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	软件工程	班级	4	学号	17343105	姓名	田皓
完成日期： 2019 年 12 月 30 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

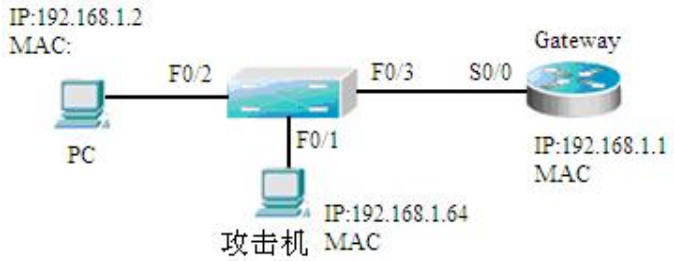
原理：伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

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】

本次实验以小组形式完成：

组员：

17343105 田皓

17343103 孙浥尘

17343106 王嘉浚

17343108 王然

我负责的工作：连线，配置路由器，使用wireshark抓包，以及共同分析实验结果。

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。

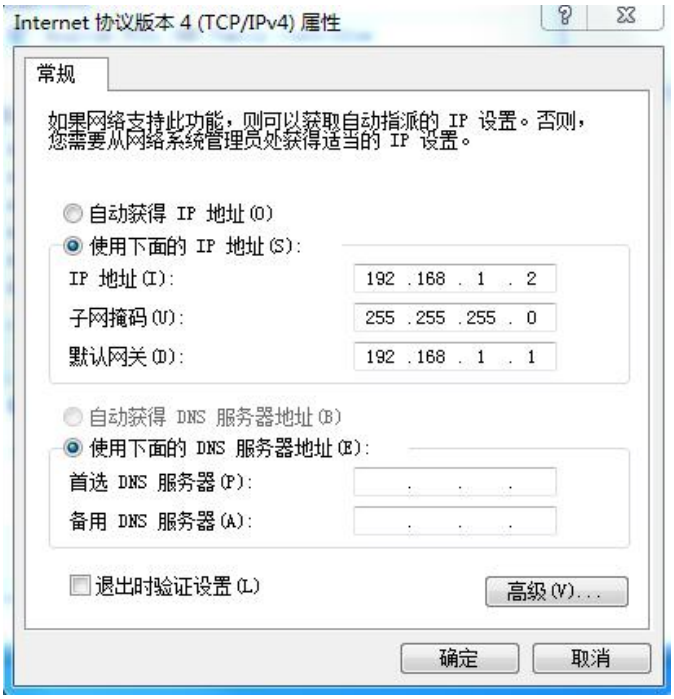
首先按照拓扑图连接网络。

路由器配置：

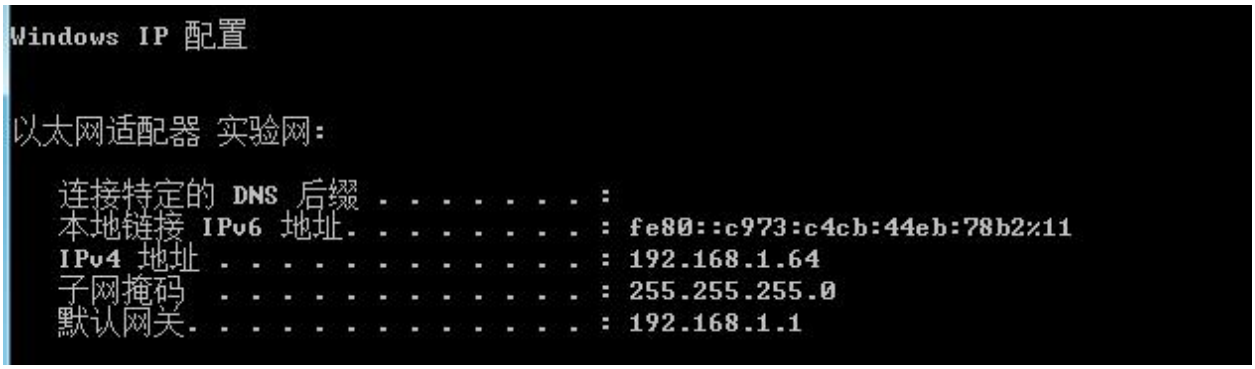
```
10-RSR20-1(config-if-GigabitEthernet 0/0)#$2.168.1.1 255.255.255.0
10-RSR20-1(config-if-GigabitEthernet 0/0)#no shutdown
10-RSR20-1(config-if-GigabitEthernet 0/0)#exit
```

```
10-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
10-RSR20-1(config)#
```

