**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 学号

同作者

实验日期 2024 年 05 月 25 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

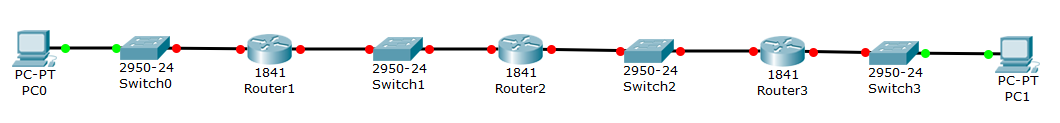
1. 使用自己的语言简述该实验原理。

因为OSPF是一个链路状态协议，它在路由器之间传播链路状态信息来构建路由表。在OSPF路由项欺骗攻击中，攻击者通过接入网络入侵路由器，伪造与目标网络的直接连接信息，并将这些伪造的链路状态信息发送给合法路由器。这导致合法路由器错误的更新路由表，并将数据报错误地转发给入侵者，从而实现对数据报的窃听。

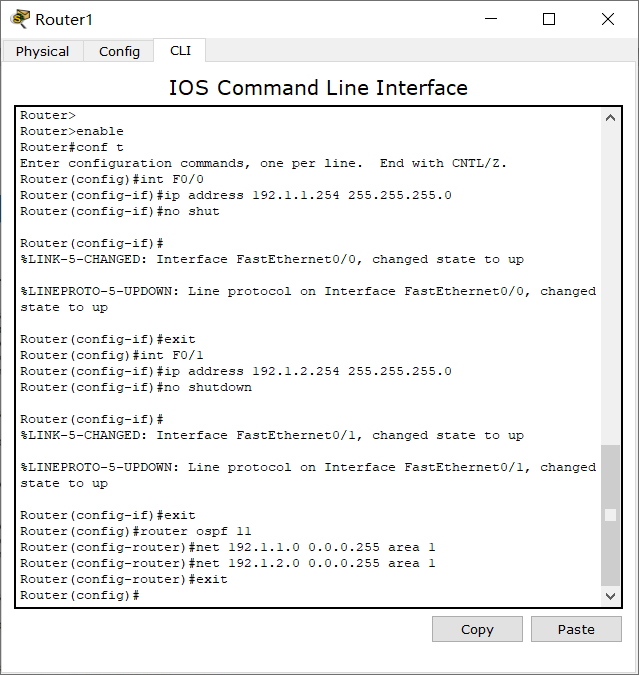
为了防御OSPF路由项欺骗攻击，OSPF协议可以配置源端鉴别功能。使每一台路由器只能接收和处理授权路由器发送的路由信息。路由消息是否授权路由器发送的依据是：发送路由消息的路由器是否和接收路由消息的路由器拥有相同的共享密钥。

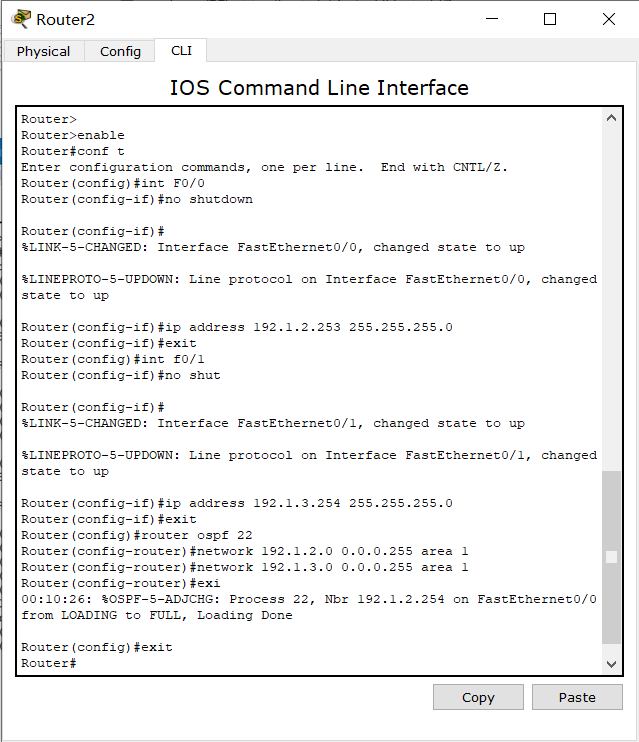
1. 实验步骤

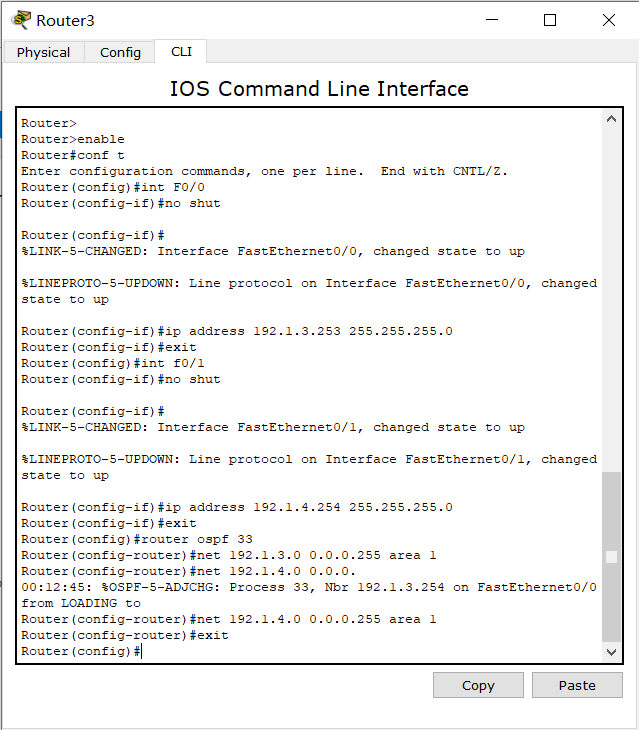
首先给出实验的初始拓扑图：



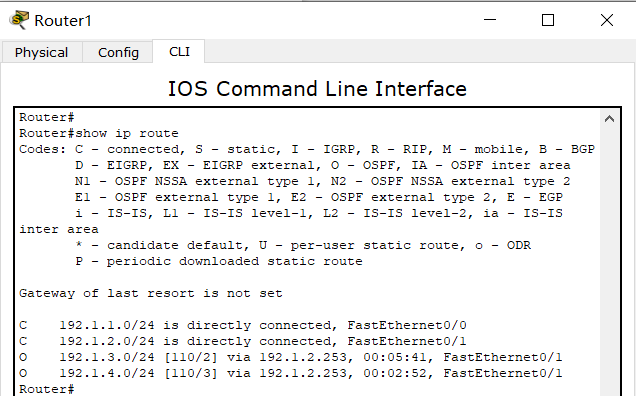
之后配置Router1、Router2、Router3的接口IP地址、子网掩码和OSPF协议的配置：



