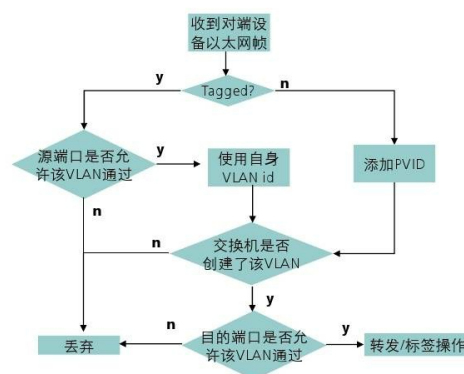


# VLAN

## 基础知识

- 避免网络风暴
- 传统的以太网帧中插入4字节的 VLAN 标签，源/目的 MAC 地址之后
- VLAN 标签中的 VLAN ID 占12比特，所以共有2的12次方——4096个 VLAN 标签，一般不用首尾两个，所有一般能用的 VLAN 标签是4094个
- PVID（port default vlan id）：某交换机对 untagged 的标签会打上 PVID
- VLAN 划分方式(一个接口配置一个 VLAN)
  - 基于接口划分（最简单）
  - 基于 MAC 地址划分
  - 基于 IP 子网地址划分
  - 基于协议划分

## VLAN转发流程



- VLAN 转发流程

各类型接口对数据帧的处理方式			
接口类型	对接收不带 Tag 的报文处理	对接收带 Tag 的报文处理	发送帧处理过程
Access 接口	接收该报文，并打上缺省的 VLAN ID。	当 VLAN ID 与缺省 VLAN ID 相同时，接收该报文； 当 VLAN ID 与缺省 VLAN ID 不同时，丢弃该报文。	先剥离帧的 PVID Tag，然后再发送。
Trunk 接口	打上缺省的 VLAN ID，当缺省 VLAN ID 在允许通过的 VLAN ID 列表里时，接收该报文； 当缺省 VLAN ID 不在允许通过的 VLAN ID 列表里时，丢弃该报文。	当 VLAN ID 在接口允许通过的 VLAN ID 列表里时，接收该报文； 当 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，丢弃该报文。	当 VLAN ID 与缺省 VLAN ID 相同，且是该接口允许通过的 VLAN ID 时，去掉 Tag，发送该报文； 当 VLAN ID 与缺省 VLAN ID 不同，且是该接口允许通过的 VLAN ID 时，保持原有 Tag，发送该报文。
Hybrid 接口	打上缺省的 VLAN ID，当缺省 VLAN ID 在允许通过的 VLAN ID 列表里时，接收该报文； 打上缺省的 VLAN ID，当缺省 VLAN ID 不在允许通过的 VLAN ID 列表里时，丢弃该报文。	当 VLAN ID 在接口允许通过的 VLAN ID 列表里时，接收该报文； 当 VLAN ID 不在接口允许通过的 VLAN ID 列表里时，丢弃该报文。	当 VLAN ID 是该接口允许通过的 VLAN ID 时，发送该报文。  可以通过命令设置发送时是否携带 Tag。

- VLAN 端口类型
- hybrid 端口更灵活，可以在主机与设备或者设备与设备之间设置，可自定义
  - 比如某端口设置 hybrid 端口，其 PVID 为 5
  - 可自定义设置允许放行的 VLAN，比如：untagged 方式放行 vlan 1 5，tagged 方式放行 vlan 7
  - 当转发 vlan 1 5 时，去标签 untagged 转发
- 自动配置：GVRP 协议
  - GVRP(GARP Vlan Registration Protocol)
  - GARP(Generic Attribute Registration Protocol, 通用属性注册协议)

## VLAN 路由

- VLAN 的缺点：
  - VLAN 隔离了二层广播域,也就隔离了各个 VLAN 之间的任何流量，分属于不同 VLAN 的用户不能通信
- VLAN 间通信：
  - 借助路由器的三层转发功能
    - 路由器的不同接口加入不同的 VLAN，并且这些接口设置好网关
      - 当 VLAN 数量较多时，要配置很多路由器接口，
    - 单臂路由：VLAN TRUNKING，虚接口
      - 二层交换机和路由器之间相连的接口配置 VLAN TRUNKING，虚接口，单臂路由，，使多个 VLAN 共享同一条物理链路连接到路由器
  - 交换和路由的集成——三层交换机
    - 二层交换机和路由器在功能上的集成构成了三层交换机
    - 三层交换机在功能上实现了 VLAN 的划分、VLAN 内部二层交换和 VLAN 间路由的功能
    - 通过 VLANIF 接口配置

