

# 《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\_\_\_\_11\_\_\_\_月\_\_\_\_28\_\_\_\_日

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

实验名称\_\_\_\_访问控制列表（ACL）实验\_\_\_\_

实验成绩\_\_\_\_

## 一、实验目的

- (1) ACL 能正常工作的前提是所有主机都能 ping 通。
- (2) 掌握路由器的基本配置：设置路由器接口的 IP 地址、配置 RIP 路由。
- (3) 根据以上拓扑划分出的两个网段，禁止主机 PC6 访问 172.1.1.0/24 网段。

## 二、实验仪器设备及软件

- (1) Cisco Packet Tracer 8.2.0 模拟器
- (2) 6 台 PC
- (3) 2 台 4331 路由器
- (3) 2 台 2970 交换机

## 三、实验方案

使用 4331 路由器进行实验，需要在路由器上添加串口，两个网段中分别 3 台 PC，两个路由器之间使用串口通信，

## 四、实验步骤

### 1. 路由器的基本配置

- (1) 配置两个路由器的接口 IP 地址并将其开启
- (2) 配置各 PC 的 IP 地址及默认网关

## 2. 配置 RIP

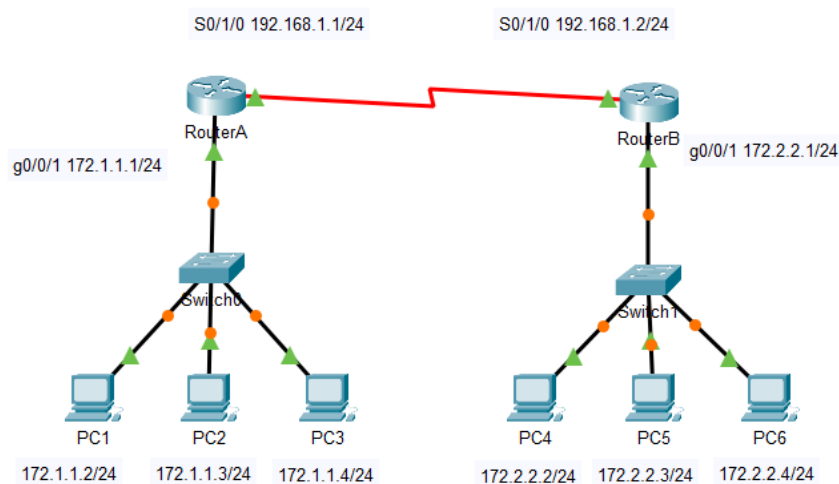
- (1) 配置两个路由器的 RIP 协议，添加与之直接相连网络的网段
- (2) 测试两个网段之间是否能连通

## 3. 配置 ACL

- (1) 在路由器 A 配置 ACL，使得 PC6 无法访问 172.1.1.0/24 网段
- (2) 测试 PC6 到 172.1.1.0/24 网段的连通性
- (3) 删除刚刚设置的 ACL 限制
- (4) 再次测试 PC6 到 172.1.1.0/24 网段的连通性

