**计算机网络**

**实验报告**



**访问控制列表设计实验**

**任课教师 李俊娥**

**年 级 2020级**

**学 号 2020302191130**

**姓 名 陈骁孚**

**作业完成时间：2023年 05 月**

**目录**

[一、实验目的 1](#_Toc135247634)

[二、实验内容 1](#_Toc135247635)

[三、实验原理 2](#_Toc135247636)

[四、实验环境 3](#_Toc135247637)

[4.1连接逻辑拓扑图 3](#_Toc135247638)

[4.2实验相关设备和系统 4](#_Toc135247639)

[五、实验过程 4](#_Toc135247640)

[5.1 设计网络拓扑图，分配路由器和主机端口IP地址 4](#_Toc135247641)

[5.2 路由器配置 5](#_Toc135247642)

[5.3 查看路由器的路由协议和路由表以及ACL 9](#_Toc135247643)

[5.4 配置PC5的TFTP服务 10](#_Toc135247644)

[5.5 连接配置好的路由器、交换机以及终端，并配置相应终端的IP地址 11](#_Toc135247645)

[六、实验结果 14](#_Toc135247646)

[七、实验心得 17](#_Toc135247647)

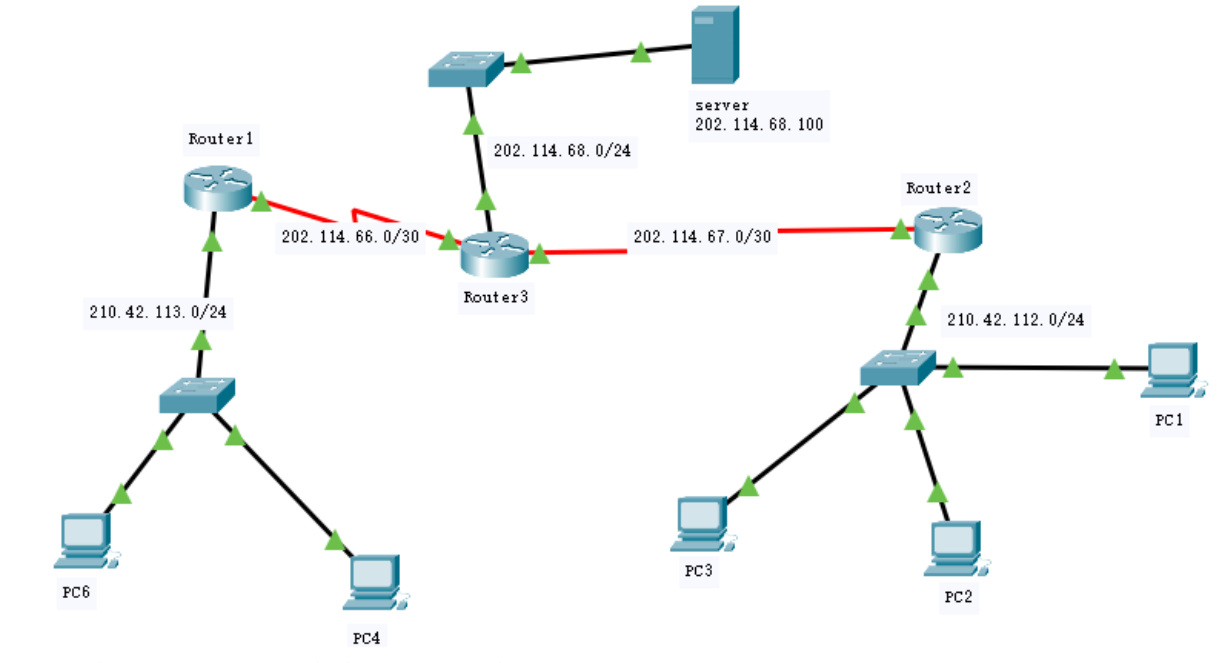
# 一、实验目的

1. 理解访问控制列表的工作机制和基本原理
2. 理解不同ACL的类型之间控制粒度上的差异和其适用场景
3. 掌握不同ACL类型在路由器中的配置方法
4. 掌握构造合理的ACL规则

# 二、实验内容

1. A公司的企业网络如下图所示，由三台路由器、三台交换机和一台服务器构成。现要求网络管理员进行如下配置：

* 进行IP地址规划，然后配置IP和动态路由，实现企业网络的互连互通；
* 配置标准ACL: 210.42.112.0网络中的PC2不能访问210.42.113.0网络，其他PC机可以访问；
* 配置标准ACL: 210.42.112.0网络中的PC1可以Telnet到 Router2，其他PC不行；
* 配置扩展ACL: 210.42.113.0网络中的计算机可以访问Server中的WWW服务，其他网络中的PC机不能访问;
* 配置扩展ACL: 210.42.112.0网络中的计算机可以访问Server中的TFTP服务，其他网络中的PC机不能访问。



