

《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：



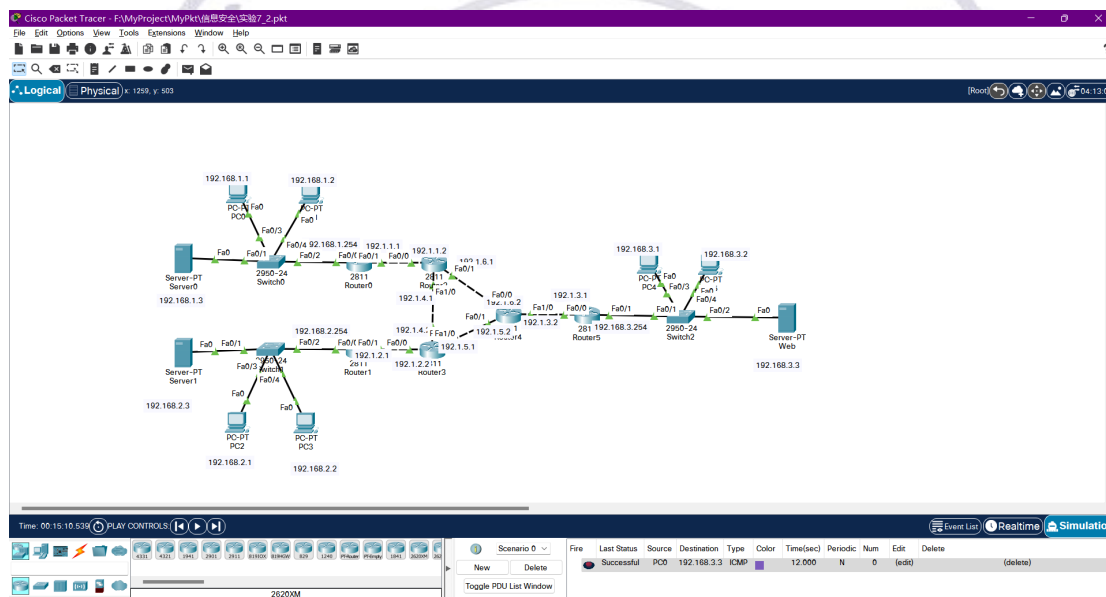
IOS 路由器 IP Sec VPN 实验

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：



- (2) 完成三个路由器隧道两端安全策略配置过程：

Router0:

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 3600
Router(config-isakmp)#exit
Router(config)#
```

Router1:

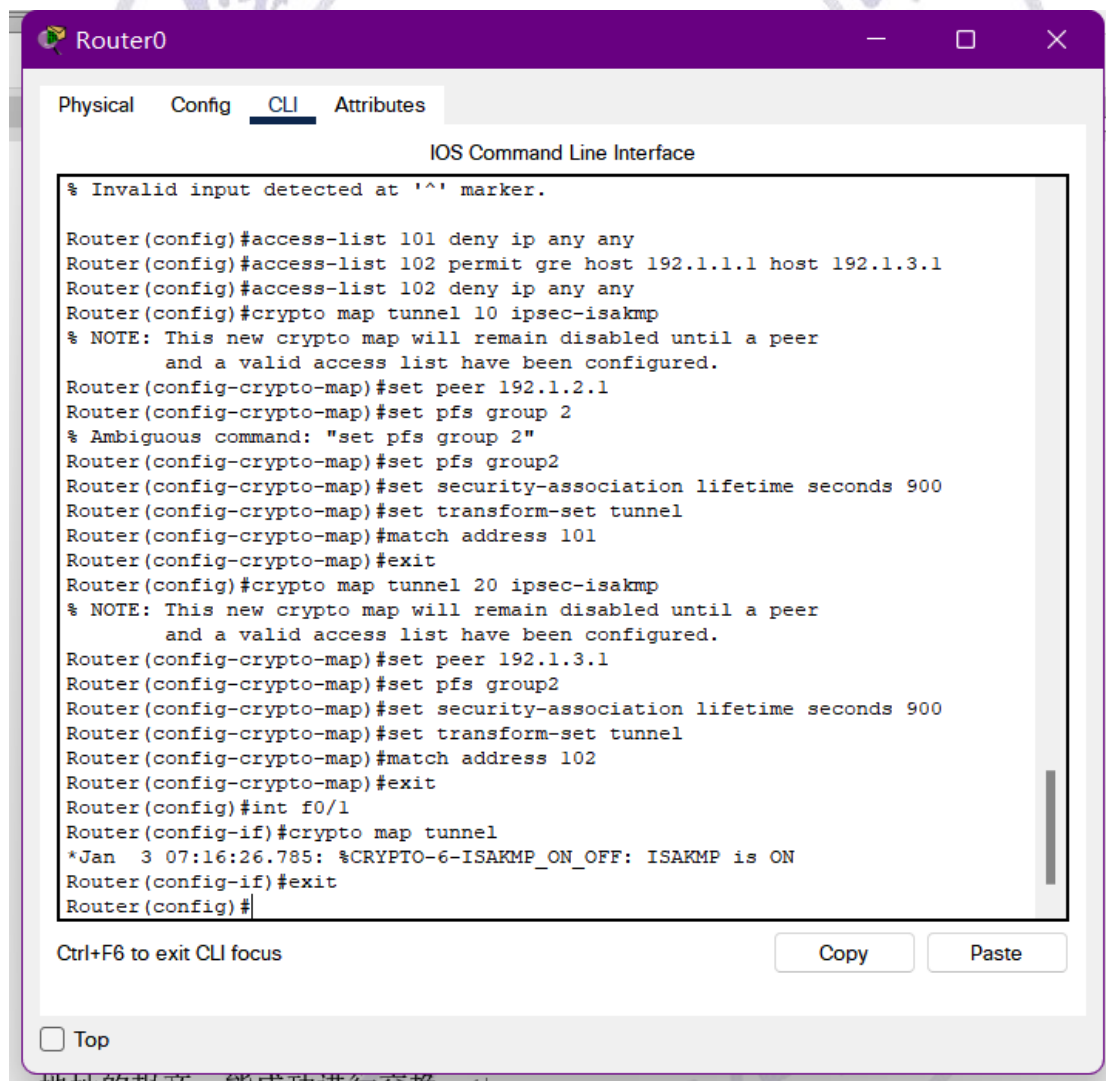
```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 3600
Router(config-isakmp)#exit
Router(config)#
```

Router5:

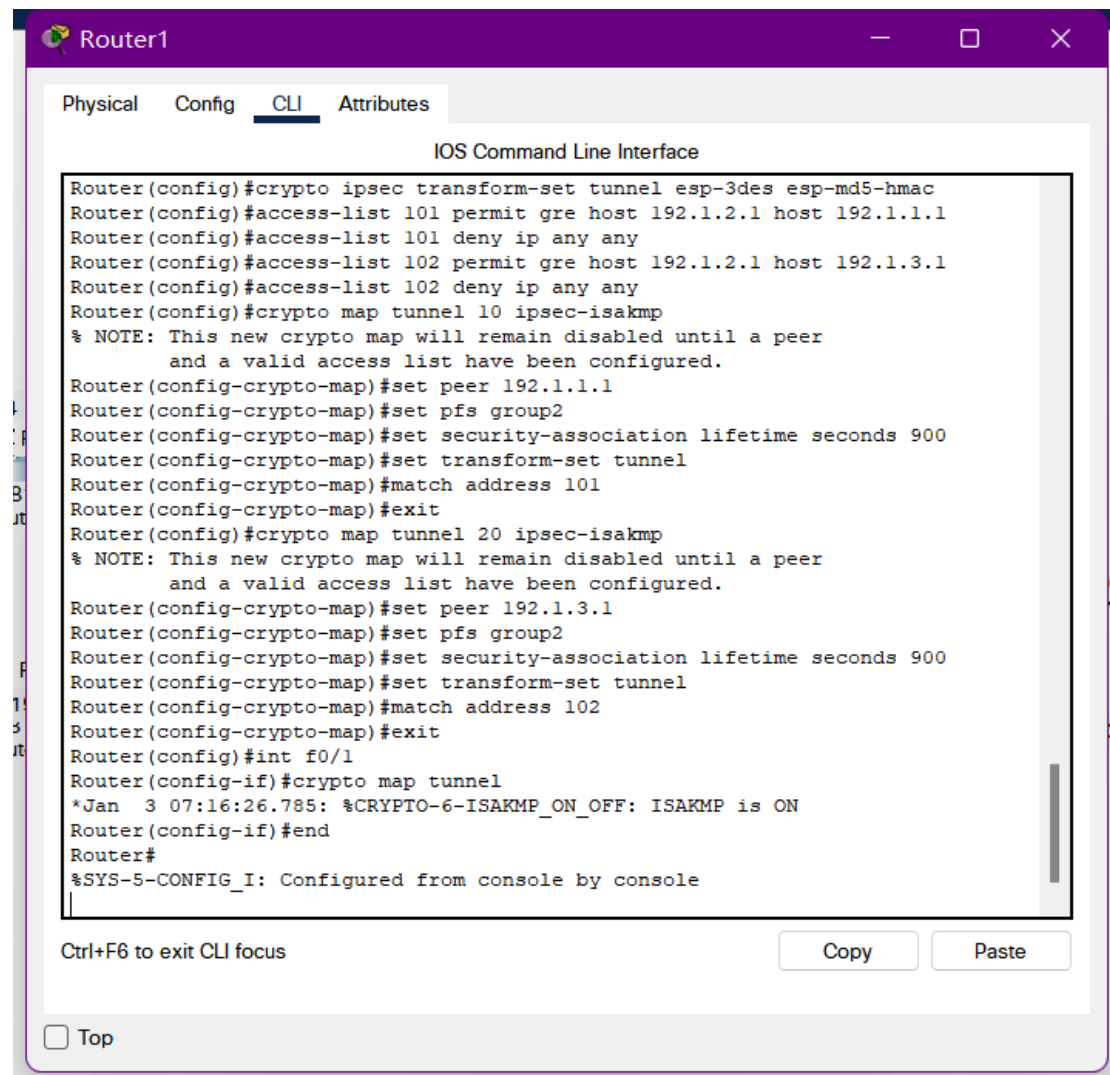
```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 3600
Router(config-isakmp)#exit
Router(config)#
```

(3) 建立安全传输通道、安全关联、配置分组过滤器:

Router0:



Router1:



The screenshot shows a web-based interface for a Cisco router named 'Router1'. The 'CLI' tab is selected, displaying the IOS Command Line Interface. The configuration includes two IPsec tunnels, each using a transform set of ESP-3DES and ESP-MD5-HMAC. Tunnel 10 is configured with peer 192.1.1.1 and matches access list 101. Tunnel 20 is configured with peer 192.1.3.1 and matches access list 102. Both tunnels use ISAKMP for peer authentication. The interface also shows the physical configuration of interface f0/1 and the system configuration mode.

