

ERG3 系列路由器限制内网访问外网

目录

1 配置需求或说明	2
1.1 适用产品系列	2
1.2 配置需求及实现的效果	2
2 组网图	2
3 配置步骤	2
3.1 登录设备	2
3.2 配置外网以及内网地址池	3
3.3 限制内网上网	4
3.4 结果验证	5
3.5 保存配置	6

1 配置需求或说明

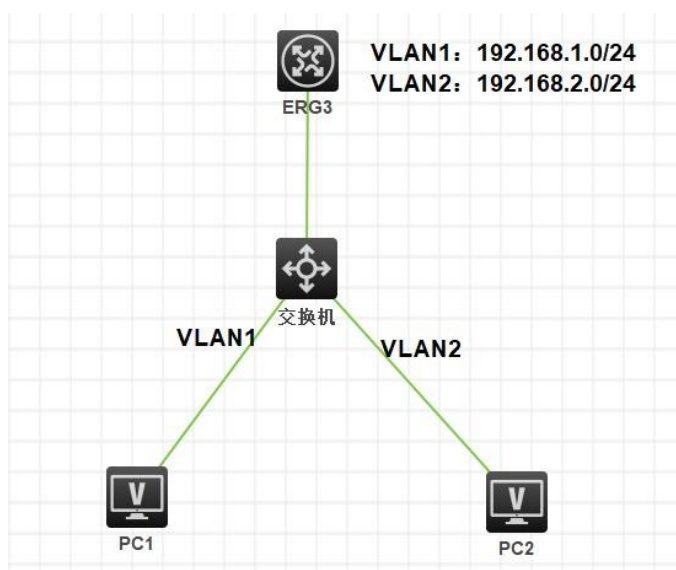
1.1 适用产品系列

本案例适用于 ERG3 系列路由器，如 ER3200G3、ER8300G3、ER5200G3 等。

1.2 配置需求及实现的效果

路由器作为企业网络的出口路由器，要实现 WAN 口自动获取上网，路由器上创建了两个内网网段，分别为 192.168.1.0/24, 192.168.2.0/24，1 网段的用户可以上网，2 网段的用户不能上网。**注意：**WAN 口自动获取的网段不能和内网网段 192.168.1.1/24 冲突，否则会导致内网无法上外网。

