南開大學

网络技术与应用课程实验报告

实验七：防火墙实验

学　　院　密码与网络空间安全学院

专　　业　信息安全、法学双学位班

学　　号　2313815

姓　　名　段俊宇

班　　级　信息安全、法学双学位班

一、实验目的

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. 在仿真环境下利用标准 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。

二、实验原理

1. 包过滤防火墙配置

包过滤防火墙通过配置访问控制列表（ACL）在网络层对数据包进行过滤控制。其配置核心是定义 ACL 规则，并按顺序匹配执行“允许”或“拒绝”动作。配置时需将 ACL 绑定到防火墙接口的特定方向，通过规则设计可实现网络间访问控制、服务权限管理及简单的连接状态监控。这种防火墙配置灵活、效率高，是网络安全的基础防护手段。

三、实验过程

1.包过滤防火墙的基本配置方法

包过滤防火墙的配置需要指定接口，并且明确允许通过和拒绝通过的 IP。命令如下：

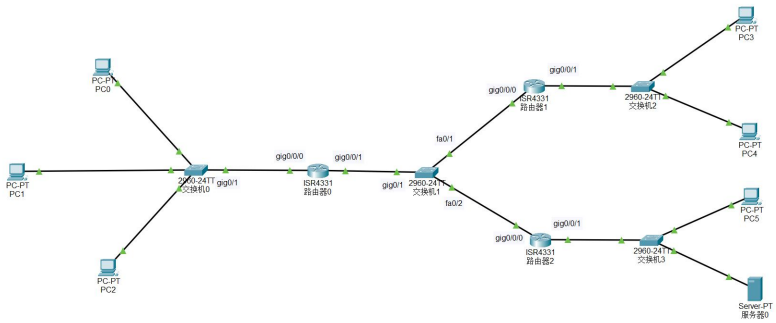
命令名称	命令作用
access-list <标号> permit <目的网络或指定主机 IP><通配符掩码>	访问编号为 number 的控制列表，允许通过的目的网络或指定主机的流量通过，通配符掩码是子网掩码取反得到的
access-list <标号> deny <指定主机或 any>	拒绝指定主机或其他网络的流量，any 表示除了允许通过之外其他 IP 的流量
ip access-group <标号> in/out	将标号对应的 ACL 应用于某个接口的入或者出，入方向表示从外部进入防火墙，也就

	是确定路由转发之前；出方向表示从防火墙进入外部网络，也就是确定路由转发之后
access-list <标号> deny tcp host <主机 IP> host <服务器 IP> eq <端口号>	拒绝指定主机向指定服务器发送的 TCP 数据包，端口为指定端口号。扩展 ACL 的编号为 100-199，标准 ACL 的编号为 0-99
access-list <标号> permit ip any any	允许其他所有 IP 的流量

2. 防火墙配置

2.1 标准 ACL 配置

该实验需要三个独立的网络，因此使用了很多的设备，我在图中标注了三个路由器和中间交换机的接口，网络拓扑图如下所示：



主机和服务器的 IP 地址如下所示：

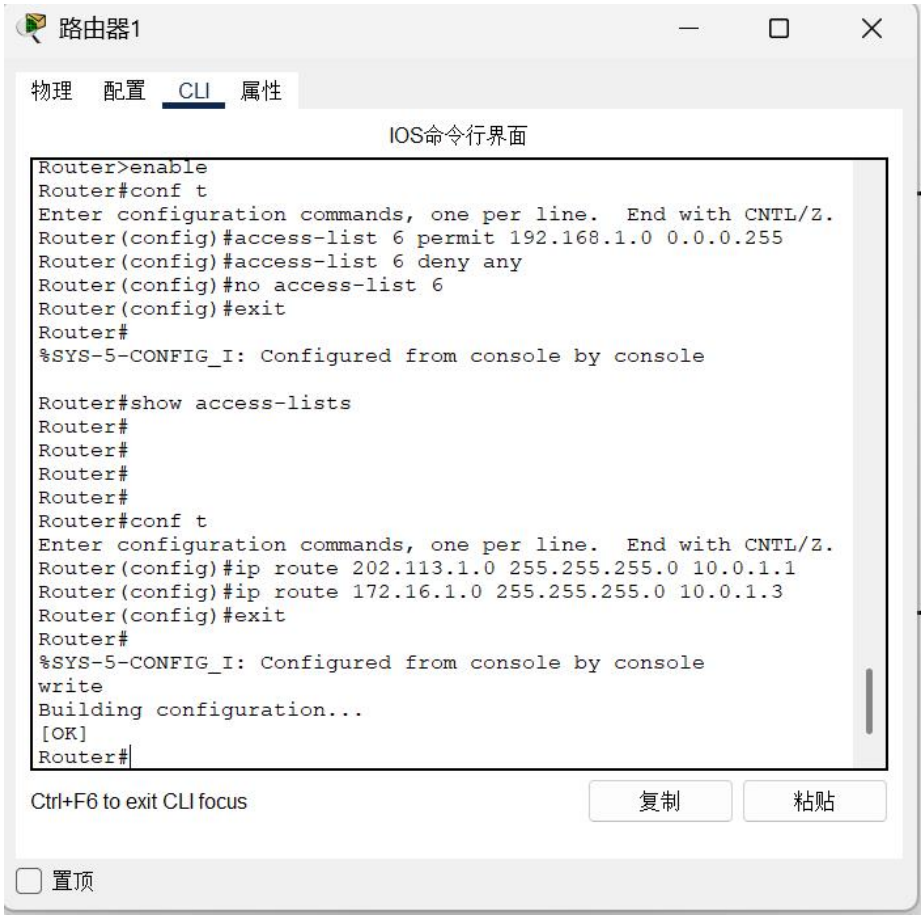
设备名称	IP 地址	子网掩码	网关地址
PC0	202.113.1.1	255.255.255.0	202.113.1.10
PC1	202.113.1.2	255.255.255.0	202.113.1.10
PC2	202.113.1.3	255.255.255.0	202.113.1.10
PC3	192.168.1.1	255.255.255.0	192.168.1.10
PC4	192.168.1.2	255.255.255.0	192.168.1.10
PC5	172.16.1.1	255.255.255.0	172.16.1.10
服务器 0	172.16.1.2	255.255.255.0	172.16.1.10

