

**警示：**实验报告如有雷同，雷同各方当次实验成绩均以 0 分计；在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计；实验报告文件以 PDF 格式提交。

院系	计算机学院	班级	软工三班	学号	18342069	姓名	罗炜乐
完成日期： 2020 年 12 月 28 日							

## ARP 测试与防御实验

### 【实验要求】

选择一：使用交换机的ARP检查功能，防止ARP欺骗攻击。下面的【实验步骤】提供了建议。

**选择二：在缺乏设备支持的情况下，学生可自行设计实验过程。**

### 【实验原理】

ARP（Address Resolution Protocol，地址解析协议）是一个位于 TCP/IP 协议栈中的低层协议，负责将某个 IP 地址解析成对应的 MAC 地址。

#### (1) 对路由器 ARP 表的欺骗

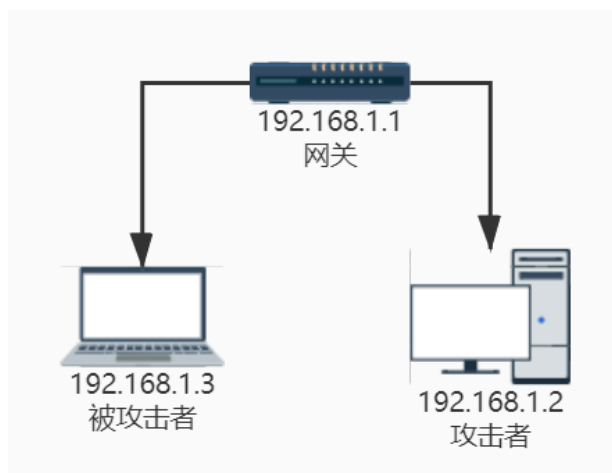
原理：截获网关数据。它通知路由器一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。

#### (2) 对内网 PC 的网关欺骗

原理：伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

交换机的 ARP 检查功能，可以检查端口收到的 ARP 报文的合法性，并可以丢弃非法的 ARP 报文，防止 ARP 欺骗攻击。

### 【实验拓扑】



ARP 实验拓扑图

### 【实验设备】

PC机2台，其中一台需要安装ARP欺骗攻击工具  
路由器 1 台（作为网关）。

通过使用Wireshark捕获攻击机发出的报文，可以看出攻击机发送了经过伪造的ARP应答（Reply）报文。

正在捕获 WLAN

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

应用显示过滤器: (Ctrl-F)

No.	Time	Source	Destination	Protocol	Length	Info
7	1.246640	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
16	3.246876	Raspberr_89:5d:b5	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
19	3.666468	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	42	Who has 192.168.1.3? Tell 192.168.1.1 (duplicate use of 192.168.1.1 detected...)
20	3.666527	Chongqin_2e:00:2d	Shenzhen_12:1a:3f	ARP	42	192.168.1.3 is at 5c:3a:45:2e:00:2d (duplicate use of 192.168.1.1 detected!)
377	5.246671	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
416	7.246290	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
442	9.247682	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
457	11.246941	Raspberr_89:5d:b5	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
472	13.248900	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
486	15.247168	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
503	17.247799	Raspberr_89:5d:b5	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
515	19.247829	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
521	19.577221	Chongqin_2e:00:2d	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.3
522	19.579290	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	42	192.168.1.1 is at 1c:40:e8:12:1a:3c
597	21.247912	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
600	23.248318	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5
607	25.248438	Shenzhen_12:1a:3f	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5

## 步骤7 验证测试。

使用PC机ping网关的地址，发现无法ping通。查看PC机的ARP缓存，可以看到PC机收到了伪造的ARP应答报文后，更新了ARP表，表中的条目为错误的绑定，即网关的IP地址与攻击机的MAC地址进行了绑定。这可在命令窗口下用arp -a进行显示。

```
C:\Users\luowle>ping 192.168.1.1
正在 Ping 192.168.1.1 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\luowle>arp -a

接口: 192.168.1.3 --- 0xe
Internet 地址      物理地址      类型
192.168.1.1        dc-a6-32-89-5d-b5 动态
192.168.1.2        dc-a6-32-89-5d-b5 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
239.255.255.250    01-00-5e-7f-ff-fa 静态
```

