

# 网络技术与应用课程实验报告

## 实验7：防火墙的配置

姓名：孟启轩 学号：2212452 专业：计算机科学与技术

### 一、实验内容说明

防火墙实验在虚拟仿真环境下完成，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) 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

#### 防火墙 (Firewall)

防火墙是一种位于计算机网络不同信任级别之间的系统，它可以是硬件设备、软件程序或两者的结合。防火墙根据预设的安全规则监控并过滤进出网络的数据流，以阻止潜在的威胁，保护内部网络不受外部攻击。防火墙可以基于多种因素进行流量过滤，包括但不限于源地址、目的地址、端口号和服务类型等。防火墙通常被部署在网络边界处，例如企业内部网络与互联网之间。

#### 访问控制列表 (ACL, Access Control List)

ACL 是一种用于定义哪些数据包允许通过网络设备（如路由器或交换机）的规则集。ACL 可以配置在接口上，以决定是否允许或拒绝特定类型的流量。ACL 通常基于以下信息来匹配数据包：

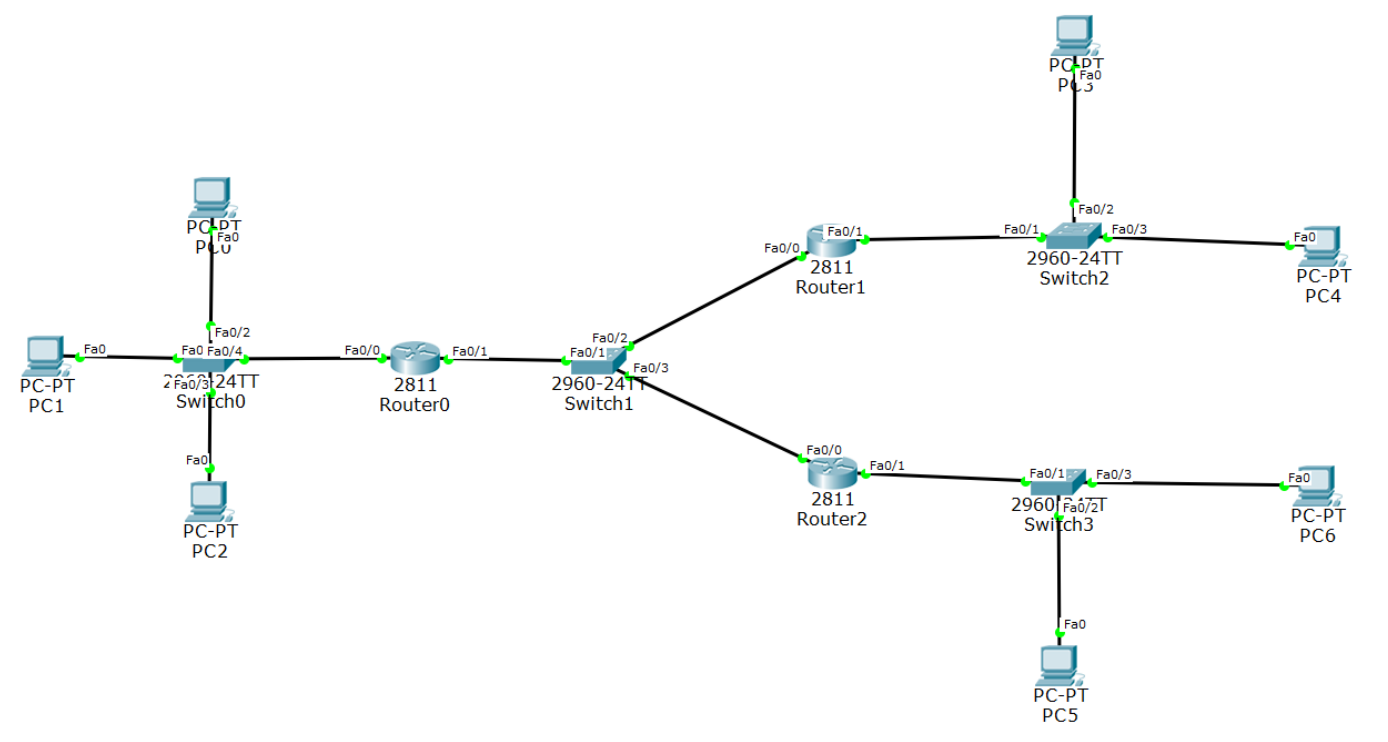
- 源IP地址
- 目的IP地址
- 协议类型（TCP、UDP、ICMP等）
- 源端口或目的端口

