

# 南昌大学



## 软件学院实验报告书

课程名称：网络系统工程实训

题目：动态路由协议 RIP 深入配置

专业：信息安全

班级：193 班

学号：8003119100

学生姓名：丁俊

完成人数：1 人

起讫日期：20210716-20210930

任课教师：鄢志辉 职称：高级工程师

部分管主任：邹春华

完成时间：20210930

# 实训十六 访问控制列表配置实训

## 一、实验目的

- 理解 NAT 的转换机制
- 理解 NAT 转换表的作用
- 理解 NAT 静态地址和动态地址转换方式
- 熟悉常用的 NAT 地址转换命令

## 二、实验设备及条件

- 运行 Windows 操作系统计算机一台
- Cisco Packet Tracer 模拟软件
- 或
- Cisco 1841 或 2811 路由器两台
- 普通交换机两台
- 运行 Windows 操作系统计算机四台、HTTP 服务器一台
- 路由器串口线一根、RJ-45 转 DB-9 反接线一根、RJ-45 双绞线若干
- 超级终端应用程序

## 三、实验原理

对于许多网管员来说，配置路由器的访问控制列表是一件经常性的工作，可以说，路由器的访问控制列表是网络安全保障的第一道关卡。访问列表提供了一种机制，它可以控制和过滤通过路由器的不同接口去往不同方向的信息流。这种机制允许用户使用访问表来管理信息流，以制定公司内部网络的相关策略。这些策略可以描述安全功能，并且反映流量的优先级别。例如，某个组织可能希望允许或拒绝 Internet 对内部 Web 服务器的访问，或者允许内部局域网上一个或多个工作站能够将数据流发到广域网上。这些情形，以及其他的一些功能都可以通过访问表来达到目的。

目前的路由器一般都支持两种类型的访问表：标准访问控制列表和扩展访问控制列表。标准访问表控制基于网络地址的信息流，且只允许过滤源地址。扩展访问表通过网络地址和传输中的数据类型进行信息流控制，允许过滤源地址、目的地址和上层应用数据。

### 3.1 标准 IP 访问控制列表的格式

标准 IP 访问控制列表的格式为：

```
access-list listnumber permit|deny [host] sourceaddress[any [wildcardmask] [log]
```

listnumber---表号范围，标准 IP 访问表的表号从 1 到 99。

permit/deny----允许或拒绝，permit 表示允许匹配报文通过接口，而 deny 表示匹配报文要被丢弃掉。

sourceaddress----源地址，如:198.78.46.8。

wildcardmask-----通配符屏蔽码，与子网屏蔽码的方式是刚好相反的，二进制的 0 表示

一个“匹配”条件，二进制的 1 表示一个“不关心”条件

host/any----指定单个主机和所有主机

log----日志记录

### 3.2 扩展的 IP 访问控制列表的格式

扩展 IP 访问控制列表的格式为：

```
access-list listnumber permit|deny protocol [host] sourceaddress[any [wildcardmask]]
[sourceport] [host] destinationaddress[any [wildcardmask]] [destinationport] [log] [option]
```

listnumber---表号范围，扩展 IP 访问表的表号从 100 到 199。

protocol-需要被过滤的协议，如 IP、TCP、UDP、ICMP

sourceport 和 destinationport-源端口和目的端口，用 eq|lt|gt portnumber 指定，表示等于、小于或大于某个端口

option-扩展选项，如 established 表示过滤 ACK 或 RST 位已设置的 tcp 报文

### 3.3 IP 访问控制列表的配置命令

在一个路由器接口上配置一对一的访问控制列表一般按以下三步骤进行：

- 在全局配置模式下定义访问表，采用 access-list ...命令。
- 指定访问表所应用的接口，进入接口子配置模式，采用 interface ethernet|fastethernet|serial slot\_#/port\_# 命令。
- 定义访问表作用于接口上的方向，采用 ip access-group listnumber in|out 命令。

除此之外，还可以采用 no access-list listnumber 命令删除访问控制列表；采用 show access-list [listnumber]查看访问控制列表。

## 四、实验步骤

### 1、网络配置

使用网络仿真软件 Cisco Packet Tracer 模拟图 1 网络，按图 1 设置路由器、主机 A-D 和 HTTP 服务器的 IP 地址。

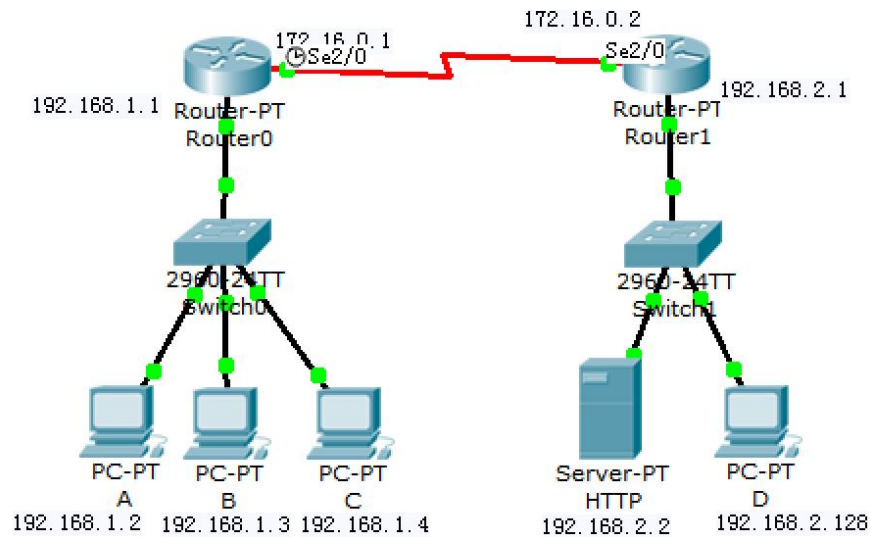


图 1 网络结构

网络拓扑结构如图 2 所示。

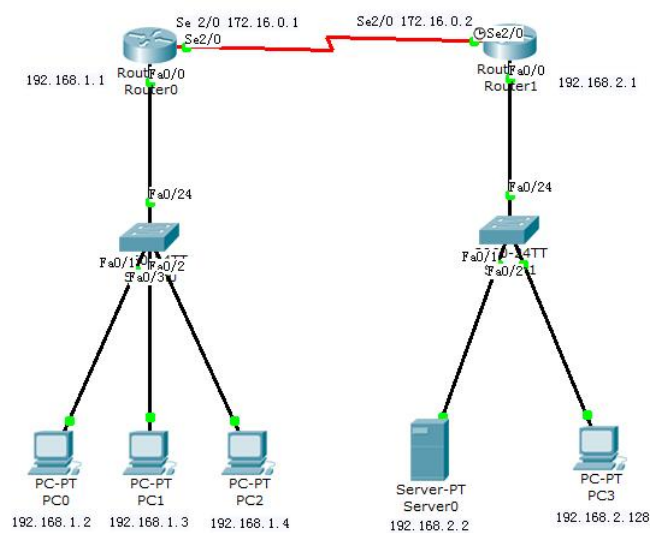


图 2 网络拓扑结构

## 2、配置默认路由

在路由器 Router0 和 Router1 上各配置一条默认路由：默认情况下数据包从 Serial2/0 端口转发出去。使用 ping 命令，测试主机 A、B、C、D 和 HTTP 服务器之间的连通性，确保两两互通。如图 3、4 所示。

