南開大學

网络技术与应用课程实验报告

实验 7：防火墙和 SSL 实验

学院：网络空间安全学院

专业：信息安全-法学

学号：2111954

姓名：许积君

目录

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。

- 标准访问控制列表——标准 ACL
  - 利用 IP 数据报中的源 IP 地址对过往的数据包进行控制
  - 列表号范围：1-99
- 扩展访问控制列表——扩展 ACL
  - 按照协议类型、源 IP 地址、目的 IP 地址、源端口号、目的端口号对过往的数据包进行控制，列表号范围：101-199

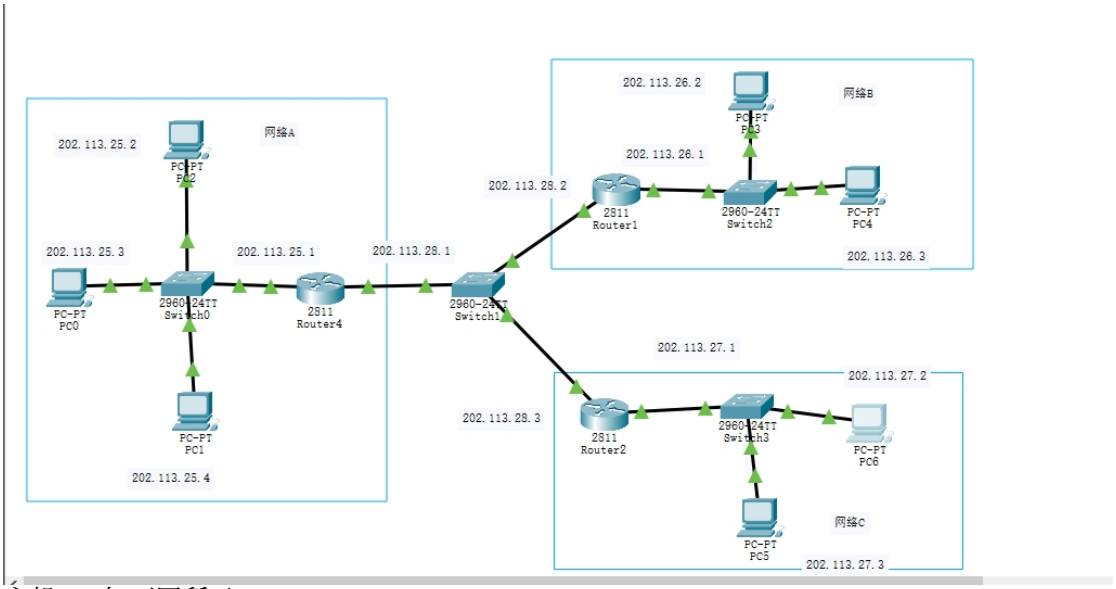
ACL 的包过滤技术具体可分为一下过程：

1. 对进出的数据包逐个过滤，丢弃或允许通过；
2. ACL 应用于接口上，每个接口的出入双向分别过滤；
3. 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；

二、 防火墙实验

（一） 标准 ACL 实验

1. 网络配置



主机 IP 如下图所示

主机号	IP 地址	掩码	默认路由	所在网络
PC0	202.113.25.3	255.255.255.0	202.113.25.1	A
PC1	202.113.25.4	255.255.255.0	202.113.25.1	A
PC2	202.113.25.2	255.255.255.0	202.113.25.1	A
PC3	202.113.26.2	255.255.255.0	202.113.26.1	B
PC4	202.113.26.3	255.255.255.0	202.113.26.1	B
PC5	202.113.27.3	255.255.255.0	202.113.27.1	C
PC6	202.113.27.2	255.255.255.0	202.113.27.1	C

路由器配置如下图所示

路由器号	端口	IP 地址	掩码	所在网络
Router4	0/0	202.113.25.1	255.255.255.0	A
Router4	0/1	202.113.28.1	255.255.255.0	A
Router1	0/0	202.113.28.2	255.255.255.0	B
Router1	0/1	202.113.26.1	255.255.255.0	B
Router2	0/0	202.113.28.3	255.255.255.0	C
Router2	0/1	202.113.27.1	255.255.255.0	C

路由器动态路由表具体配置命令如下:

```
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
=======================================router4
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 202.113.26.0
Router(config-router)#network 202.113.28.0
=======================================router1
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 202.113.27.0
Router(config-router)#network 202.113.28.0
=======================================router2
```

此时三个网络是联通的，分别由 B、C 网络的主机 pingA 网络的主机，可以 ping 通，结果如下图

```
Ping statistics for 202.113.25.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 202.113.25.3

Pinging 202.113.25.3 with 32 bytes of data:

Reply from 202.113.25.3: bytes=32 time=1ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time=6ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.25.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 202.113.25.3

Pinging 202.113.25.3 with 32 bytes of data:

Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.25.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2. 配置标准访问控制列表

具体指令如下，允许 B 网络的进入，其他网络都不允许

