**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 互联网安全实验**

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 5 月 31 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. OSPF路由项欺骗攻击和防御实验

## 一、实验目的

## 验证路由器OSPF配置过程。

## 验证OSPF建立动态路由项过程。

## 验证OSPF路由项欺骗攻击过程。

## 验证OSPF源端鉴别功能的配置过程。

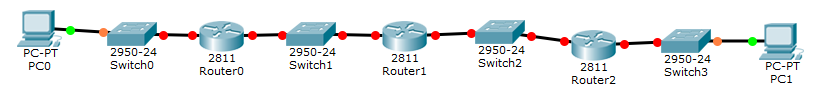
## 验证OSPF防路由项欺骗攻击功能的实现过程。

## 二、实验任务

1. 使用自己的语言简述该实验原理。

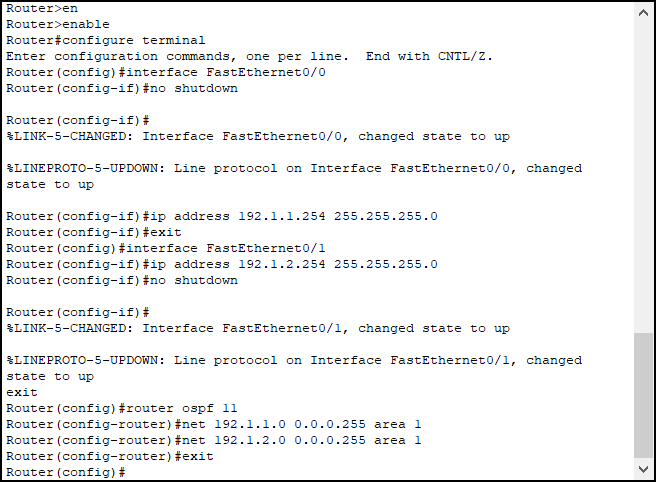
OSPF欺骗是指插入的网络的路由器广播距离下一跳更近的路由信息，从而劫持路由器下一跳地址的过程。如果让路由器之间开启消息鉴别功能，拒绝接收未鉴别的消息，即可防御OSPF欺骗攻击。