ACL 可以分为标准 ACL 和扩展 ACL。标准 ACL 主要基于 IP 地址进行过滤，而扩展 ACL 还可以根据协议类型和端口号等更详细的信息进行过滤。

#### 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

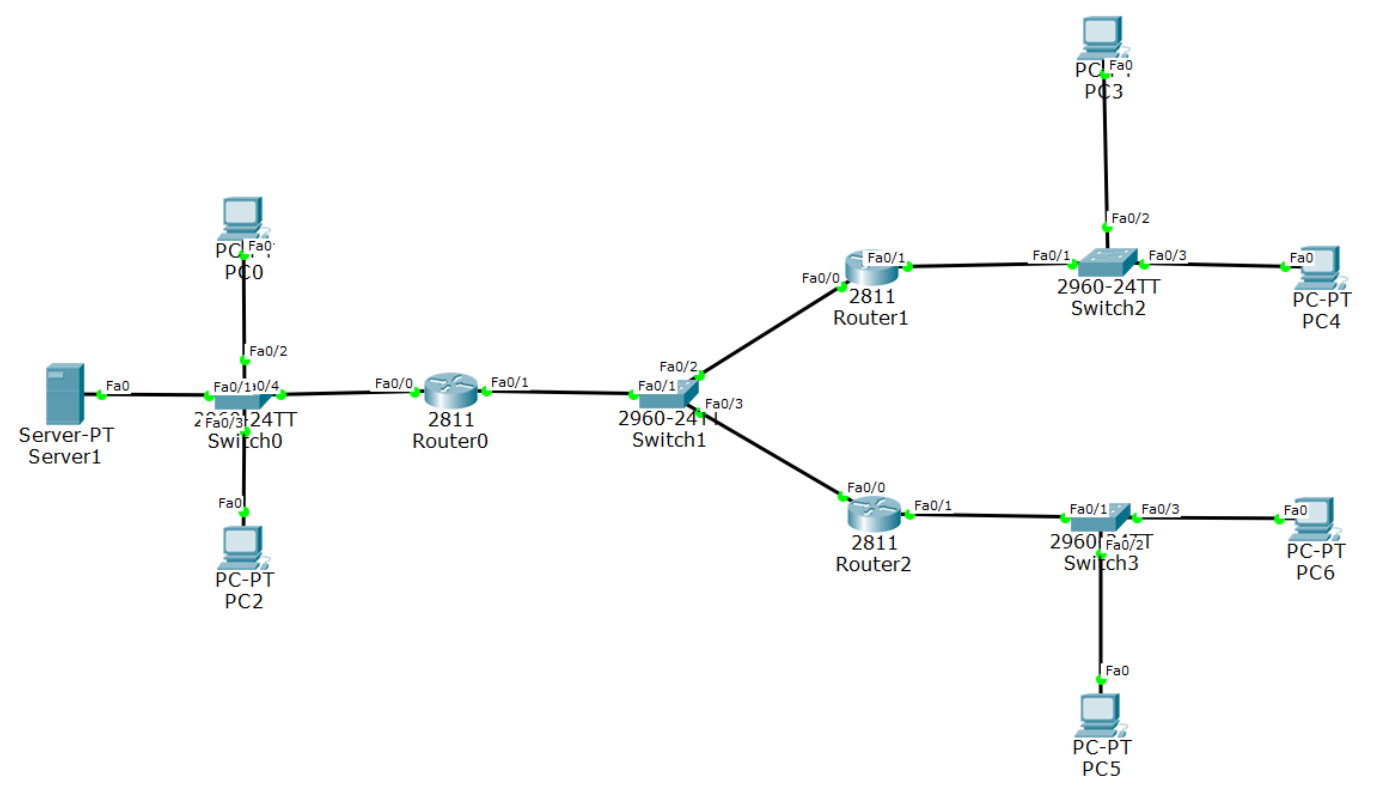
标准ACL实验的IP地址分配如下所示：

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

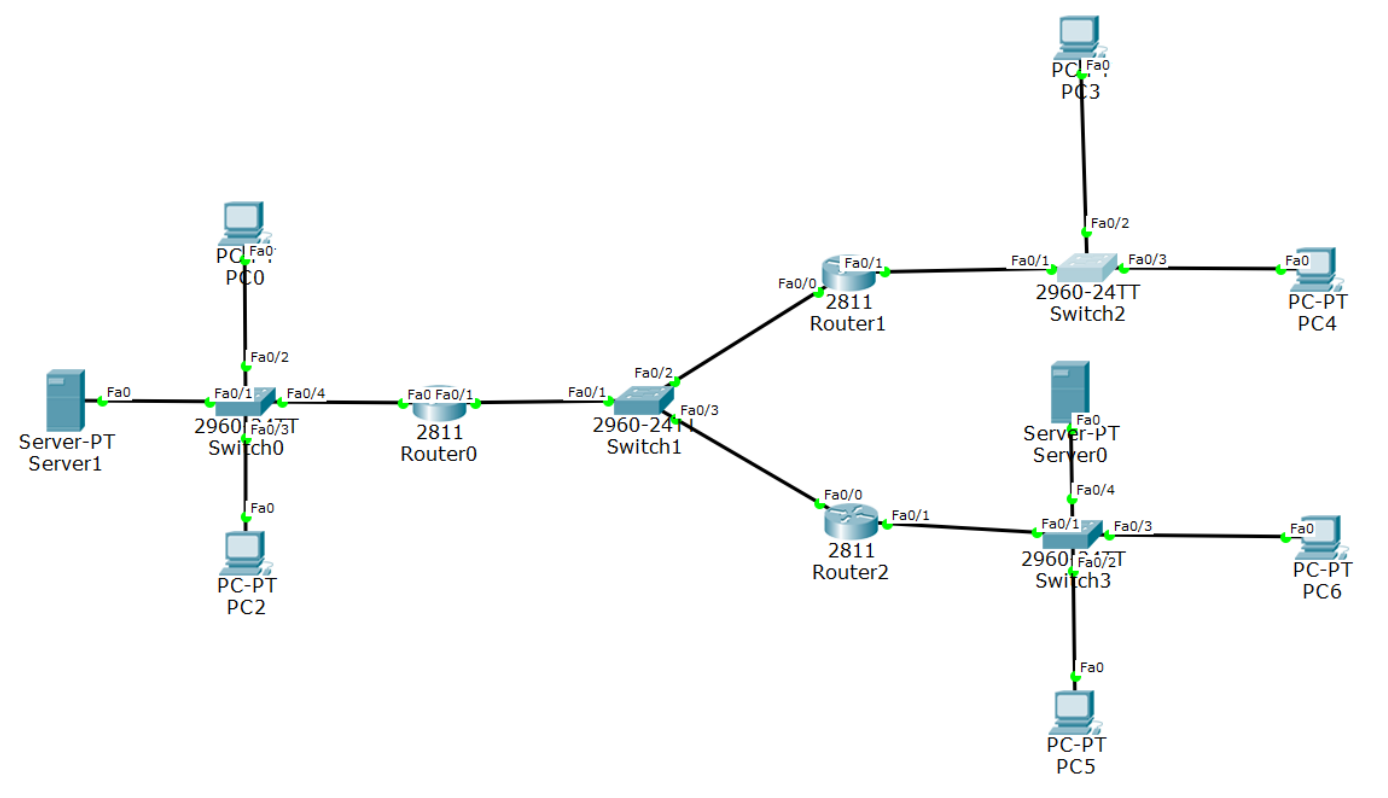
扩展ACL实验的IP地址分配如下所示：

Machine	IPv4 Address	Subnet Mask	网关
PC0	202.113.25.2	255.255.255.0	202.113.25.1
Server0	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	

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。

(1)拓扑图

实验的拓扑图如下所示：



(2)IP地址分配

实验的IP地址分配如下所示：

设备	IP地址	子网掩码	默认网关
PC0	202.113.25.2	255.255.255.0	202.113.25.1
Server0	202.113.25.3	255.255.255.0	202.113.25.1
Server1	202.113.27.4	255.255.255.0	202.113.27.1
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	

设备	IP地址	子网掩码	默认网关
