《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12月2日 |

|  |  |
| --- | --- |
| 实验名称： | OSPF路由项欺骗攻击和防御实验和NAT实验 |

|  |  |
| --- | --- |
| 实验成绩： |  |

OSPF路由项欺骗攻击和防御实验

一、实验目的

(1)验证路由器OSPF配置过程。

(2)验证OSPF建立动态路由项过程。

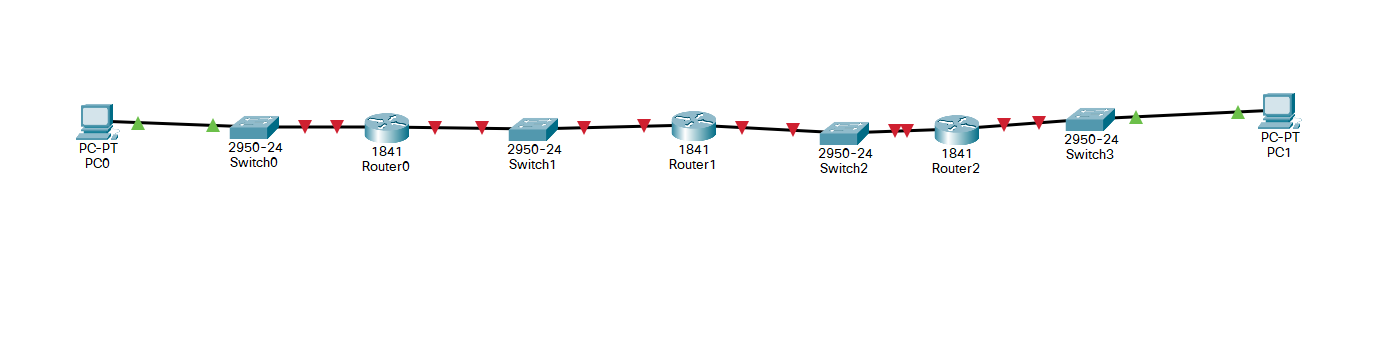
(3)验证OSPF路由项欺骗攻击过程。

(4)验证OSPF源端鉴别功能的配置。

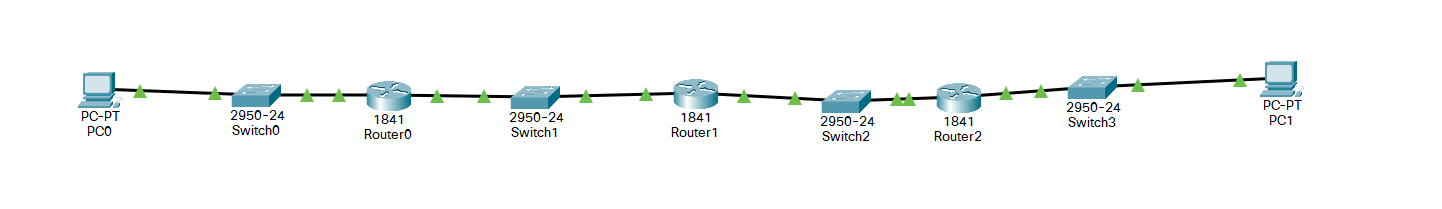
(5)验证OSPF防路由项欺骗攻击功能的实现过程。

二、实验步骤

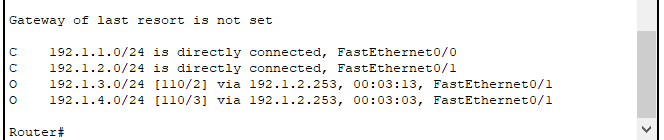
