编号：

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 实验 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 总评 | 教师签名 |
| 成绩 |  |  |  |  |  |  |  |  |  |  |

武汉大学国家网络安全学院

课程实验(设计)报告

题 目： ACL设计实验

专业(班)： 信息安全

学 号： 2021302181156

姓 名： 赵伯俣

课程名称： 计算机网络实践

任课教师： 杜瑞颖

2024年5月20日

**目录**

[1 实验目的 3](#_Toc14037)

[2 实验内容 3](#_Toc19697)

[3 实验原理窗体顶端 4](#_Toc3761)

[4 实验环境 5](#_Toc15399)

[5 实验过程 7](#_Toc7888)

[5.1 设计拓扑图 7](#_Toc11302)

[5.2 连线图及逻辑拓扑图 8](#_Toc16613)

[5.3 配置路由器 9](#_Toc30292)

[6 实验结果 13](#_Toc15669)

[6.1 路由器Router1的详细信息 13](#_Toc11379)

[6.2 路由器Router2的详细信息 14](#_Toc26311)

[6.3 路由器Router3的详细信息 15](#_Toc25748)

[6.4 PC间通信 16](#_Toc22015)

[6.4.1 PC1 ping PC4 16](#_Toc11708)

[6.4.2 PC2 ping PC4 16](#_Toc7480)

[6.4.3 PC4 访问Server WWW服务 17](#_Toc15003)

[6.4.4 PC2 访问Server WWW服务 18](#_Toc28445)

[6.4.5 PC2 访问Server TFTP服务 18](#_Toc31488)

[6.4.6 PC4 访问Server TFTP服务 19](#_Toc11470)

[6.4.7 PC1-telnet登录-R2 20](#_Toc25073)

[7 实验心得 20](#_Toc16910)

# 1 实验目的

了解访问控制列表的原理以及配置方法。通过在网络中特定路由器端口设置ACL，实现限制网段或主机访问目标网段或服务的效果，了解在路由器或交换机端口配置访问控制列表的方法以及标准和扩展ACL的限制范围区别，并通过实际通信得到限制的效果，理解访问控制列表的实质和ACL的有效配置在网络安全性中发挥的作用。

# 2 实验内容

2.1 按照指定实验拓扑图，正确连接网络设备，控制用户的安全接入

2.2 为各个路由器配置端口的ip

2.3 为各个路由器配置RIPv2协议和控制访问列表

2.4 实验题目：

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:

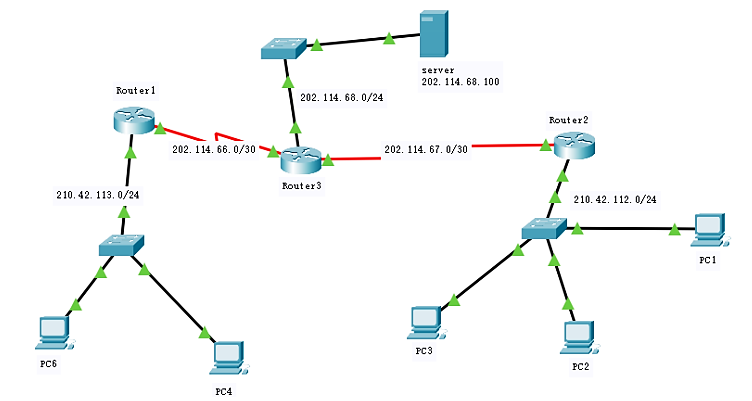
1)进行IP地址规划．然后配置IP和动态路由，实现企业网络的互连互通;

2)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;

3)配置标准ACL:210.42.112.0网络中的PC1可以 Telnet到 Router2，其他PC不行;

4)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;

5)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。



# 3 实验原理窗体顶端

**3.1 ACL访问控制列表**

IP ACL(IP访问控制列表或P访问列表)是实现对流经路由器或交换机的数据包根据一定的规则进行过滤，从而提高网络可管理性和安全性。IP ACL分为两种：标准IP访问列表和扩展IP访问列表。

标准P访问列表可以根据数据包的源P地址定义规则，进行数据包的过滤。

扩展P访问列表可以根据数据包的源P、目的P、源端口、目的端口、协议来定义规则，进行数据包的过滤。

IP ACL基于接口进行规则的应用，分为：入栈应用和出栈应用。

入栈应用是指由外部经该接口进行路由器的数据包进行过滤。

出栈应用是指路由器从该接口向外转发数据时进行数据包的过滤。

PACL的配置有两种方式：按照编号的访问列表，按照命名的访问列表。

标准IP访问列表编号范围是1~99、1300~1999，扩展IP访问列表编号范围是100~199、2000~2699

**3.2 标准ACL**

标准的ACL可以对数据包的源IP地址进行检查，当应用了ACL的接口接收或发送数据包时，将根据接口配置的ACL规则对数据进行检→查，并采取相应的措施，允许通过或拒绝通过，从而达到访问控制的目的，提高网络安全性。

**3.3 扩展ACL**

扩展ACL则支持更加细致具体的限制内容，表现为其可以对数据包的源IP地址、目的IP地址、协议、源端口、目的端口进行检查。当应用了ACL的接口接收或发送数据包时，将根据接口配置的ACL规则对数据进行检查，并采取相应的措施，允许通过或拒绝通过，从而达到访问控制的目的，提高网络安全性。

**3.4 专家ACL**

专家ACL是考虑到实际网络的复杂需求，将ACL的检测元素扩展到源MAC地址、目的MAC地址、源P地址、目的P地址、源端口、目的端口和协议，从而实现对数据的更精确的过滤，满足网络的复杂需求。

当应用了专家ACL的接口接收或发送报文时，将根据接口配置的ACL规则对数据进行检查，并采取相应的措施（允许通过或拒绝通过），从而达到访问控制的目的，提高网络安全性。

**3.5 基于时间的ACL**

基于时间的ACL是在各种ACL规则（标准ACL、扩展ACL等）后面应用时间段选项(time-range)以实现基于时间段的访问控制。当ACL规则应用了时间段后，只有在此时间范围内规则才会生效。此外，只有配置了时间段的规则才会在指定的时间段内生效，其他未引用时间段的规则将不受影响。

