

403 Forbidden

本电子书由CyberArticle制作。点击[这里](#)下载CyberArticle。注册版本不会显示该信息。[删除广告](#)

V7交换机禁止VLAN互访方法（WEB版）

目录

[V7交换机划分VLAN方法（WEB版） 1](#)

[1 配置需求或说明 1](#)

[1.1 适用产品系列 1](#)

[1.2 配置需求 1](#)

[2 组网图 2](#)

[3 配置步骤 2](#)

[3.1创建VLAN 2](#)

1 配置需求或说明

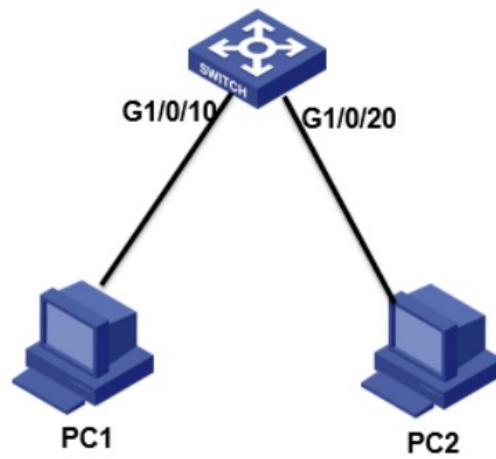
1.1 适用产品系列

本案例适用于如S5130-28F-WiNet、S5500V2-24P-WiNet、S5500V2-48P-WiNet等的V7交换机，V5、V7交换机具体分类及型号可以参考“1.1 Comware V5、V7平台交换机分类说明”。

1.2 配置需求

公司将交换机做为核心交换机，现在在核心交换机上划分2个VLAN网段，VLAN 10和VLAN 20。PC1属于VLAN 10，PC2属于VLAN20，要求VLAN 10和VLAN 20之间不能互相访问。

2 组网图




3 配置步骤

3.1创建VLAN和虚接口地址

1) 导航栏：网络---链路—VLAN

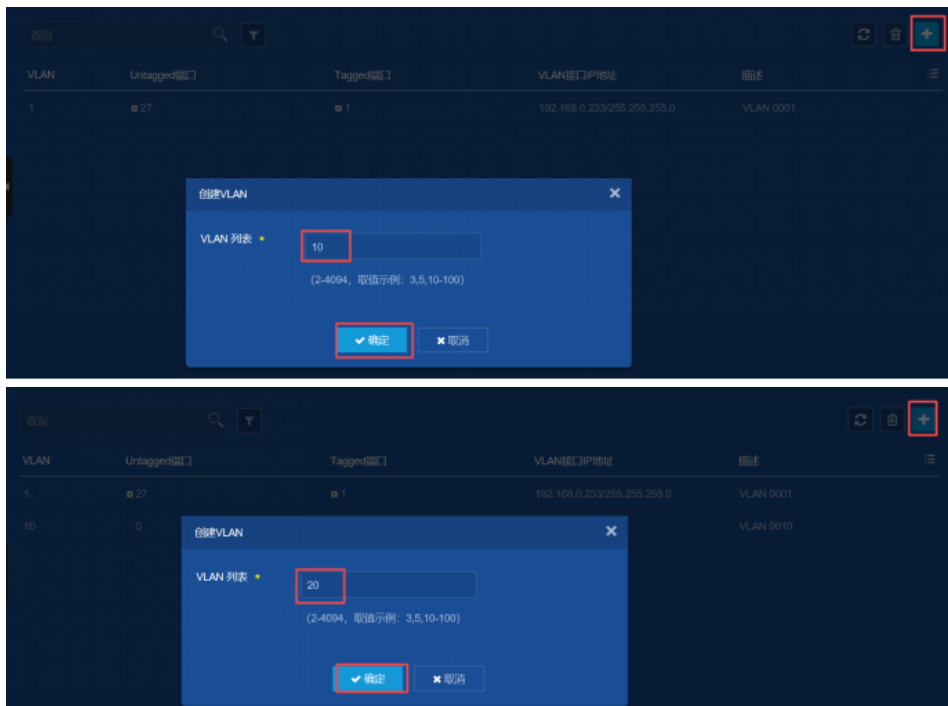


2) 点击“+”新增VLAN



VLAN	Untagged端口	Tagged端口	VLAN接口IP地址	描述
1	27	0	192.168.100.1/255.255.255.0	VLAN 0001
16	1	0	192.168.16.245/255.255.255.0	VLAN 0016
4092	0	0	—	VLAN 4092
4093	0	0	—	VLAN 4093

