**西安电子科技大学**

**计算机与网络安全综合实验 课程实验报告**

**实验名称 网络攻击实验**

网络与信息安全 学院 2118021 班

成 绩

姓名 盖乐 学号 21009200991

同作者

实验日期 2024 年 4 月 27 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

# 实验1.集线器和嗅探攻击实验

## 一、实验目的

## 验证利用集线器实施嗅探攻击的过程。

## 验证嗅探攻击不会影响正常的MAC帧传输过程。

## 验证嗅探攻击对于源和目的终端是透明的。

## 二、实验任务

1. 使用自己的语言简述利用集线器实施嗅探攻击的过程。

（不能从老师的资料中截图，从自己的界面里截图）

嗅探终端发给路由器的MAC帧，可以在路由器和交换机之间添加集线器，并在集线器上连接一个终端，可通过此终端嗅探其他终端和路由器之间传输的MAC帧。

1. 使用自己的语言简述该实验原理。

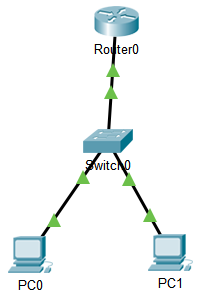
（不能从老师的资料中截图，从自己的界面里截图）

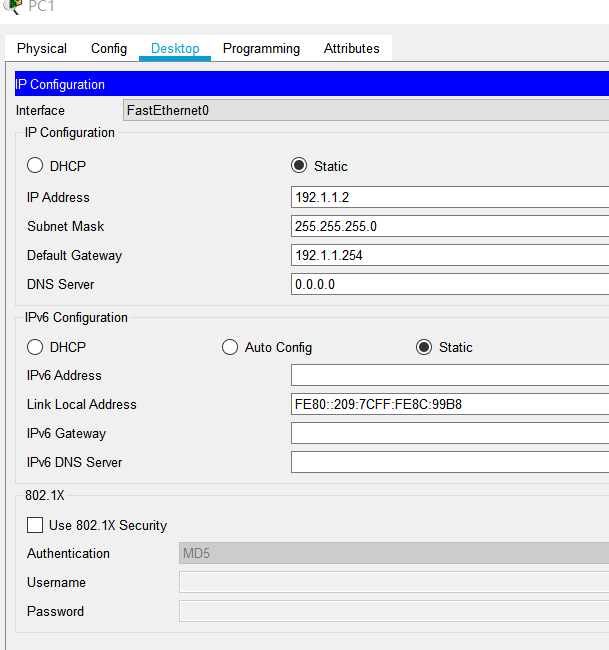
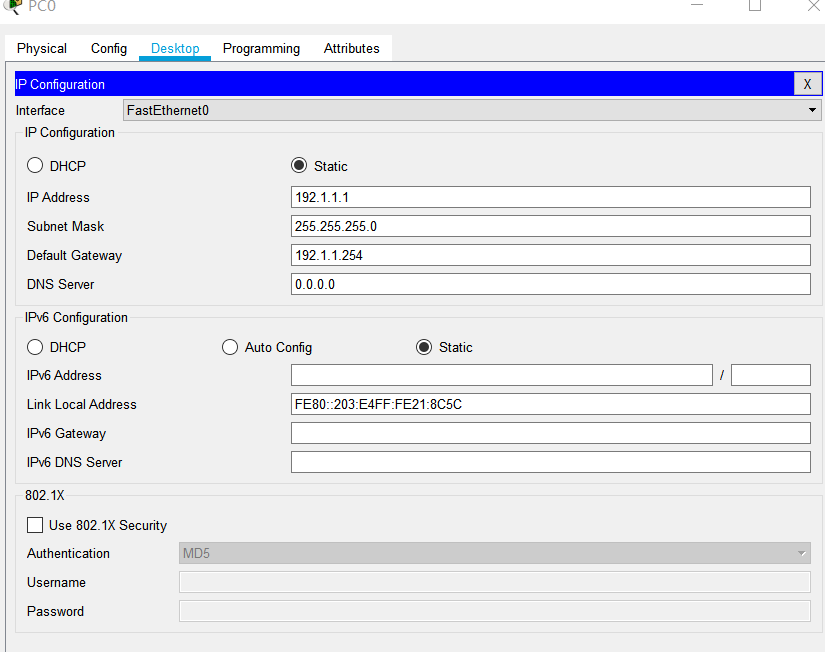
集线器是广播设备，所以集线器其中一个端口收到MAC帧后会向其他所有端口发送此MAC帧，黑客终端连接到集线器上便可嗅探此MAC帧。

1. 实验步骤

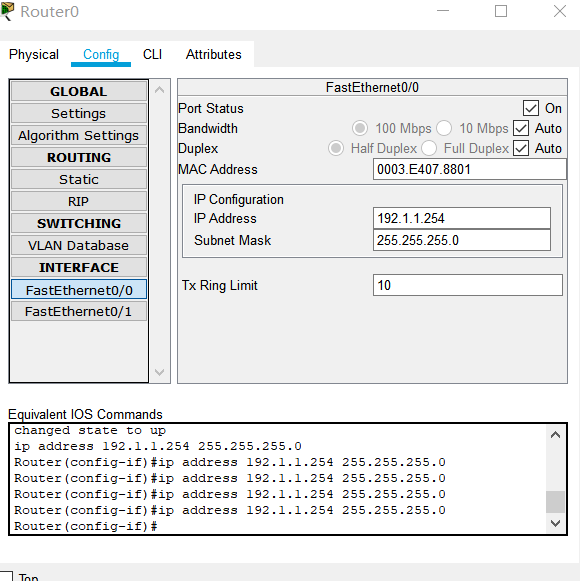
（根据教材或老师给的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