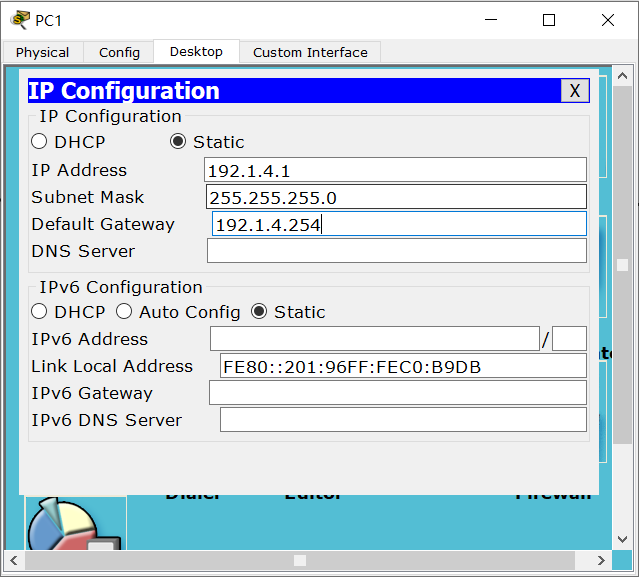
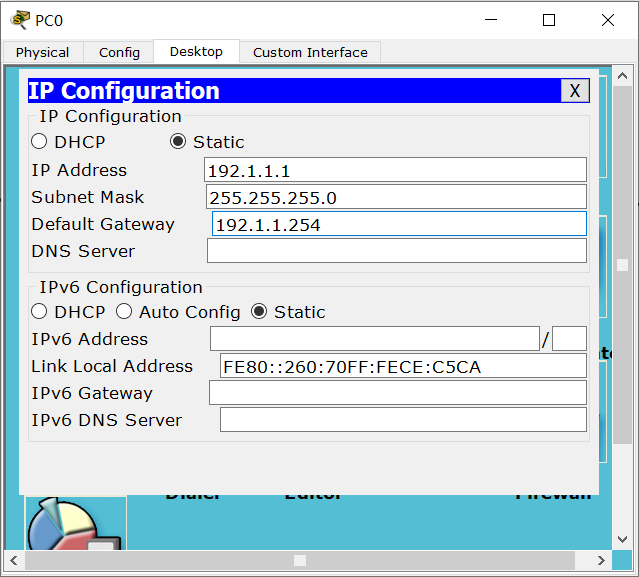




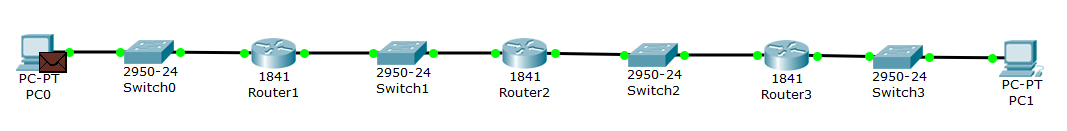
之后查看Router1的路由表，可以发现经过配置以后，各个设备均为联通的。

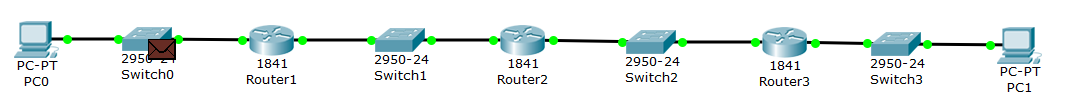


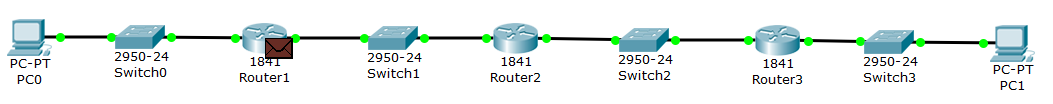
之后配置PC0和PC1的IP地址和默认网关。

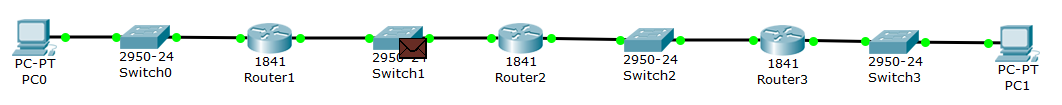


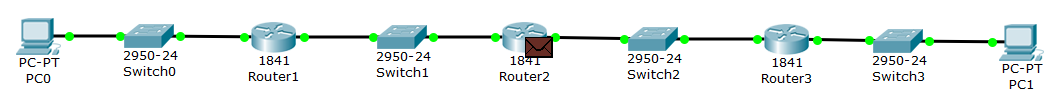
然后在PC0和PC1之间设置一个简单PDU，并开启仅查看ICMP报文，观察报文在PC0—PC1之间的传播路径（由于长度原因，原路返回的路径省略），可以发现PC0与PC1之间可以联通，存在传输路径。

