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	数据科学与计算机学院	班级	软工五班	学号	17343153	姓名	张淇
完成日期： 2019 年 12 月 25 日							

ARP 测试与防御实验

【实验名称】

ARP测试与防御。

【实验目的】

使用交换机的ARP检查功能，防止ARP欺骗攻击。

【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

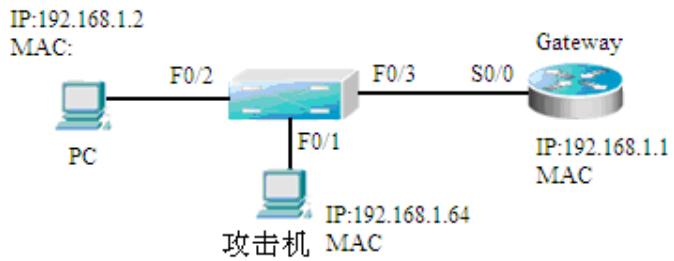
原理：伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

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。

【需求分析】

ARP欺骗攻击是目前内部网络出现的最频繁的一种攻击。对于这种攻击，需要检查网络中ARP报文的合法性。交换机的ARP检查功能可以满足这个要求，防止ARP欺骗攻击。

【实验拓扑】



ARP 实验拓扑图（例）

【实验设备】

交换机1台；

PC机2台，其中一台需要安装ARP欺骗攻击工具（下面以WinArpSpoofer为例，同学也可自行选择其他软件工具）；

路由器 1 台（作为网关）。

【实验步骤】

关于下文图中部分MAC地址不一致的说明：

本人在实验中心D502中完成此实验，在A组机器上完成近一半的实验时出现了一些“玄学BUG”，求助同学、上网查询无果后只能换成B组机器**继续完成剩余实验**。

步骤1 配置IP地址，测试网络连通性。

按照拓扑图正确配置PC机、攻击机、路由器的IP地址，使用ping命令验证设备之间的连通性，保证可以互通。查看PC机本地的ARP缓存，ARP表中存有正确的网关的IP与MAC地址绑定，在命令窗口下，arp –a。

- PC机

IP地址：

```
C:\Users\Administrator>ipconfig

Windows IP 配置


以太网适配器 实验网:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::cc75:4cc9:67e8:d5e5%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.1.2
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.1.1
```

连通性：

```
C:\Users\Administrator>ping 192.168.1.64

正在 Ping 192.168.1.64 具有 32 字节的数据:
来自 192.168.1.64 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=128

192.168.1.64 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 = 0ms, 最长 = 1ms, 平均 = 0ms
```

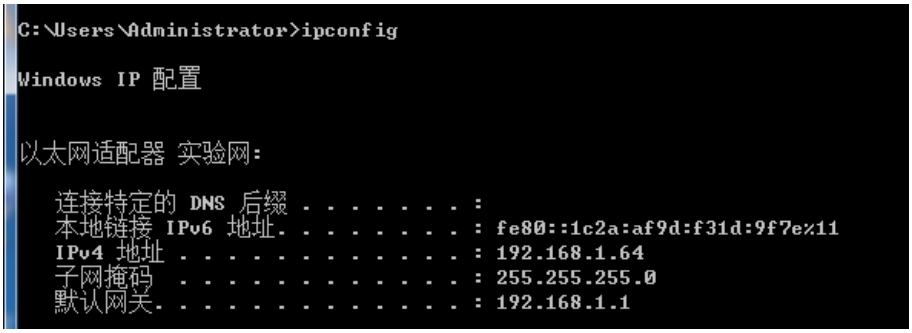
ARP缓存：

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>arp -a

接口: 192.168.1.2 --- 0xb
  Internet 地址         物理地址              类型
  192.168.1.1           58-69-6c-27-be-ad     动态
  192.168.1.64          00-88-99-00-13-53     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
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

