南开大学
Nankai University

南　开　大　学

网络空间安全学院

网络技术与应用课程报告

防火墙和 SSL 实验

学号：2011897

姓名：任薏霖

年级：2020 级

专业：物联网工程

2022 年 12 月 4 日

第 1 节 实验内容说明

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。

第 2 节 实验准备

一、ACL 概述

ACL（AccessControlList，访问控制列表）是用来实现数据包识别功能的，在本次实验中使用 ACL 用于包过滤防火墙功能。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；

其具体工作流程图如下所示：

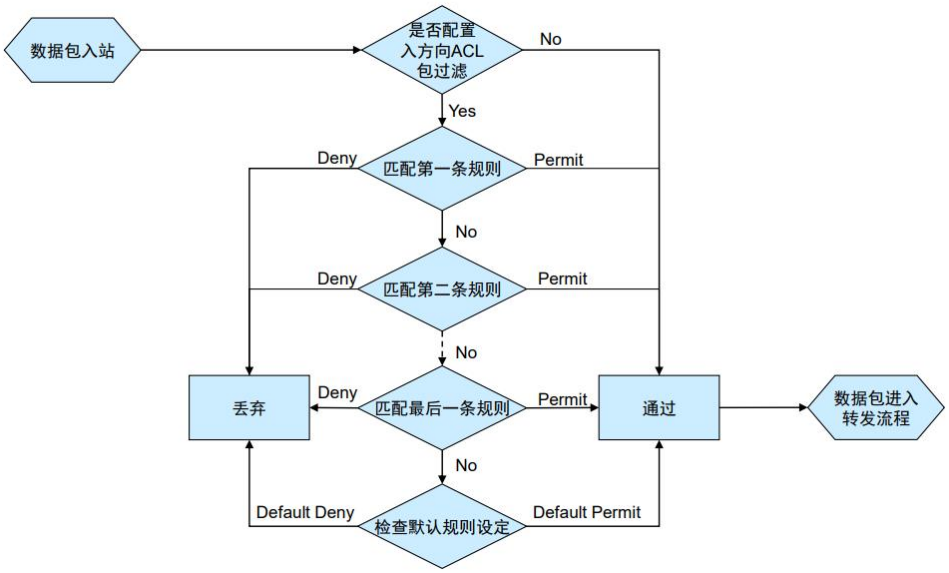

图 1 ACL 工作流程图

第 3 节 实验过程

1. 标准 ACL 实验

本次实验的主要目的是：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。因此需要在路由器 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。

