3 用 WinPCAP 监听并分析以太网的帧

3.1 实验目的

通过捕获并分析以太网帧，分析常见数据包的帧格式，熟悉以太网中常用协议及其报文格式，如 ARP、ICMP、IP 协议。

学会对捕获到的数据帧按指定的条件进行过滤，为网络流量深入分析做基础。所谓的指定条件可包含：指定的目的 IP 地址、指定的源 IP 地址、指定的协议类型等（参考 Wireshark 的过滤条件），比如当指定协议类型为 IP 时，其它类型的数据帧将被丢弃，仅留下 IP 数据帧。

3.2 实验基本要求

本实验是“用 WinPCAP 监听并解析 FTP 口令”实验的第一部分。在实验 4 中，我们还将根据 FTP 包的内容提取用户登陆的用户名和密码，并记录下该用户本次访问的相关信息。

限制使用 C/C++，拒绝其他语言；允许基于 libpcap 使用 Linux 编程实现。

IDE 推荐：VS2019

3.3 实验介绍

3.4 事前准备

此小节参考的是文件《捕获并分析帧和 IP 报文.pdf》，需要做的是配置开发环境，详细教程自行上网搜索，本次实验不再提供额外协助（3.7 **参考** 中的 3）。

安装 WinPCAP·

– WinPcap_4_1_3.exe

解压缩 WpdPack 将文件夹拷出备用

– 4.1.1-WpdPack.zip

– Include、Lib

正确解析 MAC 和 IP 地址是本节课第一要务，也是基本功

3.5 验收打分细则

实验项	验收依据	分数	备注
-2	使用 Windows 自带的“命令提示符”或“PowerShell”完成本机 IP、MAC 地址等信息的查询工作	10	ipconfig 命令的使用
-1	使用 Windows 自带的“命令提示符”或“PowerShell” 完成“本机与具有某个 IP 的主机是否连通”的检测	10	ping 命令的使用
0	熟悉 Wireshark 的使用，会设置过滤条件，如过滤出指定 IP 的数据帧	20	熟悉抓包工具的使用
1	配置好实验环境，在控制台打印出网卡	30	2、3、4 的基础

	设备列表		
2	捕获到以太网帧，并能够解析出目的MAC、源MAC	20	
3	能够过滤出特定类型的数据包，指定类型的为ARP，ICMP等	10	抓不到ARP报文时，可以根据ARP的机制来创造产生报文的条件
4(附加)	能够将捕获到的帧保存到CSV文件中，包含：时间、源MAC、源IP、目标MAC、目标IP、帧长度（以逗号间隔）	10	对侦听到的网络流量做记录，方便查阅

