

## 《信息安全及实践》课程实验报告

学院： 信息学院    专业： 计算机科学与技术    年级： 2019

姓名： 白文强                      学号： 20191060064

姓名： 赵浩杰                      学号： 20191060074

姓名： 李泽昊                      学号： 20191060065

实验时间： 2021 年 10 月 08 日

实验名称： MAC 地址欺骗攻击实验和 Smurf 攻击实验

实验成绩：

---



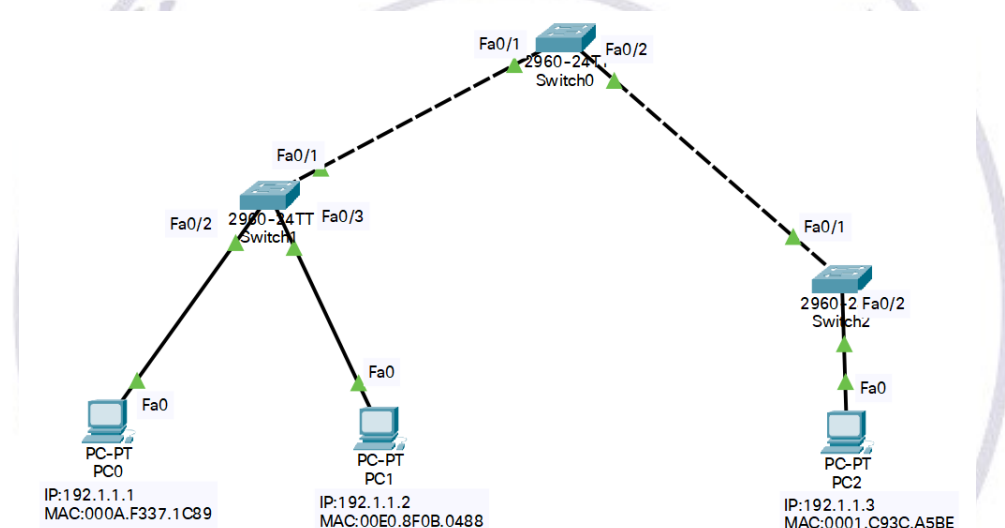
# MAC 地址欺骗攻击实验

## 一、实验目的

- (1)验证交换机建立 MAC 表(转发表) 过程。
- (2)验证交换机转发 MAC 帧机制。
- (3)验证 MAC 地址欺骗攻击原理。
- (4)掌握 MAC 地址欺骗攻击过程。

