网络技术验证性实验---配置包防火墙

姓名：董伊萌

学号：2012482

专业：信息安全

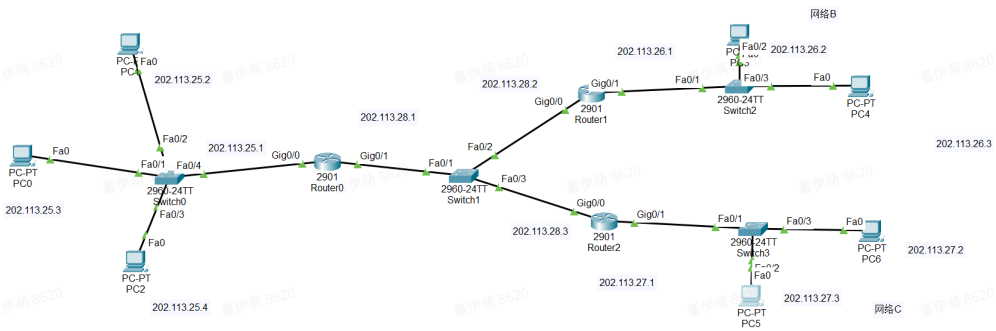
一. 实验内容说明

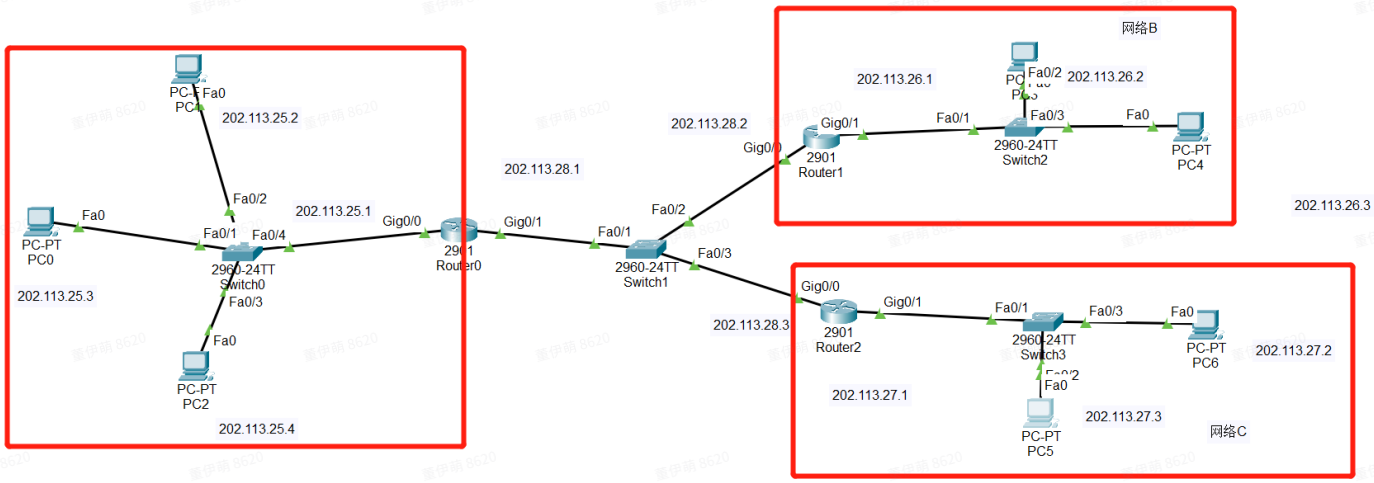
防火墙实验在虚拟仿真环境下完成，要求如下：（1）了解包过滤防火墙的基本配置方法、配置命令和配置过程。（2）利用标准ACL，将防火墙配置为只允许某个网络中的主机访问另一个网络。（3）利用扩展ACL，将防火墙配置为拒绝某个网络中的某台主机访问网络中的Web服务器。（4）将防火墙配置为允许内网用户自由地向外网发起TCP连接，同时可以接收外网发回的TCP应答数据包。但是，不允许外网的用户主动向内网发起TCP连接（选做）。

二. 实验准备

路由器通常都带有一定的防火墙功能，在Cisco路由器中，可以使用访问控制列表ACL实现简单的数据报过滤。本次实验将会利用访问控制列表实现一个简单的数据包过滤防火墙。

