

重庆大学大数据与软件学院

上机报告

上机名称

利用 wireshark 分析以太网帧与 ARP 协议

课程名称

计算机网络

开课实验室：DS-1501

2025 年 4 月 27 日

姓 名		学号		成 绩	
上机（项目）名称		利用 wireshark 分析以太网帧与 ARP 协议		指导教师	
教师评语		教师签名：高旻 年 月 日			

一、实验目的

分析以太网帧、MAC 地址和 ARP 协议

二、实验内容

1、俘获和分析以太网帧

- (1) 打开浏览器，选择 工具->Internet 选项->清除历史记录
- (2) 启动 Wireshark 分组嗅探器
- (3) 在浏览器地址栏中输入如下网址：www.baidu.com。（实验中输入其他的网址进行分析）
- (4) 停止分组俘获。在俘获分组列表中（listing of captured packets）中找到 HTTP GET 信息和响应信息。

回答相关问题

2、分析地址 ARP 协议

- (1) 清除 ARP cache，具体做法：以管理员身份打开命令提示符，输入命令 `arp -d *`，其中的 `-d` 表示清除操作，`*` 删除 all table entries.
- (2) 打开浏览器，选择 工具->Internet 选项->清除历史记录
- (3) 启动 Wireshark 分组俘获器
- (4) 在浏览器地址栏中输入如下网址：www.qq.com。（实验报告中采用其他网址）
- (5) 停止分组俘获。
- (6) 选择 Analyze->Enabled Protocols->取消 IP 选项->选择 OK。

回答相关问题

三、使用的软件、硬件

与因特网连接的计算机网络系统；主机操作系统为 windows；使用 Wireshark、IE 等软件

四、实验步骤及实验过程原始记录(回答问题，需要有截图和简要说明)

1.

主机 48-bit Ethernet 地址：

Source: c8:6e:08:f4:f7:9f (c8:6e:08:f4:f7:9f)

2.

目的地址：

Destination: 92:ec:ea:09:17:64 (92:ec:ea:09:17:64)

2. IP 协议

Type: IPv4 (0x0800)

4.

从第 55 个开始

92	ec	ea	09	17	64	c8	0e	08	f4	f7	9f	08	00	45	00u.n.....E.
01	ba	00	ad	40	00	80	06	00	00	ac	14	0a	0e	6f	7b@... ..o{
38	3c	c4	8e	00	50	60	b6	c3	21	60	d0	eb	ef	50	18	8<...P`. .!`...P.
00	fd	5f	86	00	00	47	45	54	20	2f	66	69	6c	65	73	.._...GET /files
74	72	65	61	6d	69	6e	67	73	65	72	76	69	63	65	2f	treaming service/
66	69	6c	65	73	2f	32	61	30	64	35	39	37	63	2d	61	files/2a 0d597c-a
30	39	63	2d	34	34	30	30	2d	62	65	38	36	2d	38	37	09c-4400 -be86-87
35	39	36	64	64	32	65	36	39	36	3f	50	31	3d	31	37	596dd2e6 96?P1=17
34	36	30	35	31	30	31	33	26	50	32	3d	34	30	34	26	46051013 &P2=404&

1.

目的地址:

Destination: c8:6e:08:f4:f7:9f (c8:6e:08:f4:f7:9f)

源地址: 92:ec:ea:09:17:64 (92:ec:ea:09:17:64)

Source: 92:ec:ea:09:17:64 (92:ec:ea:09:17:64)

2.ARP 协议:

Type: ARP (0x0806)

7.

目的地址:

Destination: 92:ec:ea:09:17:64 (92:ec:ea:09:17:64)

源地址: c8:6e:08:f4:f7:9f (c8:6e:08:f4:f7:9f)

源地址:

Source: c8:6e:08:f4:f7:9f (c8:6e:08:f4:f7:9f)

8.

相应时 opcode 为 0002

```

Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: c8:6e:08:f4:f7:9f (c8:6e:08:f4:f7:9f)
Sender IP address: 172.20.10.14
Target MAC address: 92:ec:ea:09:17:64 (92:ec:ea:09:17:64)
Target IP address: 172.20.10.1

```

0000	92	ec	ea	09	17	64	c8	6e	08	f4	f7	9f	08	06	00	01d.n
0010	08	00	06	04	00	02	c8	6e	08	f4	f7	9f	ac	14	0a	0en
0020	92	ec	ea	09	17	64	ac	14	0a	01						d.. ..

请求时 opcode 为 0001

```

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: 92:ec:ea:09:17:64 (92:ec:ea:09:17:64)
Sender IP address: 172.20.10.1
Target MAC address: c8:6e:08:f4:f7:9f (c8:6e:08:f4:f7:9f)
Target IP address: 172.20.10.14

```

0000	c8	6e	08	f4	f7	9f	92	ec	ea	09	17	64	08	06	00	01	.n..... ..d....
0010	08	00	06	04	00	01	92	ec	ea	09	17	64	ac	14	0a	01n ..d....
0020	c8	6e	08	f4	f7	9f	ac	14	0a	0e							.n..... ..