实验7：防火墙和SSL实验

学号：2112066 姓名：于成俊 专业：密码科学与技术

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、实验理论

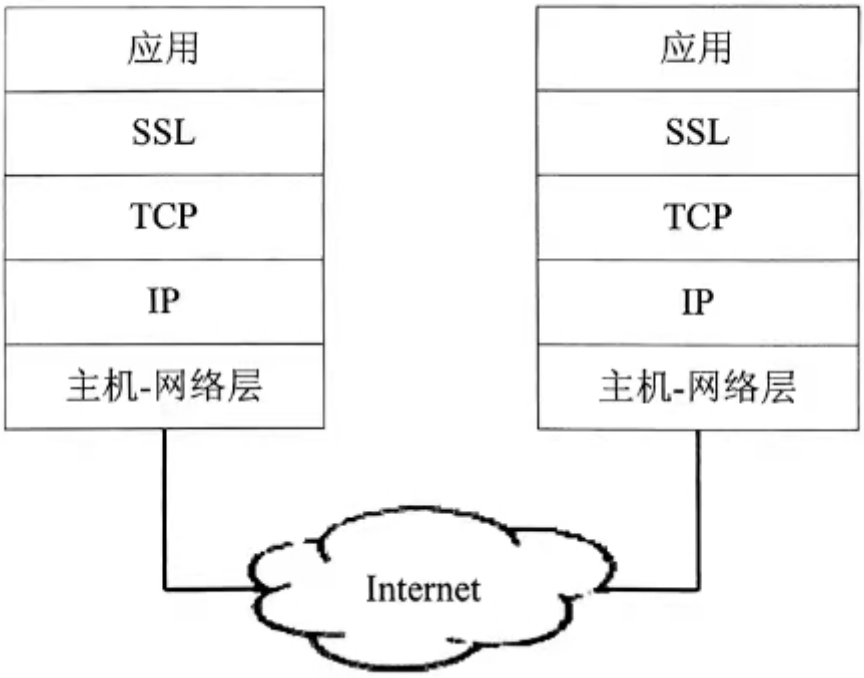
1.防火墙

防火墙是一种安全设备，它部署在内部Internet和外部Internet之间，认为内部网络是安全的和可信赖的，外部网络是不太安全的和不太可信的。通过检查和检测所有进出内部网的信息流，防火墙防止未经授权的通信进出被保护的内部网络。防火墙采用的技术主要有两种类型：

- 包过滤：采用包过滤技术的防火墙检查每个流经的IP数据包，通过匹配这些IP数据包与设定的过滤规则是否相符，不相符的话通常有两种处理方式，一种是丢弃，另一种是转发。过滤规则主要依据数据包中IP头部和TCP头部的一些字段进行编写，主要包括：
    - 源IP地址和目的IP地址
    - IP数据包协议字段
    - 源端口和目的端口号
    - TCP的ACK字段
- 应用网关：也叫应用代理，通常运行在内部网络的某些具有访问Internet权限的专用服务器上，为内部网络用户访问外部网络的一些特定服务（或为外部网络用户访问内部网络的一些特定服务）提供转接或控制。

2.SSL协议

安全套接字SSL是目前应用最广泛的安全传输协议之一。SSL运行在端系统的应用层与传输层之间，通过在TCP之上建立一个安全通道，为应用数据的传输提供安全保障。



3.访问控制列表（ACL）

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（检查从该接口发出的所有数据包）。一个ACL可以包含多条规则，网络设备通常采用**优先匹配原则**，当出站（或入站）的数据包到来时，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。如果所有规则都没有匹配成功，Cisco生产的网络设备采用丢弃的方式。ACL中的规则一般按照加入的先后顺序进行排序，先加入的在前，后加入的在后。

在Cisco网络设备中，常用的访问控制列表有两种：一种是标准ACL，另一种是扩展ACL。

- 标准ACL是最简单的一种ACL，它利用IP数据包中的**源IP地址**对过往的数据包进行控制。
- 扩展ACL是对标准ACL的扩充，可以按照**源IP地址、目的IP地址、源端口、目的端口等条件**进行ACL规则定义。
- 标准ACL的列表号的范围是1~99；扩展ACL的列表号的范围是101~199

4.反向ACL

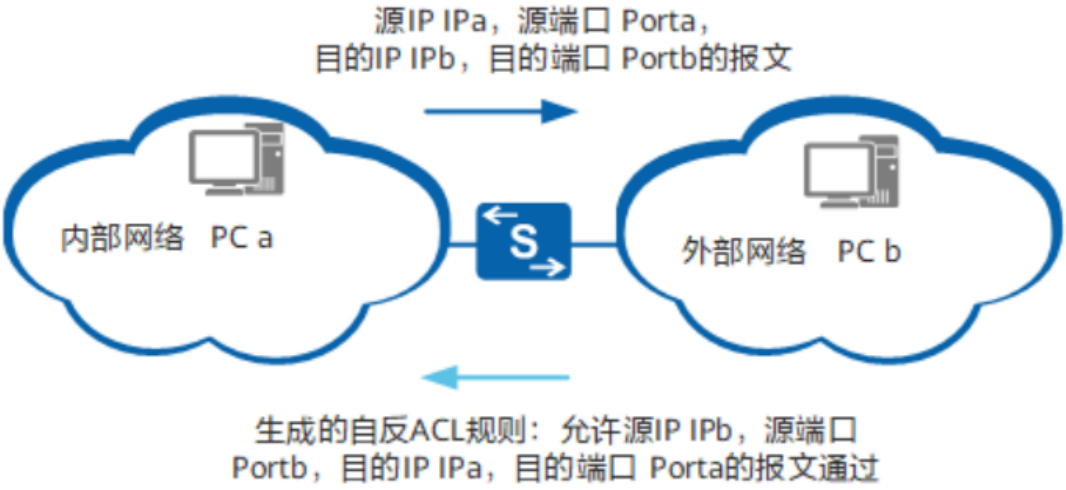
- 反向访问控制列表（Reverse Access Control List，ACL）是ACL的一种高级应用。它可以有效地防范病毒，通过配置反向ACL，可以保证A网段可以PING通B网段，而B网段不能PING通A网段。这是因为数据传输可以分为两个过程，首先是源主机向目的主机发送连接请求和数据，然后是目的主机在双方建立好连接后发送数据给源主机。反向ACL控制的就是连接请求。