## 二、实验步骤

- (1)设备放置并连接，并配置 IP 地址及子网掩码，查看 MAC 地址



- (2)完成 PC0 PC1 和 PC2 两两之间的 ICMP 报文传输过程，查看 MAC 地址转发表 switch1:

```
Switch#show mac address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	0001.c93c.a5be	DYNAMIC	Fa0/1
1	000a.f337.1c89	DYNAMIC	Fa0/2
1	00e0.8f0b.0488	DYNAMIC	Fa0/3
1	00e0.8fd3.be01	DYNAMIC	Fa0/1

switch0:

Mac Address Table			
Vlan	Mac Address	Type	Ports
1	0001.c93c.a5be	DYNAMIC	Fa0/2
1	0009.7c5d.0d01	DYNAMIC	Fa0/2
1	000a.f337.1c89	DYNAMIC	Fa0/1
1	00e0.8f0b.0488	DYNAMIC	Fa0/1
1	00e0.b083.ce01	DYNAMIC	Fa0/1

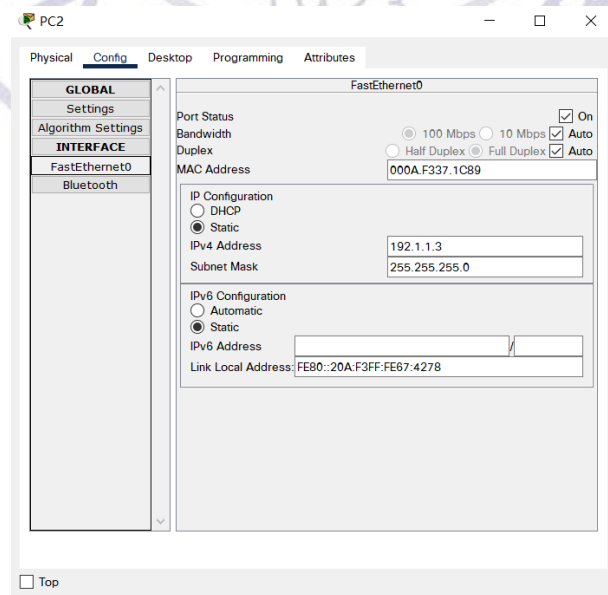
switch2:

Mac Address Table			
Vlan	Mac Address	Type	Ports
1	0001.c93c.a5be	DYNAMIC	Fa0/2
1	000a.f337.1c89	DYNAMIC	Fa0/1
1	00e0.8f0b.0488	DYNAMIC	Fa0/1
1	00e0.8fd3.be02	DYNAMIC	Fa0/1

(3) 切换到模拟操作模式，进入“EditFilters”配置界面，勾选协议 ICMP。通过简单报文工具启动 PC1 至 PC0 的 ICMP 报文传输过程。

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch1	ICMP
	0.002	--	Switch1	ICMP
	0.003	Switch1	PC0	ICMP
	0.004	PC0	Switch1	ICMP
	0.005	Switch1	PC1	ICMP

(4) 切换到实时操作模式。修改 PC2 的 MAC 地址改为 PC0 的 MAC 地址 000A.F337.1C89。



(5)通过简单报文工具启动 PC2 到 PC1 的 ICMP 报文传输过程。查看交换机的 MAC 地址转发表。

switch1:

```
Switch#show mac address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	000a.f337.1c89	DYNAMIC	Fa0/1
1	00e0.8f0b.0488	DYNAMIC	Fa0/3
1	00e0.8fd3.be01	DYNAMIC	Fa0/1

switch0:

```
Switch#show mac address-table
Mac Address Table
```

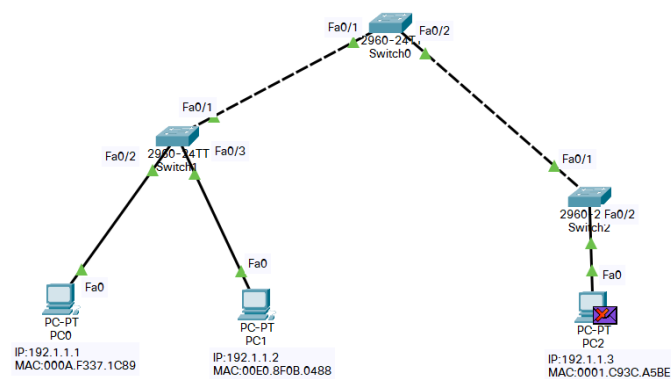
Vlan	Mac Address	Type	Ports
1	0009.7c5d.0d01	DYNAMIC	Fa0/2
1	000a.f337.1c89	DYNAMIC	Fa0/2
1	00e0.8f0b.0488	DYNAMIC	Fa0/1
1	00e0.b083.ce01	DYNAMIC	Fa0/1