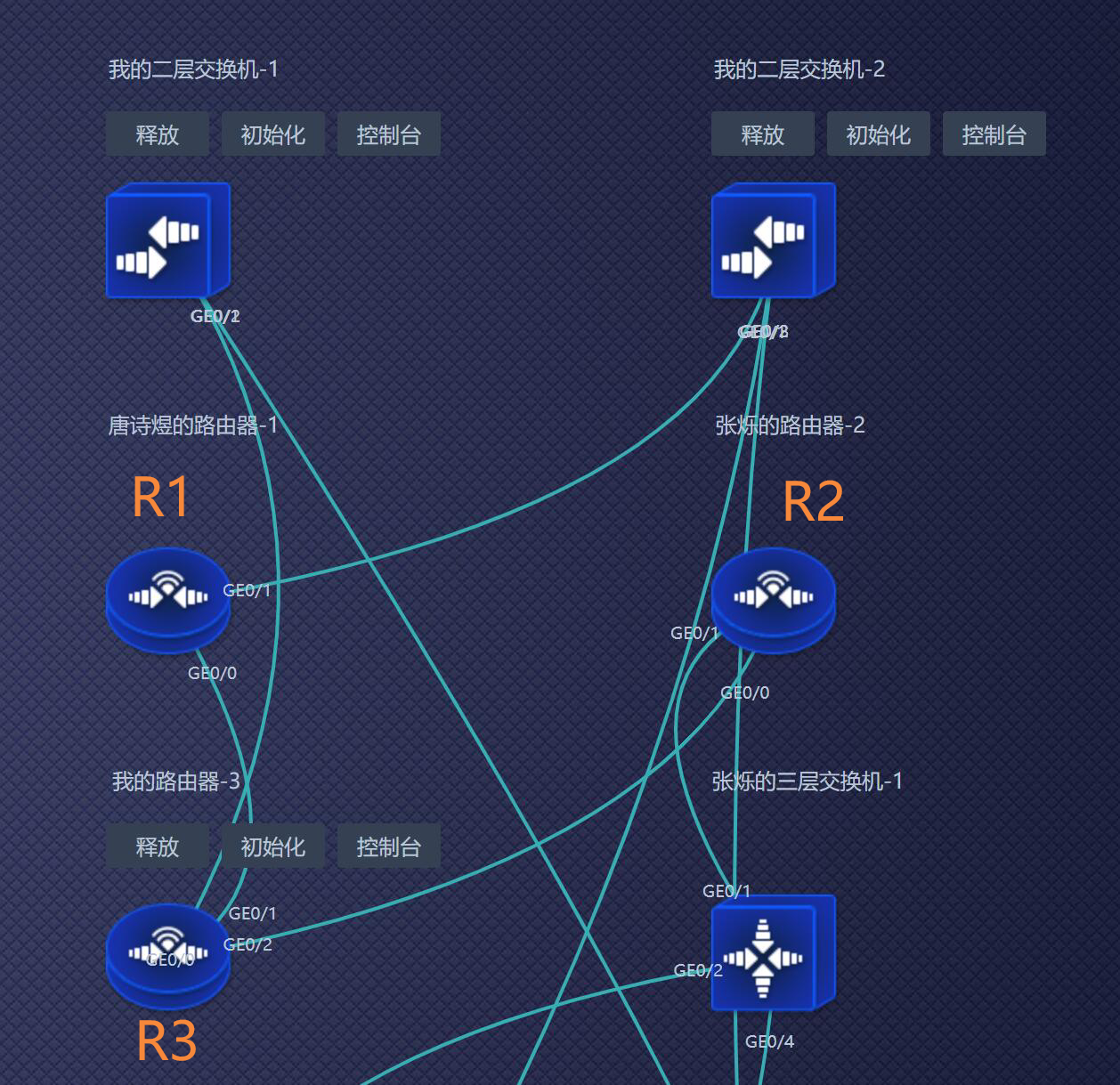
1. 查看路由器Router2的路由协议和路由表。
2. 查看路由器Router1的路由协议和路由表。
3. 实验报告中包含路由器Router1、Router2和 Router3中的全部配置信息;以及从PC1->PC4、PC2->PC4、PC4访问Server WWW服务、PC2访问Server WWW服务、PC2访问Server TFTP服务、PC4访问Server TFTP服务的测试截图。

# 三、实验原理

1. 访问控制列表（Access Control Lists，ACL）是应用在路由器接口的指令列表。这些指令列表用来告诉路由器哪些数据包可以收、哪些数据包需要拒绝。至于数据包是被接收还是拒绝，可以由类似于源地址、目的地址、端口号等的特定指示条件来决定。
2. ACL中有四种类型：标准IP ACL、扩展IP ACL，专家ACL以及基于时间的ACL。第一种只检查源IP地址，编号1-99和1300-1999。
3. ACL中有两种控制规则：permit和deny，默认最后一个规则为deny any，也就是拒绝所有IP数据包。ACL采用就近匹配，一旦有匹配成功的规则，就不再考虑后续规则的检查。
4. 对于一个路由器端口，可以配置其两个方向（in/out）的ACL。

