

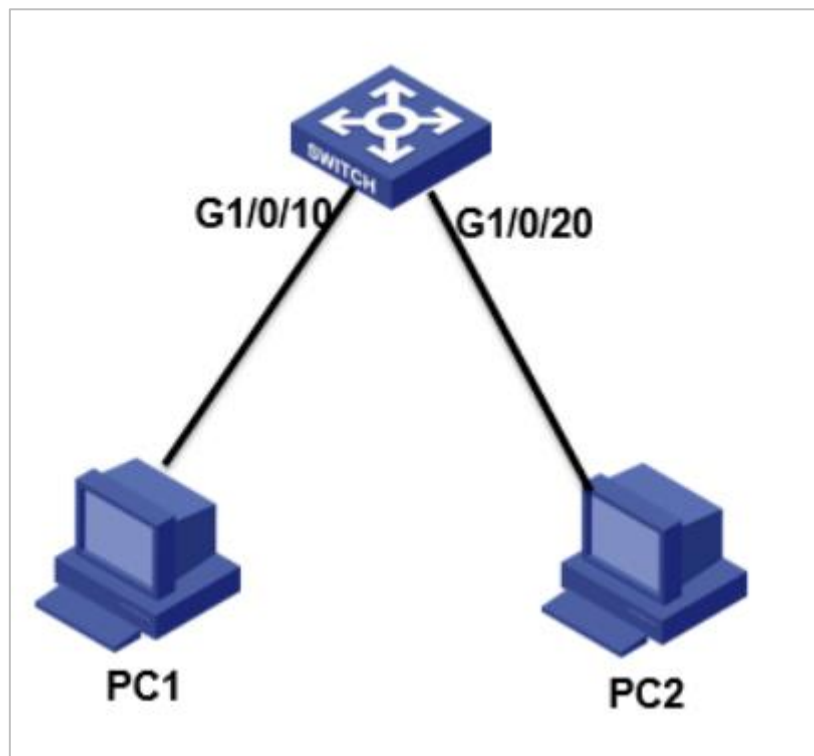
小贝交换机禁止 VLAN 互访配置案例（WEB）

一、配置需求

本案例小贝优选 US500S 以及 US500S 以上系列交换

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。

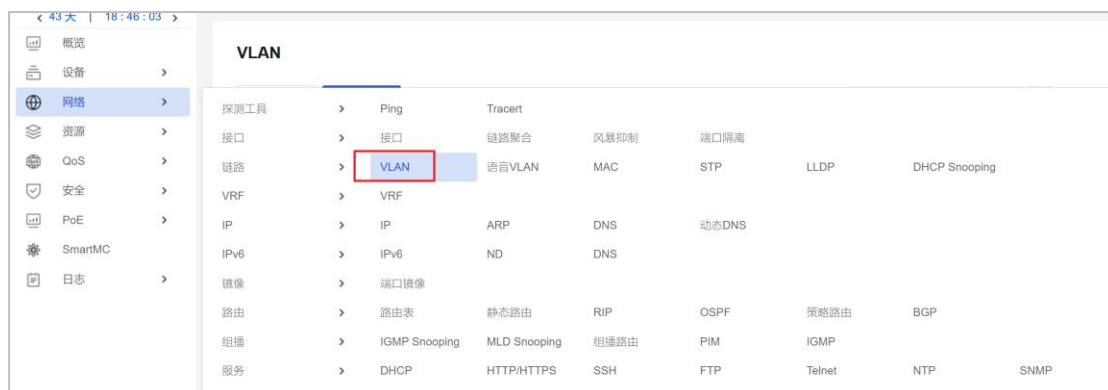
二、组网图



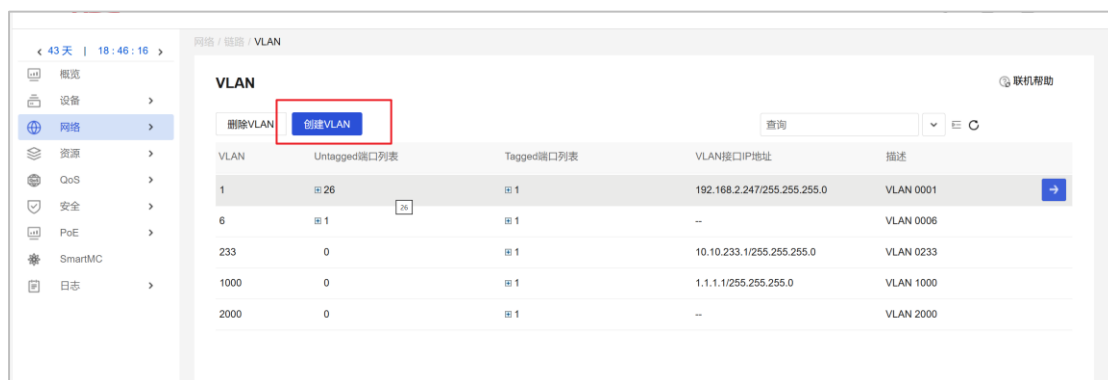
三、配置步骤

3.1 创建 VLAN 和虚接口地址

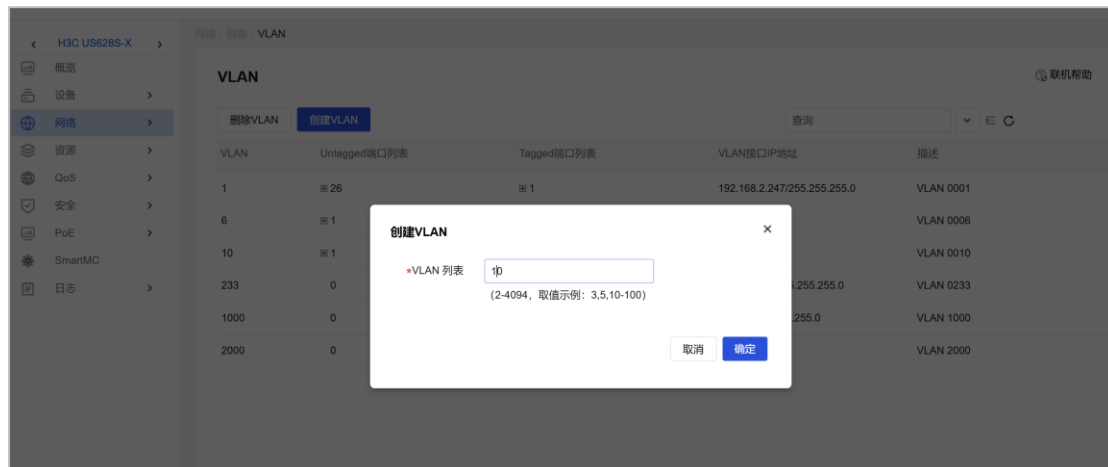
1) 导航栏：网络---链路—VLAN

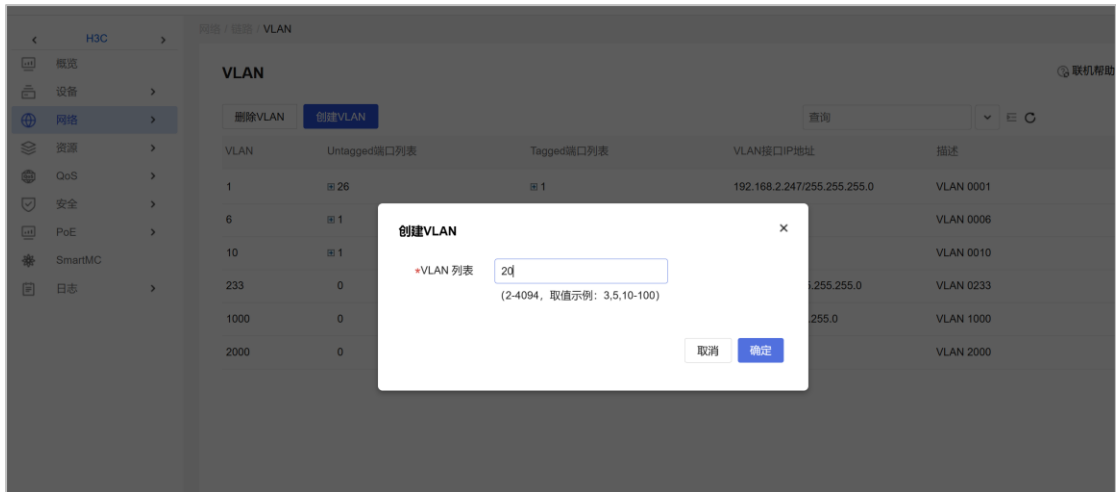


2) 点击 “+” 新增 VLAN

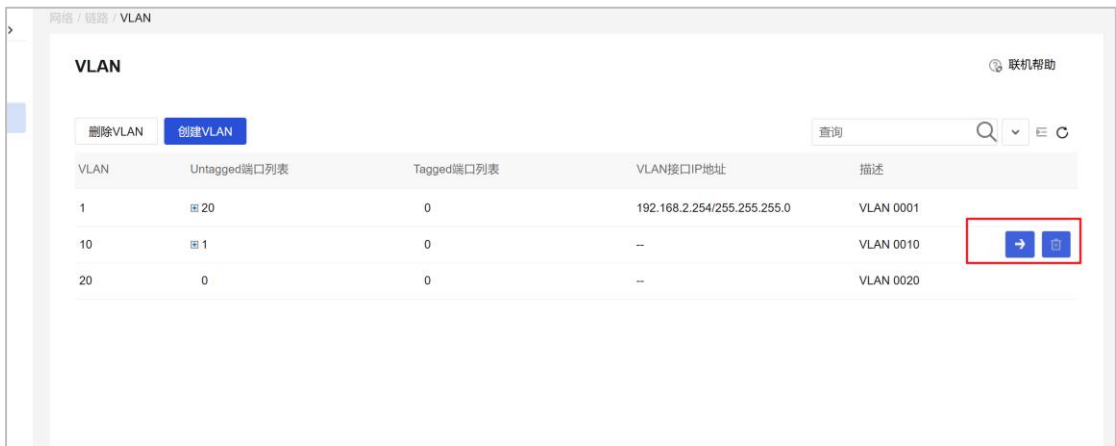


