杭州电子科技大学 计算机网络 实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 | 黄茂祥 | 学号 | 22590502 | | |
| 组别 |  | 时间 | 2023/12/22 | | |
| 小组成员 |  | | | | |
| 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。

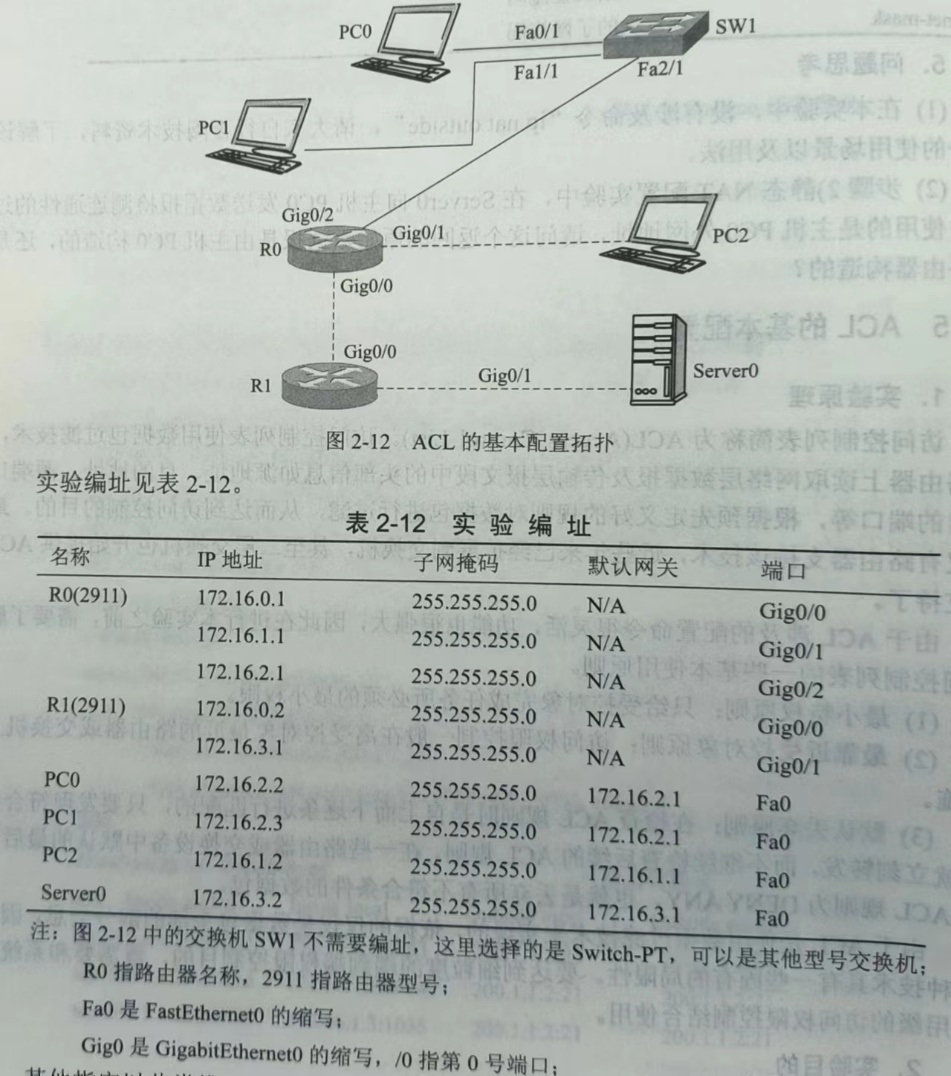
（2）最靠近受控对象原则：访问权限控制一般在离受控对象最近的路由器或交换机上实施。

（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：

本实验模拟一个企业的应用场景。路由器RO是企业的分支机构网关，与两个子网相连，其中的一个子网使用交换机和RO连接，另一个子网只有一台主机与RO直接相连。路由器R1代表企业总部的网络，与一个服务器直接相连。整个网络使用OSPF协议进行路由。网络的拓扑结构如图2-12所示。

