**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 学号

同作者

实验日期 2024 年 05 月 29 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。

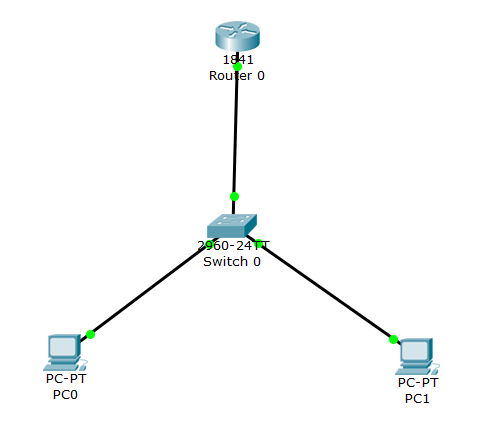
由于集线器是广播设备，攻击者可以将自己的终端连接在与交换机相接的集线器上，当有数据包经其它端口到达该交换机时，交换机会将该数据包转发至该端口，从而经集线器到达攻击者的主机；当有数据包经此端口到达交换机时，会通过集线器发送至攻击者。即攻击者可以利用集线器通过上述两个过程完成嗅探攻击。

1. 使用自己的语言简述该实验原理。

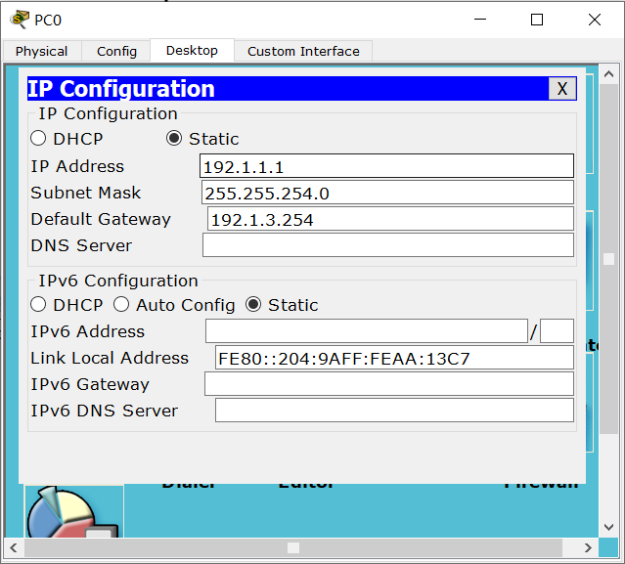
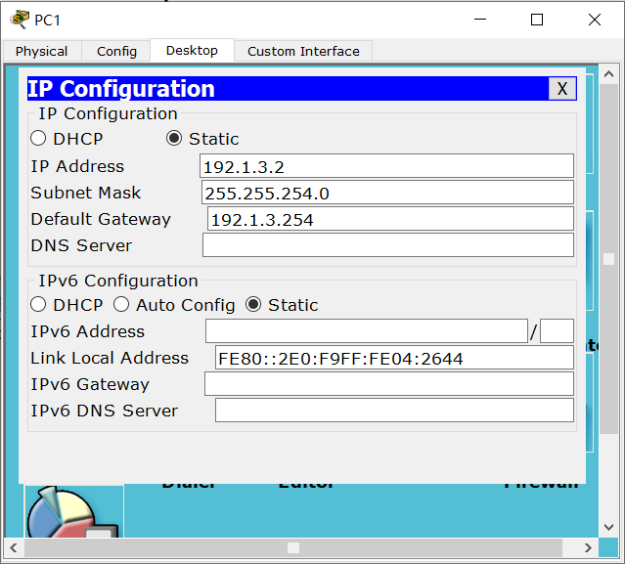
因为集线器是广播设备，因此任何经集线器传输的数据包都会被集线器以广播的形式经其它端口发送。攻击者可以将自己的主机连接在与交换机相连的集线器上，进而实现将所用通过交换机的数据包都转发至自己主机，实现对交换机数据包的嗅探攻击。

1. 实验步骤

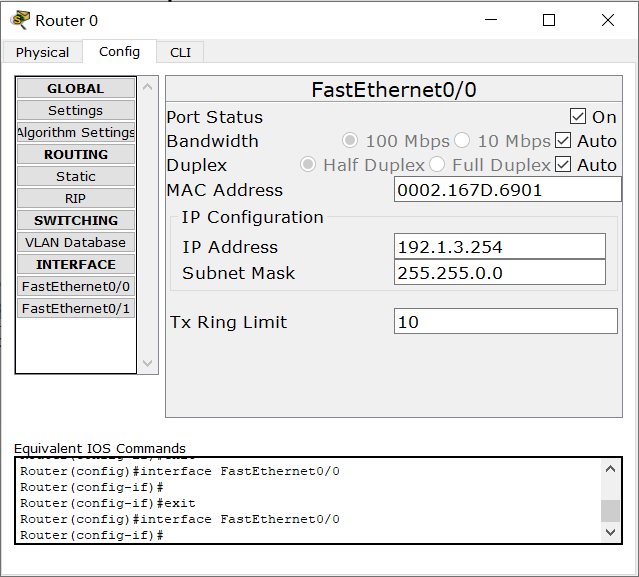
首先搭建如图所示的拓扑图：



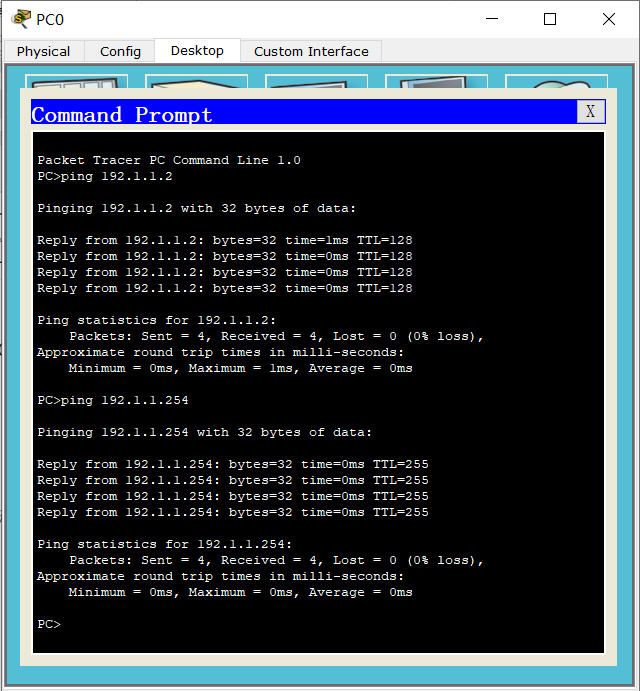
此后分别配置PC0与PC1的IP地址及其子网掩码。由于根据实验原理，PC0与PC1进行通信时要经过R0路由器，因此PC0与PC1不应该在同一子网中，所以PC0的IP地址设置为192.1.1.1，PC1设置为192.1.3.2。

接着进行路由器的相关配置，进入Router中与交换机相连的FE0/0端口，配置其IP地址与子网掩码，并据此配置PC0与PC1的默认网关。此处需要指出，我的子网掩码与实验指导中设置的并不相同，因为按照指导中的255.255.255.0的子网掩码，PC0的192.1.1.1就不在R0的子网中，因此会导致通信异常。

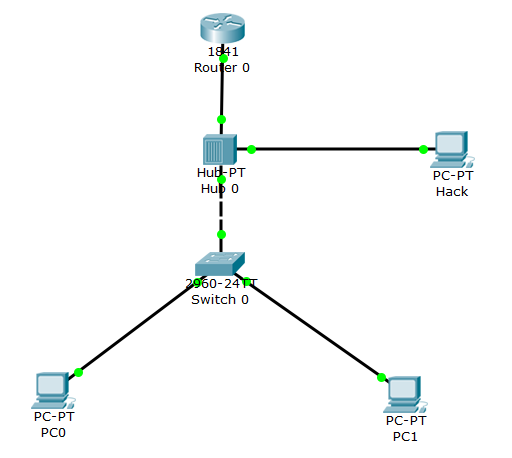


完成上述配置后，使用ping命令测试PC0与PC1见得连通性如下：

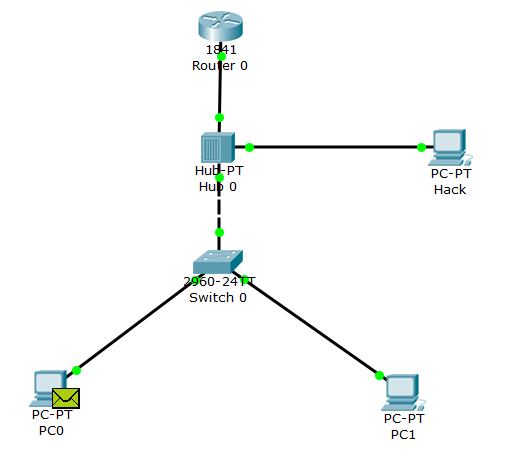
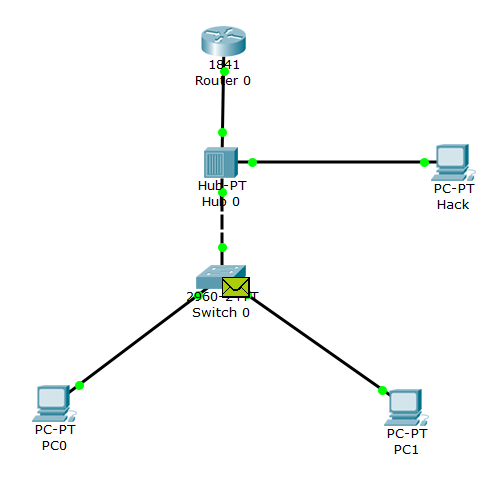
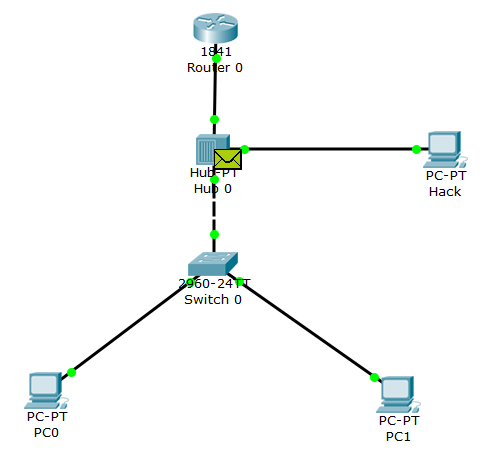


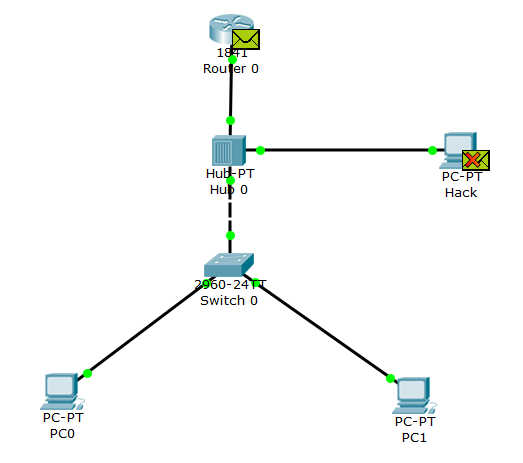
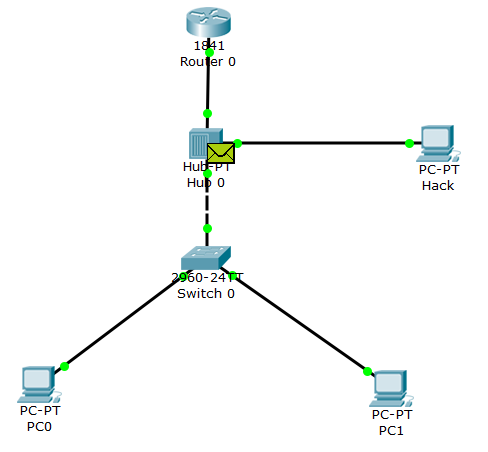
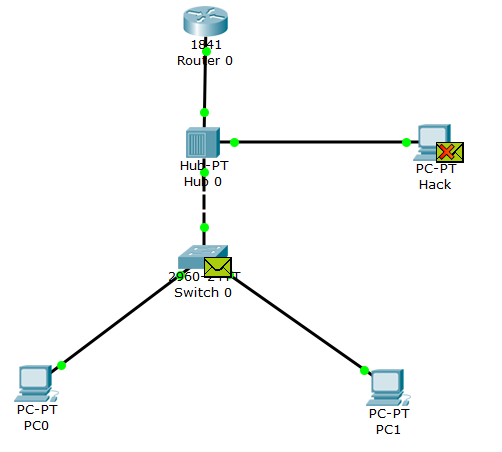
由图可知，PC0与PC1互通。

