**江苏科技大学**

**课程实验报告**

课 程： 计算机网络与安全

课 题： 防火墙配置与应用

学 院： 计算机学院

姓 名： 陈四贵

班 级： 1822107101

学 号： 182210710119

指导老师： 张笑非

目 录

[一、 实验目的 1](#_Toc59043707)

[二、 实验条件 1](#_Toc59043708)

[三、 实验步骤 1](#_Toc59043709)

[标准访问控制列表 1](#_Toc59043710)

[扩展访问控制列表 2](#_Toc59043711)

[四、 实验记录 2](#_Toc59043712)

[五、 实验结果分析与心得 4](#_Toc59043713)

[六、 思考题 4](#_Toc59043714)

# 实验目的

1. 根据实验要求的拓扑结构，利用路由器及交换机连接成网络；

2. 根据要求对数据流进行分类，并配置相应的 ACL；

3. 选择最佳部署位置的路由器，开启基于包过滤的防火墙功能；

4. 将 ACL 绑定到正确接口，并指定其作用于接口的正确队列。

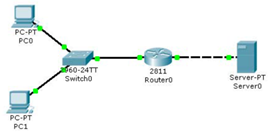
# 实验条件

1. 创建标准访问控制列表；

2. 创建扩展访问控制列表；

3. 将ACL绑定到路由器的接口。

# 实验步骤



### 标准访问控制列表

配置示例：

Step 1：创建标准ACL，拒绝来自某IP子网的所有分组

Router0# config terminal

Router0(confg)# access-list 1 deny 192.168.1.0 0.0.0.255

Router0(config)# access-list 1 permit any

Step 2：将ACL 绑定到路由器接口上

Router0(config)# interface fa0/0

Router0(config‐if)# ip access-group 1 in

Step 3：测试网络的连通性并记录结果

Step 4：清除该策略no ip access-group 1 in

### 扩展访问控制列表

配置示例：

Step 1：创建扩展ACL，拒绝来自某套接字的分组

Router0# config terminal

Router0(config)# access-list 100 deny tcp 192.168.1.2 0.0.0.0 192.168.2.2 0.0.0.0 eq www

Router0(config)# access-list 100 permit ip any any

Step 2：将ACL绑定到路由器接口上

Router0(config)# interface fa0/0

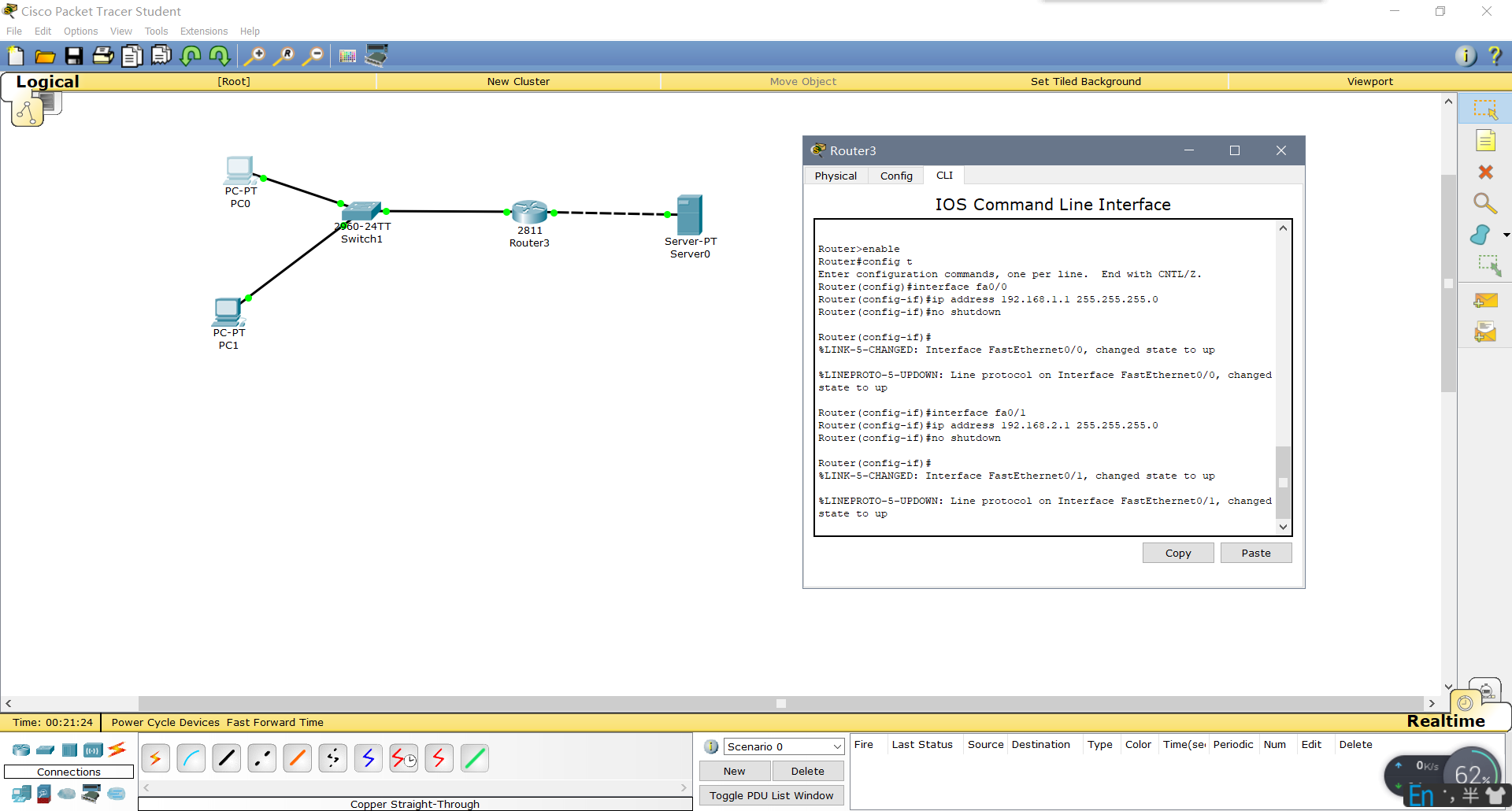
Router0(config‐if)# ip access-group 100 in