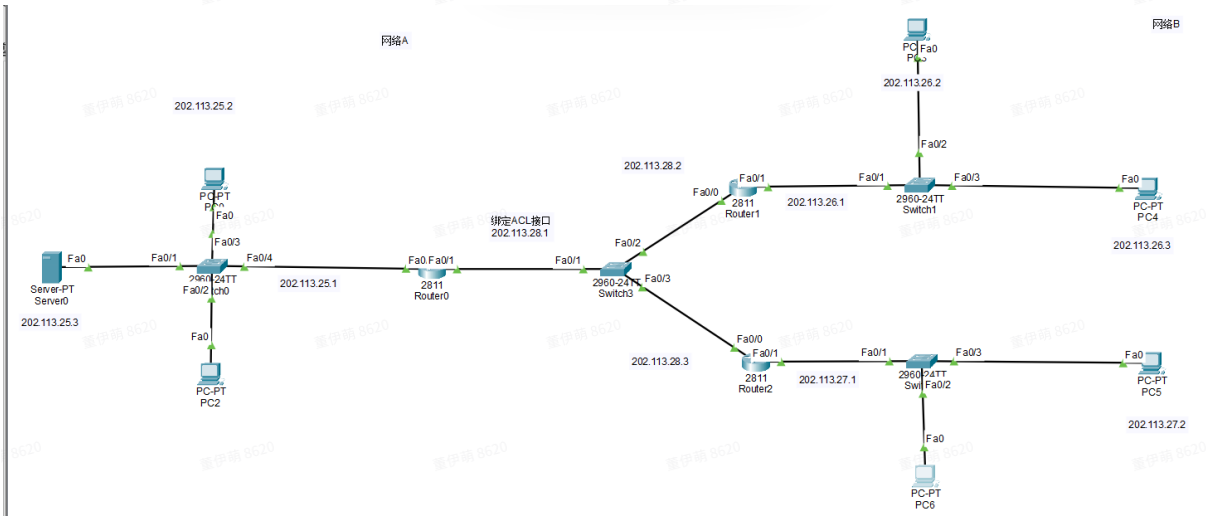
1. **标准访问控制列表实验网络拓扑图如下：**

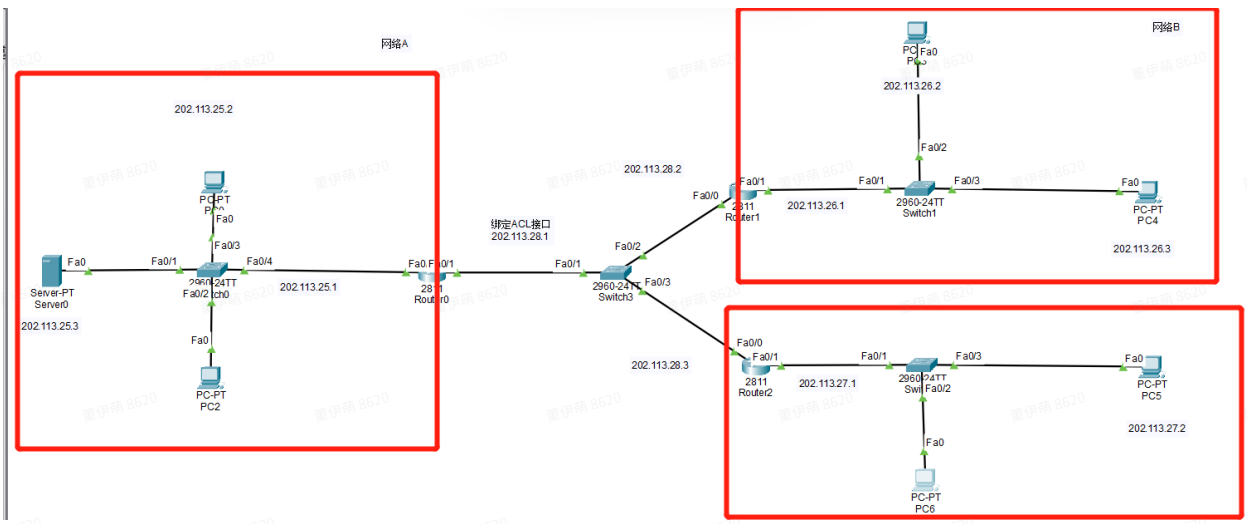




IP号已经在图上显示，实验的目标允许网络B中的主机访问网络A中的主机，但网络C中的主机不能访问网络A中的主机。

2. **扩展访问控制列表实验网络拓扑图如下：**





目标是不允许PC4浏览服务器上的web服务。

三. 实验过程

访问控制列表（ACL）是应用在网络设备接口上的规则列表，这些规则列表用于告诉网络设备哪些数据包可以通过，哪些数据包需要拒绝。ACL可应用于网络接口的入站方向（检查从该接口接收的所有数据包），或出站方向（检查从接口发出的所有数据包），一个ACL可以有多条规则，网络设备通常采用有限匹配原则，当出站的数据包到来的时候，网络设备按照次序依次对ACL列表中的规则进行匹配。一旦匹配成功，网络设备立即执行匹配规则中指定的动作，不再进行后续规则的匹配。