- 反向ACL的格式非常简单，只要在配置好的扩展访问列表最后加上established即可。

5.自反ACL

为了**实现拓展功能。**我查找资料，发现**自反ACL**可以实现这个功能，以下是它的相关说明：

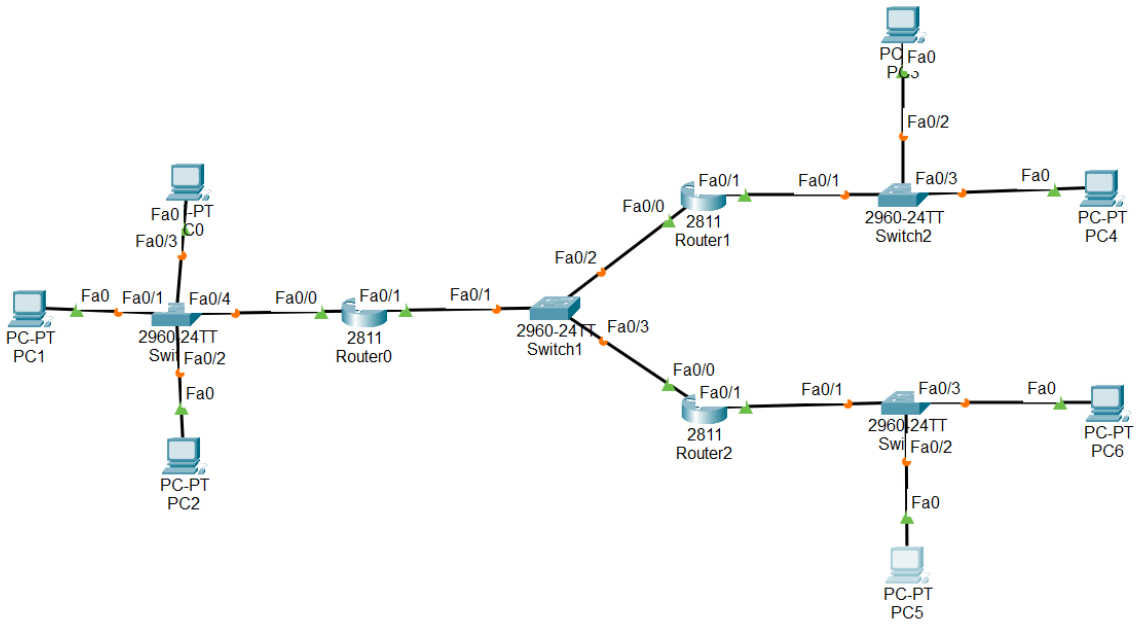
- 自反ACL（Reflective ACL）是动态ACL技术的一种应用。它根据IP报文的上层会话信息生成，只有当私网用户先访问了公网后才允许公网访问私网。利用自反ACL可以很好的保护企业内部网络，免受外部非法用户的攻击。
- 配置自反ACL之后，外网用户**主动发起**的请求报文不能进入内部网络，无法主动访问内网用户。当内网用户向外网用户主动发起请求报文之后，设备的接口会根据用户的源IP地址、目的IP地址和端口号等信息**生成一个反向的ACL**，并保持一段时间，从而允许外部网络至内网用户的回程访问。
- 如下图所示，配置自反ACL后，外网无法主动访问内网。这时，一个源IP为IPa、源端口为Porta、目的IP 为IPb、目的端口Portb的报文发往外网，设备会自动生成一条自反ACL的规则，允许源IP为IPb、源端口为Portb、目的IP为IPa、目的端口为Porta的报文通过。



三、实验过程

1. 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。

（1）我的网络拓扑图如下：



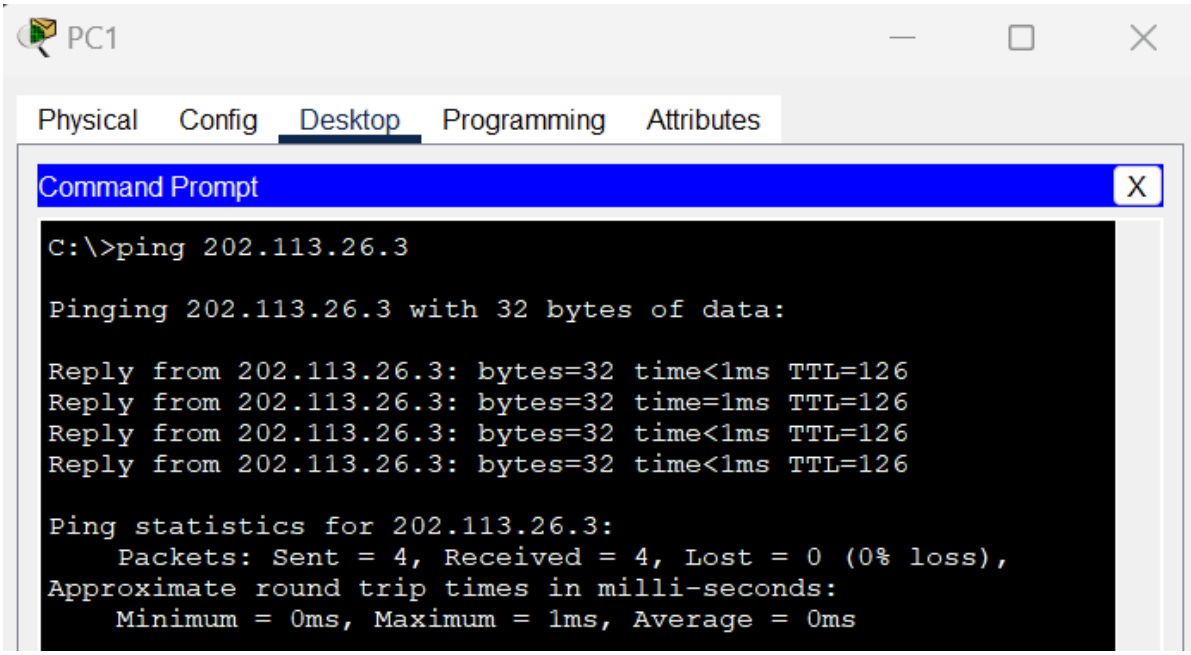
（2）分配IP地址

IP地址分配表如下：

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
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	

