网络技术与应用课程报告

实验七：防火墙和 SSL 实验

姓名：孙悦

学号：2110052

专业：物联网工程

一、实验内容

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。

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。

二、实验准备

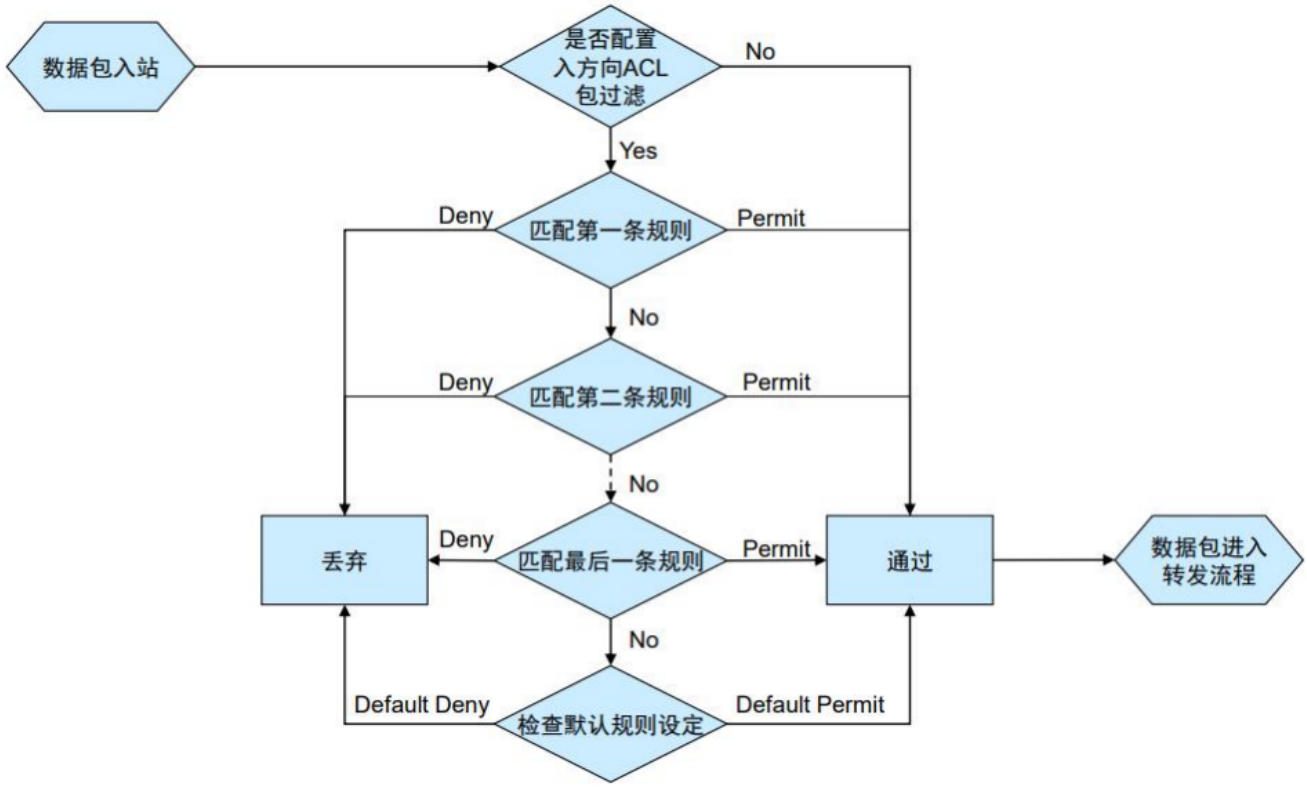
ACL概述：

ACL是用来实现数据包识别功能的，在本次实验中使用 ACL 用于包过滤防火墙功能。其中 ACL 的包过滤技术具体可分为一下过程：

- 对进出的数据包逐个过滤，丢弃或允许通过；

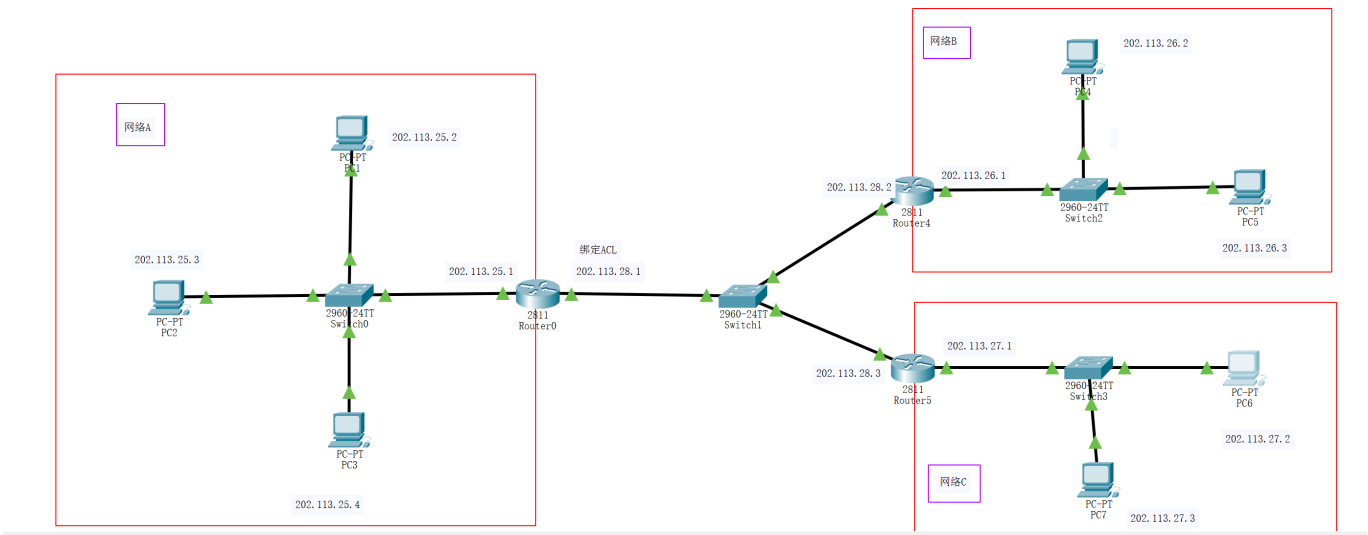
- ACL 应用于接口上，每个接口的出入双向分别过滤；
- 仅当数据包经过一个接口时，才能被此接口的此方向的 ACL 过滤；

