《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： | 李泽昊 | 学号： | 20191060065 |
| 姓名： | 白文强 | 学号： | 20191060064 |
| 姓名： | 赵浩杰 | 学号： | 20191060074 |

|  |  |
| --- | --- |
| 实验时间： | 2021年10月15日 |

|  |  |
| --- | --- |
| 实验名称： | RIP路由项欺骗攻击实验和钓鱼网站实验 |

|  |  |
| --- | --- |
| 实验成绩： |  |

RIP路由项欺骗攻击实验

一、实验目的

(1)验证路由器RIP配置过程。

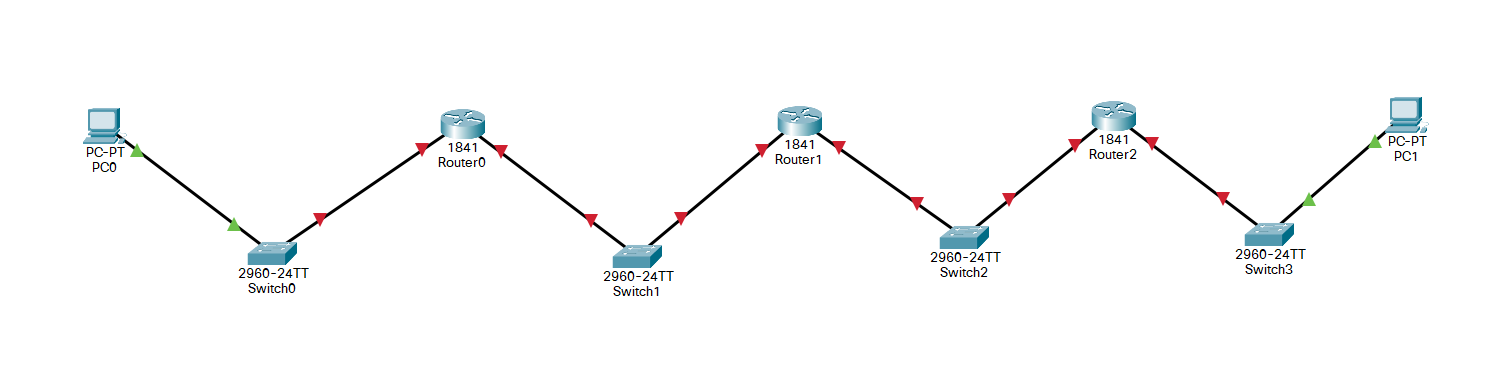