```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

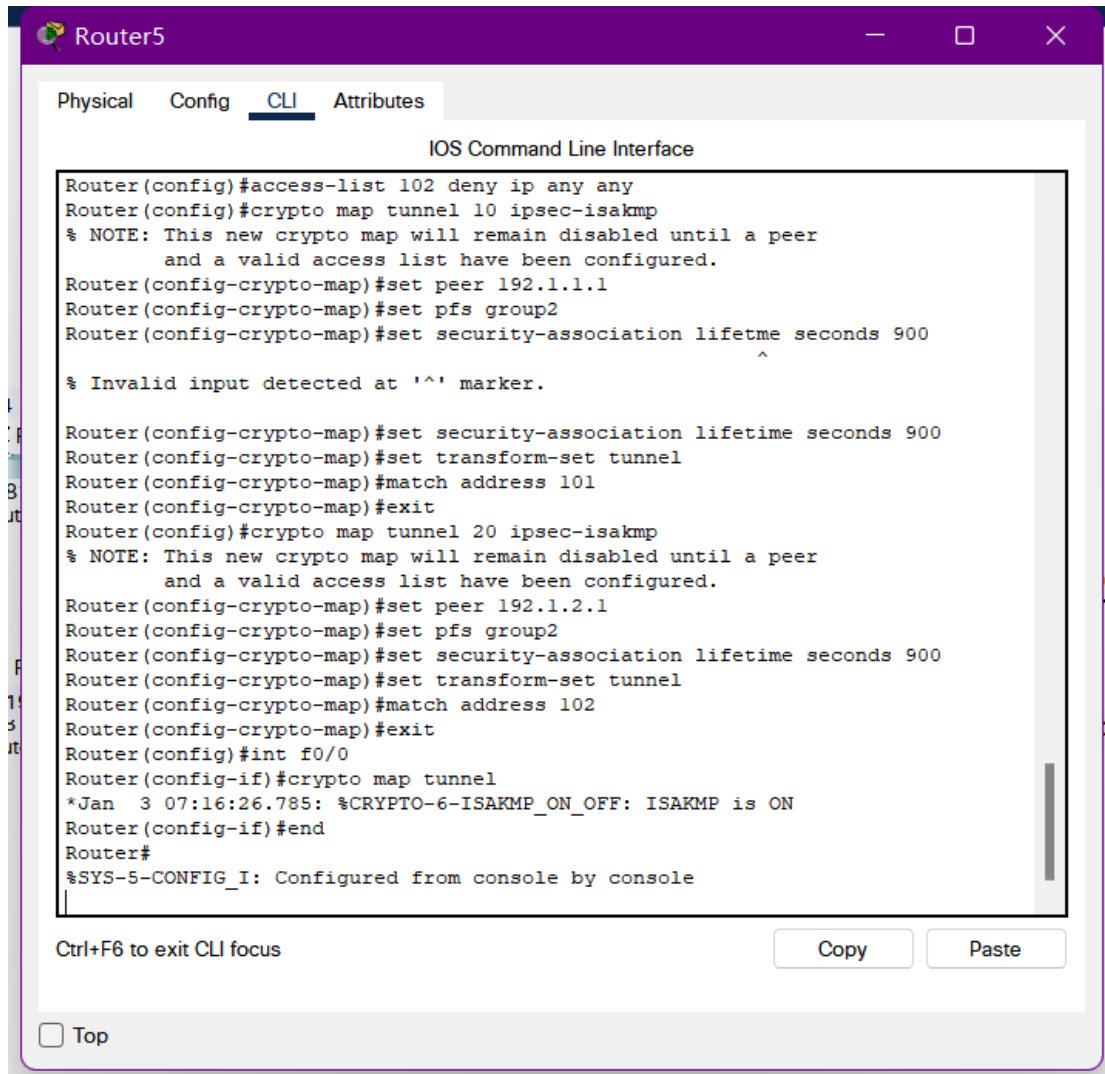
Router(config)#crypto ipsec transform-set tunnel esp-3des esp-md5-hmac
Router(config)#access-list 101 permit gre host 192.1.2.1 host 192.1.1.1
Router(config)#access-list 101 deny ip any any
Router(config)#access-list 102 permit gre host 192.1.2.1 host 192.1.3.1
Router(config)#access-list 102 deny ip any any
Router(config)#crypto map tunnel 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.1.1.1
Router(config-crypto-map)#set pfs group2
Router(config-crypto-map)#set security-association lifetime seconds 900
Router(config-crypto-map)#set transform-set tunnel
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#exit
Router(config)#crypto map tunnel 20 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.1.3.1
Router(config-crypto-map)#set pfs group2
Router(config-crypto-map)#set security-association lifetime seconds 900
Router(config-crypto-map)#set transform-set tunnel
Router(config-crypto-map)#match address 102
Router(config-crypto-map)#exit
Router(config)#int f0/1
Router(config-if)#crypto map tunnel
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