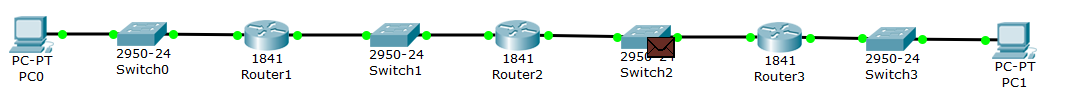


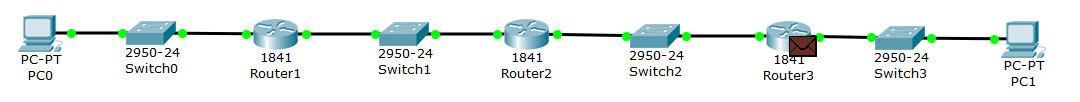


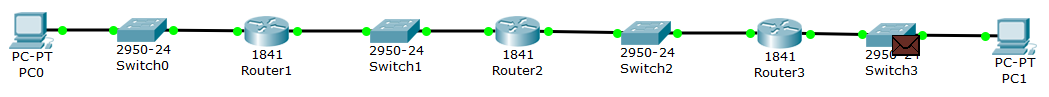


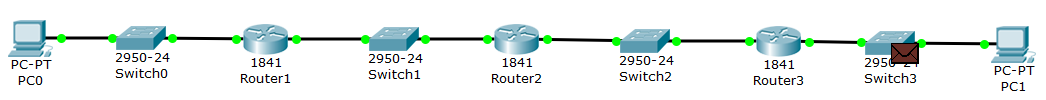


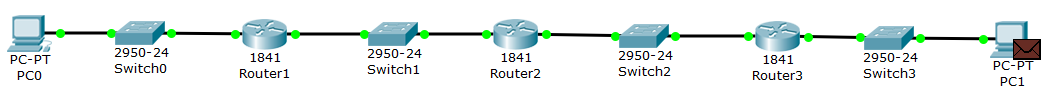


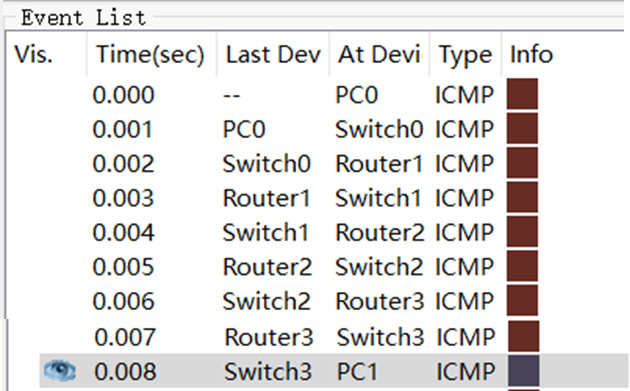




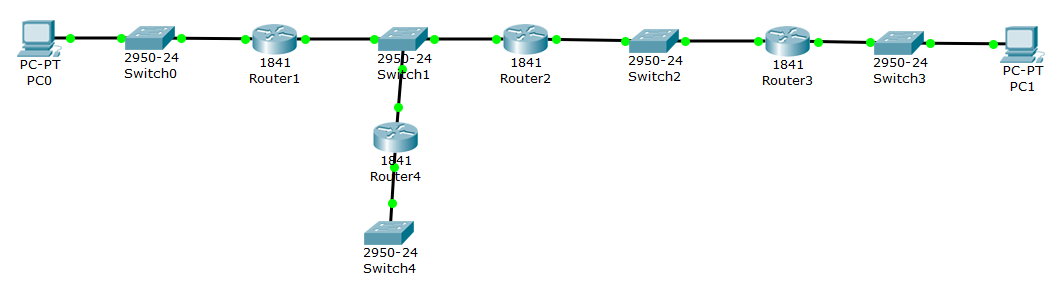




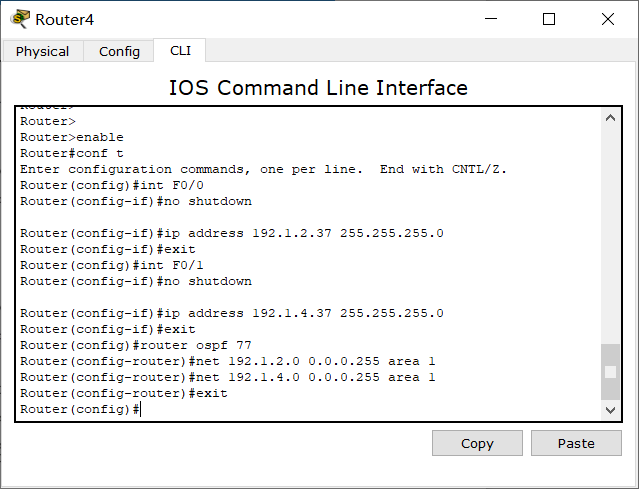




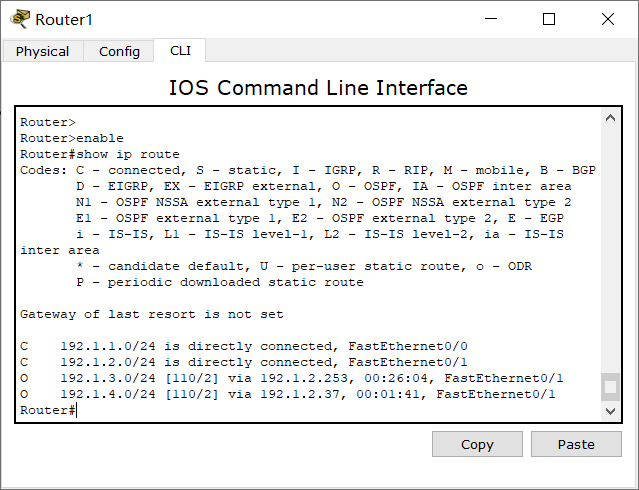
之后在Switch1另外连接一个路由器R4和交换机Switch4，来模拟OSPF路由项欺骗攻击。



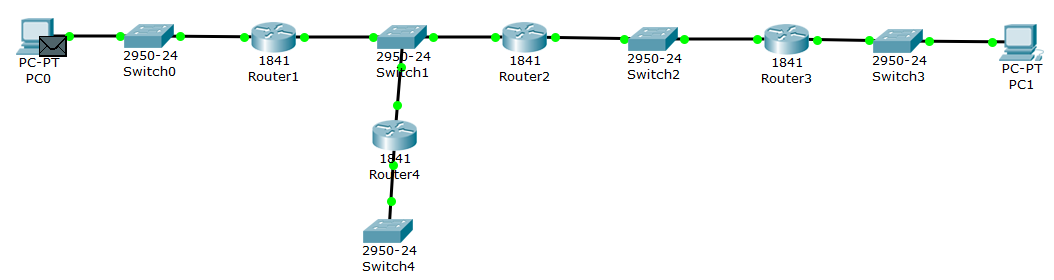
之后为R4的连接Switch1的接口分配IP 192.1.2.37/24，连接Switch4的接口分配IP 192.1.4.37/24，以此将该接口伪造成与网络192.1.4.0/24直接相连的接口

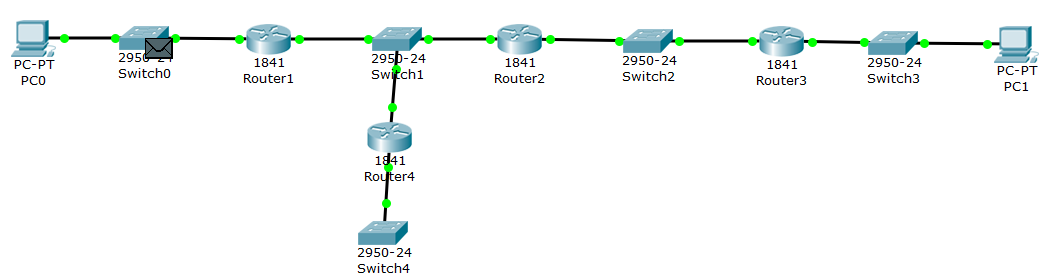


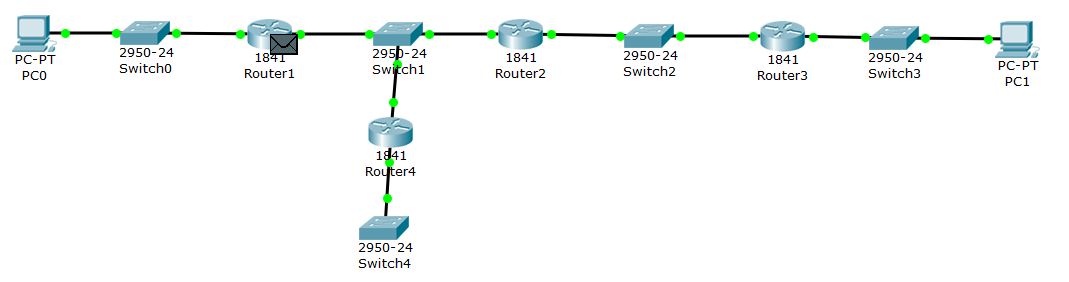
此时再次查看R1的路由表，发现R1通向192.1.4.0/24的路径经过192.1.2.37，即经过R4，说明OSPF路由项欺骗攻击成功

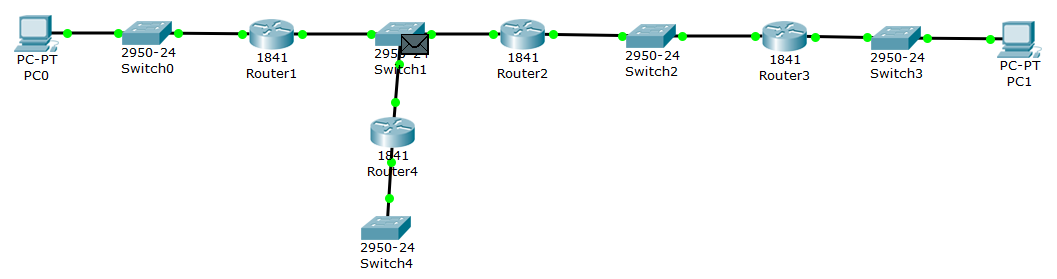


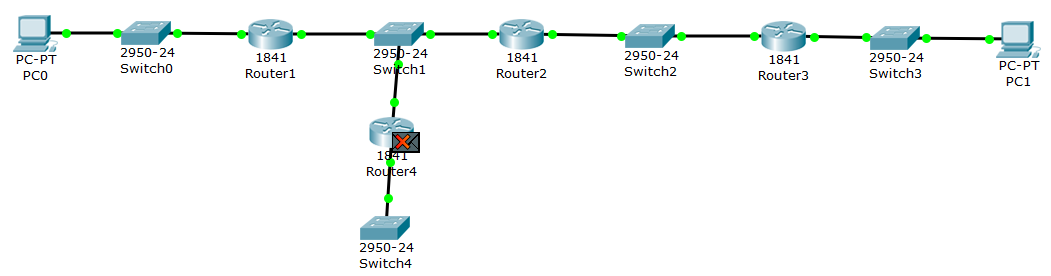
然后再次在PC0和PC1之间设置一个简单PDU，观察报文的传播路径，发现R1将IP分组转发给R4，导致IP分组无法到达PC1

