



VLAN 原理与配置

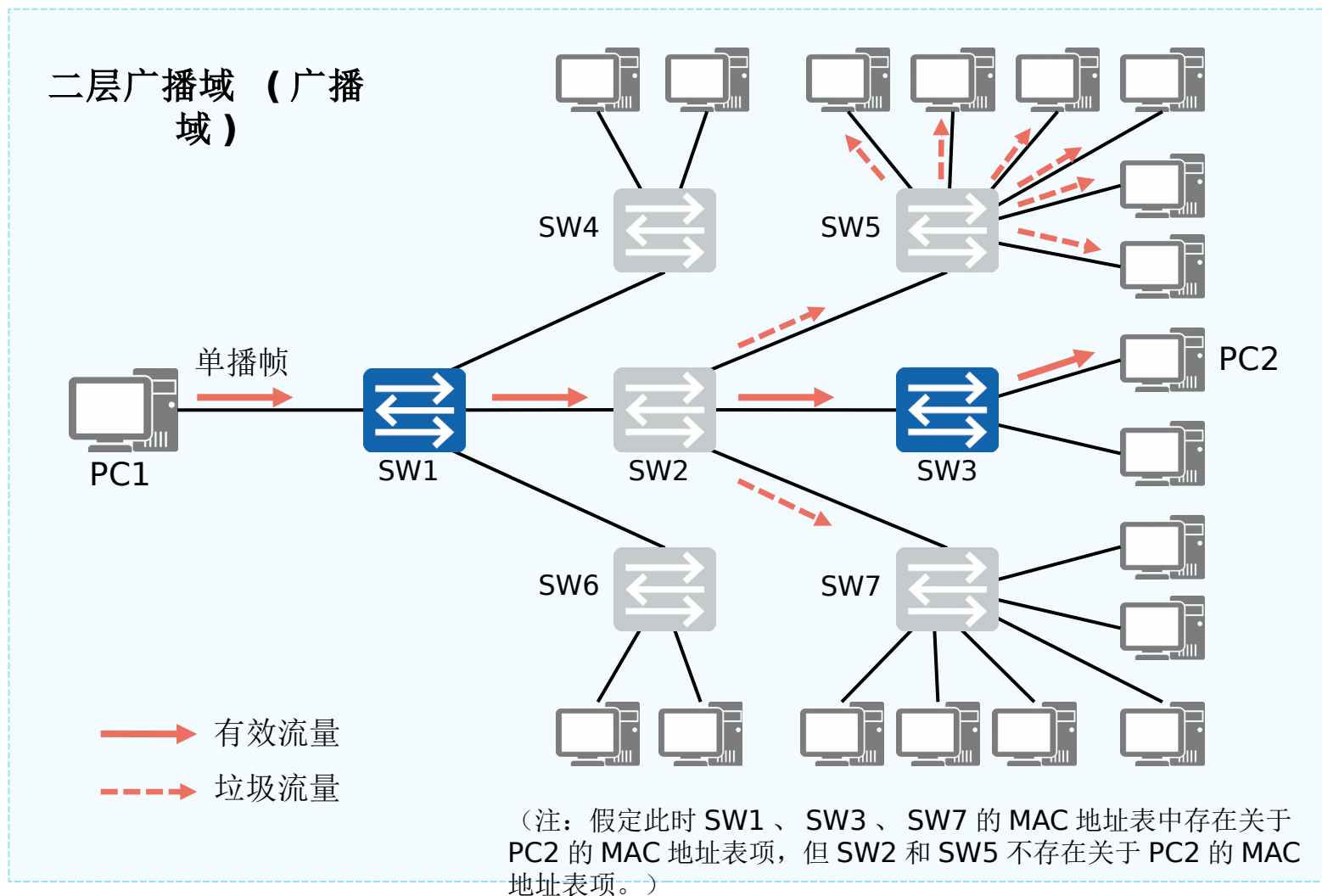


目录

- 1. 什么是 VLAN**
2. VLAN 的基本概念
3. VLAN 的应用
4. VLAN 的配置示例



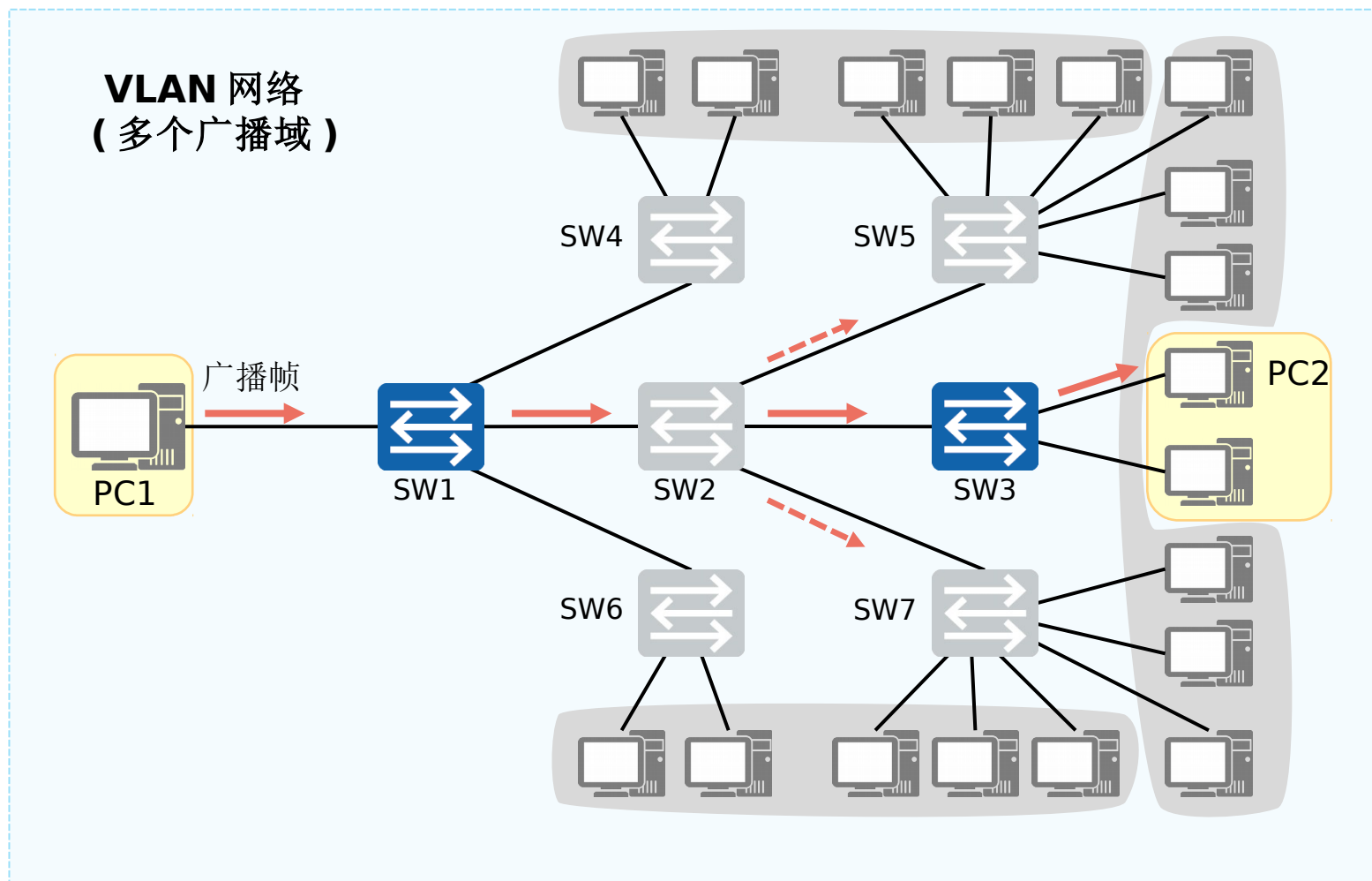
传统以太网的问题



- 在典型交换网络中，当某台主机发送一个广播帧或未知单播帧时，该数据帧会被泛洪，甚至传递到整个广播域。
- 广播域越大，产生的网络安全问题、垃圾流量问题，就越严重。



虚拟局域网 (VLAN, Virtual LAN)



