

网络技术与信息安全



第4讲：虚拟局域网

河南中医药大学信息技术学院
网络技术课程教学组

本章教学目标

- 理解VLAN的概念及通信特点
- 掌握基于端口划分VLAN的方式
- 理解IEEE802.1Q帧的结构特点
- 理解PVID和VID
- 掌握Access接口、Trunk接口的配置与应用
- 掌握VLAN通信过程中，数据帧加标签和去标签的应用



一、认识虚拟局域网

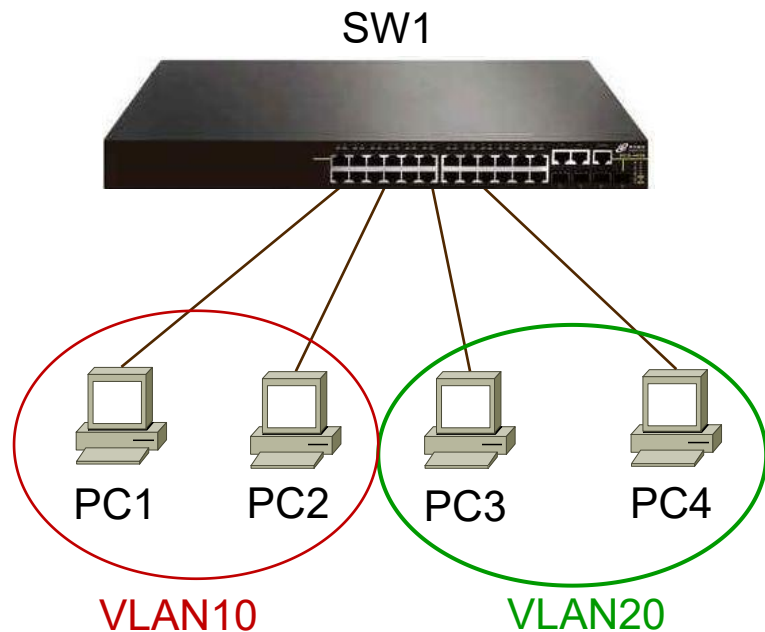
—— VLAN的概念、功能、通信特点

认识虚拟局域网

□ 什么是虚拟局域网？

- 虚拟局域网（Virtual Local Area Network，简称VLAN），是一种应用在交换机上的**技术**。IEEE于1999年颁布了用于标准化VLAN实现方案的802.1Q协议标准草案。
- 通过VLAN技术，可以把接入同一台交换机或者接入不同交换机的设备和用户，根据其功能、部门以及应用等因素，将它们划分到不同的逻辑网络，即形成不同的、虚拟的局域网（VLAN）；
- **VLAN举例**

