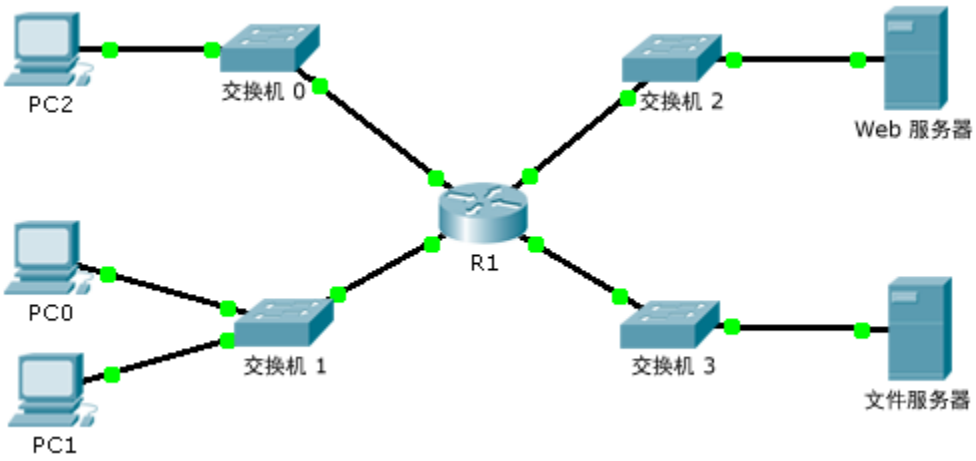
Packet Tracer - 配置命名的 IPv4 标准 ACL

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
R1	F0/0	192.168.10.1	255.255.255.0	不适用
	F0/1	192.168.20.1	255.255.255.0	不适用
	E0/0/0	192.168.100.1	255.255.255.0	不适用
	E0/1/0	192.168.200.1	255.255.255.0	不适用
文件服务器	NIC	192.168.200.100	255.255.255.0	192.168.200.1
Web 服务器	NIC	192.168.100.100	255.255.255.0	192.168.100.1
PC0	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC1	NIC	192.168.20.4	255.255.255.0	192.168.20.1
PC2	NIC	192.168.10.3	255.255.255.0	192.168.10.1

目标

第 1 部分：配置和应用命名的标准 ACL

第 2 部分：验证 ACL 实施

背景/场景

高级网络管理员指派您创建标准命名 ACL，用于阻止对文件服务器的访问。应该拒绝来自一个网络的所有客户端和来自另一个网络的一台特定工作站访问该服务器。

第 1 部分：配置和应用命名的标准 ACL

步骤 1： 在配置和应用 ACL之前，验证连接。

所有三个工作站都应该能够 ping 到 **Web 服务器**和**文件服务器**。

步骤 2： 配置命名的标准 ACL。

在 **R1** 上配置以下命名的 ACL。

```
R1(config)# ip access-list standard File_Server_Restrictions
R1(config-std-nacl)# permit host 192.168.20.4
R1(config-std-nacl)# deny any
```

注：在评分时，ACL 名称区分大小写。

步骤 3： 应用命名的 ACL。

a. 在快速以太网 0/1 接口上应用出站 ACL。

```
R1(config-if)# ip access-group File_Server_Restrictions out
```

b. 保存配置。

第 2 部分：验证 ACL 实施

步骤 1： 验证 ACL 配置以及在接口上的应用。

使用 **show access-lists** 命令验证 ACL 配置。使用 **show run** 或 **show ip interface fastethernet 0/1** 命令验证 ACL 是否已正确应用于接口。

步骤 2： 验证 ACL 是否正确工作。

所有三个工作站应通过 ping 到 **Web 服务器**，但是只有 **PC1** 应该能够 ping 到**文件服务器**。