其具体工作流程图如下所示：

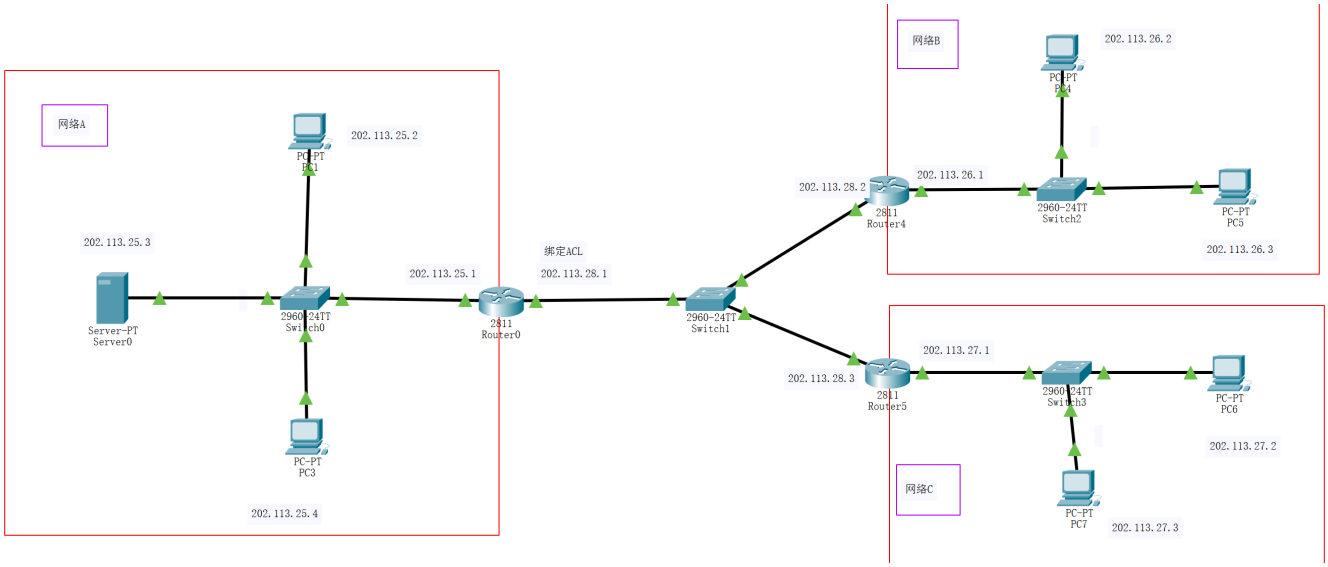


各个实验网络拓扑图如下所示：

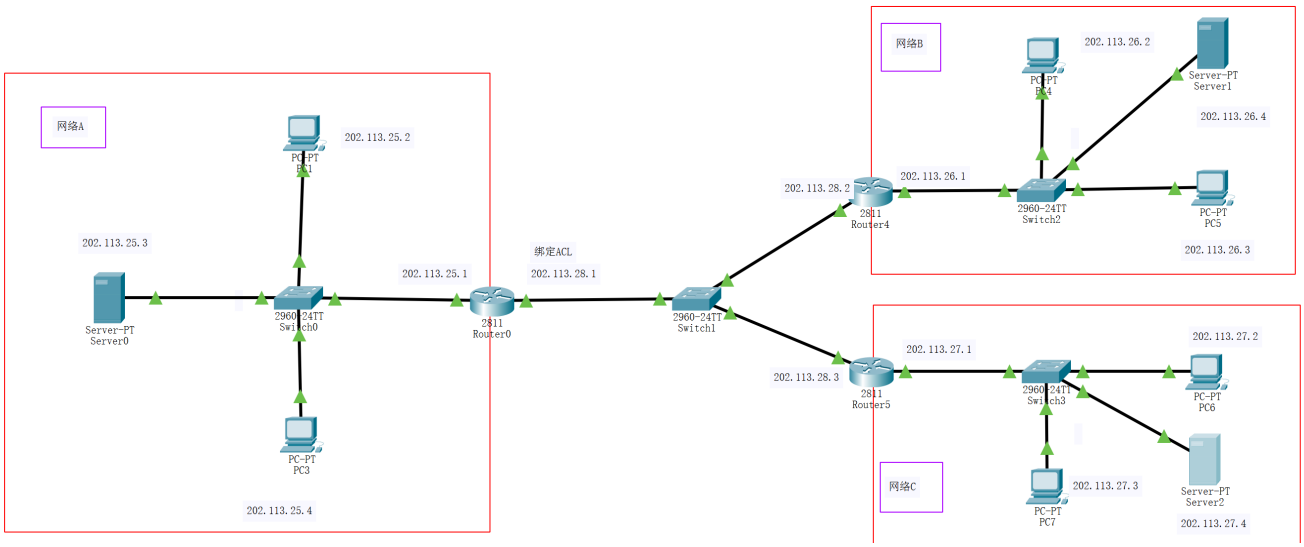
标准ACL：



扩展ACL1：



扩展ACL2：



实验各个主机和服务器和路由器IP配置如下：

主机 PC1 ： IP：202.113.25.2/24 ； 默认网关：202.113.25.1/24

主机 PC2：IP：202.113.25.3/24；默认网关：202.113.25.1/24

主机 PC3：IP：202.113.25.4/24；默认网关：202.113.25.1/24

主机 PC4：IP：202.113.26.2/24；默认网关：202.113.26.1/24

主机 PC5：IP：202.113.26.3/24；默认网关：202.113.26.1/24

主机 PC6：IP：202.113.27.2/24；默认网关：202.113.27.1/24

主机 PC7：IP：202.113.27.3/24；默认网关：202.113.27.1/24

服务器 Server0：IP：202.113.25.3/24；默认网关：202.113.25.1/24

服务器 Server1：IP：202.113.26.4/24；默认网关：202.113.26.1/24

服务器 Server2：IP：202.113.27.4/24；默认网关：202.113.27.1/24

路由器R0：IP：202.113.25.1/24 ;202.113.28.1/24

路由器R4：IP：202.113.28.2/24 ;202.113.26.1/24

路由器R5：IP：202.113.28.3/24 ;202.113.27.1/24

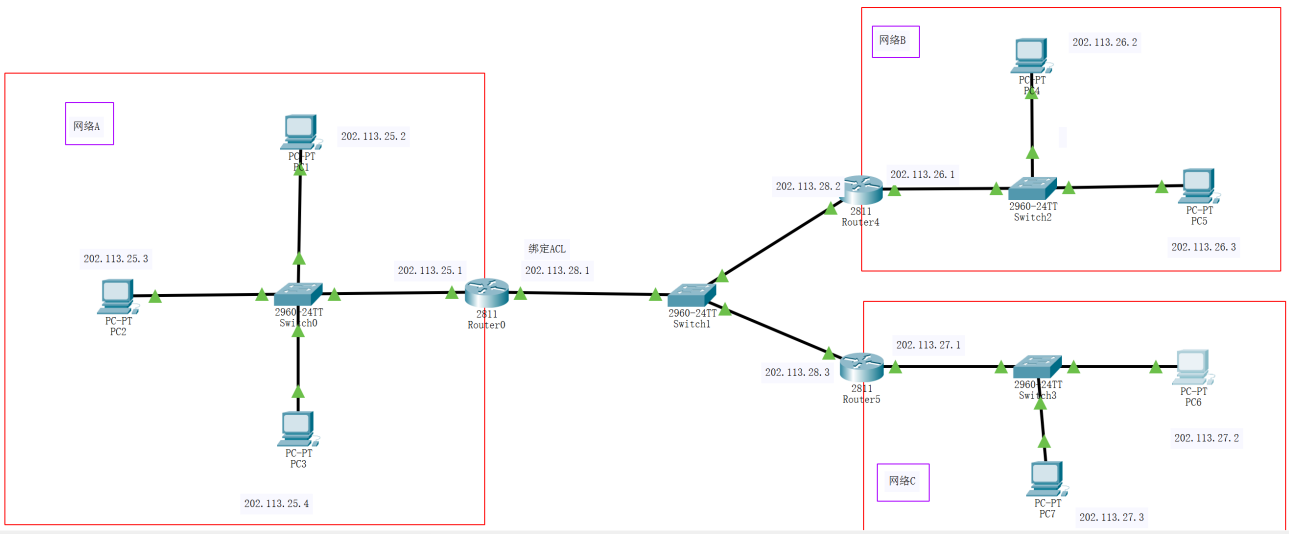
三、实验过程

1.标准ACL

本次实验的主要目的是：允许网络 B 访问网络 A，而不允许其他网络访问网络 A 中的主机。因此需要在路由器 R0 上定义标准 ACL，并把 ACL 绑定到接口的入站上，使得路由器对接口的入站数据包进行检查。

1.1主机IP地址和默认网关配置

网络拓扑图如下所示：



1.2路由器IP地址及配置ACL功能

1.2.1 IP地址配置

配置路由器 IP 地址，可以在配置界面中选择 CLI，首先使用 enable 命令进入路由器的特权执行模式，而后通过 config terminal 进入全局配置模式。路由器通常具有两个或多个网络接口，地址属

