

南 开 大 学

网络空间安全学院学院

网络技术与应用课程报告

第 7 次实验报告

学号：2011428

姓名：王天行

年级：2020 级

专业：密码科学与技术

2022 年 12 月 1 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。（可忽略）

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。

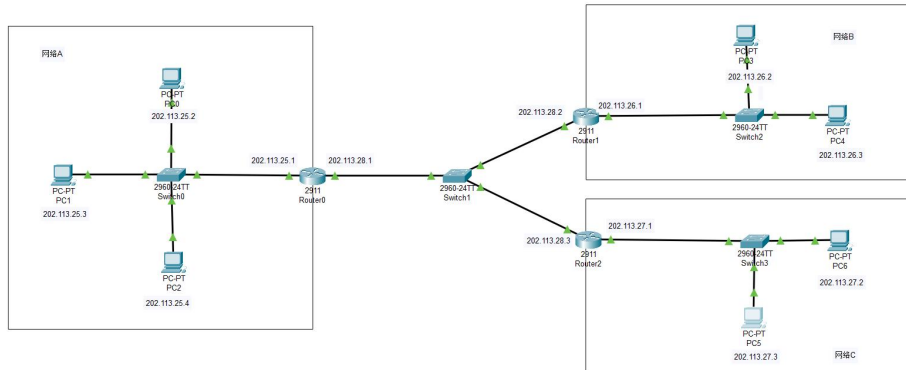
评分原则：

前期准备 25，实验过程 50，实验报告 25，总分 100。

第 2 节 实验准备

1.标准 ACL

拓扑网络：



三个路由器皆设置好动态路由。

此时三个网络间可以互相 ping 通：

1) 网络 A 中主机 ping 网络 B 和 C 中的主机

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 202.113.25.2

Pinging 202.113.25.2 with 32 bytes of data:

Reply from 202.113.25.2: bytes=32 time<1ms TTL=128
Reply from 202.113.25.2: bytes=32 time<1ms TTL=128
Reply from 202.113.25.2: bytes=32 time<1ms TTL=128
Reply from 202.113.25.2: bytes=32 time<1ms TTL=128

Ping statistics for 202.113.25.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 202.113.26.1

Pinging 202.113.26.1 with 32 bytes of data:

Reply from 202.113.26.1: bytes=32 time<1ms TTL=254
Reply from 202.113.26.1: bytes=32 time<1ms TTL=254
Reply from 202.113.26.1: bytes=32 time<1ms TTL=254
Reply from 202.113.26.1: bytes=32 time=5ms TTL=254

Ping statistics for 202.113.26.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms

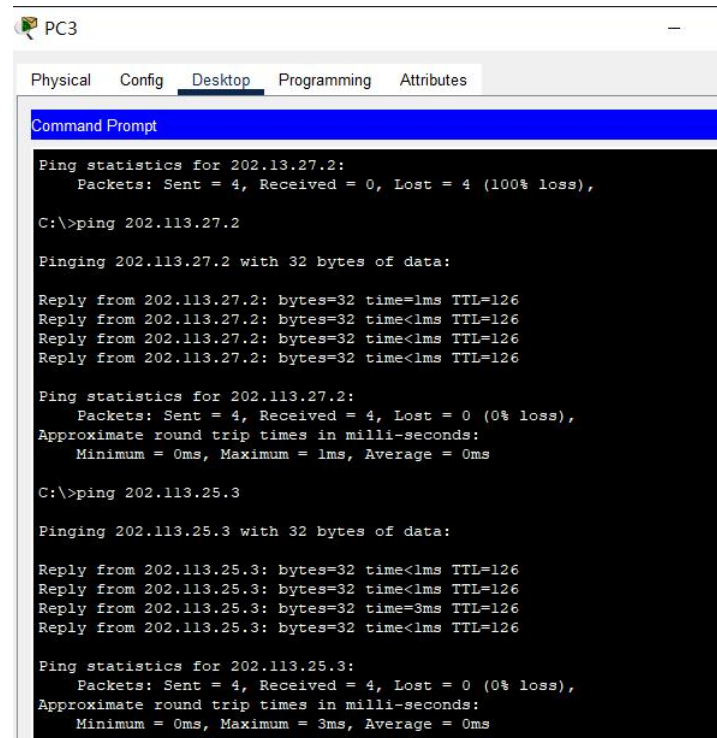
C:\>ping 202.113.27.2

Pinging 202.113.27.2 with 32 bytes of data:

Request timed out.
Reply from 202.113.27.2: bytes=32 time=4ms TTL=126
Reply from 202.113.27.2: bytes=32 time<1ms TTL=126
Reply from 202.113.27.2: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.27.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

