

**网络技术与应用课程实验报告**

**实验七：防火墙**

****

专 业 信息安全

学 号 2113662

姓 名 张丛

班 级 信息安全一班

1. **实验目的**

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。

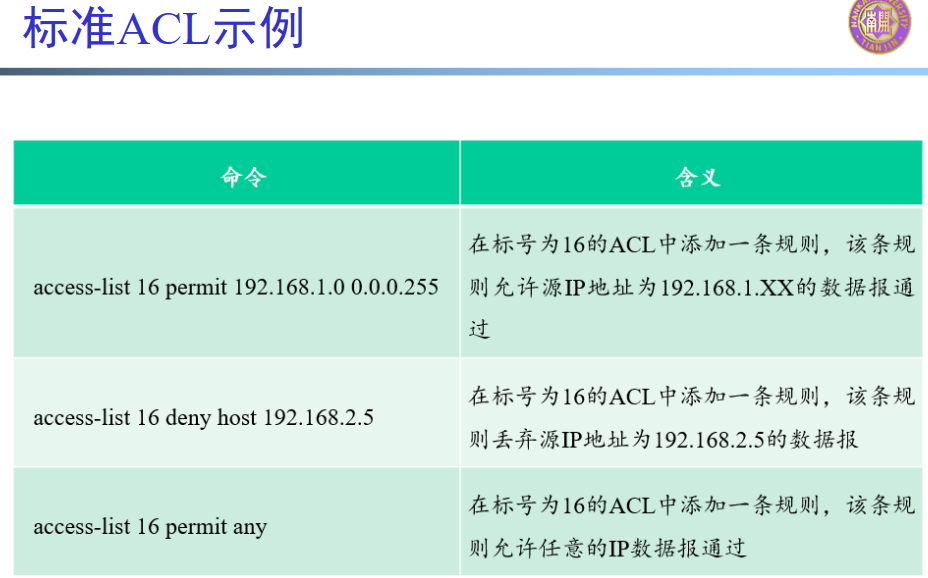
1. **实验原理**

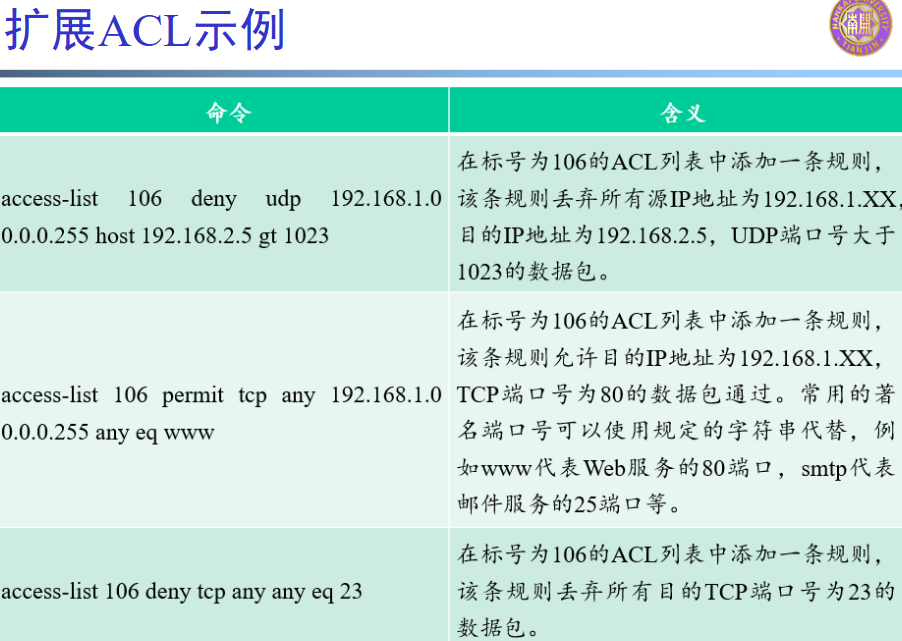
ACL（AccessControlList，访问控制列表）是用来实现数据包识别功能的，ACL用于控制网络设备（如路由器、交换机、防火墙）上的数据流动，以决定哪些数据包被允许通过或被阻止。