（1）画出正常的网络拓扑图，并完成PC0和PC1的网络配置

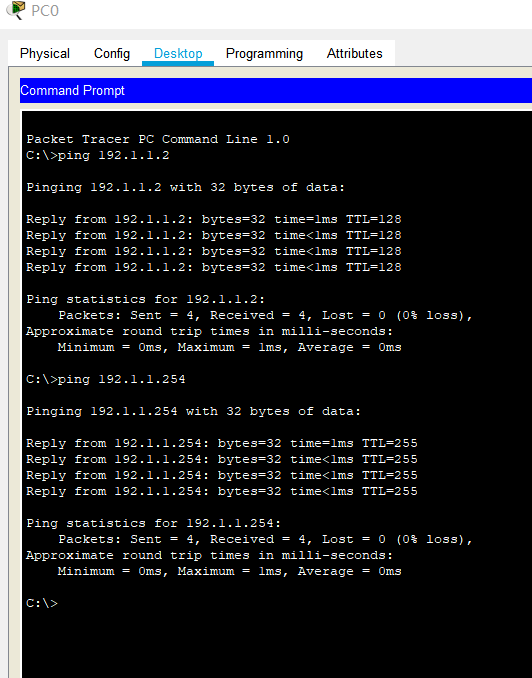




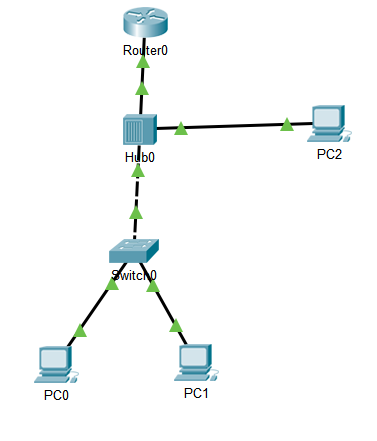
（2）配置路由器接口



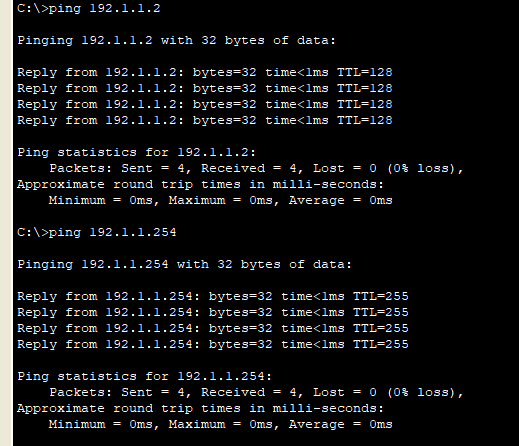
（3）测试PC和路由器之间的连通性



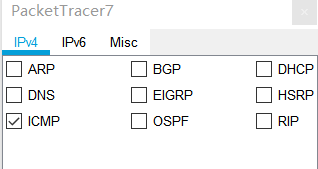
（4）接入集线器和黑客终端



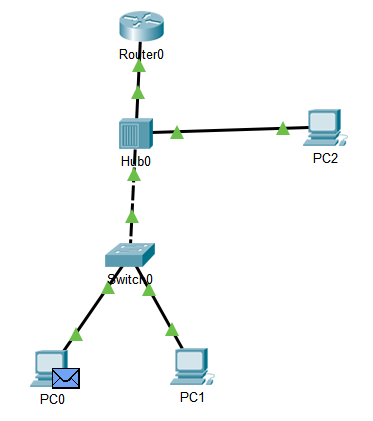
（5）首先证明PC和路由器之间的连通性



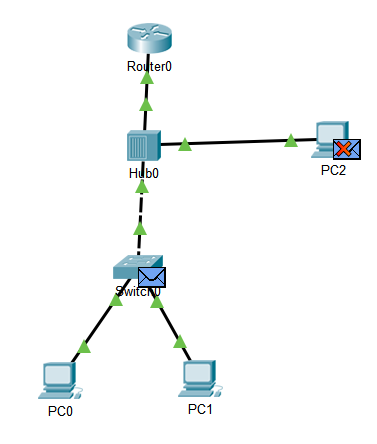
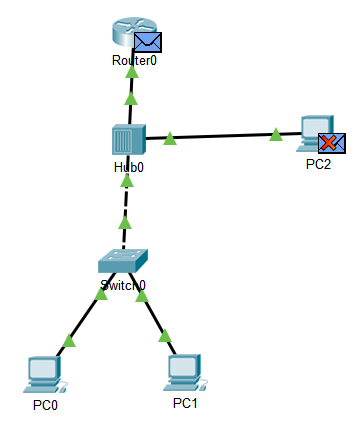
切换到模拟模式

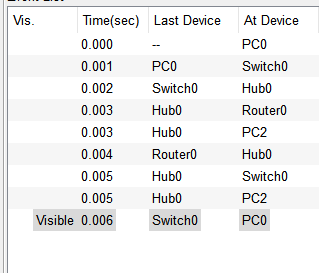


添加PC0到路由器的报文



仿真发现在两段过程中黑客终端都能嗅探到ICMP报文





## 三、思考与总结

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

在测试PC和路由器连通性时，出现了第一个包的丢失，经查阅资料发现一个包丢弃的原因是因为第一次ping没有进行ARP地址解析不知道MAC地址，ARP协议解析后得到MAC地址才会使后续的包不出现丢包。

# 实验2.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、实验任务

1. 使用自己的语言简述何谓MAC地址欺骗。

（不能从老师的资料中截图，从自己的界面里截图）

交换机建立了完整转发表后，终端B发给终端A的MAC帧只能到终端A，终端C把自己的MAC地址修改为终端A的地址再向终端B发送MAC帧，终端B再发给终端A的MAC帧会到达终端C而不是终端A。

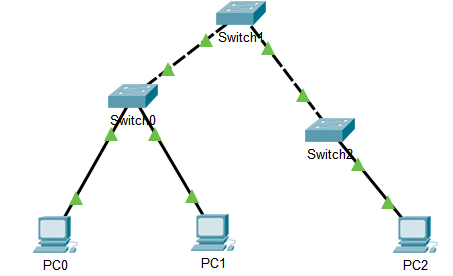
1. 使用自己的语言简述MAC地址欺骗攻击原理，附带每个交换机的转发表。（不能从老师的资料中截图，从自己的界面里截图）

正常转发过程中，转发项将通往终端A的交换路径作为通往MAC地址为MAC A的终端的交换路径。终端C修改自己的MAC地址为MAC A，并且向终端B发送MAC帧，就会修改交换机的转发表，把通往终端C的交换路径作为通往MAC地址为MAC A的终端的路径，再发送目的地址为MAC A的MAC帧会到达终端C。

