

# 网络技术与应用课程报告

---

## 第七次实验报告

---

学号：2111033

姓名：艾明旭

年级：2021级

专业：信息安全

## 一、实验内容说明

---

### 防火墙实验

要求如下：

1. 了解包过滤防火墙的基本配置方法、配置命令和配置过程
2. 利用标准ACL，将防火墙配置为只允许某个网络中的主机访问另一个网络
3. 利用扩展ACL，将防火墙配置为拒绝某个网络中的某台主机访问网络中的Web服务器
4. （选做）将防火墙配置为允许内网用户自由地向外网发起TCP连接，同时可以接收外网发回的TCP应答数据包。但是，不允许外网的用户主动向内网发起TCP连接

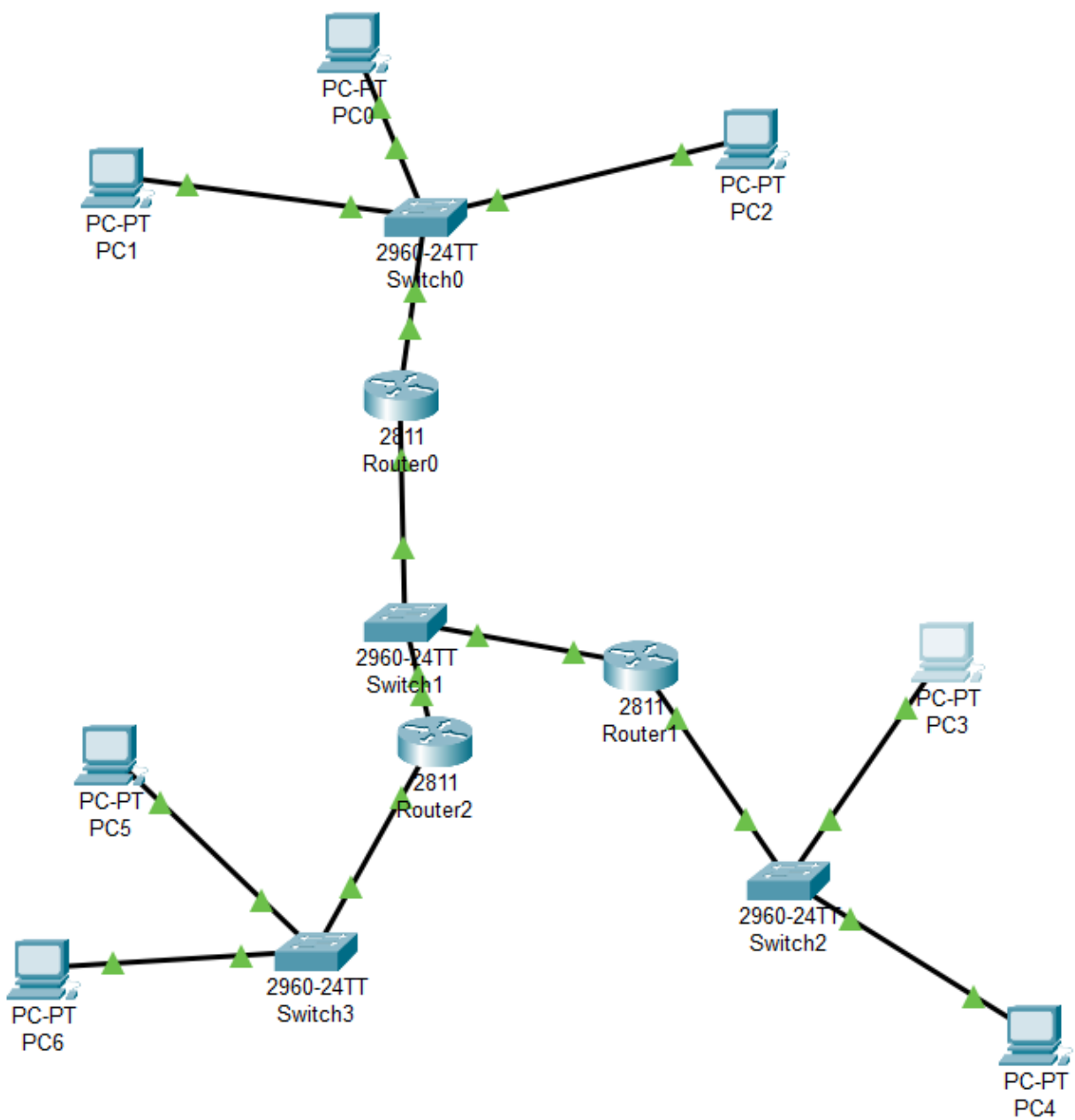
## 二、前期准备

---

标准ACL：

### (1)拓扑图

标准ACL实验的拓扑图如下所示：



## (2) ip 地址分配

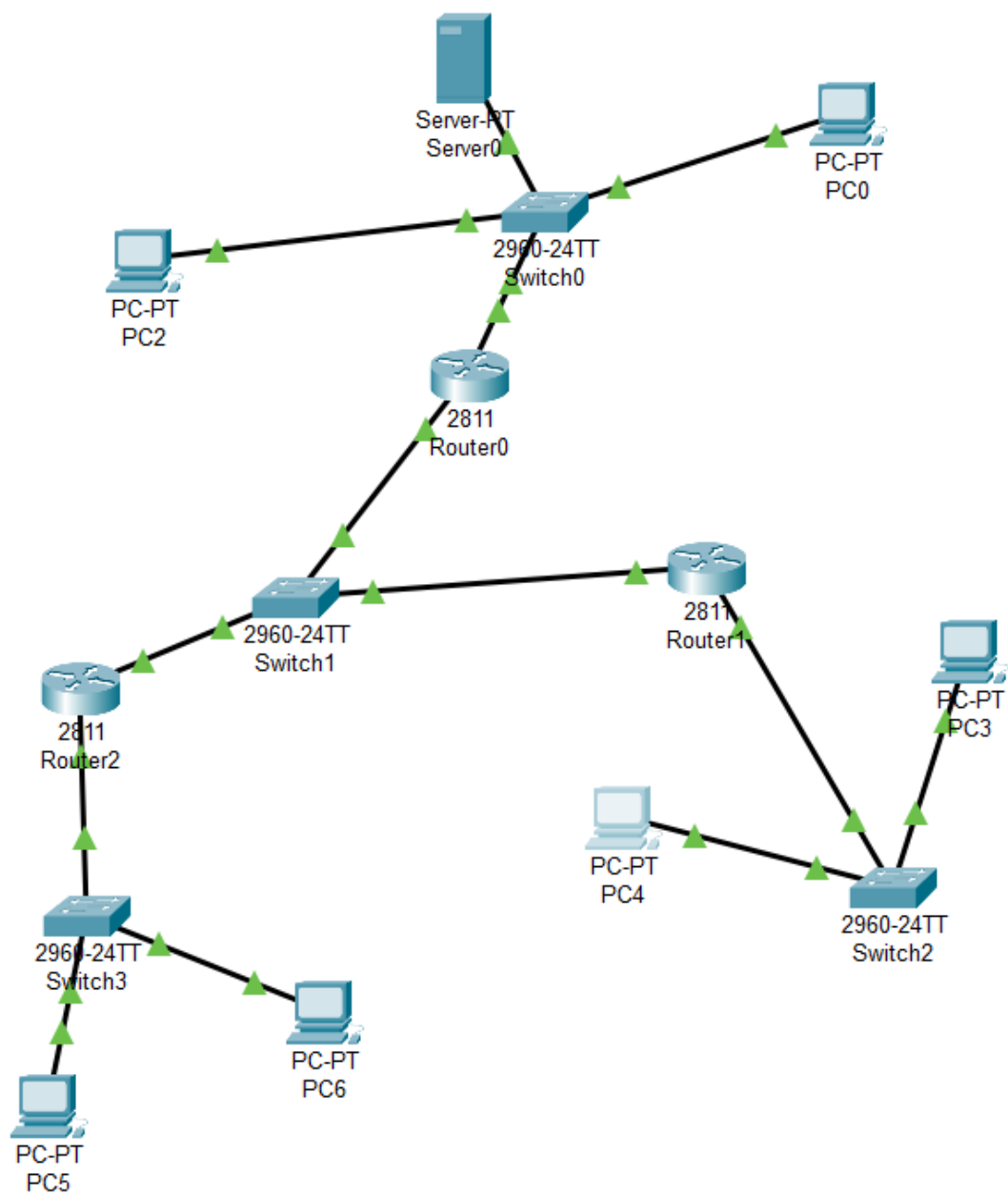
标准ACL实验的 ip 地址分配如下所示：

Machine	IPv4 Address	Subnet Mask	网关
PC0	202.113.25.2	255.255.255.0	202.113.25.1
PC1	202.113.25.3	255.255.255.0	202.113.25.1
PC2	202.113.25.4	255.255.255.0	202.113.25.1
PC3	202.113.26.2	255.255.255.0	202.113.26.1
PC4	202.113.26.3	255.255.255.0	202.113.26.1
PC5	202.113.27.3	255.255.255.0	202.113.27.1
PC6	202.113.27.2	255.255.255.0	202.113.27.1
Router0 Fa0/0	202.113.25.1	255.255.255.0	