switch2:

```
Switch#show mac address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	000a.f337.1c89	DYNAMIC	Fa0/2
1	00e0.8f0b.0488	DYNAMIC	Fa0/1
1	00e0.8fd3.be02	DYNAMIC	Fa0/1

(7)切换到模拟操作模式，通过简单报文工具启动 PC1 至 PC0 的 ICMP 报文传输过程。



Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.001	PC1	Switch1	ICMP
	0.002	Switch1	Switch0	ICMP
	0.003	Switch0	Switch2	ICMP
	0.004	Switch2	PC2	ICMP

### 三、实验结果及分析

连接设备并设置完 IP 地址后，PC0、PC1、PC2 之间可以两两 ping 通，设备连接及配置没有问题。

随后在模拟操作模式进行 PC0 和 PC1 之间的 ICMP 通信，可以看到，ICMP 报文从 PC1 到 switch1 再到 PC0，再由 PC0 经 switch1 到达 PC1，报文没有到达 switch0、switch2 和 PC2，证明本次 ICMP 通信正常。

将 PC2 的 MAC 地址改为 PC0 的 MAC 地址后，再进行 PC2 和 PC1 之间的 ICMP 报文通信，由于 PC2 的 MAC 地址和 PC0 相同，且 PC2 与 PC1 之间进行了一次 ICMP 报文通信，在交换机中的 MAC 地址转发表中，到达 MAC 地址 000A.F337.1C89 (即 PC0 MAC 地址)的报文会被转发到 switch0 进而转发到 PC2。在实验中也可以看到，从 PC1 发出的 ICMP 报文，没有到达 PC0，而是经过 switch0、switch2 到达 PC2，且 PC2 没有接收该报文，MAC 欺骗攻击成功。

### 四、实验总结及体会

在实验中并未遇到比较棘手的困难，遇到的最大问题是对软件模拟的不熟悉，一开始没有找到简单报文工具和复杂报文工具，不知道具体的模拟仿真流程，但经过研究探索，对软件的模拟仿真流程有了一些熟悉。随后的实验便比较顺利了。