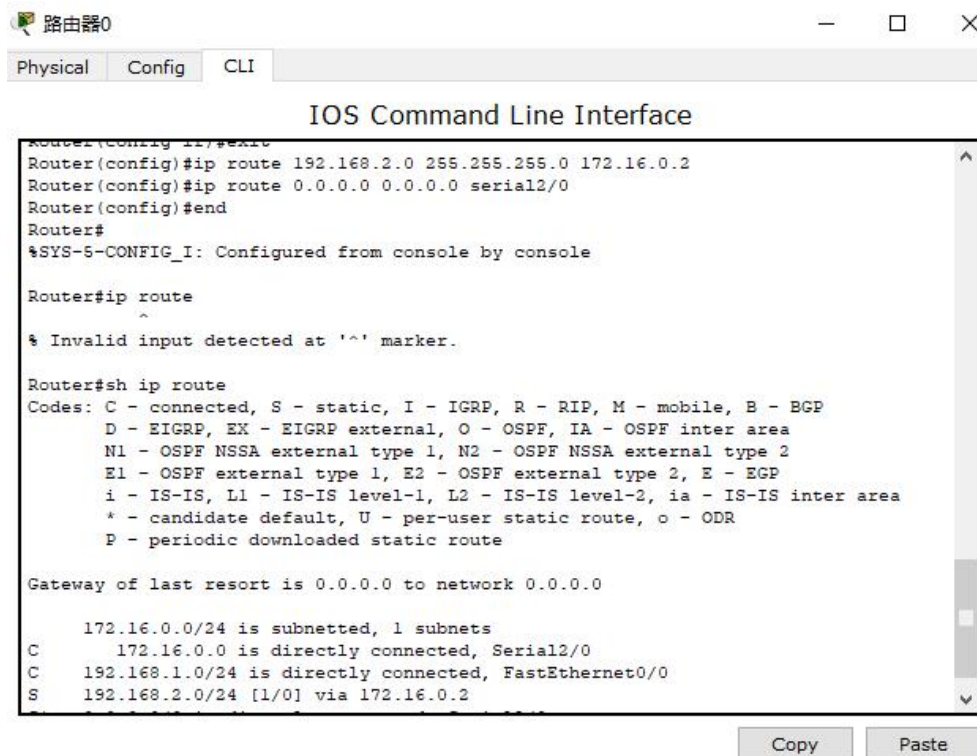


图 3 router0 配置

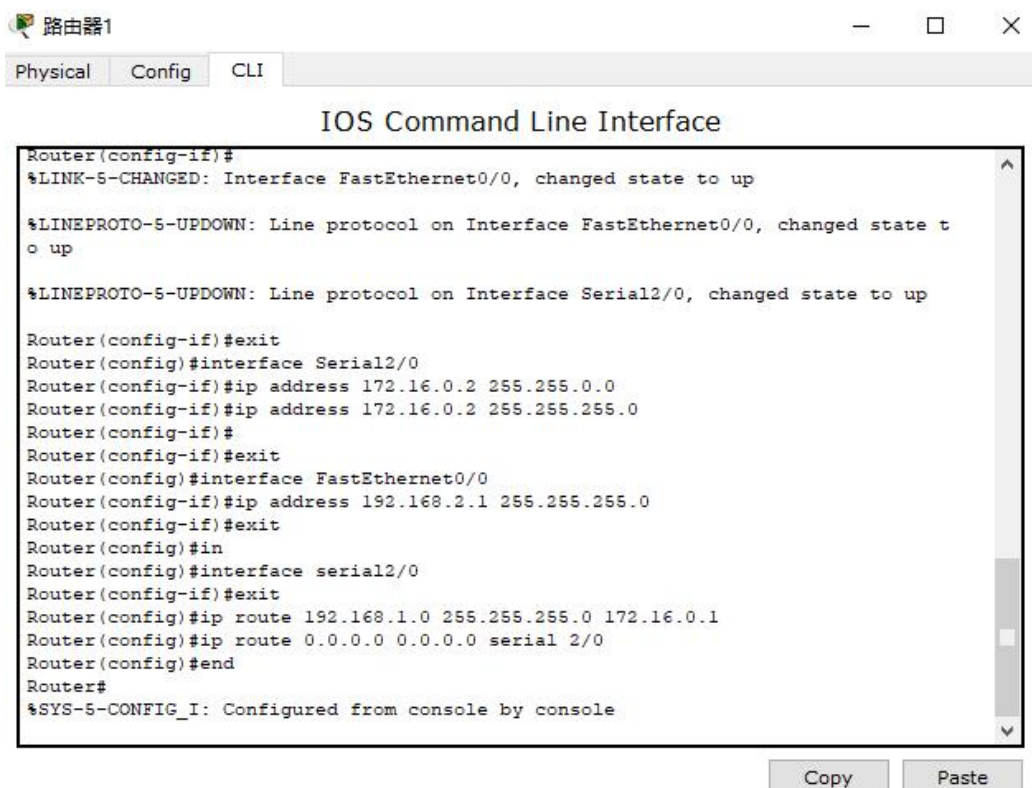


图 4 router1 配置

### 3、配置标准访问控制列表

在路由器 Router1 上配置一个标准 IP 访问控制列表 1，只禁止主机 C 对 192.168.2.0/24 网络的访问，并在 Serial2/0 端口的 in 方向引用访问控制列表 1。配置方法如下：

```
Router#configure terminal
Router(config)#access-list 1 deny host 192.168.1.4
Router(config)#access-list 1 permit any
Router(config)#interface Serial 2/0
Router(config-if)#ip access-group 1 in
Router(config-if)#end
```