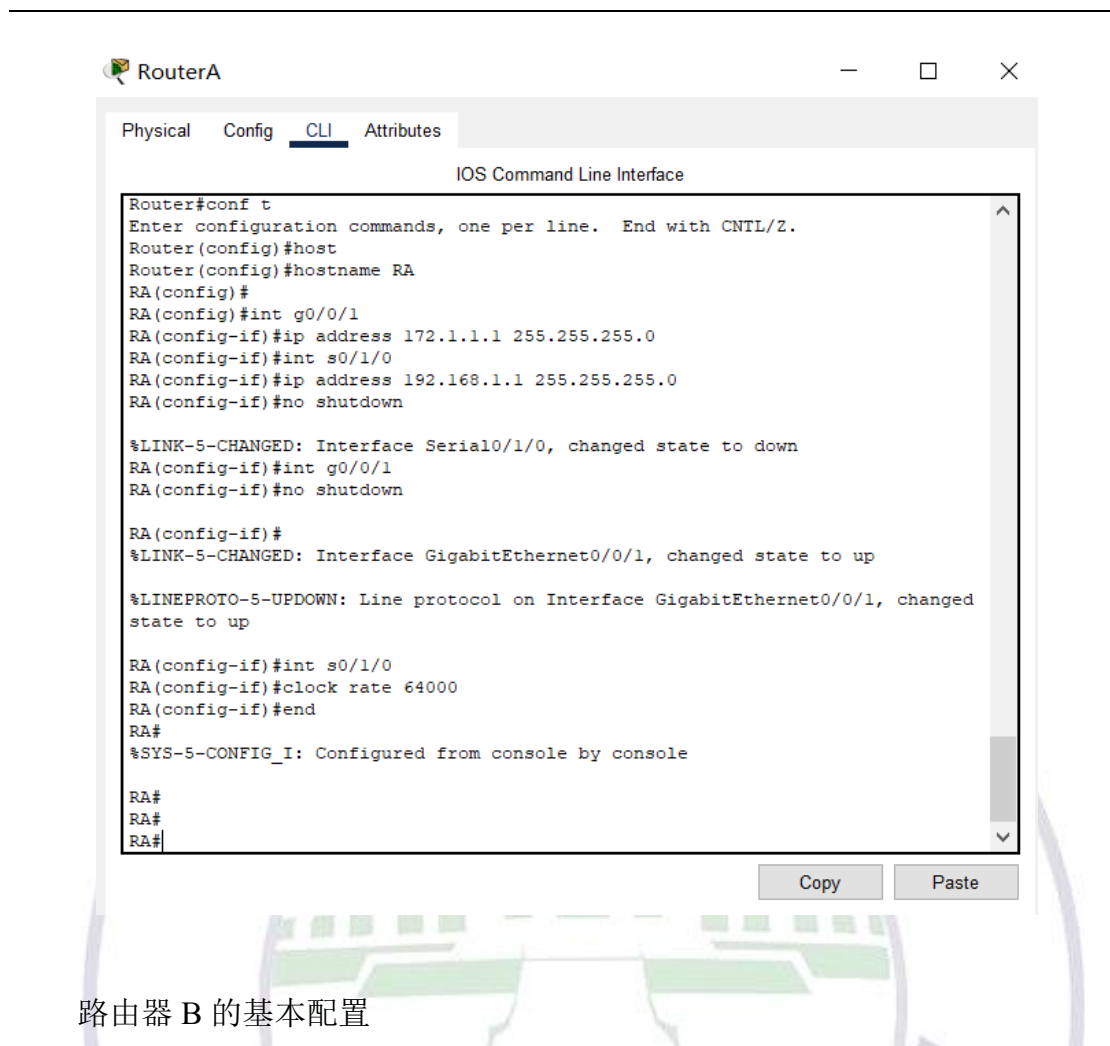
## 五、实验结果及分析

网络拓扑结构图如下

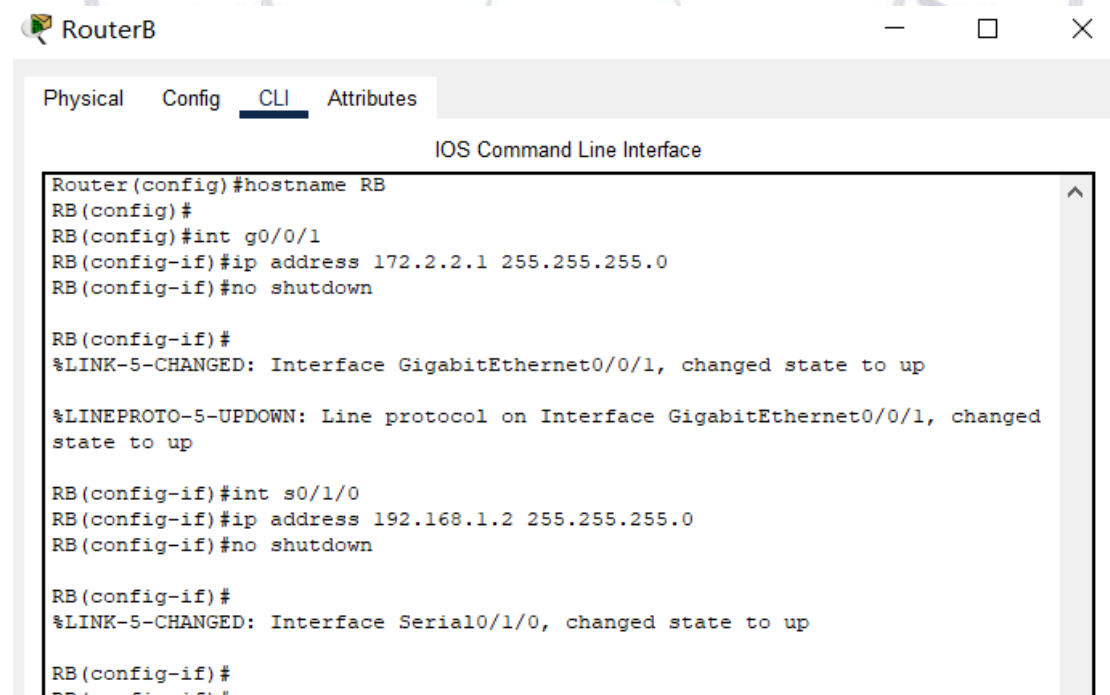


## 1. 路由器的基本配置

路由器 A 的基本配置



路由器 B 的基本配置



各台 PC 的 IP 及网关配置

名称	IP 地址	网关
PC1	172.1.1.2/24	172.1.1.1
PC2	172.1.1.3/24	172.1.1.1
PC3	172.1.1.4/24	172.1.1.1
PC4	172.2.2.2/24	172.2.2.1
PC5	172.2.2.3/24	172.2.2.1
PC6	172.2.2.4/24	172.2.2.1