◆ 例1：接入**同一交换机**的用户主机，被划分为不同的VLAN

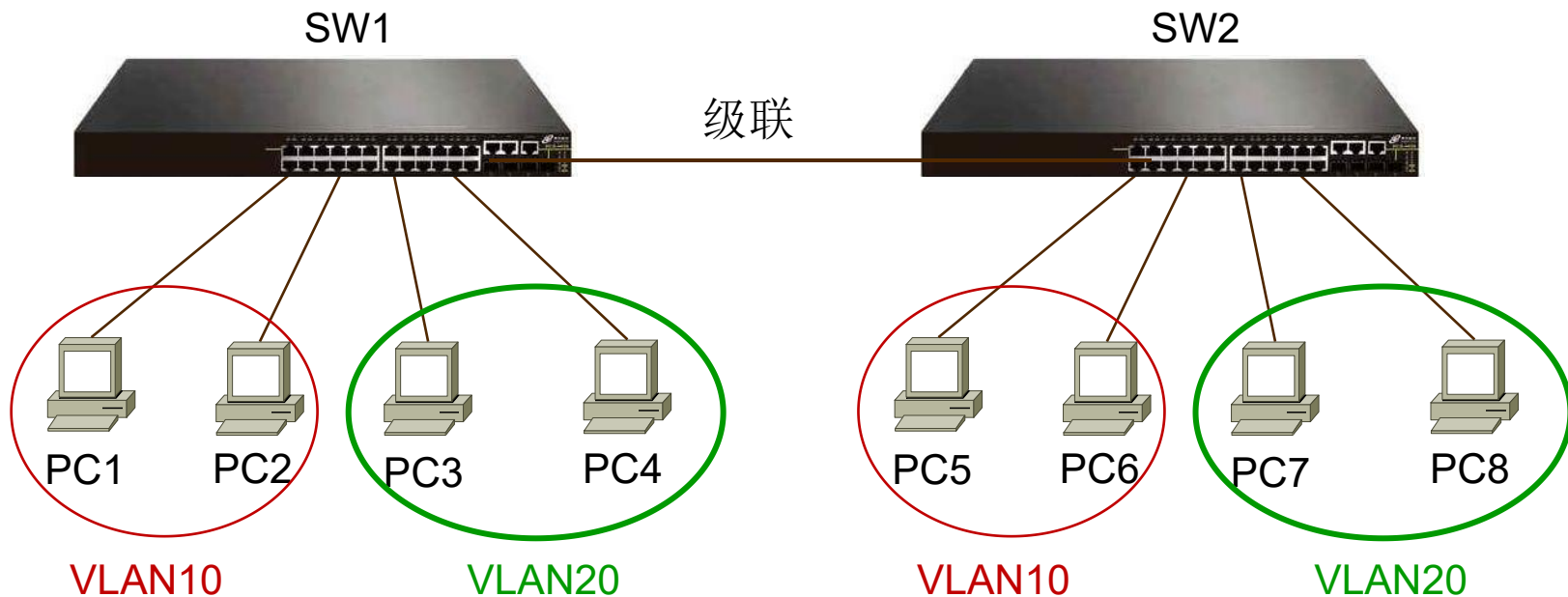


➤ 划分VLAN之后

PC1和PC2属于同一个虚拟局域网（VLAN10）

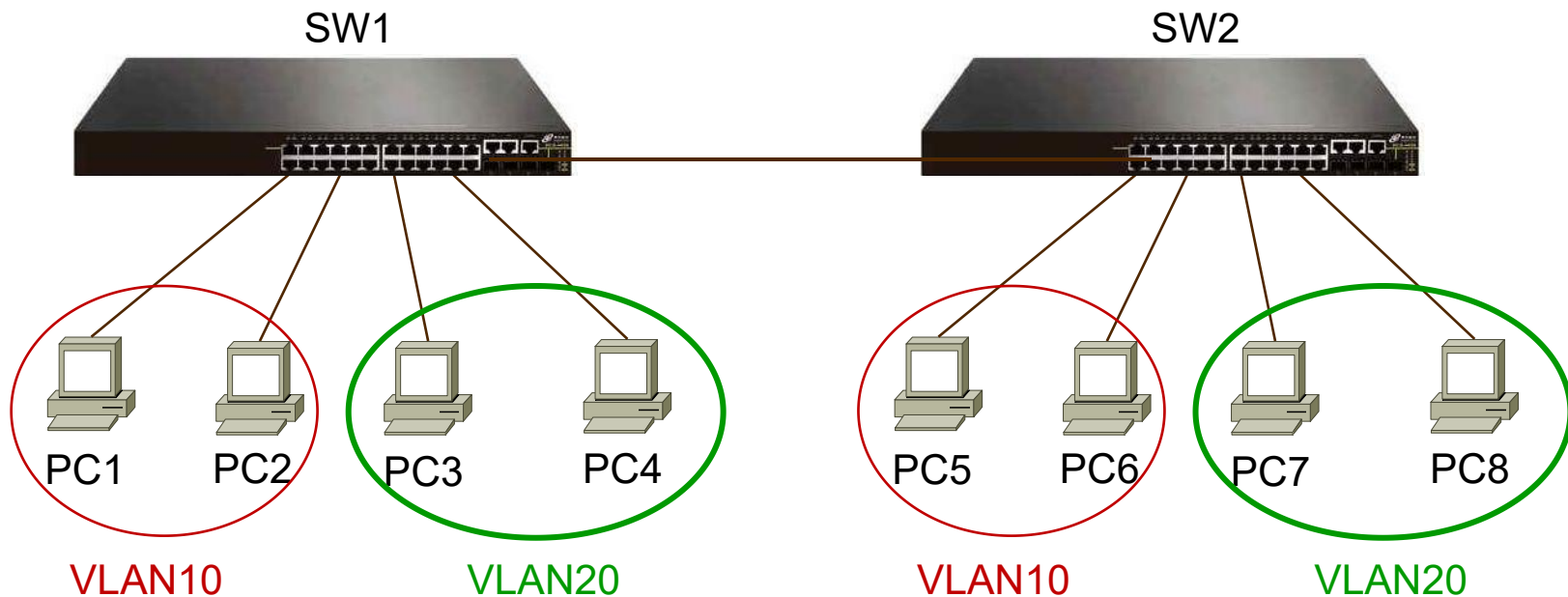
PC3和PC4属于另一个虚拟局域网（VLAN20）

◆ 例2：接入不同交换机的用户主机，被划分到同一VLAN中



- 此处，PC1、PC2、PC5、PC6属于同一个虚拟局域网（VLAN10）
- PC3、PC4、PC7、PC8属于同一个虚拟局域网（VLAN20）

例1：接入同一物理网络的用户被划分为不同的用户组，形成虚拟的局域网



- 通过应用VLAN，也可以使处于不同交换机上的用户，属于同一个虚拟的局域网

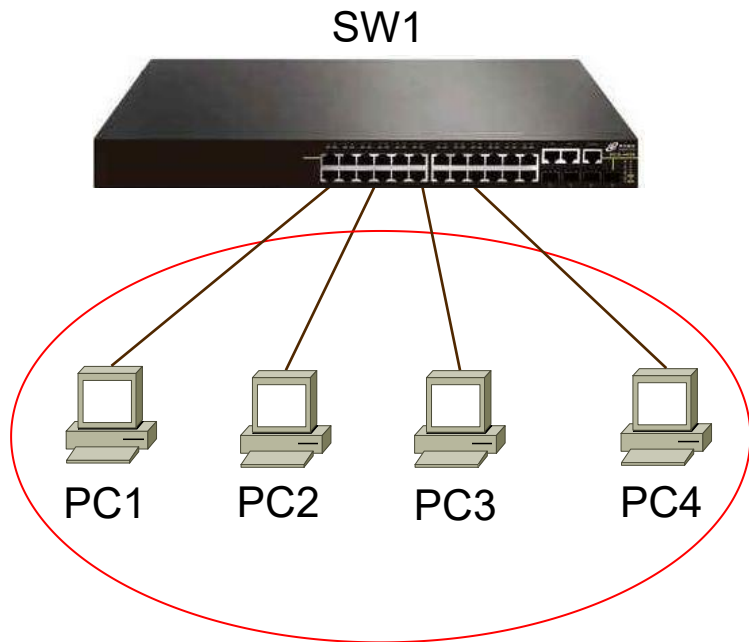
认识虚拟局域网

□ 为什么使用VLAN?

■ 限制交换机的广播域范围

- 交换机默认情况下，所有接口属于同一广播域。级联的交换机，属于同一个更大的广播域。
- 在交换机上配置VLAN，可以在逻辑上划分出不同的广播域。
- 一个VLAN就是一个独立的广播域，即同一个VLAN中的设备，可以直接通信，就像它们在同一个物理网段中一样；但不同VLAN之间，是无法直接通信的，**必须通过三层路由设备来完成转发**。
- 虚拟局域网（VLAN）的使用，限制了交换机组成的网络中，接收广播信息的主机数，使得不会因广播域过大引起网络性能下降。
- **举例**

