.251	MDNS	324	Standard query response 0x0000 PTR, cache flush
2	3.815783	f8:b4:6a:14:02:36	Broadcast	ARP	42	Who has 192.168.1.5? Tell 192.168.1.1
3	4.612637	f8:b4:6a:14:02:36	Broadcast	ARP	42	Who has 192.168.1.5? Tell 192.168.1.1
4	5.613561	f8:b4:6a:14:02:36	Broadcast	ARP	42	Who has 192.168.1.5? Tell 192.168.1.1
5	6.460330	192.168.1.1	224.0.0.251	MDNS	153	Standard query 0x0000 PTR - loop proxy - udp loss
6	14.862540	192.168.1.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
7	17.877536	192.168.1.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

首先查看第一条 ARP 报文，他发送广播报文，寻找对应的物理地址 192.68.1.5



Wireshark · 分组 2 · 以太网

▼ Ethernet II, Src: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

- > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- > Source: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36)
- Type: ARP (0x0806)

▼ Address Resolution Protocol (request)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: f8:b4:6a:14:02:36 (f8:b4:6a:14:02:36)
- Sender IP address: 192.168.1.1
- Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.1.5

寻找物理地址

0000 ff ff ff ff ff ff f8 b4 6a 14 02 36 08 06 00 01 ..... j..6....

0010 08 00 06 04 00 01 f8 b4 6a 14 02 36 c0 a8 01 01 ..... j..6....

0020 00 00 00 00 00 00 c0 a8 01 05 ..... ..

后面的报文与这一条报文相同，平均每过 1s 发送一次 ARP 报文，发送三次后，因为一直没有得到响应，就直接结束了。

总结： 主机 A ping 不存在的主机 B

(1) 主机 A 发送广播报文寻找 B (2) 在同网段中找不到主机 B，得不到反馈 (3) 主机 A 累计发送三次寻找信息后，停止发送。

## 五、实验心得与不足

思考题：

1. 使用了显示过滤器后，Wireshark 的抓包工作量会减少吗？

不会减少，显示过滤器的功能是已捕获的所有数据包中显示出符合条件的数据包，隐藏不符合条件的数据包。因此抓包工作量是不会减少的。

如果想要减少抓包工作量，则需要使用捕获过滤器，捕获过滤器作用在 wireshark 开始捕获数据包之前，只捕获符合条件的数据包，不记录不符合条件的数据包。

2. ARP 请求数据包是支撑 TCP/IP 协议正常运作的广播包。如果滥发或错发 ARP 广播包会产生那些不良影响？如何发现和应对？

- ① 造成用户掉线，频繁断网，上网慢
- ② 设备 CPU 占用率高。



③ping 有时延，丢包或不通

处理方式：arp -d 清除 arp 列表，利用 ARP 防火墙软件保护（360ARP 防火墙、AntiARPSniffer）。

心得：

1. 发现单单自己 ping 自己的时候，并不能捕捉到免费 ARP 包，据说在更改 MAC 地址的时候才能捕获的 ARP 包。
2. 以太网帧在物理层就被经过了过滤，因此捕获到的以太网帧结构不完整。