南 开 大 学

计算机与网络空间安全学院

网络技术与应用课程报告

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**第七次实验报告**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

学号：2012911

姓名：马永田

年级：2020级

专业：计算机科学与技术

2022年12月1日

1. **实验内容说明**

**（一）防火墙实验**

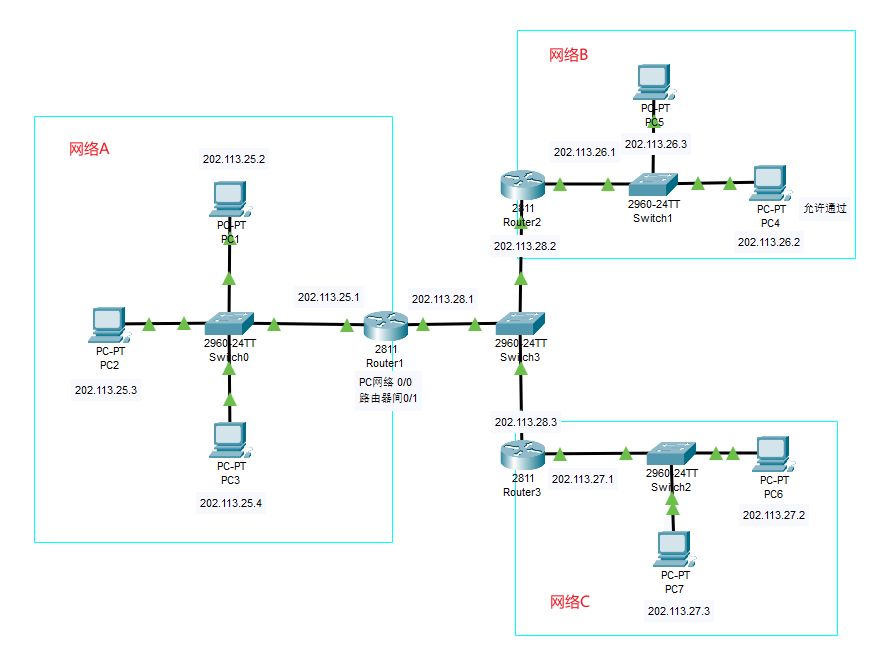
防火墙实验在虚拟仿真环境下完成，要求如下：

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。
5. **SSL实验（选做）**

SSL实验在实体环境下完成，要求如下：

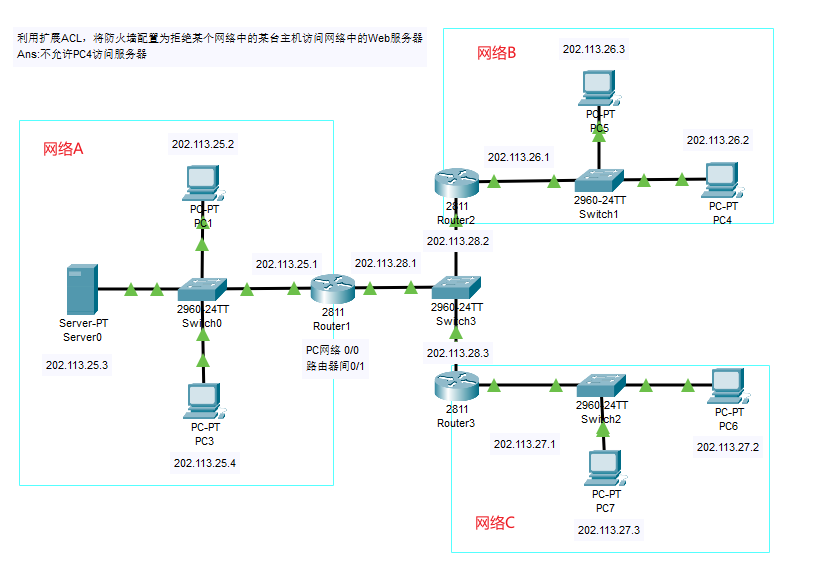
1. 完成Web服务器的证书生成、证书审批、证书安装、证书允许等整个过程。
2. 实现浏览器与Web服务器的安全通信。
3. **实验准备**
4. **搭建标准ACL网络拓扑图**

各个设备的IP设置以及网络划分如图中标签所示：



1. **搭建扩展ACL网络拓扑图**

各个设备的IP设置以及网络划分如图中标签所示：



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**

访问控制列表（ACL）是应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。也就是说，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，不同厂家生产的网络设备会有不同的处理方式。Cisco 生产的网络设备采用丢弃的方式，即如果所有规则都没有匹配成功,Cisco 网络设备将丢弃该数据包。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配置命令：**

