**任课教师：张华熊**

**《信息安全技术》**

**（2020 - 2021 学年 第 二 学期）**

**实**

**验**

**报**

**告**

**学号：202030504066姓名：许昊**

**班级：电通2班**

**实验二**

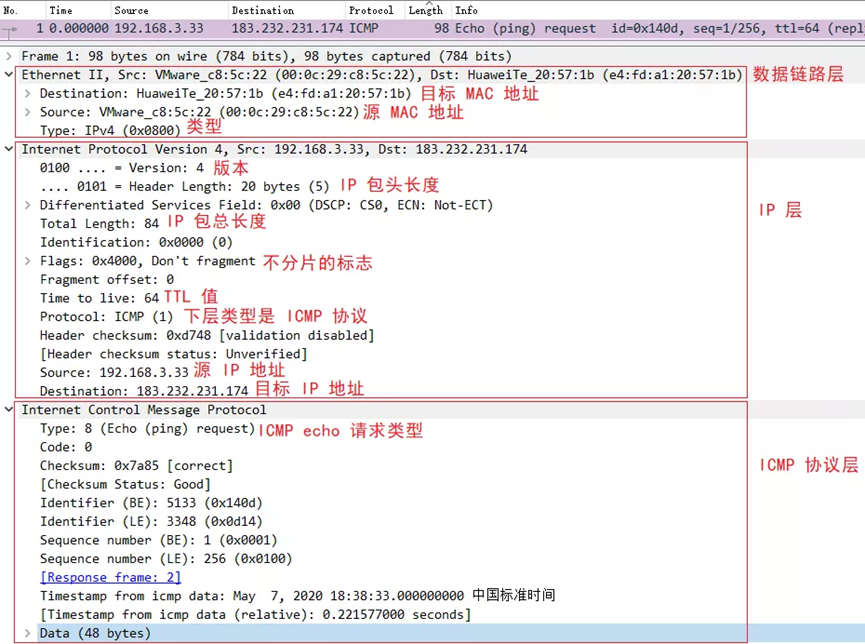
1. **实验目的**

学习虚拟机安装，版本控制Git软件、收发包、抓包软件使用及初步具备协议分析能力；

1. **实验工具**

Centos6以上系统，GitHub，科来数据包生成器/科来数据包播放器软件（pktbuilder\_x64/pktplayer\_x64），Wireshark

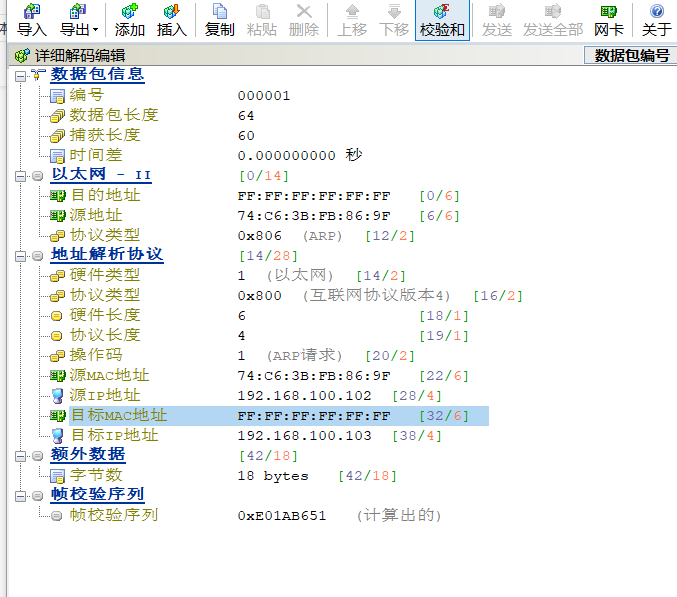
1. **实验内容**
2. 采用科来数据包生成器生成三种ARP协议数据包（请求、应答、免费(Gratuitous ARP)三种形式的ARP包；
3. 采用科来数据包播放器软件将三种伪造数据包向攻击目标机发送，检验三种形式的ARP包是否具备断网攻击能力（采用arp命令查看攻击前后的目标机ARP缓存表是否发生变化并截图说明）
4. 整个攻击过程采用Wireshark进行抓包并参考如下图对三种ARP协议进行协议分析和标注，同时对应攻击数据包导出以pcap包格式保存；



