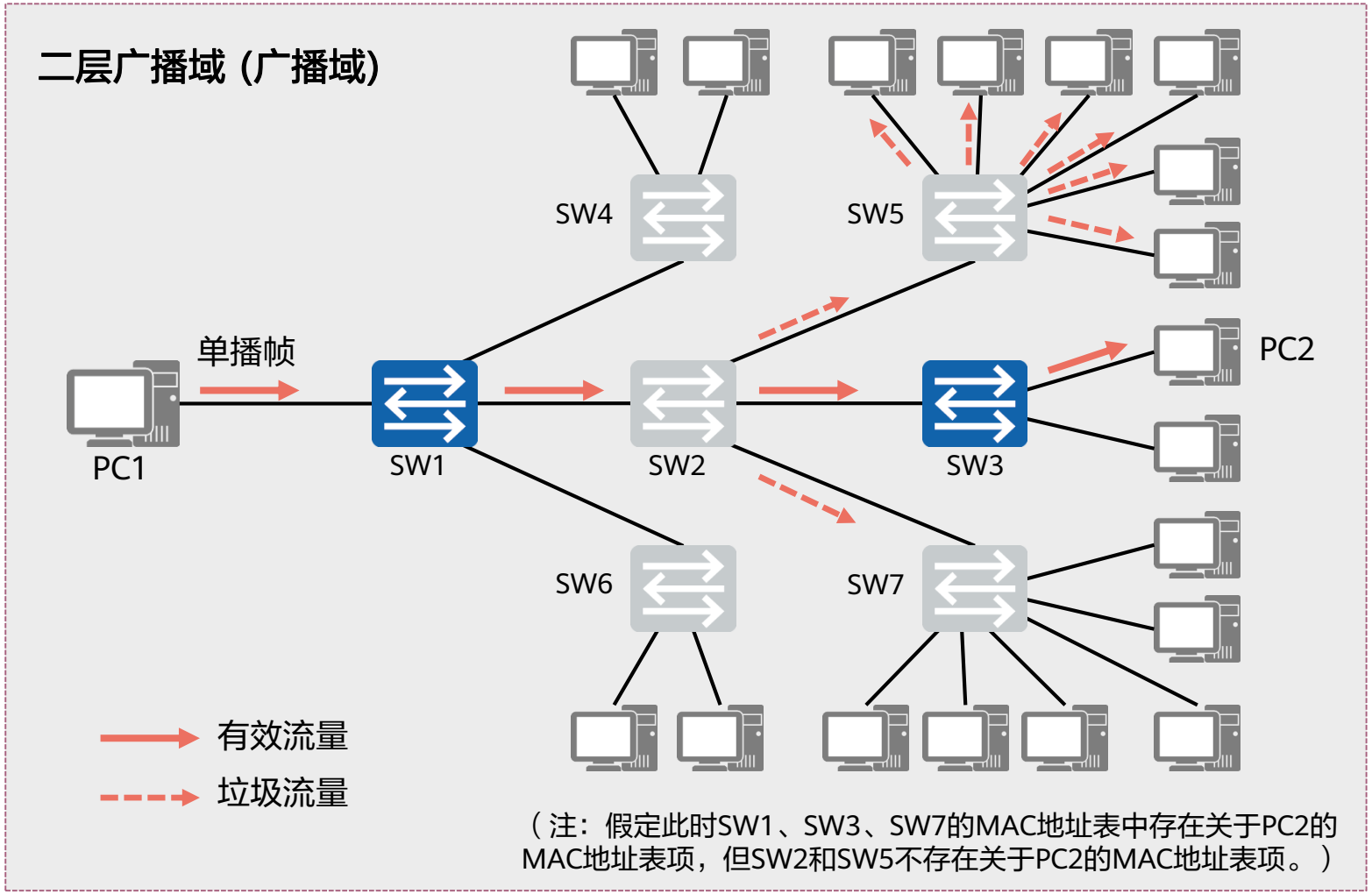
VLAN原理与配置

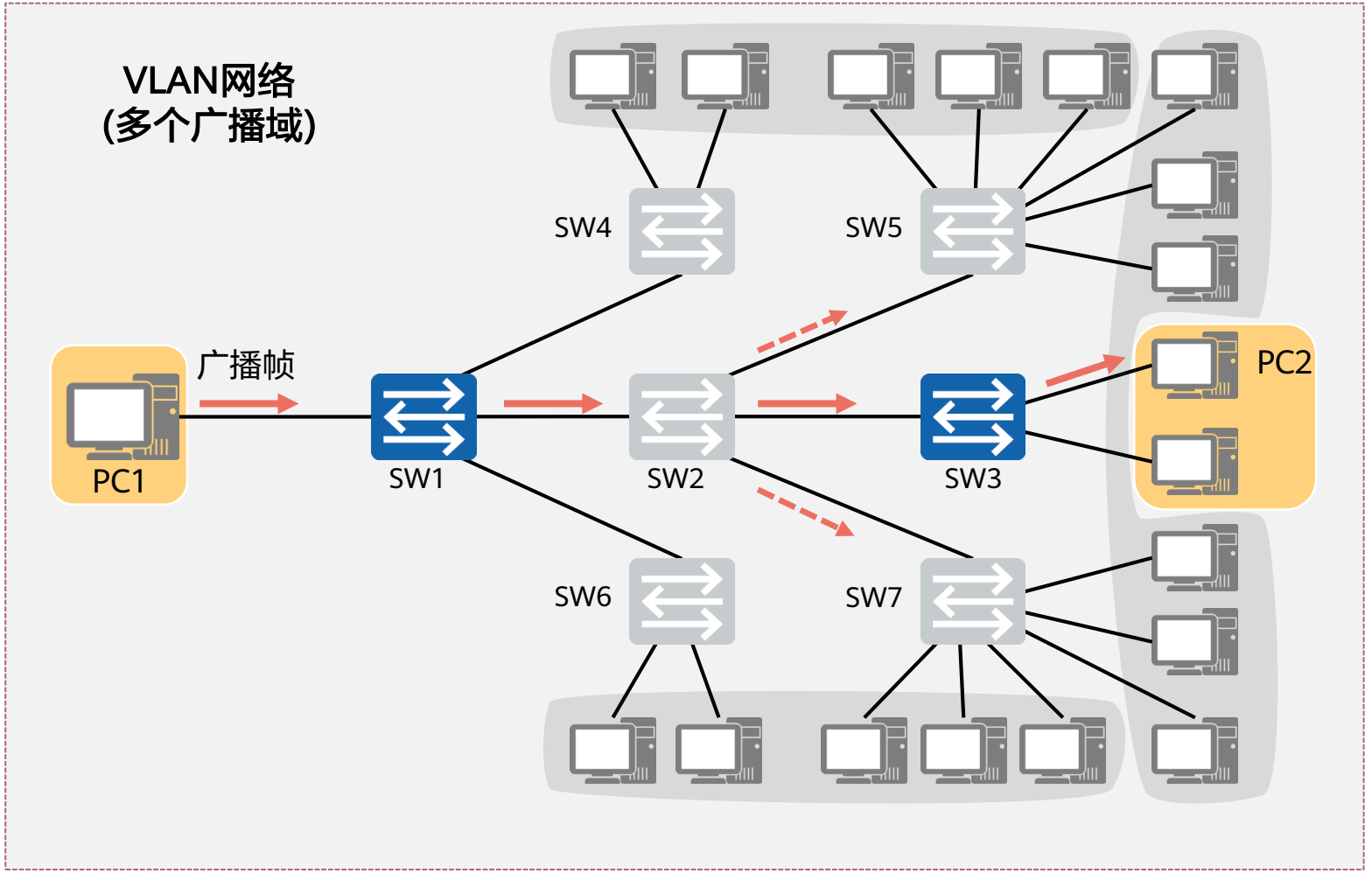
主讲人：鲍婷婷

目录

传统以太网的问题

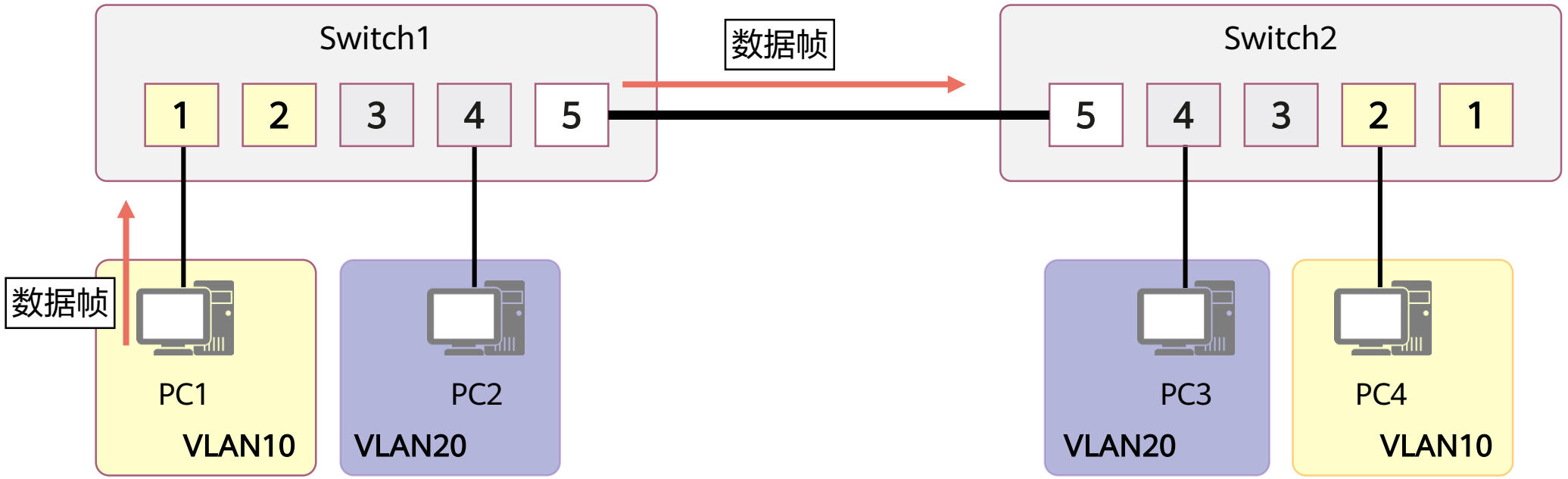


虚拟局域网（VLAN,Virtual LAN）