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；

Cisco设备支持两种类型的ACL：标准ACL（Standard ACL）和扩展ACL（Extended ACL）。





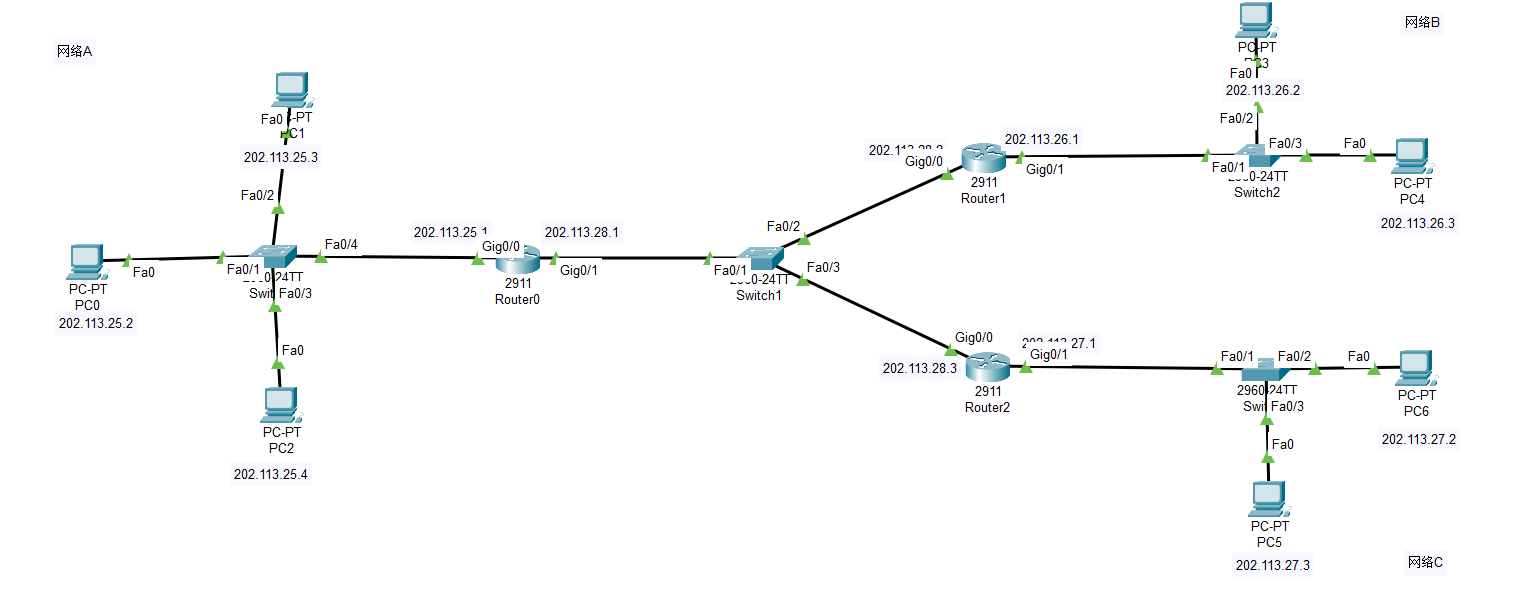
1. **实验过程**

#### 标准ACL:

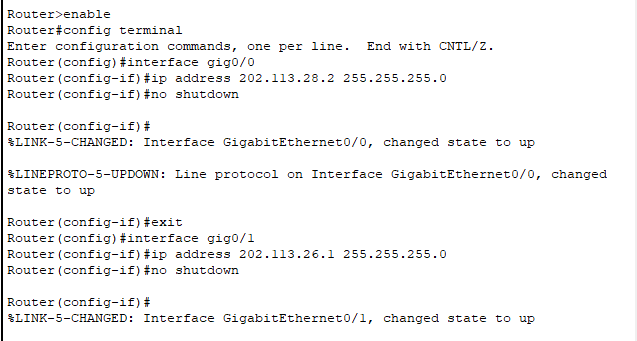
目的：允许网络 B 访问网络 A，而不允许其他网络访问网络 A 中的主机。

操作：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。

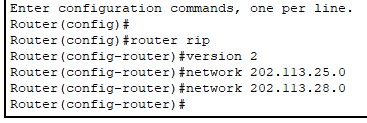
网络拓扑如下：



首先对各主机和路由器进行ip配置，已经配置过很多次了，不赘述：

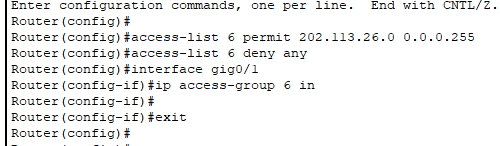


给路由器配置rip动态路由，在之前的实验也做过，如下：



对所有路由器配置完动态路由后，此时各个网络就已经连通了，需要对路由R1配置标准访问控制列表，以达到实验目的。

如下：



对上面的命令进行解释：

