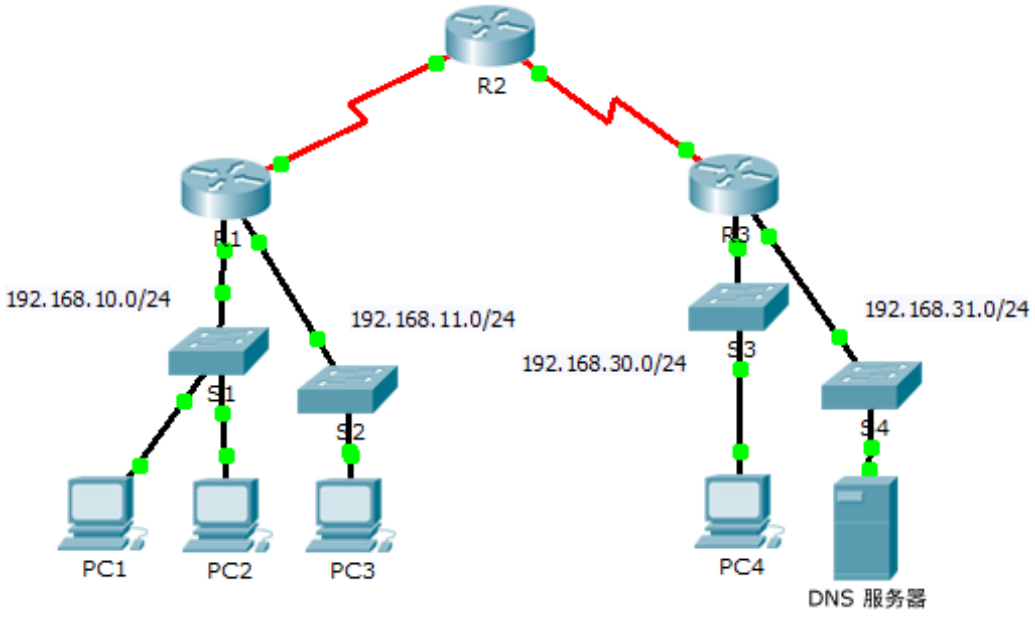
# Packet Tracer – 访问控制列表演示

## 拓扑




## 目标

**第 1 部分：验证本地连接和测试访问控制列表**

**第 2 部分：删除访问控制列表和重复测试**

## 背景信息

在本练习中，您将观察如何使用访问控制列表 (ACL) 阻止 ping 访问远程网络上的主机。从配置中删除 ACL 之后，ping 将成功。

# 第 1 部分：验证本地连接和测试访问控制列表

### 步骤 1： Ping 本地网络上的设备，以验证连接。

a. 从 **PC1** 的命令提示符中，ping **PC2**。

b. 从 **PC1** 的命令提示符中，ping **PC3**。

Ping 操作为什么成功？

_____

### 步骤 2： 在远程网络上 ping 设备以测试 ACL 功能。

a 从 **PC1** 的命令提示符中，ping **PC4**。

b 从 **PC1** 的命令提示符处，ping **DNS 服务器**。

Ping 操作为什么失败？（提示：使用模拟模式或查看路由器配置进行研究。）

_____

## 第 2 部分：删除 ACL 和重复测试

### 步骤 1： 使用 show 命令研究 ACL 配置。

a 使用 **show run** 和 **show access-lists** 命令查看当前配置的 ACL。要快速查看当前 ACL，请使用 **show access-lists**。输入 **show access-lists** 命令，后跟一个空格和一个问号 (?) 可查看可用的选项：

```
R1#show access-lists ?
  <1-199>  ACL number
  WORD     ACL name
  <cr>
```

如果您知道 ACL 编号或名称，您可以进一步筛选 **show** 输出。但是，**R1** 只有一个 ACL，因此，**show access-lists** 命令就足够了。

```
R1#show access-lists
Standard IP access list 11
    10 deny 192.168.10.0 0.0.0.255
    20 permit any
```

ACL 的第一行将阻止在 **192.168.10.0/24** 网络中发出的任何数据包，这包括互联网控制消息协议 (ICMP) 回应（ping 请求）。ACL 的第二行将允许来自**任何**来源的所有其他 **ip** 流量经过路由器。

b 为了使 ACL 能够影响路由器运行，它必须以指定方向应用到接口。在此场景中，ACL 用于过滤从接口中出来的流量。因此，离开 R1 的指定接口的所有流量都将根据 ACL 11 进行检查。

尽管您可以使用 **show ip interface** 命令查看 IP 信息，但是在某些情况简单地使用 **show run** 命令可能更高效。

使用其中一个或两个命令时，ACL 应用于哪个接口和方向？

_____

### 步骤 2： 从配置中删除访问列表 11

通过发出 **no access list** [*ACL 的编号*] 命令，您可以从配置中删除 ACL。**no access-list** 命令用于删除在路由器上配置的所有 ACL。**no access-list** [*ACL 的编号*] 命令仅用于删除特定 ACL。

a 在串行 I0/0/0 接口下，删除以前作为**出站**过滤器应用到接口的访问列表 11：

```
R1(config)# int se0/0/0
R1(config-if)#no ip access-group 11 out
```

b 在全局配置模式下，通过输入以下命令删除 ACL：

```
R1(config)# no access-list 11
```

c 验证 **PC1** 现在可以 ping 到 **DNS 服务器**和 **PC4**。

## 推荐评分规则

| 存在问题的地方 | 可能的得分点 | 实际得分 |
|---|---|---|
| 第 1 部分，步骤 1 b。 | 50 | |
| 第 1 部分，步骤 2 b。 | 40 | |
| 第 2 部分，步骤 2 b。 | 10 | |
| **总得分** | **100** | |