(2)验证RIP生成动态路由项的过程。

(3)验证RIP的安全缺陷。

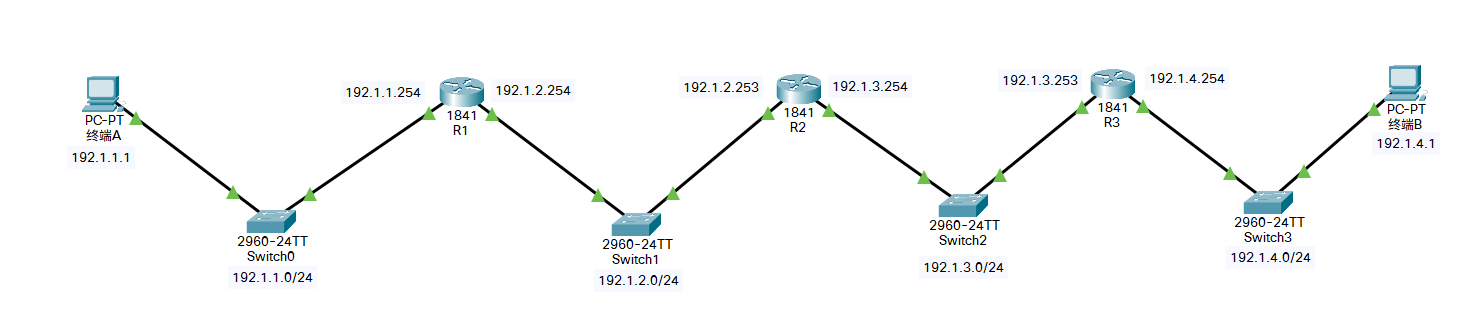
(4)验证利用RIP实施路由项欺骗攻击的过程。

二、实验步骤

(1)完成去掉入侵路由器后的设备放置

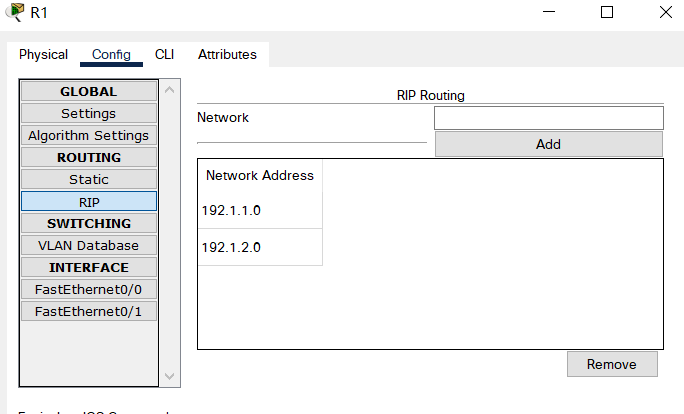


(2) 配置各个设备的IP地址和子网掩码

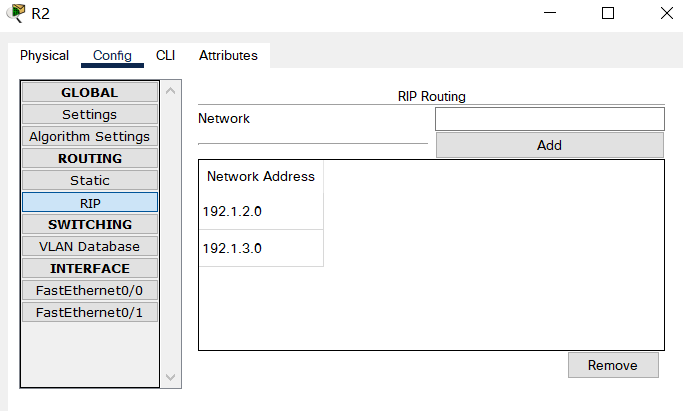


(3)完成路由器RIP协议配置

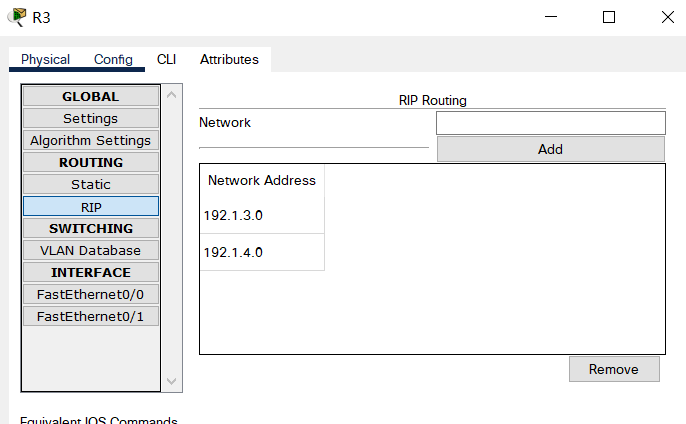
R1:



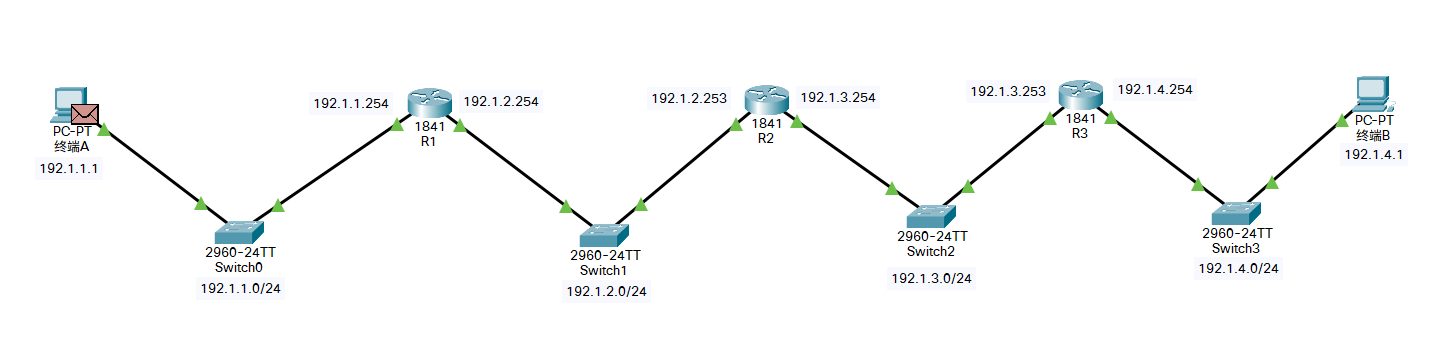
R2:

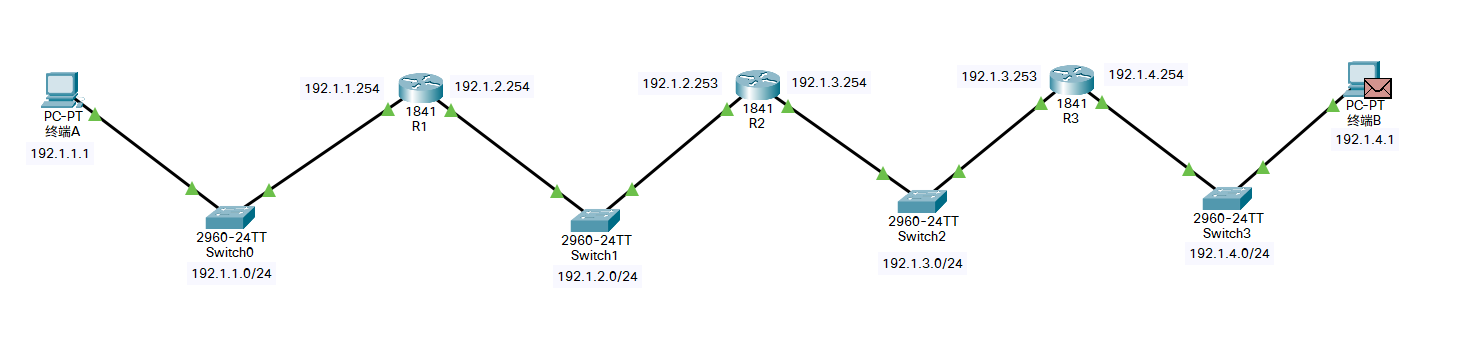


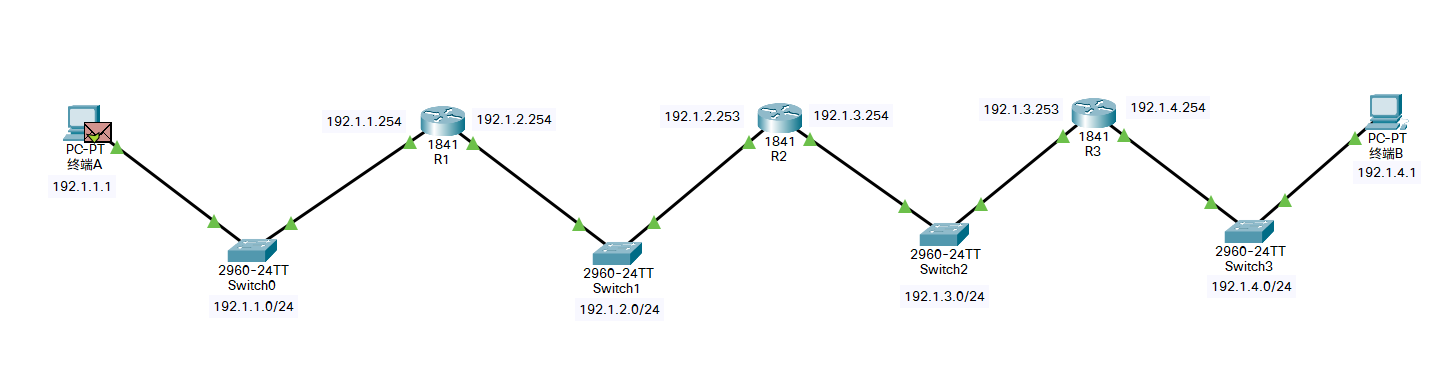
R3：



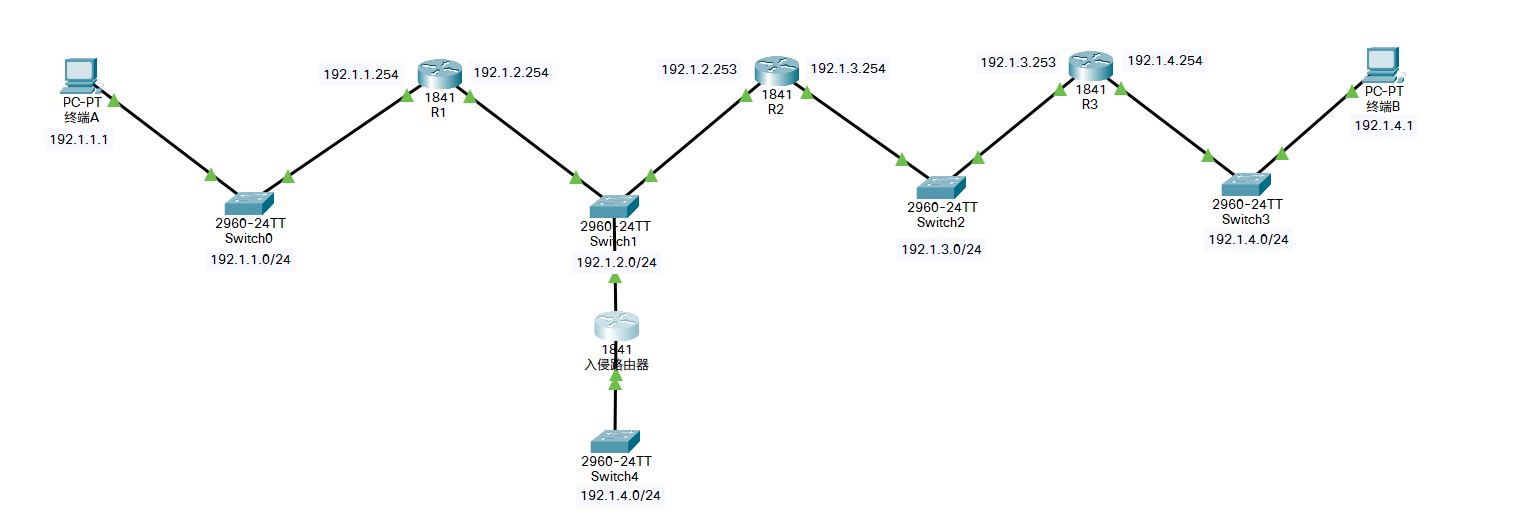
(4)通过启动PC0与PC1之间的报文传输过程验证PC0与PC1之间存在IP传输路径。