# 四、实验环境

## 4.1连接逻辑拓扑图





如上图，我们将PC5作为WWW和TFTP服务器。

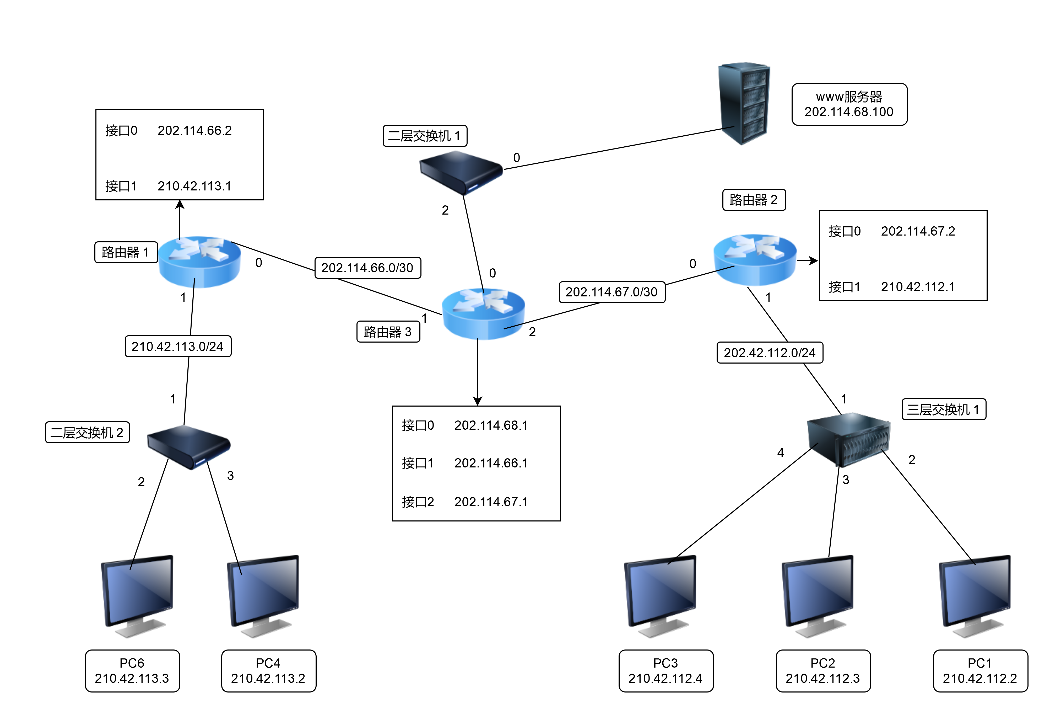
## 4.2实验相关设备和系统

* 实验使用机架：10
* 五台终端Windows 10：PC1-PC4和PC6
* 一个WWW和TFTP服务器：PC5
* 三个锐捷路由器：RG-RSR20-X-28
* 两台锐捷二层交换机：RG-S2910-24GT4XS-E
* 一台锐捷三层交换机：RG-S5310-24GT4XS
* 锐捷终端配线架

# 五、实验过程

## 5.1 设计网络拓扑图，分配路由器和主机端口IP地址

三个路由器端口以及各主机IP地址分配及网络拓扑如下：



其中PC 5作为WWW服务器，图中三层交换机(这里只用到二层的功能)。其中：

路由器1的端口0需要配置入方向的标准ACL，只拒绝来自主机202.42.112.3的流量，而接收其它主机的流量。

路由器2的虚拟终端线路0-4上的入流量配置标准访问ACL，只允许210.42.112.2的流量通过。

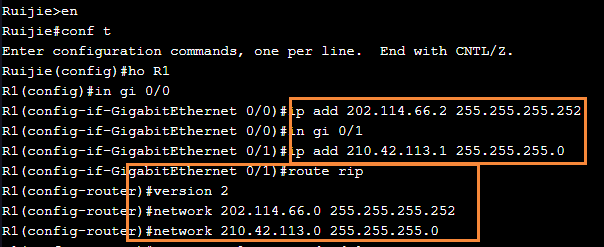
路由器3端口0的出方向需要配置扩展ACL，只允许来自210.42.113.0/24网段的向主机202.114.68.100的www请求可以通过，其它网段的www请求则拒绝；只允许来自210.42,112.0/24网段的主机对主机202.114.68.100的tftp请求通过，其余的拒绝。

## 5.2 路由器配置

**1）配置路由器1：**

配置端口IP地址，需要enable进入特权模式，接着选择配置终端，选中不同端口（使用指令int gig0/<端口号>），利用指令 ip address <ip地址> <子网掩码>设置。

配置RIPv2路由协议：需要使用route RIP；version 2启用RIPv2路由协议，接着使用network <直连网段IP> <子网掩码>配置直连网段路由信息。



配置端口0入方向的ACL：

ip access-list <type> <list-name>

// 创建类型为<type>，名称为<list-name>的ACL，type可以为standard或者extended

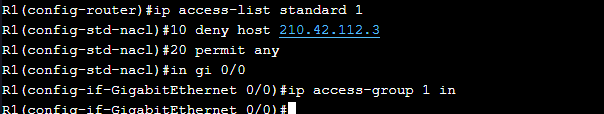
<rule-no> <permit/deny> host <host-ip>

// 添加规则序号<rule-no>，匹配动作为允许或者拒绝某个<host-ip>的规则。

设置对应端口方向启用某个ACL：

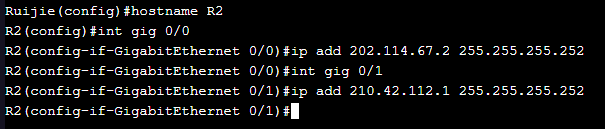
int gig 0/0

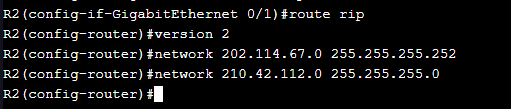
ip access-group <group-name> <in/out>



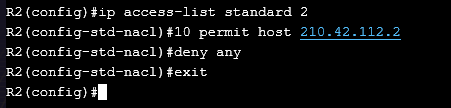
**2）配置路由器2：**

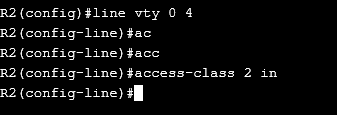
路由器-2的配置与路由器1的端口IP地址、RIPv2路由协议以及ACL配置大体类似，这里不再赘述。