- 虚拟局域网 VLAN 可以隔离广播域。
- 特点：
 - 不受地域限制。
 - 同一 VLAN 内的设备才能直接进行二层通信。



目录

1. 什么是 VLAN
- 2. VLAN 的基本原理**
3. VLAN 的应用
4. VLAN 的配置示例

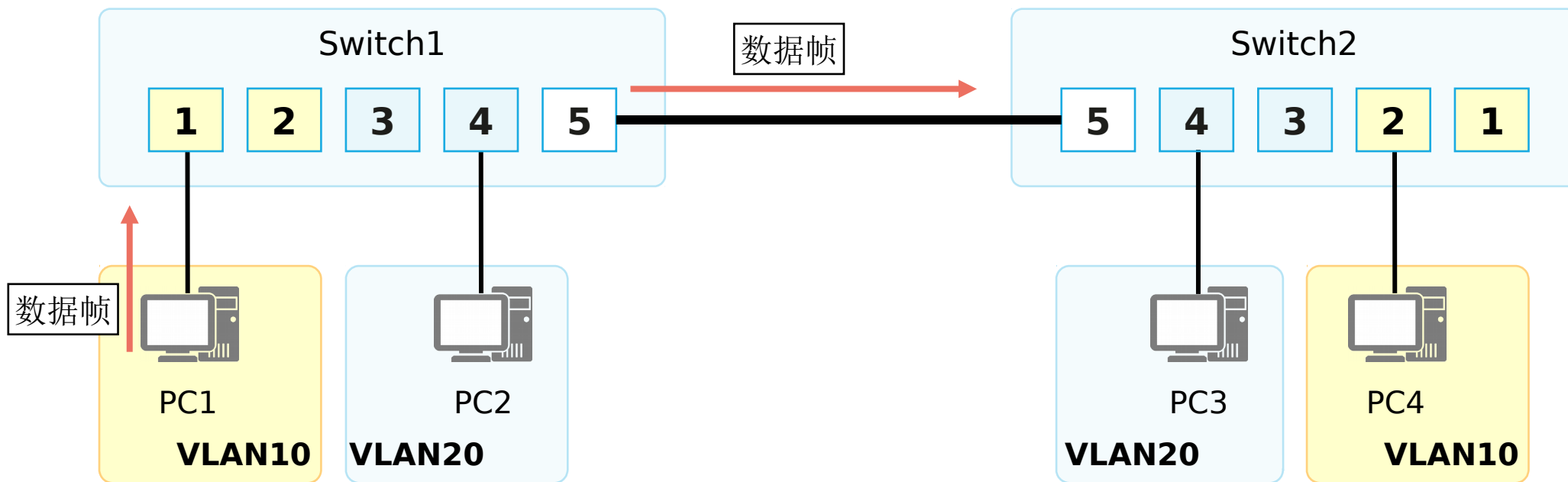


如何实现 VLAN

识别
VLAN

划分 VLAN

处理 VLAN 数据
帧

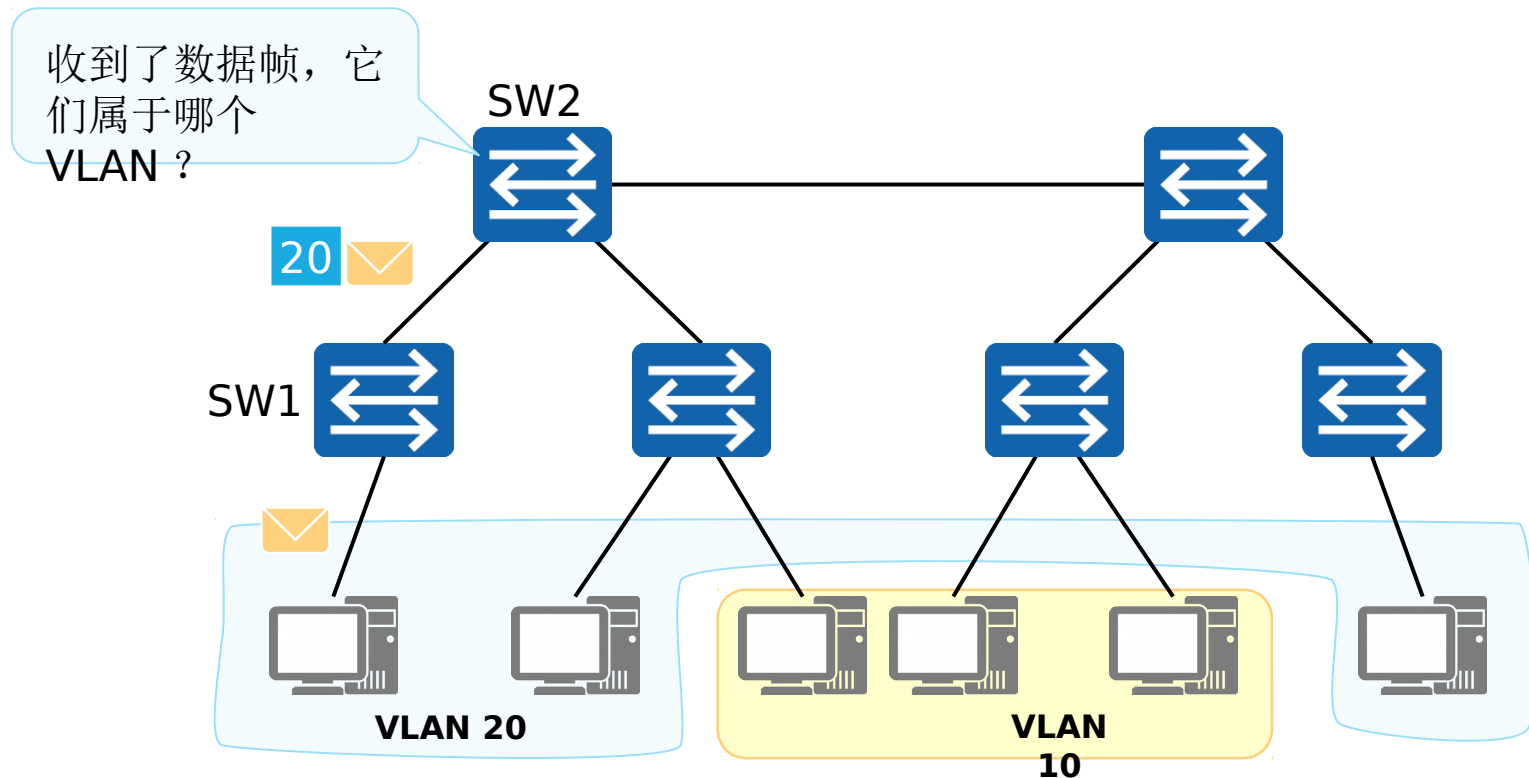


- Switch1 与 Switch2 同属一个企业，该企业统一规划了网络中的 VLAN 。其中 VLAN10 用于 A 部门， VLAN20 用于 B 部门。A 、 B 部门的员工在 Switch1 和 Switch2 上都有接入。
- PC1 发出的数据经过 Switch1 和 Switch2 之间的链路到达了 Switch2 。如果不加处理，后者无法判断该数据所属的 VLAN ，也不知道应该将这个数据输出到本地哪个 VLAN 中。



VLAN 标签 (VLAN Tag)

- 交换机如何识别接收到的数据帧属于哪个 VLAN ？



VLAN 标签

- 要使交换机能够分辨不同 VLAN 的报文，需要在报文中添加标识 VLAN 信息的字段。
- IEEE 802.1Q 协议规定，在以太网数据帧中加入 4 个字节的 VLAN 标签，又称 VLAN Tag，简称 Tag。



VLAN 数据帧

原始以太网数据帧
(无标记帧, Untagged 帧)

目的 MAC 地址	源 MAC 地址	类型	Data	FCS
-----------	----------	----	------	-----

在此处插入 802.1Q Tag

802.1Q Tag

TPID (0x8100)	PRI	CFI	VLAN ID
16bit	3bit	1bit	12bit

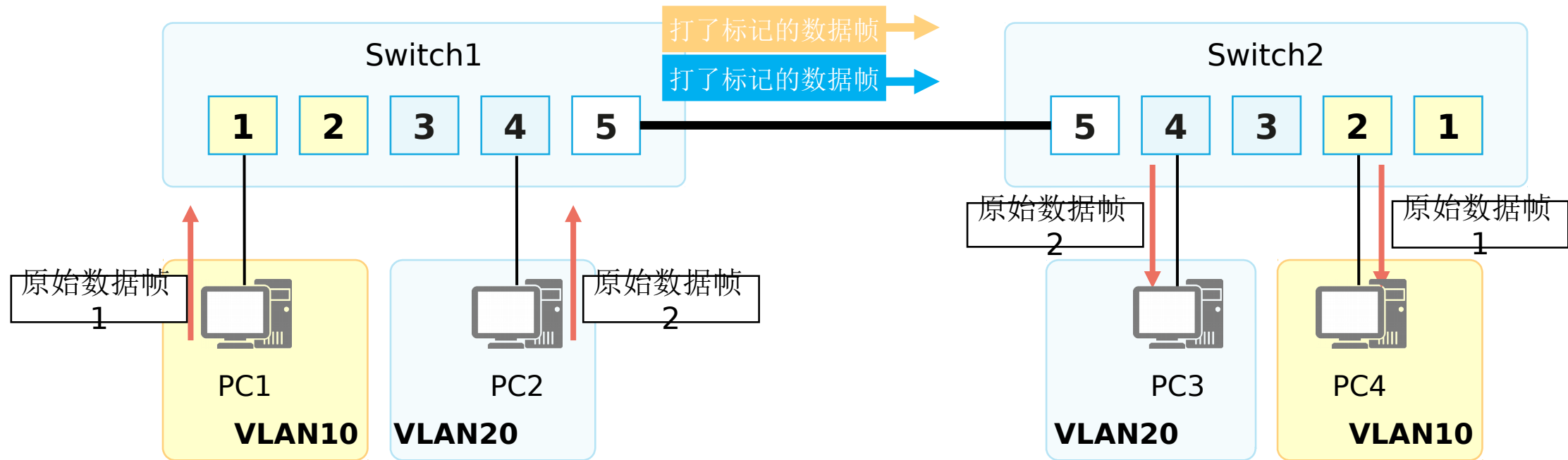
- TPID (标签协议标识符): 标识数据帧的类型, 值为 0x8100 时表示 802.1Q 帧。
- PRI (优先级): 标识帧的优先级, 主要用于 QoS。
- CFI (标准格式指示符): 在以太网环境中, 该字段的值为 0。
- VLAN ID (VLAN 标识符): 标识该帧所属的 VLAN。

802.1Q 帧
(标记帧, Tagged 帧)

目的 MAC 地址	源 MAC 地址	Tag	类型	Data	FCS
-----------	----------	-----	----	------	-----



VLAN 的实现

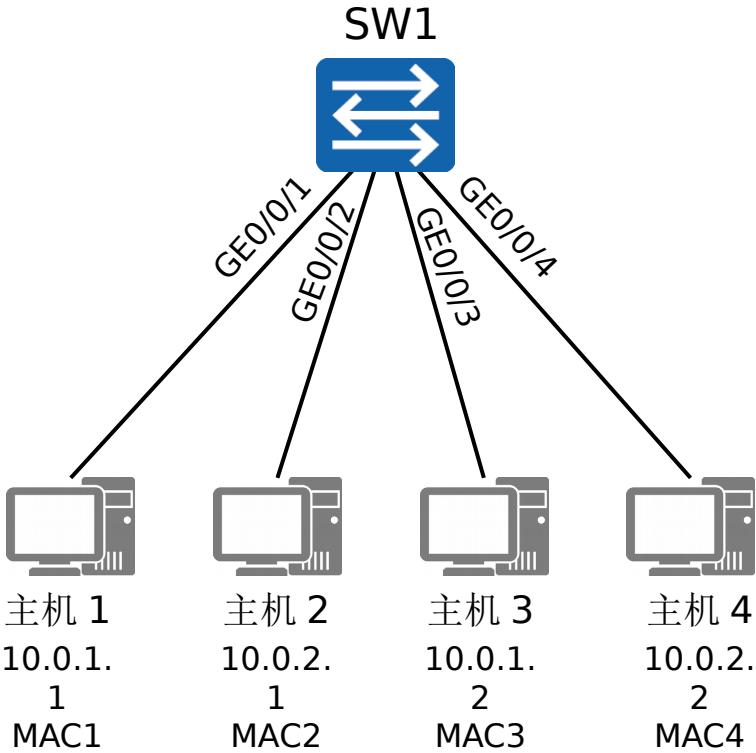


- Switch1 和 Switch2 之间的链路要承载多个 VLAN 的数据，需要一种基于 VLAN 的数据“**标记**”手段，以便对**不同 VLAN** 的数据帧进行区分。
- IEEE 802.1Q 标准（也被称为 Dot1Q）定义了“**打 Tag**”法。标准对以太网数据帧进行修改，在 802.1Q 帧头中插入 Tag，而在该 Tag 中，便可以写入 VLAN 信息。



VLAN 的划分方式

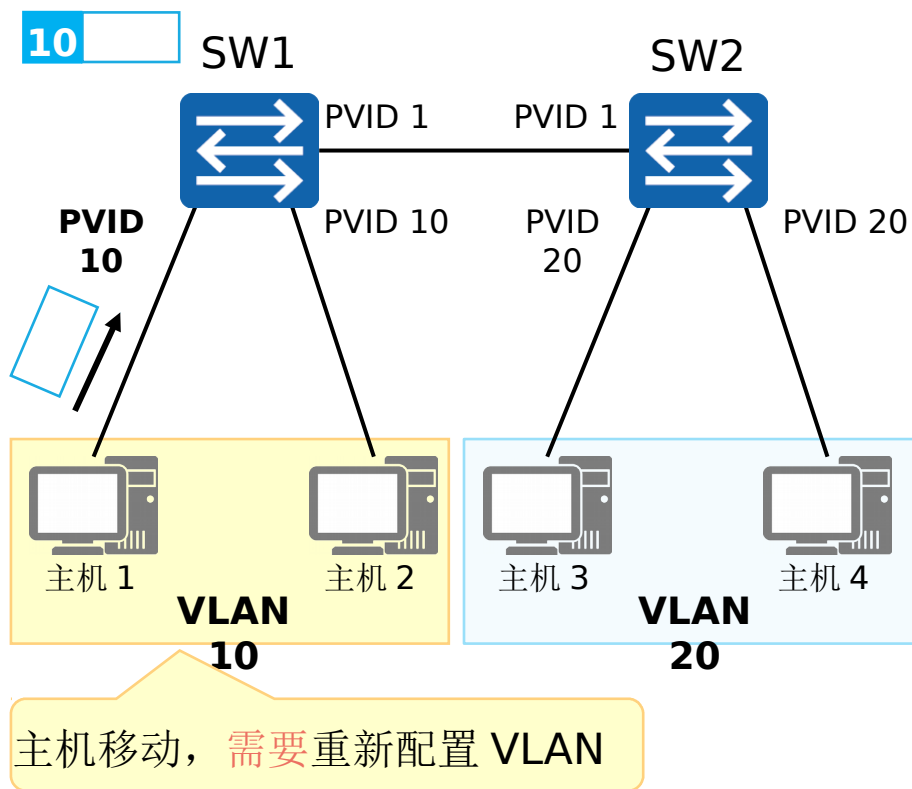
整个网络是如何划分VLAN 的？



VLAN 划分方式	VLAN 10	VLAN 20
基于接口	GE0/0/1 , GE0/0/3	GE0/0/2 , GE0/0/4
基于 MAC 地址	MAC 1 , MAC 3	MAC 2 , MAC 4
基于 IP 子网划分	10.0.1.*	10.0.2.*
基于协议划分	IP	IPv6
基于策略	10.0.1.* + GE0/0/1+ MAC 1	10.0.2.* + GE0/0/2 + MAC 2



基于接口的 VLAN 划分



基于接口的 VLAN 划分

• 原理

- 根据交换机的接口来划分 VLAN。
- 网络管理员预先给交换机的每个接口配置不同的 **PVID**，将该接口划入 PVID 对应的 VLAN。
- 当一个数据帧进入交换机时，如果没有带 VLAN 标签，该数据帧就会被打上接口指定 PVID 的 Tag，然后数据帧将在指定 PVID 中传输。

• 缺省 VLAN，PVID

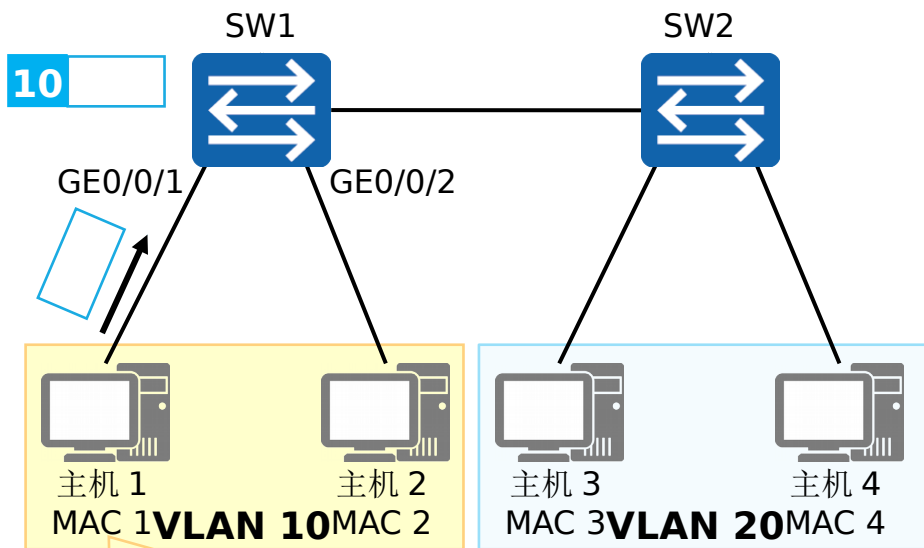
- Port VLAN ID，是接口上的缺省 VLAN。
- 取值：1~4094。



基于 MAC 地址的 VLAN 划分

SW1 的 MAC 地址与 VLAN 表

MAC 地址	VLAN ID
MAC 1	10
MAC 2	10
.....	