# 4 实验环境

实验元件如下：

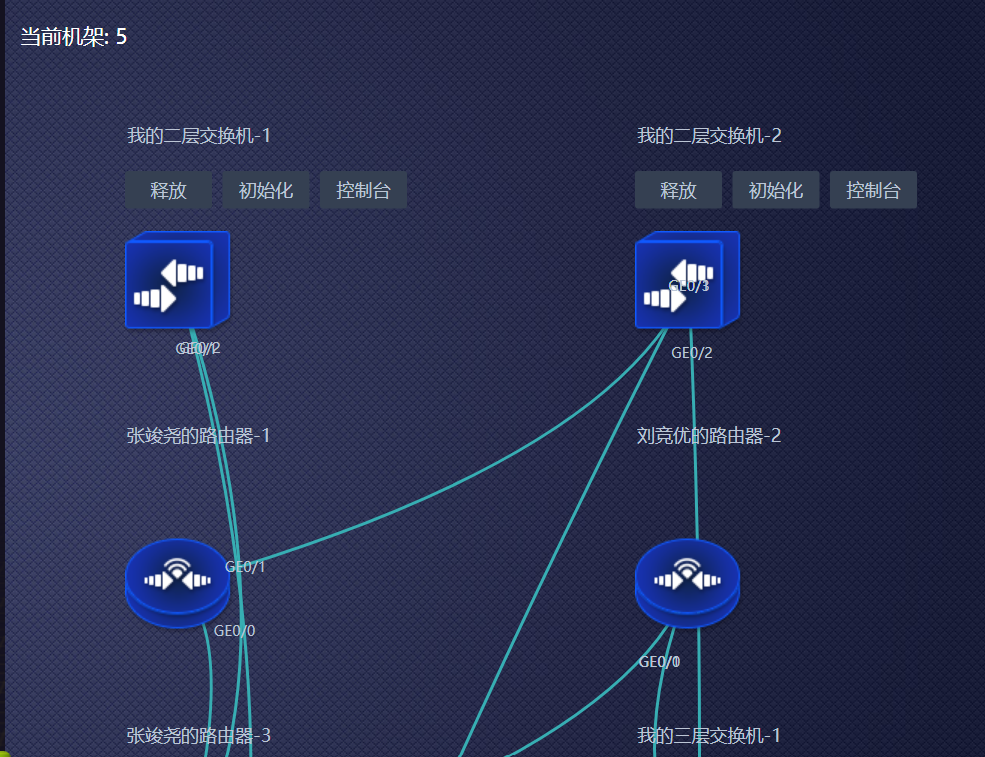
➢ 三台路由器：Router1、Router2、Router3

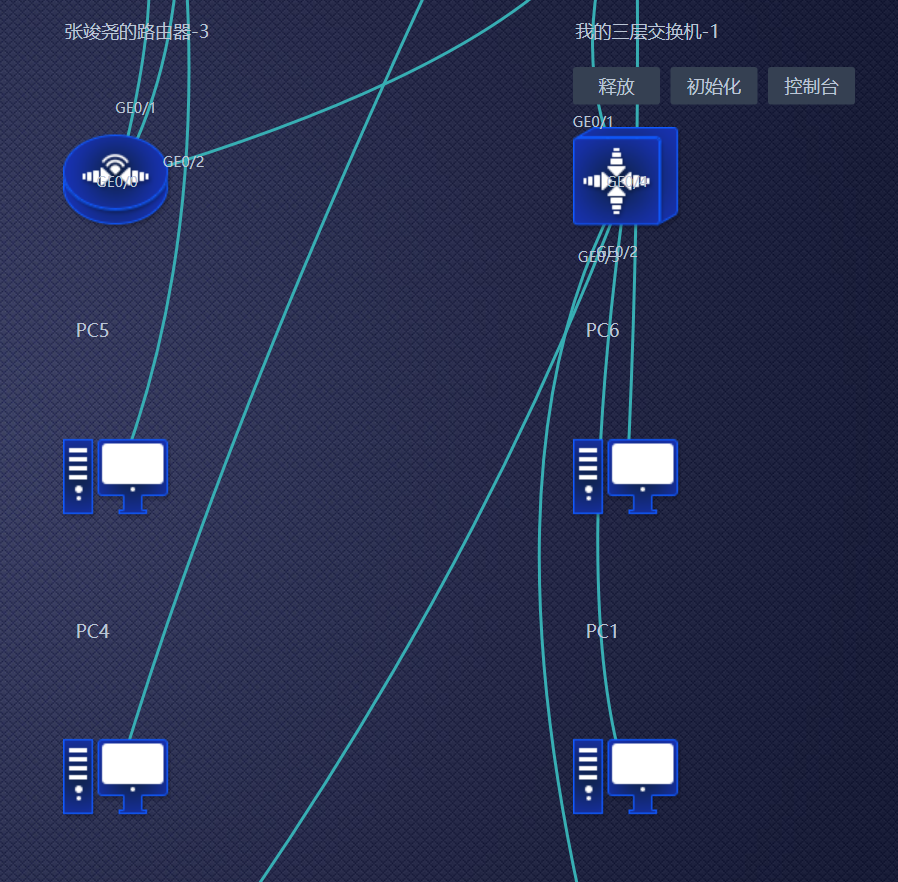
➢ 二台二层交换机、一台三层交换机：Switch1、Switch2、三层 Switch1