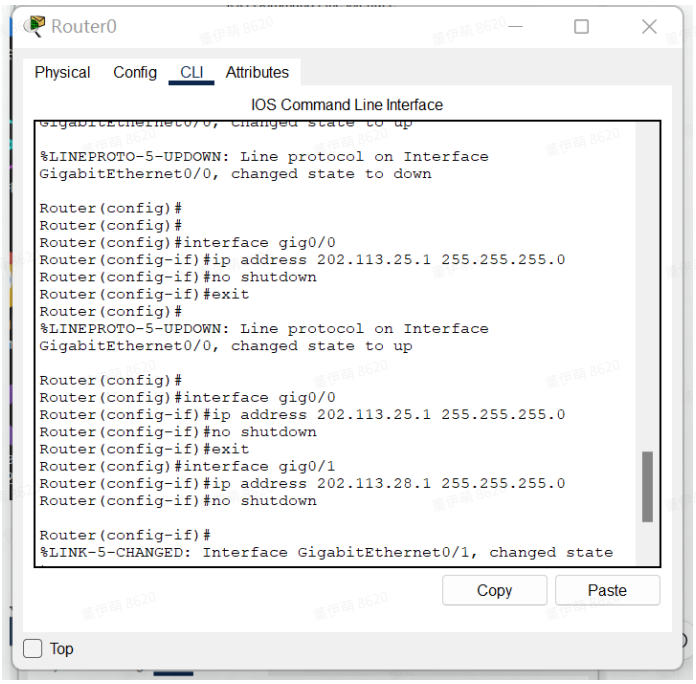
1. 标准访问控制列表实验

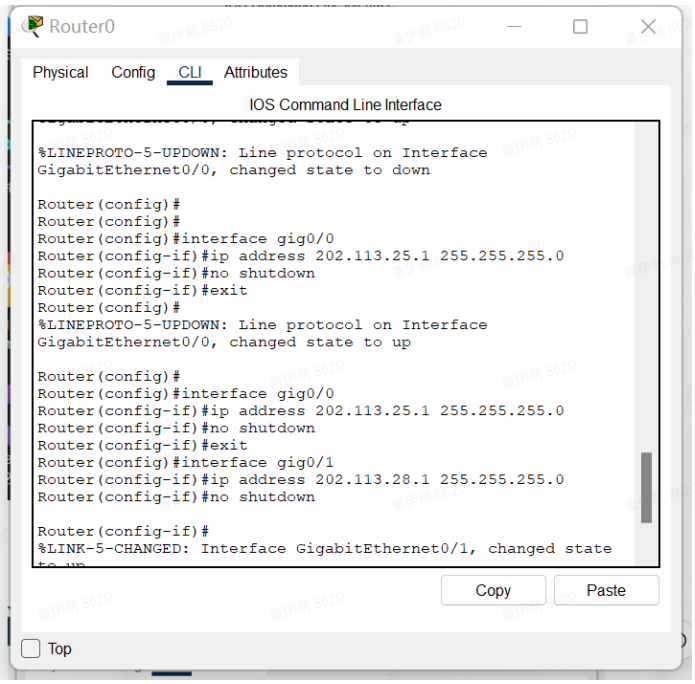
标准访问控制列表-标准ACL

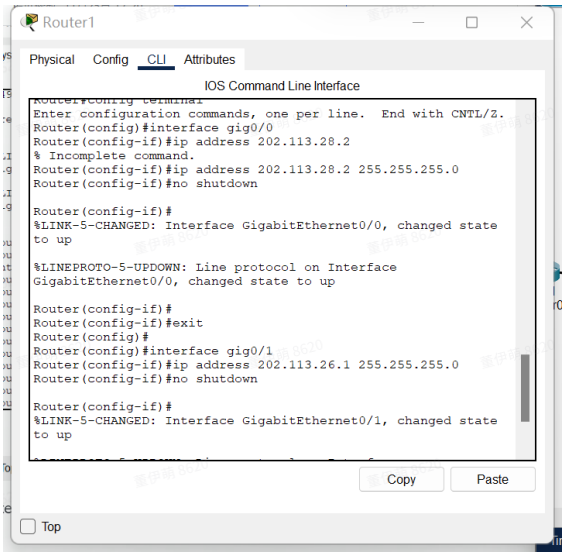
利用IP数据报中的源IP地址对过往数据包进行控制

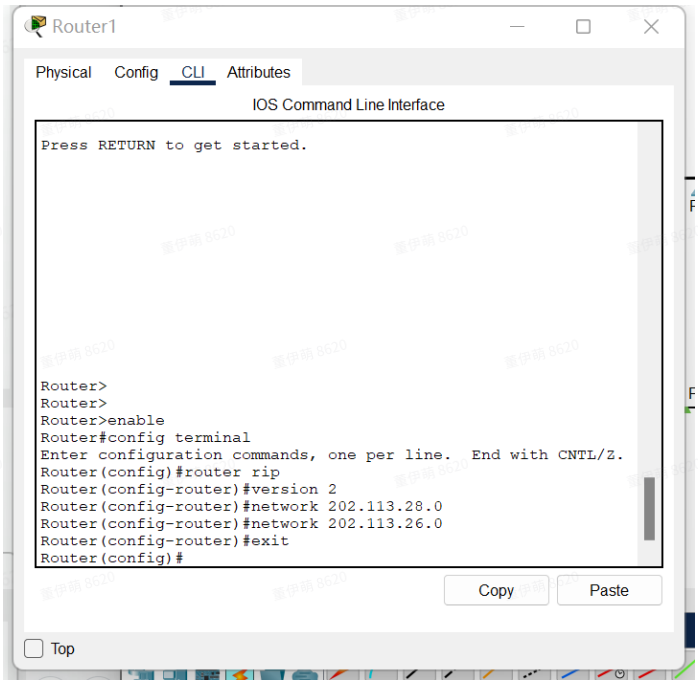
列表号范围：1~99

- 按照拓扑图给出的IP地址配置主机、路由器的IP地址，然后使用动态路由配置方法，配置路由器Router1和 Router2 的路由表，可以直接在Config 窗口中配置，然后使用no shutdown激活各接口，使网络A、网络B和网络C中的主机能够相互访问。