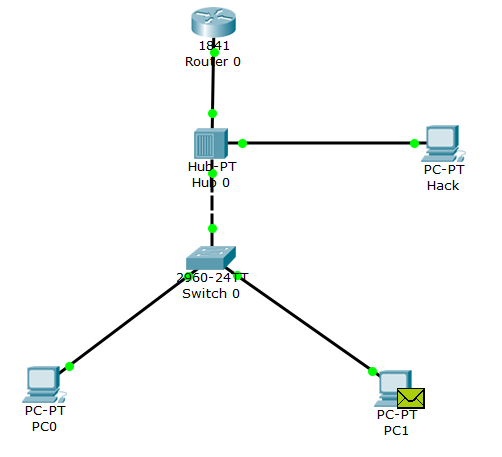
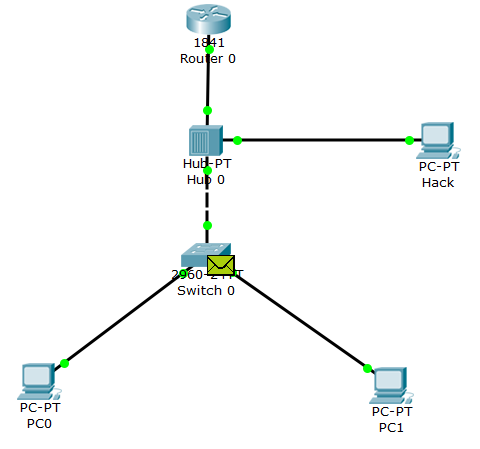
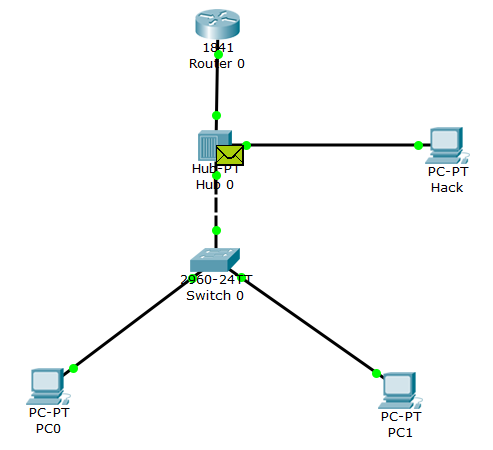
此时在交换机与路由器间加入一集线器，并将攻击者的主机连接到此集线器上，此时拓扑图如下：

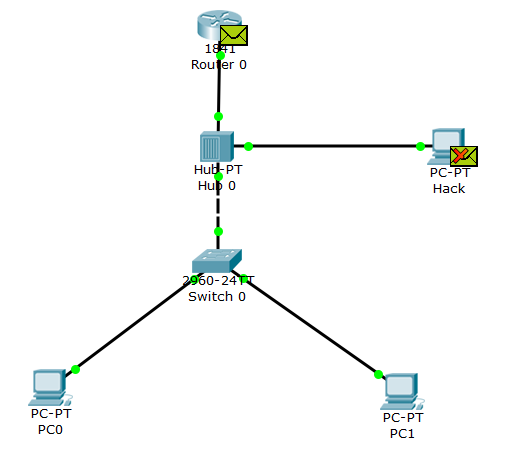
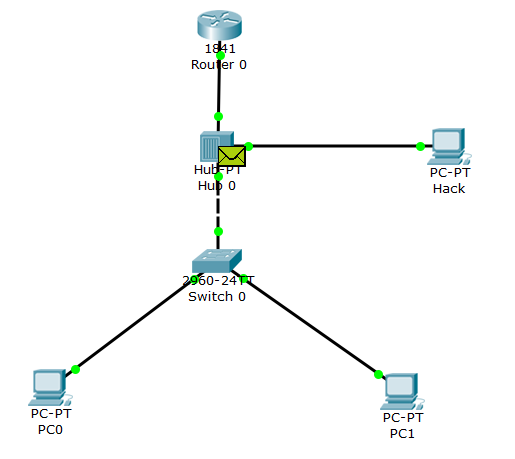
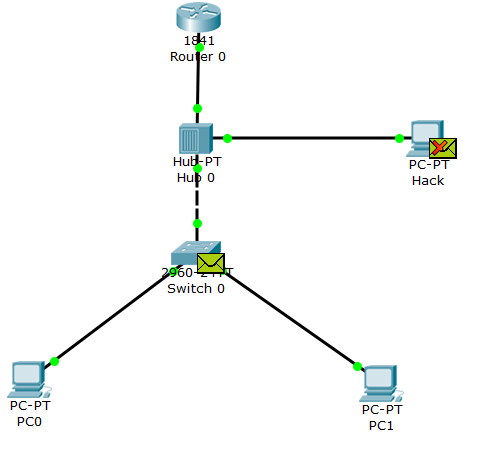


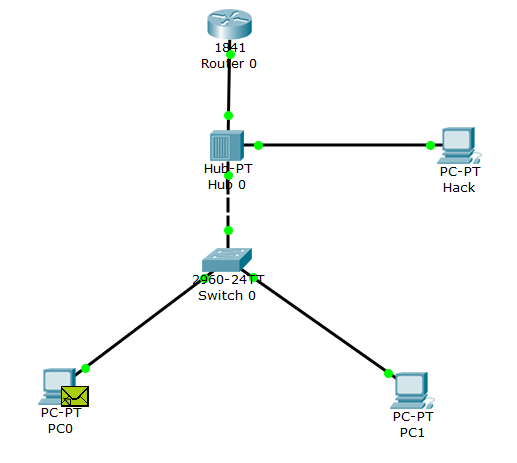
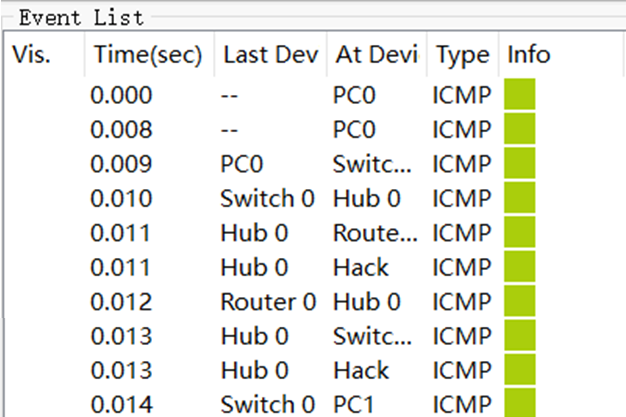
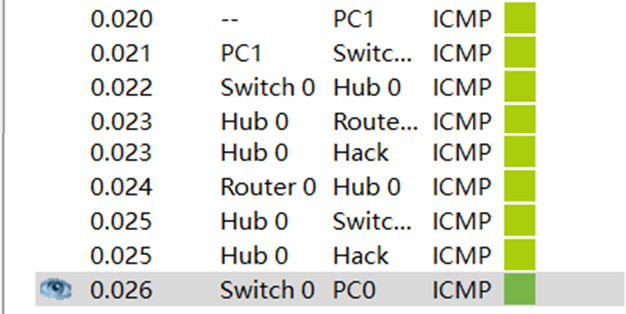
在完成如图的拓扑结构的搭建后，切换时模拟操作模式，添加PC0至PC1的简单PDU报文，选择仅查看ICMP报文，逐步查看报文的传输过程（来回）如下：

由报文的传输过程可知，该报文每次经过集线器时，都能够顺利到达攻击者的主机，并由攻击者正确接收，嗅探攻击成立。

并且，在整个从PC0到PC1再到PC0的报文发送再确认过程中，通信并没有受到影响，因此可以证明，嗅探攻击并不会影响正常的MAC帧传输过程。

除此之外，由上图可知，源端和目的端的每次报文交换，都要通过集线器，因此源端和目的端的报文也都要发送给Hack，因此嗅探攻击对于源和目的终端是透明的。

## 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？

实验搭建拓扑图时，应首先将路由器、交换机开机，在配置IP地址后，待端口对应指示灯变为绿色，才表示该端口已连接，否则这一端口为离线状态，数据包不会经此转发。

通过本次实验，我直观地认识到经集线器的嗅探攻击的过程，以及嗅探攻击透明的特点。更形象地认识到集线器在网络中的特点，当通过集线器进行嗅探攻击时，并不会影响到源终端与目的终端，使我在更深层次上理解了嗅探攻击的原理。

