《计算机网络》实验指导

实验五：ARP 协议分析

一、实验目的

1、掌握报文分析的基本方法；

2、掌握 Wireshark 软件的基本使用方法；

3、掌握使用 Wireshark 进行数据包抓取和分析的基本操作；

4、理解 ARP 报文格式和各字段含义；

5、理解 ARP 协议的通信过程。

二、实验学时

2 学时

三、实验类型

验证性

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无。

五、实验理论

1、网络嗅探的工作原理；

2、Wireshark 软件的基本使用方法；

3、ARP 协议原理与报文结构；

4、请查阅资料，列举几种常见的网络分析工具，并填写表 5-1。

表 5-1 网络分析工具对比分析一览表

序号	软件名称	版本号	软件开发商	安装环境
1				
…				

六、实验任务

1、完成 Wireshark 软件的安装和基本操作的学习；

2、完成 ARP 报文结构的分析；

3、完成 ARP 通信过程的分析。

七、实验内容及步骤

1、Wireshark 的基本操作

（1）下载软件包

可通过官方网站（http://www.wireshark.org）获得 Wireshark 软件安装程序；

可通过本课程网站（http://network.ke.51xueweb.cn）下载本教程所使用的 Wireshark 软件版本。

（2）安装软件

①双击 Wireshark 安装程序，进入如图 5-1 所示的 Wireshark 安装界面，点击【Next >】开始进行安装。在安装过程中，会提示用户选择安装相关组件程序，选择默认安装组件，具体如图 5-2 所示。