接下来配置路由器的各个接口，IP 如下所示：

设备名称	接口名称	IP 地址	子网掩码

路由器 0	Gig0/0/0	202.113.1.10	255.255.255.0
	Gig0/0/1	10.0.1.1	255.255.255.0
路由器 1	Gig0/0/0	192.168.1.10	255.255.255.0
	Gig0/0/1	10.0.1.2	255.255.255.0
路由器 2	Gig0/0/0	172.16.1.10	255.255.255.0
	Gig0/0/1	10.0.1.3	255.255.255.0

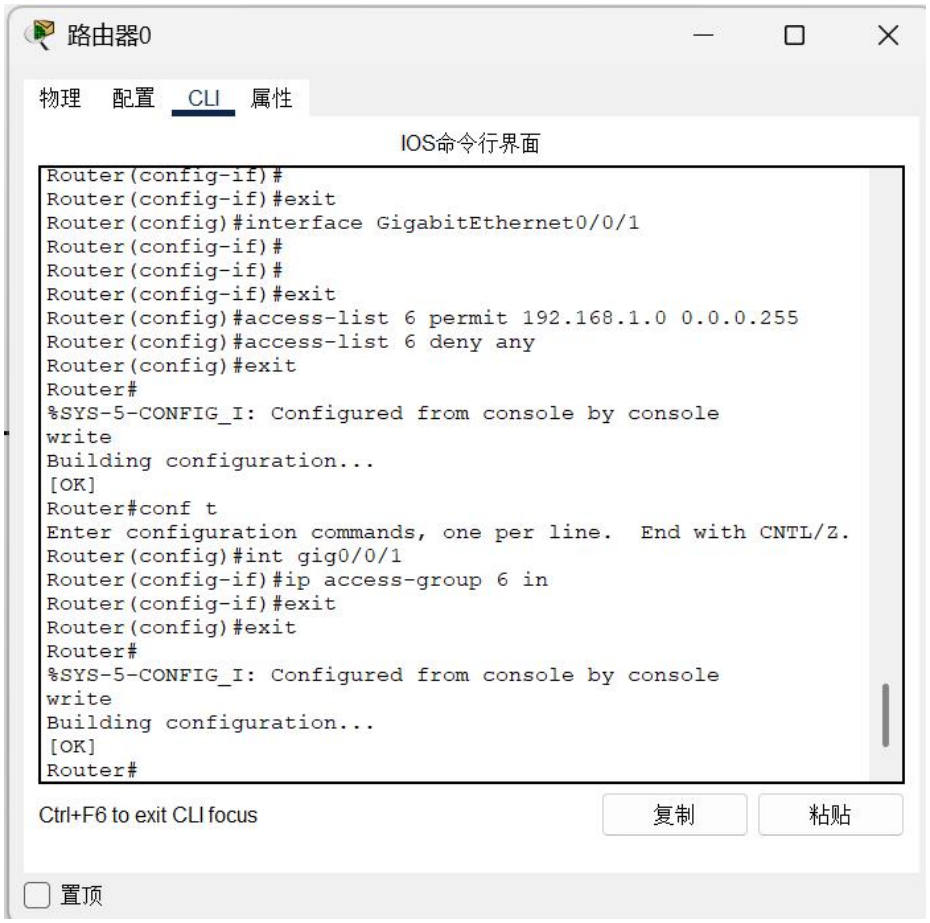
然后为三个网络的路由器配置静态路由，如下图所示分别为路由器 0、路由器 1 和路由器 2 的静态路由配置。


路由器1
物理 配置 CLI 属性
IOS命令行界面
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 6 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 6 deny any
Router(config)#no access-list 6
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show access-lists
Router#
Router#
Router#
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 202.113.1.0 255.255.255.0 10.0.1.1
Router(config)#ip route 172.16.1.0 255.255.255.0 10.0.1.3
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
Router#
Ctrl+F6 to exit CLI focus
复制
粘贴
置顶