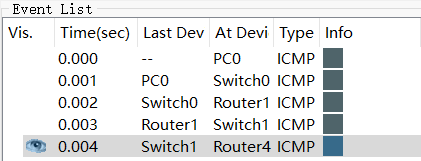




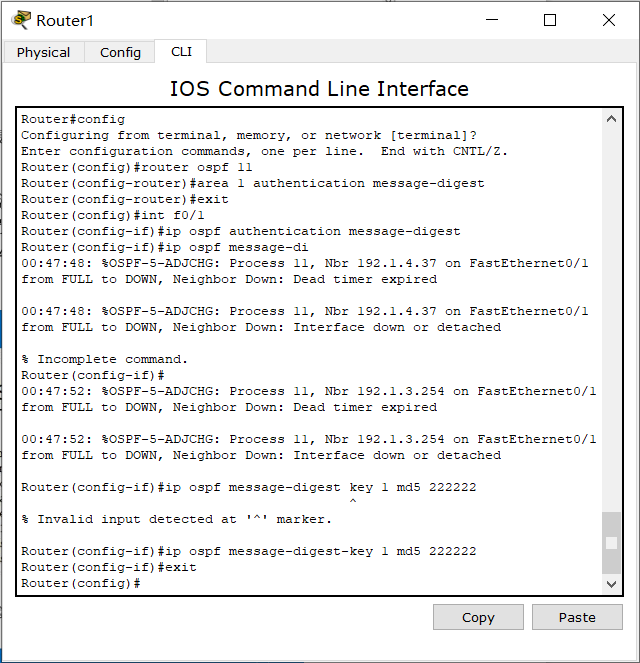


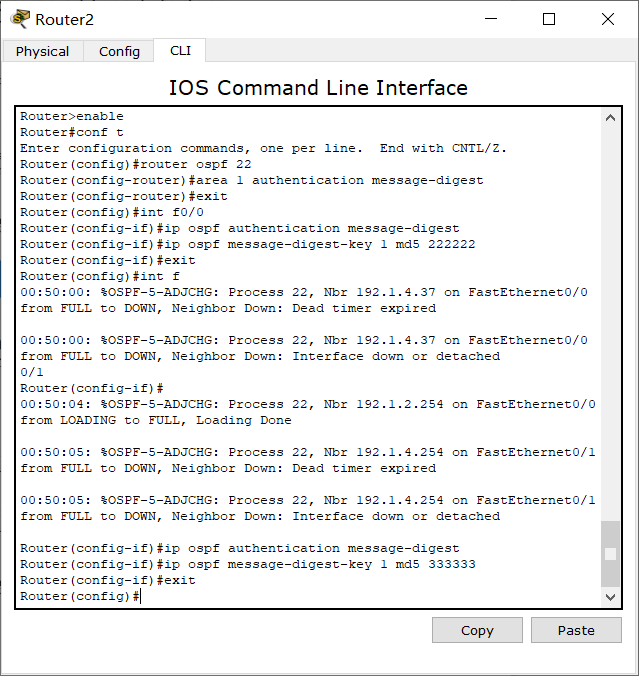


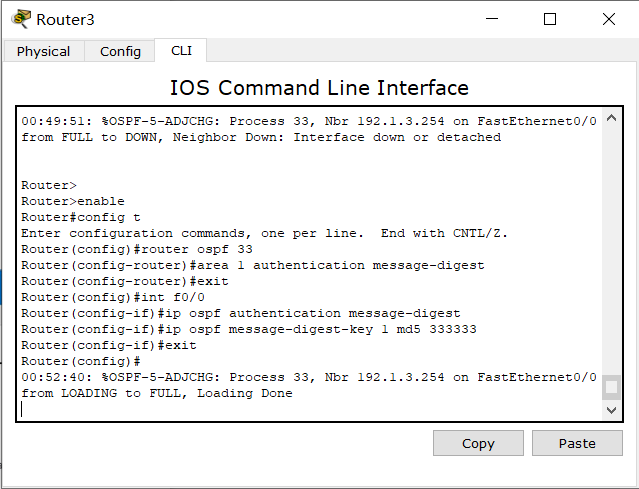




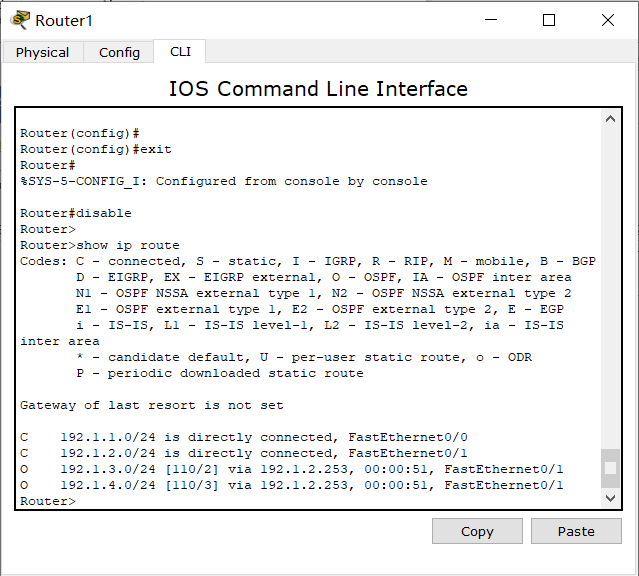
之后进行OSPF路由欺骗攻击的防护配置，完成R1、R2、R3与源端鉴别和完整性检测功能相关的配置，为相邻路由器实现互连的接口配置相同的密钥。







之后查看R1的路由表，发现R1通向192.1.4.0/24的路径又改为经过192.1.2.253，即经过R3最终到达PC1，这说明OSPF路由项欺骗攻击防御成功。



## 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？

在连接初始拓扑图并安排简单PDU时，一直使用put forward发现最后IP分组并不能从PC0到达PC1，而是在R3处报文无法继续传递。重新尝试第二次后发现报文又成功传递到了PC1。此时我反应过来，在我刚刚配置好各个路由器的所有端口ip时，路由器之间需要通过OSPF协议自学习路由表，因此在simulation模式下刚刚配置完PC0与PC1并不能通信。

通过该实验，我对OSPF路由表欺骗攻击有了基本的认识，同时对其防御有了基本的掌握，并通过实验对复习了OSPF协议。

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Packet Tracer不支持路由信息协议（RIP）的路由消息源端鉴别功能，但支持路由信息开放最短路径优先（OSPF）的路由消息源端鉴别功能，该实验线上完成，因此使用OSPF协议的路由消息源端鉴别功能。

# 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

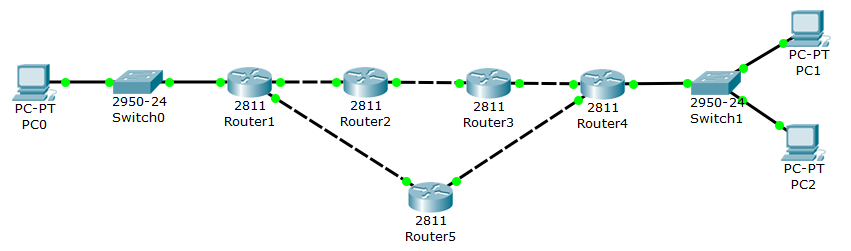
1. 使用自己的语言简述该实验原理。

该实验的目的是通过配置静态路由项，改变特定目的地的IP分组传输路径，以实现基于安全理由规避特定路由器的目的。

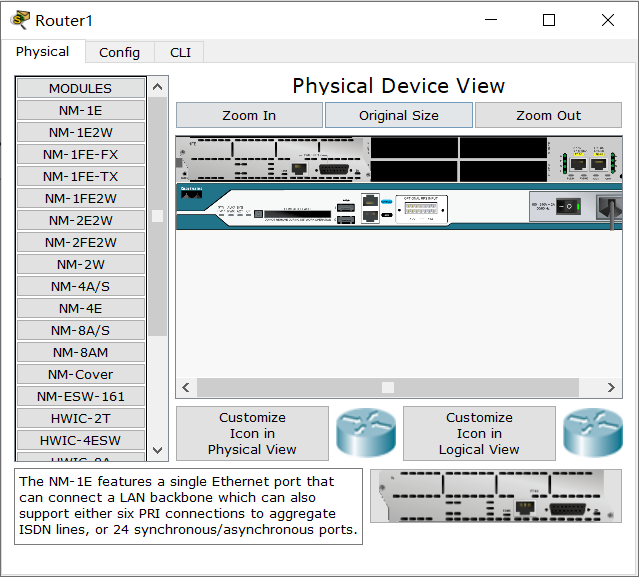
根据最长前缀匹配原则，配置掩码更长的静态路由项，其优先级高于RIP生成的动态路由项，因此，通过在路由器中添加一项目的网络为终端的IP地址，下一跳则为路由器的静态路由项，据此规避危险路由。