PC机配置：


Internet 协议版本 4 (TCP/IPv4) 属性
常规
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I): 192 .168 . 1 . 2
子网掩码(U): 255 .255 .255 . 0
默认网关(D): 192 .168 . 1 . 1
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P):
备用 DNS 服务器(A):
退出时验证设置(L)
高级(V)...
确定
取消

攻击机配置：


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::c973:c4cb:44eb:78b2%11
IPv4 地址 . . . . . : 192.168.1.64
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.1.1

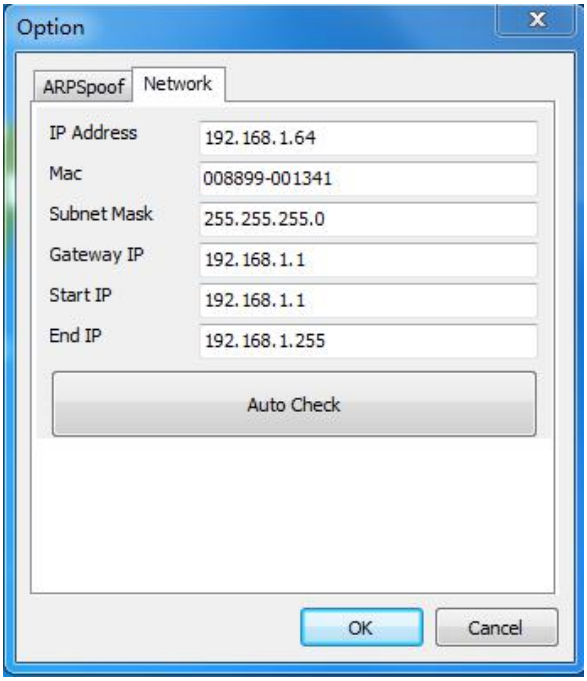
互相Ping验证连通性：

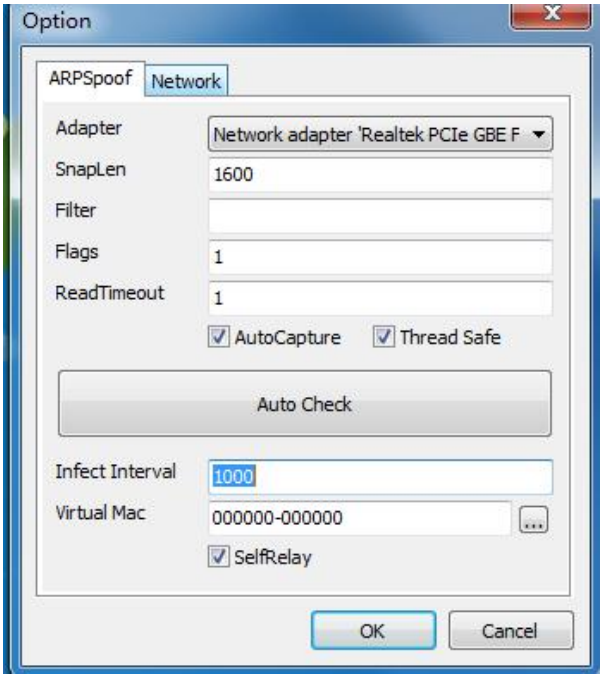
```
C:\Users\Administrator>ping 192.168.1.2

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=2ms 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 = 2ms, 平均 = 0ms

C:\Users\Administrator>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=5ms TTL=64
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=10ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间=3ms 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 = 3ms, 最长 = 10ms, 平均 = 5ms

C:\Users\Administrator>
```

```
C:\Users\Administrator>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=2ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间=8ms 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 = 0ms, 最长 = 8ms, 平均 = 2ms

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=2ms 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 = 2ms, 平均 = 0ms
```