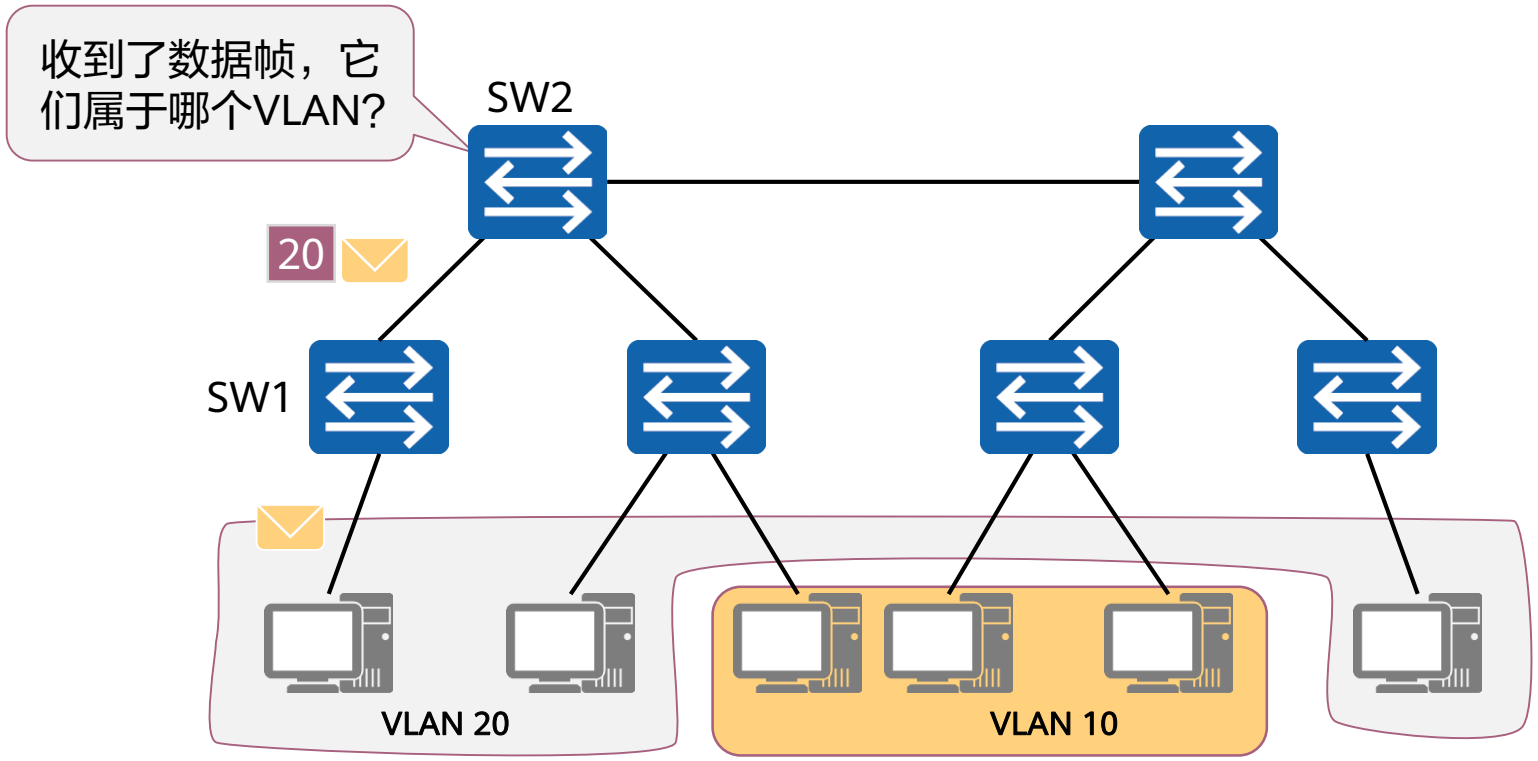
目录

如何实现VLAN



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

- 报文中添加标识VLAN信息的字段使交换机能够分辨不同VLAN的报文。
- 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）