配置ACL：注意，在配置路由器2的时候，我们把ACL应用到虚拟终端线路0-4上的入流量，也就是对通过这个终端线路所有远程访问变量采取过滤。





配置路由器登录密码（配置之前进入config模式）：

enable password <口令>

// 配置路由器特权口令

ling vty 0 4

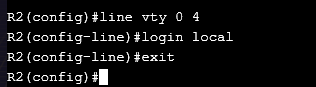
// 进入虚拟终端0-4的配置模式

login local

// 配置使用本地数据库进行登录验证

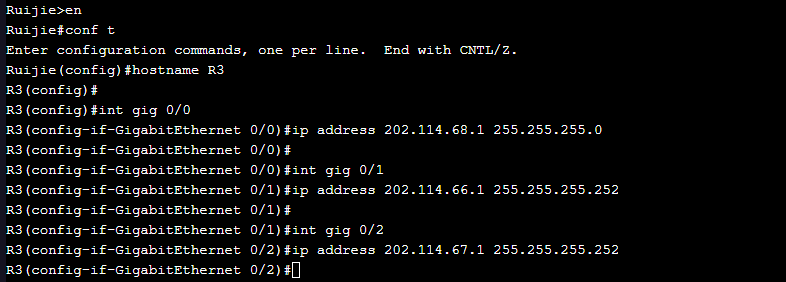
username <用户名> password <口令>



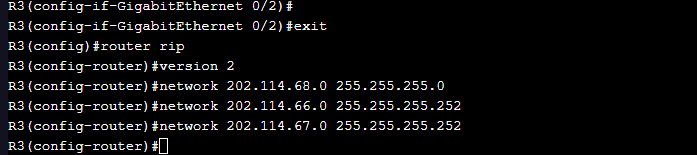


3）**配置路由器3：**

端口IP地址配置：



RIPv2路由协议配置：

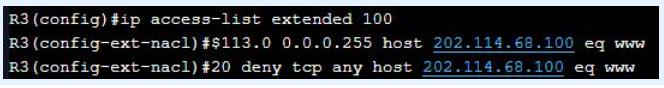


扩展的ACL配置：

在配置路由器1和2时，我们采用的都是标准IP ACL类型，只能起到限制IP地址的作用，这里路由器3需要更细力度的控制，要限制源IP地址以及它向某一个主机请求的服务，规则定义的格式如下。值得注意的是，应用层服务名称要和其传输层采用的协议相匹配，否则无法添加规则成功！

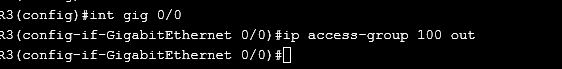
<rule-no> <permit/deny> <tcp/udp> <source-ip> <反子网掩码> host <destination-ip> eq <service>