**access-list 6 permit 202.113.26.0 0.0.0.255**

1. 创建一个名为6的ACL，并允许来自202.113.26.0/24网段的数据包通过。这里的“0.0.0.255”表示子网掩码为255.255.255.0，即202.113.26.0/24网段。

**access-list 6 deny any**

1. 在ACL中添加一个拒绝任何来源IP地址的规则。这个规则将拒绝所有未被允许的数据包。

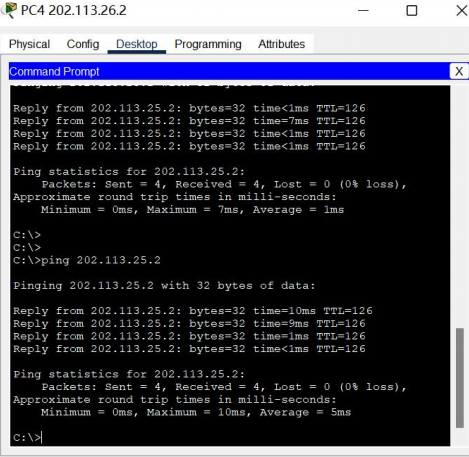
**Router(config)#interface gig0/1**

**Router(config-if)#ip access-group 6 in**

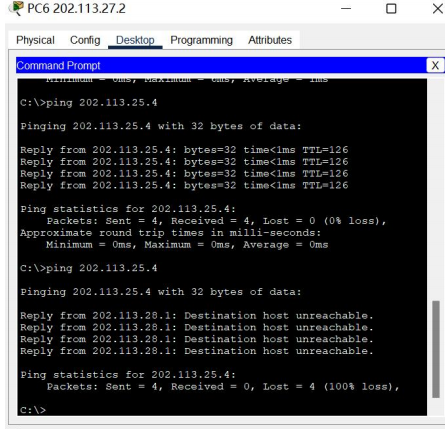
1. 将ACL 6应用到接口gig0/1的入方向，即所有进入该接口的数据包都会被ACL过滤。

配置完成后，就实现了仅网络B的主机可以访问网络A的主机。

如网络B的主机4（202.113.26.2）访问网络A的主机0（202.1113.25.2）：



网络C的主机访问网络A的则不行：



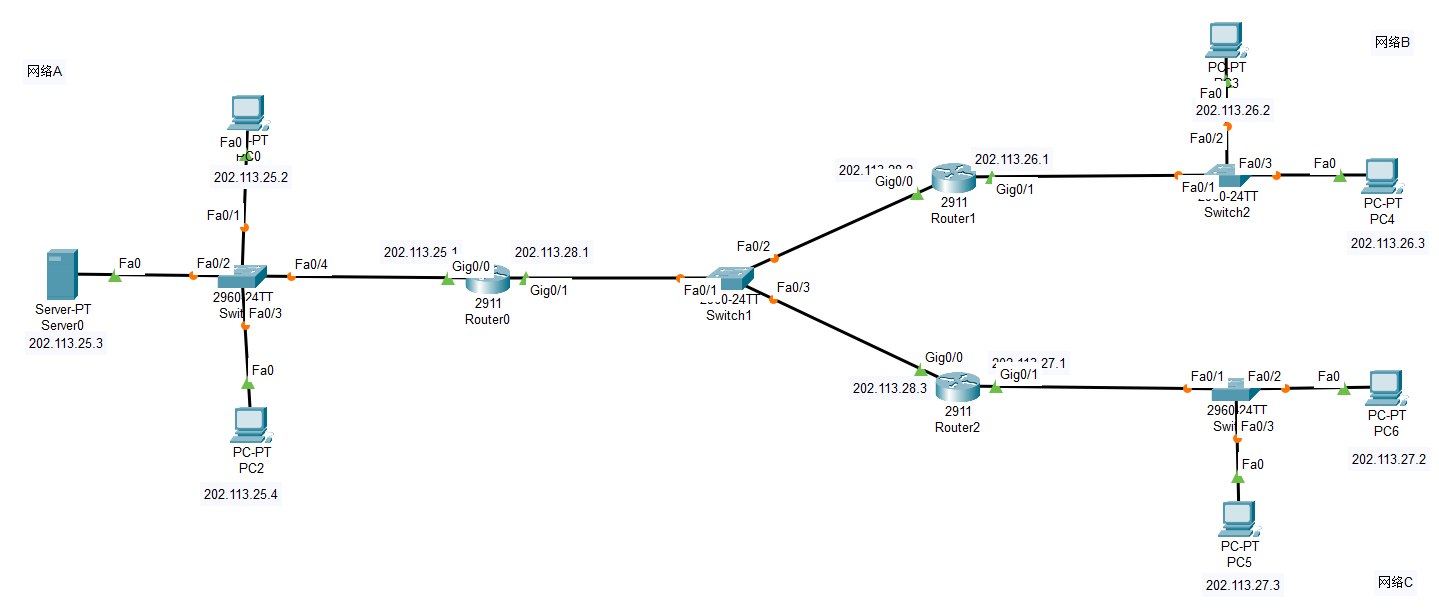
并且，与一般的ping不通于是显示timeout不同，这里是直接告诉我们不可访问。