于某个特定接口。在为接口配置 IP 地址之前，首先使用“interface 接口名”进入接口的配置模式，并使用 `no shutdown` 命令激活接口。并通过 `router rip` 为其配置动态路由表。

具体指令如下：

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 202.113.25.1 255.255.255.0
Router(config-if)#ip address 202.113.25.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#

Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 202.113.28.1 255.255.255.0
Router(config-if)#ip address 202.113.28.1 255.255.255.0
Router(config-if)#no shutdown

Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 202.113.28.0
Router(config-router)#network 202.113.25.0
Router(config-router)#exit
```

1.2.2配置标准访问控制列表

对路由器R0进行配置，指令如下：

- 命令1建立标准控制列表指定能够通过的 IP 地址，在全局配置模式下进行；

```
Router(config)#access-list 6 permit 202.113.26.0 0.0.0.255
```

创建了序号为 6 的访问控制列表，允许 202.113.26.0 开始的地址通过，注意此处的通配符与掩码相反，能够改变的位为1，不能改变的位为0。

- 再在该ACL中增加一条规则：（可以省略不写）

```
Router(config)#access-list 6 deny any
```

拒绝其他所有IP地址通过，达到了仅允许 202.113.26.0 开始的地址通过的目的。

- 进入接口配置模式，将ACL绑定到路由器进入 202.113.26.0 的方向：

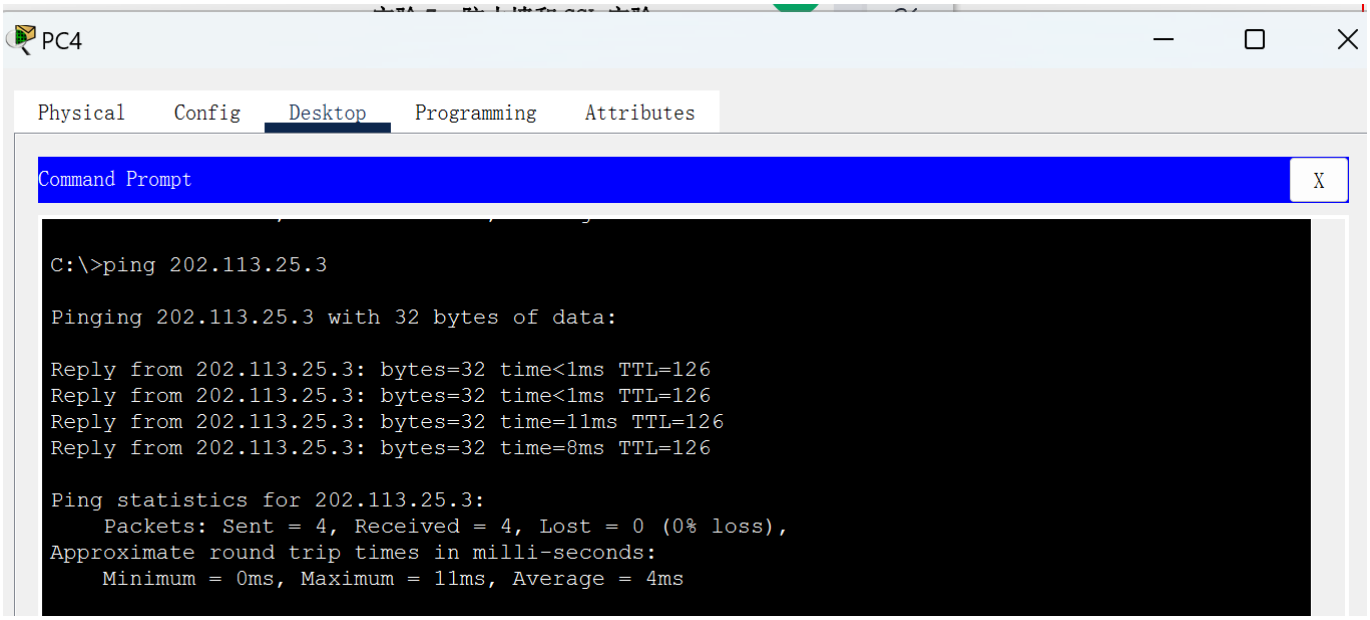
```
Router(config)#interface gig0/1
Router(config-if)#ip access-group 6 in
Router(config-if)#exit
```

1.3实验结果

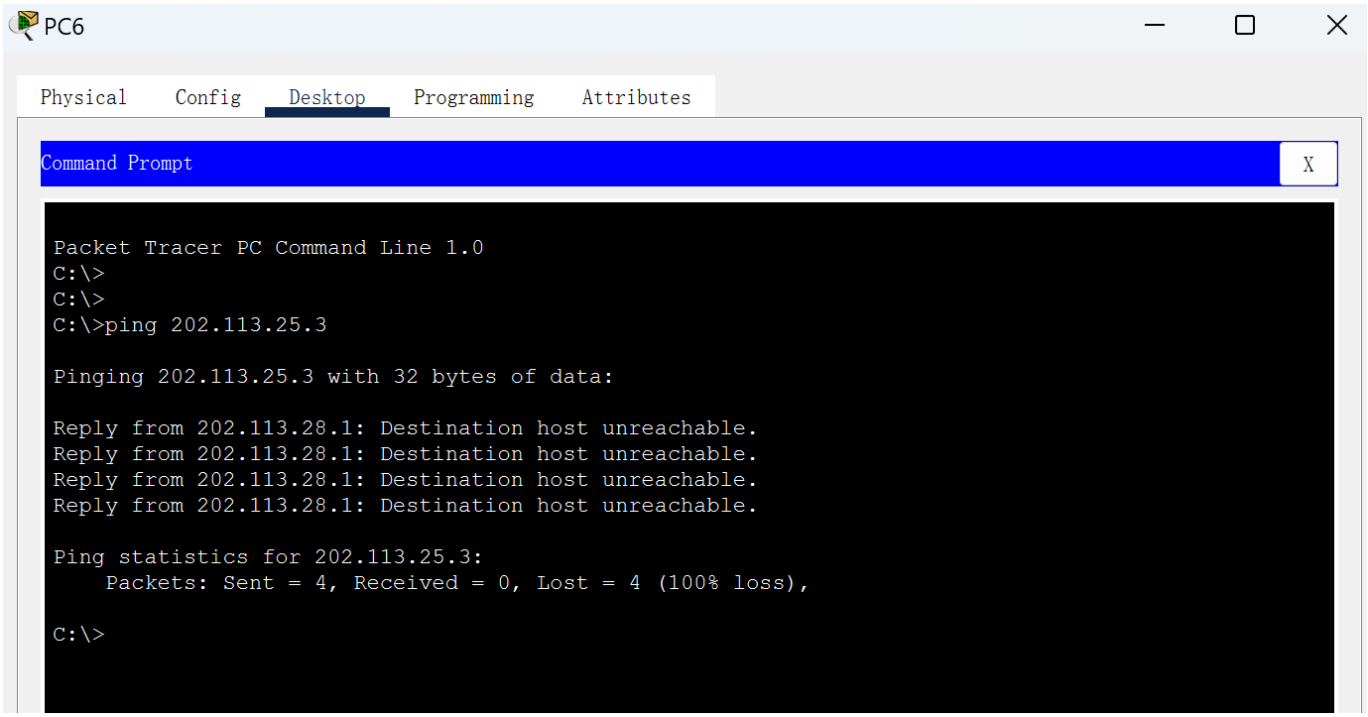
未配置ACL时网络B和网络C都可以访问网络A的主机。

配置完成后，网络 B 仍可以访问网络 A 的主机，而其他网络的主机访问网络 A 的主机时，显示无法到达：

网络B的PC4 ping PC2可以ping通



网络C的PC6 ping PC2无法ping通，显示不可达

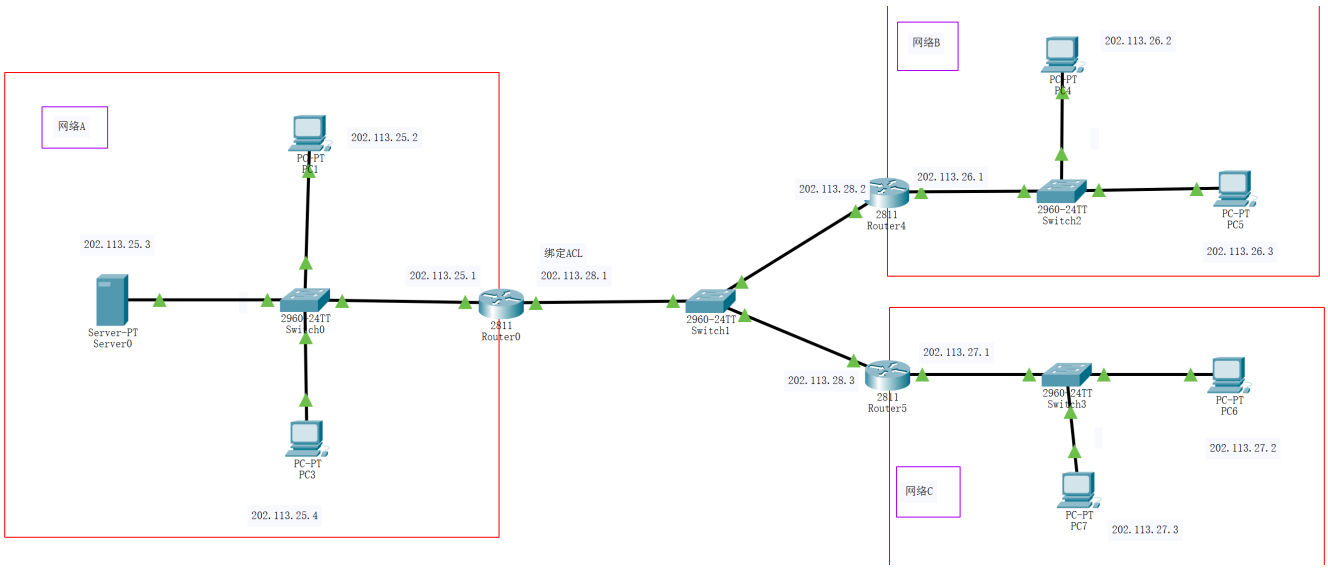


2.扩展ACL-1

原理：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包进行控制，列表号范围：101~199。 目的：不允许IP地址为 202.113.26.2 的主机访问地址为 202.113.25.3 的服务器的Web服务，允许其他任何主机访问。

2.1 主机IP地址和默认网关配置

本次实验所需配置的网络拓扑图如下所示：



2.2路由器IP地址及配置ACL功能

2.2.1 IP地址配置

配置路由器 IP 地址，可以在配置界面中选择 CLI，首先使用 `enable` 命令进入路由器的特权执行模式，而后通过 `config terminal` 进入全局配置模式。需要注意，路由器通常具有两个或多个网络接口，地址属于某个特定接口。

在为接口配置 IP 地址之前，首先使用“`interface 接口名`”进入接口的配置模式，并使用 `no shutdown` 命令激活接口。

具体指令如下：（R0）为例

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 202.113.25.1 255.255.255.0
Router(config-if)#ip address 202.113.25.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
```

```
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 202.113.28.1 255.255.255.0
Router(config-if)#ip address 202.113.28.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
```