(1)完成去掉入侵路由器的网络结构放置和连接设备。



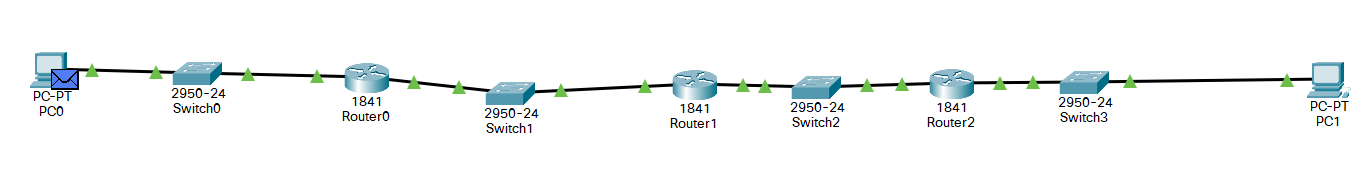
(2) 完成各设备配置和路由器OSPF配置，完成配置后生成路由表。

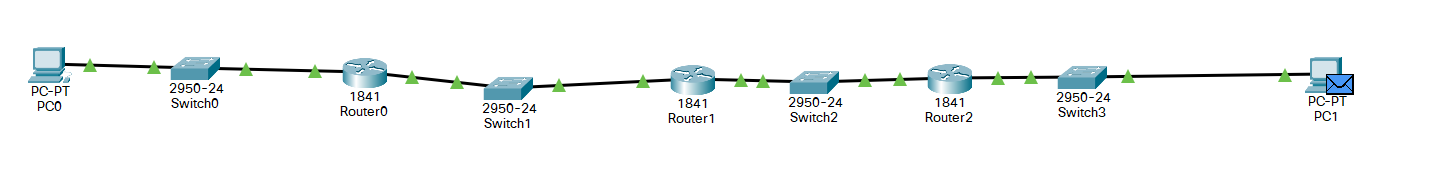


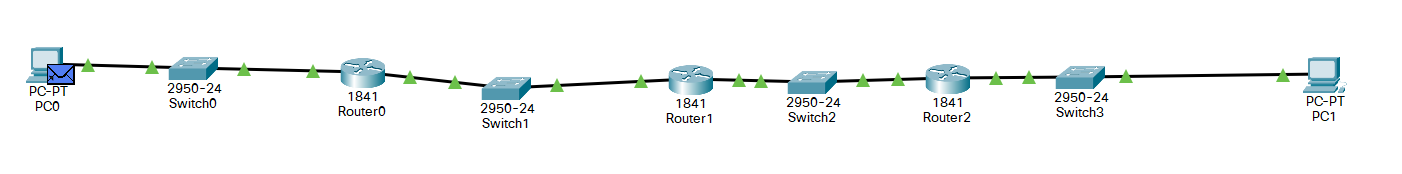
**Router0路由表：**



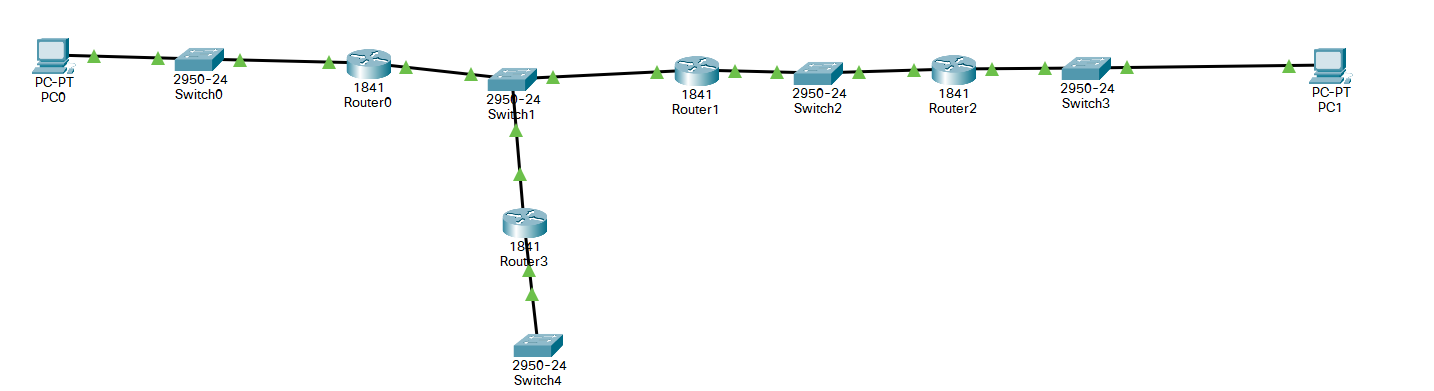
(3)切换到模拟操作模式，启动PC0和PC1的ICMP报文传输过程。



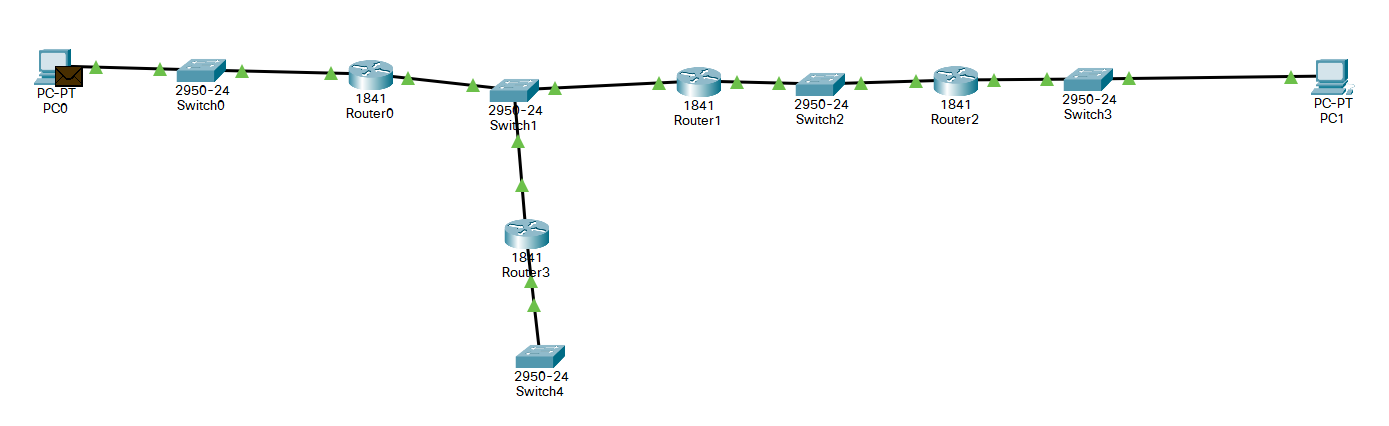


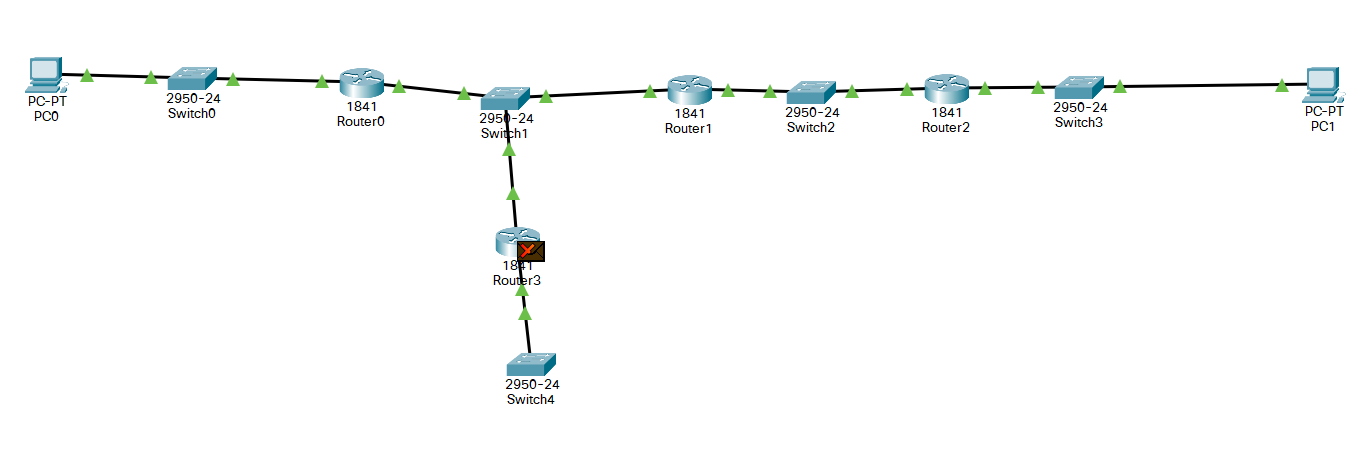


(4)加入入侵路由器，并配置OSPF协议。