1. 实验步骤
2. 链接网络拓扑

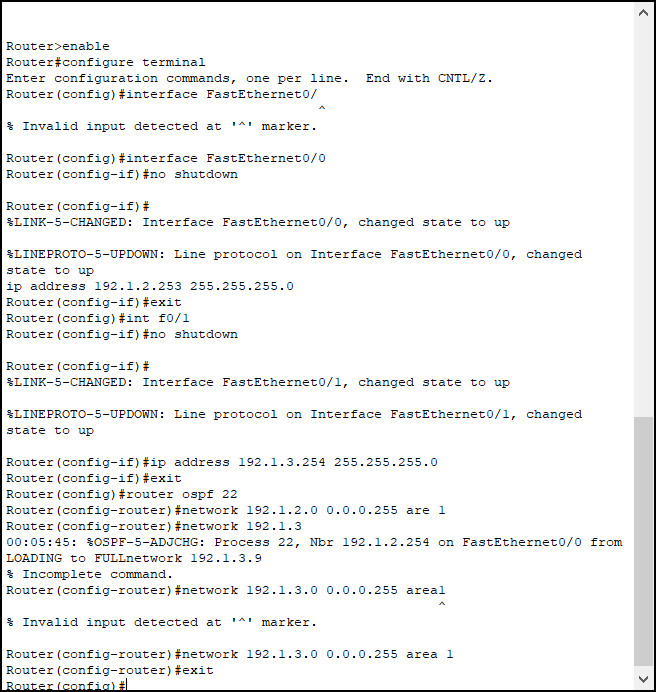


1. 配置路由器IP和OSPF

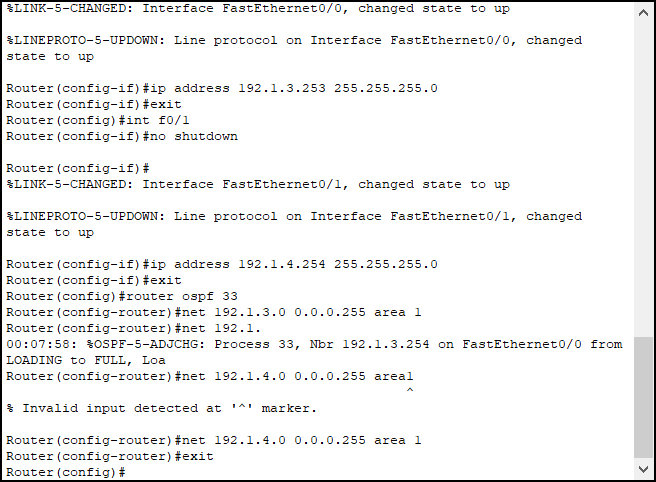
R1：



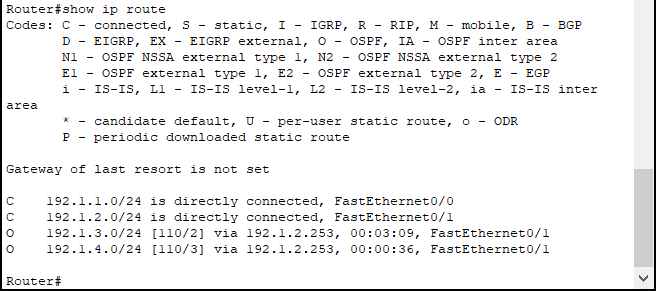
R2：



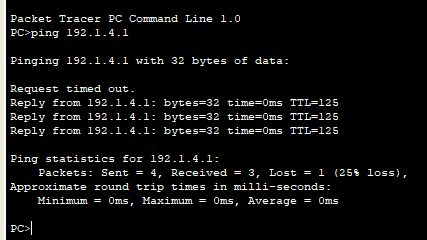
R3:



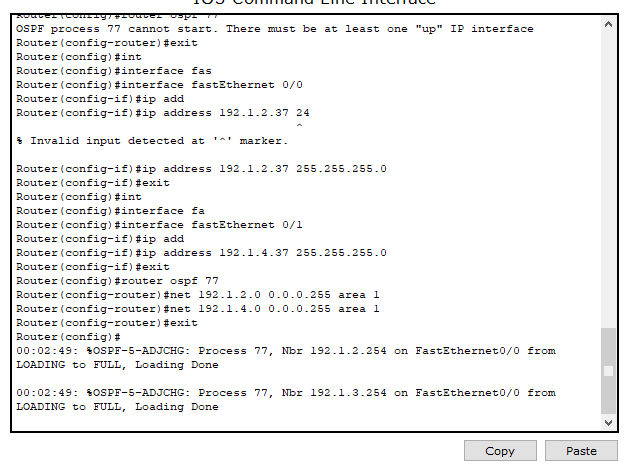
R1路由表：



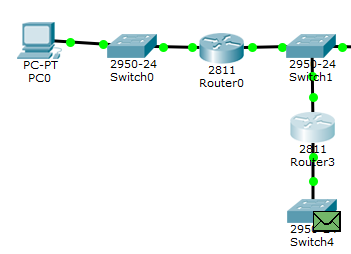
1. 测试PC0和PC1的连通性



1. 加入入侵路由器，配置端口和ospf路由

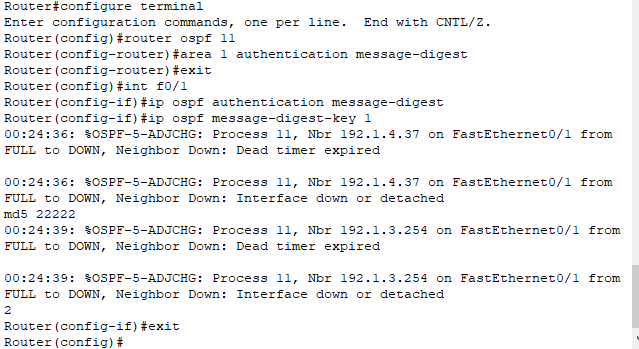


1. 在仿真模式下再次测试连通性，发现数据包已经被劫持

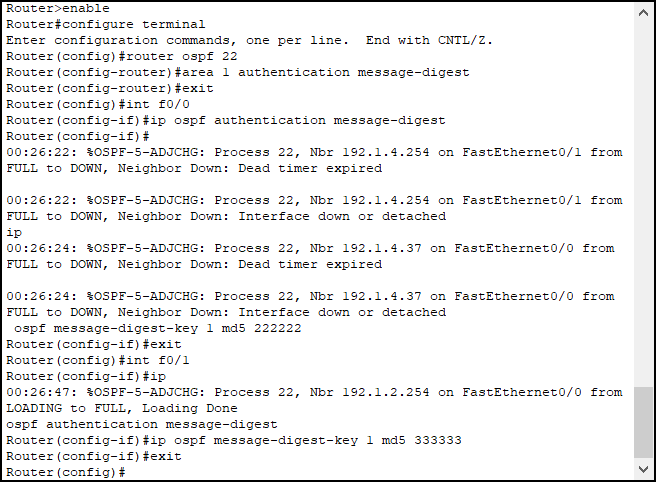


1. 配置路由器的消息鉴别和完整性检验功能

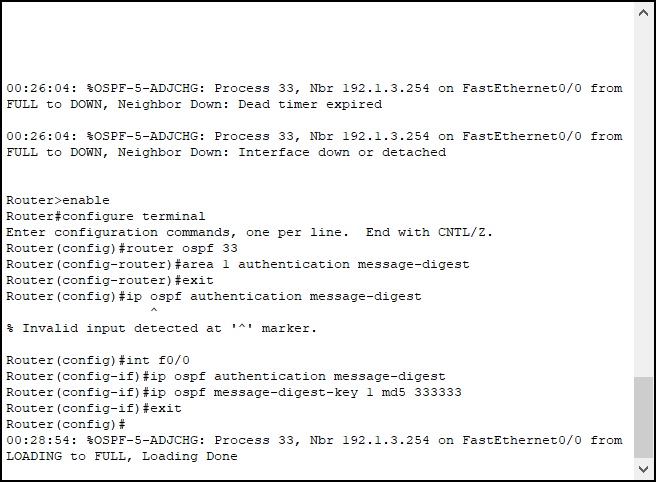
R1:



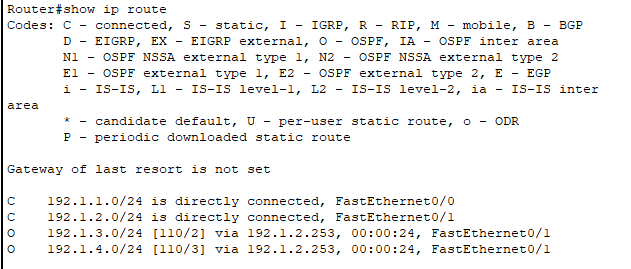
R2:



R3:



R1路由表：



## 三、思考与总结

1. 实验过程中你遇到什么问题，如何解决的？通过该实验有何收获？

遇到的问题：PC0和PC1不同

解决方案：逐个路由器排查，发现router2端口误关闭

实验收获：本次实验学习了OSPF欺骗攻击及防御，强化了组网能力，加深了计算机网络知识的理解

1. 这个实验为什么不使用RIP协议的路由消息源端鉴别功能，而使用的是OSPF协议的路由消息源端鉴别功能？

因为实验使用的是OSPF路由协议，RIP和OSPF路由表建立不同。

# 实验2. 策略路由项实验

## 一、实验目的

1. 验证RIP生成动态路由项的过程。
2. 验证最长前缀匹配过程。
3. 验证静态路由项改变IP分组传输路径的过程。
4. 验证基于安全理由规避特定路由器的过程。