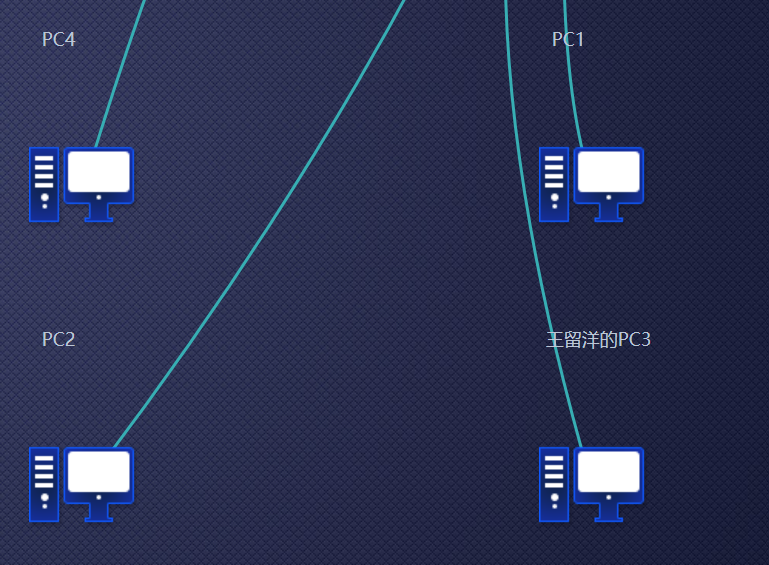
➢ 一台WWW服务器：使用PC5充当

➢ 六台PC：PC1-PC6

实验逻辑拓扑图如下：



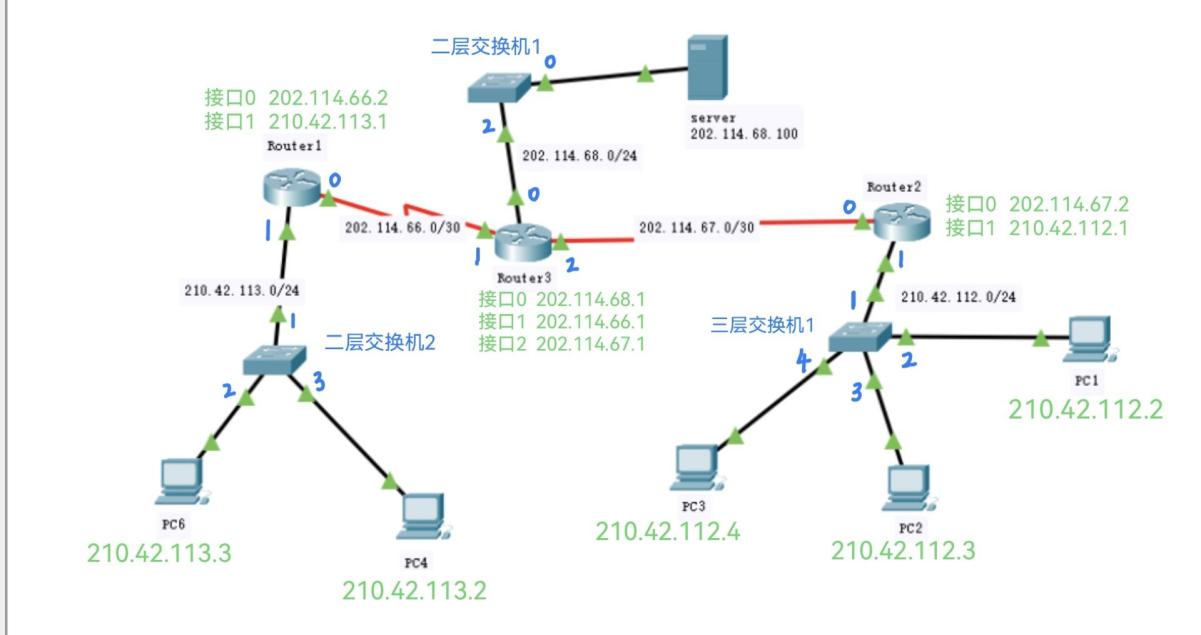




# 5 实验过程

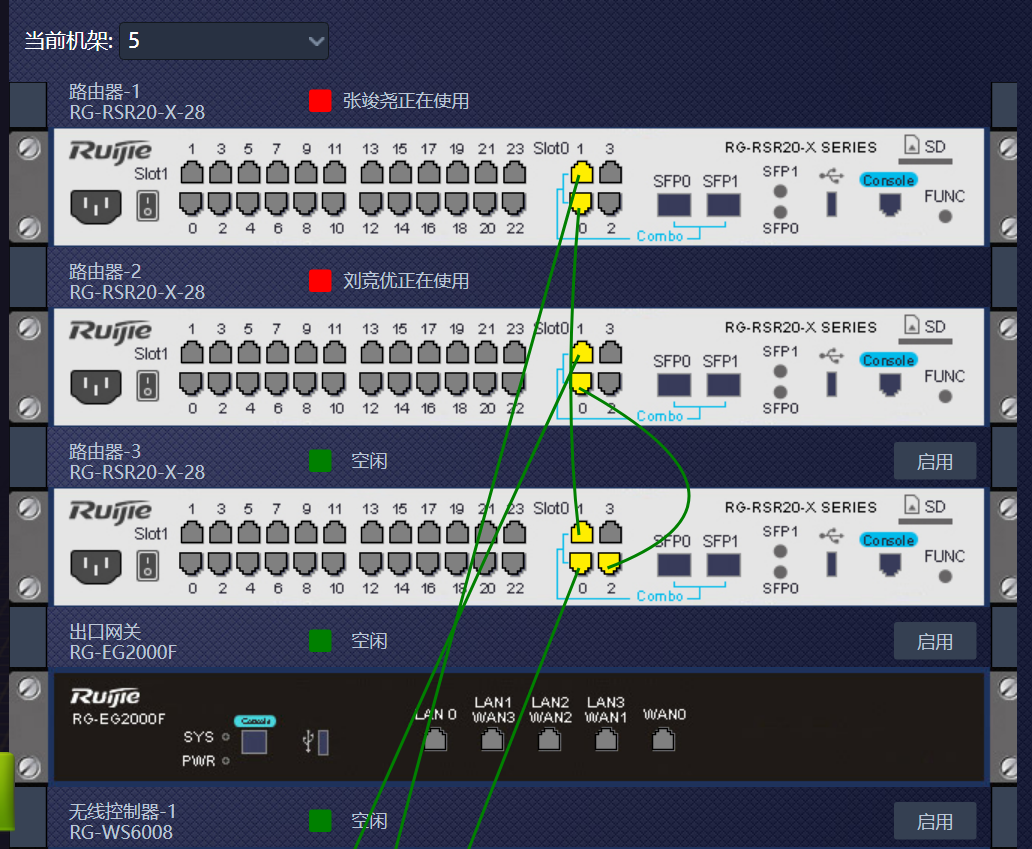
## 5.1 设计拓扑图

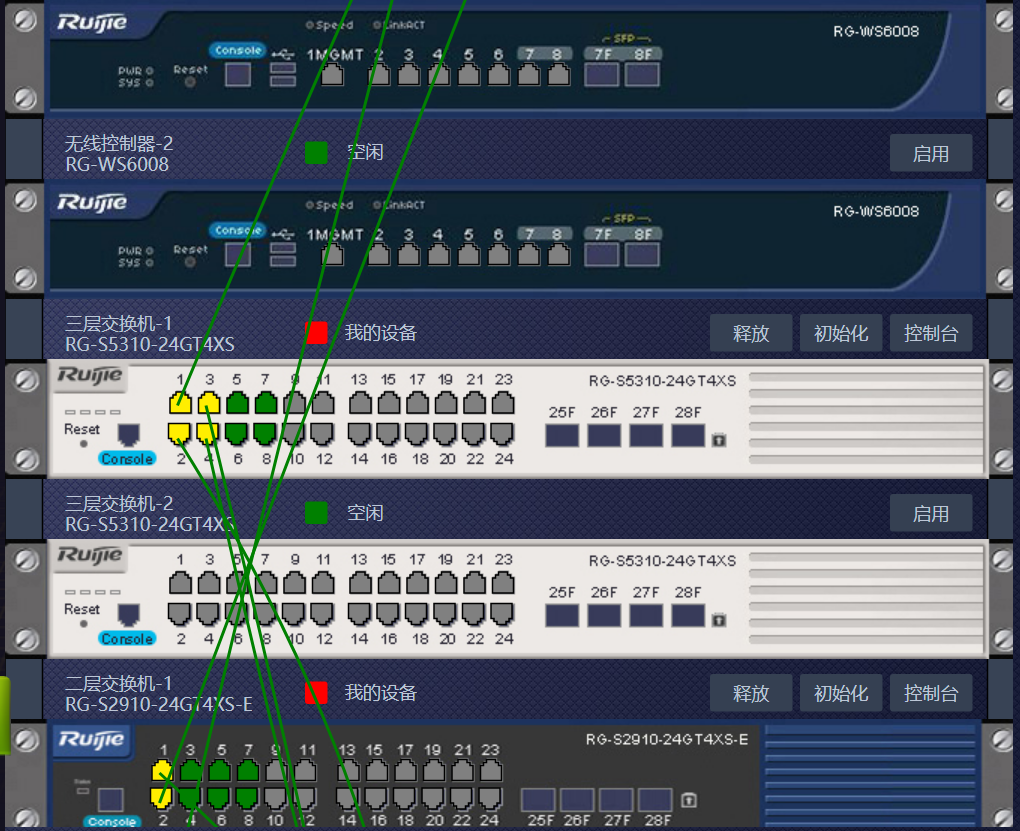
按照题目的网络通信需求，设计网络拓扑图与通信设备的接口以及PC的IP地址，实验拓扑图如下：