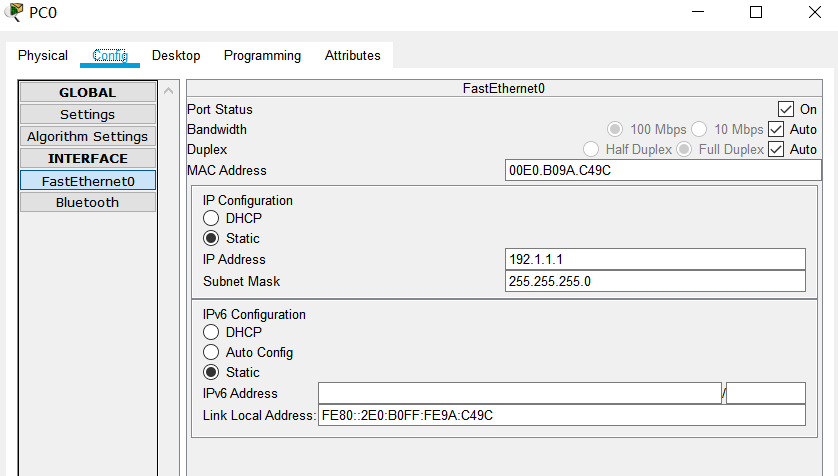
1. 实验步骤

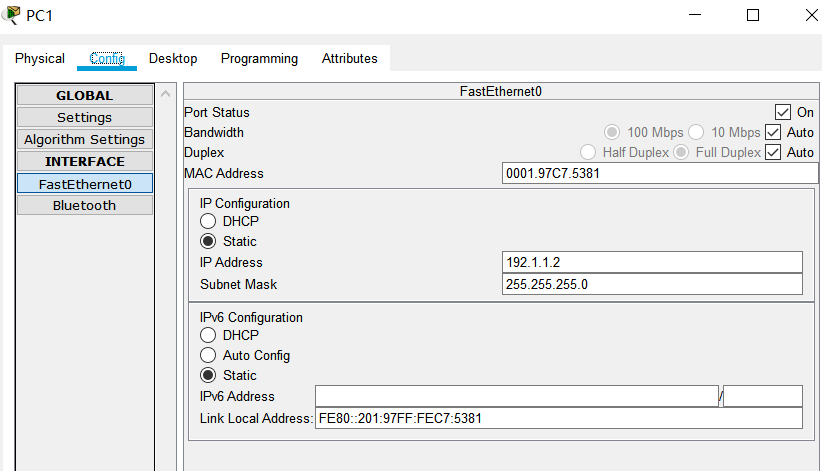
（根据教材或老师给的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

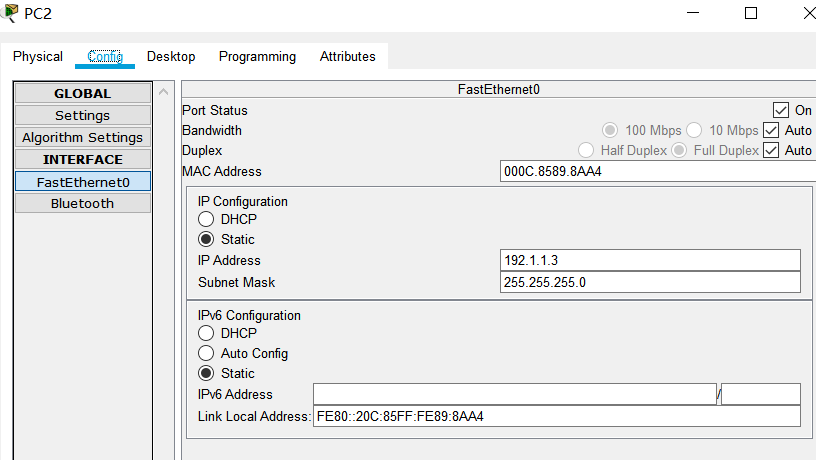
（1）完成网络拓扑图



（2）配置PC ip地址





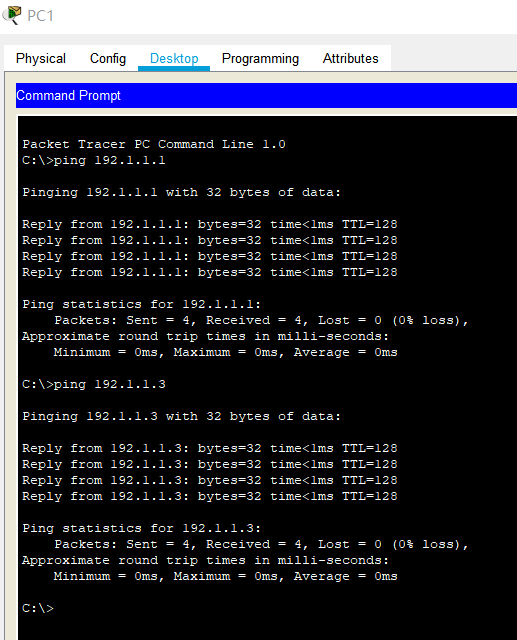
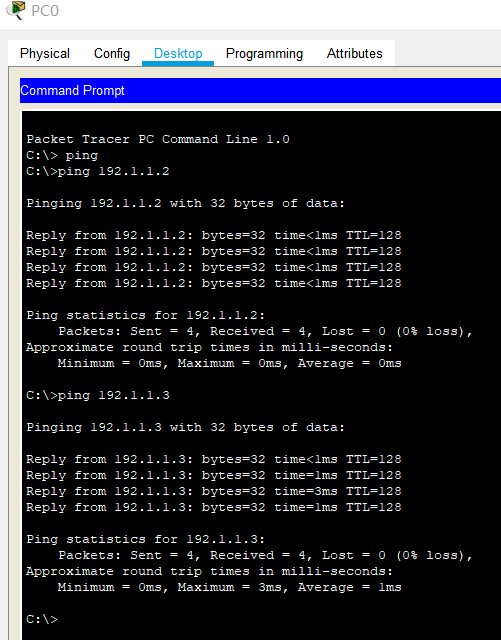