由于IP地址的配置并不是本次实验的重点，所以这里不再赘述。

在配置防火墙之前，需要保证所连接的设备能够ping通，如下图所示：



在PC1上 **ping** PC4，可以ping通，说明设置正确。

（3）建立标准ACL

本次实验想要实现左边的网络**允许**右上角的网络中的主机访问，但**不允许**右下角的网络，即其他网络。

为了实现上述功能，我在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：

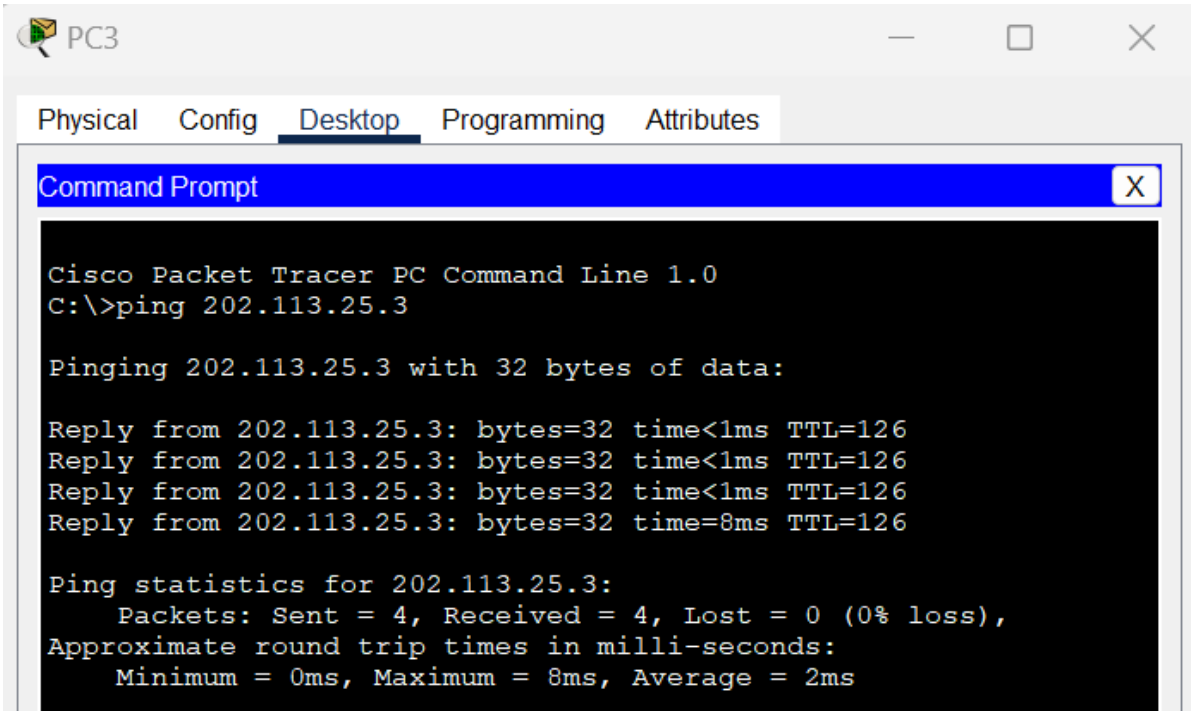
```
Router>en
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 6 permit 202.113.26.0  0.0.0.255
Router(config)#access-list 6 deny any
Router(config)#interface fa0/1
Router(config-if)#ip access-group 6 in
Router(config-if)#exit
Router(config)#
```

其中：

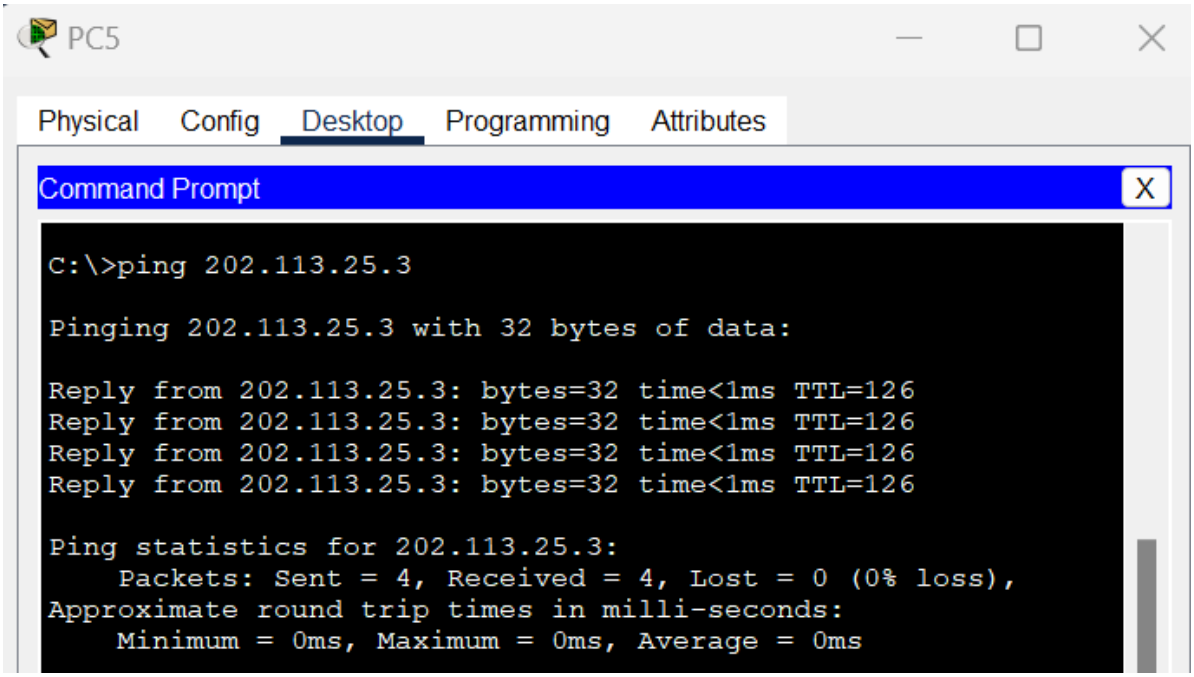
- `access-list 6 permit 202.113.26.0  0.0.0.255` 这条命令允许右上角网络中的主机发送的数据报通过。
- `access-list 6 deny any` 这条命令拒绝所有其他网络的数据报送来的数据报。
- `ip access-group 6 in` 这条命令将6号ACL绑定在fa0/1的入站上。

（4）标准ACL验证：

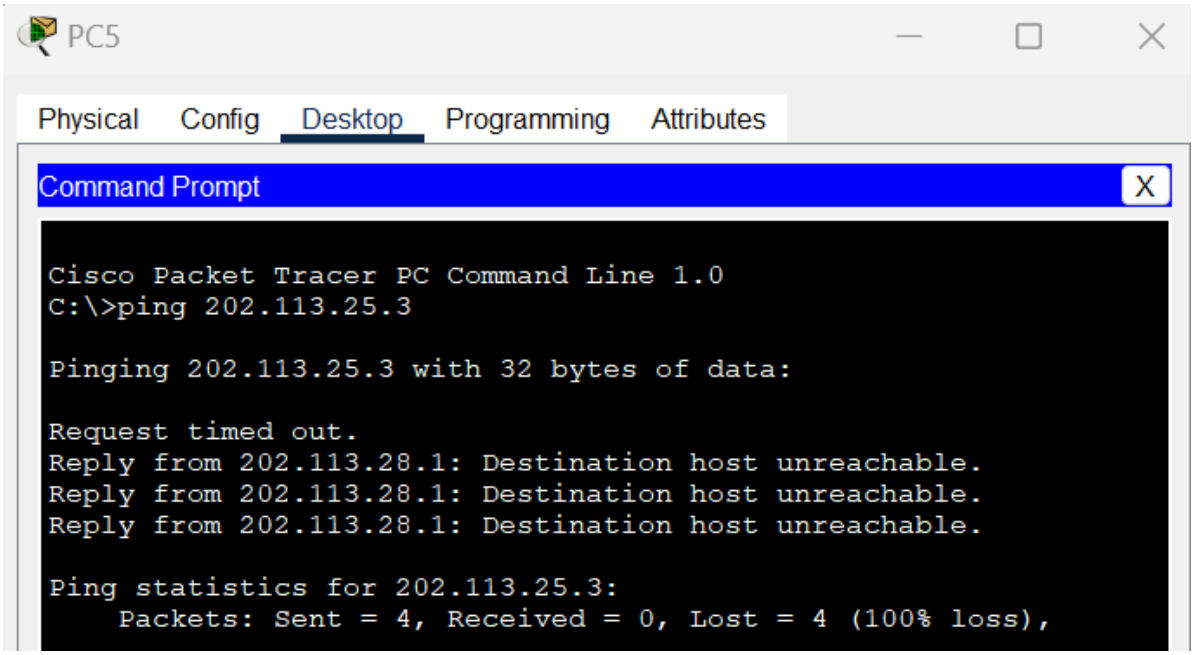
用右上角网络中的主机（PC3）去**ping**左边网络中的主机（PC1），发现此时依然可以 ping 通，如下图所示：



