网络技术与应用第七次实验报告

物联网工程 2211999 邢清画

一、实验名称

实验7—防火墙的配置

二、实验要求

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。

三、实验内容

3.0 实验准备

1. 包过滤防火墙的基本配置方法

包过滤防火墙（Packet Filtering Firewall）是一种基于预定规则检查每个数据包的网络设备。其工作原理是通过查看数据包的头部信息（如源IP地址、目的IP地址、协议类型、端口号等）来判断是否允许或拒绝该数据包的传输。

基本配置命令和过程：

- 访问控制列表（ACL）：用于定义允许或拒绝的流量规则。ACL基于数据包的来源、目的、协议类型、端口号等信息进行过滤。

  配置ACL的基本命令格式：

```
access-list [ACL编号] [permit|deny] [源地址] [通配符掩码] [协议] [目的地址] [目的端口]
```

激活ACL：

```
interface [接口名称]
ip access-group [ACL编号] in|out
```

配置步骤：

1. 创建标准或扩展ACL。
2. 将ACL应用于接口（入站或出站）。
3. 配置规则，以允许或拒绝流量。

2. 利用标准ACL限制访问

标准ACL主要通过源IP地址进行过滤，因此它只能控制来源地址。通过配置标准ACL，可以限制某个网络中的主机访问另一个网络中的资源。

标准ACL的配置：

标准ACL使用简单的IP地址过滤规则，通常应用在入站流量的过滤上。例如，允许来自某个网络的流量进入特定的目标网络：

示例配置：

```
access-list 1 permit 192.168.1.0 0.0.0.255
interface GigabitEthernet0/0
ip access-group 1 in
```

这条规则表示允许源IP地址在 `192.168.1.0/24` 网络范围内的主机访问目标网络。

3. 利用扩展ACL拒绝特定主机访问Web服务器

扩展ACL允许根据更多的条件（如源IP地址、目标IP地址、协议类型、端口号等）来进行更加细粒度的流量控制。在此实验中，需要拒绝某个特定主机访问Web服务器，可以通过指定IP地址和Web服务器的端口（通常是HTTP端口80）来配置。

扩展ACL的配置：

- 配置拒绝特定主机访问Web服务器：

```
access-list 100 deny ip host 192.168.1.10 host 10.0.0.5
access-list 100 permit ip any any
interface GigabitEthernet0/0
ip access-group 100 in
```

这条规则拒绝IP地址为 `192.168.1.10` 的主机访问Web服务器（IP地址 `10.0.0.5`），而允许其他所有流量。

4. 内网与外网的TCP连接控制

在实验中，需要配置防火墙以允许内网用户向外网发起TCP连接并接收外网的TCP应答数据包，但不允许外网用户主动向内网发起TCP连接。这个需求可以通过配置扩展ACL来实现。

配置要求：

- **允许内网用户向外网发起TCP连接：** 内网的TCP流量可以使用 `permit` 规则进行允许，确保可以建立连接。

```
access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq www
access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq https
```

上述规则允许内网 `192.168.1.0/24` 网络的主机访问外网的HTTP（端口80）和HTTPS（端口443）服务。

- **允许接收外网的TCP应答数据包：** 需要配置允许外网响应内网的连接请求，并通过状态检查确保只允许应答数据包进入。

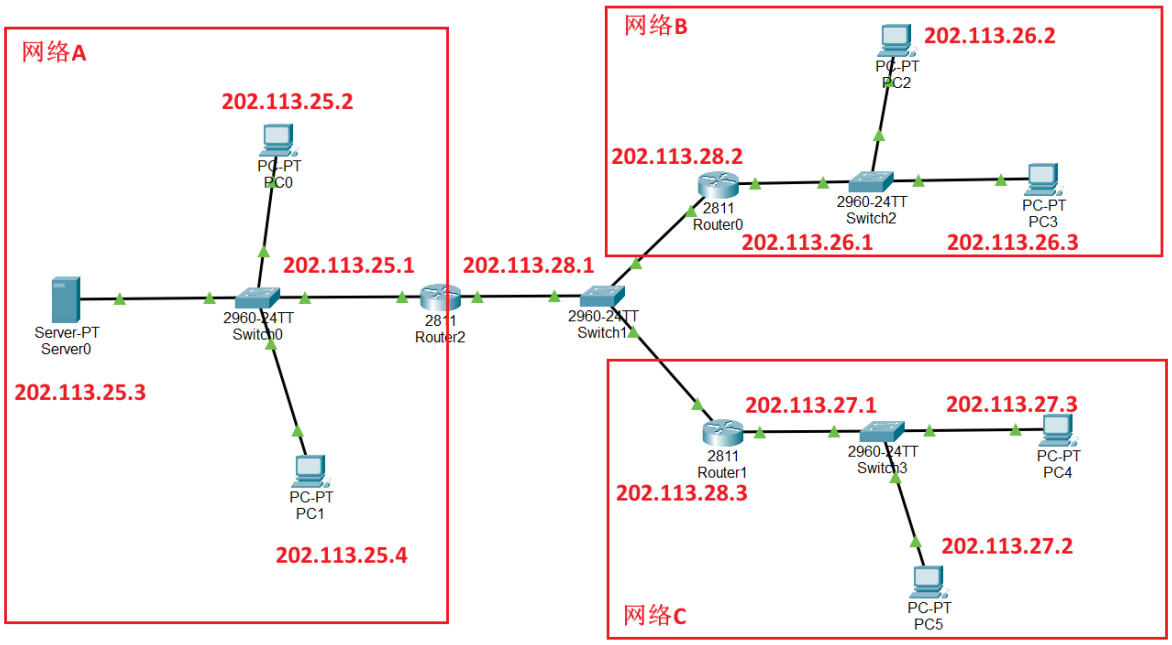
```
access-list 110 permit tcp any 192.168.1.0 0.0.0.255 established
```

- **不允许外网用户向内网发起TCP连接：** 防止外部用户主动发起TCP连接到内网，可以配置拒绝外网流量直接进入内网。

```
access-list 110 deny tcp any 192.168.1.0 0.0.0.255
```

3.1 设计网络拓扑图

按下图所示连接线路：



IP配置信息：

设备	IP地址	子网掩码	默认路由
PC0	202.113.25.2	255.255.255.0	202.113.25.1
PC1	202.113.25.4	255.255.255.0	202.113.25.1
PC2	202.113.26.2	255.255.255.0	202.113.26.1
PC3	202.113.26.3	255.255.255.0	202.113.26.1
PC4	202.113.27.3	255.255.255.0	202.113.27.1
PC5	202.113.27.2	255.255.255.0	202.113.27.1