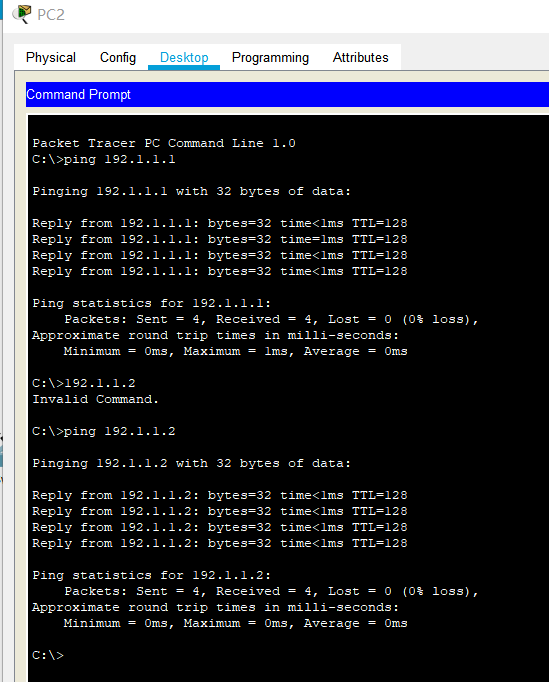
PC0的MAC地址为00E0.B09A.C49C

PC1的MAC地址为0001.97C7.5381

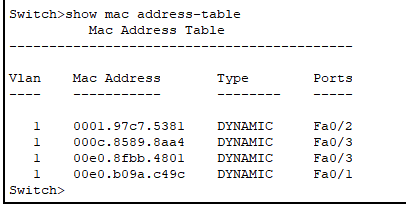
PC2的MAC地址为000C.8589.8AA4

（3）完成 PC0、PC1 和 PC2 两两之间的 ICMP 报文传输过程

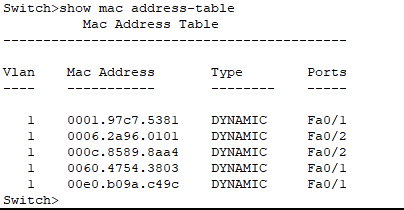




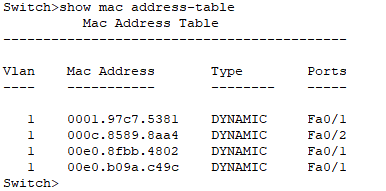
Switch0的转发表 MAC地址00E0.B09A.C49C对应连接PC0的端口0/1



Switch1的转发表 MAC地址00E0.B09A.C49C对应的转发端口是该交换机连接交换机Switch0的端口0/1。

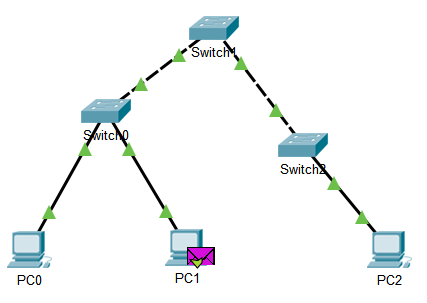


Switch1的转发表 MAC地址00E0.B09A.C49C对应的转发端口是该交换机连接交换机Switch1的端口0/1。

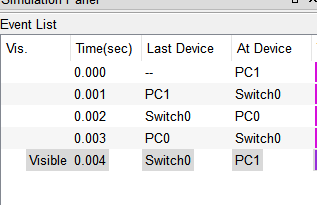


所有交换机中的转发路径将通往PC0的交换路径作为通往MAC地址为00E0.B09A.C49C的终端的交换路径。

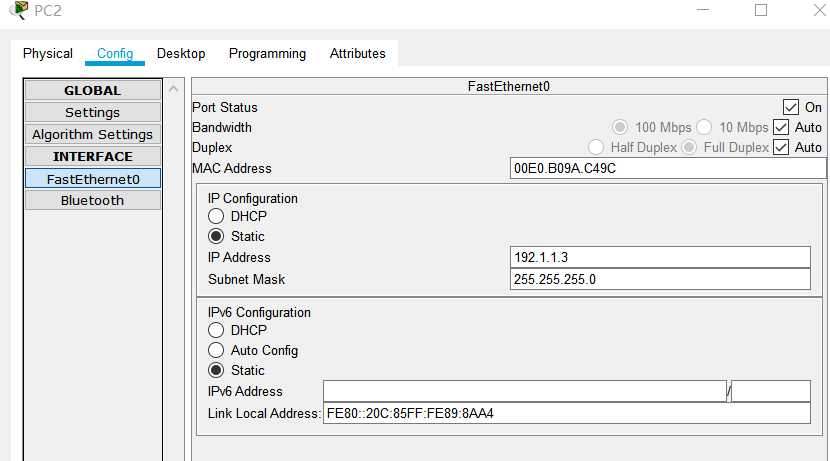
（4）切换到模拟操作模式，进入“Edit Filters”配置界面，勾选协议 ICMP。通过简单报文工具启动 PC1 至 PC0 的 ICMP 报文传输过程。



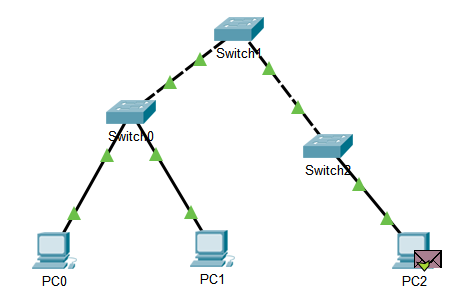
发现报文只到PC0。

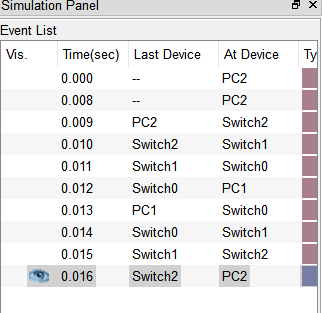


（5）切换到实时模式修改PC2的端口0的MAC地址修改为PC0的端口0的MAC地址00E0.B09A.C49C



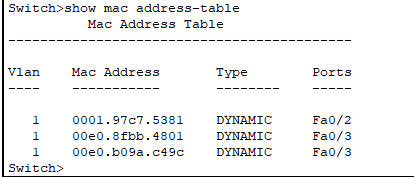
（6）通过简单报文工具启动 PC2 至 PC1 的 ICMP 报文传输过程，让交换机学习到新的转发表。