#### 扩展ACL:

目的：不允许网络 B 中的某个主机访问网络 A 中的 Web 服务。

操作同样是在路由器 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。

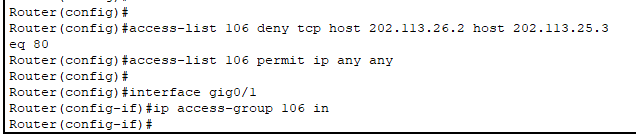
网络拓扑有所改变：



主要区别是网络A存在一个Web服务器。

首先还是配置ip，配置动态路由，不再赘述。

然后配置ACL：



解释：

**access-list 106 deny tcp host 202.113.26.2**

**host 202.113.25.3 eq 80**

1. 创建一个名为106的ACL，并添加一个拒绝TCP数据包的规则，这个规则将拒绝源IP地址为202.113.26.2，目标IP地址为202.113.25.3，目标端口为80的TCP数据包。

**access-list 106 permit ip any any**

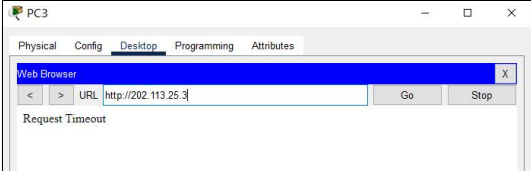
1. 在ACL中添加一个允许所有IP数据包的规则，这个规则将允许所有其他的IP数据包通过。

**Router(config)#interface gig0/1**

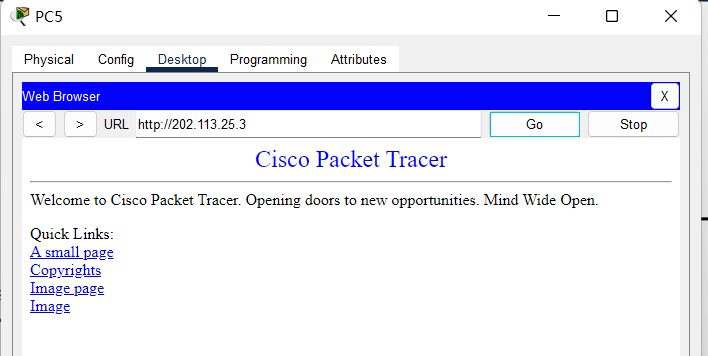
**Router(config-if)#ip access-group 106 in**

1. 将ACL 106应用到接口gig0/1的入方向，即所有进入该接口的数据包都会被ACL过滤。

对于网络B的主机3访问网络A的Web服务器：



对于网络C的主机访问：



于是达到了我们的实验目的。

1. **总结与思考**

课上的理论学习了数据加密、数字签名和防火墙，让我知道了防火墙主要应用了两种技术：包过滤和应用网关。

实验则配置了相对来说简单的包过滤，学习了ACL，和一些配置命令。

受益匪浅。