服务器配置信息：

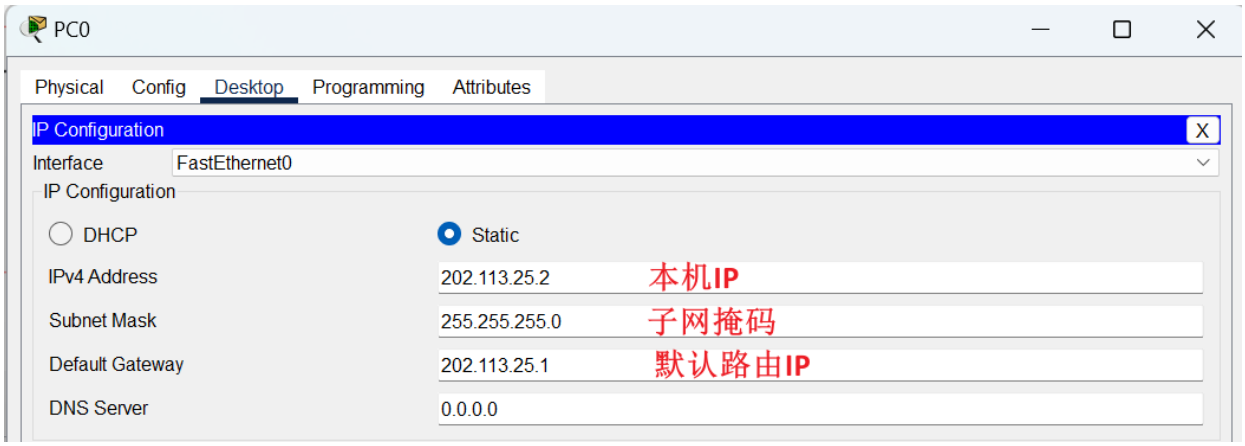
设备	IP地址	子网掩码	默认路由
Server0	202.113.25.3	255.255.255.0	202.113.25.1

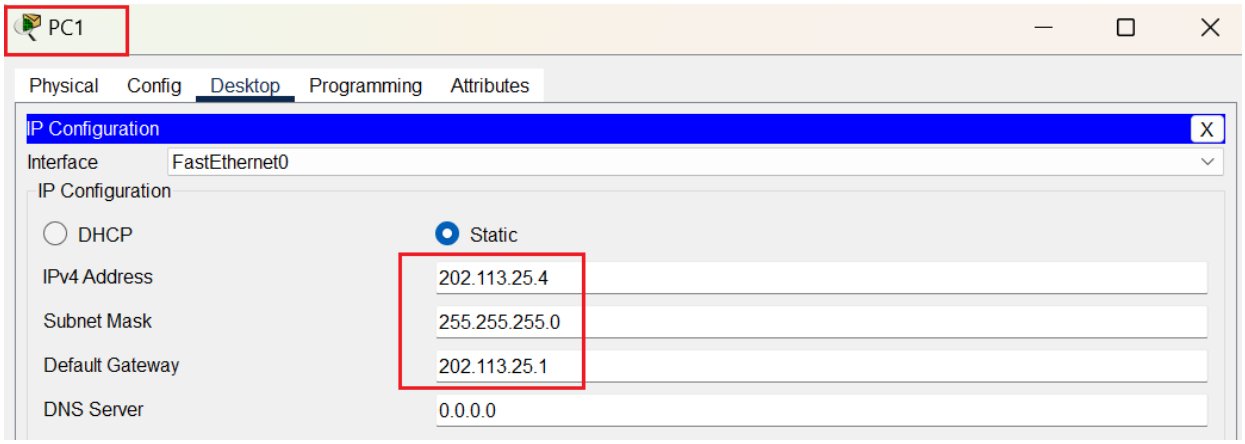
路由器端口配置：

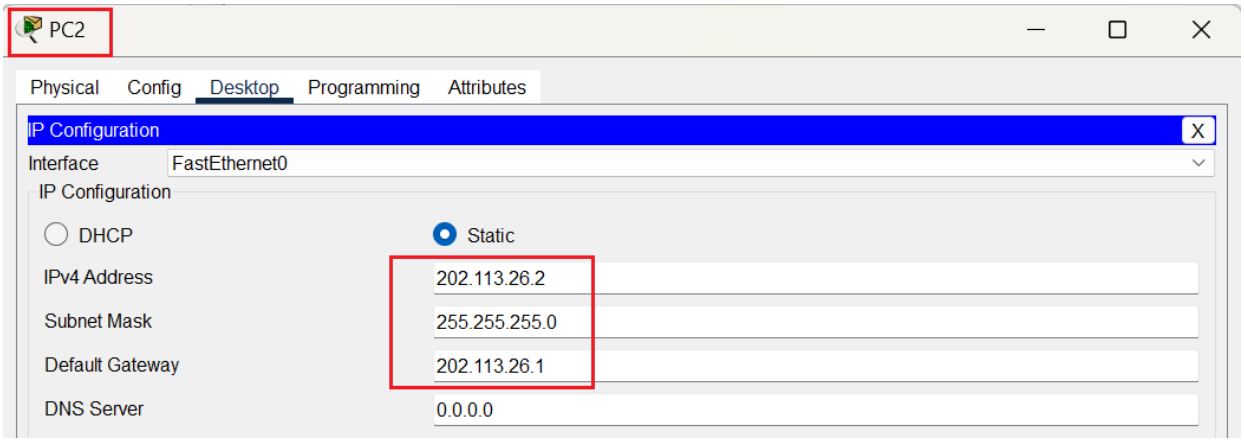
设备	端口IP（interface0/0）/子网掩码	端口Ip（interface0/1）/子网掩码
Router0	202.113.28.2/255.255.255.0	202.113.26.1/255.255.255.0
Router1	202.113.28.3/255.255.255.0	202.113.27.1/255.255.255.0
Router2	202.113.25.1/255.255.255.0	202.113.28.1/255.255.255.0