如图所示，此时网络B中的主机和网络C中的主机都可以和网络A中的主机连通。

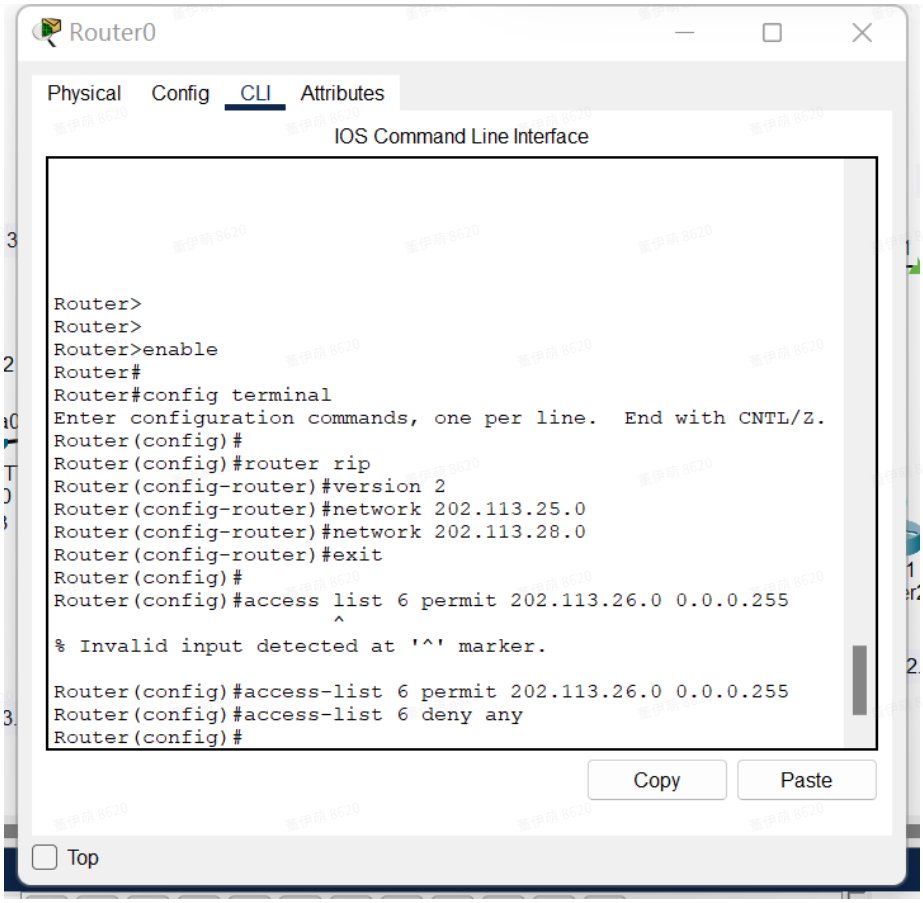
- 配置ACK，使得网络A允许网络B中的主机访问，但不允许其他网络（如网络C）中的主机访问。

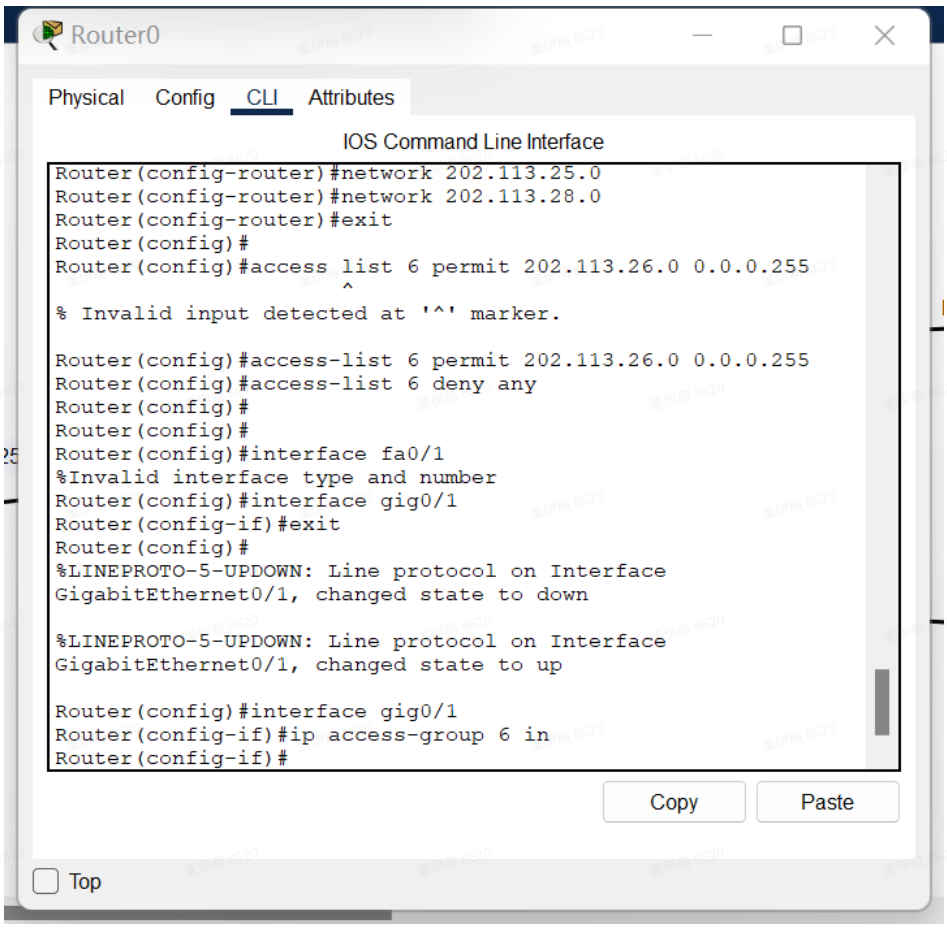
在Router1的全局配置模式下使用如下命令建立一个标号为6、包含两条规则的标准ACL：

`access-list 6 permit 202.113.26 0.0.0.255` 6是ACL的列表号，取值范围为1~99，相同列表号的规则属于同一个ACL，其先后顺序按照加入的先后顺序定，匹配成功后，网络设备采取的动作有两种，一种是permit(允许通过），另一种是deny（丢弃），`202.113.26` 是源起始IP地址，后面 `0.0.0.255` 是通配符，从而允许网络B中的主机发送的数据报通过，用于定义IP地址的范围