主机移动, 不需要重新配置 VLAN

基于 MAC 地址的 VLAN 划分

• 原理

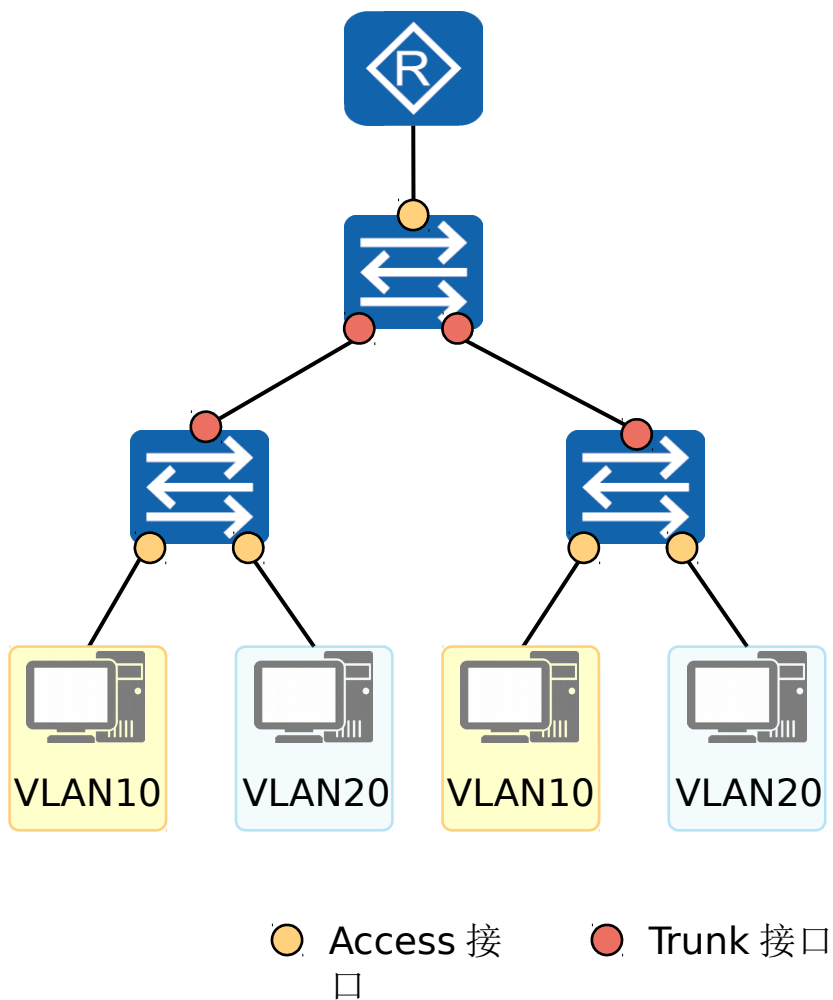
- 根据数据帧的源 MAC 地址来划分 VLAN。
- 网络管理员预先配置 MAC 地址和 VLAN ID 映射关系表。
- 当交换机收到的是 Untagged 帧时, 就依据该表给数据帧添加指定 VLAN 的 Tag, 然后数据帧将在指定 VLAN 中传输。

• 映射表

- 记录了 MAC 地址和 VLAN ID 的关联情况。



以太网二层接口类型



接口类型

• Access 接口

交换机上常用来连接用户 PC、服务器等终端设备的接口。Access 接口所连接的这些设备的网卡往往只收发无标记帧。Access 接口只能加入一个 VLAN。

• Trunk 接口

Trunk 接口允许多个 VLAN 的数据帧通过，这些数据帧通过 802.1Q Tag 实现区分。Trunk 接口常用于交换机之间的互联，也用于连接路由器、防火墙等设备的子接口。

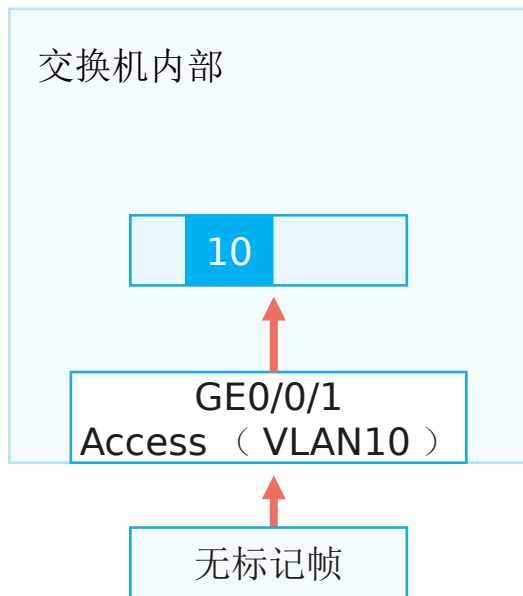
• Hybrid 接口

Hybrid 接口与 Trunk 接口类似，也允许多个 VLAN 的数据帧通过，这些数据帧通过 802.1Q Tag 实现区分。用户可以灵活指定 Hybrid 接口在发送某个（或某些）VLAN 的数据帧时是否携带 Tag。

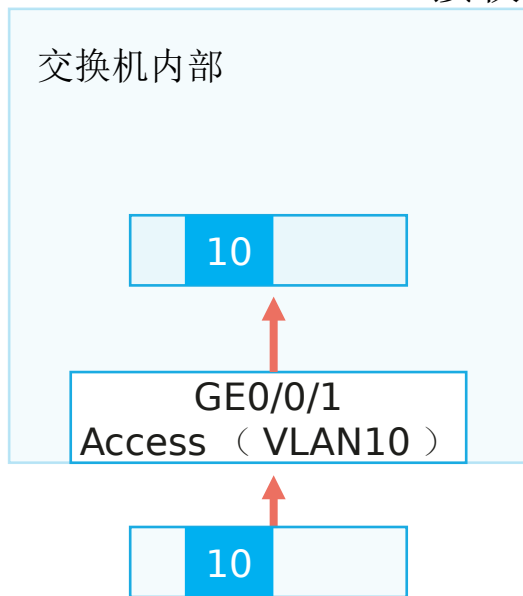


Access 接口

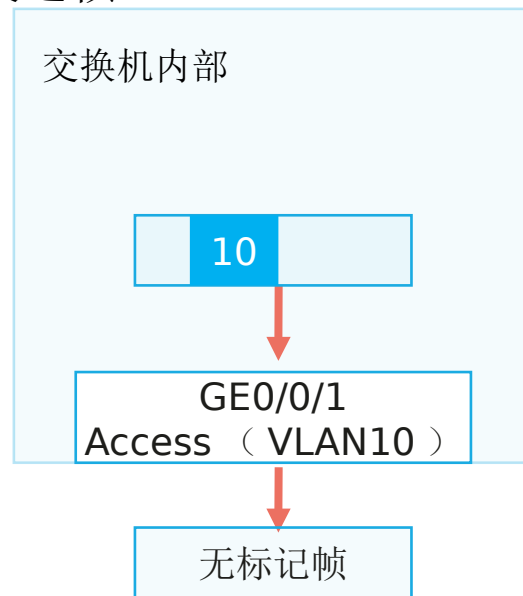
接收帧 发送帧



接口收到 **Untagged** 帧：
接收该帧，并打上该接口 PVID 的 Tag 。



接口收到 **Tagged** 帧：
当该帧的 VLAN ID 与该接口的 PVID 相同时，接收该帧。
当该帧的 VLAN ID 与该接口的 PVID 不同时，丢弃该帧。



帧的 **VLAN ID** 与接口 **PVID** 相同：
先剥离该帧的 Tag ，然后再将其从该接口发出。



帧的 **VLAN ID** 与接口 **PVID** 不同：
禁止将该帧从该接口发出。

无标记帧

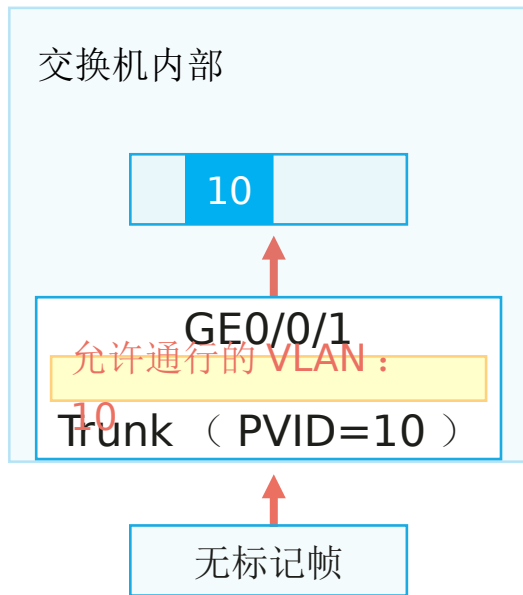
10 标记帧



Trunk 接口

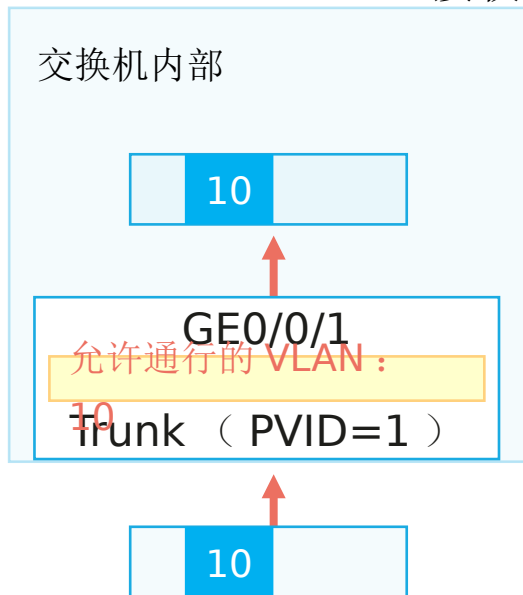
接收帧

发送帧



接口收到 **Untagged** 帧:

该帧打上 PVID , 当 PVID 在该接口允许通过的 VLAN 列表里时接收该帧; 当 PVID 不在允许通过的 VLAN 列表里时, 丢弃该帧。

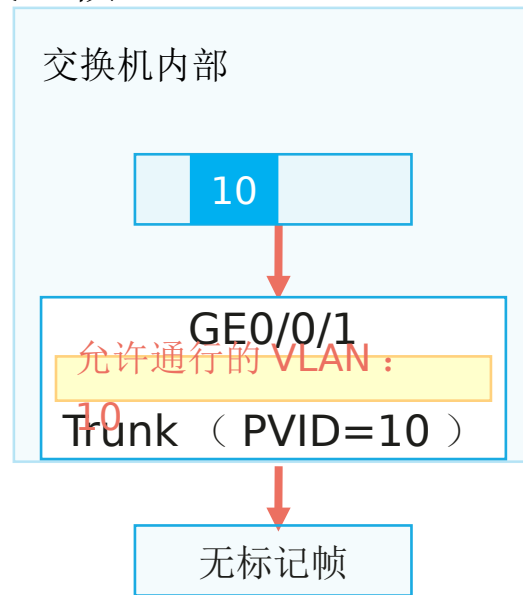


接口收到 **Tagged** 帧:

当该帧的 VLAN ID 在该接口允许通过的 VLAN 列表里时, 接收该帧, 否则丢弃该帧。

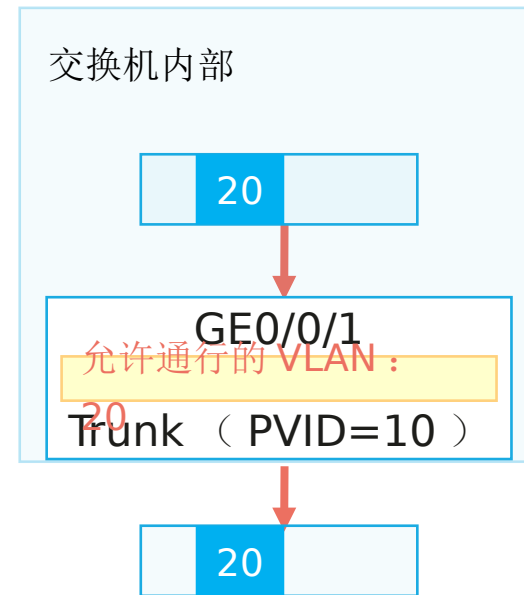
无标记帧

10 标记帧



帧的 **VLAN ID** 与接口 **PVID** 相同:

当该帧的 VLAN ID 在该接口允许通过的 VLAN 列表中, 则将该帧的 Tag 剥除, 然后将其从该接口发送出去; 如果 VLAN ID 不在允许通过的 VLAN 列表中则禁止将该帧从该接口发出。



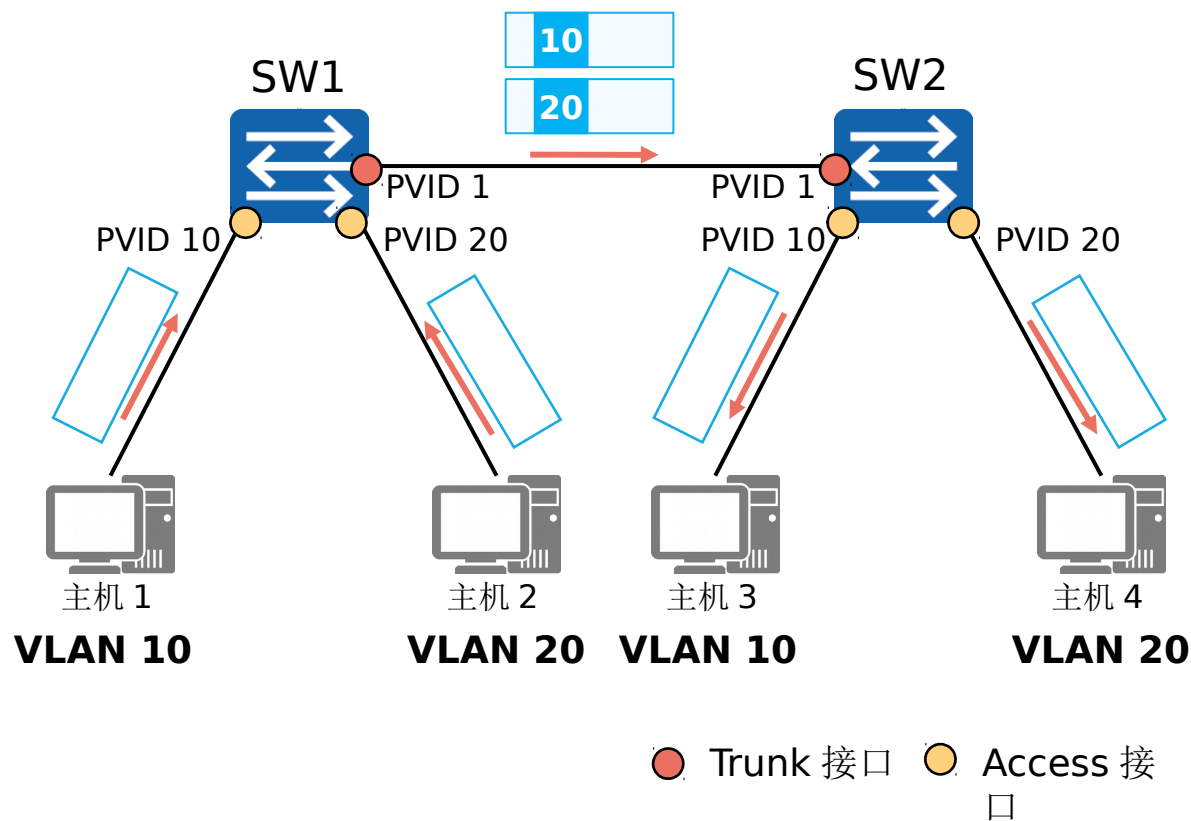
帧的 **VLAN ID** 与接口 **PVID** 不同:

当该帧的 VLAN ID 在该接口允许通过的 VLAN 列表中, 则保留该帧的 Tag , 然后将其从该接口发送出去; 如果 VLAN ID 不在允许通过的 VLAN 列表中则禁止将该帧从该接口发出。



Access 接口与 Trunk 接口举例

- 请描述主机之间数据访问的全流程。



SW1 与 SW2 的 Trunk 接

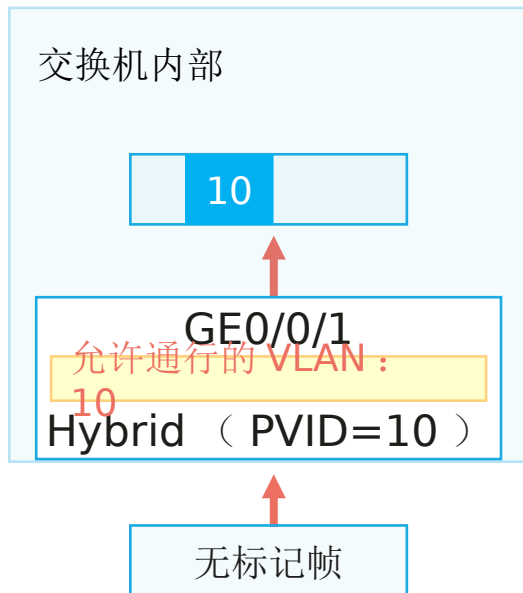
允许通过列表	
VLAN ID	1
	10
	20



Hybrid 接口

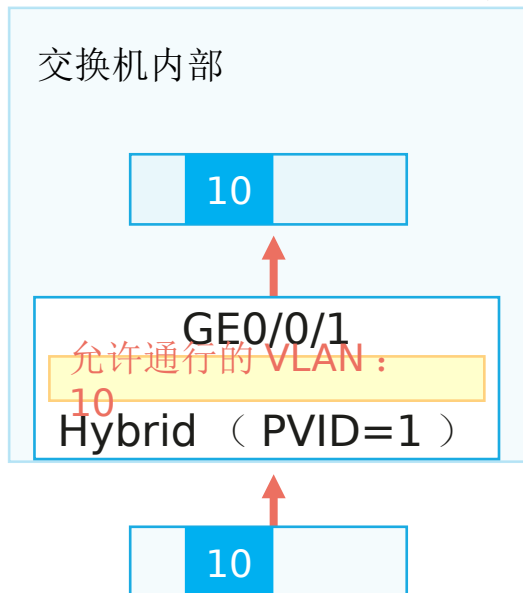
接收帧

发送帧



接口收到 **Untagged** 帧:

打上 PVID , 当 PVID 在该接口允许通过的 VLAN 列表里时接收该帧; 当 PVID 不在允许通过的 VLAN 列表里时, 丢弃该帧。

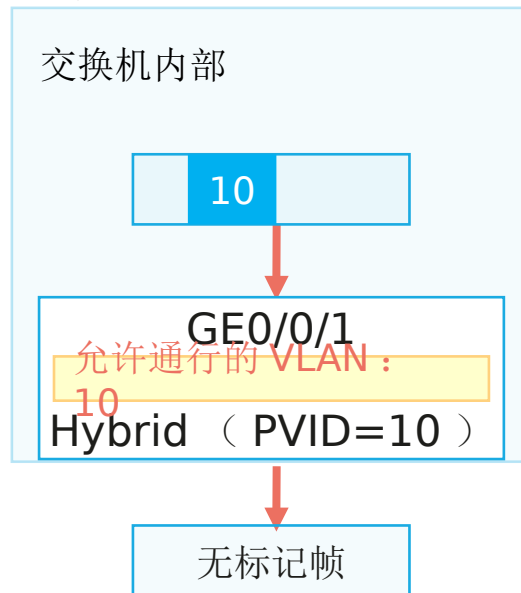


接口收到 **Tagged** 帧:

当该帧的 VLAN ID 在该接口允许通过的 VLAN 列表里时, 接收该帧, 否则丢弃该帧。

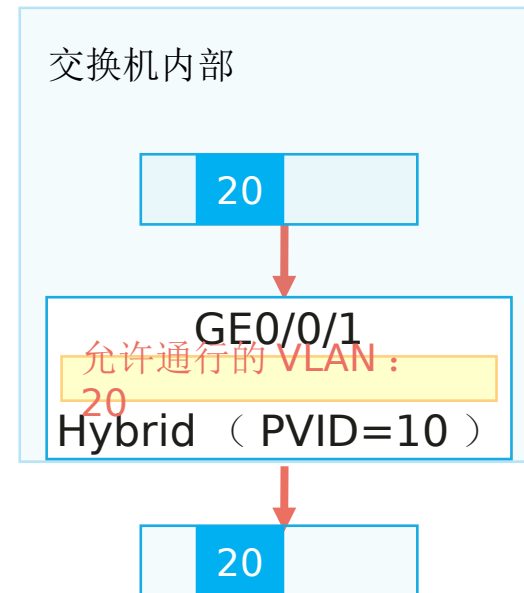
无标记帧

10 标记帧



帧的 **VLAN ID** 是该接口允许通过的 **VLAN ID** :

当管理员通过命令设置发送该 VLAN 的帧时不携带 Tag , 则将该帧的 Tag 剥除, 然后将其从该接口发送出。



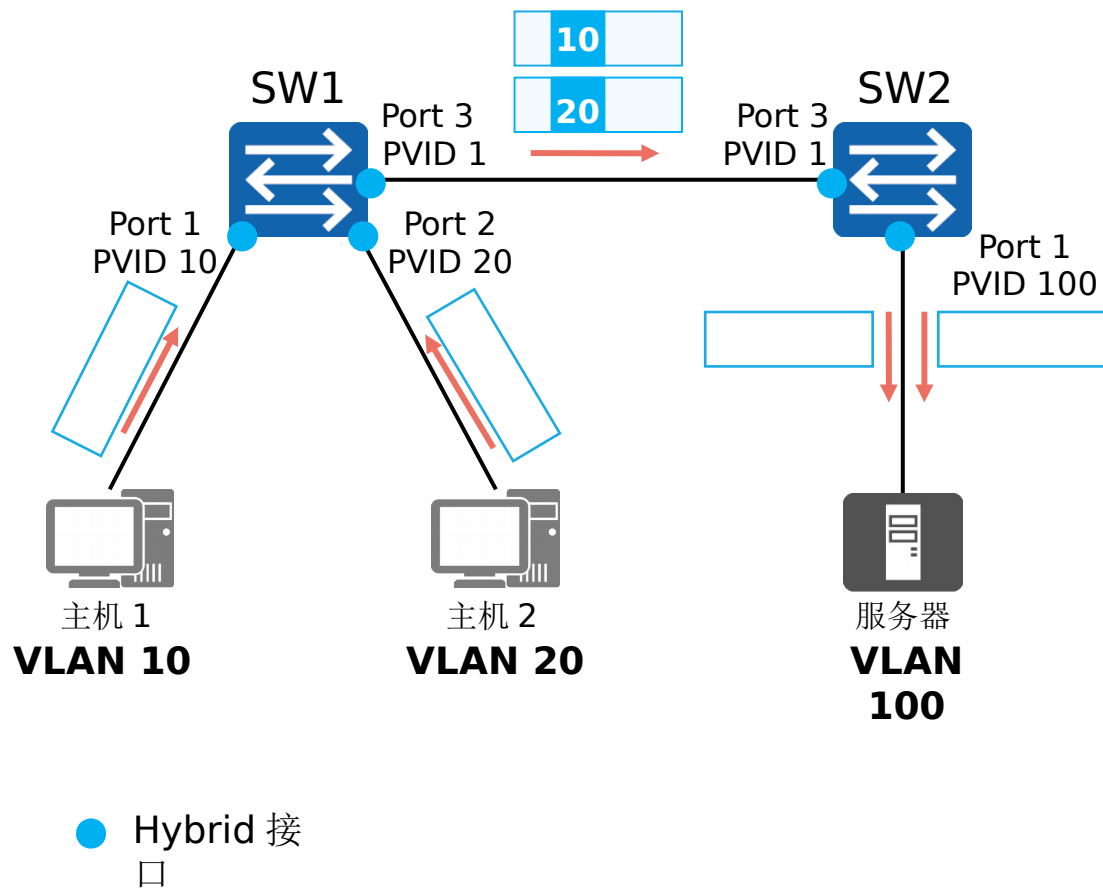
帧的 **VLAN ID** 是该接口允许通过的 **VLAN ID** :

