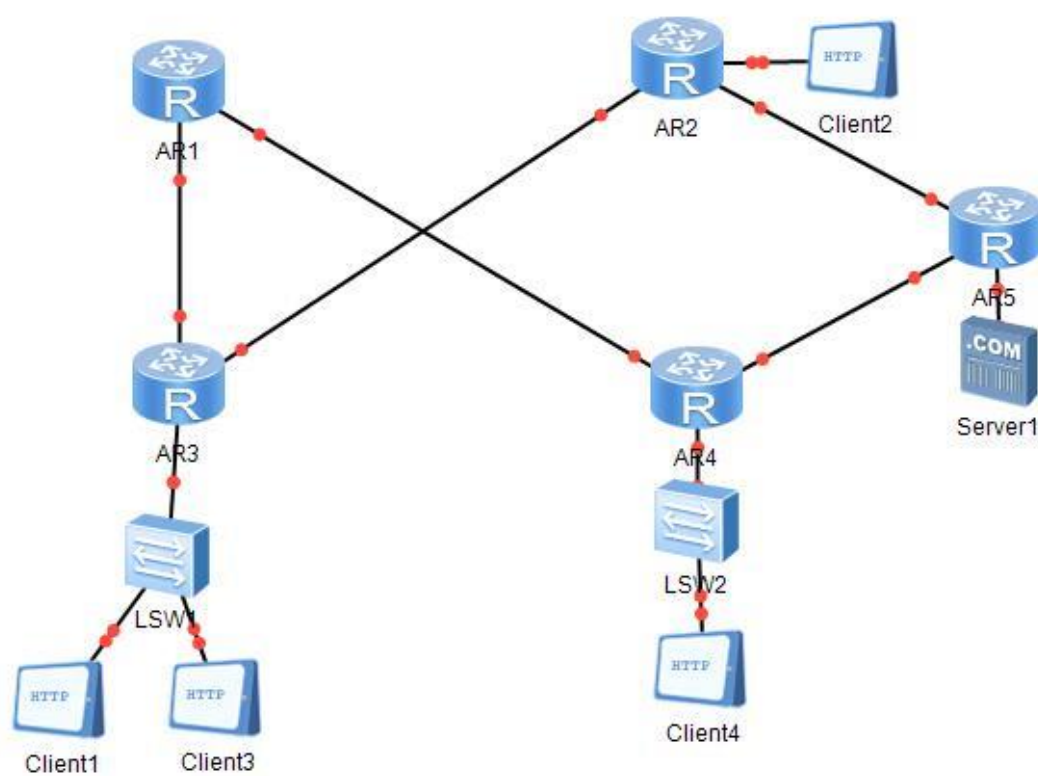
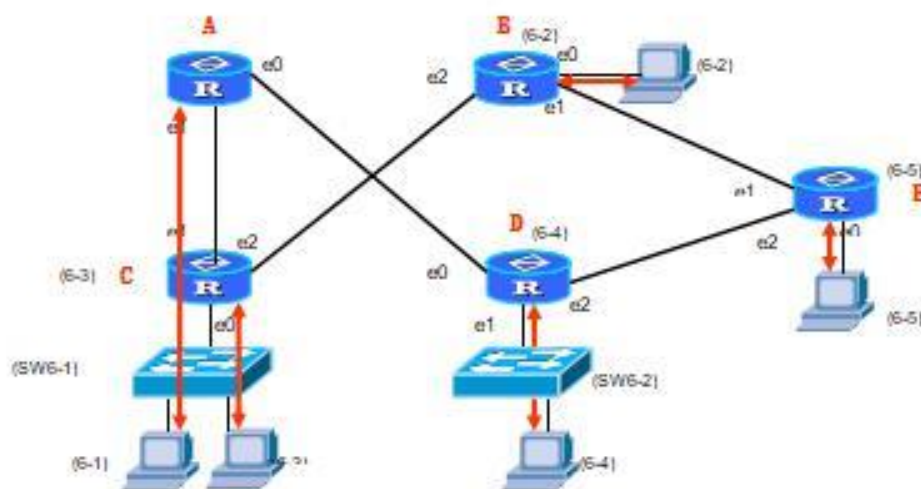


实验报告：使用高级访问控制列表

Hollow Man

一、实验小组拓扑





二、实验准备

1、路由器网络地址方案设计

	E0	E1	E2
A	219.246.2.1/24	219.246.1.1/24	
B	219.246.9.1/24	219.246.8.2/24	219.246.4.2/24
C	219.246.3.1/24	219.246.1.2/24	219.246.4.1/24
D	219.246.2.2/24	219.246.5.1/24	219.246.6.1/24
E	219.246.7.1/24	219.246.8.1/24	219.246.6.2/24

2、PC 机设置方案

主机序号	IP 地址	网关
6-1	219.246.3.2/24	219.246.3.1/24
6-2	219.246.9.2/24	219.246.9.1/24
6-3	219.246.3.3/24	219.246.3.1/24
6-4	219.246.5.2/24	219.246.5.1/24
6-5	219.246.7.2/24	219.246.7.1/24

三、实验内容

实验 1：FTP 访问控制实验；

- (1)、在 PC5 上搭建 FTP server；
- (2)、测试各个主机是否能打开 ftp；
- (3)、禁止特定主机 PC3 访问 FTP；
- (4)、禁止特定网络 201.1.1.0/192 的所有主机访问 FTP；
- (5)、改变 FTP 的端口为 2121 后，禁止特定网络 201.1.1.0/192 的所有主机访问 FTP。