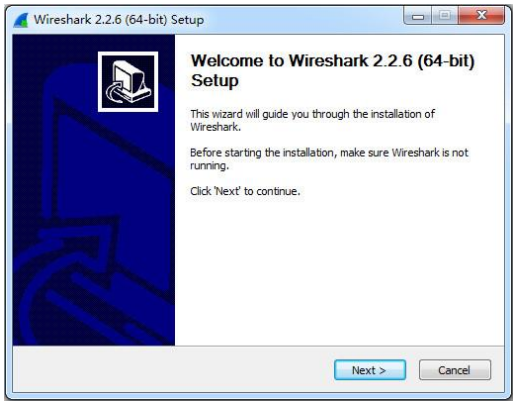

图 5-1 安装提示

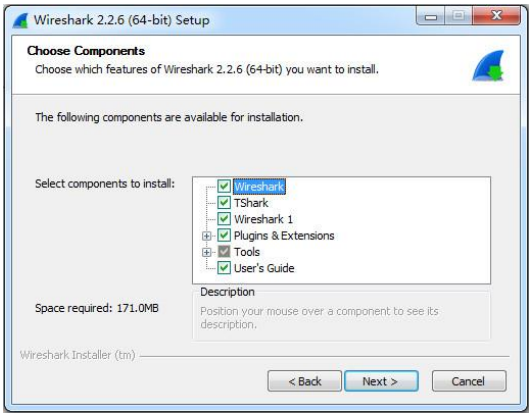

图 5-2 组件选择

②选择自定义配置，如创建快捷方式和文件扩展等，如图 5-3 所示。

③用户可使用默认的 Wireshark 安装目录，也可自行修改安装路径，如图 5-4 所示。

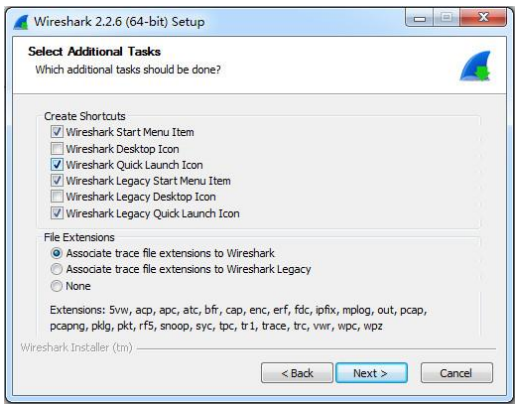

图 5-3 选择自定义配置

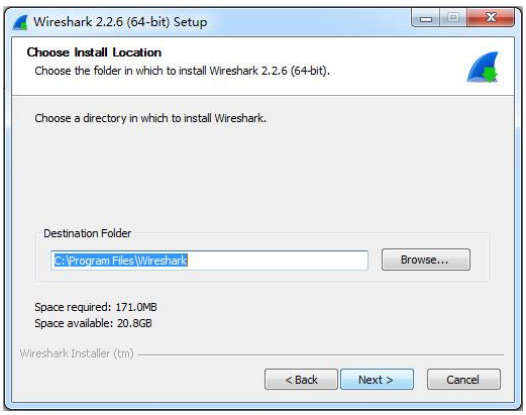

图 5-4 安装路径

④选择安装 WinPcap 软件。WinPcap 是针对 Windows 32 平台上的抓包和网络分析的一个框架软件，是 Windows 平台下免费、公共的网络访问系统。选择安装该框架软件，如图 5-5 所示，点击【Next >】继续进行 Wireshark 软件安装。

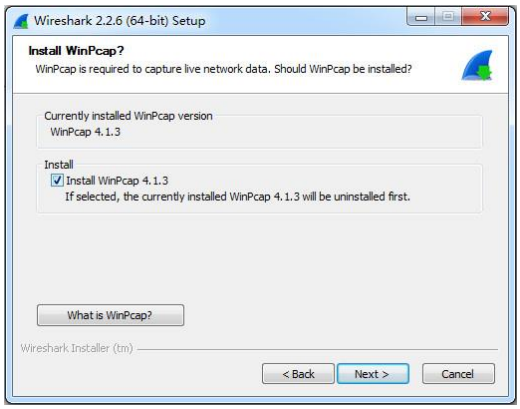

图 5-5 选择安装 Winpcap

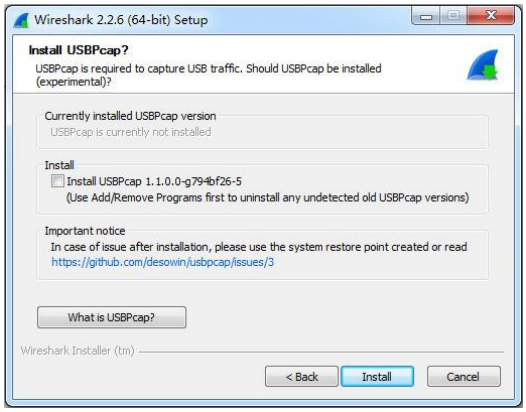

图 5-6 不安装 USBinpcap

⑤不安装 USBPcap 软件。USBPcap 是针对 USB 设备进行分析的一个框架软件，本实验不针对 USB 设备进行网络分析，所以不安装该框架，如图 5-6 所示。点击【Install】，开始进行 Wireshark 软件安装。