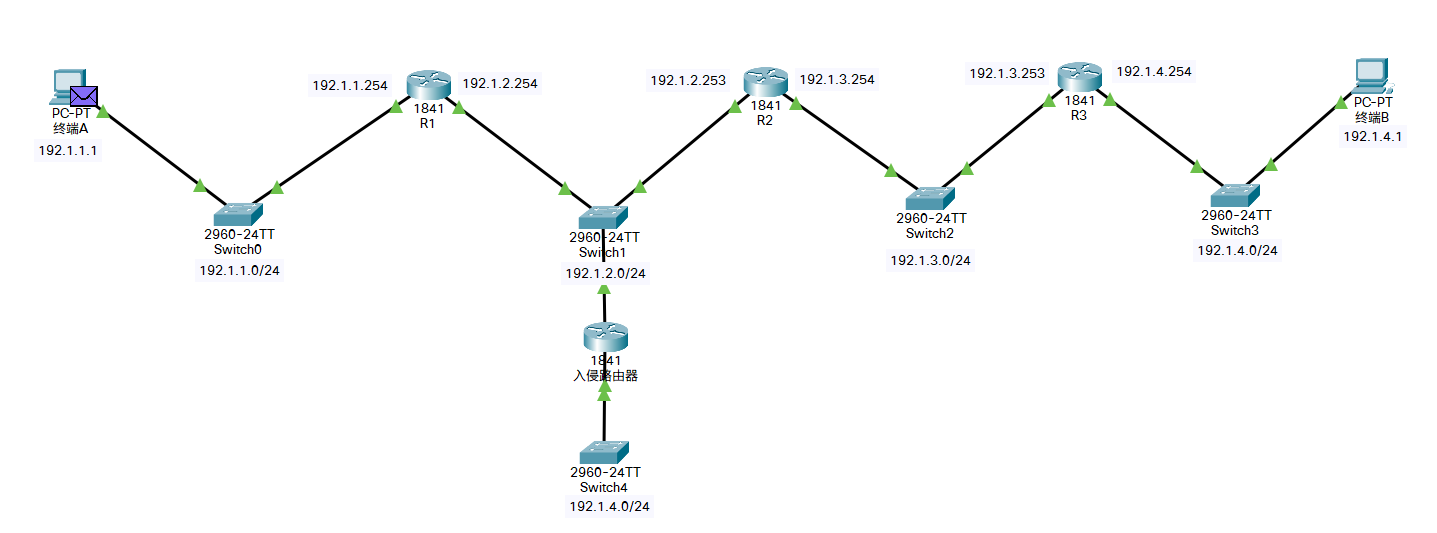


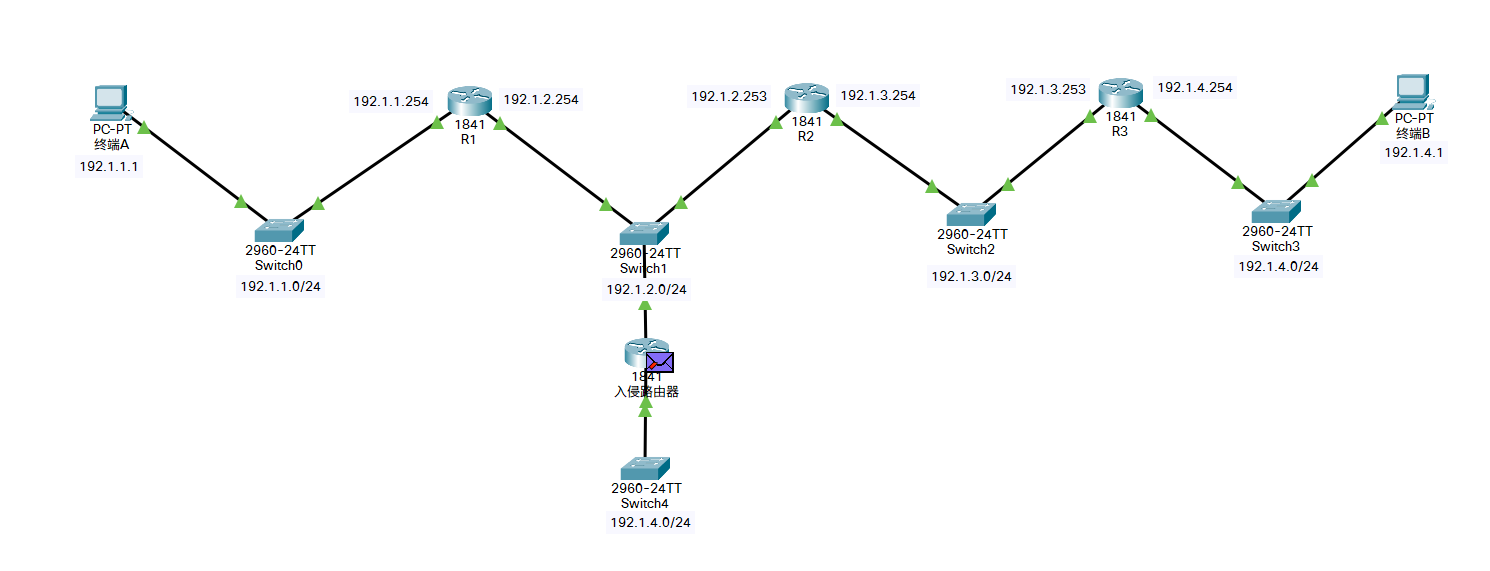


(5)用路由器Router作为入侵路由器进行入侵



(6)切换到模拟操作模式，启动PC0至PC1的IP分组传输过程，发现IP分组无法到达PC1





三、实验结果及分析

一开始在没有加入入侵路由器之前，配置好各个设备的IP地址后，PC0与PC1也就是终端A与终端B之间是可以进行正常通信的，因为三个路由器都配置好了RIP协议，保证网络通信的正常。

在加入入侵路由器之后，配置路由器IP协议，一端为192.1.2.0的子网，另一端为192.1.4.0的子网，也就是模拟PC1的子网，通过误导R0的RIP协议信息，从而使得PC0发往PC1的IP分组转发往入侵路由器。

四、实验总结及体会

如果想要对处在不同子网下的设备进行攻击，我们可以采用RIP协议欺骗的方法，通过设置入侵路由器，一端连接正常子网，另一端连接欺骗子网，欺骗子网需要设置为目的IP地址所在的子网，通过RIP协议自动配置所发的路由消息，误导其他路由器，从而将发往目的IP地址的截获下来，转发给入侵路由器。

