

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	2015 级电子政务	学号	15331191	姓名	廖颖泓
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

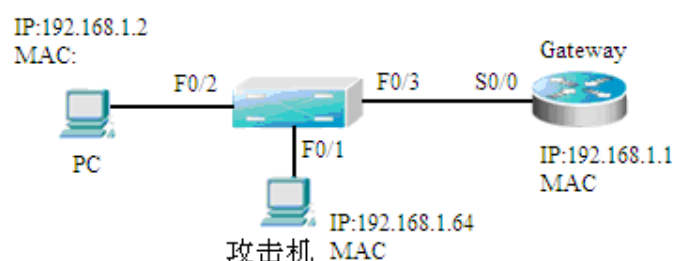
原理：伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉了”。

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WinArpSpoofers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。

按照拓扑图正确配置PC机、攻击机、路由器的IP地址之后，双方可以相互ping通：

```
C:\Users\B402>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
```

攻击机ping通PC机

```
C:\Users\B403>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 = 0ms, 平均 = 0ms
```

PC机ping通攻击机

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：

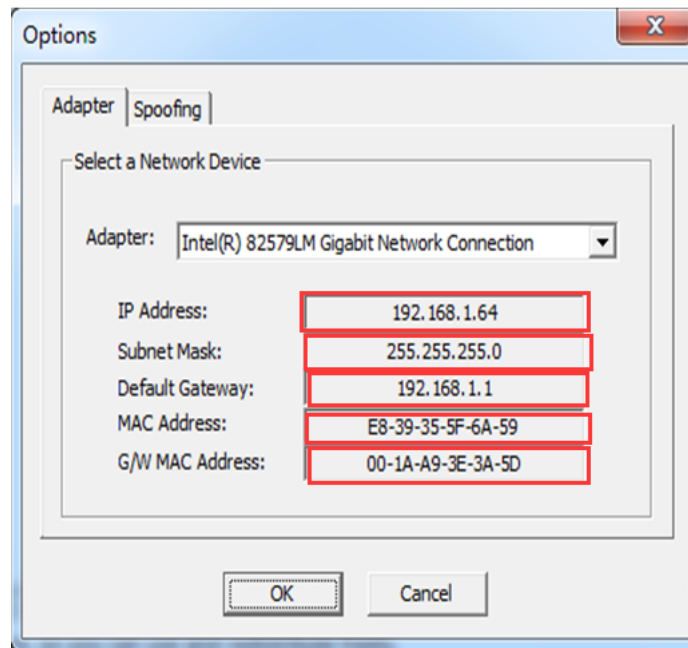
```
管理员: C:\Windows\system32\cmd.exe
C:\Users\B403>arp -a

接口: 192.168.1.2 --- 0xb
Internet 地址      物理地址          类型
192.168.1.1        00-1a-a9-3e-3a-5d 动态
192.168.1.64       00-00-00-00-e0-fe 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
239.255.255.250    01-00-5e-7f-ff-fa 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态

接口: 192.168.23.1 --- 0xf
Internet 地址      物理地址          类型
192.168.23.254     00-50-56-f2-0b-9e 动态
192.168.23.255     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
239.255.255.250    01-00-5e-7f-ff-fa 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态

接口: 192.168.94.1 --- 0x11
Internet 地址      物理地址          类型
192.168.94.254     00-50-56-ef-2e-5b 动态
192.168.94.255     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
239.255.255.250    01-00-5e-7f-ff-fa 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态
```