- 攻击机

IP地址：



连通性：

- 路由器

```
22-RSR20-1(config)#interface gigabitethernet 0/0
22-RSR20-1(config-if-GigabitEthernet 0/0)#$2.168.1.1 255.255.255.0
22-RSR20-1(config-if-GigabitEthernet 0/0)#no shutdown
22-RSR20-1(config-if-GigabitEthernet 0/0)#exit
22-RSR20-1(config)#
22-RSR20-1(config)#show ip interface brief
Interface                      IP-Address(Pri)      IP-Address(Sec)      Status               Protocol
Serial 2/0                     no address           no address           down                 down
SIC-3G-WCDMA 3/0               no address           no address           up                   down
GigabitEthernet 0/0            192.168.1.1/24       no address           down                 down
GigabitEthernet 0/1            no address           no address           up                   down
VLAN 1                         no address           no address           up                   down
22-RSR20-1(config)#show ip interface brief
Interface                      IP-Address(Pri)      IP-Address(Sec)      Status               Protocol
Serial 2/0                     no address           no address           down                 down
SIC-3G-WCDMA 3/0               no address           no address           up                   down
GigabitEthernet 0/0            192.168.1.1/24       no address           up                   up
GigabitEthernet 0/1            no address           no address           down                 down
VLAN 1                         no address           no address           up                   down
22-RSR20-1(config)#
```

步骤2 在攻击机上运行WinArpSpoofer软件（在网络上下载）后，在界面“Adapter”选项卡中，选择正确的网卡后，WinArpSpoofer会显示网卡的IP地址、掩码、网关、MAC地址以及网关的MAC地址信息。

在网上没有搜索到WinArpSpoofer这款软件，与之对应的我找到一款名为WinArpAttacker的软件，下载后发现具有本实验所需要的功能，所以我用它来完成本实验。

在WinArpAttacker中找到【实验网】对应的信息（在没有进行Scan操作时，该软件无法确定网关的MAC地址，所以在此处显示为00-00-00-00-00-00-00-00）：

步骤3 在WinArpSpoofer配置

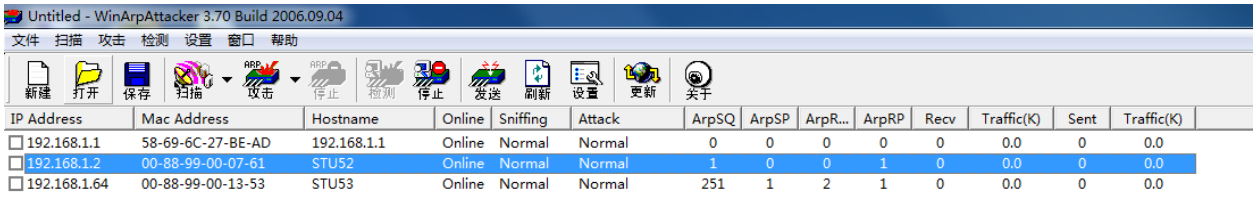
在WinArpSpoofer界面中选择“Spoofing”标签，打开“Spoofing”选项卡界面；

在“Spoofing”页面中，取消选中“Act as a Router（or Gateway）while spoofing.”选项。如果选中，软件还将进行ARP中间人攻击。点选“->Gateway”，配置完毕后，单击“OK”按钮。