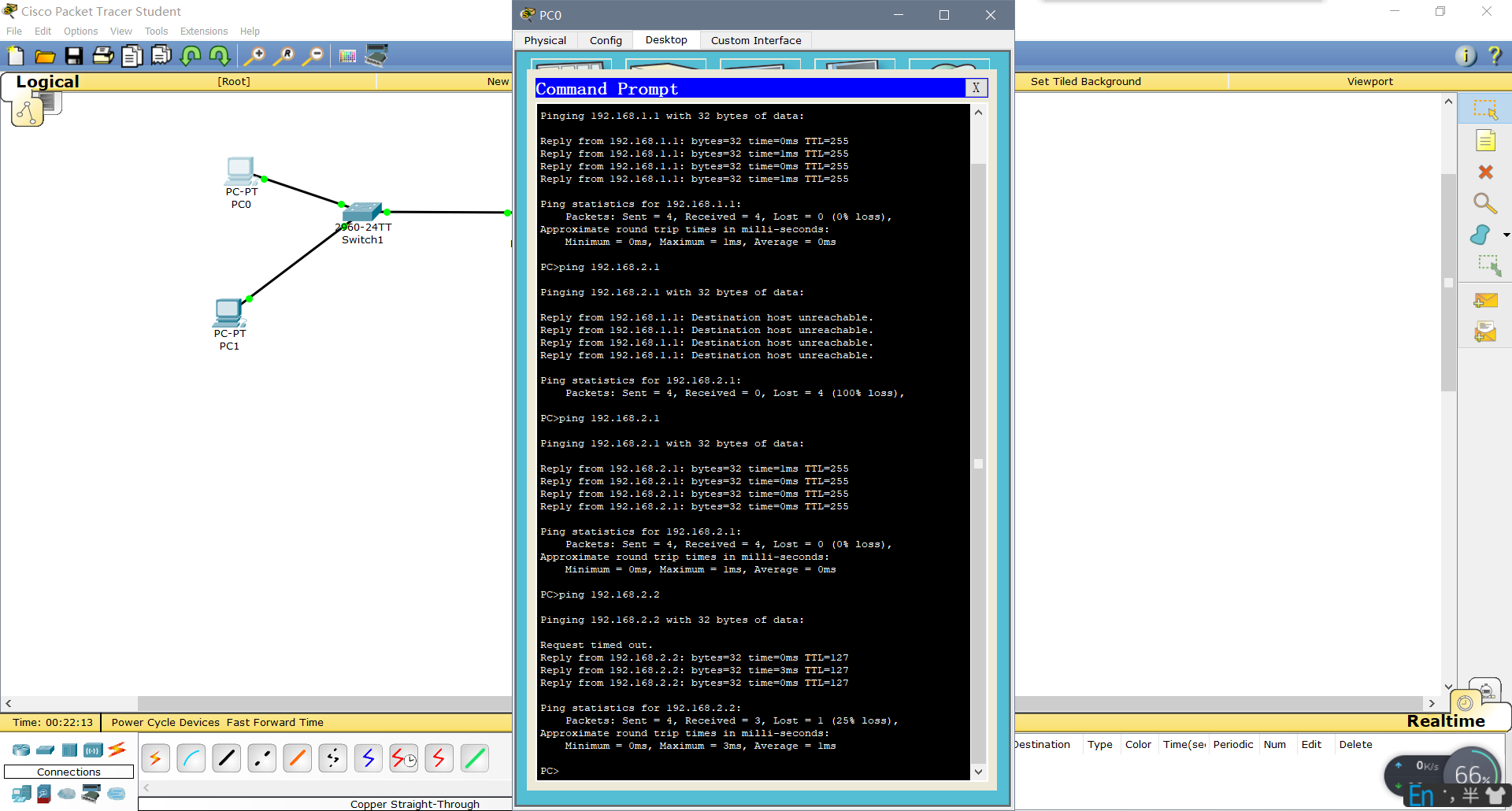
Step 