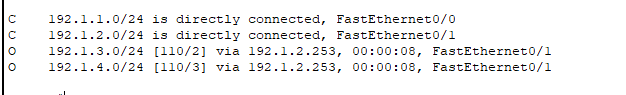


(5)通过简单报文工具启动PC0到PC1的ICMP报文传输过程。

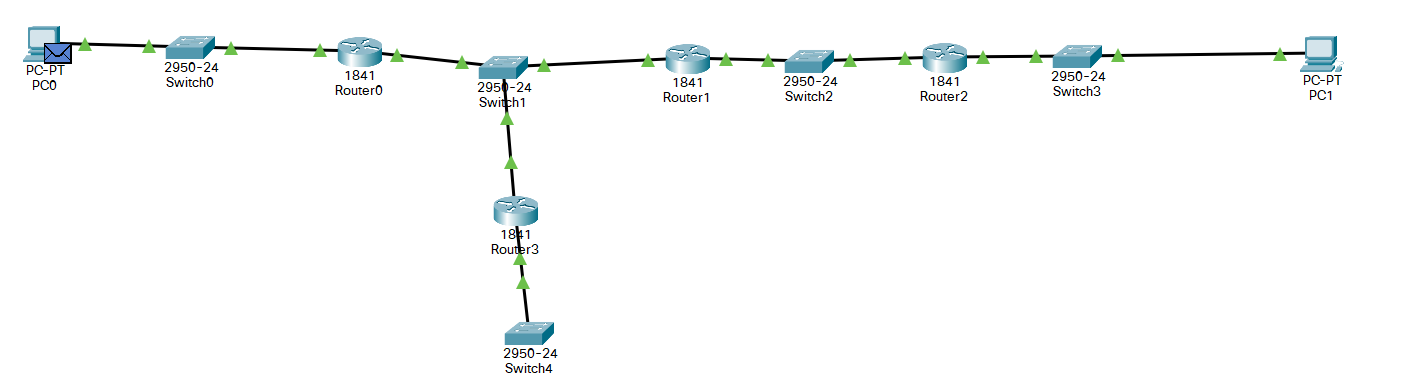


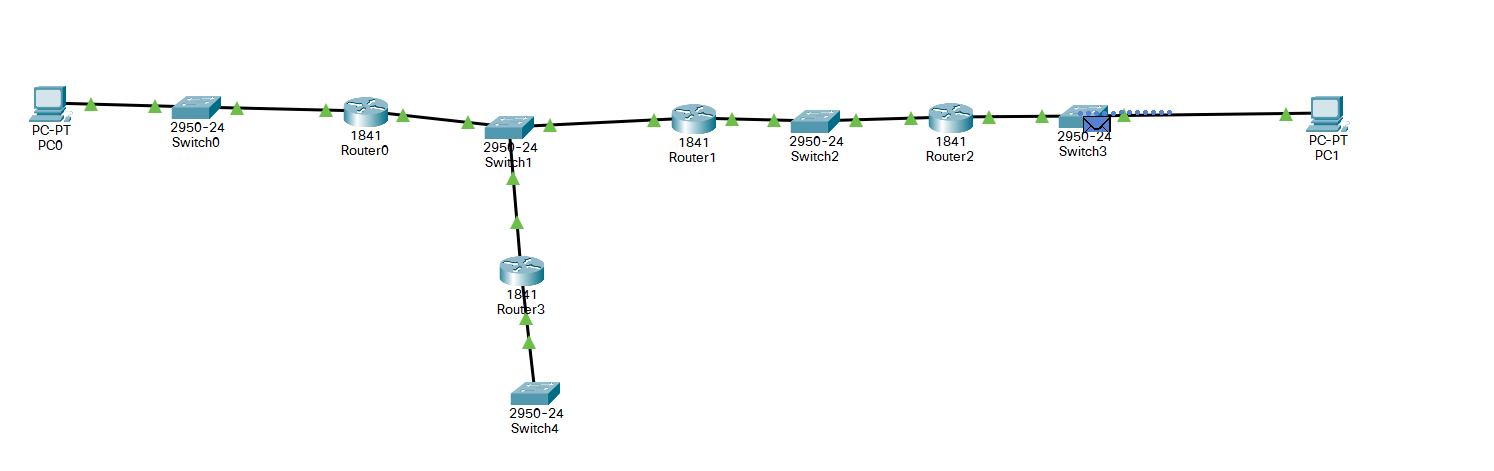


(6)在CLI命令下配置三个路由器的源鉴端鉴别和完整性检测功能的配置，为相邻路由器配置相同的密钥，查看R0的路由表。



(7)验证ICMP报文传输过程。





实验结果验证鉴别成功，成功在入侵路由器干扰下实现PC0和PC1的通信过程。

三、实验结果及分析

在未加入路由器的情况下连接设备并设置完IP地址后，配置OSPF协议。

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PC0到PC1，再由PC1到达PC1，证明本次ICMP通信正常。

加入入侵路由器后，将路由器远端配置好和192.1.4.0一样的子网，通过路由欺骗进行攻击，发现PC0送往PC1的报文被截获。

为了防止OSPF路由项欺骗，通过设置在路由器上的源端鉴别协议，通过鉴别报文来源和密钥是否匹配进行传输，可以防止路由项欺骗协议，最后发现PC0到PC1的报文通信正常。

四、实验总结及体会

在实验中并未遇到比较棘手的困难，遇到的最大问题是第一次做实验的时候，设置好OSPF协议都不能通信，尝试了各种方法也不行，但是关掉软件，重新配置过一次后，发现可以正常通信，我怀疑是因为在第一次配置OSPF的地方某个小地方出现了错误，导致整个区块的OSPF不能正常通畅。

防止路由项欺骗的原理其实很简单，通过鉴别双方共同的密钥是否正确，是否一致来判断你是否是消息的真正接收方，但是同样也有缺点，如果密钥被破解，那么这个源端鉴别协议将不再安全。

