**【实验名称】：**ACL访问控制

**学生姓名：2151133**孙韩雅 **合作学生：2151780**袁皓玥

**实验地点：**济事楼330 **实验时间：**2023-10-23

**【实验目的】**

了解ACL的概念与技术原理，利用控制列表实施网络安全。

**【实验原理】**

ACLs的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，在有的文档中还称之为包过滤。

ACLs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；

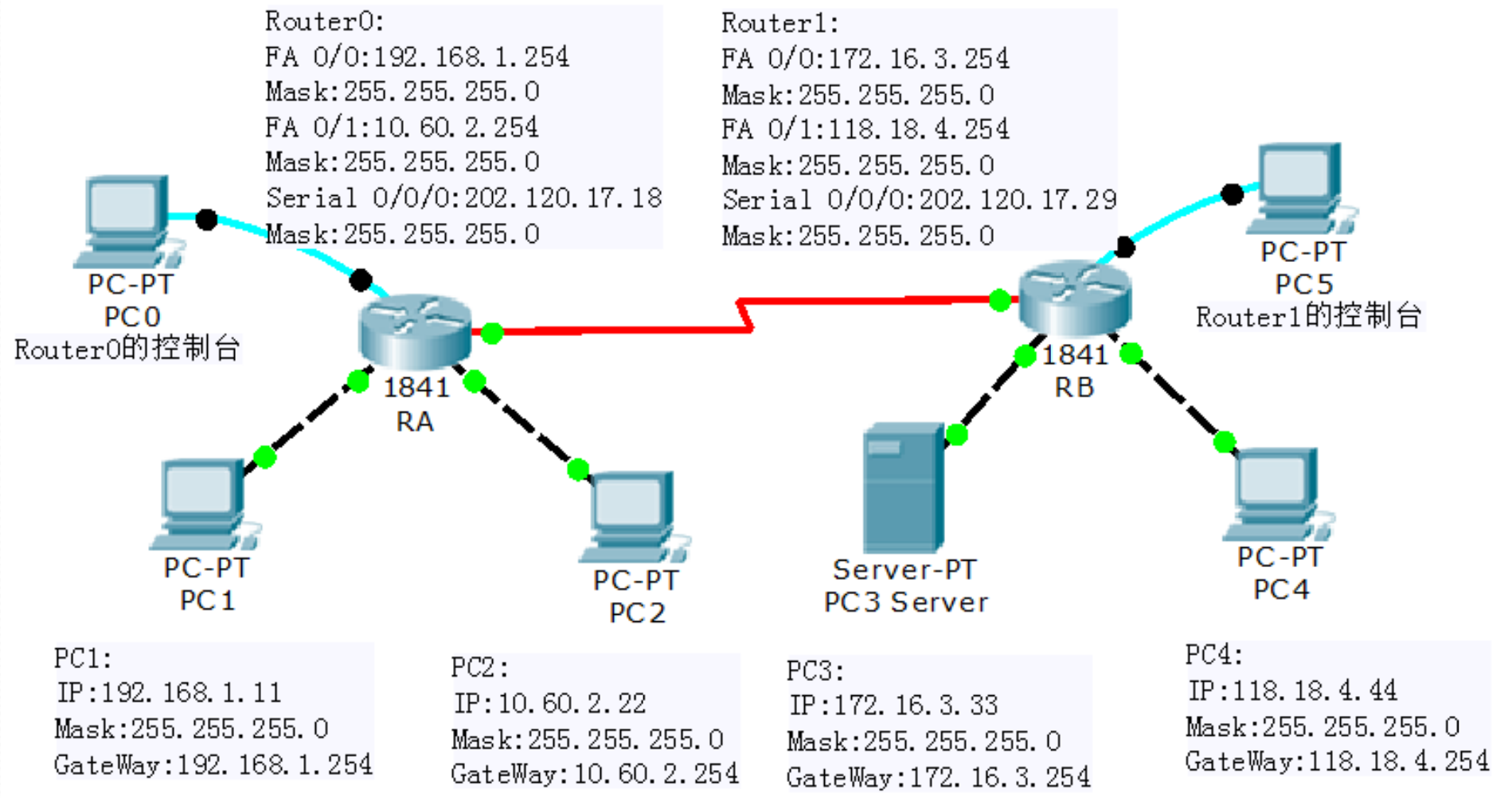
IP ACL分为标准IP访问列表和扩展IP访问列表，它们的编号范围分别为1-99、1300-1999、100-199、2000-2699.标准IP当问列表可以根据数据包的源IP地址定义规则，进行数据报的过滤，而扩展IP访问列表可以根据数据包的源IP、目的IP、源端口、目的端口、协议来定义规则，进行数据包的过滤。

