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	周一_3-4_节	学号	15331151	姓名	李佳
完成日期： 2017 年 12 月 9 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

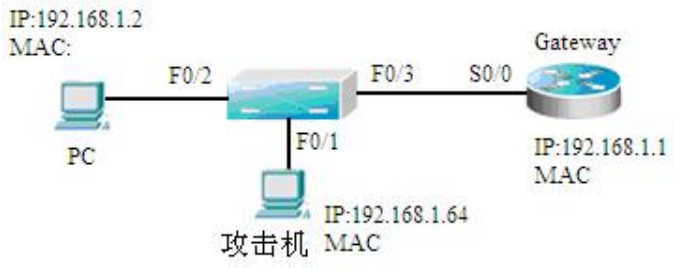
原理：伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

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）；

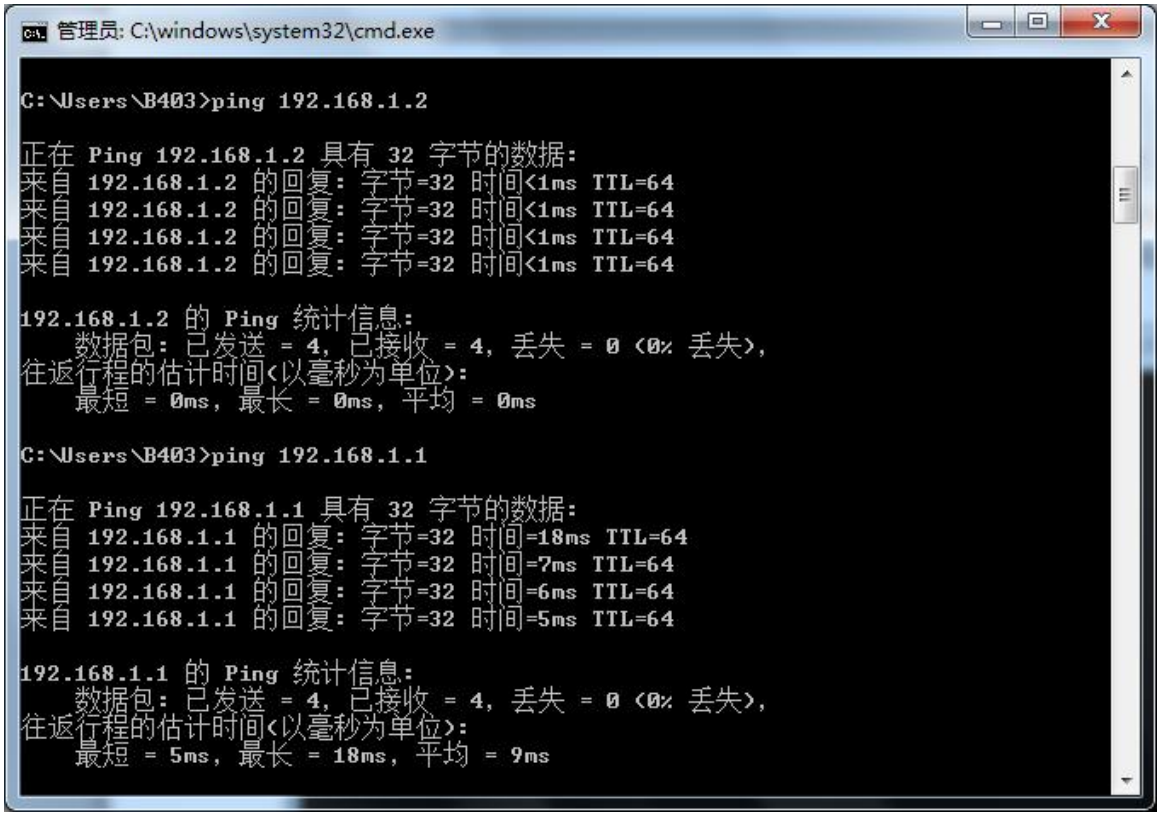
