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		班级		学号		姓名	
完成日期： 2017 年 月 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

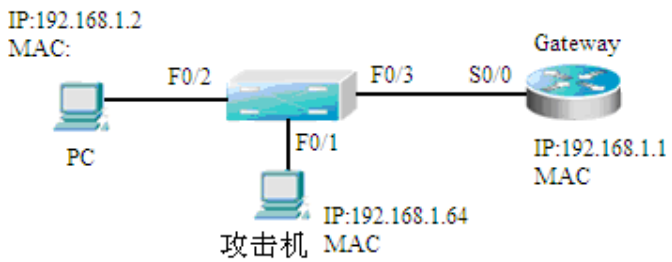
原理：伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

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）；

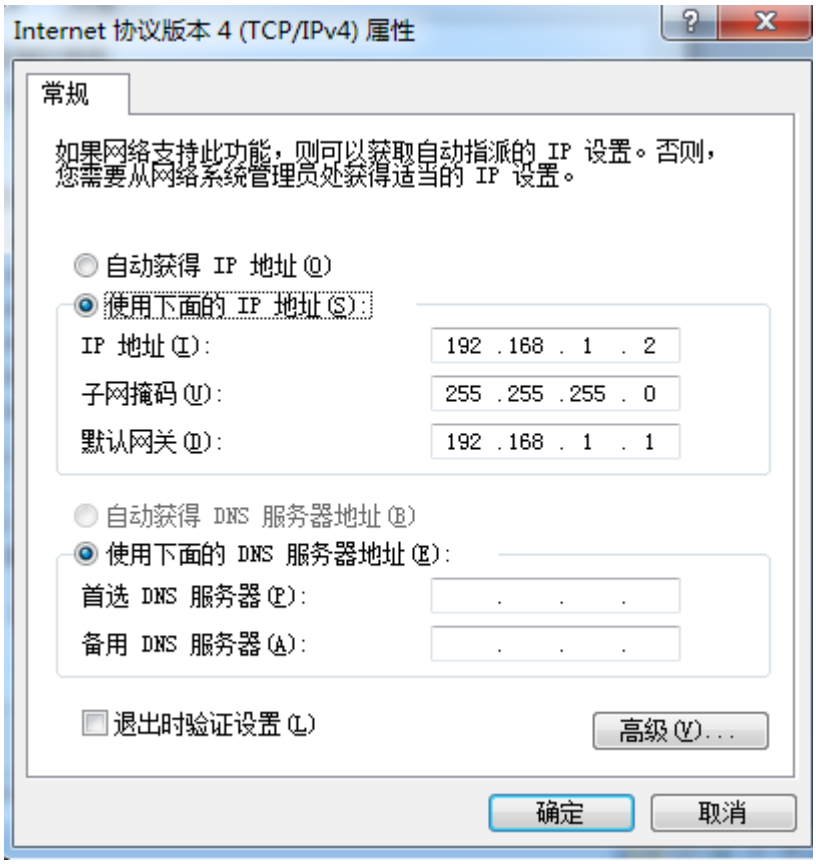
路由器 1 台（作为网关）。

【实验步骤】

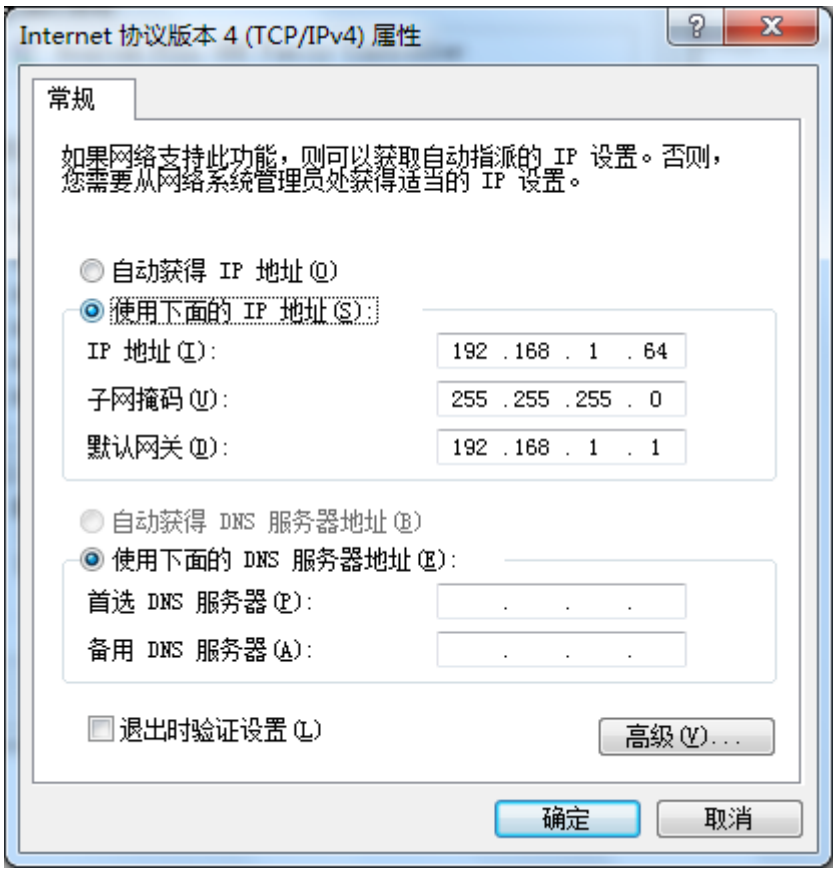
步骤1 配置IP地址，测试网络连通性。

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。

配置PC机地址



攻击机



路由器IP地址

```
8-RSR20-1(config)#interface gigabitethernet 0/0
8-RSR20-1(config-if-GigabitEthernet 0/0)#ip address 192.168.1.1 255.255.255.0
8-RSR20-1(config-if-GigabitEthernet 0/0)#no shutdown
8-RSR20-1(config-if-GigabitEthernet 0/0)#exit
```

```
8-RSR20-1(config)#show ip interface brief
Interface                  IP-Address(Pri)      IP-Address(Sec)      Statu
s                Protocol
Serial 2/0                 no address           no address           up
                 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
8-RSR20-1(config)#
```

使用ping命令验证设备之间的连通性，保证可以互通。

```
C:\Users\B402>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=64
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.64 的回复: 字节=32 时间<1ms TTL=64

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 = 0ms, 平均 = 0ms
```

```
C:\Users\B403>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.2 的回复: 字节=32 时间<1ms TTL=128

192.168.1.2 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 = 0ms, 平均 = 0ms

C:\Users\B403>
```

