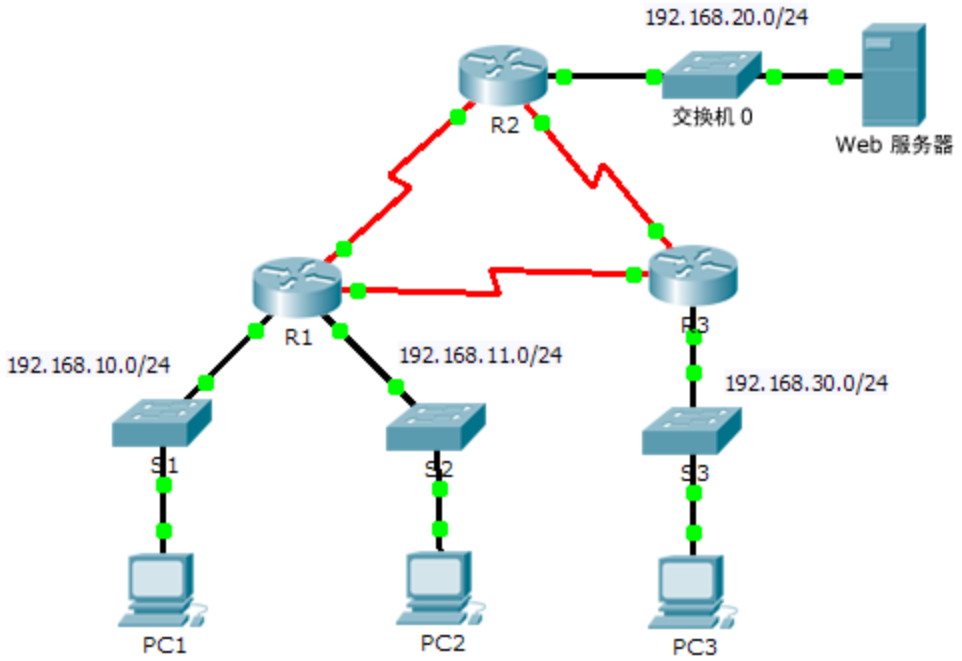
Packet Tracer - 配置编号标准 IPv4 ACL

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	192.168.10.1	255.255.255.0	不适用
	G0/1	192.168.11.1	255.255.255.0	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
	S0/0/1	10.3.3.1	255.255.255.252	不适用
R2	G0/0	192.168.20.1	255.255.255.0	不适用
	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
R3	G0/0	192.168.30.1	255.255.255.0	不适用
	S0/0/0	10.3.3.2	255.255.255.252	不适用
	S0/0/1	10.2.2.2	255.255.255.252	不适用
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
Web 服务器	NIC	192.168.20.254	255.255.255.0	192.168.20.1

目标

第 1 部分：计划 ACL 实施

第 2 部分：配置、应用和验证标准 ACL

背景/场景

标准访问控制列表 (ACL) 为路由器配置脚本，基于源地址控制路由器是允许还是拒绝数据包。本练习的主要内容是定义过滤标准、配置标准 ACL、将 ACL 应用于路由器接口并验证和测试 ACL 实施。路由器已配置，包括 IP 地址以及增强型内部网关路由协议 (EIGRP) 路由。

第 1 部分：计划 ACL 实施

步骤 1: 研究当前网络配置。

将任何 ACL 应用于网络中之前，都必须确认网络完全连通。通过选择一个 PC，然后 ping 网络上的其他设备，验证网络具有全面连接。您应该能够成功 ping 每个设备。

步骤 2: 评估两个网络策略，计划 ACL 实施。

a. 在 **R2** 上实施了以下网络策略：

- 192.168.11.0/24 网络不允许访问 192.168.20.0/24 网络上的 **Web 服务器**。
- 允许所有其他访问。

要限制从 192.168.11.0/24 网络访问 192.168.20.254 网络上的 **Web 服务器**，而不干扰其他流量，则必须在 **R2** 上创建 ACL。该访问列表必须放置在连接 **Web 服务器**的出站接口上。必须在 **R2** 上创建另一个规则以允许所有其他流量。

b. 在 **R3** 上实施了以下网络策略：

- 不允许 192.168.10.0/24 网络与 192.168.30.0/24 网络通信。
- 允许所有其他访问。

要限制从 192.168.10.0/24 网络访问 192.168.30/24 网络，而不干扰其他流量，则需要在 **R3** 上创建访问列表。该访问列表必须放置在连接 **PC3** 的出站接口上。必须在 **R3** 上创建另一个规则以允许所有其他流量。

第 2 部分：配置、应用和验证标准 ACL

步骤 1： 在 R2 上配置和应用编号的标准 ACL。

a 在 **R2** 上使用编号 1 创建一个 ACL，通过一个语句拒绝从 192.168.11.0/24 网络访问 192.168.20.0/24 网络。

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b 默认情况下，访问列表将拒绝与任何规则都不匹配的所有流量。要允许所有其他流量，请配置以下语句：

```
R2(config)# access-list 1 permit any
```

c 为了使该 ACL 实际过滤流量，必须将它应用于某些路由器操作。通过在千兆以太网 0/0 接口上放置 ACL 来过滤出站流量，应用 ACL。

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

步骤 2： 在 R3 上配置和应用编号的标准 ACL。

a 在 **R3** 上使用编号 1 创建一个 ACL，通过一个语句拒绝从**PC1** (192.168.10.0/24) 网络访问 192.168.30.0/24 网络。

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b 默认情况下，ACL 将拒绝与任何规则都不匹配的所有流量。要允许所有其他流量，请为 ACL 1 创建另一个规则。

```
R3(config)# access-list 1 permit any
```

c 通过在千兆以太网 0/0 接口上放置 ACL 来过滤出站流量，应用 ACL。

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

步骤 3： 验证 ACL 配置和功能。

a 在 **R2** 和 **R3** 上，输入 **show access-list** 命令以验证 ACL 配置。输入 **show run** 或 **show ip interface gigabitethernet 0/0** 命令以验证 ACL 放置。

b 通过使用两个 ACL，将根据第 1 部分详述的策略限制网络流量。使用以下测试验证 ACL 实施：

- 从 192.168.10.10 到 192.168.11.10 的 ping 成功。
- 从 192.168.10.10 到 192.168.20.254 的 ping 成功。
- 从 192.168.11.10 到 192.168.20.254 的 ping 失败。
- 从 192.168.10.10 到 192.168.30.10 的 ping 失败。
- 从 192.168.11.10 到 192.168.30.10 的 ping 成功。
- 从 192.168.30.10 到 192.168.20.254 的 ping 成功。