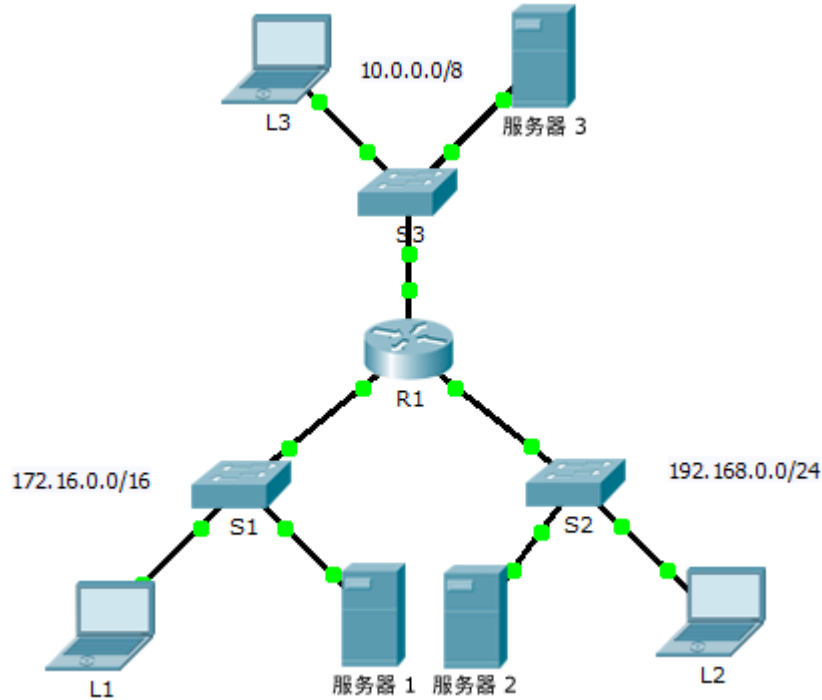


Packet Tracer - 标准 IPv4 ACL 故障排除

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
R1	G0/0	10.0.0.1	255.0.0.0	不适用
	G0/1	172.16.0.1	255.255.0.0	不适用
	G0/2	192.168.0.1	255.255.255.0	不适用
服务器 1	NIC	172.16.255.254	255.255.0.0	172.16.0.1
服务器 2	NIC	192.168.0.254	255.255.255.0	192.168.0.1
服务器 3	NIC	10.255.255.254	255.0.0.0	10.0.0.1
L1	NIC	172.16.0.2	255.255.0.0	172.16.0.1
L2	NIC	192.168.0.2	255.255.255.0	192.168.0.1
L3	NIC	10.0.0.2	255.0.0.0	10.0.0.1

目标

第 1 部分：ACL 问题 1 故障排除

第 2 部分：ACL 问题 2 故障排除

第 3 部分：ACL 问题 3 故障排除

场景

此网络打算实施以下三个策略：

- 来自 192.168.0.0/24 网络的主机不能访问网络 10.0.0.0/8。
- L3 不能访问网络 192.168.0.0/24 中的任何设备。
- L3 不能访问**服务器 1** 或 **服务器 2**。L3 只能访问**服务器 3**。
- 来自 172.16.0.0/16 网络的主机具有**服务器 1**、**服务器 2** 和 **服务器 3** 的完全访问权限。

注：所有 FTP 用户名和密码均为 “cisco”。

此外，则无其他限制。遗憾的是，实施的规则未起到应有的作用。您的任务是查找并修复与 **R1** 上的访问列表相关的错误。

第 1 部分：ACL 问题 1 故障排除

来自 192.168.0.0/24 网络的主机应该不能访问 10.0.0.0/8 网络上的任何设备。当前情况不是这样。

步骤 1：确定 ACL 问题。

在执行以下任务时，将结果与您期望 ACL 实现的效果作比较。

- a. 使用 **L2** 时，尝试访问**服务器 1**、**服务器 2** 和 **服务器 3** 的 FTP 和 HTTP 服务。
- b. 使用 **L2** 时，ping **服务器 1**、**服务器 2** 和 **服务器 3**。
- c. 查看 **R1** 上的运行配置。检查访问列表 **FROM_192** 以及它在接口上的放置。访问列表是否放置在正确的接口上并且方向正确？列表中是否有任何语句允许或拒绝流量传输到其他网络？语句顺序是否正确？
- d. 根据需要执行其他测试。

步骤 2：实施解决方案。

对 **FROM_192** 或它的放置进行必要调整，以修复问题。

步骤 3：验证问题是否已解决，并记录解决方案。

如果问题已解决，请记录解决方案，否则返回到步骤 1。

第 2 部分：ACL 问题 2 故障排除

L3 应该不能访问**服务器 1** 或 **服务器 2**。当前情况不是这样。

步骤 1：确定 ACL 问题。

在执行以下任务时，将结果与您期望 ACL 实现的效果作比较。

- a 使用 **L3** 时，尝试访问**服务器 1**、**服务器 2** 和 **服务器 3** 的 FTP 和 HTTP 服务。
- b 使用 **L3** 时，ping **服务器 1**、**服务器 2** 和 **服务器 3**。

- c 查看 R1 上的运行配置。检查访问列表 **FROM_10** 以及它在接口上的放置。访问列表是否放置在正确的接口上并且方向正确？列表中是否有任何语句允许或拒绝流量传输到其他网络？语句顺序是否正确？
- d 根据需要运行其他测试。

步骤 2： 实施解决方案。

对访问列表 **FROM_10** 或它的放置进行必要调整，以修复问题。

步骤 3： 验证问题是否已解决，并记录解决方案。

如果问题已解决，请记录解决方案，否则返回到步骤 1。

第 3 部分： ACL 问题 3 故障排除

来自 172.16.0.0/16 网络的主机应该具有**服务器 1**、**服务器 2** 和**服务器 3** 的完全访问权限，但是当前情况不是这样，因为 **L1** 无法与**服务器 2** 或**服务器 3** 通信。

步骤 1： 确定 ACL 问题。

在执行以下任务时，将结果与您对 ACL 的预期作比较。

- a 使用 **L1** 时，尝试访问**服务器 1**、**服务器 2** 和**服务器 3** 的 FTP 和 HTTP 服务。
- b 使用 **L1** 时，ping **服务器 1**、**服务器 2** 和**服务器 3**。
- c 查看 **R1** 上的运行配置。检查访问列表 **FROM_172** 以及它在接口上的放置。访问列表是否放置在正确的端口上并且方向正确？列表中是否有任何语句允许或拒绝流量传输到其他网络？语句顺序是否正确？
- d 根据需要运行其他测试。

步骤 2： 实施解决方案。

对访问列表 **FROM_172** 或它的放置进行调整，以修复问题。

步骤 3： 验证问题是否已解决，并记录解决方案。

如果问题已解决，请记录解决方案，否则返回到步骤 1。

第 4 部分： 思考（可选）

访问列表带来的逻辑问题通常有多种解决方案。您是否能想出不同的一组规则或放置来产生所需要的相同访问过滤结果？

推荐评分规则

存在问题的地方	可能的得分点	实际得分
演示分数	10	
Packet Tracer 评分	90	
总得分	100	