## 步骤8 配置ARP防火墙，防止ARP欺骗攻击。



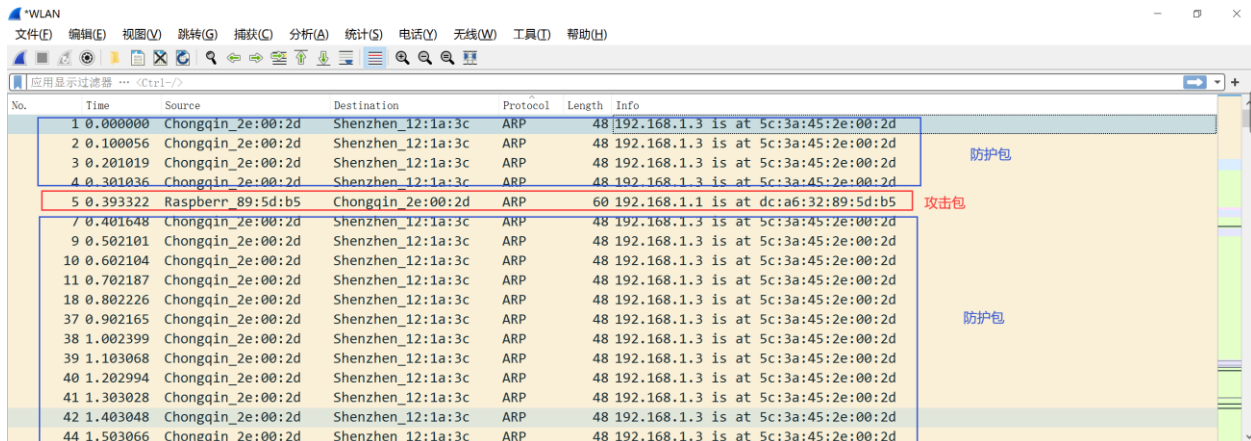
## 步骤9 验证测试。此时被攻击机的ARP表是正常的，且能ping通网关。

```
C:\Users\luowle>ping 192.168.1.1
正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=64

192.168.1.1 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 = 2ms, 最长 = 4ms, 平均 = 2ms

C:\Users\luowle>arp -a

接口: 192.168.1.3 --- 0xe
Internet 地址      物理地址      类型
192.168.1.1        1c-40-e8-12-1a-3c 动态
192.168.1.2        dc-a6-32-89-5d-b5 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
239.255.255.250    01-00-5e-7f-ff-fa 静态
```



No.	Time	Source	Destination	Protocol	Length	Info	Label
1	0.000000	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
2	0.100056	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
3	0.201019	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
4	0.301036	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
5	0.393322	Raspberr_89:5d:b5	Chongqin_2e:00:2d	ARP	60	192.168.1.1 is at dc:a6:32:89:5d:b5	攻击包
7	0.401648	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
9	0.502101	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
10	0.602104	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
11	0.702187	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
18	0.802226	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
37	0.902165	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
38	1.002399	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
39	1.103068	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
40	1.202994	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
41	1.303028	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
42	1.403048	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包
44	1.503066	Chongqin_2e:00:2d	Shenzhen_12:1a:3c	ARP	48	192.168.1.3 is at 5c:3a:45:2e:00:2d	防护包

可见，360的arp防火墙的核心是让arp表快速刷新。（只要我刷新的够快，你就骗不了我）

### 【思考题】

(1) ARP 欺骗攻击比较常见，讨论有那些普通适用的防御措施。

- ARP 防火墙（arpables、360、腾讯电脑管家等）
- 在被攻击机中静态绑定 IP 和 MAC
- 划分 VLAN 分割重要网络
- Dynamic ARP Inspection（动态 ARP 检测）
- 在交换机进行 ARP 绑定

(2) 在 IPv6 协议下，是否有 ARP 欺骗攻击？

IPv6 没有 ARP 协议。自然不存在 ARP 欺骗攻击。但是 IPv6 存在 NDP（邻居发现协议），它整合了 IPv4 中的 ARP、ICMP 和路由器广播 RA 等协议。在 NDP 中，攻击者可以像 ARP 欺骗一样针对 NS(邻居请求)/NA(邻居通告)过程进行欺骗，而针对该欺骗的防护也可以参考 ARP 欺骗防护。