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 202.113.25.0
Router(config-router)#network 202.113.28.0
Router(config-router)#exit
```

对路由器R0进行扩展ACL-1配置：

- 建立标准控制列表指定不能够通过的 IP 地址，在全局配置模式下进行：

```
Router(config)#access-list 106 deny tcp host 202.113.26.2 host
202.113.25.3 eq 80
```

创建了序号为 106 的访问控制列表，不允许 202.113.26.2 的地址通过 TCP 协议中 80 端口进行访问， host 为单个主机关键字， eq 表示等于，注意此处要写明源主机和目的主机。

- 再在该ACL中增加一条规则：（不可以省略不写）

```
Router(config)#access-list 106 permit ip any any
```

允许其他所有IP数据报通过，达到了仅不允许 202.113.26.2 开始的地址通过 TCP 协议访问的目的。

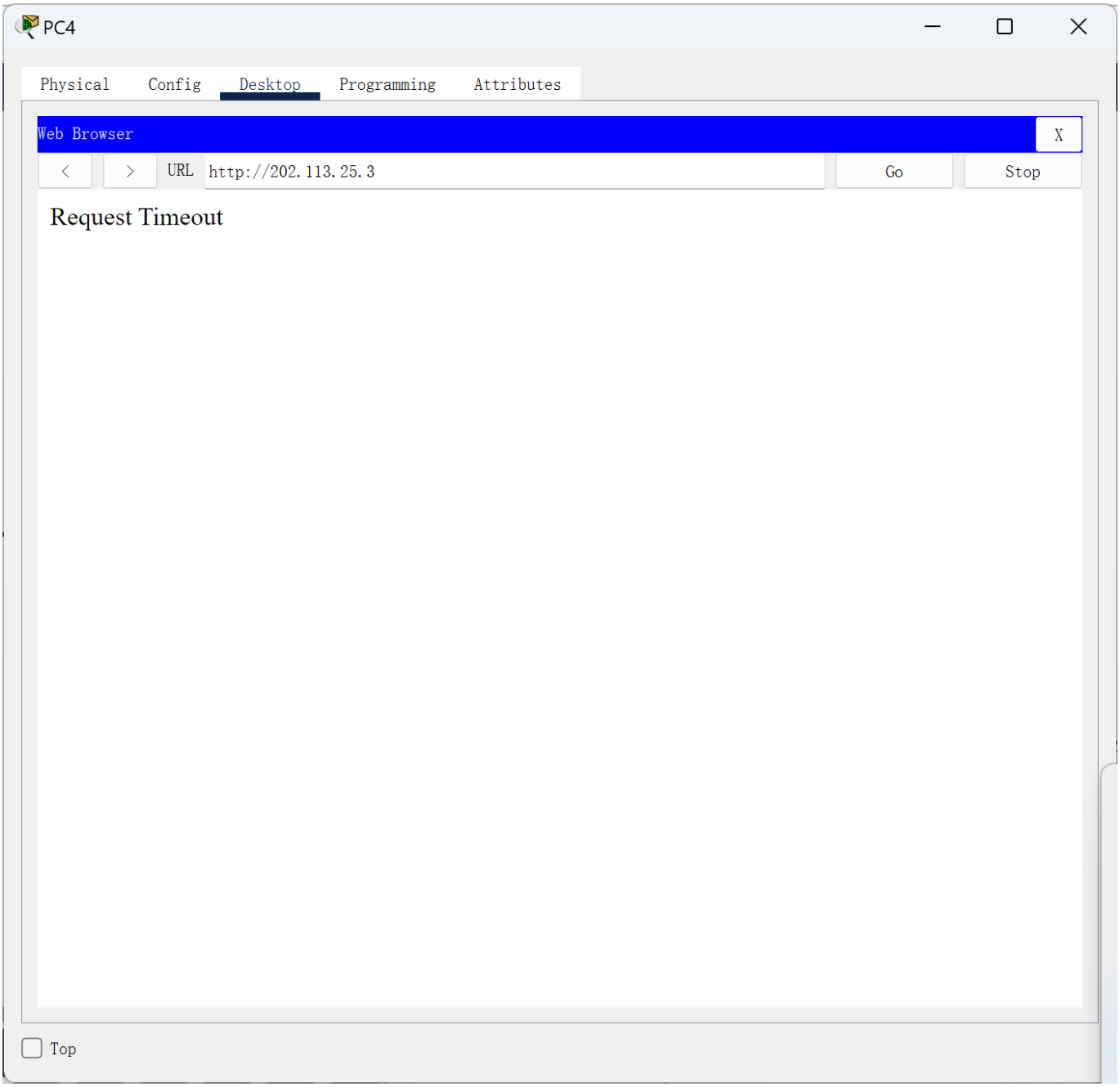
- 进入接口配置模式，将ACL绑定到路由器进入 202.113.26.0 的方向：

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

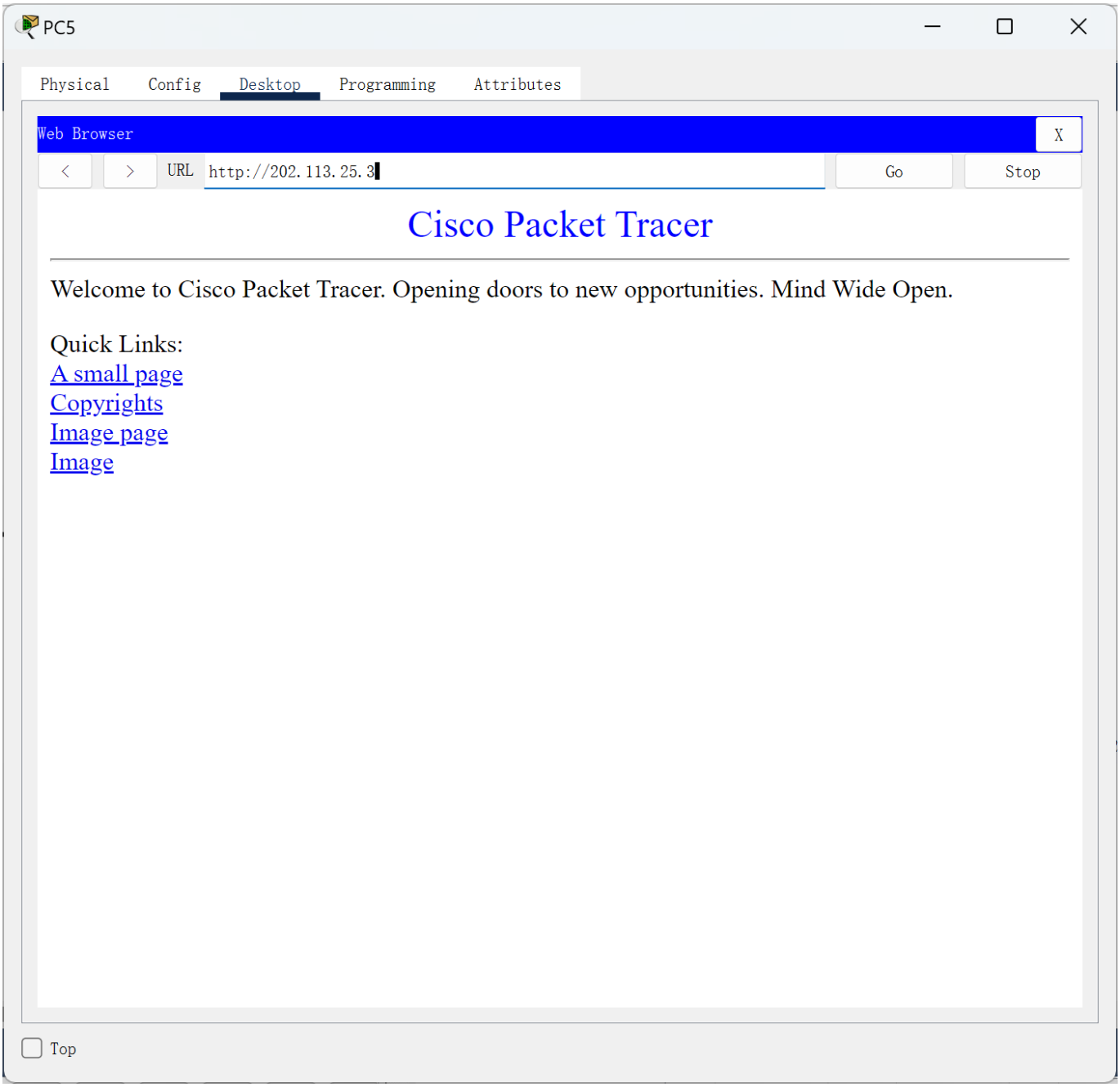
将序号为 106 的访问控制列表绑定到路由器 gig0/1 端口进入方向。

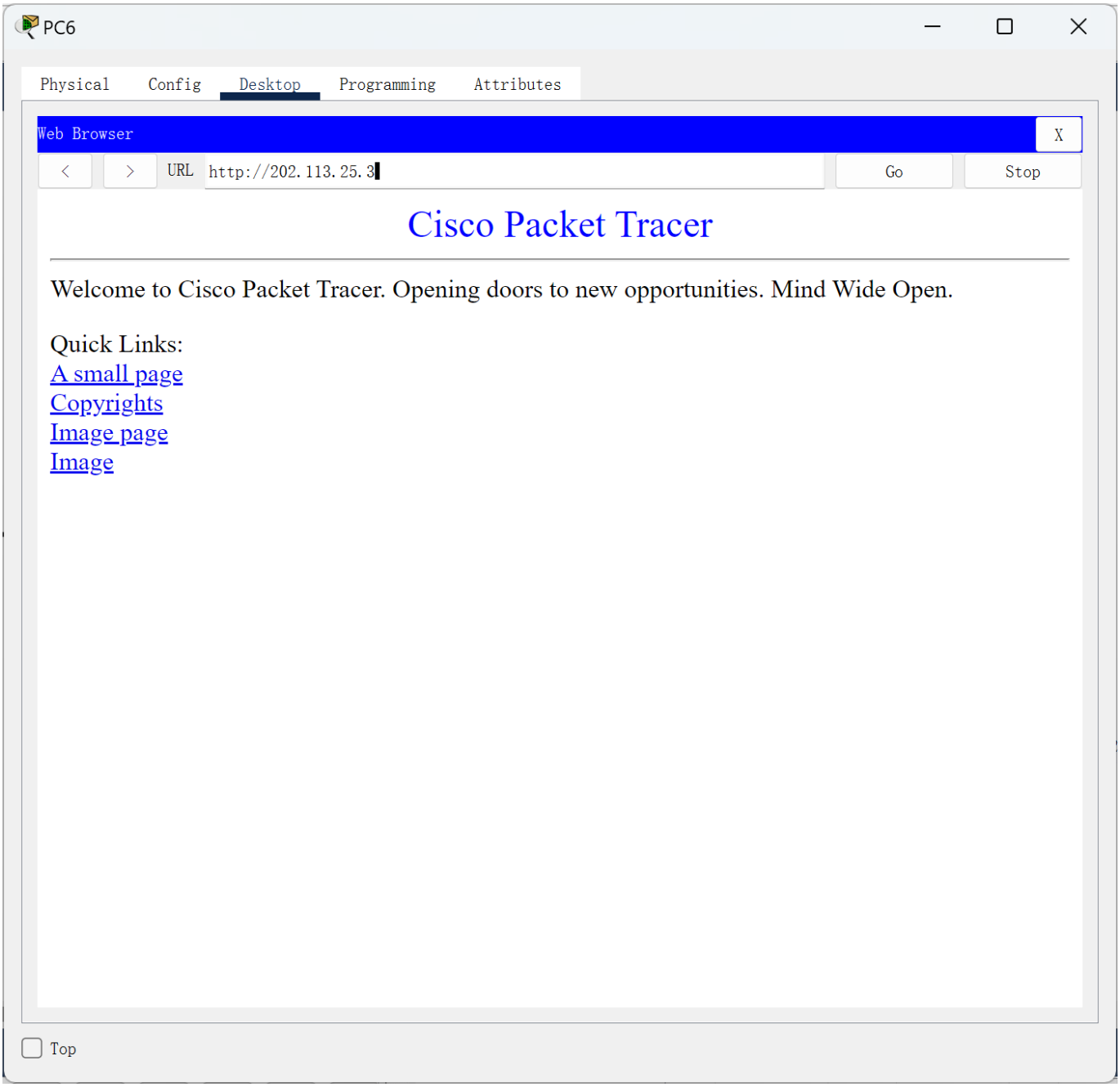
2.3实验结果

- 主机PC4（202.113.26.2）不能访问Server0，访问web失败：



- 其他主机均可访问Server0：