1.1 主机 IP 地址和默认网关配置

本次实验所需配置的网络拓扑图如图 1 所示。

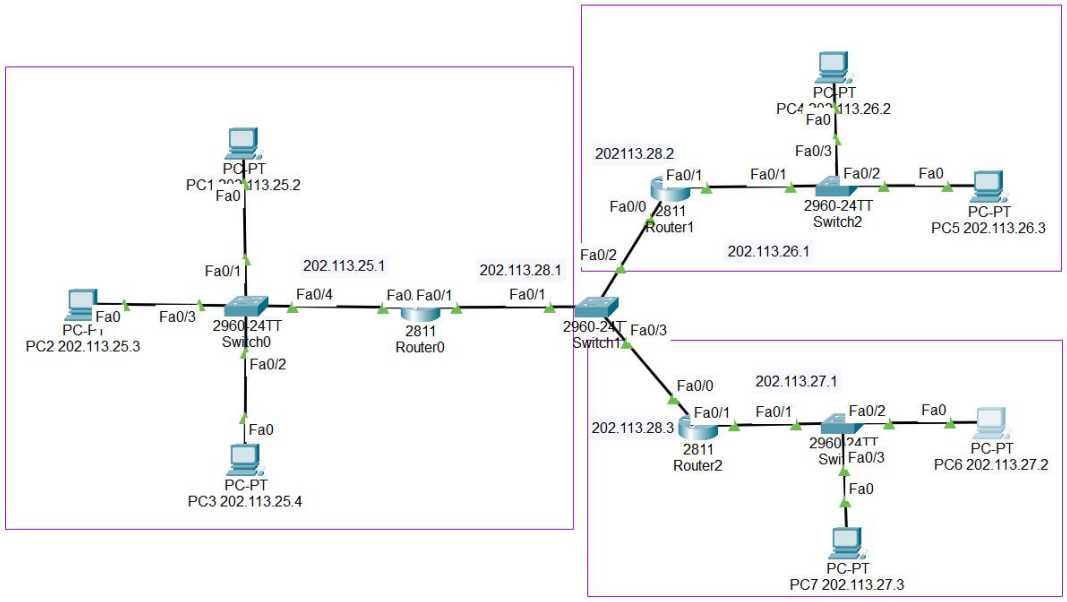

图 2 网络拓扑图

1.2 路由器 IP 地址及配置 ACL 功能

1.2.1 IP 地址配置

配置路由器 IP 地址，可以在配置界面中选择 CLI，首先使用 enable 命令进入路由器的特权执行模式，而后通过 config terminal 进入全局配置模式。需要注意，路由器通常具有两个或多个网络接口，地址属于某个特定接口。

在为接口配置 IP 地址之前，首先使用“interface 接口名”进入接口的配置模式，并使用 no shutdown 命令激活接口。并通过 router rip 为其配置动态路由表。

具体指令如下：

```
Router(config)#interface fa0/0
Router(config-if)#ip address 202.113.25.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fa0/1
Router(config-if)#ip address 202.113.28.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 202.113.25.0
Router(config-router)#network 202.113.28.0
```