当管理员通过命令设置发送该 VLAN 的帧时携带 Tag , 则保留该帧的 Tag , 然后将其从该接口发送出去。



Hybrid 接口举例

- 请描述主机访问服务器的全流程。



交换机 1 的允许通过列表

Port1	Port2	Port3
Untagged	Untagged	Tagged
VLAN ID	VLAN ID	VLAN ID
1	1	10
10	20	10
100	100	100

交换机 2 的允许通过列表

Port1	Port3
Untagged	Tagged
VLAN ID	VLAN ID
1	10
10	20
20	100
100	



小结

Access 接口

接收数据帧

- **Untagged** 数据帧，打上 **PVID**，接收。
- **Tagged** 数据帧，与 **PVID** 比较，相同则接收；不同则丢弃。

发送数据帧

- **VID** 与 **PVID** 比较，相同则剥离标签发送；不同则丢弃。

Trunk 接口

接收数据帧

- **Untagged** 数据帧，打上 **PVID**，且 **VID** 在允许列表中，则接收；**VID** 不在允许列表，则丢弃。
- **Tagged** 数据帧，查看 **VID** 是否在允许列表中，在允许列表中，则接收；**VID** 不在允许列表，则丢弃。

发送数据帧

- **VID** 在允许列表中，且 **VID** 与 **PVID** 一致，则剥离标签发送。
- **VID** 在允许列表，但 **VID** 与 **PVID** 不一致，则直接带标签发送。
- 不在允许列表中，则直接丢弃。

Hybrid 接口

接收数据帧

- **Untagged** 数据帧，打上 **PVID**，且 **VID** 在允许列表中，则接收；**VID** 不在允许列表中，则丢弃。
- **Tagged** 数据帧，查看 **VID** 是否在允许列表中，在允许列表中，则接收；**VID** 不在允许列表，则丢弃。

发送数据帧

- **VID** 不在允许列表中，直接丢弃。
- **VID** 在 **Untagged** 列表中，剥离标签发送。
- **VID** 在 **Tagged** 列表中，带标签直接发送。



目录

1. 什么是 VLAN
2. VLAN 的基本原理
- 3. VLAN 的应用**
4. VLAN 的配置示例



VLAN 的规划

- **VLAN 分配原则**

- 按业务规划：可分为语音、视频和数据。
- 按部门规划：可分为工程部、市场部、财经部等。
- 按应用规划：可分为服务器、办公、教室等。

- **VLAN 分配技巧**

VLAN ID 的分配在有效范围内，可以随意分配和选取，但是为了提高 VLAN ID 的连续性，可以采用 VLAN ID 和子网关联的方式进行分配。

- **VLAN 规划示例**

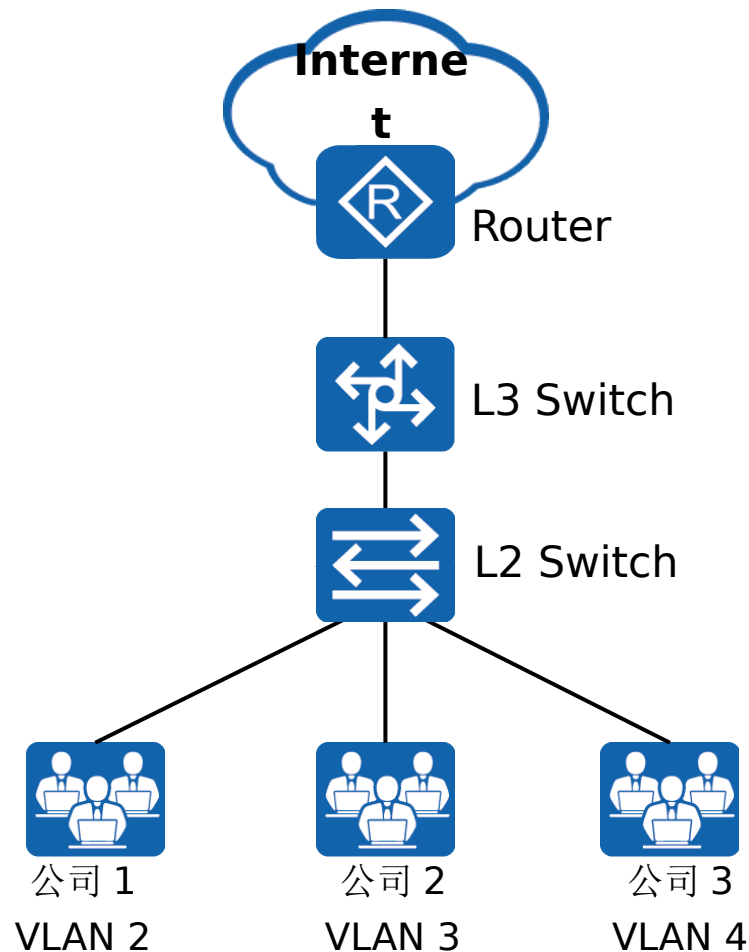
- 假设某园区有三栋楼，分别为行政楼、教学楼、办公楼；每栋楼各有 1 台接入交换机，核心交换机在行政楼；行政楼内有办公室、财务部和教室；办公楼内有办公室和财务部；教学楼内有办公室和教室。
- VLAN 规划如下：

VLAN	IP 地址段	描述
1	X.16.10.0/24	办公室用户所属的 VLAN
2	X.16.20.0/24	财务部用户所属的 VLAN
3	X.16.30.0/24	教室用户所属的 VLAN
100	Y.16.100.0/24	设备管理所属的 VLAN



应用场景 - 基于接口的 VLAN 划分

- 应用场景：
 - 某商务楼内有多家公司，为了降低成本，多家公司共用网络资源，各公司分别连接到一台二层交换机的不同接口，并通过统一的出口访问 Internet。
- VLAN 划分：
 - 为了保证各公司业务独立和安全，可将每个公司所连接的接口划分到不同的 **VLAN**，实现公司间业务数据的完全隔离。可以认为每个公司拥有独立的网络，每个 **VLAN** 就是一个“虚拟工作区”。





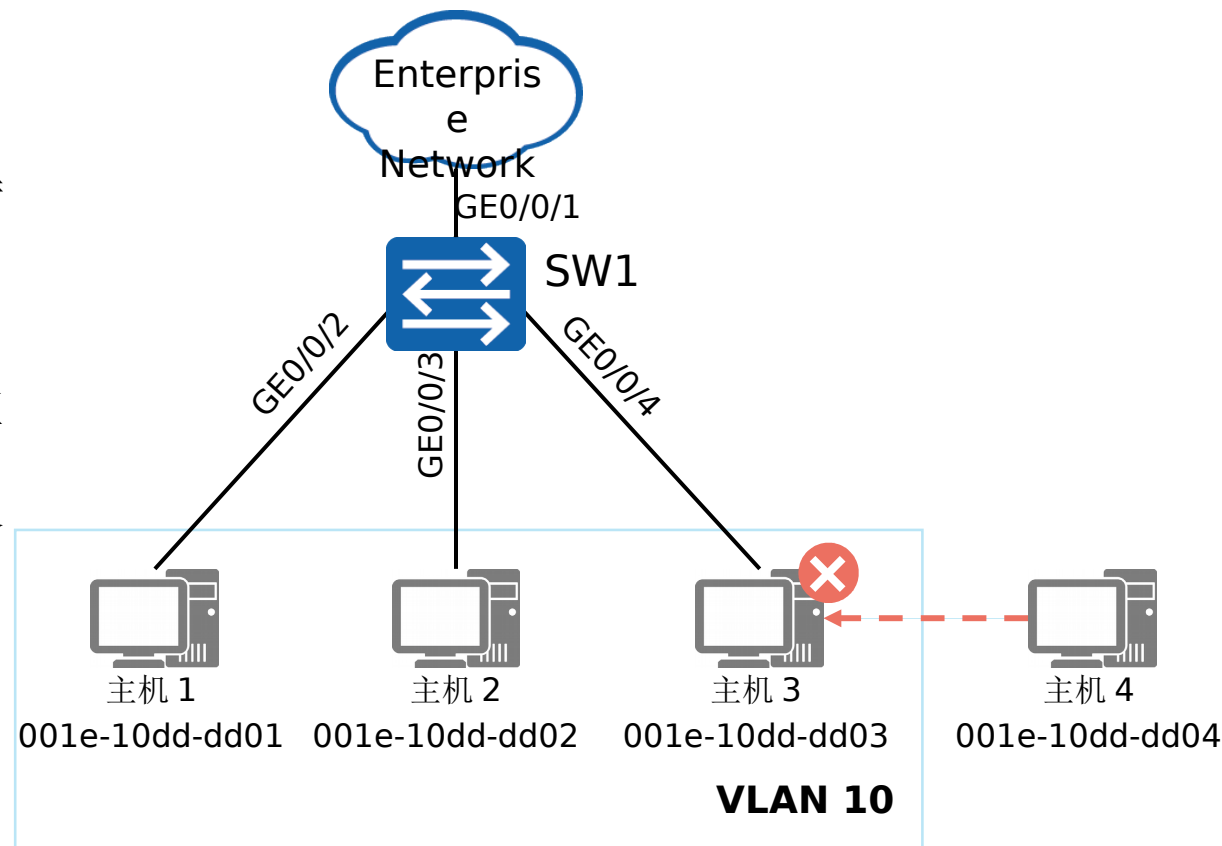
应用场景 - 基于 MAC 的 VLAN 划分

- 应用场景：

- 某个公司的网络中，网络管理者将同一部门的员工划分到同一 **VLAN**。为了提高部门内的信息安全，要求只有本部门员工的主机才可以访问特定网□ □ 源□。

- VLAN 划分：

- 为了保证非本部门员工不能访问网络资源，可在 **SW1** 上配置基于 **MAC 地址** 划分 **VLAN**。这样，新的主机接入网络，就无法访问公司的网络资源。





目录

1. 什么是 VLAN
2. VLAN 的基本原理
3. VLAN 的应用
- 4. VLAN 的配置示例**



VLAN 的基础配置命令

1. 创建 VLAN

```
[Huawei] vlan vlan-id
```

通过此命令创建 VLAN 并进入 VLAN 视图，如果 VLAN 已存在，直接进入该 VLAN 的视图。

- *vlan-id* 是整数形式，取值范围是 1 ~ 4094 。

```
[Huawei] vlan batch { vlan-id1 [ to vlan-id2 ] }
```

通过此命令批量创建 VLAN 。其中：

- **batch**：指定批量创建的 VLAN ID 。
- *vlan-id1*：表示第一个 VLAN 的编号。
- *vlan-id2*：表示最后一个 VLAN 的编号。



Access 接口的基础配置命令

1. 配置接口类型

```
[Huawei-GigabitEthernet0/0/1] port link-type access
```

在接口视图下，配置接口的链路类型为 Access。

2. 配置 Access 接口的缺省 VLAN

```
[Huawei-GigabitEthernet0/0/1] port default vlan vlan-id
```

在接口视图下，配置接口的缺省 VLAN 并同时加入这个 VLAN。

- *vlan-id*：配置缺省 VLAN 的编号。整数形式，取值范围是 1 ~ 4094。



Trunk 接口的基础配置命令

1. 配置接口类型

```
[Huawei-GigabitEthernet0/0/1] port link-type trunk
```

在接口视图下，配置接口的链路类型为 Trunk。

2. 配置 Trunk 接口加入指定 VLAN

```
[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } | all }
```

