

---

## Private VLAN 配置

## 目录

|   |   |
|---|---|
| Private VLAN 配置.....                            | 1 |
| 第一章 Private VLAN 配置.....                        | 1 |
| 1.1 Private Vlan 概述.....                        | 1 |
| 1.2 私有 VLAN 的类型和私有 VLAN 中端口的类型.....             | 1 |
| 1.2.1 有一种类型的主 VLAN: .....                       | 1 |
| 1.2.2 有二种类型的辅助 VLAN: .....                      | 1 |
| 1.2.3 私有 VLAN 端口是如下类型的端口: .....                 | 1 |
| 1.2.4 私有 VLAN 对 VLAN TAG 中的字段的修改特性.....         | 2 |
| 1.3 Private VLAN 配置任务列表.....                    | 2 |
| 1.4 Private VLAN 配置任务.....                      | 2 |
| 1.4.1 配置 Private VLAN.....                      | 2 |
| 1.4.2 配置 Private VLAN 中的私有 VLAN 域的关联.....       | 2 |
| 1.4.3 配置 Private VLAN 中的二层接口为私有 VLAN 的主机接口..... | 3 |
| 1.4.4 配置 Private VLAN 中的二层接口为私有 VLAN 的混杂接口..... | 3 |
| 1.4.5 配置 private vlan 出端口报文中的相关字段修改.....        | 3 |
| 1.4.6 private vlan 配置信息的显示.....                 | 4 |
| 1.5 配置实例.....                                   | 4 |

# 第一章 Private VLAN 配置

## 1.1 Private Vlan 概述

Private Vlan 解决了服务提供商在应用 VLAN 时所面临的问题：如果服务提供商给每一个用户提供一个 VLAN，由于每一台设备最多支持 4094 个 VLAN 从而限制了服务提供商能支持用户的总数量。

## 1.2 私有VLAN的类型和私有VLAN中端口的类型

私有 VLAN(private vlan)将一个 VLAN 的二层广播域划分成多个子域，每个子域都由一个私有 VLAN 对组成：主 VLAN(Primary VLAN)和一个或若干个辅助 VLAN(Secondary VLAN)。一个私有 VLAN 域可以有多个私有 VLAN 对，每一个私有 VLAN 对代表一个子域。在一个私有 VLAN 域中只有一个主 VLAN，所有的私有 VLAN 对共享同一个主 VLAN。每个子域的辅助 VLAN ID 不同。

### 1.2.1 有一种类型的主 VLAN：

- 主 vlan(Primary VLAN)：是一个与混杂端口相关联的 VLAN，Private VLAN 中只能有一个 Primary VLAN，每个在 Primary VLAN 中的端口都是 Primary VLAN 的成员。

### 1.2.2 有二种类型的辅助 VLAN：

- 隔离 VLAN(Isolated VLAN)：同一个隔离 VLAN 中的端口不能互相进行二层通信。一个私有 VLAN 域中只有一个隔离 VLAN。一个隔离 vlan 必须与一个 Primary VLAN 关联。
- 共用 VLAN(Community VLAN)：同一个共用 VLAN 中的端口可以互相进行二层通信，但不能与其它共用 VLAN 中的端口进行二层通信。一个私有 VLAN 域中可以有多个共用 VLAN。一个公共 vlan 必须与一个 Primary VLAN 相关联。

### 1.2.3 私有 VLAN 端口是如下类型的端口：

- 混杂端口 (Promiscuous Port)：属于主 VLAN 中的端口。可以与所有端口通讯，包括同一个私有 VLAN 域中辅助 VLAN 的隔离端口和共用端口。
- 隔离端口(Isolated Port)：属于隔离 VLAN 中的主机端口(Host Port)。在同一个私有 VLAN 域中，除了混杂端口外，隔离端口与其它的所有端口完全二层隔离，从隔离端口收到的流量只能转发到混杂端口。
- 共用端口(Community Port)：属于共用 VLAN 中的主机端口(Host Port)。在一个私有 VLAN 域中，同一个共用 VLAN 的共用端口可以互相进行二层通讯，也可以与混杂端口进行二层通讯，不能与其它共用 VLAN 中的共用端口及隔离 VLAN 中的隔离端口进行二层通讯。

## 1.2.4 私有 VLAN 对 VLAN TAG 中的字段的修改特性

此功能支持在 VLAN 的 tag 中修改 VLAN ID 和优先级字段，以及私有 VLAN 的出端口的报文是否带 tag。

## 1.3 Private VLAN配置任务列表

- 配置 Private VLAN
- 配置 Private VLAN 中的私有 VLAN 域的关联
- 配置 Private VLAN 中的二层接口为私有 VLAN 的主机接口
- 配置 Private VLAN 中的二层接口为私有 VLAN 的混杂接口
- 配置 Private VLAN 出端口报文中的相关字段修改
- Private VLAN 配置信息的显示