Router0 Fa0/1	202.113.28.1	255.255.255.0	
Router1 Fa0/0	202.113.28.2	255.255.255.0	
Router1 Fa0/1	202.113.26.1	255.255.255.0	
Router2 Fa0/0	202.113.28.3	255.255.255.0	
Router2 Fa0/1	202.113.27.1	255.255.255.0	

**扩展ACL:**

**(1)拓扑图**

扩展ACL实验的拓扑图如下所示:



## (2) ip 地址分配

扩展ACL实验的 ip 地址分配如下所示：

Machine	IPv4 Address	Subnet Mask	网关
PC0	202.113.25.2	255.255.255.0	202.113.25.1
PC1	202.113.25.3	255.255.255.0	202.113.25.1
Server0	202.113.25.4	255.255.255.0	202.113.25.1
PC3	202.113.26.2	255.255.255.0	202.113.26.1
PC4	202.113.26.3	255.255.255.0	202.113.26.1
PC5	202.113.27.3	255.255.255.0	202.113.27.1
PC6	202.113.27.2	255.255.255.0	202.113.27.1
Router0 Fa0/0	202.113.25.1	255.255.255.0	
Router0 Fa0/1	202.113.28.1	255.255.255.0	
Router1 Fa0/0	202.113.28.2	255.255.255.0	
Router1 Fa0/1	202.113.26.1	255.255.255.0	
Router2 Fa0/0	202.113.28.3	255.255.255.0	
Router2 Fa0/1	202.113.27.1	255.255.255.0	