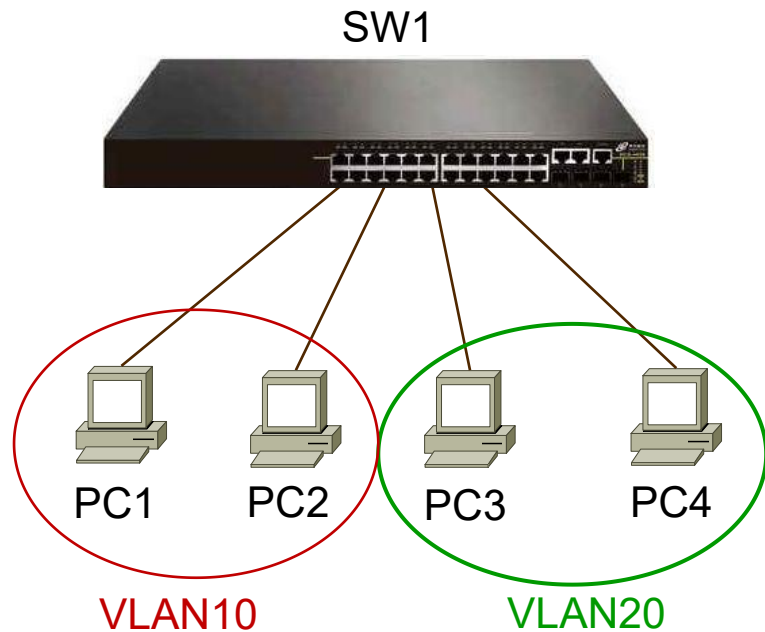
◆ 演示：VLAN限制广播域范围



➤ 划分VLAN之前

所有用户主机属于同一个广播域

◆ 演示：VLAN限制广播域范围

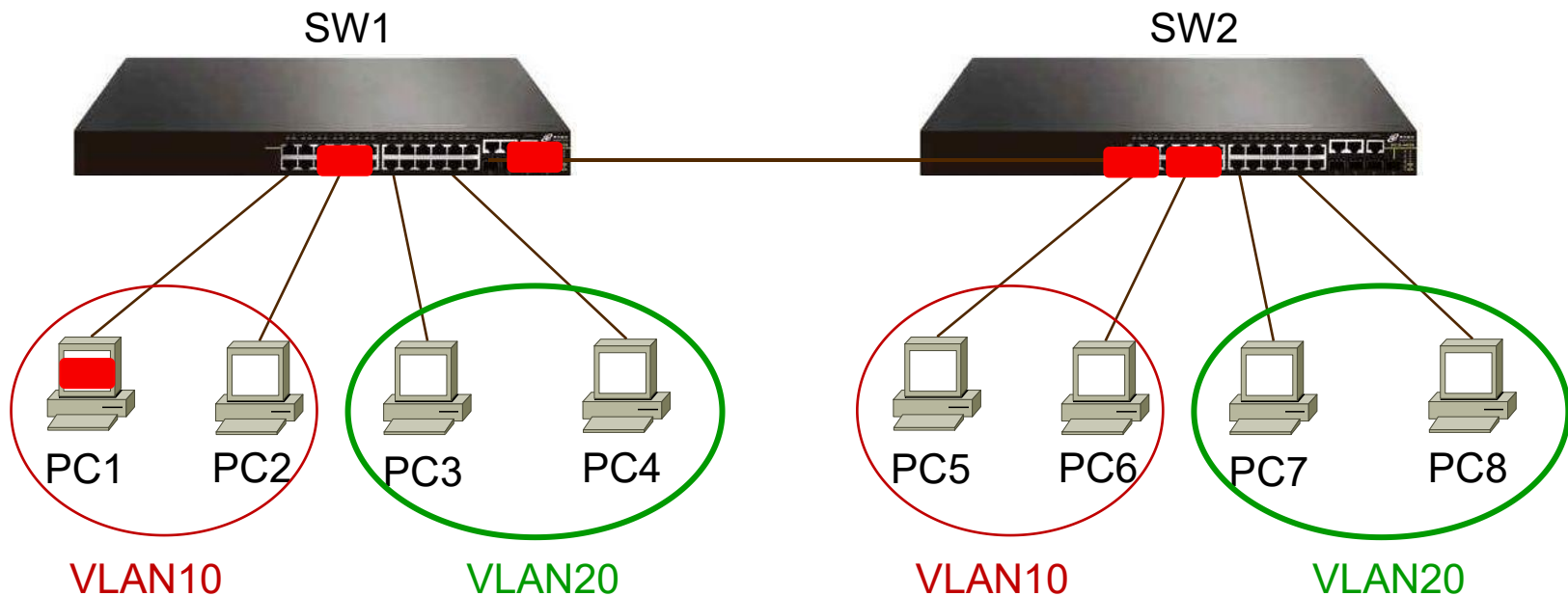


➤ 划分VLAN之后

PC1和PC2属于同一个广播域

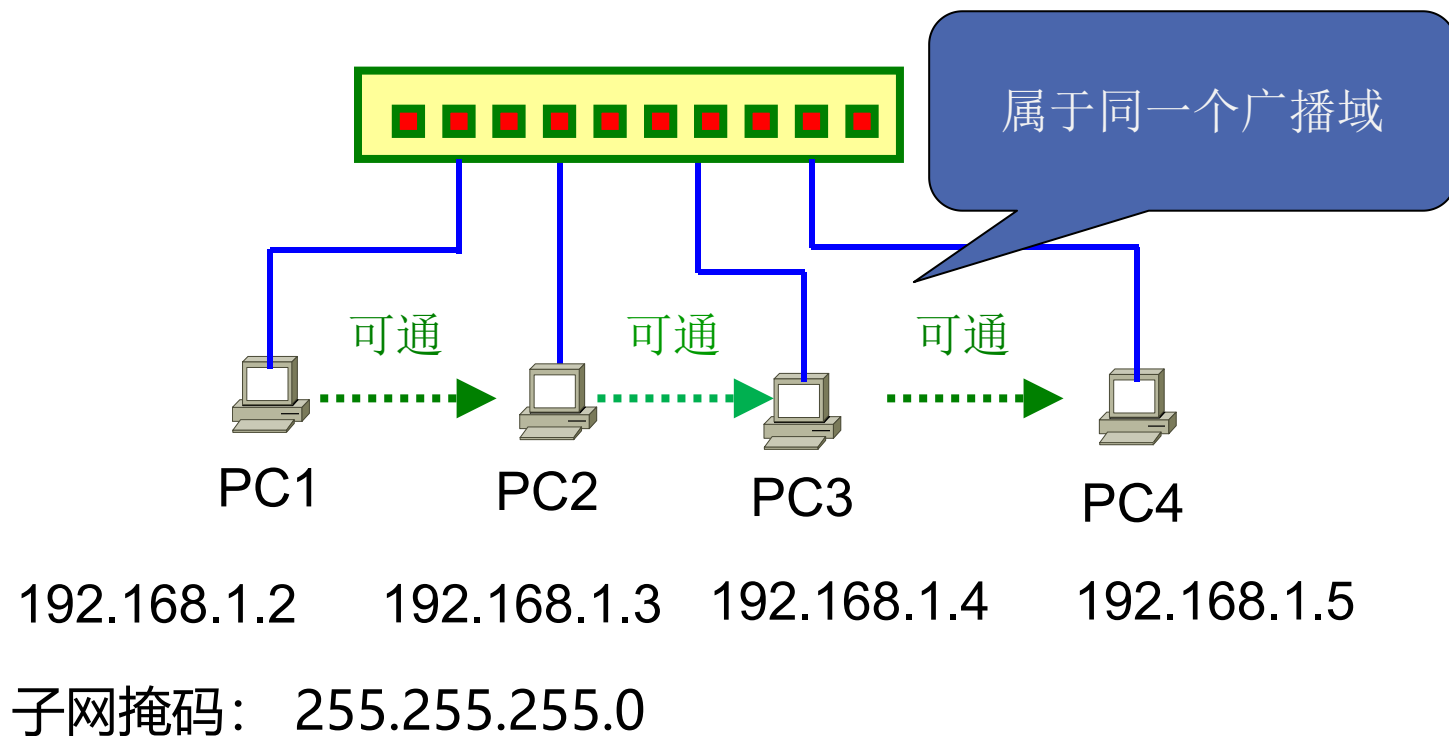
PC3和PC4属于另一个广播域

◆ 演示：VLAN限制广播域范围

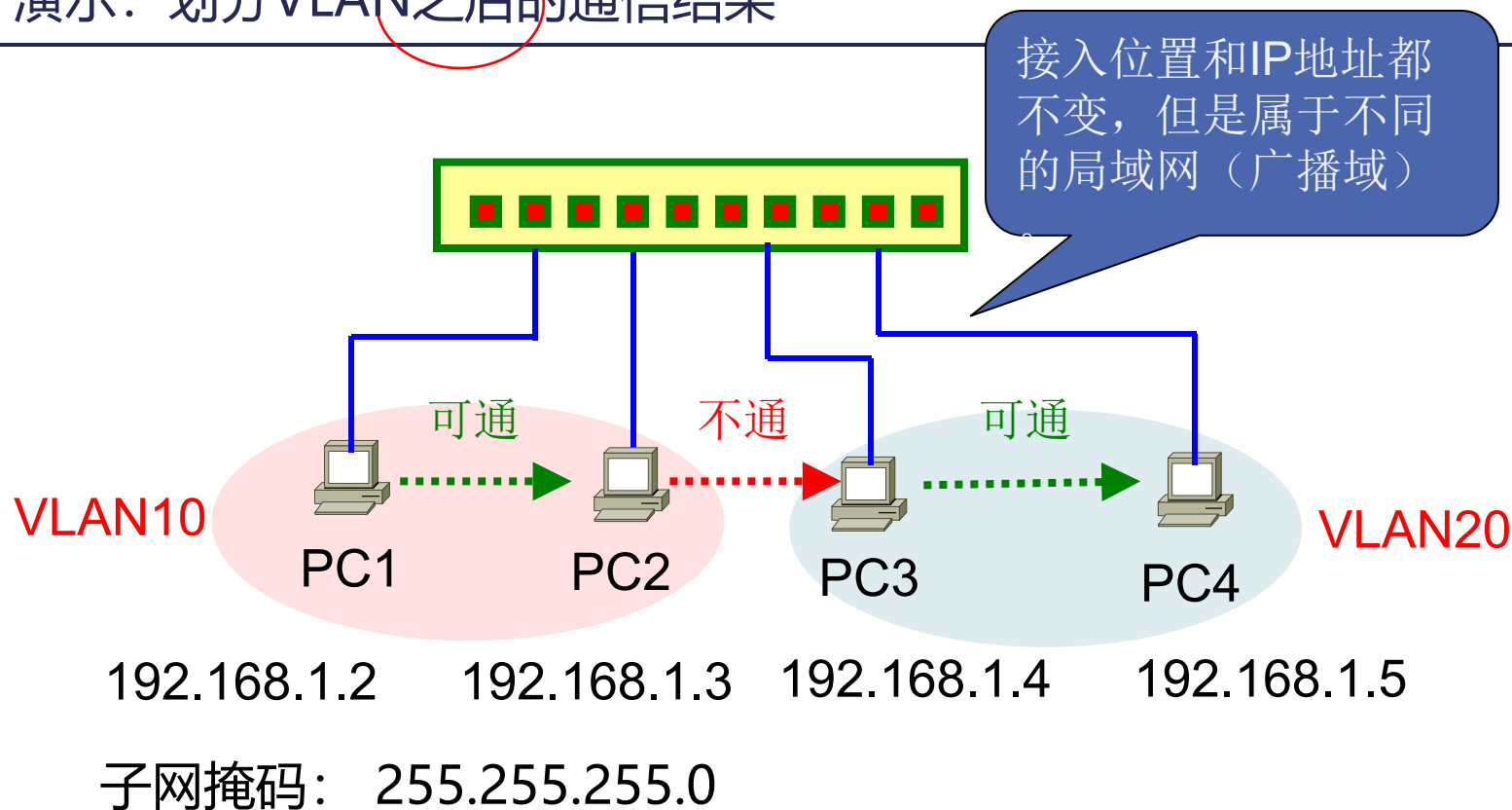


- 划分VLAN前，当PC1发出广播包时，PC2—PC8都能收到；
- 划分VLAN后，当PC1发出广播包时，只有属于同一个VLAN的设备（包括PC2、PC5、PC6）能够收到，即VLAN隔离了广播。

◆ 演示：划分VLAN之前的通信结果



◆ 演示：划分VLAN之后的通信结果



认识虚拟局域网

□ 为什么使用VLAN?

■ 增强局域网的安全性

- 不同VLAN内的报文在传输时是相互隔离的，即一个VLAN内的用户不能和其他VLAN内的用户直接通信。含有敏感数据的用户组可与网络的其余部分隔离，从而降低泄露机密信息的可能性。

认识虚拟局域网

□ 为什么使用VLAN?

