

## 项目 5：项目实施

### 1.1.1 ARP 攻击预防任务实施

#### 1. 实施规划

##### 1) 实训拓扑结构

根据任务的需求与分析，实训的拓扑结构及网络参数如图 4-38 所示，以 PC1 模拟公司员工电脑，PC2 模拟 ARP 攻击机，DHCP 模拟公司 DHCP 服务器。

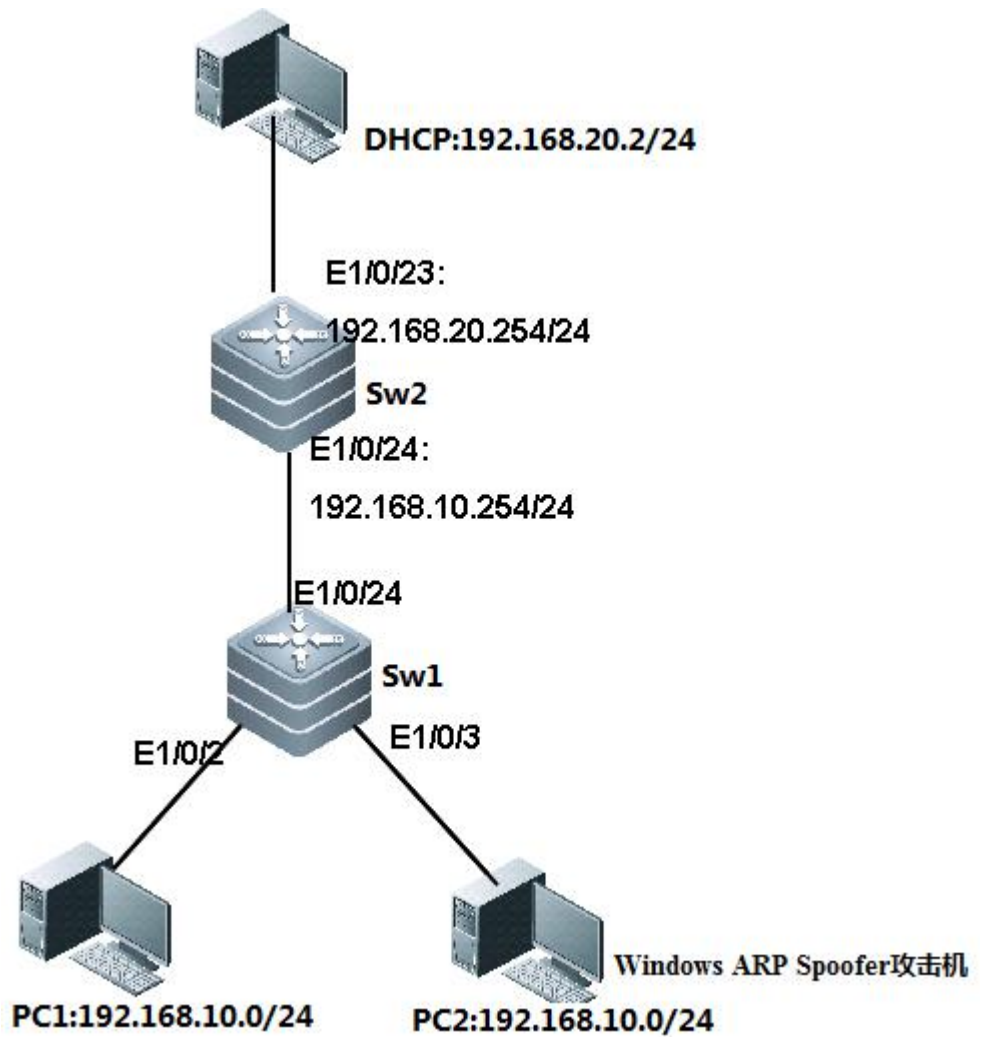


图 4-38 实训任务拓扑

##### 2) 实训设备

根据任务的需求和实训拓扑，每实训小组的实训设备配置建议，如表 4-4 所示。

表4-4 实训设备配置清单

设备类型	设备型号	数量
交换机	H3CS3610-28TP	2
计算机	windows2003/windows7	2
计算机	Win2008	1

Arp 攻击模拟软件	Windows ARP Spoofer	1
双绞线	RJ-45	若干

### 3) IP 地址规划

根据需求分析，本任务的 IP 地址规划，如表 4-5 所示。

表4-5 IP地址规划

设备	IP 地址	网关
PC1	DHCP 自动获取	192.168.10.254
PC2	DHCP 自动获取	192.168.10.254
DHCP	192.168.20.2/24	192.168.20.254

### 3) VLAN 规划

根据需求分析，本任务的 VLAN 规划，如表 4-6 所示。

表4-6 VLAN规划

所属 switch	VLAN	包含端口
Sw1	VLAN 10	Ethernet 1/0/1 to Ethernet 1/0/5
Sw1/sw2	VLAN 20	Ethernet 1/0/20 to Ethernet 1/0/23

