

# 目录

一、实验目的及内容	1
1.1 实验内容	1
1.2 实验要求	1
二、实验原理	2
三、实验步骤	2
3.1 分配端口并连线	2
3.2 路由器 1	4
3.3 路由器 2	5
3.4 路由器 3	6
四、出现的问题及解决方法	7
五、实验结果	7
六、实验心得	12
七、指导教师评语及成绩	14

# 计算机网络实践九

## 一、 实验目的及内容

### 1.1 实验内容

A 公司的企业网络如下图所示，由三台路由器、三台交换机和一合服务器构成。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。

网络拓扑图如下：

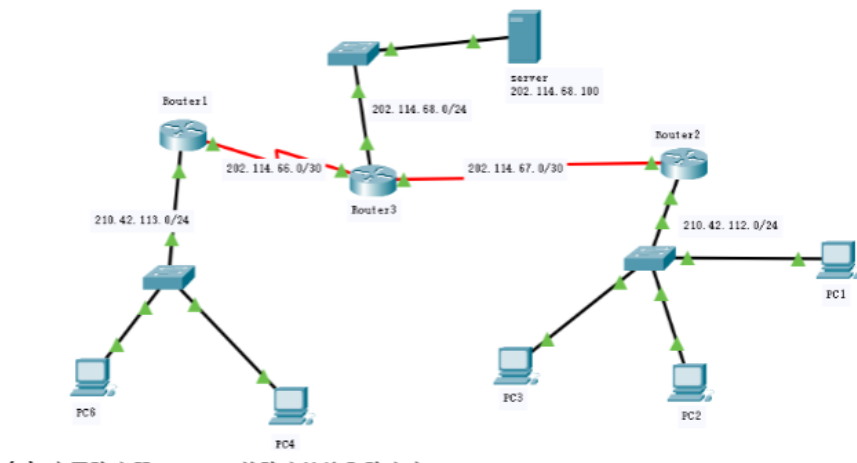


图 1: 网络拓扑图

### 1.2 实验要求

1. 查看路由器 Router2 的路由协议和路由表；
2. 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 SerVerTFTP 服务、PC4 访问 Server TFTP 服务的测试截图。

## 二、 实验原理

### 1.ACL 简介

访问控制列表 ACL (Access Control List) 是由一条或多条规则组成的集合。所谓规则,是描述报文匹配条件的判断语句,这些条件可以是报文的源地址、目的地址、端口号等。

ACL 本质上是一种报文过滤器,规则是过滤器的滤芯。设备基于这些规则进行报文匹配,可以过滤出特定的报文,并根据应用 ACL 的业务模块的处理策略来允许或阻止该报文通过。访问控制列表 ACL 可分为两种:标准 IP 访问列表和拓展 IP 访问列表。

ACL 是实现对流经路由器或交换机的数据包根据一定规则进行过滤的访问控制列表,以此来限制特定的网段或者主机对某网络或主机地址的访问权,从而提高网络的可管理性,保障网络通信的安全性。

### 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. 拓展 ACL

拓展 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。

## 三、 实验步骤

### 3.1 分配端口并连线

根据设备分配端口信息,新的拓扑图如下:

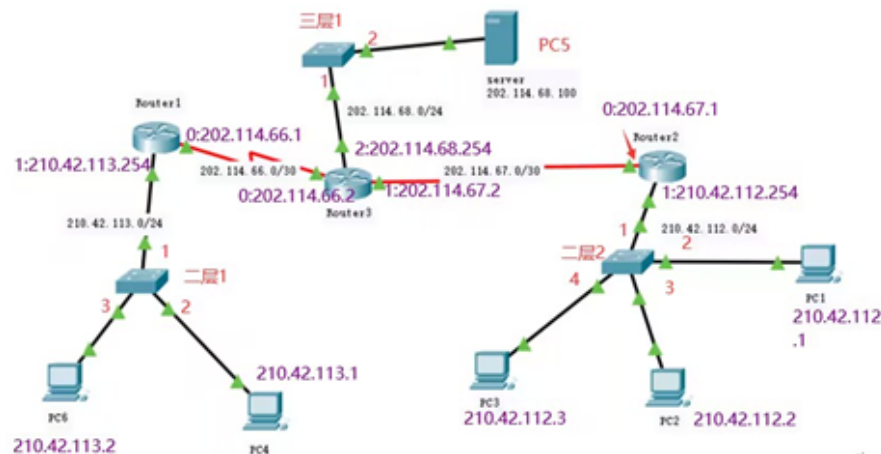


图 2: 新的网络拓扑图

物理连线如下:

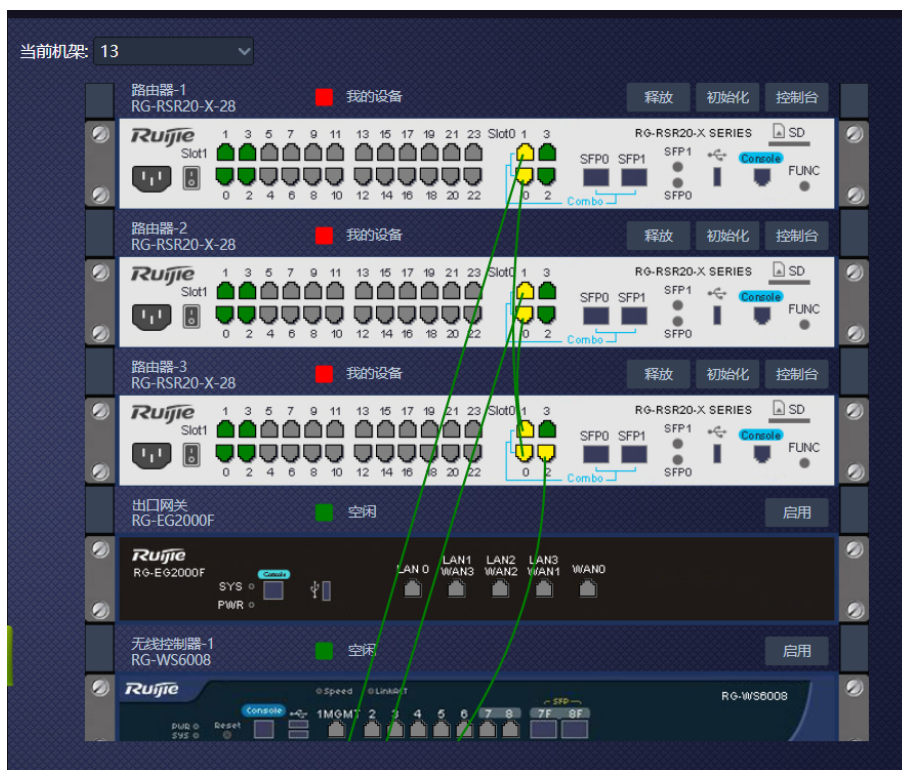


图 3: 物理连线

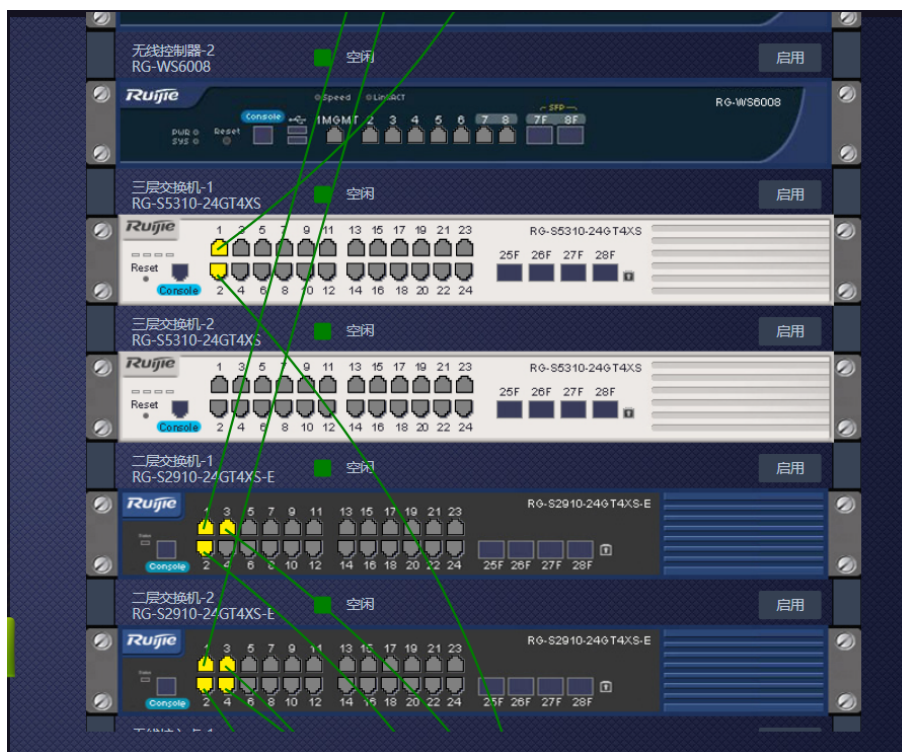


图 4: 物理连线 (续)



图 5: 物理连线 (续)

### 3.2 路由器 1

首先配置路由器接口 IP 地址：

```
en
con t
int gig 0/0
ip add 202.114.66.1 255.255.255.252
int gig 0/1
ip add 210.42.113.254 255.255.255.0
exit
```

配置 OSPF：

```
route ospf 1
network 202.114.66.0 255.255.255.252 area 0
network 210.42.113.0 255.255.255.0 area 0
```

```
Ruijie>en
Ruijie#con t
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#int gig 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip add 202.114.66.1 255.255.255.252
Ruijie(config-if-GigabitEthernet 0/0)#int gig 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip add 210.42.113.254 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#route ospf 1
Ruijie(config-router)#network 202.114.66.0 255.255.255.252 area 0
Ruijie(config-router)#*May 20 09:37:53: %OSPF-5-ADJCHG: Process 1, Nbr 202.114.68.2
4-GigabitEthernet 0/0 from Down to Init, HelloReceived.
*May 20 09:37:53: %OSPF-5-ADJCHG: Process 1, Nbr 202.114.68.254-GigabitEthernet 0/0
from Loading to Full, LoadingDone.

Ruijie(config-router)#network 210.42.113.0 255.255.255.0 area 0
Ruijie(config-router)#
```

图 6: 路由器 1 配置

### 3.3 路由器 2

采用 OSPF 路由协议对路由器 2 进行端口地址配置, 每个端口都纳入 area0 区域简化跨域操作。

```
Ruijie>en
Ruijie#conf
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#int g 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 202.114.67.1 255.255.255.252
Ruijie(config-if-GigabitEthernet 0/0)#exit
Ruijie(config)#int g 0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip address 210.42.112.254 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

图 7: 路由器 2 路由配置 a

```
Ruijie(config)#route ospf 1
Ruijie(config-router)#net work 202.114.67.0 255.255.255.252 area 0
^
% Invalid input detected at '^' marker.

Ruijie(config-router)#network 202.114.67.0 255.255.255.252 area 0
Ruijie(config-router)#network 210.42.112.0 255.255.255.0 area 0
Ruijie(config-router)#exit
```

图 8: 路由器 2 路由配置 b

配置完成过后查看路由器 2 的路由协议信息和路由表, 如下图:



```
Ruijie(config)#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 210.42.112.254
  Memory Overflow is enabled
  Router is not in overflow state now
  Number of areas in this router is 1: 1 normal 0 stub 0 nssa
  Routing for Networks:
    202.114.67.0 0.0.0.3 area 0
    210.42.112.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Distance: (default is 110)
```

图 9: 路由器 2 路由协议信息