Router5:



```
Router5
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#access-list 102 deny ip any any
Router(config)#crypto map tunnel 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.1.1.1
Router(config-crypto-map)#set pfs group2
Router(config-crypto-map)#set security-association lifetime seconds 900
^
% Invalid input detected at '^' marker.
Router(config-crypto-map)#set security-association lifetime seconds 900
Router(config-crypto-map)#set transform-set tunnel
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#exit
Router(config)#crypto map tunnel 20 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 192.1.2.1
Router(config-crypto-map)#set pfs group2
Router(config-crypto-map)#set security-association lifetime seconds 900
Router(config-crypto-map)#set transform-set tunnel
Router(config-crypto-map)#match address 102
Router(config-crypto-map)#exit
Router(config)#int f0/0
Router(config-if)#crypto map tunnel
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

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。



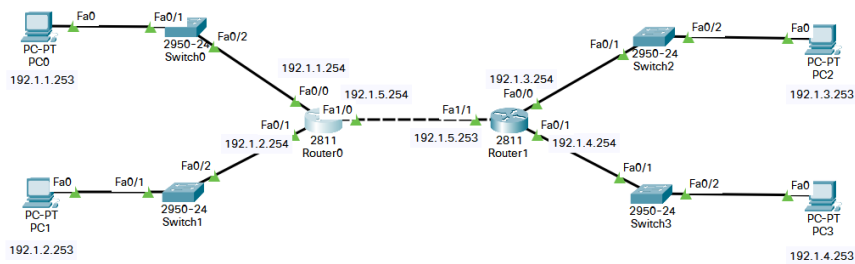
标准分组过滤器实验

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：



- (2) 完成路由器 0 和路由器 1 的 RIP 配置；

Router0:

```
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.1.0
Router(config-router)#network 192.1.2.0
Router(config-router)#network 192.1.5.0
Router(config-router)#exit
Router(config)#
```

路由表:

```
C    192.1.1.0/24 is directly connected, FastEthernet0/0
L    192.1.1.254/32 is directly connected, FastEthernet0/0
     192.1.2.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.2.0/24 is directly connected, FastEthernet0/1
L    192.1.2.254/32 is directly connected, FastEthernet0/1
R    192.1.3.0/24 [120/1] via 192.1.5.253, 00:00:01, FastEthernet1/0
R    192.1.4.0/24 [120/1] via 192.1.5.253, 00:00:01, FastEthernet1/0
     192.1.5.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.5.0/24 is directly connected, FastEthernet1/0
L    192.1.5.254/32 is directly connected, FastEthernet1/0
```

Router1:

```

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.1.3.0
Router(config-router)#network 192.1.4.0
Router(config-router)#network 192.1.5.0
Router(config-router)#exit
Router(config)#

```

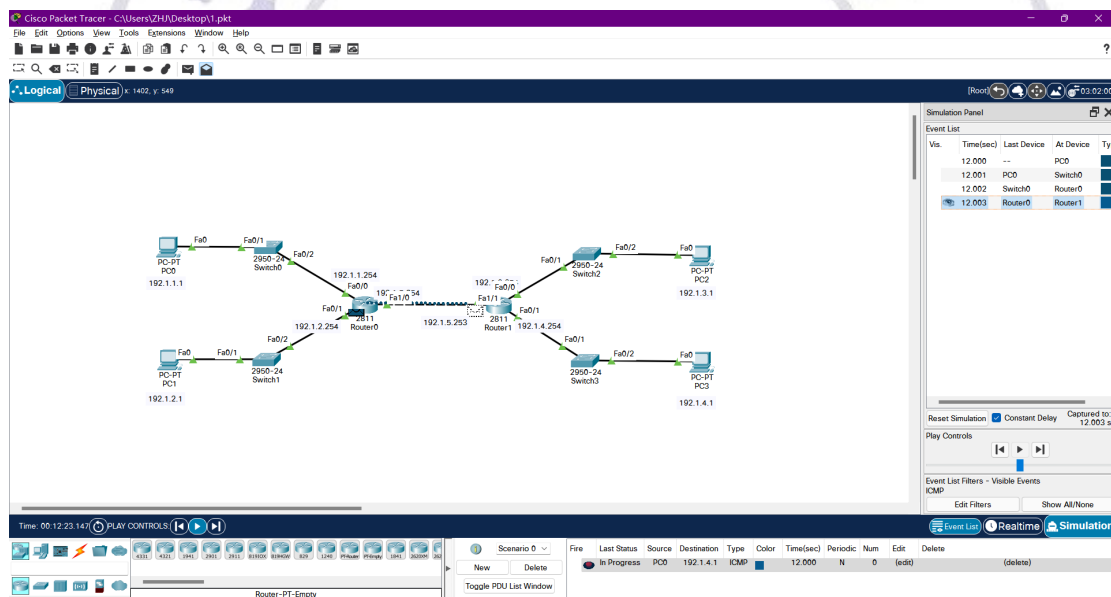
路由表：

