# 实验7：防火墙和SSL实验


- 姓名：陈睿颖
- 学号：2013544
- 专业：计算机科学与技术


## 1. 实验内容

### 1.1 防火墙实验

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。

## 1.2 SSL实验（选做）

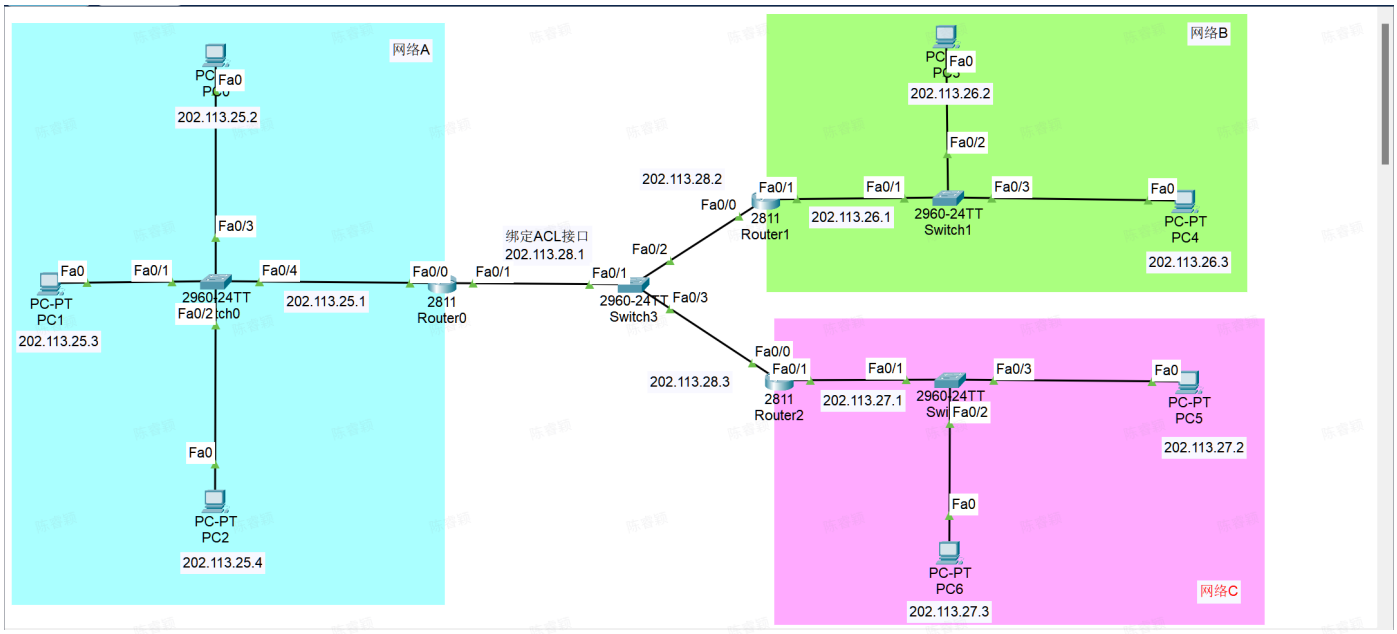
SSL实验在实体环境下完成，要求如下：

1. 完成Web服务器的证书生成、证书审批、证书安装、证书允许等整个过程。
2. 实现浏览器与Web服务器的安全通信。

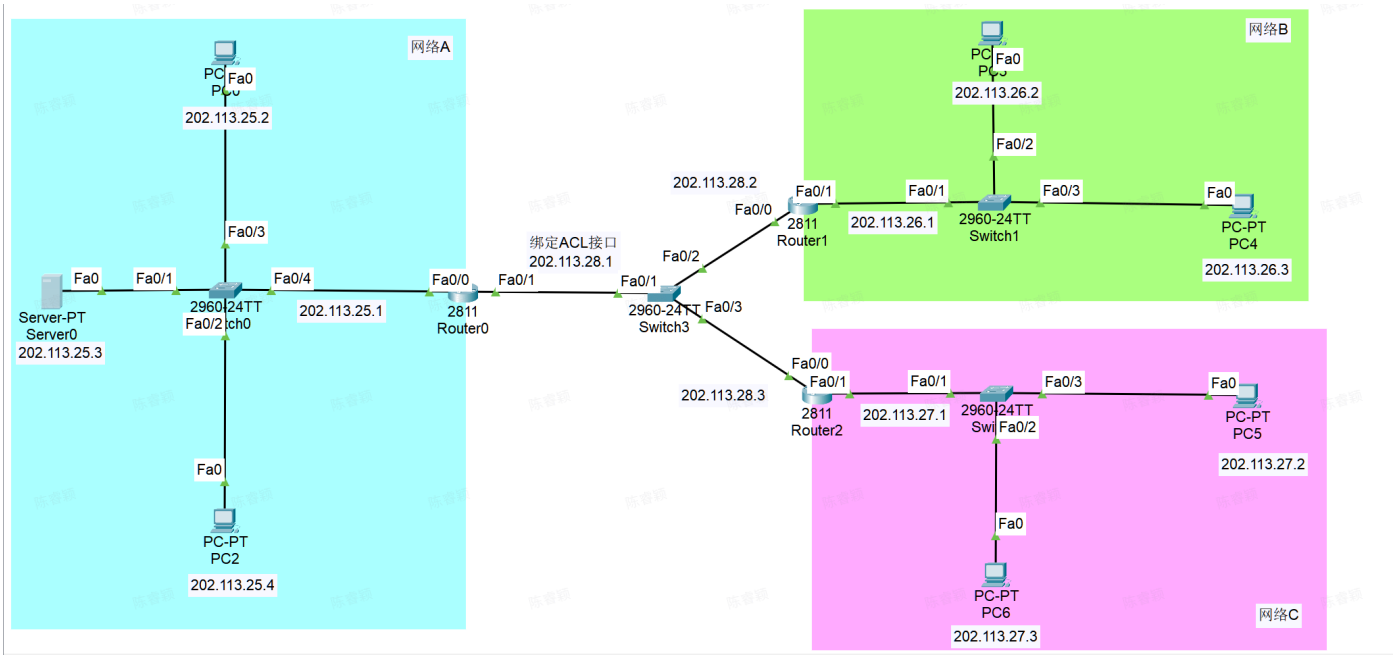
# 2. 实验准备

## 配置包过滤防火墙

- 标准ACL：
  - 利用IP数据报中的源IP地址对过往的数据包进行控制
  - 列表号范围：1~99
  - 实验拓扑图如下：




- 扩展ACL：
  - 按照协议类型、源IP地址、目的IP地址、源端口号、目的端口号对过往的数据包进行控制
  - 列表号的范围：101~199
  - 实验拓扑图如下：