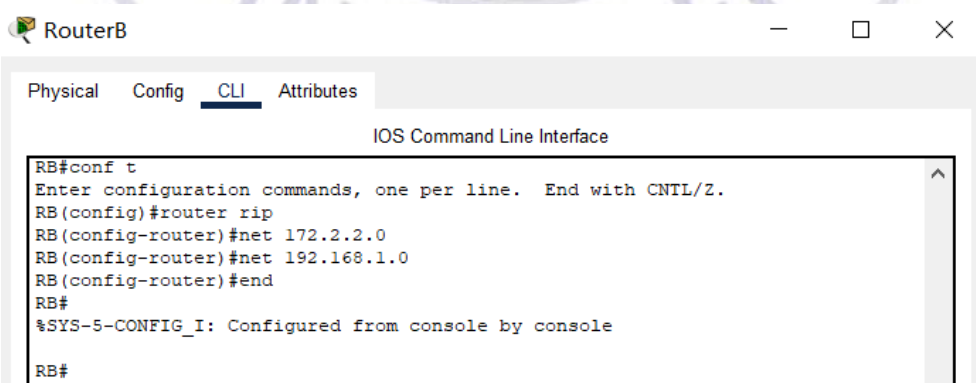
## 2. 配置 RIP

给路由器 A 设置 RIP 协议，添加 172.1.1.0 与 192.168.1.0 两个与之直接相连的网络

A screenshot of the RouterA configuration window. The window has tabs for Physical, Config, CLI, and Attributes, with CLI selected. The title bar says "RouterA". The main area is titled "IOS Command Line Interface" and shows the following commands: RA(config)#router rip, RA(config-router)#net 192.168.1.0, RA(config-router)#net 172.1.1.0, RA(config-router)#end, RA#, %SYS-5-CONFIG\_I: Configured from console by console, RA#.

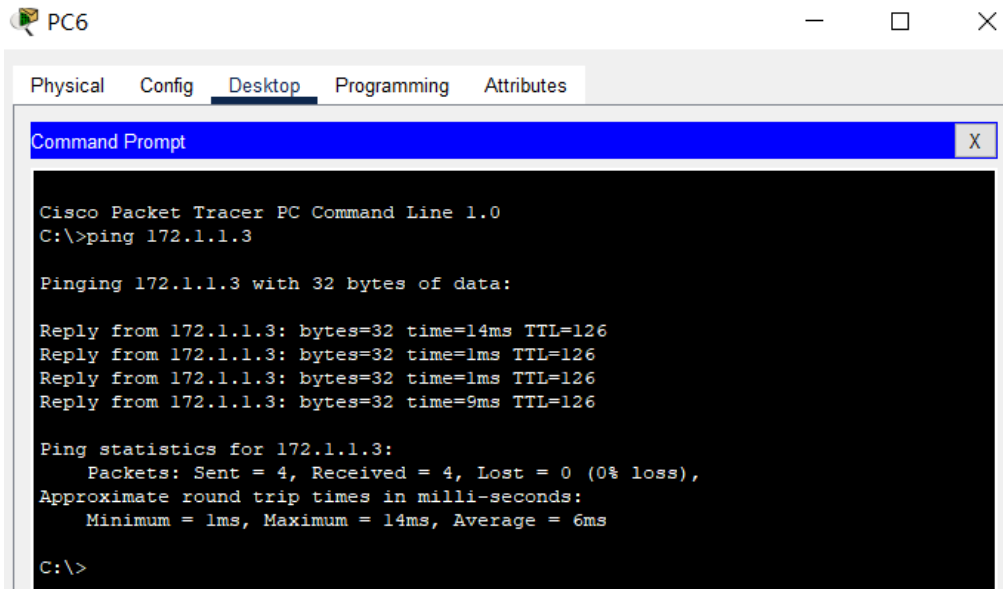
```
RouterA
Physical Config CLI Attributes
IOS Command Line Interface
RA(config)#router rip
RA(config-router)#net 192.168.1.0
RA(config-router)#net 172.1.1.0
RA(config-router)#end
RA#
%SYS-5-CONFIG_I: Configured from console by console
RA#
```

给路由器 B 设置 RIP 协议，添加 172.2.2.0 与 192.168.1.0 两个与之直接相连的网络

A screenshot of the RouterB configuration window. The window has tabs for Physical, Config, CLI, and Attributes, with CLI selected. The title bar says "RouterB". The main area is titled "IOS Command Line Interface" and shows the following commands: RB#conf t, Enter configuration commands, one per line. End with CNTL/Z., RB(config)#router rip, RB(config-router)#net 172.2.2.0, RB(config-router)#net 192.168.1.0, RB(config-router)#end, RB#, %SYS-5-CONFIG\_I: Configured from console by console, RB#.