3：测试网络的连通性并记录结果

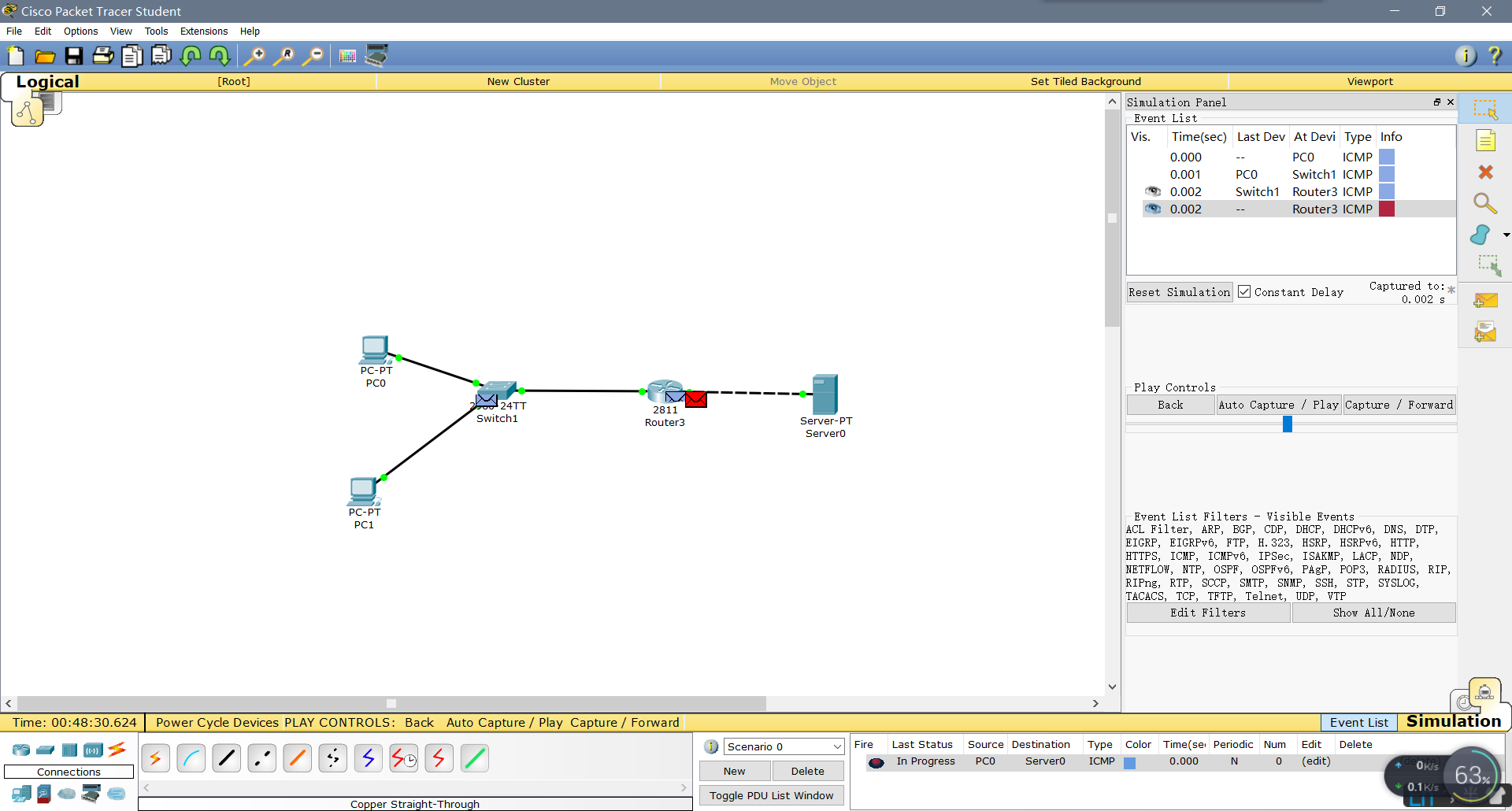