实验 2：禁止使用 QQ 实验(假设 PC5 为 QQ 服务器，禁止网络上的主机访问 QQ，即访问到特定主机 PC5)。

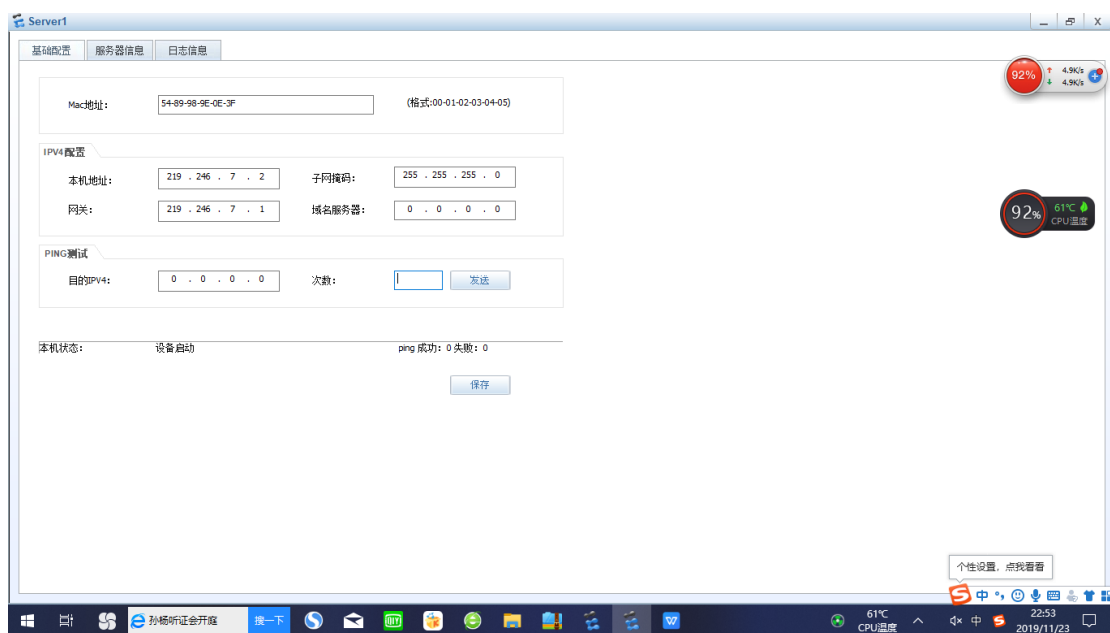
- (1)、禁止特定主机 PC3 访问 PC5：

(2)、禁止特定网络 201.1.1.0/192 中的主机访问 PC5

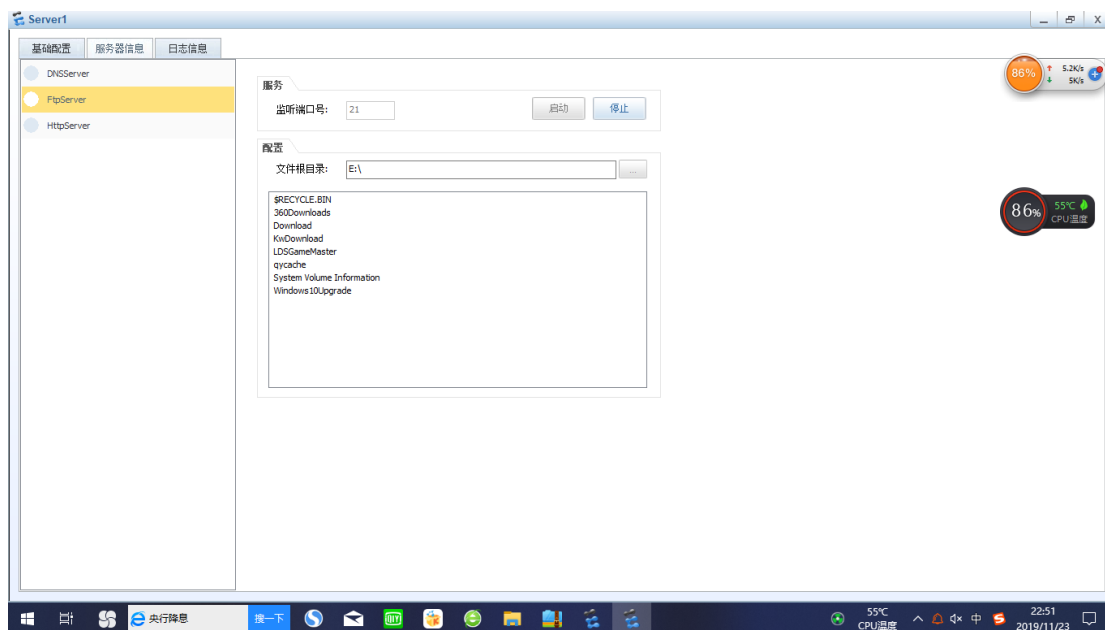
实验一：FTP 访问控制实验

(1)在 PC5 上搭建 FTP server;