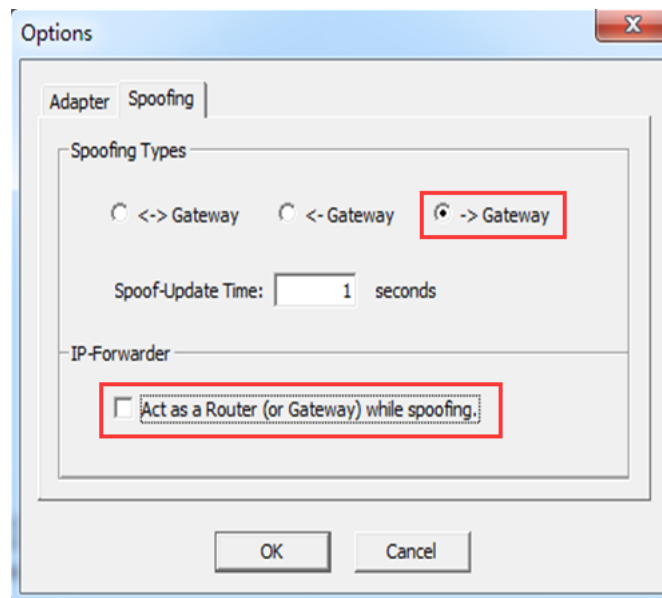
步骤2 在攻击机上运行WinArpSpoofers软件（在网络上下下载）后，在界面“Adapter”选项卡中，选择正确的网卡后，WinArpSpoofers会显示网卡的IP地址、掩码、网关、MAC地址以及网关的MAC地址信息。



步骤3 在WinArpSpoofers配置

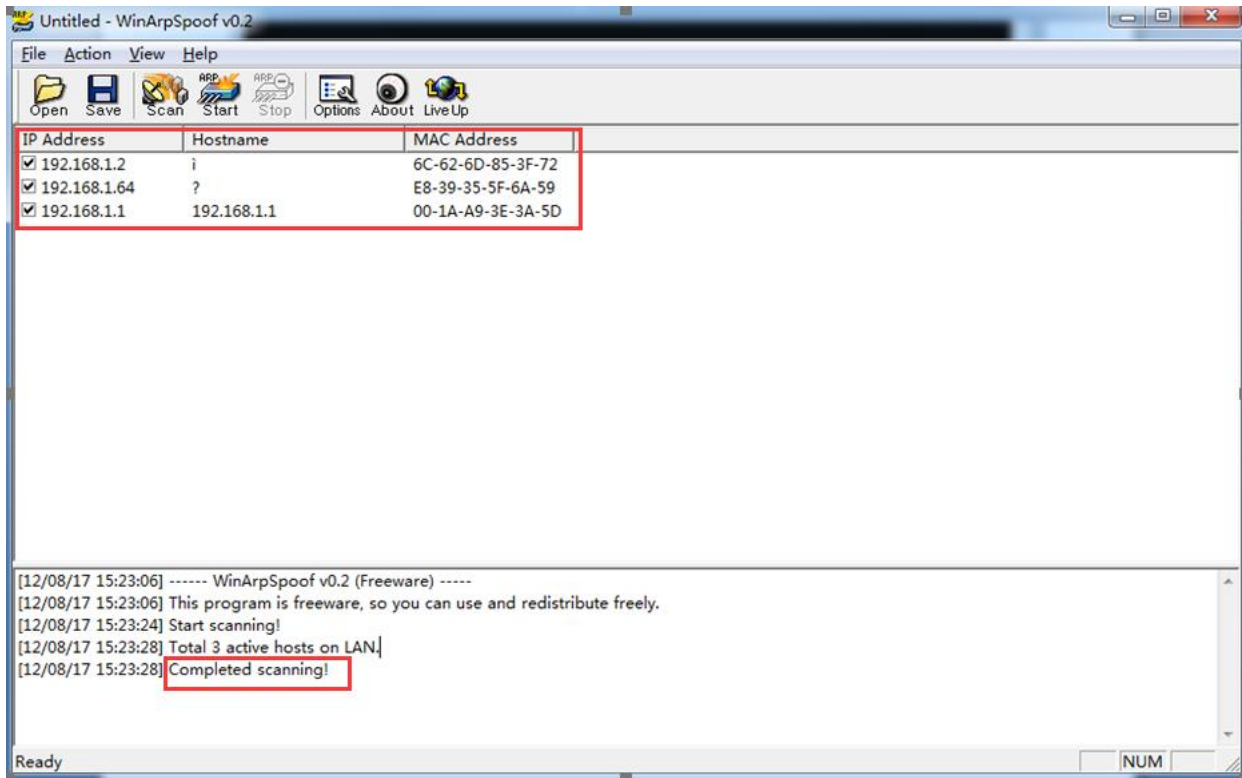
在WinArpSpoofers界面中选择“Spoofing”标签，打开“Spoofing”选项卡界面：