## 二、实验任务

1. 使用自己的语言简述该实验原理。

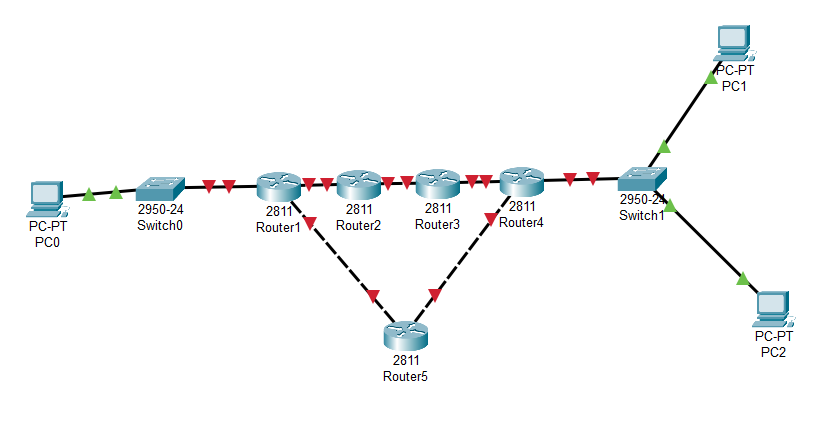
原本的路由算法会选择最短路径路由，但如果因为安全原因不允许访问某个路由器，则要强行将某一路由器的下一跳修改为另一路由器。

1. 实验步骤

（1）添加以太网接口：

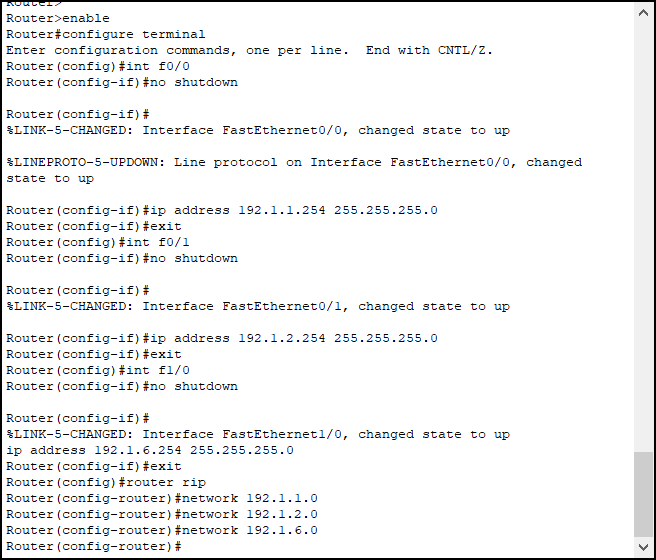


（2）完成配置图

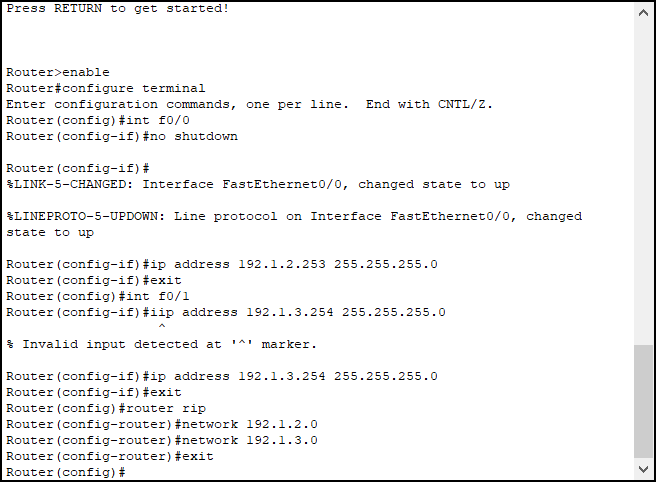


1. 完成各台路由器中每一个接口的 IP 地址、子网掩码配置过程

## R1:



R2:



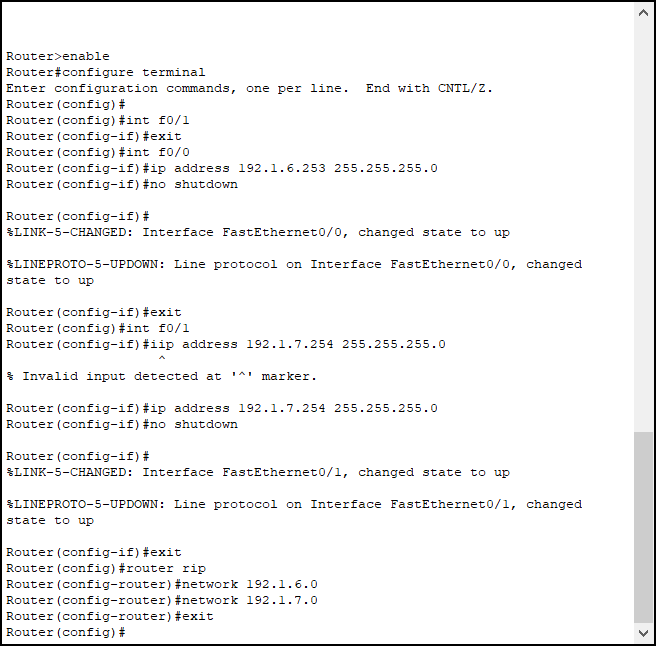
R3:

## 

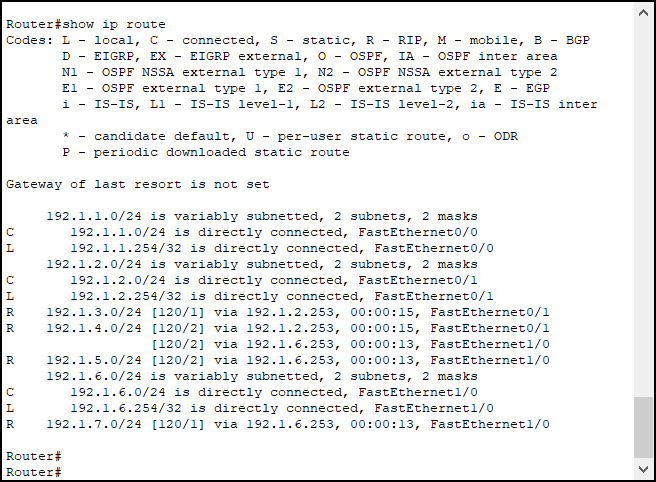
R4:

## 

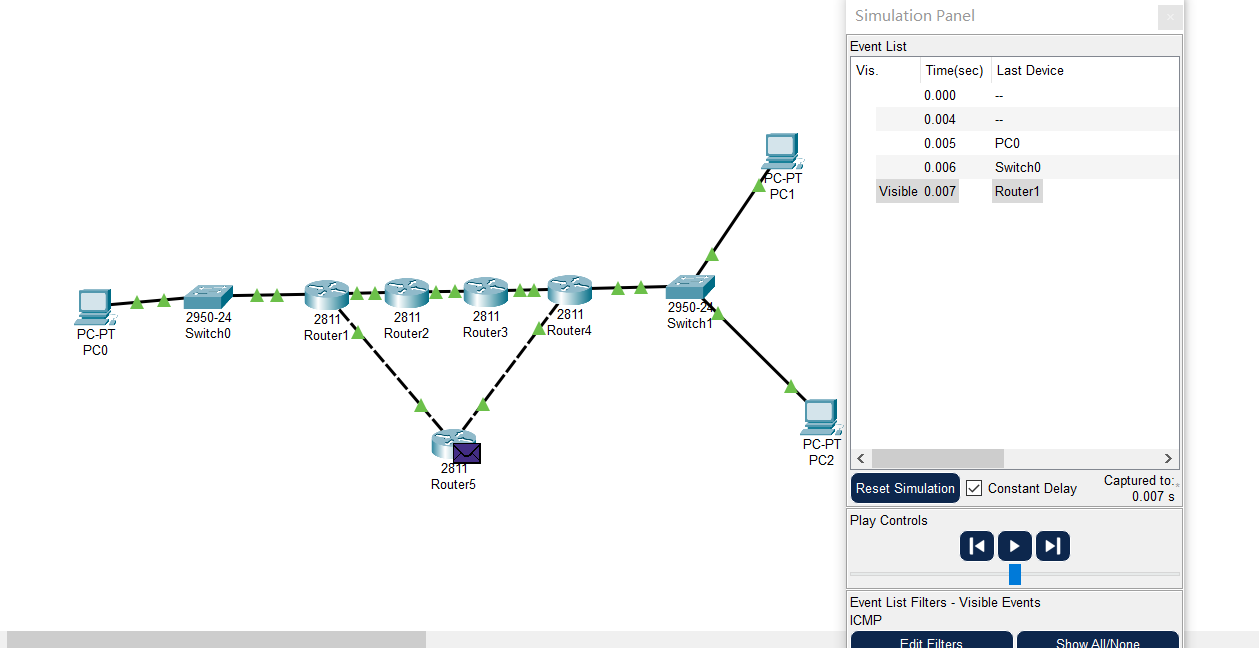
R5:



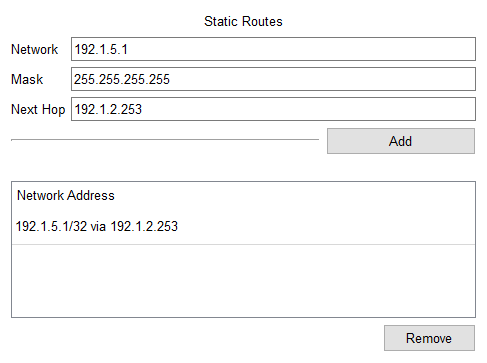
R1路由表：

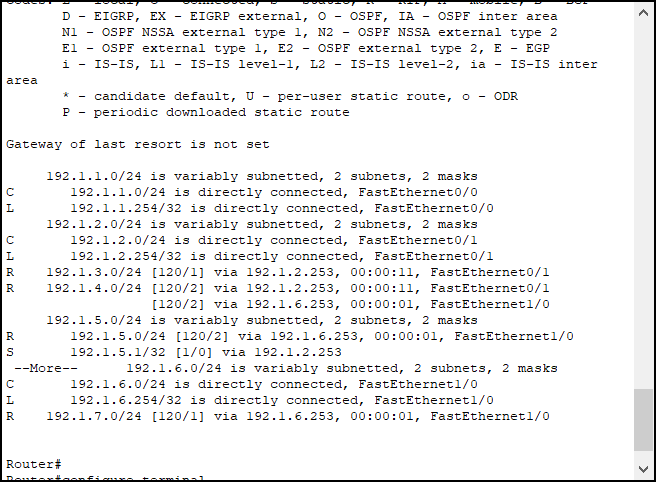


1. 切换到模拟操作模式，查看PC0发送给PC2的ICMP报文，该ICMP报文经路由器Router5



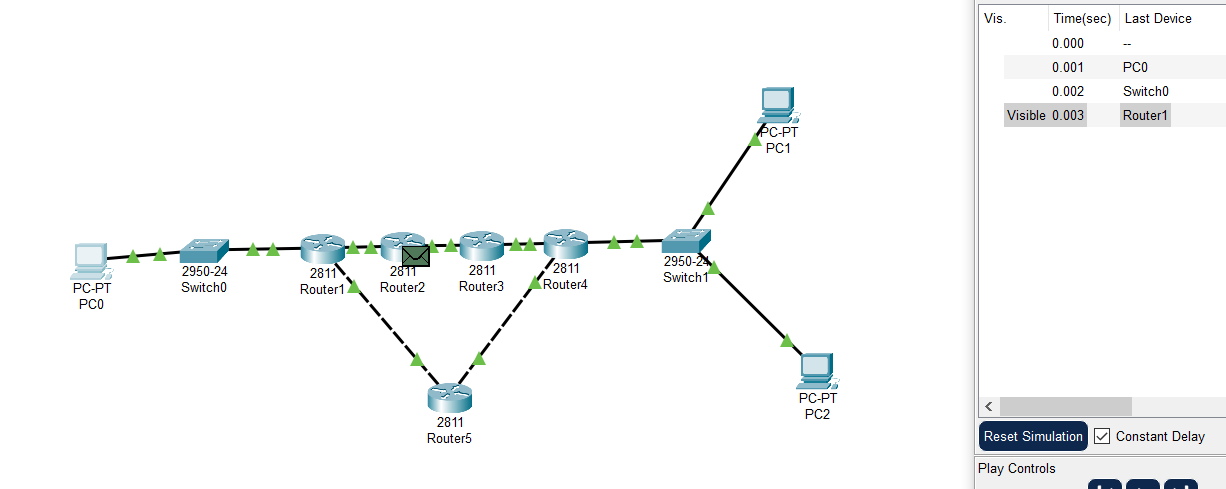
（5）换到实时操作模式，在路由器 Router1 中配置一项静态路由项



