**【实验名称】：**ACL访问控制

**学生姓名：**马威 **合作学生：**无

**实验地点：**济事楼330网络实验室 **实验时间：**2023年10月23日

**【实验目的】**

初步学习ACL访问控制的基本原理，在Cisco Packet Tracer中尝试进行ACL访问控制的配置，并实现对一个服务器ping包请求的控制。

**【实验原理】**

**1.ACL技术原理**

ACL全称为接入控制列表(Access Control Lists)，也称为访问列表（Access Lists），俗称为防火墙。其通过定义一些规则，可以控制网络设备接口上数据报文的通过或丢弃，提高网络可管理性和安全性。

IP ACL分为两种：

* 标准IP访问列表：1-99、1300-1999
* 扩展IP访问列表：100-199、2000-2699

标准IP访问列表可以根据数据包的源IP地址定义规则，进行数据包的过滤；扩展IP访问列表可以根据数据包的源IP、目的IP、源端口、目的端口、协议来定义规则，进行数据包的过滤。可以说扩展就是对规则可设置项的扩展。在Cisco Packet Tracer中，可以通过access-list指令设置路由器的ACL表。

**【实验设备】**

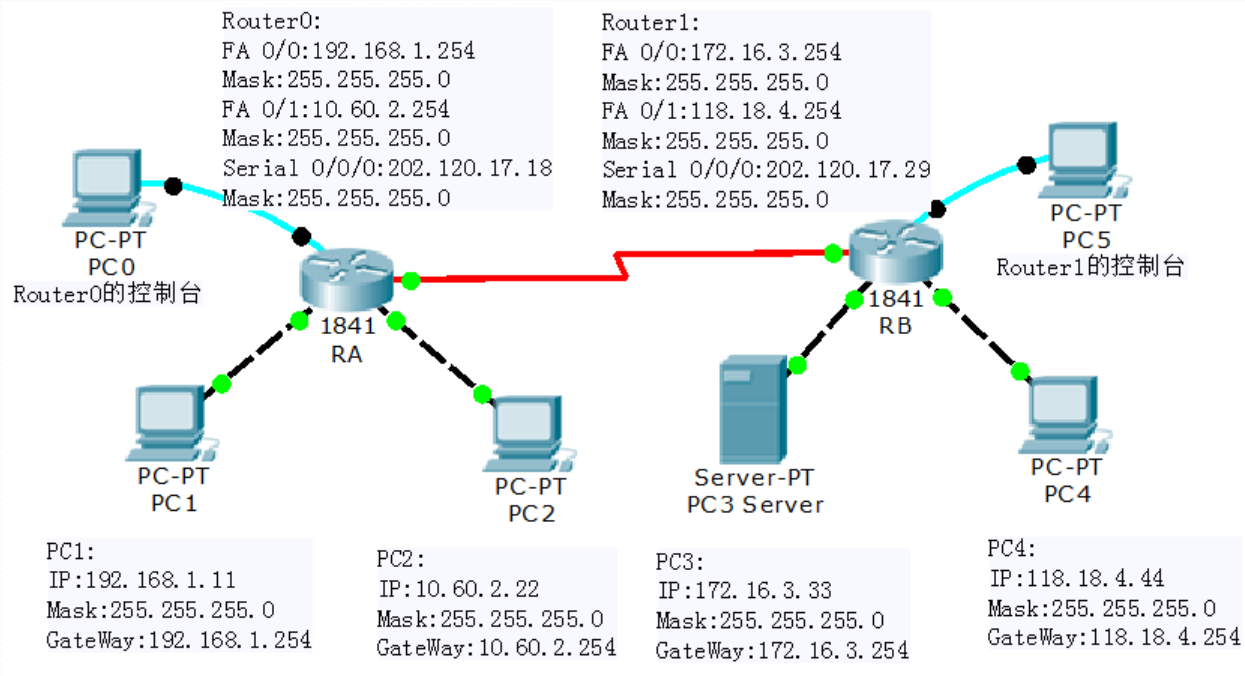
Windows10 x64电脑 1台

**【实验步骤】**

1.启动并进入Windows环境，打开Cisco Packet Tracer

2.创建两个路由器，并添加串口

3.按照下图构建仿真网络，连线



4.配置PC、服务器的地址、网关和掩码

5.配置路由器端口地址：

* Router0：
  + enable
  + configure terminal
  + interface FastEthernet0/0
  + ip address 192.168.1.254 255.255.255.0
  + no shutdown
  + exit
  + interface FastEthernet0/1
  + ip address 10.60.2.254 255.255.255.0
  + no shutdown
* Router1：
  + enable
  + configure terminal
  + interface FastEthernet0/0
  + ip address 172.16.3.254 255.255.255.0
  + no shutdown
  + exit
  + interface FastEthernet0/1
  + ip address 118.18.4.254 255.255.255.0
  + no shutdown

6.配置路由器串口地址：

* Router0：
  + enable
  + configure terminal
  + interface Serial0/1/0
  + ip address 202.120.17.18 255.255.255.0
  + clock rate 56000
  + no shutdown
* Router1：
  + enable
  + configure terminal
  + interface Serial0/1/0
  + ip address 202.120.17.29 255.255.255.0
  + clock rate 56000
  + no shutdown

7.配置路由器静态路由表：

* Router0：
  + ip route 172.16.3.0 255.255.255.0 Serial0/1/0
  + ip route 118.18.4.0 255.255.255.0 Serial0/1/0
* Router1：
  + ip route 192.168.1.0 255.255.255.0 Serial0/1/0
  + ip route 10.60.2.0 255.255.255.0 Serial0/1/0