1. **实验结果**

A、

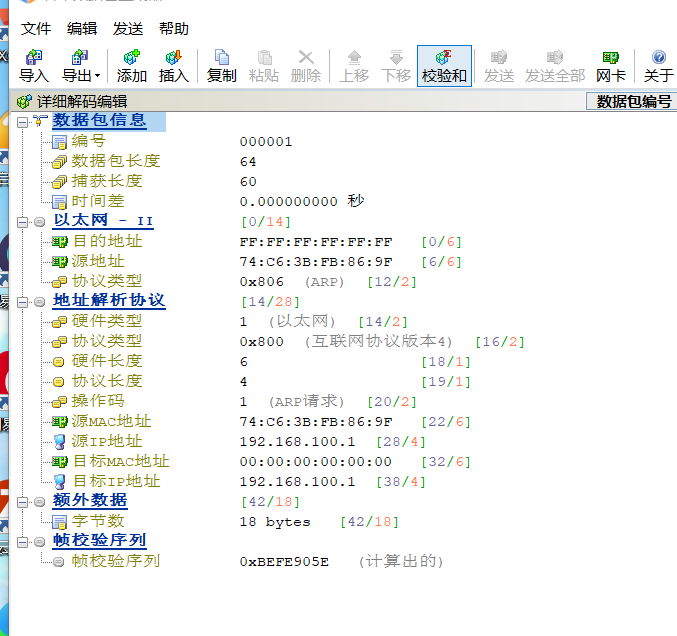
1、（请求包）



2、（应答包）

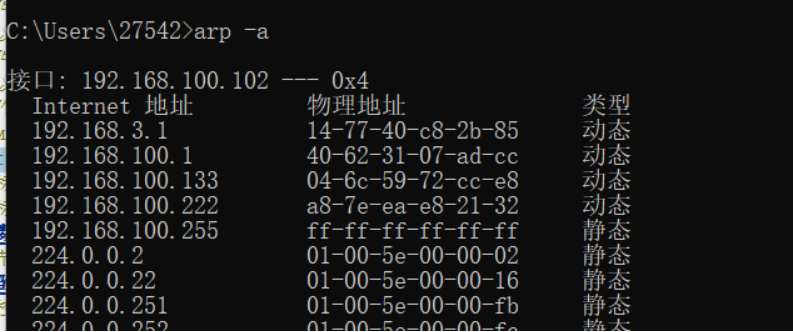


3、（免费包）[1]