**【实验设备】**

机房电脑（安装有**Cisco Packet Tracer**）

**【实验步骤】**

1.首先规划网络地址及拓扑图，如示例图；



2.配置PC机、服务器及路由器口IP地址；

3.在各路由器上配置静态路由协议，让pc间能相互ping通；

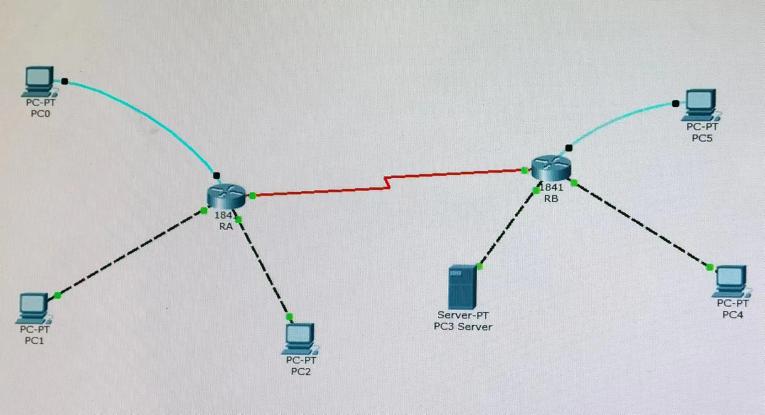
4.在RB上配置ACL；

5.在RB接口上应用ACL；

6.验证主机之间的互通性及WWW访问。

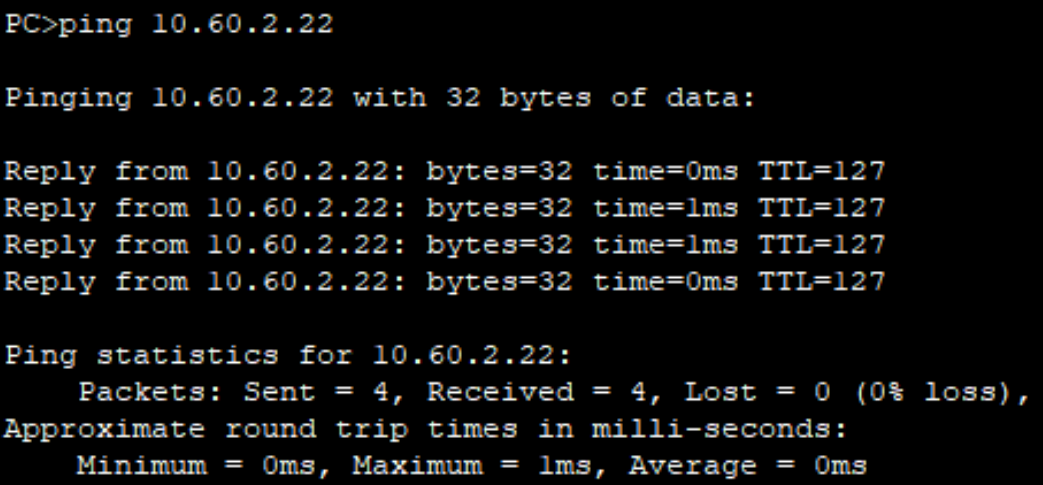
**【实验现象】**

1.按照课件拓扑图连线并配置各个PC的IP、子网掩码和网关：



2.配置路由器的端口和串口端口地址。

3.检测PC能够ping通：



4.配置RouterB的扩展ACL表：

a.拒绝ping包：access-list 101 deny icmp host 192.168.1.11 host172.16.3.33

b.允许www访问：access-list 101 permit tcp host 192.168.1.11 host 172.16.3.33eq www

5.测试是否能够联通：当PC1通过ping访问172.16.3.33时无法连通，但当PC1通过URL访问172.16.3.33能够成功访问。但PC2通过ping和url都不能连通。

**【分析讨论】**

ACL是一种非常重要的网络安全机制，它可以帮助我们控制网络流量和保护网络资源的安全。通过ACL，我们可以定义规则来限制特定IP地址或IP地址范围的访问，或者允许特定的端口或服务进行通信。这有助于保护网络免受潜在的安全威胁和未经授权的访问。在默认情况下，除非明确规定允许通过，访问列表总是阻止或拒绝一切数据包的通过，即实际上在每个访问列表的最后，都隐含有一条"deny any"的语句。因此PC2也不能通过ping访问172.16.3.33且由于没有明确规定可以通过www访问，所以PC2始终无法访问172.16.3.33。

在实验中，我学会了使用不同的ACL类型，如标准ACL和扩展ACL，并熟悉了它们的不同用途和限制。我还学会了如何排查和调试ACL配置中可能出现的问题，以确保ACL的正确性和有效性