NAT实验

一、实验目的

(1)理解“内部网络对于外部网络是透明的”的含义。

(2)验证动态NAT实现过程。

(3)验证静态NAT实现过程。

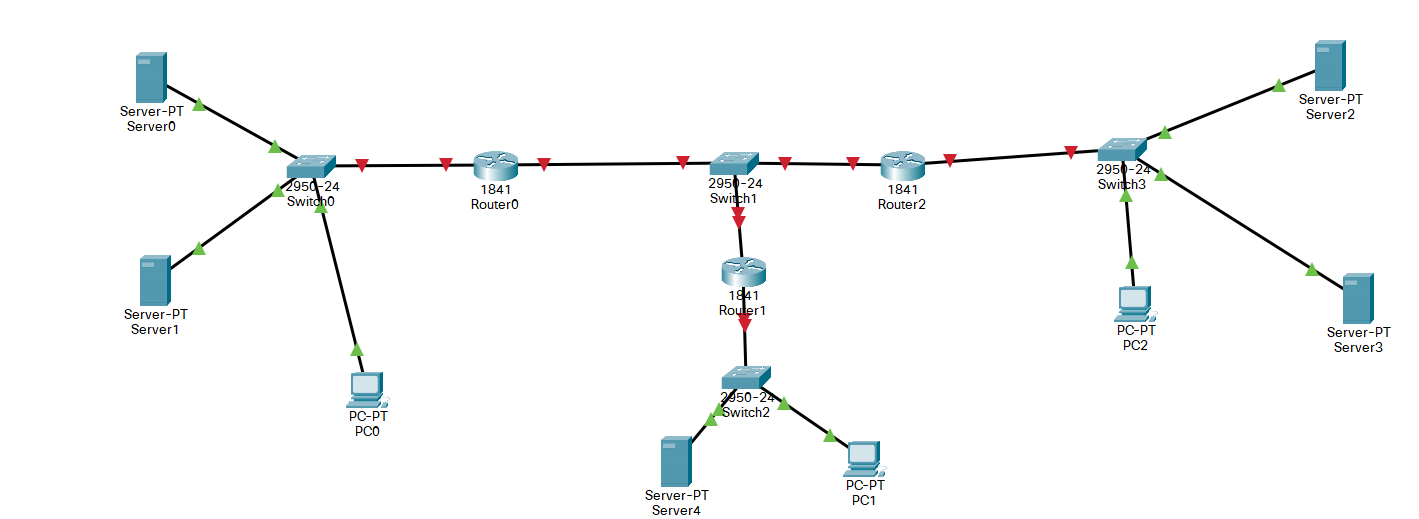
(4)验证动态NAT配置过程

(5)验证静态NAT配置过程

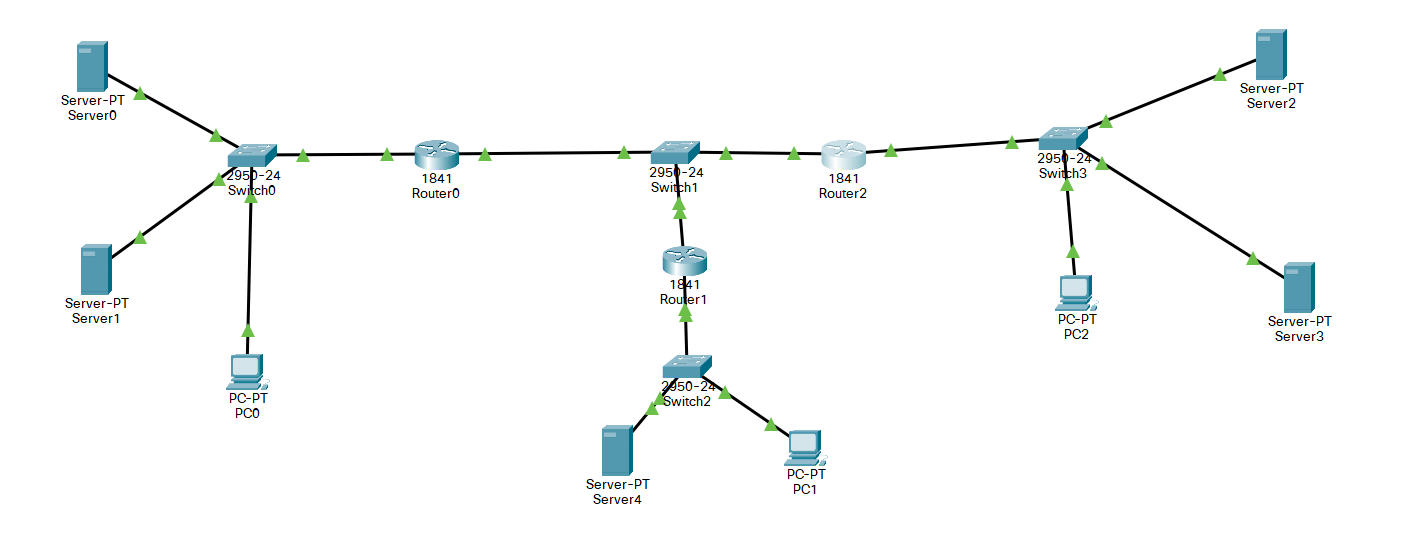
(6)验证NAT的安全性。

二、实验步骤

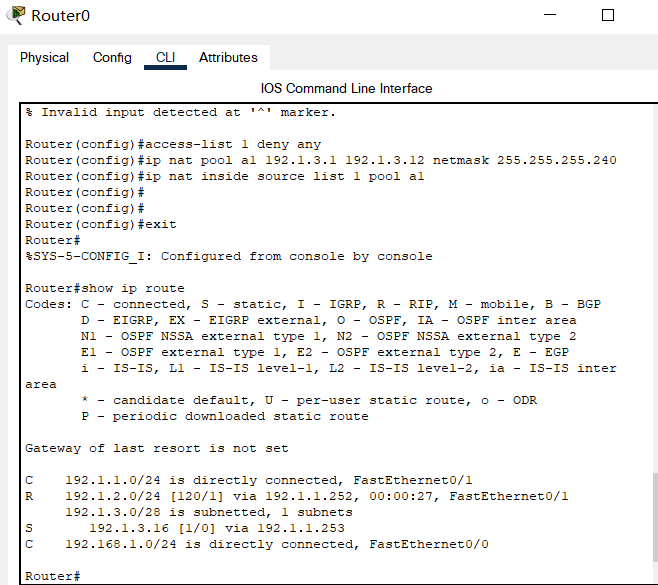
(1)完成内部网络和外部网络的设备放置和连接。



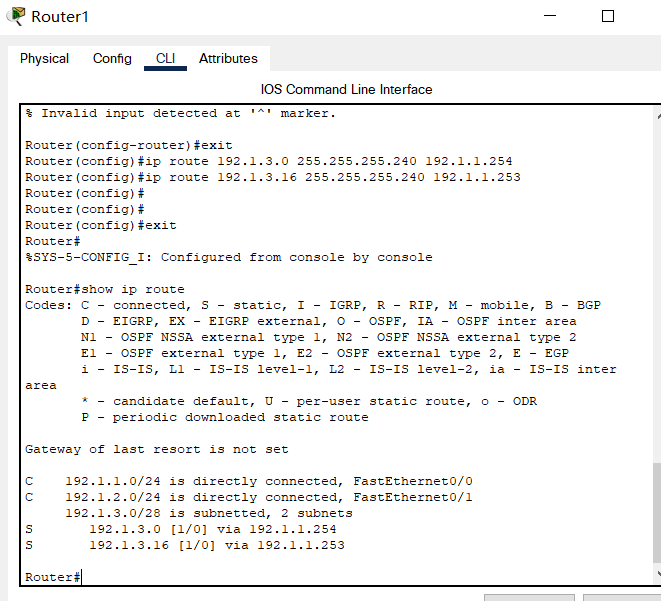