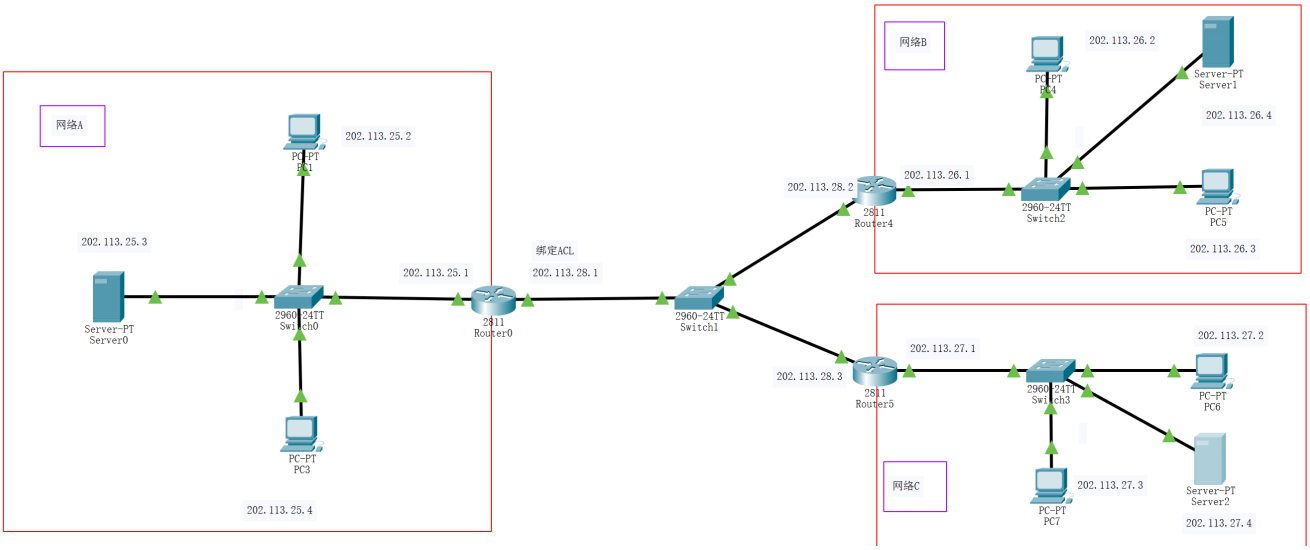

PC5
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
URL
http://202.113.25.3
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Top



3.扩展实验-2

网络A主机可访问网络A、网络B、网络C的web服务器，网络B 和网络C的主机不可访问网络A的web服务器，即网络A是内网，网络B和C是外网。

3.1实验拓扑图

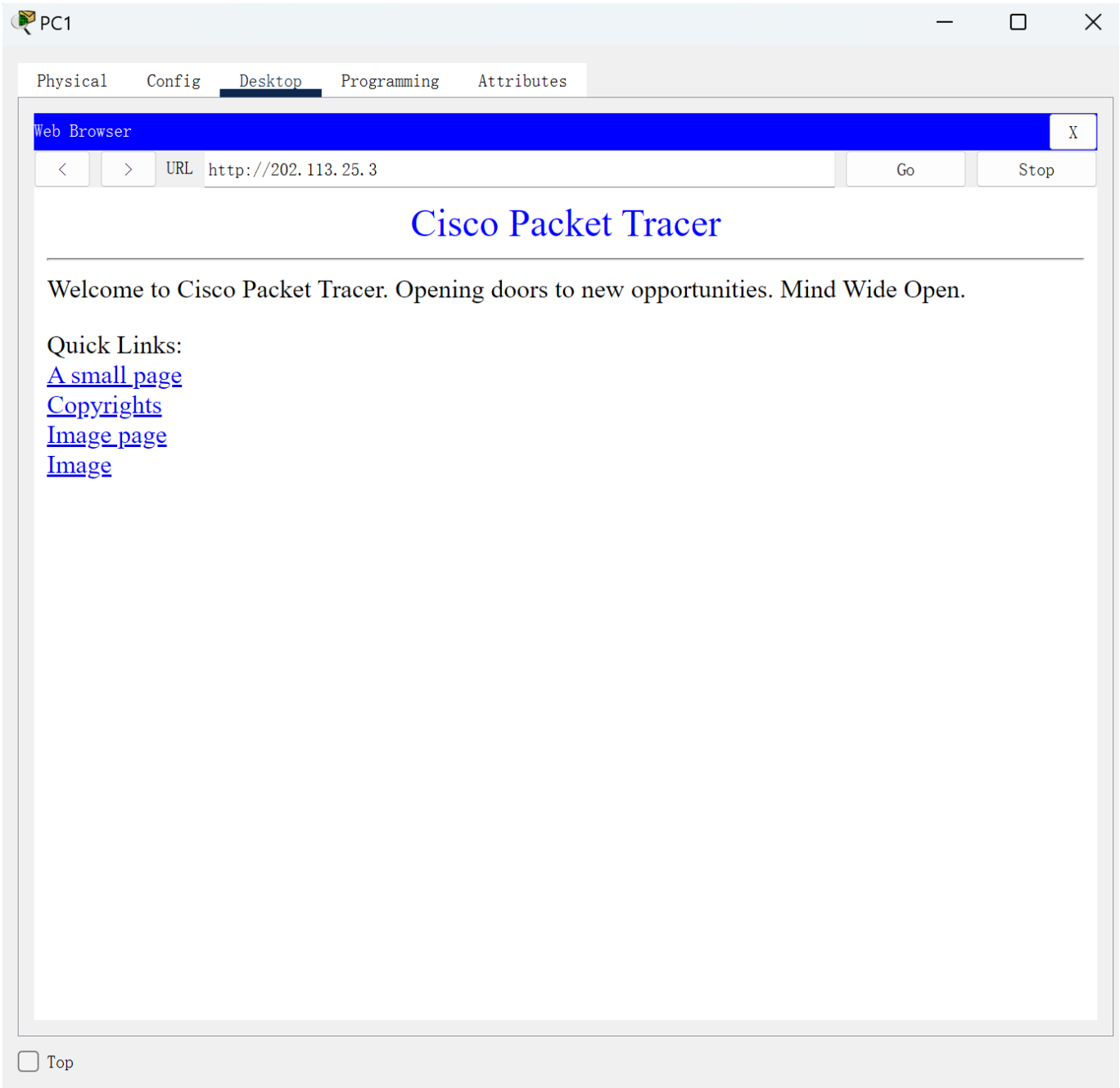


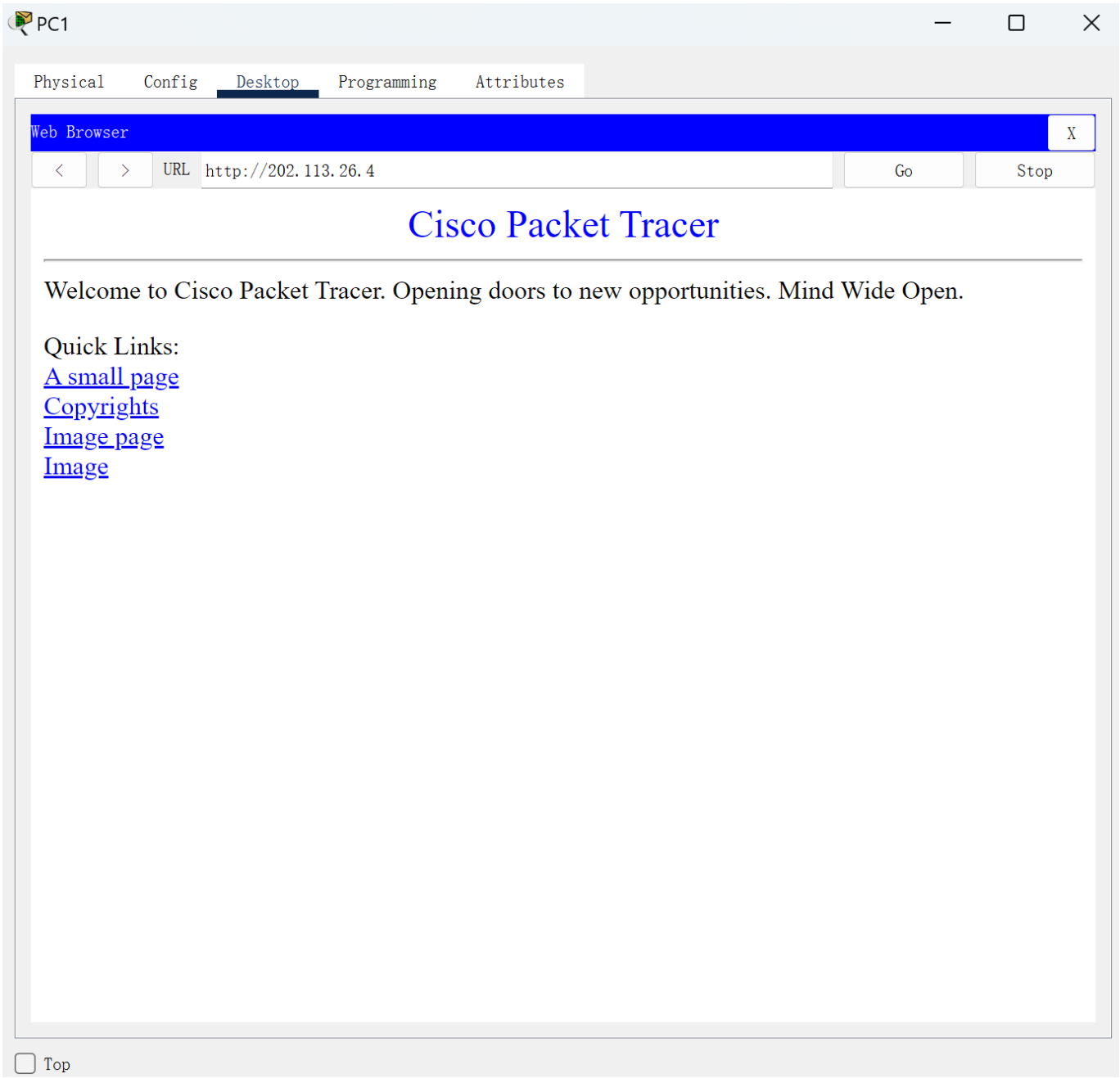
3.2路由器R0配置

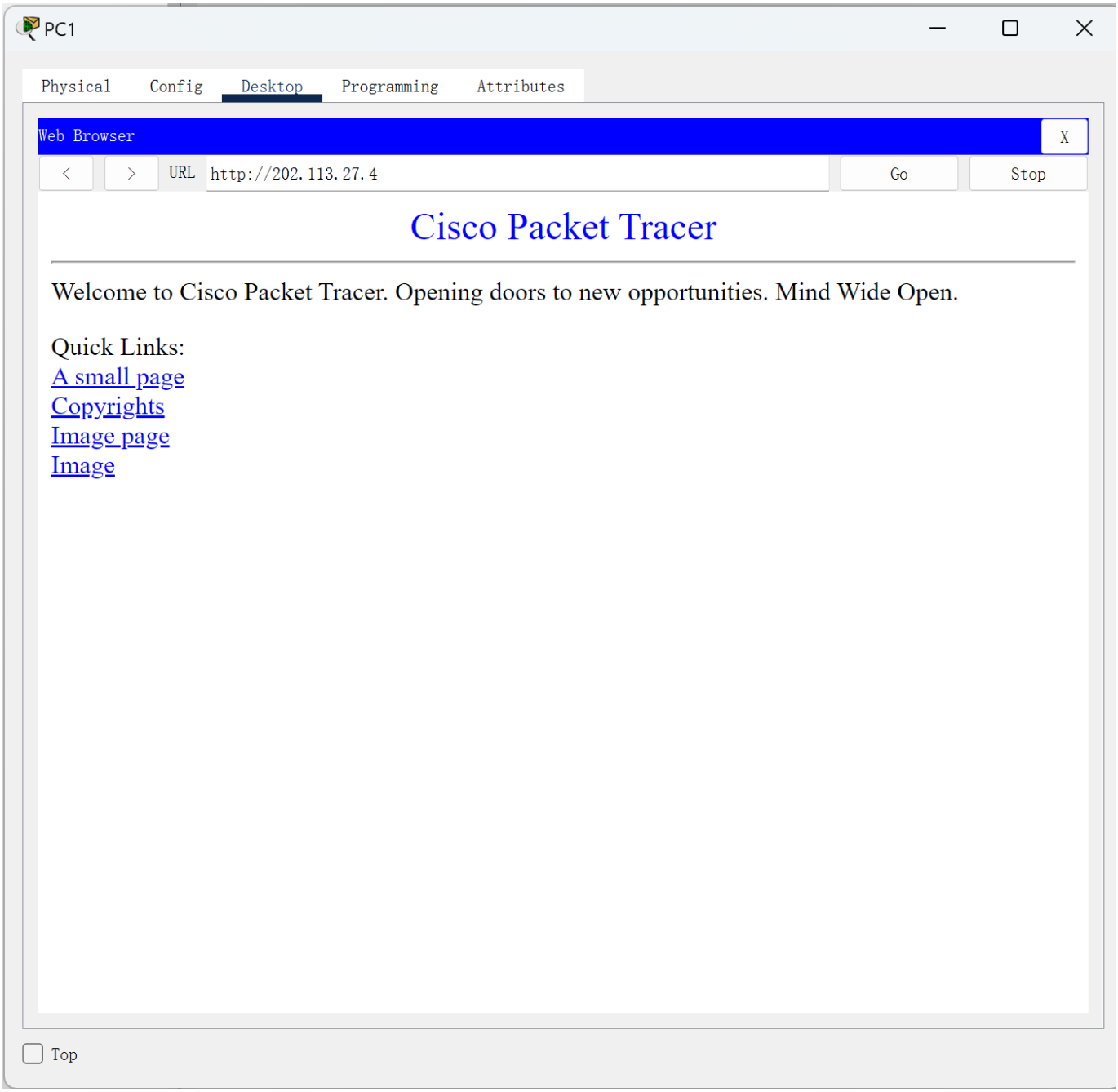
```