8.在其它PC端访问172.16.3.33服务器端（ping+http），观察现象

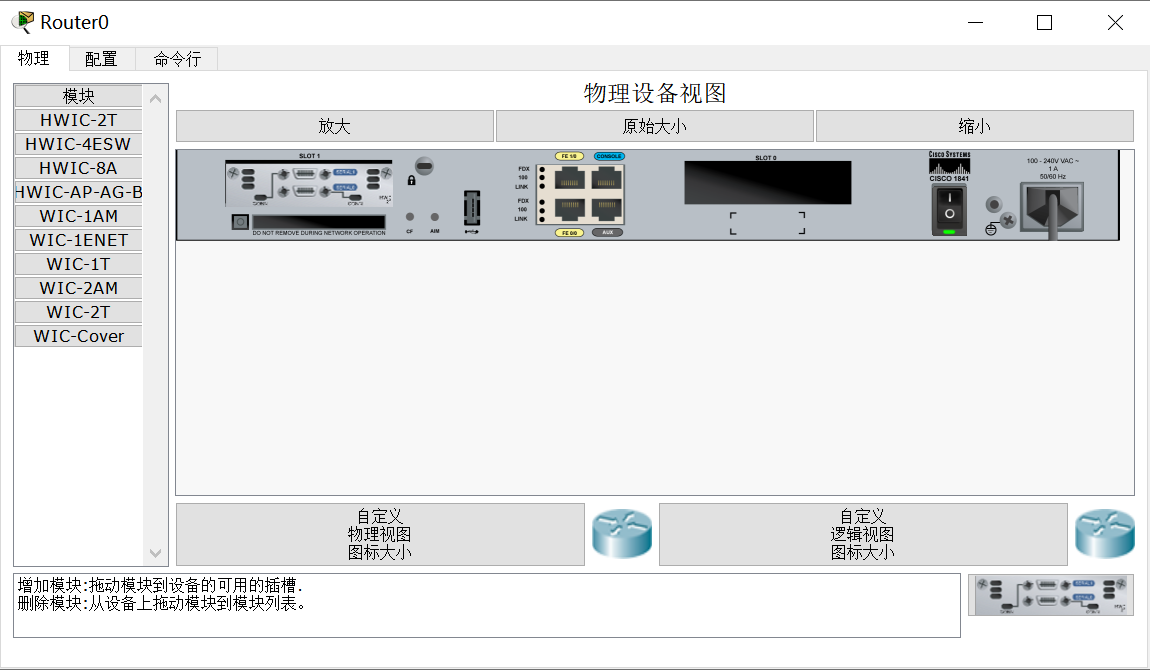
9.配置Router1的扩展ACL表：

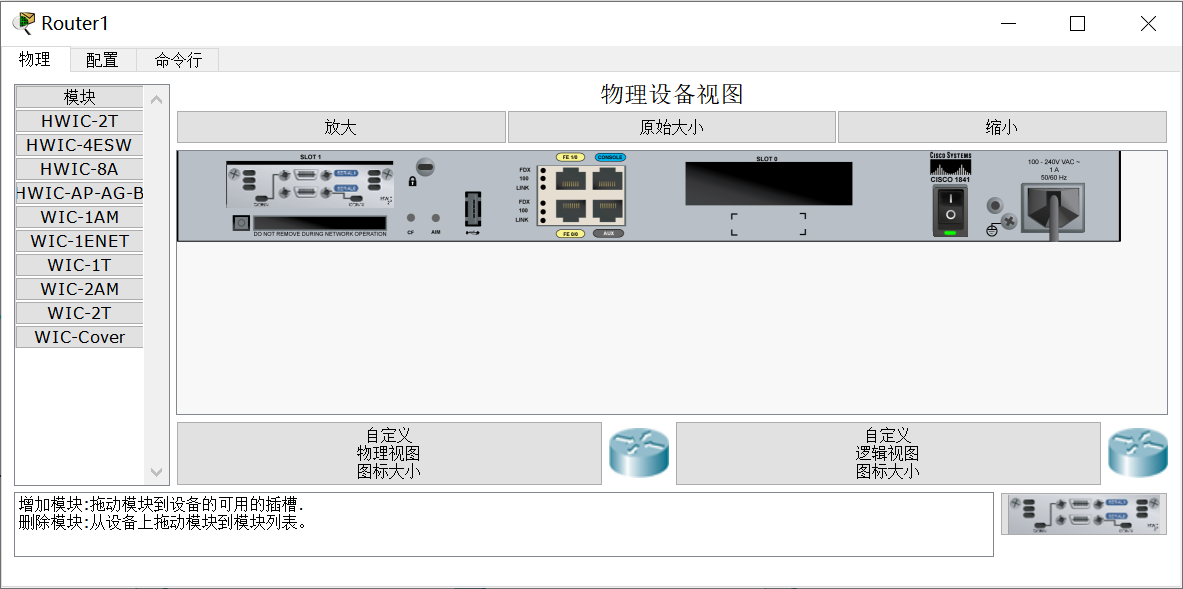
* 拒绝ping包
* access-list 101 deny icmp host 192.168.1.11 host 172.16.3.33
* 允许www访问
* access-list 101 permit tcp host 192.168.1.11 host 172.16.3.33 eq www
* 应用到端口上
* interface Serial0/1/0
* ip access-group 101 in

