杭州电子科技大学计算机网络实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 | 郑凯心 | 学号 | 19063140 | | |
| 组别 | 4 | 时间 | 20211224 | | |
| 小组成员 | 郑凯心 张浩杨 符振皓 林伟杰 汤丰瑜 蔡思林 王常平 王浩冰 | | | | |
| 实验名称 | ACL的基本配置 | | | 序号 | 1 |

一、实验目的：

(1) 理解标准和扩展访问控制列表应用场景

(2)掌握标准访问控制列表的配置方法

(3)掌握扩展访问控制列表的配置方法

(4)掌握基于名称的访问控制列表的配置方法

二、实验内容及原理：

访问控制列表简称为ACL(Access Control List)。 访问控制列表使用数据包过滤技术，在路由器上读取网络层数据报及传输层报文段中的头部信息如源地址、目的地址、源端口和目的端口等，根据预先定义好的规则对数据包进行过滤，从而达到访问控制的目的。最初仅有路由器支持该技术，近些年来已经扩展到交换机，甚至二层交换机也开始提供ACL的支持了。

由于ACL涉及的配置命令很灵活，功能也很强大，因此在进行本实验之前，需要了解

访问控制列表的一-些基本使用原则。

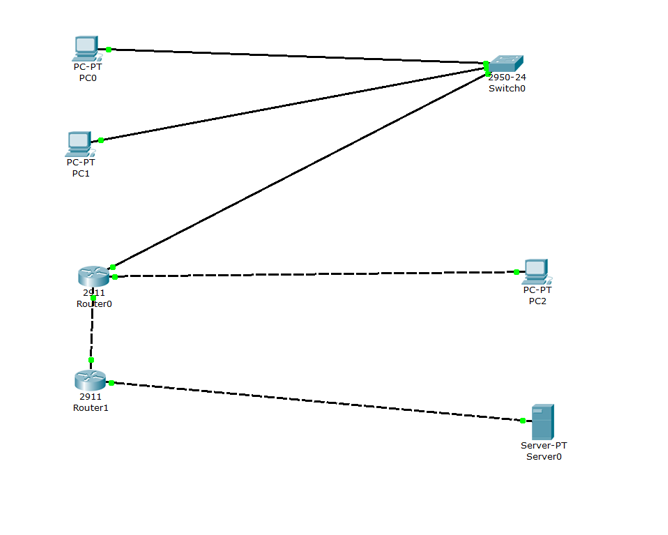
(1)最小特权原则:只给受控对象完成任务所必须的最小权限。

(2)最靠近受控对象原则:访问权限控制--般在离受控对象最近的路由器或交换机上实施。

(3)默认丢弃原则:在检查ACL规则时是自上而下逐条进行匹配的，只要发现符合条件就立刻转发，而不继续检查后续的ACL规则。在一些路由器或交换设备中默认的最后一条ACL规则为DENY ANY,也就是丢弃所有不符合条件的数据包。

由于ACL是使用数据过滤技术来实现的，依据的仅仅是数据包头部的部分信息，因此这种技术具有一些固有的局限性。要达到细粒度的端到端权限控制目的，就需要和系统及应用级的访问权限控制结合使用。

三、实验设备及拓扑结构：



四、实验过程及结果