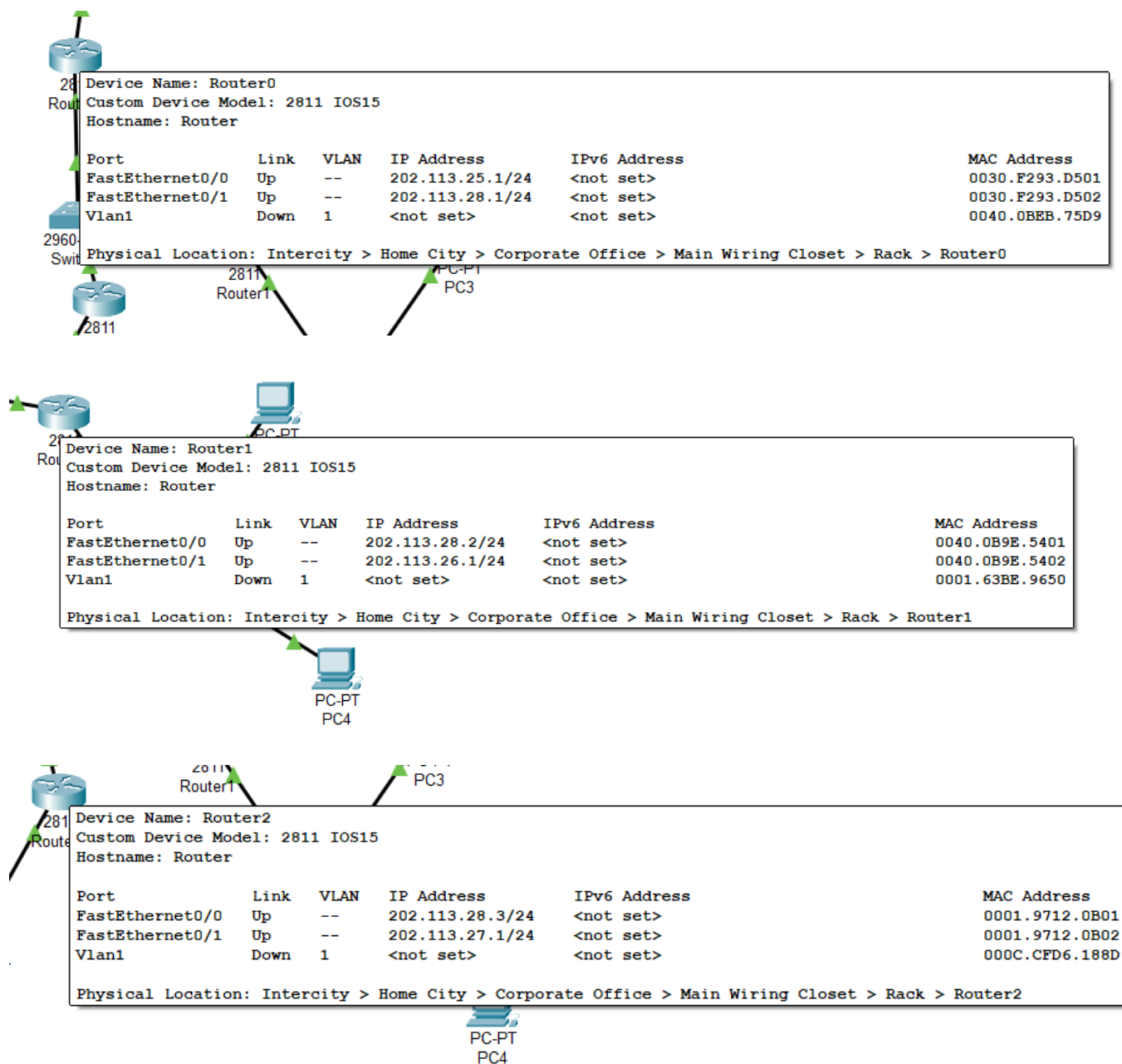
### 三、实验过程

本次实验将分为两个部分来进行，分别是标准控制列表和扩展控制列表，所以下面将从整个项目来对本次实验过程进行介绍。

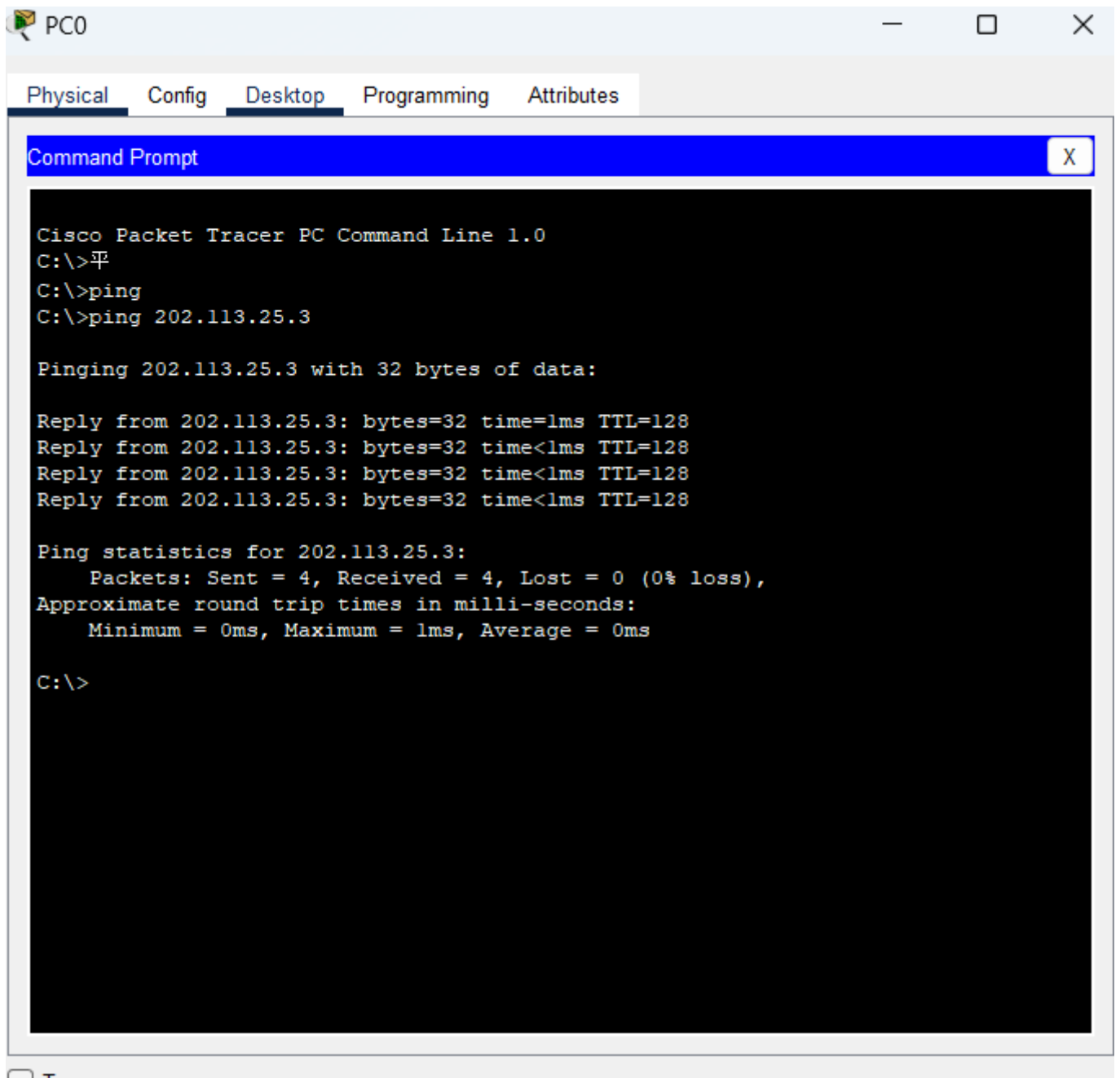
#### 1、标准ACL

##### (1)网络拓扑和基本配置

首先对三台主机以及服务器按照准备过程中的地址进行ip地址配置，由于ip地址的配置并不是本次实验的重点，这里只展示出三个路由器配置完成后的地址分配：



按照拓扑图配置仿真环境下的网络，在配置防火墙之前，保证所连接的设备能够ping通，如下图所示：



## (2)建立标准访问列表

本次实验的实现目标是在上方的网络允许右下角的网络中的主机访问，但不允许其他网络中的主机访问（在本次实验中为左下角的网络）

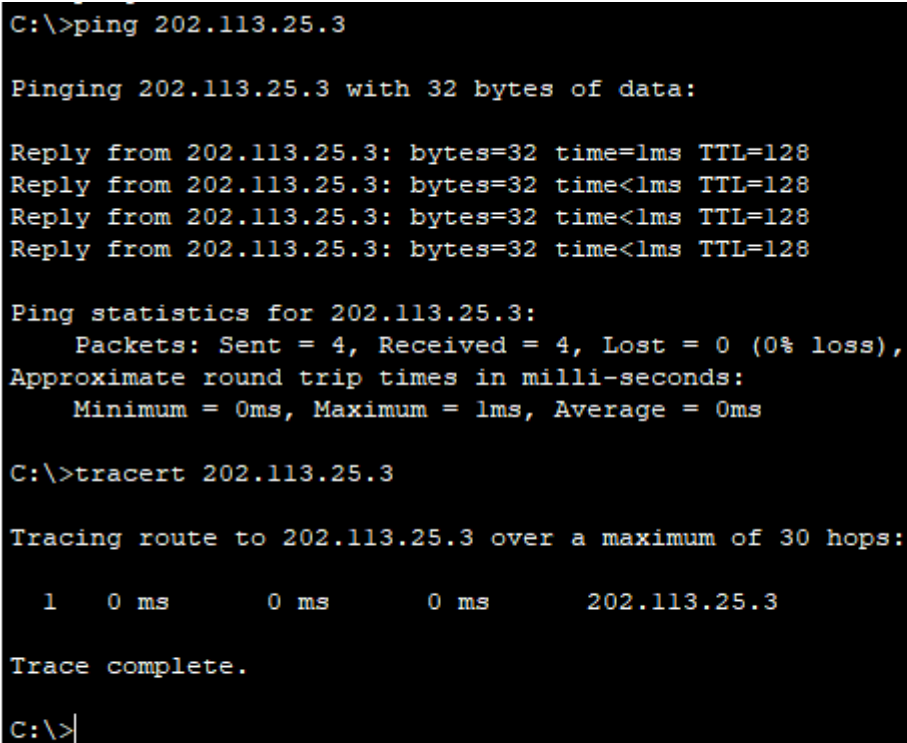
为了实现上述功能，可以在Router0的fa0/1接口上绑定一个标准ACL，对进入fa0/1接口的数据报进行检查和过滤命令如下所示：

```
Router#config terminal
Router(config)#access-list 6 permit 202.113.26.0 0.0.0.255
Router(config)#access-list 6 deny any
Router(config)#interface fa0/1
Router(config-if)#ip access-group 6 in
Router(config-if)#exit