B、

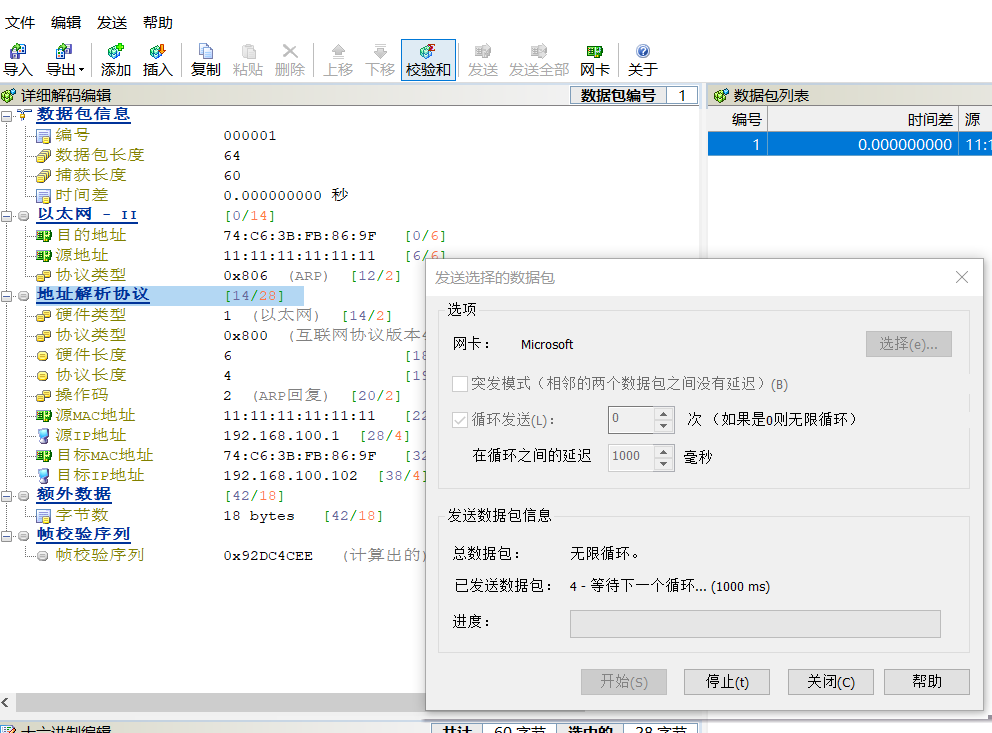
1、发送请求包



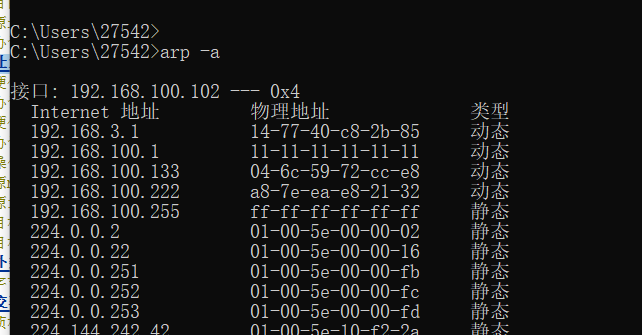


电脑可以连上网络

1. 发送回复包

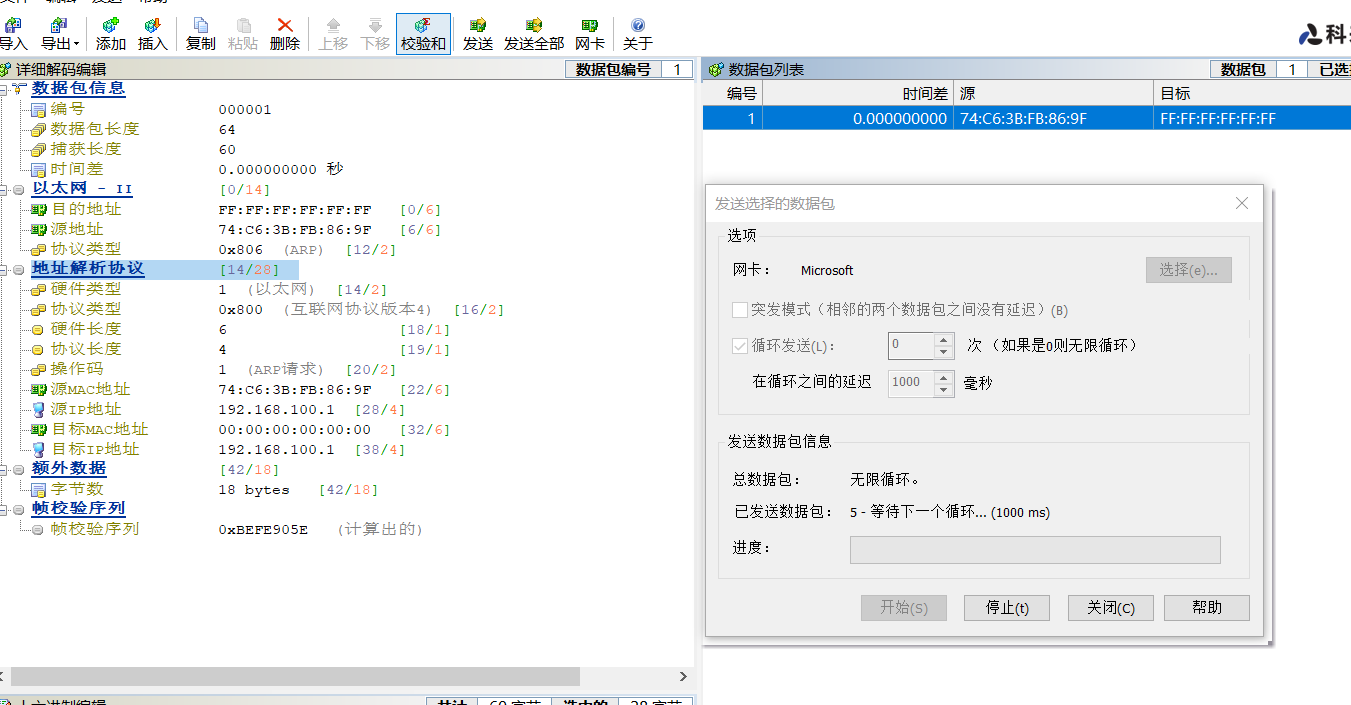


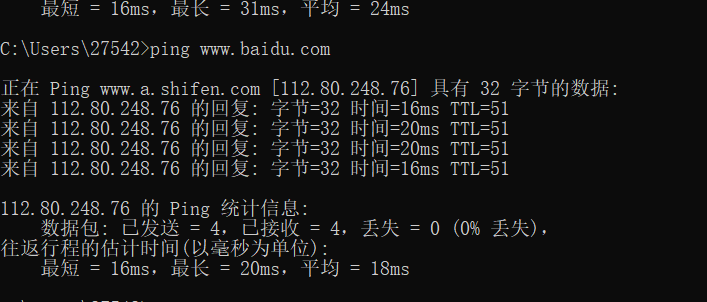




电脑连不上网，且MAC地址为11-11-11-11-11-11