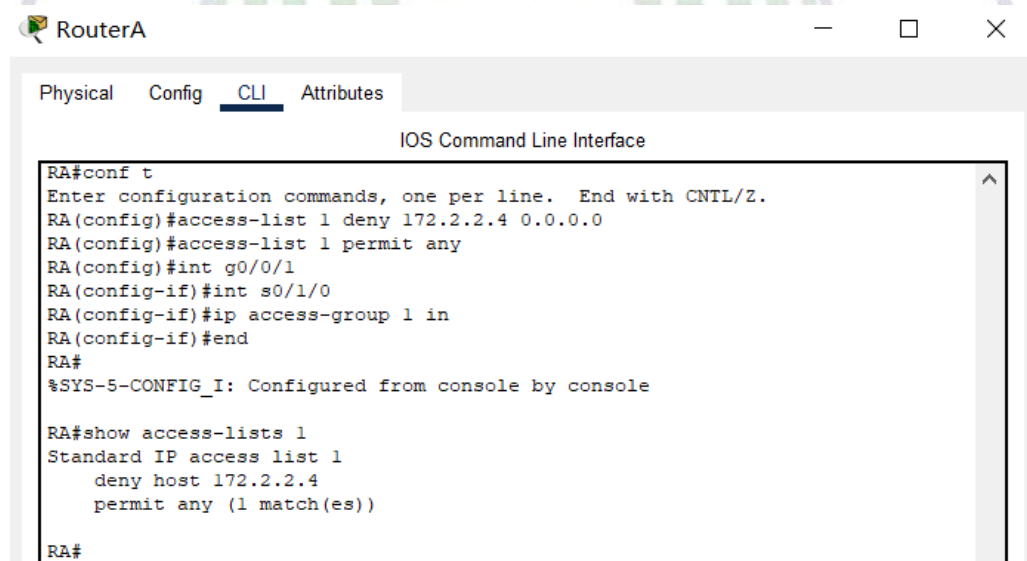
```
RouterB
Physical Config CLI Attributes
IOS Command Line Interface
RB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RB(config)#router rip
RB(config-router)#net 172.2.2.0
RB(config-router)#net 192.168.1.0
RB(config-router)#end
RB#
%SYS-5-CONFIG_I: Configured from console by console
RB#
```

