**西安电子科技大学**

**计算机与网络安全 课程实验报告**

**实验名称 标准分组过滤器实验**

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 24 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） |

## 一、实验目的

1.验证标准分组过滤器过滤IP分组的原理和过程。

2.验证路由器标准分组过滤器的配置过程。

3.验证标准分组过滤器防御源 IP 地址欺骗攻击的原理和过程。

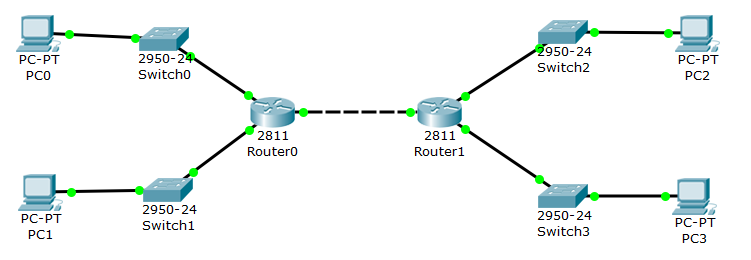
## 二、实验原理

路由器 R1 接口 1 和接口 2、路由器 R2 接口 2 和接口 3 的输入方向配置只允许输入源IP地址属于该接口连接的网络的网络地址的IP分组的标准分组过滤器，使这些接口连接的网络中的终端无法冒用其他网络的IP地址。

## 三、实验步骤

为了防止终端实施源IP地址欺骗攻击，路由器每一个接口只允许输入源IP地址属于该接口连接的网络的网络地址的IP分组。如路由器R1接口1连接的网络的网络地址是192.1.1.0/24，路由器R1接口1只允许输入源IP地址属于网络地址192.1.1.0/24的IP分组。

首先搭建如图所示的拓扑结构：



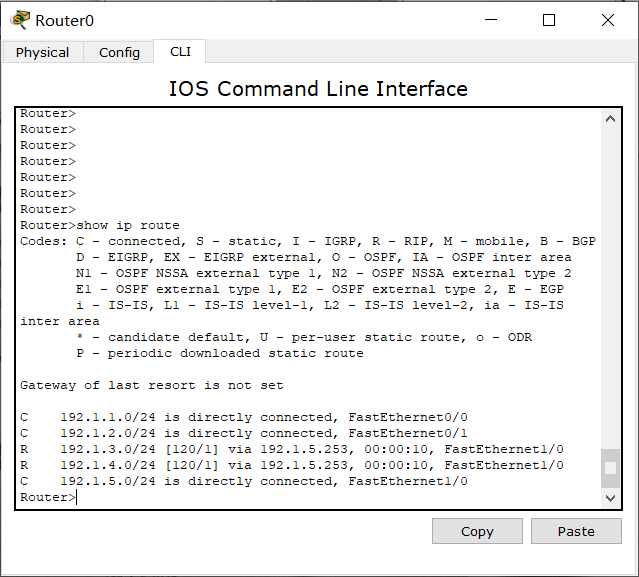
首先进入Router0的CLI选项卡，通过命令行对其进行配置。分别进入其相连的端口，开启端口并分配指定的IP地址，并在路由器上设置192.1.1.0和192.1.2.0网络的RIP协议。之后配置访问控制列表ACL 1和2，ACL 1用于E0/0，允许来自192.1.1.0/24的流量并拒绝其他流量；ACL 2用于E0/1，允许来自192.1.2.0/24的流量，并拒绝其他流量