`access-list 6 deny any` any 表示任意的主机

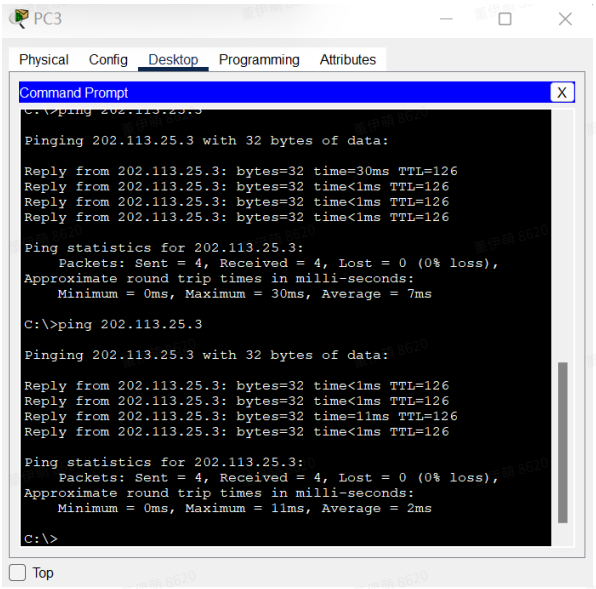
进入gig0/1接口配置模式，利用 `ip access-group 6 in` 将6号ACL绑定在gig0/1的入站上。



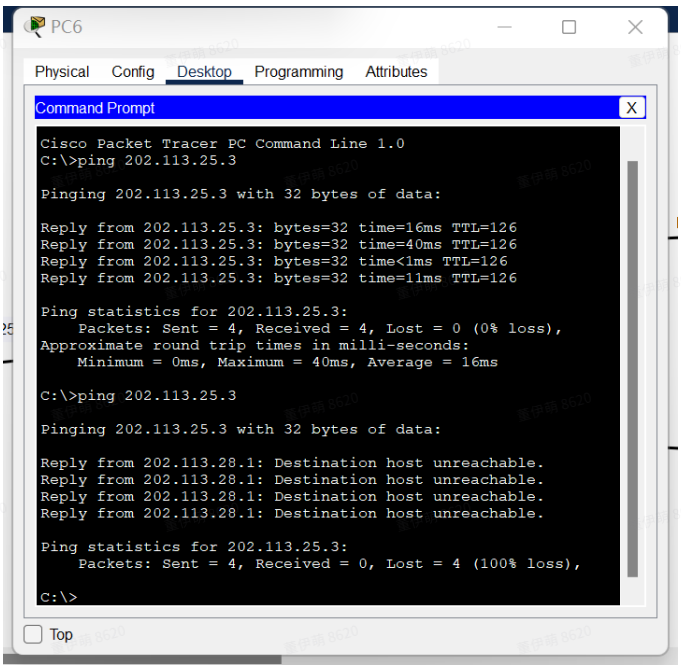


- 测试验证

利用网络B中的主机ping网络A中的主机，可以ping通：



利用网络C中的主机ping网络A中的主机，发现Router1阻止了它：

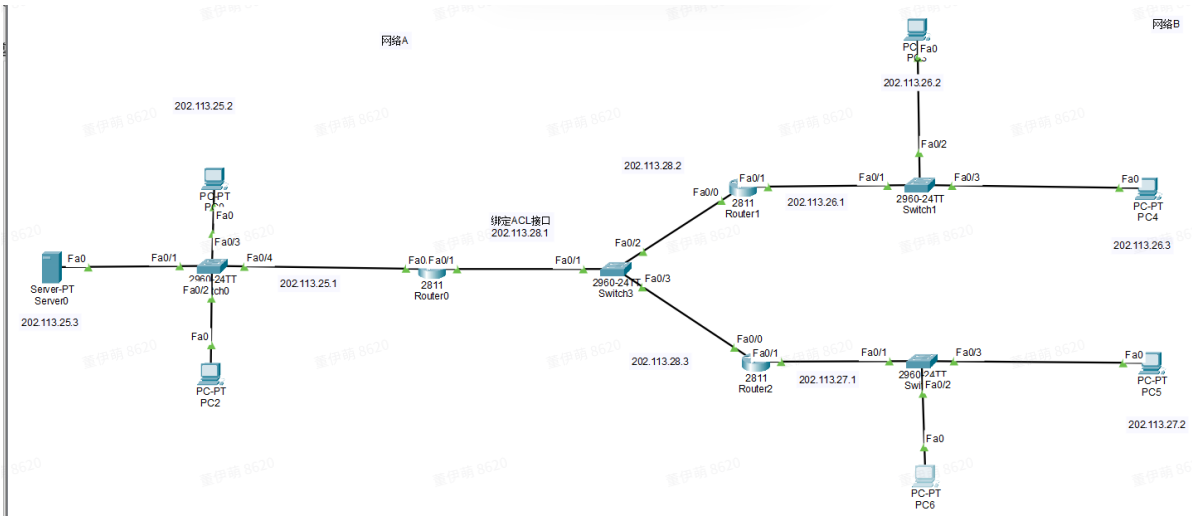


2. 标准访问控制列表实验

扩展访问控制列表-扩展ACL

按照协议类型、源IP地址、目的IP地址、源端口号、目的端口号对过往数据报进行控制。

- 按照如下拓扑图给出的IP地址配置主机、路由器的IP地址，然后配置路由器Router1和 Router2 的路由表，可以直接在Config 窗口中配置，然后使用no shutdown激活各接口，使网络A、网络B和网络C中的主机能够相互访问。