实验总结：MAC 地址欺骗可以利用交换机端口学习的漏洞，通过客户端向交换机发送欺骗报文、攻击交换机的 CAM 表的方式，使交换机 CAM 表的记录与真实的主机对应 MAC 地址不一致，从而使交换机将报文错误转发给攻击者。

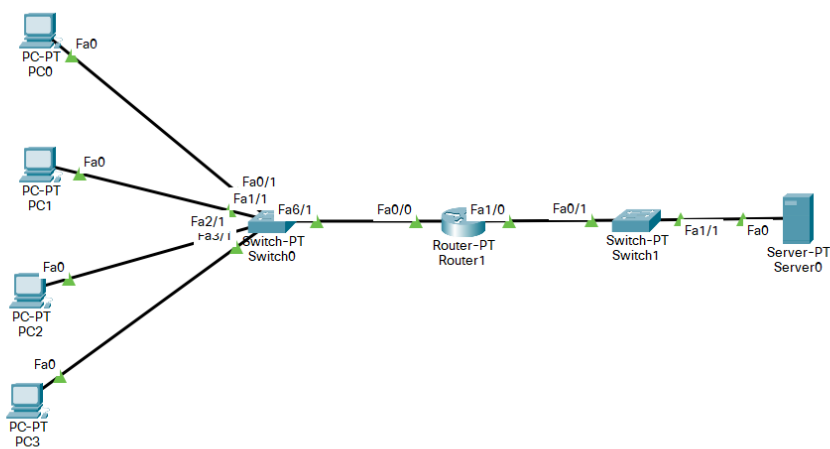
# Smurf 攻击实验

## 一、实验目的

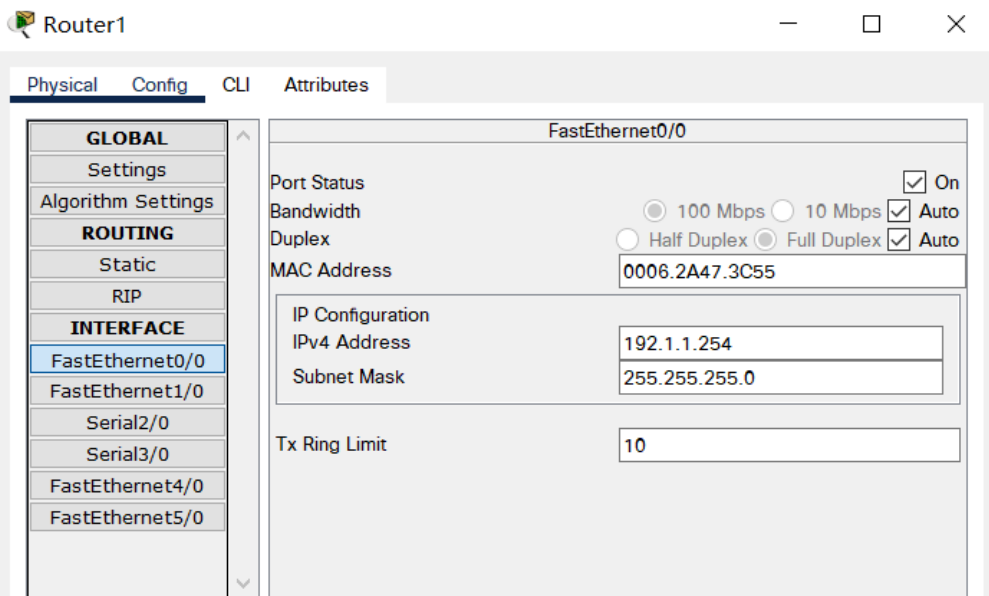
- (1) 验证 ICMP Echo 请求、响应过程。
- (2) 验证网络放大 ICMP Echo 响应报文的过程。
- (3) 验证间接攻击原理。
- (4) 验证 Smurf 攻击过程。

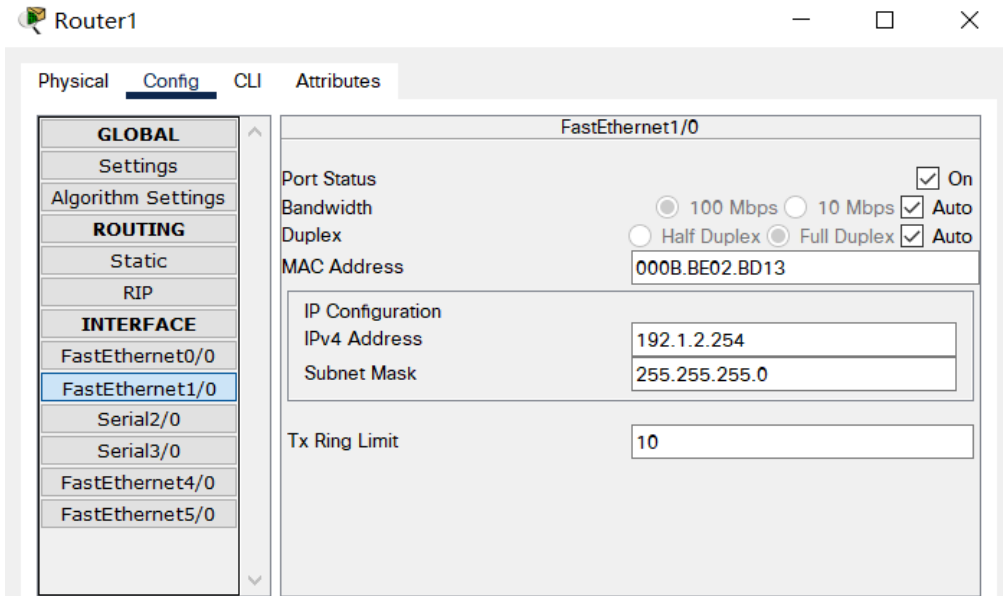
## 二、实验步骤

- (1) 启动 PacketTracer，放置和连接设备。



- (2) 完成路由器接口 IP、子网掩码配置

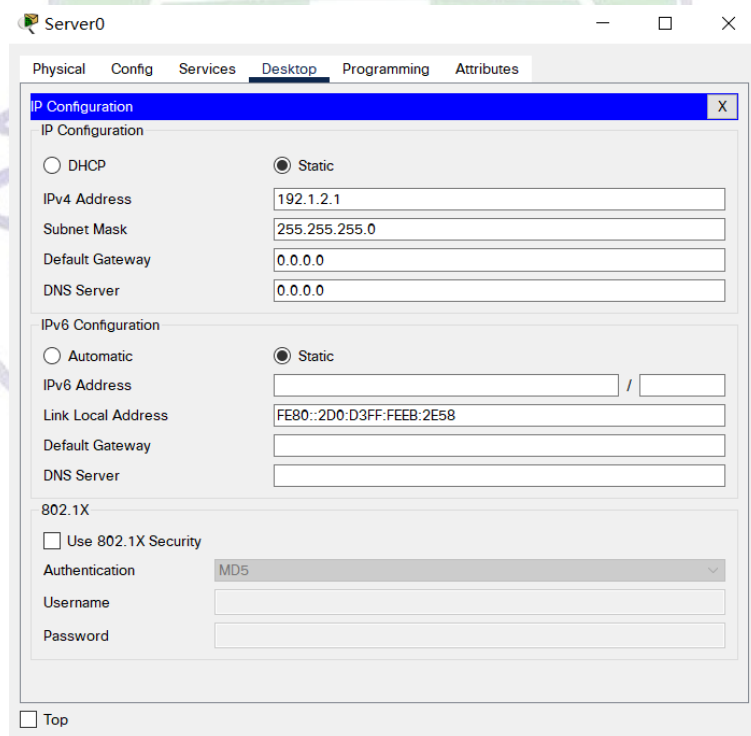




(3)完成路由器 Router DHCP 服务器配置过程

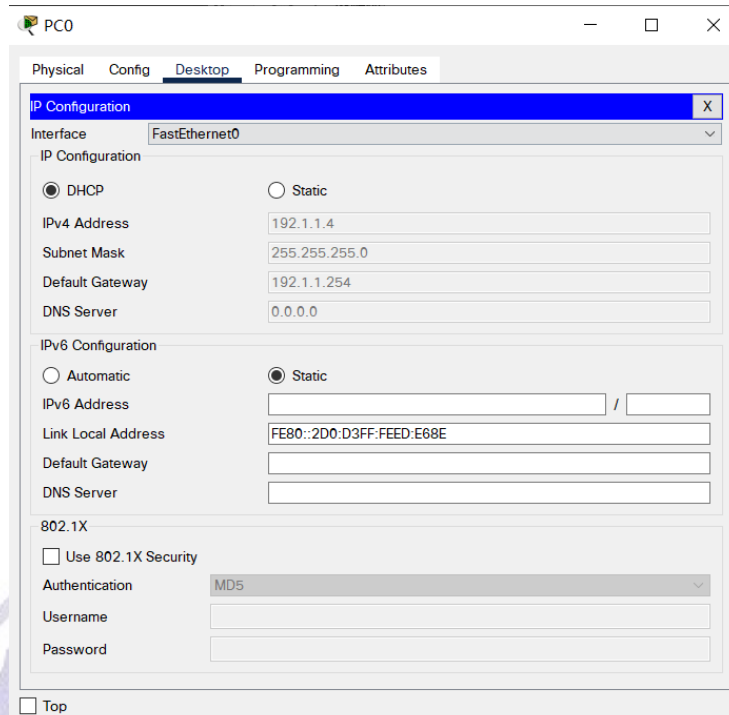
```
Router(config)#ip dhcp pool lan1
Router(dhcp-config)#default-router 192.1.1.254
Router(dhcp-config)#network 192.1.1.0 255.255.255.0
Router(dhcp-config)#exit
Router(config)#
```

(4)完成 Web 服务器网络信息配置过程



(5)给 PC0、PC1、PC2、PC3 配置 DHCP，使其可以自动获取网络信息





PC0

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 192.1.1.4

Subnet Mask: 255.255.255.0

Default Gateway: 192.1.1.254