1. 实验步骤

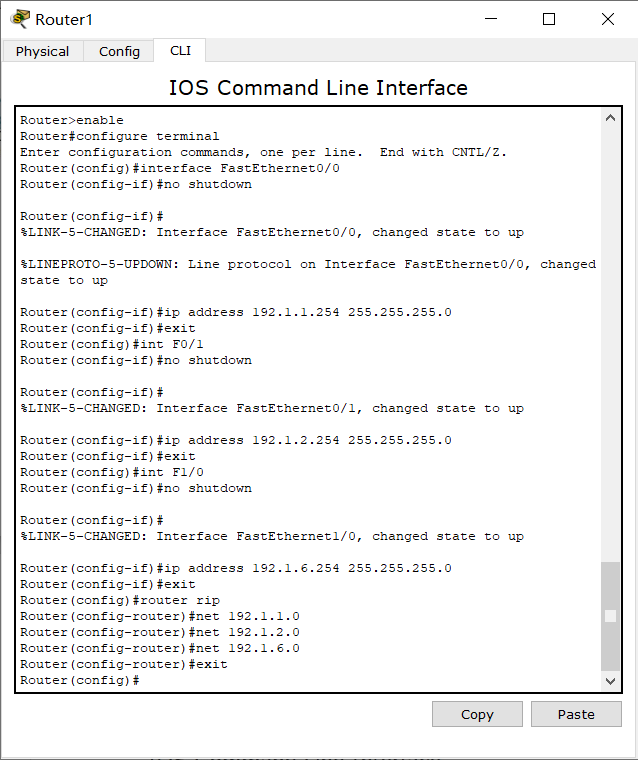
首先给出实验所引用的拓扑图。

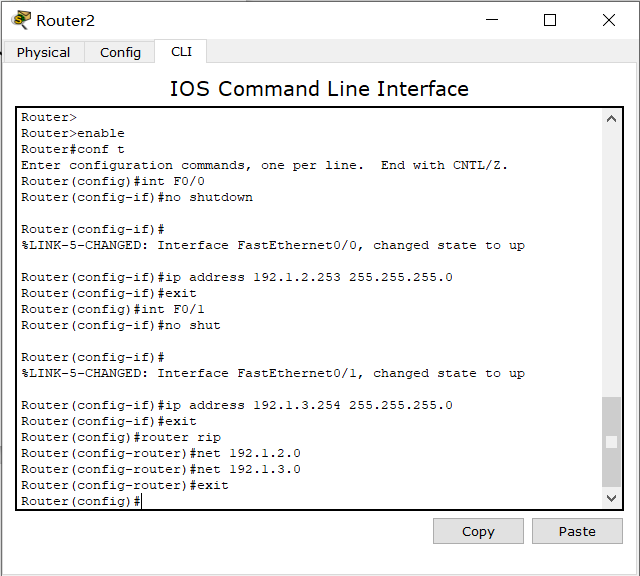


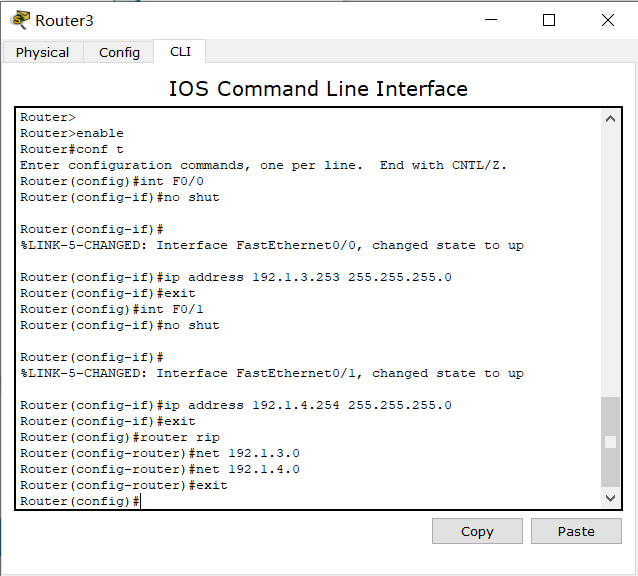
此处，由于R1和R4都需要三个以太网接口，而Ciso 2811默认只有两个以太网接口，因此需要再添加一个。关闭电源后，将NM-1FE1TX模块拖入路由器空槽中，再重新打开电源。