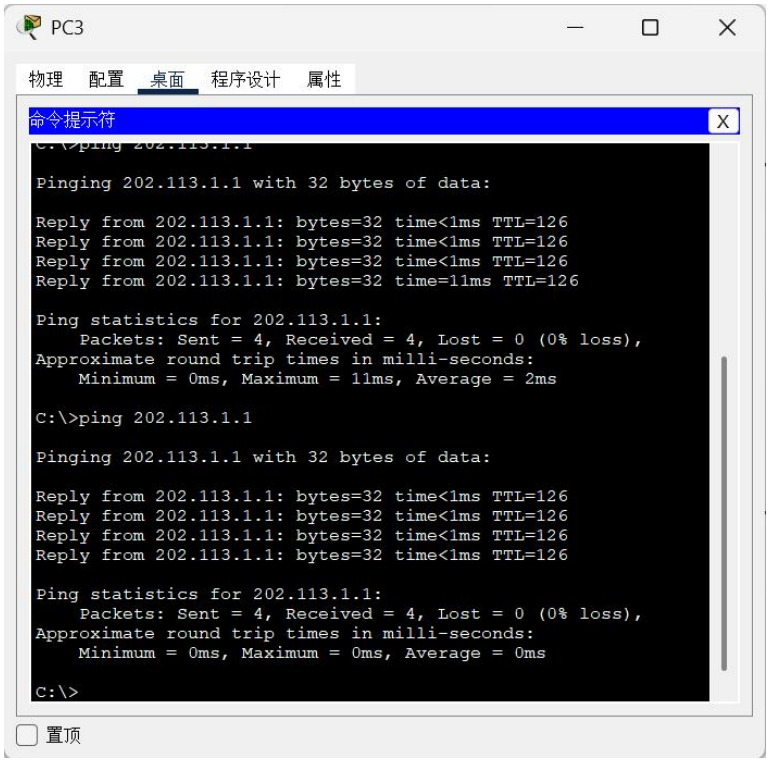

路由器2
物理 配置 CLI 属性
IOS命令行界面
Press RETURN to get started.
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 202.113.1.0 255.255.255.0 10.0.1.1
Router(config)#ip route 192.168.1.0 255.255.255.0 10.0.1.2
Router(config)#
Ctrl+F6 to exit CLI focus
复制
粘贴
置顶

这样就完成了基础配置，现在各个网络的设备之间是可以互相 ping 通的。开始正式配置标准 ACL，允许 192.168.1.0 网络中的设备访问 202.113.1.0 网络中的设备，但是拒绝 172.16.1.0 网络中的设备访问。因此需要在路由器 0 上进行配置，在接收到来自 192.168.1.0 和 172.16.1.0 的流量时，允许前者通过，拒绝后者的流量。配置命令如下所示，我使用注释的形式解释。

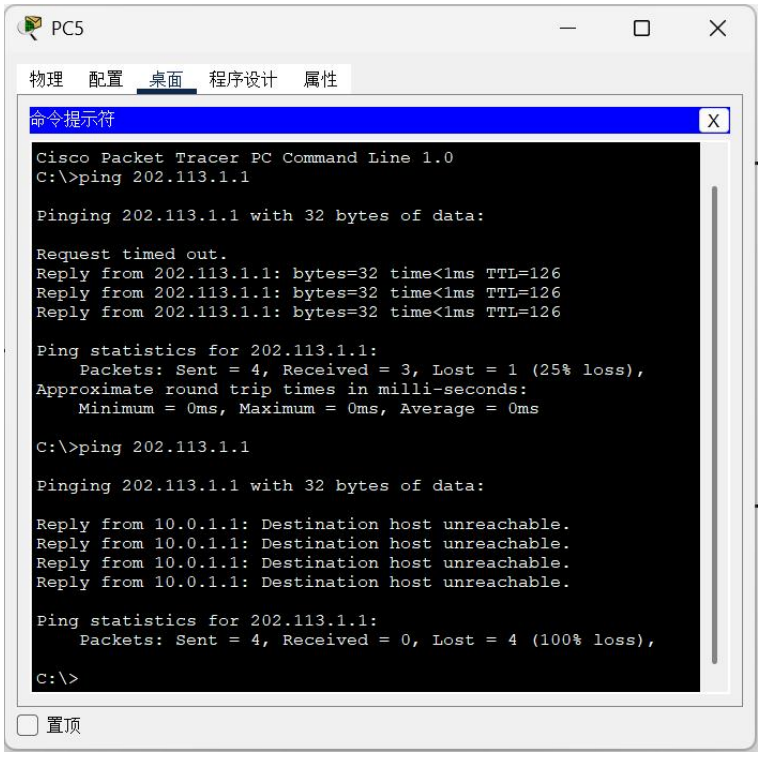
```
// 允许 192.168.1.0 的流量通过
access-list 6 permit 192.168.1.0 0.0.0.255
// 拒绝来自其他网络的流量
access-list 6 deny any
// 打开右边接口
int gig0/0/1
// 在该接口的入方向上应用这个 ACL，也就是进入接口前就检查是否满足 ACL 规则
ip access-group 6 in
```