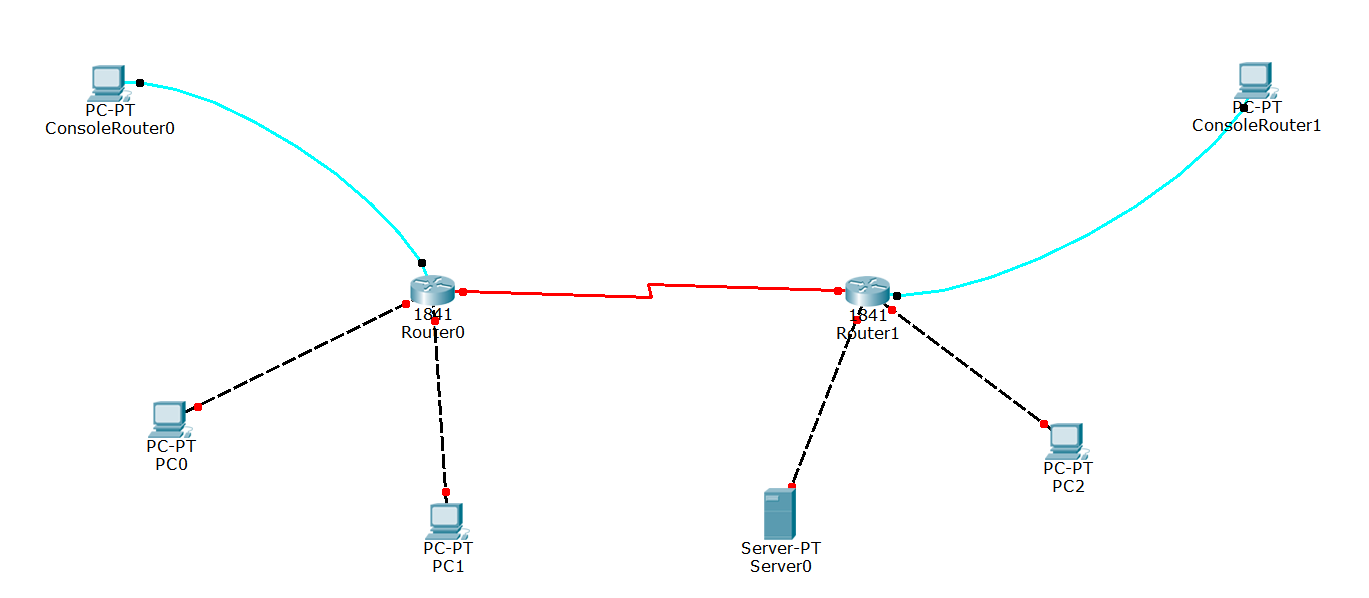
10.在其它PC端再次访问172.16.3.33服务器端（ping+http），观察现象