- 打开网络A中的服务器的HTTP服务，利用网络B和网络C主机的Web Browser浏览WebServer服务器上的网页，配置成功。
- 配置扩展ACK，使得除PC4外，允许其他主机浏览WebServer服务器的Web界面。

添加扩展ACL规则的一般命令形式为：

Access-list ListNum {permit|deny} Protocol SrcIPAddr SrcPort DesIPAddr DesPort

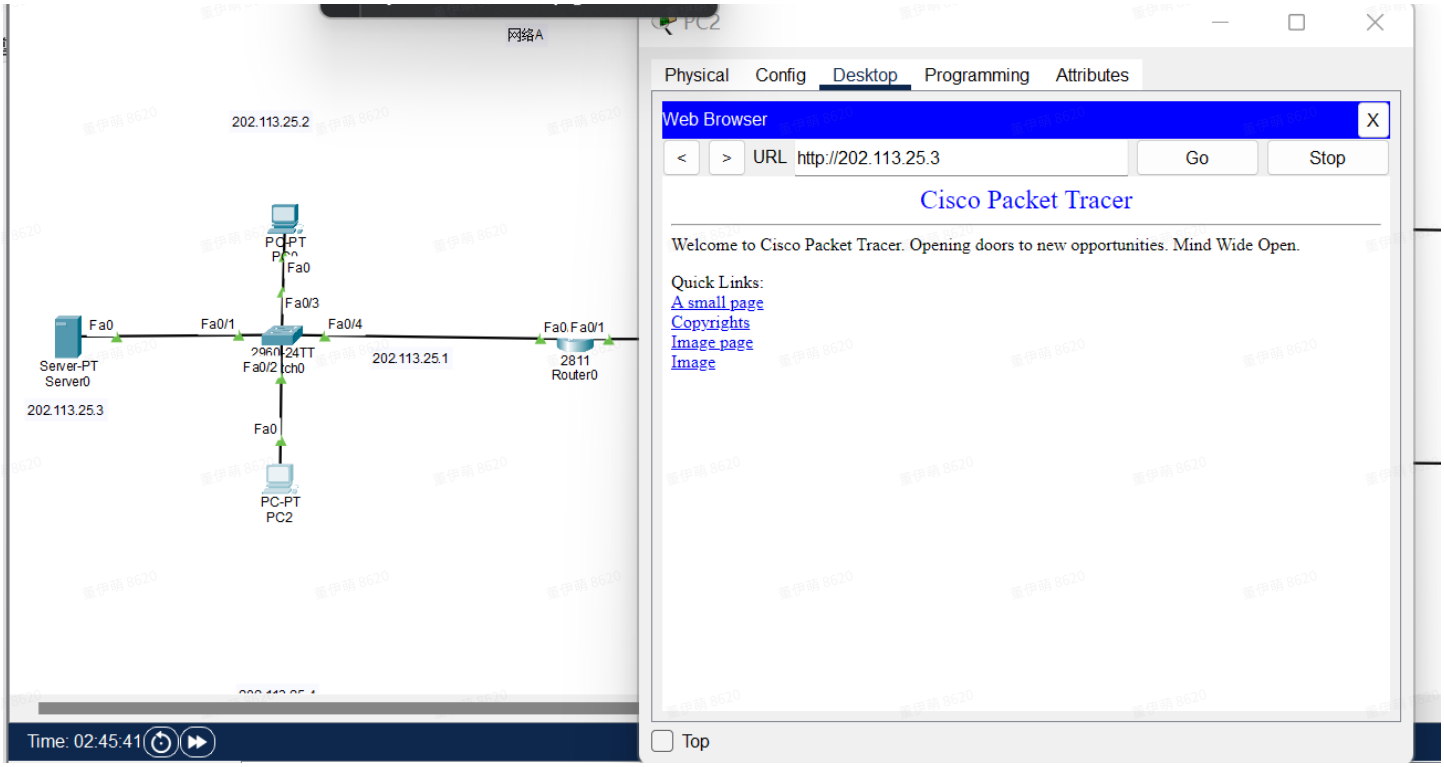
其中 ListNum 是ACL号，取值范围是101~199;{permit|deny} 表示匹配成功后，网络设备采取的动作；permit为允许通过，deny是丢弃；Protocol 指定该条规则适用的协议类型，协议类型可以是ip,icmp，tcp,udp。SrcPAddr,指定源IP地址范围。SrcPort指定源TCP或者是UDP端口范围。