完成了标准 ACL 的配置，测试结果应为 192.168.1.0 网络中的主机和 202.113.1.0 网络中的主机可以连通，但是 172.16.1.0 网络中的主机不能连通。结果如下所示：



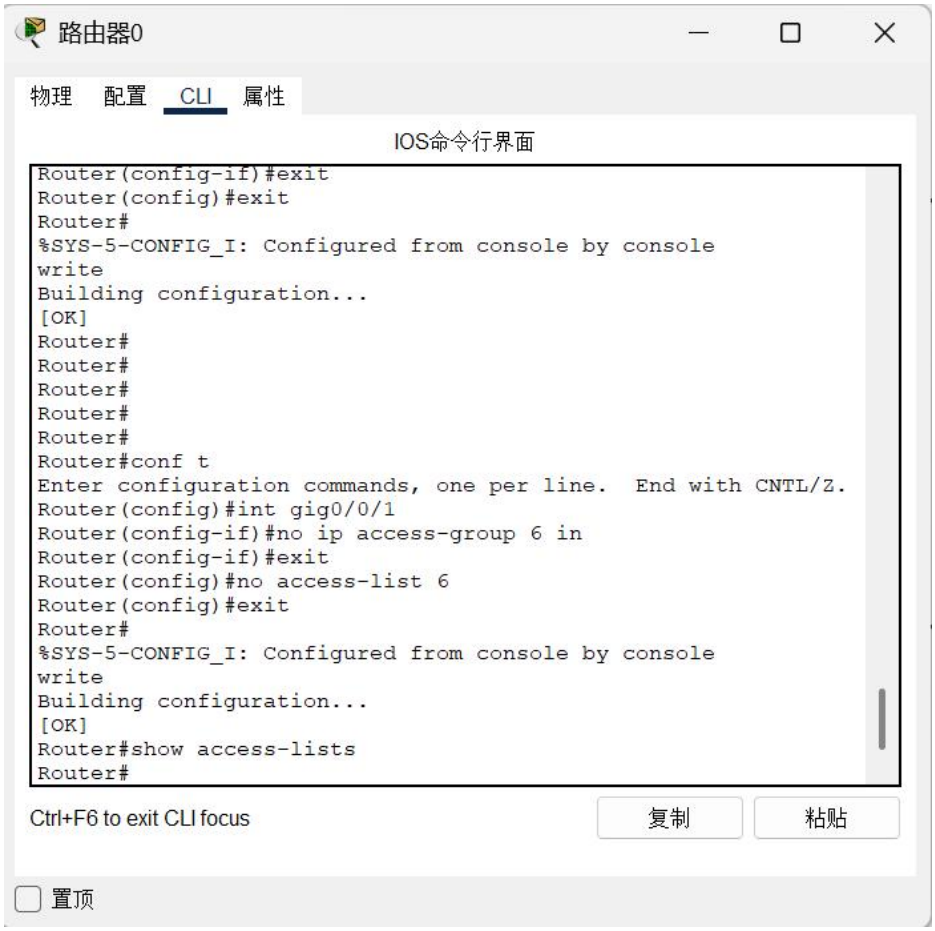
PC3 是 192.168.1.0 网络中的主机，可以 ping 通 202.113.1.1，符合预期结果。



PC5 是 172.16.1.0 网络中的主机，在没有设置 ACL 之前可以 ping 通，设置之后显示目标主机不可达，回复包来自路由器 0，说明流量被路由器 0 拒绝了，符合预期结果。