在接口视图下，配置 Trunk 类型接口加入的 VLAN。

3. （可选）配置 Trunk 接口的缺省 VLAN

```
[Huawei-GigabitEthernet0/0/1] port trunk pvid vlan vlan-id
```

在接口视图下，配置 Trunk 类型接口的缺省 VLAN。



Hybrid 接口的基础配置命令

1. 配置接口类型

```
[Huawei-GigabitEthernet0/0/1] port link-type hybrid
```

在接口视图下，配置接口的链路类型为 Hybrid。

2. 配置 Hybrid 接口加入指定 VLAN

```
[Huawei-GigabitEthernet0/0/1] port hybrid untagged vlan { { vlan-id1 [ to vlan-id2 ] } | all }
```

在接口视图下，配置 Hybrid 类型接口加入的 VLAN，这些 VLAN 的帧以 Untagged 方式通过接口。

```
[Huawei-GigabitEthernet0/0/1] port hybrid tagged vlan { { vlan-id1 [ to vlan-id2 ] } | all }
```

在接口视图下，配置 Hybrid 类型接口加入的 VLAN，这些 VLAN 的帧以 Tagged 方式通过接口。

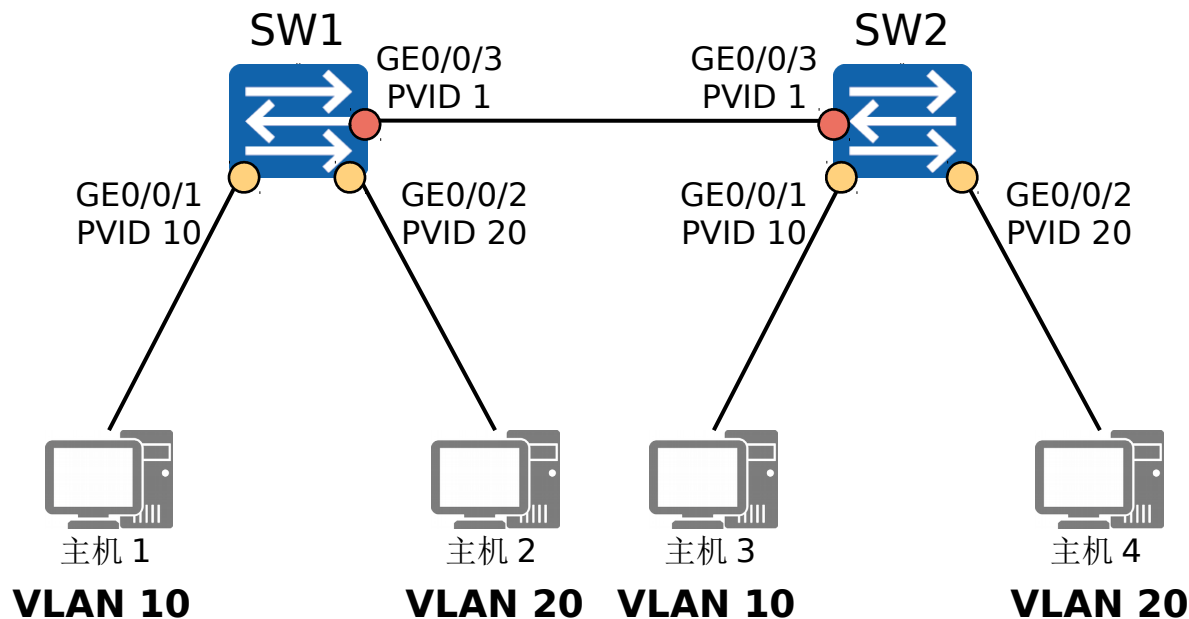
3. （可选）配置 Hybrid 接口的缺省 VLAN

```
[Huawei-GigabitEthernet0/0/1] port hybrid pvid vlan vlan-id
```

在接口视图下，配置 Hybrid 类型接口的缺省 VLAN。



案例 1：基于接口划分 VLAN



- Access 接口
-
- Trunk 接口

组网需求：

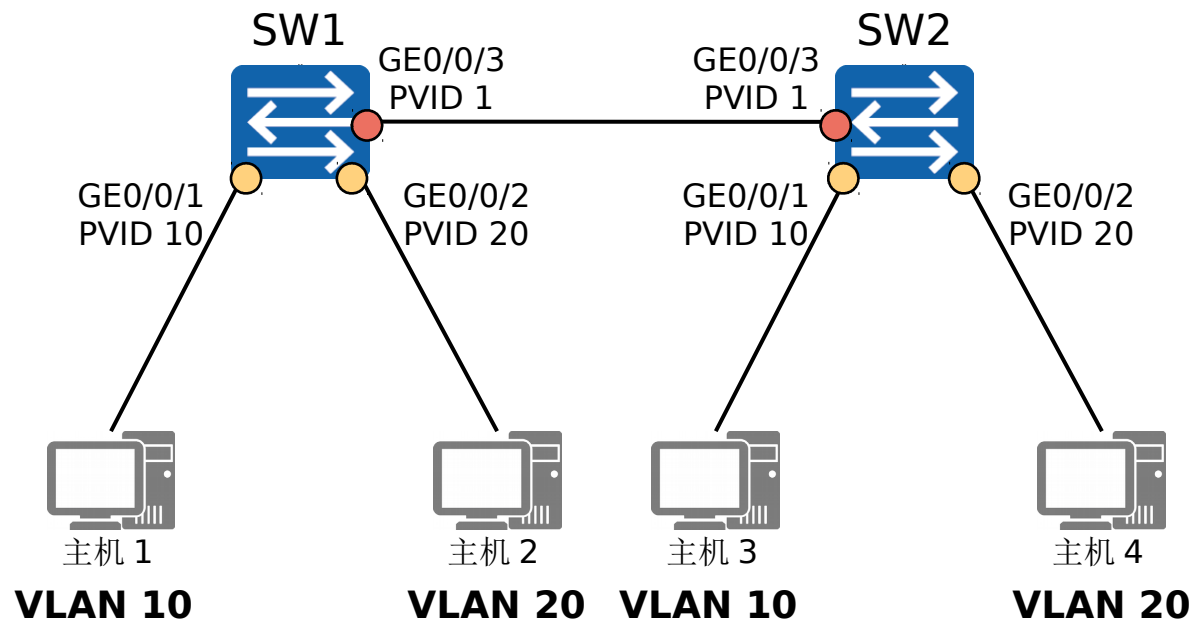
- 某企业的交换机连接有很多用户，且相同业务用户通过不同的设备接入企业网络。为了通信的安全性，企业希望业务相同用户之间可以互相访问，业务不同用户不能直接访问。
- 可以在交换机上配置基于接口划分 **VLAN**，把业务相同的用户连接的接口划分到同一 **VLAN**。这样属于不同 **VLAN** 的用户不能直接进行二层通信，同一 **VLAN** 内的用户可以直接互相通信。



创建 VLAN

基于接口划分 VLAN

基于 MAC 地址划分 VLAN



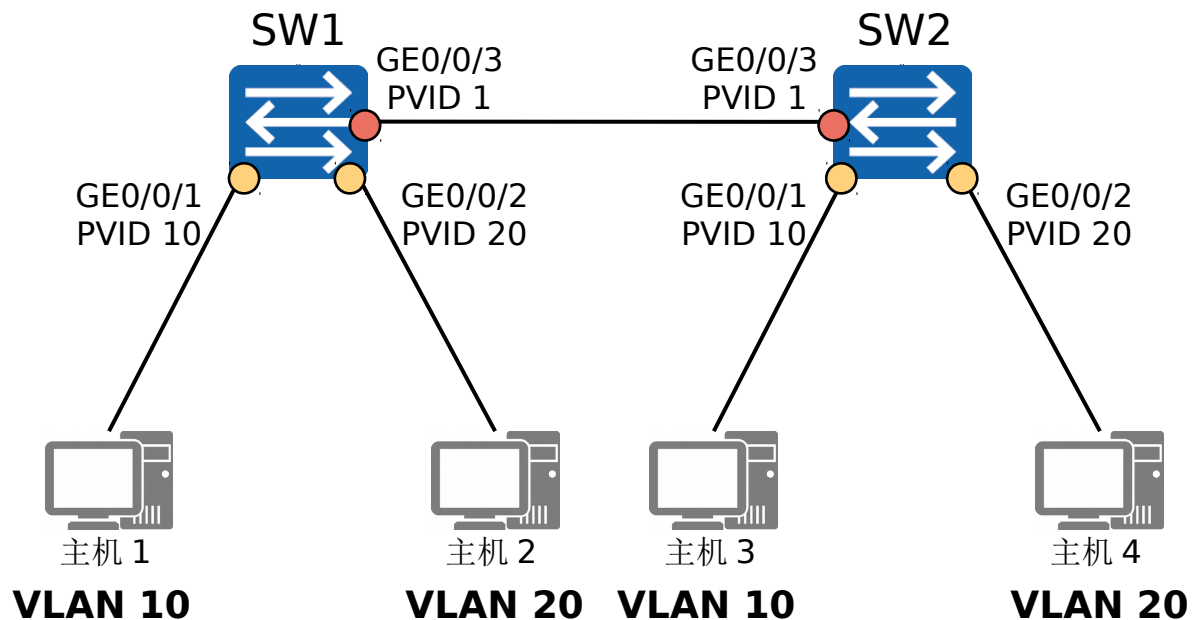
创建 VLAN :

```
[SW1] vlan 10  
[SW1-vlan10] quit  
[SW1] vlan 20  
[SW1-vlan20] quit
```

```
[SW2] vlan batch 10 20
```



配置 Access 接口和 Trunk 接口



配置 Access 接口，并加入对应的 VLAN：

```
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 10
```

```
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type access
[SW1] vlan 20
[SW1-vlan20] port GigabitEthernet0/0/2
[SW1-vlan20] quit
```

配置 Trunk 接口，并创建对应的允许通过列表：

```
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type trunk
[SW1-GigabitEthernet0/0/3] port trunk pvid vlan 1
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan
10 20
```

