【实验名称：ACL控制访问】

学生姓名：李雪菲 合作学生：无

实验地点：济事楼330 实验时间：2025-04-17

【实验目的】

实验旨在通过配置和应用接入控制列表（ACL）加深学生对网络安全和数 据包过滤的理解。通过规划网络拓扑、设置设备 IP 和应用 ACL 规则，学生将实 践如何控制网络流量，包括允许或拒绝特定的网络访问，以此提高对网络可管理 性和安全性的认知和操作技能。

【实验原理】

1. ACL技术原理：

ACLs (Access Control Lists)，全称为接入控制列表，也称为访问列表（Access Lists），俗称为防火墙，有的文档中还称之为包过滤。ACL 通过定义一些规则对网络设备接口上的数据报文进行控制：允许通过或丢弃，从而提高网络可管理性和安全性。

ACL的语句顺序决定了对数据包的控制顺序。在ACL中各描述语句的放置顺序是很重要的。当路由器决定某一数据包是被转发还是被阻塞时，会按照各项描述语句在ACL中的顺序，根据各描述语句的判断条件，对数据包进行检查，一旦找到了某一匹配条件就结束比较过程，不再检查以后的其他条件判断语句。

1. ACL的3P规则：

3P规则是指在路由器上应用ACL的一般规则，即可以为每种协议 (per protocol)、每个方向 (per direction)、每个接口 (per interface) 配置一个ACL；例如：一个ACL只能控制接口上一个方向的流量。要控制入栈流量和出栈流量，必须分别定义两个ACL来实现。

1. ACL的分类：

根据定义字段（元素）：标准ACL（标准IP ACL）、扩展ACL（扩展IP ACL、MAC ACL、专家ACL）；根据定义的层次：基于IP的ACL（ IP ACL ）、基于MAC的ACL（ MAC ACL ）、专家ACL（Expert ACL）；根据命名规则：编号ACL、命名ACL（即使用名称代替表号）。