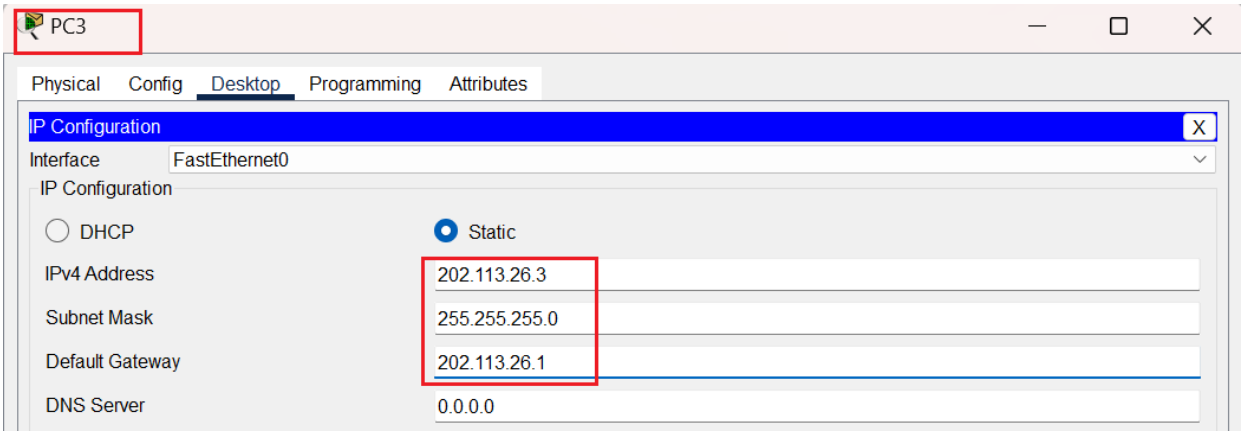
3.2 设置PC端信息

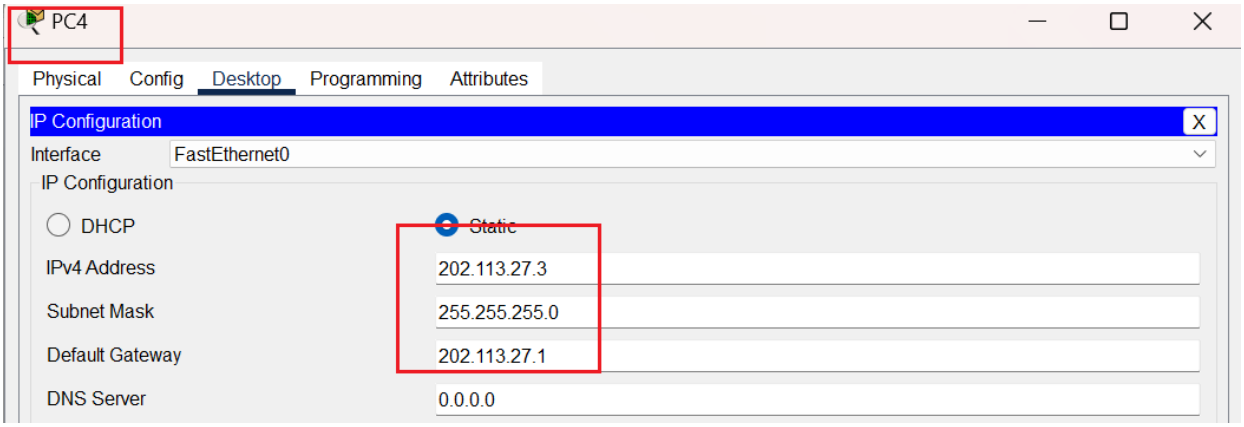
对于PC端更改IP地址、子网掩码、默认路由：

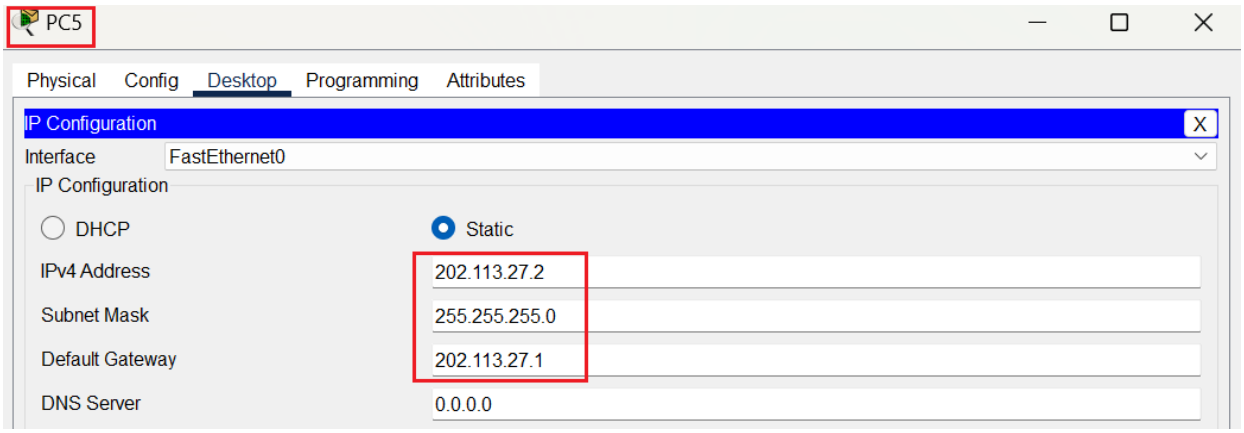





PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
202.113.26.2
Subnet Mask
255.255.255.0
Default Gateway
202.113.26.1
DNS Server
0.0.0.0

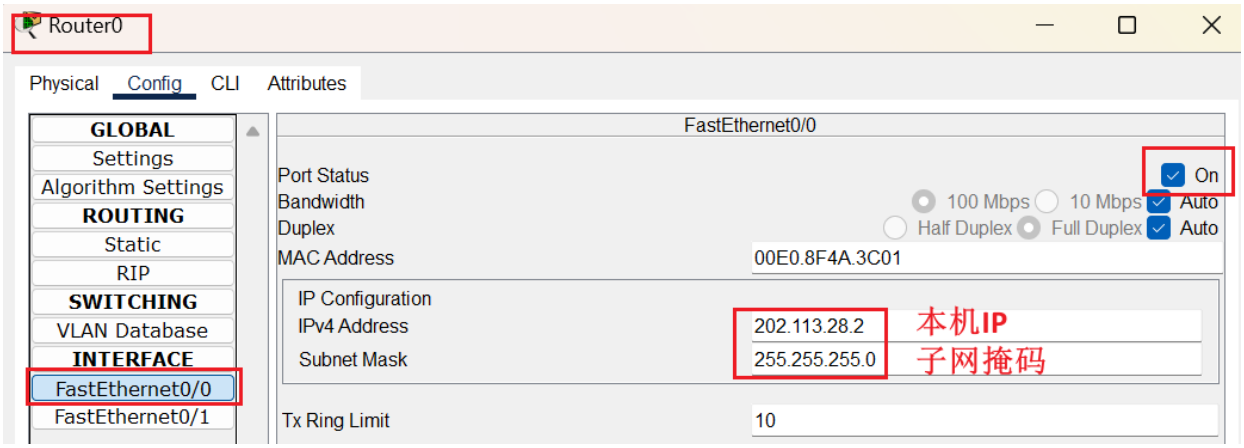

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
202.113.26.3
Subnet Mask
255.255.255.0
Default Gateway
202.113.26.1
DNS Server
0.0.0.0

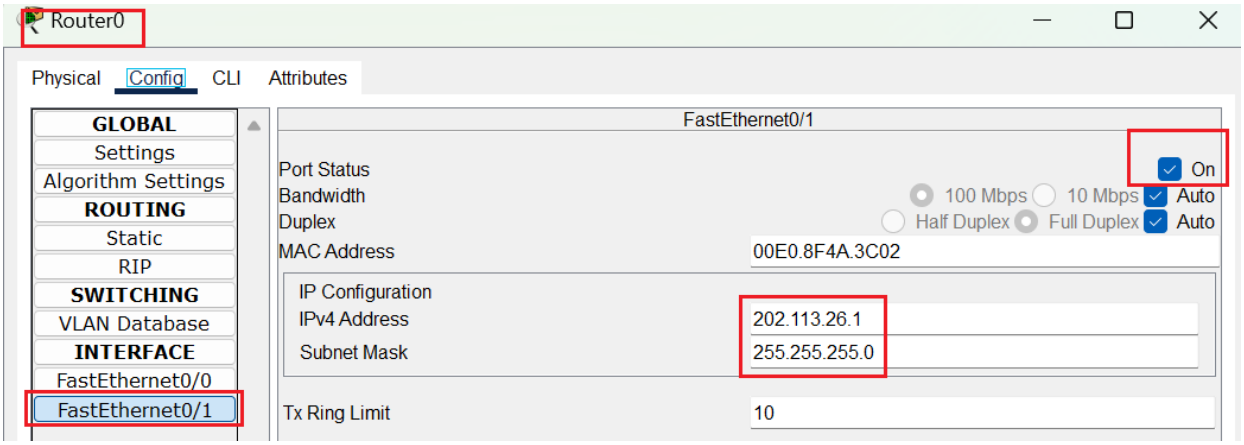

PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
202.113.27.3
Subnet Mask
255.255.255.0
Default Gateway
202.113.27.1
DNS Server
0.0.0.0