钓鱼网站实验

一、实验目的

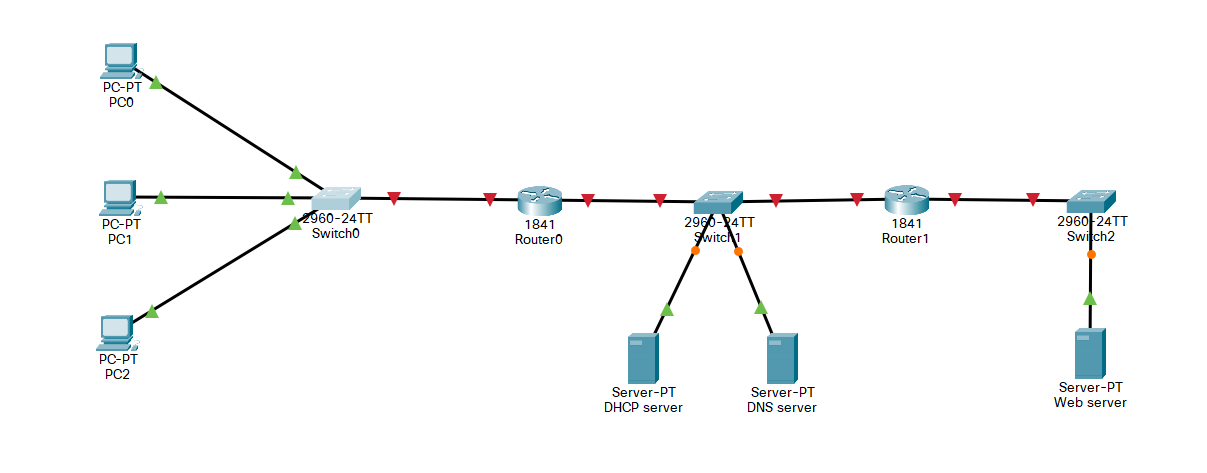
(1)验证伪造的DHCP服务器为终端提供网络信息配置服务的过程。

(2)验证错误的本地域名服务器地址造成的后果。

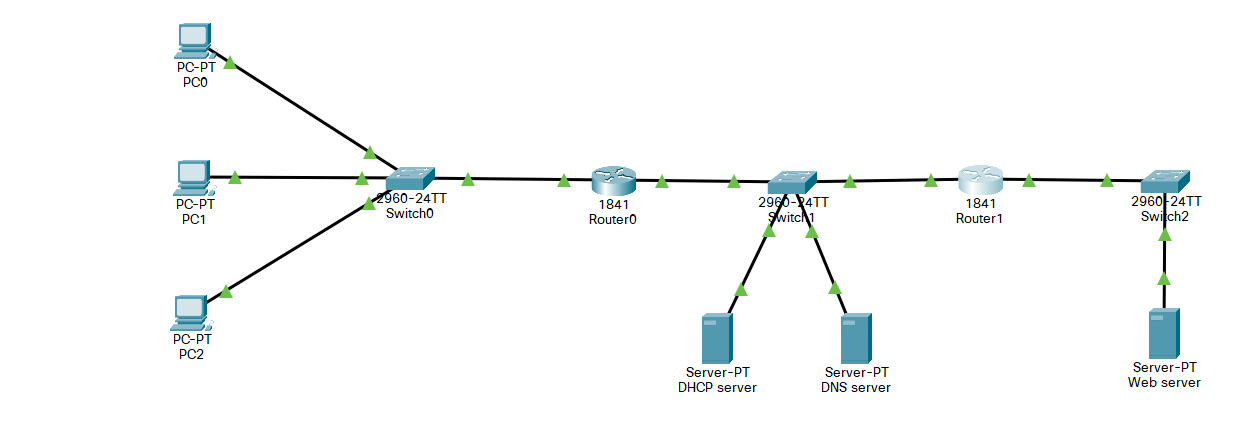
(3)验证利用网络实施钓鱼网站的过程。

二、实验步骤

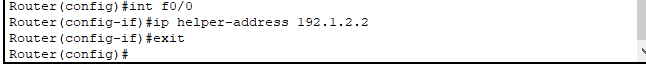
(1)实现正常的Web服务器访问过程，完成设备的放置和连接。