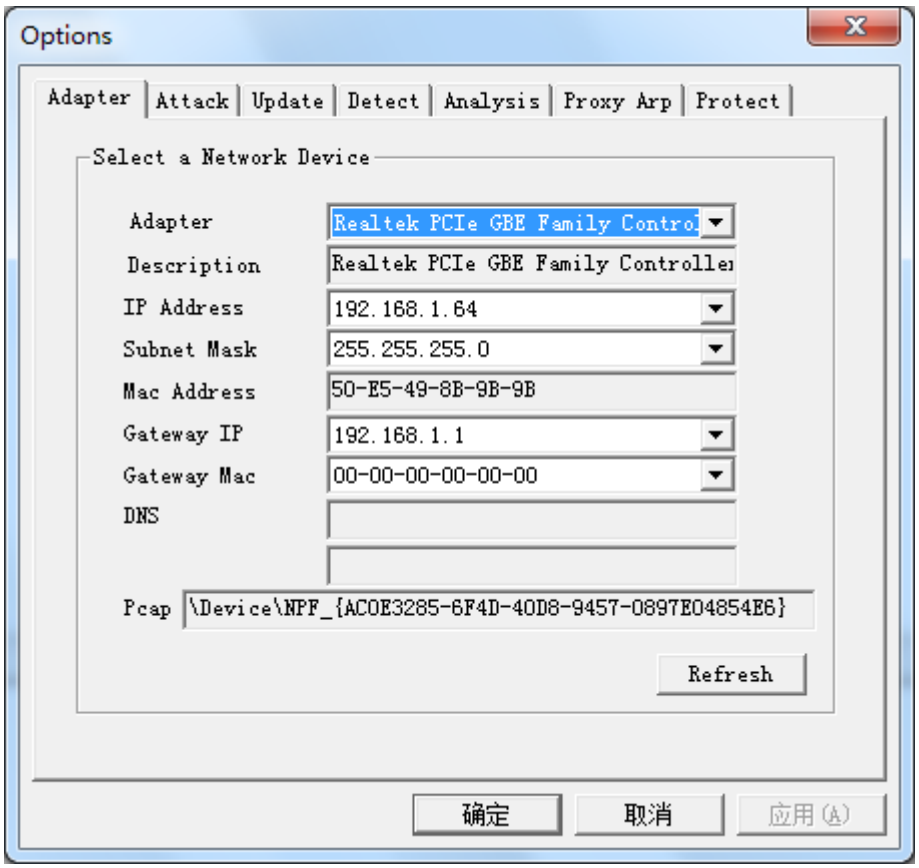
查看PC机本地的ARP缓存，ARP表中存有正确的网关的IP与MAC地址绑定，在命令窗口下，arp –a。

```
C:\Users\B402>arp -a

接口: 192.168.1.2 --- 0xc
  Internet 地址         物理地址              类型
  192.168.1.1           58-69-6c-27-bd-51     动态
  192.168.1.64          50-e5-49-8b-9b-9b     动态
  192.168.1.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     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
  239.192.152.143       01-00-5e-40-98-8f     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

C:\Users\B402>
```

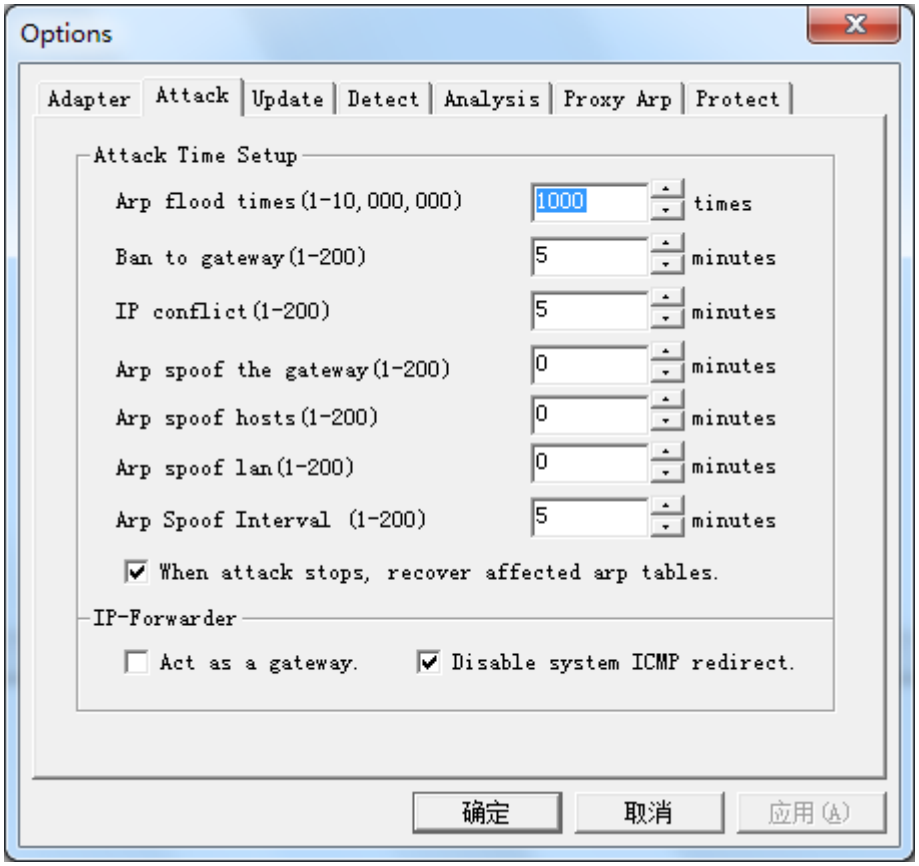
步骤2 在攻击机上运行WinArpSpoofer软件（在网络上下载）后，在界面“Adapter”选项卡中，选择正确的网卡后，WinArpSpoofer会显示网卡的IP地址、掩码、网关、MAC地址以及网关的MAC地址信息。