在Router1的全局配置模式下使用如下命令建立一个标号为106、包含两条规则的扩展ACL：

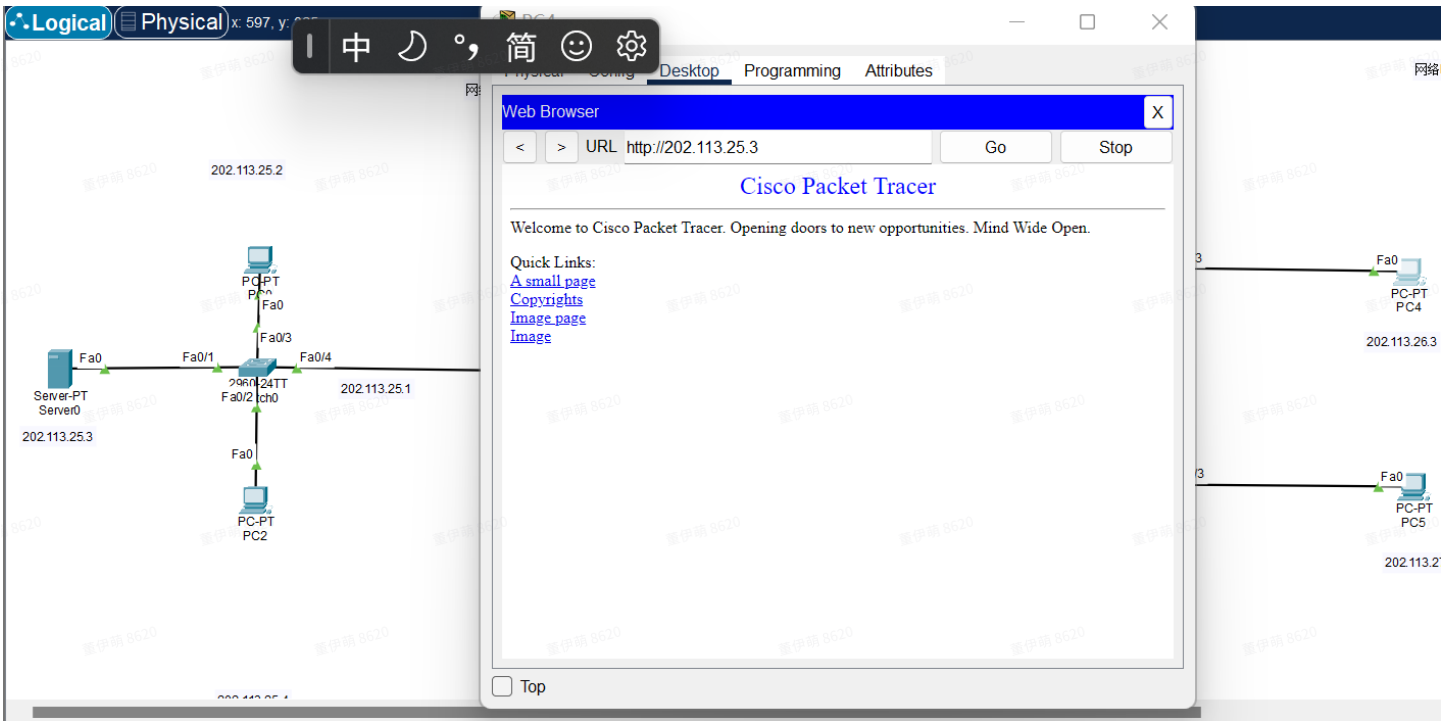
```
access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 eq www
access-list 106 permit ip any any
```