3) 输入要新增的 VLAN 10 和 VLAN 20

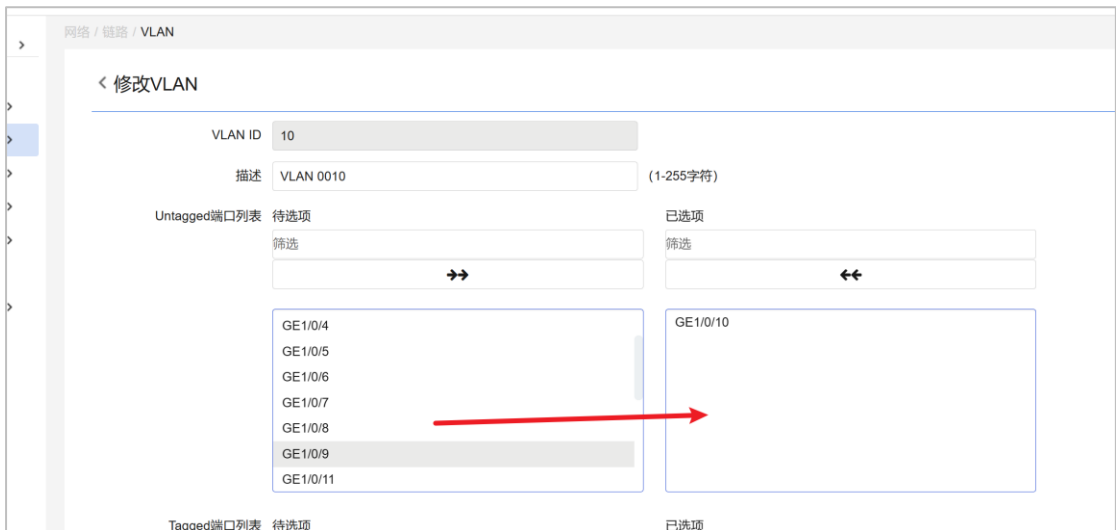




4) 新增 VLAN 10 之后在 VLAN 10 显示界面点击 “→” 进行编辑



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

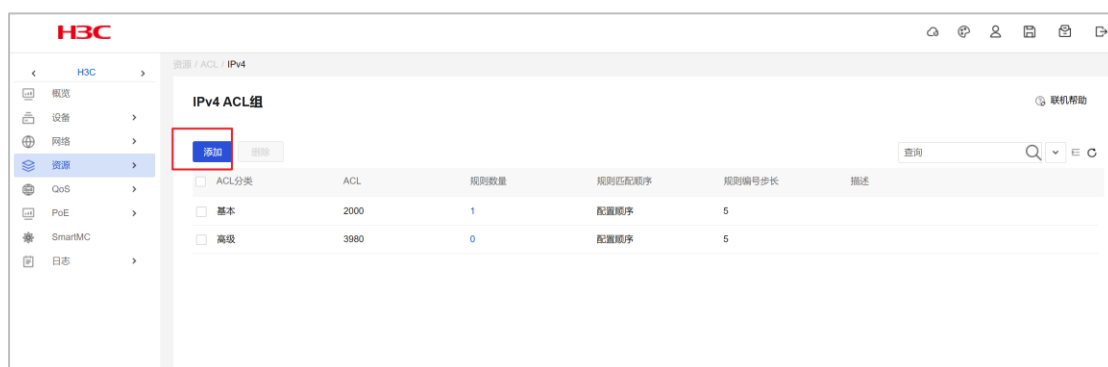
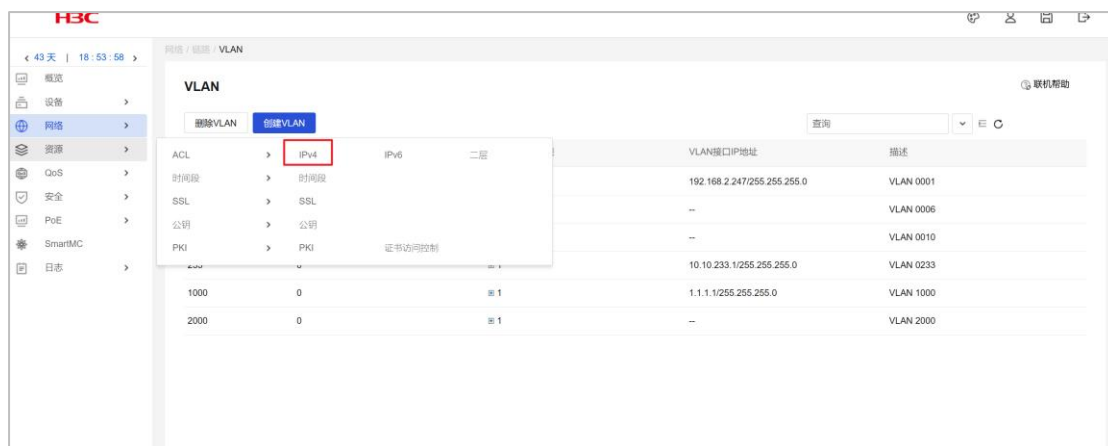
The screenshot shows a configuration window for a VLAN. At the top, there are two panels: 'Tagged端口列表' (Tagged Port List) and '已选项' (Selected Options). The 'Tagged端口列表' panel has a search bar and a list of ports: GE1/0/1, GE1/0/2, GE1/0/3, GE1/0/4, GE1/0/5, GE1/0/6, and GE1/0/7. The '已选项' panel is empty. Below these panels, there are radio buttons for 'VLAN接口IP地址' (VLAN Interface IP Address): '创建VLAN接口' (Create VLAN Interface) is selected, and '通过DHCP自动获取IP地址' (Obtain IP address automatically via DHCP) is unselected. Under '指定IP地址' (Specify IP address), the IPv4 address is set to 192.168.10.1 and the mask is 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

This screenshot shows the same configuration window as the previous one, but with additional changes. In the 'Tagged端口列表' panel, the port GE1/0/20 is now selected and highlighted with a red box. In the 'VLAN接口IP地址' section, the '指定IP地址' (Specify IP address) option is selected, and the IPv4 address is now 192.168.20.1 with a mask of 255.255.255.0. The '创建VLAN接口' (Create VLAN Interface) option remains selected. At the bottom, there are '确定' (Confirm) and '取消' (Cancel) buttons.

