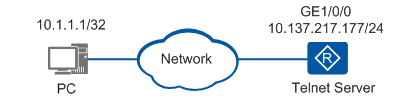
**一、使用基本ACL限制Telnet登录权限**

**1.拓扑图：**



**2.组网需求：**

如图所示，PC与设备之间路由可达，用户希望简单方便的配置和管理远程设备，可以在服务器端配置Telnet用户使用AAA验证登录，并配置安全策略，保证只有符合安全策略的用户才能登录设备。

**3.配置思路：**

采用如下的思路配置通过Telnet登录设备：

1.配置Telnet方式登录设备，以实现远程维护网络设备。

2.配置管理员的用户名和密码，并配置AAA认证策略，保证只有认证通过的用户才能登录设备。

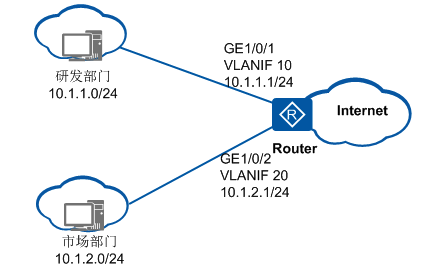
3.配置安全策略，保证只有符合安全策略的用户才能登录设备

**4.操作步骤：**

**5.验证配置结果：**

**二·、使用高级ACL限制不同网段的用户互访**

**1.拓扑图：**



**2. 组网需求：**

如图所示，某公司通过Router实现各部门之间的互连。为方便管理网络，管理员为公司的研发部和市场部规划了两个网段的IP地址。同时为了隔离广播域，又将两个部门划分在不同VLAN之中。现要求Router能够限制两个网段之间互访，防止公司机密泄露。

**3. 配置思路：**

采用如下的思路在Router上进行配置：

1.配置高级ACL和基于ACL的流分类，使设备可以对研发部与市场部互访的报文进行过滤。

2.配置流行为，拒绝匹配上ACL规则的报文通过。

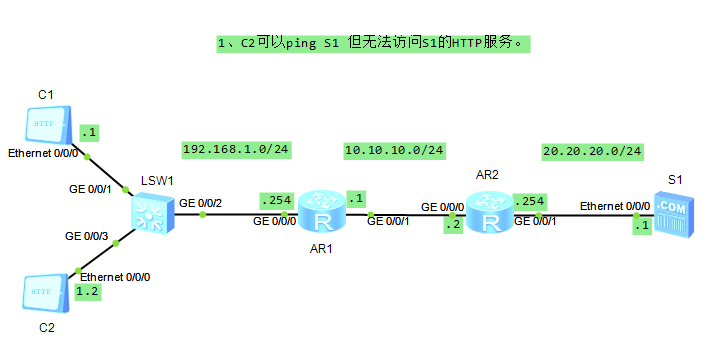
3.配置并应用流策略，使ACL和流行为生效。

**4.操作步骤：**

**5.验证配置结果：**

**三、 高级ACL配置**

1、拓扑



2、需求说明：

C2可以ping S1 但无法访问S1的HTTP服务。

这个需求该如何实现，这里就要用到高级的ACL了。

ACL特点3：基本的ACL只能针对报文中的源IP地址进行过滤