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	

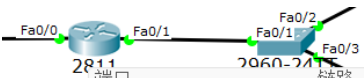
### 三、实验过程

本次实验将分为三个部分来进行，分别是标准控制列表、扩展控制列表和反向扩展列表，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

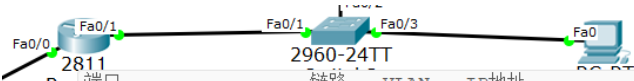
首先对三台主机以及服务器按照准备过程中的地址进行ip地址配置，由于ip地址的配置并不是本次实验的重点，这里不过多赘述，只展示出三个路由器配置完成后的地址分配：



端口	链路	VLAN	IP地址	IPv6地址	MAC地址
FastEthernet0/0	启用	--	202.113.25.1/24	<not set>	0000.0C87.AC01
FastEthernet0/1	启用	--	202.113.28.1/24	<not set>	0000.0C87.AC02
Vlan1	禁用	1	<not set>	<not set>	00E0.B03A.E255

主机名:Router

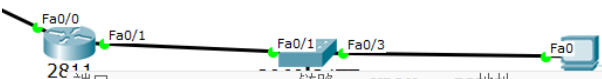
物理位置:InterCity, Home City, Corporate Office, Main Wiring Closet



端口	链路	VLAN	IP地址	IPv6地址	MAC地址
FastEthernet0/0	启用	--	202.113.28.2/24	<not set>	0030.F260.4501
FastEthernet0/1	启用	--	202.113.26.1/24	<not set>	0030.F260.4502
Vlan1	禁用	1	<not set>	<not set>	0090.0CBD.68DA