# 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

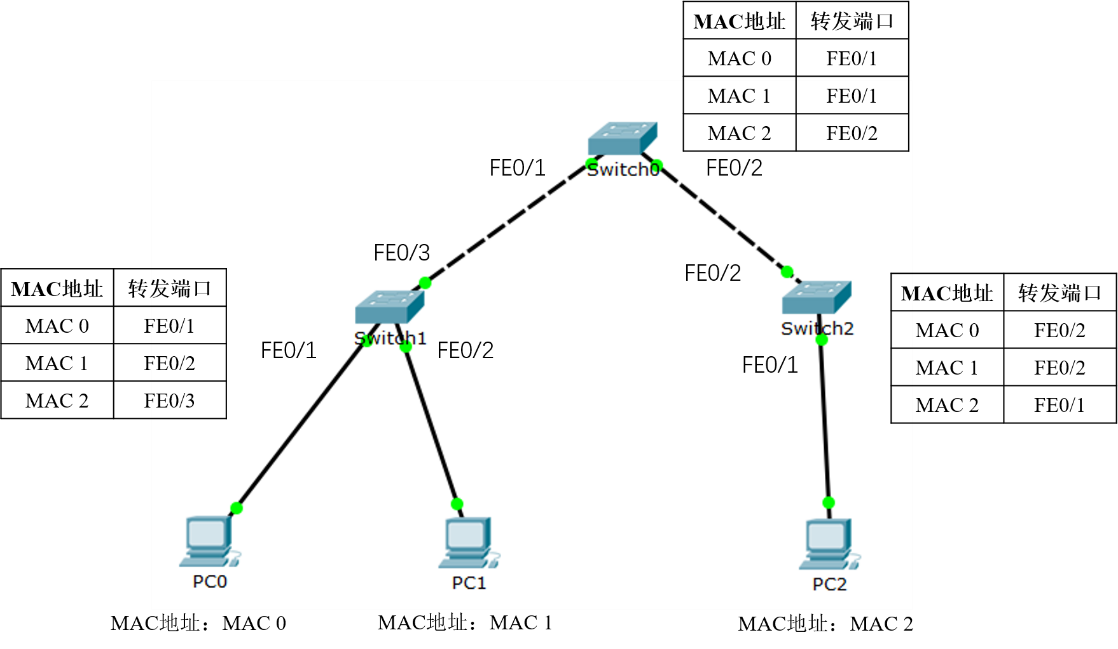
1. 使用自己的语言简述何谓MAC地址欺骗。

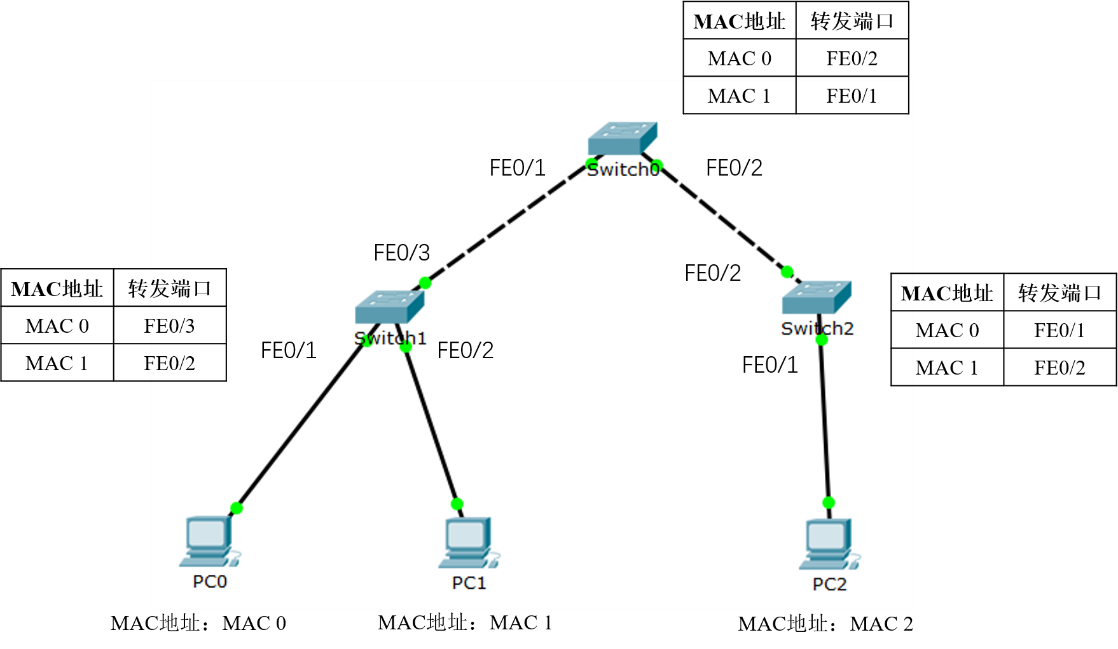
由于交换机转发表动态表项建立时的自学习特点，使得当攻击者将其主机的MAC地址修改为网络中其它设备的MAC地址后，使得原本应发送至原设备的数据包，均被转发至攻击者的主机。

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。

攻击者将其设备的MAC地址修改为网络中其它设备的MAC地址后，不断向网络中发送数据包，使得网络中交换机关于该MAC地址的转发表表项的转发端口均指向攻击者的主机，从而实现截获原本应发送至原设备的数据包。即攻击者主机2已知网络中主机0的MAC地址，将主机2的MAC地址改为主机0的MAC地址，并利用交换机交换表自学习特点，修改交换表。

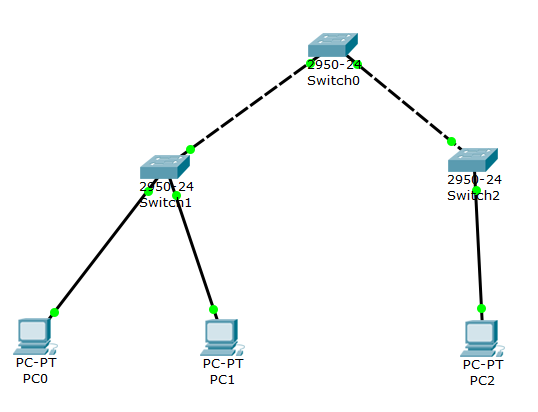
交换机的转发表如下：



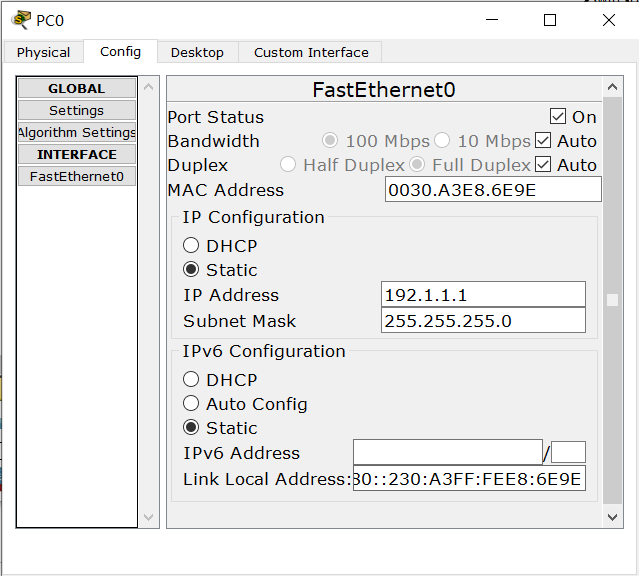
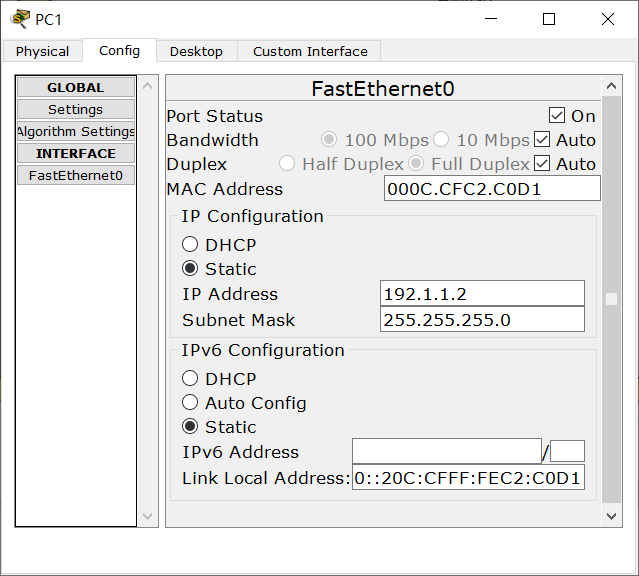


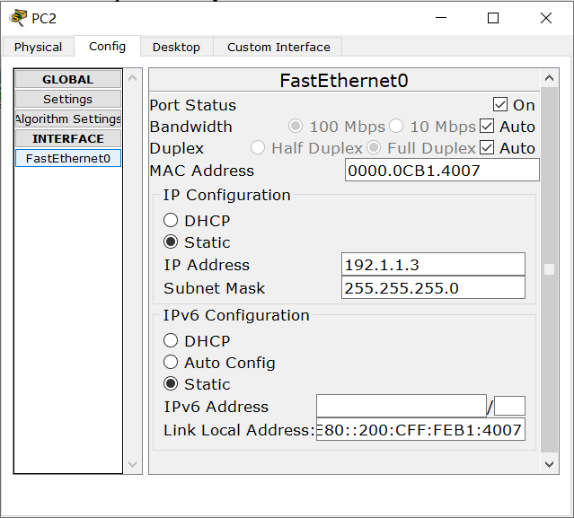
1. 实验步骤

首先展示实验所用的拓扑图：

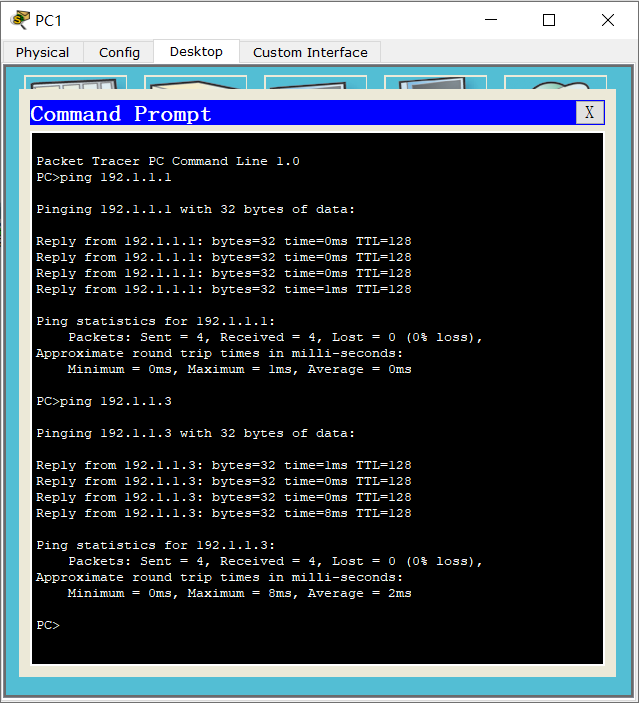
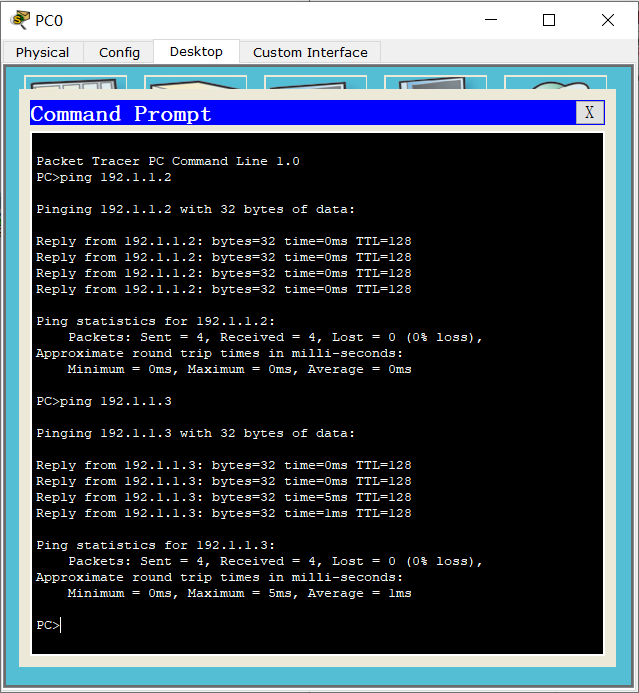