## 2. 实施步骤

1) 根据实训拓扑图进行交换机、计算机的线缆连接，配置 PC3（DHCP 服务器）的 IP 地址。

2) 使用计算机 Windows 操作系统的“超级终端”组件程序通过串口连接到交换机的配置界面，其中超级终端串口的属性设置还原为默认值（每秒位数 9600、数据位 8、奇偶校验无、数据流控制无）。

3) 超级终端登录到路由器，进行任务的相关配置。

4) Switch 1 主要配置清单如下：

```

一、sw1 的基本配置
1、初始化配置
<H3C>system-view
[H3C]sysname sw1
二、配置 vlan
[sw1]vlan 10
[sw1-vlan10]port Ethernet 1/0/1 to Ethernet 1/0/5
三、上联端口的配置
[sw1-vlan10]quit
[sw1]interface Ethernet 1/0/24
[sw1-Ethernet1/0/24]port link-type trunk
[sw1-Ethernet1/0/24]port trunk permit vlan all

```

5) Switch 2 主要配置清单如下：

```

一、sw2 的基本配置
1、初始化配置
<H3C>system-view
[H3C]sysname sw2
二、vlan 配置
[sw2]vlan 10
[sw2-vlan10]vlan 20

```

```
[sw2-vlan20]port Ethernet 1/0/20 to Ethernet 1/0/23
```

三、vlan 路由配置

```
[sw2-vlan20]quit
```

```
[sw2]interface Vlan-interface 10
```

```
[sw2-Vlan-interface10]ip address 192.168.10.254 24
```

```
[sw2-Vlan-interface10]quit
```

```
[sw2]interface Vlan-interface 20
```

```
[sw2-Vlan-interface20]ip address 192.168.20.254 24
```

四、下联端口配置

```
[sw2-Vlan-interface20]quit
```

```
[sw2]interface Ethernet 1/0/24
```

```
[sw2-Ethernet1/0/24]port link-type trunk
```

```
[sw2-Ethernet1/0/24]port trunk permit vlan all
```

#### 6) DHCP 中继代理配置。

一、DHCP 中继代理配置

```
[sw2-Ethernet1/0/24]quit
```

```
[sw2]dhcp enable
```

```
[sw2]dhcp relay server-group 1 ip 192.168.20.2 /*创建 DHCP 服务器组，并指明  
DHCP 服务器的 IP 地址
```

```
[sw2]interface Vlan-interface 10
```

```
[sw2-Vlan-interface10]dhcp select relay /*让 VLAN 10 工作在中继模式下
```

```
[sw2-Vlan-interface10]dhcp relay server-select 1
```

注：此时需要测试 PC1、PC2 是否能够正常获取 IP 地址

#### 7) DHCP Snooping

一、DHCP Snooping 配置

1、sw1 的配置

```
[sw1]dhcp-snooping
```

```
[sw1]interface Ethernet 1/0/24
```

```
[sw1-Ethernet1/0/24]dhcp-snooping trust
```

2、sw2 的配置

```
[sw2]interface Ethernet 1/0/23
```

```
[sw2-Ethernet1/0/23]dhcp-snooping trust
```

#### 8) 配置 DHCP 服务器。

DHCP 服务器配置步骤省略，请参考“第 3 章任务 4 企业网络 IP 地址安全管理”部分的 DHCP 服务器配置。

#### 9) 测试 DHCP 服务是否正常。

此时可以测试公司内部 PC1、PC2 是否可以从 DHCP 服务器获取 IP 地址。分别将 PC1、PC2 设置为自动获取 IP 地址，并在 PC1、PC2 上分别运行 `ipconfig /all` 命令，查看获取的 IP 地址参数，如图 4-39、4-40 所示。

```
命令提示符
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : win2003-01
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix . . :
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 00-0C-29-E4-B6-B3
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.10.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.254
    DHCP Server . . . . . : 192.168.20.2
    Lease Obtained. . . . . : 2016年6月6日 14:43:34
    Lease Expires . . . . . : 2016年6月14日 14:43:34
```

图 4-39 PC1 获取到的 IP 参数

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : t251301
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