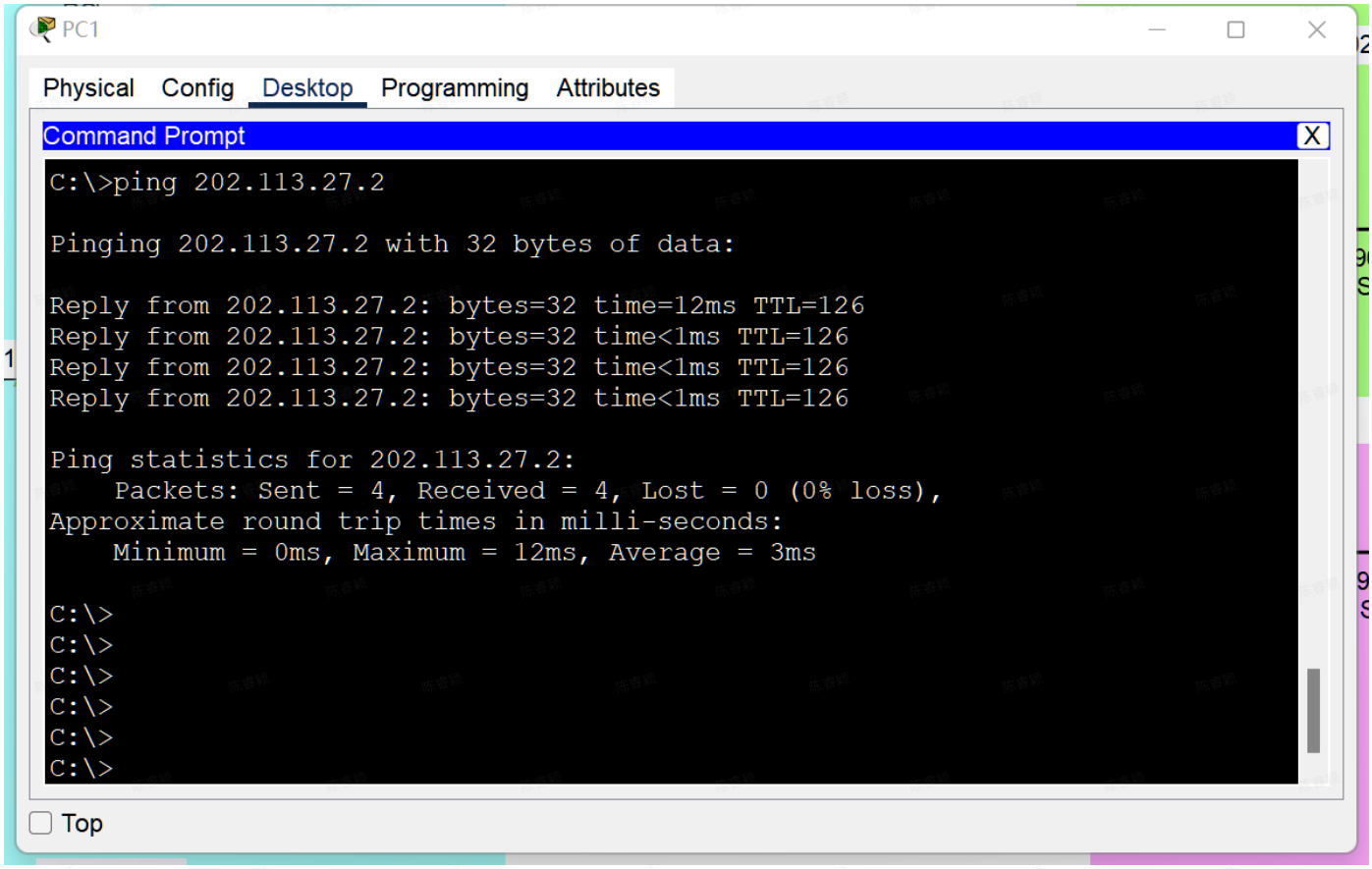

各个设备的IP地址及掩码已在拓扑图中给出，路由表的配置同样是使网络A、B、C中的主机能够互相连通。

# 3. 实验步骤

## 3.1 标准访问控制列表实验

3. 按照第2节实验准备中的拓扑图进行IP的设置和路由器路由表的配置，最后应使网络A、B、C中的主机均能通信：