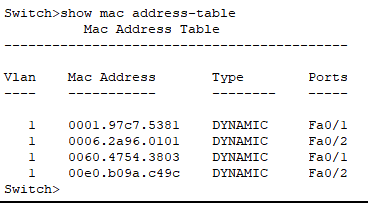


新的转发表如下图所示

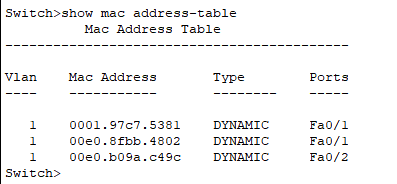
Switch0：



Switch1：

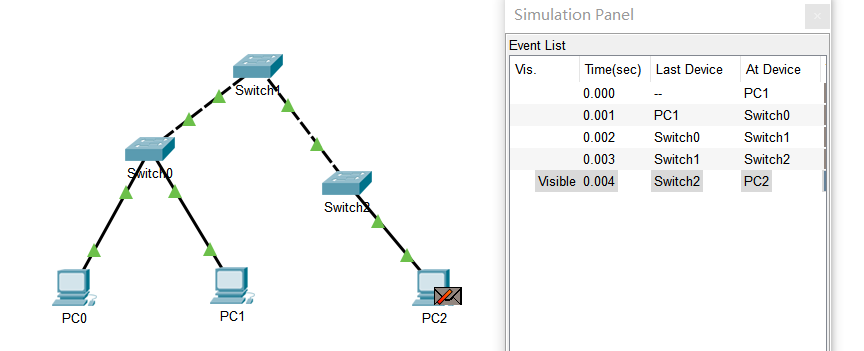


Switch2：



（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。

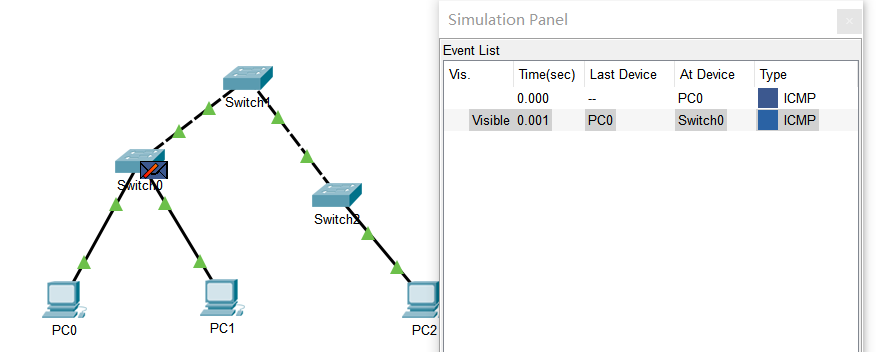
发现该报文到达了PC2



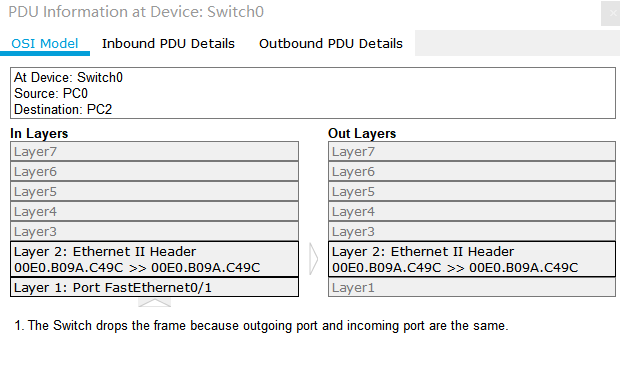
## 三、思考与总结

1. PC0和PC2之间可以通信吗？为什么？

不可以。



原因是在Switch0处，输入端口和输出端口相同。



1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

第一次终端互相ping后集线器并没有完整的MAC表，再次互相ping后得到完整的MAC表。

# 实验3.钓鱼网站实验

## 一、实验目的

## 1. 验证伪造的DHCP服务器为终端提供网络信息配置服务的过程。

## 2. 验证错误的本地域名服务器地址造成的后果。

## 3. 验证利用网络实施钓鱼网站的过程。

## 二、实验任务

1. 使用自己的语言简述钓鱼网站实施过程

（不能从老师的资料中截图，从自己的界面里截图）

黑客在网络中接入伪造的DHCP服务器，伪造的DNS服务器和伪造的Web服务器，向终端提供合格的域名和伪造的Web地址，导致终端访问伪造的Web地址。

1. 使用自己的语言简述本实验原理

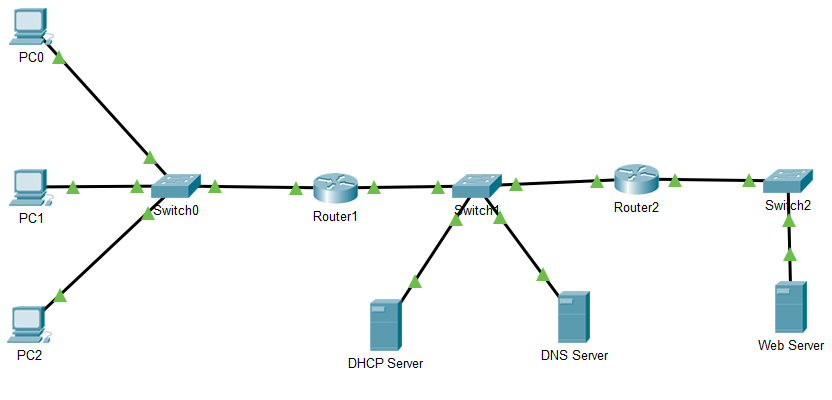
（不能从老师的资料中截图，从自己的界面里截图）

终端发送广播DHCP发现DHCP服务器并且选择第一个到达终端的发送DHCP的DHCP服务器为其提供网络信息配置服务。伪造的DHCP服务器和终端接在一个网络中，发送的DHCP消息先到达终端，导致终端选择伪造的DHCP服务器为其提供网络信息配置服务。