2.2 扩展 ACL 配置

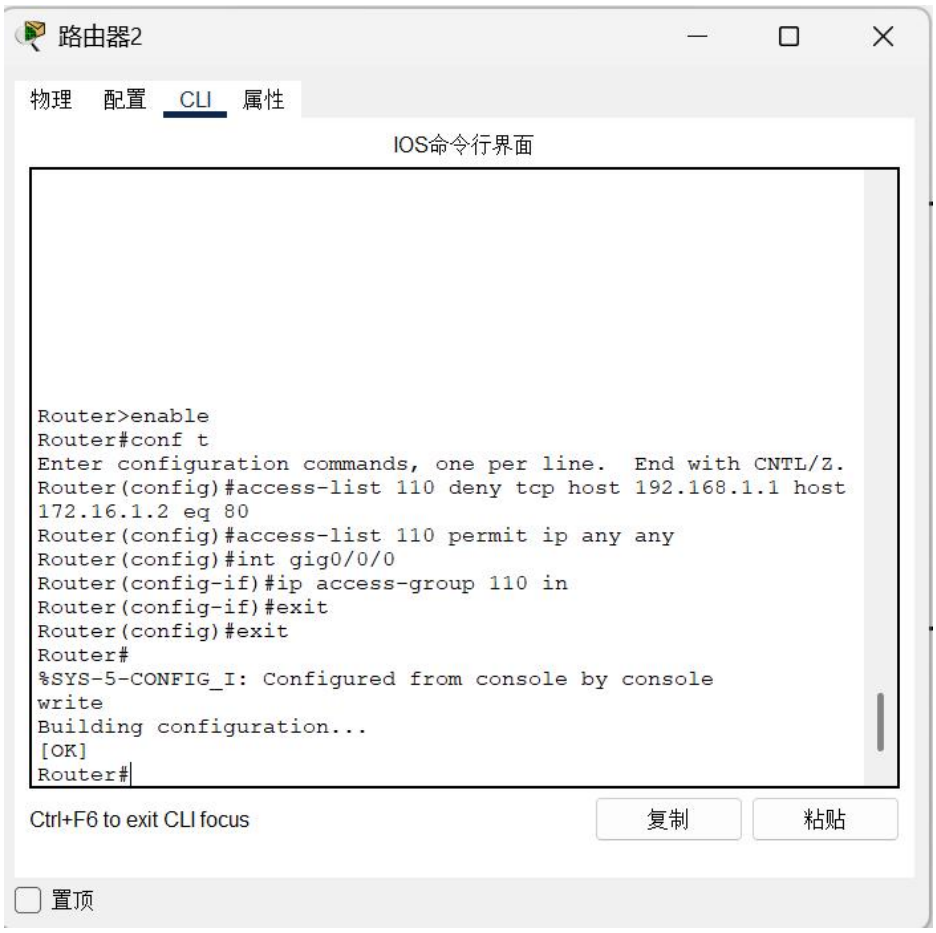
配置扩展 ACL 之前，先清除前面配置的扩展 ACL，防止发生干扰。使用 no access-list 6 命令清除已经配置的 ACL 规则，打开 gig0/0/1，使用 no ip access-group 6 in 命令清除规则的应用。



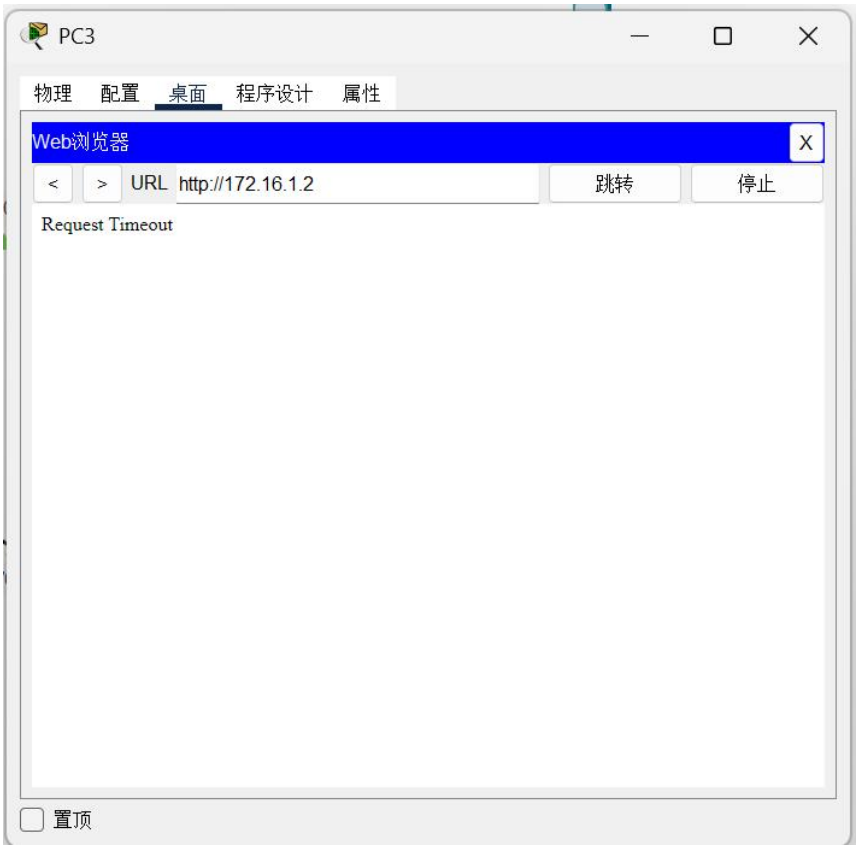
然后再配置扩展 ACL，拒绝 IP 为 192.168.1.1 的主机访问 IP 为 172.16.1.2 的服务器，允许其他主机访问。因此需要在路由器 2 上配置，在接收到流量时，如果来自 192.168.1.1，目的 IP 是 172.16.1.2，端口为 80，那么就拒绝，其他的流量均允许通过。

```
// 拒绝源 IP 为 192.168.1.1，目的 IP 为 172.16.1.2，协议为 tcp，端口为 80 的数据包
access-list 110 deny tcp host 192.168.1.1 host 172.16.1.2 eq 80
```