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。



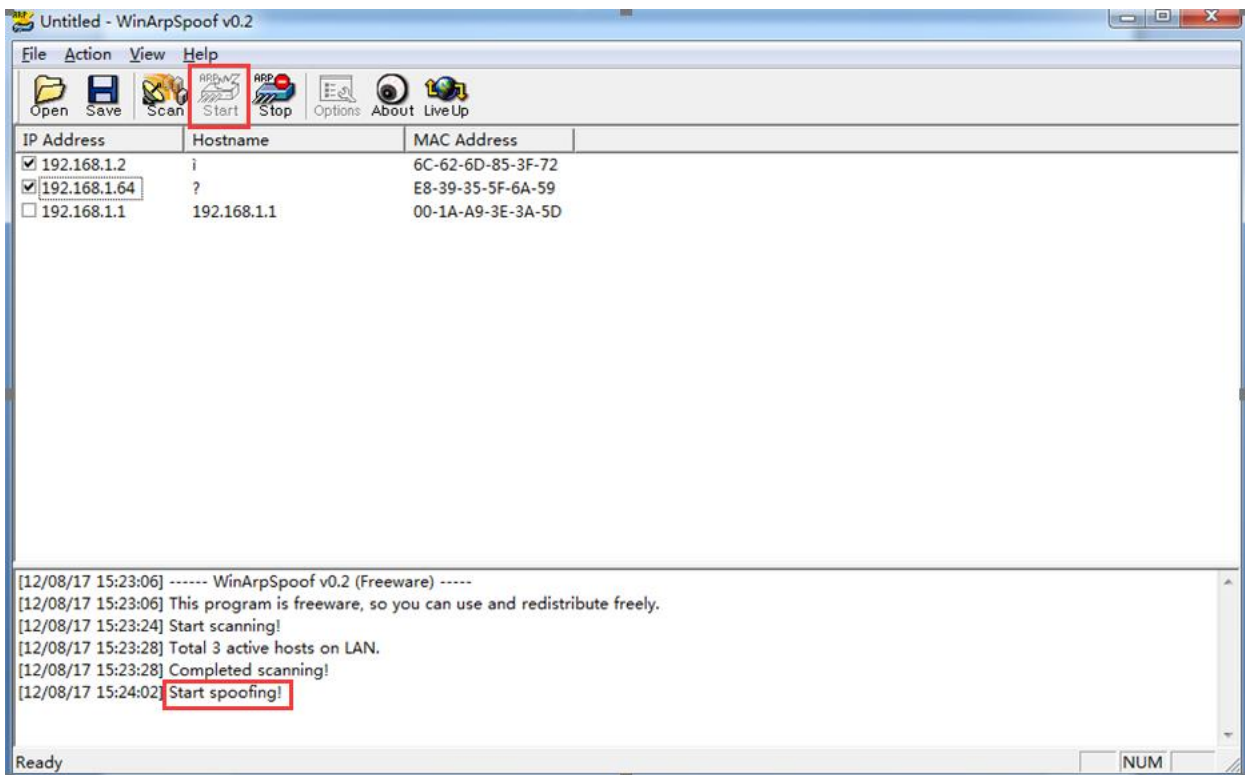
步骤4 使用WinArpSpoofers进行扫描。

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。