在配置标准ACL之前，PC5 去ping PC1是可以ping通的，如下图：



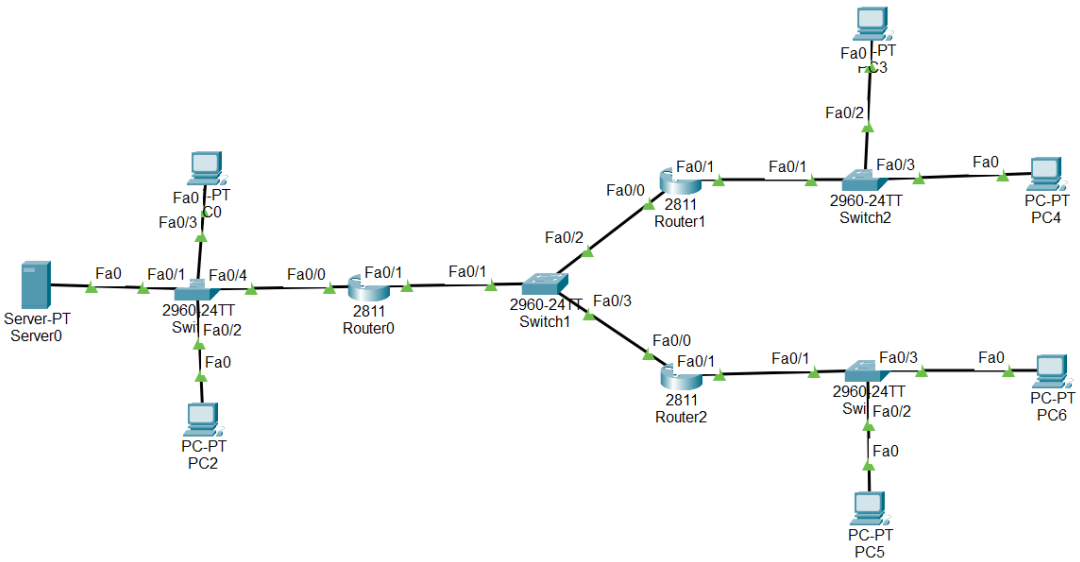
但是现在用右下角的主机（PC5）去ping 左边网络中的主机（PC1），发现此时已经ping不通了，如下图所示：



2.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。

（1）我的网络拓扑图如下：

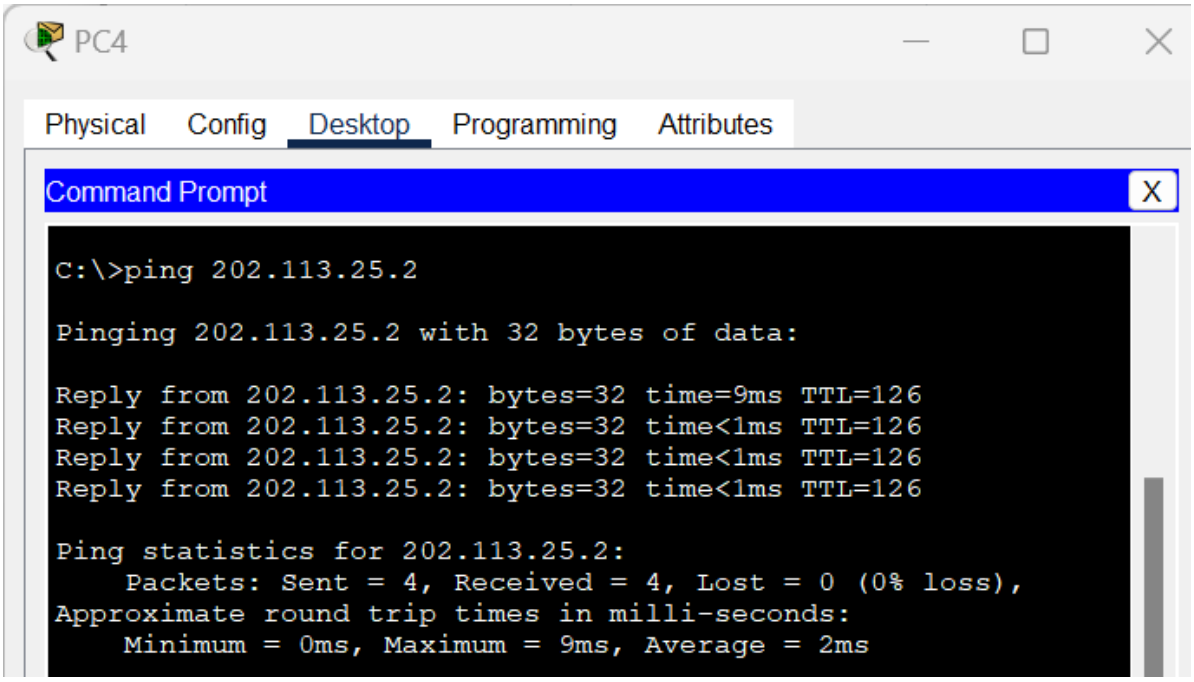
与标准ACL类似，将左边网络中的一台主机换成服务器，为外部的主机提供Web服务，IP的配置与标准ACL中的配置相同，在这里就不再赘述。



（2）分配IP地址

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
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	