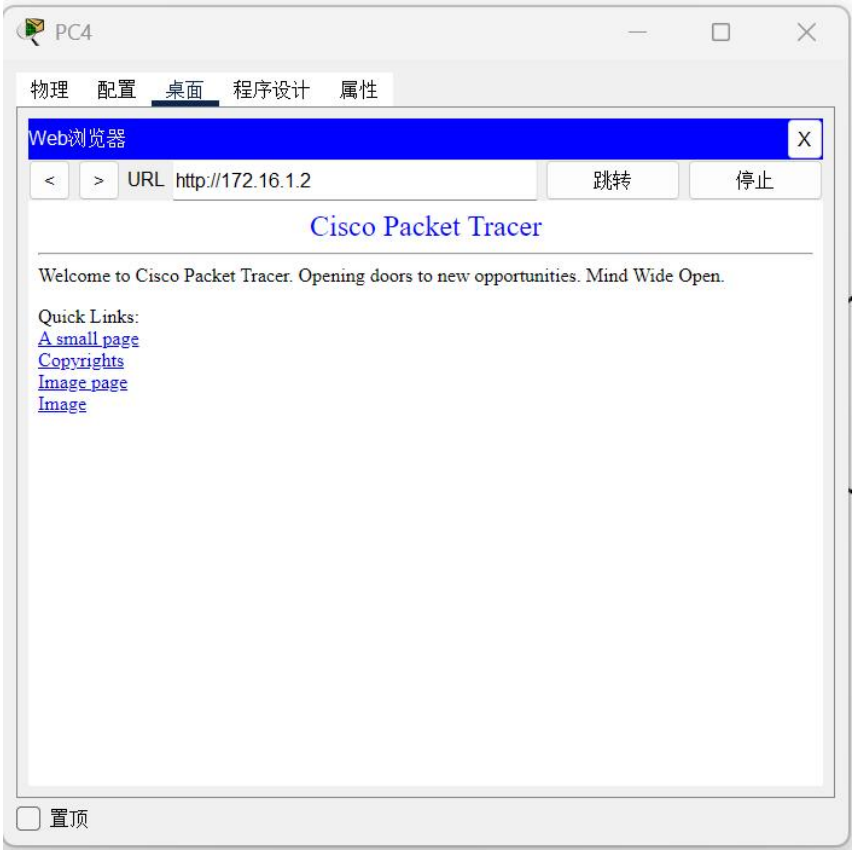
```
// 允许其他 IP 的流量通过
access-list 110 permit any any
// 打开左边接口
int gig0/0/0
// 在该接口的入方向上应用这个 ACL，也就是进入接口前就检查是否满足 ACL 规则
ip access-group 110 in
```



完成了扩展 ACL 的配置，预期结果应为 IP 为 192.168.1.1 的主机通过 web 浏览器无法访问 172.16.1.2，而其他主机可以。测试结果如下：



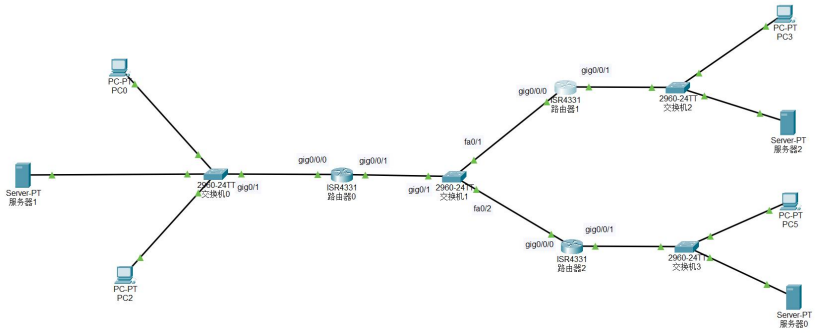
PC3 的 IP 为 192.168.1.1，访问目的服务器时显示超时，符合预期结果。