1. 实验步骤

（根据教材或老师给的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

（1）实现正常的Web服务器访问过程，完成网络拓扑图。

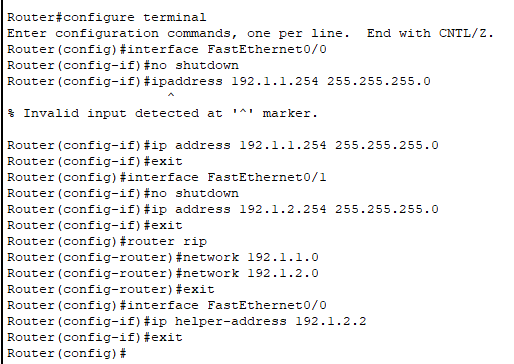


（2）完成路由器接口 IP 地址和子网掩码配置过程，完成路由器 RIP 配置过程。路由器Router1 和 Router2 建立完整路由表。

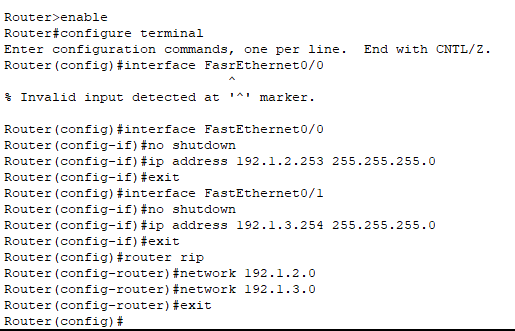
（3）完成路由器 Router1 接口 FastEthernet0/0 的中继地址配置过程。

步骤（2）步骤（3）配置过程如下图所示。

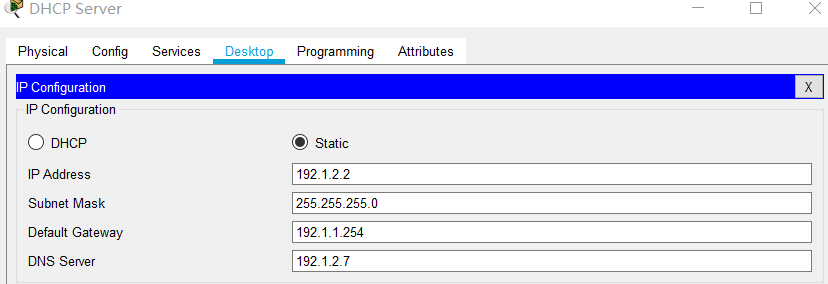
Router1：

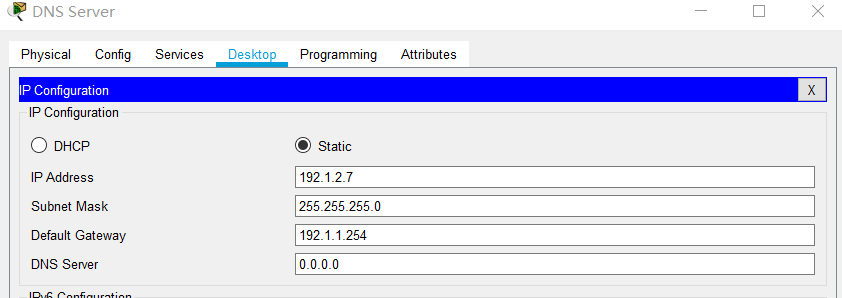


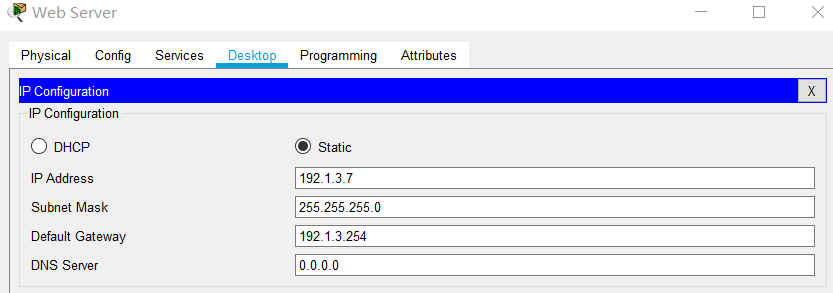
Router2：



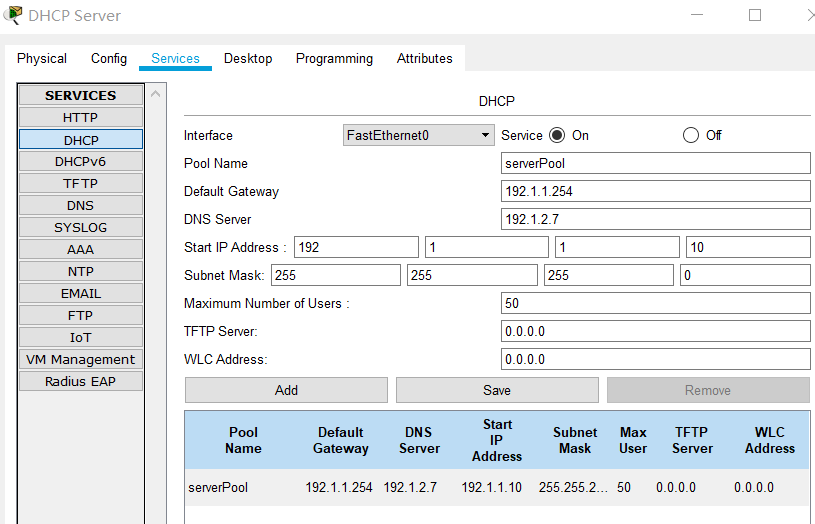
（4）完成 3 台服务器 IP 地址、子网掩码和默认网关地址配置过程，服务器的默认网关地址是路由器连接服务器所在网络的接口的 IP 地址。