3) 输入要新增的VLAN 10和VLAN 20



创建VLAN

VLAN 列表: 10
(2-4094, 取值示例: 3,5,10-100)

确定 取消

创建VLAN

VLAN 列表: 20
(2-4094, 取值示例: 3,5,10-100)

确定 取消

4) 新增VLAN 10之后在VLAN 10显示界面点击“→”进行编辑

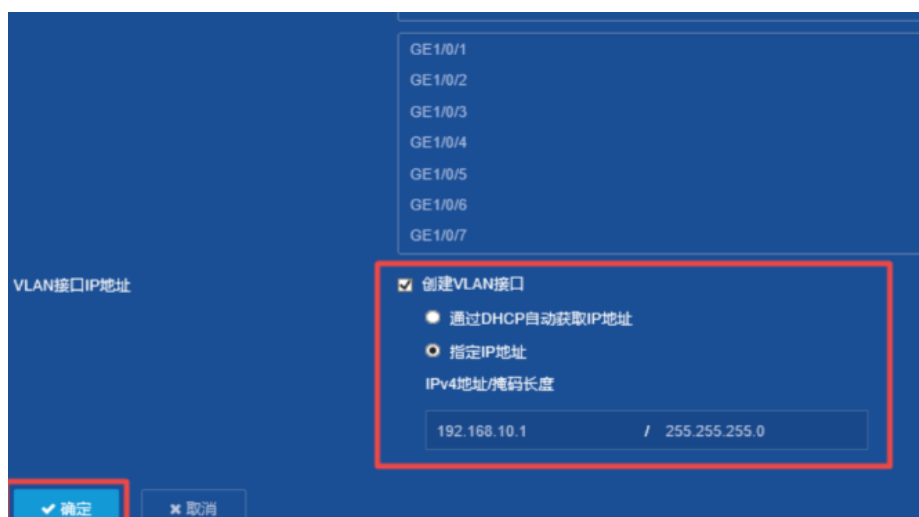


1	27	1	192.168.0.233/255.255.255.0	VLAN 0001
10	0	0	—	VLAN 0010
20	0	0	—	VLAN 0020

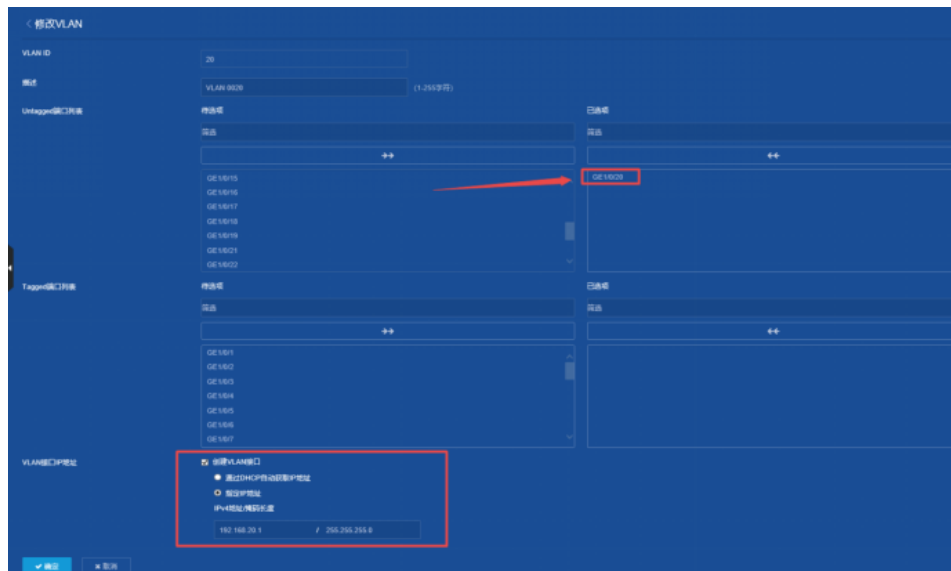
5) 在修改VLAN设置界面选中并点击GE1/0/10, 表示把此接口加入到VLAN 10里



6) 在“VLAN接口IP地址”选项这里选择“指定IP地址”，并配置好VLAN接口地址192.168.10.1，掩码为255.255.255.0

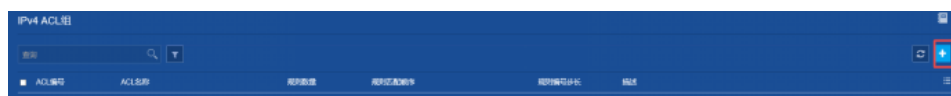


7) 在修改VLAN设置界面选中并点击GE1/0/20，表示把此接口加入到VLAN 20里在“VLAN接口IP地址”选项这里选择“指定IP地址”，并配置好VLAN接口地址192.168.20.1，掩码为255.255.255.0