示例：

由于-2、-1、0项本应该是学生自己课外学习的实验辅助技能，这里不给出示例。

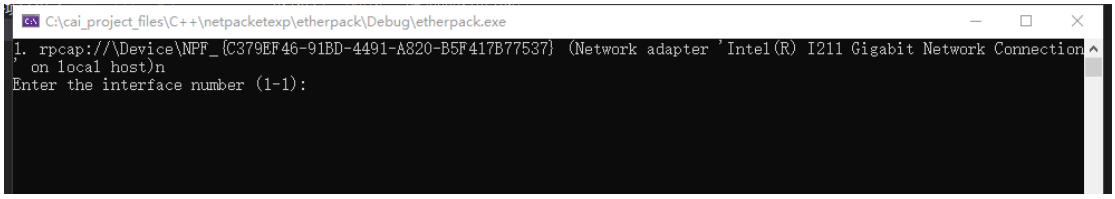

图 实验项 1

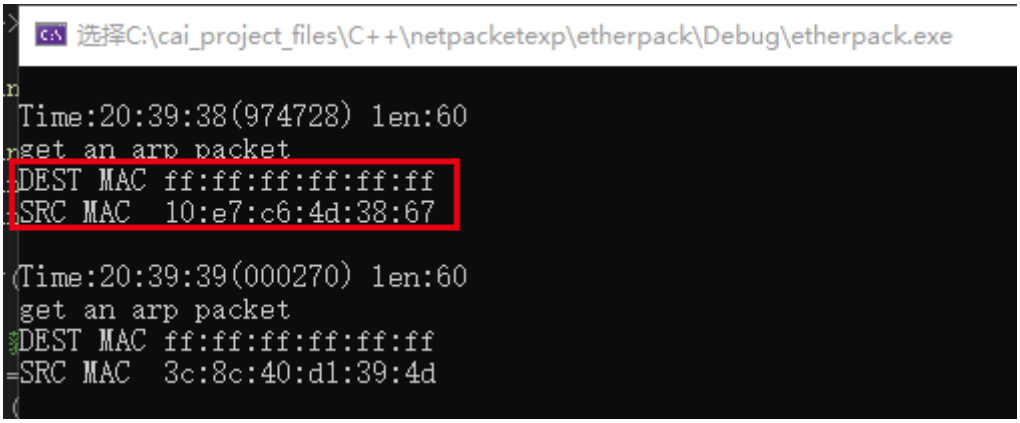

图 实验项 2

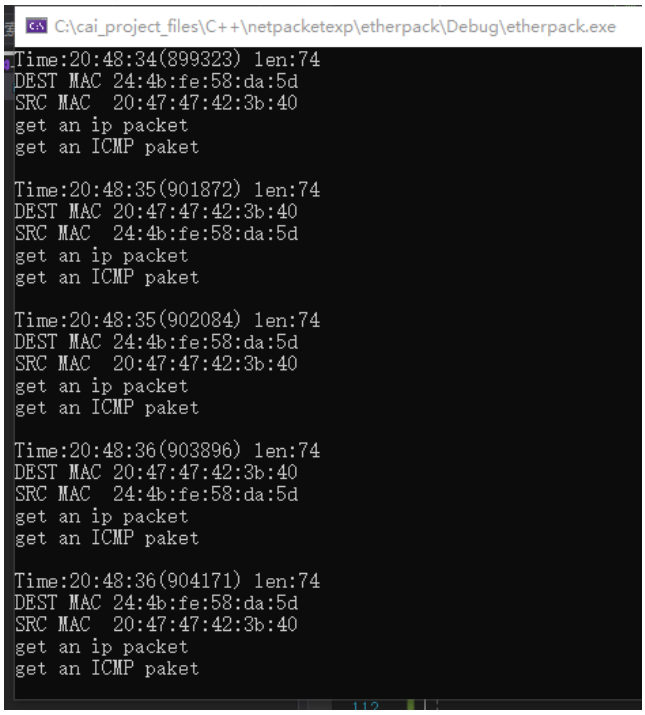

图 实验项 3 之过滤 ICMP

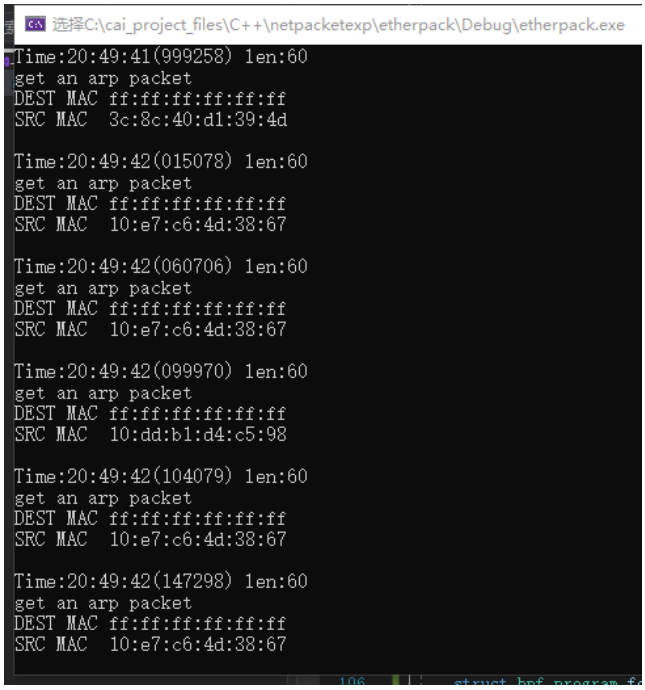

图 实验项 3 之过滤 ARP

3.6 实验提交文件

报告和源码一并打包提交，命名格式为：“E3+学号+姓名”。

报告

对于结果图片，可以根据验收项，截图对应结果。其余要求照旧。

源码

只需提交核心代码部分，额外的库等缓存文件不用提交。比如你只在 main.cpp 文件里面实现所有功能，那只需提交 main.cpp 文件即可。

3.7 参考（对你不一定有用）

0、捕获并分析帧和 IP 报文.pdf

黄老师提供的参考文件

1、Wireshark 的简单使用

参考链接：https://zhuanlan.zhihu.com/p/92993778

2、以太网帧报文格式

https://zhuanlan.zhihu.com/p/265020587?utm_source=qq

更为详细的，请查阅上课用的教材、PPT，或自行查找网上资料。

3、VS2017 配置 winpcap

参考链接：https://www.dazhuanlan.com/2019/12/16/5df6764797ac6/

问：为什么不是 VS 2019 的？

答：配置过程大同小异。

4、WinPcap 文档翻译之《Filtering expression syntax》

https://blog.csdn.net/qsycn/article/details/7378088

备注：这个用来设置过滤数据帧的条件的

5、ARP 协议原理

https://zhuanlan.zhihu.com/p/59066874

简而言之，ARP 协议是知道 IP 找 MAC。RARP 则是知道 MAC 找 IP。

更为详细的，请自行查找网上资料。

6、使用 C++操作 CSV 文件（最基本的写与读）

https://blog.csdn.net/u012234115/article/details/64465398