## 1.4 Private VLAN 配置任务

一个私有 VLAN 对生效的条件如下：

1. 具有主 VLAN。
2. 具有辅助 VLAN。
3. 辅助 VLAN 和主 VLAN 之间有关联。
4. 主 VLAN 内有混杂端口。

### 1.4.1 配置 Private VLAN

使用下面的命令来将 VLAN 配置成私有 VLAN

| 命令  | 目的              |
|---|-----------------|
| <b>vlan <i>vlan-id</i></b>                          | 进入VLAN模式进行配置    |
| <b>private-vlan {primary community isolated}</b>    | 配置VLAN的私有VLAN属性 |
| <b>no private-vlan {primary community isolated}</b> | 清除VLAN的私有VLAN属性 |
| <b>show vlan private-vlan</b>                       | 显示私有VLAN的配置信息   |
| <b>exit</b>   | 退出VLAN的配置模式     |

### 1.4.2 配置 Private VLAN 中的私有 VLAN 域的关联

使用下面的命令来关联私有 VLAN 中的主 VLAN 和辅助 VLAN

| 命令   | 目的                   |
|--|----------------------|
| <b>vlan <i>vlan-id</i></b>   | 进入主VLAN配置模式进行配置      |
| <b>private-vlan association<br/>{<i>svlist</i>   add <i>svlist</i>   remove <i>svlist</i>}</b> | 配置要关联的Secondary VLAN |

|                                    |                                      |
|------------------------------------|--------------------------------------|
| <b>no private-vlan association</b> | 清除当前Primary VLAN与所有Secondary VLAN的关联 |
| <b>exit</b>                        | 退出VLAN配置模式                           |

#### 1.4.3 配置 Private VLAN 中的二层接口为私有 VLAN 的主机接口

使用下面的命令来配置 Private VLAN 中的二层接口为私有 VLAN 的主机接口

| 命令   | 目的                 |
|--|--------------------|
| <b>Interface</b> <i>interface</i>  | 进入接口配置模式           |
| <b>switchport mode private-vlan host</b>                                     | 配置二层接口为主机端口模式      |
| <b>no switchport mode</b>  | 清除二层接口的私有VLAN模式配置  |
| <b>switchport private-vlan host-association</b> <i>p_vid</i><br><i>s_vid</i> | 关联二层主机接口与私有VLAN的关联 |
| <b>no switchport private-vlan host-association</b>                           | 清除二层主机接口与私有VLAN的关联 |
| <b>exit</b>  | 退出接口的配置模式          |

#### 1.4.4 配置 Private VLAN 中的二层接口为私有 VLAN 的混杂接口

使用下面的命令来配置 Private VLAN 中的二层接口为私有 VLAN 的混杂接口

| 命令  | 目的                 |
|---|--------------------|
| <b>Interface</b> <i>interface</i>   | 进入接口配置模式           |
| <b>switchport mode private-vlan promiscuous</b>   | 配置二层接口为混杂端口模式      |
| <b>no switchport mode</b>   | 清除二层接口的私有VLAN模式配置  |
| <b>switchport private-vlan mapping</b><br><i>p_vid</i> { <i>svlist</i>   <i>add svlist</i>   <i>remove svlist</i> } | 关联二层混杂接口与私有VLAN的关联 |
| <b>no switchport private-vlan mapping</b>   | 清除二层混杂接口与私有VLAN的关联 |
| <b>exit</b>   | 退出接口的配置模式          |

#### 1.4.5 配置 private vlan 出端口报文中的相关字段修改

使用下面的命令来配置 Private VLAN 中出端口报文中的相关字段修改

| 命令   | 目的                     |
|--|------------------------|
| <b>Interface</b> <i>interface</i>                      | 进入接口配置模式               |
| <b>switchport private-vlan tag-pvid</b> <i>vlan-id</i> | 配置出端口报文tag中的vlan id字段  |
| <b>switchport private-vlan tag-pri</b> <i>pri</i>      | 配置出端口报文tag中的priority字段 |
| <b>[no] switchport private-vlan untagged</b>           | 配置出端口报文是否带tag          |
| <b>exit</b>  | 退出端口的配置模式              |

## 1.4.6 private vlan 配置信息的显示

使用下面的命令来显示 Private VLAN 中的私有 VLAN 和二层接口的私有 VLAN 配置信息，配置的模式为全局配置模式，接口配置模式和 VLAN 配置模式

| 命令  | 目的                      |
|---|-------------------------|
| <b>show vlan private-vlan</b>                     | 显示私有VLAN的配置信息           |
| <b>show vlan private-vlan interface interface</b> | 显示私有VLAN中的二层接口的VLAN配置信息 |