**access−list ListNum (permit/deny) SrcIPAddr SrcWildMask**

ListNum: 为 ACL 的列表号，取值范围为 1～99。

permit/deny: 匹配成功后，网络设备釆取的动作。其中 permit为允许通过,deny为丢弃。

SrcIPAddr和SrcWildMask: 分别表示源起始IP地址和通配符，用于定义IP地址的范围; 在指定一台特定的主机时,可以使用host关键词;如果要表示任意的主机,可以使用any代替。

**扩展ACL配置命令：**

**access−list ListNum (permit/deny) Protocol SrcIPAddr SrcPort DesIPAddr DesPort**

ListNum: ACL号，取值范围为 101～199。拥有相同 ListNum 的规则属于同一个ACL, 其先后顺序按照加入的先后顺序定。

permit/deny: 匹配成功后，网络设备釆取的动作。其中permit为允许通过,deny为丢弃。

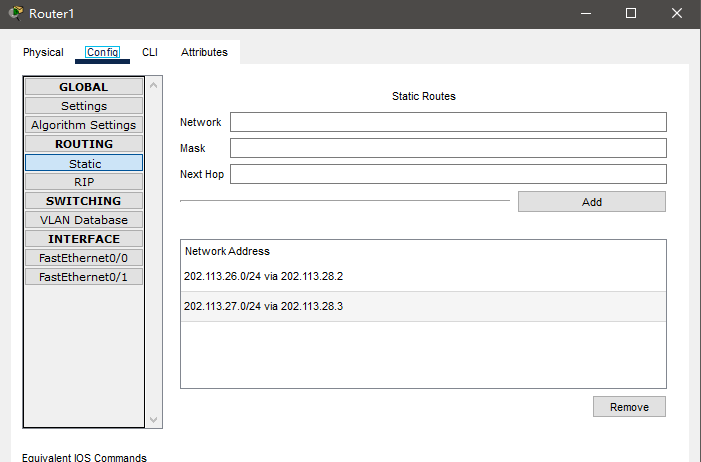
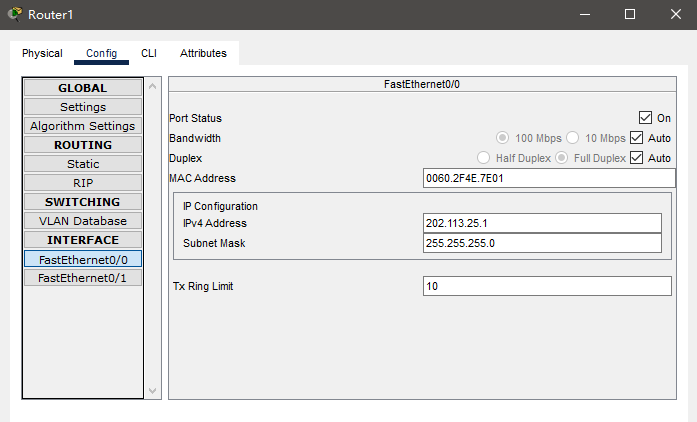
Protocol：指定该条规则适用的协议类型。协议类型可以是 ip、icmp、tcp、udp 等。 SrcIPAddr：指定源 IP 地址范围。如果只有一个 IP 地址，那么可以釆用“host IP 地址”的方式定义；如果要表示任意的主机，那么可以使用 any 代替。 SrcPort：指定源 TCP 或 UDP 端口范围。其中，“eq 端口号”用于指定一个具体端口。