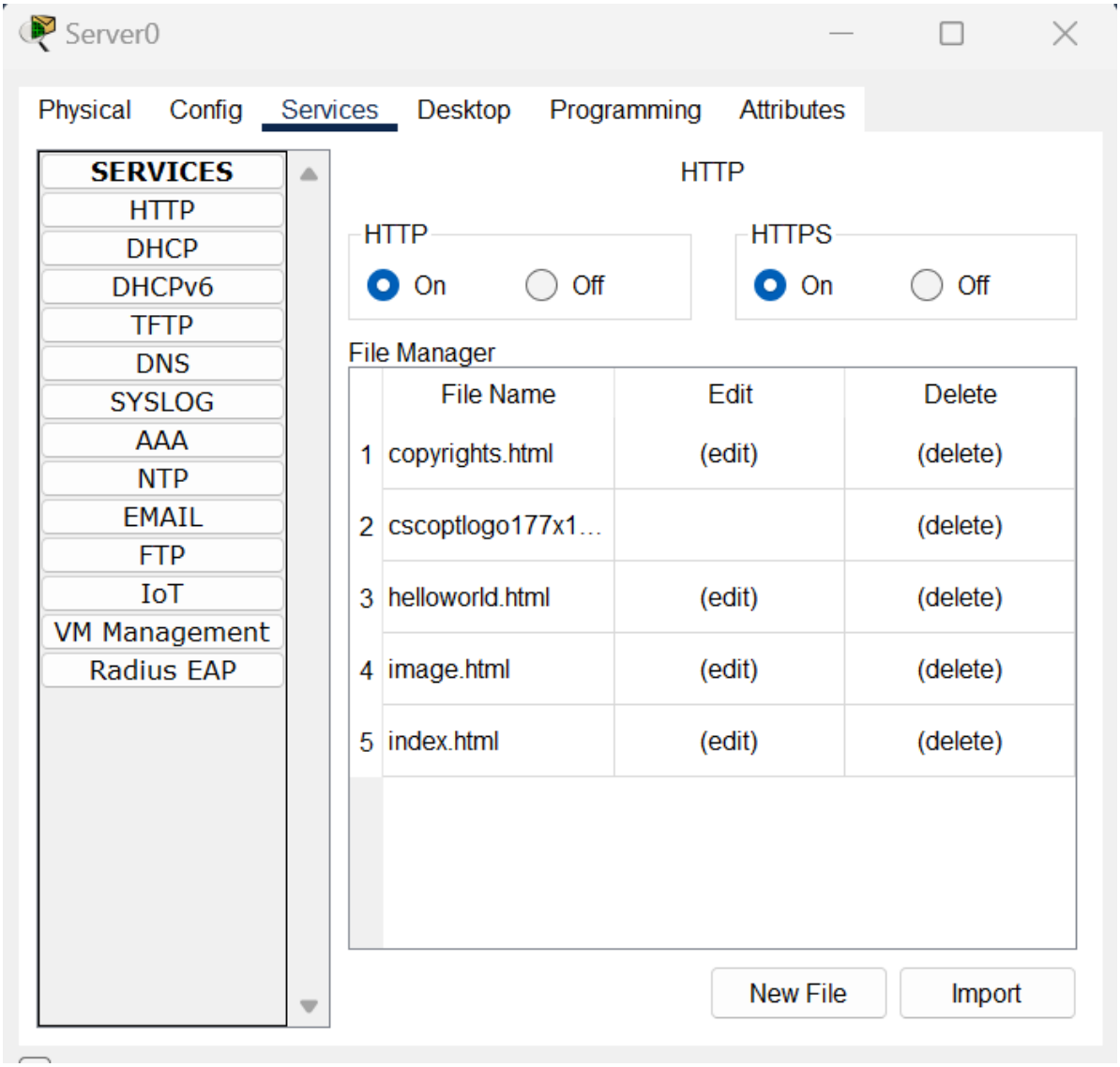
配置好后，在配置防火墙前，需要保证所连接设备能够ping通，如下图：



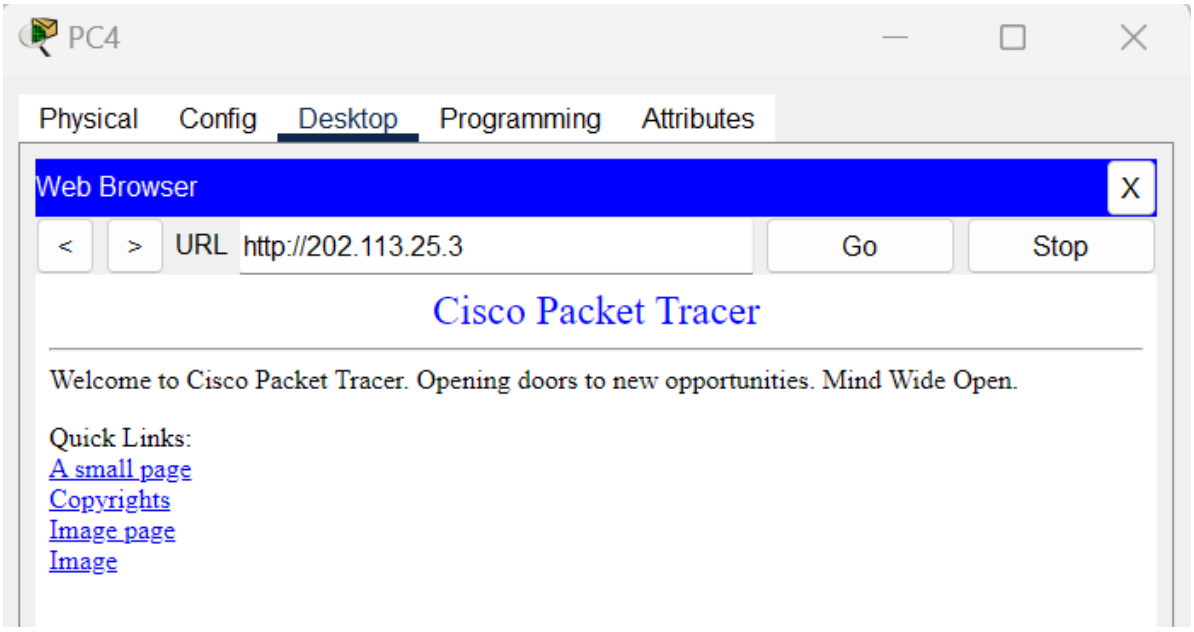
在PC4上ping PC0，可以ping通，说明设置正确。

（3）确保服务打开

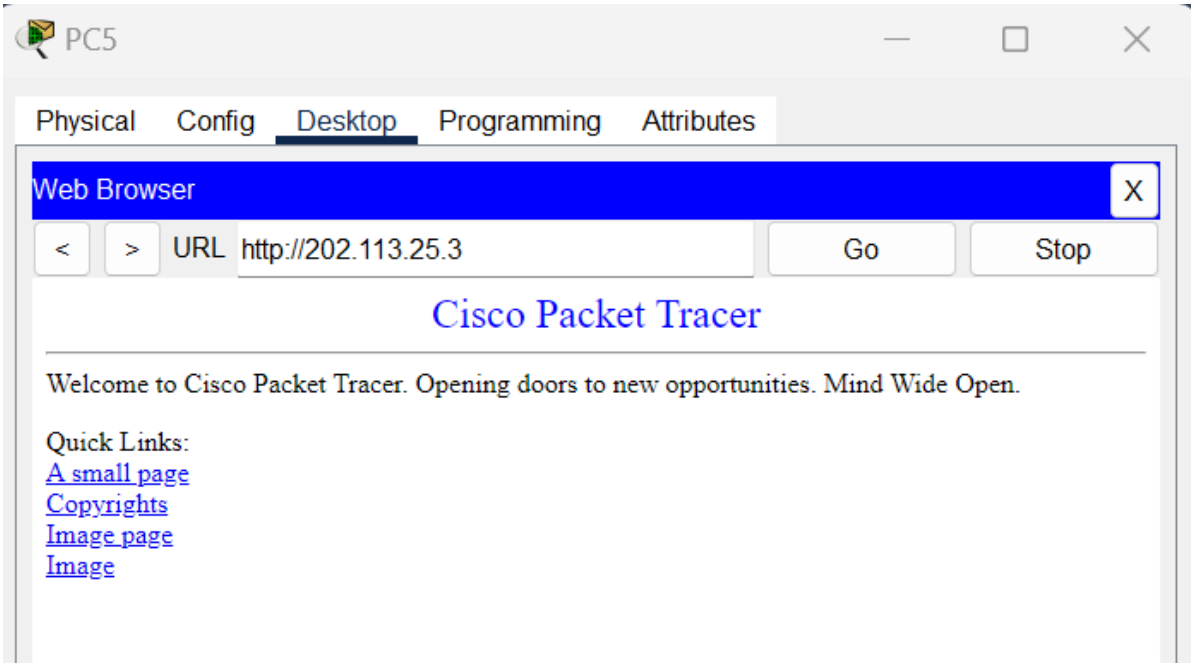
点击服务器Server0的Services，保证HTTP服务处于On状态，让右边的两个网络中的主机访问这个服务器上的网页，确保在配置扩展ACL前浏览成功。