(2)完成各个设备接口IP、子网掩码配置，RIP协议配置、静态路由项的配置。



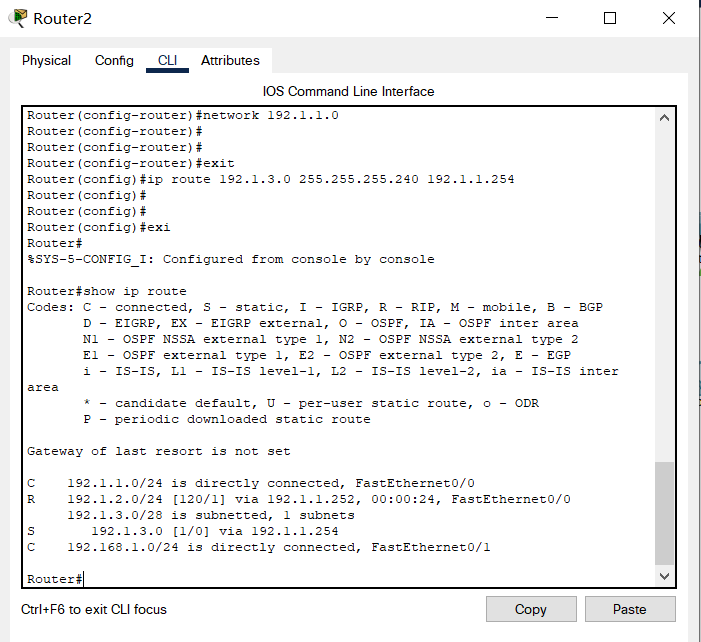
Route0：



Router1

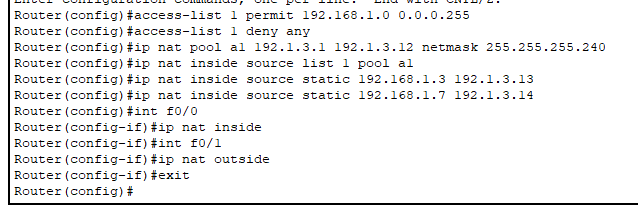


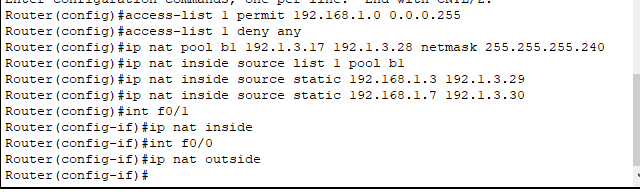
Router2：



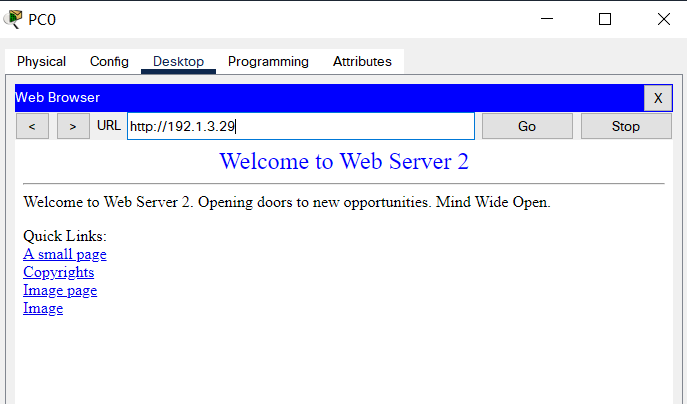
(3)完成各个服务器和终端的网络信息配置。

(4)完成两个路由器的地址池的建立，建立全球IP地址和服务器私有地址的静态映射。