步骤3 在WinArpSpoofer配置

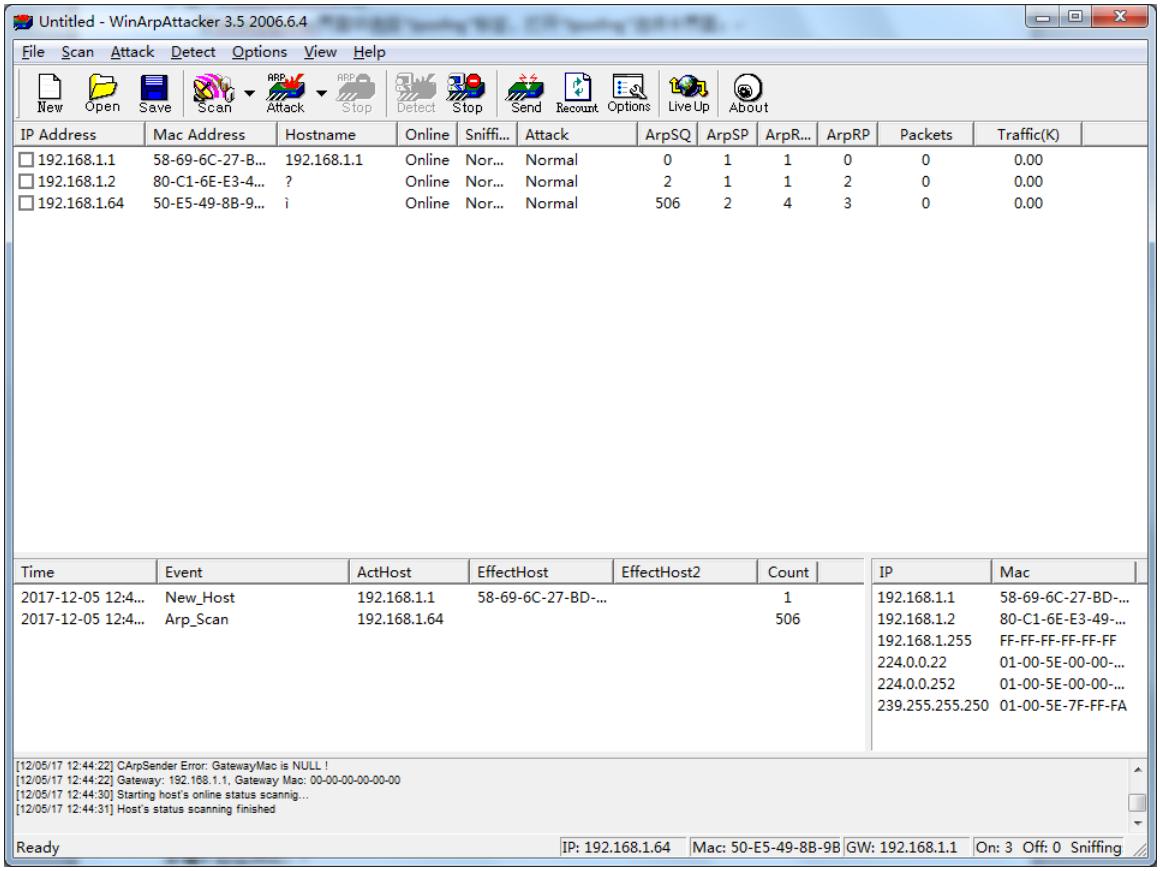
在WinArpSpoofer界面中选择“Spoofing”标签，打开“Spoofing”选项卡界面；