查看访问控制列表 1：

```
Router#show access-list 1
```

如图 5 所示。

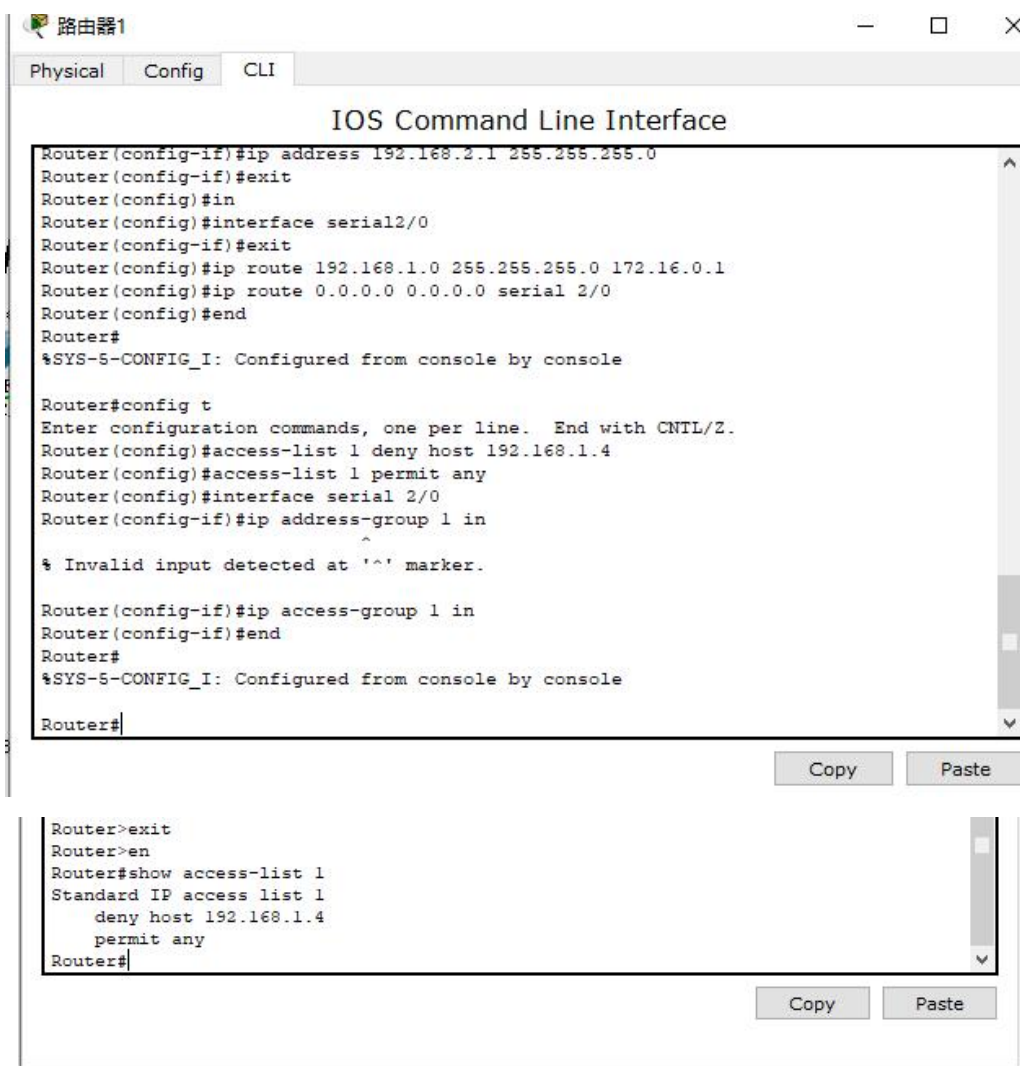
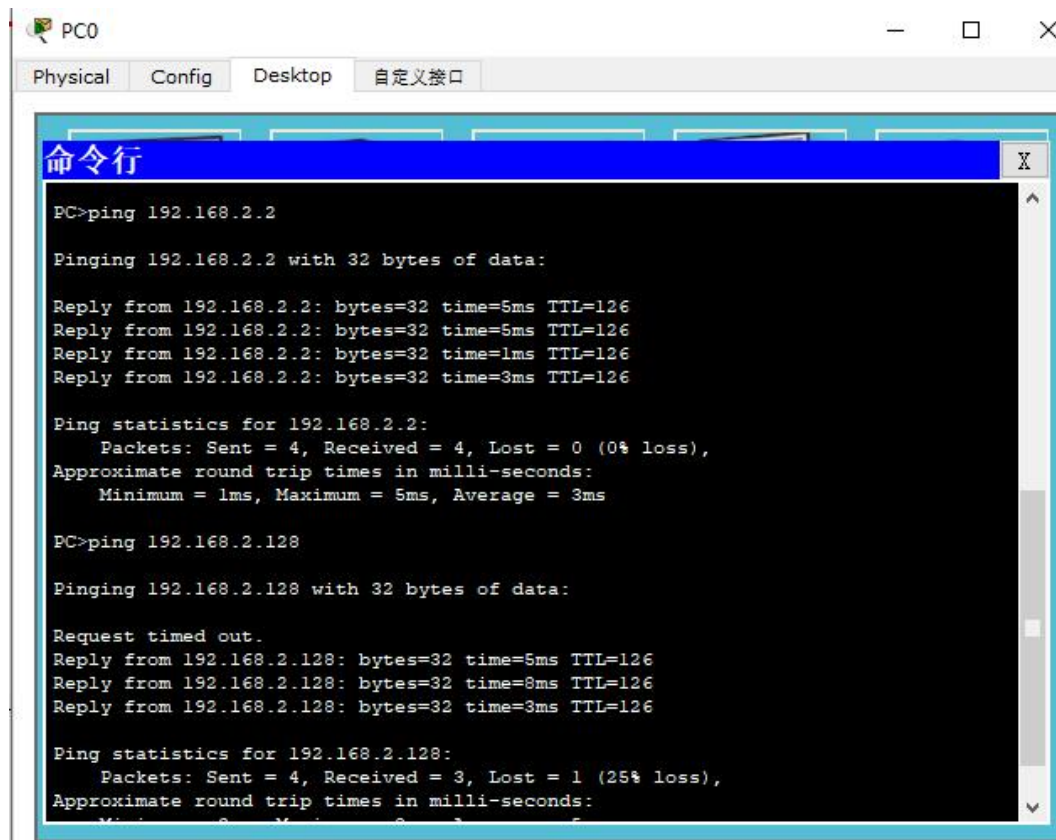


图 5 配置标准访问控制列表

连通结果如下 3 图所示。



The image shows a screenshot of a PC0 terminal window. The window has a title bar with 'PC0' and standard minimize, maximize, and close buttons. Below the title bar are tabs for 'Physical', 'Config', 'Desktop', and '自定义接口'. The 'Desktop' tab is active, and a terminal window titled '命令行' is open. The terminal displays the results of two ping commands. The first command is 'ping 192.168.2.2', which shows four successful replies with varying times (5ms, 5ms, 1ms, 3ms) and a TTL of 126. The statistics for 192.168.2.2 show 4 packets sent, 4 received, and 0% loss. The second command is 'ping 192.168.2.128', which shows one 'Request timed out' and three successful replies (5ms, 8ms, 3ms) with a TTL of 126. The statistics for 192.168.2.128 show 4 packets sent, 3 received, and 25% loss.

```
PC0>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=5ms TTL=126
Reply from 192.168.2.2: bytes=32 time=5ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 3ms

PC0>ping 192.168.2.128

Pinging 192.168.2.128 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.128: bytes=32 time=5ms TTL=126
Reply from 192.168.2.128: bytes=32 time=8ms TTL=126
Reply from 192.168.2.128: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.2.128:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
```