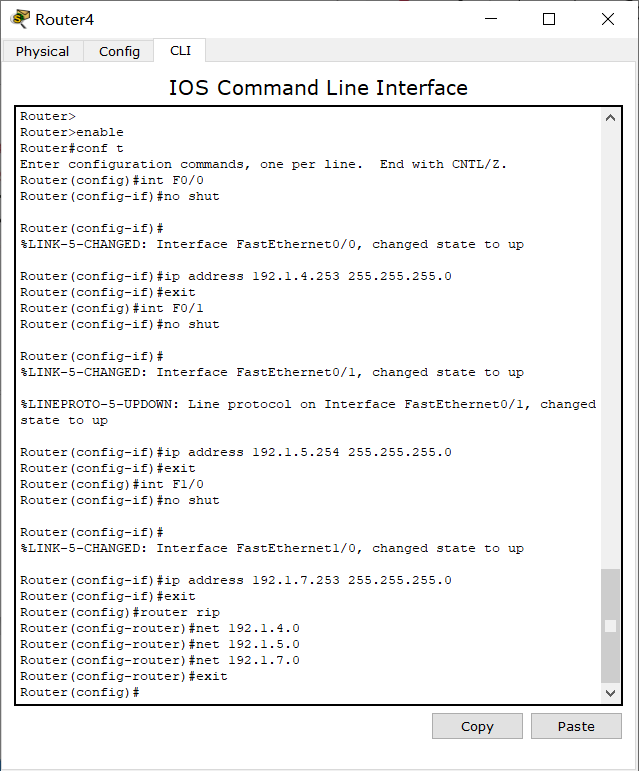


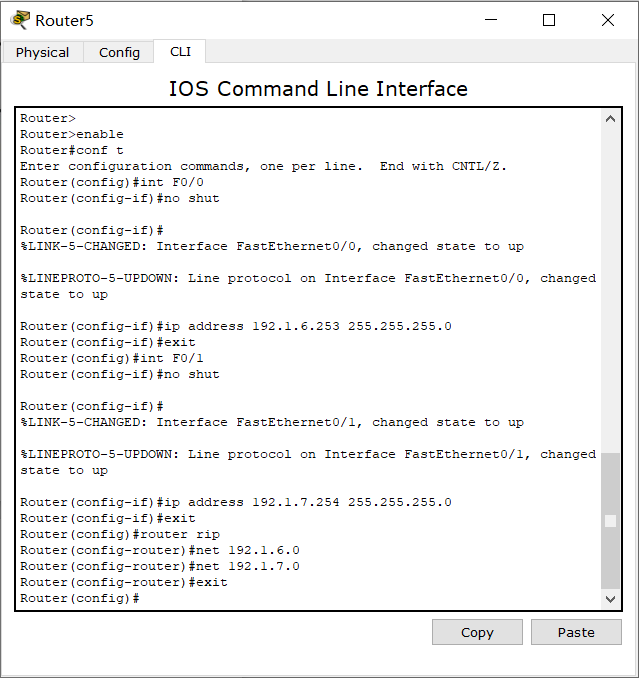
之后按照实验指导配置R1-R5的各端口IP地址，配置结果如图。



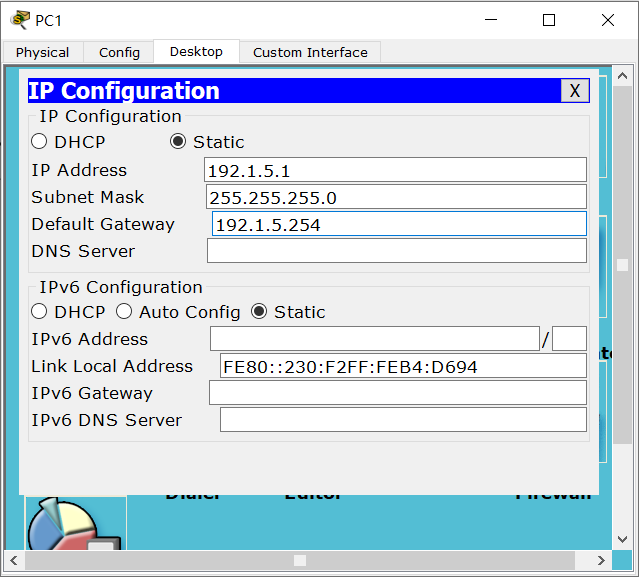
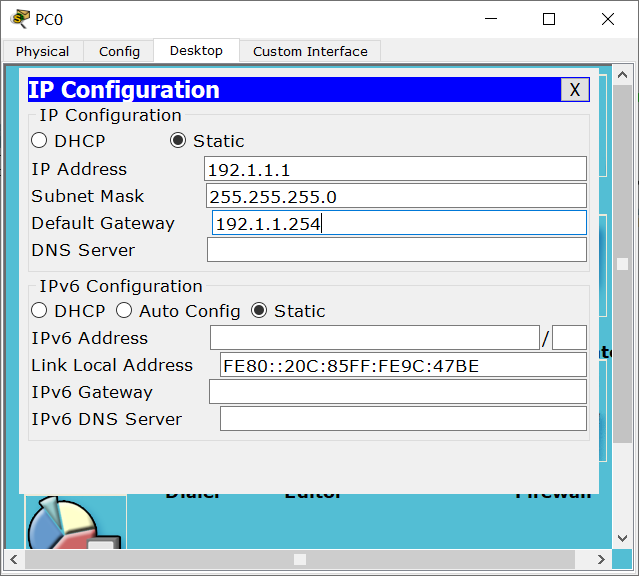


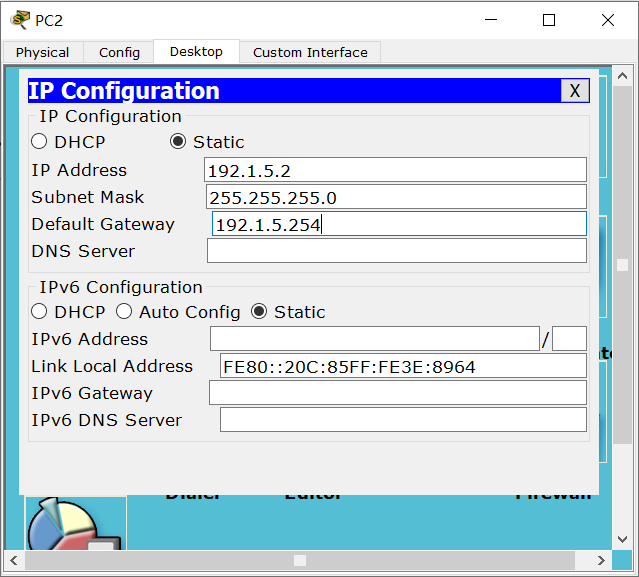




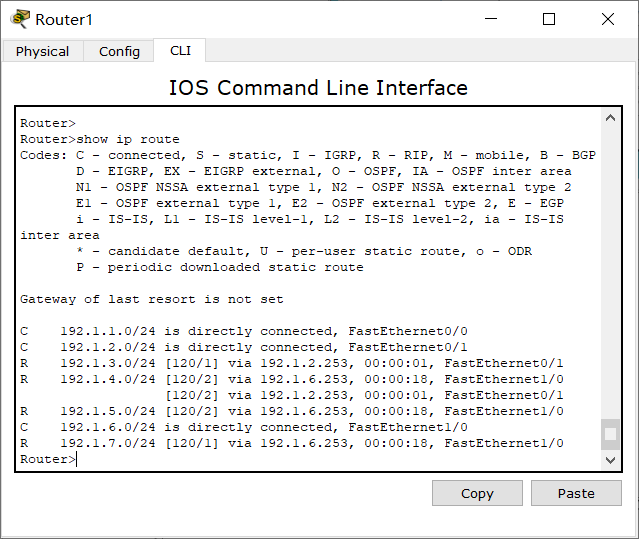


之后还需要配置PC0、PC1和PC2。

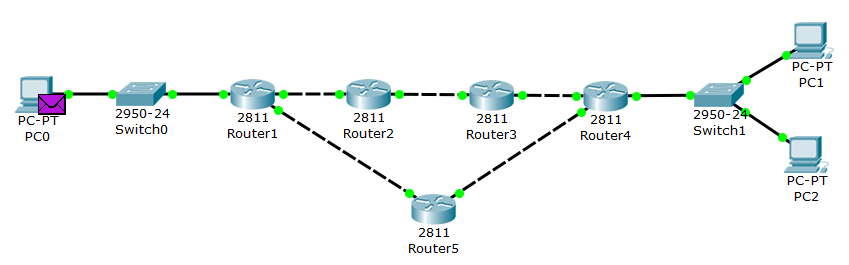


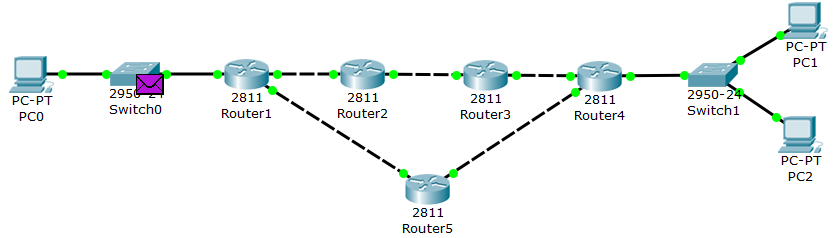


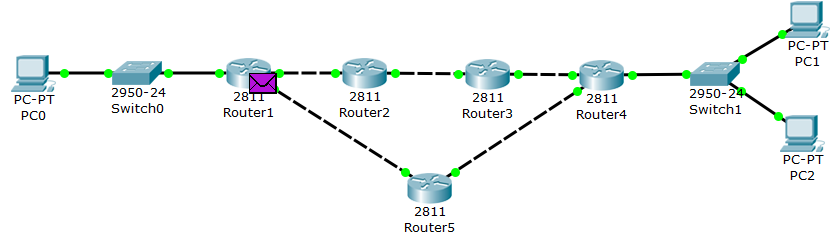
之后查看Router1的路由表，可以发现路由表中到达目的IP（192.1.5.0/24）的下一跳为R5（192.1.6.253，R5的E0/0端口）。