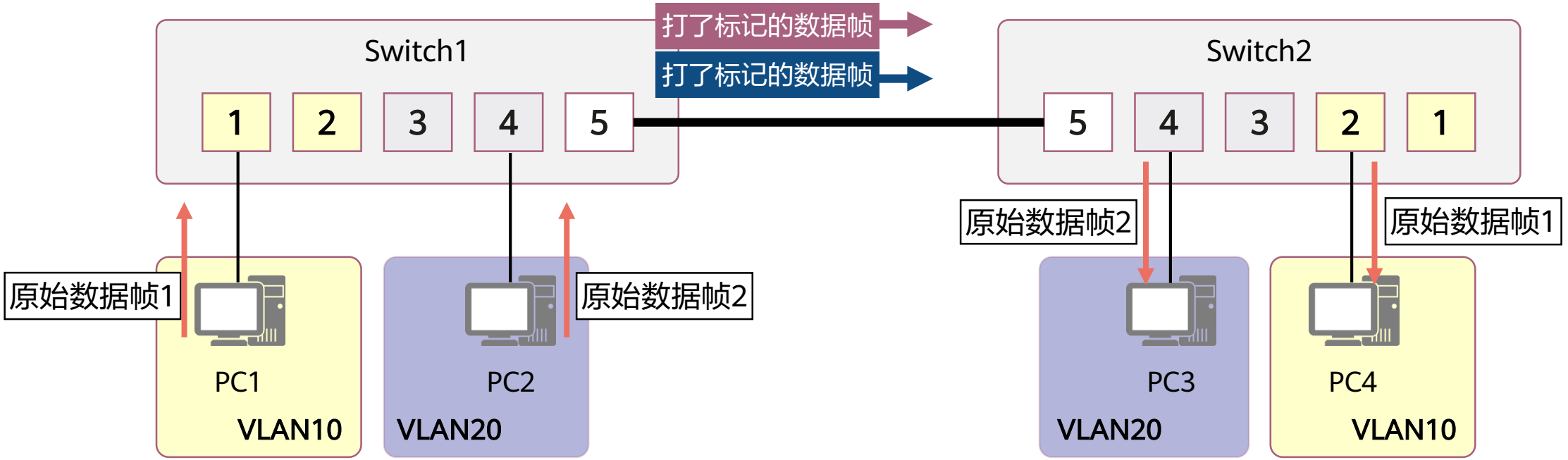
在此处插入802.1Q Tag

802.1QTag

- TPID（标签协议标识符）
- PRI（优先级）
- CFI（标准格式指示符）
- VLAN ID（VLAN标识符）

802.1Q帧
（标记帧，Tagged帧）

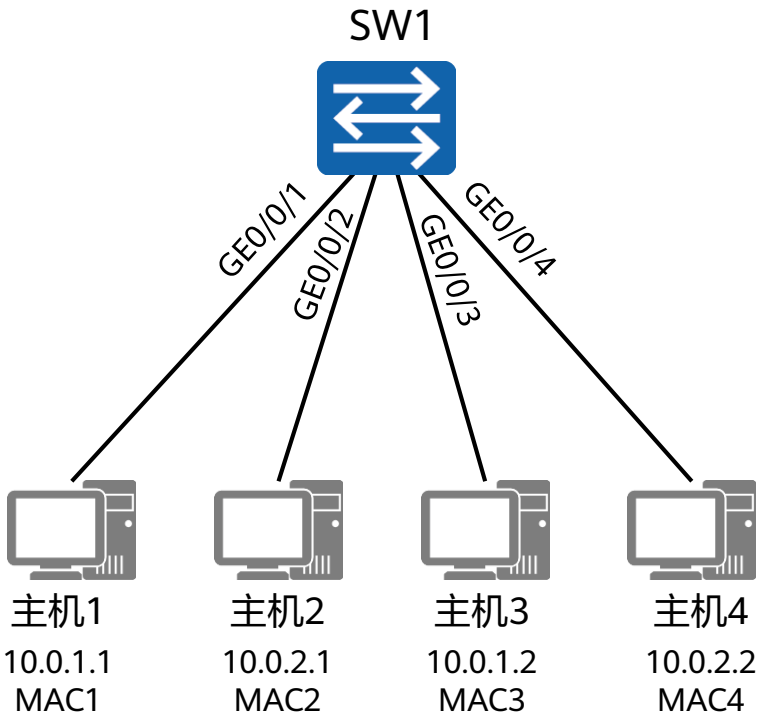
VLAN的实现



目录

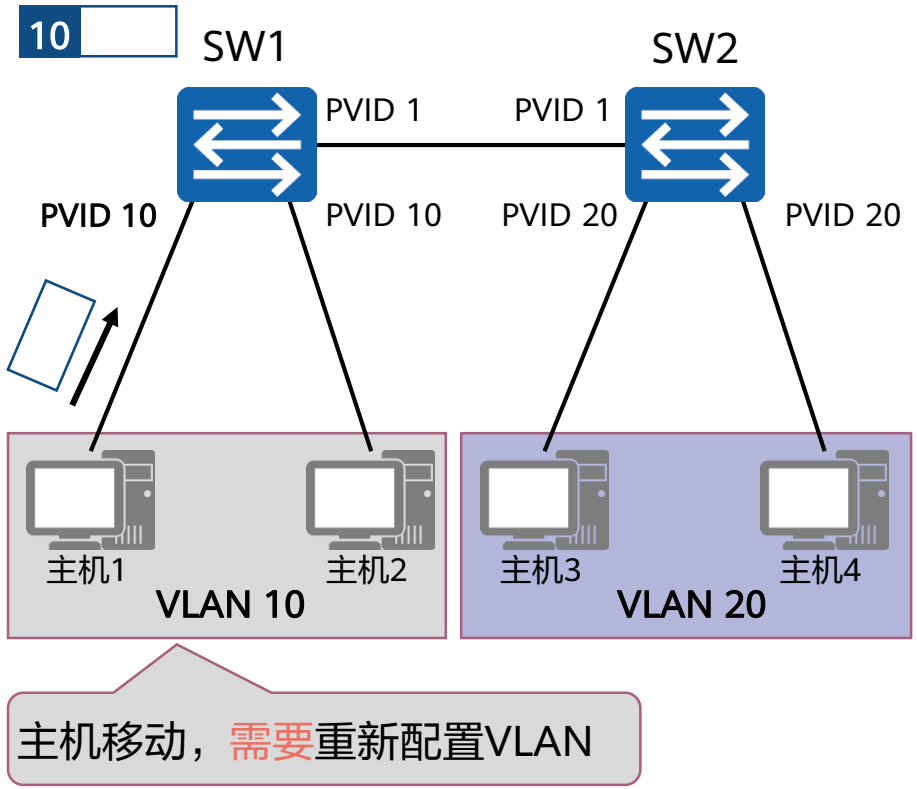
VLAN的划分方式

- 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



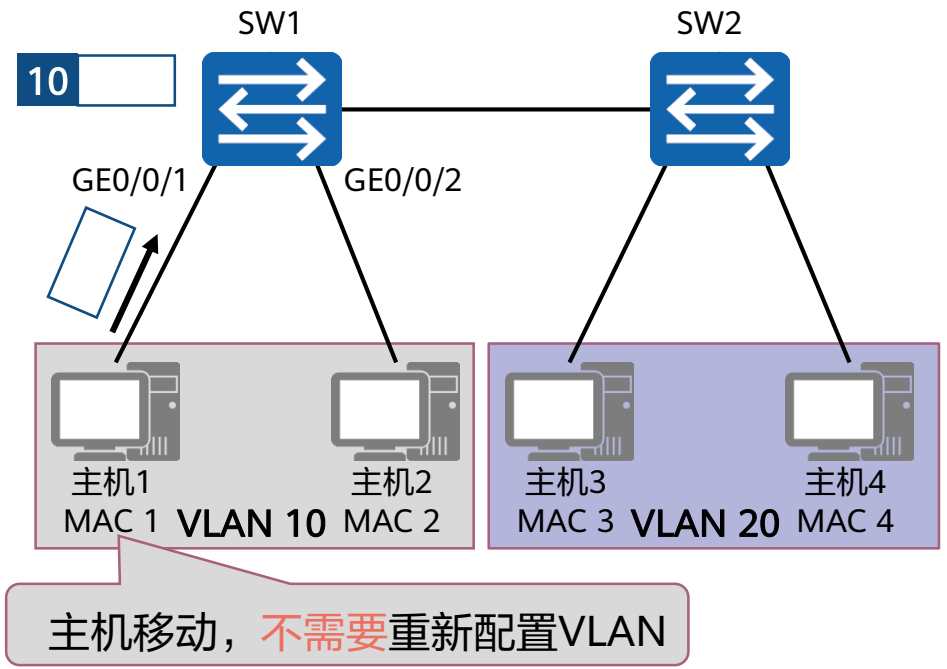
基于接口的VLAN划分

- **原理**
  - 根据交换机的接口来划分VLAN。
- **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

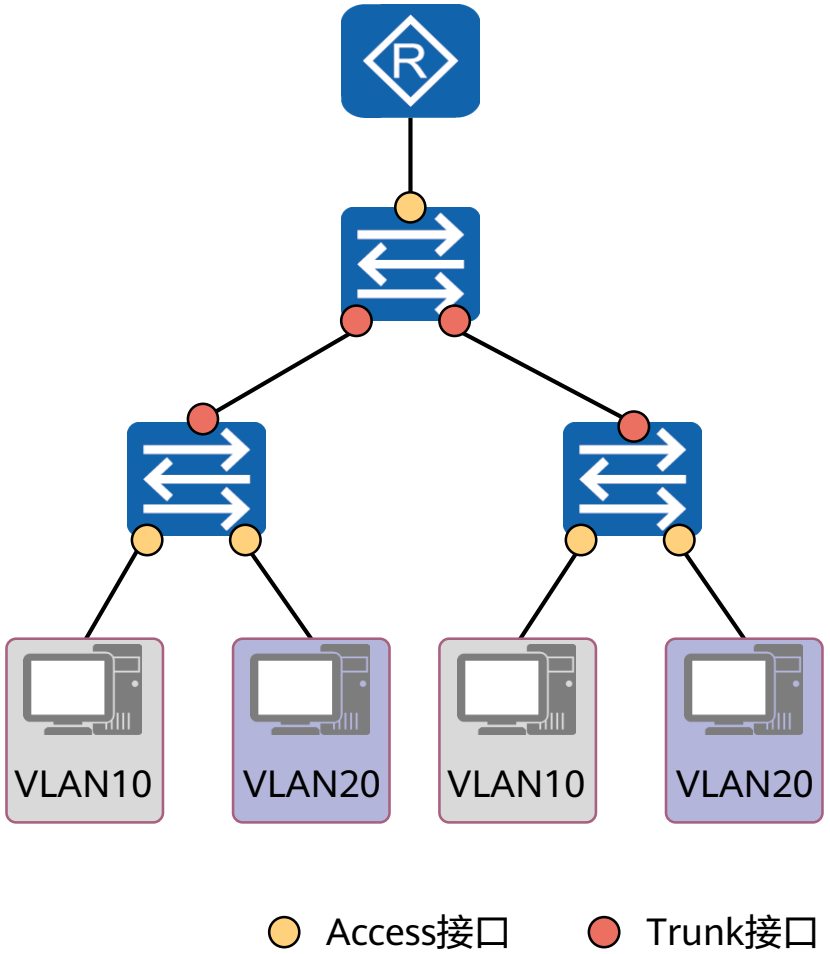
MAC地址	VLAN ID
MAC 1	10
MAC 2	10
……	……



基于MAC地址的VLAN划分

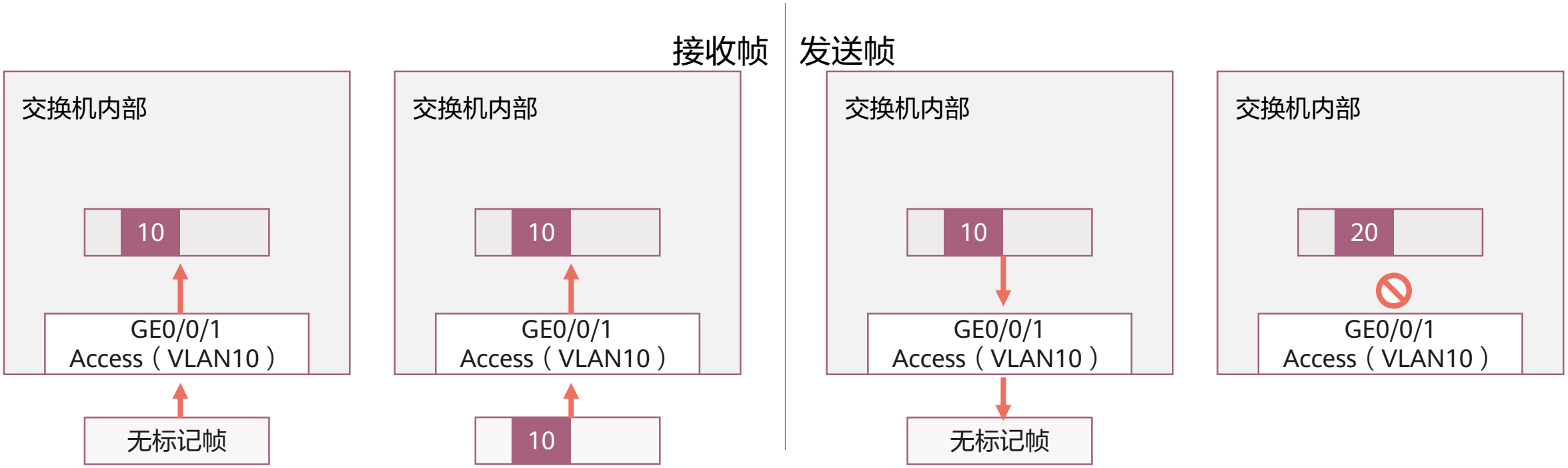
- **原理**
  - 根据数据帧的源MAC地址来划分VLAN。
- **映射表**
  - 记录了MAC地址和VLAN ID的关联情况。