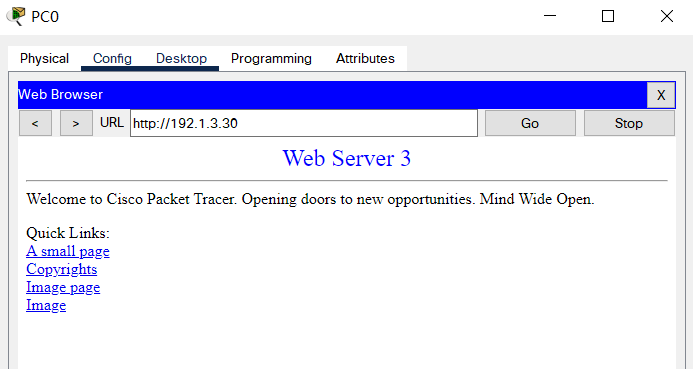


(5)PC0用全球IP地址192.1.3.29 访问私有IP地址192.168.1.3的web2界面。



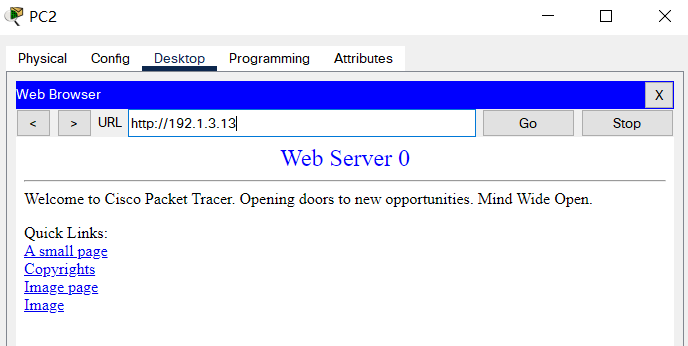
Web2界面

PC0用全球IP地址192.1.3.30访问私有IP地址为192.168.1.7的Web3界面

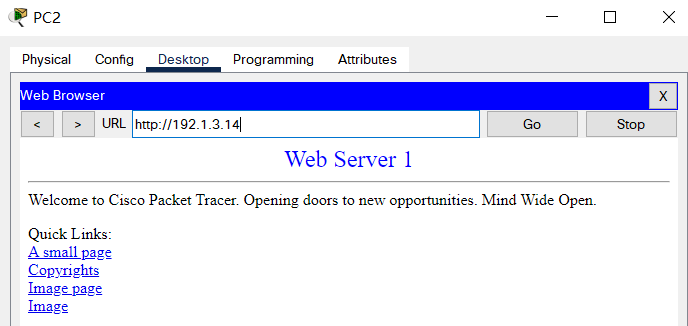


Web3界面

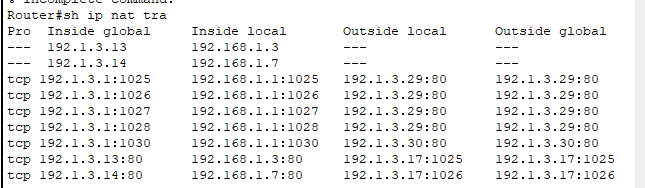
PC2用全球IP地址192.1.3.13访问私有IP地址为192.168.1.3的Web1界面