图 6 PC0 连通信息



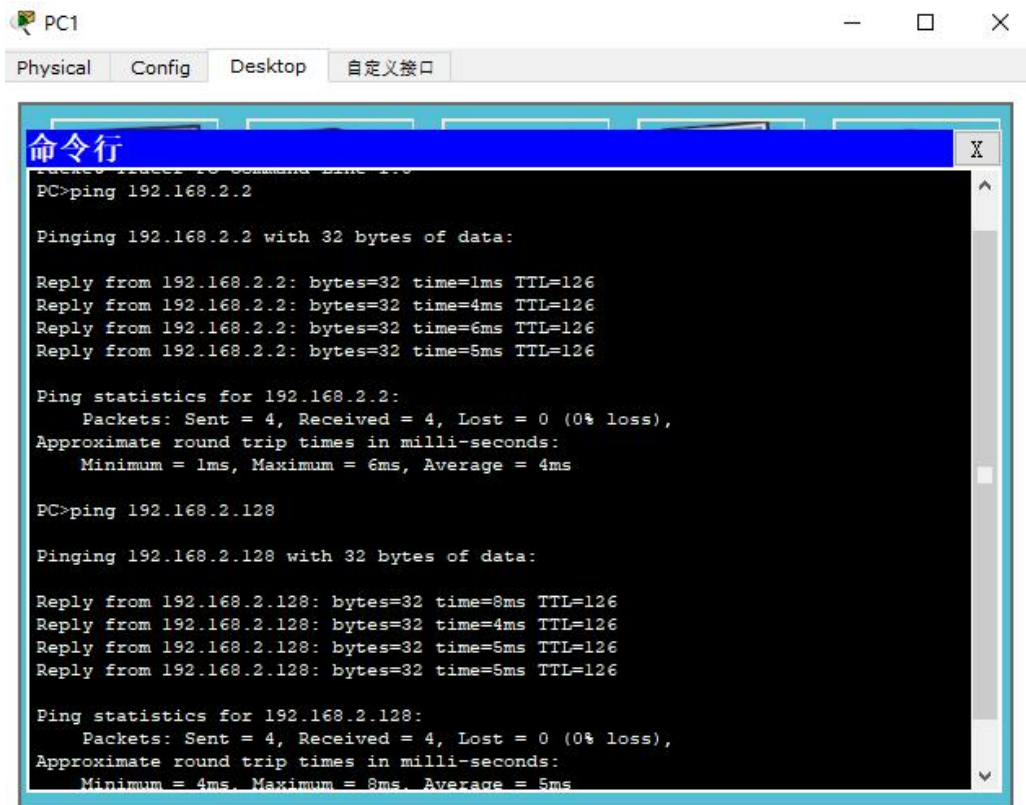


图 7 PC1 连通信息

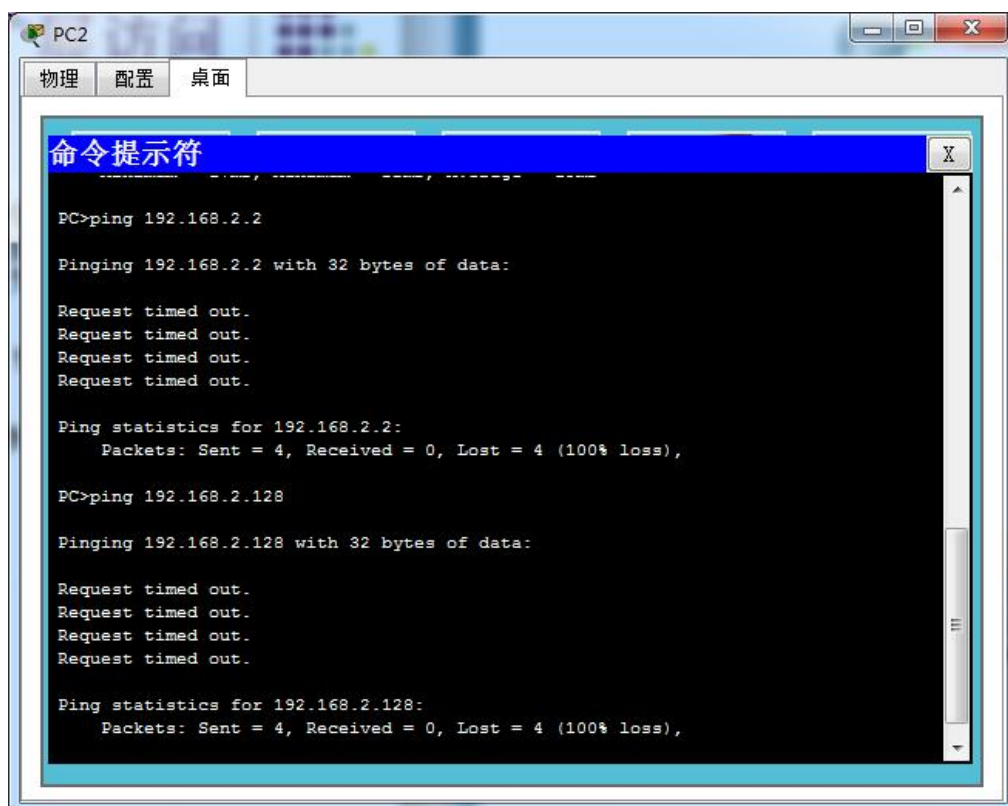


图 8 PC2 连通信息



PC3 不能连通原因：在配置标准访问控制列表中禁止了地址为 192.168.1.4 主机的访问。

#### 4、配置基于源/目的 IP 的扩展访问控制列表

在路由器 Router1 上配置一个基于源/目的 IP 的扩展访问控制列表 110，只禁止 192.168.1.0/24 对 192.168.2.128/25 网络的访问，并在 Serial2/0 端口的 in 方向引用访问控制列表 110。配置方法如下：

```
Router#configure terminal
Router(config)#access-list 110 deny ip any 192.168.2.128 0.0.0.127
Router(config)#access-list 110 permit ip any any
Router(config)#interface Serial 2/0
Router(config-if)#ip access-group 110 in
Router(config-if)#end
```

