|  |  |
| --- | --- |
| 实验名称：ACL网络访问控制 | |
| 实验台号： | 实验时间：2024/1/2 |
| 实验小组： | |
| 实验目的：  •理解基本和扩展访问控制列表应用场景；  •掌握标准访问控制列表的配置方法；  •掌握扩展访问控制列表的配置方法；  •掌握基于名称的访问列表的配置方法。 | |
| 实验环境说明：  PacketTracer6 | |
| 实验过程、步骤（可另附页、使用网络拓扑图等辅助说明）及结果：  实验拓扑图    设备编址  C53659661CB13CA0698CECB9A0C19611  检查server0和router0之间的连通性    检查router0和router1之间的连通性    配置r0和r1的ospf协议      测试server0与server3之间的连通性    基本acl配置  router1配置acl允许172.16.2.0/24网段禁止172.16.1.0/24网段访问172.16.3.0/24子网    检查router1acl配置    检查配置效果    基于主机的acl配置在router1配置acl允许访问172.16.2.0子网但是server0除外并禁止172.16.1.0/24子网访问172.16.3.0/24子网          拓展acl配置  扩展acl配置禁止server0访问server3      基于名称访问控制列表的使用方法    删除acl规则deny 172.16.1.0 0.0.0.255 | |
| 实验总结（遇到的问题及解决办法、体会）：   1. 主机之间ping不通，忘记配置默认网关导致主机之间连接失败：为每一台终端设备配置默认网关 2. ACL允许管理员根据特定的规则对网络流量进行过滤，从而控制哪些流量可以访问网络设备或通过设备传输。通过定义规则，可以限制或允许特定的IP地址、端口号等数据包特征的流量通过。在PacketTracer6平台上，我进行了一次ACL配置的仿真实验。我模拟了一个简单的网络环境，包括路由器、交换机和几台终端设备。然后，我按照实验指导，在路由器上配置了ACL规则，以控制不同终端设备之间的网络访问。在配置ACL的过程中，我实际操作了添加规则、应用规则到接口等步骤。通过这些操作，我深入了解了ACL的配置方法。同时，我也在实际应用中遇到了一些问题，例如如何精确匹配特定的流量、如何处理冲突的规则等。通过解决这些问题，我对ACL的应用有了更深入的理解。这次仿真实验让我对路由器ACL控制有了更直观的认识。通过实际操作，我不仅掌握了ACL的基本配置方法，还理解了其在网络安全中的重要作用。ACL不仅可以帮助我们限制不必要的网络访问，提高网络安全性，还可以用于流量分类和流量整形等应用场景。 | |
| 器材、工具领用及归还负责人： | 实验记录人：（签名） |
| 实验执笔人：（签名） | 报告协助人：（签名） |
| 小组成员签名：（签名） | |
| 验收人： | 成绩评定： |