以太网二层接口类型



接口类型
• Access接口
• Trunk接口
• Hybrid接口

Access接口



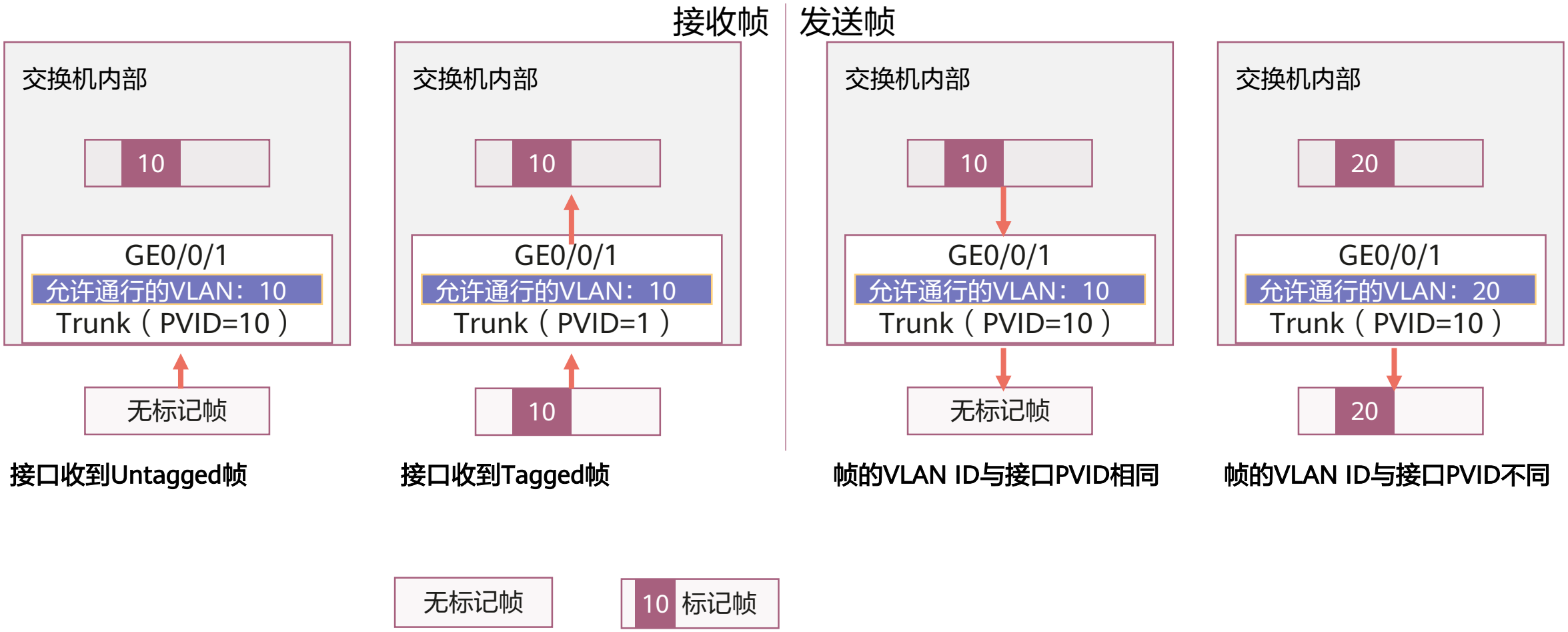
接口收到Untagged帧

接口收到Tagged帧

帧的VLAN ID与接口PVID相同

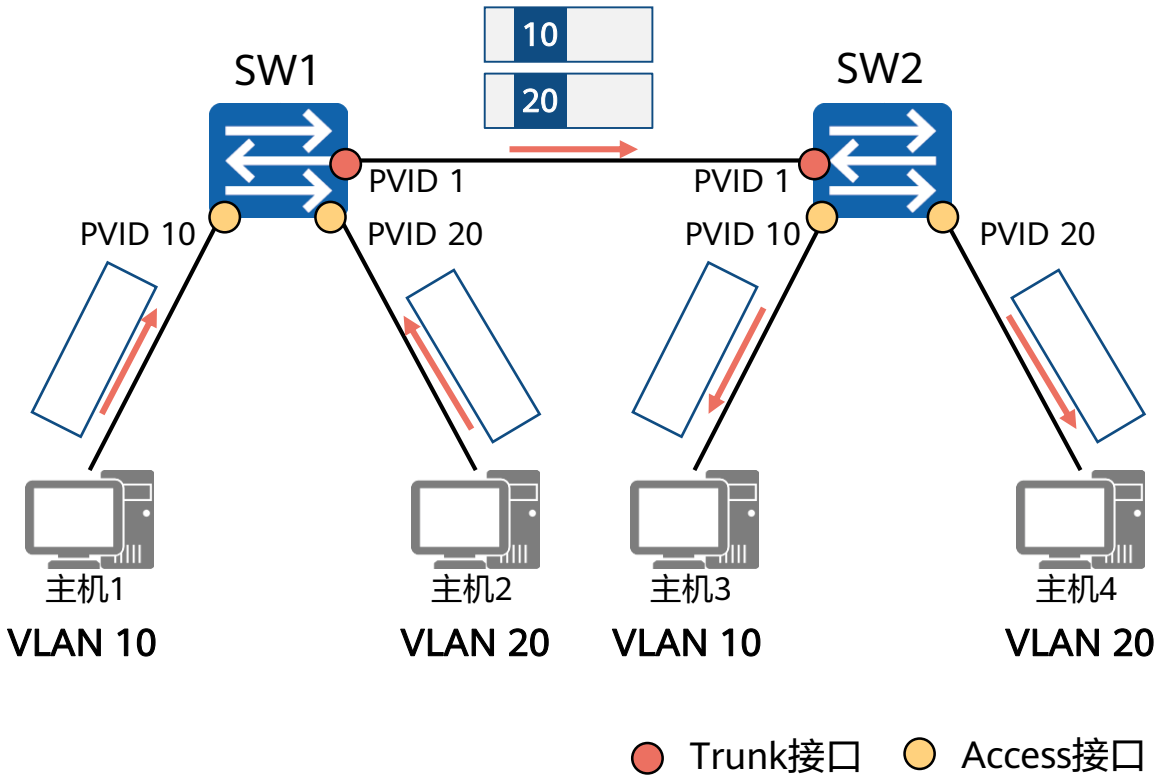
帧的VLAN ID与接口PVID不同

Trunk接口



Access接口与Trunt接口举例

- 请描述主机之间数据访问的全流程。

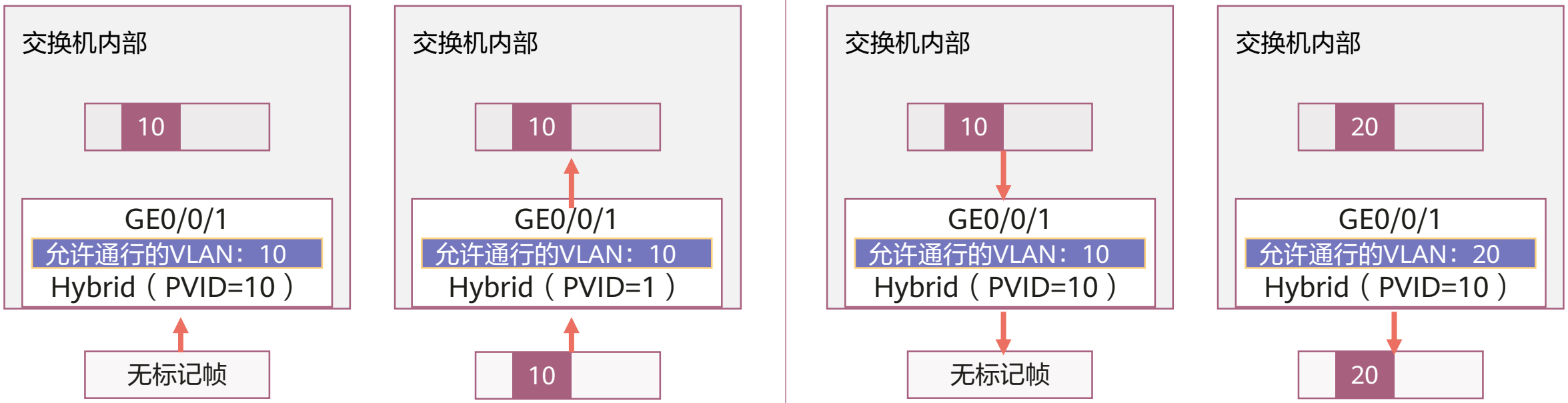


SW1与SW2的Trunk接口

允许通过列表	
VLAN ID	1
	10
	20

Hybrid接口

接收帧 | 发送帧



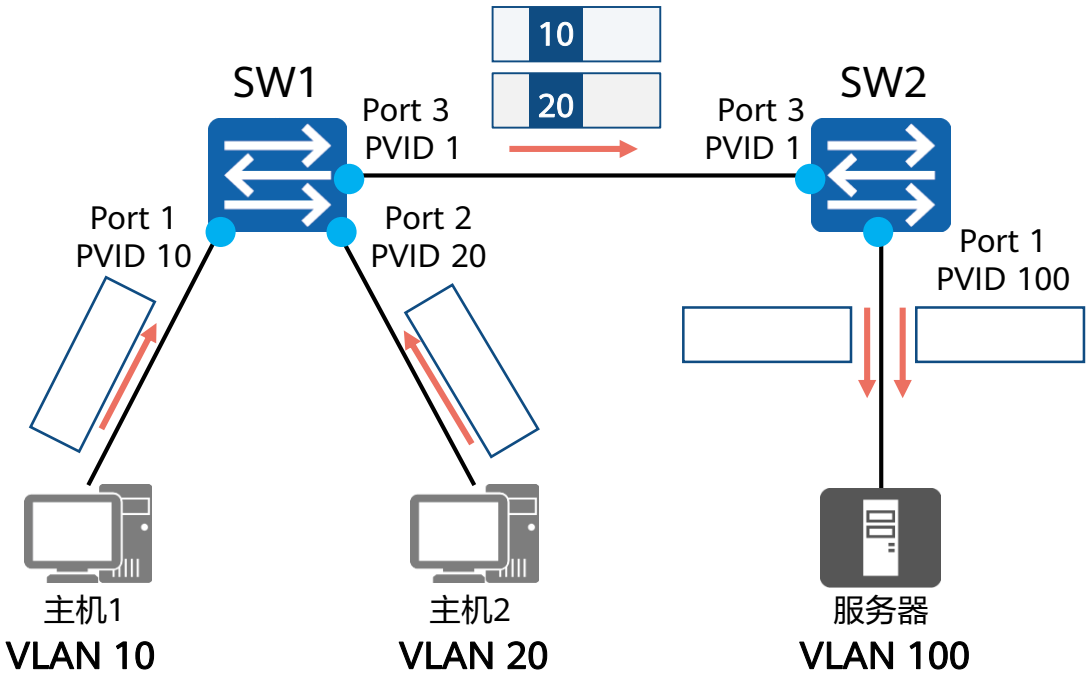
接口收到Untagged帧

接口收到Tagged帧

帧的VLAN ID是该接口允许通过的VLAN ID，且该VLAN ID属于Untagged VLAN ID列表

帧的VLAN ID是该接口允许通过的VLAN ID，且该VLAN ID属于tagged VLAN ID列表

Hybrid接口举例



交换机1的允许通过列表

Port1

Untagged	
VLAN ID	1
	10
	100

Port2

Untagged	
VLAN ID	1
	20
	100

Port3

Tagged	
VLAN ID	10
	10
	100

交换机2的允许通过列表

Port1

Untagged	
VLAN ID	1
	10
	20
	100

Port3

Tagged	
VLAN ID	10
	20
	100

小结