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。

我们使用ARPSpoof软件





由于实验室电脑的实验网和校园网网卡名称相同，而软件中看不到后面的#2，所以尝试之后才选择到了正确的网卡，即实验网网卡。

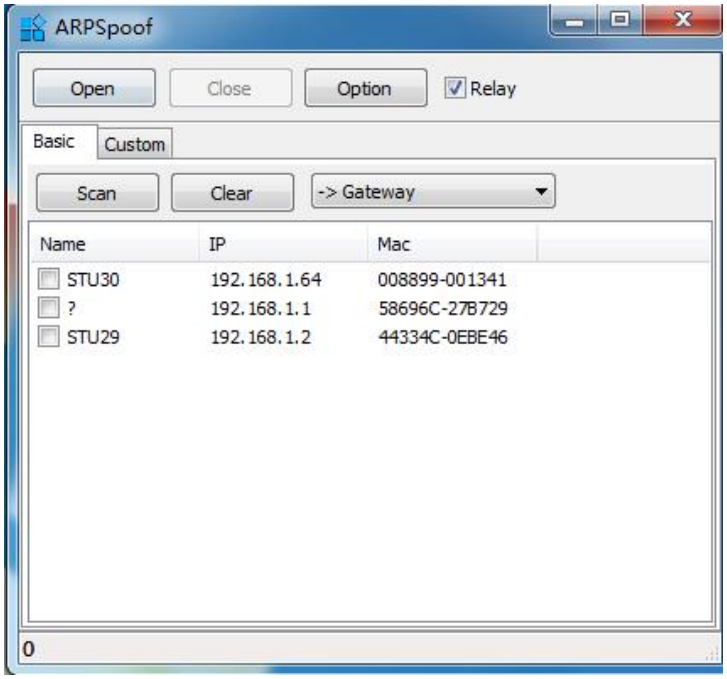
步骤3 在WinArpSpoofer配置

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。

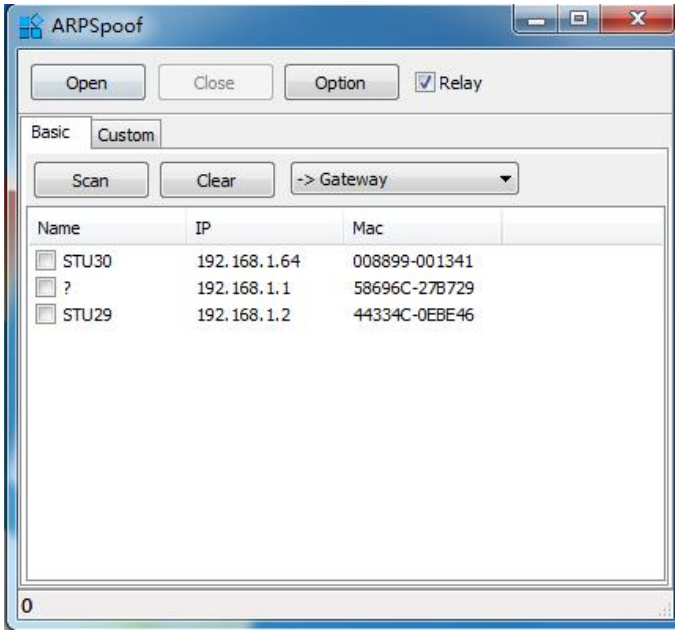
单击工具栏中的“Scan”按钮，软件将扫描网络中的主机，并获取其IP地址、MAC地址等信息。



可以看到扫描到了网络中的三个设备。

步骤5 进行ARP欺骗。

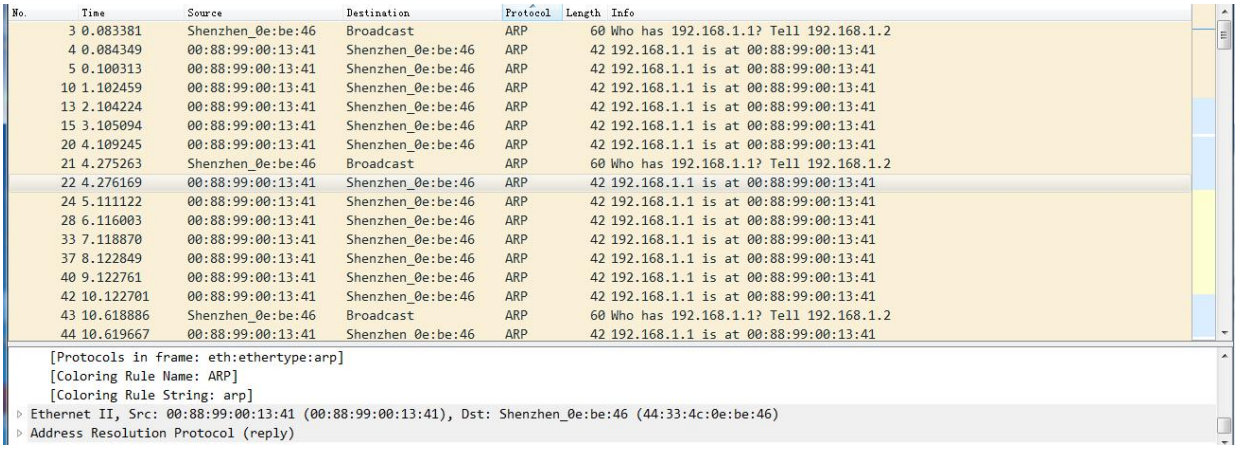
单击工具栏中的“Start”按钮，软件将进行ARP欺骗攻击。



选择STU29，即PC机后点击OPEN开始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。



攻击机一直在广播ARP欺骗报文。

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。

一开始我们发现还是可以ping通，但是抓包发现回包是攻击机回的。

查看PC机ARP缓存，发现已经被欺骗：

```
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>arp -a

接口: 192.168.1.2 --- 0xb
  Internet 地址         物理地址              类型
  169.254.120.178       00-88-99-00-13-41     动态
  192.168.1.1           00-88-99-00-13-41     动态
  192.168.1.64          00-88-99-00-13-41     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
```