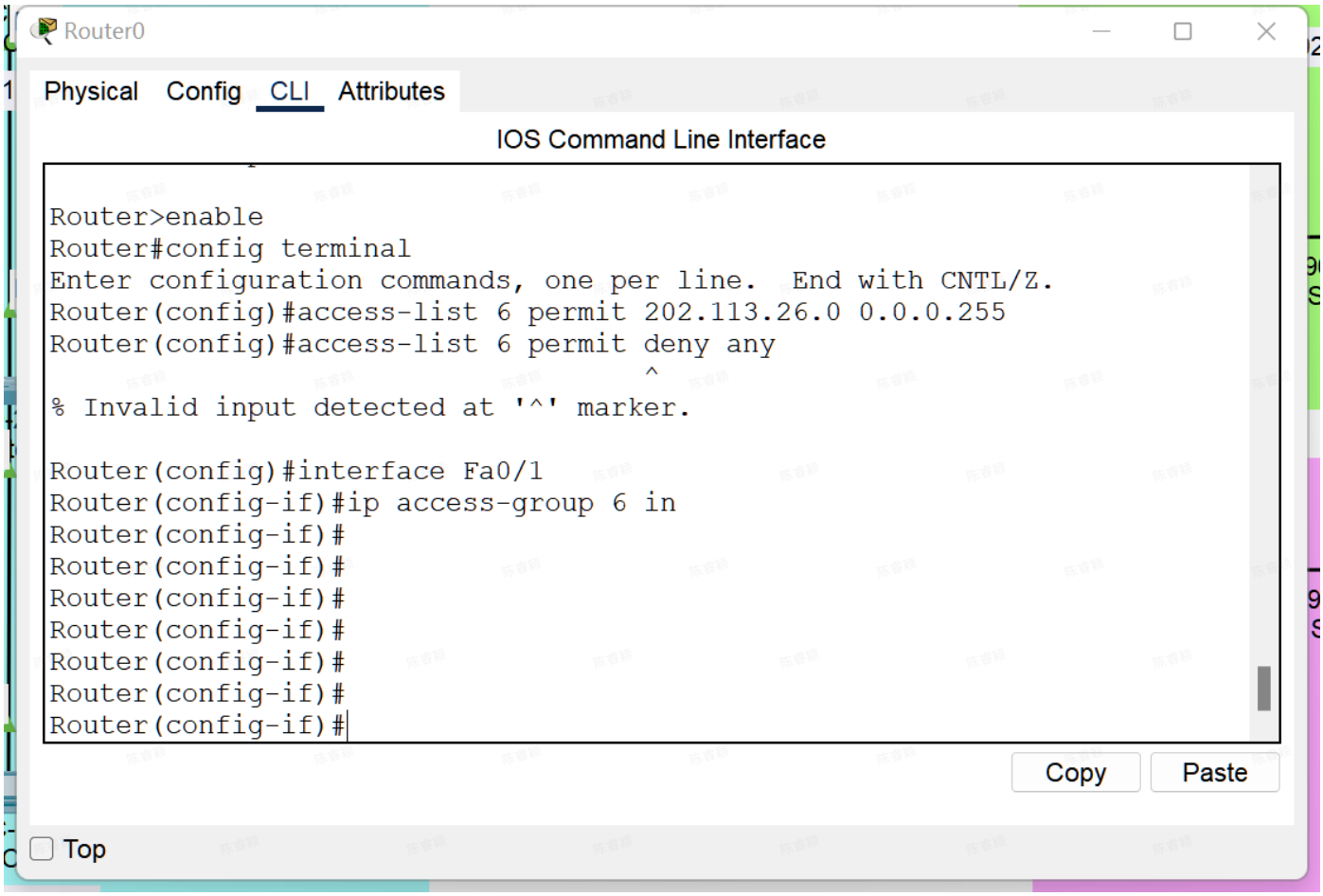
   例如使用PC1 ping PC5：




网络是连通的！

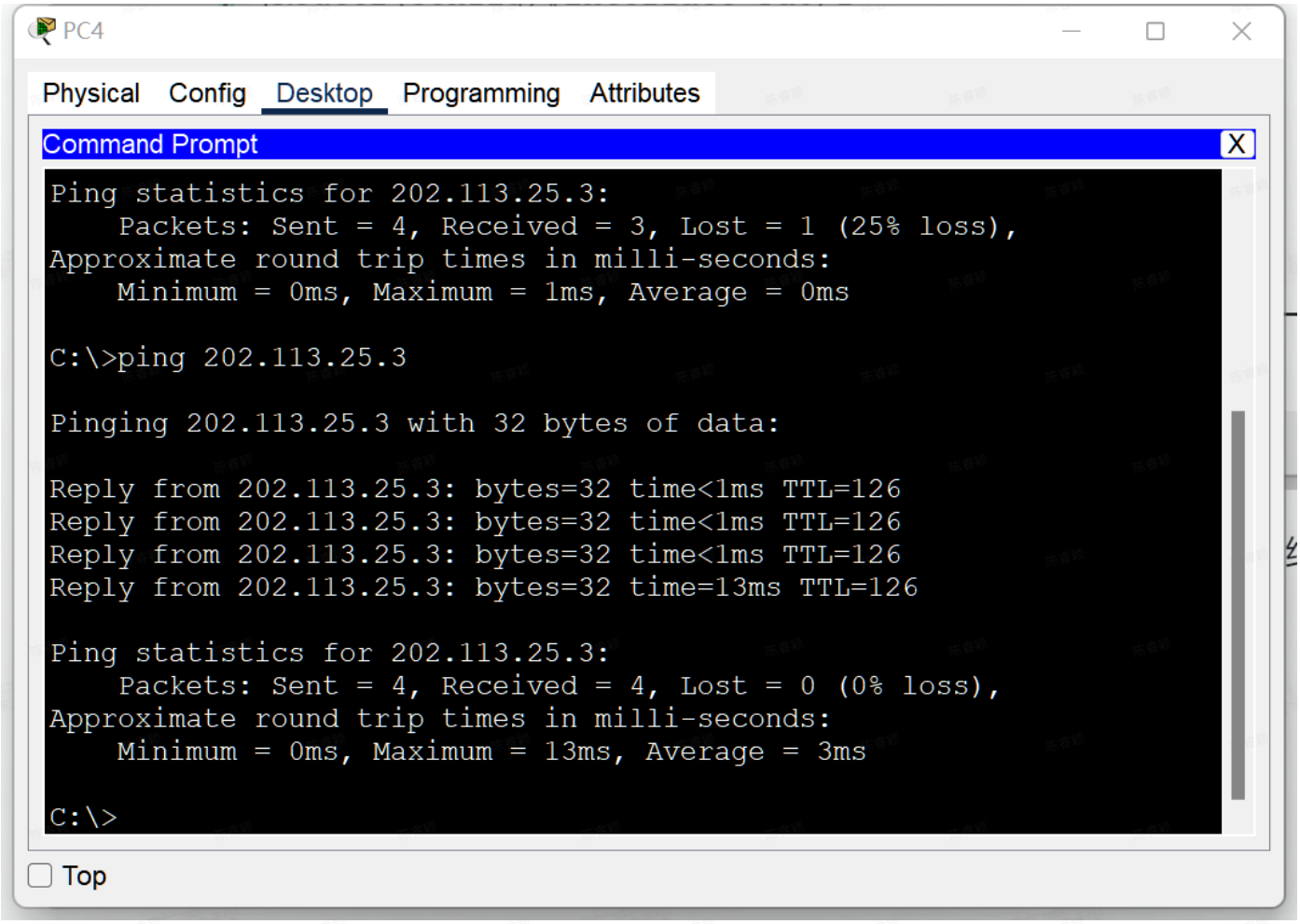
4. 在Router0的0/1接口上绑定一个ACL，对进入该接口的数据报进行过滤。使用如下命令：

```
Router(config)#access-list 6 permit 202.113.26.0 0.0.0.255
Router(config)#access-list 6 permit deny any
Router(config)#interface Fa0/1
Router(config-if)#ip access-group 6 in
```