Access接口	Trunk接口	Hybrid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。	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。	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与PVID比较，相同则剥离标签发送；不同则丢弃。	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。	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

VLAN的规划

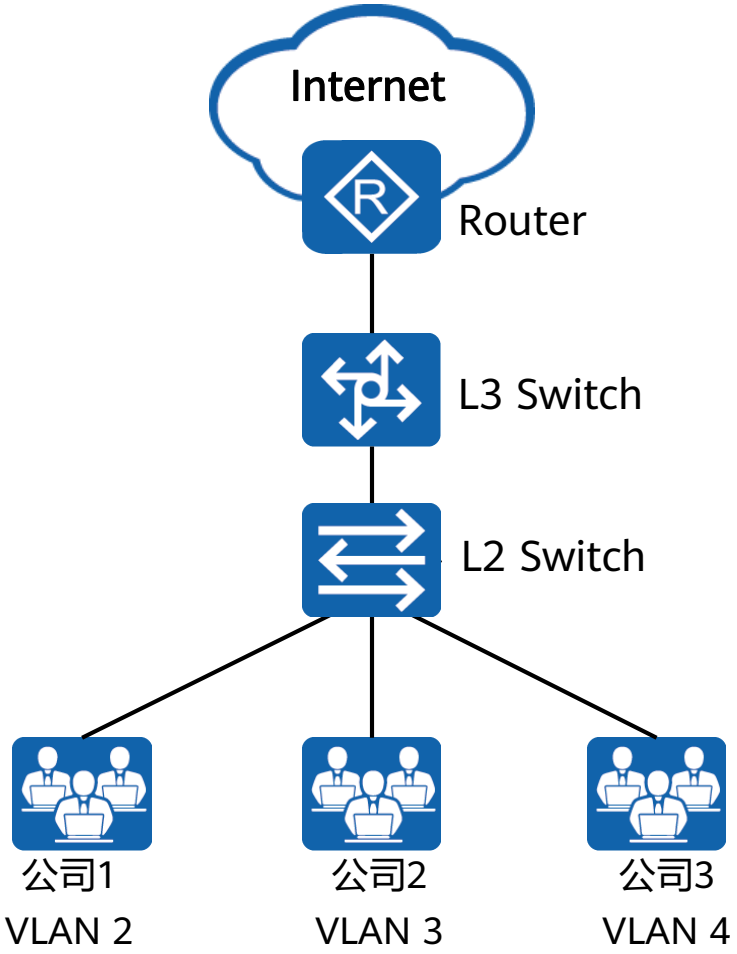
- VLAN分配原则
  - 按业务规划
  - 按部门规划
  - 按应用规划
- VLAN分配技巧

  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

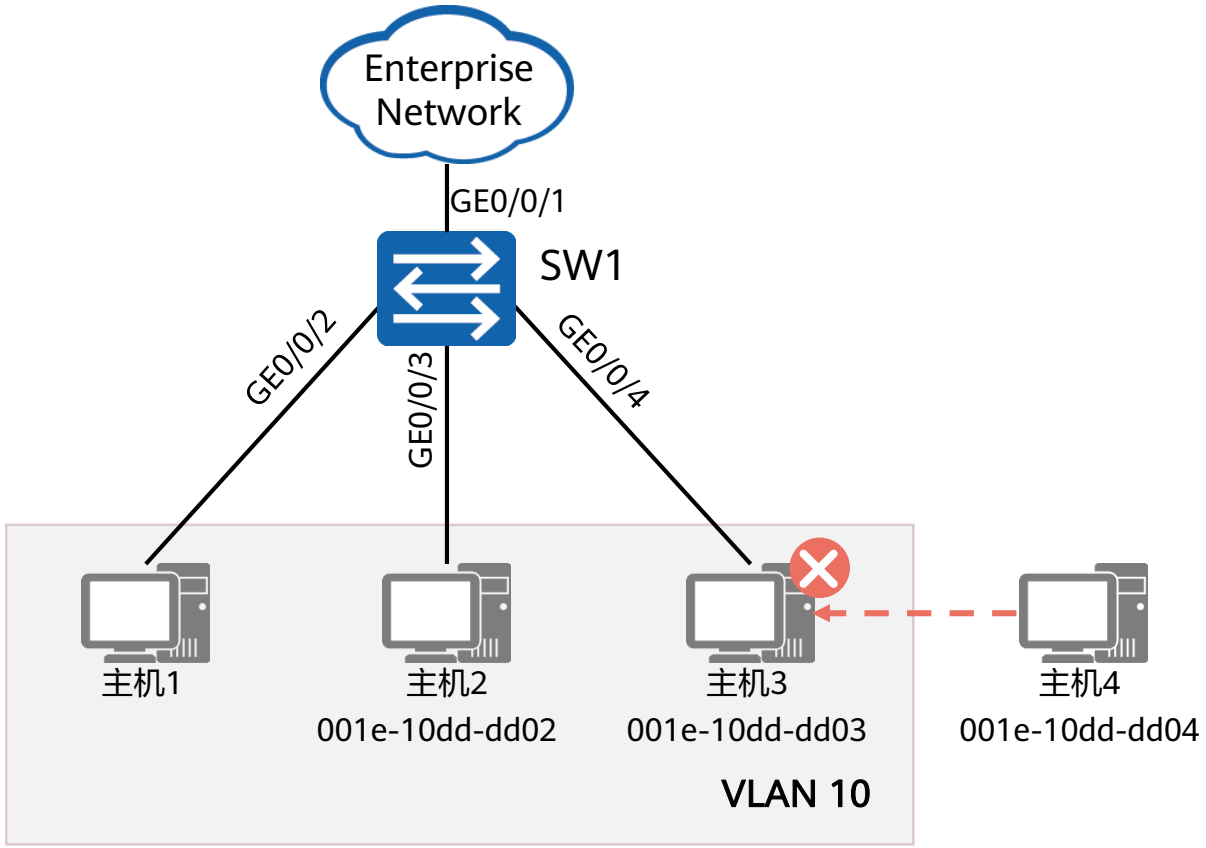
应用场景 – 基于接口的VLAN划分

- 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的独立和安全，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“虚拟工作组”。



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络资源。
- 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