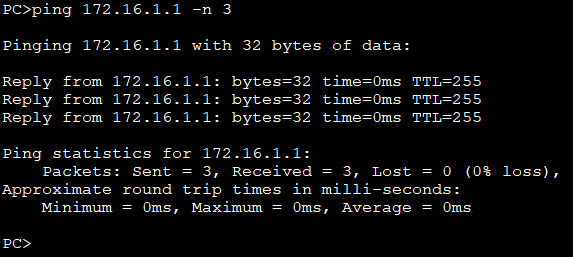


1. 实验过程及结果

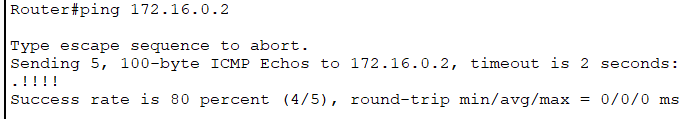
1）基本配置

根据实验编址进行相应的配置，使用ping命令检测各个直连链路的连通性。

实例2-47：检测主机PCO和路由器RO之间的连通性

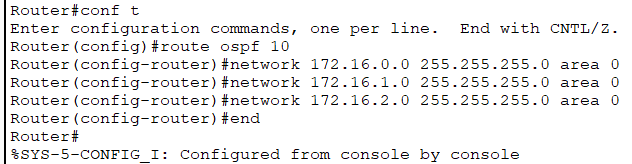


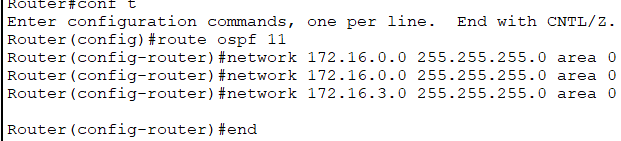
实例2-48：检测路由器RO和R1之间的连通性



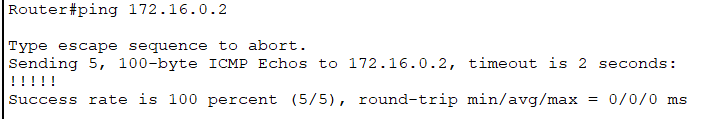
其他直连链路的连通性检测这里省略。

在各个直连链路的连通性得到确认后，配置路由器RO和R1的OSPF协议。





实例2-49：检测主机PC0和服务器Server0之间的连通性



2）基本ACL配置

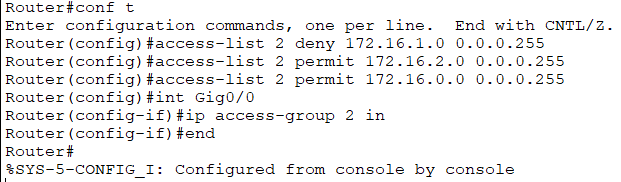
访问控制列表 ACL分很多种，不同场合应该使用不同的ACL，其中最简单的就是标准访问控制列表。标准访问控制列表使用IP数据报中的源IP地址进行过滤，在Packet Tracer模拟器中，使用ACL号1到99来创建相应的访问控制列表规则。

源主机范围可以是任何主机，某一台主机或者一个网段。

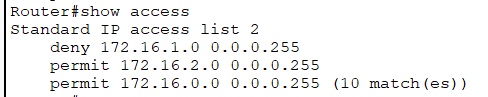
当源主机是任何主机时使用“any”表示，如是某一台主机则以“host”开始，然后跟随该主机的IP地址。

如果源主机范围是一个网段，那么使用网络地址，然后跟随该网段掩码。

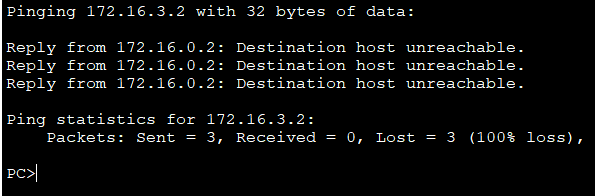
实例2-50：路由器R1配置ACL允许172.16.2.0/24网段，禁止172.16.1.0/24网段主机访问172.16.3.0/24子网



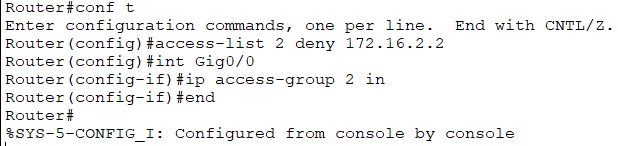
实例2-51：检查路由器R1的ACL配置



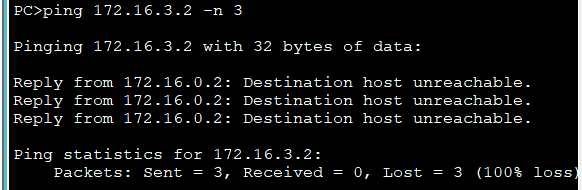
检测路由器RI的ACL配置效果，在主机PC2上测试与服务器的连通性。



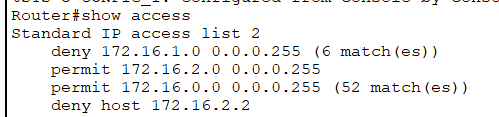
实例2-52：基于主机的ACL配置，在路由器R1配置ACL允许访问 172.16.2.0/24子网，但是主机 PC0(172.16.2.2)除外，并禁止172.16.1.0/24子网主机访问172.16.3.0/24子网。