## 命令总结

- 查看 VLAN 信息：

```
dis vlan 11
```

会显示:

```
[RT]dis vlan 11
* : management-vlan
-----
VLAN ID Type          Status  MAC Learning Broadcast/Multicast/Unicast
Property
-----
11      common        enable  enable    forward  forward  forward
default

-----
Untagged      Port: Ethernet0/0/0      Ethernet0/0/1
              Ethernet0/0/2

-----
Active Untag  Port: Ethernet0/0/0      Ethernet0/0/1
              Ethernet0/0/2

-----
Interface          Physical
Ethernet0/0/0      UP
Ethernet0/0/1      UP
Ethernet0/0/2      UP
```

可以看到: e 0/0/0 ~ e 0/0/2 加入了 VLAN 11

- 修改端口类型时, 报错:

```
Error: Please renew the default configurations.
```

解决方案: 需要一层一层的来删除配置, 直到恢复到默认的配置。

比如:

配置的时候为:

```
port link-type access

port default vlan 4
```

如果直接更改端口模式就会报错为:

```
Error: Please renew the default configurations.
```

所以如果出现这种错误，在这里就需要从后往前删除，即：

```
undo port default vlan 4  
  
undo port link-type
```

到这里以后 才可以重新更改端口的模式。

- 配置 access 接口类型：

```
[SWA]vlan 3  
[SWA-Ethernet0/1]port link-type access  
[SWA-Ethernet0/1]port default vlan 3
```

- 配置 trunk 接口类型：

```
[SWA]vlan 3  
[SWA-Ethernet0/3]port link-type trunk  
[SWA-Ethernet0/3]port trunk pvid vlan 3  
\\ 配置 trunk-like 所允许通过的 vlan 标签 (permitted vlan)  
[SWA-Ethernet0/3]port trunk allow-pass vlan 5
```

- 配置 hybrid 接口类型：
- 配置 GVRP（在所有端口配置 GVRP 协议）：

```
[SWA]gvrp  
[SWA]int e 0/1  
[SWA-Ethernet0/1]port link-type access  
[SWA-Ethernet0/1]port default vlan 3  
[SWA-Ethernet0/1]gvrp
```

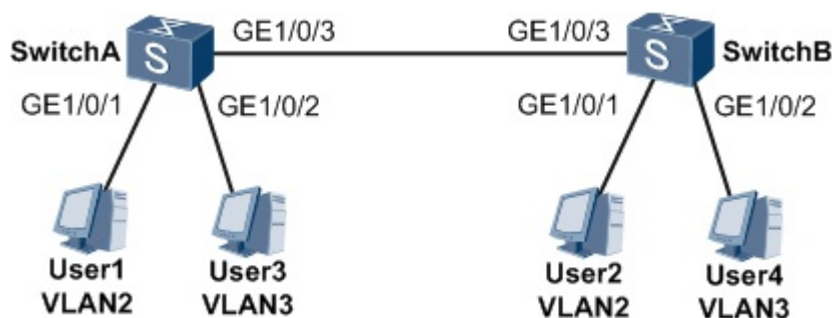
- 配置子接口：

```
<HUAWEI> system-view  
[HUAWEI] sysname Switch  
[Switch] interface gigabitethernet1/0/1  
[Switch-GigabitEthernet1/0/1] port link-type hybrid
```

```
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet1/0/1.1
[Switch-GigabitEthernet1/0/1.1] dot1q termination vid 10
[Switch-GigabitEthernet1/0/1.1] ip address 10.10.10.1 24
[Switch-GigabitEthernet1/0/1.1] arp broadcast enable
[Switch-GigabitEthernet1/0/1.1] quit
```