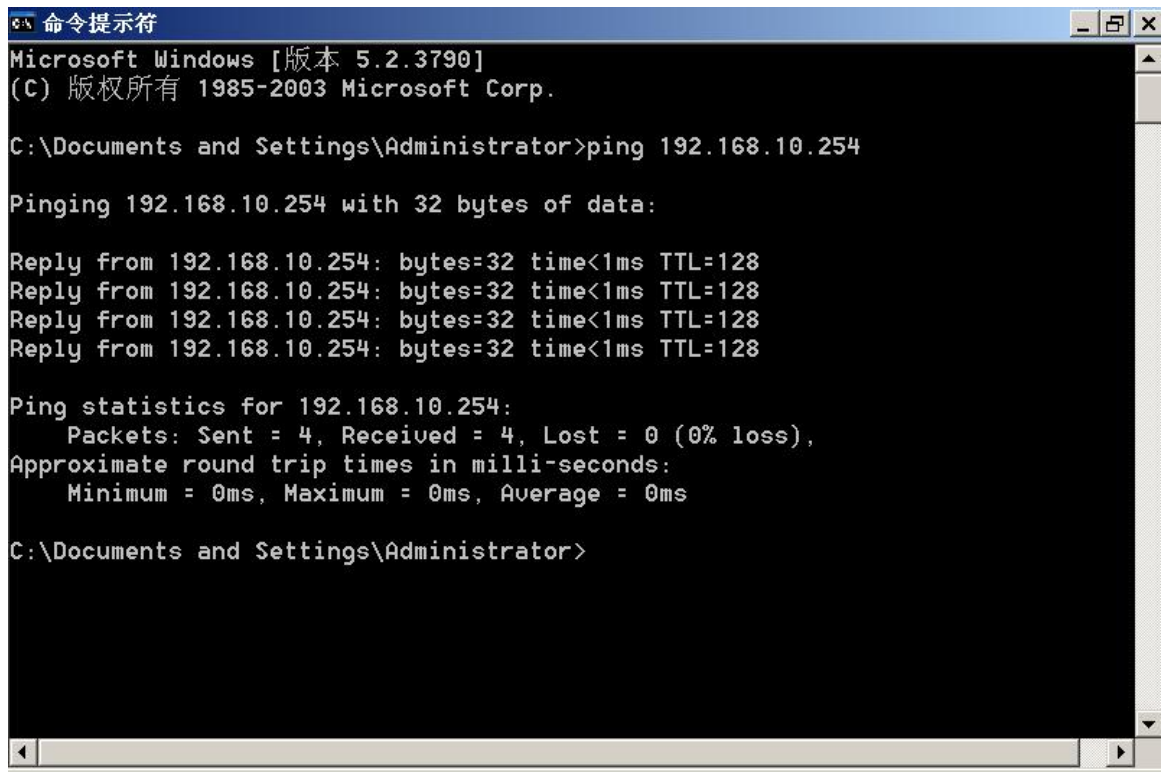
Ethernet adapter 本地连接:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : E0-69-95-29-ED-5D
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.10.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.254
    DHCP Server . . . . . : 192.168.20.2
    Lease Obtained. . . . . : 2016年6月6日 14:40:44
    Lease Expires . . . . . : 2016年6月14日 14:40:44
```

图 4-40 PC2 获取的 IP 参数

10) 测试内部主机是否能访问网关。

在正常情况下,在没有 ARP 攻击时,此时 PC1、PC2 均能正常访问网关: 192.168.10.254。在 PC1 上测试是否能访问网关,访问情况如图 4-41 所示,由此可以看出此时网络是正常的,PC1 可以正常访问网关。



```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.10.254

Pinging 192.168.10.254 with 32 bytes of data:

Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

图 4-41 PC1 能正常访问网关

11) PC2 上模拟发起 ARP 网关欺骗攻击。

本次任务利用“Windows ARP Spoofer”软件发起对 PC1 的网关欺骗攻击，迫使 PC1 断网（无法访问网关）。具体实施步骤如下。

(1) 安装“Windows ARP Spoofer”。

运行安装程序“setup.exe”，弹出“安装向导”对话框，如图 4-42 所示。

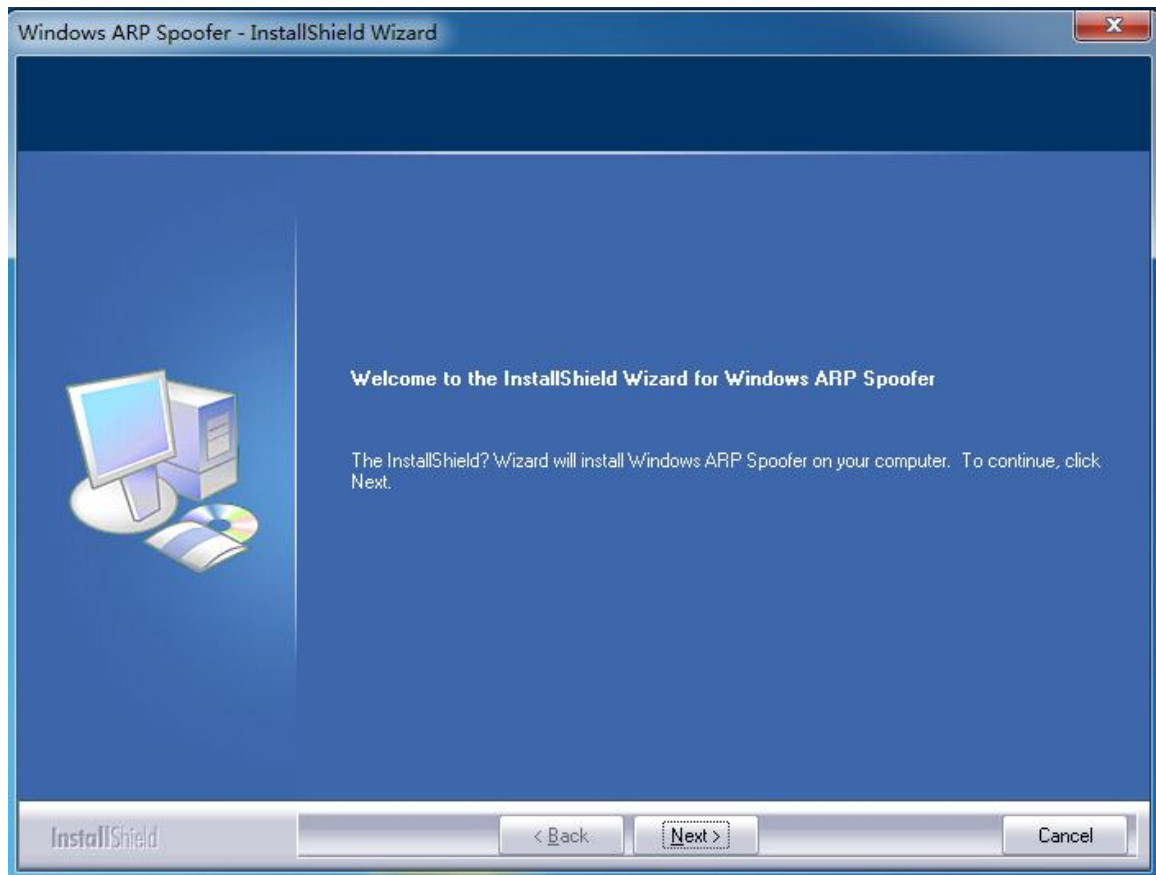


图 4-42 Windows ARP Spoofer 安装向导

全部单击 Next 按钮，采用默认方式安装，安装完成后单击 Finish 按钮，并重启系统，即完成了 Windows ARP Spoofer 的安装。

(2) 启动并配置 Windows ARP Spoofer 程序。

安装完成后，会在桌面上生成一个 Windows ARP Spoofer 的快捷图标，双击，即可打开 Windows ARP Spoofer 程序。第一次打开 Windows ARP Spoofer 程序，会显示该主机的网络配置参数，如图 4-43 所示。