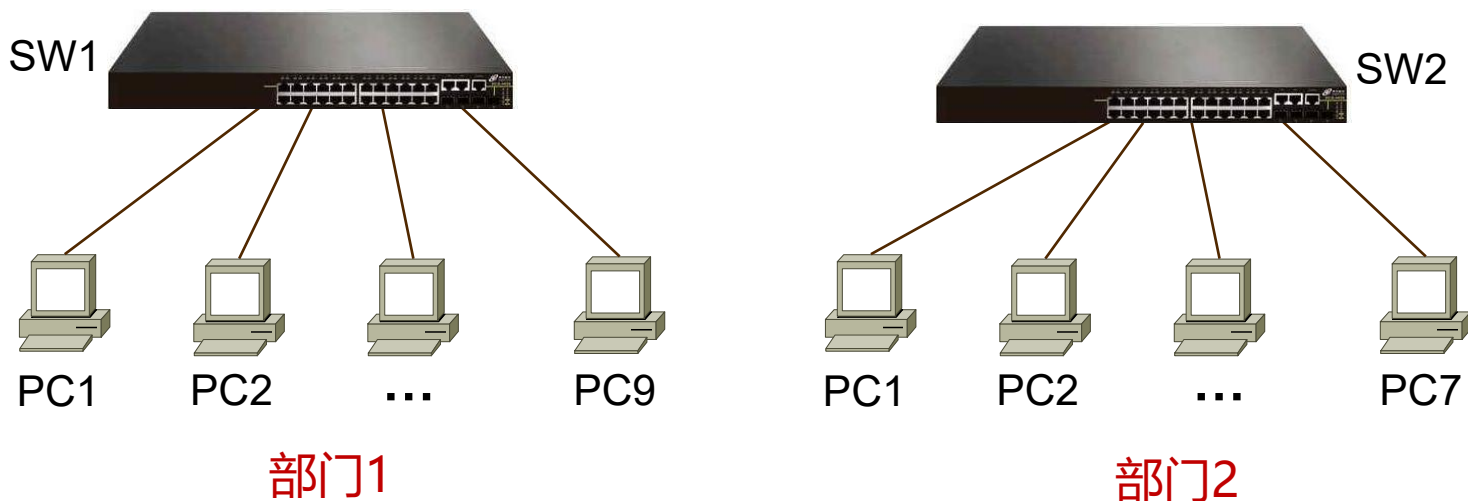
■ 减少设备投资，使网络部署更加灵活

➤ 两个部门要想成为两个独立的网络，可以把两个部门通过一台交换机接入，分属于不同的虚拟局域网，不必要接入两台交换机。

➤ 举例

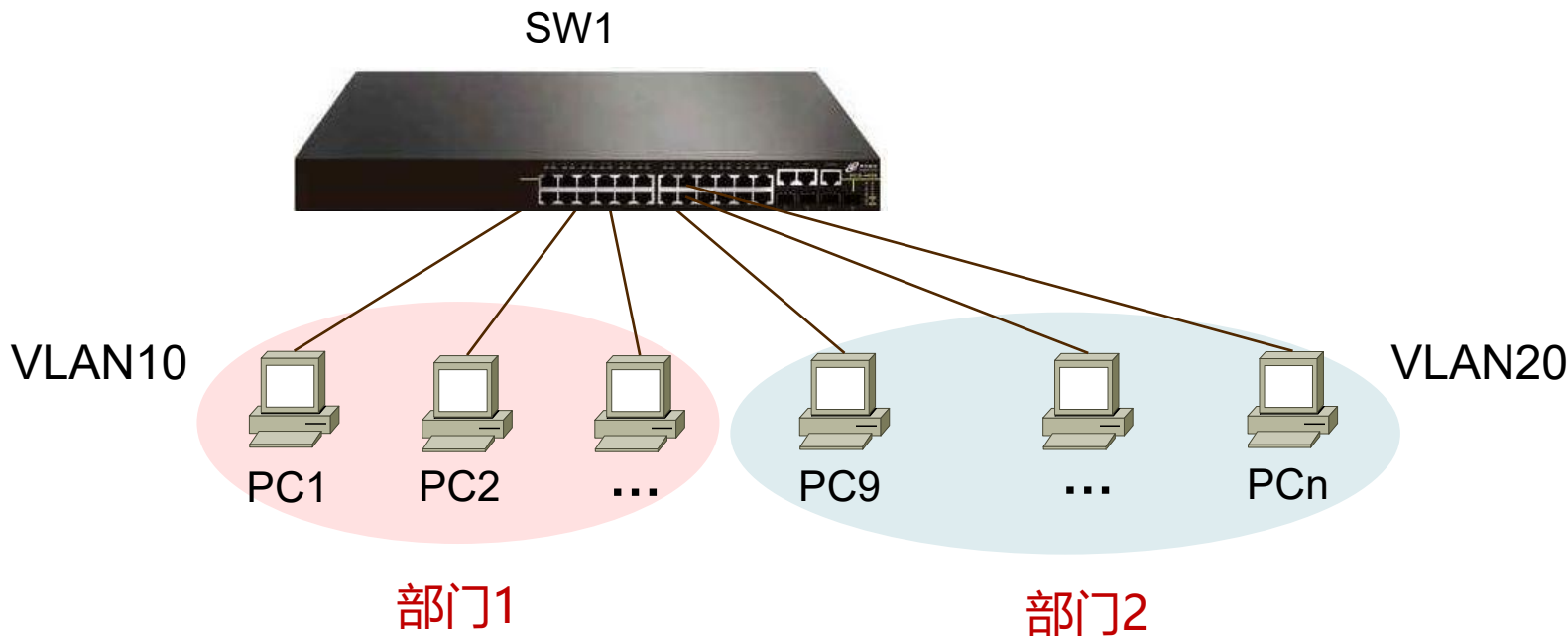
◆ 演示：VLAN减少设备投资，使网络部署更加灵活

- 不使用VLAN，两个部门要想分属于两个局域网，就必须接入到不同的交换机上。



◆ 演示：VLAN减少设备投资，使网络部署更加灵活

➤ 使用**VLAN**，两个部门接入同一个交换机，也可以属于不同的局域网。



认识虚拟局域网

□ 初步归纳：虚拟局域网

- 虚拟局域网简称VLAN，它不是一种网络类型，而是一种应用在交换机上的网络配置技术；
- 通过VLAN技术，可把一个由交换机组成的物理网络，划分为多个不同的虚拟的局域网，使得用户的接入位置不变，但是从逻辑上属于不同的广播域。
- 一个VLAN就是一个广播域，不同的VLAN之间想要通信，需要通过路由设备。

二、VLAN的划分方式

—— 如何在交换机上创建VLAN?

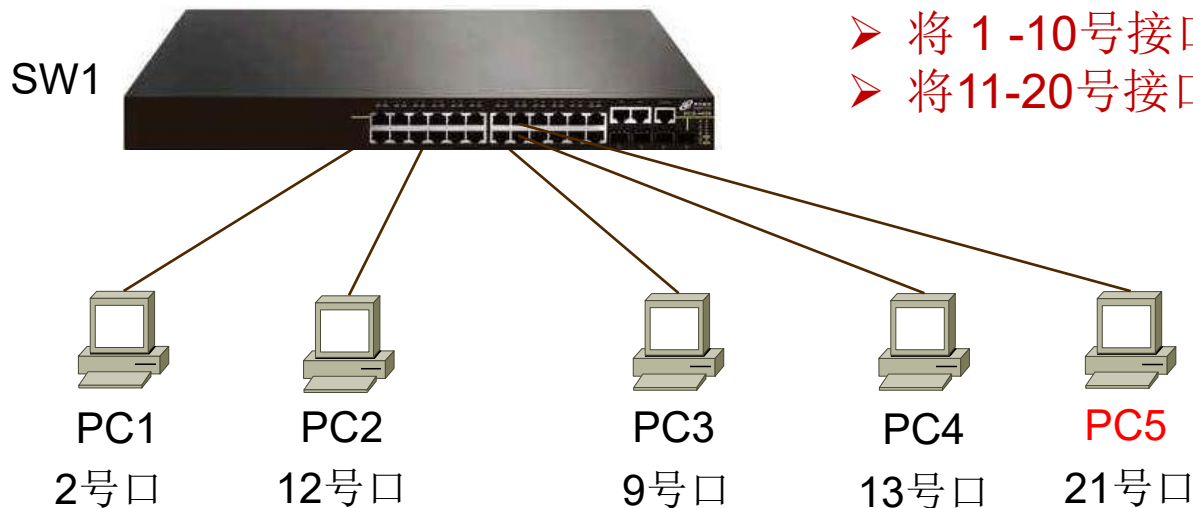
VLAN的划分方式

□ 基于接口划分VLAN

- 这是最常应用的创建VLAN的方法。
- 它在交换机上创建VLAN，然后将指定的接口划分入指定的VLAN，属于同一VLAN的接口就构成一个虚拟局域网，具有与其他接口组不同的广播域。
- 举例

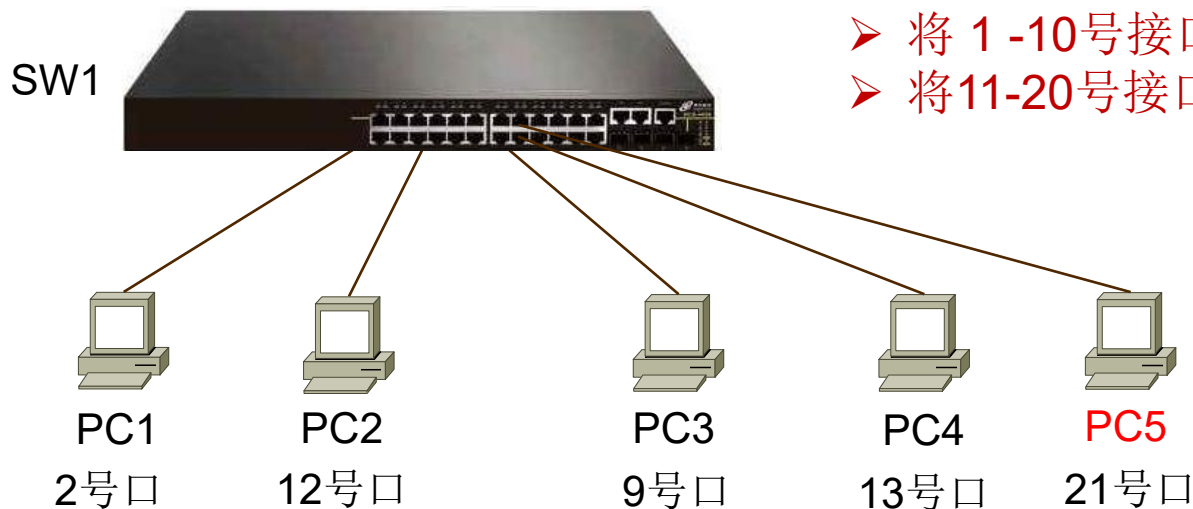
[SW-1]vlan 10	//创建VLAN10
[SW-1]interface Ethernet0/0/1	//进入接口Ethernet 0/0/1视图
[SW-1-Ethernet0/0/1]port link-type access	//配置接口类型为Access
[SW-1-Ethernet0/0/1]port default vlan 10	//将Ethernet0/0/1划分到VLAN10

◆ 示例：基于交换机接口划分VLAN —— 单交换机



- PC1和PC3属于VLAN2，在同一个广播域内，相互之间可直接通信；
- PC2和PC4属于VLAN3，在同一个广播域内，相互之间可直接通信；

◆ 示例：基于交换机接口划分VLAN —— 单交换机



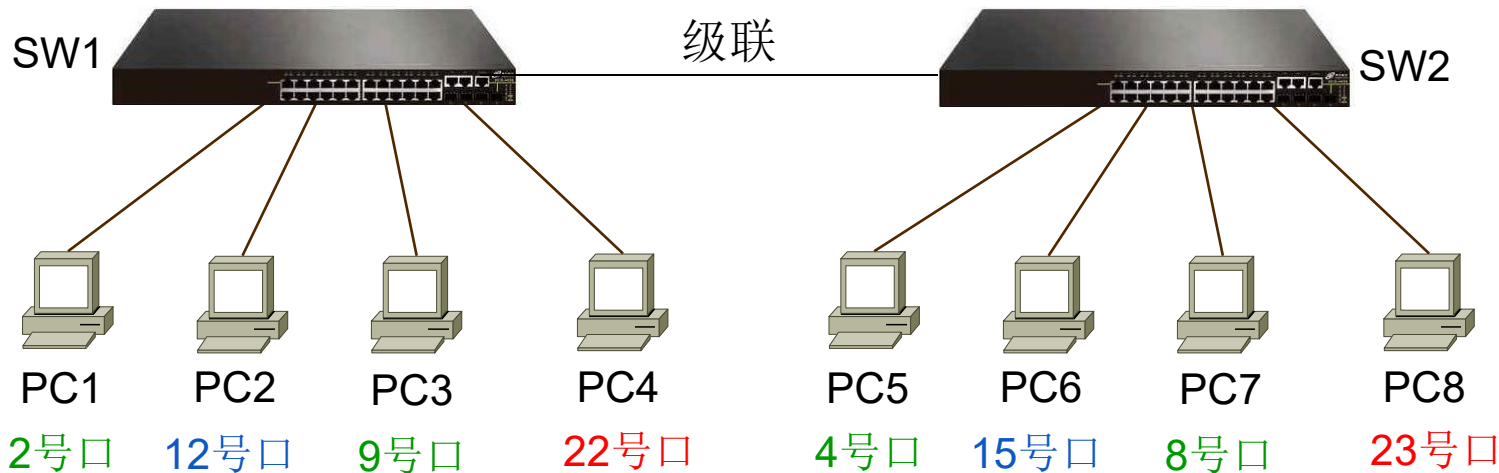
- 将 1 -10号接口划分到VLAN2
- 将11-20号接口划分到VLAN3

