

# 《计算机网络》实验报告

\_\_\_\_信息\_\_\_\_学院 \_\_\_\_计算机科学与技术\_\_\_\_专业\_\_\_\_2020\_\_\_\_级

实验时间\_\_\_\_2022\_\_\_\_年\_\_\_\_10\_\_\_\_月\_\_\_\_17\_\_\_\_日

姓名\_\_\_\_胡诚皓\_\_\_\_学号\_\_\_\_20201060330\_\_\_\_

实验名称\_\_\_\_三层交换机的访问控制\_\_\_\_

实验成绩\_\_\_\_

## 一、实验目的

- (1) ACL (标准访问控制列表) 能正常工作的前提是所有主机都能 ping 通。
- (2) 设置三层交换机的 IP 地址及配置路由信息协议 (RIP) 路由。
- (3) 根据以上拓扑划分出的两个网段，要求禁止主机 PC4 访问 172.1.1.0/24 网段。该如何实现？

## 二、实验仪器设备及软件

- (1) Cisco Packet Tracer 8.1.1 模拟器
- (2) 4 台 PC
- (3) 2 台 2960 交换机
- (4) 2 台 3560 交换机

## 三、实验方案

先使用 2960 交换机正确配置好两个子网，再使用 3560 交换机将两个子网进行连接，最后通过设置 3560 的 ACL 表实现访问控制。

## 四、实验步骤

### 1. 网络的连接与地址设置

(1) 使用直通线 (Straight-Through) 将 PC1、PC2 连接到左侧的 S1 交换机，PC3、PC4 连接到右侧的 S2 交换机；再使用交叉线 (Cross-Over) 将 S1、S2 分别连接到具有路由功能的三层交换机 SwitchA、SwitchB。

---

(2) PC1、PC2 属于网络 172.1.1.0/24；PC3、PC4 属于网络 172.2.2.0/24，分配配置 PC1~PC4 的 IP 地址为 172.1.1.2/24、172.1.1.3/24、172.2.2.2/24、172.2.2.3/24

(3) 使用 ip routing 开启两个 3560 的路由功能，进入端口配置模式后使用 no switchport 修改 f0/1、f0/2 处于路由模式下。对于 SwitchA，配置 f0/1、f0/2 的 IP 地址分别为 192.168.1.1/24、172.1.1.1/24；对于 SwitchB，配置 f0/1、f0/2 的 IP 地址分别为 192.168.1.2/24、172.2.2.1/24。

(4) 将 SwitchA 的 f0/2 作为网络 172.1.1.0/24 的网关，即配置 PC1 与 PC2 的默认网关为 172.1.1.1；将 SwitchB 的 f0/2 作为网络 172.2.2.0/24 的网关，即配置 PC3 与 PC4 的默认网关为 172.2.2.1

## 2. 配置三层交换机的 RIP 协议并测试网络连通性

(1) 在全局配置模式下使用 router rip 进入 RIP 路由协议配置界面，使用 version 2 设置为 RIP2，使用 network ip\_addr 为 RIP 协议添加直连的网络的 IP。为 SwitchA 添加 172.1.1.0、SwitchB 添加 192.168.1.0。

(2) 测试 PC1 与 PC2、PC1 与 PC3 之间的连接是否通畅，并查看两个三层交换机的路由表情况。

## 3. 配置 SwitchA 的 ACL 表，禁止 PC4 访问 172.1.1.0/24 网段

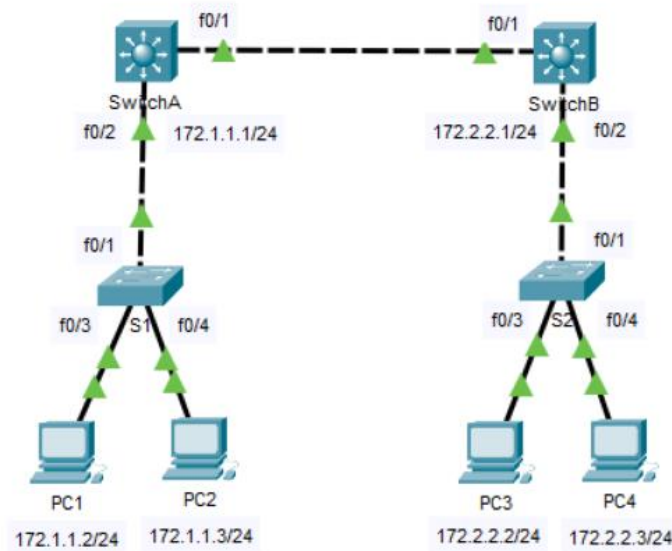
(1) 使用 access-list 命令在 SwitchA 中添加一个 ACL 扩展表，禁止 172.2.2.3 的 IP 访问 172.1.1.0/24 网段。