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
202.113.27.2
Subnet Mask
255.255.255.0
Default Gateway
202.113.27.1
DNS Server
0.0.0.0

3.2 设置路由器信息

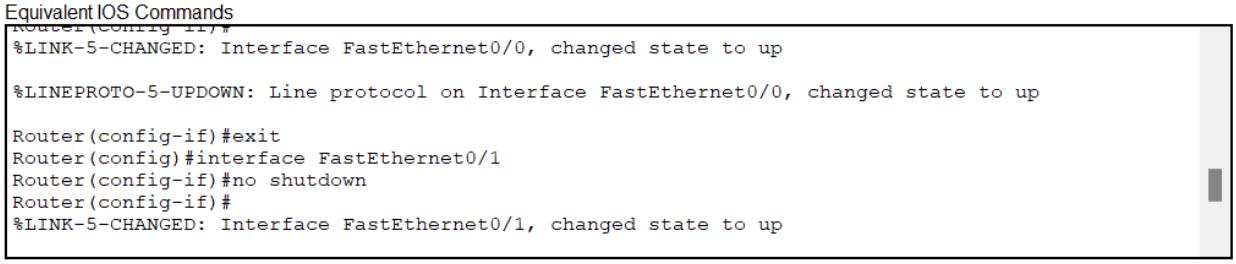
对于路由器更改IP地址、子网掩码、静态路由、同时要设置路由转发表：



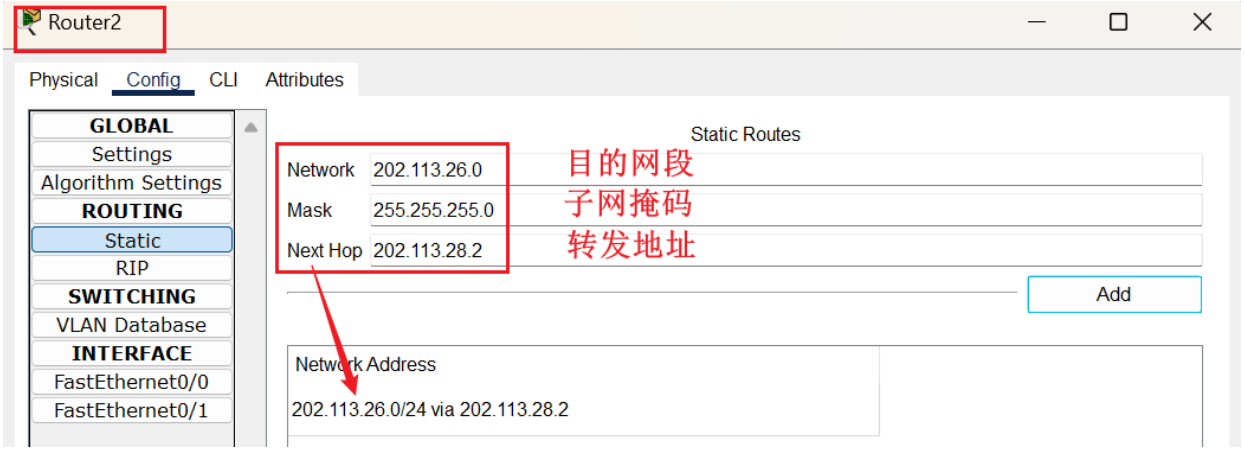


或使用终端命令行：

```
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
```

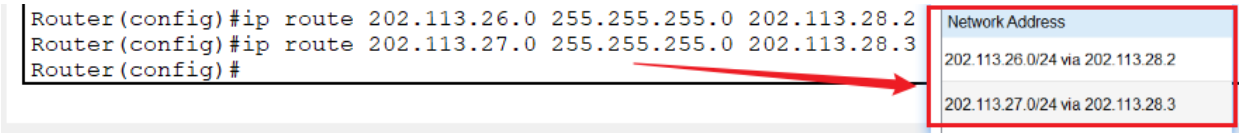


在**Static**中添加静态路由转发表：

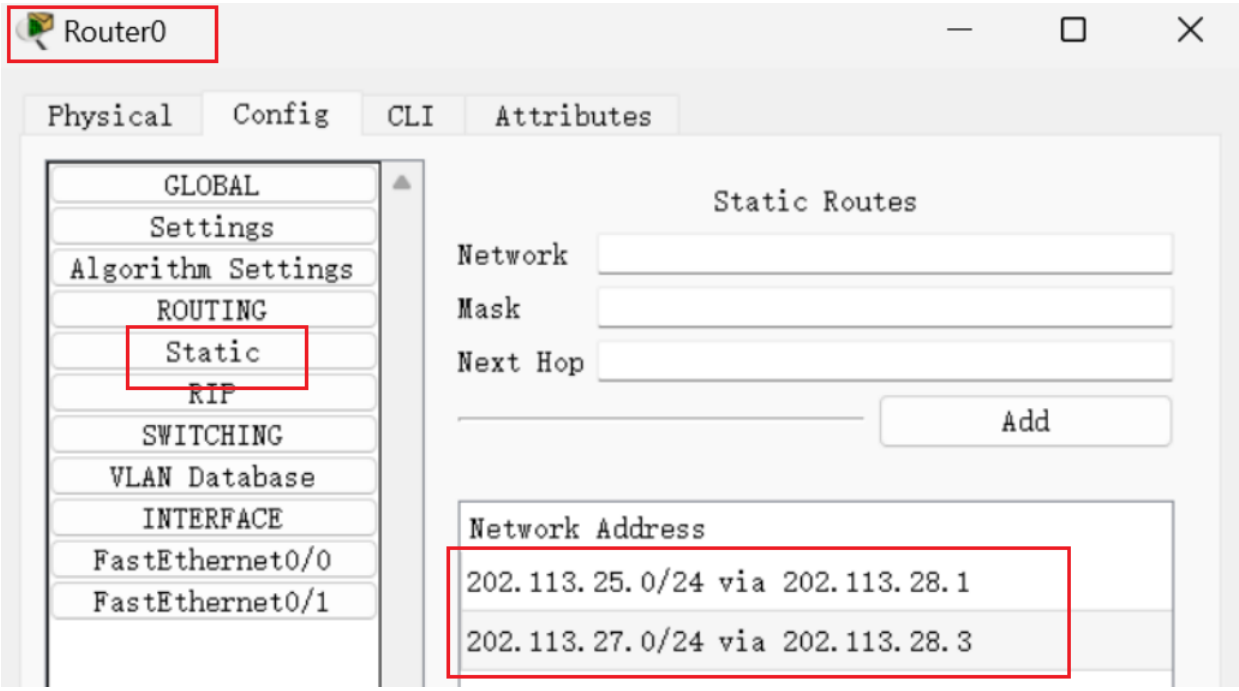


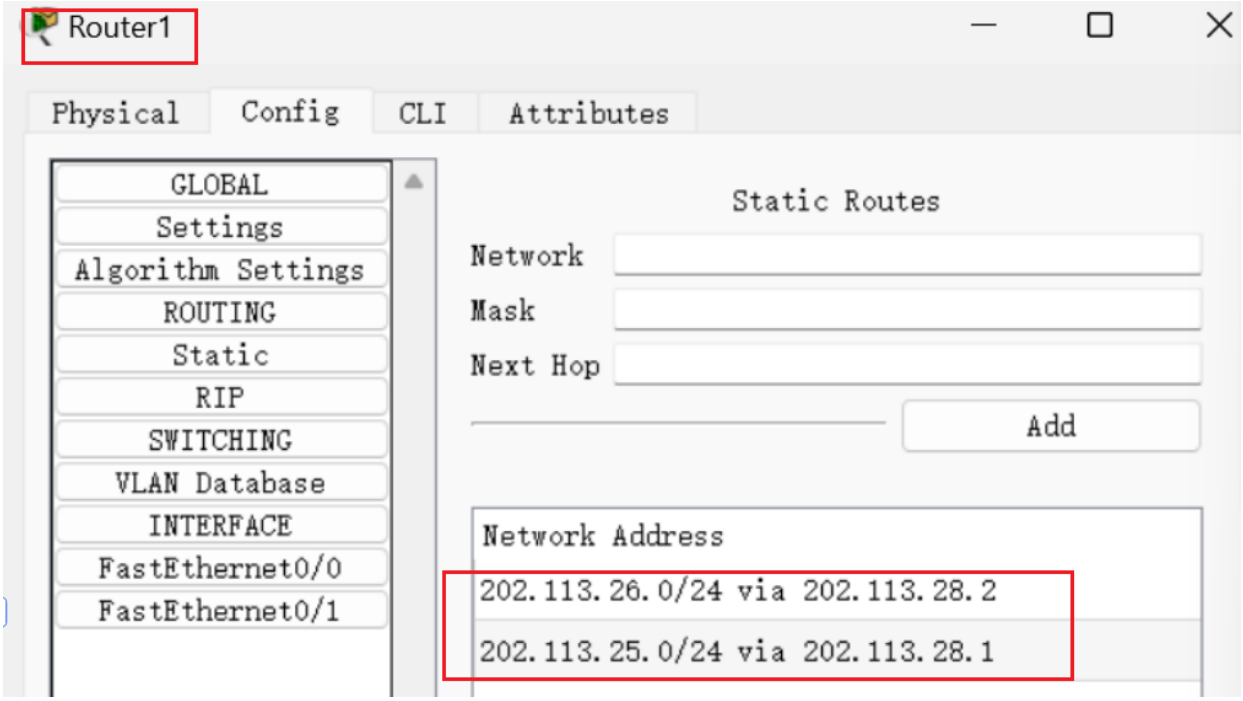
或使用终端命令行：

```
Router(config)#ip route 202.113.26.0 255.255.255.0 202.113.28.2