⑥Wireshark 软件在安装过程中将安装 WinPcap 框架，根据默认安装提示，完成该框架的安装，如图 5-7 所示。

⑦点击【Finish】完成 Wireshark 软件的安装，如图 5-8 所示。

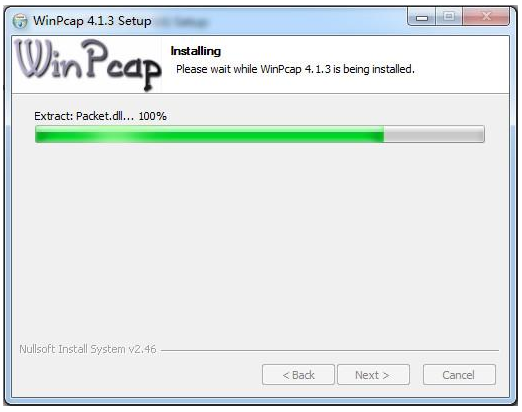

图 5-7 安装 Winpcap

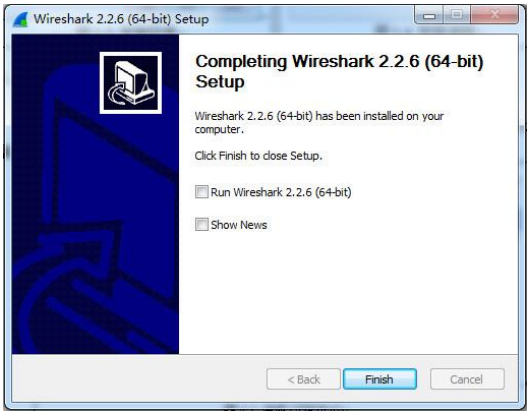

图 5-8 安装完成

⑧打开 Wireshark 软件，界面展示如图 5-9 所示，选择某一网卡适配器，选择【Start】，可查看该网卡上所传输的数据报文信息，如图 5-10 所示。

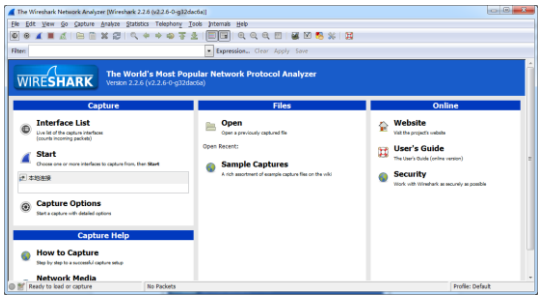

图 5-9 选择分析网卡

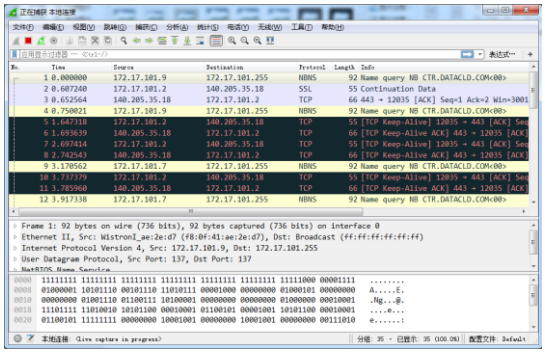

图 5-10 数据报文内容

2、ARP 数据包分析

（1）创建 ARP 协议抓包任务

打开 Wireshark，在【Filter】选项中输入报文过滤条件“arp”，选择【Start】，开始进行报文采集，如图 5-11 所示。

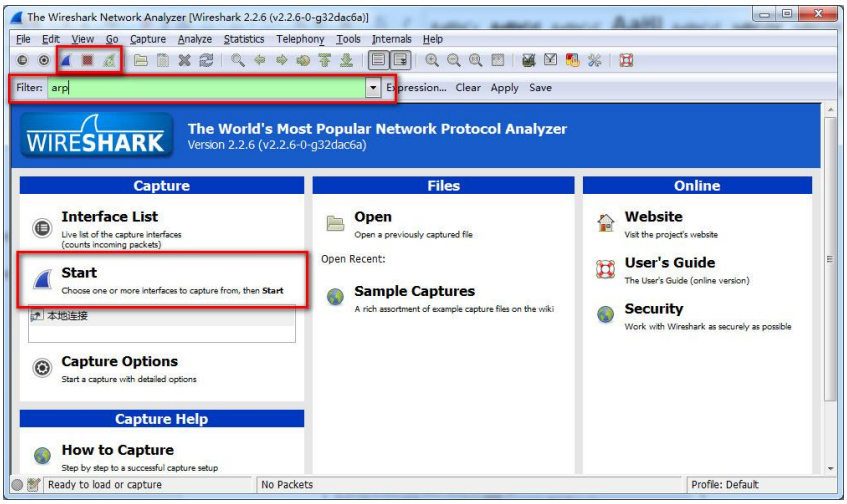

图 5-11 创建 ARP 协议抓包任务

（2）对数据包进行分析

在 Wireshark 的抓包窗体中，可以发现整个软件分为三个区域，如图 5-12 所示。上部分为抓取的数据包，中间部分为数据详细分析，下部分为数据包的内容。

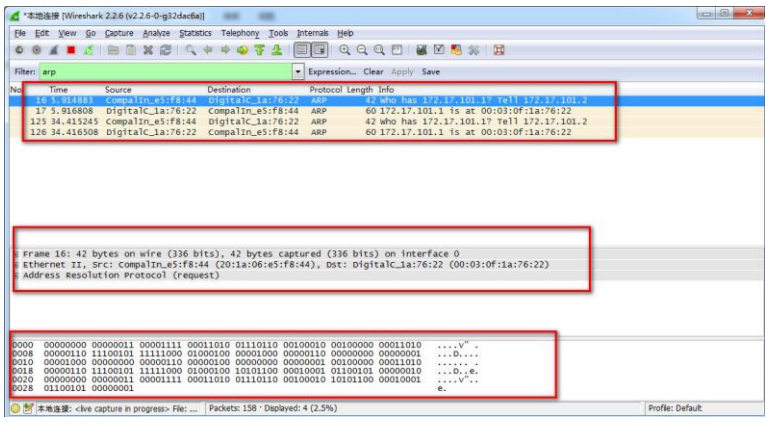

图 5-12 抓包主界面

（3）从多条 ARP 协议数据报文中任意选择其中一条数据报文，对该数据报文进行详细分析，并填写表 5-2。