// 添加一个对于tcp/udp数据包，某一个源地址向目标主机请求某一种服务的请求的过滤。



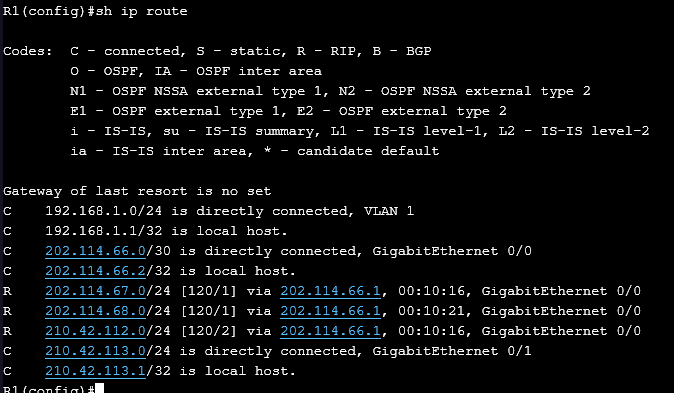


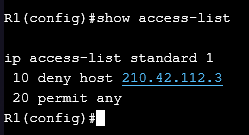




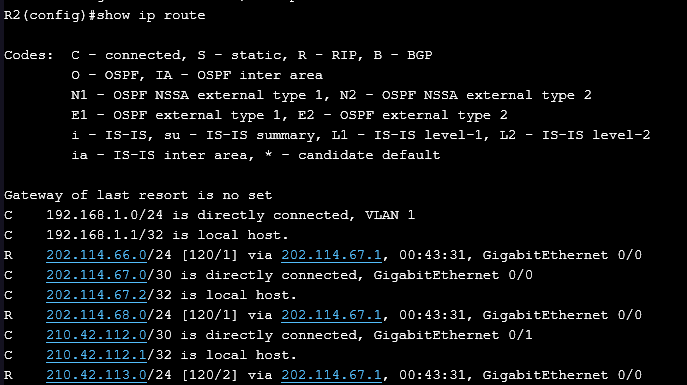
## 5.3 查看路由器的路由协议和路由表以及ACL

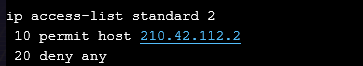
1）路由器1：



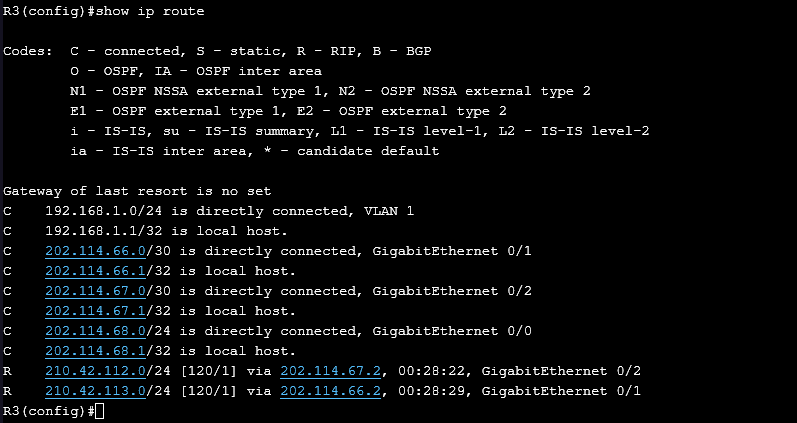


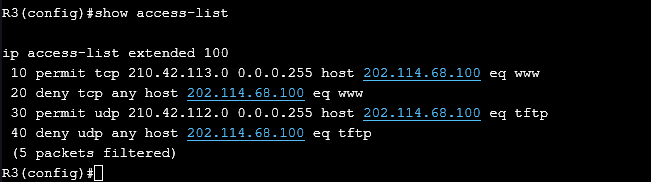
2）路由器2：





3）路由器3：



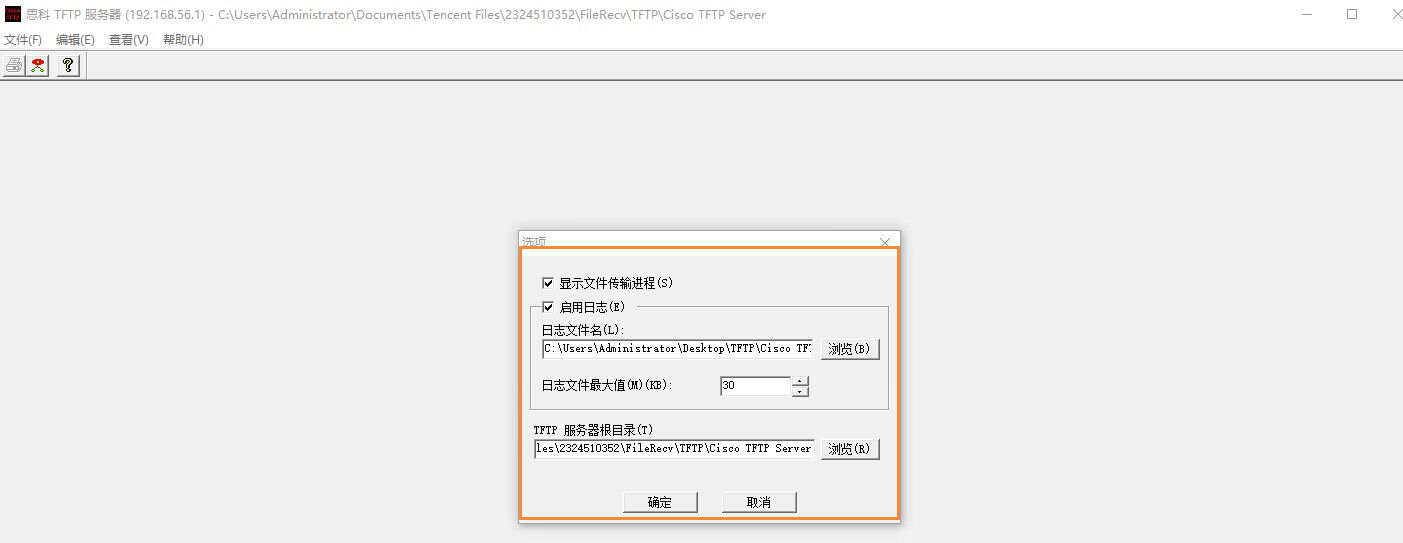


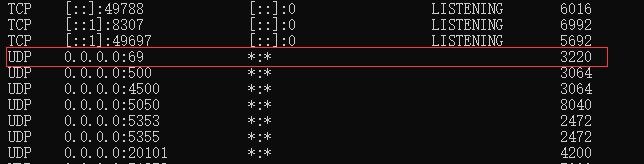
从上面三个路由表表项可以看出RIPv2成功学习到非直连网段的路由信息。并且ACL配置已完成。