主机名:Router

物理位置:InterCity, Home City, Corporate Office, Main Wiring Closet

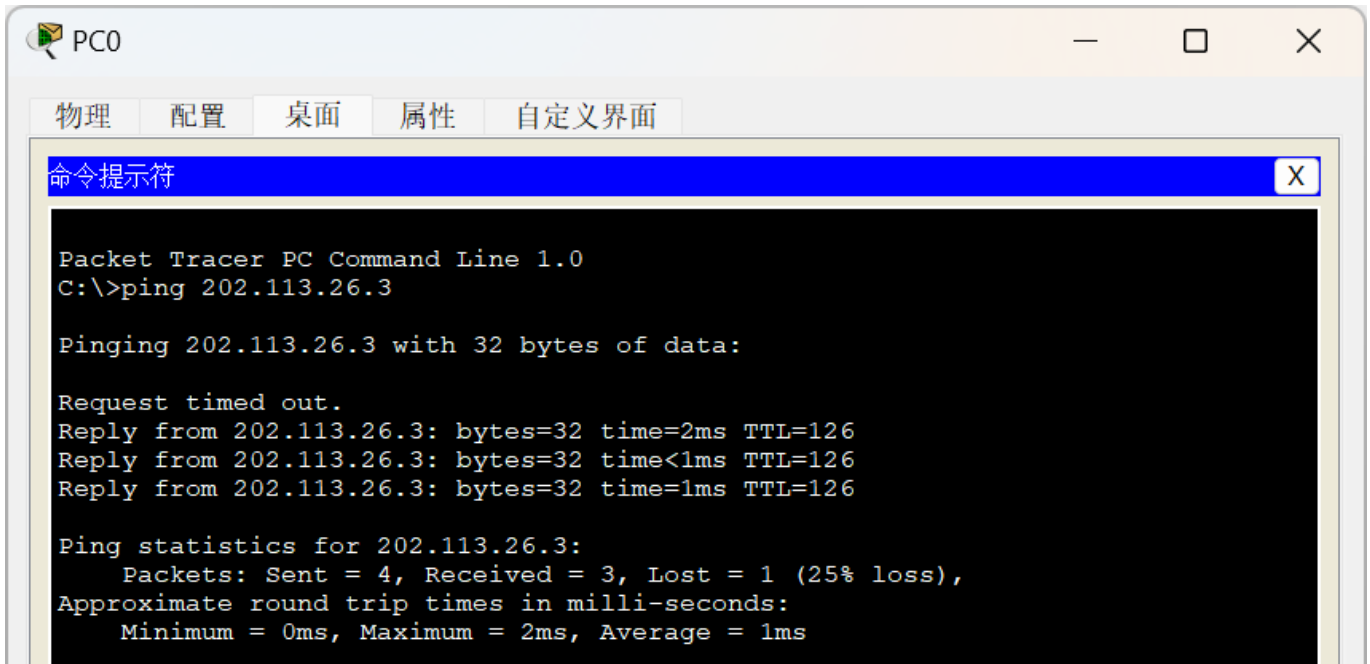


端口	链路	VLAN	IP地址	IPv6地址	MAC地址
FastEthernet0/0	启用	--	202.113.28.3/24	<not set>	0001.6398.1401
FastEthernet0/1	启用	--	202.113.27.1/24	<not set>	0001.6398.1402
Vlan1	禁用	1	<not set>	<not set>	0001.9658.0C86