```
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
```

此时只有 B 网络能 ping 通 A 网络的主机，其他网络会显示无法到达

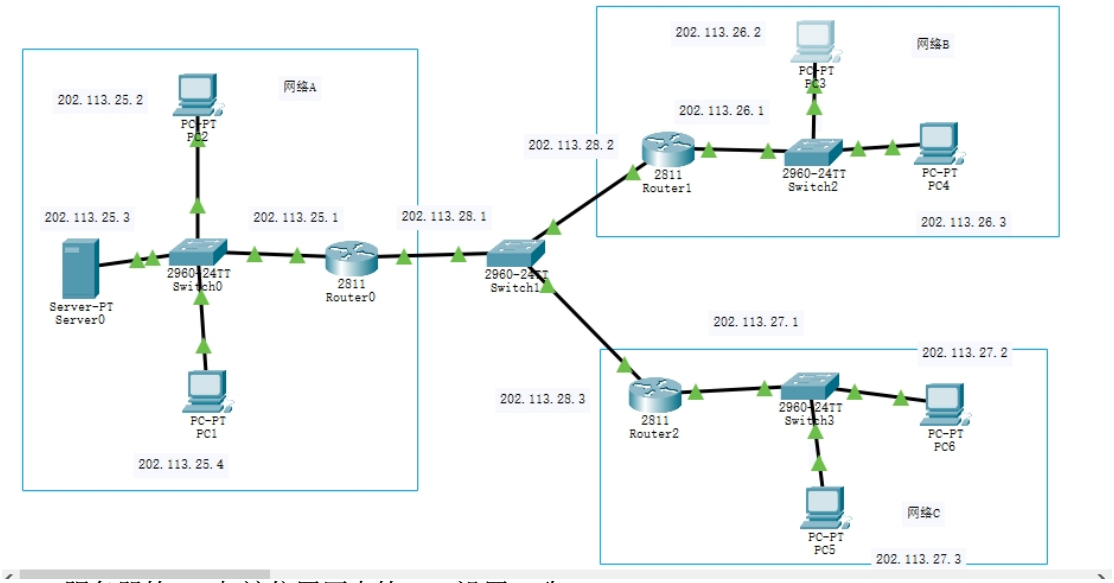
```
C:\>ping 202.113.25.3

Pinging 202.113.25.3 with 32 bytes of data:

Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time<1ms TTL=126
Reply from 202.113.25.3: bytes=32 time=1ms TTL=126