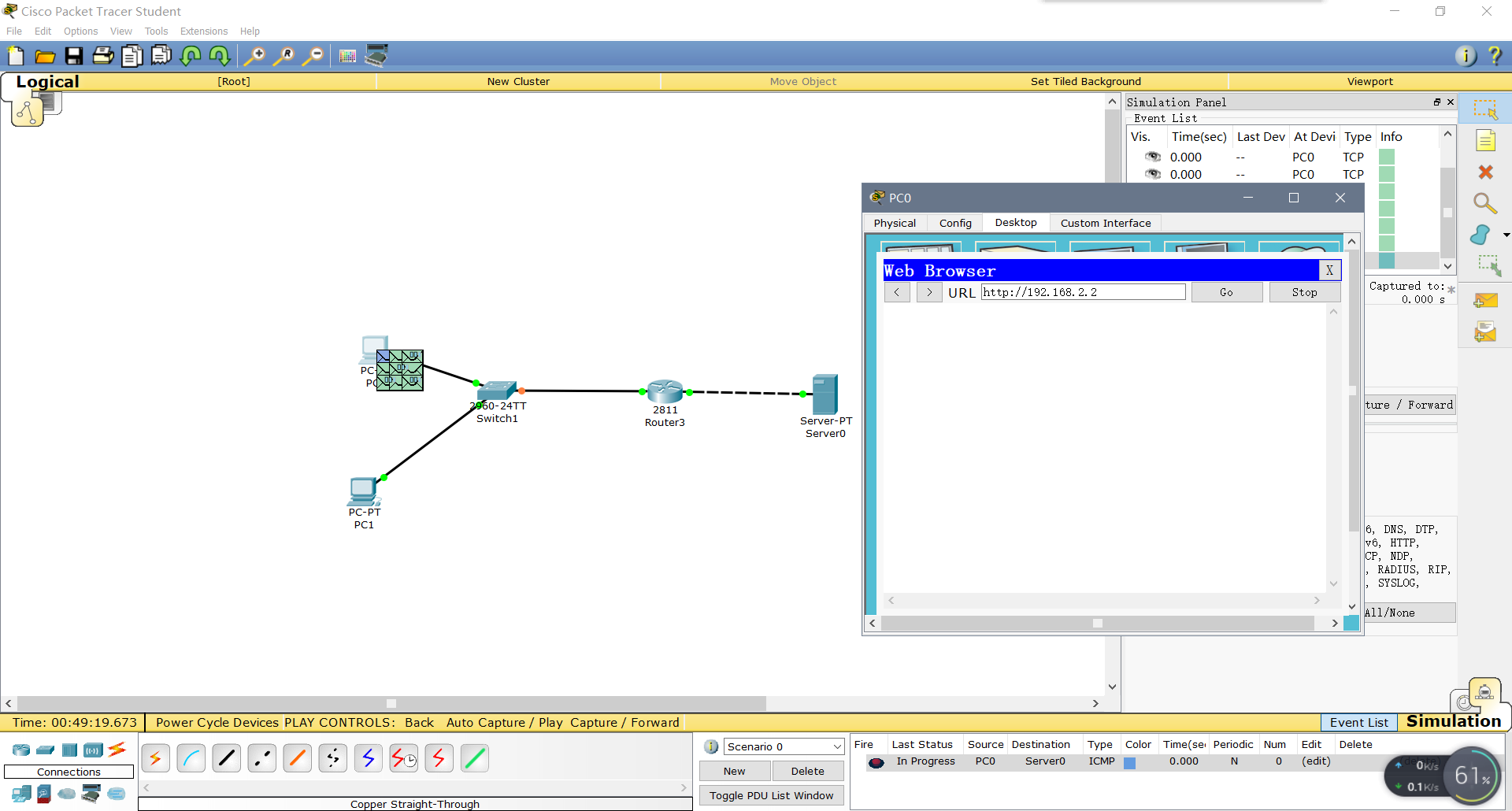
# 实验记录