步骤4 使用WinArpSpoofer进行扫描。

单击工具栏中的“Scan”按钮，软件将扫描网络中的主机，并获取其IP地址、MAC地址等信息。

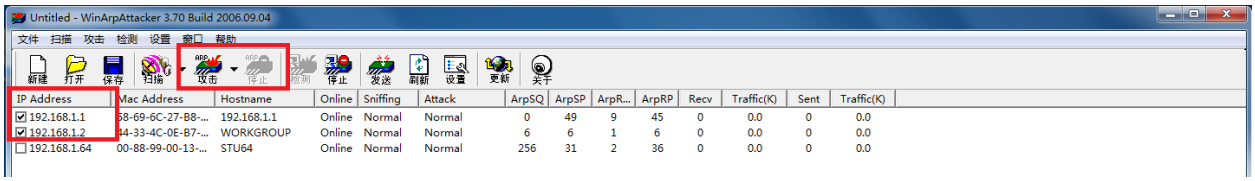
通过“Scan”得到局域网中的主机信息（从上至下依次为PC机、网关、攻击机）：



步骤5 进行ARP欺骗。

单击工具栏中的“Start”按钮，软件将进行ARP欺骗攻击。

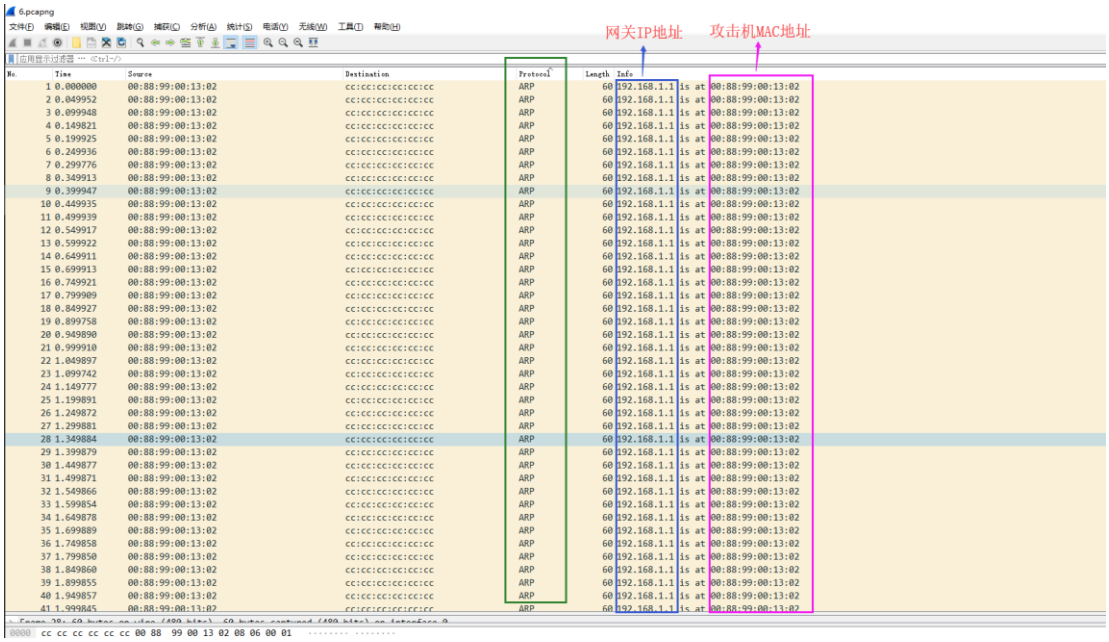
如下图：选中PC机与网关进行ARP欺骗攻击。



步骤6 验证测试。

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。

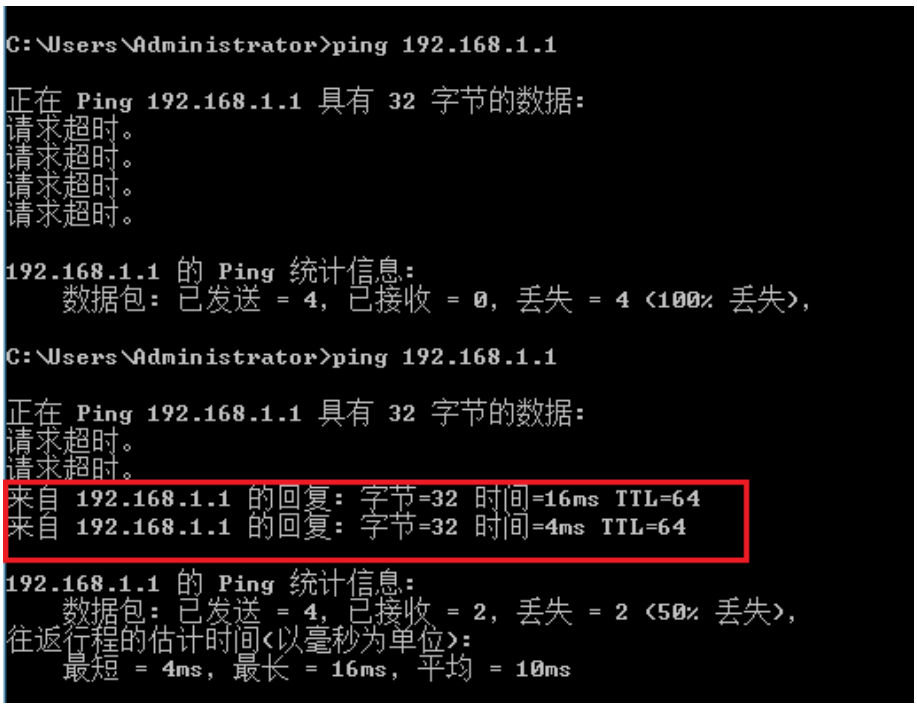
在欺骗攻击的时候在攻击机上使用Wireshark进行抓取报文，得到的结果如下：



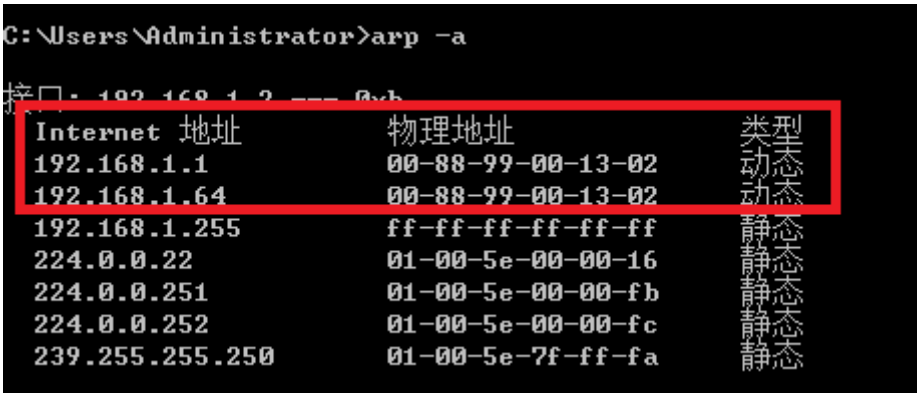
步骤7 验证测试。

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。

在欺骗的时候使用PC机ping网关，得到的结果如下（**下图红框部分出现可以ping通的原因是因为WinArpAttacker的攻击最小时间间隔为1min，所以当我在攻击后第一次ping网关的时候是全部“请求超时”，第二次ping网关的时候最后两个包是可以ping 通**）：