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2D0:D3FF:FEED:E68E

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

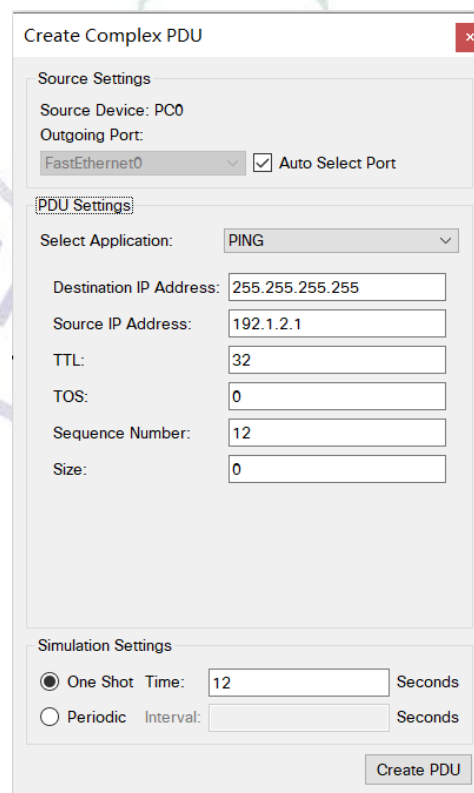
Authentication: MD5

Username:

Password:

☐ Top

(6)切换到模拟操作模式，通过复杂报文工具在 PC0 上生成 ICMP ECHO 请求报文，该 ICMP ECHO 请求报文封装成源 IP 地址是 Web 服务器的 IP 地址 192.1.2.1、目的 IP 地址是全 1 的广播地址的 IP 分组。该 IP 分组在由 Switch1 构成的以太网上广播，到达所有其他终端和路由器 Router。



Create Complex PDU

Source Settings

Source Device: PC0

Outgoing Port: FastEthernet0 ☒ Auto Select Port

PDU Settings

Select Application: PING

Destination IP Address: 255.255.255.255

Source IP Address: 192.1.2.1

TTL: 32

TOS: 0

Sequence Number: 12

Size: 0

Simulation Settings

☒ One Shot Time: 12 Seconds

☐ Periodic Interval: Seconds

Create PDU



### (7)进行 ICMP 通信

Vis.	Time(sec)	Last Device	At Device	Type
	12.000	--	PC0	ICMP
	12.001	PC0	Switch0	ICMP
	12.002	Switch0	PC1	ICMP
	12.002	Switch0	PC2	ICMP
	12.002	Switch0	PC3	ICMP
	12.002	Switch0	Router1	ICMP
	12.006	--	PC1	ICMP
