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

|  |  |
| --- | --- |
| 实验时间： | 2021年10月29日 |

|  |  |
| --- | --- |
| 实验名称： | IOS路由器IP Sec VPN实验和标准分组过滤器实验 |

|  |  |
| --- | --- |
| 实验成绩： |  |

IOS路由器IP Sec VPN实验

一、实验目的

(1)掌握ISAKMP策略配置过程。

(2)掌握IP Sec参数配置过程。

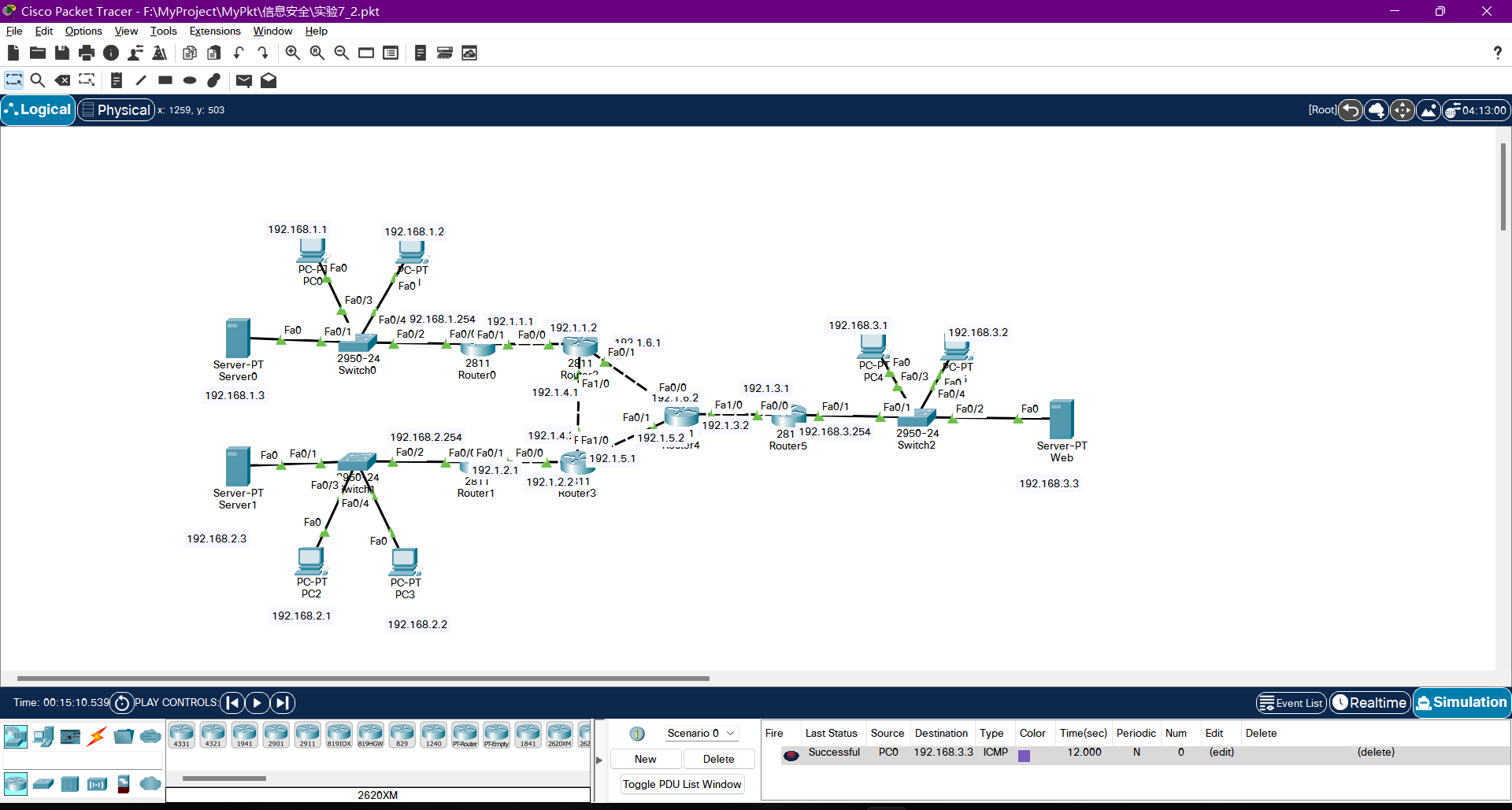
(3)验证IP Sec安全关联建立过程。

(4)验证封装安全净荷(Encapsulating Security Payload, ESP)报文的封装过程。

(5)验证基于IP Sec VPN的数据传输过程。