主机名:Router

物理位置:InterCity, Home City, Corporate Office, Main Wiring Closet

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(PC0和PC4可以ping通)：



## (2)建立标准访问列表

本次实验的实现目标是左边的网络允许右上角的网络中的主机访问，但不允许其他网络中的主机访问（在本次实验中为右下角的网络）

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

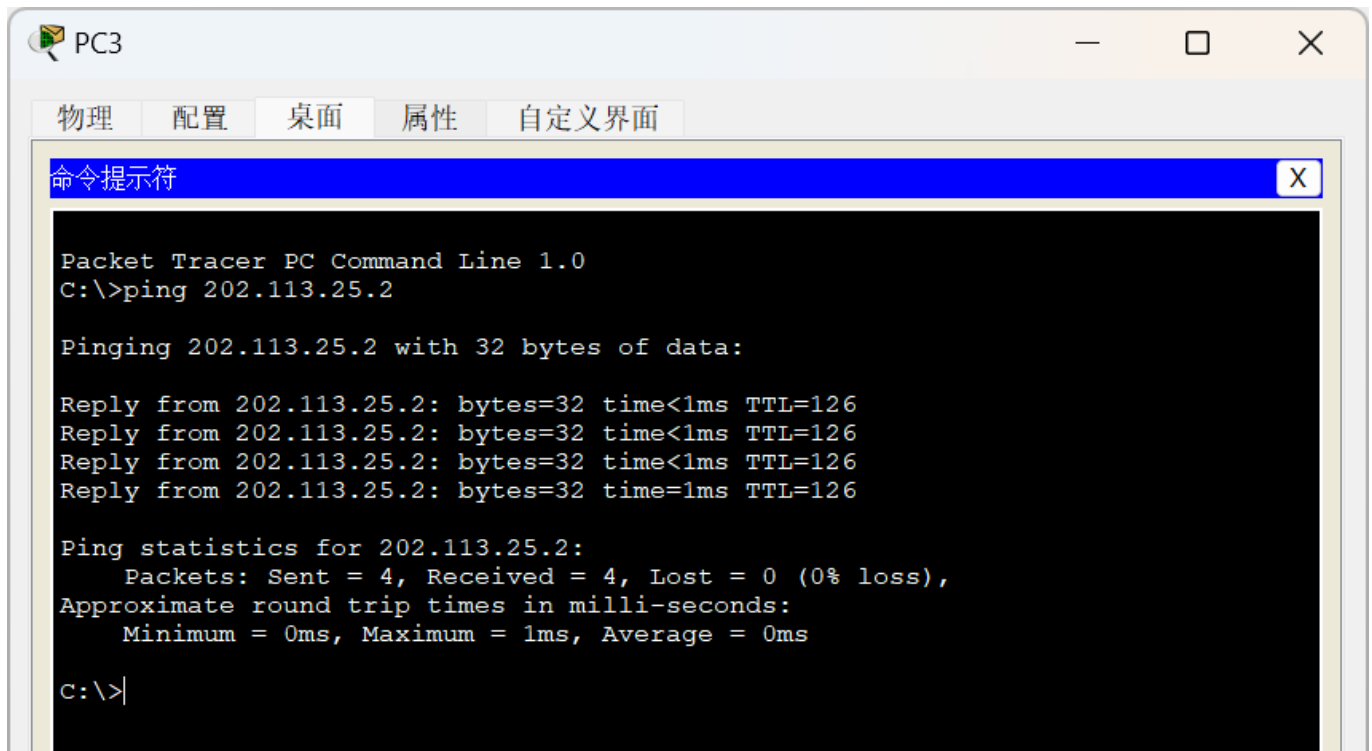
配置命令如下两图所示：

```
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#access-list 6 permit 202.113.26.0 0.0.0.255
Router(config)#access-list 6 deny any
Router(config)#
Router(config)#
```

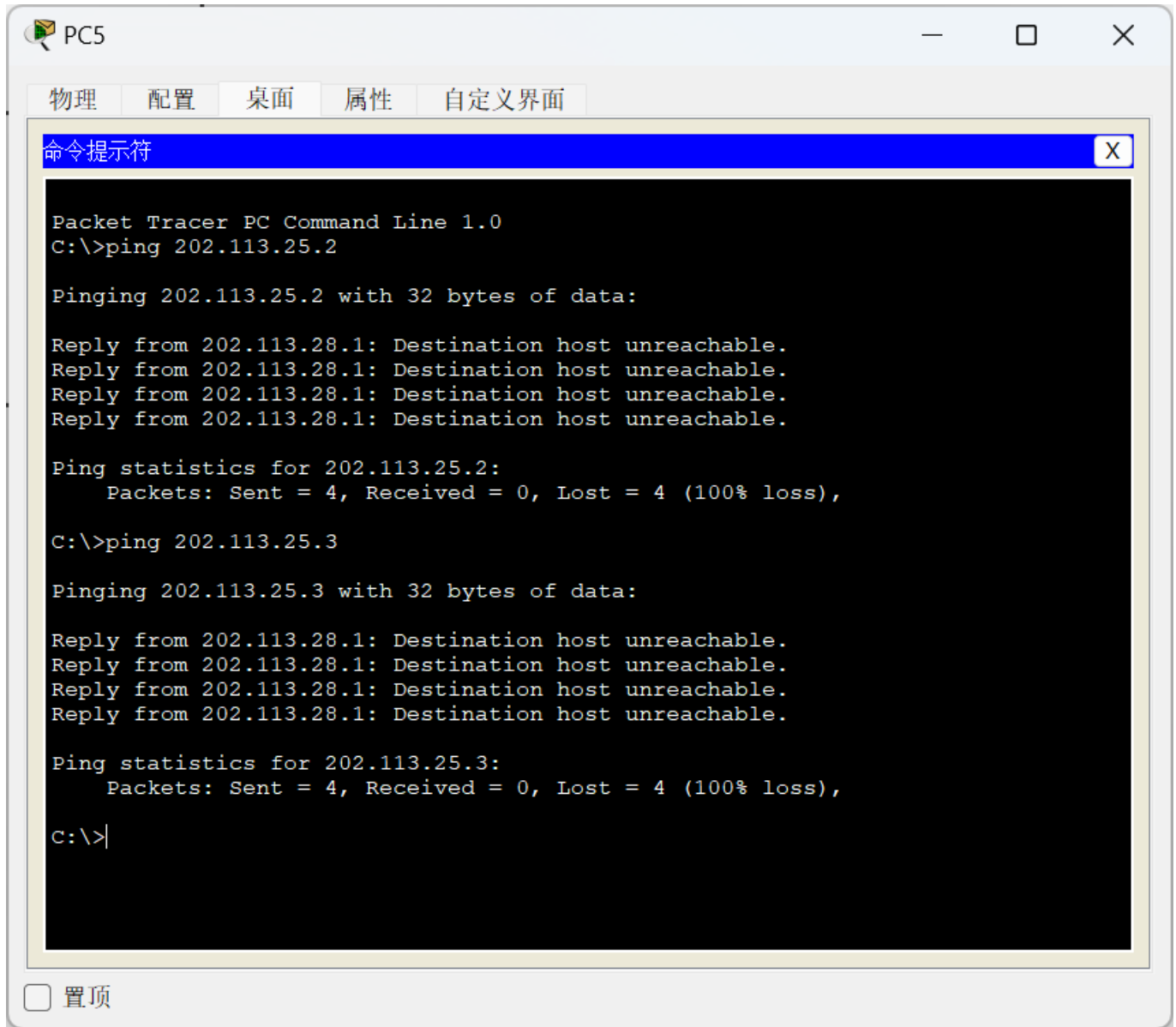
```
Router(config)#  
Router(config)#interface fa0/1  
Router(config-if)#ip access-group 6 in  
Router(config-if)#  
Router(config-if)#
```