PC4访问网页：



PC5访问网页：



（4）建立扩展ACL

本次实验想要实现除**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：

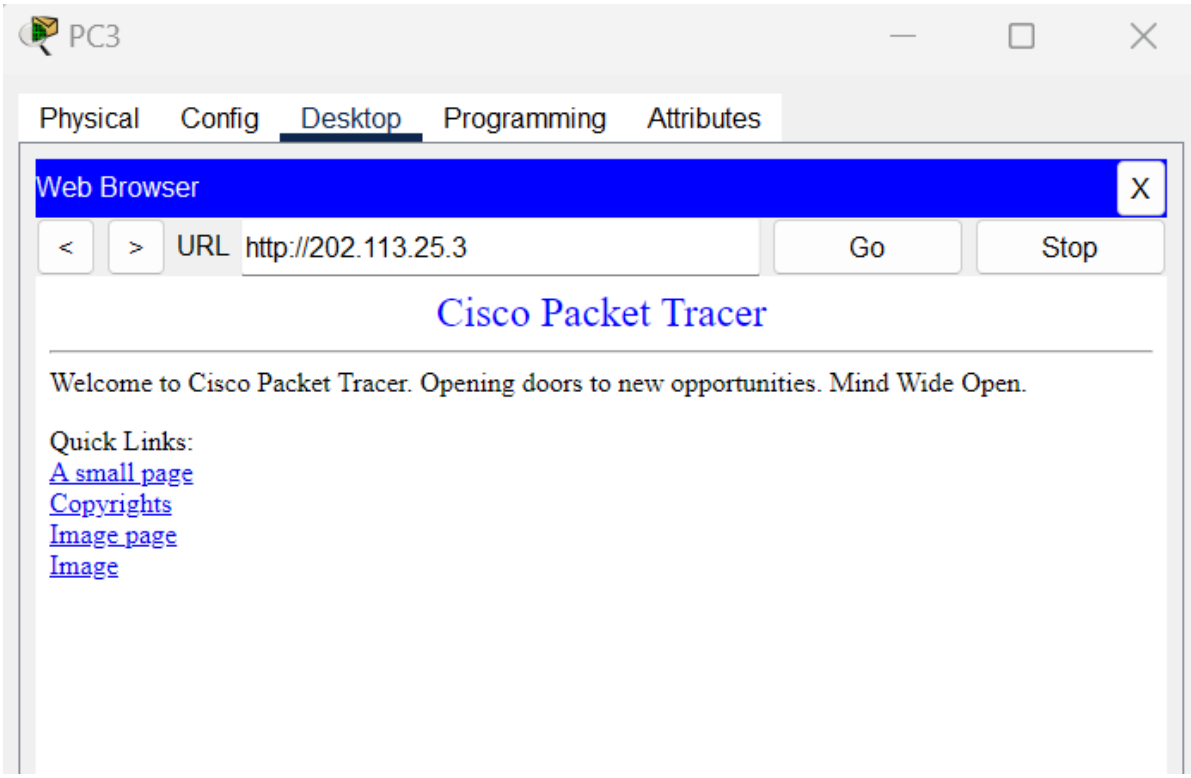
```
Router>en
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 106 deny tcp host 202.113.26.2
host 202.113.25.3 eq www
Router(config)#access-list 106 permit ip any any
Router(config)#interface fa0/1
Router(config-if)#ip access-group 106 in
Router(config-if)#exit
Router(config)#
```

其中

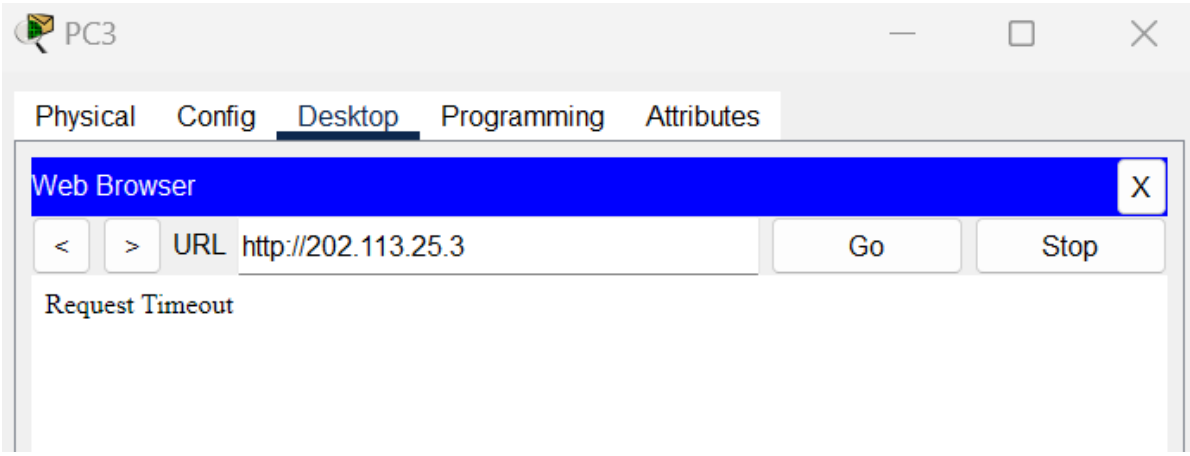
- `access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 eq www`命令含义为抛弃源IP地址为202.113.26.2、目的地址为202.113.25.3、目的端口号为80的TCP的数据报。
- `access-list 106 permit ip any any`命令允许其他所有的数据报通过
- `ip access-group 106 in`命令将106号ACL绑定在fa0/1的入站上