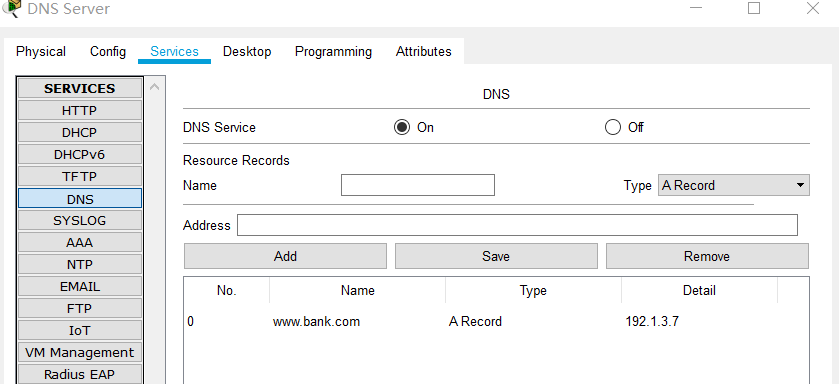




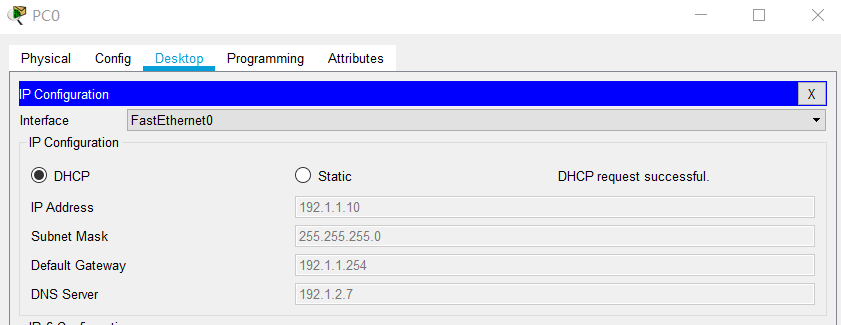
1. 完成 DHCP 服务器配置。



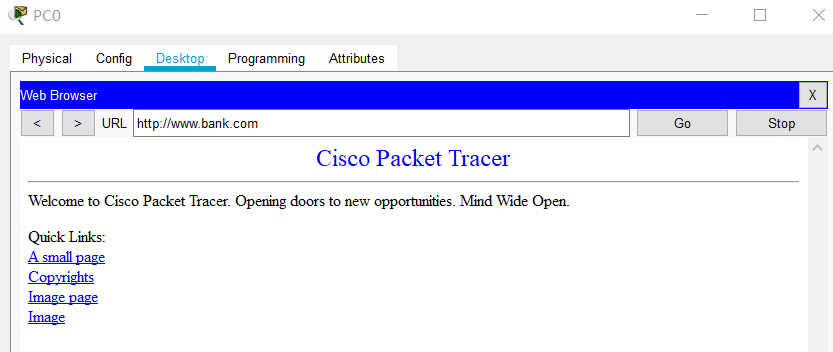
（6）完成DNS服务器配置过程



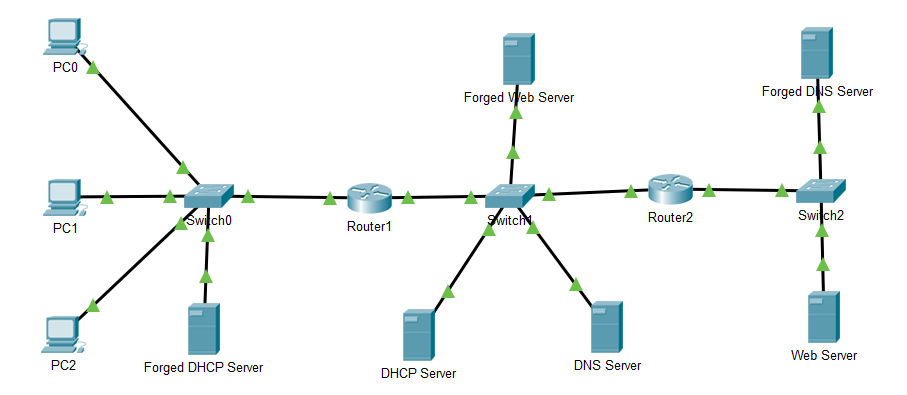
（7）完成 PC0 通过 DHCP 自动获取IP地址的过程

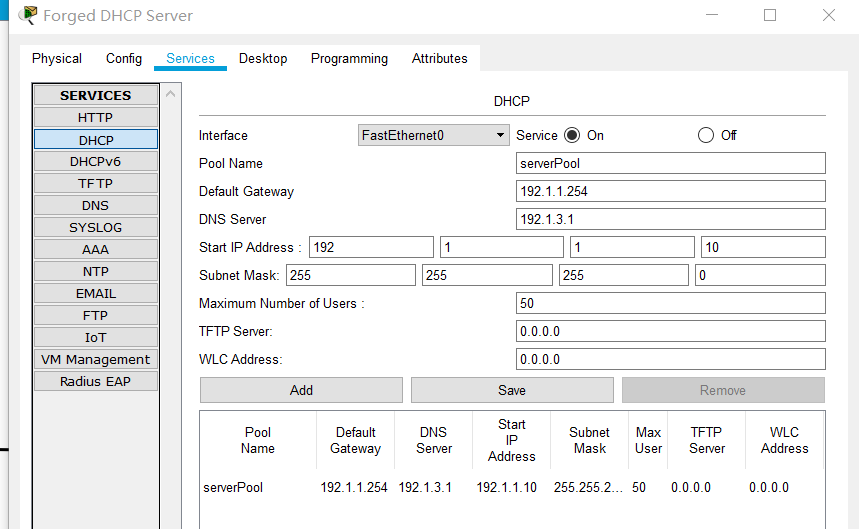


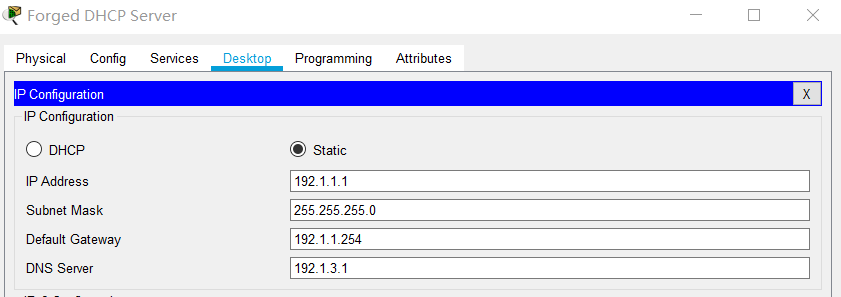
（8）PC0访问www.bank.com：

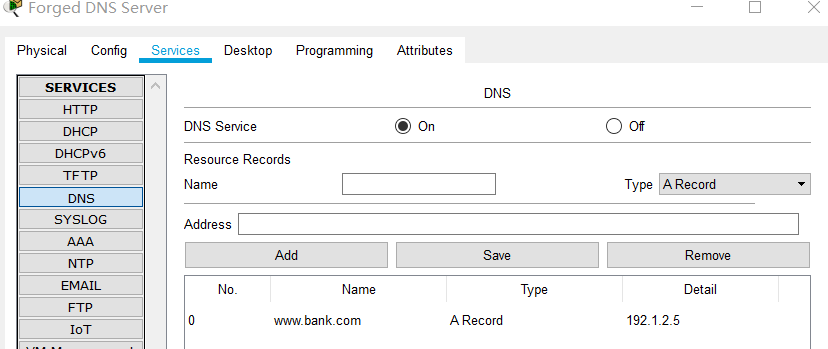


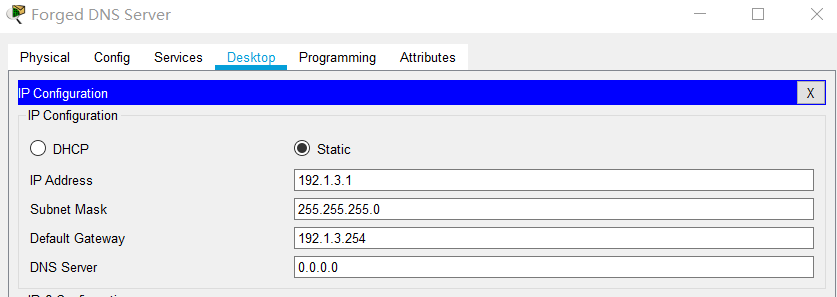
（9）接入伪造的服务器，完成3台伪造服务器的相关配置。

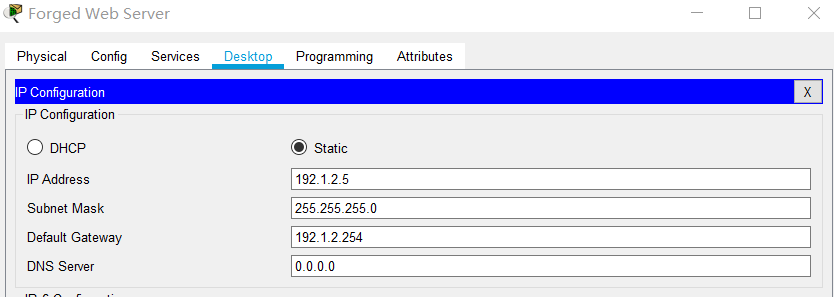




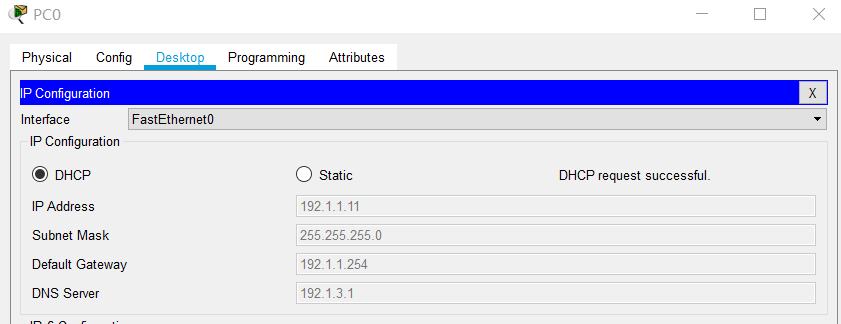