在模拟器中设置 FTP 服务器：

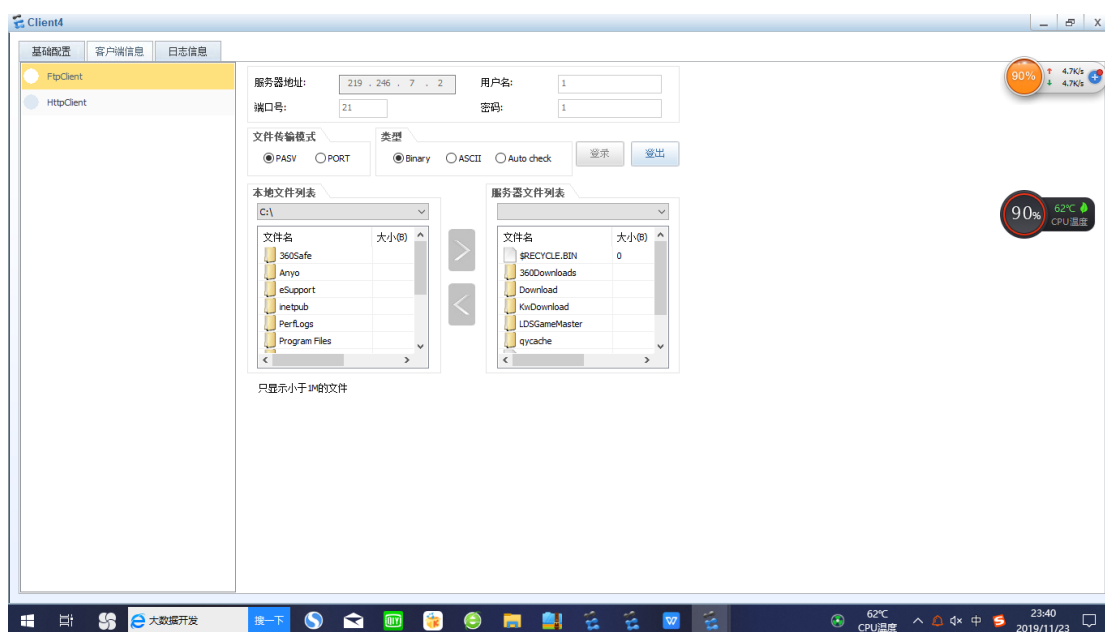


设置 FTP 服务器端口号并启动服务器



(2)测试各个主机是否能打开 ftp

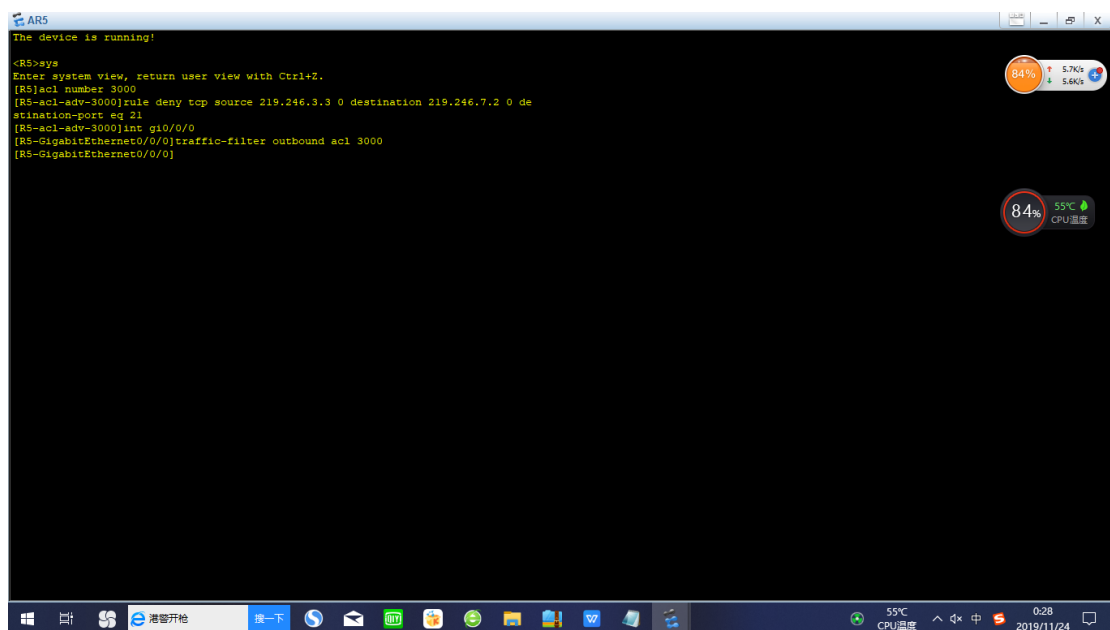
客户机 4 登录 ftp 成功



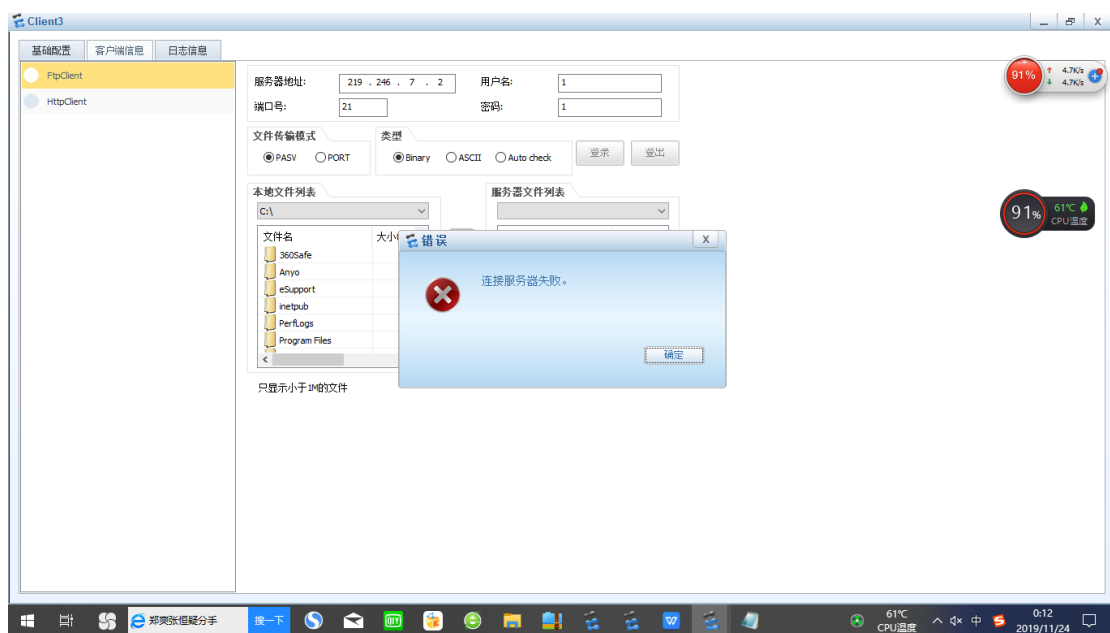