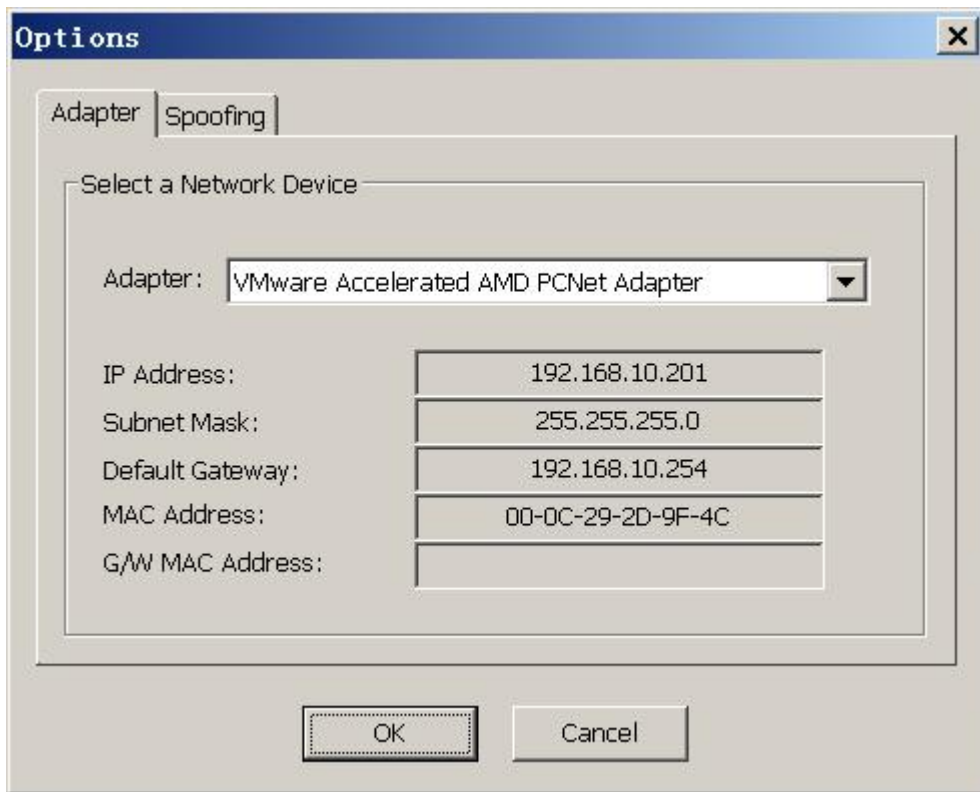


图 4-43 Windows ARP Spoofer 显示主机网络配置参数

从对话框中我们可以看到攻击机 PC2 的 IP 地址、子网掩码、网关、MAC 地址等相关参数，检查参数是否准确无误。

在 WinArpSpoofer 界面中选择 Spoofing 选项卡，如图 4-44 所示。

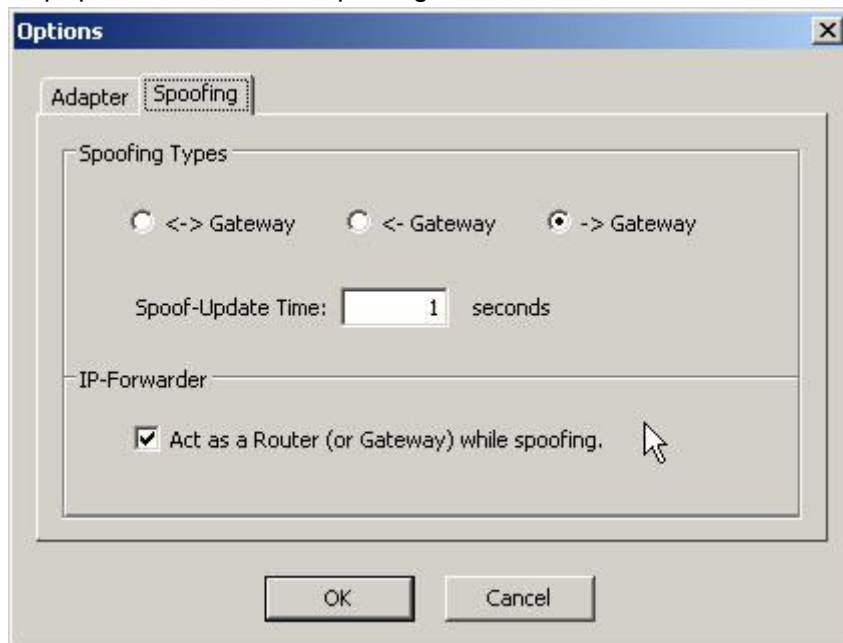


图 4-44 “Spoofing” 页签

在 Spoofing 界面中，取消选中 Act as a Router (or Gateway) while spoofing 复选框，如图 4-45 所示。配置完毕后，单击 OK 按钮。