2 组网图



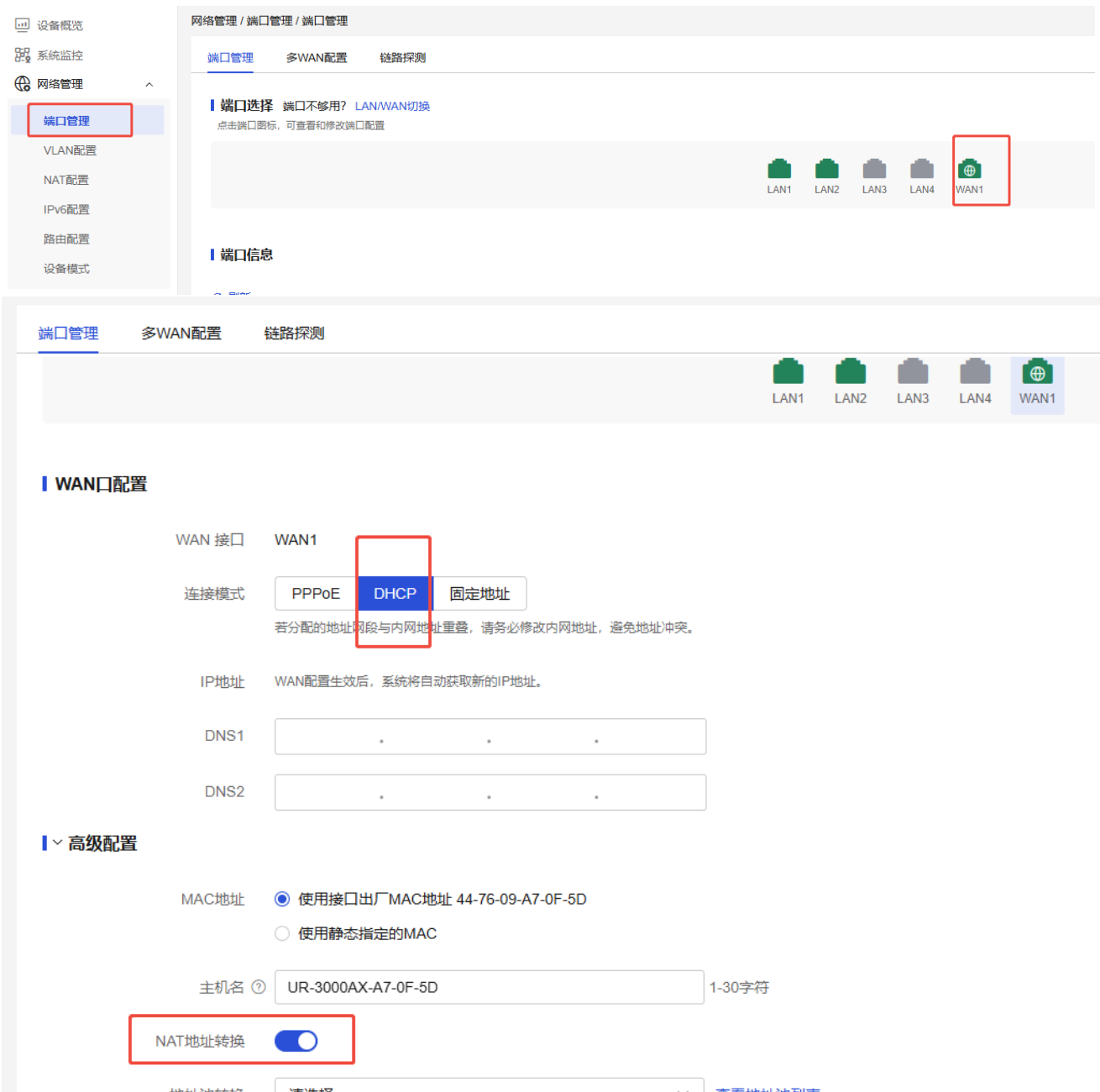
3 配置步骤

3.1 登录设备

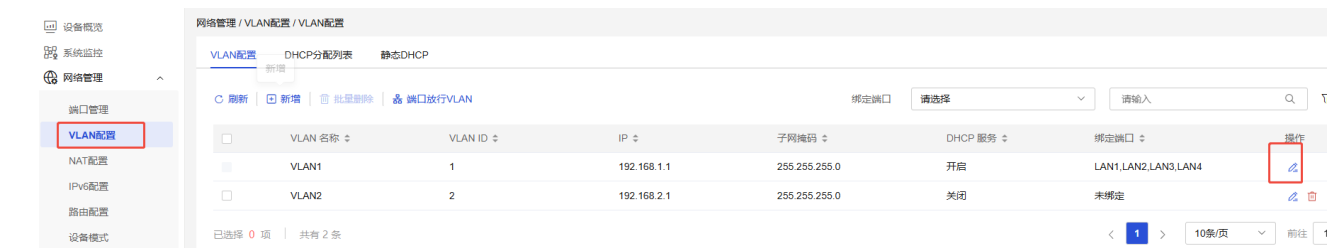
#登陆 WEB 管理页面（默认情况下，登陆地址为 192.168.1.1/24（新版本地址为 192.168.77.1），登陆用户名为 admin，登陆密码为 admin）。