Router(config)#access-list 102 deny tcp any host 202.113.25.3 eq 80
Router(config)#access-list 102 permit ip any any
Router(config)#interface fa0/1
Router(config-if)#ip access-group 102 in
Router(config-if)#exit
```

3.3实验结果

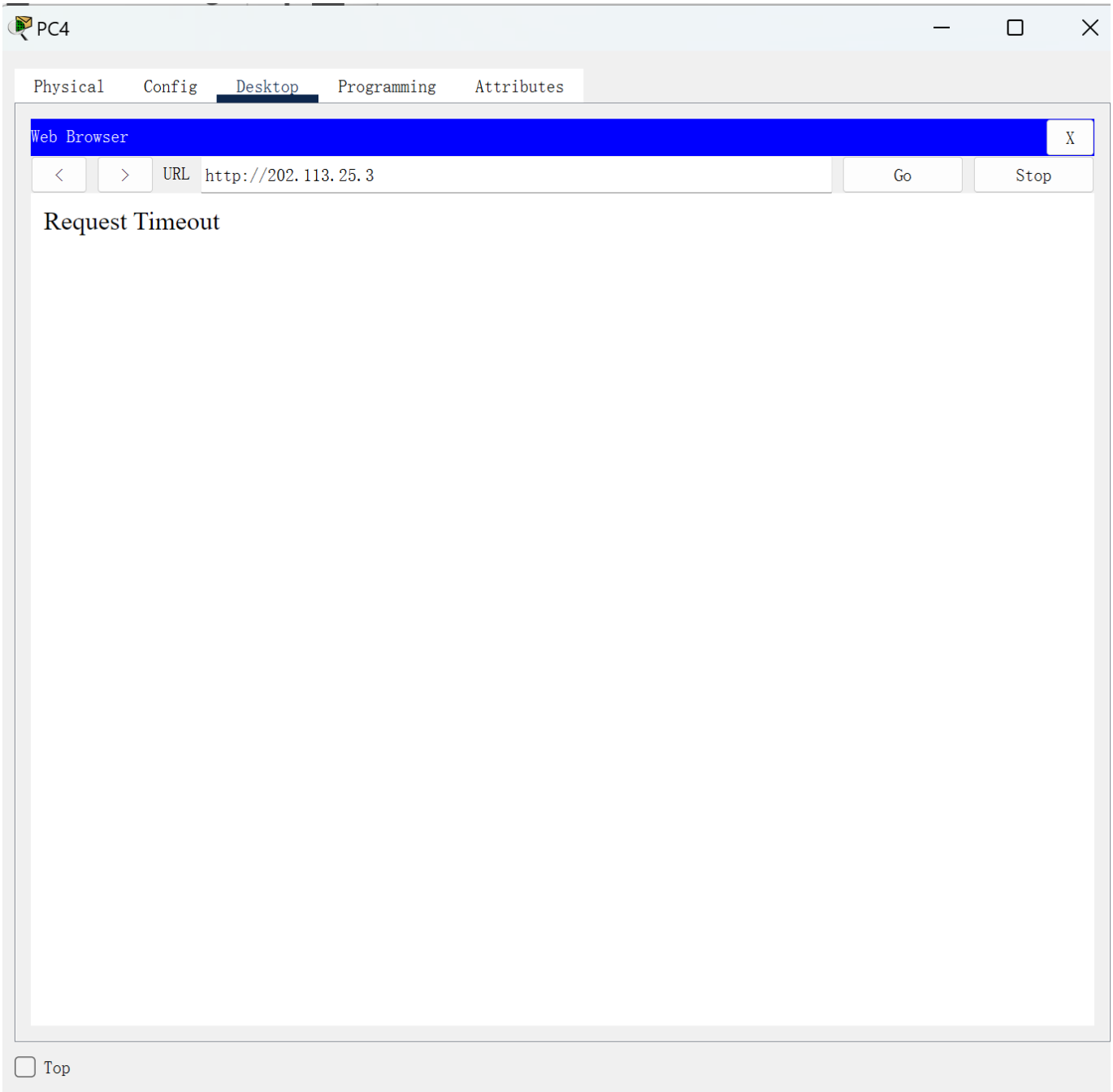
网络A中的主机可以访问三个网络中的web服务器：

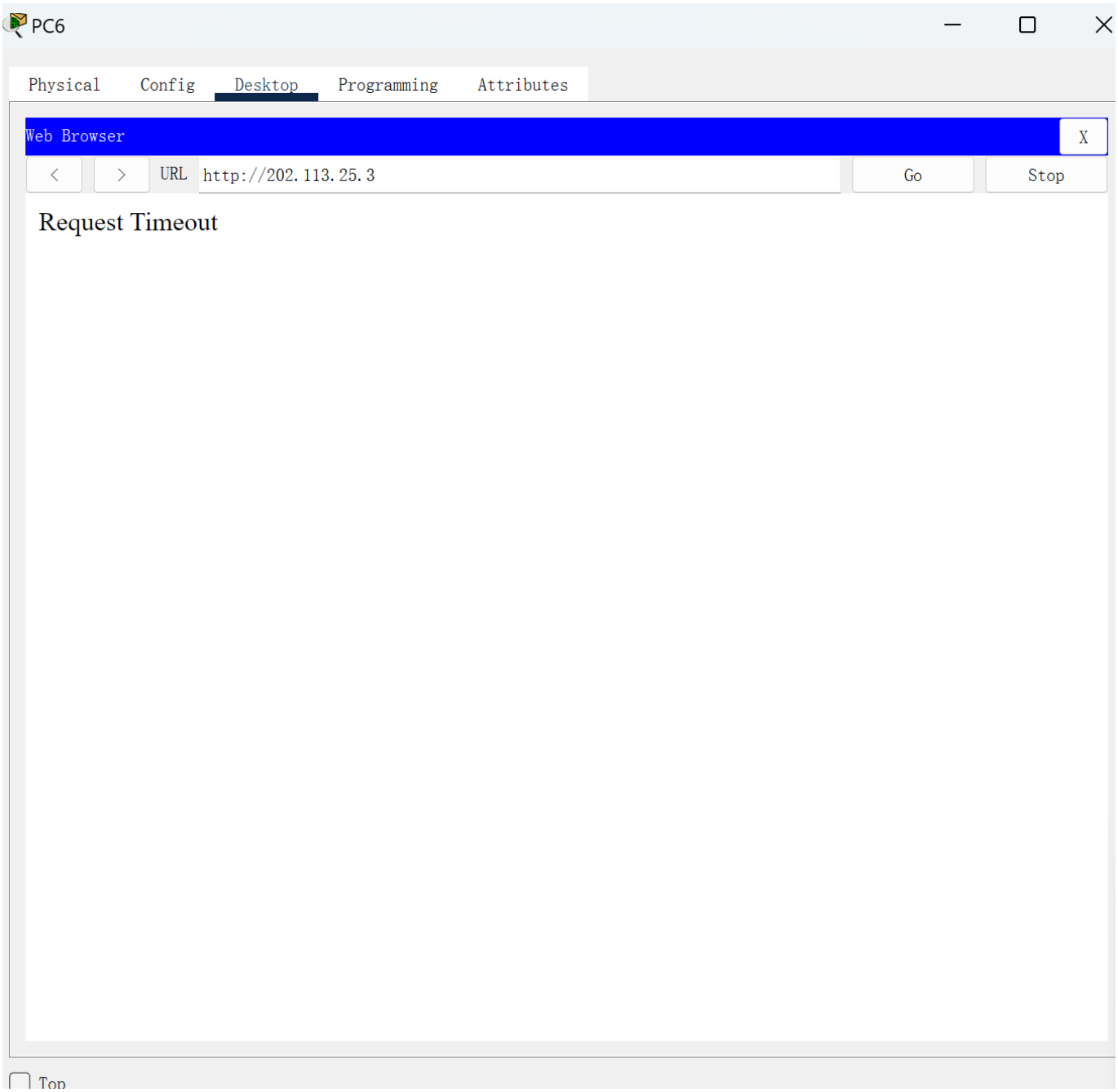

PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
URL
http://202.113.25.3
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Top


PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
URL
http://202.113.26.4
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Top



- 网络B和网络C的主机无法访问网络A的web服务器：


PC4
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
URL
http://202.113.25.3
Go
Stop
Request Timeout
Top


PC6
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
URL
http://202.113.25.3
Go
Stop
Request Timeout
Top

实验完成!