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



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: 3000 (3000-3999 或 1-63个字符)

*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: 255 (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报文的标识
- ☐ 匹配ICMP报文的类型和消息码
- ☐ 匹配DSCP优先级
- ☐ 匹配IP优先级
- ☐ 匹配ToS优先级
- ☐ 匹配GreKey

5) 在 安全---包过滤---包过滤 进入后点击右上角的 “+”

< 43 天 | 18:55:43 >

*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ICMP报文的类型和消息码
- ☐ 匹配DSCP优先级
- ☐ 匹配IP优先级
- ☐ 匹配ToS优先级
- ☐ 匹配GreKey

规则生效时间段: 请选择...

包过滤 > 包过滤

接入 > 802.1X

认证 > ISP域

IP Source Guard

MAC地址认证

端口安全

Portal

RADIUS

TACACS

本地认证

< H3C >

安全 / 包过滤 / 包过滤

包过滤

接口 VLAN 全局

添加 删除

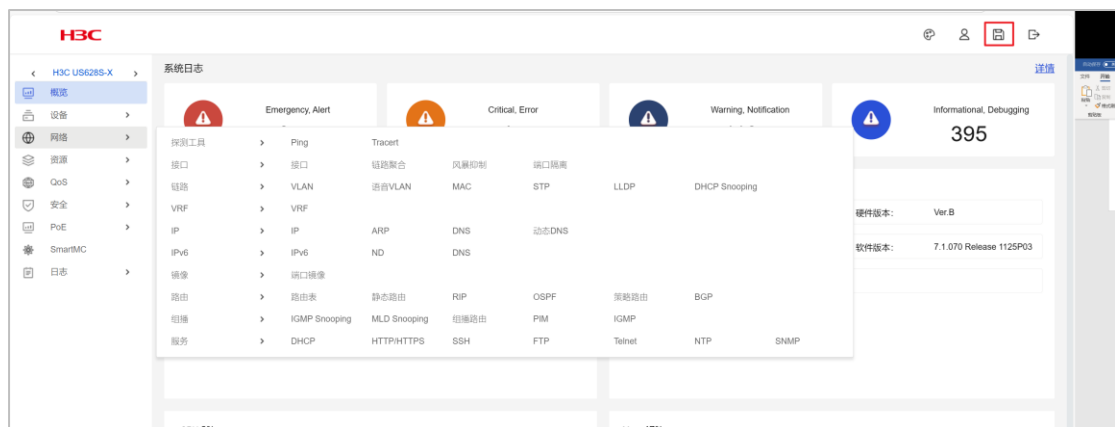
查询

接口 方向 过滤规则 ACL 默认动作 规则应用 匹配统计

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) 保存交换机配置信息

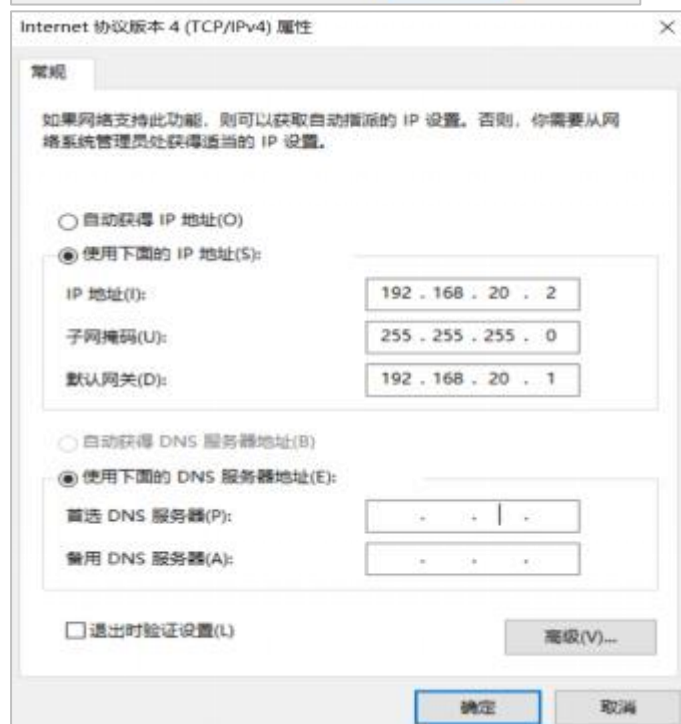


四、验证配置

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),
```