路由器 1 台（作为网关）。

【实验步骤】

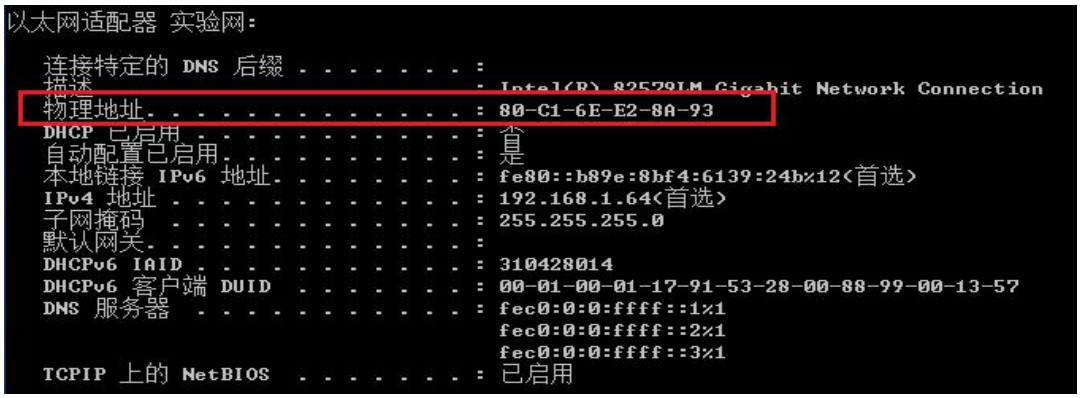
步骤1 配置IP地址，测试网络连通性。

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。

攻击机ping PC机和路由器，两台PC与路由器互相连通。



PC机本地ARP缓存及攻击机的MAC地址：



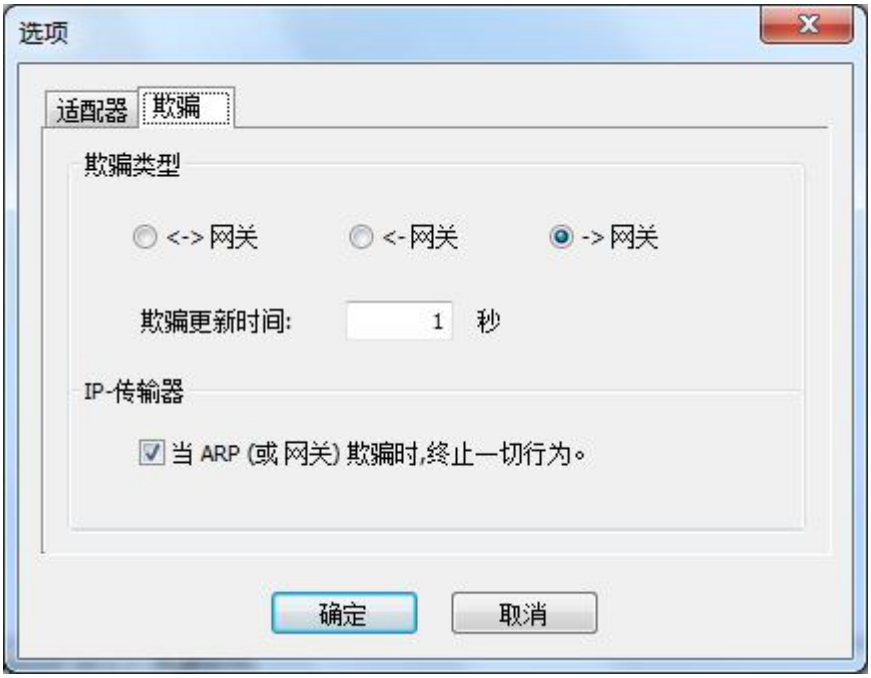
步骤2 在攻击机上运行WinArpSpoofer软件（在网络上下载）后，在界面“Adapter”选项卡中，选择正确的网卡后，WinArpSpoofer会显示网卡的IP地址、掩码、网关、MAC地址以及网关的MAC地址信息。