➤ PC5属于：VLAN1

【注意】 VLAN 1是系统自带的VLAN，不需要创建，也不可以删除。在缺省情况下，交换机的所有接口都属于VLAN1。

◆ 示例：基于交换机接口划分VLAN —— 跨交换机

➤ 将每台交换机的 1-10号接口划分到VLAN2，将11-20号接口划分到VLAN3



- PC1、PC3、PC5、PC7属于VLAN2，在同一个广播域内，可直接通信；
- PC2和PC6属于VLAN3，在同一个广播域内，可直接通信；
- PC4和PC8属于VLAN1，在同一个广播域内，可直接通信；

VLAN的划分方式

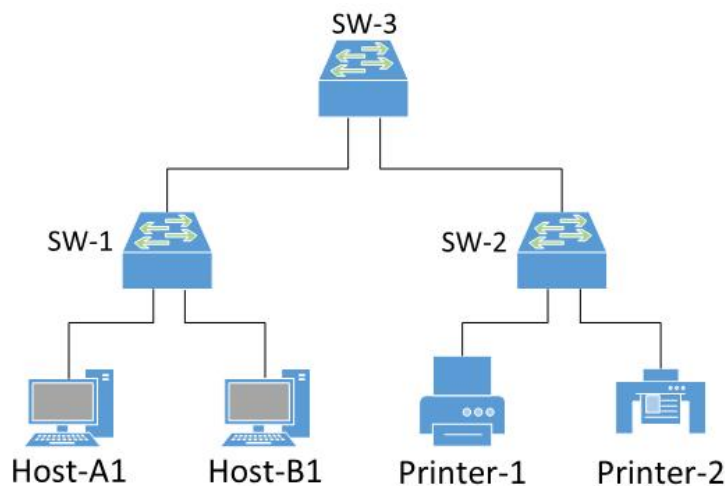
□ 基于MAC地址划分VLAN（自主学习）

- 基于接口划分VLAN时，当用户主机从交换机一个接口换到另一个接口时，所属VLAN就可能发生改变。若要保持VLAN不变，就需要重新配置接口，因此，通常用于用户主机位置不变的场合；
- 当用户对安全和移动性需求较高时，可以使用基于MAC地址划分VLAN的方法，即将用户计算机的MAC地址与指定的VLAN绑定起来，用户在变换物理位置后不需要重新划分VLAN，提高了终端用户的安全性和接入的灵活性。。

◆ 示例：基于MAC地址划分VLAN

□ 情景描述

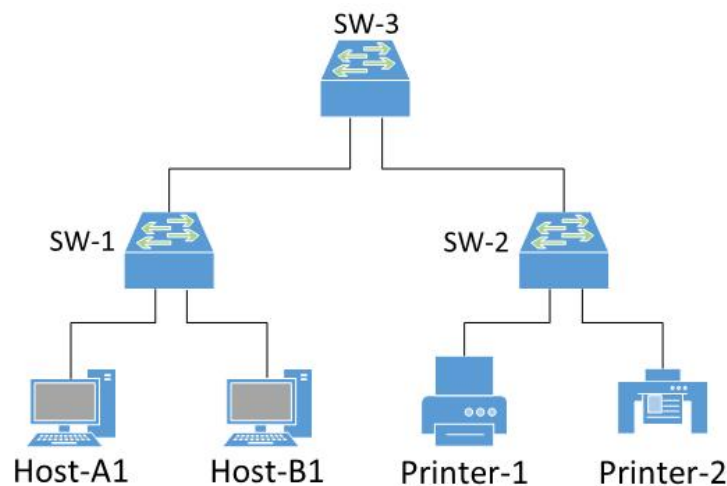
- 某公司A、B两部门的员工电脑通过交换机（SW-1）接入到公司网络，所有电脑的IP地址在同一网段。由于工作需要，每台电脑接入交换机的具体位置（即接口）不是固定的。
- 此外，公司有两台网络打印机，通过交换机SW-2接入到公司网络，并且接入到SW-2的位置固定。
- **要求：**通过VLAN设置，使得Printer-1只能被部门A的电脑访问，Printer-2只能被部门B的电脑访问。



◆ 示例：基于MAC地址划分VLAN

□ 分析

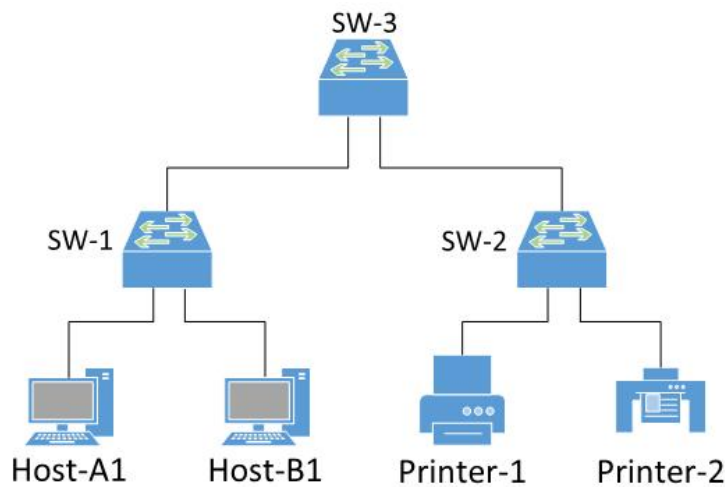
- 交换机SW-2应该基于接口划分VLAN，因为两台打印机的接入位置是固定的。
- 交换机SW-1不能基于接口划分VLAN，因为用户计算机的接入位置不固定



◆ 示例：基于MAC地址划分VLAN

□ 做法

- 在交换机SW-2上创建VLAN2和VLAN3，将Printer-1的接入接口划入VLAN2，Printer-2的接入接口划入VLAN3；
- 在交换机SW-1上也创建VLAN2和VLAN3；
- 将Host-A1的MAC地址与VLAN2绑定，将Host-B1的MAC地址与VLAN3绑定；
- 此时，Host-A1不论接入到SW-1的任何接口，只要其MAC地址不变，它都属于VLAN2，Host-B1同理。
- 实现情景描述的要求！



VLAN的划分方式

□ 其他划分VLAN的方法（略）

- 基于协议划分VLAN
- 根据IP组播划分VLAN
- 按策略划分VLAN
- 按用户定义、非用户授权划分VLAN

注意：本课程重点讲授基于接口划分VLAN的应用

三、IEEE802.1Q帧的结构与应用

- 应用VLAN后，帧结构有何变化？
- 应用VLAN后，交换机的通信有何变化？

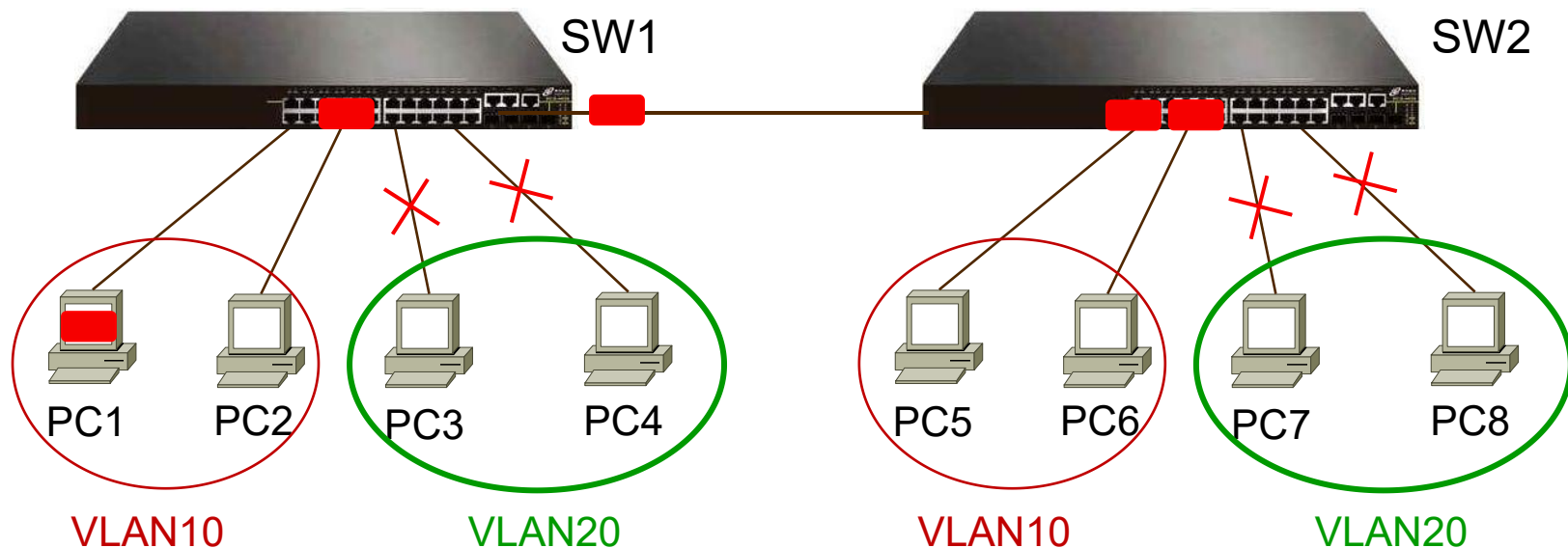
IEEE802.1Q帧的结构与应用

□ IEEE802.1Q标准的应用

- IEEE于1999年颁布了用于标准化VLAN实现方案的802.1Q协议标准草案。
- IEEE 802.1Q标准提供了对VLAN明确的定义及在交换式网络的应用。该标准的发布，确保了不同厂商提供的产品间的互操作能力，并在业界获得了广泛的推广，成为VLAN发展史上的里程碑。
- IEEE 802.1Q的出现打破了VLAN依赖单一厂商的僵局，从而推动了VLAN技术的迅速发展。