```

R   192.1.1.0/24 [120/1] via 192.1.5.254, 00:00:20, FastEthernet1/1
R   192.1.2.0/24 [120/1] via 192.1.5.254, 00:00:20, FastEthernet1/1
C   192.1.3.0/24 is variably subnetted, 2 subnets, 2 masks
L   192.1.3.0/24 is directly connected, FastEthernet0/0
L   192.1.3.254/32 is directly connected, FastEthernet0/0
C   192.1.4.0/24 is variably subnetted, 2 subnets, 2 masks
L   192.1.4.0/24 is directly connected, FastEthernet0/1
L   192.1.4.254/32 is directly connected, FastEthernet0/1
C   192.1.5.0/24 is variably subnetted, 2 subnets, 2 masks
L   192.1.5.0/24 is directly connected, FastEthernet1/1
L   192.1.5.253/32 is directly connected, FastEthernet1/1

```

(3) 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：



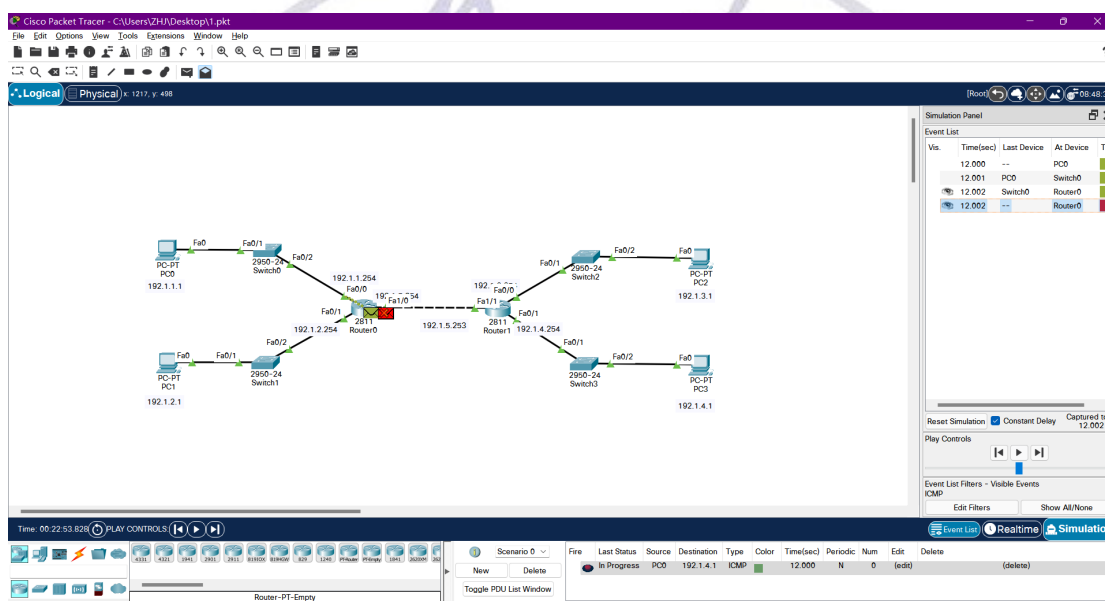
(4) 切换到实时操作模式完成路由器 0 标准分组过滤器配置，作用到 F0/0 接口输入方向，使得 Router0 只允许继续转发源 IP 地址属于 CIDR 地址块 192.1.1.0/24 的 IP 分组：


```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 1 permit 192.1.1.0 0.0.0.255
Router(config)#access-list 1 deny any
Router(config)#access-list 2 permit 192.1.2.0 0.0.0.255
Router(config)#access-list 2 deny any
Router(config)#int f0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
Router(config)#int f0/1
Router(config-if)#ip access-group 2 in
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

```

(5) 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。