(2)完成路由器接口IP、子网掩码配置，完成RIP配置过程

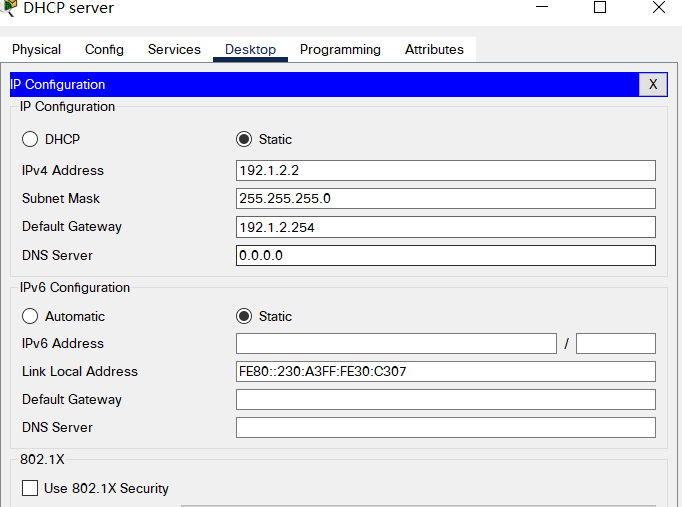


(3)完成路由器接口中继地址配置过程。

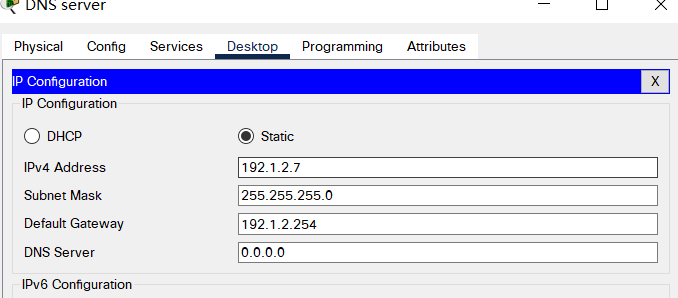


(4)完成服务器IP地址、子网掩码、默认网关

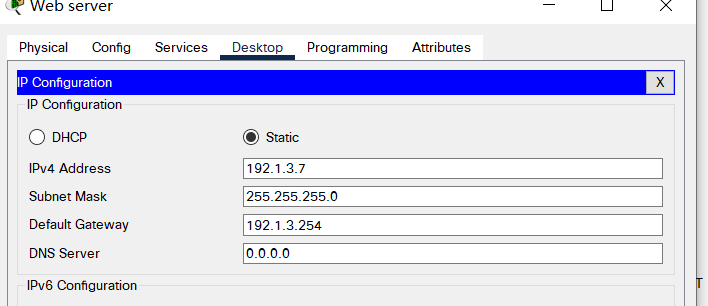
DHCP:



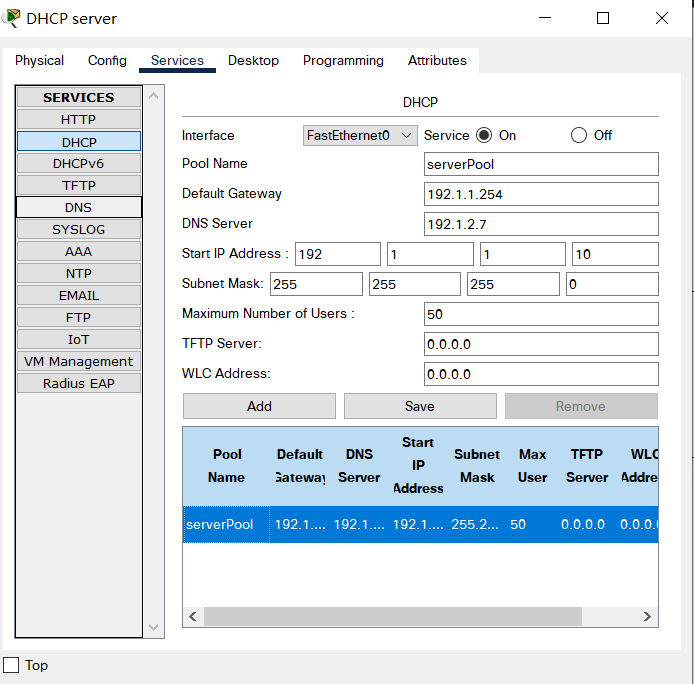
DNS:



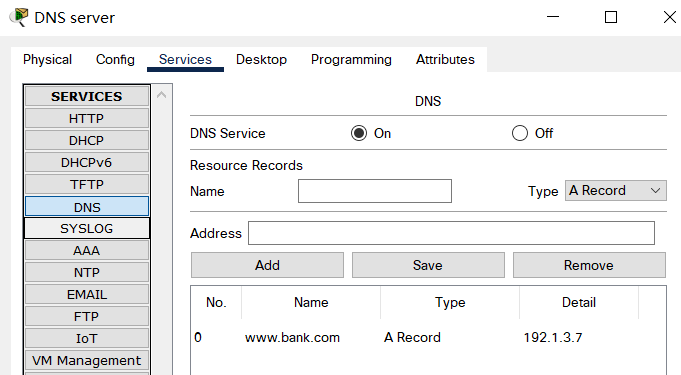
WEB:



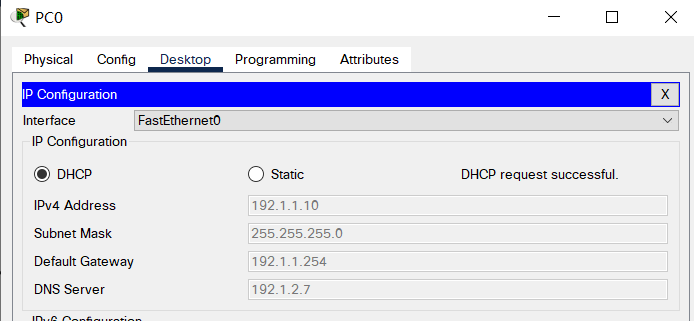
(5)完成DHCP服务器配置



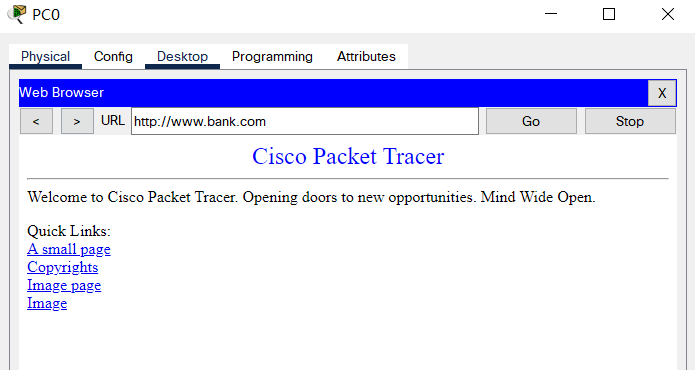
(6)完成DNS服务器配置



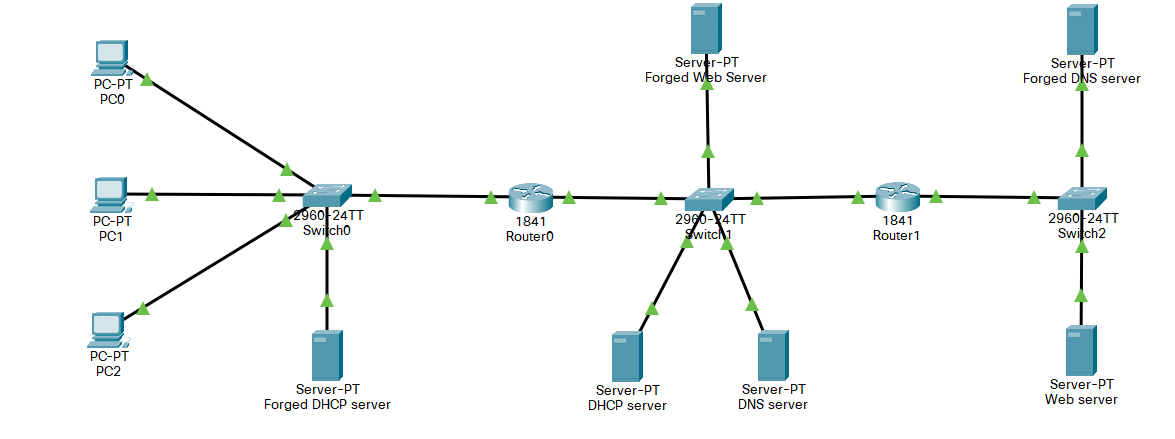
(7)完成PC0自动获取网络信息



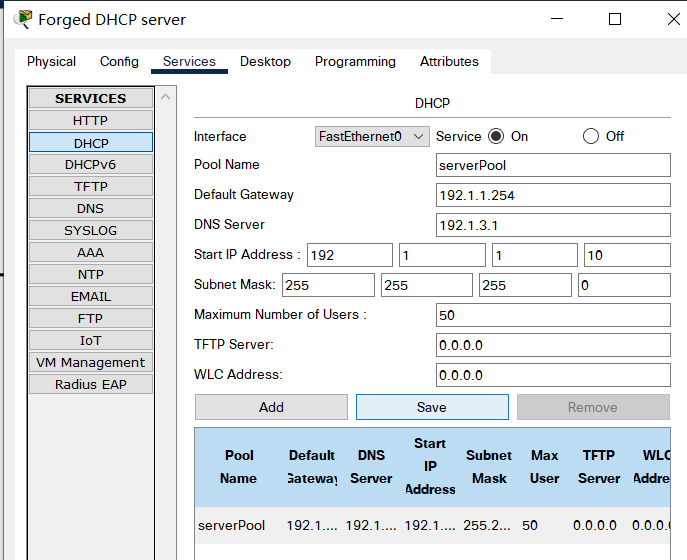
(8)完成PC0浏览服务器过程



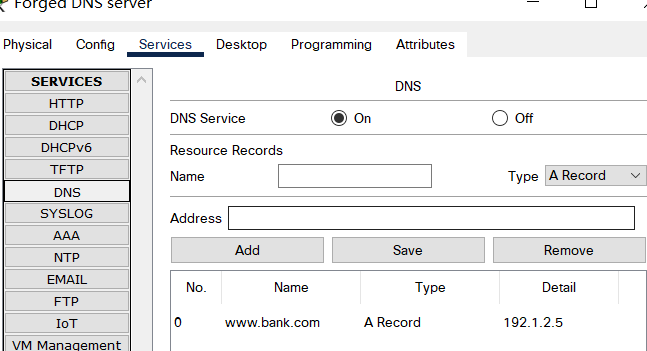
(9)接入三台伪造的服务器，完成三台伪造服务器的IP地址、子网掩码、默认网关配置



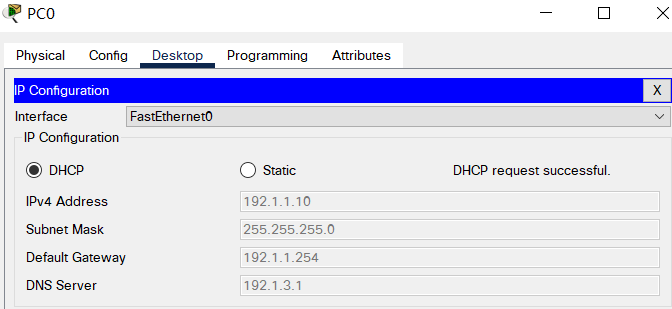
伪造DHCP：



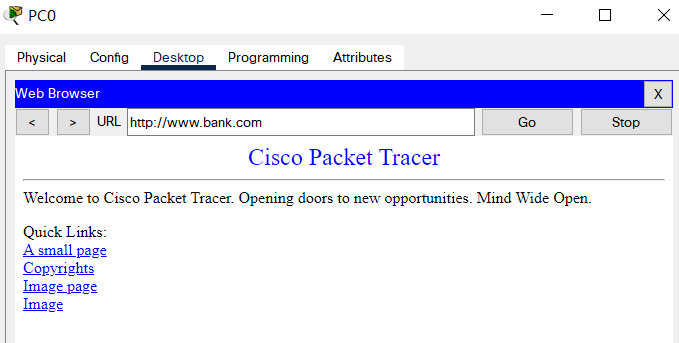
伪造的DNS：



PC0再次获得IP地址：



(10)用PC0再次访问浏览器