从 PC6 ping PC2 的结果，可以 ping 通

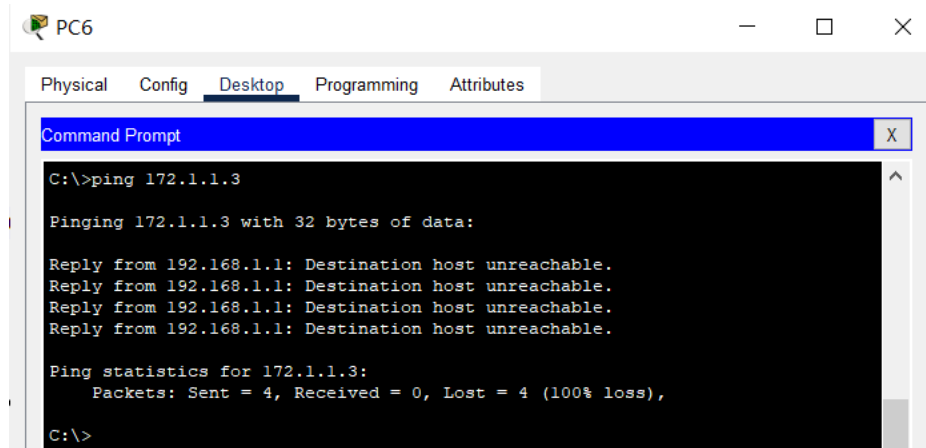


### 3. 配置 ACL

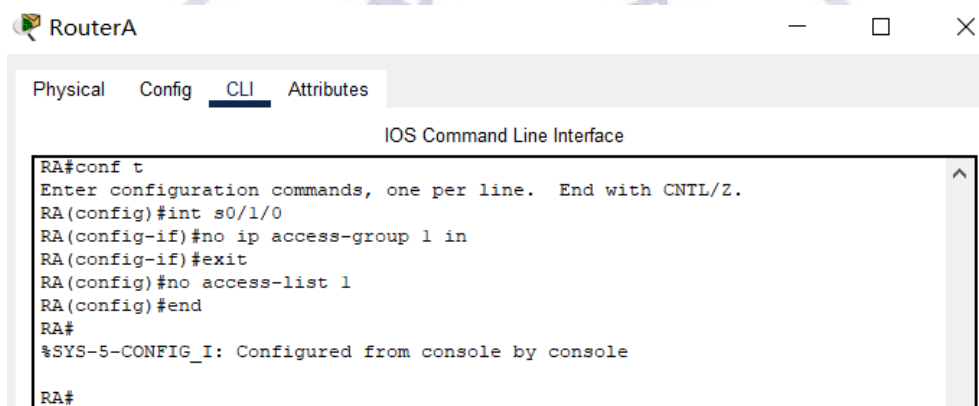
和书上不同，此处将限制规则设置在路由器 A 上的 s0/1/0 接口，按照此规则限制 s0/1/0 接口的流入流量



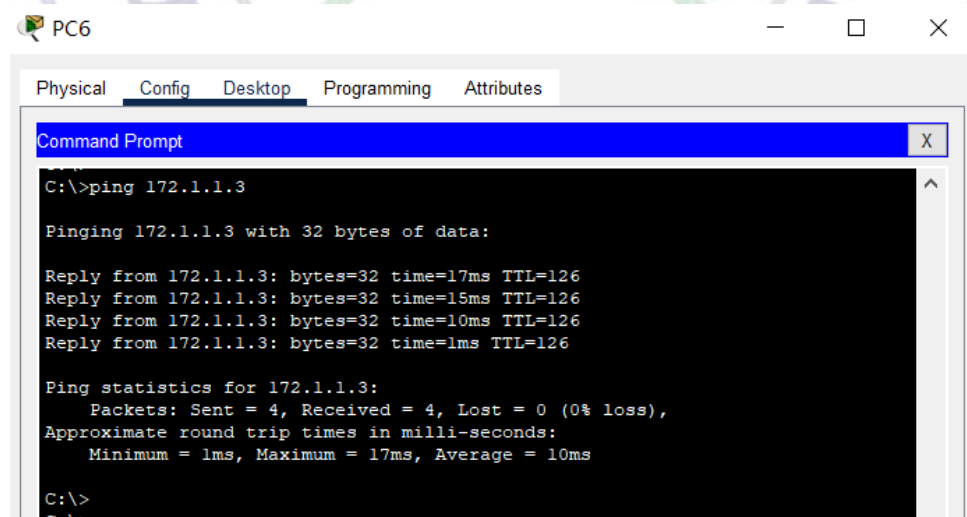
下图为从 PC6 ping PC2 的结果，可见此时已经无法 ping 通



删除访问控制列表 1



此时 PC6 又可以 ping 通 PC2 了



## 六、实验总结及体会

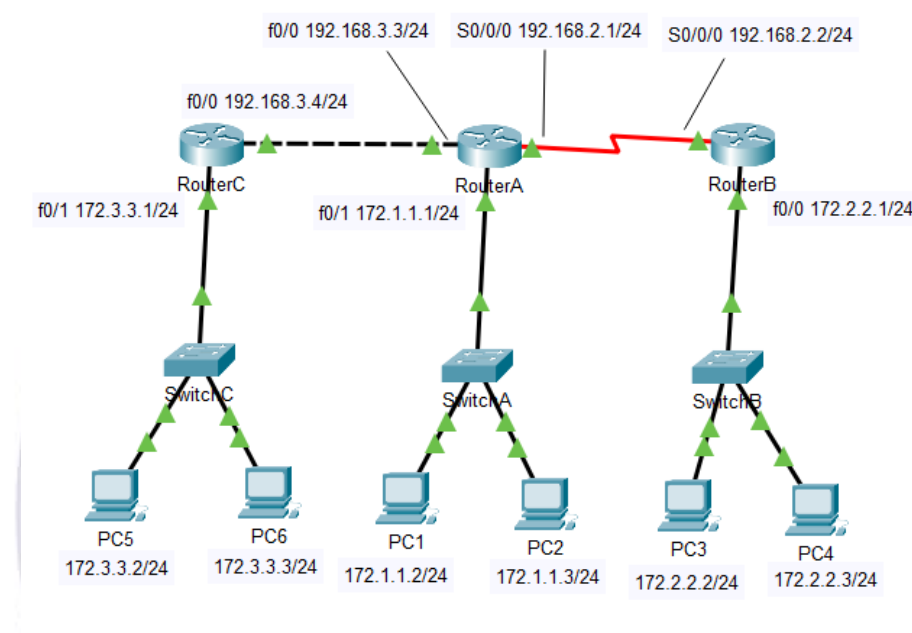
配置 ACL 使得某主机无法访问某网段时，使用 ping 命令会得到 Destination