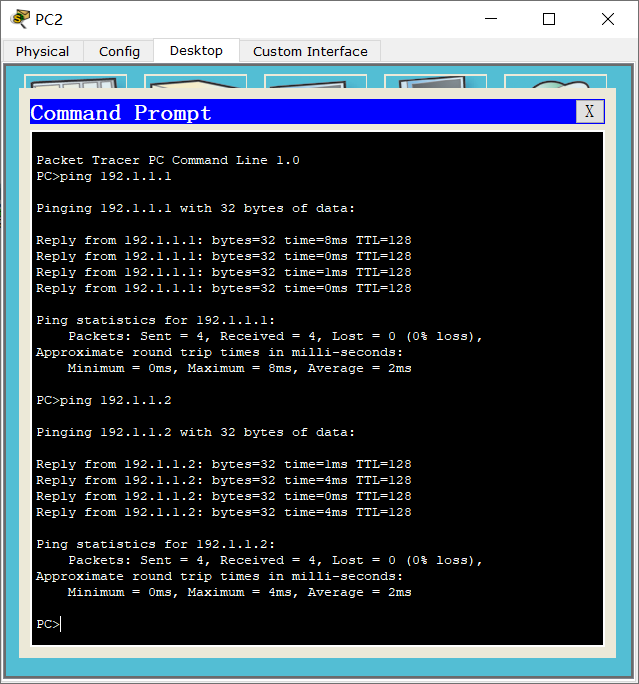
接着分别对PC0、PC1与PC2的IP地址与子网掩码进行配置：

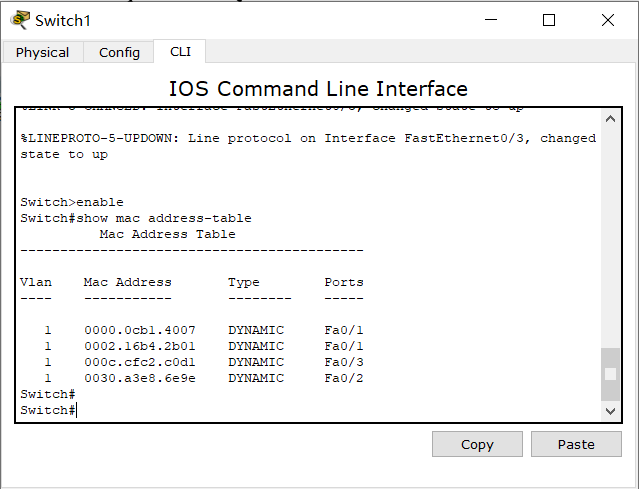
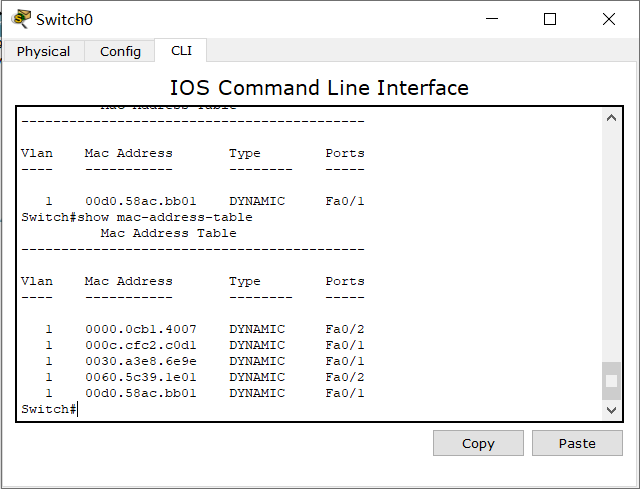


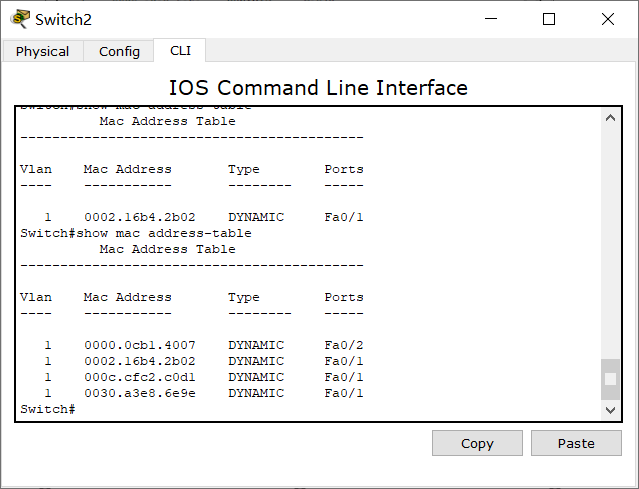
配置完毕后，在三台主机之间互相使用ping命令测试其连通性结果如下。由图可知，PC0、PC1、PC2三台主机亮亮互通.





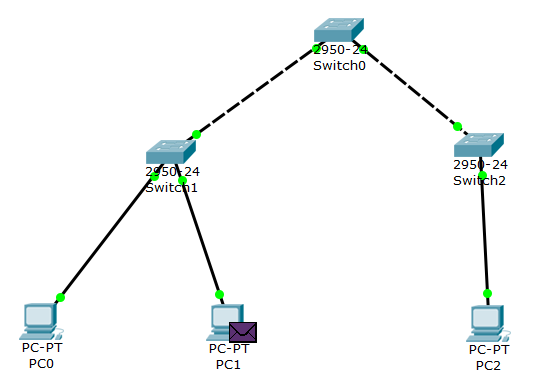
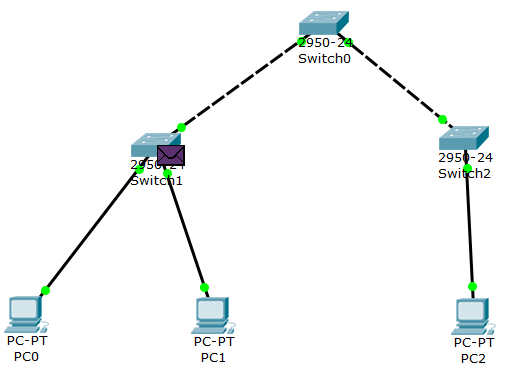
此时查看三台交换机的转发表：

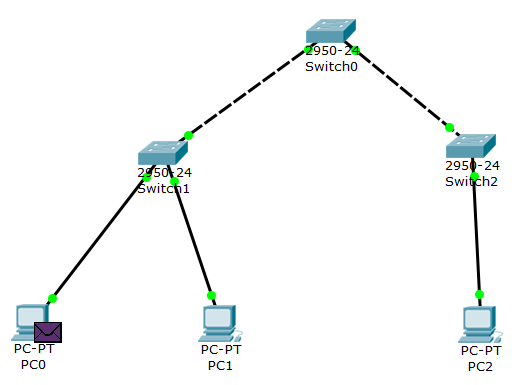
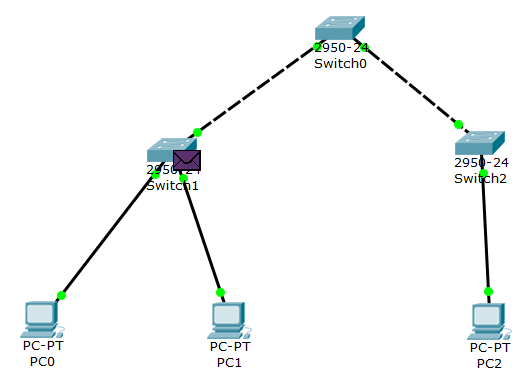


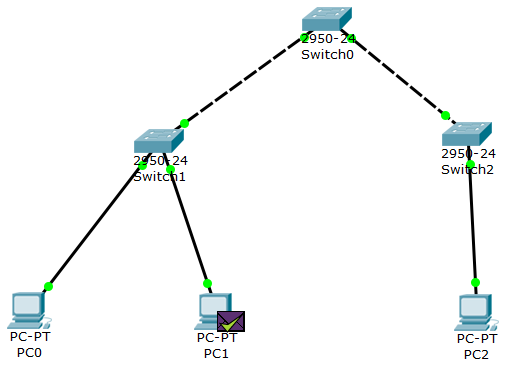
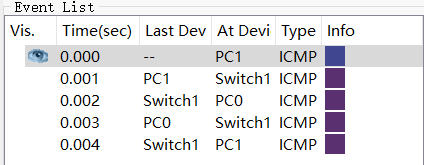


由各个交换机的交换表表项可知，对于PC0的MAC地址0030.A3E8.6E9E，Switch0通过FE0/2端口进行转发，Switch1通过FE0/2端口转发，Switch2通过FE0/1端口转发，此时各个转发表关于PC0的表项均正确指向PC0。

此时发送由PC1至PC0的简单PDU报文，发送路径如下：

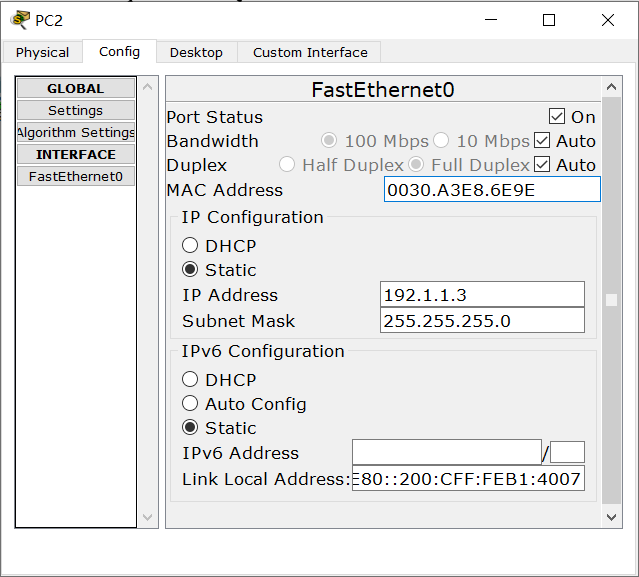
 

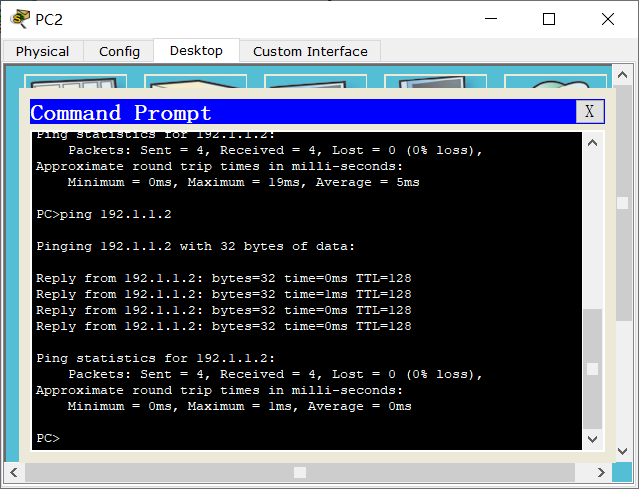
 

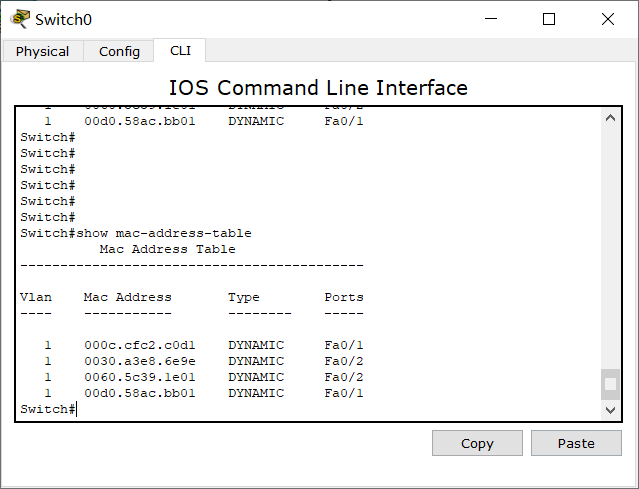
此时该报文仅会到达PC0，交换机并不向PC2转发该报文。

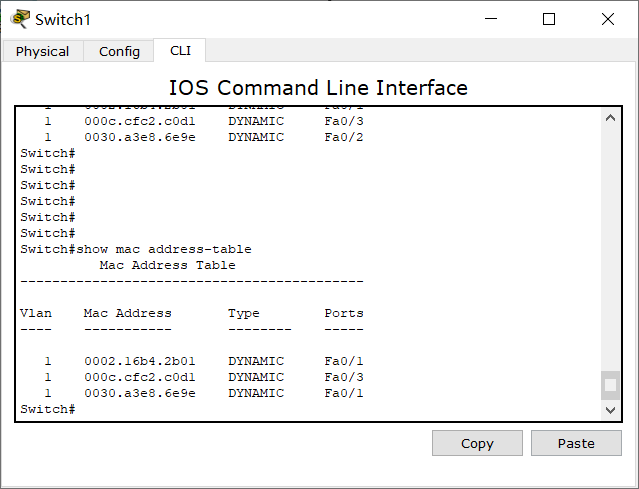
接着将PC2的MAC地址修改为PC0的MAC地址，并使PC2向PC1发送数据包（此处进行ping操作），使得交换机学习欺骗后的交换表。