等待一段时间再次Ping，出现这样的结果：

```
C:\Users\Administrator>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.2 的回复: 无法访问目标主机。
请求超时。
请求超时。
来自 192.168.1.1 的回复: 字节=32 时间=7ms TTL=64

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 2, 丢失 = 2 (50% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 7ms, 最长 = 7ms, 平均 = 7ms

C:\Users\Administrator>
```

```
    28 4.886868    192.168.1.2      192.168.1.1      ICMP     74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=128 (no response found!)
    46 8.728815    192.168.1.1      192.168.1.2      ICMP     70 Destination unreachable (Network unreachable)
    53 9.819704    192.168.1.2      192.168.1.1      ICMP     74 Echo (ping) request  id=0x0001, seq=18/4608, ttl=128 (no response found!)
    74 14.819508   192.168.1.2      192.168.1.1      ICMP     74 Echo (ping) request  id=0x0001, seq=19/4864, ttl=128 (no response found!)
   100 19.828341   192.168.1.2      192.168.1.1      ICMP     74 Echo (ping) request  id=0x0001, seq=20/5120, ttl=128 (reply in 101)
   101 19.838412   192.168.1.1      192.168.1.2      ICMP     74 Echo (ping) reply    id=0x0001, seq=20/5120, ttl=64 (request in 100)
    81 16.168642   RuijieNe_15:58:ce LLDP_Multicast   LLDP    244 TTL = 121 System Name = 10-S5750-2 System Description = Ruijie Layer 3 FULL
    23 3.943691    fe80::795f:4b75:b3b… ff02::1:3      LLMNR    86 Standard query 0x7c37 A isatap
    24 3.943730    192.168.1.2      224.0.0.252      LLMNR    66 Standard query 0x7c37 A isatap

▷ Frame 74: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▷ Ethernet II, Src: Shenzhen_0e:c2:d0 (44:33:4c:0e:c2:d0), Dst: 00:88:99:00:13:41 (00:88:99:00:13:41)
```

经过多次测试我们发现，ping的时候ICMP包既有发送到路由器（真网关）的，也有发送到攻击机（假网关），我们认为这是由于ARPSpoofer软件的攻击频率不够高，交换机还是保存有正确的的MAC与IP的对应。ARP表的更新策略是后到优先原则，但是其实由于攻击机一直持续不断的发送欺骗包，所以最后PC机的ARP缓存表放的肯定是错误的映射关系。

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 gigabitethernet 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）。

```
10-S5750-2(config)#interface gigabitethernet 0/1
10-S5750-2(config-if-GigabitEthernet 0/1)#switchport port-security
10-S5750-2(config-if-GigabitEthernet 0/1)#$1 ip-address 192.168.1.64
switchport port-security mac-address 008899-001341 ip-address 192.168.1.64
                                                    ^
% Invalid input detected at '^' marker.

10-S5750-2(config-if-GigabitEthernet 0/1)#$ ip-address 192.168.1.64
10-S5750-2(config-if-GigabitEthernet 0/1)#exit
10-S5750-2(config)#
```

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。

```
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-b7-29     动态
  192.168.1.64          00-88-99-00-13-41     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
```

执行 arp -d 清空后，再次查看 PC 机的 ARP 缓存，已经正确。

```
C:\Users\Administrator>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=5ms TTL=64
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=10ms TTL=64
来自 192.168.1.1 的回复: 字节=32 时间=3ms 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 = 3ms, 最长 = 10ms, 平均 = 5ms

C:\Users\Administrator>
```

可以 ping 通路由器。

【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。

安装 ARP 欺骗防护软件
支持 ARP 过滤的防火墙
使用静态 ARP 缓存表
路由器，交换机等网络设备采用 IP+MAC 绑定，即开启 ARP 检查功能

(2) 在 IPv6 协议下，是否有 ARP 欺骗攻击？

IPv6 采用 NDP 协议替代 IPv4 中的 ARP 协议，二者实现原理基本一致，所以 ARP 欺骗攻击在 IPv6 协议中仍然存在。