查看访问控制列表 110：

```
Router#show access-list 110
```

如图 9 所示。

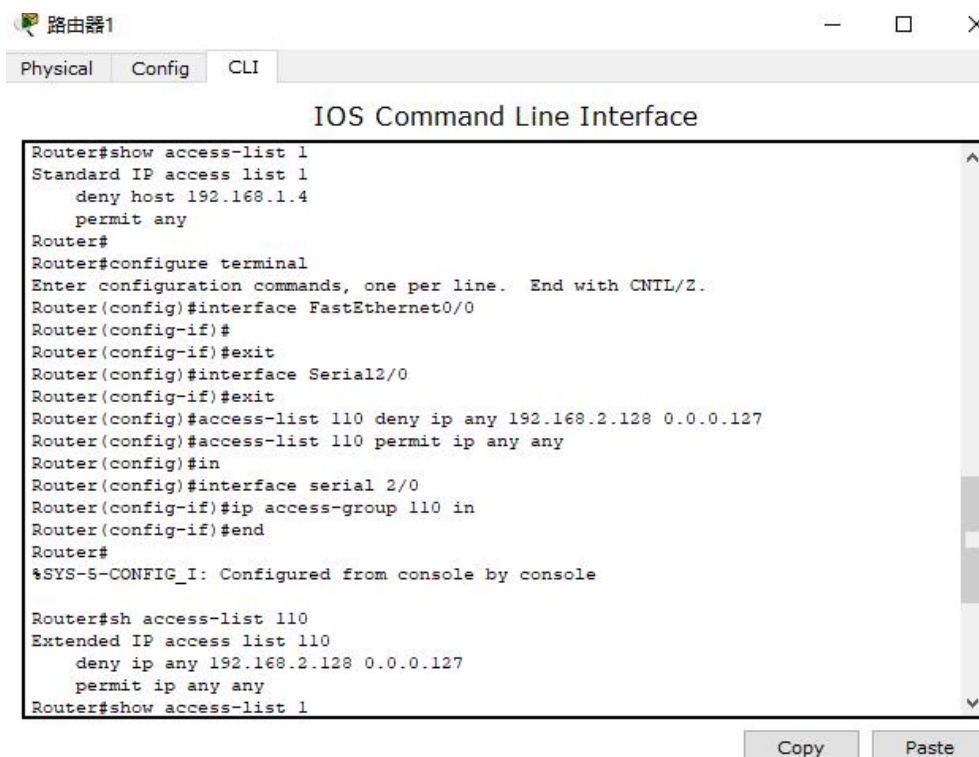


图 9 配置基于源/目的 IP 的扩展访问控制列表

结果如下 3 图。

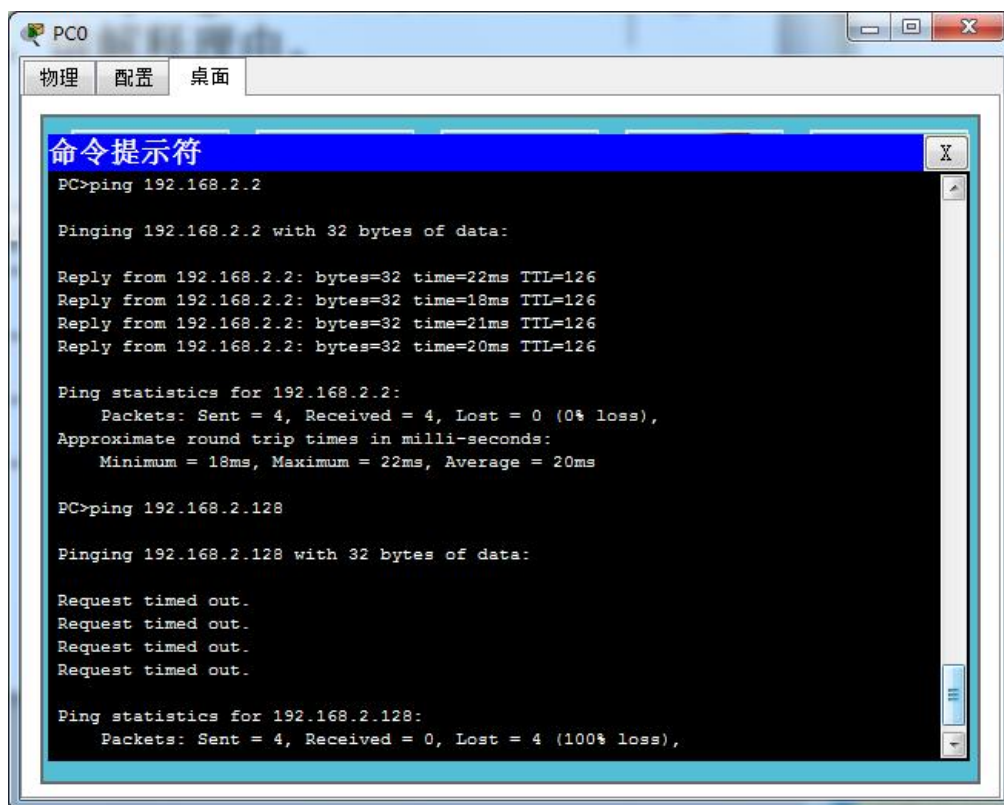


图 10 PC0 连通信息

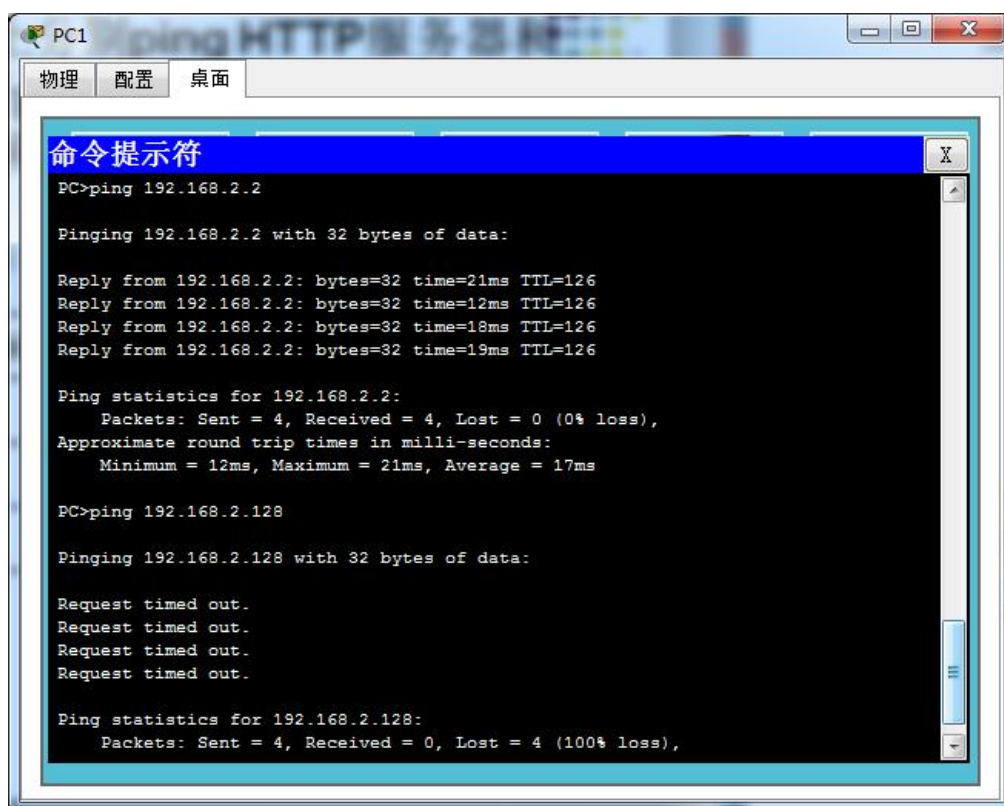


图 11 PC1 连通信息

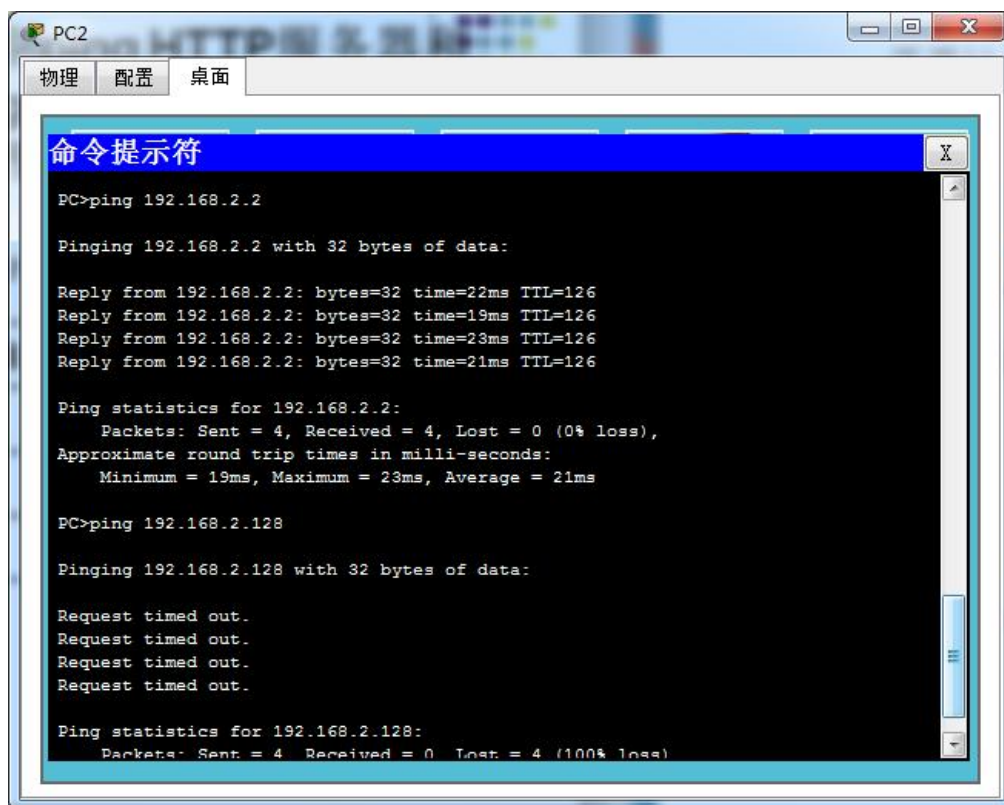


图 12 PC2 连通信息

三台主机不能连通 PC3 的原因：在配置基于源/目的 IP 的扩展访问控制列表时，禁止 192.168.1.0/24 对 192.168.2.128/25 网络的访问。

##### 5、配置基于应用业务的扩展访问控制列表

在路由器 Router1 上配置一个基于应用业务的扩展访问控制列表 101，只允许对 HTTP 服务器的 80 端口的访问，并在 Serial2/0 端口的 in 方向引用访问控制列表 101。配置方法如下：

```
Router#configure terminal
Router(config)#access-list 101 permit tcp any host 192.168.2.2 eq 80
Router(config)#access-list 101 deny ip any any
Router(config)#interface Serial 2/0
Router(config-if)#ip access-group 101 in
Router(config-if)#end
```