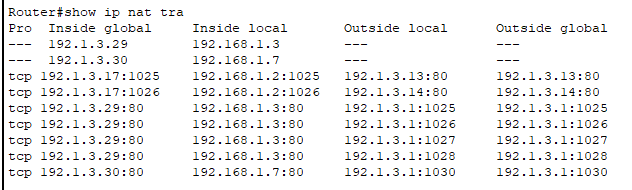
PC2用全球IP地址192.1.3.14访问私有IP地址为192.168.1.7的Web2界面



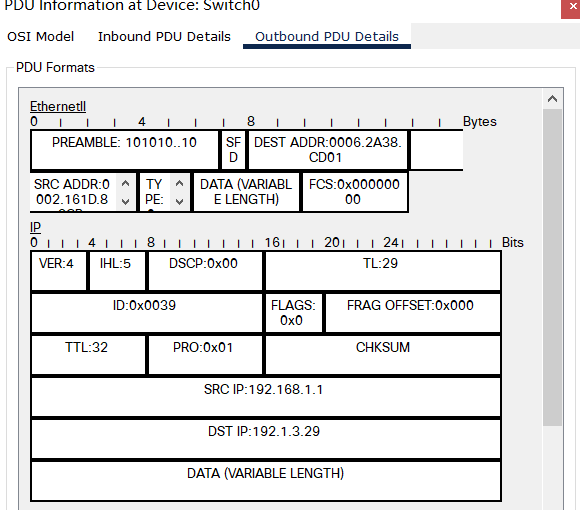
(6)PC0用全球IP地址192.1.3.29和192.1.30分别访问私有IP地址为192.168.1.3和192.168.1.7的两个web后，路由器0的NAT表如下图所示



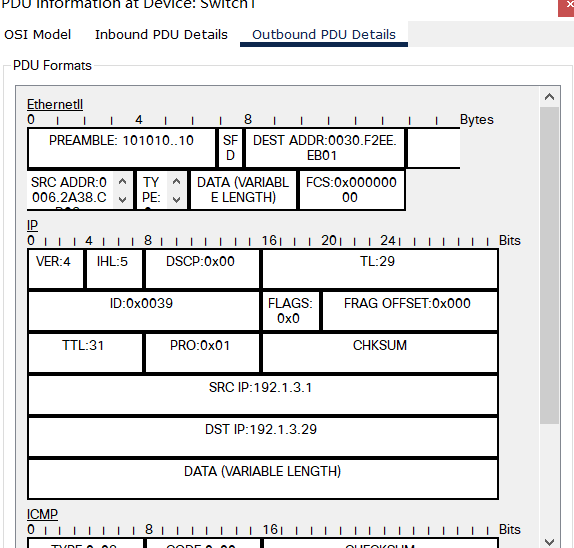
路由器2的转换表如下图所示



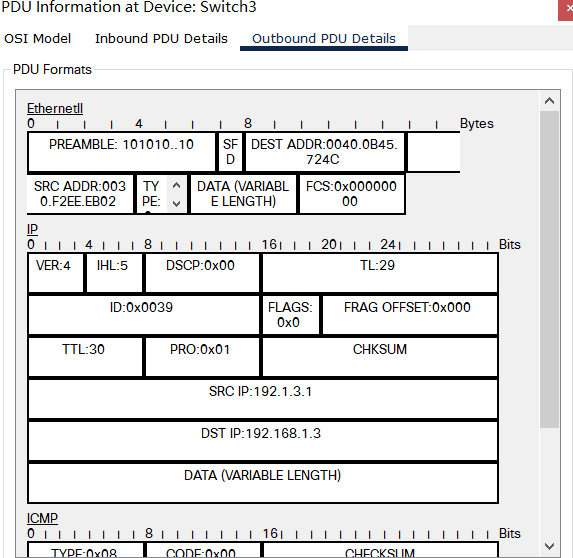
(7)PC0通过浏览器访问Web Server2产生的IP分组分别由路由器R0和R2完成NAT过程，查看各路由器中的分组格式。



PC0至R0



R0至R2



R2至服务器

三、实验结果及分析

首先通过建立两个内部网路和一个外部网，建立三个路由器，分别设置好各自路由的RIP协议，保证外部网络的通畅。

其次通过设置全球地址池，给内部网络映射到全球地址的空间。

最后通过设置动态NAT和静态NAT，实现内部网络终端访问外部网络的过程，实现外部网络的终端和其他内部网络的终端访问某个内部网络的Web服务器的过程。

四、实验总结及体会

本次实验的易错点在于静态路由项的设置，由于外部网络采用的RIP协议无法连接到内部网络，因此当内部网路的地址想要访问外部网络并进行通信时，需要进行静态路由项的设置，当有任意一个静态路由项未设置成功，都有可能导致实验失败。

学会如何更好地利用动态NAT协议和静态NAT协议，才能更好地搭建一个映射的网络环境，才能保证内部网路与外部网络的正常通信。