(2) 进入 SwitchA f0/2 的端口配置模式，将添加好的 ACL 表应用到该端口上，并且配置为出站流量规则。

(3) 分别使用 PC3 与 PC4 ping 172.1.1.0/24 网段，查看是否成功限制访问。

## 五、实验结果及分析

网络拓扑结构图如下。



配置好 RIP 协议后，两个子网可以互相 ping 通，也就是各台主机之间都能 ping 通。下图为 PC1 ping PC3 的结果。

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.2.2.2

Pinging 172.2.2.2 with 32 bytes of data:

Reply from 172.2.2.2: bytes=32 time=9ms TTL=126
Reply from 172.2.2.2: bytes=32 time=11ms TTL=126
Reply from 172.2.2.2: bytes=32 time=12ms TTL=126
Reply from 172.2.2.2: bytes=32 time=11ms TTL=126

Ping statistics for 172.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 12ms, Average = 10ms
C:\>
```

下图分别为在两个子网互相通信之后，SwitchA 与 SwitchB 上的路由表。

```
SwitchA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    172.1.0.0/24 is subnetted, 1 subnets
C       172.1.1.0 is directly connected, FastEthernet0/2
R       172.2.0.0/16 [120/1] via 192.168.1.2, 00:00:19, FastEthernet0/1
C       192.168.1.0/24 is directly connected, FastEthernet0/1
```

SwitchA#