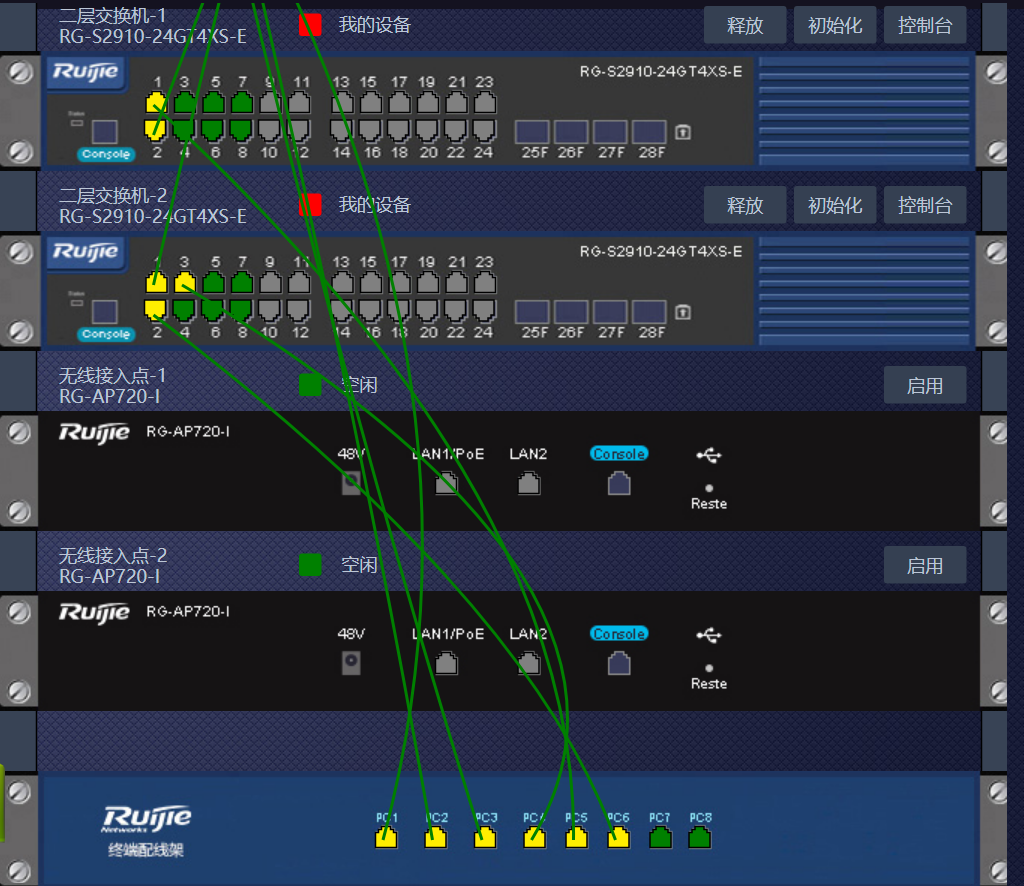


## 5.2 连线图及逻辑拓扑图

机架连线图如下：





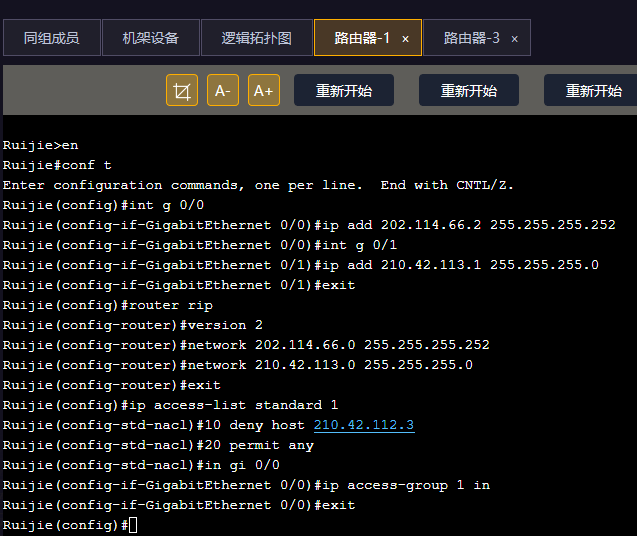


## 5.3 配置路由器

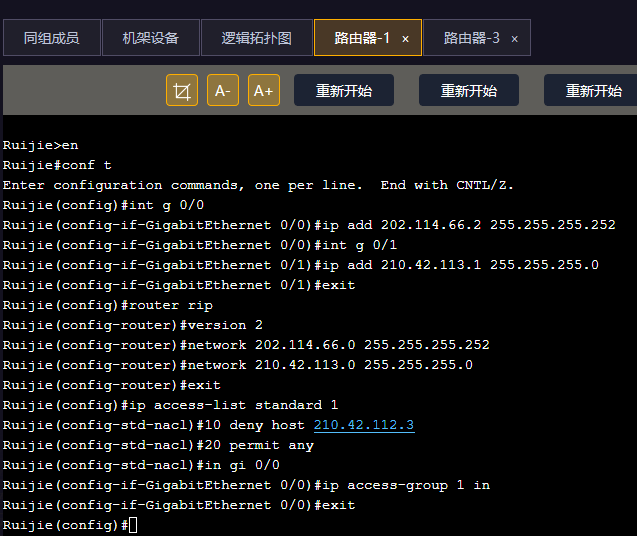
（1）路由器R1全部配置信息：

首先配置接口IP，然后指定要使用的协议，配置直接相邻的网络，以及路由器ACL配置。

配置路由器1端口ip



开启rip协议



**➢ 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**

首先执行如下指令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

ip access-list standard 1

需要在路由器1中配置标准ACL，过滤PC2的请求。如下命令是在路由器的访问控制列表（ACL）中添加一个条目，用于阻止IP地址为210.42.112.3的主机访问路由器。具体来说，这个命令告诉路由器，如果有任何流量的源或目的IP地址为210.42.112.3，则路由器应该拒绝该流量。这个命令中的“deny”关键字指示ACL不允许与该IP地址匹配的任何流量通过路由器。

10 deny host 210.42.112.3

相应的第二条指令含义为允许其他任何流量通过。它用于将一个访问控制列表（ACL）应用于接口的入方向上。当在接口配置中添加这个命令时，它会告诉路由器或交换机在接收到进入该接口的数据包时，应该应用指定的ACL来控制该数据包的流向。