PC4 和 PC3 都在 192.168.1.0 网络中，但是它可以通过 web 浏览器访问目的服务器，符合预期结果。

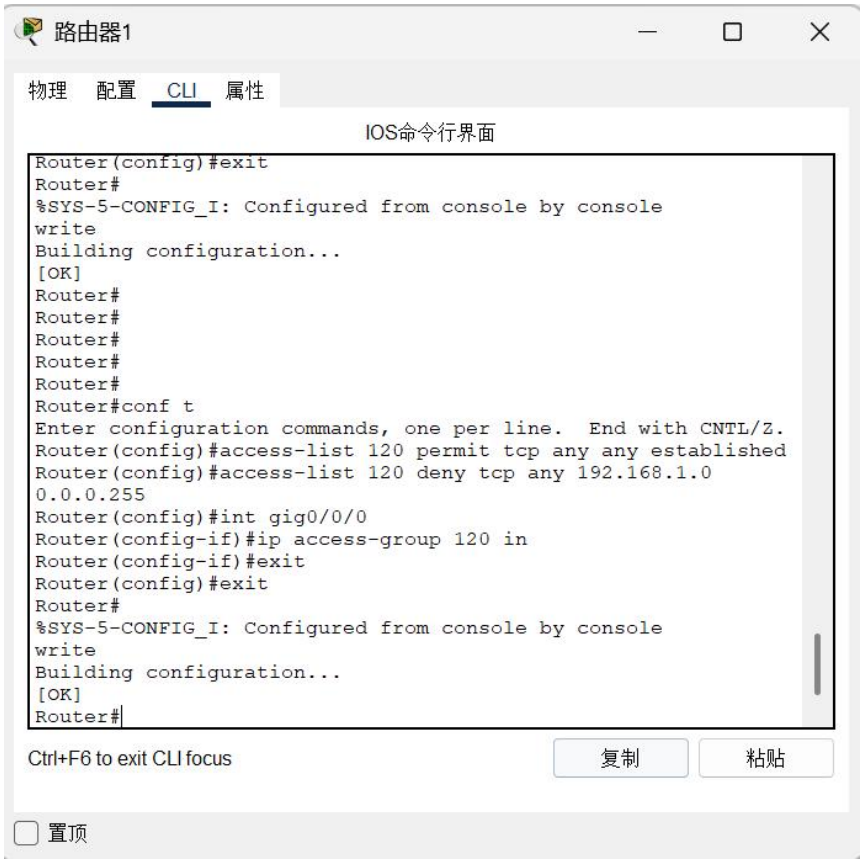
2.3 内网和外网配置

首先清除先前配置，防止干扰之后的 ACL 配置，命令与上面相同，这里就不再赘述。现在将网络拓扑图进行修改，把 PC1 和 PC4 换成服务器 1 和服务器 2，IP 地址等配置不变，如下所示：