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。



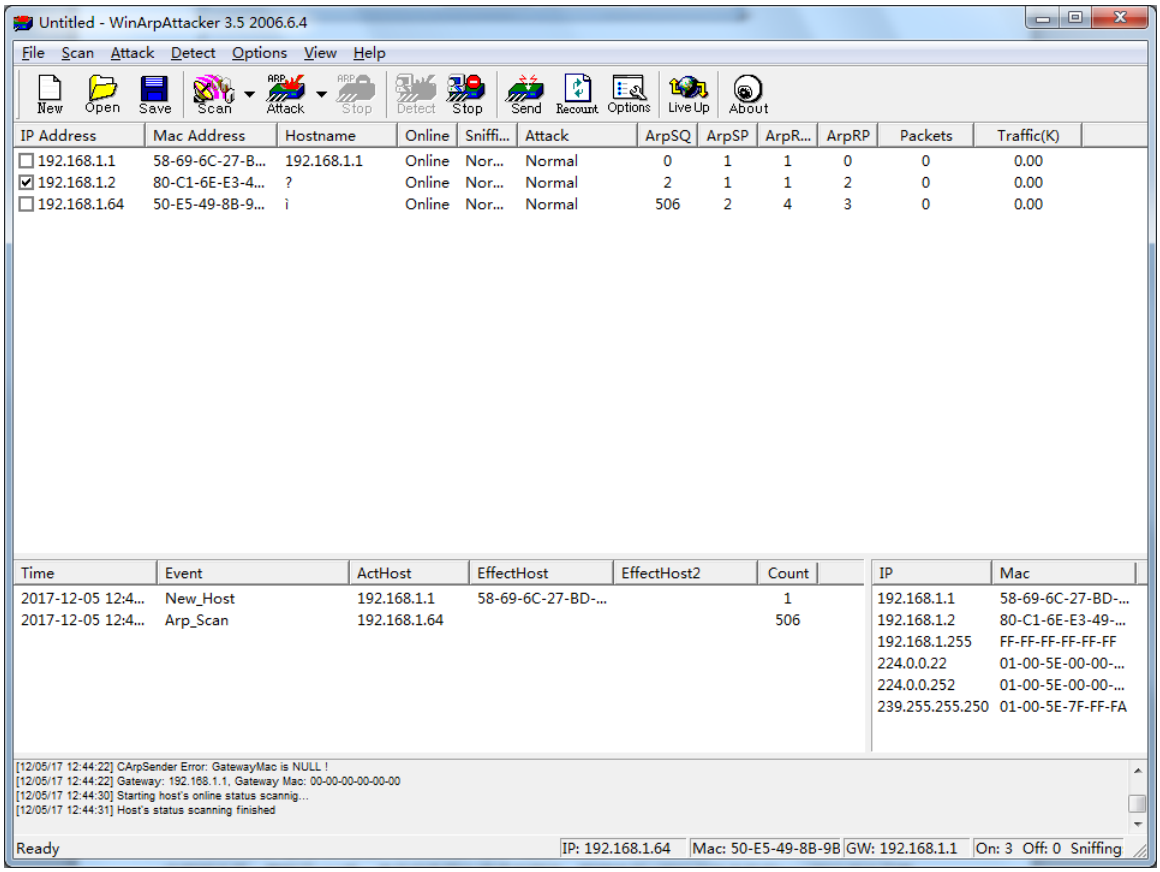
步骤4 使用WinArpSpoofer进行扫描。