```
SwitchB#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

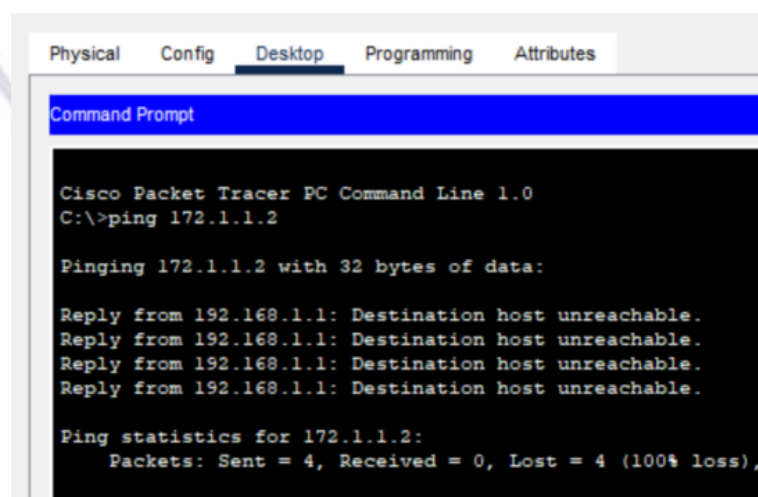
Gateway of last resort is not set

R       172.1.0.0/16 [120/1] via 192.168.1.1, 00:00:07, FastEthernet0/1
    172.2.0.0/24 is subnetted, 1 subnets
C       172.2.2.0 is directly connected, FastEthernet0/2
C       192.168.1.0/24 is directly connected, FastEthernet0/1
```

SwitchB#

对 SwitchA 的 f0/2 端口应用 ACL 规则后，从 PC4 已经无法到达 172.1.1.0/24 网段。下图为 PC4 ping PC1 的结果。

PC4



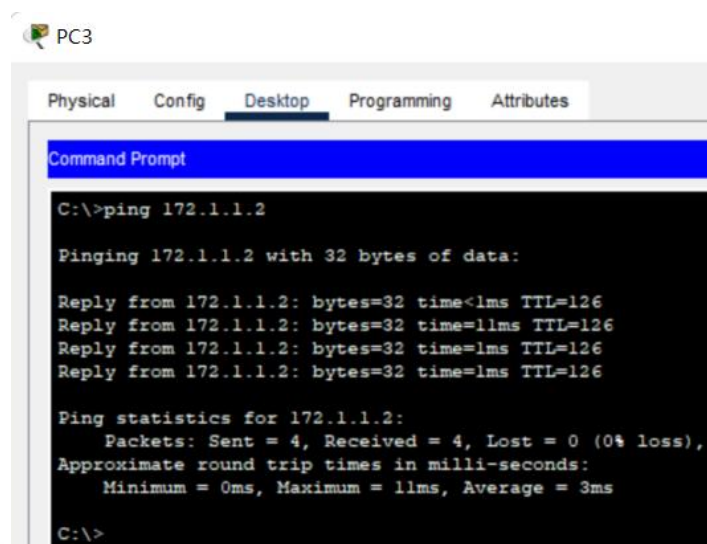
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.1.1.2

Pinging 172.1.1.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 172.1.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

下图为 PC3 ping PC1 的结果。



下图为 SwitchA 的 ACL 表。

```
SwitchA#show access-lists
Extended IP access list 100
 10 deny ip host 172.2.2.3 172.1.1.0 0.0.0.255 (4 match(es))
 20 permit ip 172.2.2.0 0.0.0.255 172.1.1.0 0.0.0.255
SwitchA#
```

## 六、实验总结及体会

### (1) 对 ACL 表定义命令 `access-list` 的理解

`access-list` 命令用于在全局配置模式下定义和删除 ACL 访问控制列表，对于 1~99 号标准 ACL 表，只能根据源地址来限制访问，而 100~199 号扩展 ACL 表，可以针对不同的协议、协议的特征、端口号、时间范围等定义过滤规则。

源地址通配符掩码不能简单地理解为子网掩码的反码，其意义是不同的。源地址通配符掩码中的 0 表示该位需要严格与指定的源地址相同、1 则表示该位任意（即该位 1/0 都能匹配上，不管指定源地址中是什么）

标准 ACL 创建的基本格式为“`access-list list-number deny/permit 源地址/any 源地址通配符掩码`”，由于是标准 ACL 其中的 `list-number` 需要定义在 1~99 之间，源地址可以是一个网络的地址，也可以是一个主机的 IP 地址。

扩展 ACL 创建的基本格式为“`access-list list-number deny/permit 过滤的依据 源地址/any 源地址通配符掩码 根据过滤依据的具体规则`”，由于是扩展 ACL 其中的 `list-number` 需要定义在 100~199 之间，过滤的依据可以选择各种协议进行



过滤，包括 ip、tcp、udp、icmp 等，后面的具体规则根据选择的协议不同有具体区别。

## （2）对出站入站的理解

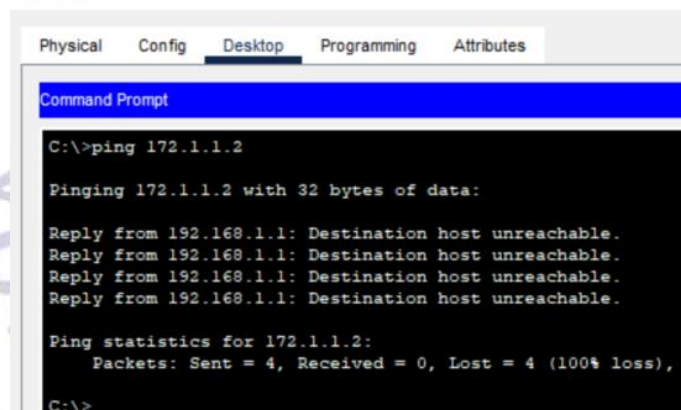
在将 ACL 表应用于某接口时，需要指定限制的流量方向，这个方向分为出站和入站，是对该接口所在设备来说的方向。

在上文的配置中，限制 PC4 访问 172.1.1.0/24 网段事实上是限制了 PC4 在 SwitchA 上向外向 172.1.1.0/24 发送信息。

若要在 SwitchA 的接口 f0/1 接口上设置 ACL，只要先删除原先 f0/2 接口上配置的规则，再在该接口的接口配置模式中使用 ip access-group 100 in 命令即可。