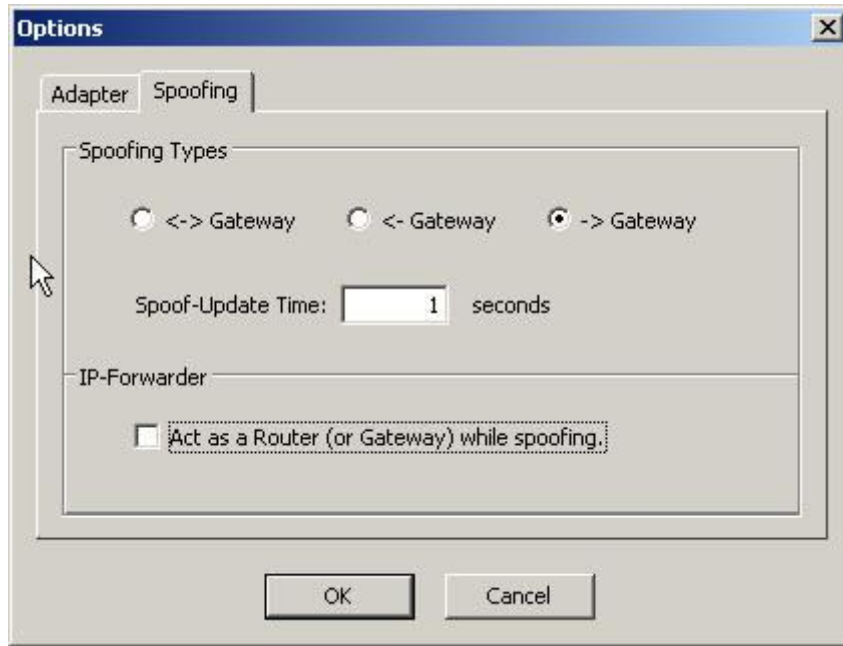


图 4-45 IP-Forwarder 选项

单击 OK 按钮，即可完成 Windows ARP Spoofer 的启动，启动界面如图 4-46 所示。

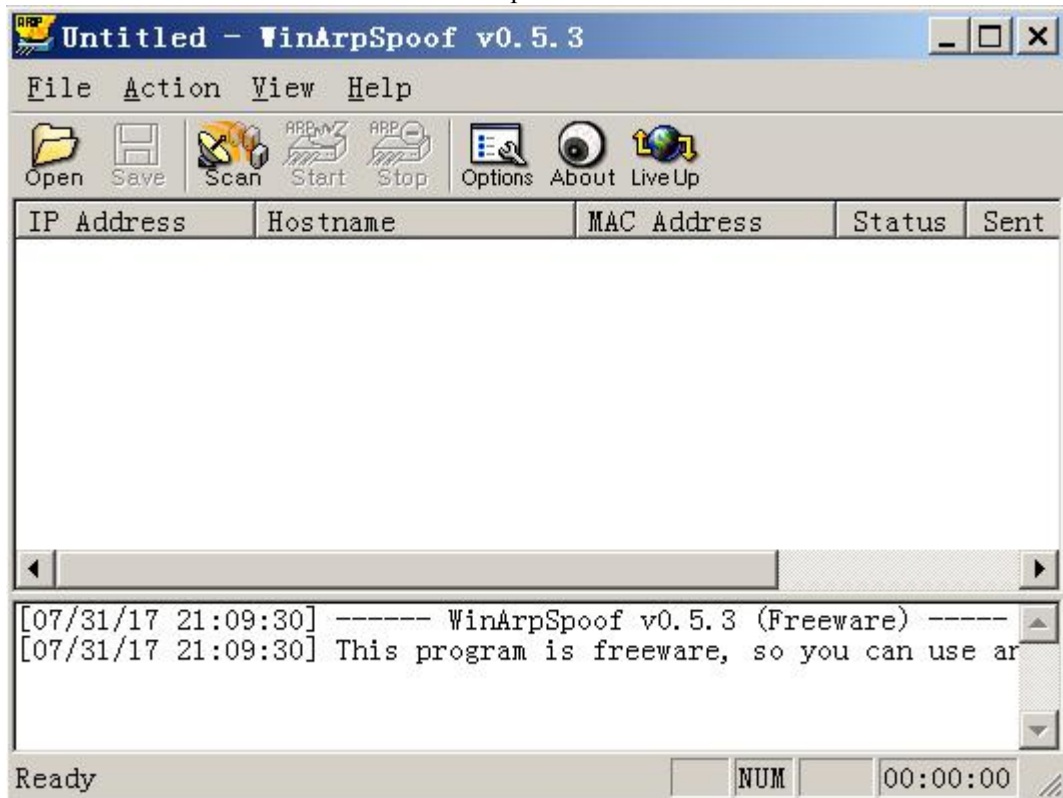


图 4-46 Windows ARP Spoofer 启动界面

### (3) 扫描主机。

一般而言，但凡是网络攻击，首先需要扫描网络，寻找到被攻击的目标主机。同样，利用 Windows ARP Spoofer 发起网关欺骗攻击，首先也是扫描主机。单击 Scan 按钮，即可扫描当前网络中的主机，如图 4-47 所示。