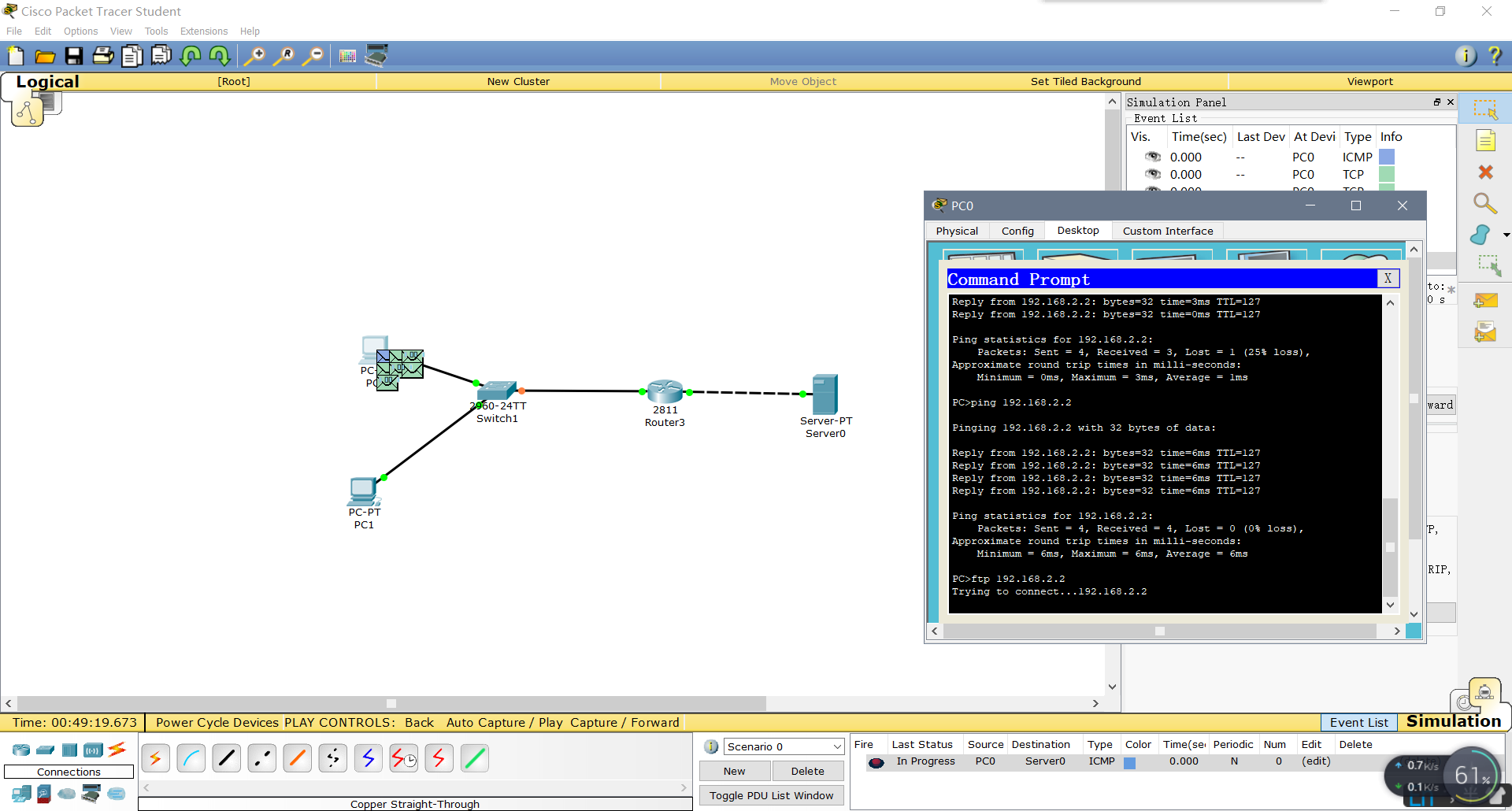
1.设置局域网，测试网络连通性；

2.创建访问控制列表，实现防火墙。







# 实验结果分析与心得

1.在配置好路由器的以太网接口后，需要运行”no shutdown”命令打开以太网接口，否则数据包将无法流通；

2.标准ACL具有普适性，屏蔽所有策略中的报文；扩展ACL可实行一对一定点控制，只屏蔽来自某一ip的某一类型的报文。

# 思考题

1.ACL在定义规则时，除了五元组以外还可以参考哪些信息？

答：可以参考需要屏蔽的报文类型，以及设备性能等。

2.放置标准ACL和扩展ACL的策略有什么不同？

答：标准ACL屏蔽所有策略中的报文；扩展ACL可实行一对一定点控制，只屏蔽来自某一ip的某一类型的报文。