主机可正常登录 ftp 服务器，其余截图不予展示

(3)禁止特定主机 PC3 访问 FTP

添加访问规则：

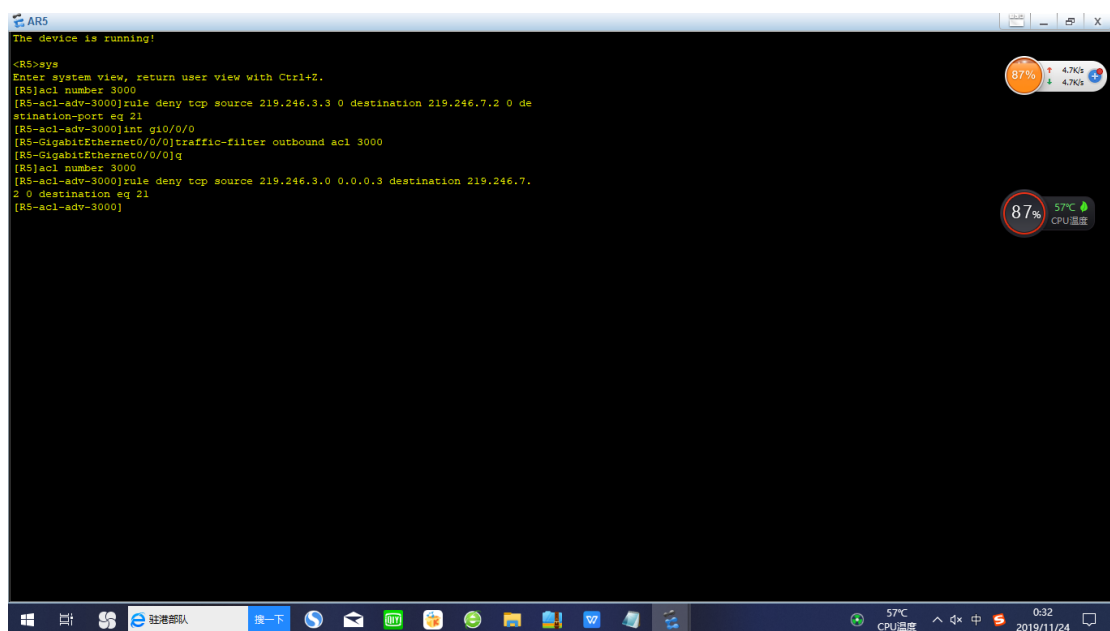


添加访问规则后客户机 3 无法登录 ftp 服务器：

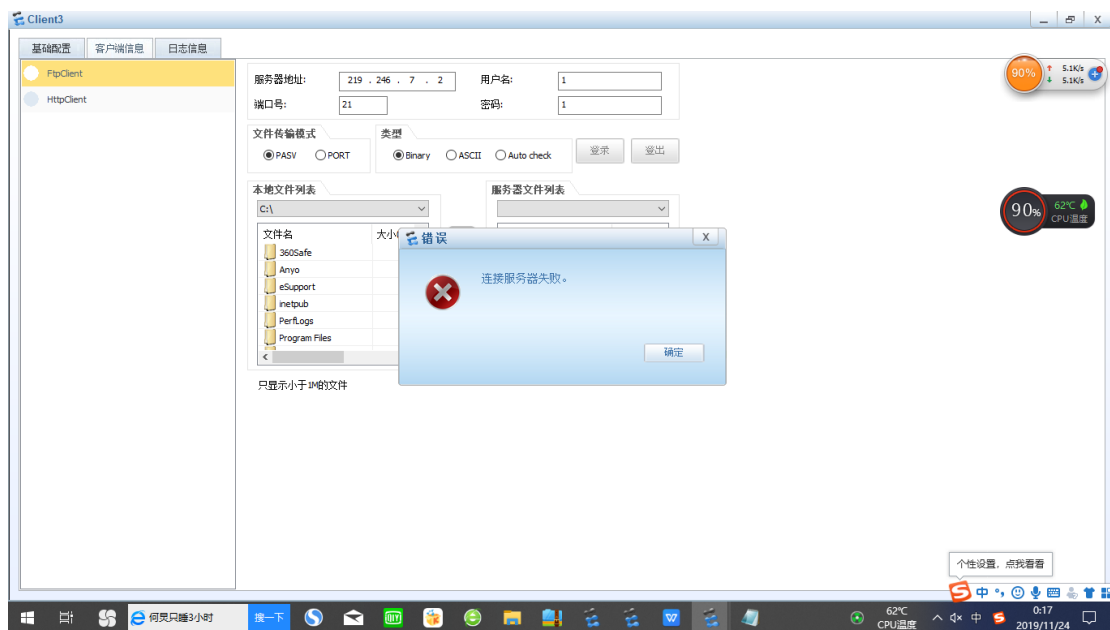
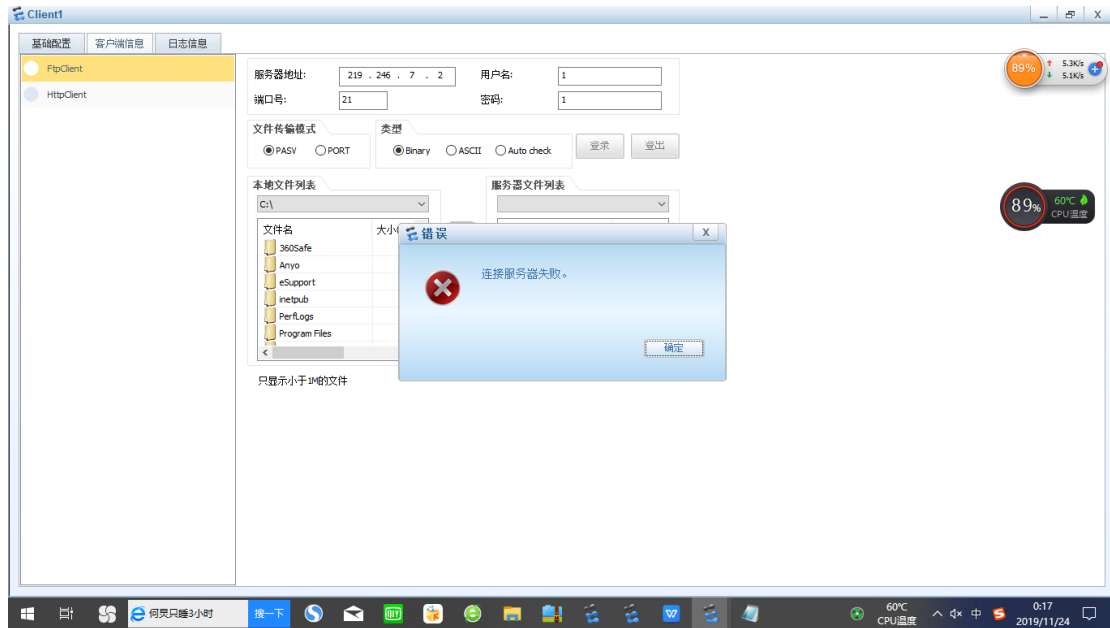