Router(config)#ip route 202.113.27.0 255.255.255.0 202.113.28.3
```



类似的操作去配置**Router0,Router1**：





3.4 防火墙配置

将防火墙配置为只允许网络2中的主机访问网络1，网络1拒绝网络3访问：

配置ACL，使得网络1允许网络2中的主机访问，但不允许网络C中的主机访问。

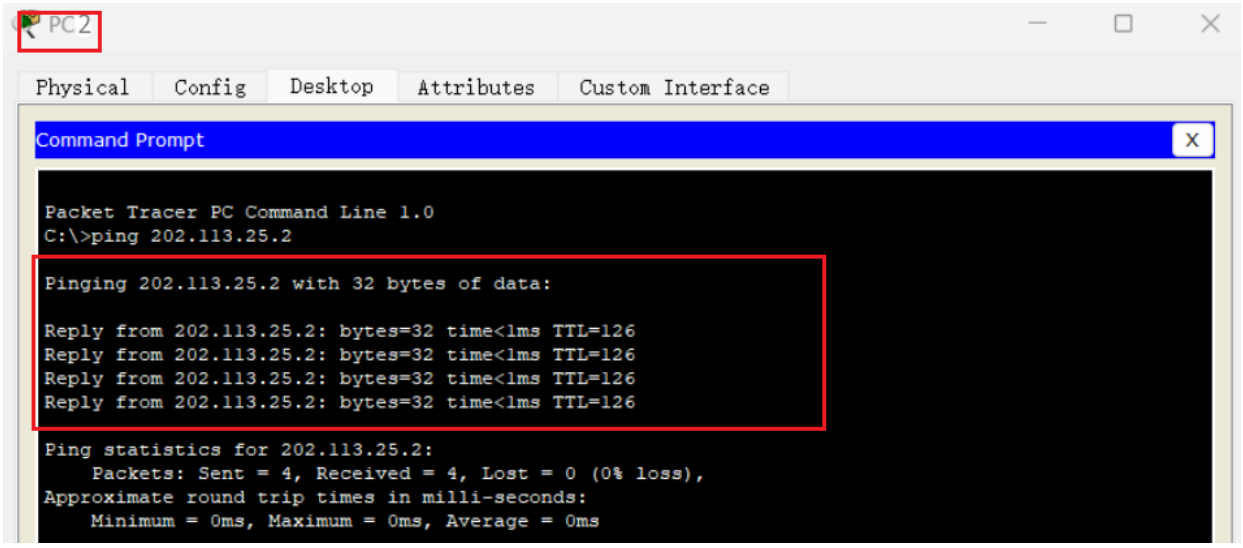
在Router0的全局配置模式下使用如下命令建立一个标号为6、包含两条规则的标准ACL，接着进入Fa0/1接口配置模式，利用将6号ACL绑定在Fa0/1的入站上。

在使用该语句之前发现网络3中的主机可以连通

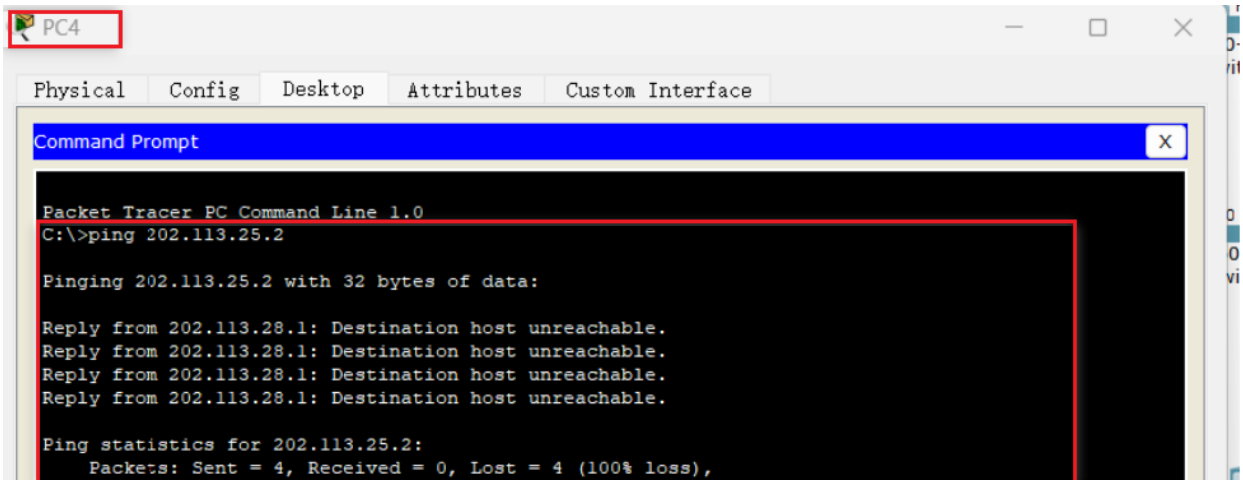
```
access-list 6 permit 202.113.26.0 0.0.0.255
access-list 6 deny any # 拒绝其他所有访问
interface fa0/1
ip access-group 6 in
```

```
Router(config-if)#exit
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
```