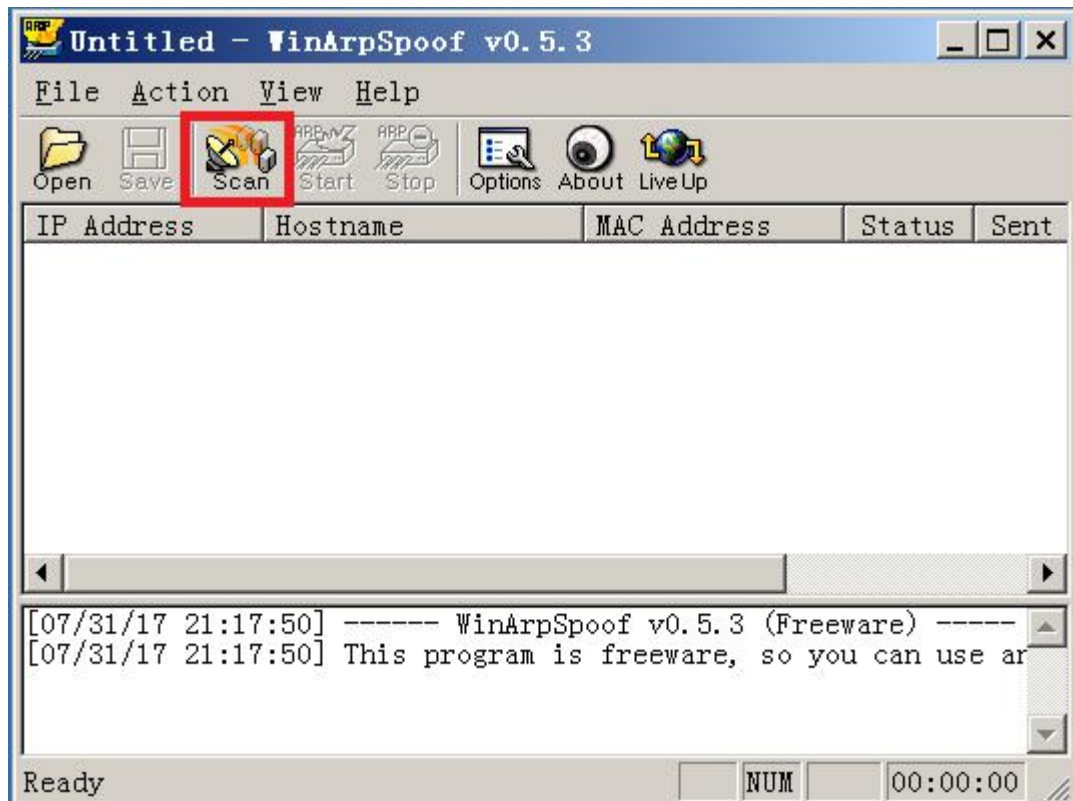


图 4-47 扫描主机

单击 Scan 按钮后，过几秒钟后，即可完成对当前网络的扫描，扫描结果如图 4-48 所示。

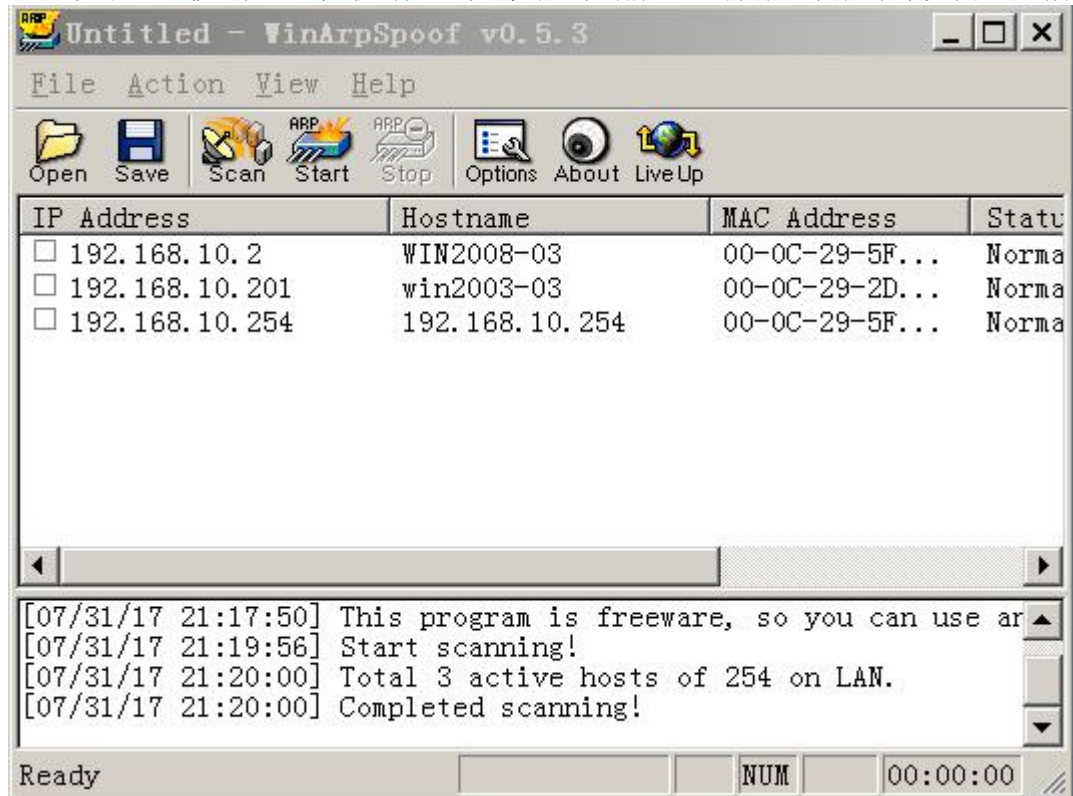


图 4-48 网络扫描结果

(4) 发起攻击。

当完成主机扫描后，即可选择被攻击的主机，此处我们勾选 192.168.10.2 这台主机，即 PC1，选中 PC1 后单击 Start 按钮，即可发起对 PC1 的网关欺骗攻击，此时我们去观察 PC1