**【实验现象】**

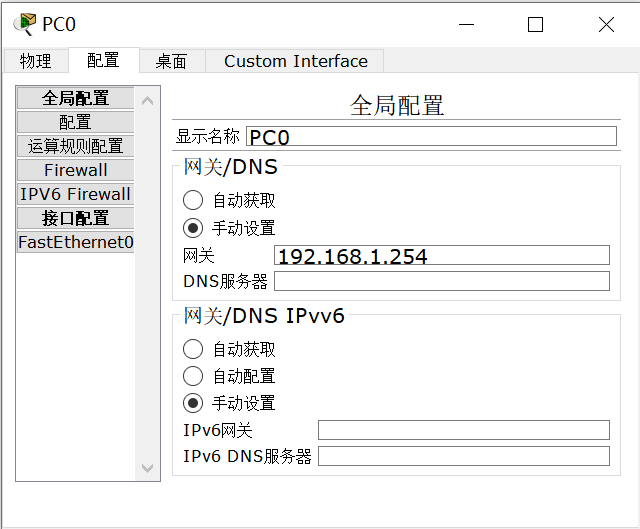
1.给各个路由器添加串口，并构建仿真网络：

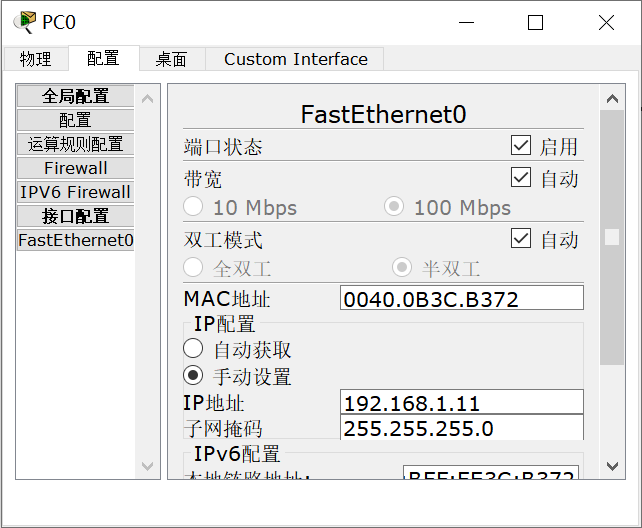


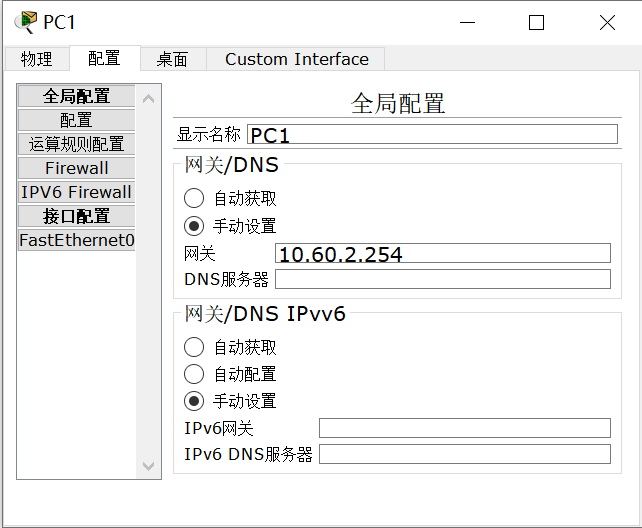


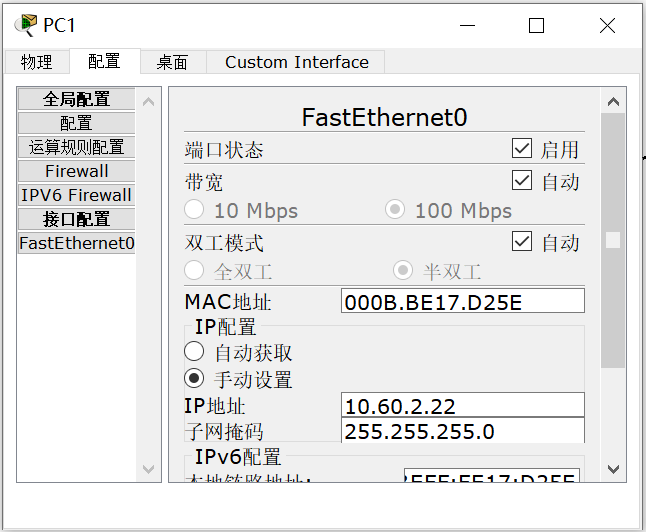


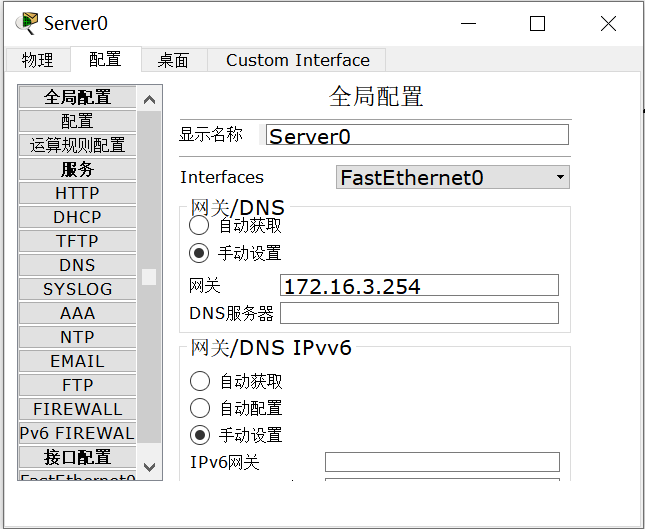
2.配置PC、服务器的地址、网关和掩码：