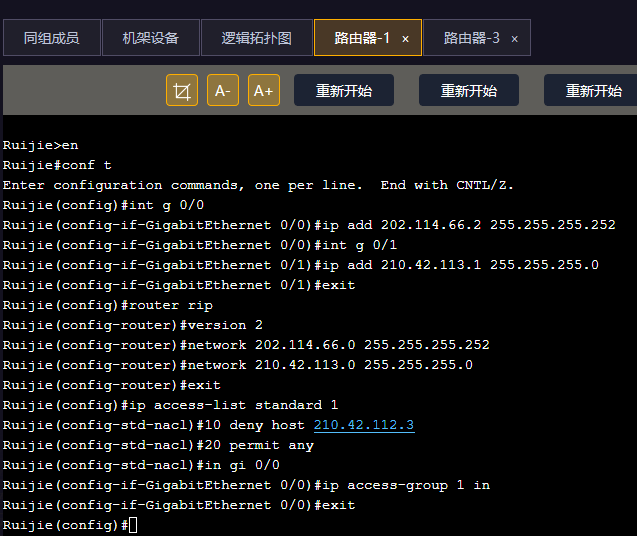
20 permit any

接下来执行指令ip access-group <group-name> <in/out>在0/0端口开启ACL

in gi 0/0

ip access-group 1 in

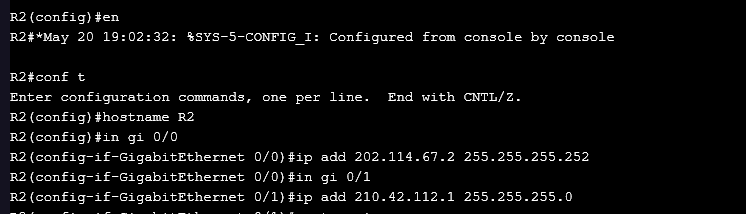
配置ACL指令如下所示



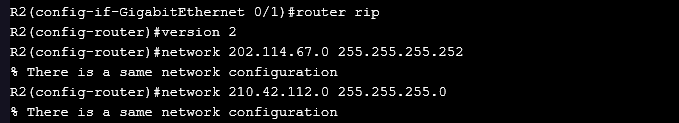
（2）路由器R2全部配置信息

路由器2的配置与路由器1的配置基本上是一致的，也是首先配置ip地址和路由协议，然后再配置acl访问控制。

配置路由器端口ip地址



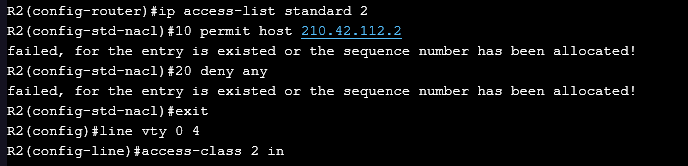
配置rip协议



配置ACL：

➢ **配置标准ACL:210.42.112.0网络中的PC1可以 Telnet到 Router2，其他PC不行**

在router2上配置，使用的指令与router1类似。

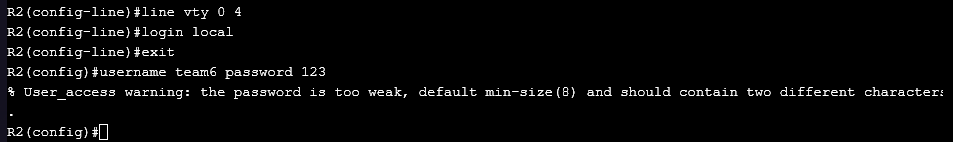


配置本地用户：

执行指令ling vty 0 4进入虚拟终端0-4的配置模式

执行指令login local配置使用本地数据库进行登录验证

执行指令username <用户名> password <口令>配置用户名和口令



（3）路由器R3全部配置信息

路由器3的配置与路由器1、2的配置基本上是一致的，也是首先配置ip地址和路由协议，然后再配置acl访问控制。

➢ **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**

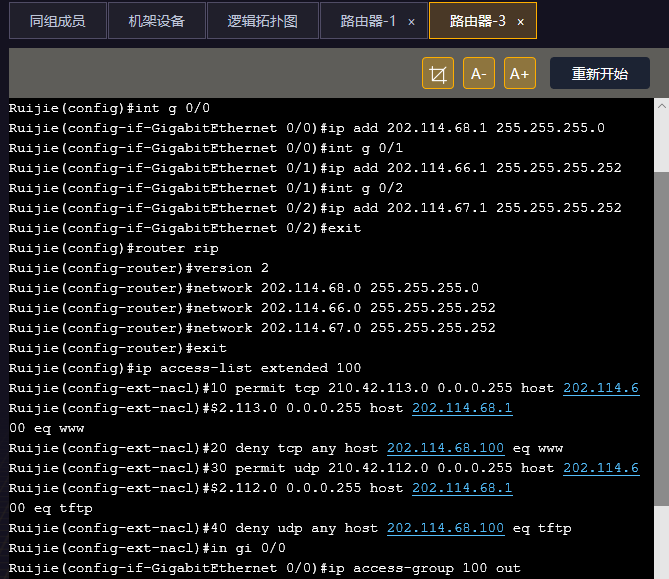
**permit tcp 210.42.113.0 0.0.0.255 host 202.114.68.100 eq www**

允许来自IP地址段为210.42.113.0/24的主机，通过TCP协议连接到目标IP地址为202.114.68.100，目标端口为80（即Web服务的默认端口）的主机。“tcp”关键字表示该条目应该应用于TCP协议的流量。“eq www”表示这个条目仅允许连接到目标主机的80端口（即Web服务的默认端口）

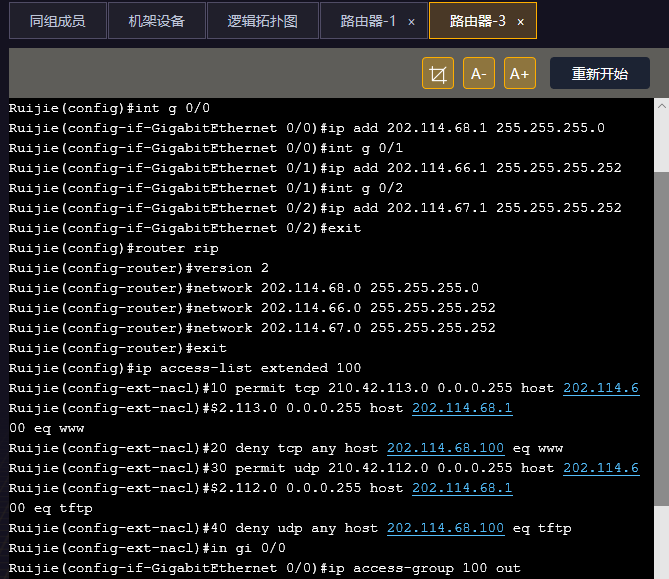
➢ **配置扩展ACL: 210.42.112.0网络中的计算机可以访问Server中的TFTP服务,其他网络中的PC机不能访问**