（5）扩展ACL验证

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



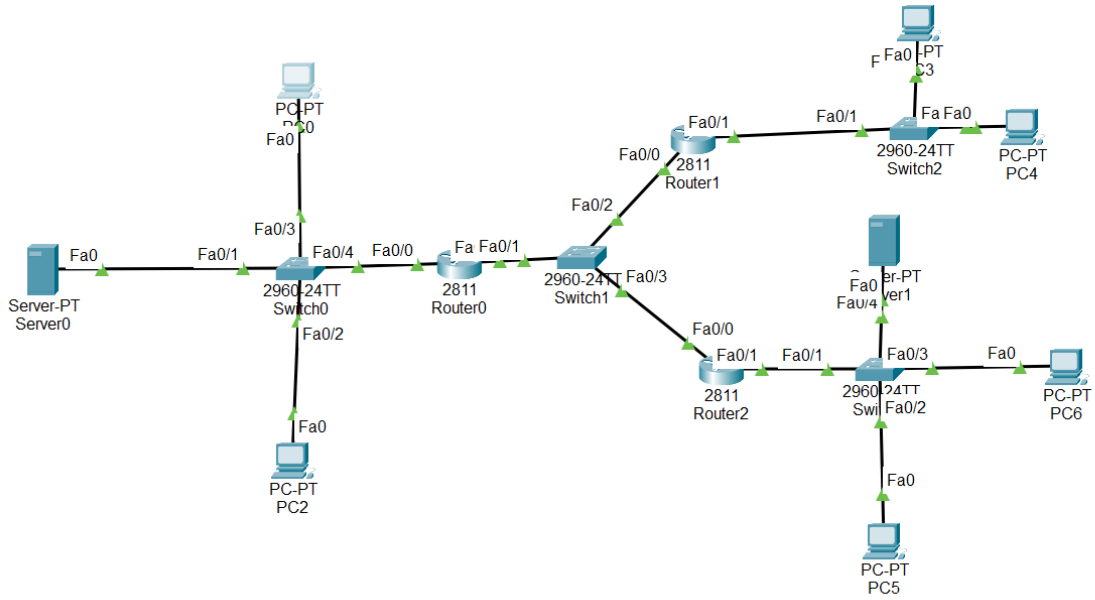
在配置扩展ACL之后用PC3去访问左部网络中的Web网络，发现不可以访问，如下图所示：



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）我的网络拓扑图如下：

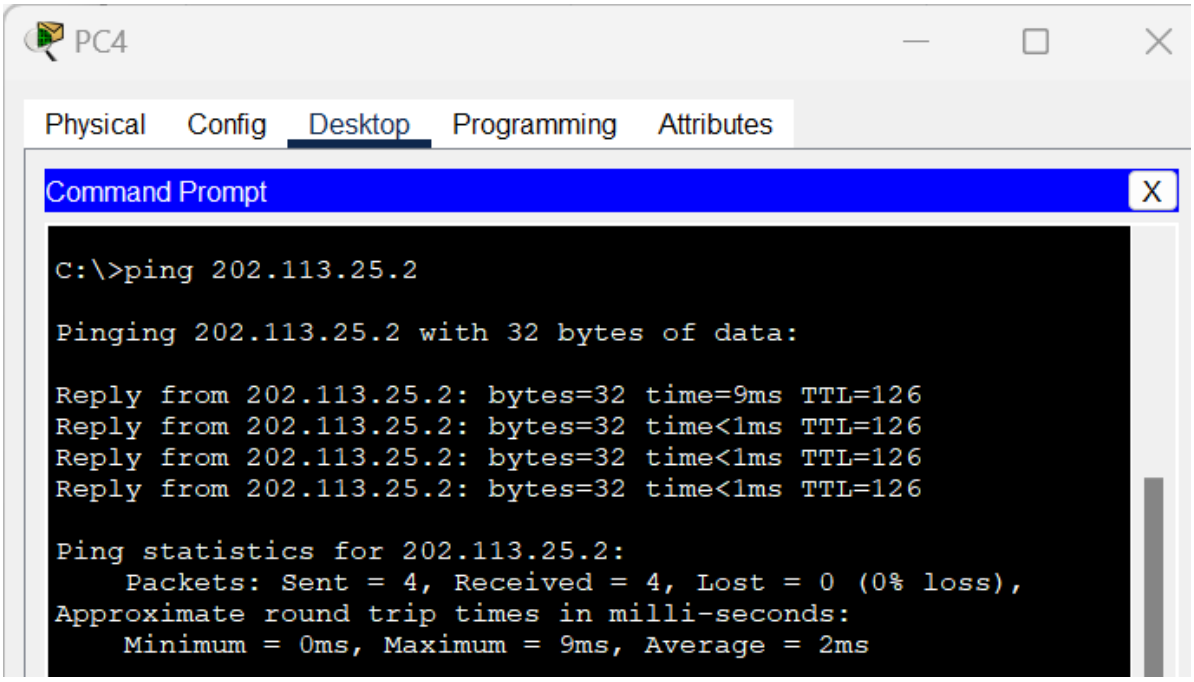
与扩展ACL类似，但在右下角网络中增加了一个服务器，为左边网络中的主机提供Web服务，IP的配置与扩展ACL中的配置相同，在这里就不再赘述。为了实现实验要求，我采用**反向访问控制列表**的方法，即反向ACL。



（2）分配IP地址

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	
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	

配置好后，在配置防火墙前，需要保证所连接设备能够ping通，如下图：



在PC4上ping PC0，可以ping通，说明设置正确。

（3）建立反向ACL

我使用了以下命令

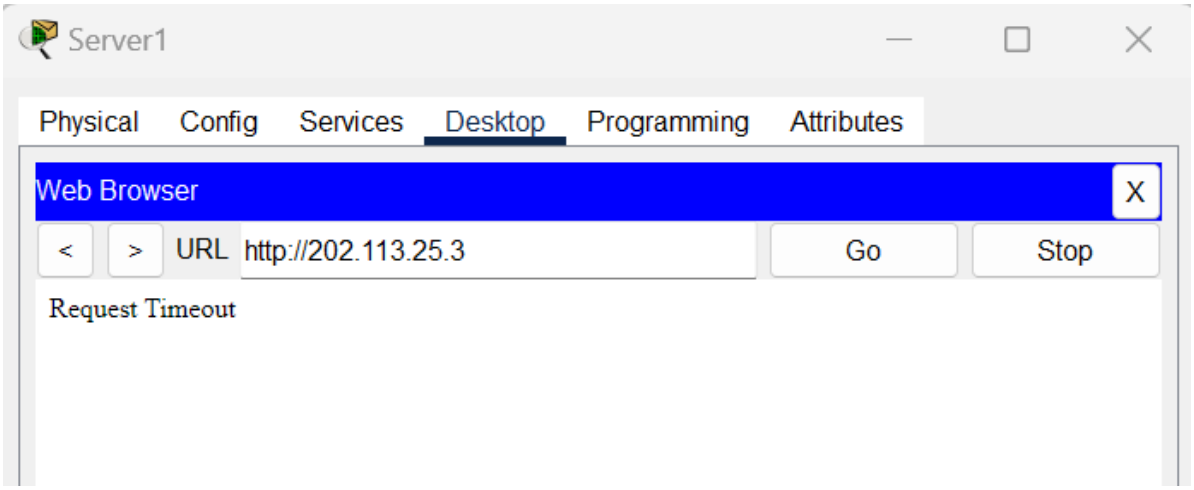
- `access-list 101 permit tcp any 202.113.25.0 0.0.0.255 established`：这条命令定义了ACL101,允许所有其他网段的计算机访问202.113.25.0网段中的计算机，**前提**是TCP连接已经建立了的。当TCP连接**没有建立**的话是**不容许**其他网段访问202.113.25.0的。
- `ip access-group 101 in`：将ACL101应用到相应端口（Fa0/1）的入站上