查看PC机的ARP表：



可以看到网关（192.168.1.1）和攻击机（192.168.1.64）的MAC地址是一样的，说明ARP欺骗攻击成功。

步骤8 配置ARP检查，防止ARP欺骗攻击。

在交换机连接攻击者PC的端口上启用ARP检查功能，防止ARP欺骗攻击。

Switch(config)#interface fastEthernet 0/1

Switch(config-if)#switchport port-security

Switch(config-if)#switchport port-security mac-address [MAC] ip-address [IP] ！将攻击者的MAC地址与其真实的IP地址绑定（MAC、IP以实际值代入）。

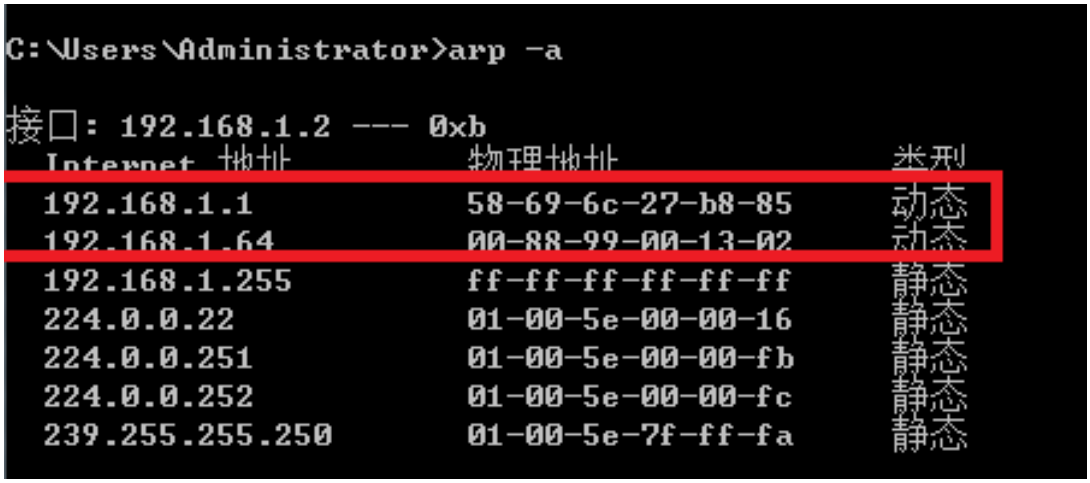
配置交换机（注：下文中的“$”是输入的指令过长而自动缩减造成的）：

```
22-S5750-1(config)#interface gigabitethernet 0/1
22-S5750-1(config-if-GigabitEthernet 0/1)#$t-security
22-S5750-1(config-if-GigabitEthernet 0/1)#$08899001302 ip-address 192.168.1.1
22-S5750-1(config-if-GigabitEthernet 0/1)#
```