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。



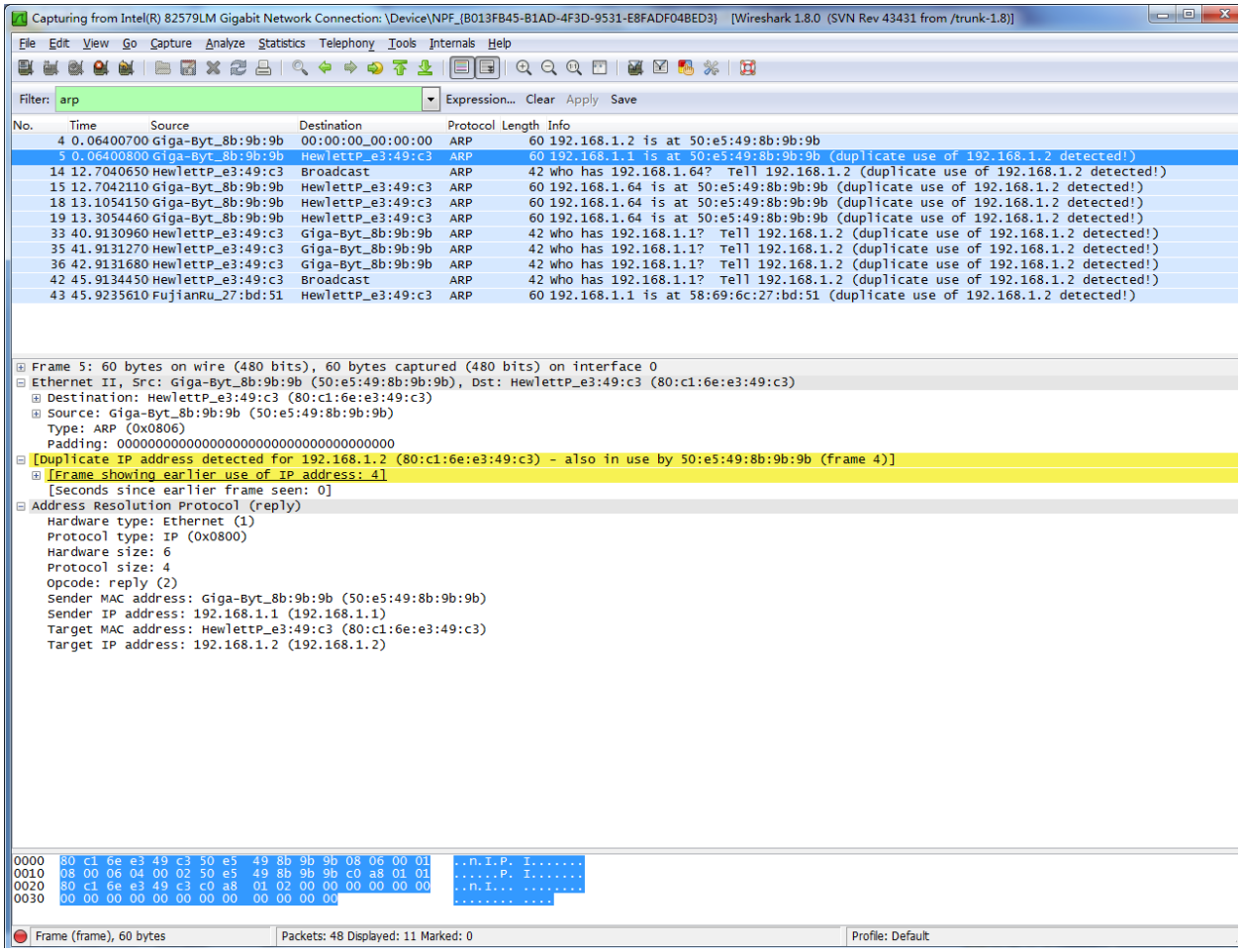
步骤5 进行ARP欺骗。

单击工具栏中的“Start”按钮，软件将进行ARP欺骗攻击。