IEEE802.1Q帧的结构与应用

□ 创建了VLAN的交换机，如何知道从某一个接口进入的数据帧是属于哪个VLAN呢？（例，SW1如何知道PC1发出的帧，不能发给PC3和PC4呢？）



IEEE802.1Q帧的结构与应用

□ 创建了VLAN的交换机，如何知道从某一个接口进入的数据帧是属于哪个VLAN呢？

- 解决的方法就是：给普通帧（以太网帧）加上VLAN标签。
- IEEE 802.1Q标准规定：配置VLAN的交换机，在接收到以太网帧后，入接口会自动在帧头中的源MAC地址后增加一个4字节的802.1Q标签，用来指明该帧的VLAN属性。
- 这样，一个普通帧（untagged帧），就变成了802.1Q帧（tagged帧），会依据交换机的VLAN配置，进行传输。
- 802.1Q帧结构？（见下页）

➤ 802.1Q的帧结构

802.1Q帧



1. 2字节的协议标识符，置0x8100固定值，表明该帧带有802.1Q标记信息；
2. 2字节的标记控制信息，包含了3个域：
 - ① 表示报文优先级，占3bit，取值0到7，7为最高；
 - ② 表示规范格式指示符，占1bit，0表示规范格式，应用于以太网，1表示非规范格式，应用于Token Ring；
 - ③ VID：表示VLAN编号，占12bit，用于表示VLAN的归属，其中，VID=0用于识别帧优先级，4095 (FFF) 作为预留值，**所以有效的VLAN ID范围为1-4094。**

IEEE802.1Q帧的结构与应用

□ 划分VLAN后，交换机如何转发数据？

- **回忆：**交换机在收到数据帧之后，通常会根据帧首部的MAC地址与自身的MAC表来决定如何转发数据帧。这里我们将VLAN信息结合在一起理解。
- 引入VLAN概念后，MAC地址表项中，增加了VLAN ID属性，表示接口所属的VLAN。
- **举例说明**

➤ 举例：划分VLAN后，交换机如何转发数据？

目的 MAC地址	VLAN ID	接口
MAC_PC1	1	1
MAC_PC2	1	2
MAC_PC3	2	4
MAC_PC4	3	6

- 主机发出的数据帧是untagged帧，进入交换机后，被加上VLAN标签成为tagged帧，其中的VID值等于入接口所属的VLAN值；
- 交换机在MAC地址表中查找时，不仅要判断目的MAC是否匹配，还要判断相应接口的VID值是否与tagged帧的VID值相同，若全部匹配则转发，否则就丢弃。

例如：交换机内部的一个tagged帧，帧头中目的MAC是PC3-MAC，VLAN标签中VID=4
处理：虽然目的MAC与第3条记录对应，但因为帧的VID与对应接口的VID值不匹配，丢弃

IEEE802.1Q帧的结构与应用

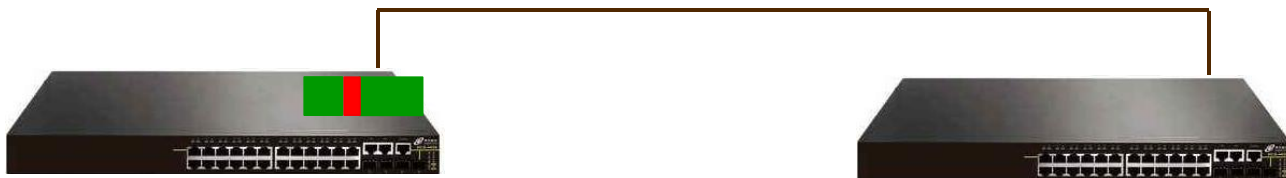
□ 802.1Q帧的传输

- 一个untagged帧进入交换机，被加上入接口的VLAN标签，变为tagged帧；
- 当tagged帧从交换机中发出时，VLAN标签是保留？还是去掉？
- 分为两种情况

IEEE802.1Q帧的结构与应用

□ 802.1Q帧的传输——情况1

- 如果发送至另一个支持 802.1Q 的设备（如另一个交换机），那么这些 tagged 帧可以被传送到另一个 802.1Q 设备中，即在交换机之间传送 VLAN 成员信息，这样 VLAN 就可以跨越多台交换机。

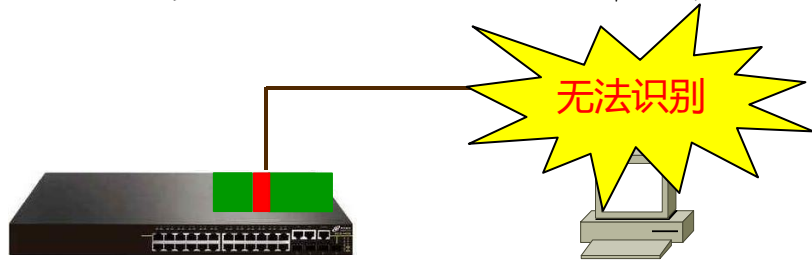


加标签帧在不同交换机之间传输，通常保留VLAN标签

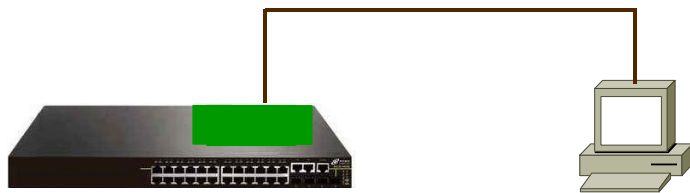
IEEE802.1Q帧的结构与应用

□ 802.1Q帧的传输——情况2

- 若交换机接口连接的是一个**不支持**802.1Q的设备，则加标签帧在离开接口时必须**去掉**VLAN标签，使其**变为普通帧**，这一点非常重要。因为很多PC和打印机的网卡并不支持 802.1Q，一旦它们收到一个加标签帧，它们会因为读不懂VLAN标签而丢弃该帧。



PC机无法识别加标签的VLAN帧



加标签帧发送到PC机之前，必须去掉VLAN标签

IEEE802.1Q帧的结构与应用

□ 因此，支持 802.1Q 的交换机，其必须具有**两种动作**：

■ **(1) 加标签**

➤ 将802.1Q 标签加入到普通帧（untagged帧）首部的操作。通常指**入接口**操作。

■ **(2) 去标签**

➤ 将802.1Q 标签从tagged帧头中去掉的操作。通常指**出接口**操作。

IEEE802.1Q帧的结构与应用

□ 提出问题:

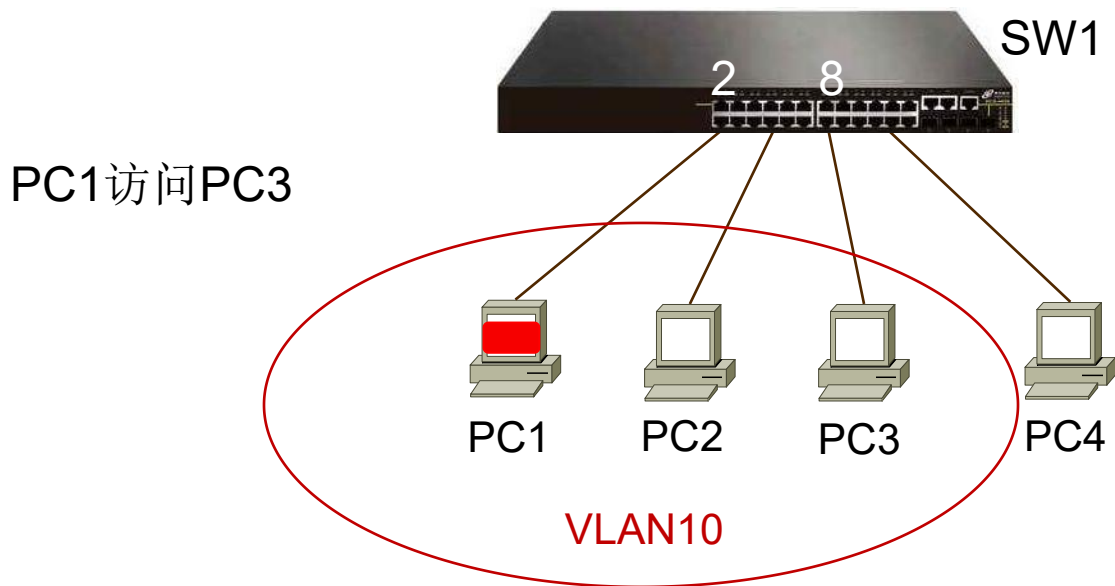
- 加标签和去标签的具体操作是如何进行的呢?