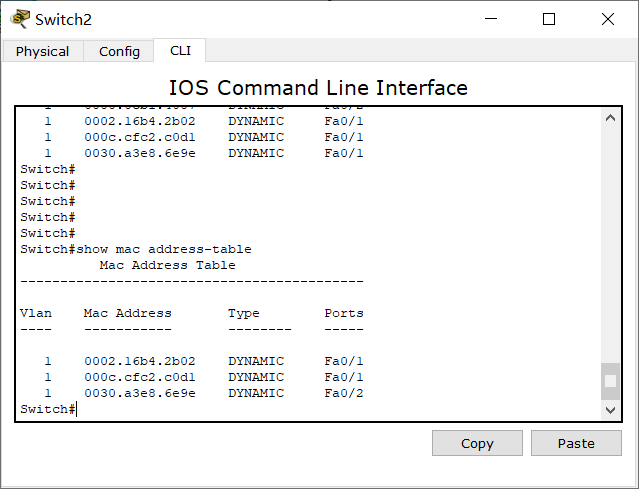




此时查看各个交换机的交换表如下：

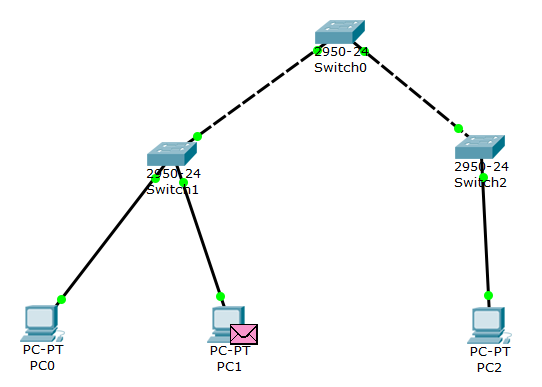
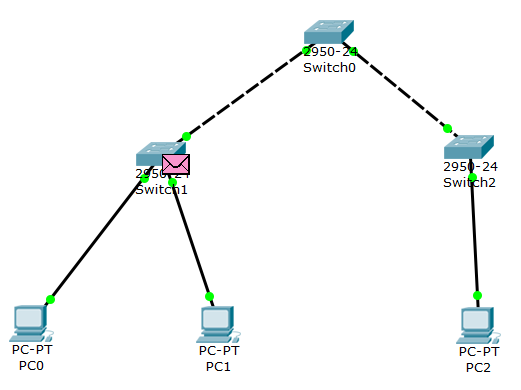


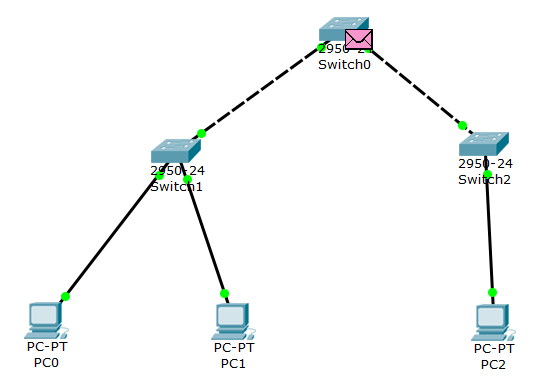
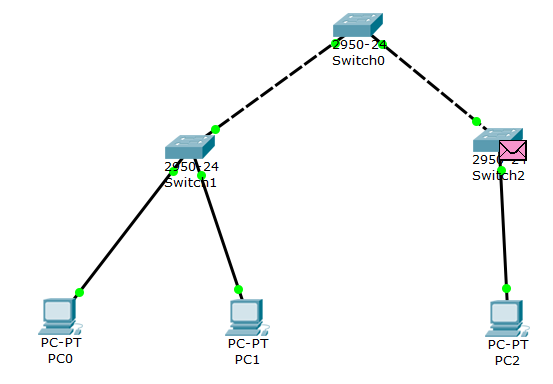


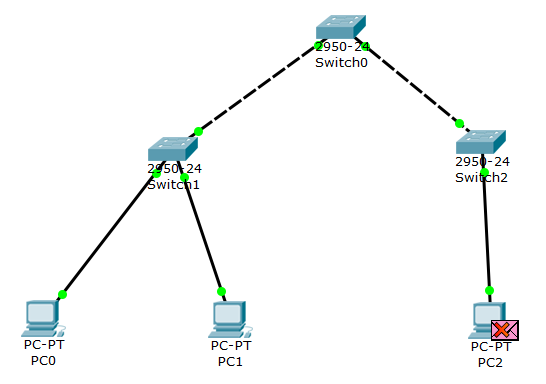
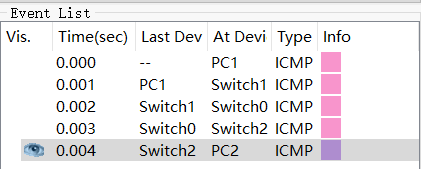


由交换表可知，在将PC2的MAC地址修改为PC0的MAC地址后，成功欺骗交换机修改其交换表，使得PC0的MAC地址的转发端口均指向PC2，即欺骗成功。

此时再次添加由PC1至PC0的简单PDU报文并跟踪如下：

此时报文不能正确转发至PC0，而是转发至PC2，证明PC2成功欺骗交换机。

## 三、思考与总结

1. PC0和PC2之间可以通信吗？为什么？

不可以。

PC2向PC0发送数据包时，交换机Switch2接收到发送的数据包，并根据数据包的源MAC地址更改转发表，此时该MAC地址对应的转发端口与进入端口相同，因此这个数据包被丢弃，无法到达PC0。

PC0向PC2发送数据包时，首先会通过ARP协议解析目的IP对应的MAC地址，ARP请求到达PC2后，PC2返回包含目的IP对应的MAC地址的数据包，交换机Switch2接收到此数据包时，根据数据包的源MAC地址更改转发表，此时该MAC地址对应的转发端口与进入端口相同，因此这个数据包被丢弃，PC0无法通过ARP请求到目的IP对应的MAC地址，因此PC0无法向PC2发送数据包。

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？

将PC2的MAC地址修改为PC0的MAC地址后，应使PC2向PC1发送一数据包。由于路由器关于三台主机的转发表均为动态建立，此时交换机的转发表才能将PC0的MAC地址对应的转发端口修改为指向PC2的端口，否则转发表不会修改，现象与欺骗前一致。

通过本次实验，我进一步加深了交换机转发表建立的过程，以及数据发送过程中ARP协议的流程，更形象的认识到交换机转发数据包的方法，并以此为基础，从更深层次上理解了MAC地址欺骗的背景及原因，通过操作对MAC地址欺骗有了基本的掌握。

# 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

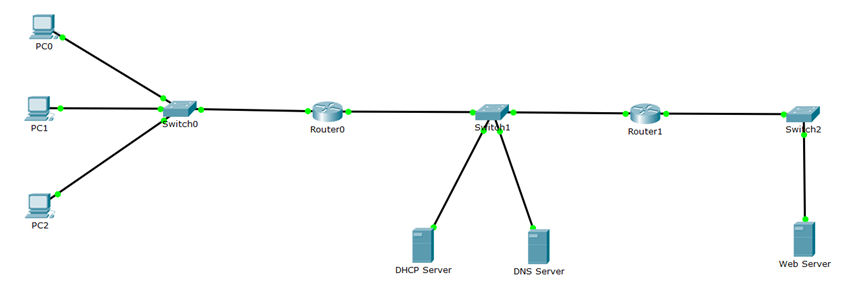
钓鱼网站首先通过伪造DHCP服务器修改主机的网络信息，将主机的DNS服务器地址修改为伪造DNS服务器的IP地址，在伪造的DNS服务器中，DNS服务将希望钓鱼的网站域名解析为伪造Web服务器的IP地址，从而使得用户尝试访问该网站时，解析到错误的IP地址，被引导访问伪造Web服务器，访问钓鱼网站。

1. 使用自己的语言简述本实验原理

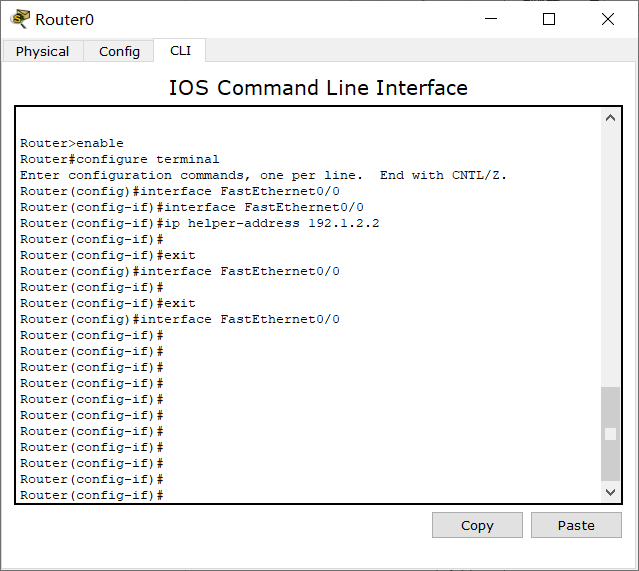
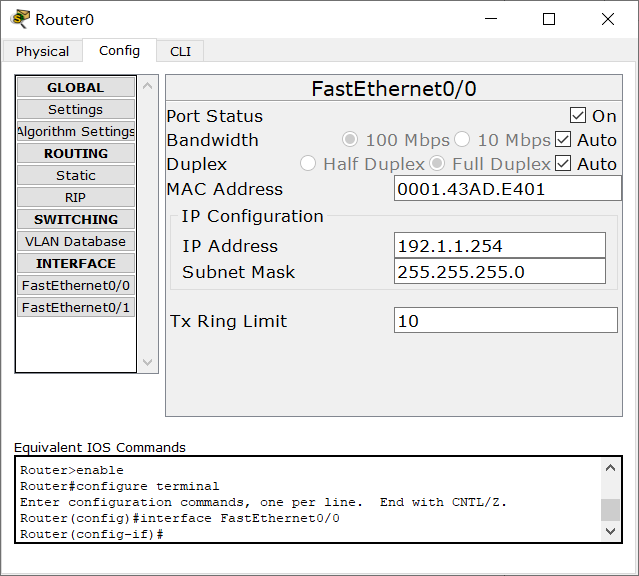
网络中DHCP服务可以为网络中主机分配IP地址、默认网关、DNS服务器地址等内容，而DNS服务可以将域名解析为对应IP地址。攻击者可以伪造一台DHCP服务器，使得通过DHCP服务获取网络信息的主机获取到错误的网络信息，特别是伪造的DNS服务器地址，此时攻击者在DNS服务器上的DNS服务中，将期望钓鱼的域名解析为伪造Web服务器的IP地址，进而使得用户在访问该域名时，错误的访问伪造Web服务器的钓鱼页面。