2) 网络 B 中的主机 ping 网络 A 和 C 中的主机



PC3

Physical Config Desktop Programming Attributes

Command Prompt

```
Ping statistics for 202.113.27.2:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 202.113.27.2

Pinging 202.113.27.2 with 32 bytes of data:

Reply from 202.113.27.2: bytes=32 time<1ms TTL=126
Reply from 202.113.27.2: bytes=32 time<1ms TTL=126
Reply from 202.113.27.2: bytes=32 time<1ms TTL=126
Reply from 202.113.27.2: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.27.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

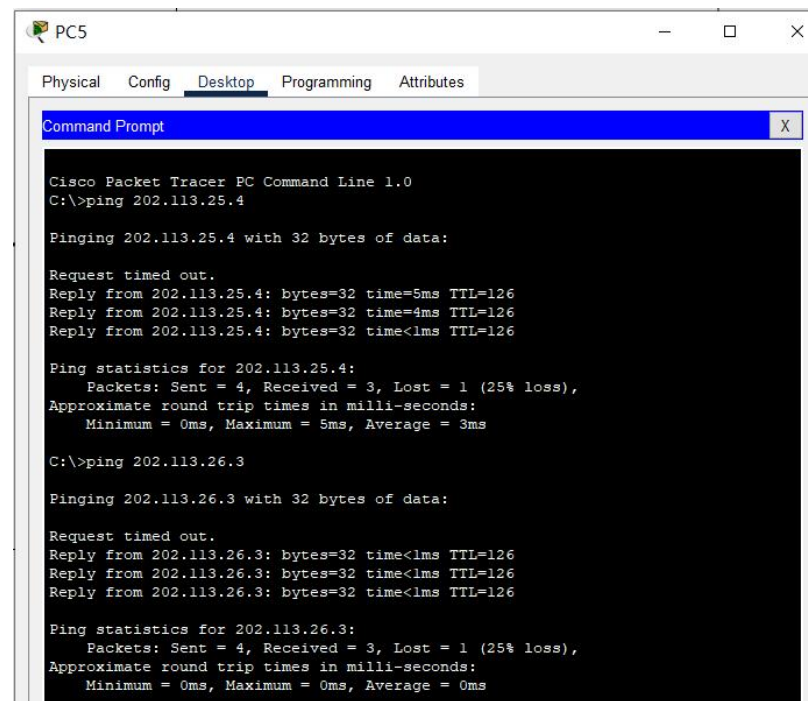
C:\>ping 202.113.25.3

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=3ms 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 = 3ms, Average = 0ms
```

3) 网络 C 中的主机 ping 网络 A 和 B 中的主机



PC5

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 202.113.25.4

Pinging 202.113.25.4 with 32 bytes of data:

Request timed out.
Reply from 202.113.25.4: bytes=32 time=5ms TTL=126
Reply from 202.113.25.4: bytes=32 time=4ms TTL=126
Reply from 202.113.25.4: bytes=32 time<1ms TTL=126

Ping statistics for 202.113.25.4:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 3ms

C:\>ping 202.113.26.3

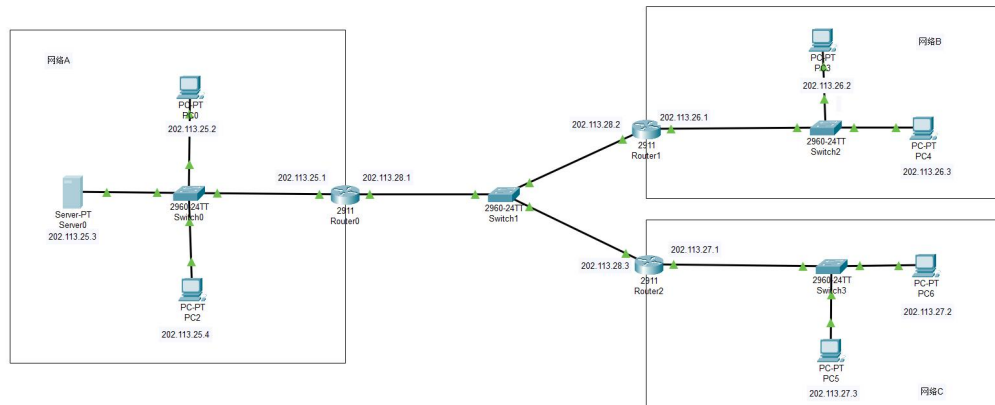
Pinging 202.113.26.3 with 32 bytes of data:

Request timed out.
Reply from 202.113.26.3: bytes=32 time<1ms TTL=126
Reply from 202.113.26.3: bytes=32 time<1ms TTL=126
Reply from 202.113.26.3: bytes=32 time<1ms TTL=126

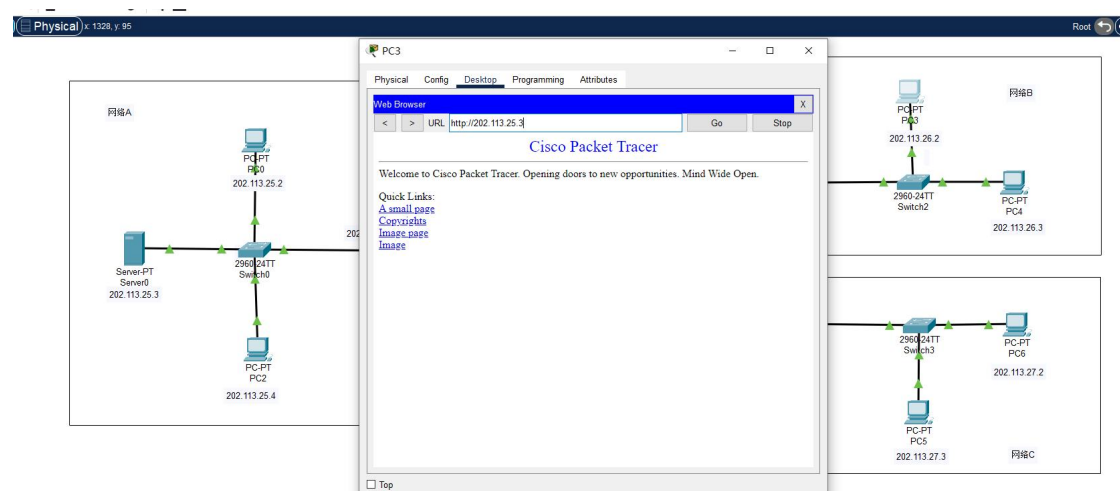
Ping statistics for 202.113.26.3:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. 扩展 ACL

拓扑图：



此时网络 B 中的主机可以访问 web 服务器



第 3 节 实验过程

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。

设置 access-list

```
Router(config)#access-list 1 permit 202.113.26.0 0.0.0.255
Router(config)#
Router(config)#access-list 1 deny any
^
% Invalid input detected at '^' marker.
Router(config)#access-list 1 deny any
```

绑定到路由器接口入栈方向

```
Router(config)#interface g1/0/1
Router(config-if)#ip access-group 1 in
```

此时，网络 B 中的主机可以 ping 通网络 A 中的主机

```
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
```

网络 C 中的主机无法 ping 通网络 A 中的主机

```
C:\>ping 202.113.25.4

Pinging 202.113.25.4 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 202.113.25.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2、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。

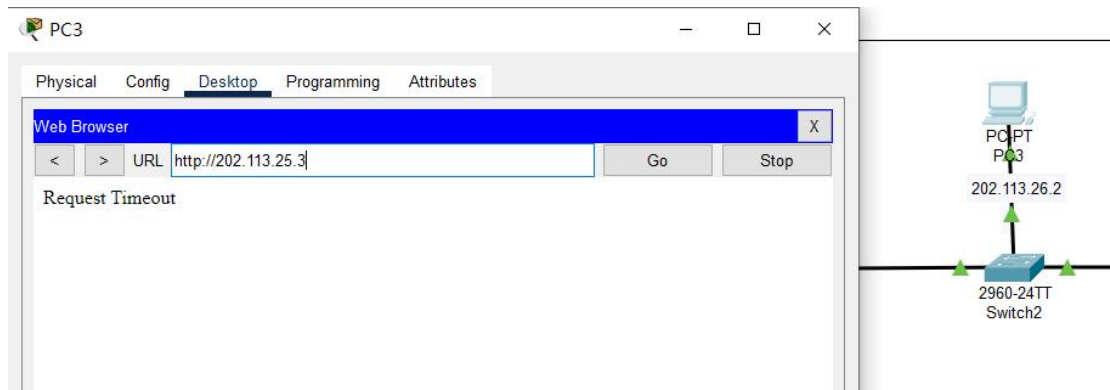
配置扩展 ACL

```
Router(config)#access-list 101 deny tcp host 202.113.26.2 host 202.113.25.3 eq 80
Router(config)#access-list 101 permit ip any any
```

绑定到路由器接口

```
Router(config-if)#ip access-group 101 in
```

此时，网络 B 中的主机（202.113.26.2）无法访问 web 服务器



网络 C 中的主机可以访问 web 服务器