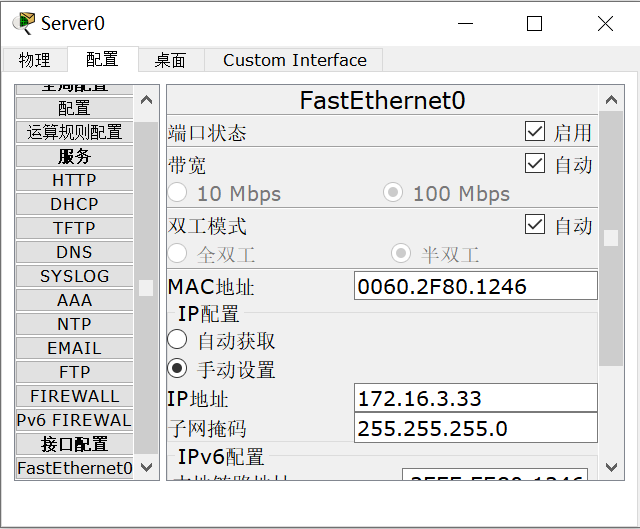


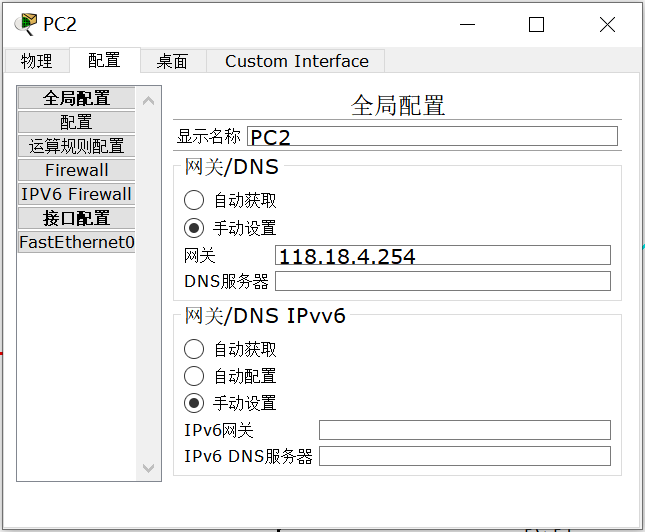


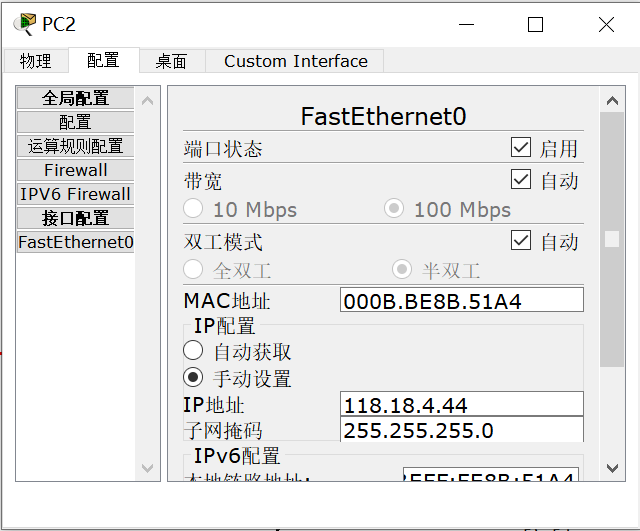




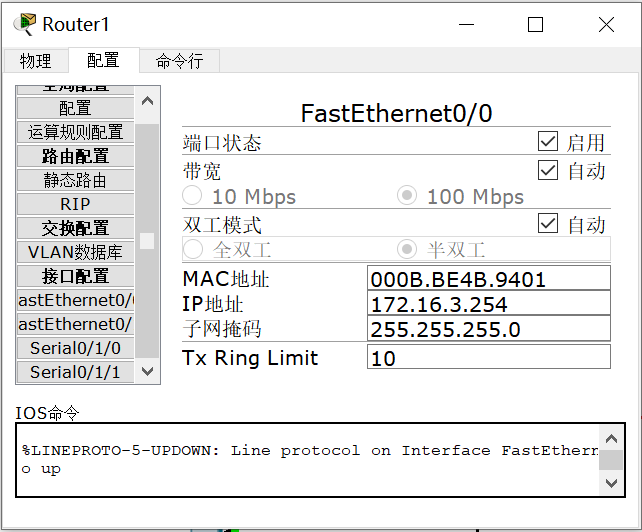
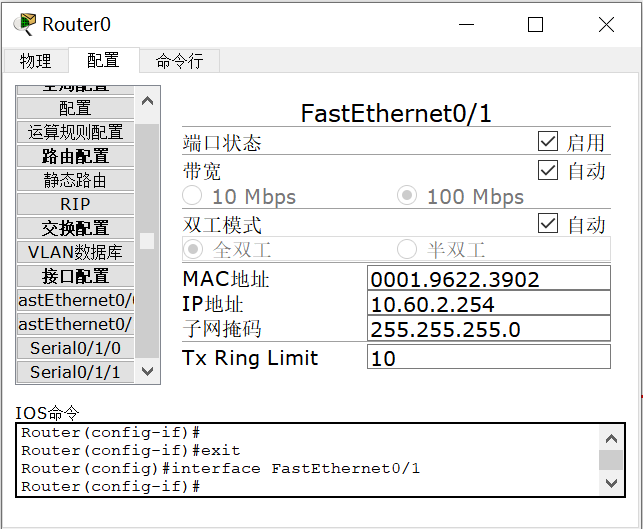
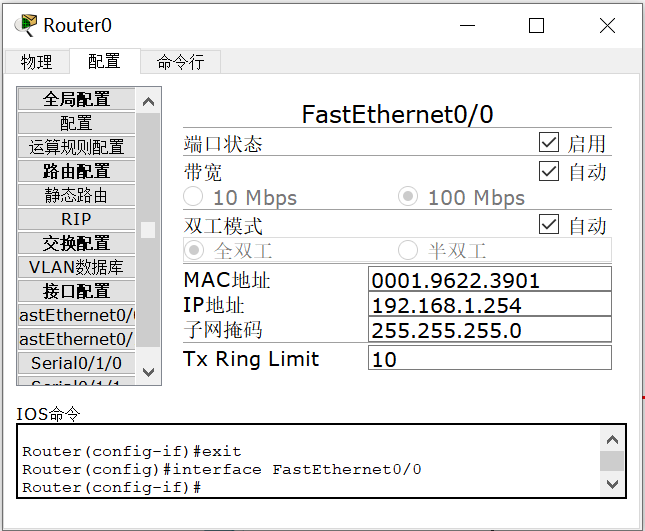