3、发送免费包

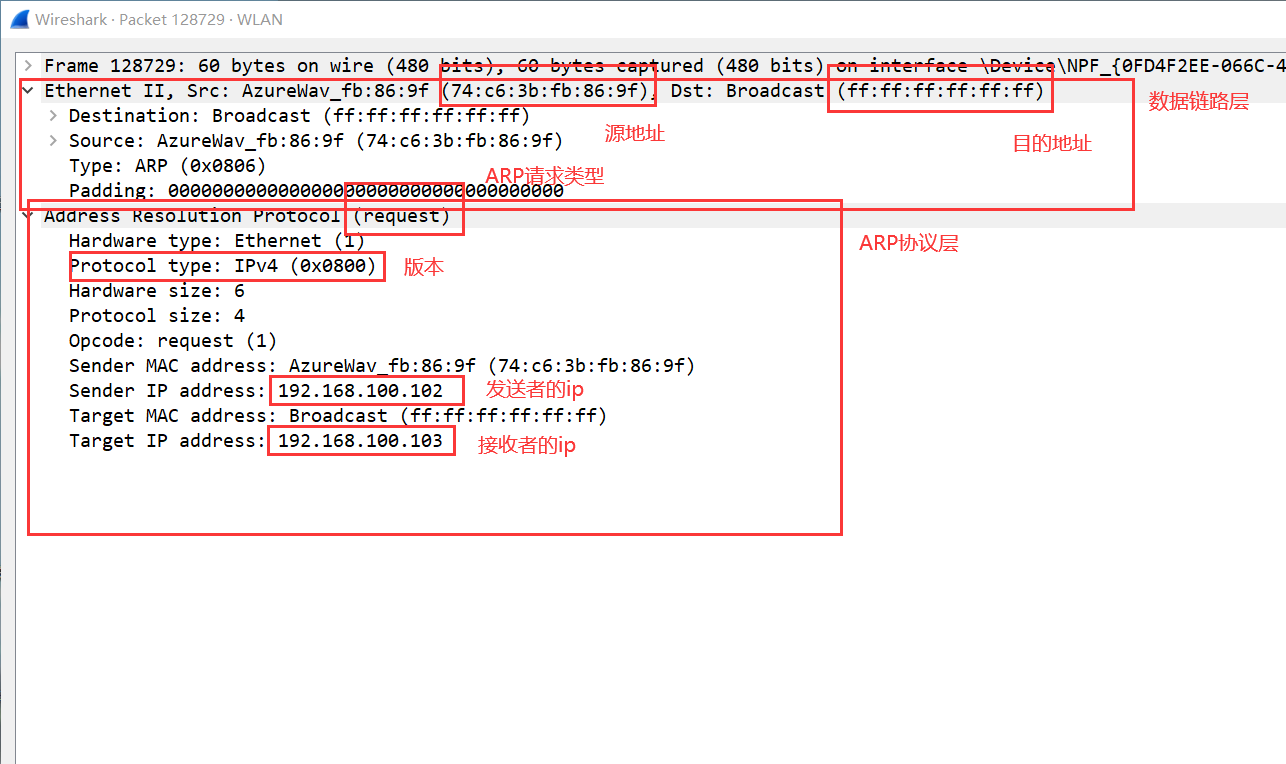




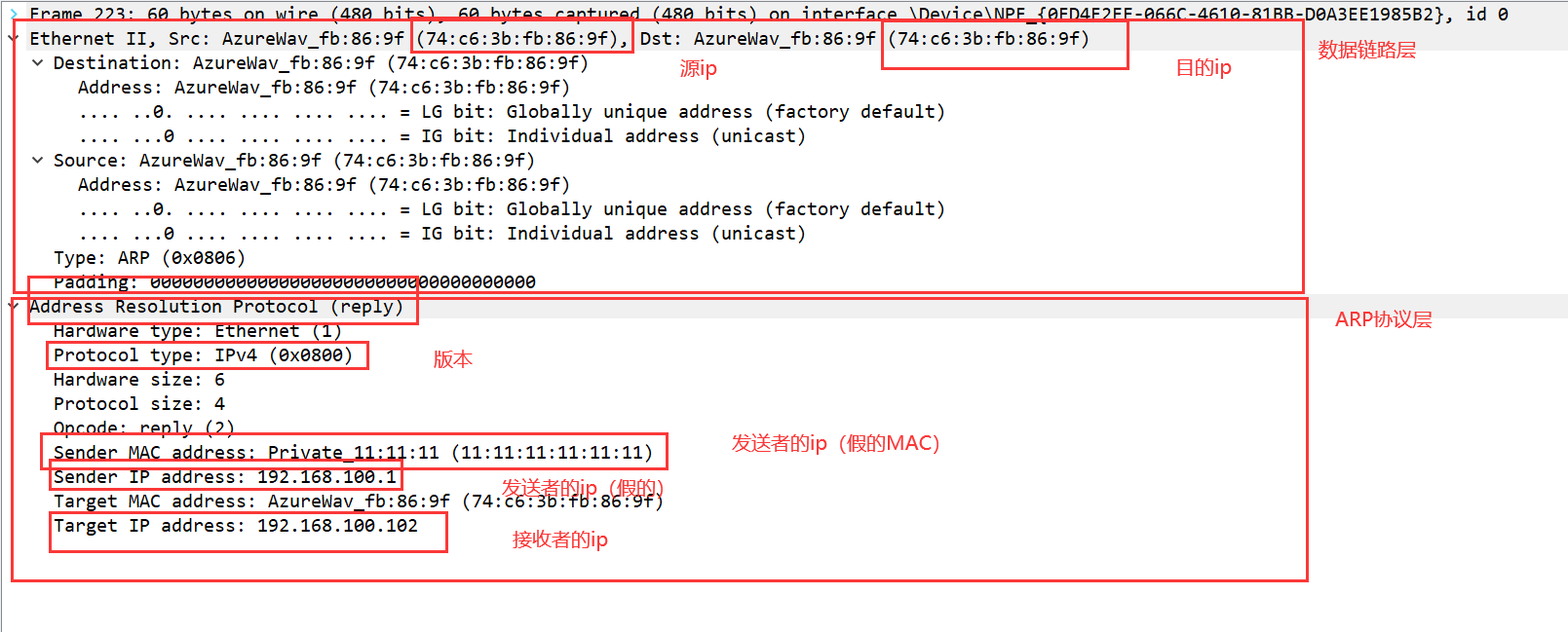
本机可以连上网络，但是本局域网内的其他主机连不上

C、

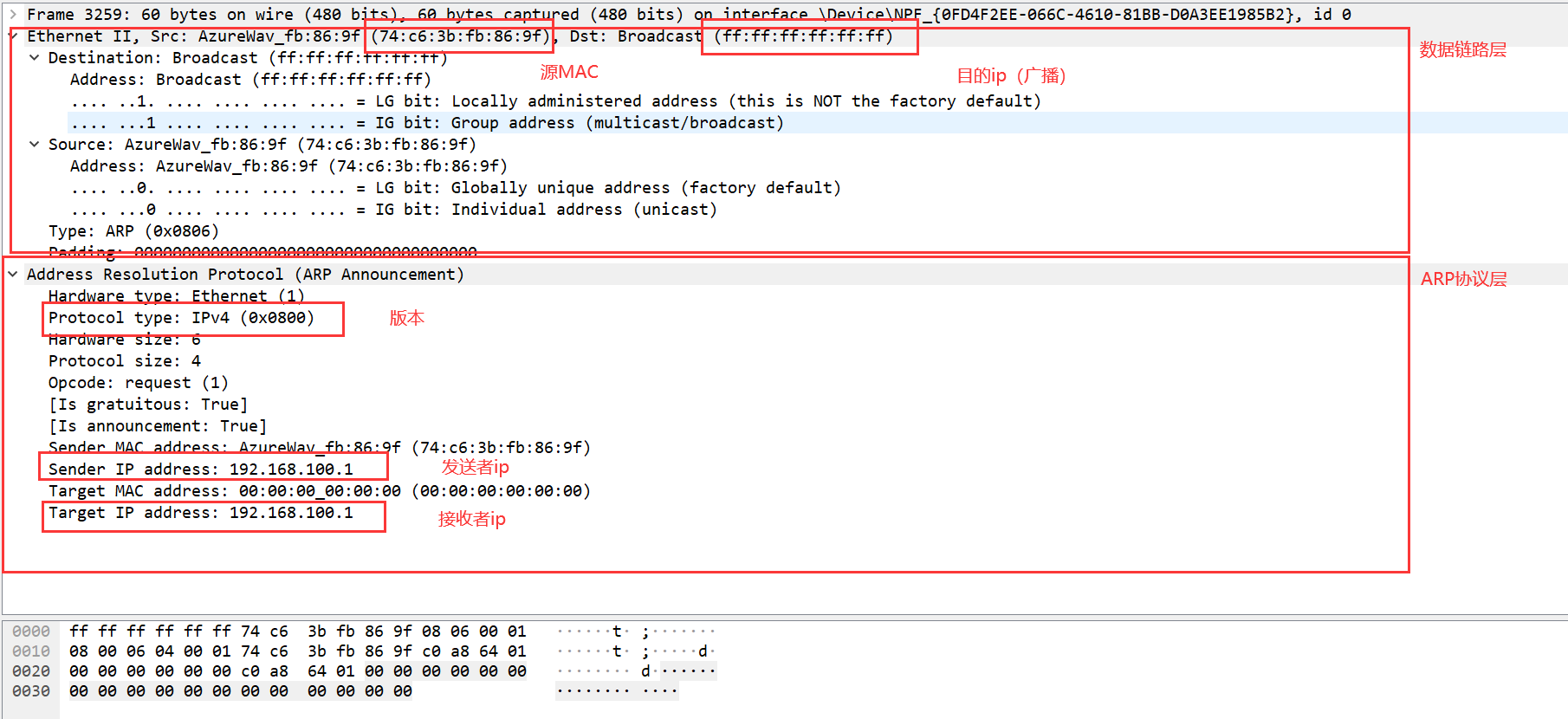
1. 发送请求包



1. 发送回复包



1. 发送免费包



D、针对ARP攻击，如何进行防护，请提出自己的意见和建议。

1. 手工静态绑定：用户接入网络之后，管理员根据此用户电脑的MAC和IP地址，然后在 接口上绑死;[2]
2. 即在交换机上开启DHCP侦听技术，当用户第一次通过DHCP获取到地址的时候，交换机 就把用户电脑的IP、MAC、Port信息记录在DHCP侦听表，后面ARP检测直接**调用**这张 DHCP侦听表即可。[2]
3. 查看wireshark抓包时，看到假装网关发包的主机MAC地址和网关的MAC地址对应不上, 因此只要降网关的ip地址和MAC地址绑定就行。
4. **参考文献：**

[1].https://blog.csdn.net/mxway/article/details/50526135?utm\_source=blogxgwz6&utm\_medium=distribute.pc\_relevant.none-task-blog-baidujs\_baidulandingword-0&spm=1001.2101.3001.4242

[2].https://www.zhihu.com/question/23401171