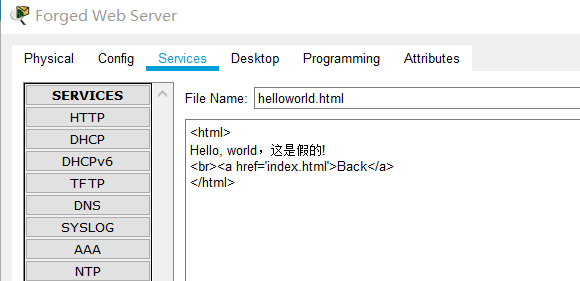


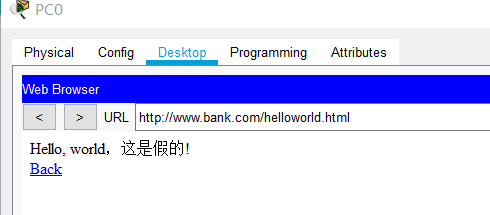
PC0再次自动获取网络信息，表明PC0从伪造的DHCP服务器获取网络信息



（10）PC0再次访问www.bank.com，证明进入了钓鱼网站。

修改了伪造Web服务器里的一条链接。





## 三、思考与总结

1. 为什么ForgedDHCPServer可以替代正常的DHCPServer实现攻击？如果把ForgedDHCPServer连接到192.1.3.0/24的网段中，还可以起到攻击效果吗？为什么？

因为ForgedDHCP服务器与终端位于同一网络，伪造的DHCP服务器发送的DHCP消息先于DHCP服务器发送的DHCP消息。

不会，这样DHCP服务器发送的DHCP消息会先被接收到。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

添加伪造的三个服务器后忘记配置IP信息，导致后面出现问题。

本次实验学习了钓鱼网站和虚假DHCP服务器攻击的原理和应用。深刻体会了DHCP和DNS协议的工作原理。