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。

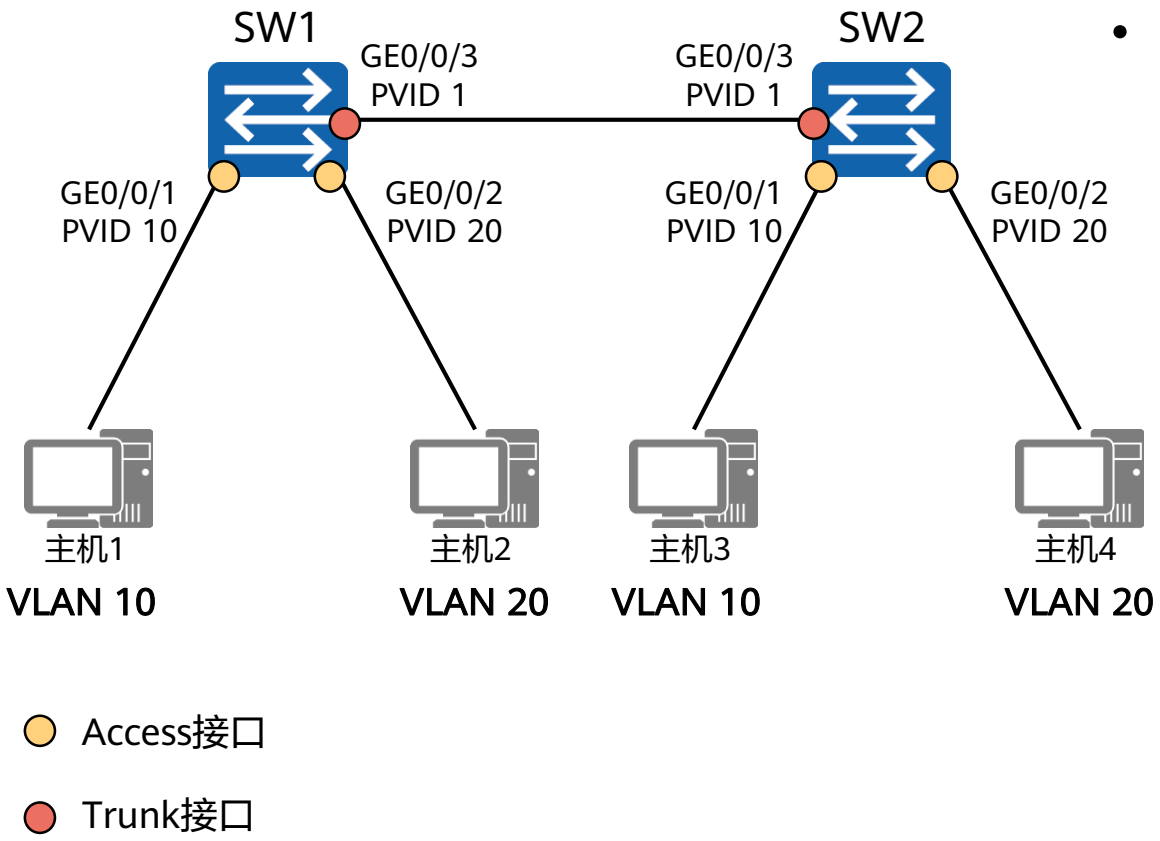
3. (可选) 配置Hybrid接口的缺省VLAN

```
[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。

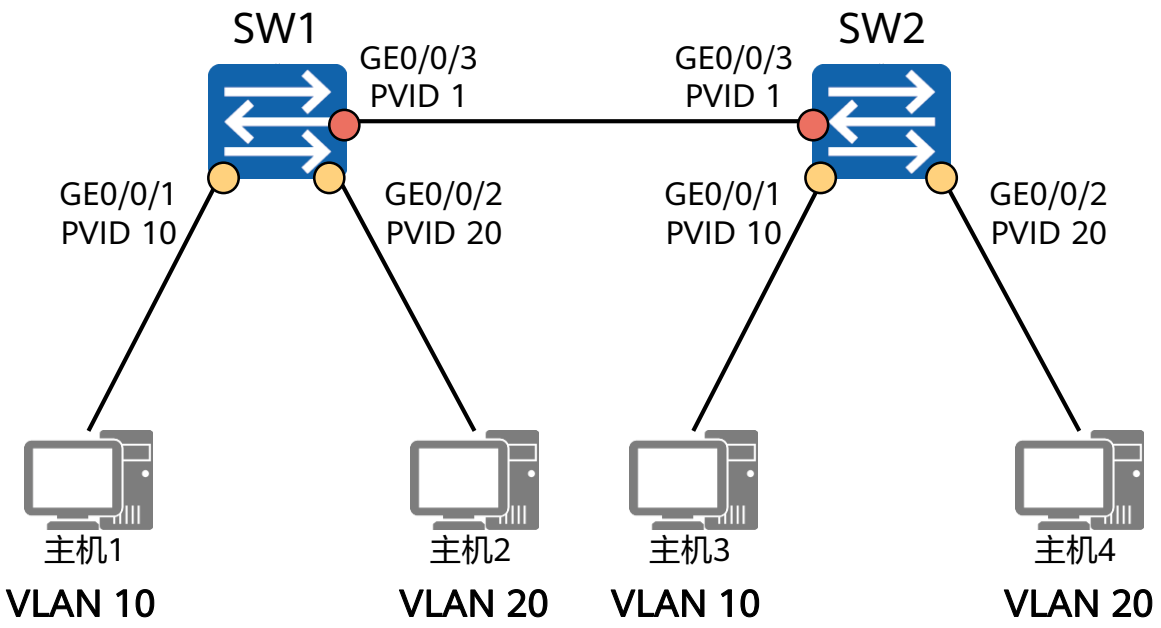
目录

案例1：基于接口划分VLAN



- 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

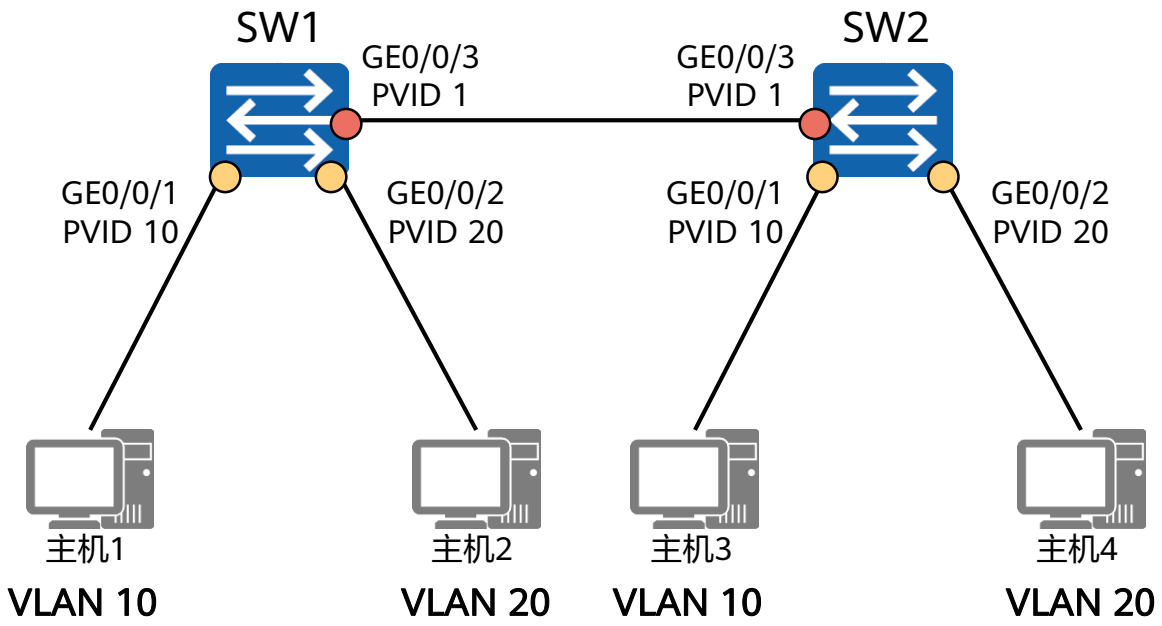


创建VLAN：

```
[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
```

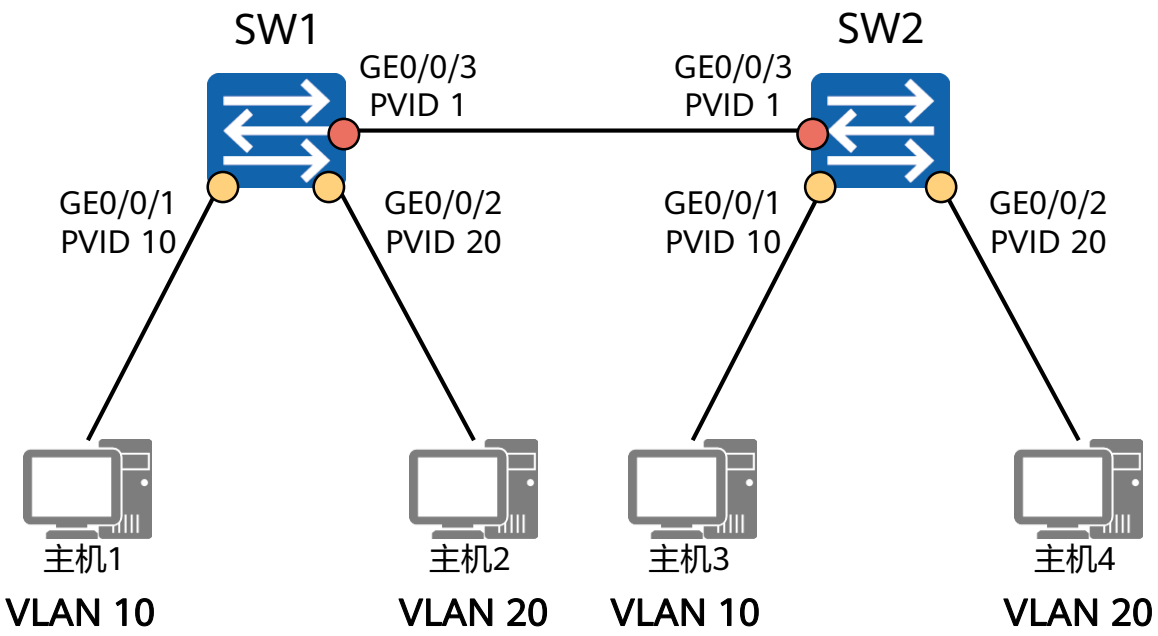
```
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type access
[SW1] vlan 20
[SW1-vlan20] port GigabitEthernet0/0/2
[SW1-vlan20] quit
```

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
```