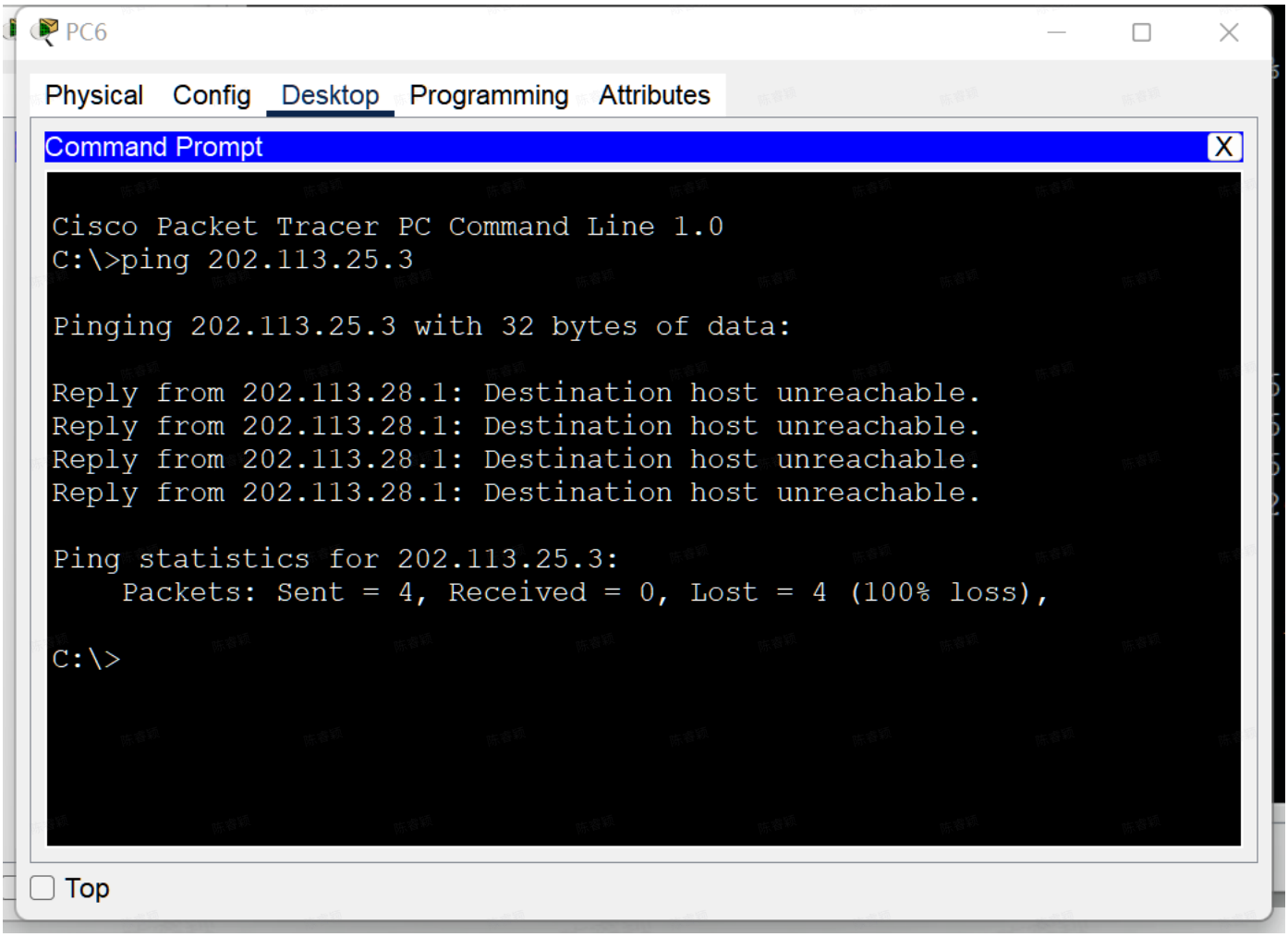

5. 利用网络B中的主机ping网络A中的主机，检查Router0是否阻止了网络B中的主机：

   例如用PC4 ping PC1：




可以连通；

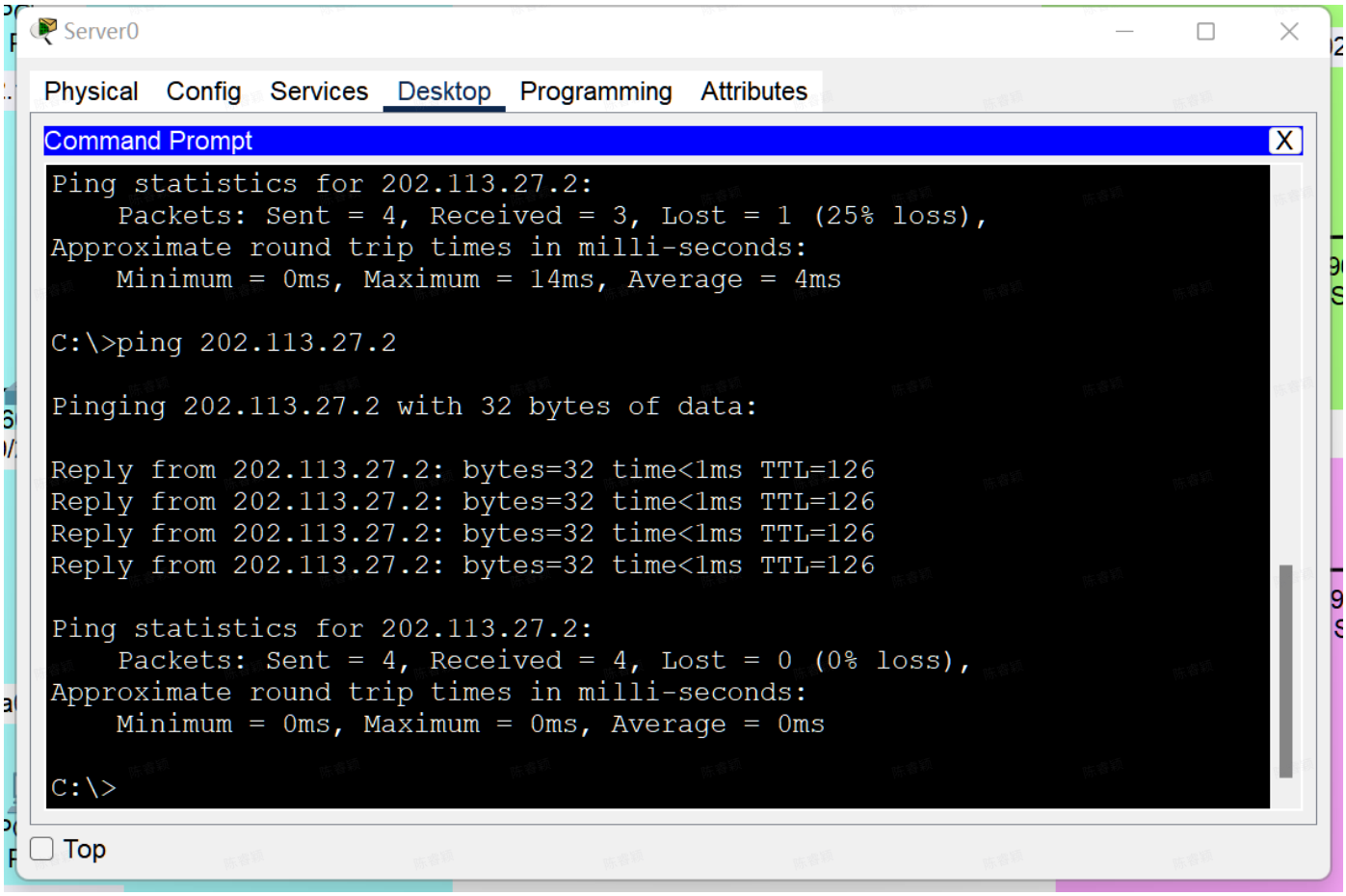
PC6 ping PC1：




不能ping通，说明网络B没有被阻止而网络C被阻止了。