### (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(PC3pingPC0), 发现此时目的地依然可达, 如下图所示:



用右下角的主机去ping左部网络中的主机(PC5pingPC0和PC1), 发现此时目的地不可达, 如下图所示:



## 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

配置命令如下两图所示：

```
Router(config)#
Router(config)#
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)#
```

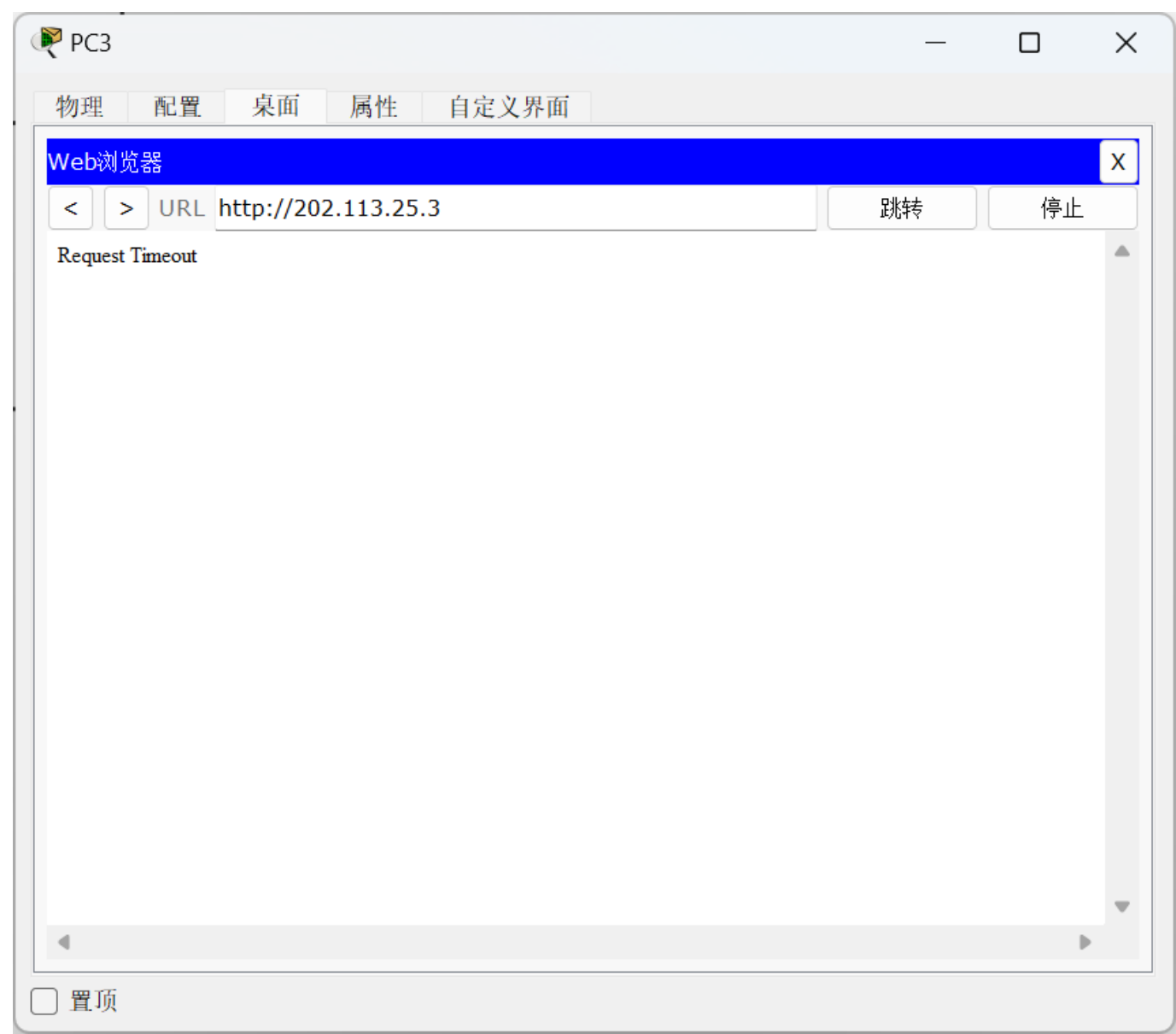
```
Router(config)#
Router(config)#
Router(config)#
Router(config)#interface fa0/1
Router(config-if)#
Router(config-if)#ip access-group 106 in
Router(config-if)#
Router(config-if)#
```