```

1. 第二条命令允许右上角网络中的主机发送的数据报通过
2. 第三条命令拒绝所有其他网络的数据报送来的数据报
3. 第五条指令将6号ACL绑定在fa0/1的入站上

### (3)标准ACL验证

用右上角网络中的主机去ping左部网络中的主机，发现此时目的地依然可达，如下图所示：



```
C:\>ping 202.113.25.3

Pinging 202.113.25.3 with 32 bytes of data:

Reply from 202.113.25.3: bytes=32 time=1ms TTL=128
Reply from 202.113.25.3: bytes=32 time<1ms TTL=128
Reply from 202.113.25.3: bytes=32 time<1ms TTL=128
Reply from 202.113.25.3: bytes=32 time<1ms TTL=128

Ping statistics for 202.113.25.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>tracert 202.113.25.3

Tracing route to 202.113.25.3 over a maximum of 30 hops:

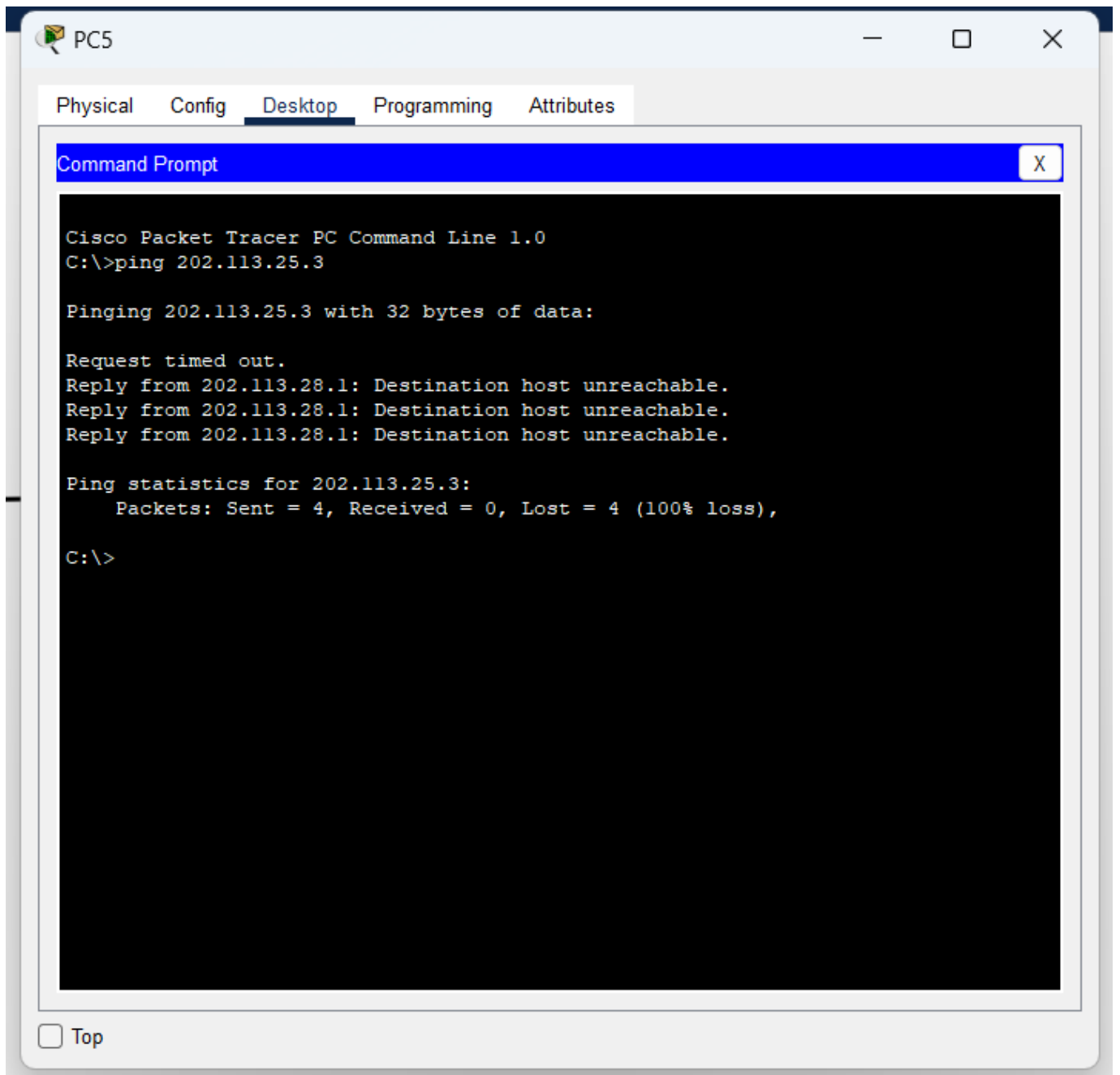
  1  0 ms      0 ms      0 ms      202.113.25.3

Trace complete.

C:\>|
```