## 1.5 配置实例

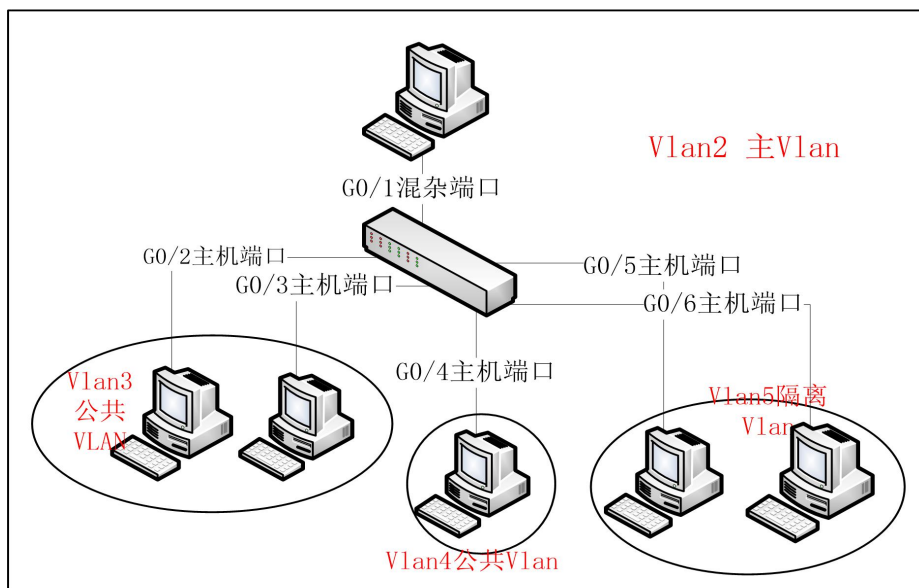


图1 Private VLAN的典型配置图

通过一个典型的组网方式来说明 Private VLAN 的应用

如图 1 所示 G0/1 为 Primary VLAN 2 下混杂端口，G0/2-G0/6 为主机端口，其中 G0/2、G0/3 为 Community VLAN 3 下的主机端口（公用端口），G0/4 为 Community VLAN 4 下的主机端口（公用端口），G0/5、G0/6 为 Isolated VLAN 5 下的的主机端口（隔离端口）。

根据 Private VLAN 的概念，混杂端口 G0/1 可以与该私有 VLAN 中的所有子 VLAN 域中的主机接口互相进行二层通信，公用 VLAN 3 下的主机端口 G0/2、G0/3 可以互相二层通信，但不能与其他辅助 VLAN 中的主机端口进行二层通信，包括不同组的公用 VLAN 4，隔离 VLAN 5 下的隔离端口 G0/5、G0/6 互相不能进行二层通信，它们只能与整个私有 VLAN 中的混杂端口 G0/1 进行二层通信。

具体在交换机下的命令配置如下：

```
Switch_config#interface GigaEthernet0/1
Switch_config_g0/1#switchport mode private-vlan promiscuous
Switch_config_g0/1#switchport private-vlan mapping 2 3-5
Switch_config_g0/1#switchport pvid 2
```

```
Switch_config#interface GigaEthernet0/2
Switch_config_g0/2#switchport mode private-vlan host
Switch_config_g0/2#switchport private-vlan host-association 2 3
Switch_config_g0/2#switchport pvid 3
```

```
Switch_config#interface GigaEthernet0/3
Switch_config_g0/3#switchport mode private-vlan host
Switch_config_g0/3#switchport private-vlan host-association 2 3
Switch_config_g0/3#switchport pvid 3
```

```
Switch_config#interface GigaEthernet0/4
Switch_config_g0/4#switchport mode private-vlan host
Switch_config_g0/4#switchport private-vlan host-association 2 4
Switch_config_g0/4# switchport pvid 4
```

```
Switch_config#interface GigaEthernet0/5
Switch_config_g0/5#switchport mode private-vlan host
Switch_config_g0/5#switchport private-vlan host-association 2 5
Switch_config_g0/5#switchport pvid 5
```

```
Switch_config#interface GigaEthernet0/6
Switch_config_g0/5#switchport mode private-vlan host
Switch_config_g0/5#switchport private-vlan host-association 2 5
Switch_config_g0/5#switchport pvid 5
```

```
Switch_config#vlan 2
Switch_config_vlan2#private-vlan primary
Switch_config_vlan2#private-vlan association 3-5
```

```
Switch_config#vlan 3
Switch_config_vlan3#private-vlan community
```

```
Switch_config#vlan 4
Switch_config_vlan4#private-vlan community
```

```
Switch_config#vlan 5
Switch_config_vlan5#private-vlan isolated
```

---

```
Switch_config#show vlan private-vlan
```

| Primary | Secondary | Type      | Ports            |
|---------|-----------|-----------|------------------|
| 2       | 3         | community | g0/1, g0/2, g0/3 |
| 2       | 4         | community | g0/1, g0/4       |
| 2       | 5         | isolated  | g0/1, g0/5, g0/6 |