查看访问控制列表 1：

```
Router#show access-list 101
```

如图 13 所示。

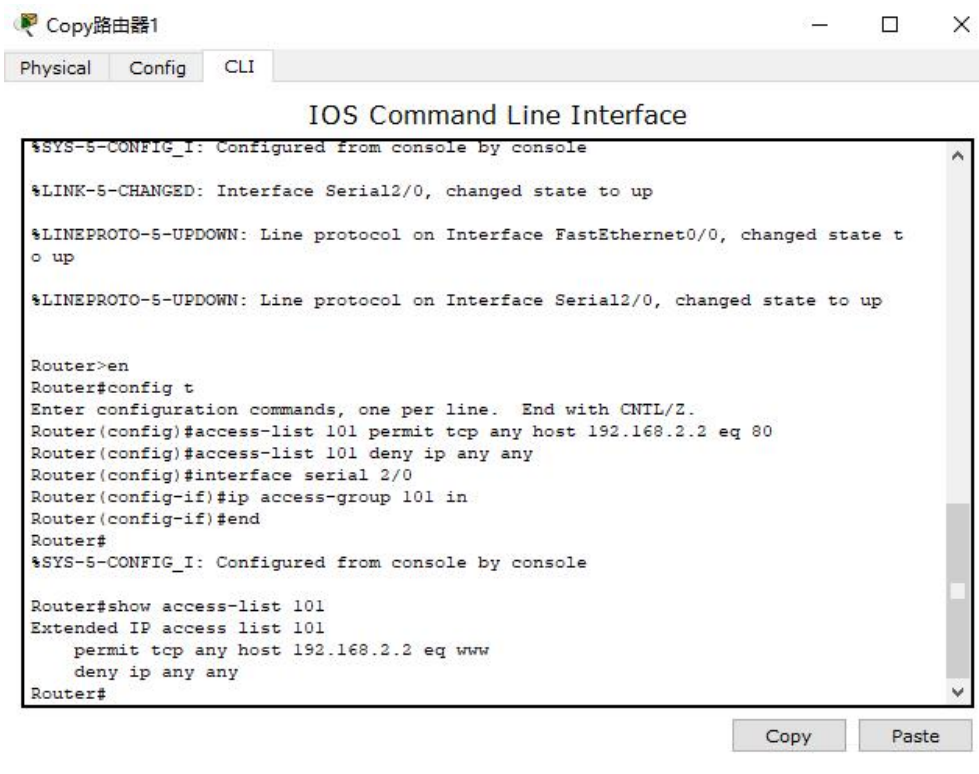


图 13 配置基于应用业务的扩展访问控制列表

结果如下 6 图。

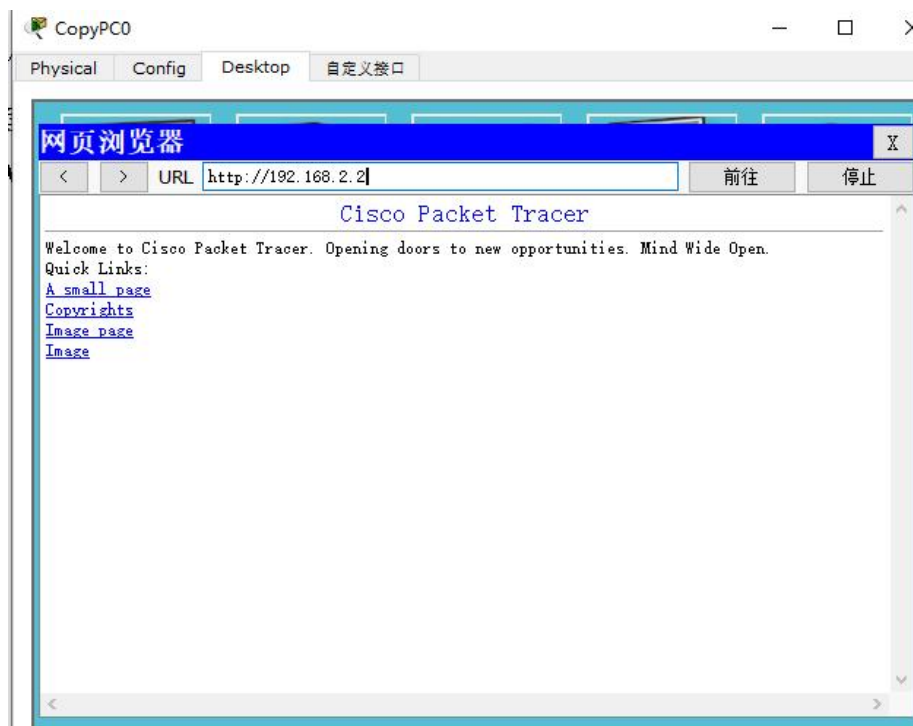


图 14 PC0 访问 http://192.168.2.2 信息

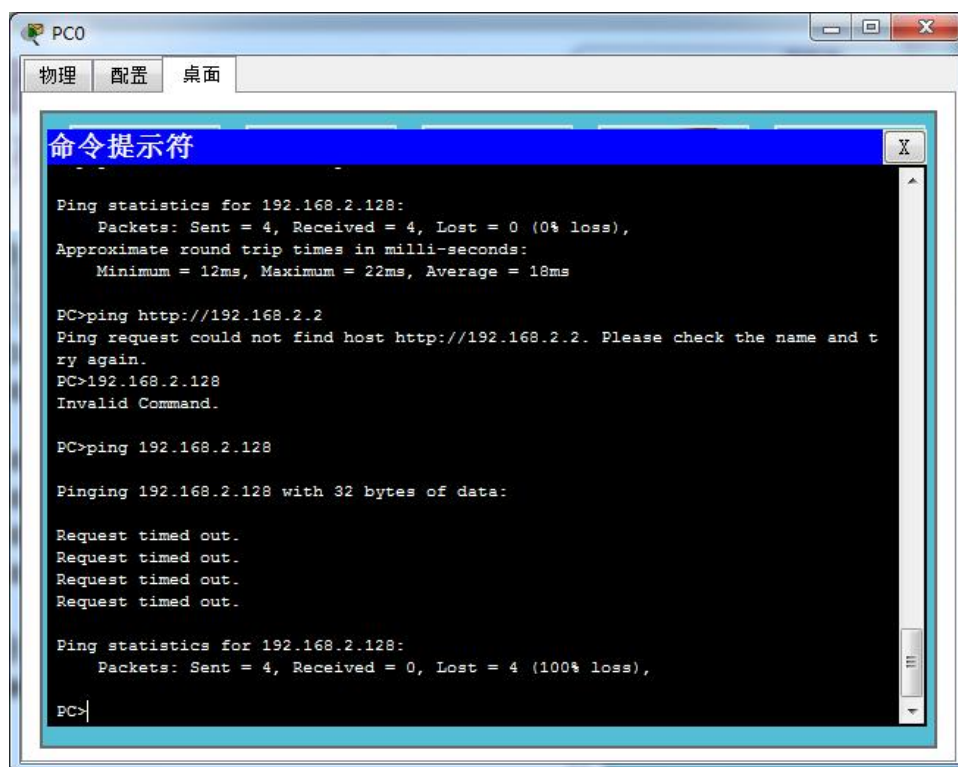


图 15 PC0 连 PC3 信息

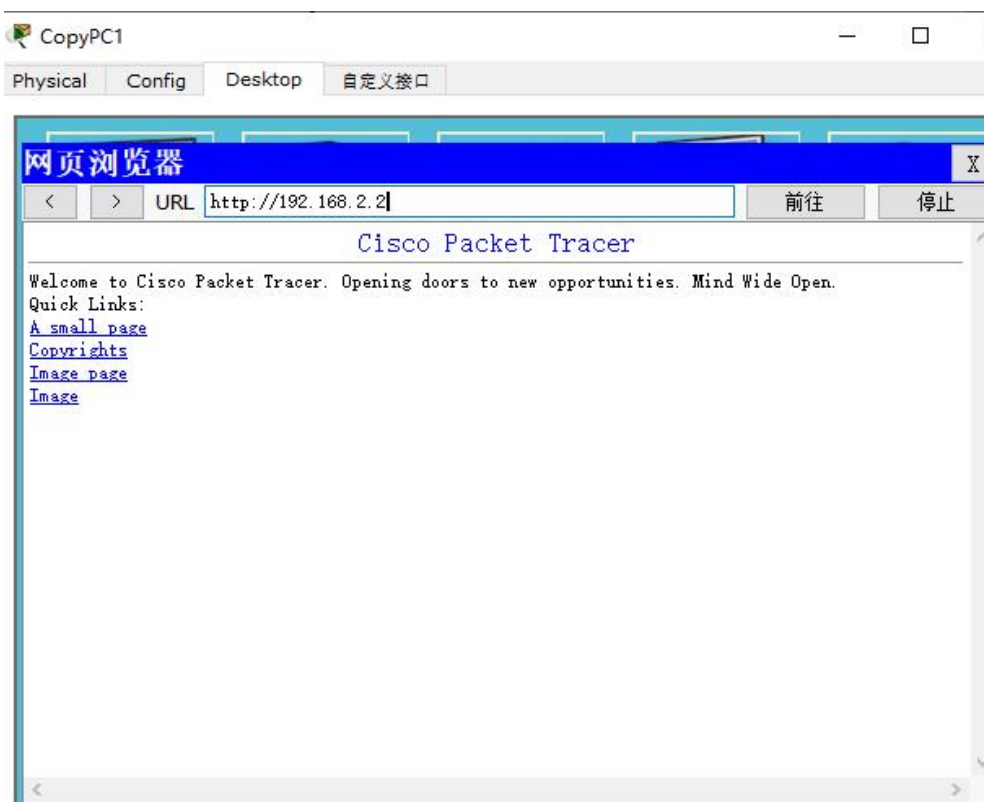


图 16 PC1 访问 http://192.168.2.2 信息