这个过程与前一个类似指令。

设置端口ip



开启rip协议



配置ACL

执行指令<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。

ip access-list extended 100

10 permit tcp 210.42.113.0 0.0.0.255 host 202.114.68.100 eq www

20 deny tcp any host 202.114.68.100 eq www

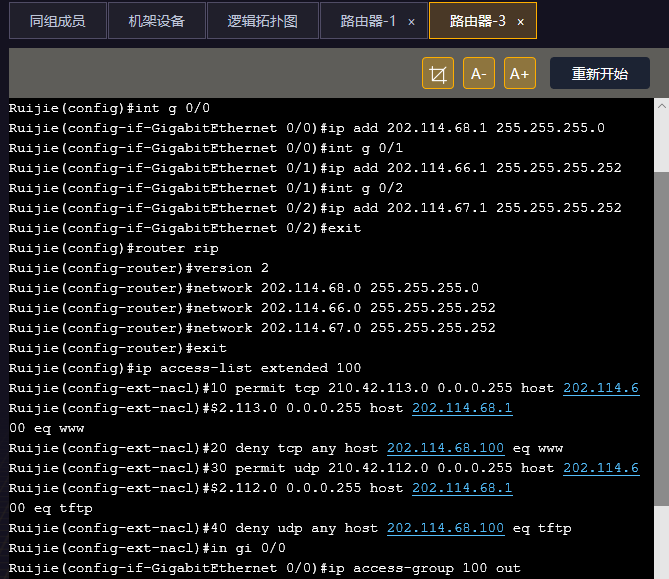
30 permit udp 210.42.112.0 0.0.0.255 host 202.114.68.100 eq tftp