## 3.2 扩展访问控制列表实验

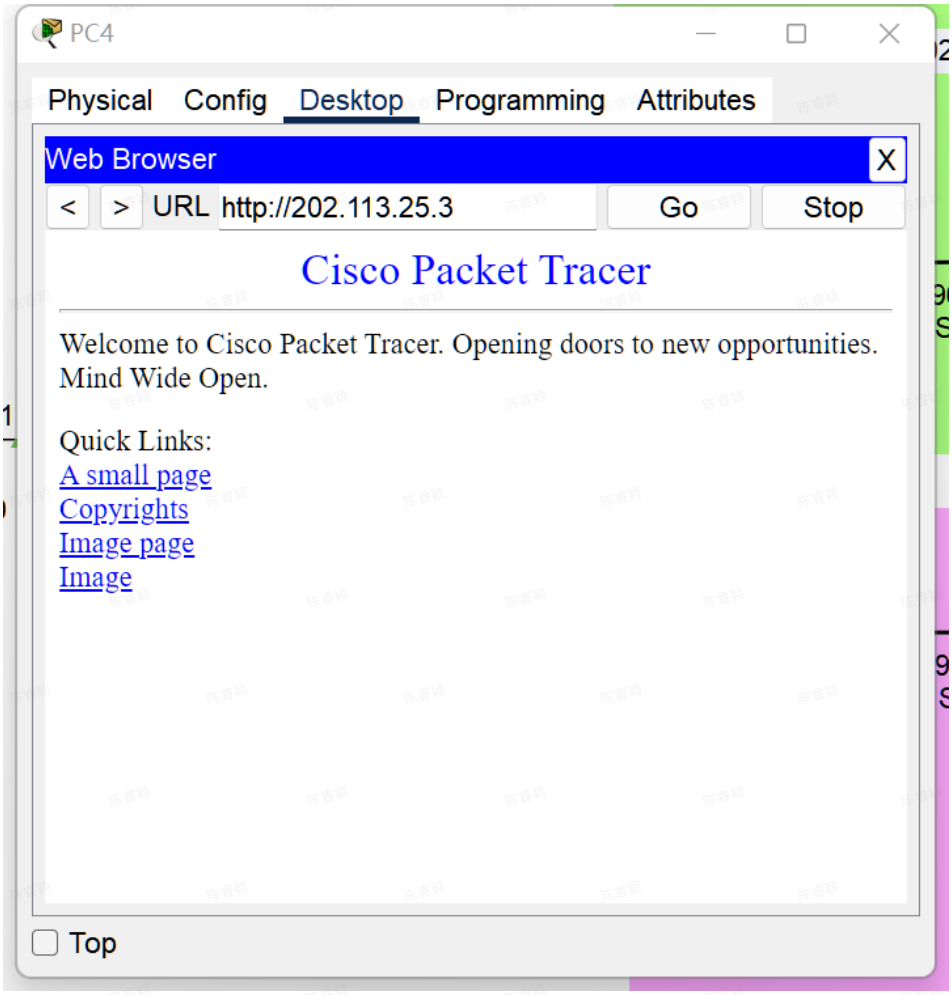
1. 按照拓扑图进行IP的配置等工作，同样测试网络A、B、C的连通性：




上图是使用server0 ping 网络C中的PC5

2. 检查web服务是否正常

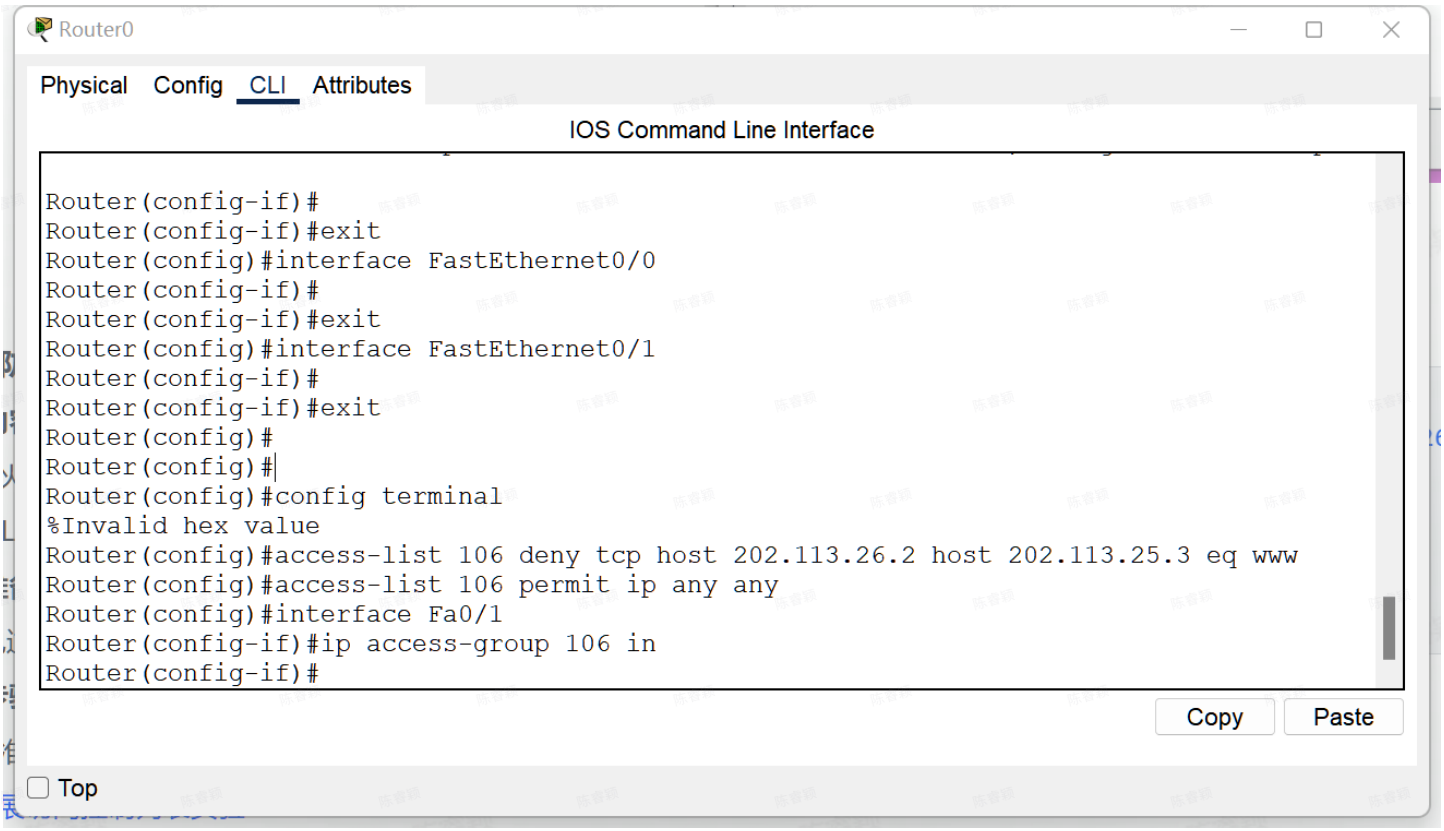
   如图是在网络B中的PC3访问server0的webserver服务：




正常显示！