### (3)扩展ACL验证

在配置扩展ACL之前用PC3去访问左部网络中的Web网络，发现可以访问，如下图所示：



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



3.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。

(1)网络拓扑和基本配置

与扩展ACL的设置类似，在右下角的网络中新增了一台服务器，负责为左侧网络的主机提供Web服务。IP配置仍然与扩展ACL中的一致，详细内容在此不再赘述。为了满足实验的需求，我选择使用反向访问控制列表（即反向ACL）的方法进行配置。

(2)建立反向ACL

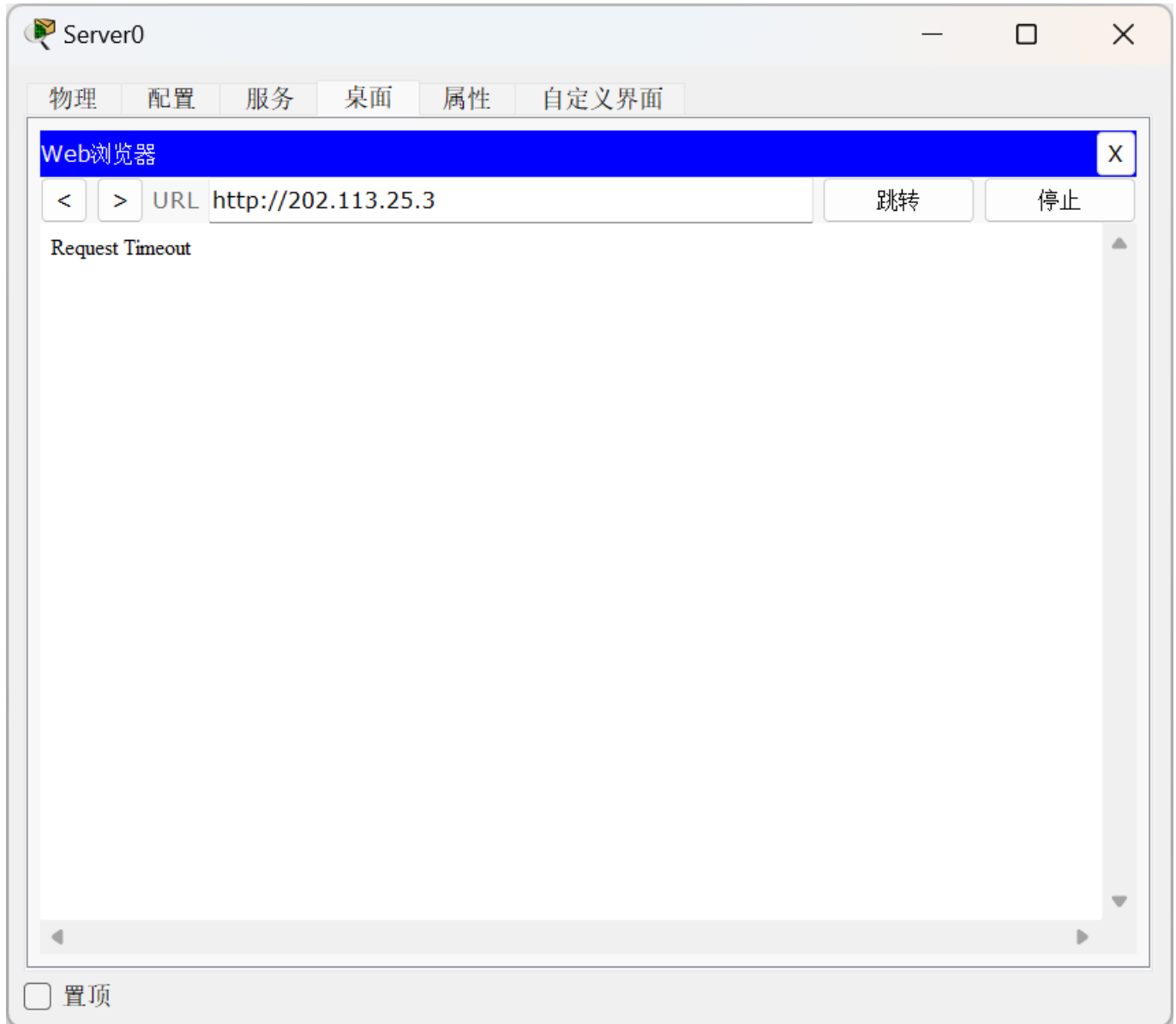
命令如下所示：

```
Router#config terminal
Router(config)#access-list 101 permit tcp any 202.113.25.0 0.0.0.255 established
Router(config)#interface fa0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
```