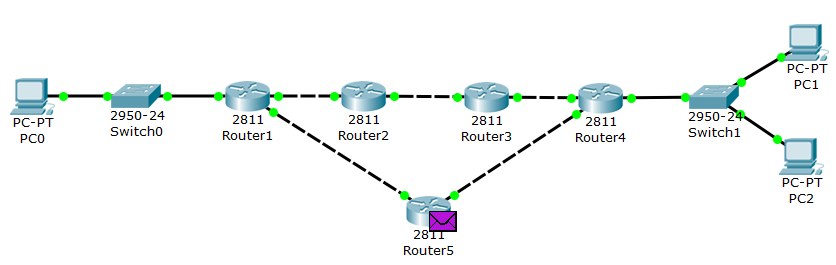


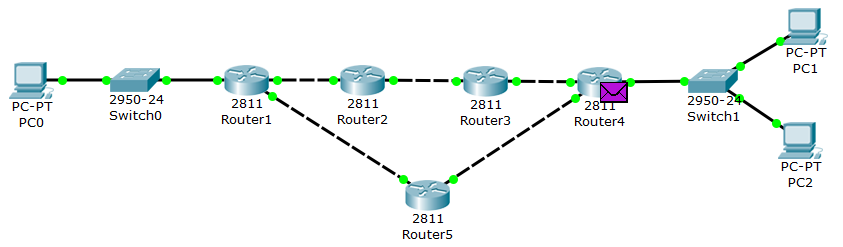
然后在PC0和PC1之间设置一个简单PDU，并开启仅查看ICMP报文，观察报文在PC0—PC1之间的传播路径（由于长度原因，原路返回的路径省略），可以发现该ICMP报文经过路由器R5。

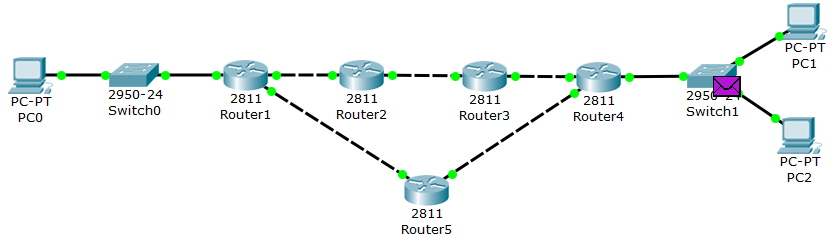


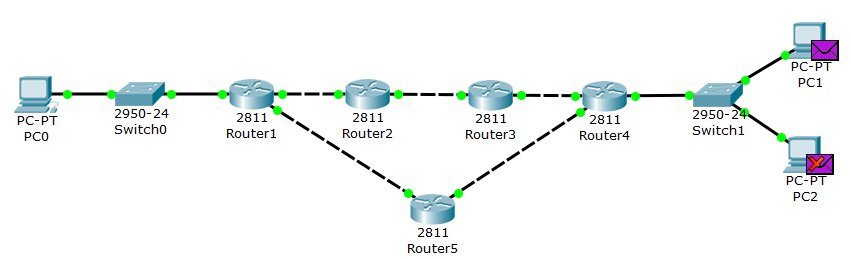


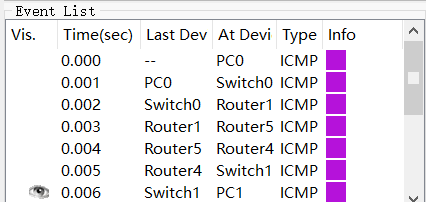




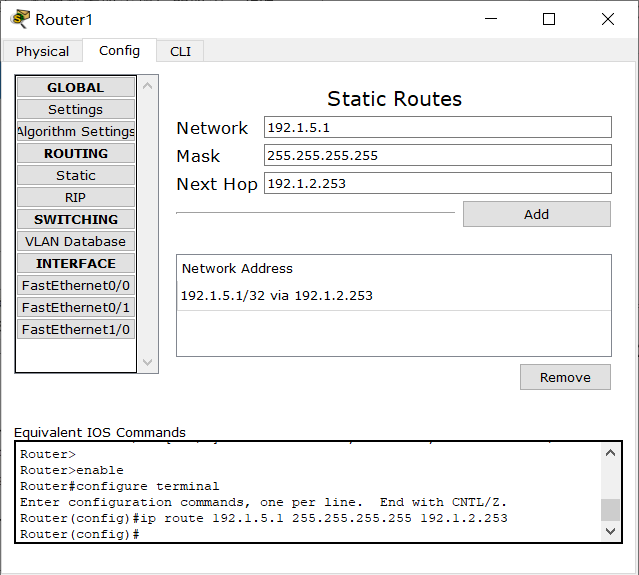




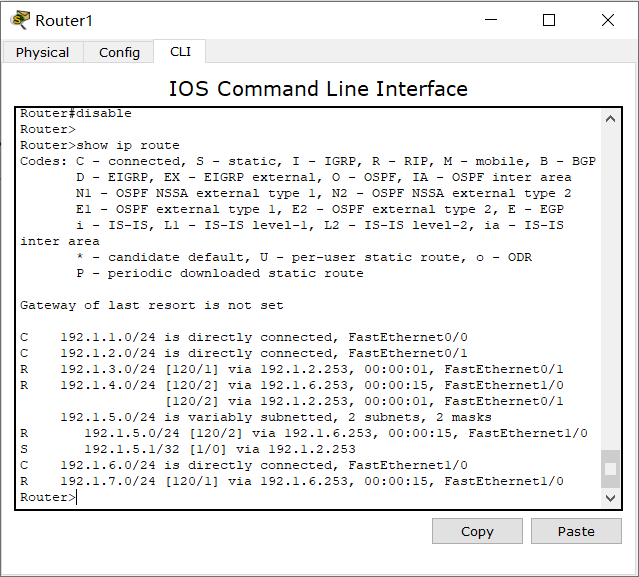




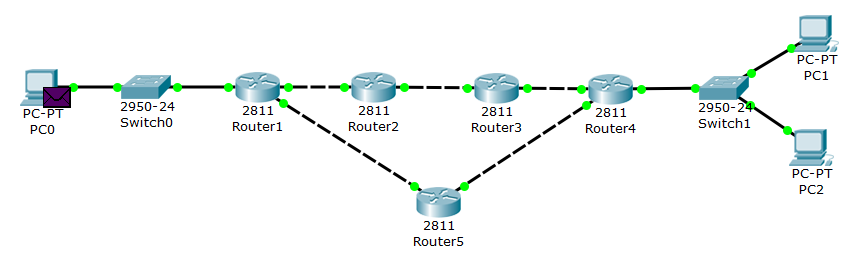
之后在R1中配置一项静态路由，目的网络是192.1.5.1/32，下一跳为192.1.2.253。