3.2 配置外网以及内网地址池

#点击网络管理—接口管理—点击 wan1 进行配置，连接模式选择“DHCP”，NAT 地址转换保持默认的“开启”状态。点击“应用”按钮。



#点击网络管理-vlan 配置-vlan1 后面的编辑选项进行修改 vlan 口相关参数，修改完成后点击确认按钮, 点击新增按钮创建 vlan2。

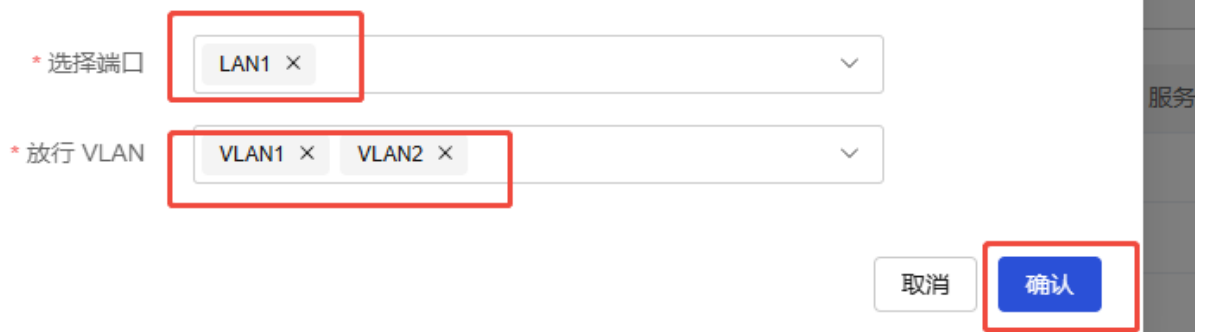




#路由器 lan1 口连接交换机，将 lan1 口放通对应 vlan 1 和 vlan2，点击网络管理—vlan 配置—端口放行vlan，放通两个 vlan



放行 VLAN



#交换机上的操作

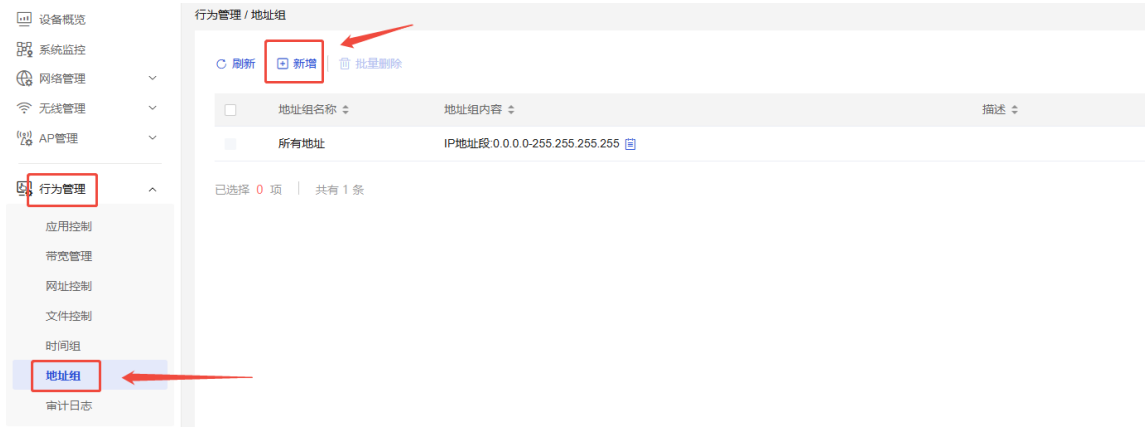
```
#
interface GigabitEthernet1/0/4 //进入接口 g1/0/4 视图
port link-type trunk //将接口配置成 trunk port trunk
permit vlan all //允许所有 vlan 通过
#
interface GigabitEthernet1/0/3 //进入接口 g1/0/3 视图
port access vlan 2 //将接口划分到 vlan2
#
```

3.3 限制内网上网

#点击网络安全—防火墙—通过防火墙实现 vlan1 用户可以上网，vlan2 用户不可上网



#点击行为管理—地址组—新增—创建 vlan2 网段对应的地址组



#地址组名称自定义—地址组类型选择 IP—地址范围写 vlan2 的网段所在范围地址，填写完成后点击确认

新增

* 地址组名称 ?

描述 ?

0 / 127

* 地址组类型
☒ IP
☐ MAC

IP地址 ?

+ -

IP地址段 ?

192 . 168 . 2 . 1 ~ 192 . 168 . 2 . 254

+ -

排除地址 ?

+ -

取消

确认

3.4 结果验证

vlan1 的用户上网正常，vlan2 下的该 MAC 地址用户无法上网，vlan2 下其他用户上网正常

```
C:\Users\sys1392>ping -S 192.168.1.2 114.114.114.114

正在 Ping 114.114.114.114 从 192.168.1.2 具有 32 字节的数据:
来自 114.114.114.114 的回复: 字节=32 时间=73ms TTL=85
来自 114.114.114.114 的回复: 字节=32 时间=91ms TTL=79

114.114.114.114 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 73ms, 最长 = 91ms, 平均 = 82ms
```

```
C:\Users\Dell>ping -S 192.168.2.2 114.114.114.114

正在 Ping 114.114.114.114 从 192.168.2.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
```

3.5 保存配置

自动保存配置