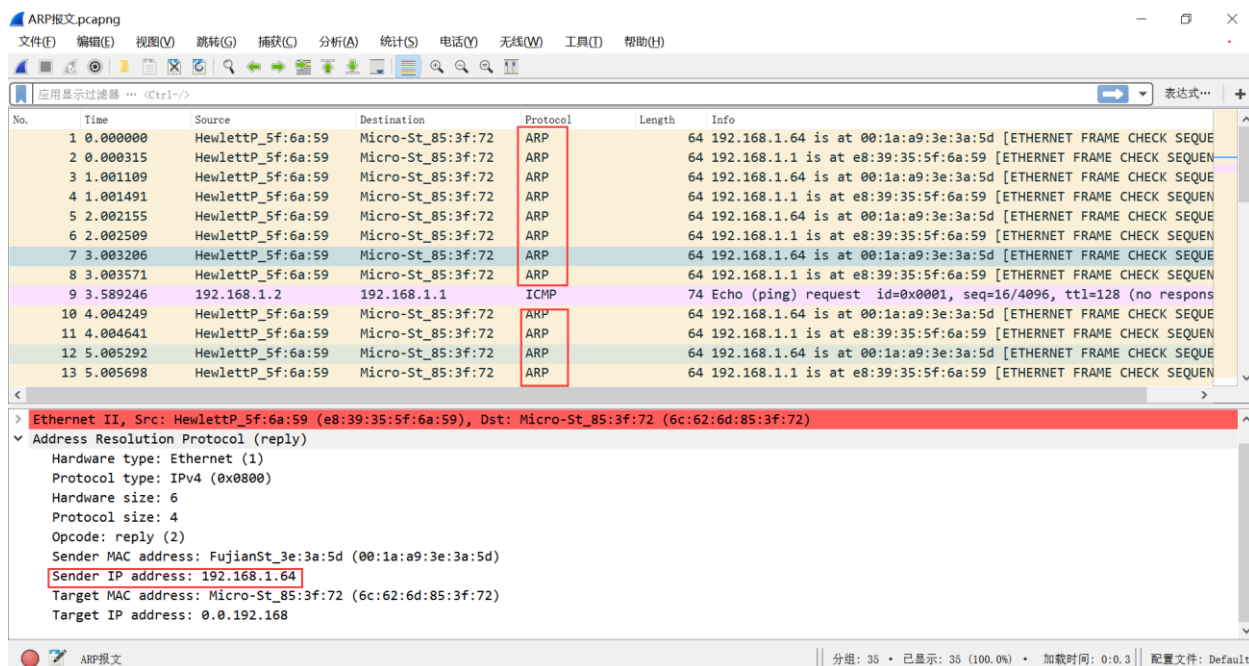
步骤5 进行ARP欺骗。

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。

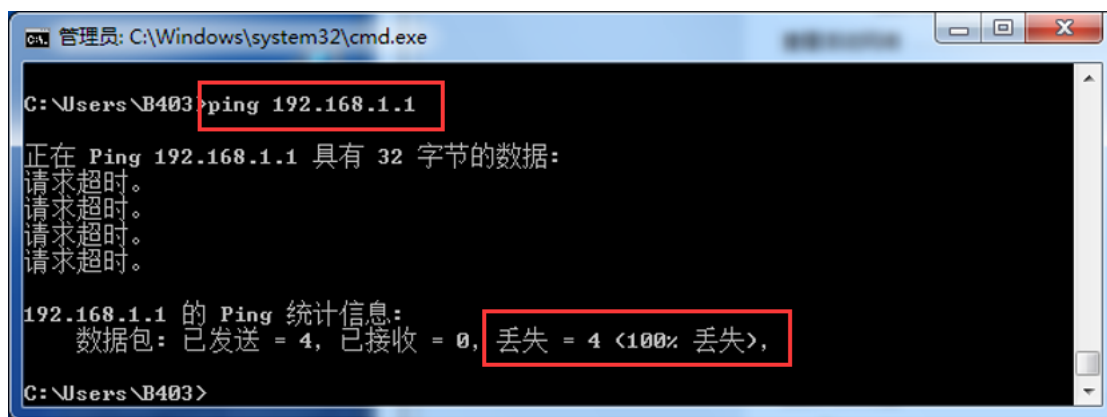
通过使用Wireshark捕获攻击机发出的报文，可以看出攻击机发送了经过伪造的ARP应答（Reply）报文。