## 5.4 配置PC5的TFTP服务

这里需要打开群里提供的思科TFTP服务器文件，运行即可。最后一张图中可以看到UDP协议69号端口正在监听，这说明TFTP服务启动成功。

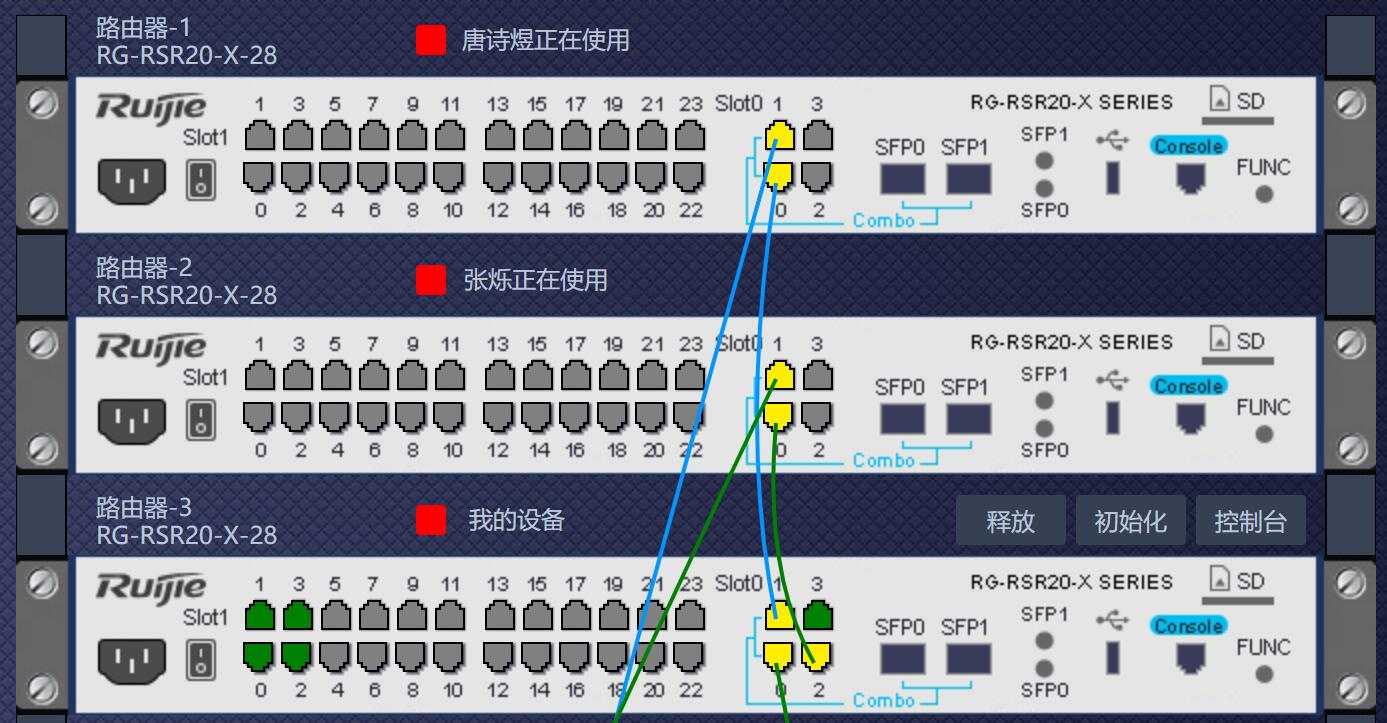




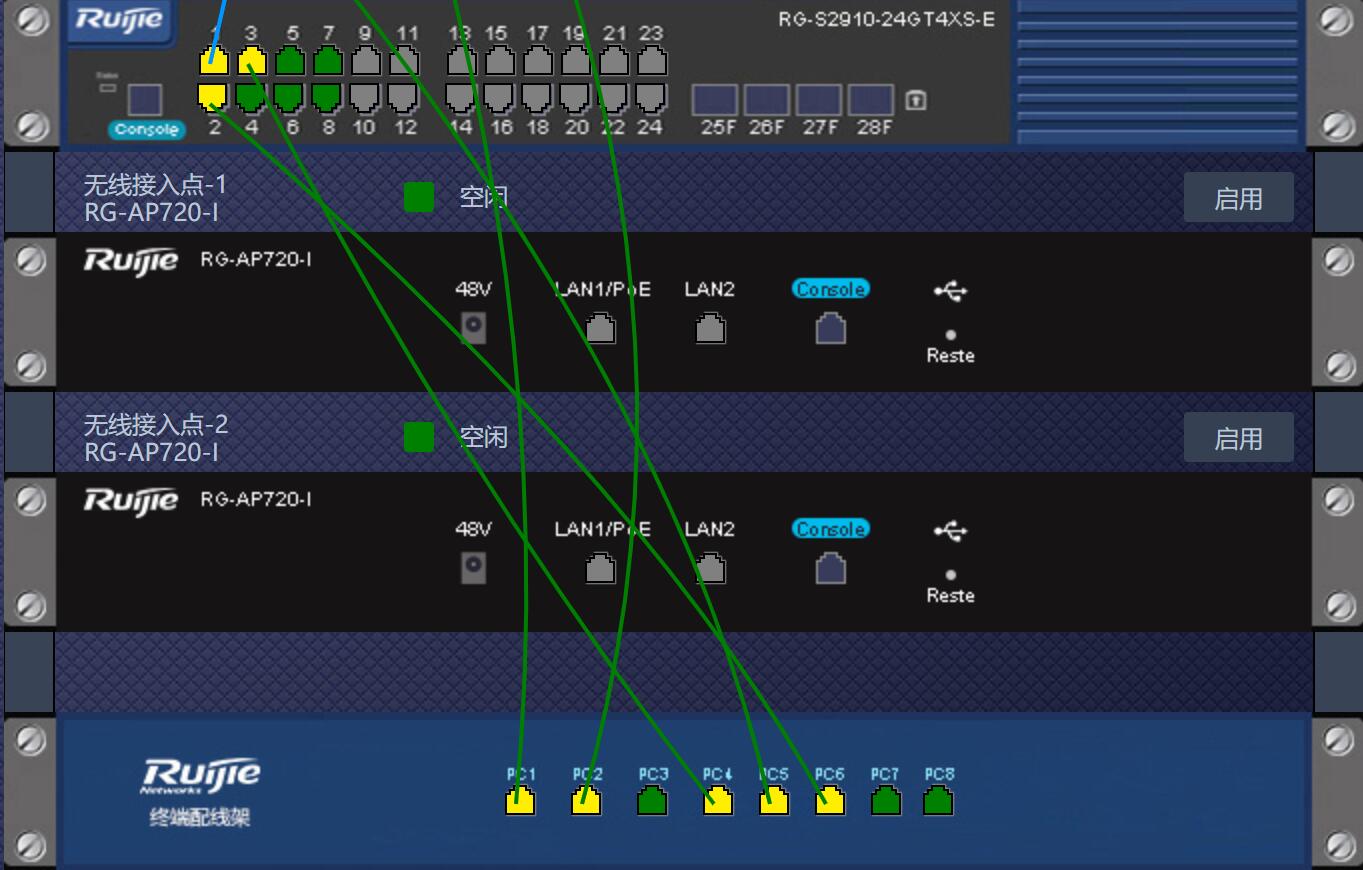


## 5.5 连接配置好的路由器、交换机以及终端，并配置相应终端的IP地址

首先，连接需要先启用相应设备。点击对应端口以连接，最终连接结果如下：







其次，禁用主机上的校园网连接，配置以太网5中的IPv4属性，需要填写本机所在网段的IP地址，子网掩码，以及默认路由信息。

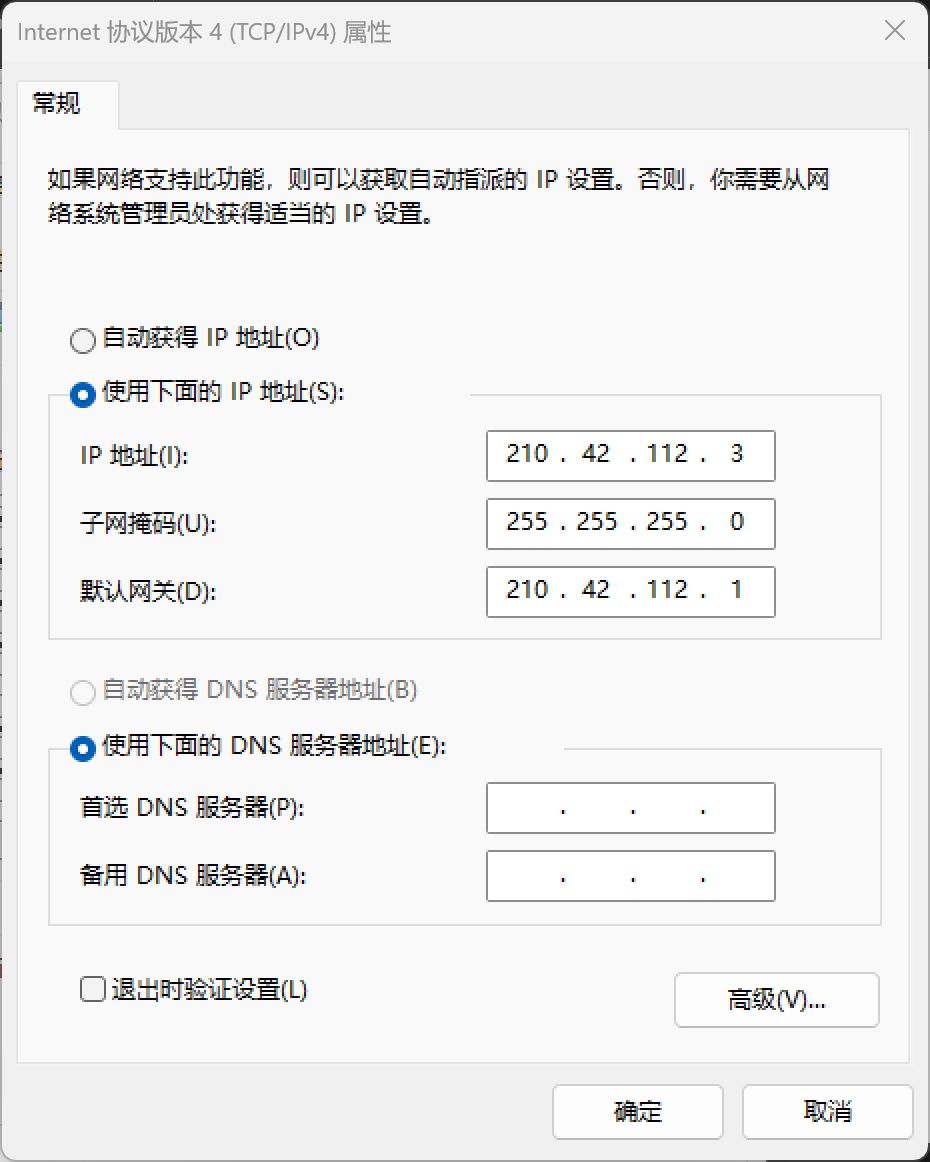
PC5作为WWW和tftp服务器，配置信息如下：



PC3、PC4的配置如下：



PC1、PC2的配置如下：