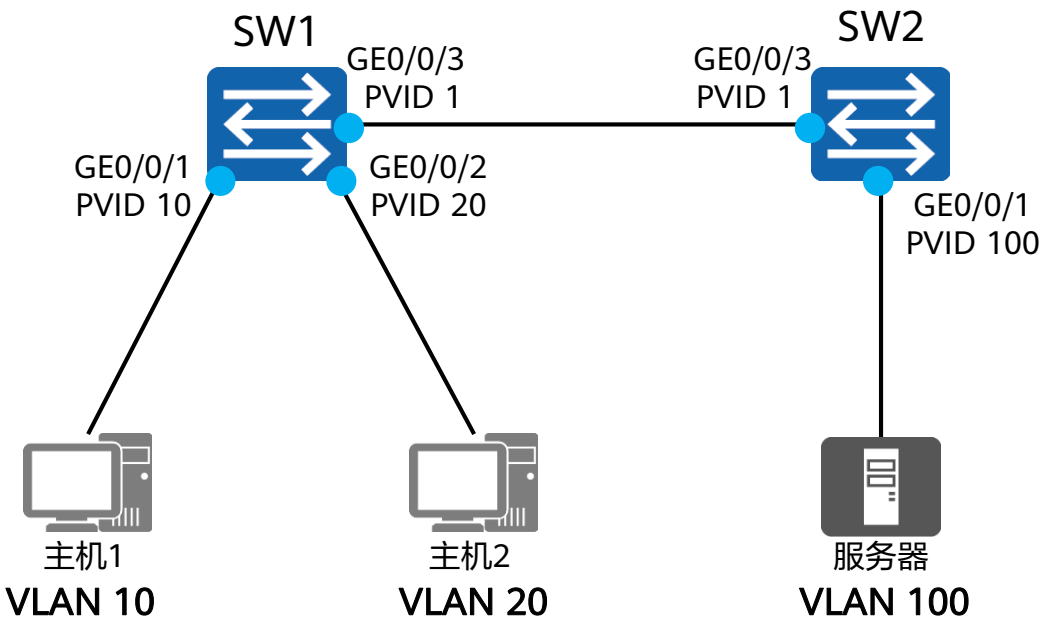
注：SW2配置与SW1类似

验证配置



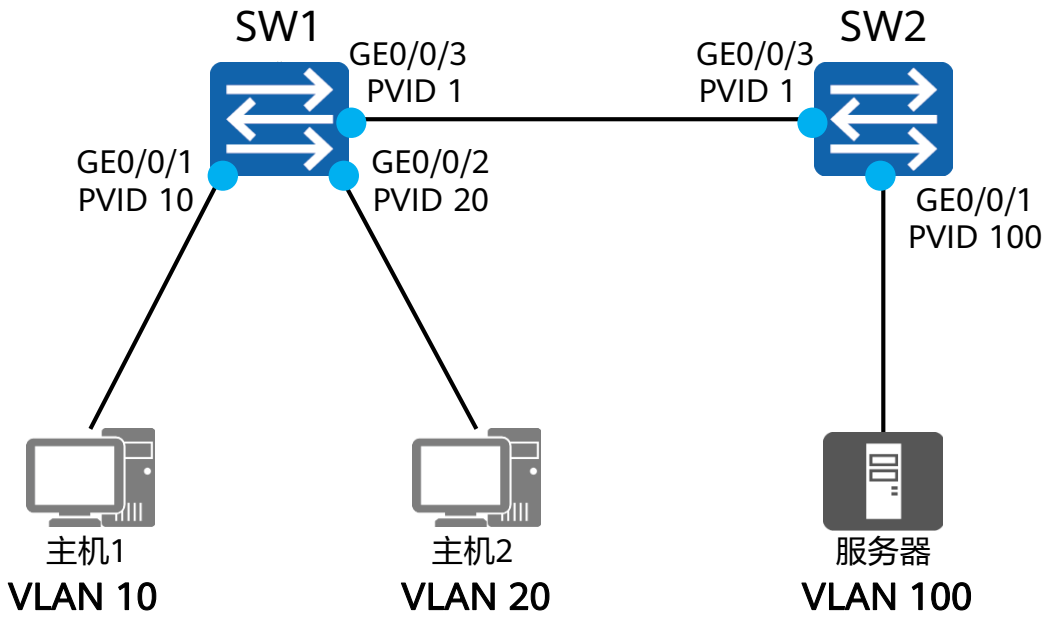

```
[SW1]display vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;          D: Down;                TG: Tagged;  UT: Untagged;
MP: Vlan-mapping;                       ST: Vlan-stacking;
#: ProtocolTransparent-vlan;            *: 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



- 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。

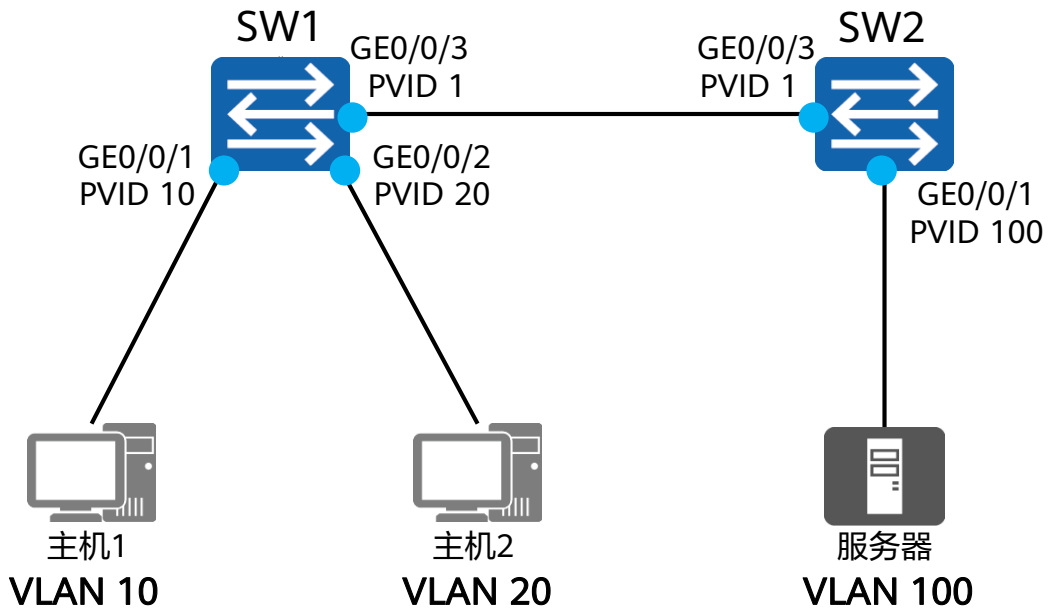
Hybrid接口的基础配置 (1)



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
```

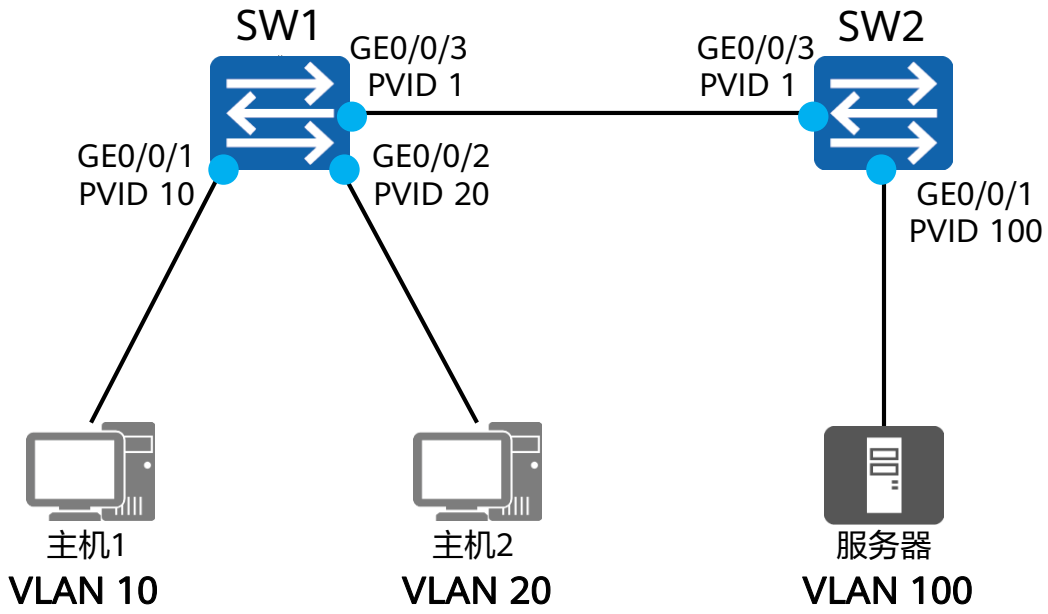
Hybrid接口的基础配置 (2)