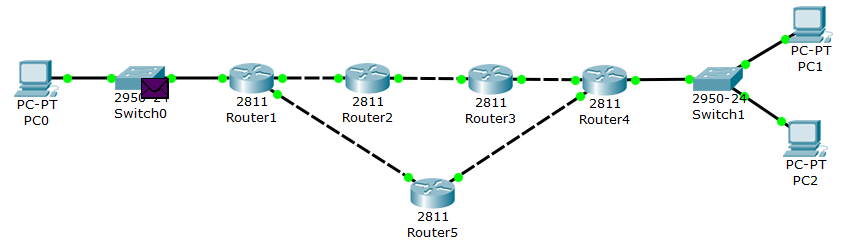


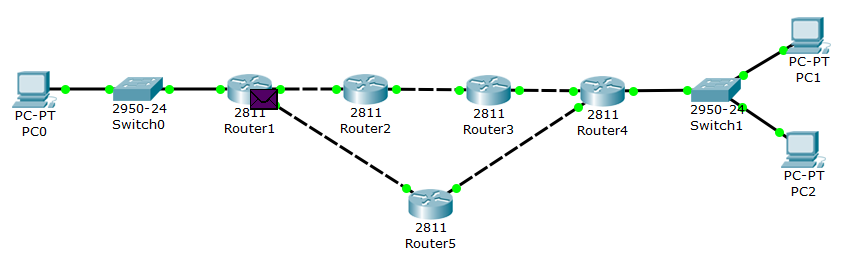
配置完成后再次查看R1的路由表，可以发现其中已经有了配置的静态路由。

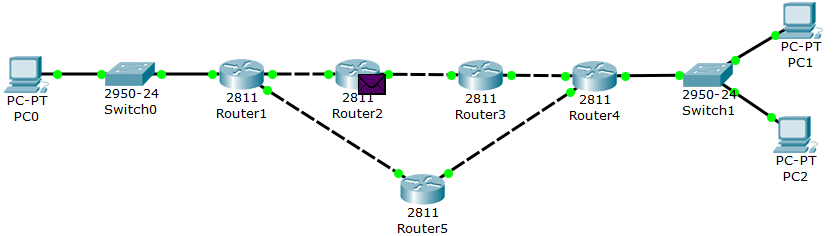


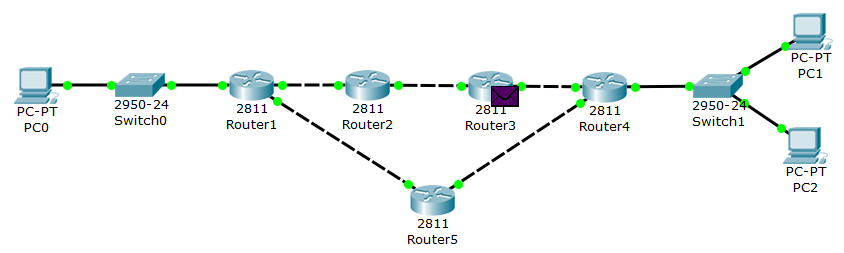
然后再次在PC0和PC1之间设置一个简单PDU，观察IP分组的传播路径，发现分组并不再通过R5到达PC1，而是通过R1 -> R2 -> R3 -> R4到达PC1。

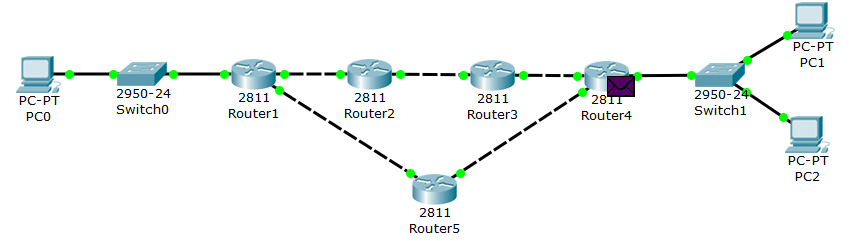


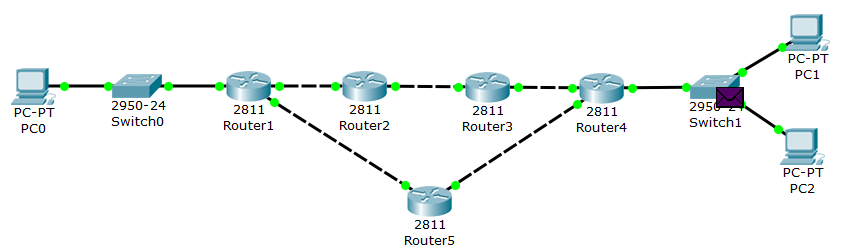


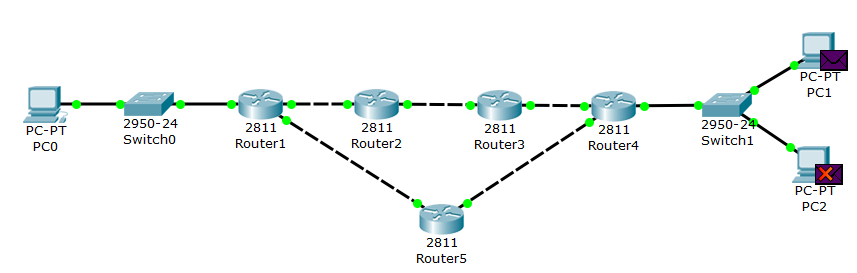


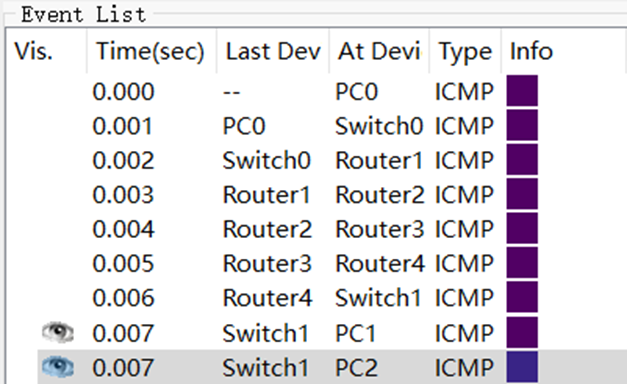




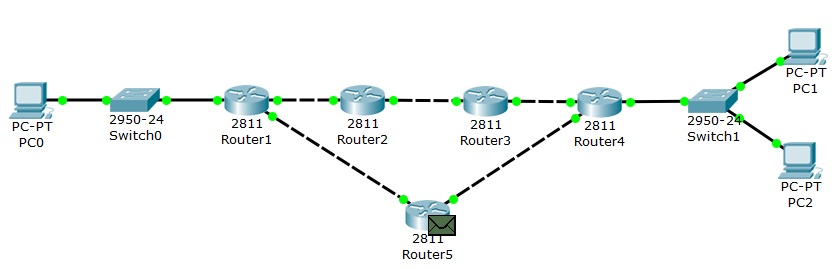


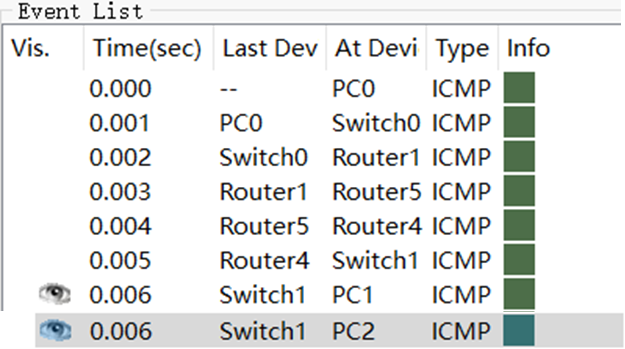






然后在PC0和PC2之间设置一个简单PDU，观察IP分组的传播路径，发现分组仍然会通过R5到达PC1。





## 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？

在配置了静态路由以后，并然后再次在PC0和PC1之间设置一个简单PDU，观察IP分组的传播路径时，发现分组从PC0到PC1时是通过R1 -> R2 -> R3 -> R4到达PC1，而返回报文仍然是R4 -> R5 -> R1到达PC0。思考可得是由于设置静态路由时仅仅设置了去方向，并没有规定回方向。在R4处同样配置静态路由后解决了该问题。

通过该实验，我对RIP策略路由有了基本的认识，同时对其应用有了基本的掌握，并通过实验再次复习了设备的rip配置过程。