Host Unreachable, 意味着当前主机根本无法得知目标网段的存在, 会认为这是一个“不存在”的网段, 没有响应。

### 思考题

(1) 如果是由三个路由器组成的拓扑图(如图 14-10 所示), 应该如何配置才能使所有 PC 机相互通信? PC5 和 PC6 属于 172.1.1.0/24 网段, PC1 和 PC2 属于 172.2.2.0/24 网段, PC3 和 PC4 属于 172.3.3.0/24 网段。

网络的拓扑结构图如下

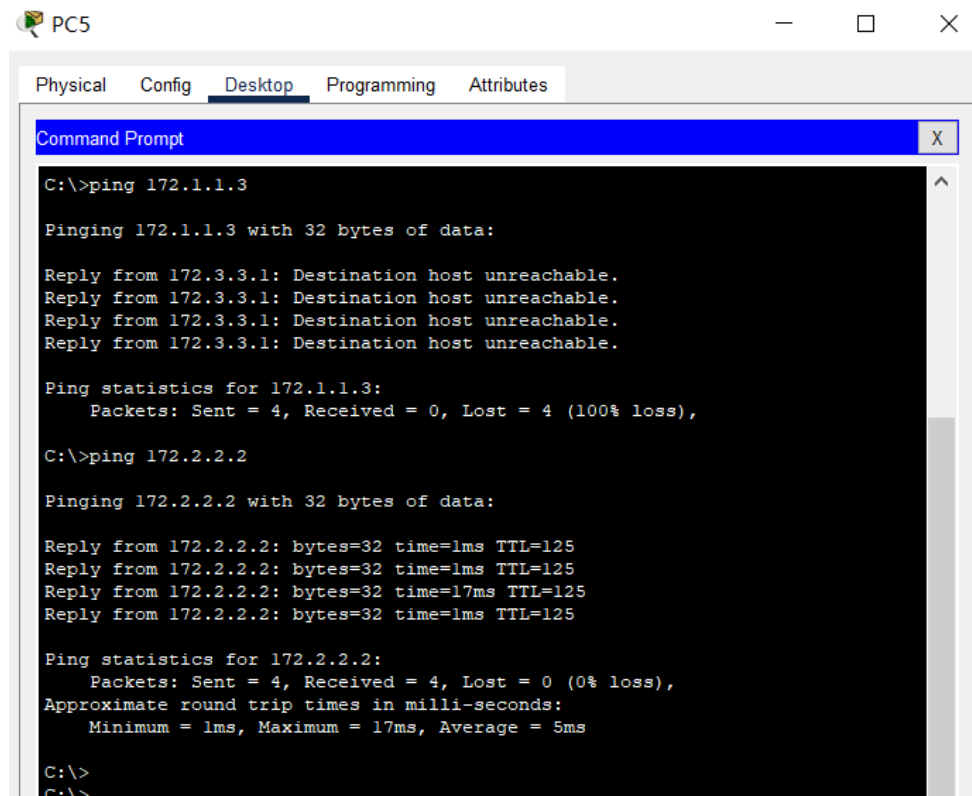


此处使用 RIP 协议。

若要禁止 172.3.3.0/24 网段上的所有用户访问 172.1.1.0/24 网段, 在路由器 C 上进行如下扩展 ACL 配置(由于要判断目的地址的情况, 必须使用扩展 ACL)

```
RouterC
Physical Config CLI Attributes
IOS Command Line Interface
RC>en
RC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RC(config)#access-list 100 deny ip 172.3.3.0 0.0.0.255 172.1.1.0 0.0.0.255
RC(config)#access-list 100 permit ip 172.3.3.0 0.0.0.255 an
RC(config)#access-list 100 permit ip 172.3.3.0 0.0.0.255 any
RC(config)#int f0/1
RC(config-if)#ip access-group 100 in
RC(config-if)#end
RC#
%SYS-5-CONFIG_I: Configured from console by console
RC#
```