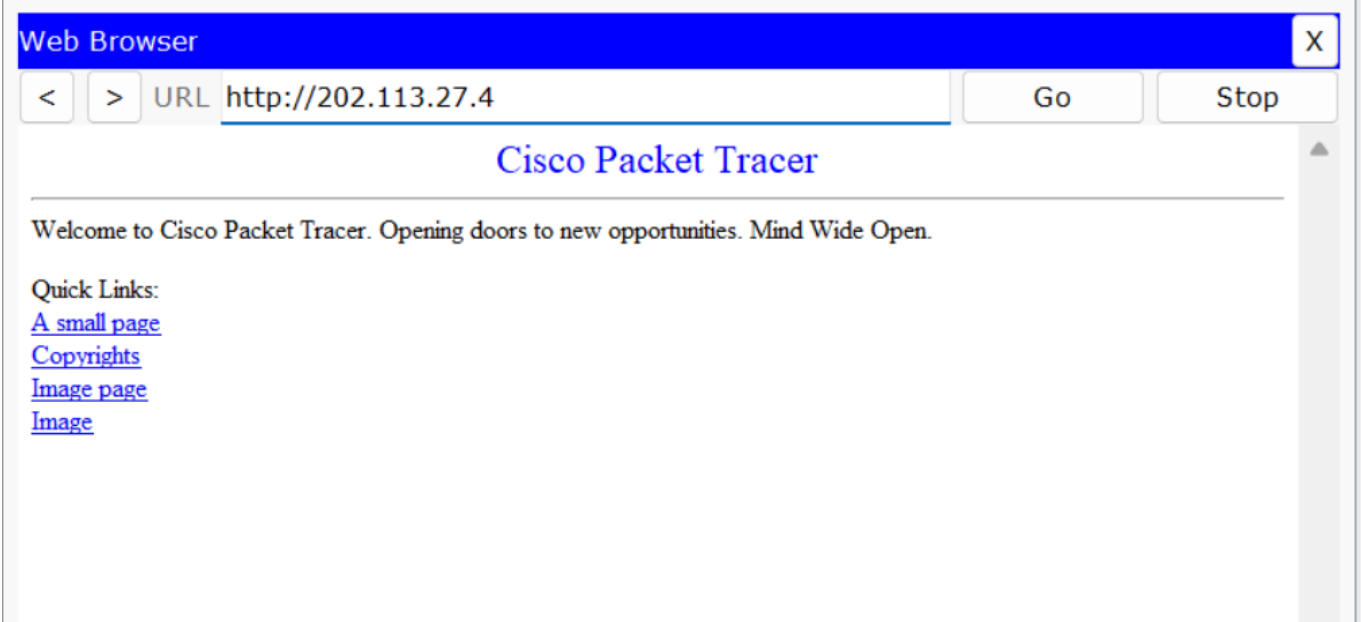
1. 第一条命令定义了ACL101，允许所有其他网段的计算机访问202.113.25.0网段中的设备，前提是TCP连接已经建立。如果TCP连接没有建立，则不允许其他网段访问202.113.25.0网段的设备。
2. 第三条命令将ACL101应用到相应端口fa0/1的入站上

#### (4) 验证反向ACL

- 配置完成后，外网（即右侧网络）中的服务器 Server0无法访问内网（即左侧网络）中的服务器 Server1。



- 但是，内网中的服务器Server1能够正常访问外网的服务器Server0。



#### 四、总结与感悟

通过本次虚拟仿真环境下的防火墙实验，我深入理解了包过滤防火墙的配置原理和方法。在实践中掌握了使用标准ACL限制特定网络之间的访问，确保只有指定网络中的主机能够互相通信；同时运用扩展ACL精确控制流量，成功阻止了特定主机对Web服务器的非授权访问。此外，还实现了内网用户对外网的TCP连接发起权限，并保障了外网响应数据包的正常接收，同时有效阻止了外网对内网的主动TCP连接尝试，这不仅强化了内部网络安全，也体现了防火墙在边界安全策略实施中的关键作用。实验过程中，我深刻体会到ACL规则设置的严谨性和顺序的重要性，以及正确配置防火墙对于维护网络安全的不可或缺性。此实验极大地增强了我对网络安全实践技能的理解和应用能力。