步骤9 验证测试。

启用 ARP 检查功能后，当交换机端口收到非法 ARP 报文后，会将其丢弃。这时在 PC 机上查看 ARP 缓存，可以看到 ARP 表中的条目是正确的，且 PC 可以 ping 通网关。（注意：由于 PC 机之前缓存了错误的 ARP 条目，所以需要等到错误条目超时或者使用 arp –d 命令进行手动删除之后，PC 机才能解析出正确的网关 MAC 地址。

此时让攻击机再次进行 ARP 欺骗攻击，再 PC 机上查看 ARP 缓存，得到的结果如下：



可以发现网关的地址恢复正常，此时用 PC 机 ping 网关：

的确是可以 ping 通的，说明交换机端口收到非法 ARP 报文后已经将其丢弃。

【实验思考】

(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 高速缓存超时设置

在 ARP 高速缓存中的表项一般都要设置超时值，缩短这个这个超时值能够有用的避免 ARP 表的溢出。

- ARP 双向绑定

在 pc 端上 IP+mac 绑定

在网络设备（交换路由）上 采用 ip+mac+端口绑定

网关也进行 IP 和 mac 的静态绑定

- 自动查询

在某个正常的时间，做一个 IP 和 MAC 对应的数据库，以后定时检查当时的 IP 和 MAC 对应联系是否正常，定时检查交换机的流量列表，检查丢包率。

- 采用支持 ARP 过滤的防火墙

- 建立 DHCP 服务器

ARP 攻击一般先攻击网关，将 DHCP 服务器建立在网关上

- 划分安全区域

ARP 广播包是不能跨子网或网段传播的，网段可以隔离广播包。VLAN 就是一个逻辑广播域，通过 VLAN 技术可以在局域网中创建多个子网，就在局域网中隔离了广播。。缩小感染范围。 但是，安全域划分太细会使局域网的管理和资源共享不方便。

(2) 在 IPv6 协议下，是否有 ARP 欺骗攻击？

不能，或者说不能抵挡类似的攻击。

- 《中兴通讯有线网络 IPv6 技术白皮书》（6.2.2 节）

IPv6 采用 NDP 协议替代 IPv4 中的 ARP 协议，二者虽然协议层次不同但实现原理基本一致，所以针对 ARP 的攻击如 ARP 欺骗、ARP 泛洪等在 IPv6 协议中仍然存在,同时 IPv6 新增的 NS、NA 也成为新的攻击目标。NDP 协议寄希望于通过 IPSec 来实现安全认证机制，但是

协议并没有给出部署指导，另一方面，SEND 协议可以彻底解决 NDP 协议的安全问题，但是目前终端及设备还普遍不支持该协议。

- 《新的契機或危機？ 一談 IPv6 網路之安全威脅與防護》（需要**科学上网，** **三、（二）**ND 協定攻擊）

IPv6 的 ND 攻擊方式類似 IPv4 的 ARP 攻擊，可分為以下四種：

- **重導 (Redirect) 攻擊**：惡意系統將資料轉送至其他位置。
- **服務阻斷 (Denial-of-Service) 攻擊**：惡意系統阻止攻擊目標與其他網路節點間的溝通。
- **洪水服務阻斷 (Flooding Denial-of-Service) 攻擊**：惡意系統傳送大量資料至攻擊目標，使其不堪負荷。
- **偽冒 (Spoofing) 攻擊**：以假造的 IP 於網路中進行非法攻擊行為，造成破壞。