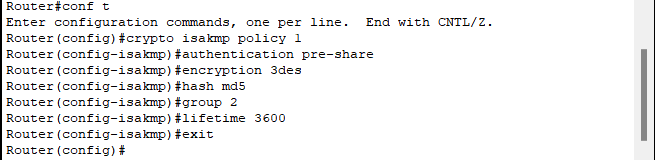
二、实验步骤

1. 在实验7.1的基础上进行该实验：

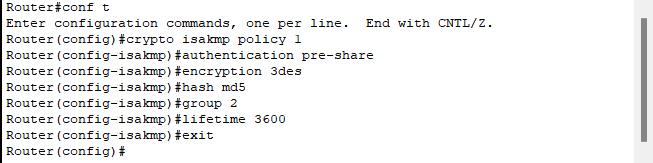


1. 完成三个路由器隧道两端安全策略配置过程：

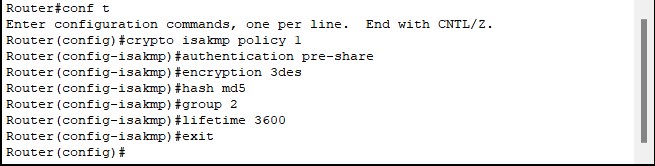
Router0：



Router1：

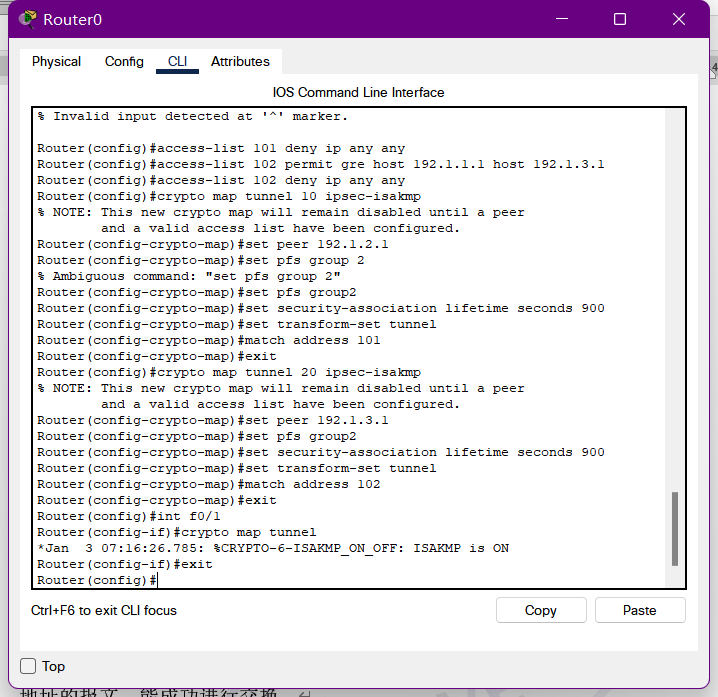


Router5：

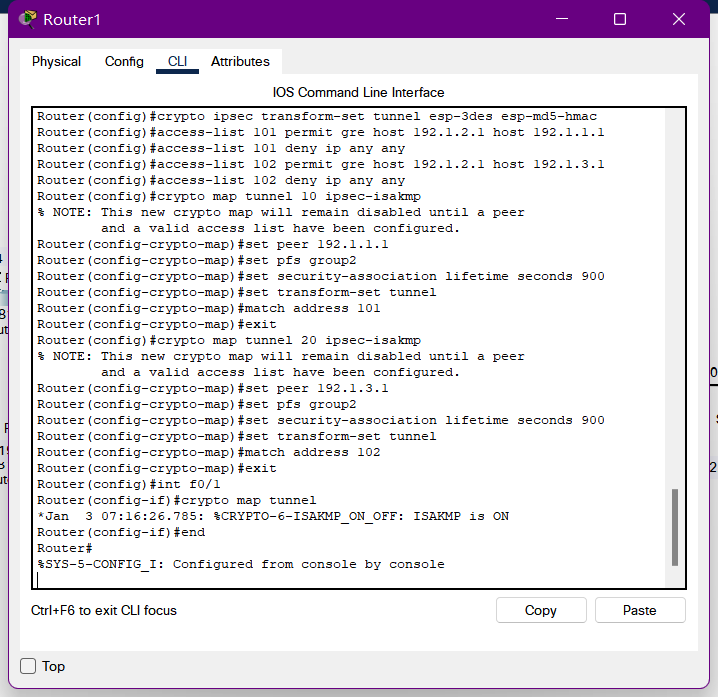


1. 建立安全传输通道、安全关联、配置分组过滤器：

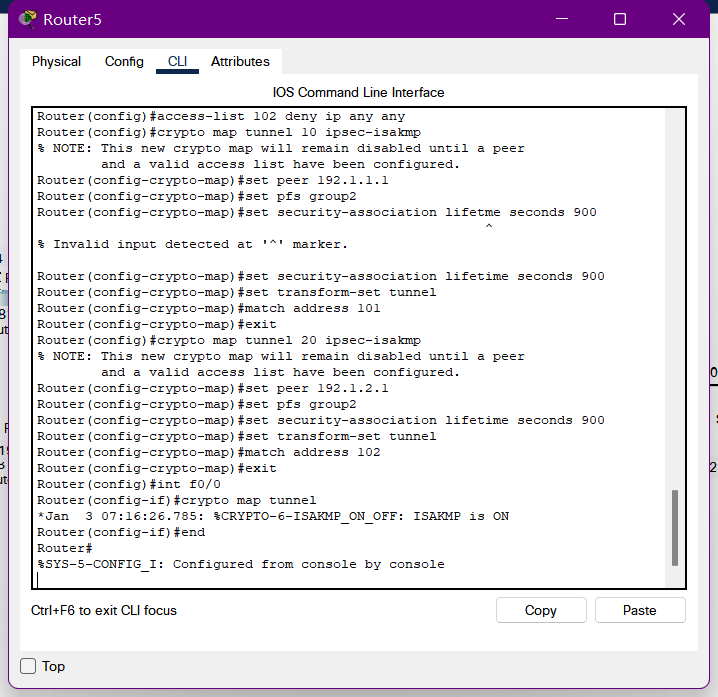
Router0：



Router1：



Router5：



三、实验结果及分析

IP Sec协议就是一种实现内层IP分组经过隧道安全通信的协议。通过ISAKMP在隧道两端之间建立IP Sec安全关联，将内层IP分组封装成ESP报文后，再经过隧道传输，ISAKMP分两阶段完成隧道两端之间IP Sec安全建立过程，第一阶段是建立安全传输通道，在这一阶段，隧道两端需要约定加密算法、保温摘要算法、鉴别方式和DH组号；第二阶段是建立IP Sec安全关联，在这一阶段，隧道两端需要约定安全协议、加密算法和散列消息鉴别码(Hashed Message Authentication Codes, HMAC)算法。

四、实验总结及体会

通过该实验，了解到点对点IP隧道只能解决由公共网络实现互联的内部子网之间的通信问题，但不能实现内部子网之间的安全通信。该实验学习到了要想实现安全通信，需要对隧道两端的路由器实现双向身份鉴别，以免发生假冒内部子网与其他内部子网通信的情况保证经过公共网络传输的数据的完整性和保密性。