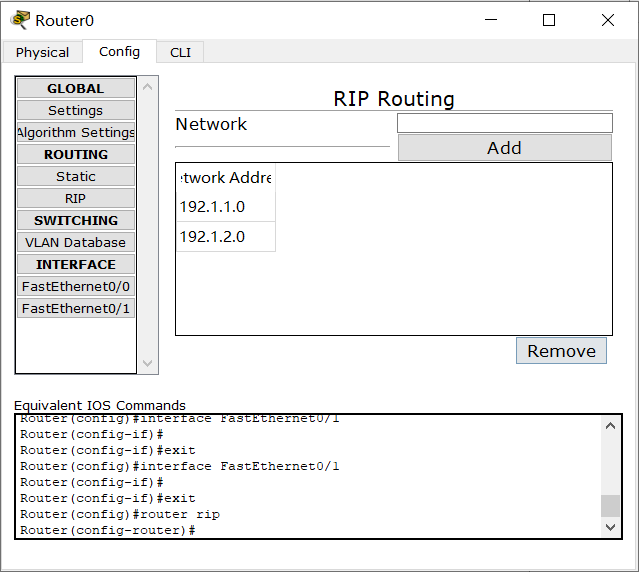
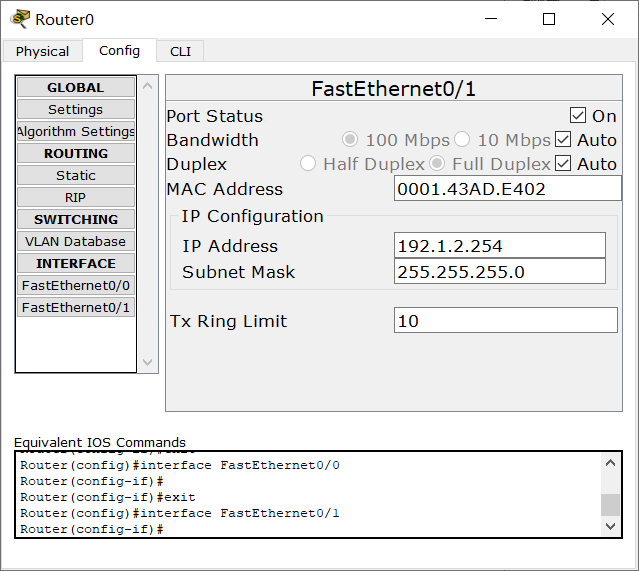
1. 实验步骤

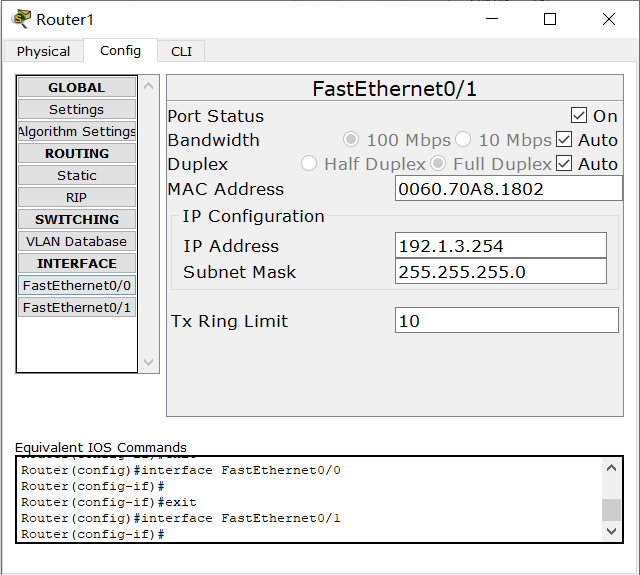
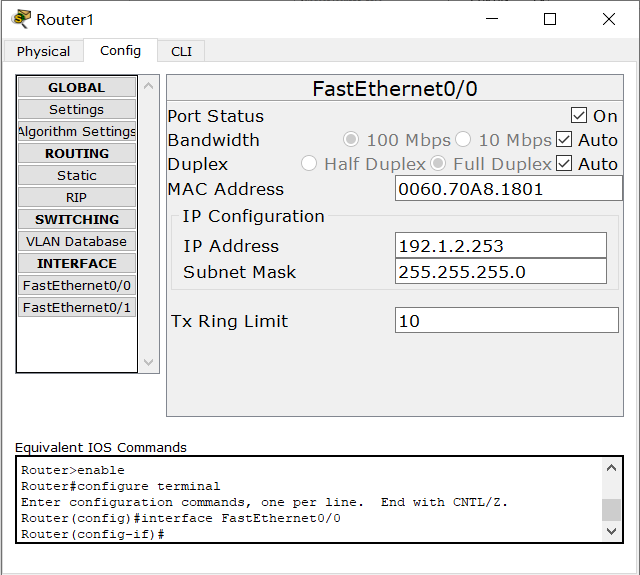
首先连接如图所示的拓扑结构：

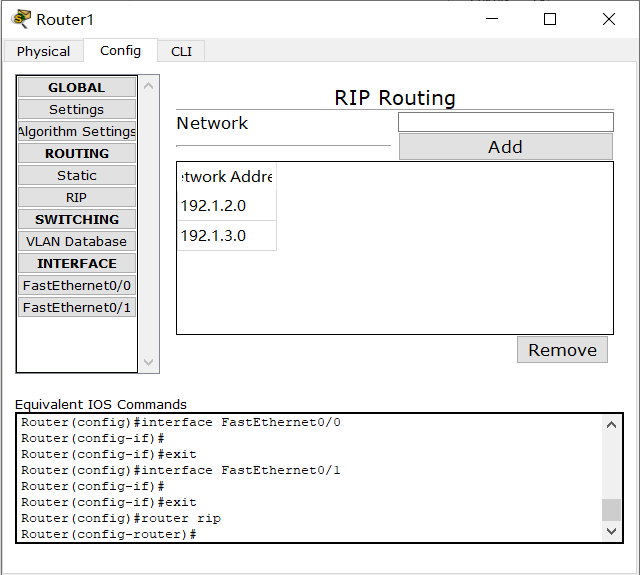


接着在Router0与Router1上分别开启与相邻交换机连接的端口，并配置端口的IP地址与子网掩码，配置完毕后将与其相邻的网络路由添加至RIP协议设置中，并在Router0的FE0/0端口配置中继地址，结果如下：

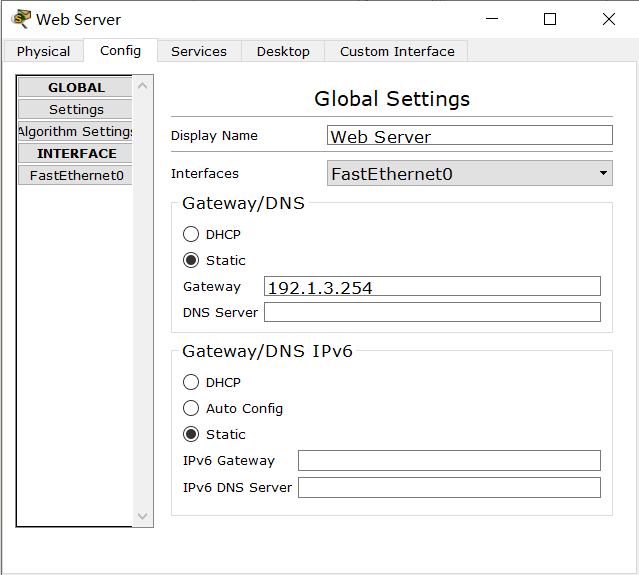
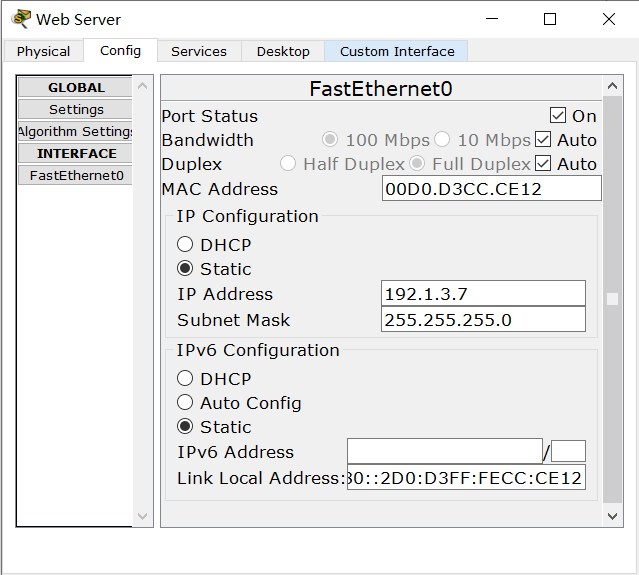


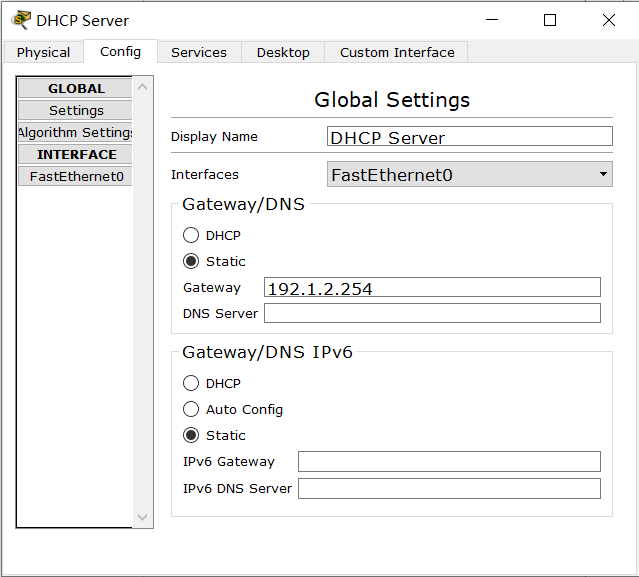
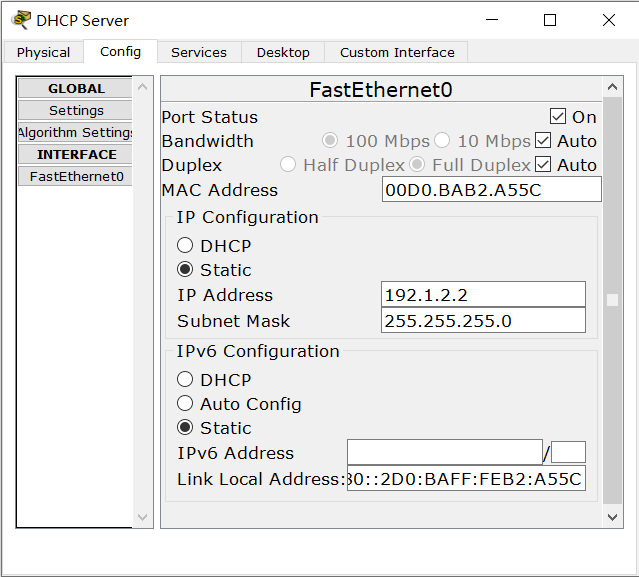


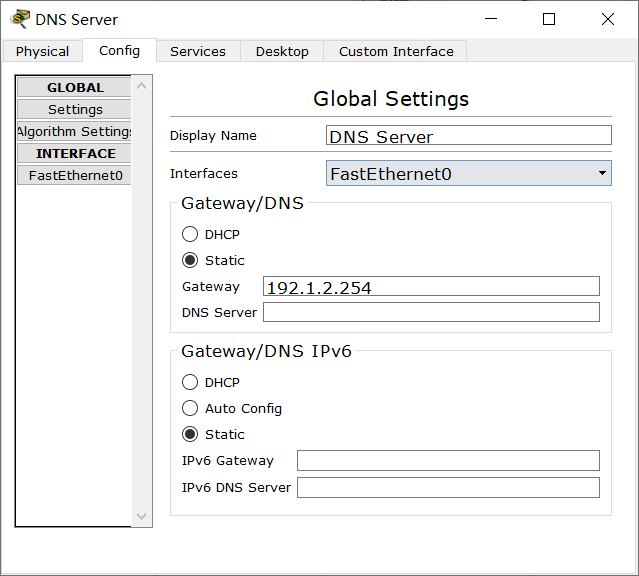
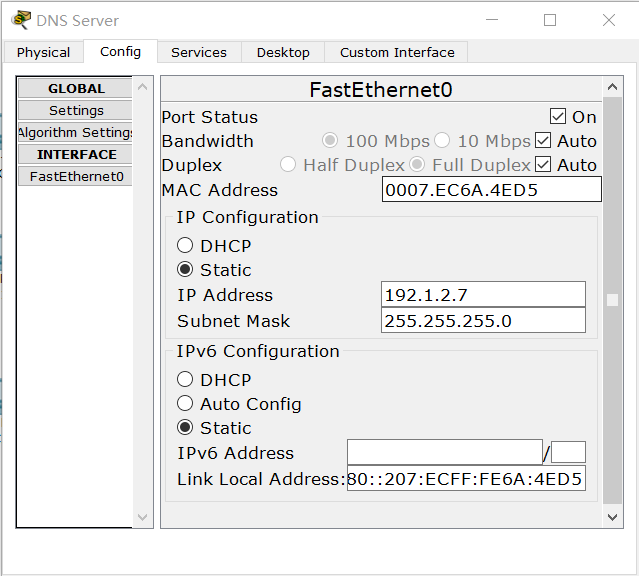