三、实验结果及分析

实验过程中，首先通过搭建好网络，实现PC机对web服务器的成功访问，终端通过从DHCP服务器获得正确的域名解析服务器，继而能够访问正确的网页，但是通过加入伪造的DHCP等服务器后，因为伪造的离终端距离更加接近，因此首先接入伪造的DHCP服务器，继而找到伪造的域名解析服务器，访问到钓鱼网站。

在实验过程中，路由器1采用到了中继的命令，是因为真正的DHCP服务器本省并不在终端的作用域里，需要通过中继命令，将DHCP服务器虚拟到真正的作用域里，达到分配网路及连接终端的功能。

四、实验总结及体会

这种攻击方法利用的是伪造的DHCP服务器比真正的DHCP服务器距离终端要更短，因此伪造的DHCP服务器会首先捕捉到PC终端。采用这种方法成功的关键有两个要点，一个是要保证真正的DHCP服务器不在本作用域，在一般情况下，DHCP距离中端都比较远。第二个要点是要保证做的钓鱼网站和原来的真是网站非常相像，不然很容易导致用户发现端倪，导致最终失败。

对于应用层来讲，钓鱼网站是一个非常好用的攻击手段，对于某些账号密码进行登录的页面，用户应该谨慎判断，谨慎思考，放置被钓鱼网站钓鱼得逞。