IP地址、掩码、网关、MAC地址等信息显示正确。

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。

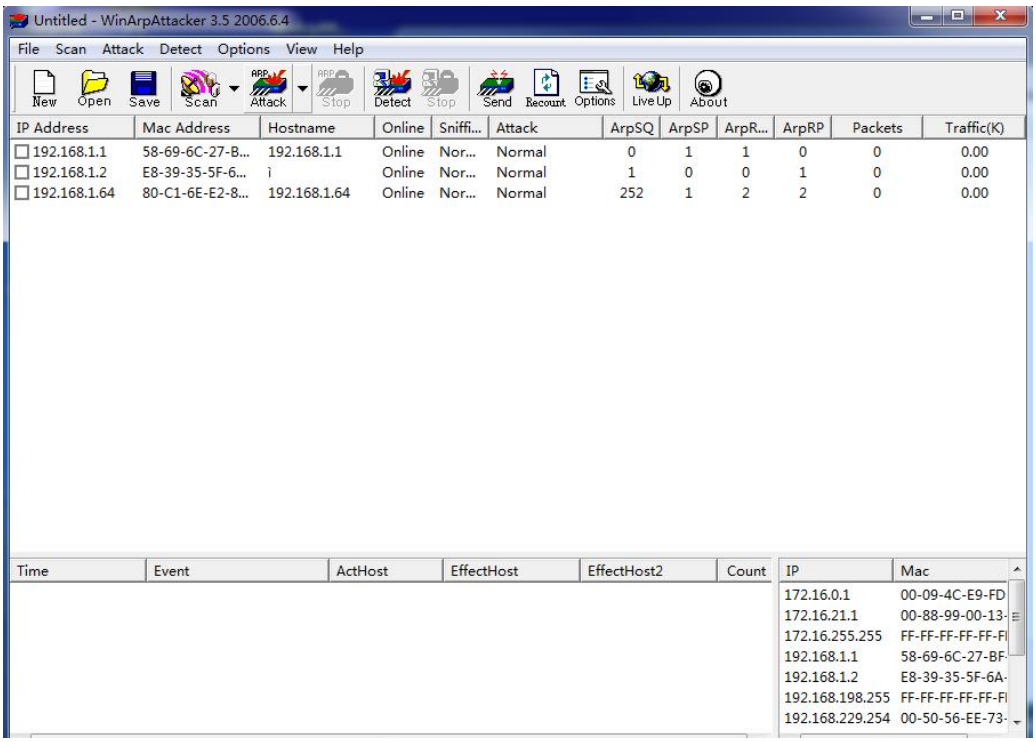
单击工具栏中的“Scan”按钮，软件将扫描网络中的主机，并获取其IP地址、MAC地址等信息。

进行WinArpSpoofer欺骗时程序不能运行，换用winArpAttacker进行ARP欺骗攻击。

Router(config)#interface gigabitethernet 0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown



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。

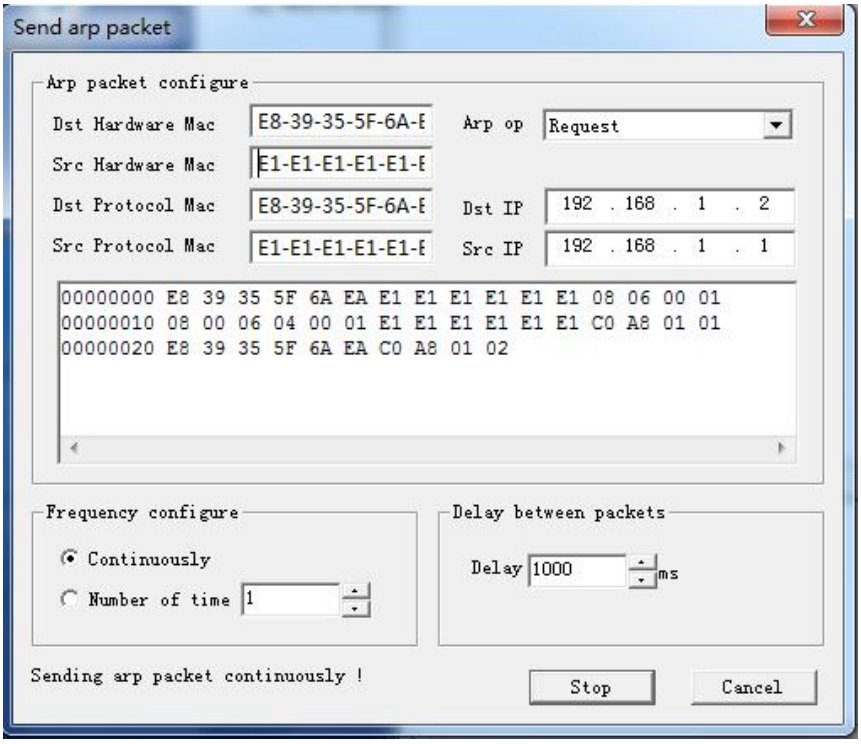
使用菜单栏的攻击方式在两三次后被自动修正。因此我自主发送欺骗包(Send)，攻击机伪造为路由器，配置为下：

