

Packet Tracer - 在 VTY 线路上配置 IPv4 ACL

拓扑



地址分配表

设备	接口	IP 地址	子网掩码	默认网关
路由器	F0/0	10.0.0.254	255.0.0.0	不适用
PC	NIC	10.0.0.1	255.0.0.0	10.0.0.254
笔记本电脑	NIC	10.0.0.2	255.0.0.0	10.0.0.254

目标

第 1 部分：配置 ACL 并应用到 VTY 线路

第 2 部分：验证 ACL 实施

背景信息

作为网络管理员，您必须具有路由器的远程访问权限。此访问权限不能提供给网络的其他用户。因此，您将配置和应用一个访问控制列表 (ACL)，允许 PC 访问 Telnet 线路，但是拒绝所有其他源 IP 地址。

第 1 部分：配置 ACL 并应用到 VTY 线路

步骤 1：在配置 ACL 之前验证 Telnet 接入。

两台计算机应该能使用 Telnet 远程登录到路由器。密码是 **cisco**。

步骤 2： 配置编号的标准 ACL

在路由器上配置以下编号 ACL。

```
Router(config)# access-list 99 permit host 10.0.0.1
```

由于我们不想允许任何其他计算机访问，访问列表的隐式拒绝属性可满足我们的要求。

步骤 3： 在路由器上放置命名的标准 ACL。

必须允许访问路由器接口，而限制 Telnet 接入。因此，必须将该 ACL 放置在 Telnet 线路 0 到 4 上。从路由器的配置提示符处，输入线路 0 - 4 的线路配置模式，使用 **access-class** 命令将 ACL 应用到所有 VTY 线路：

```
Router(config)# line vty 0 15
Router(config-line)# access-class 99 in
```

第 2 部分：验证 ACL 实施

步骤 1： 验证 ACL 配置以及在 VTY 线路上的应用。

使用 **show access-lists** 验证 ACL 配置。使用 **show run** 命令验证 ACL 是否已应用到 VTY 线路。

步骤 2： 验证 ACL 是否正确工作。

两台计算机都能够 ping 到路由器，但是只有 PC 能够使用 Telnet 远程登录。