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

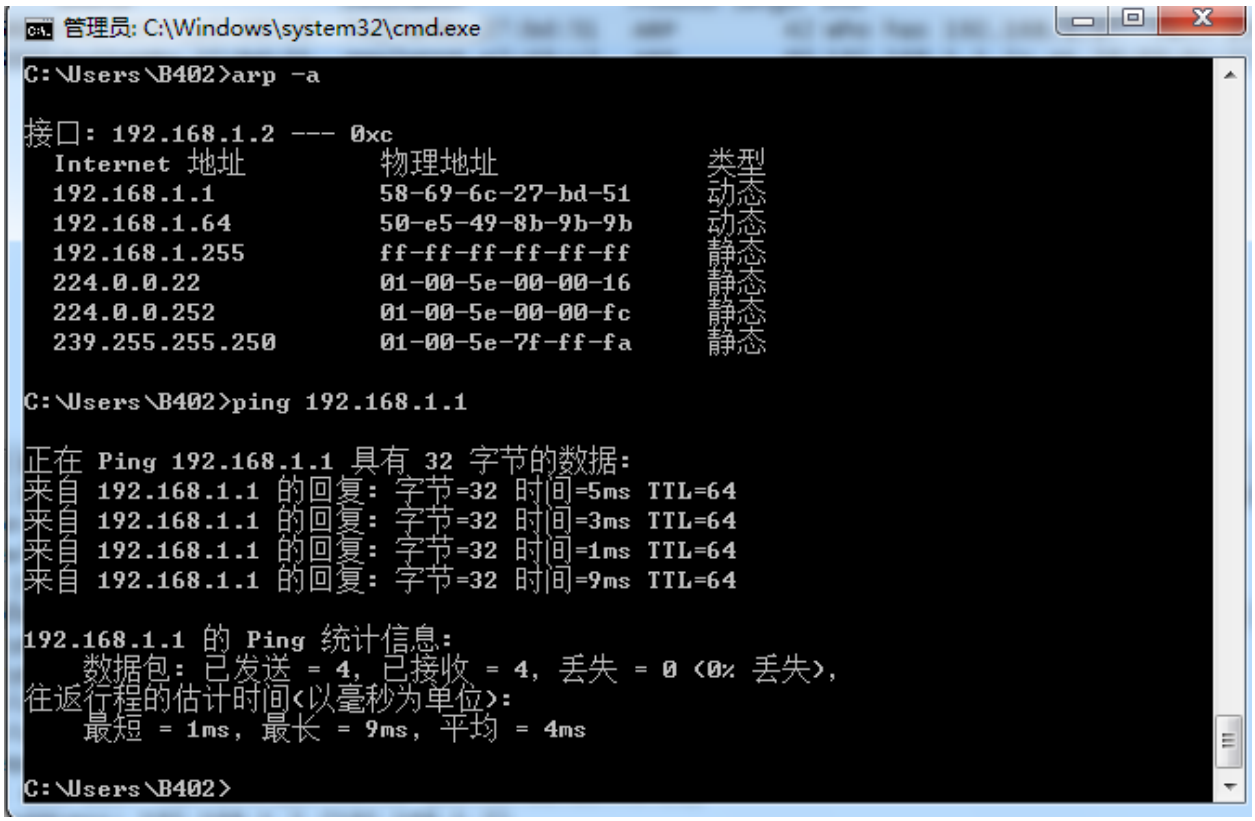
Switch(config-if)#switchport port-security