Des Mac E8-39-35-5F-6A-EA

SRC MAC E1-E1-E1-E1-E1-E1

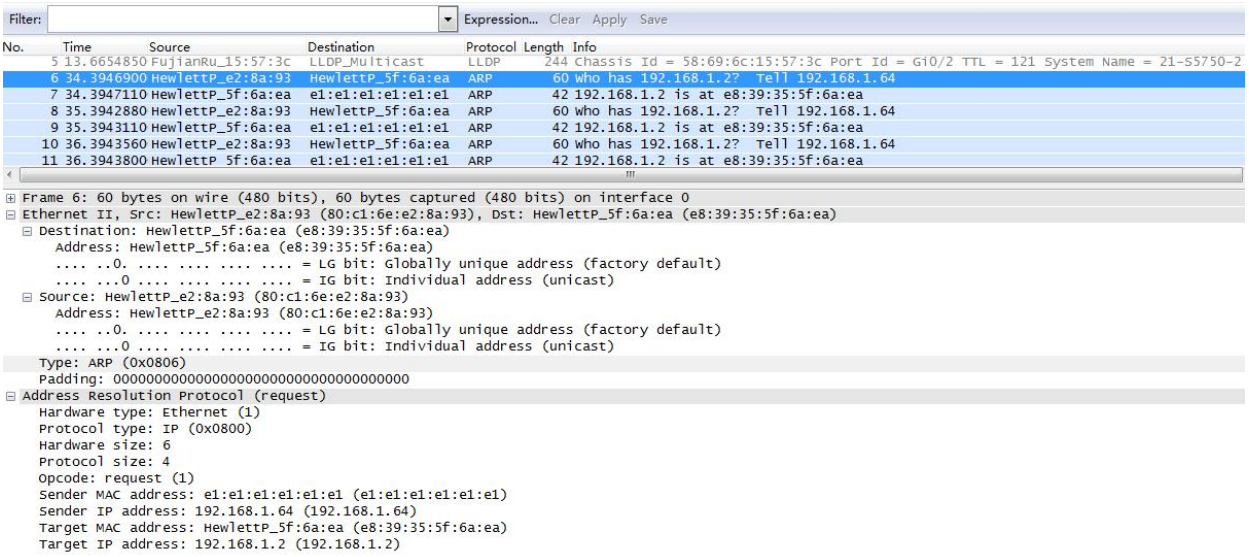
Des Mac E8-39-35-5F-6A-EA 192.168.1.2

SRC MAC E1-E1-E1-E1-E1-E1 192.168.1.1



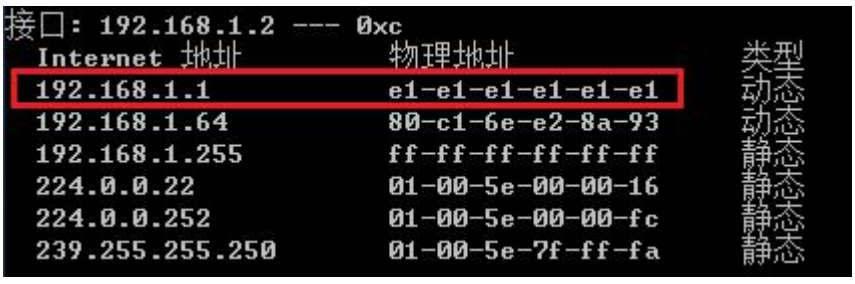
步骤6 验证测试。

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。



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。



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）。

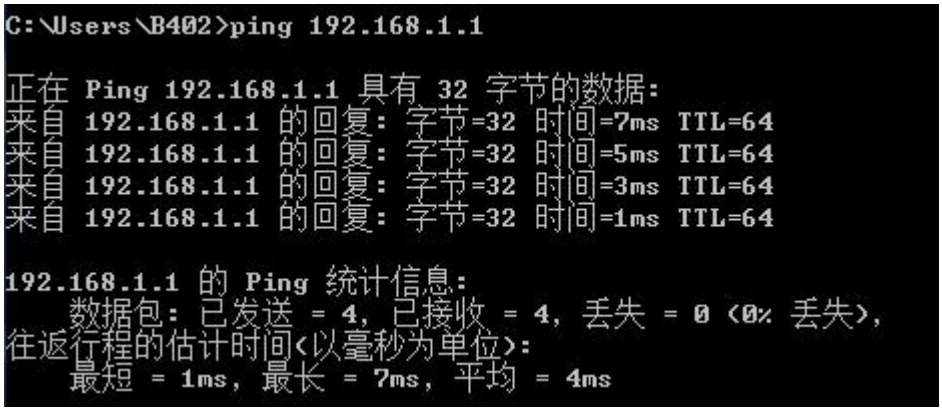
Switch(config-if)#switchport port-security mac-address 80c16ee28a93 ip-address 192.168.1.64

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。

PC机Arp －d清空缓存后

使用刚才的方式伪造一个ARP包，发送到PC机上(步骤5)，后尝试ping网关及查看arp缓存。PC ping 192.168.1.1



PC机Arp －a查看ARP缓存

启用 ARP 检查功能后交换机端口收到非法的 ARP 报文后，将其丢弃，网关 MAC 地址被正确存储。

【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。

a.在电脑上安装 ARP 个人防火墙，在终端电脑上对网关进行绑定，保证不受网络中假网关的影响;