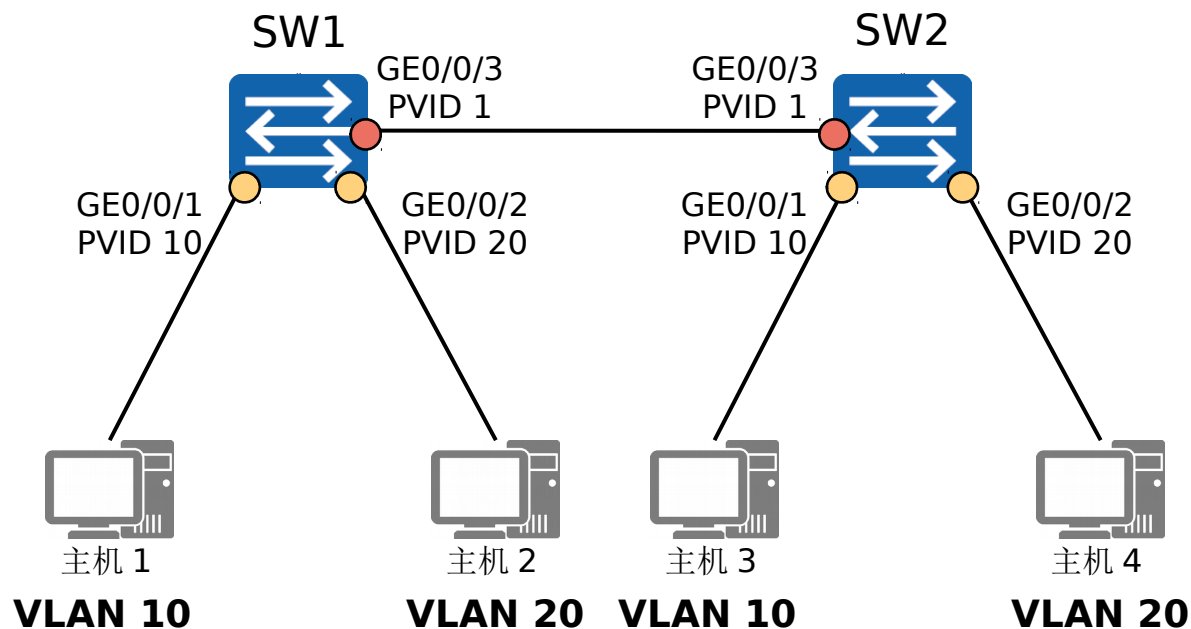
类似



验证配置

基于接口划分 VLAN

基于 MAC 地址划分 VLAN



[SW1]display vlan

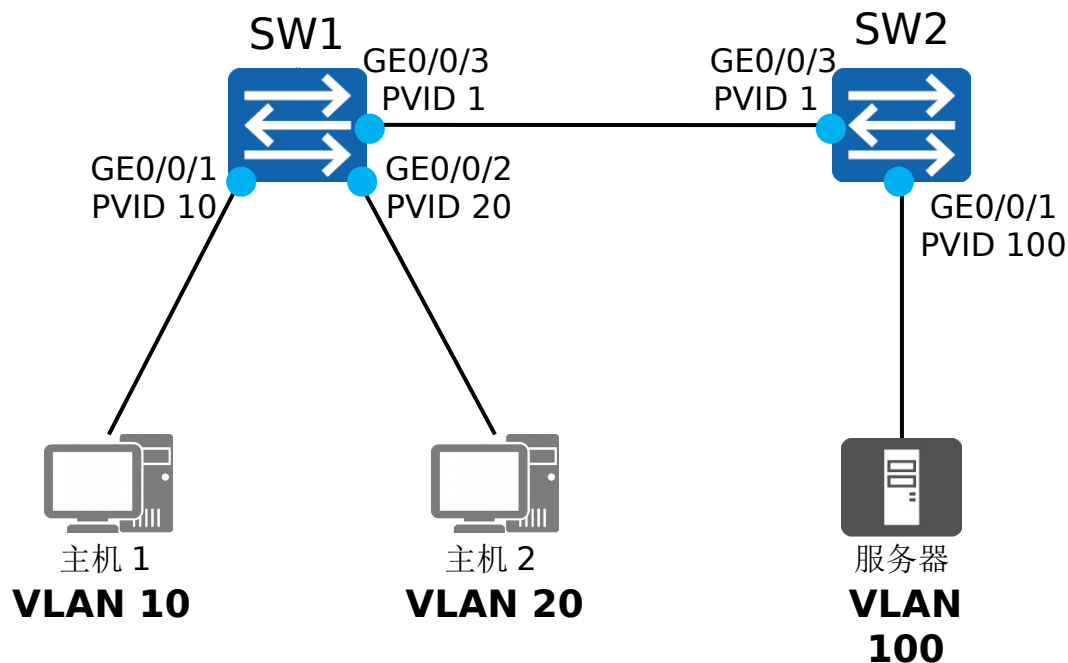
The total number of vlans is : 3

U: Up; D: Down; TG: Tagged; UT: Untagged;
MP: Vlan-mapping; ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;

VID	Type	Ports
1	common	UT:GE0/0/3(U)
10	common	UT:GE0/0/1(U) TG:GE0/0/3(U)
20	common	UT:GE0/0/2(U) TG:GE0/0/3(U)
.....		



案例 2：基于接口划分 VLAN



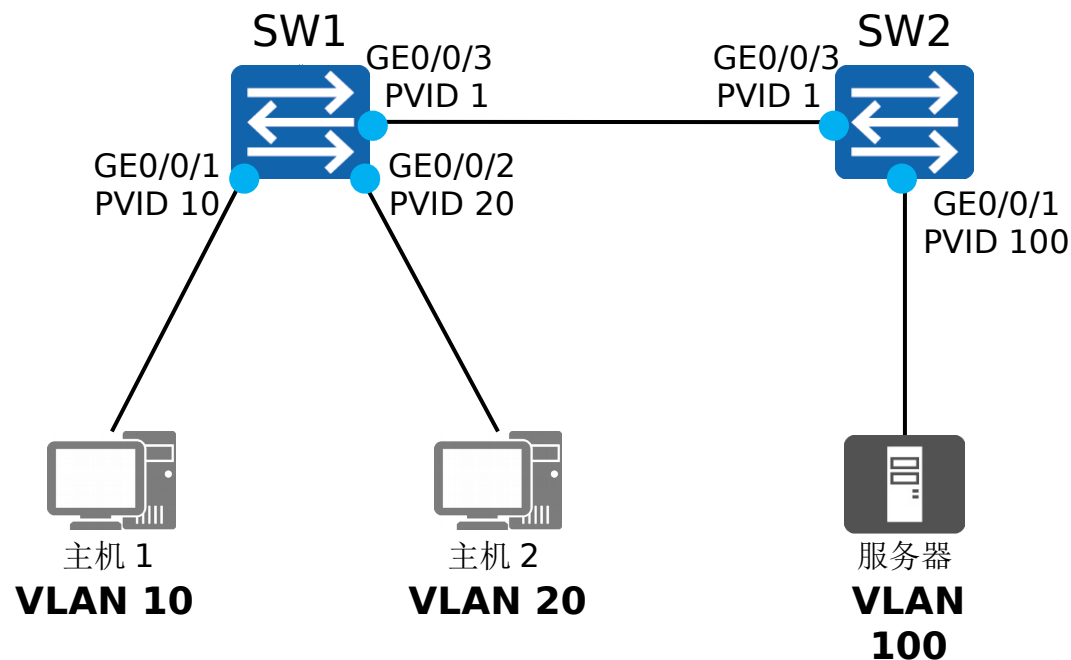
● Hybrid 接口

组网需求：

- 某企业的交换机连接有很多用户，且不同部门的用户都需要访问公司服务器。但是为了通信的安全性，企业希望不同部门的用户不能直接访问。
- 可以在交换机上配置基于接口划分 **VLAN**，并配置 **Hybrid** 接口，使得不同部门的用户不能直接进行二层通信，但都可以直接访问公司服务器。



Hybrid 接口的基础配置 (1)

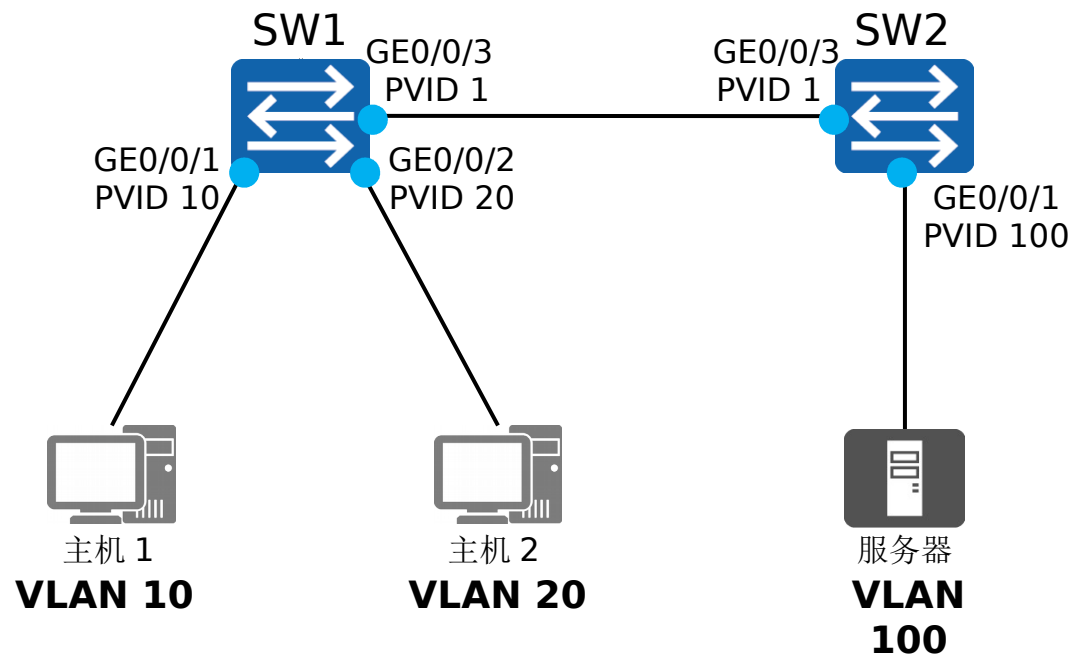


SW1 的配置如下:

```
[SW1] vlan batch 10 20 100
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type hybrid
[SW1-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SW1-GigabitEthernet0/0/1] port hybrid untagged vlan 10 100
[SW1-GigabitEthernet0/0/1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type hybrid
[SW1-GigabitEthernet0/0/2] port hybrid pvid vlan 20
[SW1-GigabitEthernet0/0/2] port hybrid untagged vlan 20 100
[SW1-GigabitEthernet0/0/2] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type hybrid
[SW1-GigabitEthernet0/0/3] port hybrid tagged vlan 10 20 100
```



Hybrid 接口的基础配置 (2)

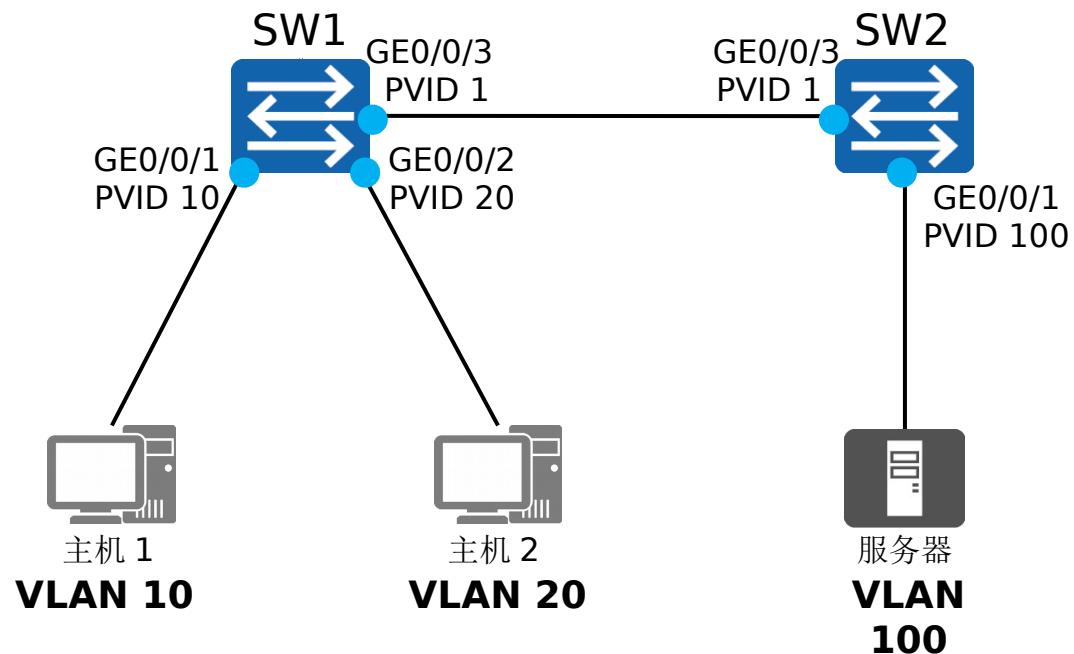


SW2 的配置如下:

```
[SW2] vlan batch 10 20 100
[SW2] interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1] port link-type hybrid
[SW2-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SW2-GigabitEthernet0/0/1] port hybrid untagged vlan 10 20 100
[SW2-GigabitEthernet0/0/1] interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/3] port link-type hybrid
[SW2-GigabitEthernet0/0/3] port hybrid tagged vlan 10 20 100
```



验证配置



```
[SW1]display vlan
```

The total number of vlans is : 4

U: Up; D: Down; TG: Tagged; UT: Untagged;
MP: Vlan-mapping; ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;

VID	Type	Ports
1	common	UT:GE0/0/1(U) GE0/0/2(U) GE0/0/3(U)
10	common	UT:GE0/0/1(U) TG:GE0/0/3(U)
20	common	UT:GE0/0/2(U) TG:GE0/0/3(U)
100	common	UT:GE0/0/1(U) GE0/0/2(U) TG:GE0/0/3(U)

.....