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。

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：


```

管理员: C:\Windows\system32\cmd.exe
C:\Users\B403>arp -a

接口: 192.168.1.2 --- 0xb
Internet 地址      物理地址      类型
192.168.1.1      00-1a-a9-3e-3a-5d 动态
192.168.1.64      00-1a-a9-3e-3a-5d 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
239.255.255.250   01-00-5e-7f-ff-fa 静态
255.255.255.255   ff-ff-ff-ff-ff-ff 静态

接口: 172.16.23.3 --- 0xc
Internet 地址      物理地址      类型
172.16.0.1        00-09-4c-e9-fd-b5 动态
172.16.1.2        44-33-4c-0e-c2-29 动态
172.16.1.3        44-33-4c-0e-ce-4c 动态
172.16.3.3        44-33-4c-0e-c3-ca 动态
172.16.4.1        44-33-4c-0e-c8-2b 动态
172.16.8.1        44-33-4c-0e-b7-9c 动态
172.16.11.1       44-33-4c-0e-c8-29 动态
172.16.12.2       44-33-4c-0e-ad-25 动态
172.16.23.5       14-14-4b-30-f8-38 动态
172.16.27.2       44-33-4c-0e-c2-e1 动态
172.16.29.2       44-33-4c-0e-d0-10 动态
172.16.255.255    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
239.255.255.250   01-00-5e-7f-ff-fa 静态
  
```

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）。

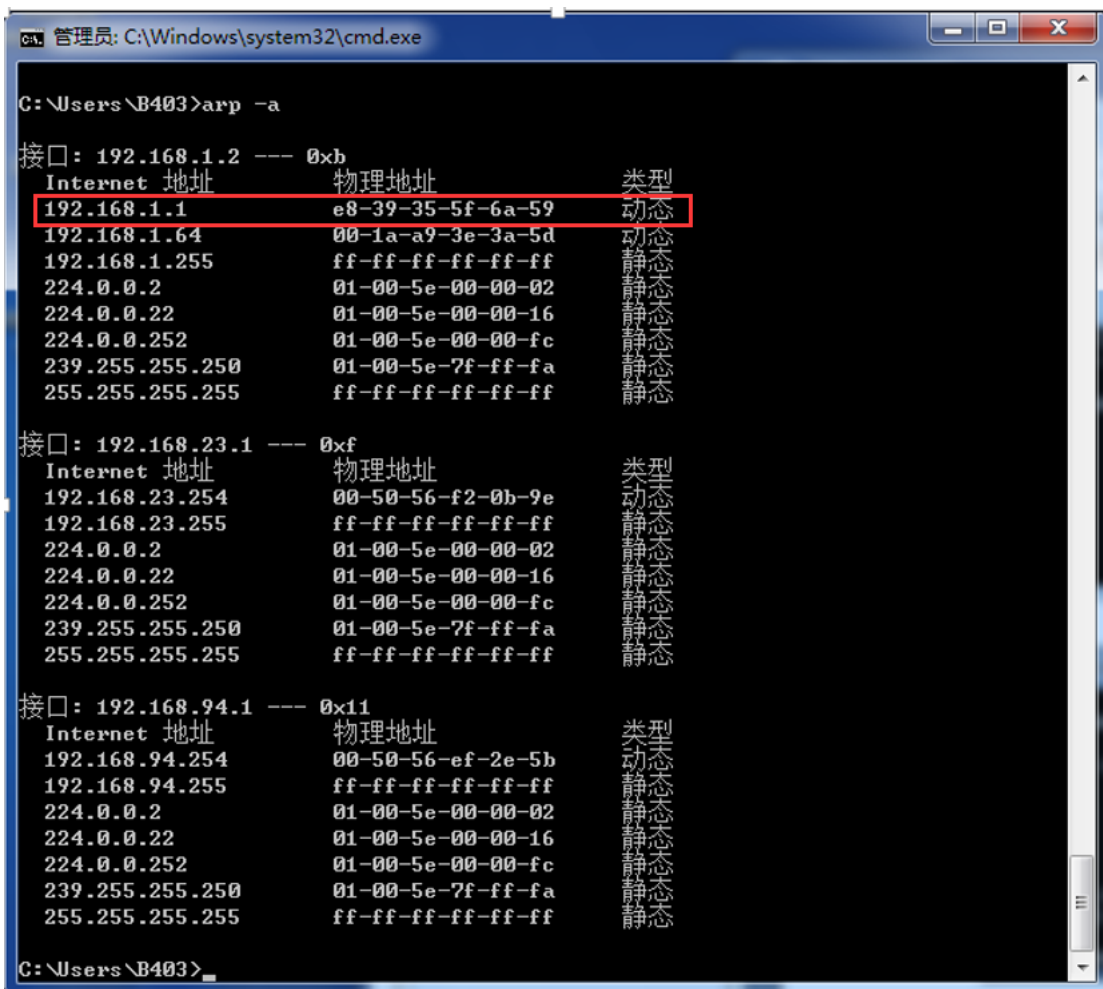
```

Telnet 172.16.23.5
23-S5750-1>
23-S5750-1>enable 14
Password:
23-S5750-1#configure
Enter configuration commands, one per line. End with CNTL/Z.
23-S5750-1(config)#interface g
23-S5750-1(config)#interface gigabitEthernet 0/1
23-S5750-1(config-if-GigabitEthernet 0/1)#switchport port-security
23-S5750-1(config-if-GigabitEthernet 0/1)#address 192.168.1.64
23-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。