（4）禁止特定网络 219.246.3.1/24 的所有主机访问 FTP

添加访问规则：

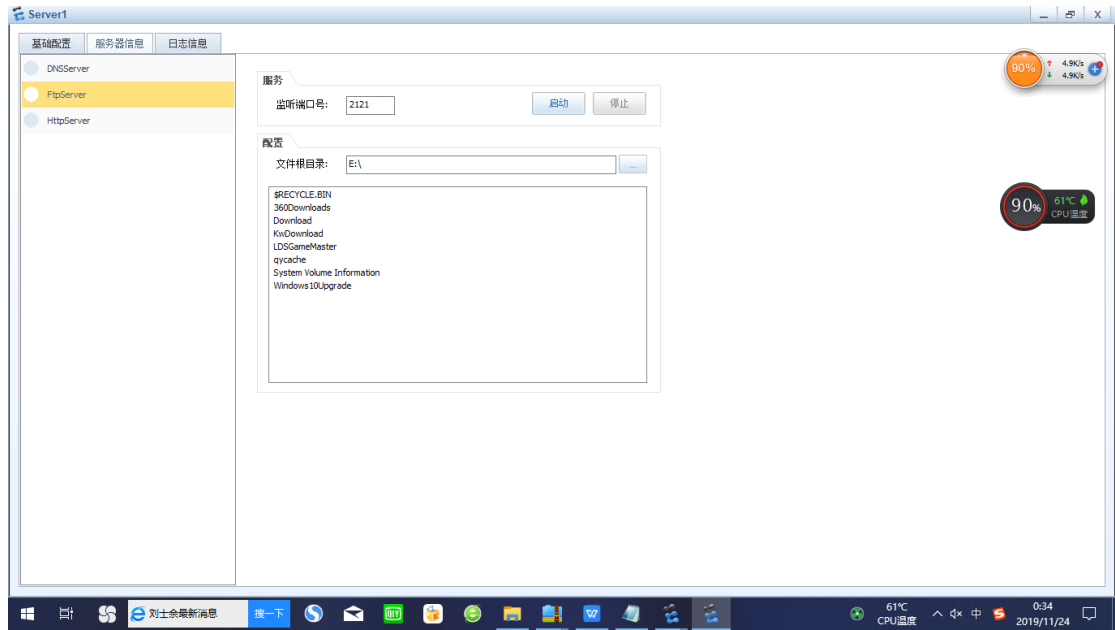


219.246.3.1 下的主机访问失败：

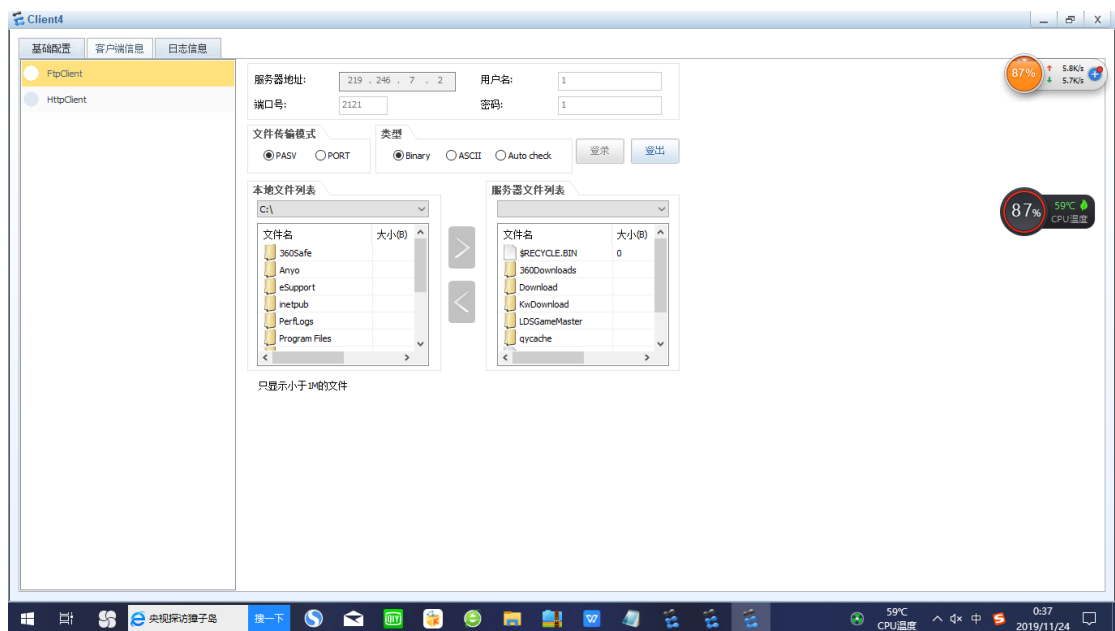


(5)改变 FTP 的端口为 2121 后,禁止特定网络 219.246.3.1/24 的所有主机访问 FTP

更改 ftp 服务器端口为 2121 并启动

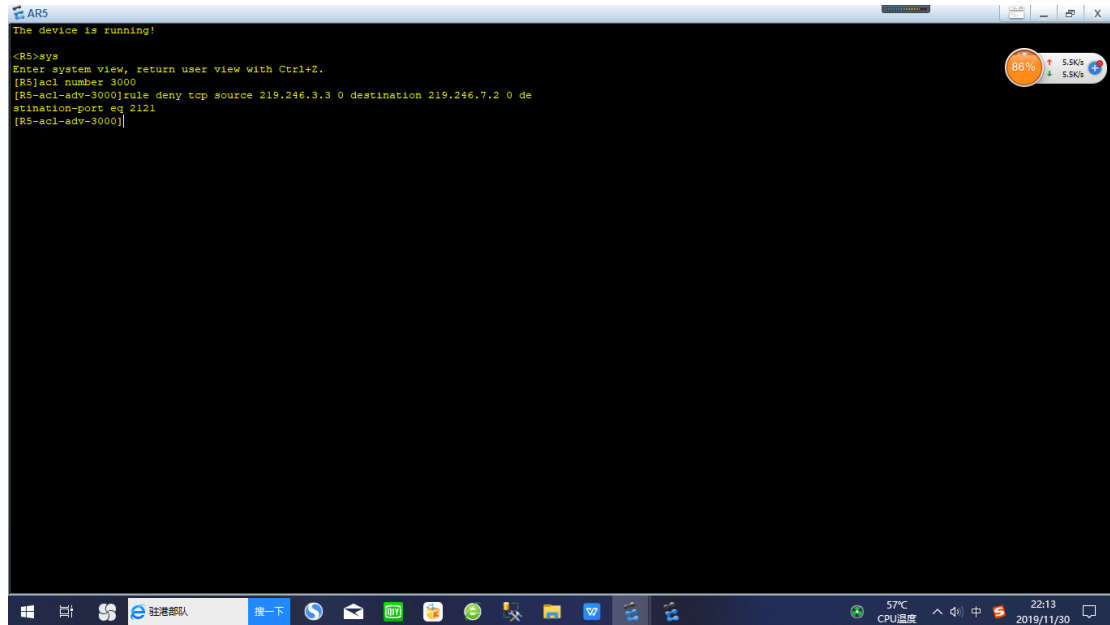


客户机 4 更改端口，显示登录成功，其余截图不予展示