四、交换机接口的PVID 和 VID属性

理解PVID 和 VID

□ 谁来对数据帧进行加标签和去标签的具体操作呢？

■ 是交换机的接口！



理解PVID 和 VID

□ 谁来对数据帧进行加标签和去标签的具体操作呢？

- 应用VLAN时，要对交换机接口进行配置，以满足加标签和去标签的需求；
- 在VLAN应用中，交换机接口有两个重要的属性：PVID和VID；它们对于VLAN的通信过程、包括加标签和去标签的过程起着重要的作用。

理解PVID 和 VID

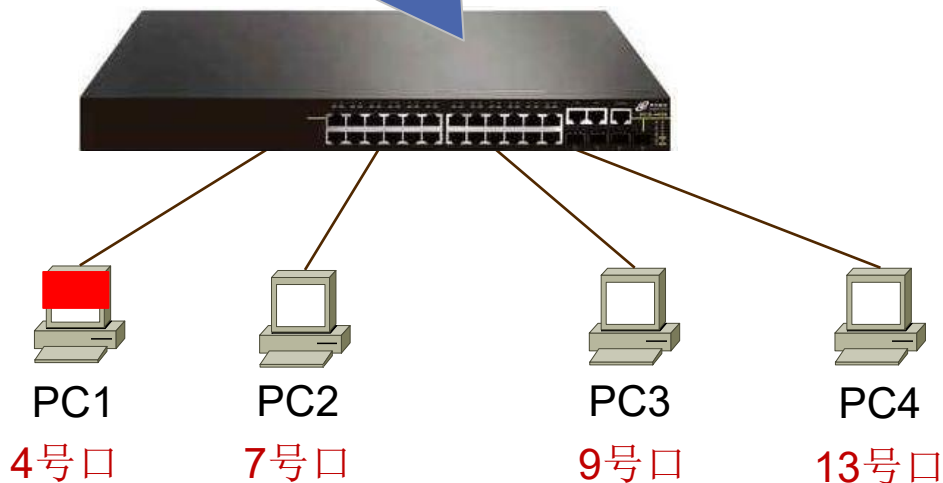
□ 接口的PVID 属性

■ PVID (Port VLAN ID)

- 表示接口能够将**从外部接收**的帧**发向哪个VLAN**，是接口的属性。强调的是**“发”**属性！
- 当一个**普通帧**（untagged帧）进入交换机接口时，会被该接口打上VLAN标签，成为tagged帧，并且将接口的PVID值，作为VLAN标签中的VID值（例如10）。
- 举例

◆ 举例：接口PVID属性的应用

该帧进入4号口，被加上VLAN标签，且标签中的VID值=4号口PVID值=2。表示该帧在交换机内部能够被发往属于VLAN 2的接口。



➤ 接口的PVID值：

4号口：PVID=2

7号口：PVID=2

9号口：PVID=2

13号口：PVID=3

21号口：PVID=1

.....

注意：接口的PVID值只有一个！

理解PVID 和 VID

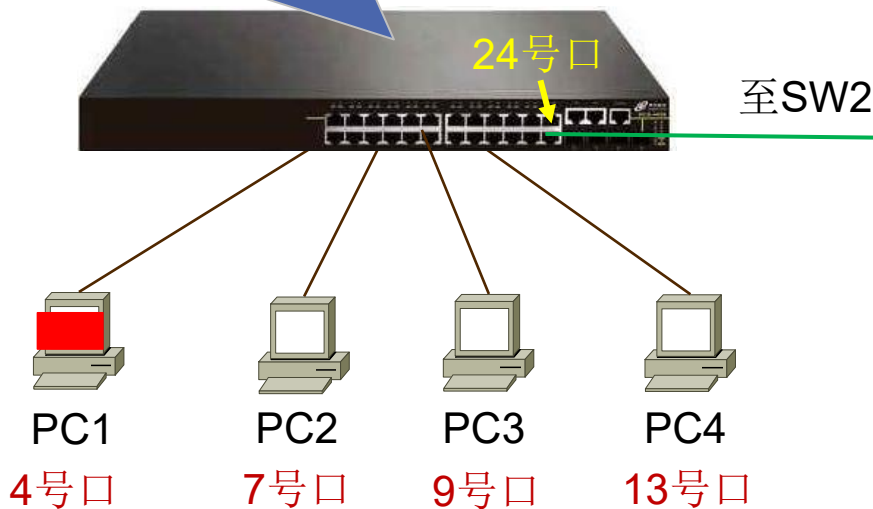
□ 接口的VID属性

■ VID (VLAN ID)

- 表示接口能够**从交换机内部接收**哪些VLAN的数据，也是接口属性。强调的是**“收”**属性！
- 交换机收到（从外部发来）一个普通帧后，会给他加上VLAN标签（用到PVID属性），交换机**内部**在转发VLAN帧（tagged帧）时，会根据该帧VLAN标签中的VID值，检查哪些接口的VID属性值与它相同，如果相同则继续比较该帧头中的目的MAC地址与接口的MAC表项是否匹配，如果匹配则转发给这个接口。（举例）

◆ 举例：接口VID属性的应用

该帧从4号口进入，被4号口加上VLAN标签，且标签中的VID值=2（假设4号口 PVID=2）。
只有VID属性值=2的接口，才能接收该帧，即只有7、9、24号接口能够接收该帧。



➤ 接口的VID值：

4号口：VID=2

7号口：VID=2

9号口：VID=2

13号口：VID=3

24号口：VID=1、2、3

.....

注意：接口的VID值可以有多个！

24号口，可以接收交换机内部发来的VID=1、VID=2或VID=3的tagged帧，并发送出去（出交换机）

理解PVID 和 VID

□ 提出问题:

- 接口的PVID值和VID值如何设置?
- 引入VLAN接口类型的概念
- Access
- Trunk
- Hybrid

五、交换机VLAN接口的类型

—— 从VLAN接口类型，深入理解VLAN通信过程

VLAN接口的类型

□ VLAN应用中的接口类型

- 根据对普通帧（untagged帧）和加标签帧（tagged帧）的处理方式，通常把交换机的VLAN接口分为：

Access接口

Trunk接口

Hybrid接口

VLAN接口的类型 —— Access接口

VLAN接口的类型 —— Access接口

□ 认识Access接口

- 当一个VLAN的接口设置成Access类型时，接口的

PVID值 = VID值 = 该接口所属VLAN的ID值

例如，把2号口设置成Access类型并划入VLAN10，则2号口的PVID=VID=10；

- Access类型的接口，只能属于一个VLAN。

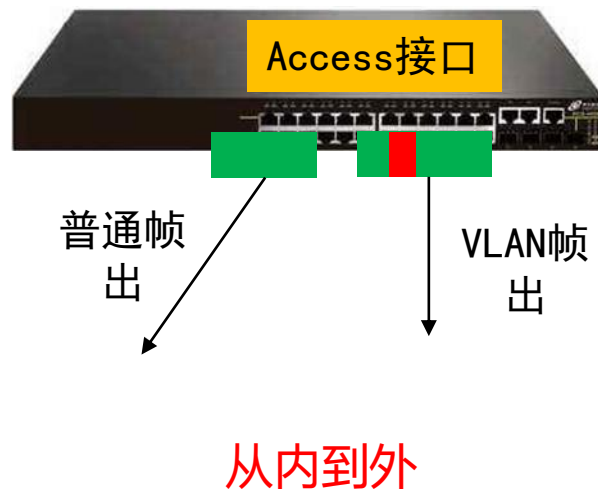
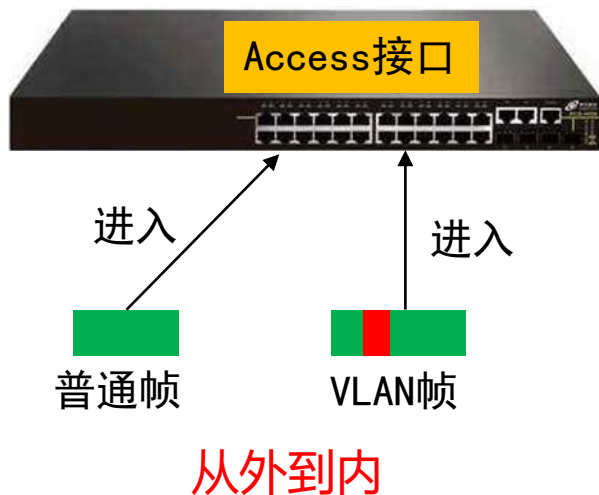
➤ 例如，一个Access接口原来属于VLAN 2，若管理员又将其重新划分到VLAN 3中，则该接口就属于VLAN 3，不再属于VLAN 2，且其PVID=VID=3。由此可知，Access类型的接口，其PVID和VID属性值都只有一个。

- Access接口通常用于连接用户主机。

VLAN接口的类型 —— Access接口

Access接口对进、出的数据帧的处理

- 帧进、出Access接口时，Access接口是如何在帧首部添加或去掉VLAN标签的？
- 统一说法：何谓进？出？



VLAN接口的类型 —— Access接口

□ Access接口对进入数据帧的处理

■ 普通帧进入Access接口时：

- 由于Access接口连接的通常是计算机，所以通常情况下进入Access接口的是普通帧（不含VLAN标签）。此时，Access接口会给普通帧添加VLAN标签，并把自己的PVID值加入到VLAN标签的VID中。然后在交换机内部进行转发，转发给同VLAN的其他接口。