【实验设备】

1.一台电脑

2.cisco packet tracer仿真软件

【实验步骤】

1 首先规划网络地址及拓扑图

2 配置PC机、服务器及路由器口IP地址

3 验证各PC间的互通性

4 各路由器上配置静态路由协议,使全网可达

5 验证各PC间能否相互 ping通

6 在RB上配置ACL： A,除PC1以外的电脑能ping通PC3；B,只有PC1可以通过WWW访问PC3；

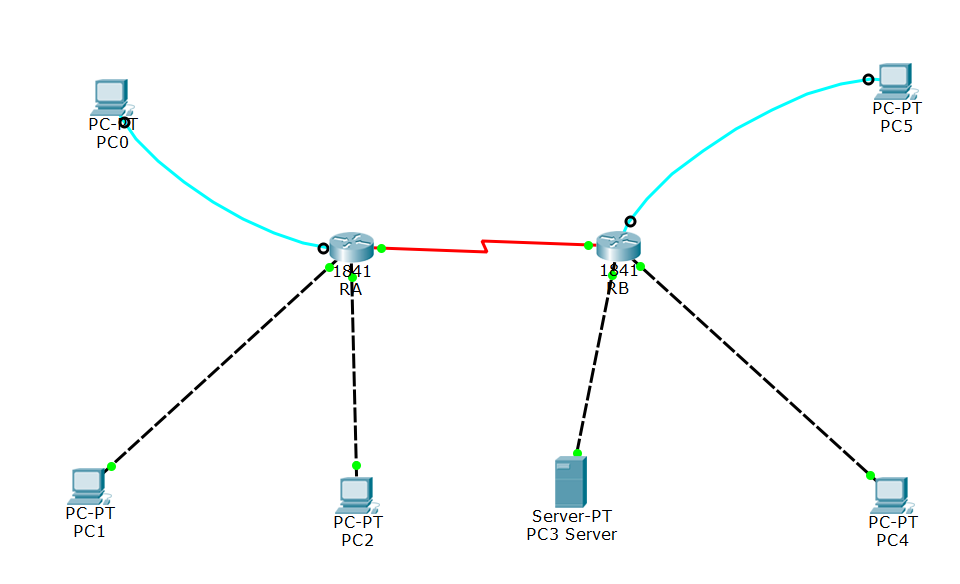
7 在端口上应用ACL；

8 验证主机之间的互通性

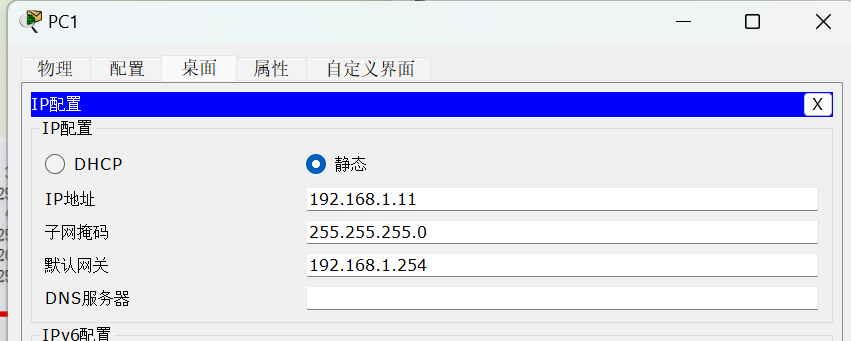
9 查看控制访问列表

【实验现象】

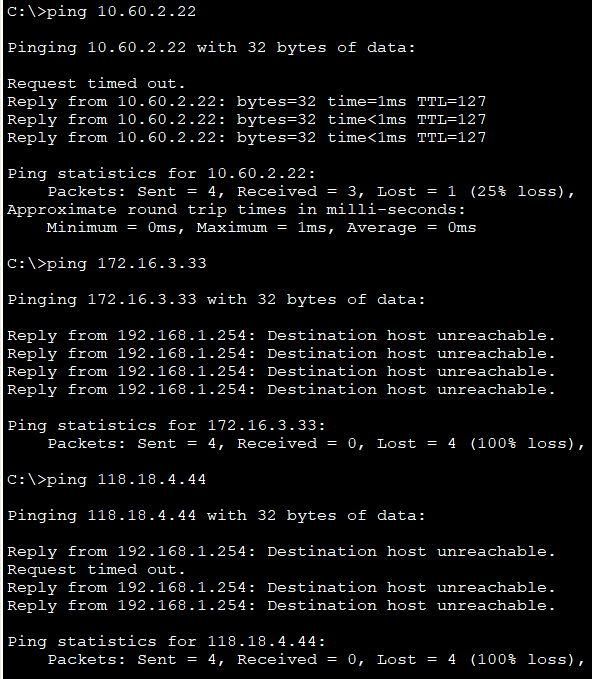