使用网络2中的PC2访问发现可以连通：



使用网络1中的PC4访问发现不能连通：



3.5 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

配置ACL，使得除了网络2中的PC3，其他都能访问网络1中的HTTP服务

首先要先取消上一个实验中的ACL配置，使用如下语句取消6号ACL的应用并删除6号ACL

```
enable
configure terminal
interface fa0/1
no ip access-group 6 in # 解除ACL绑定
no access-list 6 # 删除6号ACL
```

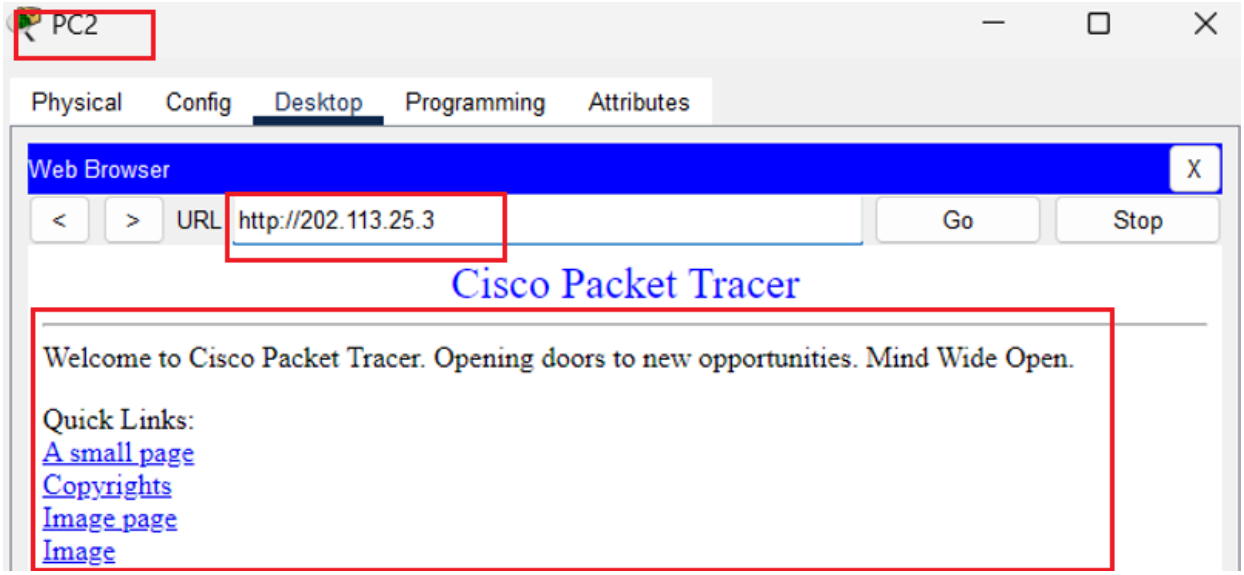
```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/1
Router(config-if)#no ip access-group 6 in
Router(config-if)#no access-list 6
```

使用如下语句设置ACL规则，拒绝202.113.26.2的主机IP访问IP是202.113.25.3的服务器：

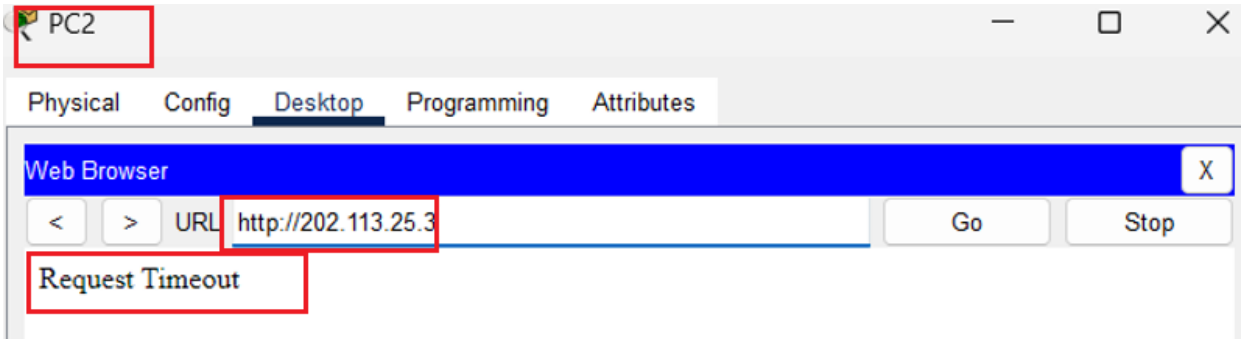
```
access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 eq www
access-list 106 permit ip any any
interface fa0/1
ip access-group 106 in
```

```
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)#
```