表 5-2 ARP 报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第　位		
2	Protocol type		第　位		
3	Hardware size		第　位		
4	Protocol size		第　位		
5	Opcode		第　位		
6	Sender MAC address		第　位		
7	Sender IP address		第　位		
8	Target MAC address		第　位		
9	Target IP address		第　位		
10	抓取数据包的详细内容：				

3、ARP 通信过程数据包分析

（1）创建 ARP 协议抓包任务

根据过程 2 中的方法获取 ARP 协议通信过程的数据包。

（2）ARP 请求报文分析

在 Wireshark 的抓包窗体中，选择一条请求数据报文进行详细分析，如图 5-13 所示，并填写表 5-3。

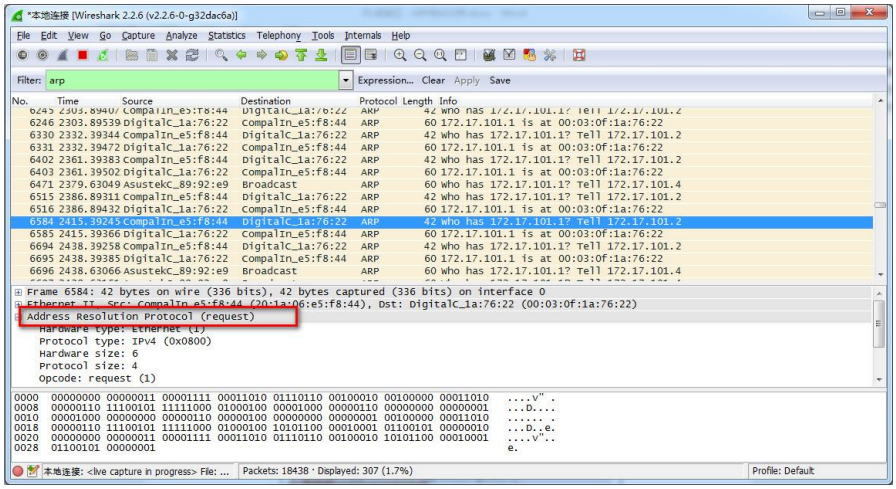

图 5-13 ARP 请求报文

表 5-3 ARP 请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第 位		
2	Protocol type		第 位		
3	Hardware size		第 位		
4	Protocol size		第 位		
5	Opcode		第 位		
6	Sender MAC address		第 位		
7	Sender IP address		第 位		
8	Target MAC address		第 位		
9	Target IP address		第 位		
10	抓取数据包的详细内容：				