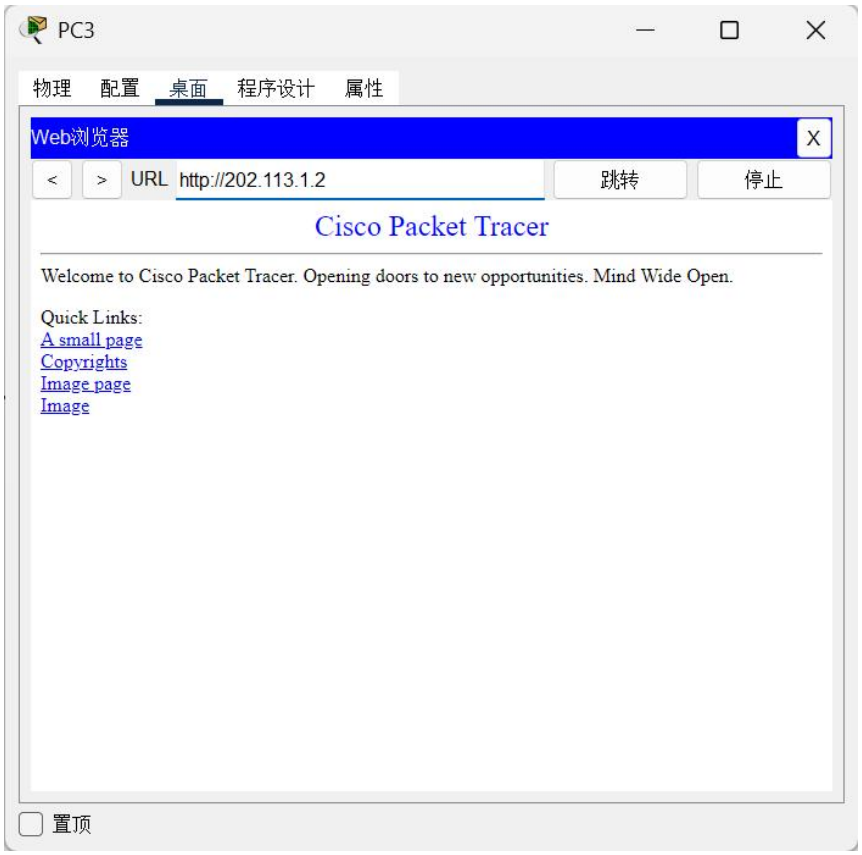


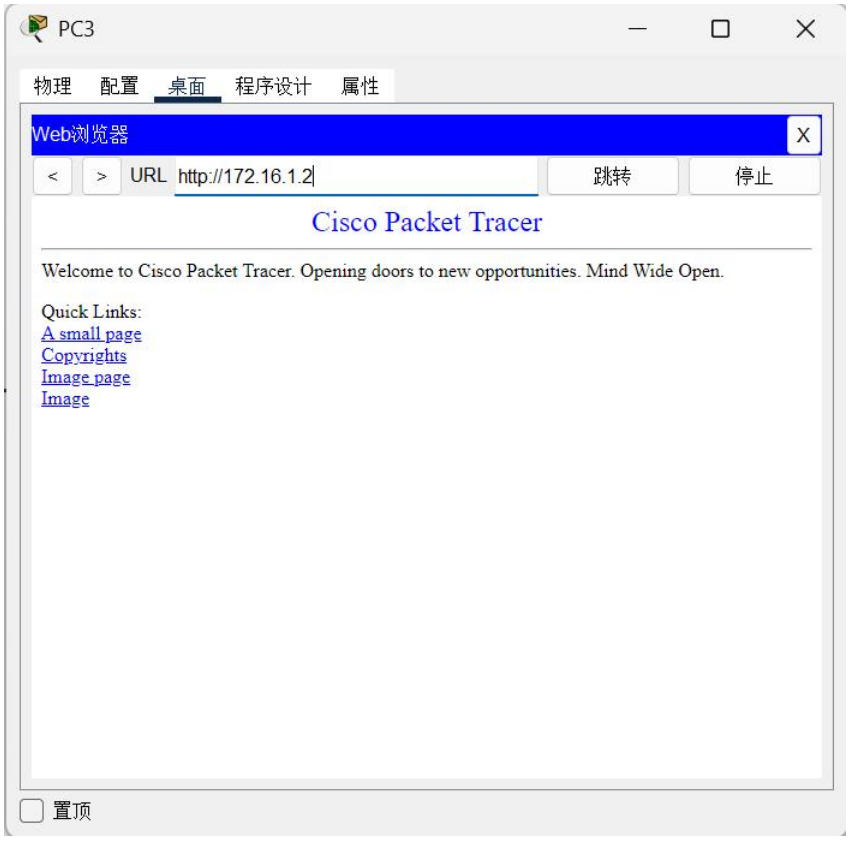
我将 192.168.1.0 设置为内网，其他两个网络属于外网。因此需要在路由器 1 上配置，允许内网主机发起向外网服务器的 TCP 连接，并且只是已建立的 TCP 连接，这样内网主机可以访问外网服务器，并且拒绝任何源 IP 为外网主机，而目的 IP 为内网的 TCP 连接。配置命令如下：

```
// 允许内网主机发起 TCP 连接，并且是已经建立的
access-list 120 permit tcp 192.168.1.0 0.0.0.255 any established
// 允许外网回复的数据包通过，并且是已经建立的连接
access-list 120 permit any any established
// 拒绝源 IP 为外网主机，目的 IP 为内网的 TCP 连接
access-list 120 deny any 192.168.1.0 0.0.0.255
// 打开左边接口
int gig0/0/0
// 在该接口的入方向上应用这个 ACL，也就是进入接口前就检查是否满足 ACL 规则
ip access-group 120 in
```

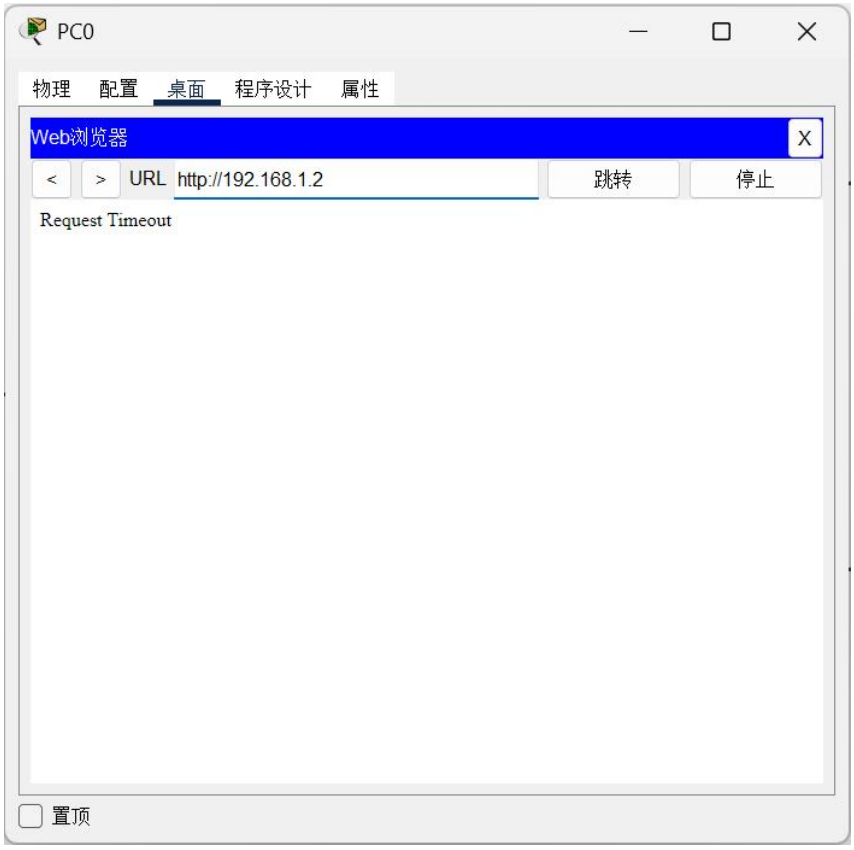


完成了内网和外网的配置，预期结果应为内网主机可以访问外网服务器，但是外网主机不能访问内网服务器。测试结果如下：





PC3 是内网主机，它可以访问外网的两个服务器，符合预期结果。



PC0 是外网主机，访问内网服务器显示超时，符合预期结果。

这样就完成了所有的实验！

四、实验结论及心得体会

本次实验我在仿真环境下配置了防火墙，并实现了内网访问外网，而外网主机不能访问内网服务器。在实验过程中我先是使用了一个路由器来完成实验，但是一个路由器配置标准 ACL 后，回复的数据包无法通过，因此需要三个独立的网络来完成该实验。通过本次实验，我加深了对 ACL 的理解，学会了防火墙配置的命令，巩固了课上学习的知识。