3.2创建包过滤策略

1) 在资源---ACL---IPv4 进入IPv4点击“+”添加



3) 类型选择“高级ACL”，编号选择“3000”，点击“确定”进入下一步操作

The screenshot shows the 'Add IPv4 ACL' configuration window. The 'Type' (类型) is set to 'Advanced ACL' (高级ACL). The 'Number' (编号) is set to '3000'. The 'Start adding rules' (开始添加规则) checkbox is checked. The 'Confirm' (确定) button is highlighted.

4) 动作选择“拒绝”，IP协议类型选择“IP”或者“256”，源地址是“192.168.10.0”通配符是“0.0.0.255”，目的地址是“192.168.20.0”通配符是“0.0.0.255”，取消勾选“继续添加下一跳规则”，点击“确定”。

< 添加IPv4高级ACL的规则

ACL编号: 3000 (3000-3999)

规则编号: (0-65534) ☒ 自动编号

描述: (1-127字符)

动作: ☐ 允许 ☒ 拒绝

IP协议类型: 256 (0-256)

匹配条件:

- ☒ 匹配源IP地址/通配符掩码
192.168.10.0 / 0.0.0.255
- ☒ 匹配目的IP地址/通配符掩码
192.168.20.0 / 0.0.0.255
- ☐ 匹配TCP/UDP报文的源端口号
- ☐ 匹配TCP/UDP报文的端口号
- ☐ 匹配TCP报文的连接建立标识
- ☐ 匹配TCP报文标识
- ☐ 匹配ICMP报文的类型和消息码
- ☐ 匹配OSPF优先级
- ☐ 匹配IP优先级
- ☐ 匹配ToS优先级

规则生效时间段: 请选择... +

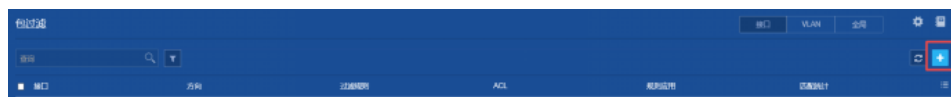
分片报文: ☐ 仅对分片报文的非首个分片有效

记录日志: ☐ 对符合条件的报文记录日志信息

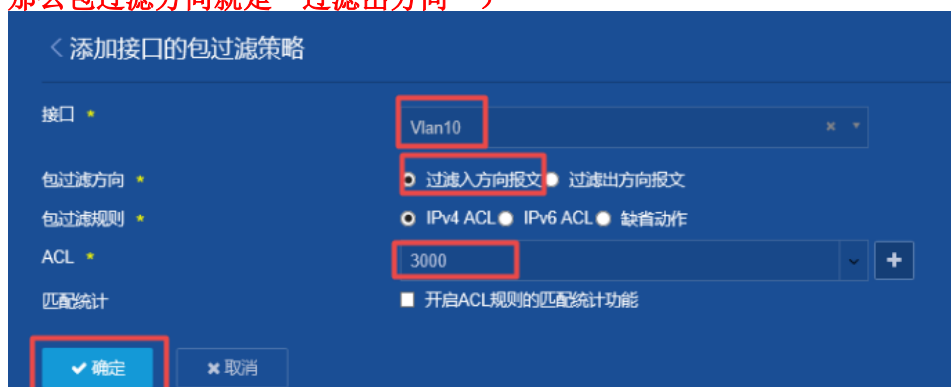
匹配统计: ☐ 开启本规则的匹配统计功能

☒ 继续添加下一条规则

5) 在 安全---包过滤---包过滤 进入后点击右上角的“+”



6) 接口选择“VLAN 10”，包过滤方向选择“过滤入方向”，ACL选择“3000”，点击“确定”即可（注意：如果这里接口选择的是“VLAN20”，那么包过滤方向就是“过滤出方向”）



8) “设备”--“配置文件”--“保存当前配置”--“保存到下次启动配置文件”，然后“确定”

或者点击左上角“admin”旁边的保存图标



3. 3验证配置

1) 电脑配置地址或者自动获取地址

接交换机10口的电脑地址为192.168.10.2

接交换机20口的电脑地址为192.168.20.2



2) 用PC1去ping PC2，发现无法ping通，实现禁止VLAN互访

```
C:\Users\>ping 192.168.20.2

正在 Ping 192.168.20.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.20.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```