3. 添加扩展ACL，阻止主机PC4访问server，使用的命令如下：

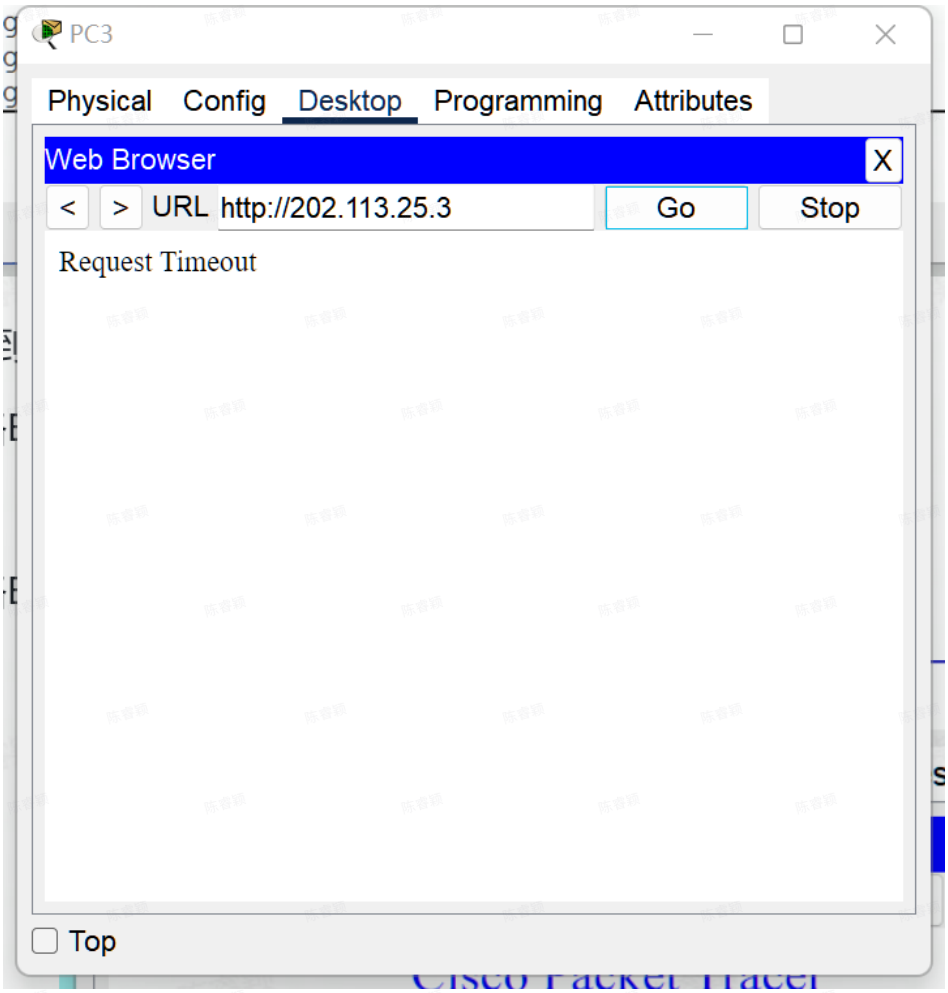
```
Router(config)#access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 e
Router(config)#access-list 106 permit ip any any