40 deny udp any host 202.114.68.100 eq tftp

in gi 0/0

ip access-group 100 out

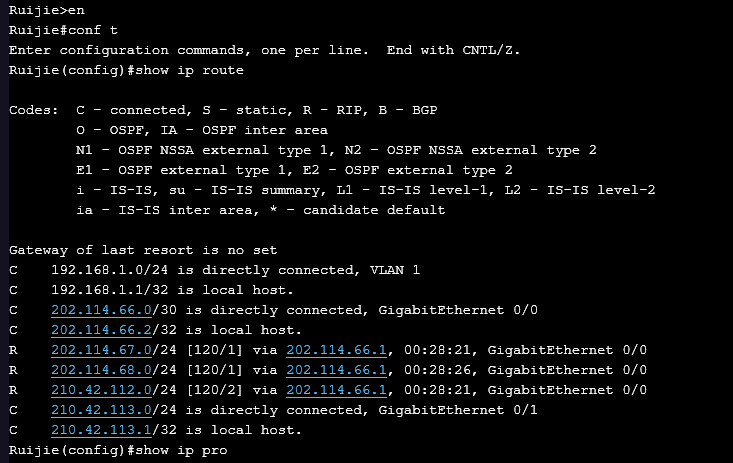
路由器3的ACL配置信息如下



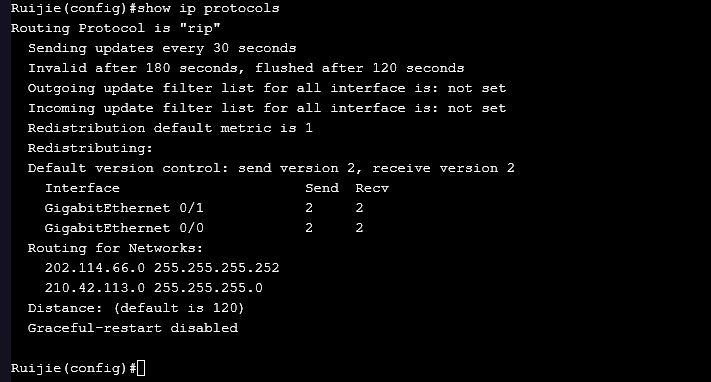
# 6 实验结果

## 6.1 路由器Router1的详细信息

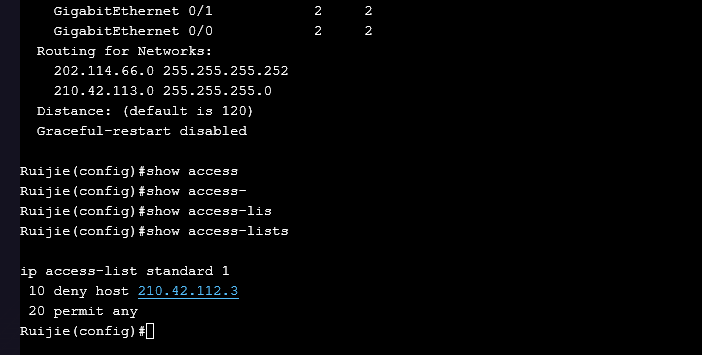
show ip route：



show ip protocols：

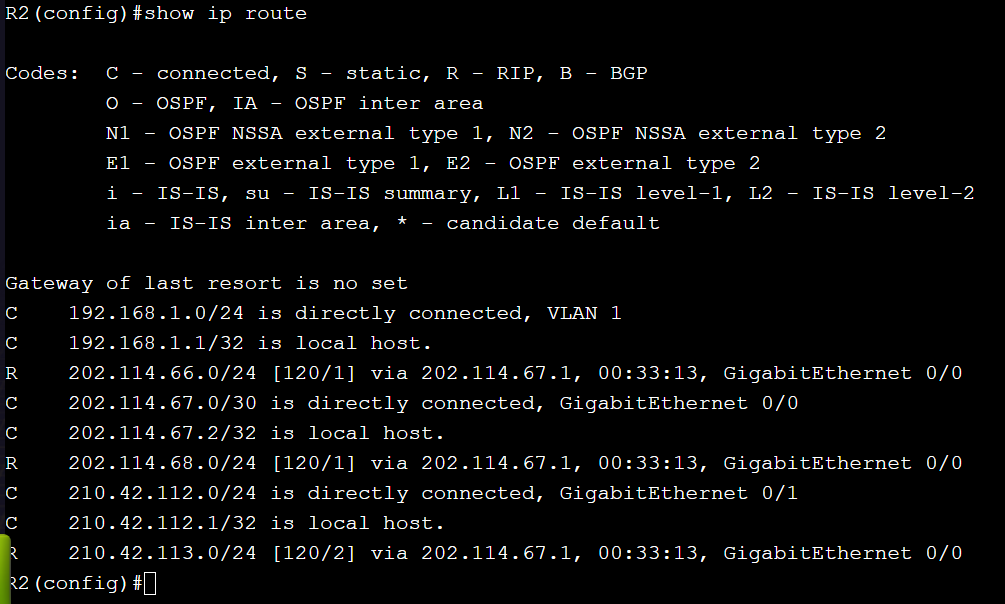


show access-list：



## 6.2 路由器Router2的详细信息

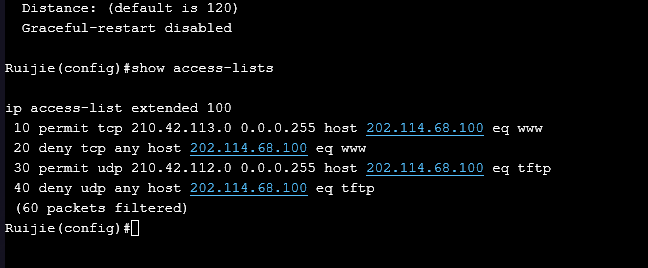
show ip route：



show ip protocols：

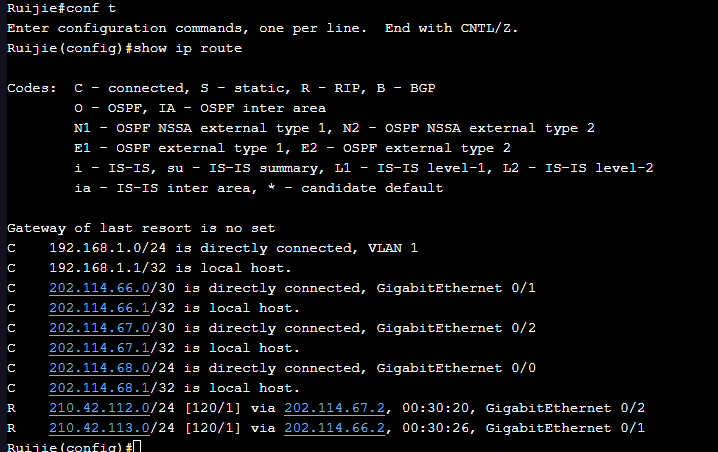


show access-list：

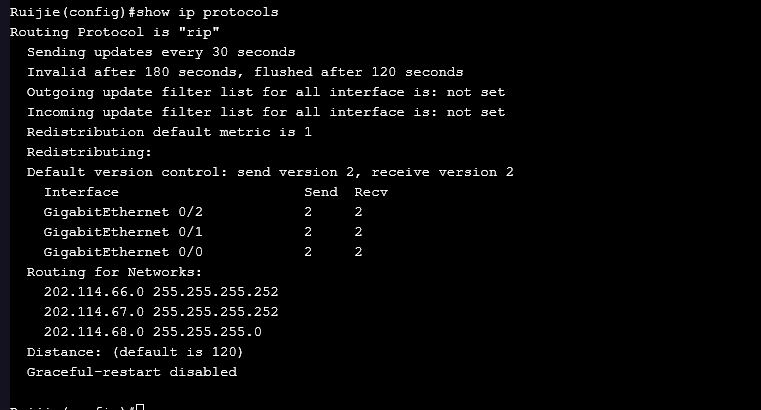


## 6.3 路由器Router3的详细信息

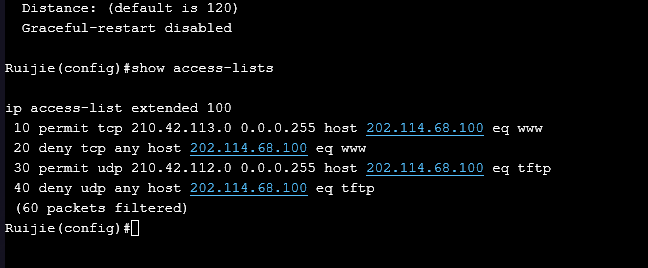
show ip route：



show ip protocols：



show access-list：

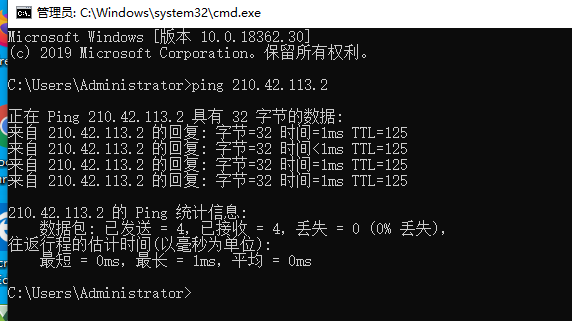


## 6.4 PC间通信

通过模拟PC间的通信，来验证实验配置的正确性，结果如下。

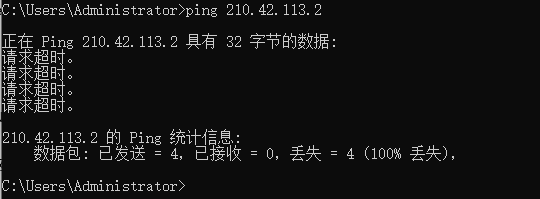
### 6.4.1 PC1 ping PC4

在PC1上使用命令ping 210.42.113.2：



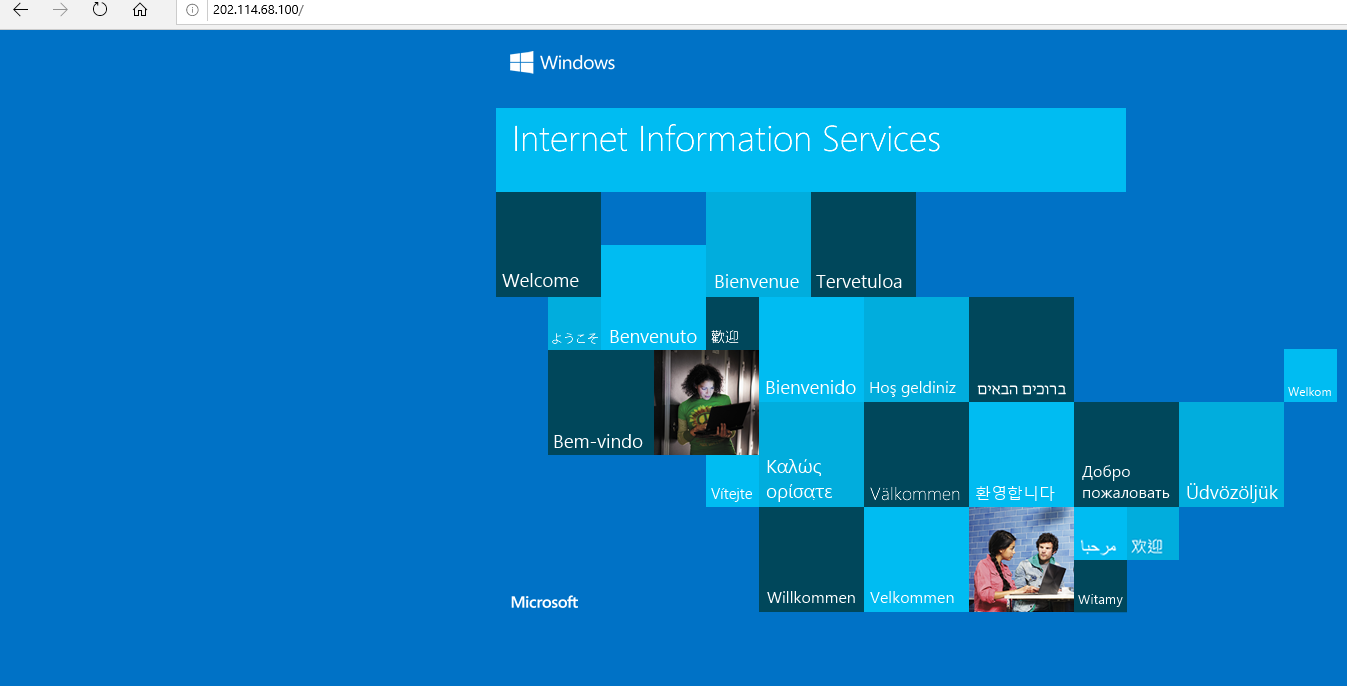
### 6.4.2 PC2 ping PC4

在PC2上使用命令ping 210.42.113.2，由于之前配置了210.42.112.0网络中的PC2不能访问210.42.113.0网络，所以PC2无法ping通PC4：