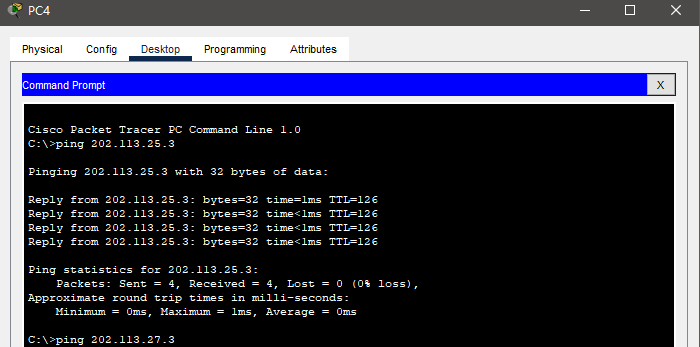
DesIPAddr：指定目的 IP 地址范围。

DesPort：指定目的 TCP 或 UDP 端口范围。

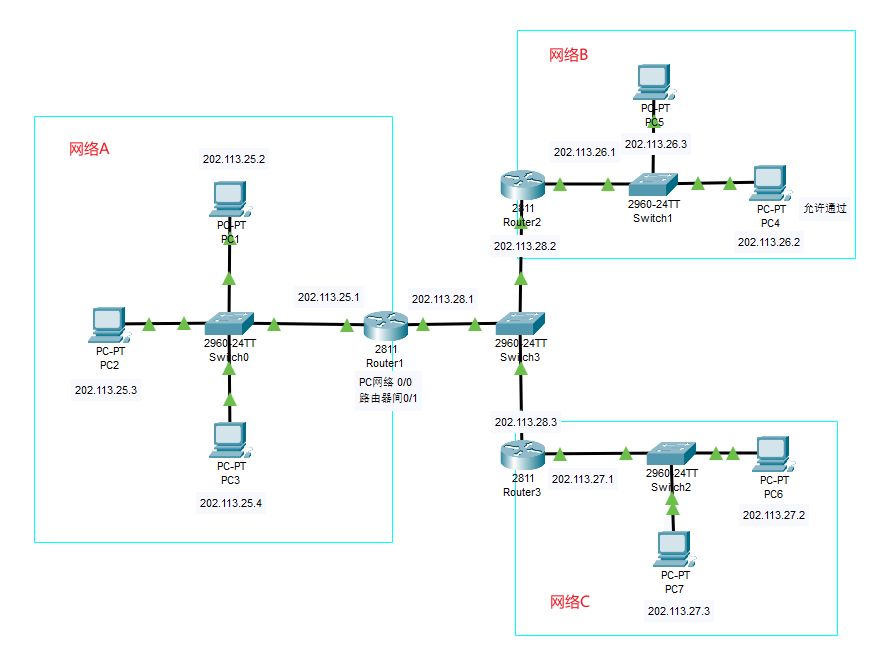
1. **实验过程**
2. **对网络中的设备进行配置**

如下图所示，使用思科提供的更加便捷的可视化界面对主机以及路由器进行配置，设置IP、使能端口、添加路由等，实现网络的正常连通。



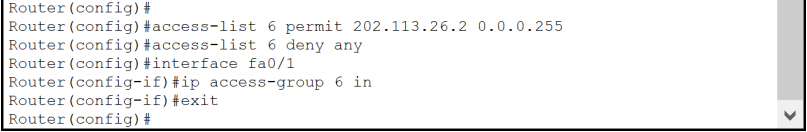


1. **利用标准ACL，将防火墙配置为只允许某个网络中的主机访问另一个网络。**



标准 ACL 是最简单的一种 ACL, 它利用 IP 数据报中的源 IP 地址对过往的数据报进行控

制。在 Router 中输入如下命令进行配置:



Router ( config )#access−list 6 permit 202.113.26.2 0.0.0.255

输入如上命令，路由器添加列表号为 6 的标准 ACL，只允许 ip 地址为 202.113.26.XX，也就是只允许网络B中的主机通过的规则。

Router ( config )#access−l i s t 6 deny any

过滤不属于已添加规则的主机发来的数据包，

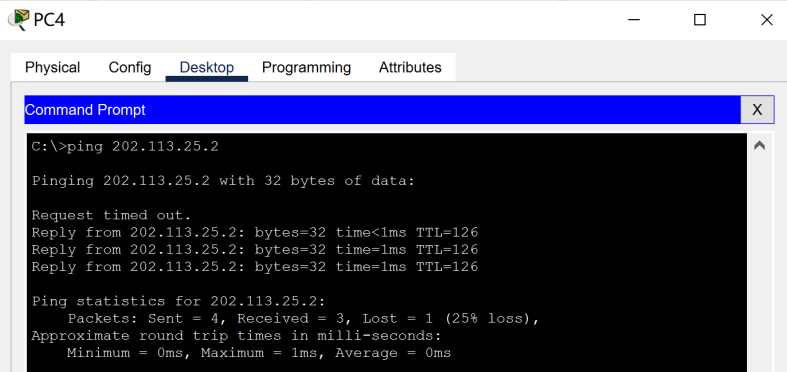
Router ( config )#interface fa0/1

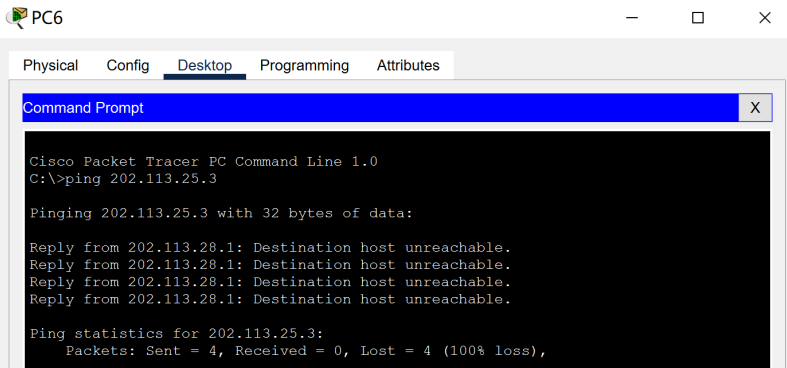
Router ( config−if )#ip access−group 6 in

Router ( config−if )#exit

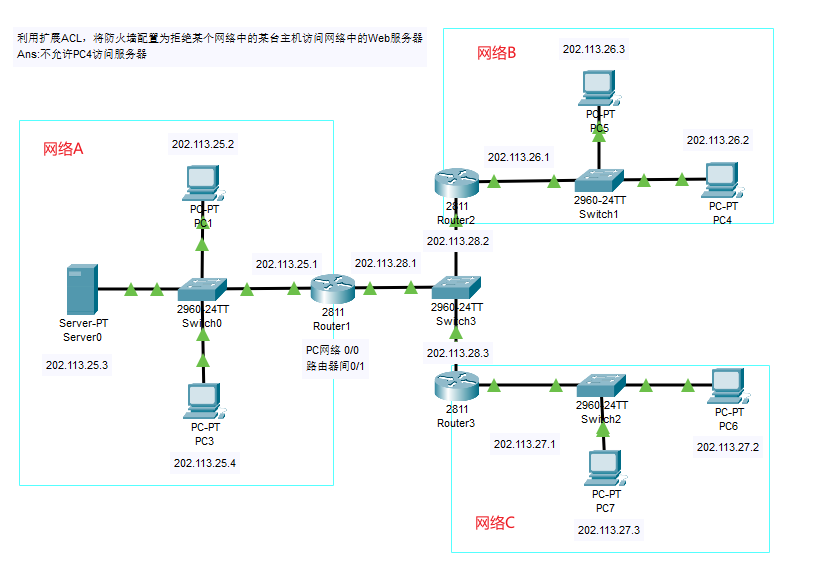
添加完规则之后，绑定路由器接口，确定是入站规则还是出站规则，此处绑定入站规则，从而实现只允许网络B的主机访问网络A中的主机。

配置完毕后进行验证，结果如下图可见，网络B中的PC4能够访问网络A的主机，但网路C中的PC6无法访问网络A中的主机：

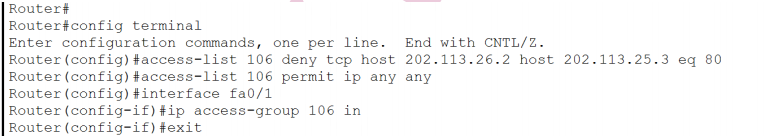




1. **利用扩展ACL，将防火墙配置为拒绝某个网络中的某台主机访问网络中的Web服务器**



路由器输入如下命令进行配置



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

路由器添加列表号为 106 的扩展 ACL，拒绝主机 ip 地 址为 202.113.25.3 的主机在 tcp 协议下通过，也就是拒绝主机 PC4 访问 Server0 服务器网页的规则。eq 80 指定了 80 端口，也就是 HTTP 协议使用的端口。

Router ( config )#access−list 106 permit ip any any

添加 ACL 规则后，路由器会默认过滤不属于已添加规则的主机发来的数据包，使用如上指令使除了 PC4 外的主机都能访问 Server0：

Router ( config )#interface fa0/1

Router ( config−if )#ip access−group 106 in

Router ( config−if )#exit

绑定路由器接口，确定是入站规则还是出站规则，此处绑定入站规则，从而实现只拒绝 PC4 访问网络 A 中的服务器。

配置完毕后进行验证，结果如下图可见，网络B中的PC4无法访问网络A中的服务器，但网络B中的PC5与网络C中的PC6均能够正常访问网络A中的服务器：