绑定ACL至端口：进入Fa0/1接口配置模式，利用 `ip access-group 106 in` 将106号ACL绑定在Fa0/1的入站上。

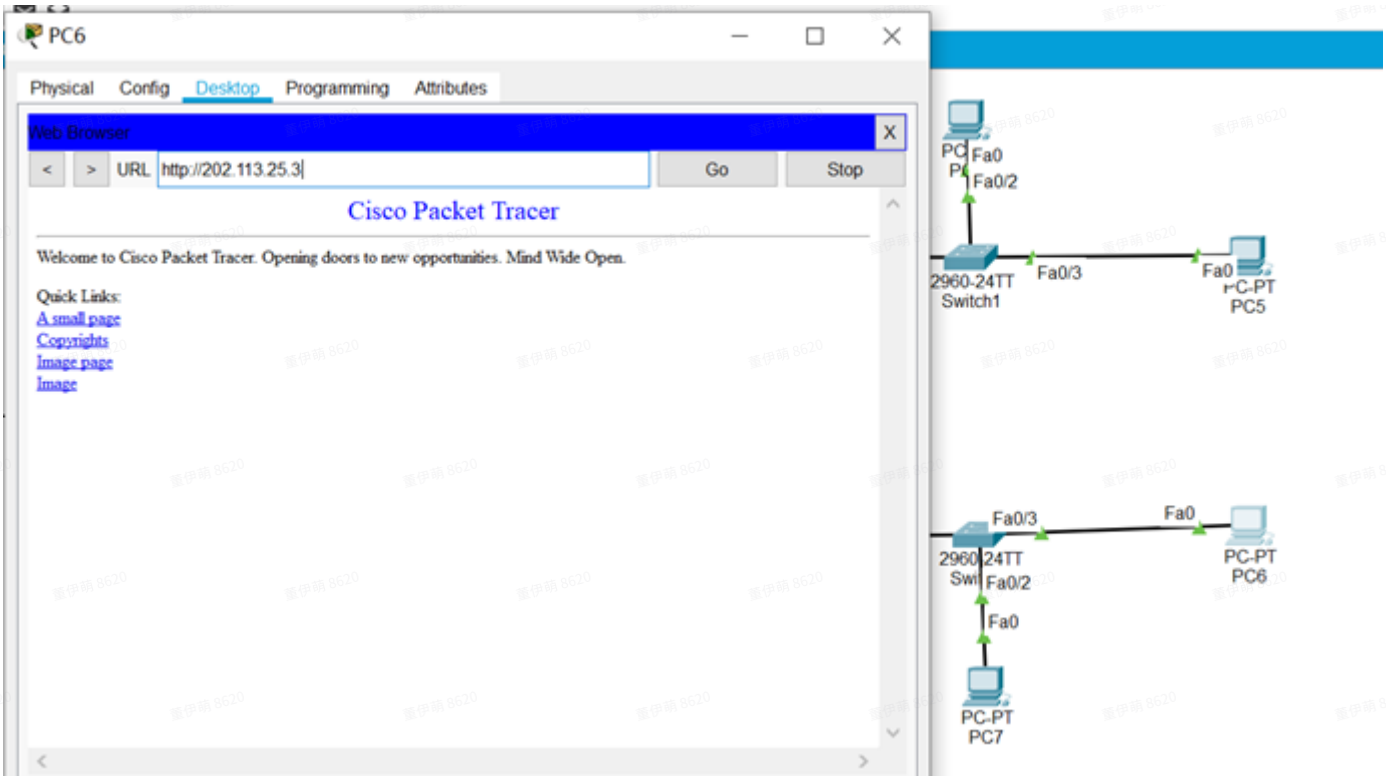
- 利用网络A中的主机浏览WebServer上的网页成功：



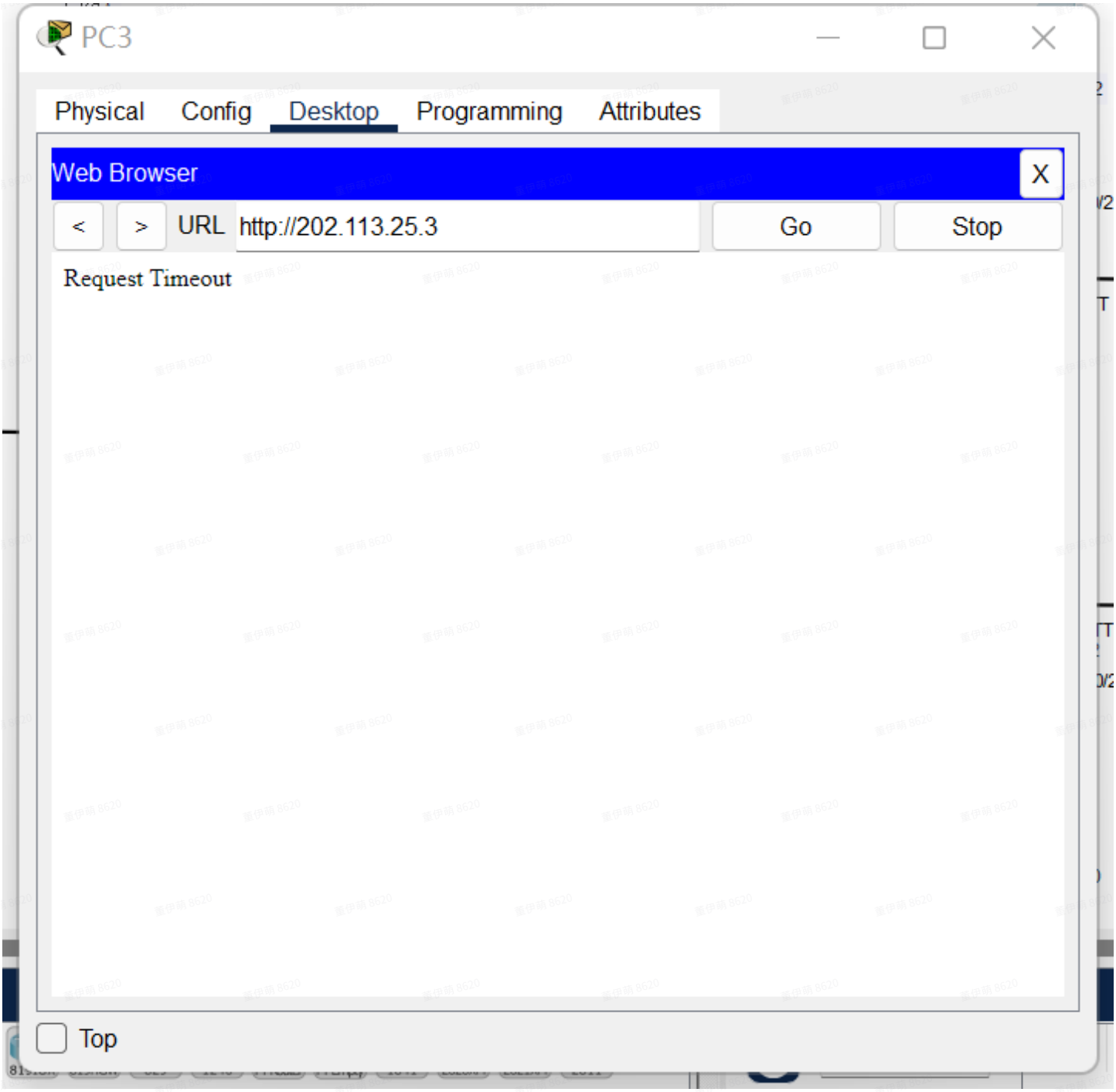
- 利用网络B中的除PC3外的主机浏览WebServer上的网页成功：



- 利用网络C中的主机浏览WebServer上的网页成功：



- 利用PC3浏览WebServer上的网页失败：



四.总结与感想

本次实验学习了利用路由器实现简单的包过滤防火墙，使用访问控制列表ACL实现。了解了标准ACL和扩展ACL的联系与区别，和实现访问控制列表的具体步骤，收获很大！