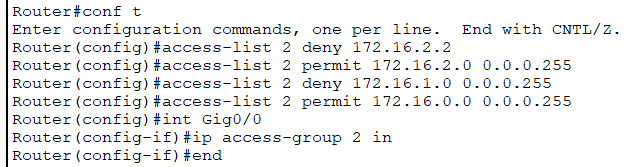
但是经过以上配置，主机PCO依然可以访问172.16.3.0/24子网。



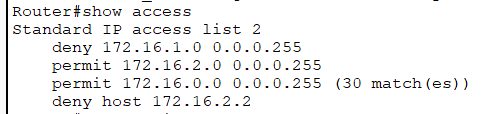
这时我们需要分析为什么会有这种现象，首先应该检查路由器的ACL配置。



原来，刚才配置的ACL规则被添加到最后面了，根据ACL规则的匹配次序，这条新增的规则没有机会被使用。我们需要重新配置路由器R1的ACL，调整ACL的访问顺序。使用以下命令：



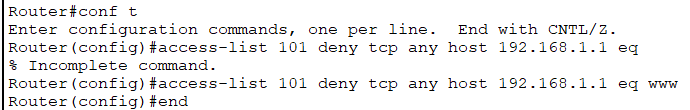
重新检查R1的ACL配置，可以发现这一次达到配置要求了。



3）扩展ACL配置

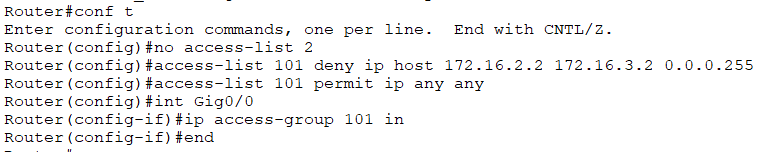
扩展访问控制列表是一种高级的ACL，可以对数据包的端口字段进行过滤。使用扩展访问列表可以有效地控制用户访间某个网段但是同时又禁止使用某个特定服务（例如WWW，FTP等）。扩展访问控制列表使用的ACL号为100到199。

实例2-53：扩展访问控制列表命令格式

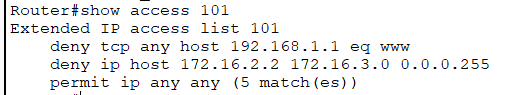


这个命令将限制所有主机访问192.168.1.1这个地址WWW 服务 TCP连接的数据报。

实例2-54：扩展ACL配置，禁止主机 PC0(172.16.2.2）访问服务器Server0（172.16.3.2)



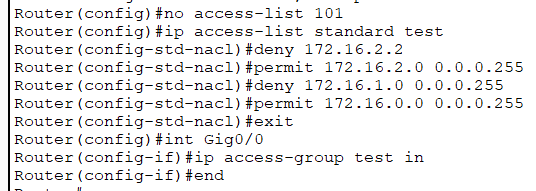
重新检查R1的ACL配置，显示访问控制列表101已配置完毕。



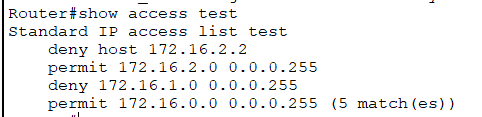
4）基于名称的访问控制列表的使用方法

前面使用的标准访问控制列表和扩展访问控制列表有一个弊端，那就是当设置好ACL的规则后发现其中的某条有问题，如果希望进行修改或删除的话只能将全部ACL信息都删除。也就是说修改一条或删除一条都会影响到整个ACL列表。这个问题给实际的工作带来了很多麻烦，我们可以用基于名称的访问控制列表来解决。使用基于名称的访问控制列表进行管理，可以减少很多后期维护工作，方便随时进行ACL规则的调整。

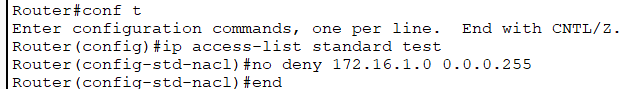
实例2-55：基于名称的访问控制列表



重新检查R1的ACL配置，显示访问控制列表test己配置完毕。



实例2-56：删除 ACL 规则“deny 172.16.1.00.0.0.255”



重新检查RI的ACL配置，显示访问控制列表中该规则已删除。