标准分组过滤器实验

一、实验目的

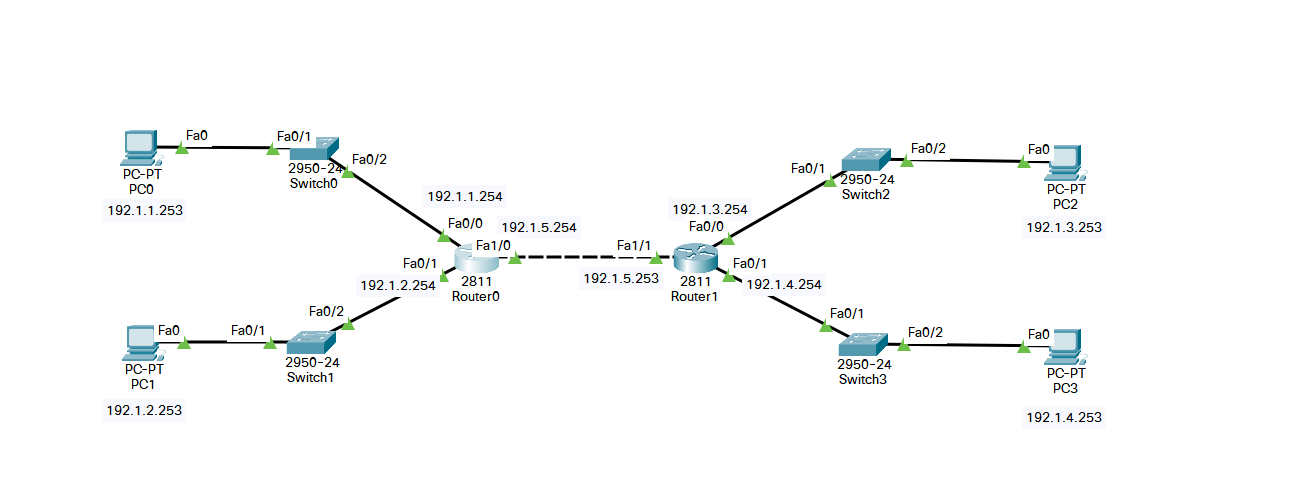
(1)验证标准分组过滤器IP分组的原理和过程。

(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。

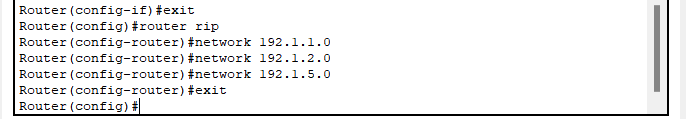
二、实验步骤

1. 完成实验的拓扑图，并配置好网络信息：

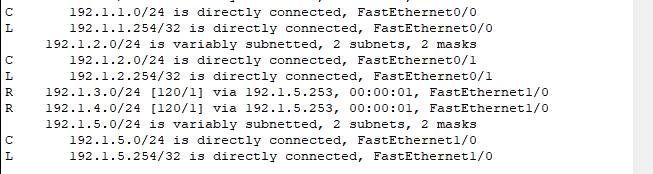


1. 完成路由器0和路由器1的RIP配置；

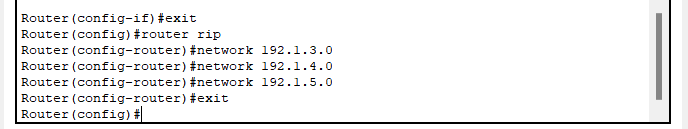
Router0：