```
SwitchA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA(config)#int f0/2
SwitchA(config-if)#no ip ac
SwitchA(config-if)#no ip access-group 100 out
SwitchA(config-if)#exit
SwitchA(config)#int f0/1
SwitchA(config-if)#ip access-group 100 in
```

PC4



## （3）制定其他访问限制的练习

实验指导书中的第二个思考题，要求进行 ACL 配置，满足下面的要求：

- ① PC1 能访问 PC3
- ② PC1 不能访问 PC4
- ③ PC2 能访问 PC4
- ④ PC2 不能访问 PC3

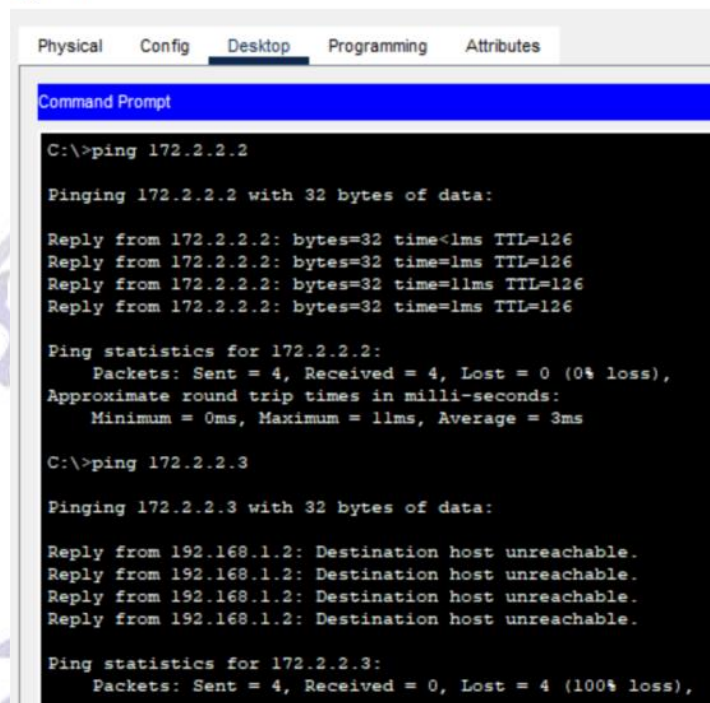
很显然，可以在 SwitchB 上新建一个具体到某个主机 IP 的 ACL 表。

在 SwitchB 上配置的 ACL 如下图，100 号扩展 ACL 表应用于 f0/2 的出站规则上。

```
SwitchB#show access-lists
Extended IP access list 100
 10 deny ip host 172.1.1.2 host 172.2.2.3 (1 match(es))
 20 deny ip host 172.1.1.3 host 172.2.2.2
 30 permit ip 172.1.1.0 0.0.0.255 172.2.2.0 0.0.0.255
SwitchB#
```

下图为 PC1 ping PC3 与 PC4 的情况。

PC1



```
Command Prompt

C:\>ping 172.2.2.2

Pinging 172.2.2.2 with 32 bytes of data:

Reply from 172.2.2.2: bytes=32 time<1ms TTL=126
Reply from 172.2.2.2: bytes=32 time=1ms TTL=126
Reply from 172.2.2.2: bytes=32 time=11ms TTL=126
Reply from 172.2.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 172.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>ping 172.2.2.3

Pinging 172.2.2.3 with 32 bytes of data:

Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.

Ping statistics for 172.2.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

下图为 PC2 ping PC3 与 PC4 的情况。

PC2

```
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.2.2.2

Pinging 172.2.2.2 with 32 bytes of data:

Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.
Reply from 192.168.1.2: Destination host unreachable.

Ping statistics for 172.2.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.2.2.3

Pinging 172.2.2.3 with 32 bytes of data:

Reply from 172.2.2.3: bytes=32 time<1ms TTL=126
Reply from 172.2.2.3: bytes=32 time=11ms TTL=126
Reply from 172.2.2.3: bytes=32 time=11ms TTL=126
Reply from 172.2.2.3: bytes=32 time=11ms TTL=126

Ping statistics for 172.2.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 8ms

C:\>|
```

七、教师评语