用右下角的主机去ping左部网络中的主机，发现此时目的地不可达，如下图所示：





接下来进行扩展ACL的实验

## 2、扩展ACL

### (1)网络拓扑和基本配置

与标准访问控制列表类似，将左部网络中的一台主机换成服务器，为外部的主机提供Web服务，路由器的配置与标准ACL中的配置相同，在这里就不在进行赘述，按照拓扑图配置仿真环境下的网络，在配置防火墙之前，保证所连接的设备能够ping通

### (2)建立扩展访问列表

本实验的目标是通过添加扩展ACL使得除PC3外，允许其他主机浏览左部网络中服务器的Web界面

为实现此功能，需要在Router0上的fa0/1接口上绑定一个扩展ACL，对进入fa0/1接口的数据报进行检查和过滤，命令如下：

```
Router#config terminal
Router(config)#access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 eq www
Router(config)#access-list 106 permit ip any any
Router(config)#interface fa0/1
Router(config-if)#ip access-group 106 in
Router(config-if)#exit
```

1. 第二条命令含义为抛弃源IP地址为202.113.26.2、目的地址为202.113.25.3、目的端口号为80的TCP的数据报
2. 第三条指令允许其他所有的数据报通过
3. 第五条指令将106号ACL绑定在fa0/1的入站上

配置之后的路由器如下图所示：

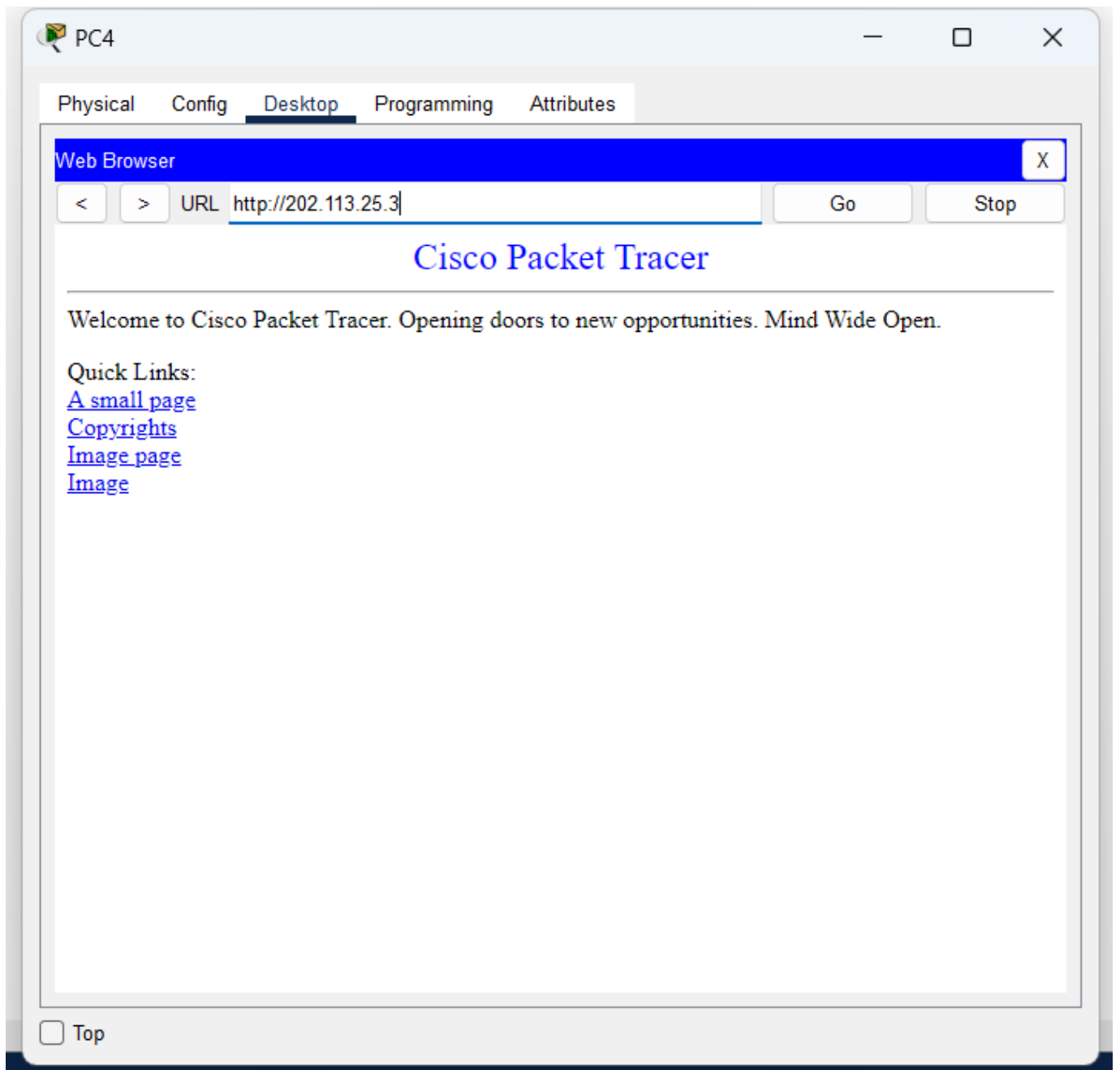
Device Name: Router0					
Custom Device Model: 2811 IOS15					
Hostname: Router					
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	202.113.25.1/24	<not set>	0030.F293.D501
FastEthernet0/1	Up	--	202.113.28.1/24	<not set>	0030.F293.D502
Vlan1	Down	1	<not set>	<not set>	0040.0BEB.75D9
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0					

Device Name: Router1					
Custom Device Model: 2811 IOS15					
Hostname: Router					
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	202.113.28.2/24	<not set>	0040.0B9E.5401
FastEthernet0/1	Up	--	202.113.26.1/24	<not set>	0040.0B9E.5402
Vlan1	Down	1	<not set>	<not set>	0001.63BE.9650
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1					