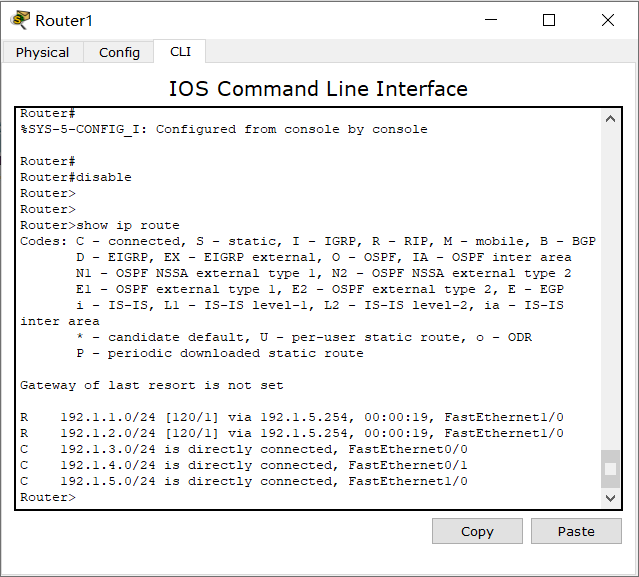


Router1与Router0操作流程类似，仅ip配置和ACL过滤ip不同。

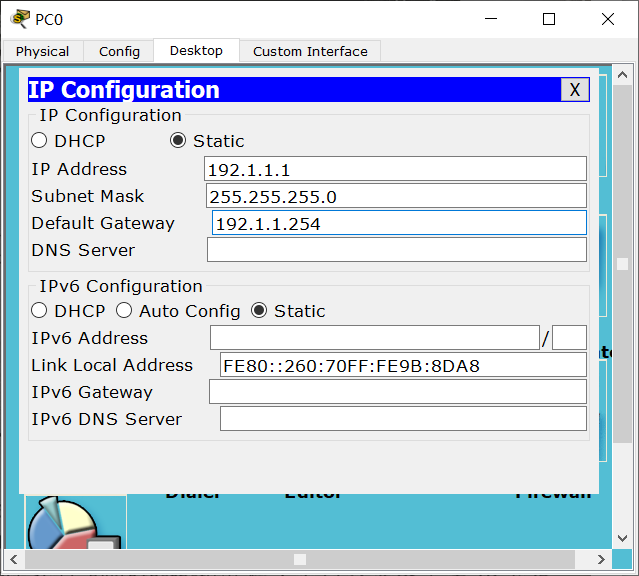


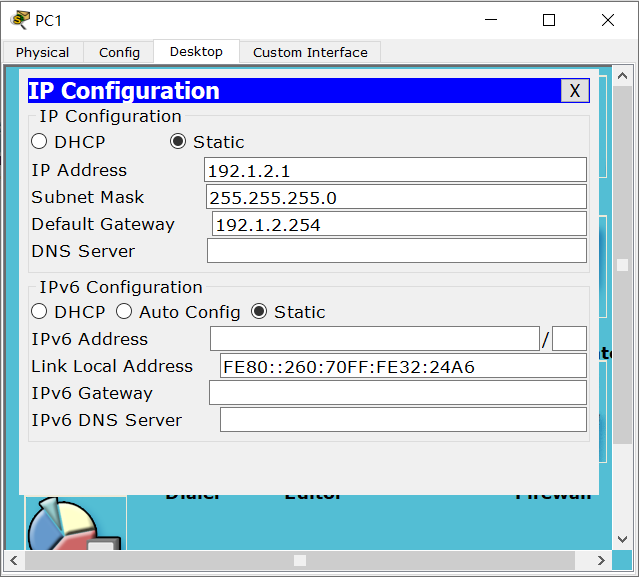
完成配置过程后，可以查看R0和R1的路由表。由路由表可知，路由器通过RIP协议，在理论上使得R0和R1的四个端口可以相互通信。

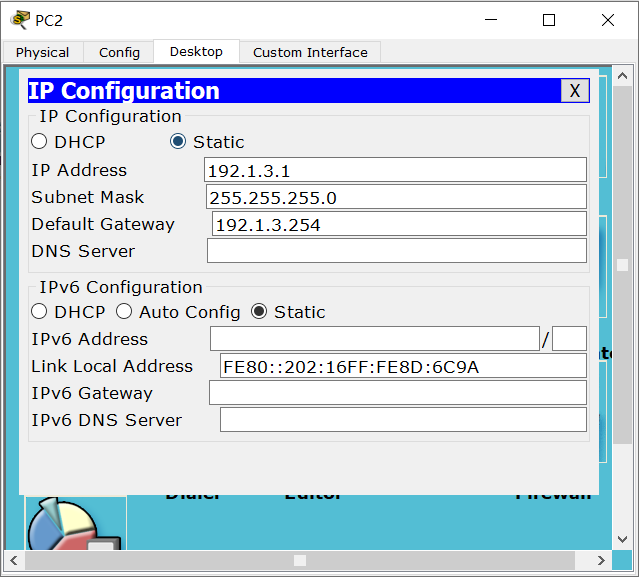


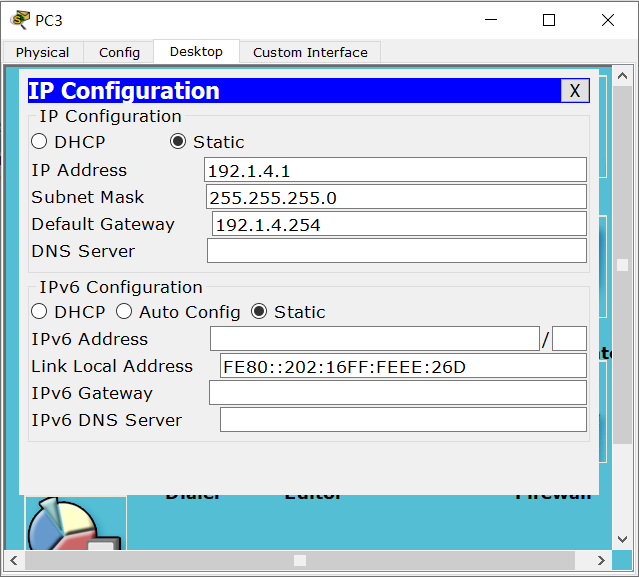


之后配置PC0-PC3的IP地址与默认网关。

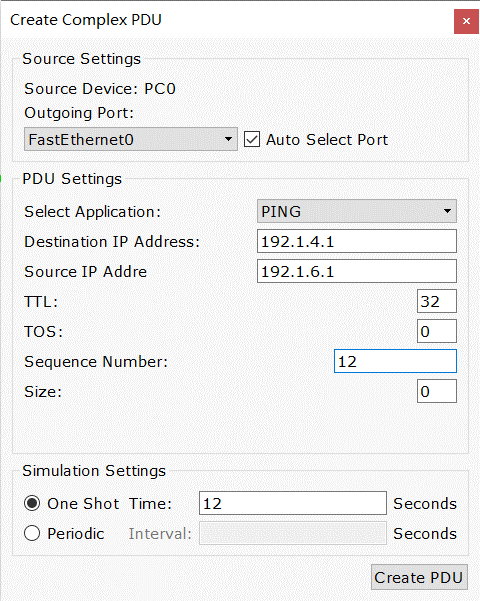








之后创建复杂PDU，用来模拟进入R0端口E0/0的，ACL规则之外的报文。



进入实时模式，观察报文发送步骤。可以发现，由于R0的ACL 1，R0的E0/0端口仅允许ip地址为192.1.1.0/24的数据报进入该端口，因此丢弃该IP分组。