命令运行如下：

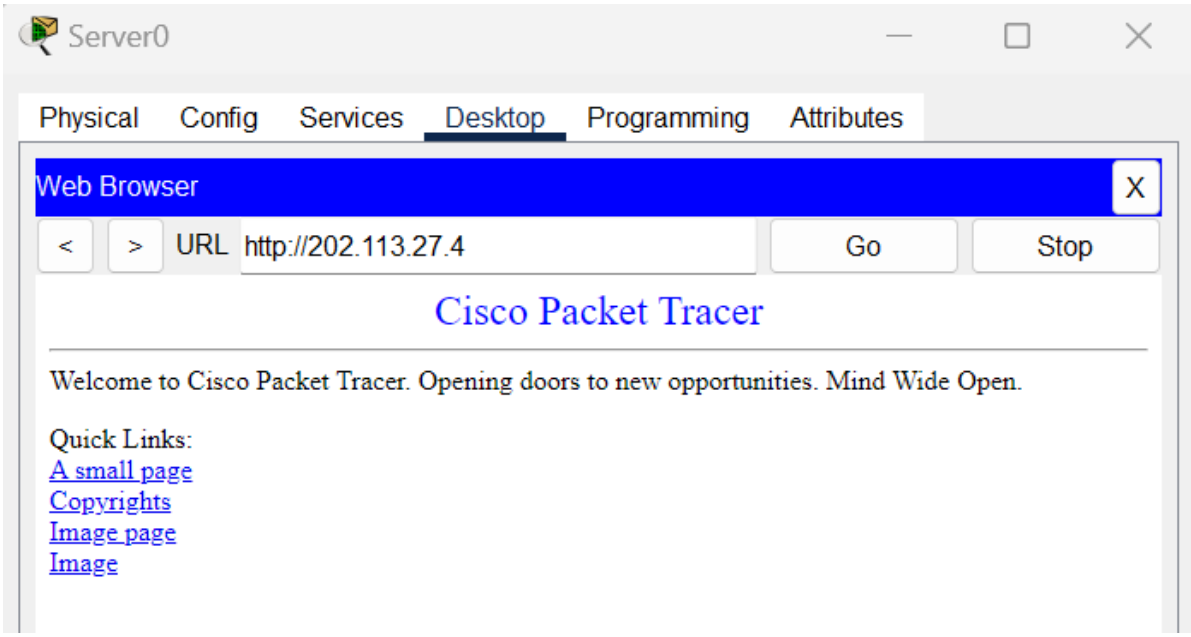
```
Router(config)#access-list 101 permit tcp any 202.113.25.0
0.0.0.255 established


        Router(config)#interface fa0/1
        Router(config-if)#ip access-group 101 in
```

（4）验证反向ACL

- 配置好后，外网（即右边的网络）中的服务器Server1访问内网（即左边的网络）中的服务器Server0，访问不通。



- 但内网中的服务器Server0可以访问外网的服务器Server1。



4.拓展功能

拓展功能：一开始外网主动访问内网访问不通，但当内网访问外网一次后，外网就可以主动访问内网了。

为了实现该功能，我在网上查资料了解了自反ACL的设置过程：

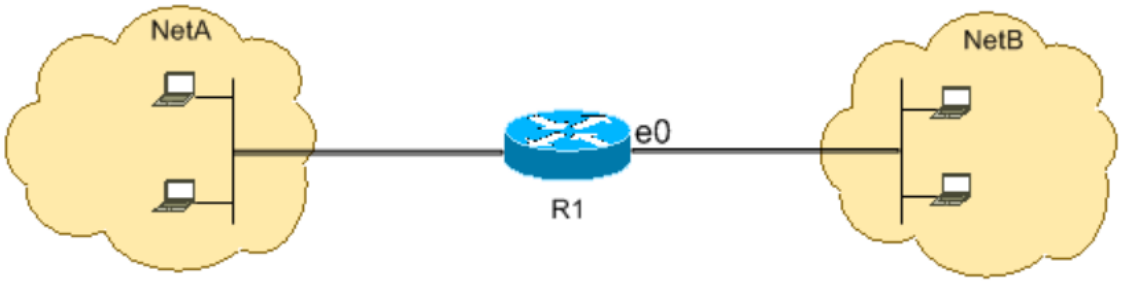
- 定义内网访问外网的ACL
  - `ip access-list extended REFIN`：这条命令是定义一个新的扩展ACL，名为REFIN。
  - `permit tcp 202.113.25.0 0.0.0.255 any reflect TCP`：这个命令的含义是：允许源IP地址在202.113.25.0到202.113.25.255范围内的TCP流量访问任何目的IP地址，并创建一个名为TCP的自反ACL来跟踪并允许返回的TCP流量。
- 定义外网访问内网的ACL
  - `ip access-list extended REFOUT`：这条命令是定义一个新的扩展ACL，名为REFOUT。
  - `evaluate TCP`：这条命令表示该 ACL 将处理所有与名为 TCP 的自反 ACL 相关的入站流量。自反 ACL 能够跟踪通过防火墙的会话，并动态地创建条目以允许返回的流量。当出站流量通过与 reflect 关键字相关联的 ACL 时，将为该流量创建一个条目。然后，evaluate 关键字允许与这些条目匹配的入站流量通过。
- 将创建的自反列表应用于相应的接口
  - `interface fa0/0`：内网接口
  - `ip access-group REFIN in`：应用内网用户访问外网的ACL
  - `interface fa0/1`：外网接口
  - `ip access-group REFOUT in`：应用外网访问内网的ACL

但是，由于Cisco Packet Tracer不支持reflect和evaluate指令，需要下载GNS3，最后还是以失败告终。

四、实验总结

1.如果想删除某一条ACL，可以用命令`no access-list number`，其中number为ACL号。

2.在实现拓展功能过程中，查找了很多资料，还是没有解决问题，不过过程收获颇丰，更加详细了解了ACL的配置过程，和一些额外的配置方法，比如下面这个配置方法，该方法也可以完成**第三个小实验**：



本示例中 ACL 的目的是：

- 允许 NetA 中的主机面向 NetB 中的主机发起并建立 TCP 会话。
- 拒绝 NetB 中的主机面向 NetA 中的主机发起并建立 TCP 会话。

当数据报具备以下条件时，此配置允许数据报通过 R1 上的以太网 0 接口入站：

- 已确认(ACK)或重置(RST)位设置（表示已建立的TCP会话）
- 目标端口值大于 1023

命令如下：

```
interface ethernet0
ip access-group 102 in
access-list 102 permit tcp any any gt 1023 established
```

由于 IP 服务的大多数常用端口都使用小于 1023 的值，ACL 102 将拒绝目标端口值小于 1023 或未设置 ACK/RST 位的所有数据报。因此，当来自NetB的主机发起TCP连接并为小于1023的端口号发送第一个TCP数据包(未设置同步/启动数据包(SYN/RST)位)时，它会遭到拒绝，并且TCP会话失败。从 NetA 发往 NetB 的 TCP 会话将得到允许，因为它已设置用于返回数据包的 ACK/RST 位并且使用的端口值大于 1023。

github链接：https://github.com/happy206/Network-Technology-and-Applications