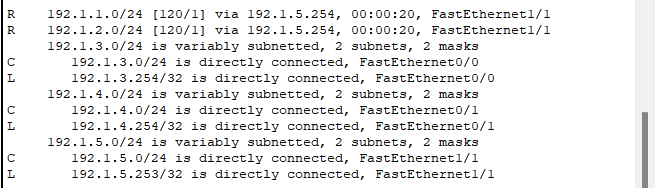
路由表：

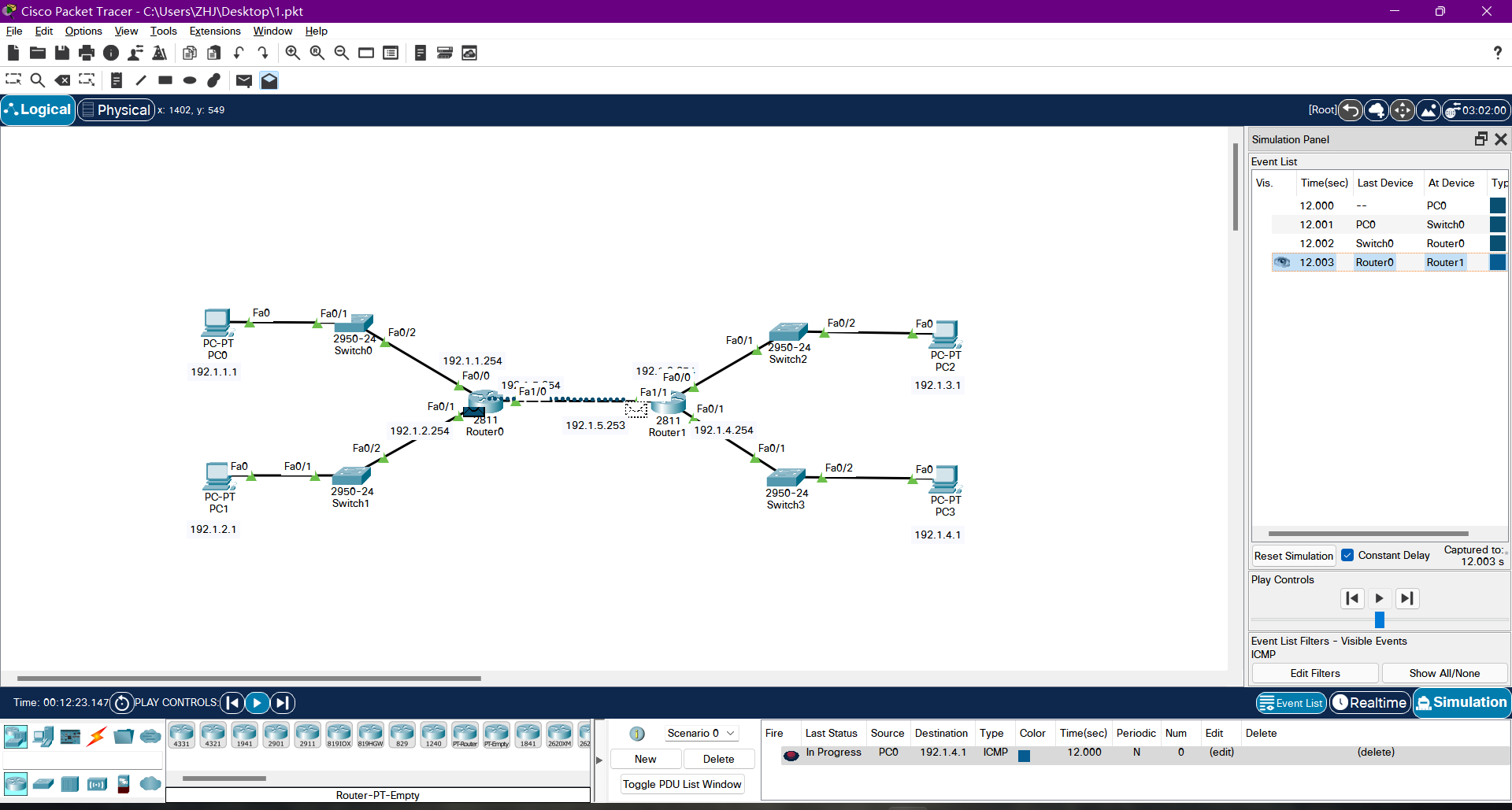


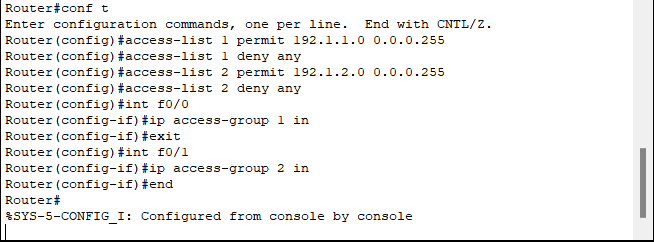
Router1：



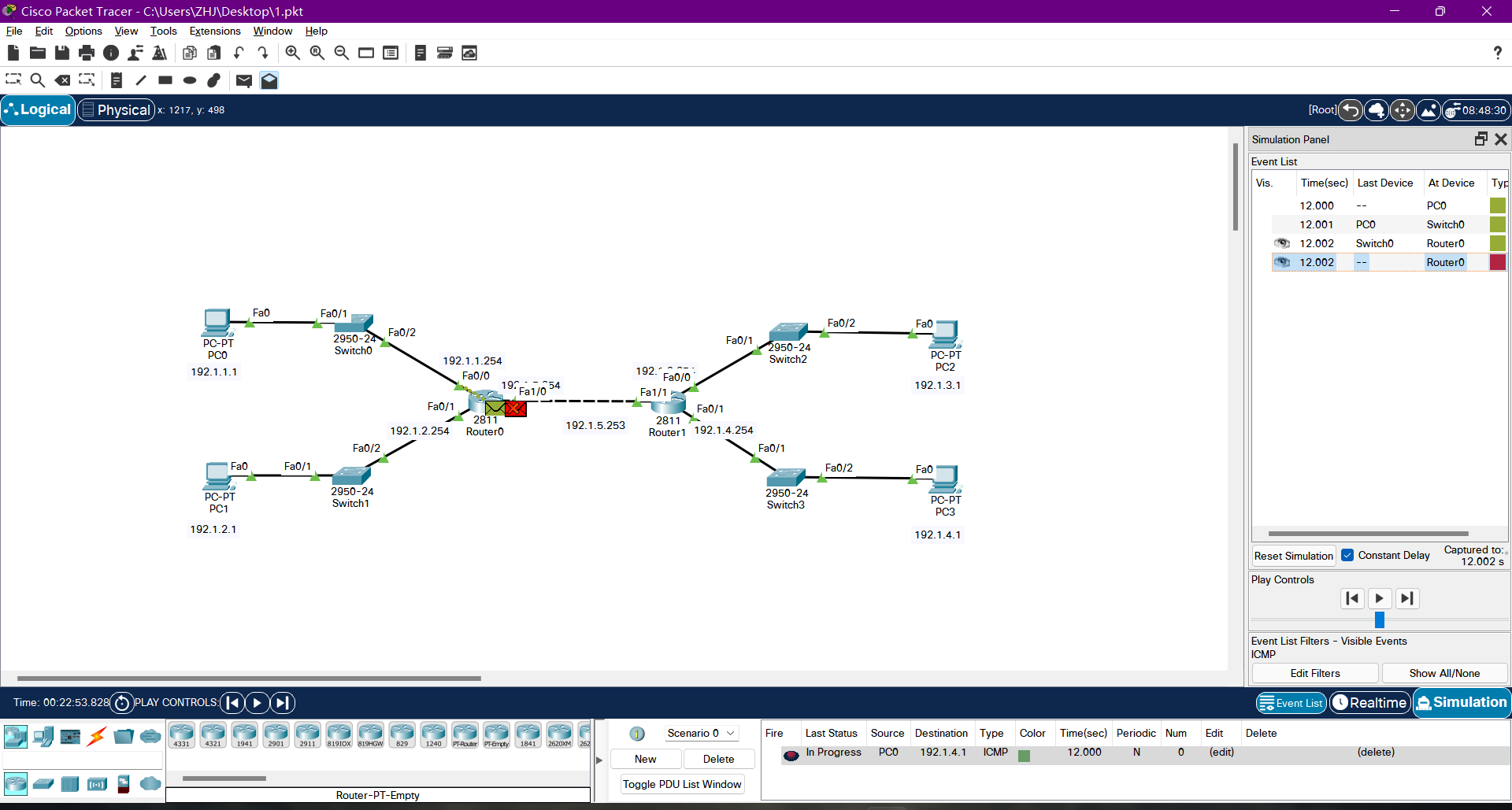
路由表：



1. 切换模拟操作模式，在PC0上创建ICMP报文，封装该报文的IP分组的源（伪造IP地址为192.1.6.1）和目的IP地址：
2. 切换到实时操作模式完成路由器0标准分组过滤器配置，作用到F0/0接口输入方向，使得Router0只允许继续转发源IP地址属于CIDR地址快192.1.1.0/24的IP分组：



1. 重复操作(3)，此时Router0的F0/0接口输入方向丢弃该IP分组：



三、实验结果及分析

在仅设置两个路由器的RIP协议时，建立PC0到PC3的ICMP报文，并将该报文封装为源地址为伪造的192.1.6.1\24时，路由器0正常转发伪造源IP地址的IP分组。在完成路由器0标准分组过滤器配置过程后，路由器0的F0/0，F0/1接口只允许输入源地址属于该接口连接的网络的网络地址的IP分组，之后再伪造源地址为192.1.6.1\24发送从PC0到PC3的ICMP报文，路由器0会丢弃该IP分组。

四、实验总结及体会

通过该实验，我们学会了配置标准分组过滤器过程，access-list-number用来指定配置的规则所属的标准分组过滤器的编号，permit和deny是指定对符合条件的IP分组实施的动作。