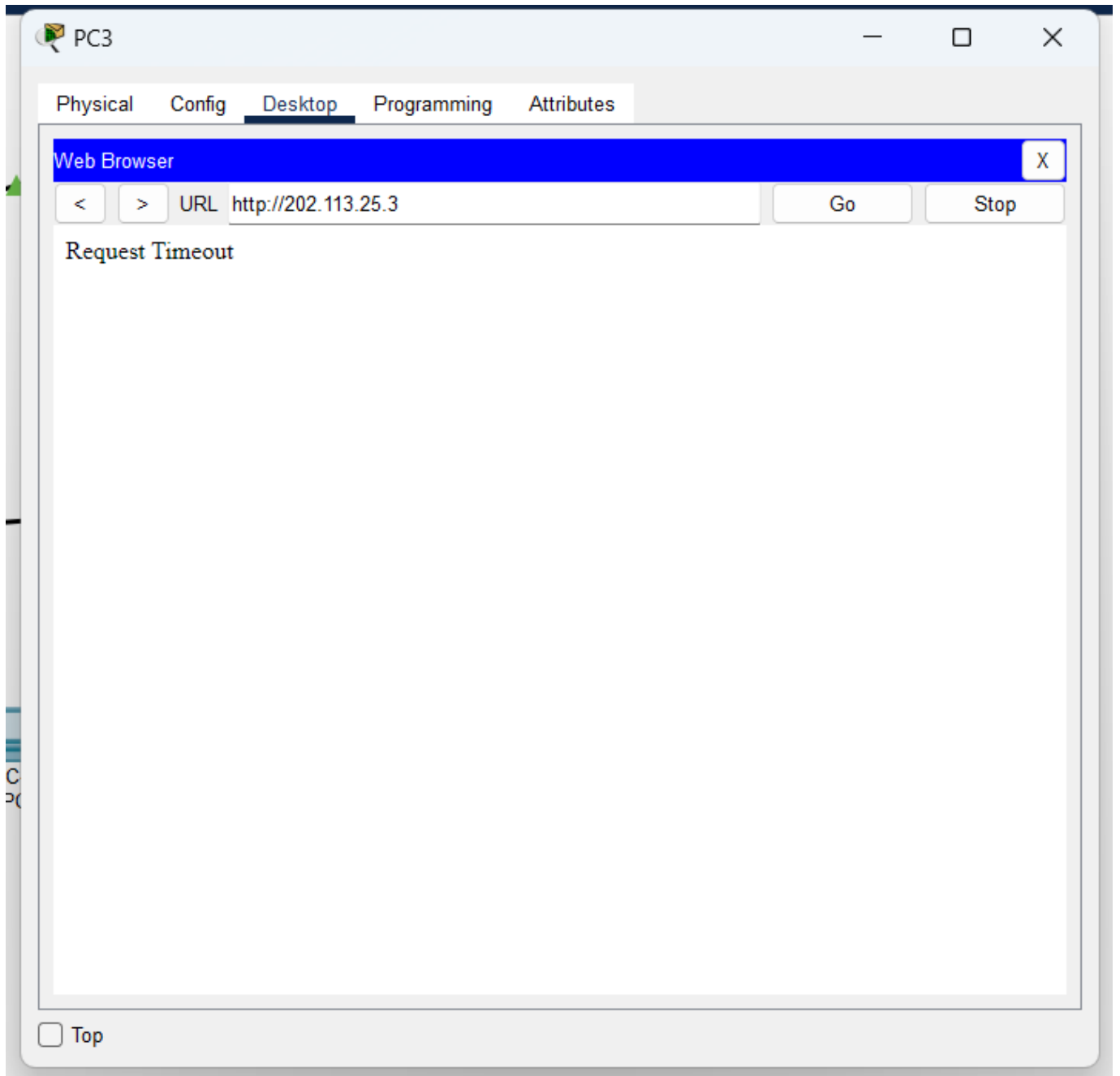
Device Name: Router2					
Custom Device Model: 2811 IOS15					
Hostname: Router					
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	202.113.28.3/24	<not set>	0001.9712.0B01
FastEthernet0/1	Up	--	202.113.27.1/24	<not set>	0001.9712.0B02
Vlan1	Down	1	<not set>	<not set>	000C.CFD6.188D
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router2					

### (3)扩展ACL验证

在配置扩展ACL之后用PC4去访问上面网络中的Web网络，发现可以访问，如下图所示：



在配置扩展ACL之后用PC3去访问上面网络中的Web网络，发现不可以访问，如下图所示：

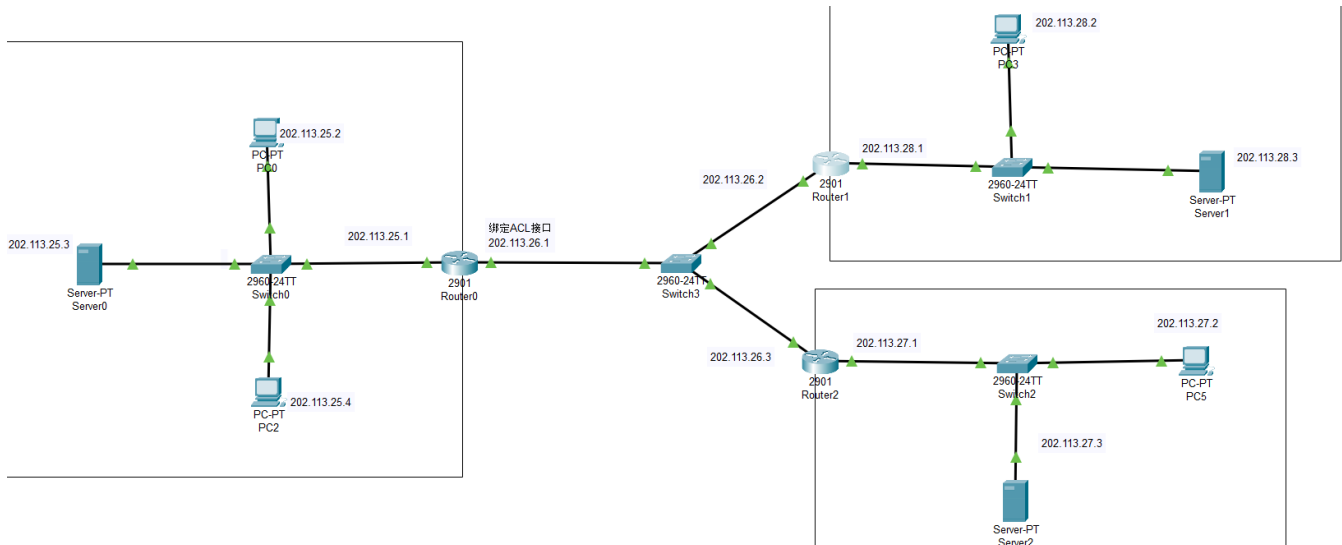


## 扩展二：

### 建立扩展访问列表

网络B主机可访问网络A、网络B、网络C的web服务器，网络A和网络C的主机不可访问网络B的web服务器

构造的网络图如下：左侧为内网，右侧两个为外网



为实现此功能，需要在Router0上的fa0/1接口上绑定一个扩展ACL，对进入fa0/1接口的数据报进行检查和过滤，命令如下：

```
Router#config terminal
Router(config)#access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 ea www
Router(config)#access-list 106 permit ip any any
Router(config)#interface fa0/1
Router(config-if)#ip access-group 106 in
Router(config-if)#exit
```