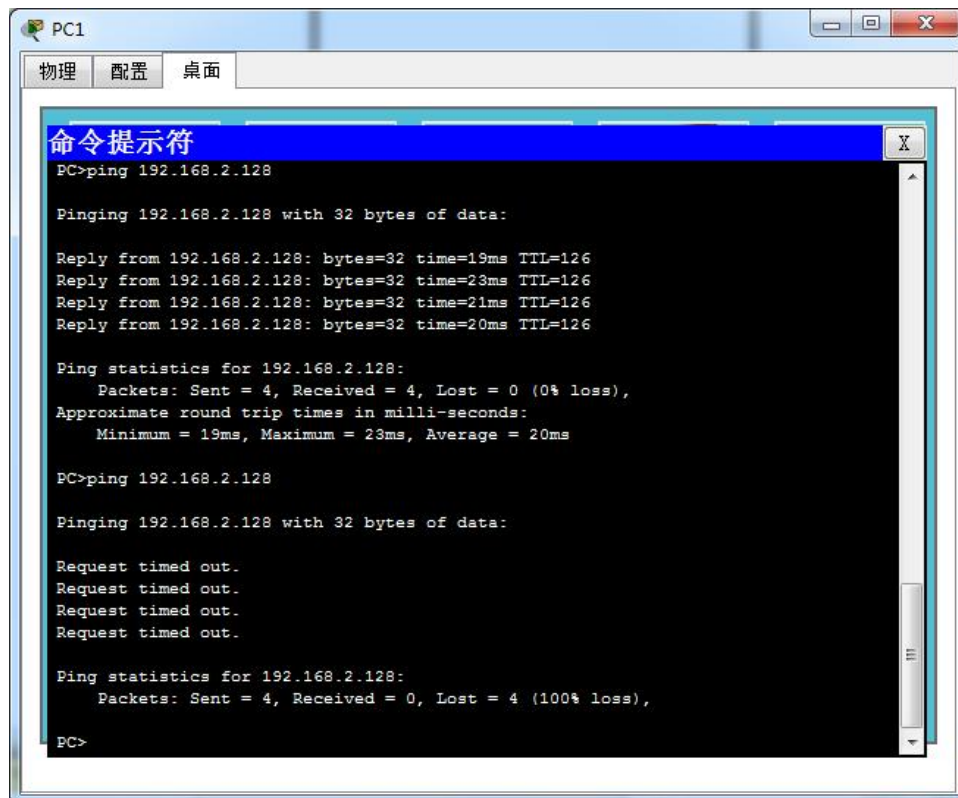


图 17 PC1 连 PC3 信息

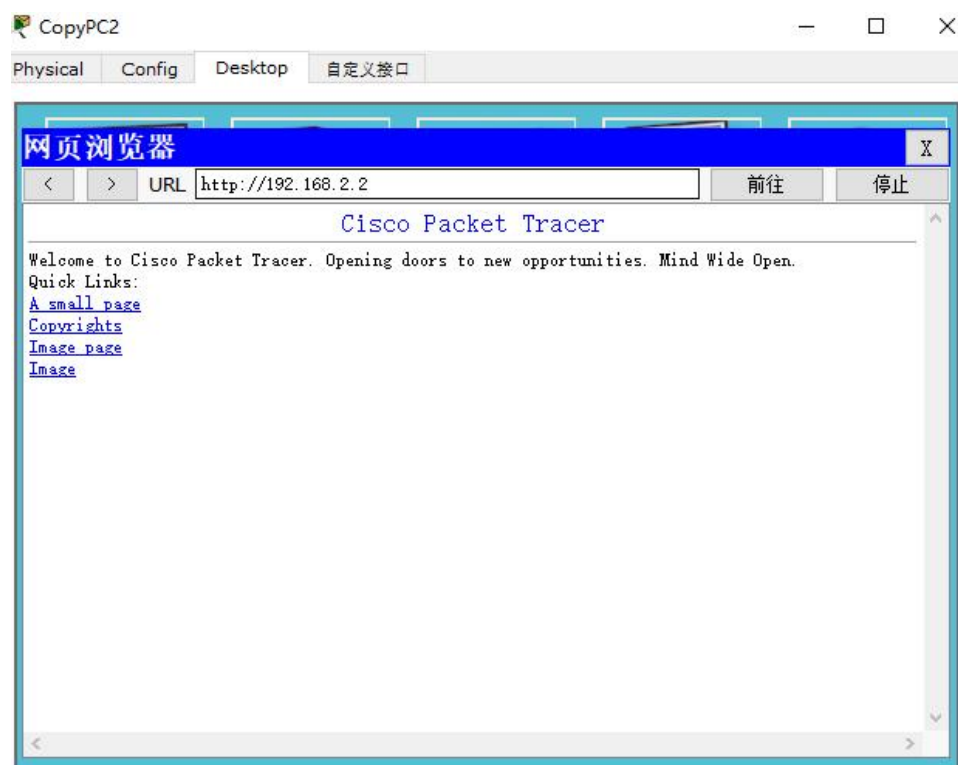


图 18 PC2 访问 http://192.168.2.2 信息



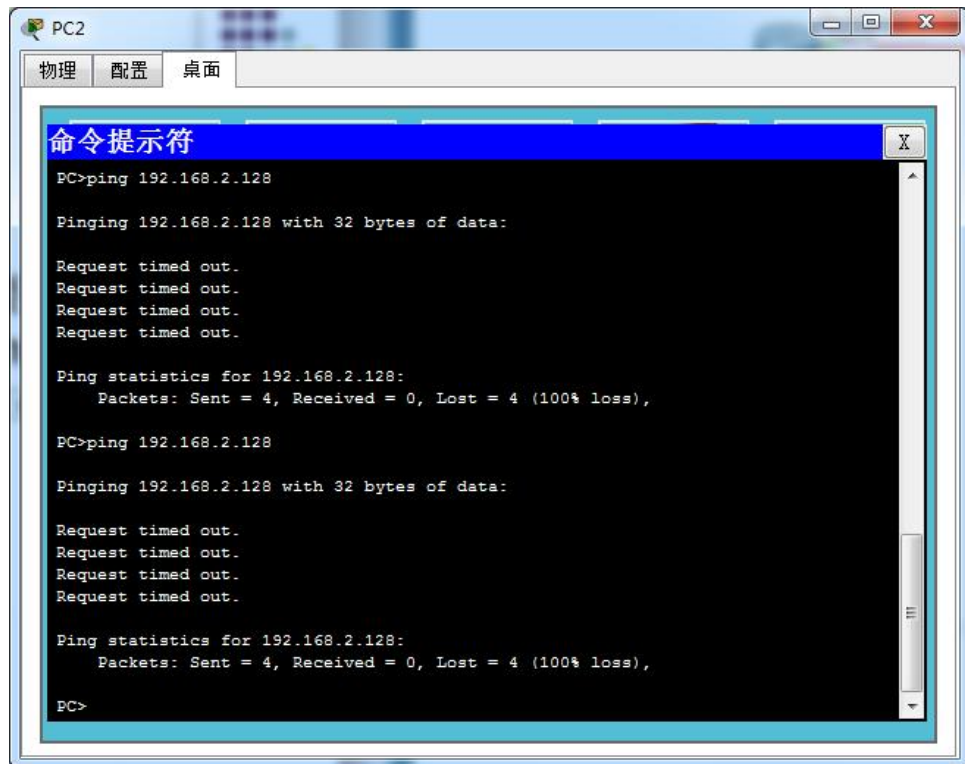


图 19 PC2 连 PC3 信息

三台主机不能连通 PC3 原因：在配置基于应用业务的扩展访问控制列表时，只允许对 HTTP 服务器的 80 端口的访问。

## 五、实验小结

在实验的过程中，要分清三个列表的功能和语句的描述还有条件，语句对谁起作用。在连网络拓扑结构配置地址的时候，要记得配网关，否则不同网络之间不能连通。