b.PPPoE 网络下给每个用户分配一个账号、密码，上网时必须通过 PPPoE 认证。

c.VLAN 和交换机端口绑定。通过划分 VLAN 和交换机端口绑定，以图防范 ARP。细致地划分 VLAN，减小广播域的范围，使 ARP 在小范围内起作用，而不至于发生大面积影响。

d.通过免疫网络来防范 ARP 欺骗。免疫网络就是现有的路由器、交换机、网卡、网线构成的普通交换网络基础上，加入一套安全和关机的解决方案。用免疫墙路由器或免疫网关，替换掉现有的宽带接入设备。在免疫墙路由器下，需自备一台服务器 24 小时运行免疫运营中心。终端绑定采用看守式绑定技术，不安装或卸载就不能上网。把正确的网关信息存储在非公开的位置加以保护，任何对网关信息的更改，由于看守程序的严密监控，都不成功。免疫墙路由器或免疫网关的 ARP 先天免疫技术。

(2) 在 IPv6 协议下，是否有 ARP 欺骗攻击？

IPv6 协议下同样会存在类似的 ARP 欺骗攻击。

与 IPv4 的 ARP 相比，IPv6 地址解析技术工作在 OSI 参考模型的网络层，与链路层协议无关。这一特点的益处如下：（1）加强了地址解析协议与底层链路的独立性。对每一种链路层协议都使用相同的地址解析，无须再为每一种链路层协议定义一个新的地址解析协议；（2）增强了安全性。在第三层实现地址解析可以利用三层标准的安全认证机制来防止 ARP 攻击和 ARP 欺骗；（3）减小了报文传播范围。IPv6 的地址解析利用三层组播寻址限制了报文的传播范围，可节省网络带宽。

IPv6 不再执行地址解析协议(ARP)或反向地址解析协议(RARP)，而以邻居发现协议中的相应功能代替，IPv6 邻居发现协议与 IPv4 区别在于，NDP 提供前缀发现、邻居不可达检测、重复地址检测、地址自动配置等功能。

但是，IPv6 协议下的地址欺骗类似于 IPv4 的 ARP 欺骗，攻击者伪造 RS/NS/NA 报文来修改受害主机或网管上受害主机的 MAC 地址，造成受害主机无法与网络进行正常的通信。所以，在 IPv6 协议下并不能完全防范此类攻击。