1.2.2 配置标准访问控制列表

具体指令如下：

```
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
```

1.3 实验结果验证

1.3.1 未配置 ACL 时

网络 B 和其他网络均可以访问网络 A 中的主机，如下图所示：

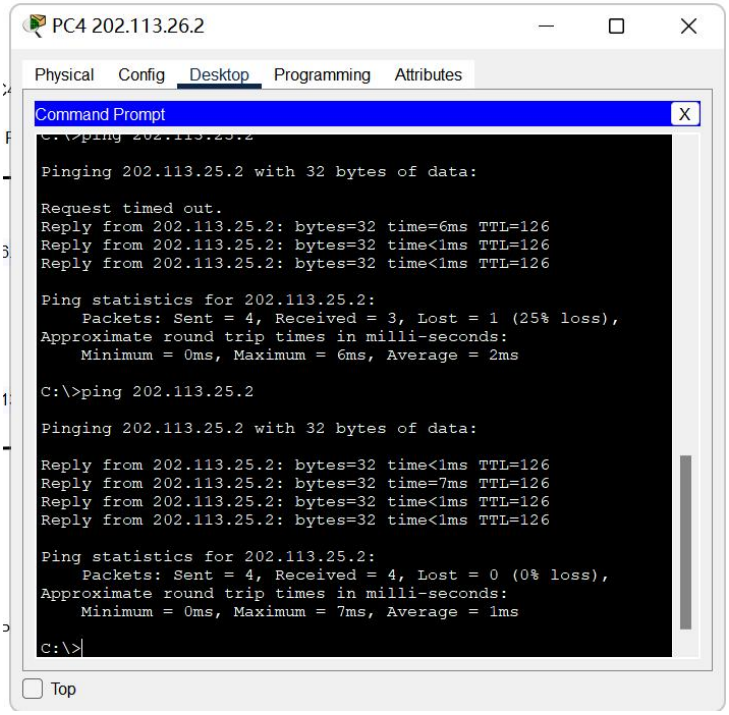

图 3 PC4 ping PC1

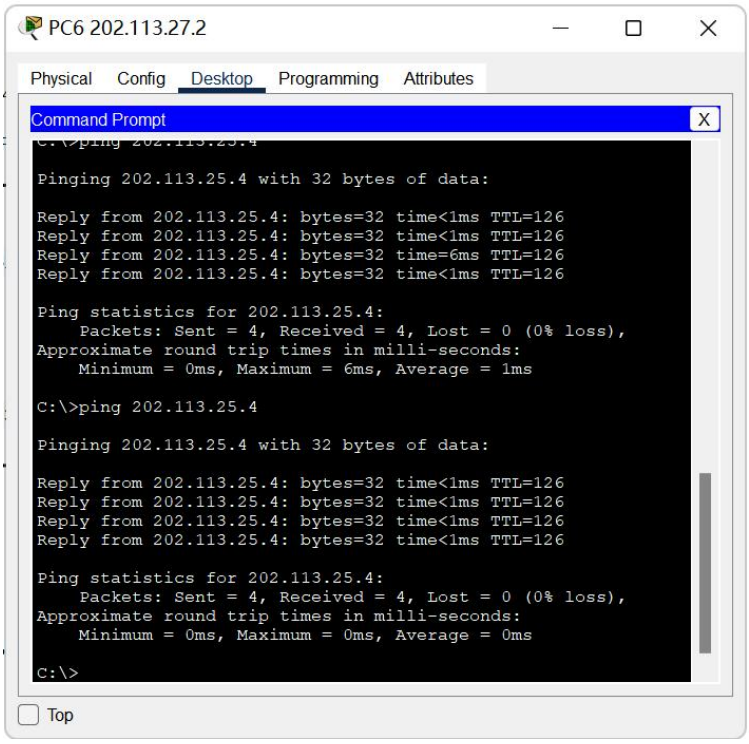

图 4 PC6 ping PC1

1.3.2 配置 ACL 后

网络 B 仍可以访问网络 A 的主机，而其他网络的主机访问网络 A 的主机时，显示无法到达，如下图所示：

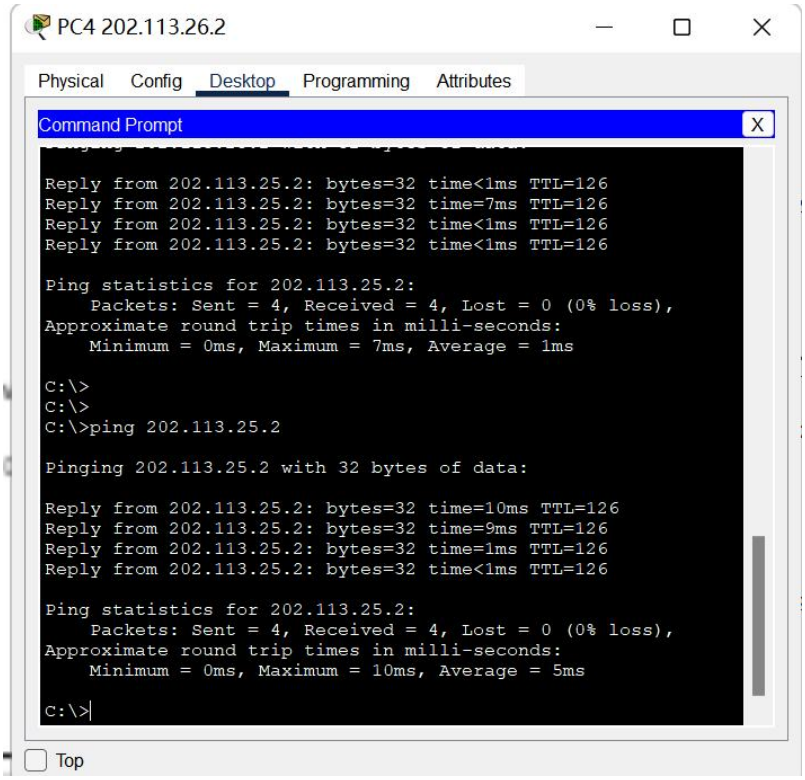

图 5 PC4 ping PC1

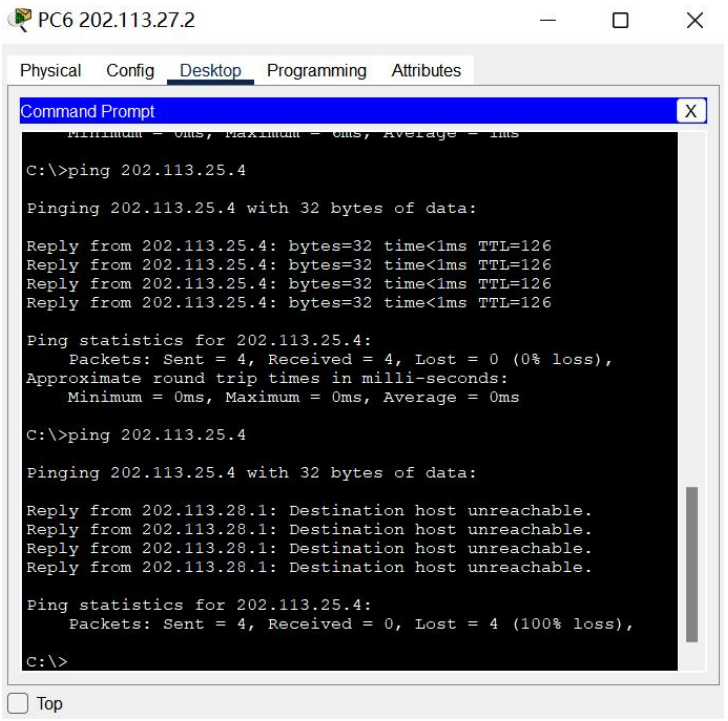

图 6 PC6 ping PC1

2. 扩展 ACL 实验

本次实验的主要目的在于，不允许网络 B 中的某个主机访问网络 A 中的 Web 服务。

2.1 主机 IP 地址和默认网关配置