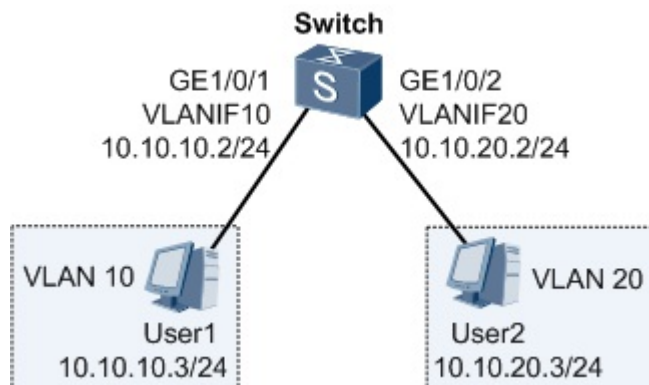
## 实例

- 基于接口划分 VLAN 配置示例（静态配置链路类型）



- 应用场景：
  - 某企业的交换机连接有很多用户，且相同业务用户通过不同的设备接入企业网络。
  - 为了通信的安全性，同时为了避免广播风暴，企业希望业务相同用户之间可以互相访问，业务不同用户不能直接访问。
  - 可以在交换机上配置基于接口划分 VLAN，把业务相同的用户连接的接口划分到同一 VLAN。这样属于不同 VLAN 的用户不能直接进行二层通信，同一 VLAN 内的用户可以直接互相通信。
- 配置思路：
  - 创建 VLAN 并将连接用户的接口加入 VLAN，实现不同业务用户之间的二层流量隔离。
  - 配置 SwitchA 和 SwitchB 之间的链路类型及通过的 VLAN，实现相同业务用户通过 SwitchA 和 SwitchB 通信。
- [参考教程](#)

- 利用 VLANIF 实现不同 VLAN 之间的通信（三层交换机）



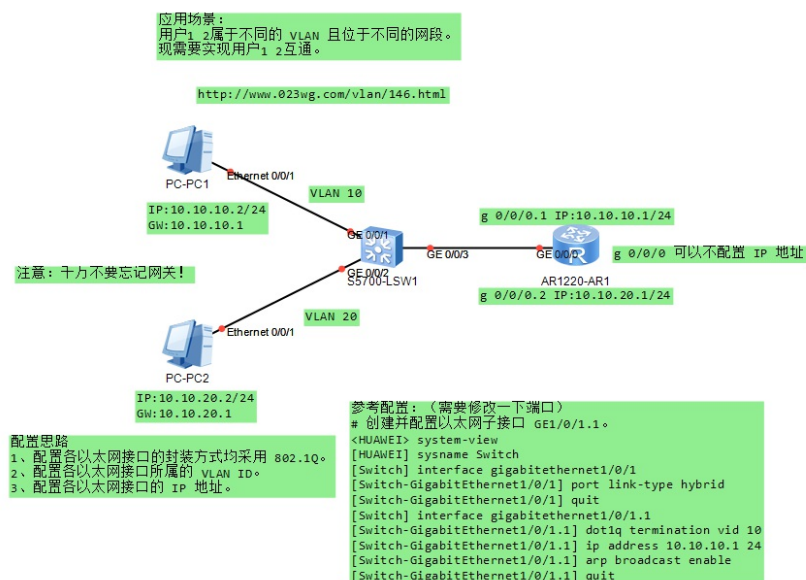
- 应用场景：
  - 企业的不同用户拥有相同的业务，且位于不同的网段。
  - 现在相同业务的用户所属的 VLAN 不相同，需要实现不同 VLAN 中的用户相互通信。

- 配置思路

1. 创建 VLAN，确定用户所属的 VLAN。
2. 配置接口加入 VLAN，允许用户所属的 VLAN 通过当前接口。
3. 创建 VLANIF 接口并配置 IP 地址，实现三层互通。
4. 为了成功实现 VLAN 间互通，VLAN 内主机的缺省网关必须是对应 VLANIF 接口的 IP 地址。

- 检查配置结果

- 在 VLAN10 中的 User1 主机上配置 IP 地址为 10.10.10.3/24，缺省网关为 VLANIF10 接口的 IP 地址 10.10.10.2/24。
- 在 VLAN20 中的 User2 主机上配置 IP 地址为 10.10.20.3/24，缺省网关为 VLANIF20 接口的 IP 地址 10.10.20.2/24。
- 配置完成后，VLAN10 内的 User1 与 VLAN20 内的 User2 能够相互访问。
- [参考教程](#) 二层交换机的接口不能配置 IP，所以要用三层交换机的 VLANIF 接口（虚拟的）



- 利用子接口实现单臂路由

- 应用场景：

- 各个部门中的用户位于不同的网段，且用业务划分了不同 VLAN，现需要实现不同 VLAN 中的用户相互通信。

- 配置思路

- 配置各以太网接口的封装方式均采用 802.1Q。
- 配置各以太网接口所属的 VLAN ID。
- 配置各以太网接口的 IP 地址。
- 路由器的接口要设置 IP 地址，并且作为主机的网关