PC5 ping PC2、PC5 ping PC3 的情况如下所示



```
PC5
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.1.1.3

Pinging 172.1.1.3 with 32 bytes of data:

Reply from 172.3.3.1: Destination host unreachable.
Reply from 172.3.3.1: Destination host unreachable.
Reply from 172.3.3.1: Destination host unreachable.
Reply from 172.3.3.1: Destination host unreachable.

Ping statistics for 172.1.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.2.2.2

Pinging 172.2.2.2 with 32 bytes of data:

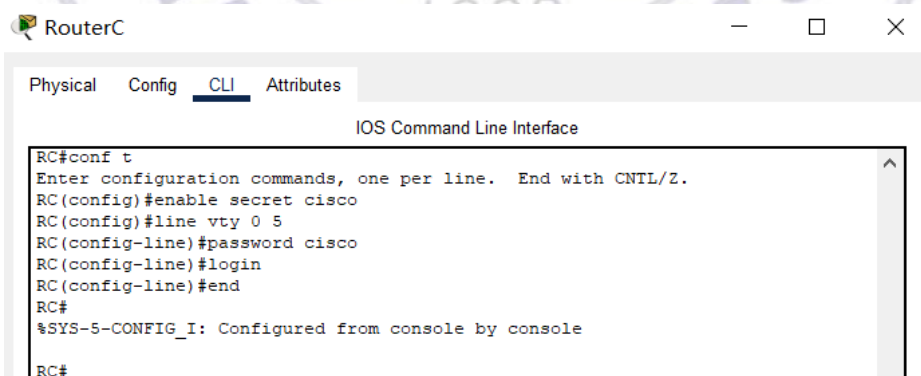
Reply from 172.2.2.2: bytes=32 time=1ms TTL=125
Reply from 172.2.2.2: bytes=32 time=1ms TTL=125
Reply from 172.2.2.2: bytes=32 time=17ms TTL=125
Reply from 172.2.2.2: bytes=32 time=1ms TTL=125

Ping statistics for 172.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 17ms, Average = 5ms

C:\>
```

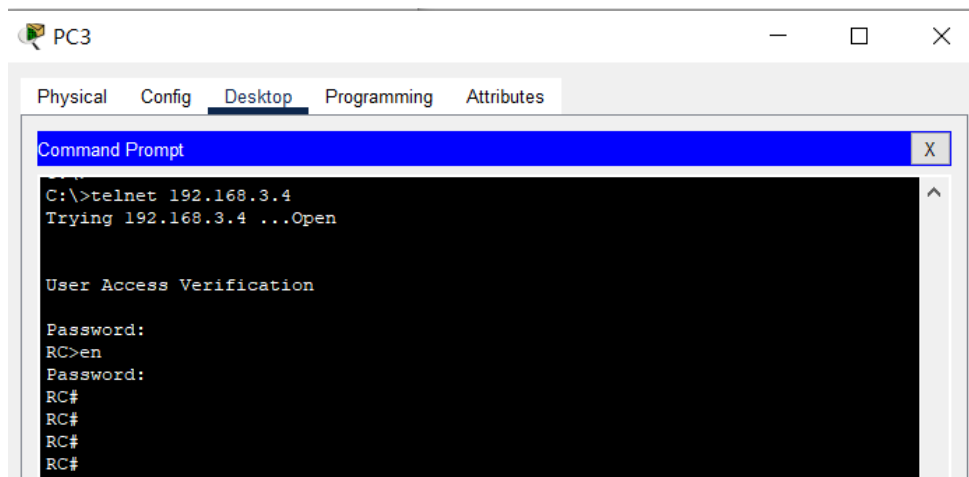
若要禁止 172.2.2.0/24 的网络对路由器 C 进行 telnet，在路由器 C 上进行如下扩展 ACL 配置

先给路由器 C 配置登录密码，使得 172.2.2.0/24 网段能通过 telnet 成功访问路由器 C。下图分别为对路由器 C 的配置和在 PC3 上 telnet 路由器 C 的结果。

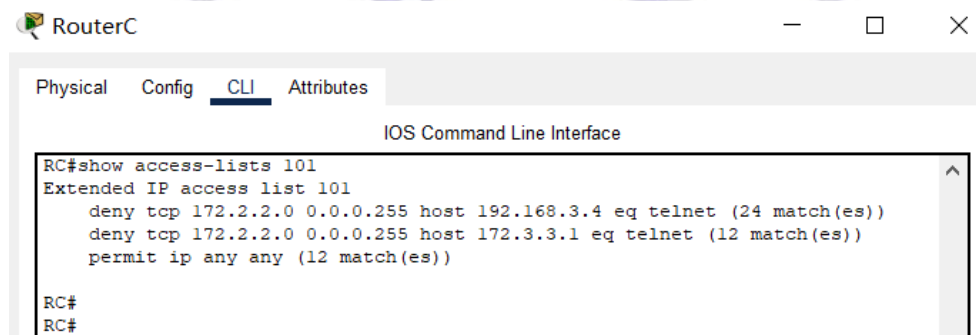


```
RouterC
Physical Config CLI Attributes
IOS Command Line Interface
RC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RC(config)#enable secret cisco
RC(config)#line vty 0 5
RC(config-line)#password cisco
RC(config-line)#login
RC(config-line)#end
RC#
%SYS-5-CONFIG_I: Configured from console by console
RC#
```