```
Ruijie(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, VLAN 1
C    192.168.1.1/32 is local host.
O    202.114.66.0/30 [110/2] via 202.114.67.2, 00:02:02, GigabitEthernet 0/0
C    202.114.67.0/30 is directly connected, GigabitEthernet 0/0
C    202.114.67.1/32 is local host.
O    202.114.68.0/24 [110/2] via 202.114.67.2, 00:01:50, GigabitEthernet 0/0
C    210.42.112.0/24 is directly connected, GigabitEthernet 0/1
C    210.42.112.254/32 is local host.
O    210.42.113.0/24 [110/3] via 202.114.67.2, 00:00:13, GigabitEthernet 0/0
```

图 10: 路由器 2 路由表

根据题目要求, 对路由器 2 配置控制访问列表, 配置标准 ACL: 210.42.112.0 网络中的 PC1 可以 Tennaet 到 Router2, 其他 PC 不行, 故对路由器 2 进行配置:

```
ip access-list standard 1
permit host 210.42.112.1
deny any
exit
line vty 0 4
access-class 1 in
```

### 3.4 路由器 3

我们首先配置基本的端口地址和路由协议。我们使用的路由协议是 OSPF, 每个端口都纳入 area0 区域, 简化跨域操作。

```
en
con
int g 0/0
```

```
ip addr 202.114.66.2 255.255.255.252
int g 0/1
ip addr 202.114.67.2 255.255.255.252
int g 0/2
ip addr 202.114.68.254 255.255.255.0

router ospf 1
network 202.114.66.0 255.255.255.252 area0
network 202.114.67.0 255.255.255.252 area0
network 202.114.68.0 255.255.255.0 area0
```

路由器 3 和 Server 相连接，我们为配置 Server 的 WWW 服务和 TFTP 服务，需要在路由器 3 进行访问控制。

```
ip access-list extended 100
permit tcp 210.42.113.0 0.0.0.255 host 202.114.68.100 eq www
permit udp 210.42.112.0 0.0.0.255 host 202.114.68.100 eq tftp
int g 0/2
ip access-group 100 out
exit
```

#### 四、 出现的问题及解决方法

- 为了避免出现之前实验出现的配置错误，我们采用分步配置的策略。  
首先配置了全部路由信息，采用 ospf 学习路由表，然后尝试不同网段相互 ping 通。都 ping 通之后，再继续逐条配置 ACL。  
一条配置成功后，再配置下一条命令控制。
- 在尝试访问 telnet 服务的时候，我们要在服务器主机上开启 telnet 服务，并且要新建一个待拉取的文件，才能成功实现

#### 五、 实验结果

Router1 路由协议以及路由表：



```
Ruijie(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, VLAN 1
C    192.168.1.1/32 is local host.
C    202.114.66.0/30 is directly connected, GigabitEthernet 0/0
C    202.114.66.1/32 is local host.
O    202.114.67.0/30 [110/2] via 202.114.66.2, 01:15:06, GigabitEthernet 0/0
O    202.114.68.0/24 [110/2] via 202.114.66.2, 01:15:06, GigabitEthernet 0/0
O    210.42.112.0/24 [110/3] via 202.114.66.2, 01:15:06, GigabitEthernet 0/0
C    210.42.113.0/24 is directly connected, GigabitEthernet 0/1
C    210.42.113.254/32 is local host.
Ruijie(config)#
```

图 11: Router1 路由协议以及路由表

Router2 路由协议以及路由表:

```
Ruijie(config)#show ip route

Codes: C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, VLAN 1
C    192.168.1.1/32 is local host.
O    202.114.66.0/30 [110/2] via 202.114.67.2, 01:14:09, GigabitEthernet 0/0
C    202.114.67.0/30 is directly connected, GigabitEthernet 0/0
C    202.114.67.1/32 is local host.
O    202.114.68.0/24 [110/2] via 202.114.67.2, 01:13:56, GigabitEthernet 0/0
C    210.42.112.0/24 is directly connected, GigabitEthernet 0/1
C    210.42.112.254/32 is local host.
O    210.42.113.0/24 [110/3] via 202.114.67.2, 01:12:20, GigabitEthernet 0/0
Ruijie(config)#
```

图 12: Router2 路由协议以及路由表

Router1 访问控制信息:

```
!
ip access-list standard 1
 10 deny host 210.42.112.2
 20 permit any
!
```

图 13: Router1 访问控制信息

Router2 访问控制信息:

```
ip access-list standard 1
 10 permit host 210.42.112.1
 20 deny any
!
```

图 14: Router2 访问控制信息

Router3 访问控制信息:

```
!
ip access-list extended 100
 10 permit tcp 210.42.113.0 0.0.0.255 host 202.114.68.100 eq www
 20 permit tcp 210.42.112.0 0.0.0.255 host 202.114.68.100 eq ftp
 30 permit udp 210.42.112.0 0.0.0.255 host 202.114.68.100 eq tftp
!
```

图 15: Router3 访问控制信息

PC1 Ping PC4:

```
C:\Users\Administrator>ping 210.42.113.1

正在 Ping 210.42.113.1 具有 32 字节的数据:
来自 210.42.113.1 的回复: 字节=32 时间=1ms TTL=125
来自 210.42.113.1 的回复: 字节=32 时间=1ms TTL=125
来自 210.42.113.1 的回复: 字节=32 时间=1ms TTL=125
来自 210.42.113.1 的回复: 字节=32 时间<1ms TTL=125

210.42.113.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

图 16: PC1 ping PC4

PC2 Ping PC4:

```
C:\Users\Administrator>ping 210.42.113.1

正在 Ping 210.42.113.1 具有 32 字节的数据:
请求超时。
请求超时。
```

图 17: PC2 Ping PC4

PC4 访问 Server WWW 服务器:

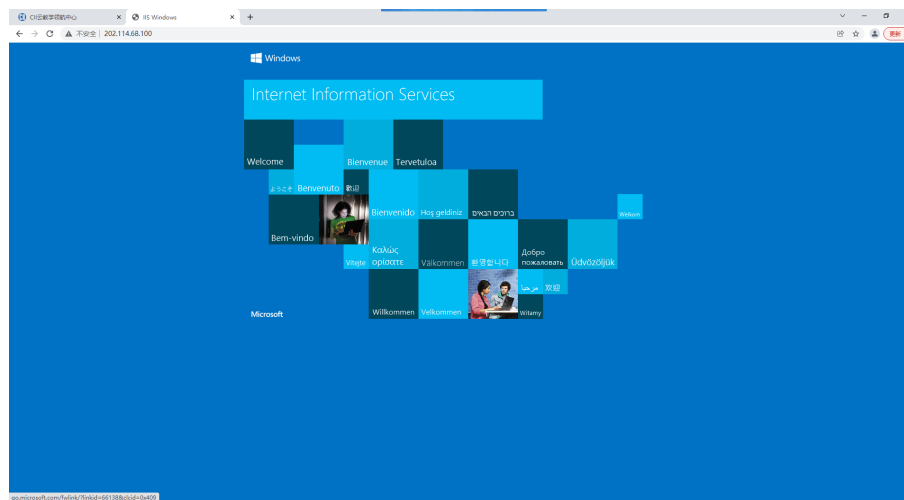


图 18: PC4 访问 Server WWW 服务器

PC2 访问 Server WWW 服务器:

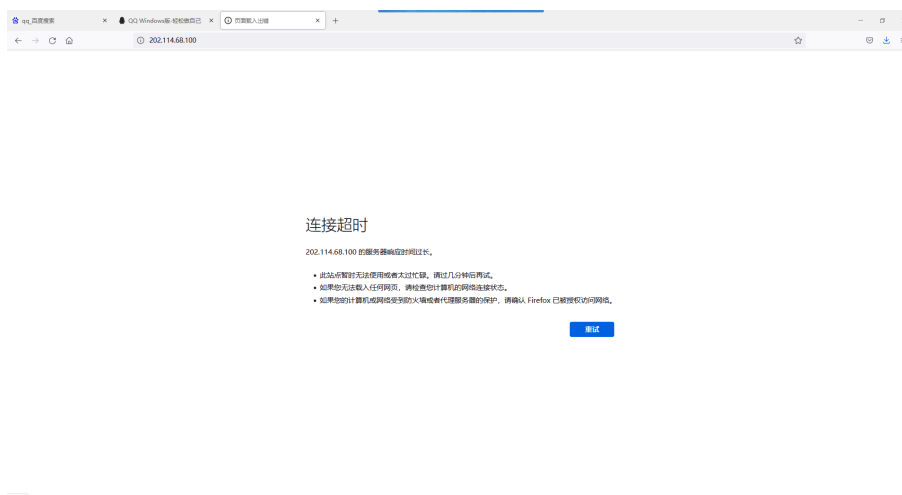


图 19: PC2 访问 Server WWW 服务器

PC2 访问 Server TFTP 服务:

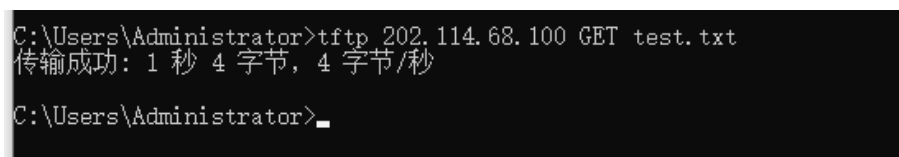


图 20: PC2 访问 Server TFTP 服务

然后在本地可以看到成功拉取到 test.txt

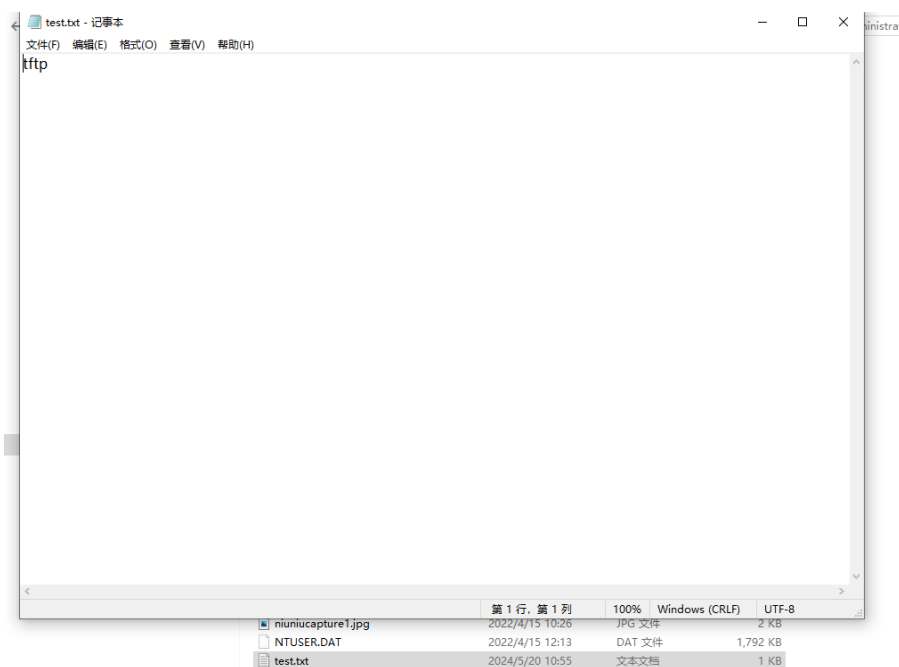


图 21: PC2 成功拉取到 test 文件



## 七、 指导教师评语及成绩

【评语】

成 绩：  
批阅日期：

指导老师签名：