```
管理员: C:\Windows\system32\cmd.exe

C:\Users\B403>arp -a

接口: 192.168.1.2 --- 0xb
Internet 地址      物理地址      类型
192.168.1.1      e8-39-35-5f-6a-59 动态
192.168.1.64     00-1a-a9-3e-3a-5d 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
239.255.255.250  01-00-5e-7f-ff-fa 静态
255.255.255.255  ff-ff-ff-ff-ff-ff 静态

接口: 192.168.23.1 --- 0xf
Internet 地址      物理地址      类型
192.168.23.254   00-50-56-f2-0b-9e 动态
192.168.23.255   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
239.255.255.250  01-00-5e-7f-ff-fa 静态
255.255.255.255  ff-ff-ff-ff-ff-ff 静态

接口: 192.168.94.1 --- 0x11
Internet 地址      物理地址      类型
192.168.94.254   00-50-56-ef-2e-5b 动态
192.168.94.255   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
239.255.255.250  01-00-5e-7f-ff-fa 静态
255.255.255.255  ff-ff-ff-ff-ff-ff 静态

C:\Users\B403>
```

【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. 使用 proxy 代理 IP 的传输。
2. 管理员定期用响应的 IP 包中获得一个 rarp 请求，然后检查 ARP 响应的真实性。
3. 管理员定期轮询，检查主机上的 ARP 缓存。除非必要，否则停止使用 ARP，将 ARP 做为永久条目保存在对应表中。
4. 使用 ARP 服务器。通过该服务器查找自己的 ARP 转换表来响应其他机器的 ARP 广播。确保这台 ARP 服务器的安全。
5. 使用硬件屏蔽主机。设置好路由，确保 IP 地址能到达合法的路径。（静态配置路由 ARP 条目），注意，使用交换集线器和网桥无法阻止 ARP 欺骗。
6. 不要把网络安全信任关系建立在 IP 基础上或 MAC 基础上，（rarp 同样存在欺骗的问题），理想的关系应该建立在 IP+MAC 基础上。
7. 使用防火墙连续监控网络。注意有使用 SNMP 的情况下，ARP 的欺骗有可能导致陷阱包丢失。

(2) 在 IPv6 协议下，是否有 ARP 欺骗攻击？

IPv6 用邻居发现协议 NDP 代替 ARP，它组合了 IPv4 中的 ARP、ICMP 路由器发现和 ICMP 重定向等协议，并对它们作了改进。作为 IPv6 的基础性协议，NDP 还提供了前缀发现、邻居不可达检测、重复地址监测、地址自动配置等功能，可以阻止 ARP 欺骗攻击。