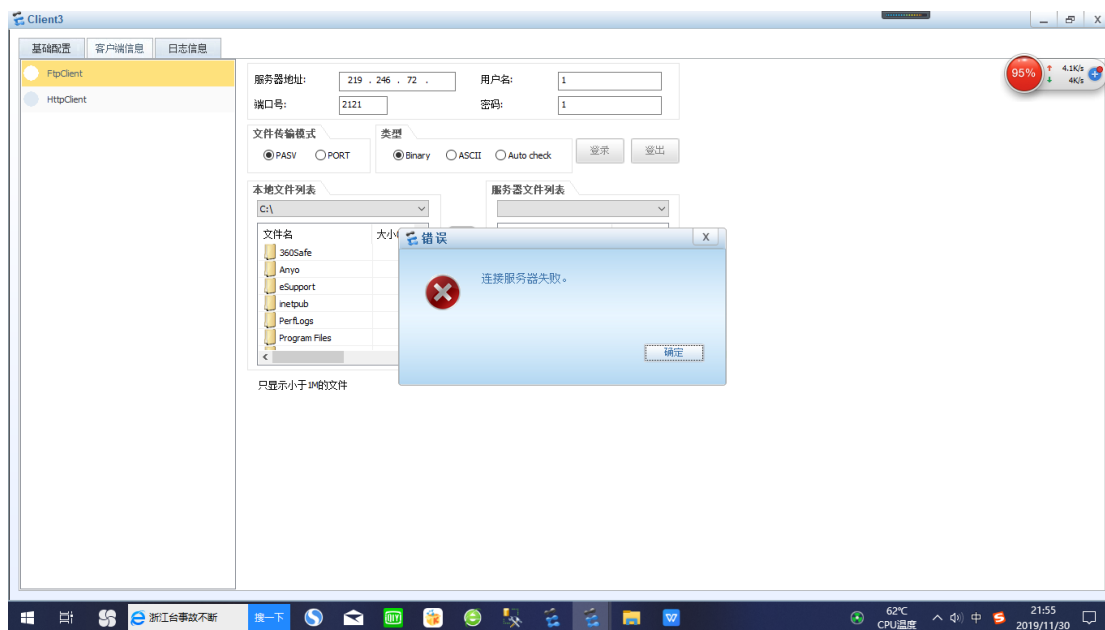
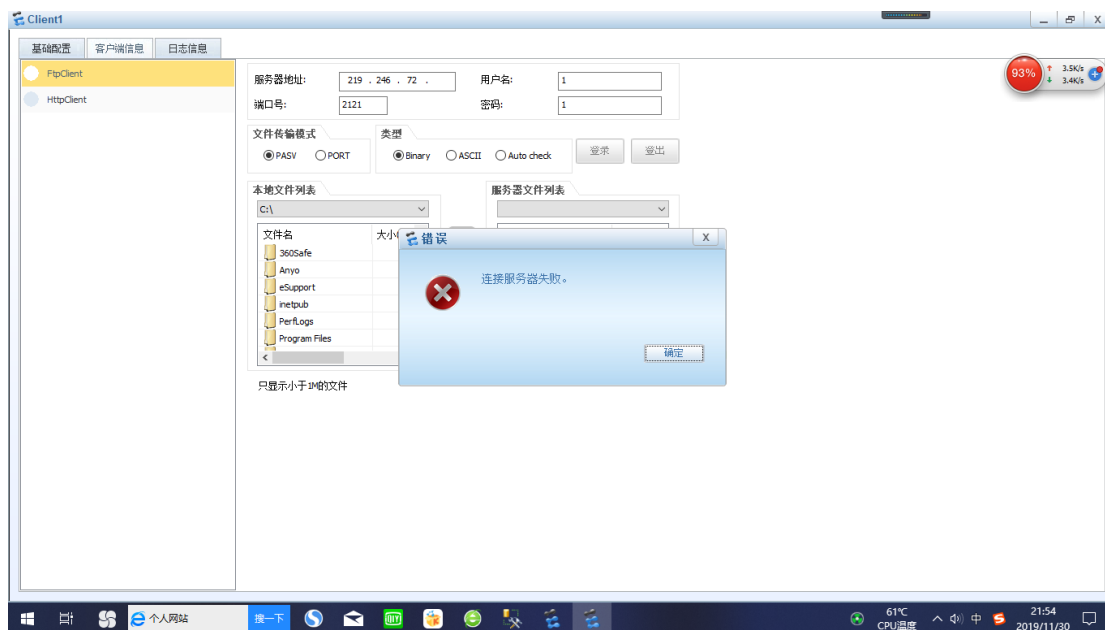


禁止特定网络 219.246.3.1/24 的所有主机访问 FTP

添加访问规则：



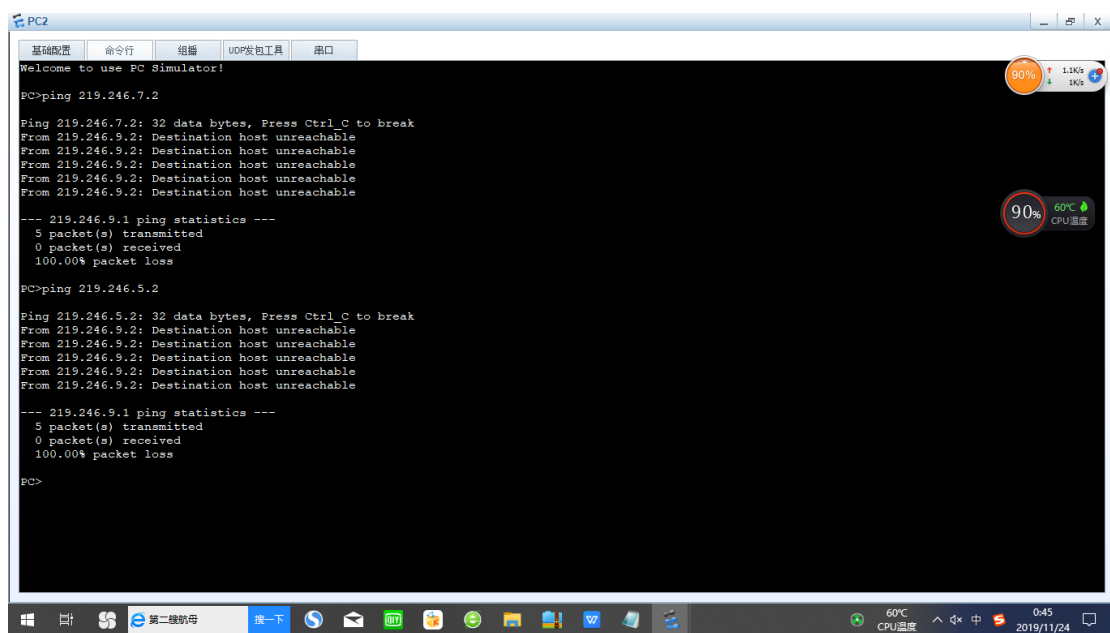
219.246.3.1 下的主机访问失败：



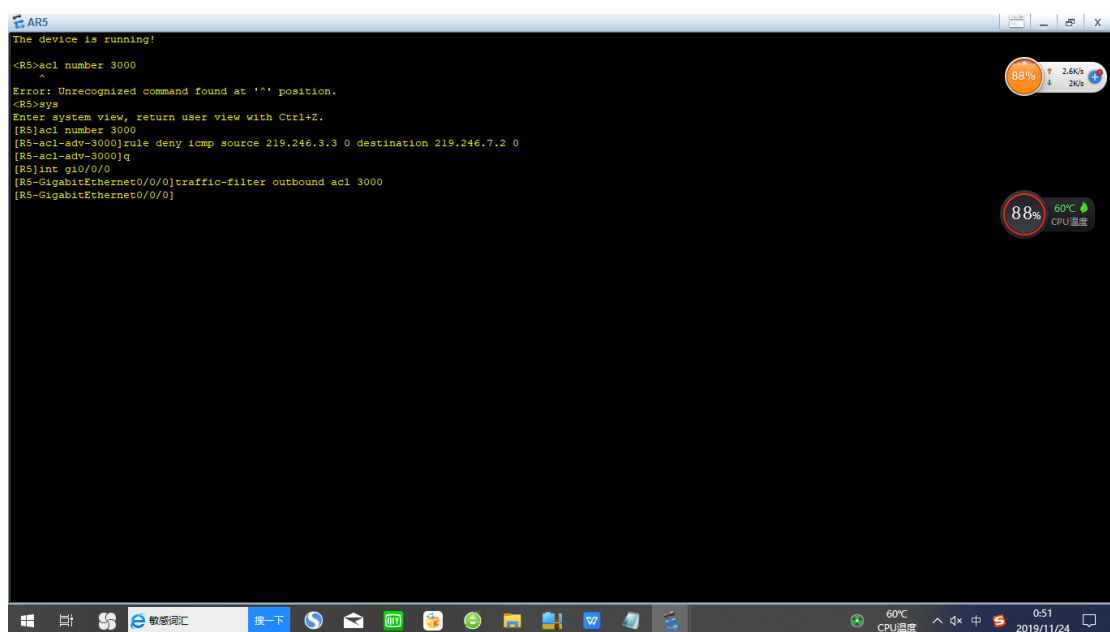
实验 2：禁止使用 QQ 实验(假设 PC5 为 QQ 服务器，禁止网络上的主机访问 QQ，即访问到特定主机 PC5