Ping statistics for 202.113.25.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

```
Packet Tracer PC Command Line 1.0
C:\>ping 202.113.25.3

Pinging 202.113.25.3 with 32 bytes of data:

Reply from 202.113.28.1: Destination host unreachable.
Reply from 202.113.28.1: Destination host unreachable.
Reply from 202.113.28.1: Destination host unreachable.
Reply from 202.113.28.1: Destination host unreachable.

Ping statistics for 202.113.25.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

（二） 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，而让其他主机都可以访问。

1. 网络配置

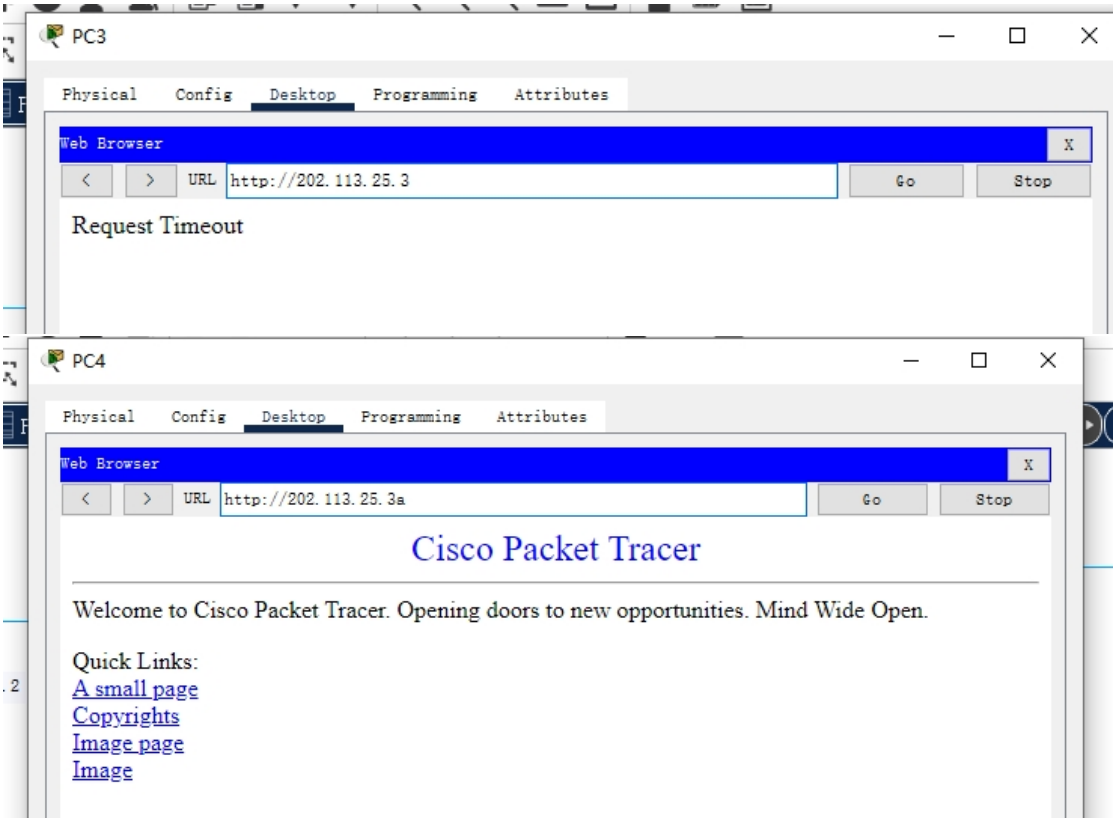


Web 服务器的 IP 与该位置原来的 PC 设置一致

2. 配置拓展 ACL

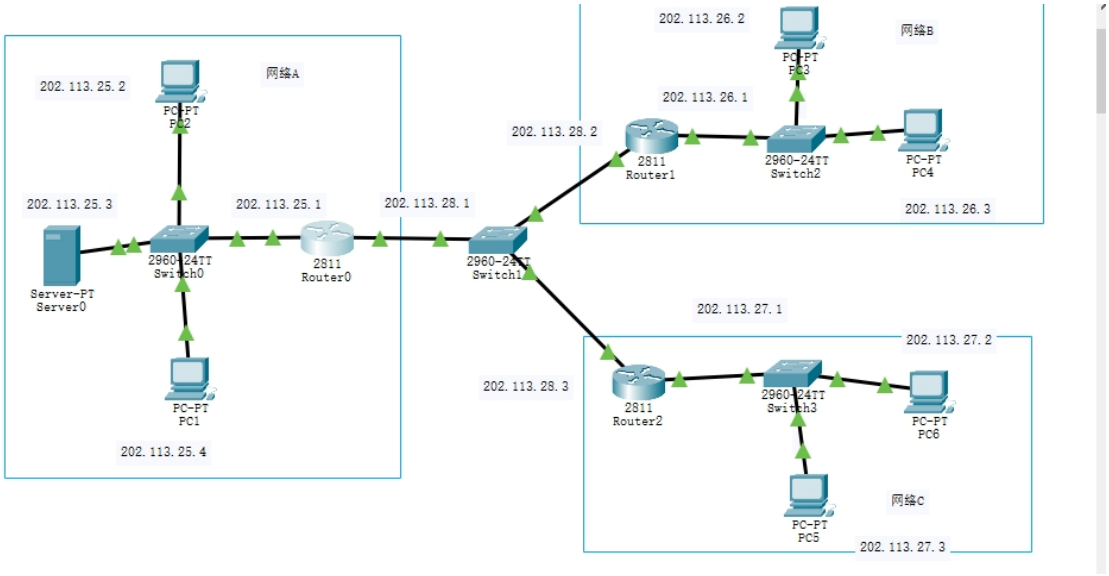
```
Router(config)#access-list 106 deny tcp host 202.113.26.2 host
    202.113.25.3 eq 80 //阻止PC3对Web服务器的访问
Router(config)#access-list 106 permit ip any any
Router(config)#interface fa0/1
Router(config-if)#ip access-group 106 in
Router(config-if)#exit
```

最终 PC3 访问 Web 服务器超时，而 PC4 仍然可以访问



（三） TCP 设置

1. 网络配置



2. 配置路由

```
! 创建用于允许外网回应内网连接的 ACL
access-list 101 permit tcp any 202.113.25.0 0.0.0.255 established
access-list 101 permit udp any 202.113.25.0 0.0.0.255 eq domain
```

```
! 防止外网用户主动向内网发起TCP连接
access-list 102 deny tcp any 202.113.25.0 0.0.0.255
access-list 102 permit ip any any

! 在外网接口应用 ACL
interface <外网接口>
  ip access-group 101 in
  ip access-group 102 out
```