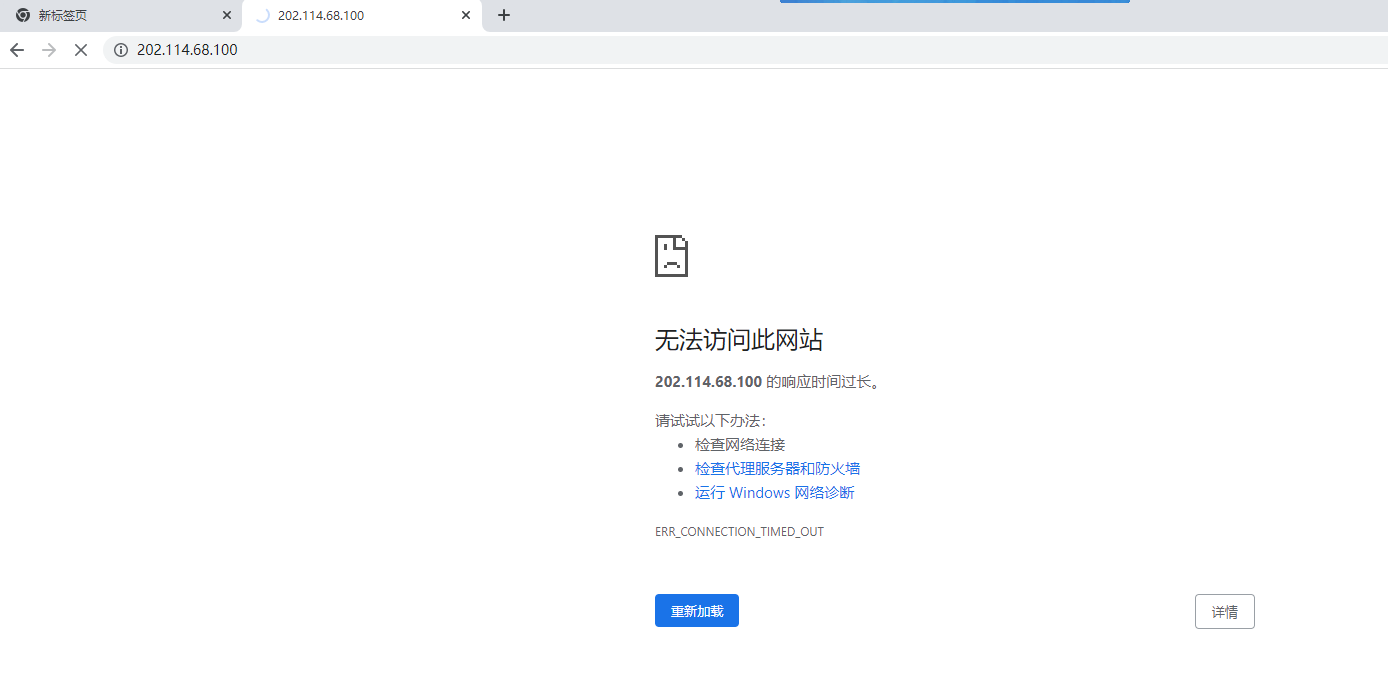
### 6.4.3 PC4 访问Server WWW服务

在PC4中保持以太网5不变，打开浏览器，访问www服务器（202.114.68.100），由于www服务器上部署了web，所以可以看到浏览器展示了web页面。



### 6.4.4 PC2 访问Server WWW服务

在PC2中保持以太网5不变，打开浏览器，访问www服务器（202.114.68.100）。由于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WWW服务，故PC2不能访问WWW服务：

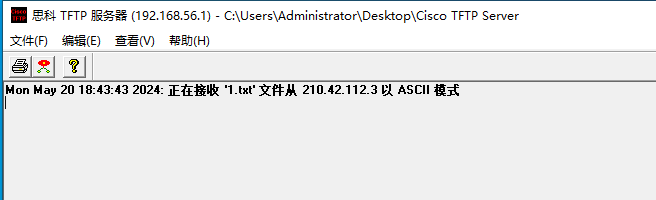


### 6.4.5 PC2 访问Server TFTP服务

创建1.txt，在PC2中使用tftp 202.114.68.100 put 1.txt进行发送，发送端命令行如下

pc2send

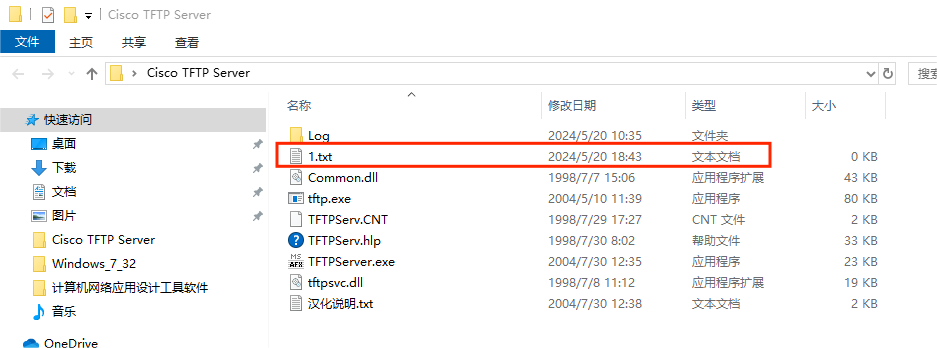
在TFTP服务器中可以看到接受文件的信息



查看TFTP服务器的日志文件

2日志

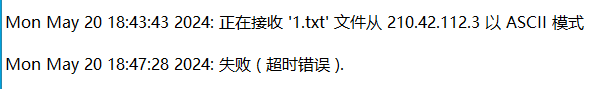
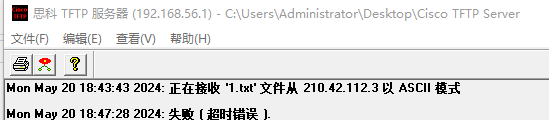
查看服务器本地目录发现存在1.txt



### 6.4.6 PC4 访问Server TFTP服务

由于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。所以PC4不能访问Server TFTP服务，显示失败：

pc4访问tftp



### 6.4.7 PC1-telnet登录-R2



# 7 实验心得

在本次实验中，我了解了访问控制列表（ACL）的原理和配置方法。通过实际操作，在网络设备中配置标准ACL和扩展ACL，我学会了如何限制特定网络或主机对目标网络或服务的访问。在配置过程中，我了解到了ACL规则的语法和应用场景，学会了如何在路由器端口上应用ACL，并了解了ACL的入栈应用和出栈应用的区别。在实际上机配置的过程中完善了理论知识体系。

在实验过程中，通过对PC间通信的模拟测试，验证了ACL配置的正确性，成功地实现了实验要求中的各项功能，加深了对ACL实际应用的理解。