本次实验所需配置的网络拓扑图如图 1 所示。

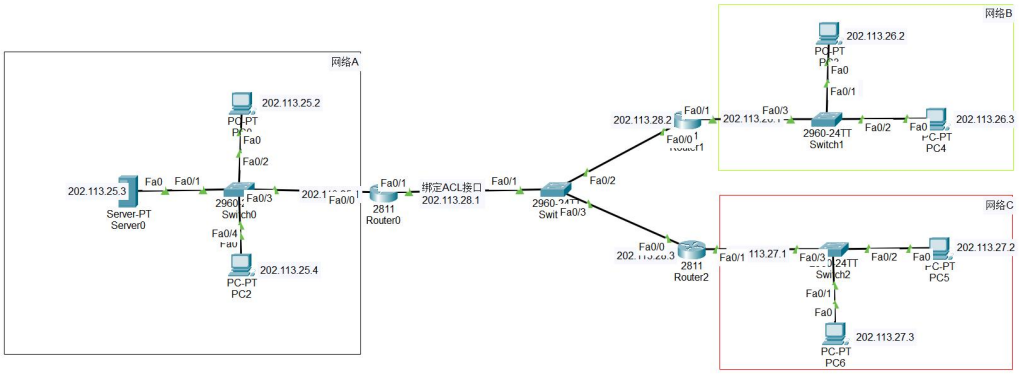

图 7 网络拓扑图

2.2 路由器 IP 地址及配置 ACL 功能

2.2.1 IP 地址配置

配置路由器 IP 地址，可以在配置界面中选择 CLI，首先使用 enable 命令进入路由器的特权执行模式，而后通过 config terminal 进入全局配置模式。需要注意，路由器通常具有

两个或多个网络接口，地址属于某个特定接口。

在为接口配置 IP 地址之前，首先使用“interface 接口名”进入接口的配置模式，并使用 no shutdown 命令激活接口。

具体指令如下：

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

Router(config-if)#exit
Router(config)#interface gig0/1
Router(config-if)#ip address 202.113.25.1 255.255.255.0
Router(config-if)#no shutdown
```

2.2.2 配置标准访问控制列表

具体指令如下：