配置完成的三个router结果如下：

<b>Device Name: Router0</b> <b>Device Model: 2901</b> <b>Hostname: Router</b>						
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address	
GigabitEthernet0/0	Up	--	202.113.25.1/24	<not set>	00D0.BAB3.5C01	
GigabitEthernet0/1	Up	--	202.113.26.1/24	<not set>	00D0.BAB3.5C02	
Vlan1	Down	1	<not set>	<not set>	0060.5C94.EE29	

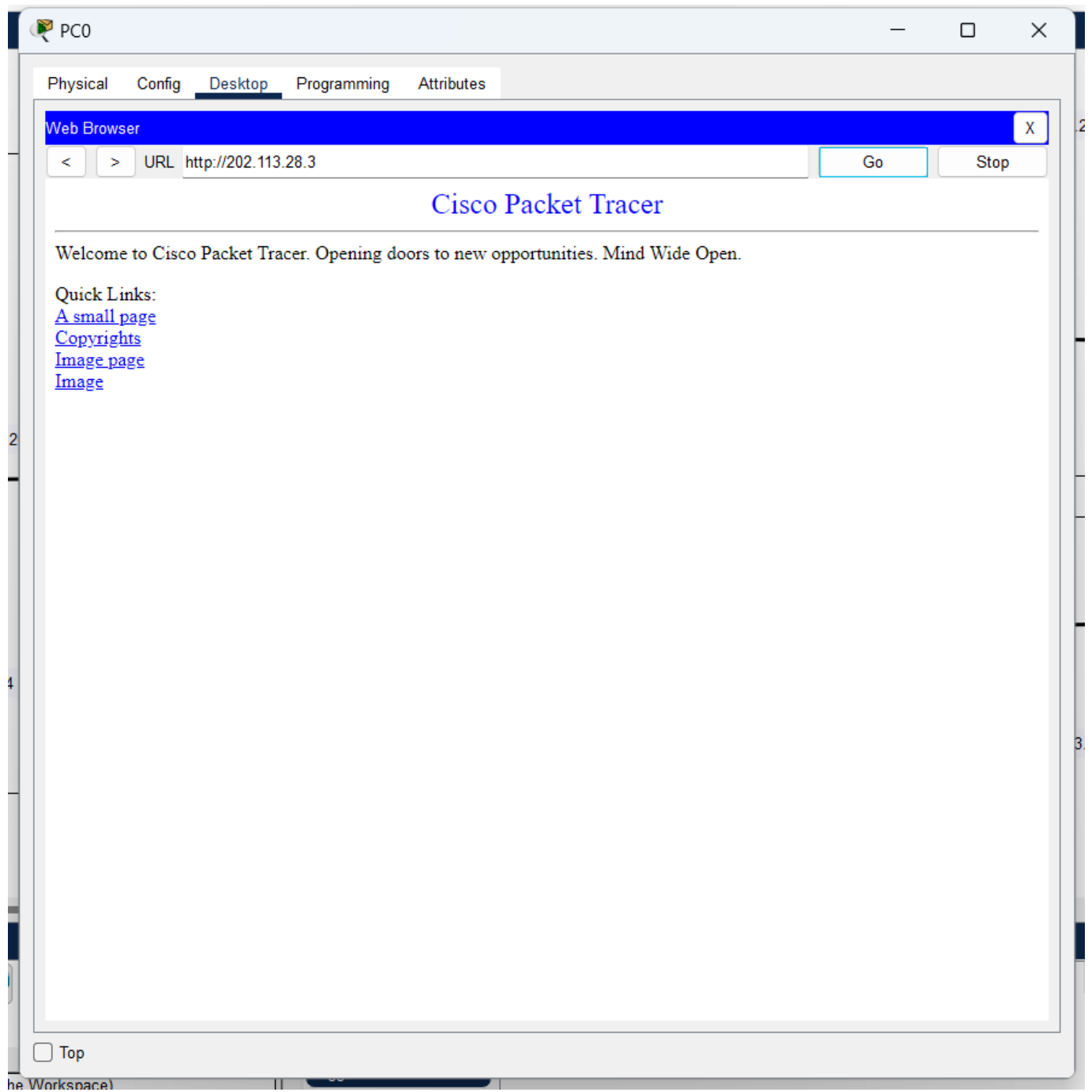
  

<b>Device Name: Router1</b> <b>Device Model: 2901</b> <b>Hostname: Router</b>						
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address	
GigabitEthernet0/0	Up	--	202.113.26.2/24	<not set>	000C.CFA8.BD01	
GigabitEthernet0/1	Up	--	202.113.28.1/24	<not set>	000C.CFA8.BD02	
Vlan1	Down	1	<not set>	<not set>	0090.2179.BB67	