	12.007	PC1	Switch0	ICMP
	12.007	--	PC2	ICMP
	12.008	PC2	Switch0	ICMP
	12.008	Switch0	Router1	ICMP
	12.008	--	PC3	ICMP
	12.009	PC3	Switch0	ICMP
	12.009	Switch0	Router1	ICMP
	12.009	Router1	Switch1	ICMP
	12.010	Switch0	Router1	ICMP
	12.010	Router1	Switch1	ICMP
	12.010	Switch1	Server0	ICMP
	12.011	Router1	Switch1	ICMP
	12.011	Switch1	Server0	ICMP
	12.012	Switch1	Server0	ICMP

### 三、实验结果及分析

由模拟状态下 ICMP 通信结果看到，最终 Server0 收到了 ICMP 报文。

分析：终端 A 将 ICMP Echo 请求报文封装成以 Web 服务器的 IP 地址为源 IP 地址、以全 1 广播地址为目的 IP 地址的 IP 分组，该 ICMP Echo 请求报文到达 LAN1 中的所有其他终端和路由器 R，接收到该 ICMP Echo 请求报文的终端均发送 ICMP Echo 响应报文，由于请求报文中的源 IP 地址为 Web 服务器的 IP 地址，因此，这些 ICMP Echo 响应报文都被封装成以 Web 服务器的 IP 地址为目的 IP 地址的 IP 分组，导致 ICMP Echo 响应报文全部到达 Web 服务器。

### 四、实验总结及体会

这种攻击方法结合使用了 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目标系统。可以试想，如果一个网络上的拥有足够多的终端，若有人利用 Smurf 攻击对一台 Web 服务器进行拒绝服务攻击，通过伪造报文源 IP 地址为服务器，目的 IP 地址广播，散步到各个终端，设置周期短、次数高的复杂报文发送，通过各个终端进行回复的报文进行占用服务器的网络信道，造成信道拥塞，使得服务器在短时间内无法与外界进行通信，造成可用性的缺失。