```
Router(config)#access-list 106 deny tcp host 202.113.26.2 host 202.113.25.3 eq
80
Router(config)#access-list 106 deny any any
Router(config)#interface fa0/1
Router(config-if)#ip access-group 106 in
```

2.3 实验结果验证

2.3.1 配置拓展 ACL

网络 B 中的 PC3 无法访问网络 A 的 Web 服务器，而其他网络的主机访问网络 A 的服务器时，则显示可以，如下图所示：

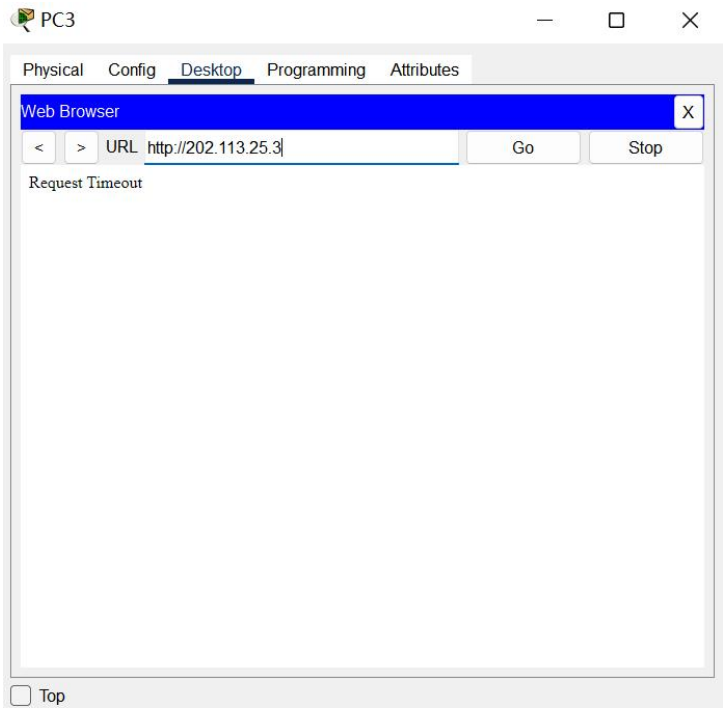

图 8 PC3 访问网络 A 中 Web 服务器

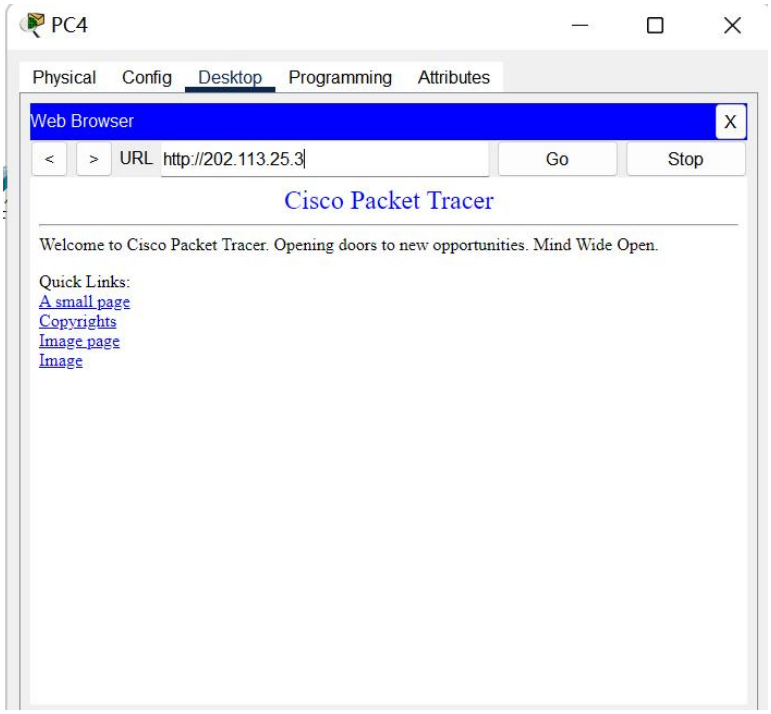

图 9 PC4 访问网络 A 中 Web 服务器