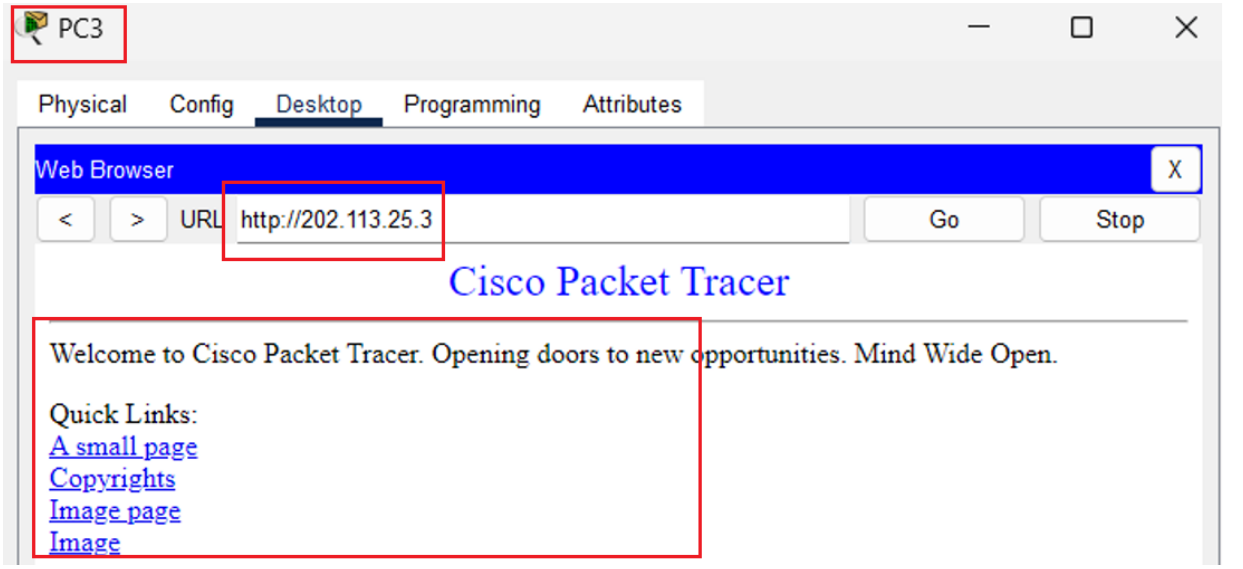
应用规则之前发现**PC2**可以正常访问：

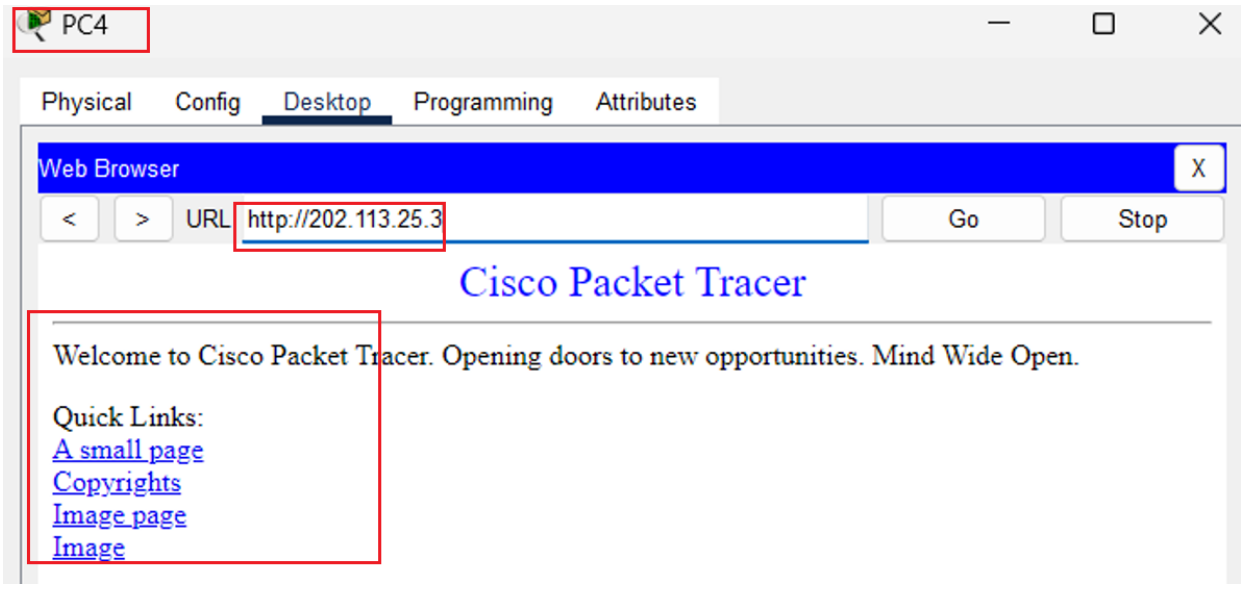


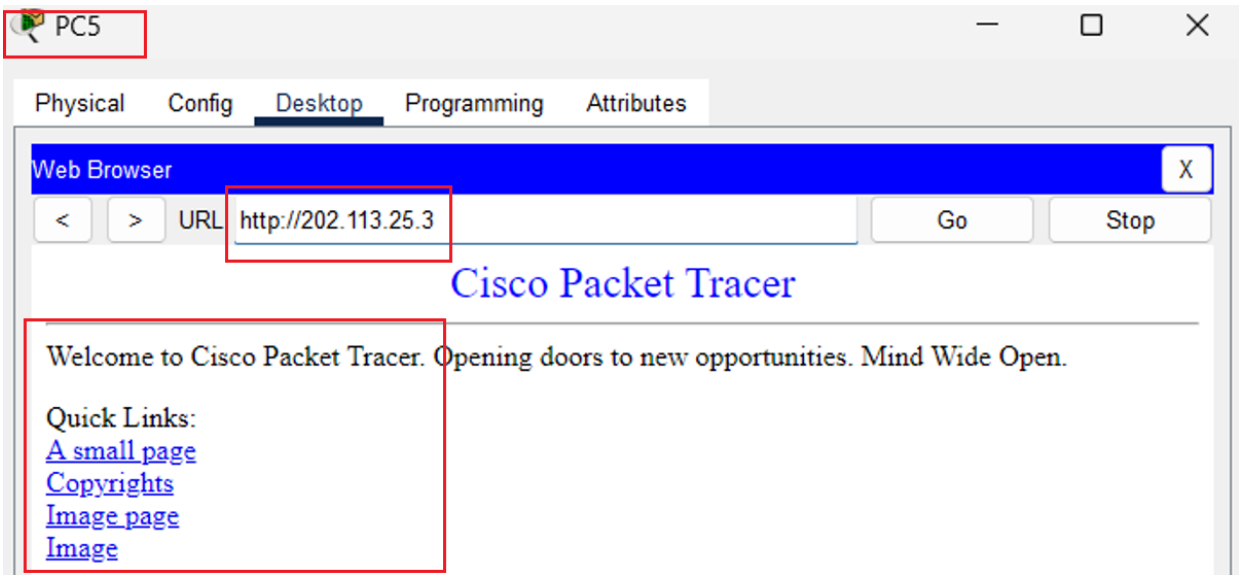
应用规则后发现**PC2**不能访问



访问其他主机如**PC3**、**PC4**、**PC5**都正常显示界面


PC3
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

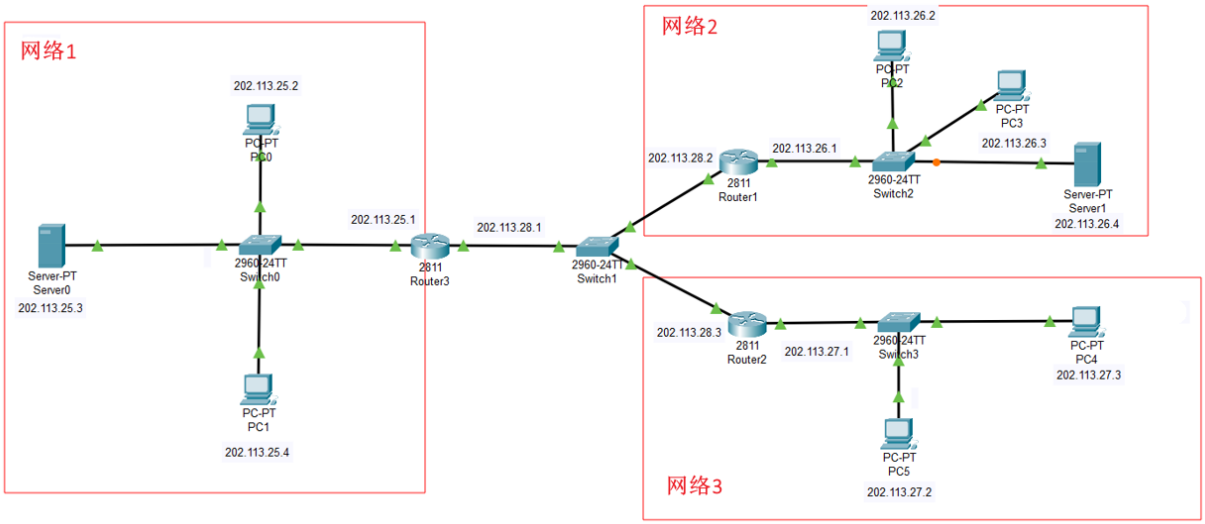

PC4
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://202.113.25.3
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