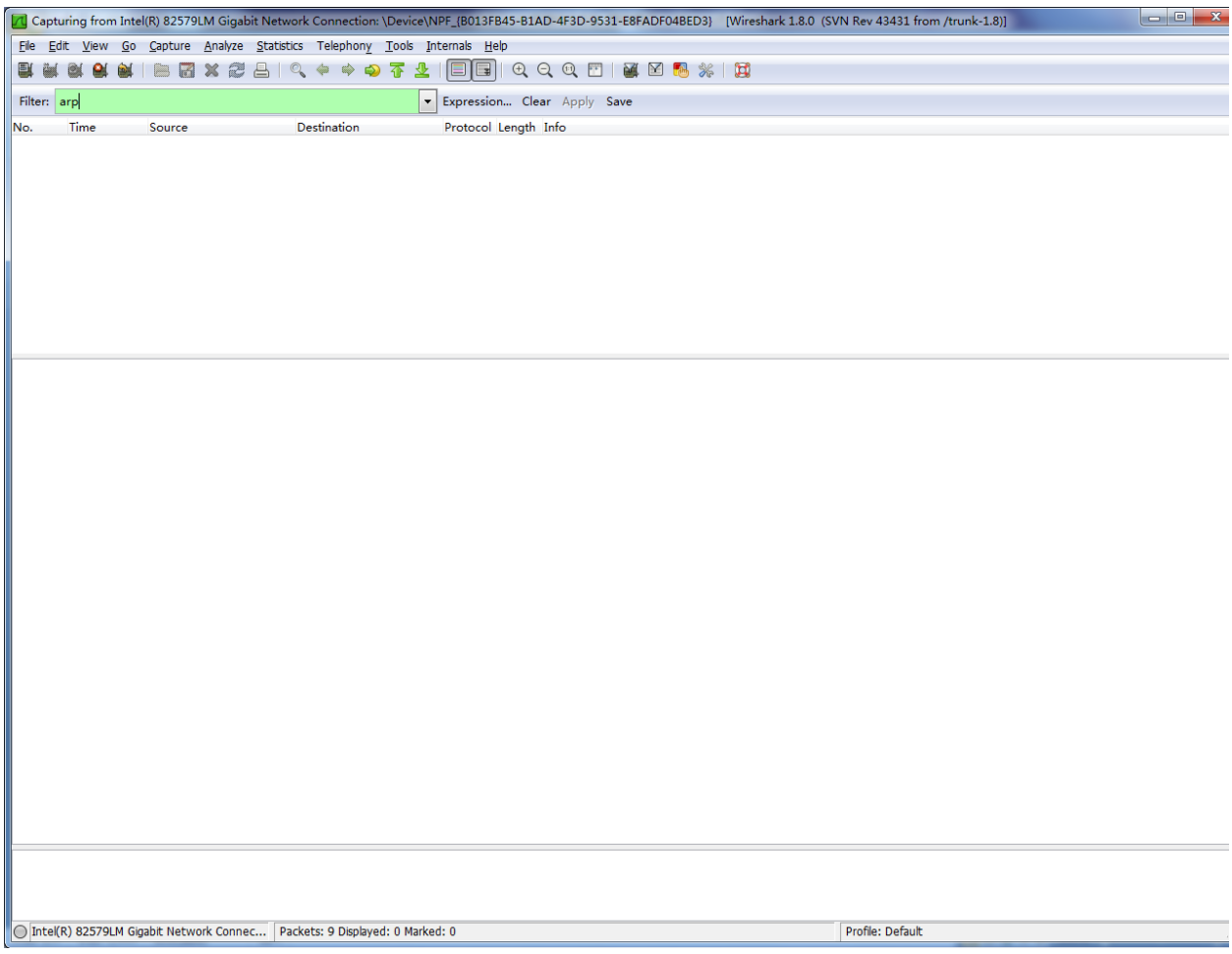
Switch(config-if)#switchport port-security mac-address [MAC] ip-address [IP] ！ 将攻击者的MAC地址与其真实的IP地址绑定（MAC、IP以实际值代入）。

```
8-S5750-1(config)#interface gigabitethernet 0/1
8-S5750-1(config-if-GigabitEthernet 0/1)#switchport port-security
8-S5750-1(config-if-GigabitEthernet 0/1)#$5498b9b9b ip-address 192.168.1.64
8-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。





【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。

1. ARP 双向绑定
2. 建立 DHCP 服务器

3. 划分安全区域

(2) 在 IPv6 协议下，是否有 ARP 欺骗攻击？

ARP 欺骗攻击在表现上，对于主机污染邻居映射关系，对于网络设备污染 FDB 表。

理论上来说，IPv6 中对应 ARP 功能的邻居发现协议中，利用 IPv6 的地址空间较长，将实际的签名信息也存在里面，用这种方式来使得源地址的拥有权是可以验证的。因而应该是不存在 ARP 欺骗攻击的。