（3）ARP 应答报文分析

在 Wireshark 的抓包窗体中，选择上述请求报文所对应的应答报文进行详细分析，如图 5-14 所示，并填写表 5-4。

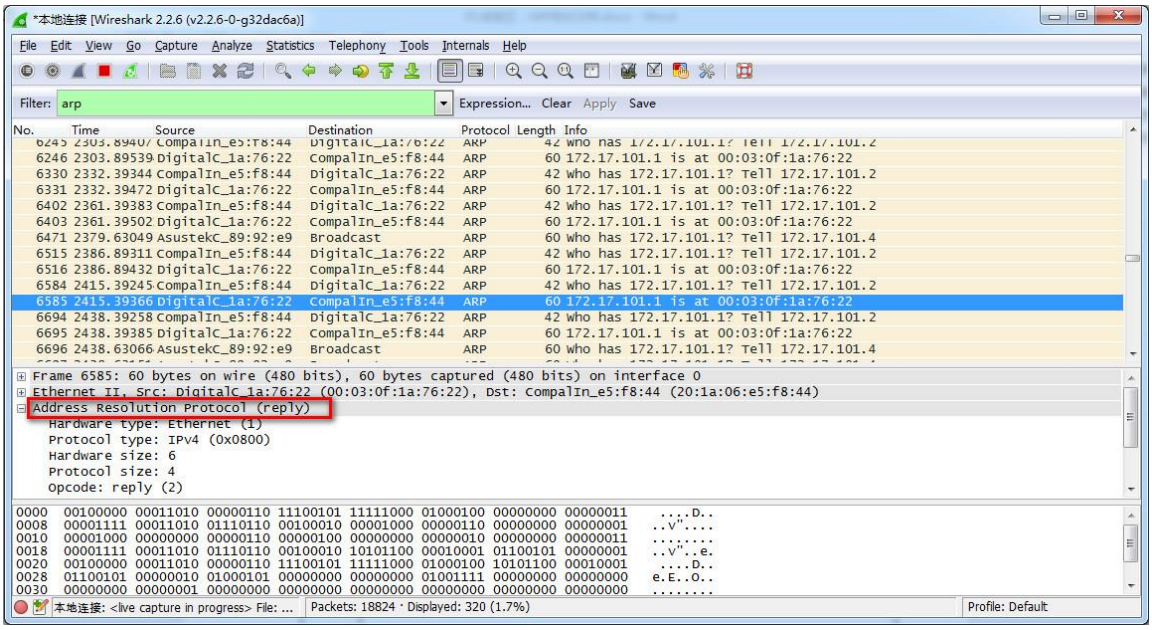

图 5-14 ARP 应答报文

表 5-4 ARP 应答报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第 位		
2	Protocol type		第 位		
3	Hardware size		第 位		
4	Protocol size		第 位		
5	Opcode		第 位		
6	Sender MAC address		第 位		
7	Sender IP address		第 位		
8	Target MAC address		第 位		
9	Target IP address		第 位		
10	抓取数据包的详细内容：				

（4）对比分析

根据 ARP 请求和应答的报文内容，比较两个数据报文内容的 5 个关键差别，并填写表 5-5。

表 5-5 ARP 通信过程报文对比分析

序号	字段名称	请求报文		应答报文	
		字段值	字段表示信息	字段值	字段表示的信息
1					
2					
3					
4					
5					
6	对比描述详细内容：				

八、实验分析

1、ARP 原理

（1）ARP 的基本原理是什么？

（2）ARP 的主要作用是什么？

2、ARP 通信报文分析

（1）观察实验过程中捕获的多个 ARP 请求报文，观察这些报文的以太网目的地址是否相同，分析其原因？

（2）观察实验过程中捕获的多个 ARP 应答报文，观察这些报文的以太网目的地址是否相同，分析其原因？