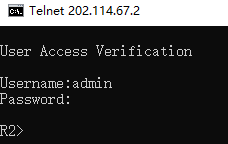


PC6的配置如下：

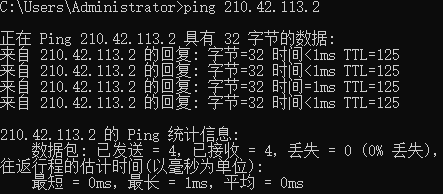


# 六、实验结果

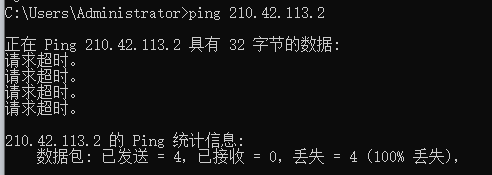
PC1-telnet登录-R2：



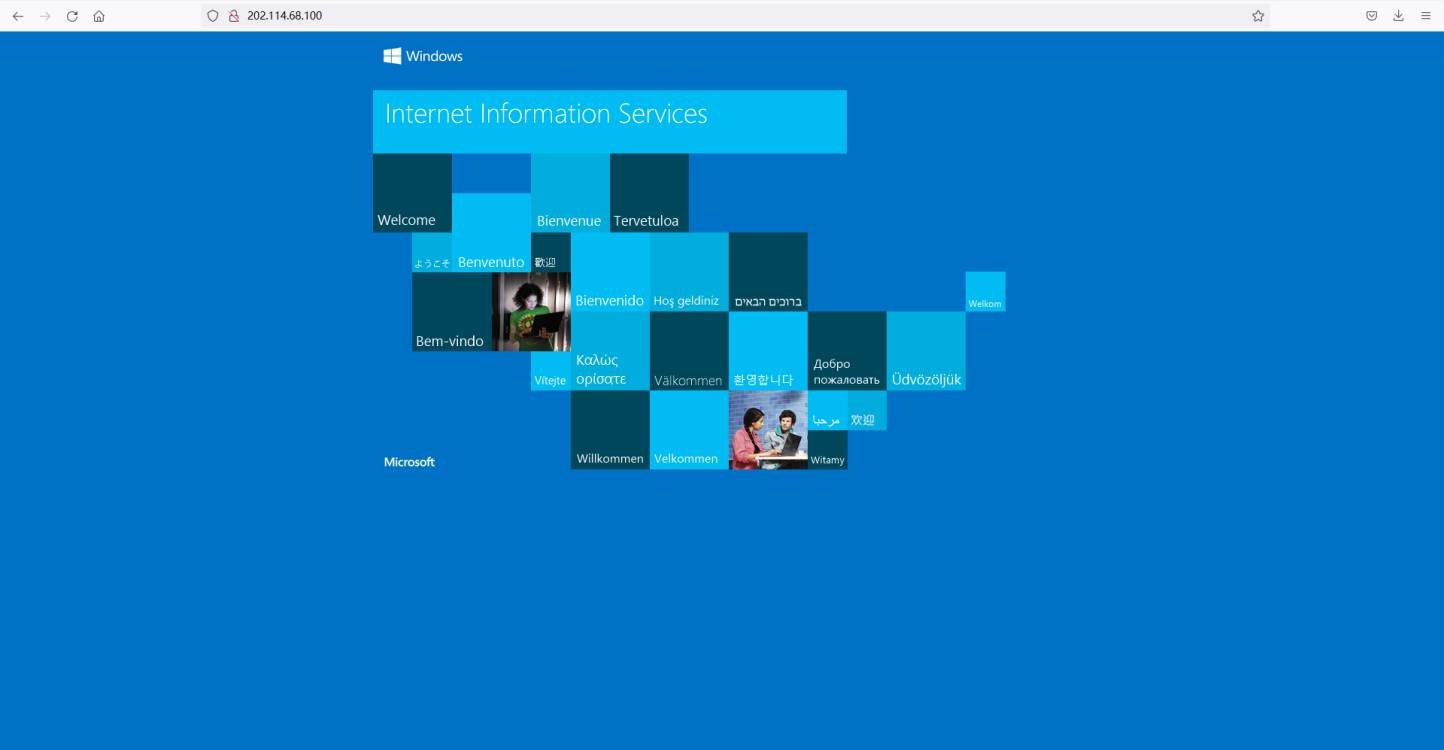
PC1->PC4:



PC2->PC4：



PC4->WWW服务器：



PC2->WWW服务器:



PC2->TFTP服务器:



PC4->TFTP服务器:



根据Ping命令可以看到，因为标准ACL配置，PC1(210.42.112.2)可以Ping通PC4，但是PC2(210.42.112.3)无法Ping通PC4。此外，只有PC1可以Telnet到R2成功。对于扩展ACL生效情况，210.42.113.0/24网段主机可以访问www服务，看以看到PC4访问成功！而PC2在112.0/24网段中，无法访问。此外，112.0/24可以访问TFTP服务，所以PC2能够正常访问是合理的，而处于113.0/24网段的PC4无法访问也符合过滤规则。综上ACL的标准和扩展类型配置成功。

# 七、实验心得

本次实验主要学习了访问控制列表的概念，这在计算机网络理论课中涉及的较少，但是好在本学期的网络安全课程中讲到防火墙包过滤策略时，和其概念大致相似，都是创建一个有序的规则列表，对于符合一定特征的数据包采取不同的行动。虽然理解上障碍不大，但是需要注意的细节还是很多的，如设置入策略还是出策略，如何制定规则语句的顺序等等。我在配置路由器三的时候就犯了一个错误，忘记了TFTP的传输层协议是UDP，仿效配置WWW服务的tcp规则，导致配置指令报错，多亏组员及时指出，可想而知，一个合格的网络管理人员，扎实的计算机网络基础是必不可少的，这也激励我多回顾基础知识，多思考运用。