Router(config)#interface Fa0/1
Router(config-if)#ip access-group 106 in
```



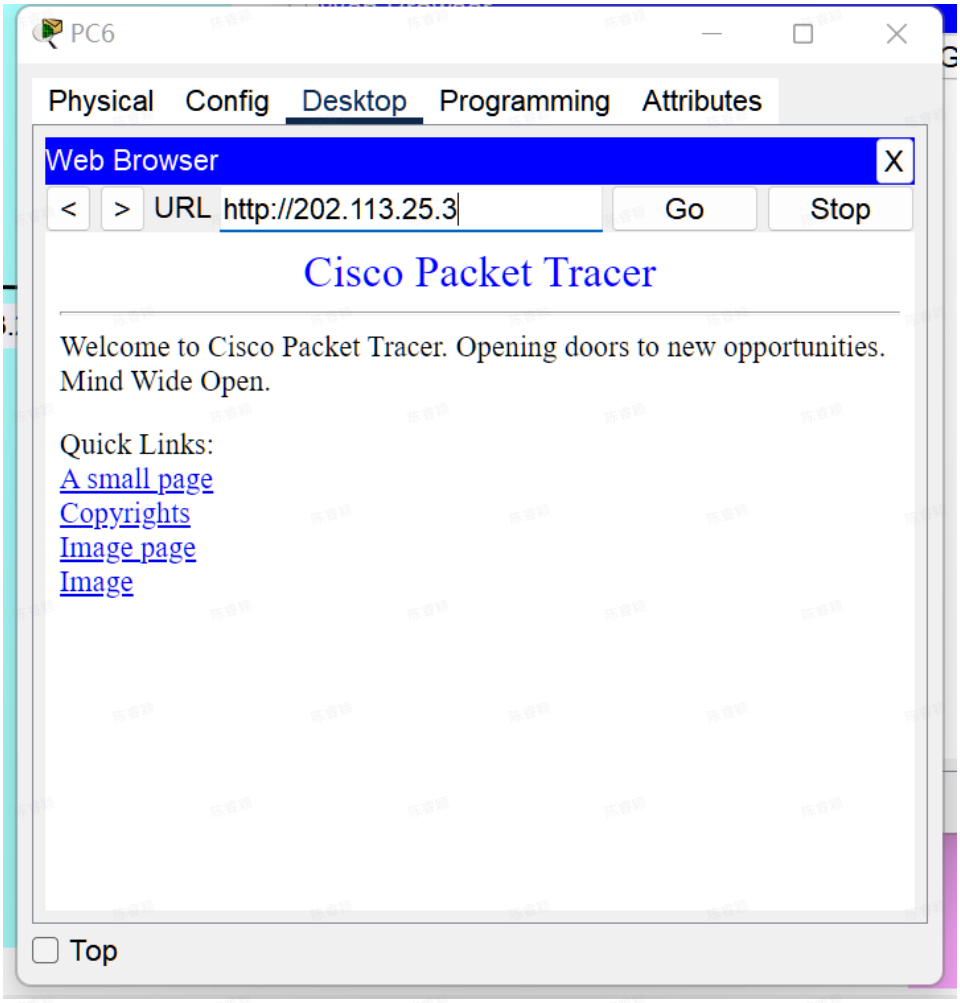

4. 测试是否达到配置的目标：

   a. 利用网络B中的主机PC3访问server的web服务：

   拒绝该地址访问成功！



b. 利用网络B中的主机PC6访问server的web服务：




允许访问！