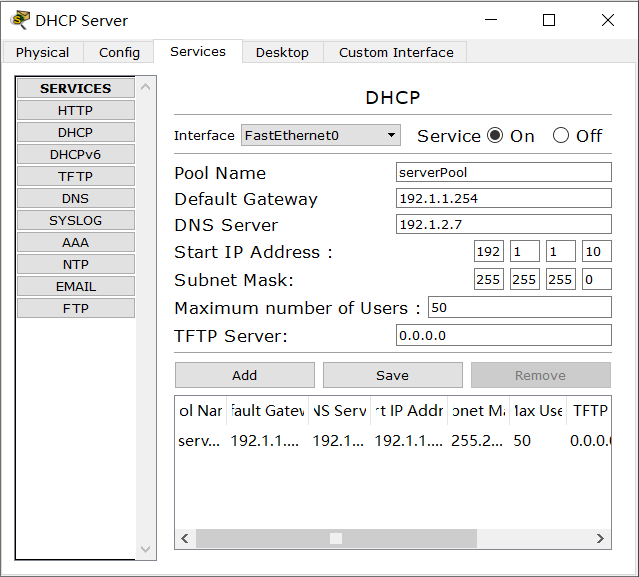
此后分别配置Web服务器、DHCP服务器、DNS服务器的IP地址、子网掩码、默认网关如下：



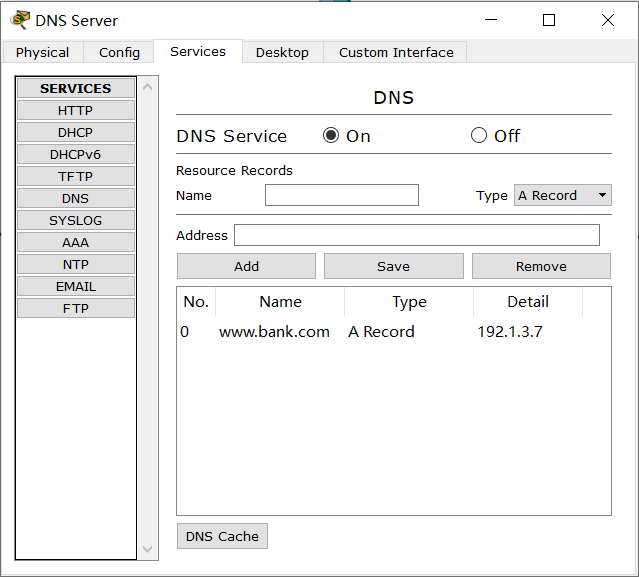




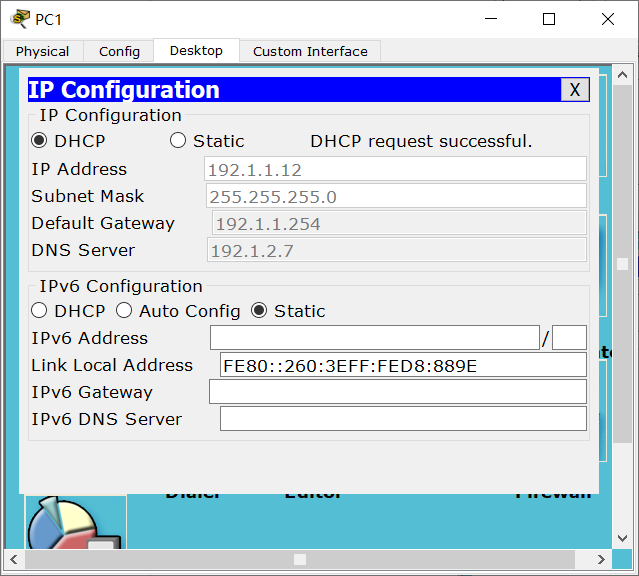
完成上述配置后，进行DHCP服务器的DHCP服务的配置。进入服务选项卡的DHCP选项，开启DHCP服务，设置服务所使用的默认网关与DNS服务器的IP地址，输入IP池的起始地址为192.1.1.10，最大用户数为50，点击保存即可完成该地址池的DHCP服务配置。



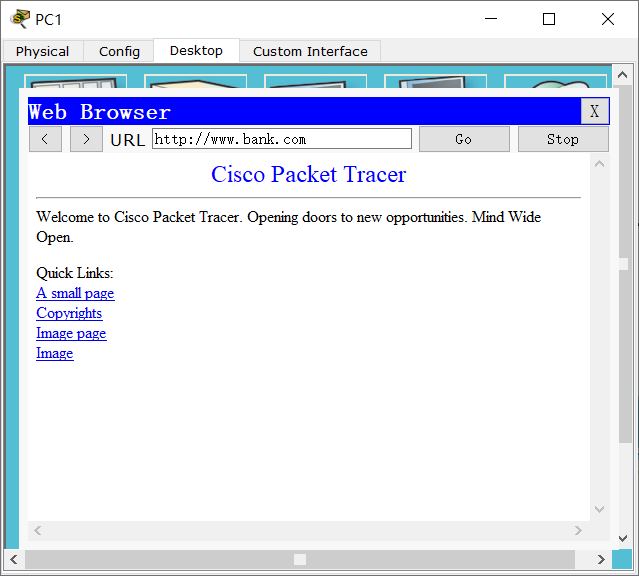
接着配置DNS服务器的DNS解析服务。首先开启DNS服务，在名称中输入域名www.bank.com，类型选择为A Record，在地址栏中输入其Web服务器的IP地址192.1.3.7，点击添加即可完成对该域名的DNS服务配置。



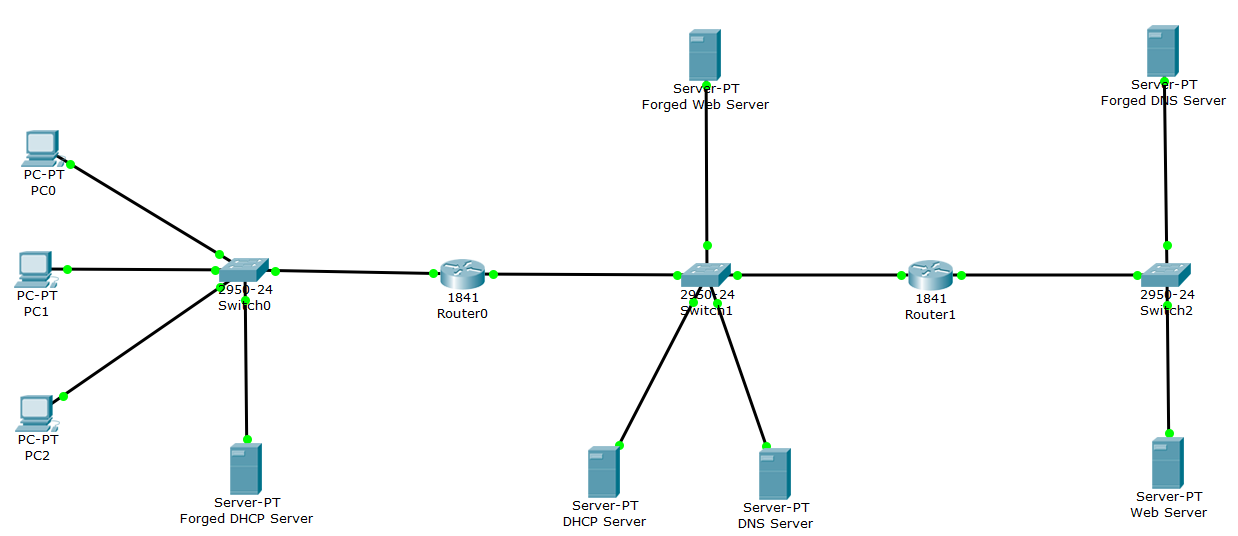
完成配置后，开启PC1的DHCP服务，此时可以看到已经通过DHCP服务器完成IP地址、默认网关与DNS服务器的获取，且IP地址为地址池中首个未分配的地址，默认网关与DNS服务器地址与设置相同。



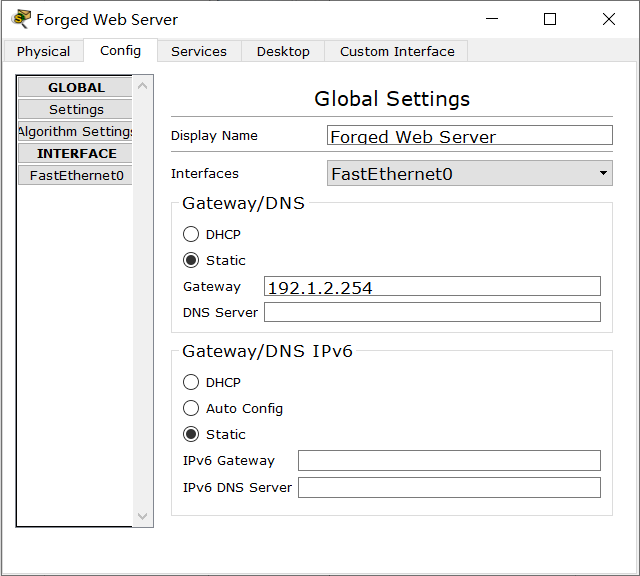
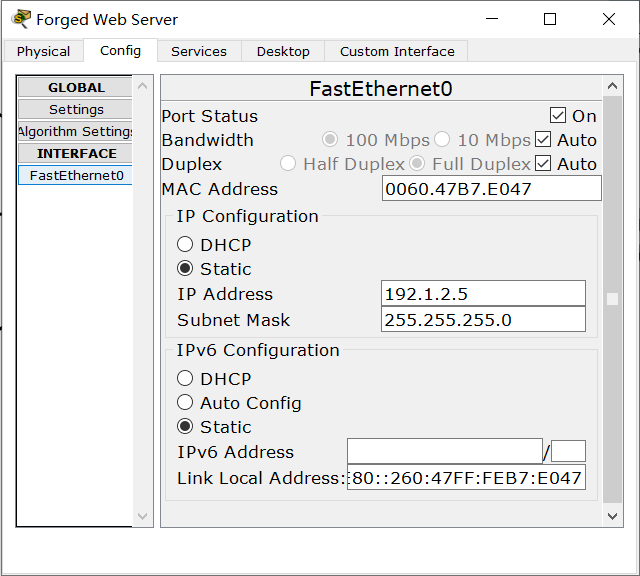
之后点击桌面选项卡，打开浏览器并输入www.bank.com，点击前往即可成功访问域名对应的Web服务器。