1 首先规划网络地址及拓扑图



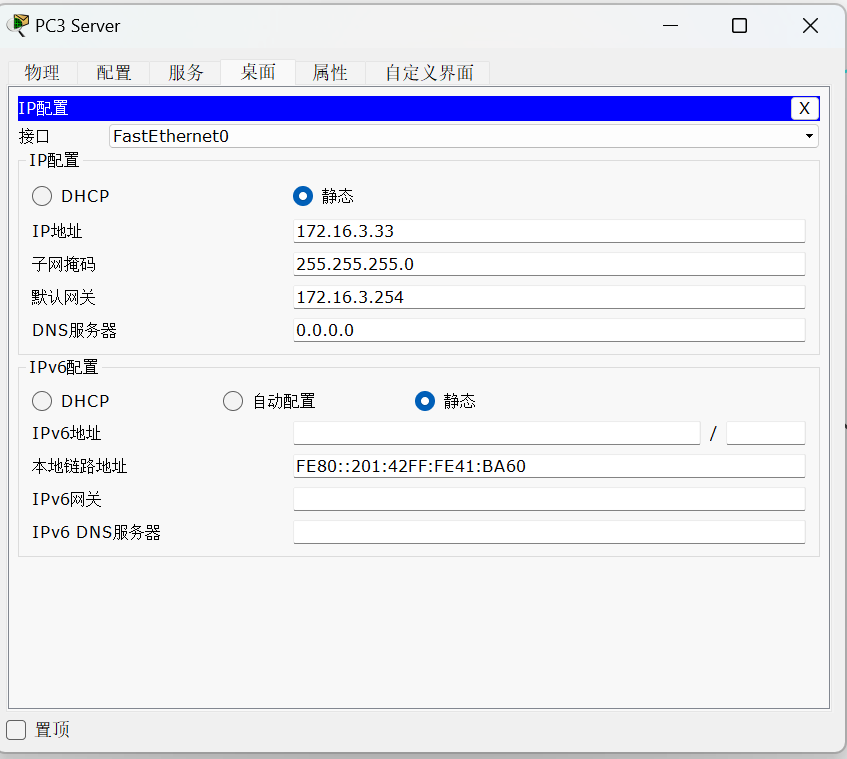
2 配置PC机、服务器及路由器口IP地址



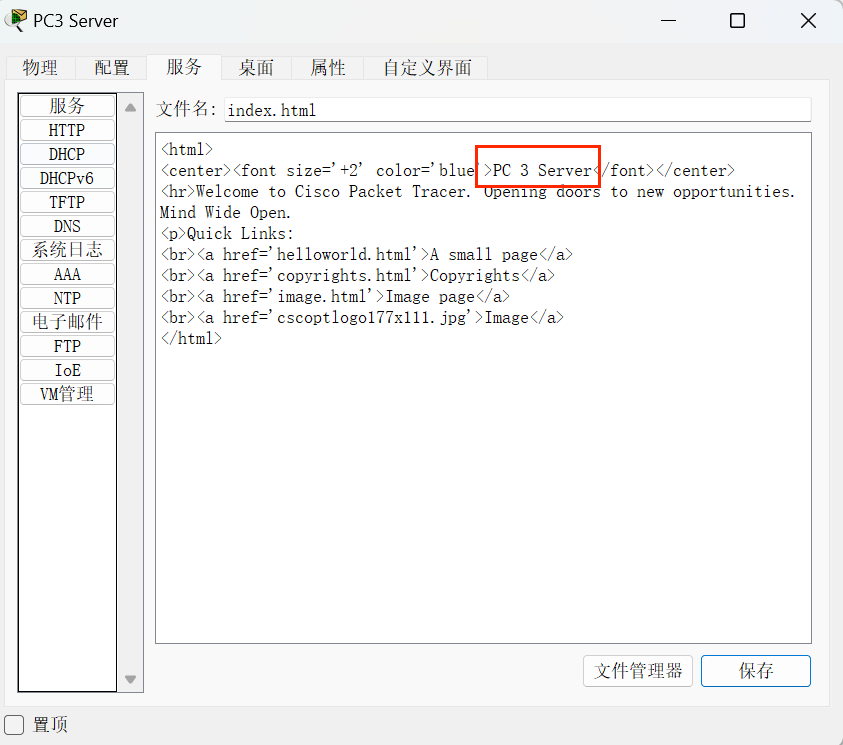
3 验证各PC间的互通性 （以PC1为例）



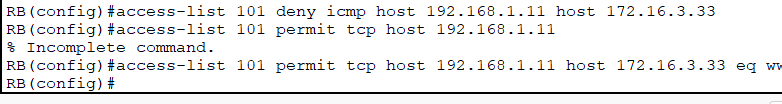
4 Server-PT (PC3 Server)配置好IP、网关及掩码



5 网页标题更新为PC3 Server，便于识别



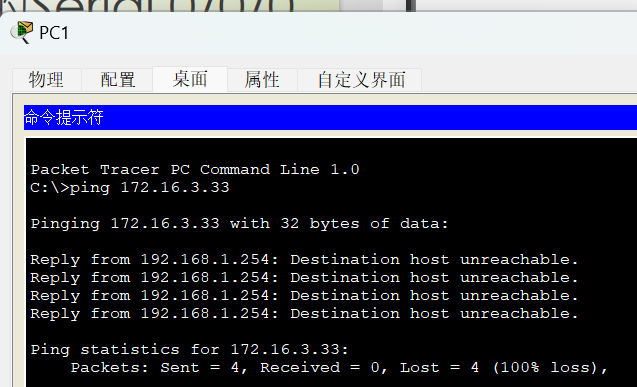
6 在RB上配置ACL： A,除PC1以外的电脑能ping通PC3；B,只有PC1可以通过WWW访问PC3；