(1) 禁止特定主机 PC3 访问 PC5:

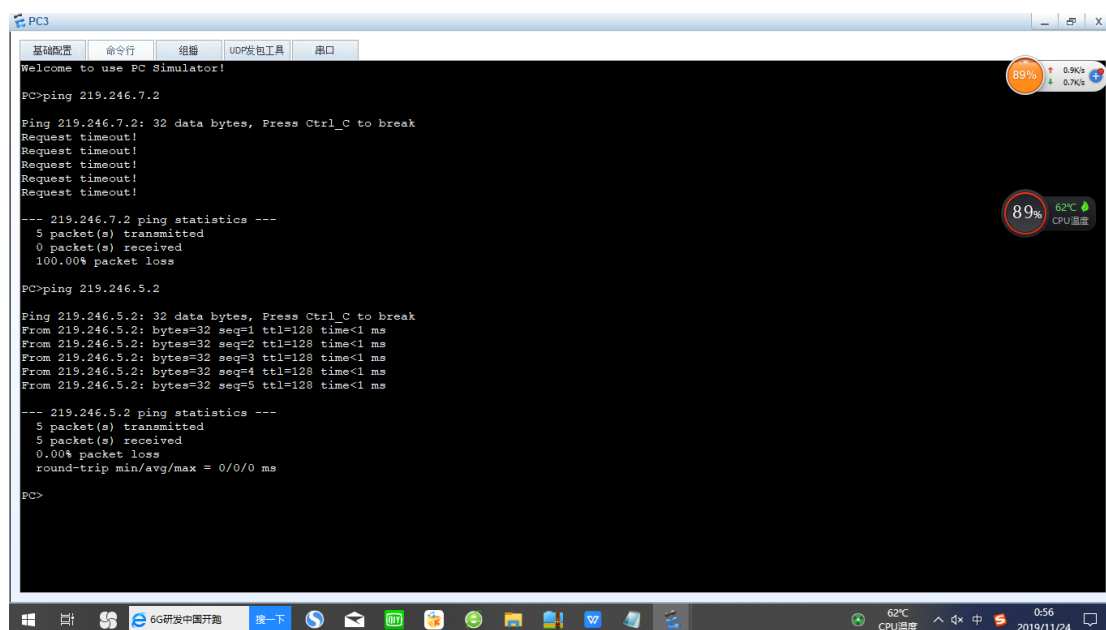
实验前 Pc3 可以访问 pc4 和 pc5



新建访问控制列表并设置到端口



设置完以后 pc3 可以访问 pc4, 无法访问 pc5, 说明操作成功 •



The screenshot shows a terminal window titled 'PC3' with a menu bar containing '基础配置', '命令行', '组播', 'UDP发包工具', and '串口'. The terminal output shows the following commands and results:

```
Welcome to use PC Simulator!

PC>ping 219.246.7.2

Ping 219.246.7.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 219.246.7.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
 100.00% packet loss

PC>ping 219.246.5.2

Ping 219.246.5.2: 32 data bytes, Press Ctrl_C to break
From 219.246.5.2: bytes=32 seq=1 ttl=128 time<1 ms
From 219.246.5.2: bytes=32 seq=2 ttl=128 time<1 ms
From 219.246.5.2: bytes=32 seq=3 ttl=128 time<1 ms
From 219.246.5.2: bytes=32 seq=4 ttl=128 time<1 ms
From 219.246.5.2: bytes=32 seq=5 ttl=128 time<1 ms

--- 219.246.5.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
  round-trip min/avg/max = 0/0/0 ms

PC>
```

The Windows taskbar at the bottom shows the system clock as 0:56 on 2019/11/24, with a CPU temperature of 62°C.

(2) 禁止特定网络 219.246.3.1/24 中的主机访问 PC5

添加访问规则

```
AR5
[RS-acl-adv-3000]rule deny icmp source 219.246.3.3 0 destination 219.246.7.2 0
[RS-acl-adv-3000]q
[RS]int gi0/0/0
[RS-GigabitEthernet0/0/0]traffic-filter outbound acl 3000
[RS-GigabitEthernet0/0/0]int gi0/0/1
[RS-GigabitEthernet0/0/1]traffic-filter outbound acl 3000
[RS-GigabitEthernet0/0/1]

Please check whether system data has been changed, and save data in time

Configuration console time out, please press any key to log on

<R5>sys
Enter system view, return user view with Ctrl+Z.
[RS]acl number 3000
[RS-acl-adv-3000]rule deny icmp source 219.246.3.0 0.0.0.3 destination 219.246.7
.2 0
[RS-acl-adv-3000]dis acl all
Total quantity of nonempty ACL number is 1

Advanced ACL 3000, 2 rules
Acl's step is 5
rule 5 deny icmp source 219.246.3.3 0 destination 219.246.7.2 0
rule 10 deny icmp source 219.246.3.0 0.0.0.3 destination 219.246.7.2 0
[RS-acl-adv-3000]rule deny icmp source 219.246.3.0 0.0.0.3 destination 219.246.7
^
Error: Wrong parameter found at '^' position.
[RS-acl-adv-3000]
[RS-acl-adv-3000].2 0
^
Error: Unrecognized command found at '^' position.
[RS-acl-adv-3000]
[RS-acl-adv-3000]rule deny icmp source 219.246.3.0 0.0.0.3 destination 219.246.7
.2 q
^
Error: Wrong parameter found at '^' position.
[RS-acl-adv-3000]q
[RS]traffic-filter outbound acl 3000
^
Error: Unrecognized command found at '^' position.
[RS]
```