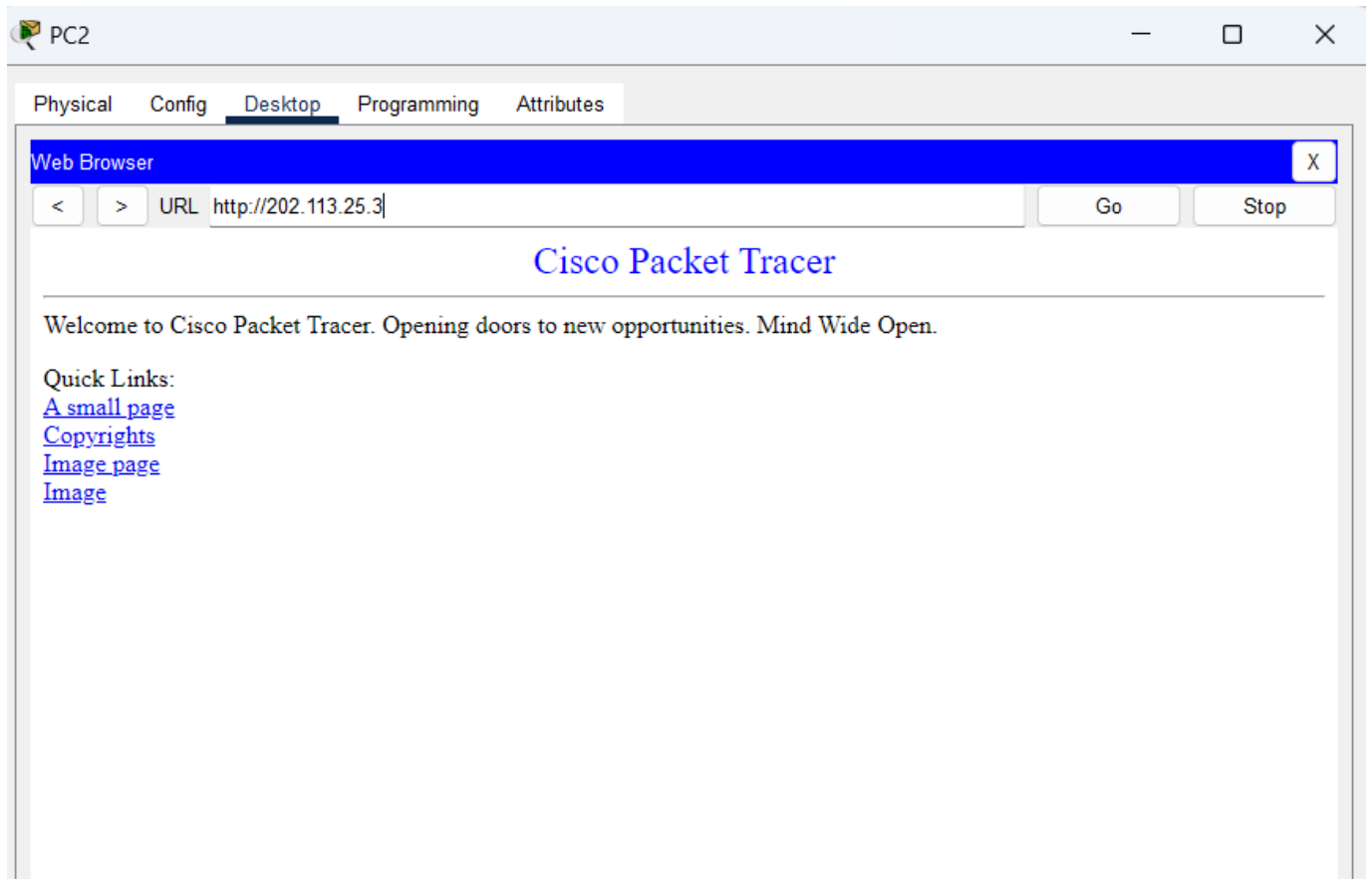
  

<b>Device Name: Router2</b> <b>Device Model: 2901</b> <b>Hostname: Router</b>						
Port	Link	VLAN	IP Address	IPv6 Address	MAC Address	
GigabitEthernet0/0	Up	--	202.113.26.3/24	<not set>	0001.962B.EC01	
GigabitEthernet0/1	Up	--	202.113.27.1/24	<not set>	0001.962B.EC02	
Vlan1	Down	1	<not set>	<not set>	0001.9716.9D54	

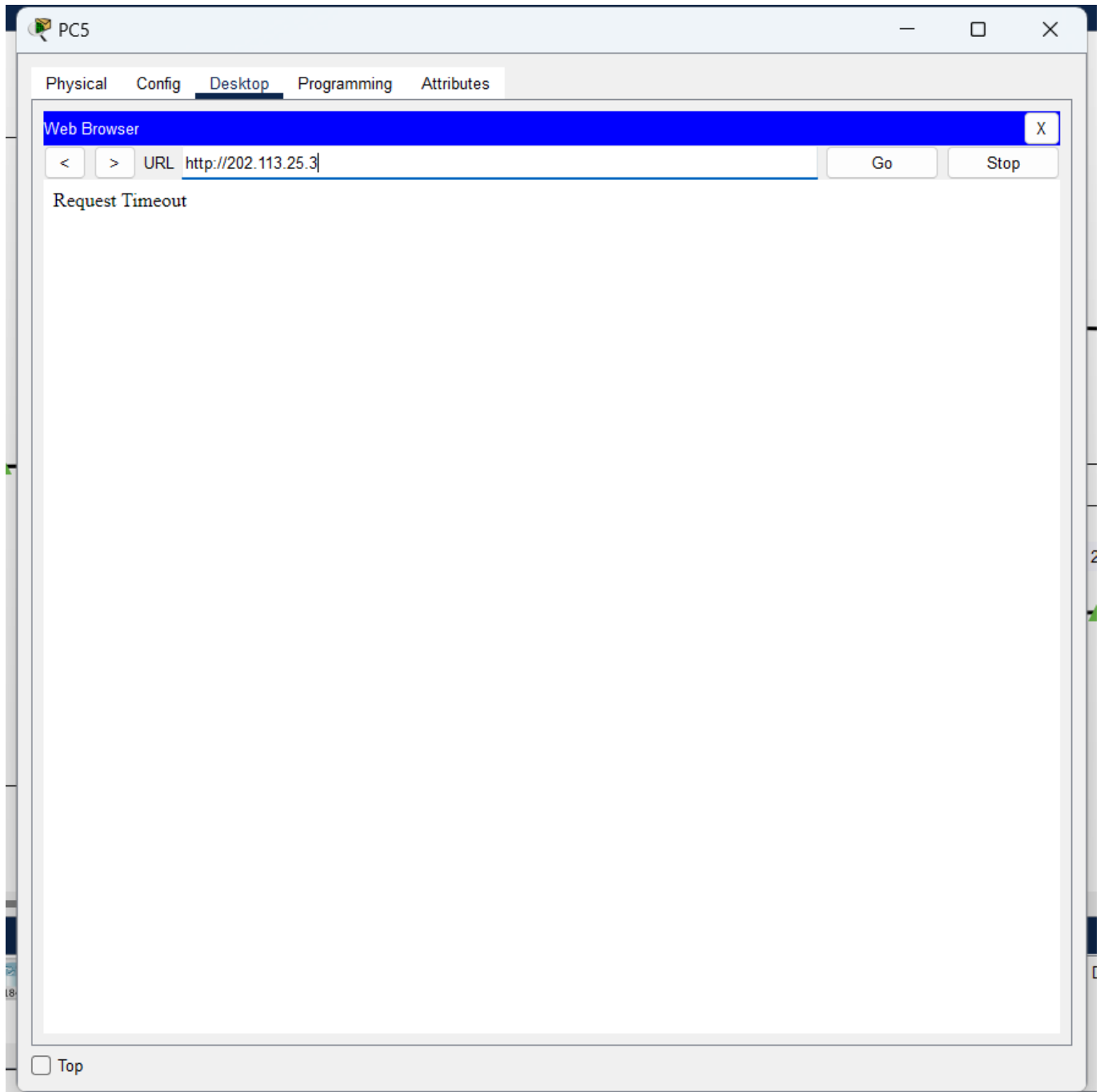
如图，内网pin外网：成功



内网pin内网：成功



外网pin内网：失败



本次实验也到此成功！

## 四、总结

本次实验是网络技术与应用的第七次实验，本次实验了解了包过滤防火墙的基本配置方法、配置命令和配置过程，见识到了防火墙的应用条件下计算机网络将会存在的诸多变化。看到了防火墙的模拟应用的效果，对自己电脑上的防火墙能够起到的实际作用也有了更加充分的认知。对标准控制列表和扩展控制列表更加的熟悉，也对网络方面的知识更加的了解，在网络方面的认知也有了新的领悟和新的思考。