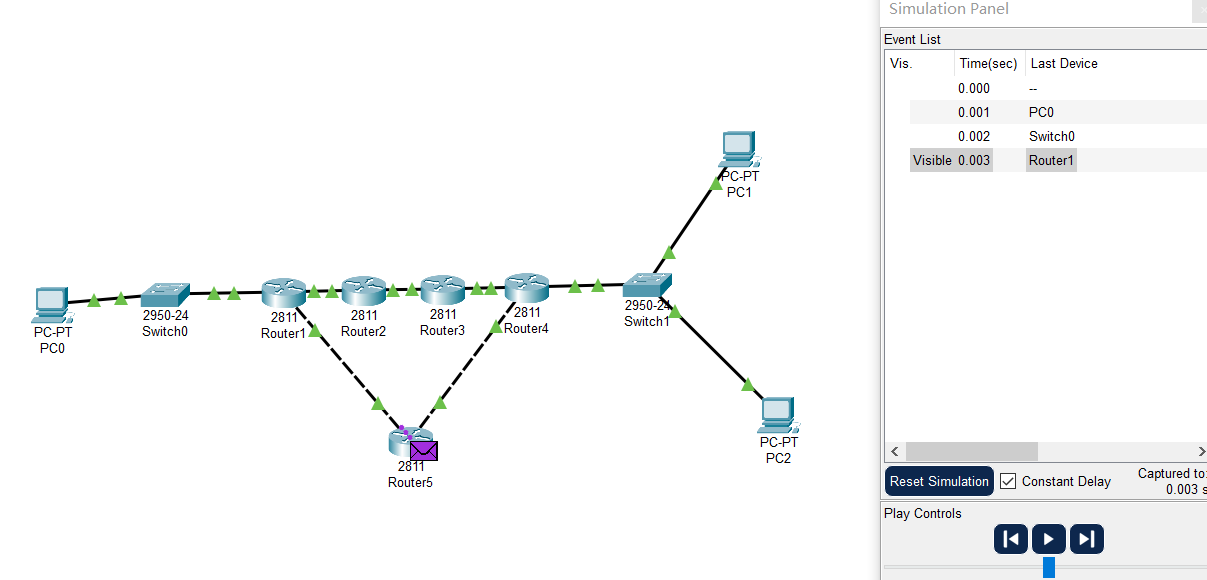


（6）切换到模拟操作模式，查看 PC0 发送给 PC2 的 ICMP 报文，路由器 Router1 将该 ICMP 报文转发给路由器 Router2。

PC0向PC2发送：



向PC1发送：



## 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？

本次实验学习了策略路由项的配置，强化了组网能力，加强了对计算机网络知识的理解。