添加完规则后 pc1 不能访问 pc5

```
PC1
Welcome to use PC Simulator!

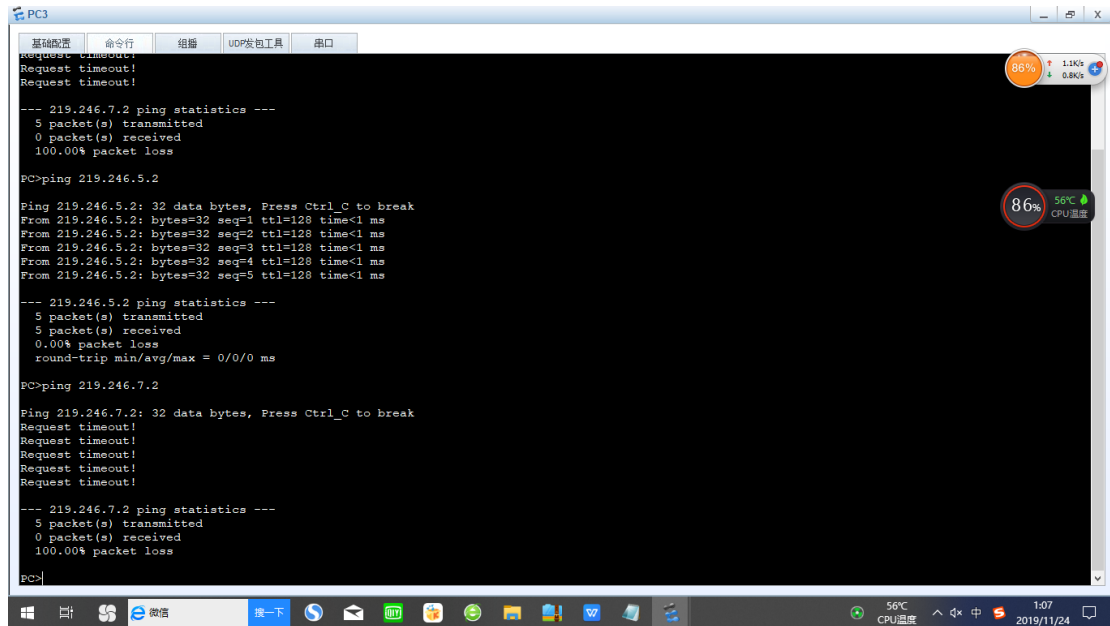
PC>ping 219.246.7.2

Ping 219.246.7.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 219.246.7.2 ping statistics ---
5 packet(s) transmitted
0 packet(s) received
100.00% packet loss

PC>
```

Pc3 不能访问 pc5



```
PC3
基础配置 命令执行 组播 UDP发包工具 串口
Request timeout!
Request timeout!
Request timeout!

--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>ping 219.246.5.2

Ping 219.246.5.2: 32 data bytes, Press Ctrl_C to break
From 219.246.5.2: bytes=32 seq=1 ttl=128 time<1 ms
From 219.246.5.2: bytes=32 seq=2 ttl=128 time<1 ms
From 219.246.5.2: bytes=32 seq=3 ttl=128 time<1 ms
From 219.246.5.2: bytes=32 seq=4 ttl=128 time<1 ms
From 219.246.5.2: bytes=32 seq=5 ttl=128 time<1 ms

--- 219.246.5.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 0/0/0 ms

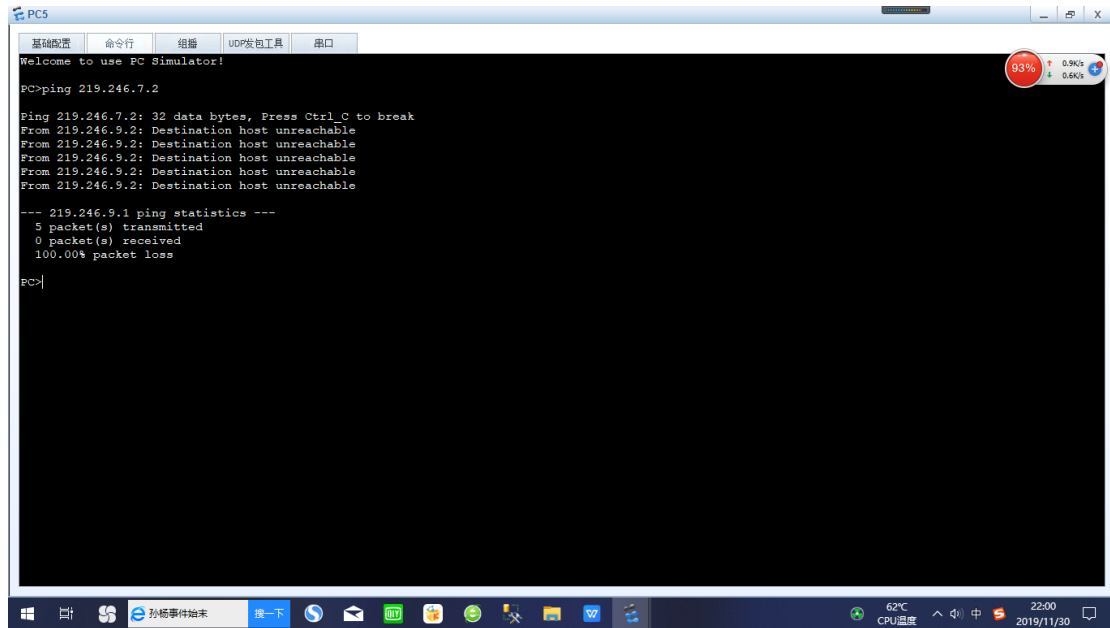
PC>ping 219.246.7.2

Ping 219.246.7.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 219.246.7.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>
```

但 Pc2 可以访问 pc5 其余截图不予展示



四、实验总结

1、实验结果

访问控制列表（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通过，哪些数据包需要拒绝。ACL 使用包裹里从技术，在路由器上读取 OSI 七层模型的第三层和第四层包头中的信息，如源地址、目的地址、源端口、目的端口等。根据预先设定好的规则对包进行过滤，从而达到访问控制的目的。

通过本实验，我们发现其实际应用有：

阻止某个网段访问服务器

阻止 A 网段访问 B 网段，但 B 网段可以访问 A 网段。

禁止某些端口进入网络，可达到安全性

2、心得体会

本次实验，在老师的指导下，和小组成员的共同努力之下，完成的过程较为顺利。在本次实验中，我们并没有具体在一个单独实验中测试，通过查阅相关资料，我们发现：

IPv4 ACL 支持两种匹配顺序：

配置顺序：按照用户配置规则的先后顺序进行规则匹配。

自动排序：按照“深度优先”的顺序进行规则匹配。