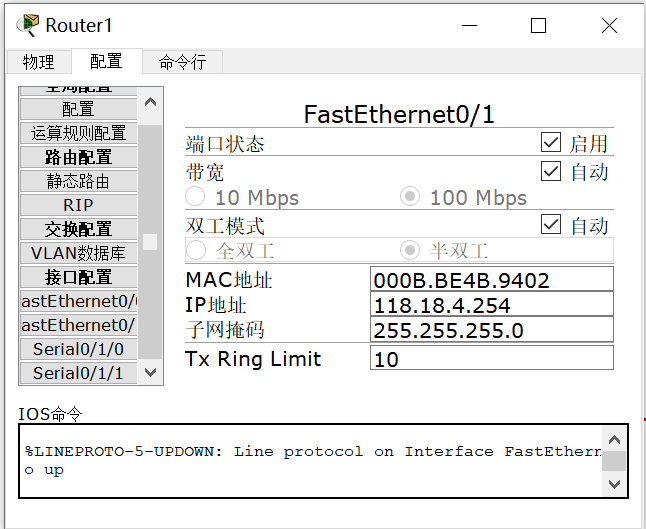




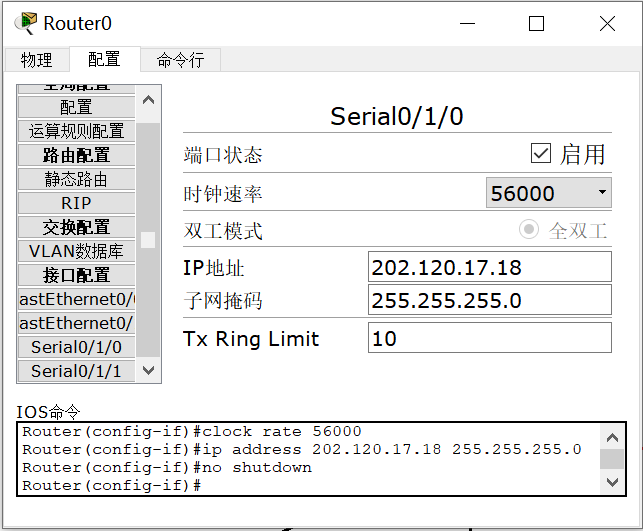


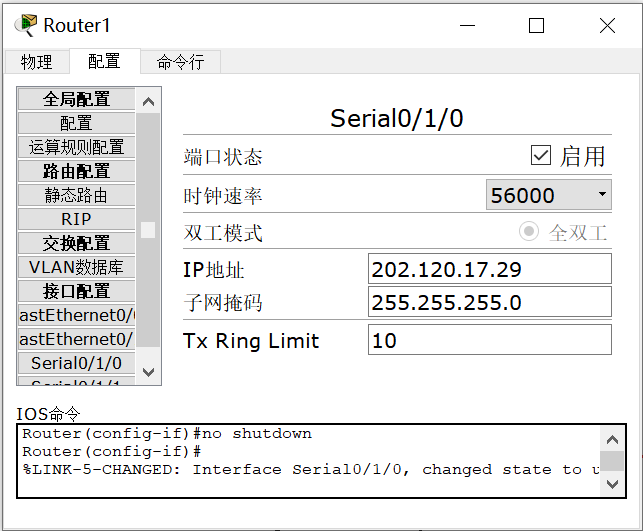
3.配置路由器端口地址：



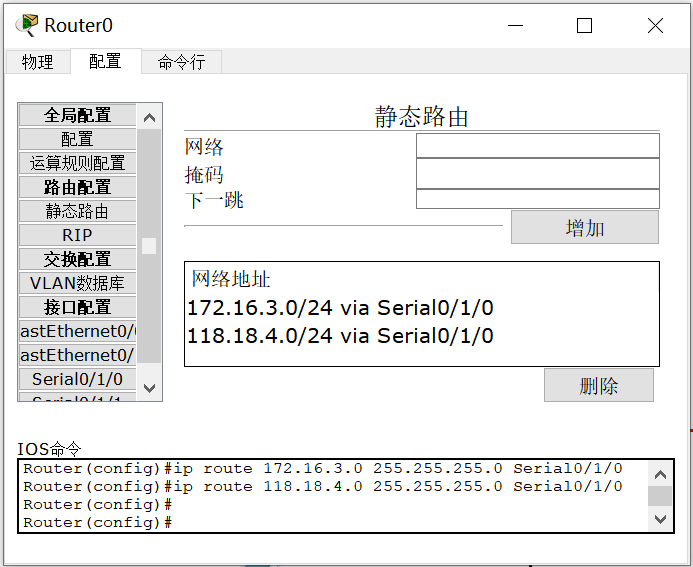


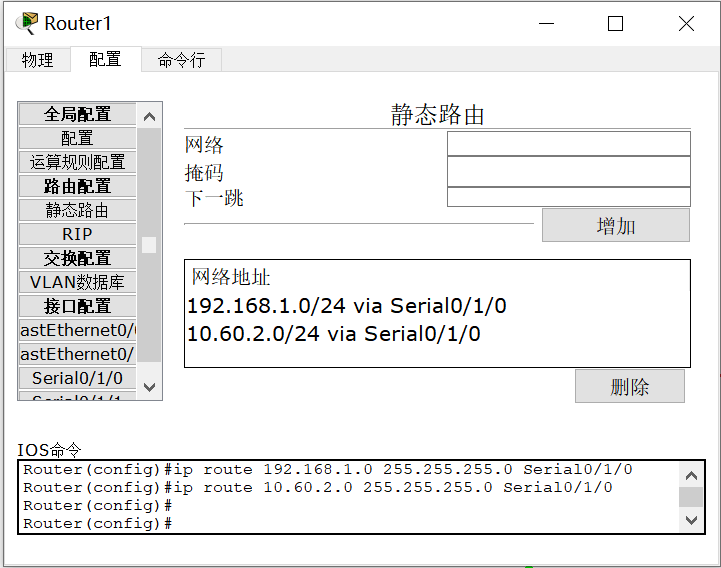
4.配置路由器串口地址：



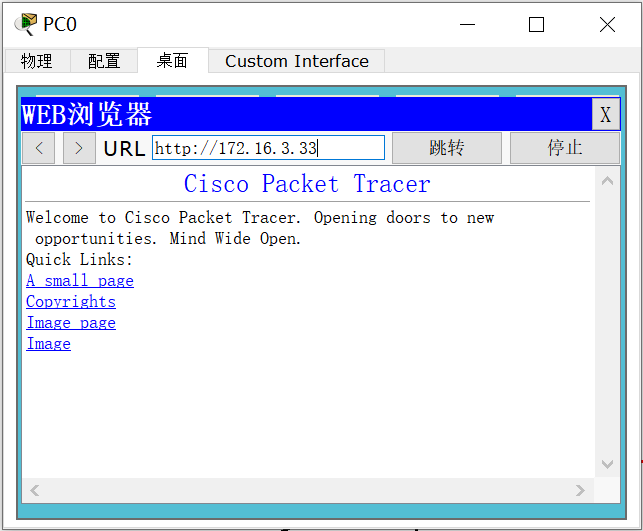
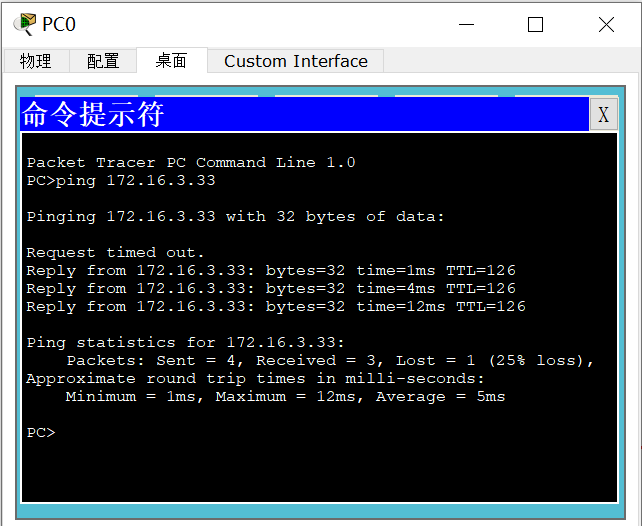


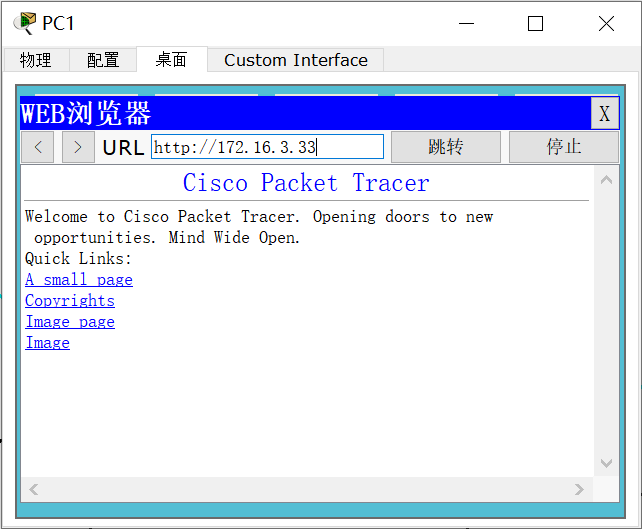
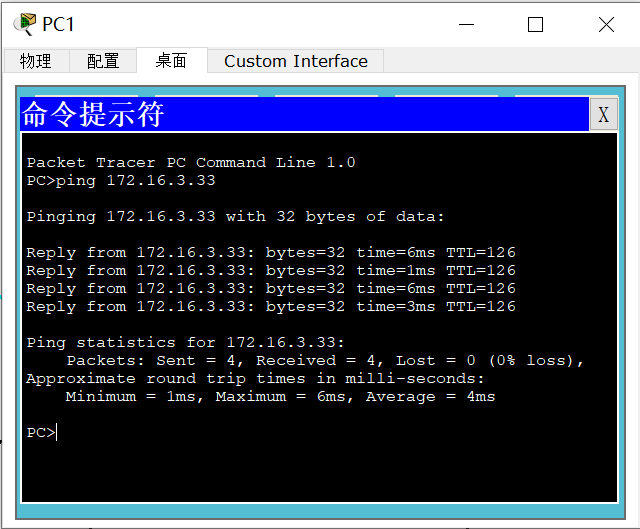
5.配置路由器静态路由表：