VLAN 的基础配置命令

1. 关联 MAC 地址与 VLAN

```
[Huawei-vlan10] mac-vlan mac-address mac-address [ mac-address-mask | mac-address-mask-length ]
```

通过此命令配置 MAC 地址与 VLAN 关联。

- **mac-address**：指定与 VLAN 关联的 MAC 地址。格式为 H-H-H。其中 H 为 4 位的十六进制数，可以输入 1 ~ 4 位，如 00e0、fc01。当输入不足 4 位时，表示前面的几位为 0，如：输入 e0，等同于 00e0。MAC 地址不可设置为 0000-0000-0000、FFFF-FFFF-FFFF 和组播地址。
- **mac-address-mask**：指定 MAC 地址掩码。格式为 H-H-H，其中 H 为 1 至 4 位的十六进制数。
- **mac-address-mask-length**：指定 MAC 地址掩码长度。整数形式，取值范围是 1 ~ 48。

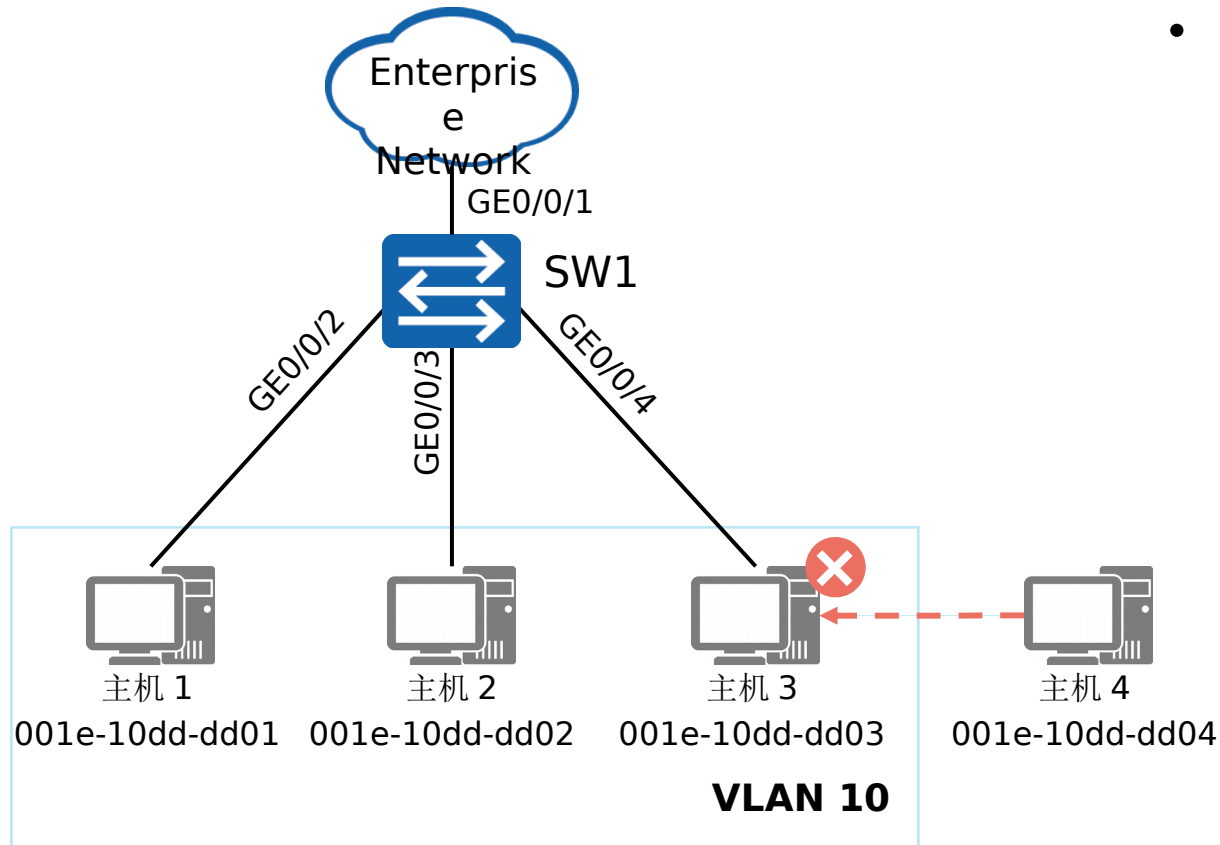
2. 使能 MAC 地址与 VLAN

```
[Huawei-GigabitEthernet0/0/1] mac-vlan enable
```

通过此命令使能接口的 MAC VLAN 功能。



案例：基于 MAC 地址划分 VLAN

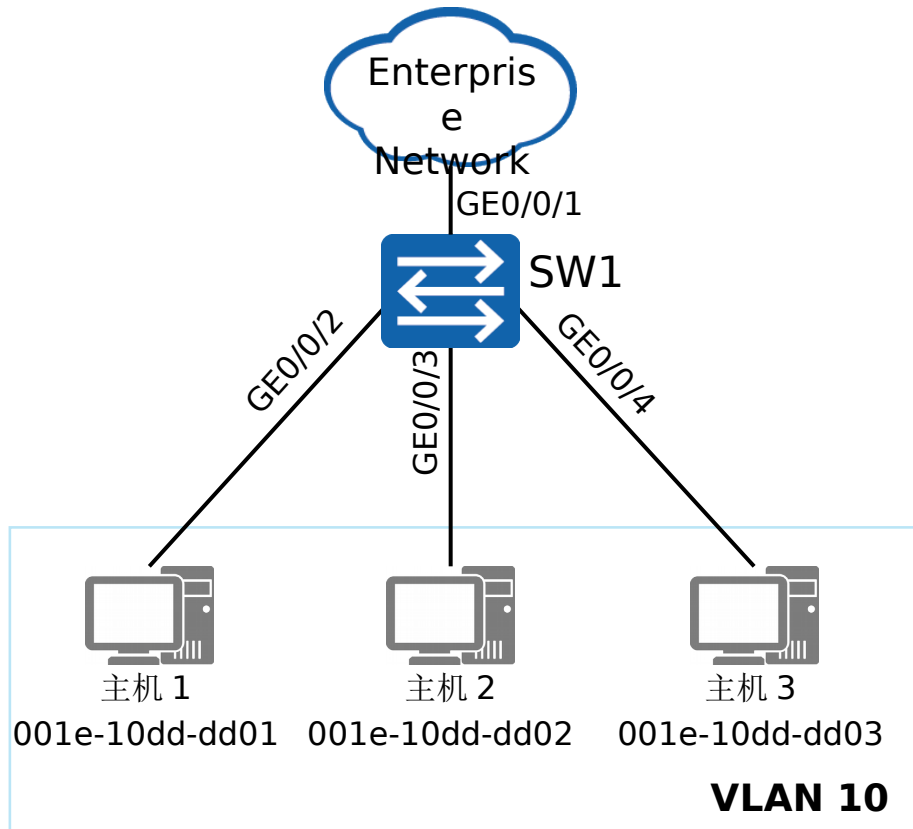


- 组网需求：

- 某个公司的网络中，网络管理者将同一部门的员工划分到同一 **VLAN**。为了提高部门内的信息安全，要求只有本部门员工的主机才可以访问公司网络。
- 主机 1、主机 2、主机 3 为本部门员工的主机，要求这几台主机可以通过 **SW1** 访问公司网络，如换成其他主机则不能访问。
- 可以配置基于 **MAC 地址划分 VLAN**，将本部门员工主机的 **MAC 地址与 VLAN 绑定**，从而实现 □ 需求。



创建 **VLAN**，并关联 **MAC** 地址和 **VLAN**



创建 **VLAN**：

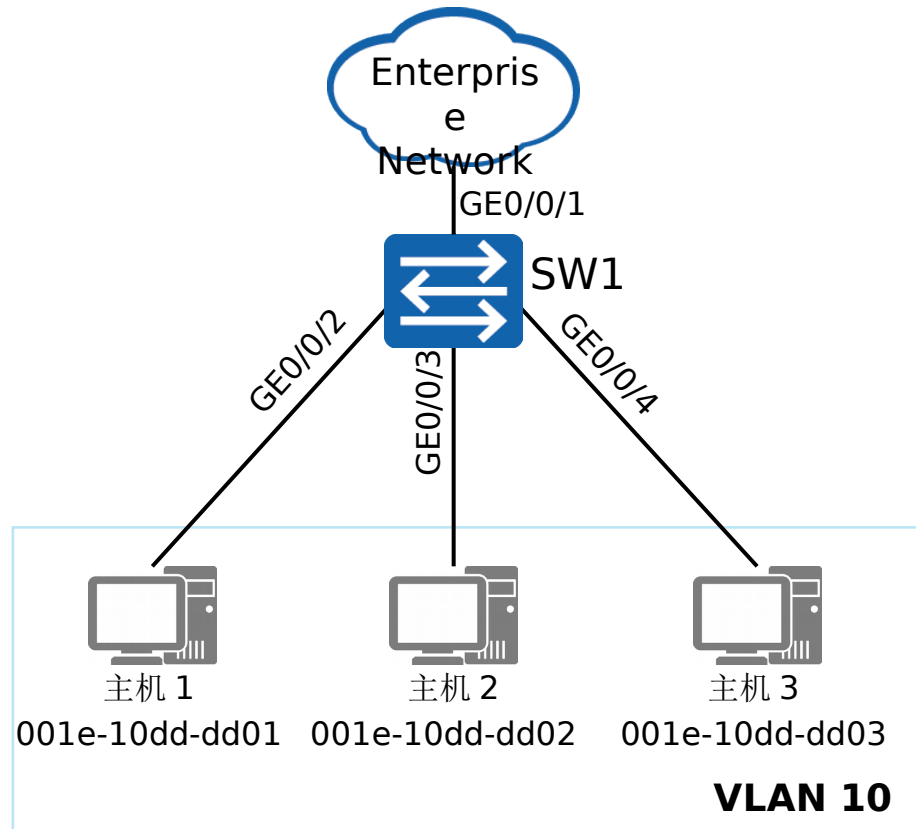
```
[SW1] vlan 10  
[SW1-vlan10] quit
```

关联 **MAC** 地址和 **VLAN**：

```
[SW1] vlan 10  
[SW1-vlan10] mac-vlan mac-address 001e-10dd-dd01  
[SW1-vlan10] mac-vlan mac-address 001e-10dd-dd02  
[SW1-vlan10] mac-vlan mac-address 001e-10dd-dd03  
[SW1-vlan10] quit
```




加入 VLAN，并使能 MAC VLAN 功能



加入 VLAN：

```
[SW1] interface gigabitethernet 0/0/1  
[SW1-GigabitEthernet0/0/1] port link-type hybrid  
[SW1-GigabitEthernet0/0/1] port hybrid tagged vlan 10
```

```
[SW1] interface gigabitethernet 0/0/2  
[SW1-GigabitEthernet0/0/2] port link-type hybrid  
[SW1-GigabitEthernet0/0/2] port hybrid untagged vlan 10
```

使能接口的基于 MAC 地址划分 VLAN 功能：

```
[SW1] interface gigabitethernet 0/0/2  
[SW1-GigabitEthernet0/0/2] mac-vlan enable  
[SW1-GigabitEthernet0/0/2] quit
```

注：GE0/0/3、GE0/0/4 的配置与 GE0/0/2 类似



验证配置

```
[SW1]display vlan
```

```
The total number of vlans is : 2
```

```
-----
U: Up;      D: Down;      TG: Tagged; UT: Untagged;
MP: Vlan-mapping;      ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;
-----
```

```
VID  Type  Ports
```

```
-----
1    common  UT:GE0/0/1(U)  GE0/0/2(U) GE0/0/3(U) .....
10   common  UT:GE0/0/2(U)  GE0/0/3(U) GE0/0/4(U)
                TG:GE0/0/1(U)
.....
```

```
[SW1]display mac-vlan mac-address all
```

```
-----
MAC Address      MASK VLAN Priority
```

```
-----
001e-10dd-dd01  ffff-ffff-ffff  10    0
001e-10dd-dd02  ffff-ffff-ffff  10    0
001e-10dd-dd03  ffff-ffff-ffff  10    0
```

```
Total MAC VLAN address count: 3
```



思考题

1. （多选）下列关于 VLAN 的描述中，错误的是？（ ）
 - A. VLAN 技术可以将一个规模较大的冲突域隔离成若干个规模较小的冲突域
 - B. VLAN 技术可以将一个规模较大的二层广播域隔离成若干个规模较小的二层广播域
 - C. 位于不同 VLAN 的计算机之间无法进行通信
 - D. 位于同一 VLAN 中的计算机之间可以进行二层通信
2. 如果一个 Trunk 接口的 PVID 是 5，且端口下配置 `port trunk allow-pass vlan 2 3`，那么哪些 VLAN 的流量可以通过该 Trunk 接口进行传输？

The background of the slide features a blue-tinted image of several business professionals in a modern office. They are standing in groups, some looking at documents or devices, and their reflections are visible on the glossy floor. The overall aesthetic is professional and corporate.

谢谢

www.huawei.com