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

3.6 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。但不允许外网的用户主动向内网发起TCP连接。

首先清除以上所有规则，并按照如下拓扑图修改：

```
configure terminal
interface fa0/1
no ip access-group 106 in  # 解除ACL绑定
no access-list 106  # 删除106号ACL
```



输入以下命令创建了一个名为 **101** 的访问控制列表。这个列表包含三个规则：

(1)允许内网用户向外网发起**TCP**连接，并且只允许与已经建立的连接相关的流量通过。

(2)允许外网发回的**TCP**应答数据包通过。

(3)阻止外网用户向内网发起**TCP**连接。

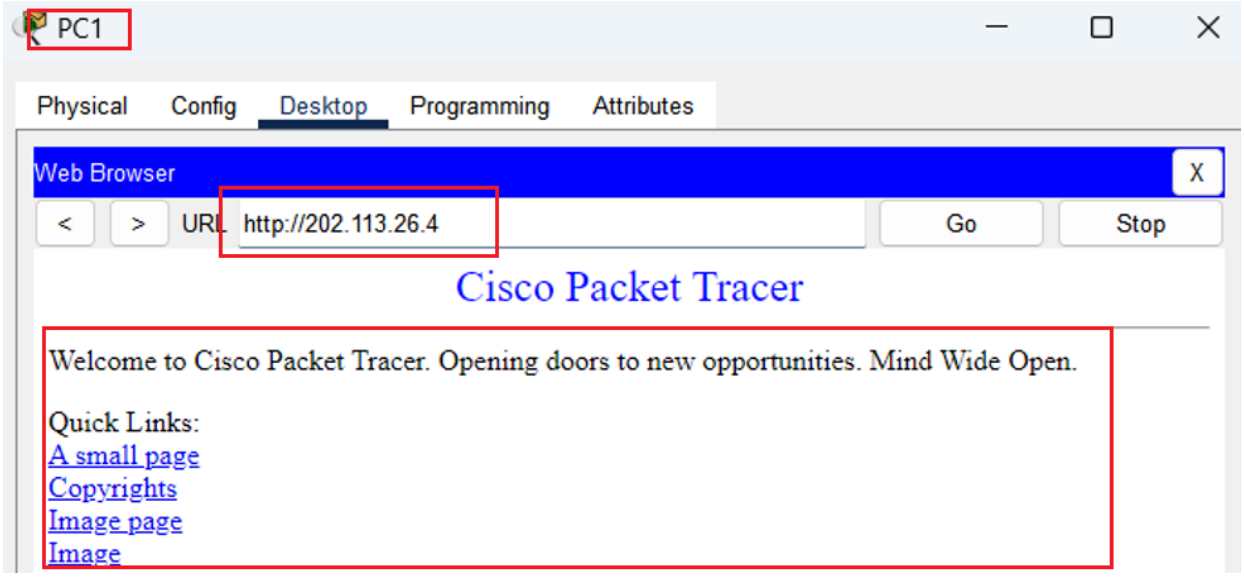
然后将该规则应用到指定接口上即可：

```
access-list 101 permit tcp 202.113.25.0 0.0.0.255 any established
access-list 101 permit tcp any any established
access-list 101 deny tcp any 202.113.25.0 0.0.0.255
Interface fa0/1
Ip access-group 101 in
```

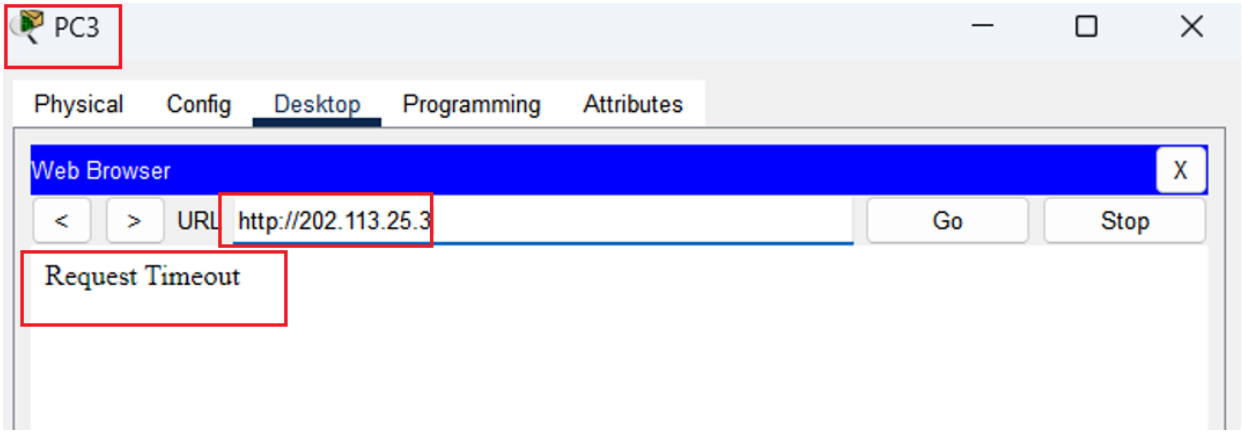
```
Router(config)#access-list 101 permit tcp 202.113.25.0 0.0.0.255 any
established
Router(config)#access-list 101 permit tcp any established

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

发现内网的**PC1**可以访问外网的服务器**IP 202.113.26.4:**



使用外网的**PC3**不可以访问内网服务器**IP 202.113.25.3:**



四、实验总结

本次实验通过配置包过滤防火墙，深入掌握了标准**ACL**和扩展**ACL**的基本配置方法与应用场景，进一步理解了它们在实际网络安全中的重要作用。在实验过程中，我成功实现了对不同网络之间访问的精确控制，具体包括限制特定网络或主机的访问权限，以及根据协议和端口号对流量进行复杂的过滤。通过使用标准**ACL**，我配置了仅允许指定网络访问目标资源的规则；而在使用扩展**ACL**时，我能够实现更细粒度的访问控制，包括基于特定协议和端口号对流量进行过滤，有效提升了网络的安全性。

此外，我还配置了状态检测功能（**Stateful Inspection**），确保了内网用户能够正常发起外网的**TCP**连接并接收响应数据包，同时防止外网用户主动向内网发起连接请求。通过这种方式，我学会了如何实现内外网之间的方向性控制，保护了内网免受外部不必要的访问。

整个实验过程加深了我对**ACL**和防火墙核心功能的理解，使我掌握了如何根据实际需求设计和配置安全策略。这些技能不仅为我提供了理论上的知识支持，也为我未来在实际网络环境中配置和管理防火墙，制定安全策略提供了宝贵的实践经验。

对于自反**ACL**，由于软件本身版本的问题对于**reflect**关键字不支持，所以无法实现自反的要求，对于某些原本外网无法访问内网但是内网访问外网后，外网又可以访问的自反情况，可能是软件本身的问题，路由器规则没有设置过滤，最开始的无法访问是因为软件的信息传输需要时间，所以第一次访问是无法访问的，但是如果重试就可以成功，这就导致了出现上述的情况，实际上是一种阴差阳错，而不是自反的实现。