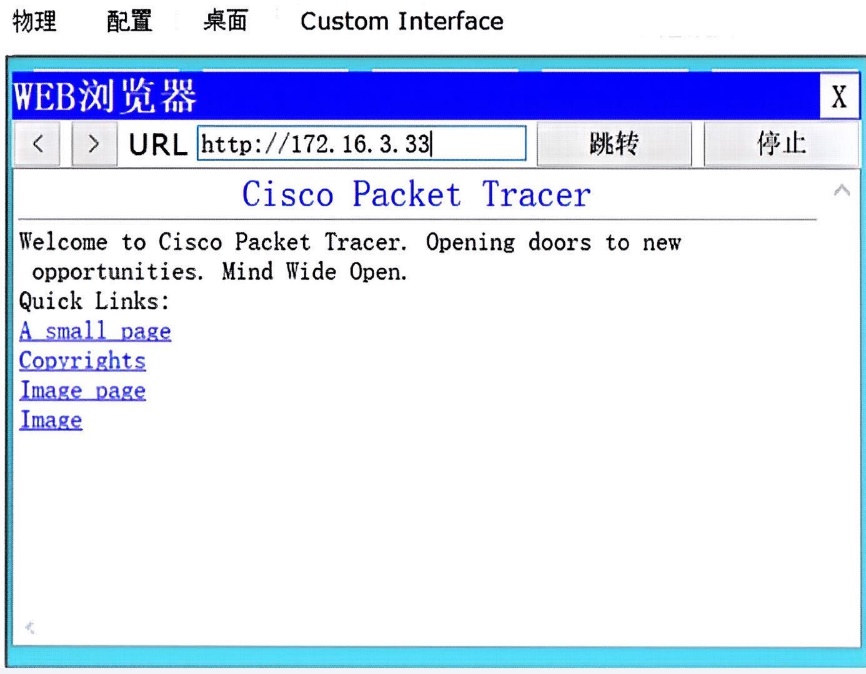


7 在端口上应用ACL；

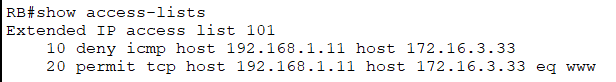


8 验证主机之间的互通性





9 查看控制访问列表



【分析讨论】

1.打开 172.16.3.33 服务器端的 WEB，并在其它 PC 端访问。

答：（1) Ping 172.16.3.33：

ACL 配置前：所有 PC（如 192.168.1.11）可以正常 ping 通 172.16.3.33，说明网络连通。

ACL 配置后（配置如下）：192.168.1.11 无法再 ping 通 172.16.3.33，因为被 ACL 显式拒绝。

（2) 访问 <http://172.16.3.33>：

ACL 配置前：PC1 可以通过浏览器访问该地址，页面正常打开。

ACL 配置后：PC1 仍然可以访问 http://172.16.3.33，因为 ACL 明确允许了 TCP 端口 80 的通信。

2．如果将 ACL 修改为如下，有什么不同效果？分析说明原因

access-list 101 deny icmp 192.168.1.0 0.0.0.255 host 172.16.3.33

答：（1）不同效果：原来只拒绝 192.168.1.11 发起的 ping。现在拒绝整个 192.168.1.0/24 网段所有主机对 172.16.3.33 的 ICMP 请求。

|  |  |  |
| --- | --- | --- |
| 主机 IP | 原 ACL ping 结果 | 新 ACL ping 结果 |
| 192.168.1.11 | 被拒绝 | 被拒绝 |
| 192.168.1.12 | 可以 ping | 被拒绝 |
| 192.168.1.13 等 | 可以 ping | 被拒绝 |

（2）原因：ACL 中使用的 192.168.1.0 0.0.0.255 是一个通配符掩码，表示整个 C 类网段。所以匹配范围从单个 IP 扩大为整个网段，访问控制范围加宽。