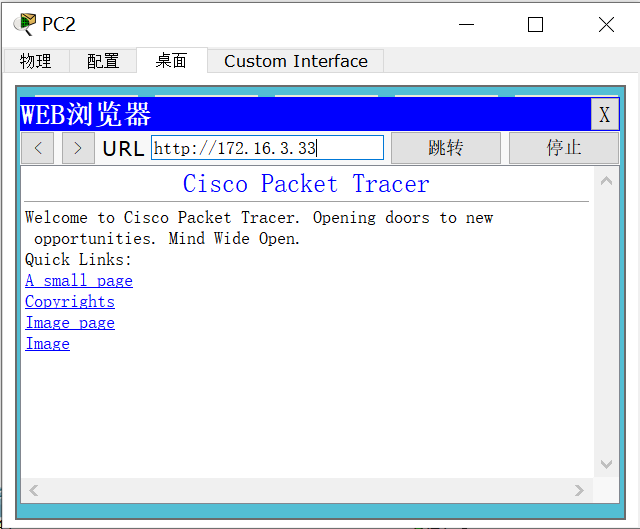
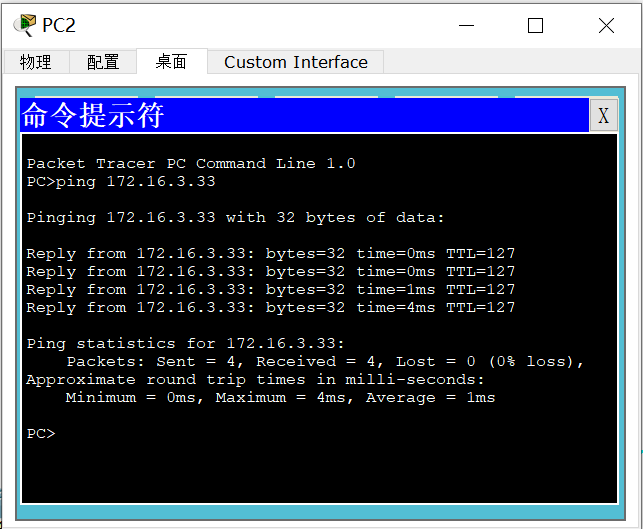




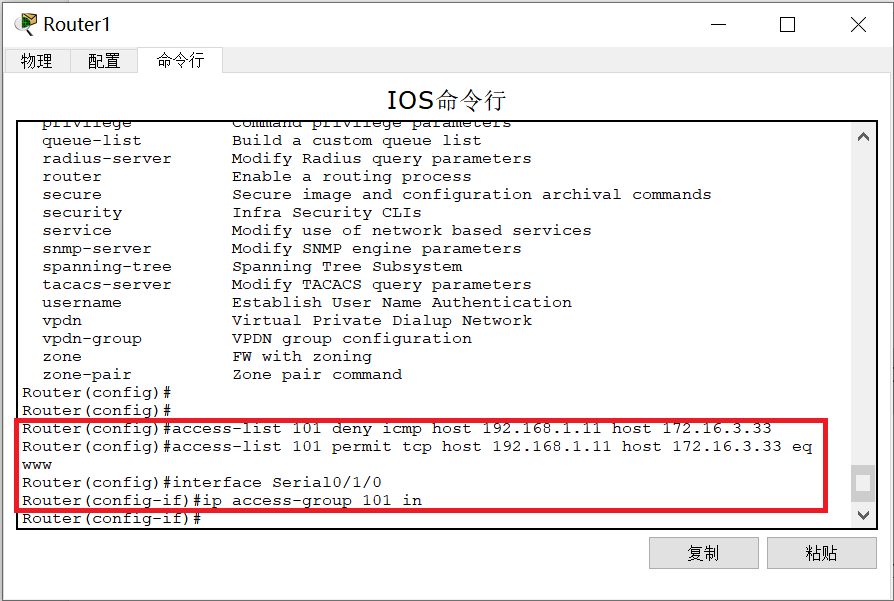
6.配置ACL前各PC访问服务器（ping+http均成功）：



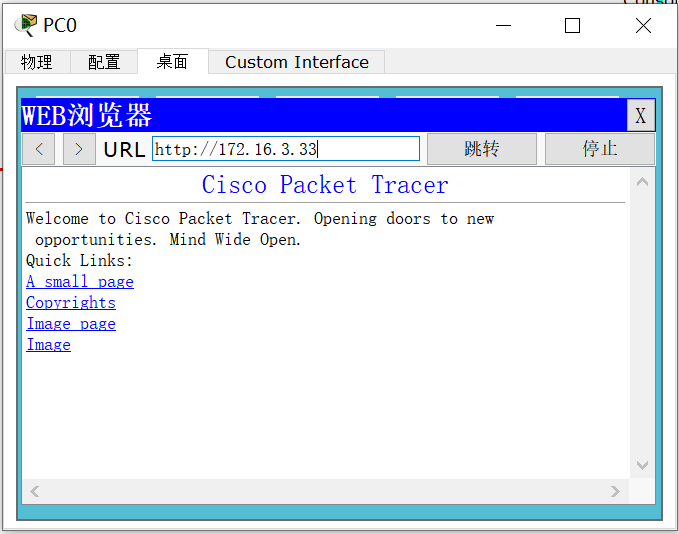
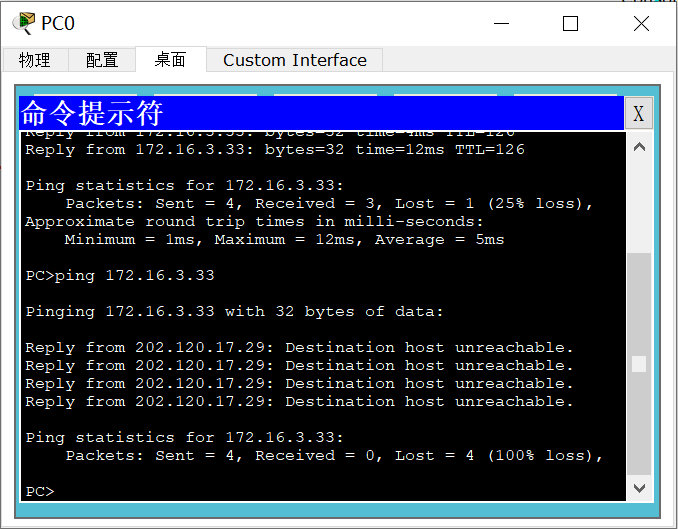