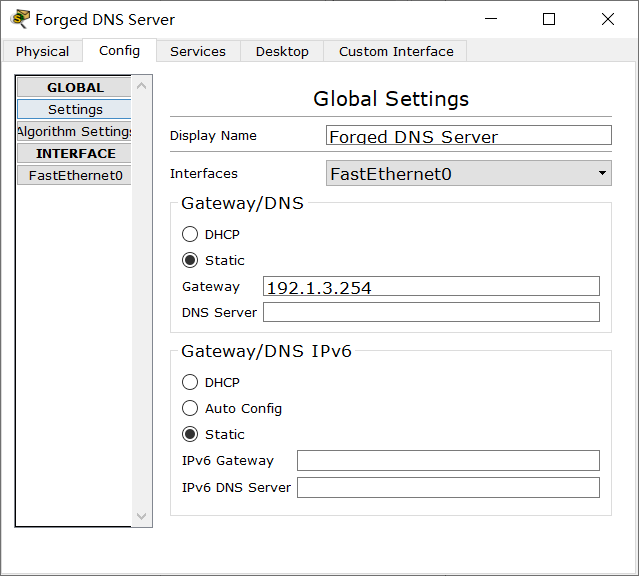
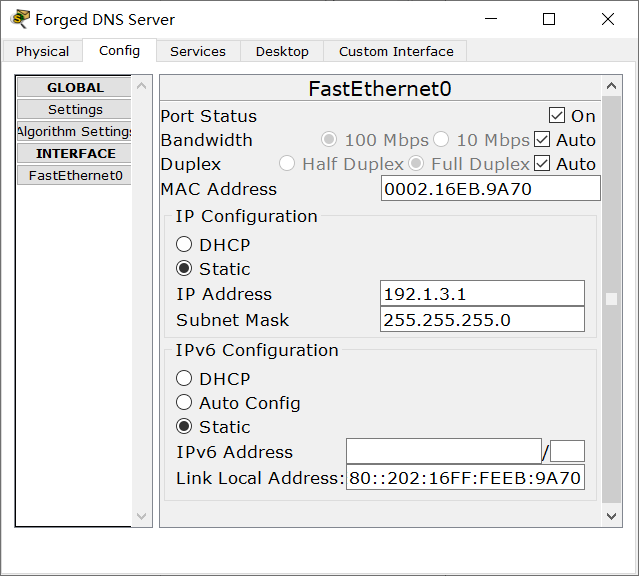


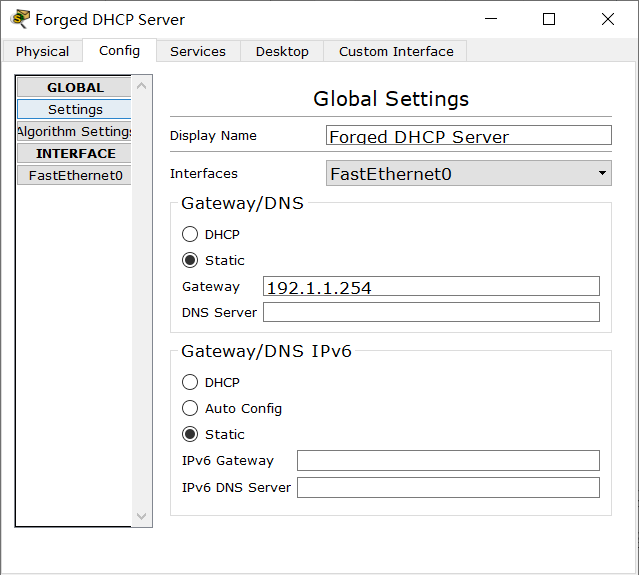
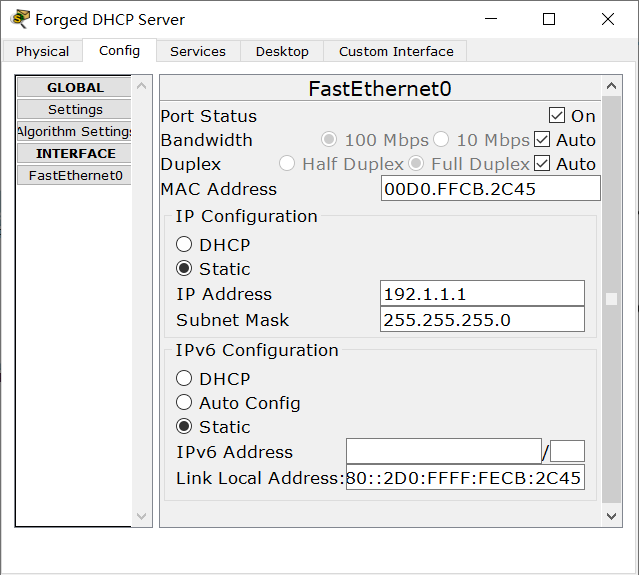
此时加入三台伪造的服务器，网络拓扑结构如下：

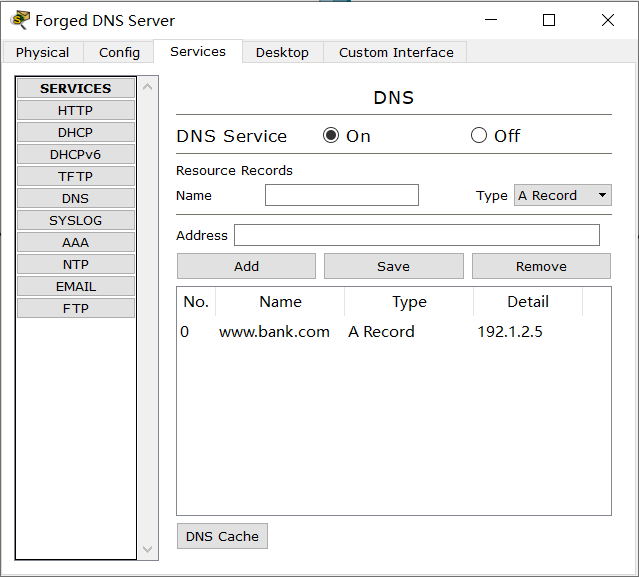
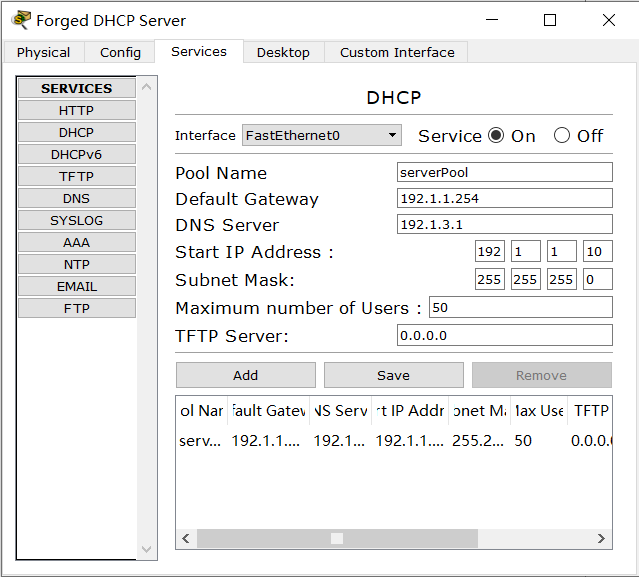


重复上述服务器IP地址、子网掩码、默认网关与DHCP服务器中DHCP服务、DNS服务器DNS解析服务的配置。

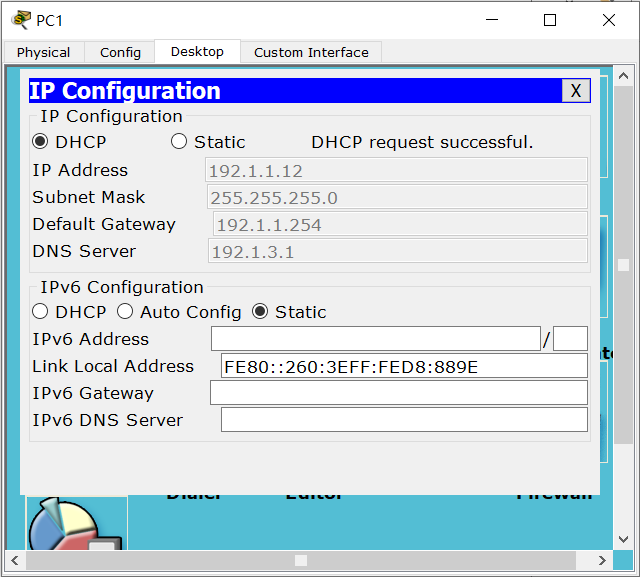






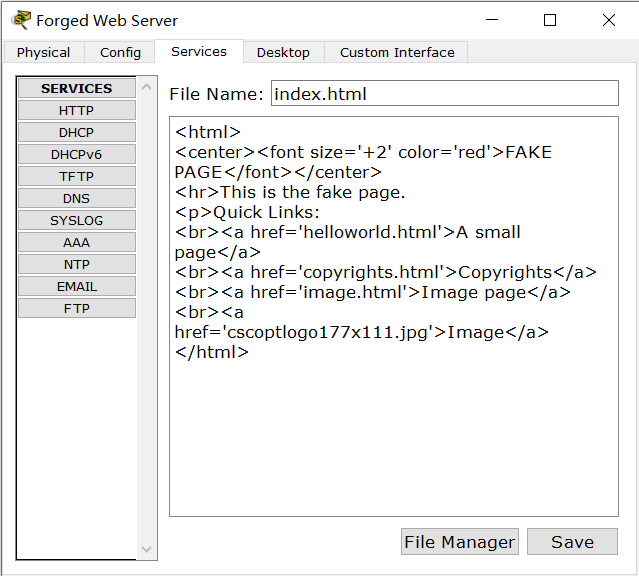


配置完毕后重新使PC1获取网络信息，结果如下：

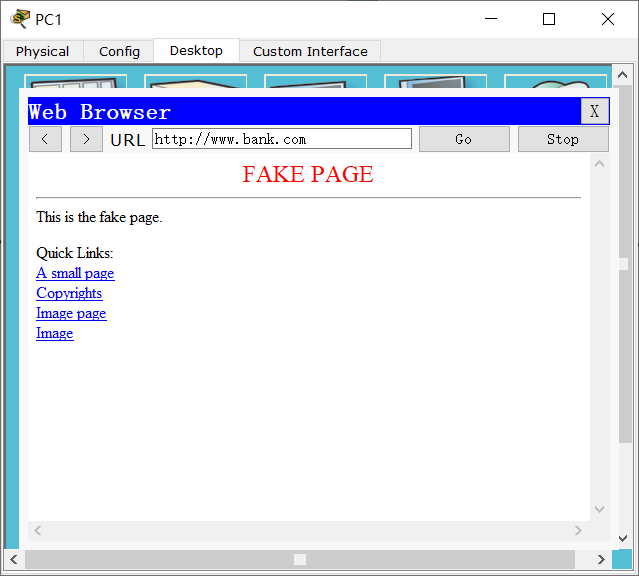


此时PC1的网络配置已被更改为伪造服务器配置信息，即此时PC1已从伪造DHCP服务器中获取网络信息。

修改伪造Web服务器的默认网页，实现与正常网页的区分：



此时再使用PC1打开www.bank.com，即可发现此时访问的页面为钓鱼页面，即PC1此时访问伪造的Web服务器。



## 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？

当主机使用DHCP服务获取网络信息时，首先在广播域内广播寻找DHCP服务器，若寻找不到，则通过路由器的中继端口进行寻找。由于正常的DHCP服务器与主机不在同一个广播域当中，而伪造的DHCP服务器与主机处于同一广播域，因此主机使用DHCP服务获取网络信息时，首先会获取到由伪造的DHCP服务器发送地配置信息，进而实现攻击。

若将伪造的DHCP服务器连接至192.1.3.0/24网段中，不会起到攻击作用。因为与该网段相连的路由器Router1并未配置中继功能，DHCP请求并不会到达该伪造服务器。

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？

在观察主机通过DHCP获取的网络信息前，应将所有主机的IP地址信息置位静态状态，待DHCP服务配置完毕后，再打开一台主机的DHCP服务，此时才能够观察到DHCP分配IP地址是从低地址开始分配的现象。

通过本次实验，我对DHCP服务与DNS解析服务有了更深的理解，同时通过操作，切实理解到钓鱼网站的具体工作原理，即通过伪造的DHCP服务器获取IP地址与伪造DNS服务器，此后在通过DNS服务解析企图钓鱼的网站时，即可解析至伪造的IP地址，进而使得用户访问伪造的Web服务器，实施钓鱼攻击。