访问网关的情况，发现刚才还能正常访问网关，发起攻击后，就不能访问网关了，如图 4-49 所示。

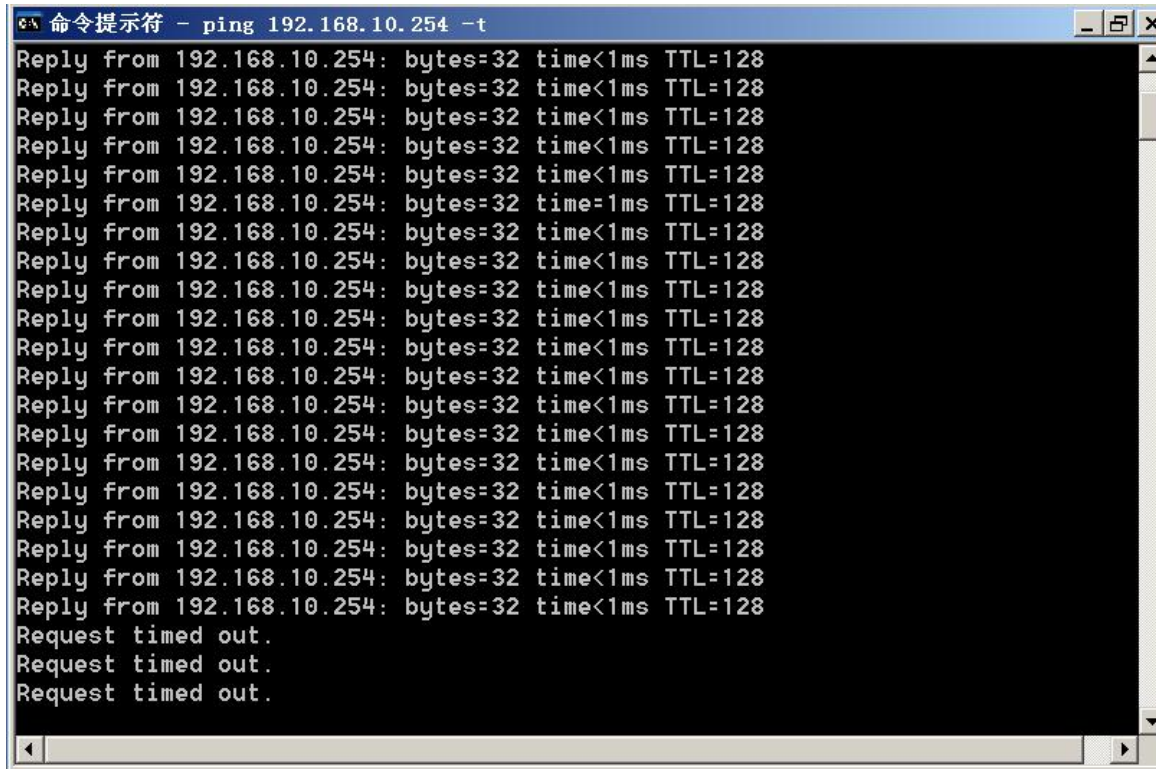


图 4-49 ARP 网关欺骗攻击效果

## 12) 配置 ARP Detection。

### 一、ARP Detection 配置

```
[sw1]arp detection mode dhcp-snooping /*设置 arp 检测的类型为 dhcp snooping
[sw1-vlan10]arp detection enable /*vlan 10 开启 arp 检测功能
[sw1]interface Ethernet 1/0/24
[sw1-Ethernet1/0/24]arp detection trust /*将端口 24 设为 arp 检测信任类型
[sw1]interface Ethernet 1/0/3
[sw1-Ethernet1/0/3]arp rate-limit rate 15 drop /*将端口 3 上交 CPU 进行 ARP 检测的数据的速率设置为 15bps，以达到保护 CPU 的能力
[sw1]interface Ethernet 1/0/2
[sw1-Ethernet1/0/2]arp rate-limit rate 15 drop
```

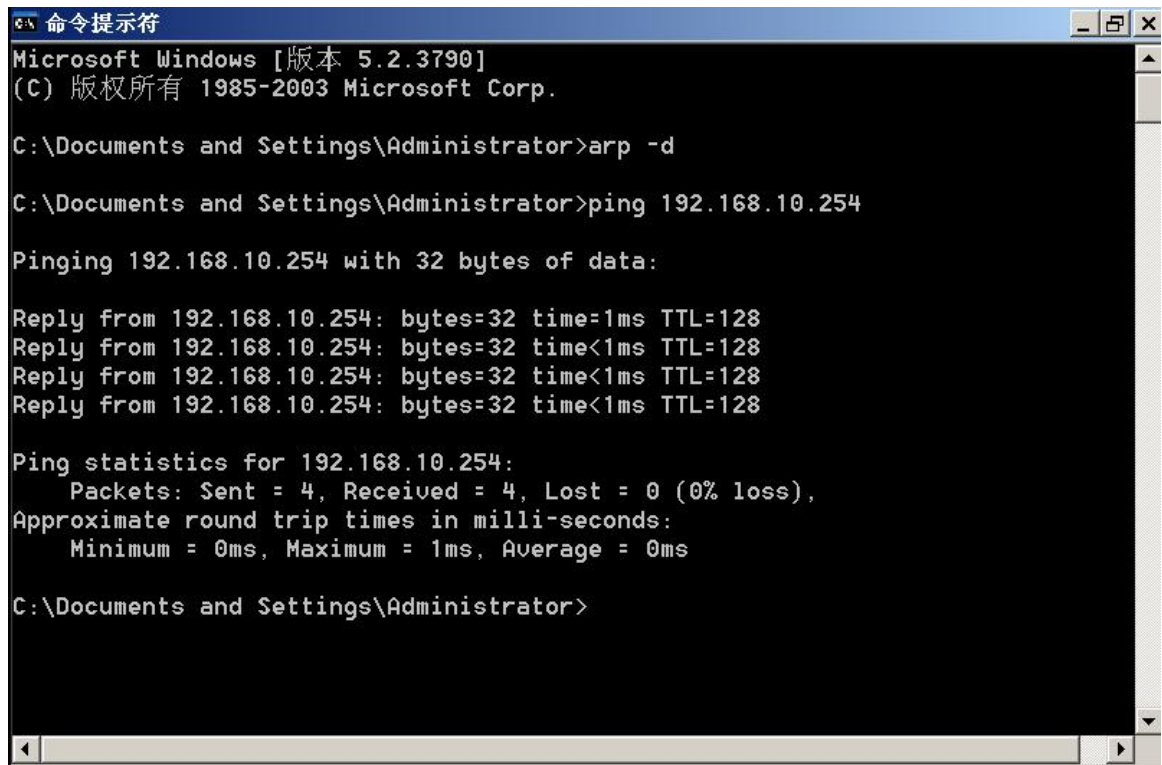
## 1.1.2 ARP 攻击预防任务验收

### 1. 设备验收

根据实训拓扑图检查验收路由器、计算机的线缆连接，检查 PC1、PC2、DHCP 的 IP 地址。

### 2. 功能验收

交换机启动 arp 攻击预防技术，此时将 PC1 的 ARP 缓存清空，PC1 与网关的通信重新恢复，PC2 的攻击不再有效，如图 4-50 所示。



```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -d

C:\Documents and Settings\Administrator>ping 192.168.10.254

Pinging 192.168.10.254 with 32 bytes of data:

Reply from 192.168.10.254: bytes=32 time=1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

图 4-50 PC1 恢复通信

### 1.1.3 ARP 攻击预防总结

针对某公司办公区网络的改造任务的内容和目标, 根据需求分析进行了实训的规划和实施, 通过本任务进行了交换机的 arp 攻击预防技术, 阻止了一些公司员工的恶意技术攻击公司网络, 提高了网络的安全性。