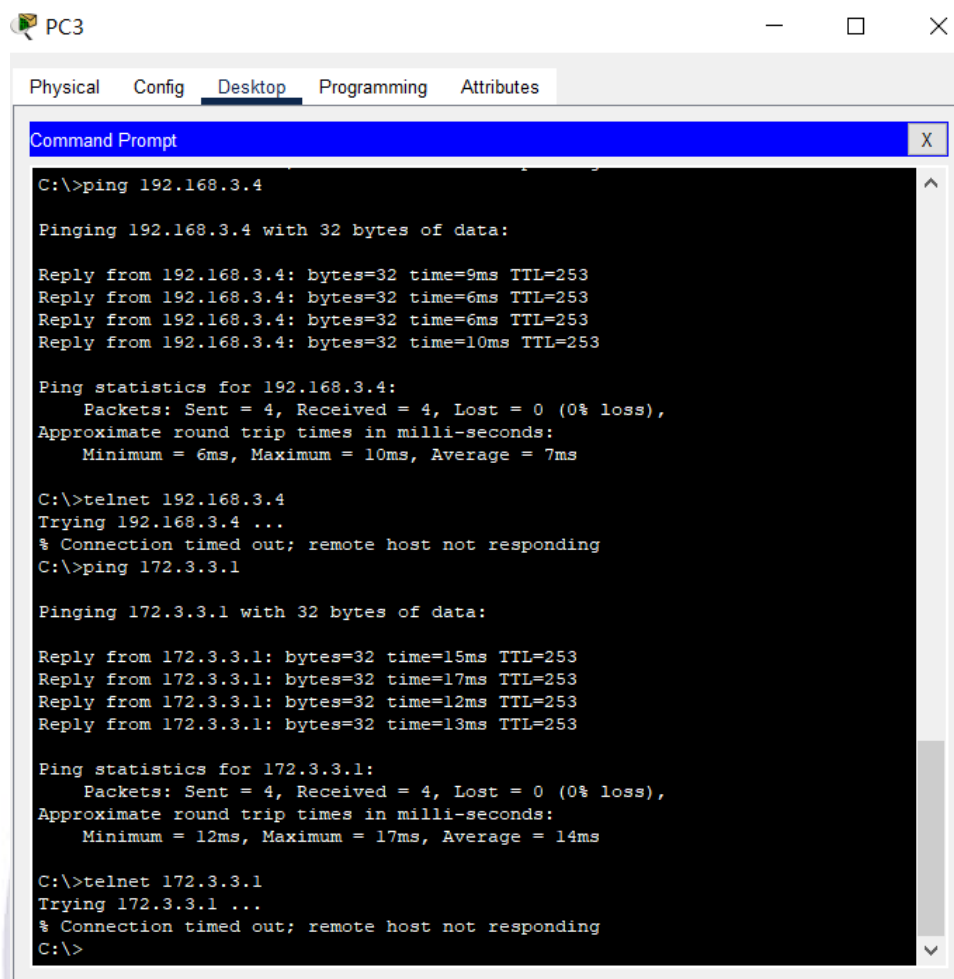




如下在路由器 C 上配置扩展 ACL



再次在 PC3 上分别通过 ping 和 telnet 访问路由器 C 的两个接口，可以发现确实只禁用了 telnet 在 23 端口的访问，依然可以 ping 通



```
C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=9ms TTL=253
Reply from 192.168.3.4: bytes=32 time=6ms TTL=253
Reply from 192.168.3.4: bytes=32 time=6ms TTL=253
Reply from 192.168.3.4: bytes=32 time=10ms TTL=253

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 10ms, Average = 7ms

C:\>telnet 192.168.3.4
Trying 192.168.3.4 ...
% Connection timed out; remote host not responding
C:\>ping 172.3.3.1

Pinging 172.3.3.1 with 32 bytes of data:

Reply from 172.3.3.1: bytes=32 time=15ms TTL=253
Reply from 172.3.3.1: bytes=32 time=17ms TTL=253
Reply from 172.3.3.1: bytes=32 time=12ms TTL=253
Reply from 172.3.3.1: bytes=32 time=13ms TTL=253

Ping statistics for 172.3.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 17ms, Average = 14ms

C:\>telnet 172.3.3.1
Trying 172.3.3.1 ...
% Connection timed out; remote host not responding
C:\>
```

(2) 一个路由器上设置了扩展 ACL，允许其中一个网段访问互联网，同时又设置了标准 ACL，禁止该网段访问互联网。问：该网段到底能否访问互联网？

不能访问互联网。标准 ACL 的列表号的范围是 1~99，扩展 ACL 的列表号的范围是 100~199。路由器对 ACL 的默认匹配原则为“从小列表号向大列表号查看，有任意一项匹配就按此过滤不再查看后面的规则”。因此，在匹配时一定先匹配到标准 ACL 中的规则，即禁止该网段访问互联网。

## 七、教师评语