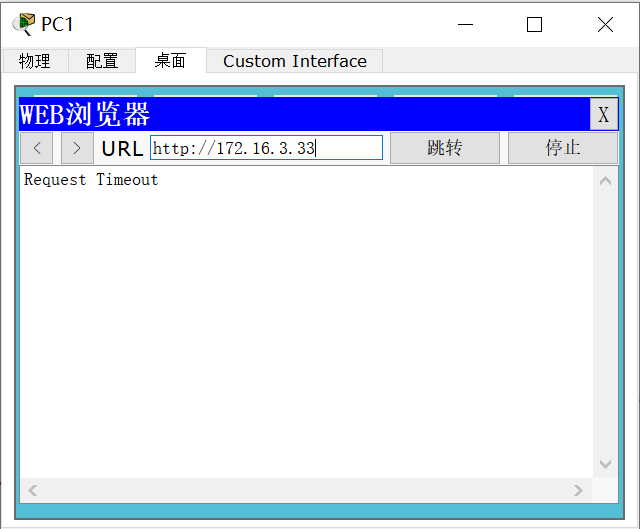
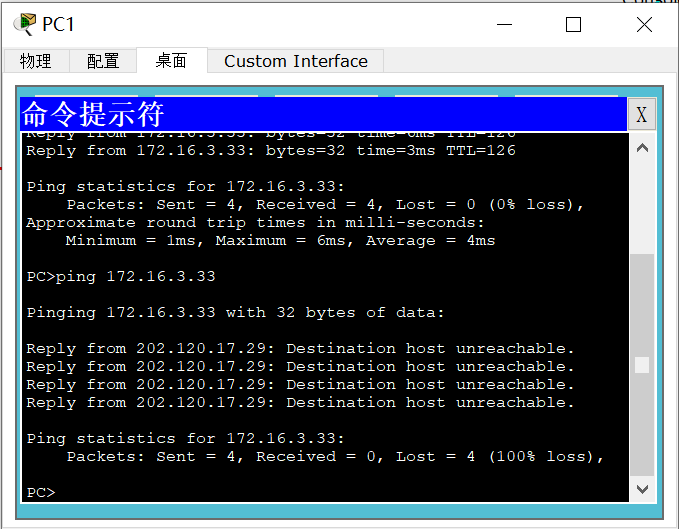


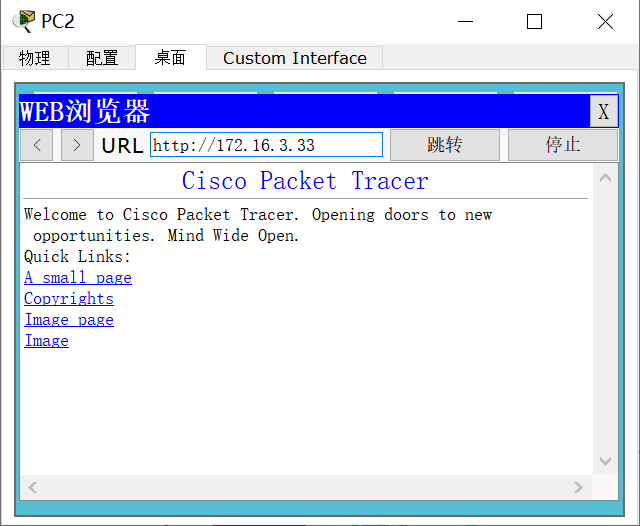
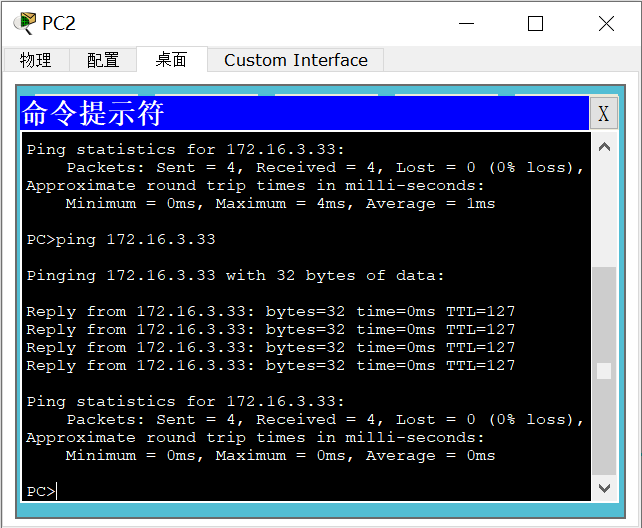
7.配置Router1的ACL表：



8.配置ACL后各PC再次访问服务器：







9.可以发现：

* PC0：ping失败，http成功
* PC1：ping失败，http失败
* PC2：ping成功，http成功

**【分析讨论】**

本次实验通过构建仿真网络并修改路由器的ACL表，对终端对服务器的访问进行了ACL控制。其中配置后三个PC结果不尽相同，可能是：

* PC0完全和配置情况一样：ping失败，http成功。因为配置时就是按照PC0的IP设置的
* PC2未受影响，可能是因为ACL设置会应用到Router1的串口上，而PC2与服务器的通信不需要通过串口，因此没有影响

总之，本次实验我学习到了访问控制的相关知识，受益匪浅。