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。

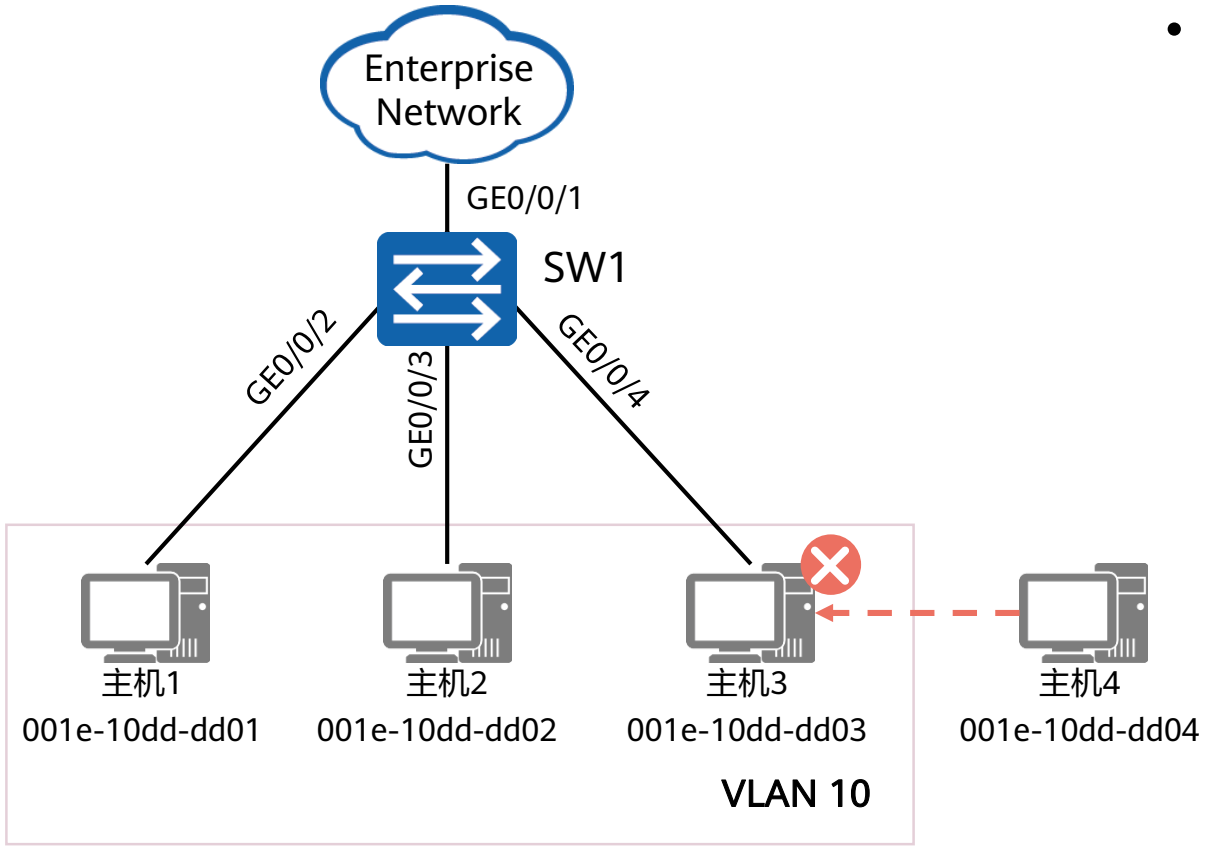
- *mac-address*：指定与VLAN关联的MAC地址。格式为H-H-H。其中H为4位的十六进制数，可以输入1～4位，如00e0、fc01。当输入不足4位时，表示前面的几位为0，如：输入e0，等同于00e0。MAC地址不可设置为0000-0000-0000、FFFF-FFFF-FFFF和组播地址。
- *mac-address-mask*：指定MAC地址掩码。格式为H-H-H，其中H为1至4位的十六进制数。
- *mac-address-mask-length*：指定MAC地址掩码长度。整数形式，取值范围是1～48。

2. 使能MAC地址与VLAN

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

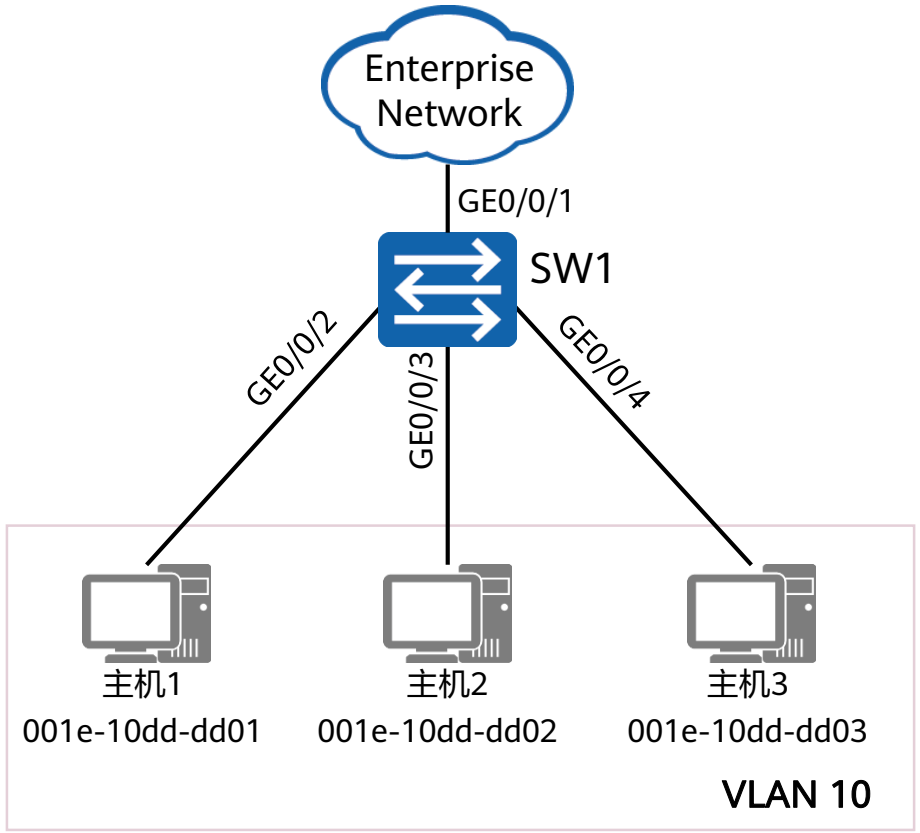
通过此命令使能接口的MAC VLAN功能。

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，从而实现该需求。

创建VLAN，并关联MAC地址和VLAN



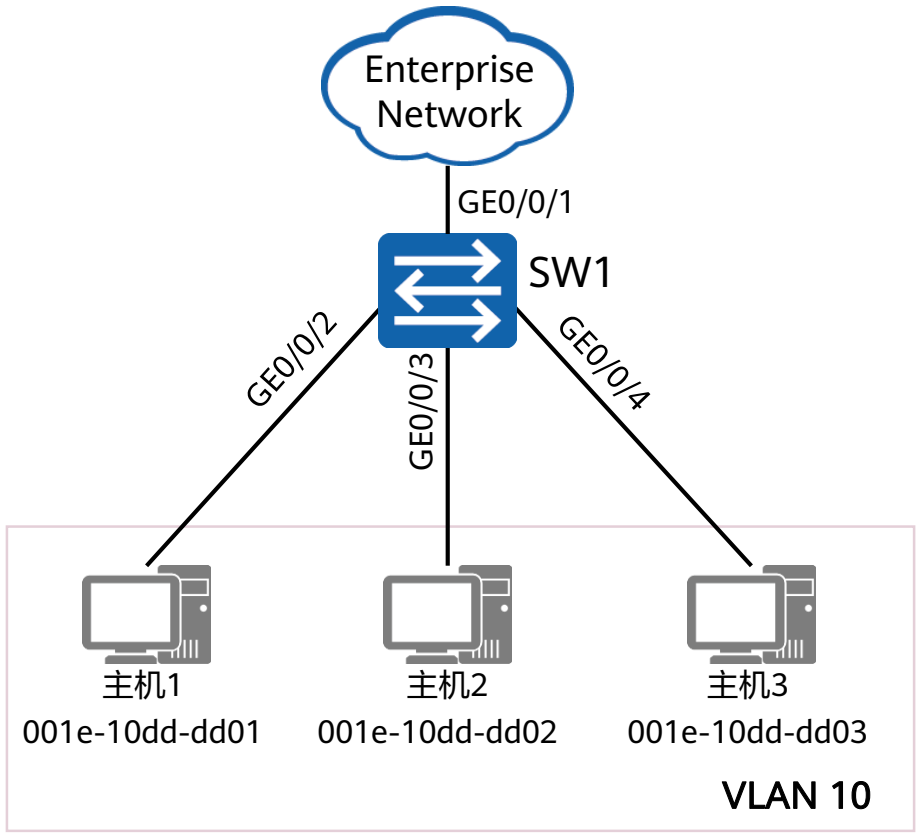
创建VLAN：

```
[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
```

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
```

本章总结

- 本章节主要介绍了虚拟局域网 (VLAN)的相关技术知识，包括：VLAN的作用，VLAN的标识及划分，VLAN的数据交互，VLAN的实际规划和应用，以及VLAN的相关基本配置。
- 通过VLAN技术，可以将物理的局域网划分成多个广播域，实现同一VLAN内的网络设备可以直接进行二层通信，不同VLAN内的设备不可以直接进行二层通信。