■ VLAN帧（tagged帧）进入Access接口时：

- Access接口用来连接计算机，而计算机发出的帧是普通帧，所以VLAN帧进入Access接口的情况很少出现。
- 可自行设计实验，验证这种情况。

VLAN接口的类型 —— Access接口

□ Access接口对发出数据帧的处理

■ VLAN帧从Access接口发出时：

- 当VLAN帧（tagged帧）从Access接口发出时，Access接口会把帧中的VLAN标签去除，然后把一个普通帧发给该Access接口所连接的计算机。

■ 普通帧从Access接口发出时：

- 无此情况。（为什么？）

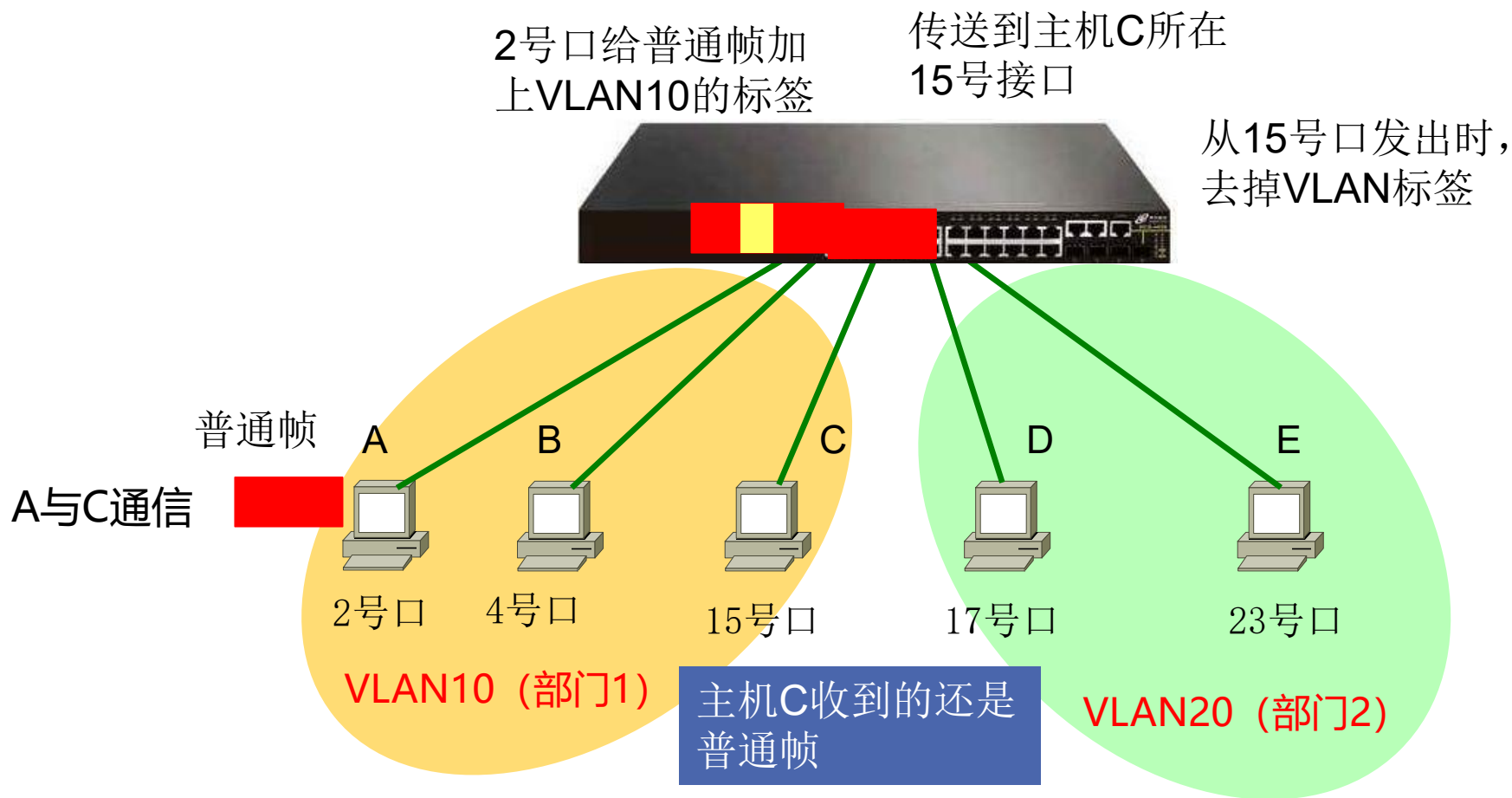
- 帧在交换机内部时，都是带VLAN标签的，别忘了，交换机还有一个默认的VLAN 1。

VLAN接口的类型 —— Access接口

□ 举例：一个Access接口被划分到了VLAN10（即PVID=VID=10）

- 当一个普通帧进入该接口，接口会给普通帧添加VLAN标签，并且在VLAN标签的VID字段中写入10。（PVID属性值的作用）
- 根据VLAN的原理，在交换机内部，该VLAN帧只能被转发到属于VLAN 10的其它接口（即这些接口的VID属性值=10）。
- 该VLAN帧（即加VLAN10标签的帧）从属于VLAN10的其它Access接口发出时，该标签会被去除，将普通帧发给计算机。
- 该VLAN帧（即加VLAN10标签的帧）不会被转发到VID≠10的接口。
- 过程见下页动画

➤ Access接口对帧的处理



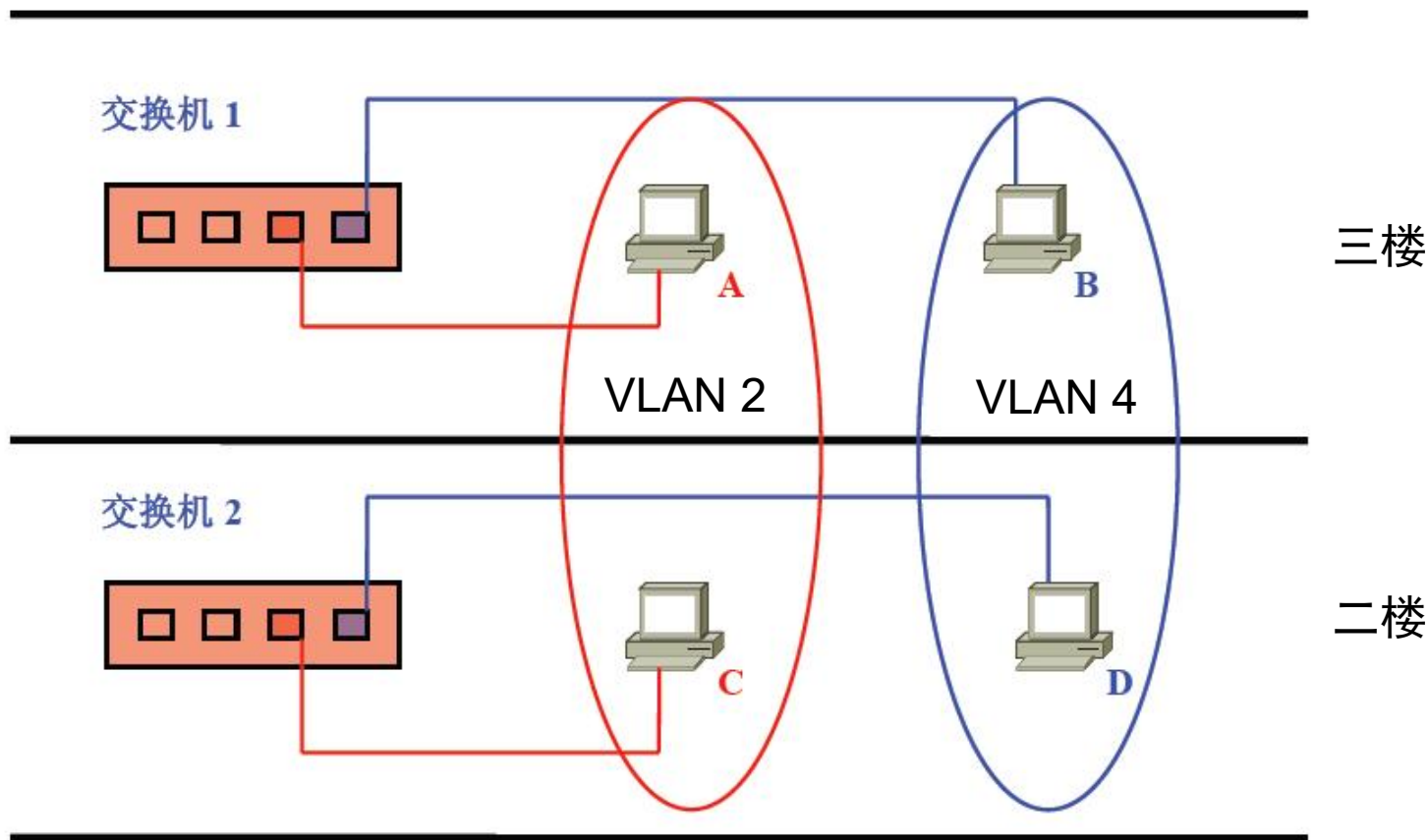
VLAN接口的类型 —— Trunk接口

VLAN接口的类型 —— Trunk接口

□ 认识Trunk接口

- 当需要在交换机之间，传递VLAN帧时，就需要用到Trunk接口。
- 先来分析以下案例：
 - 在规划企业级网络时，很有可能会遇到隶属于同一部门的用户分散在同一座建筑物中的不同楼层的情况，这时就需要跨越多台交换机设置VLAN。

- ◆ 举例：有如下图所示的网络，需要将处于不同楼层的A、C划入VLAN2，将B、D划入VLAN4。



VLAN接口的类型 —— Trunk接口

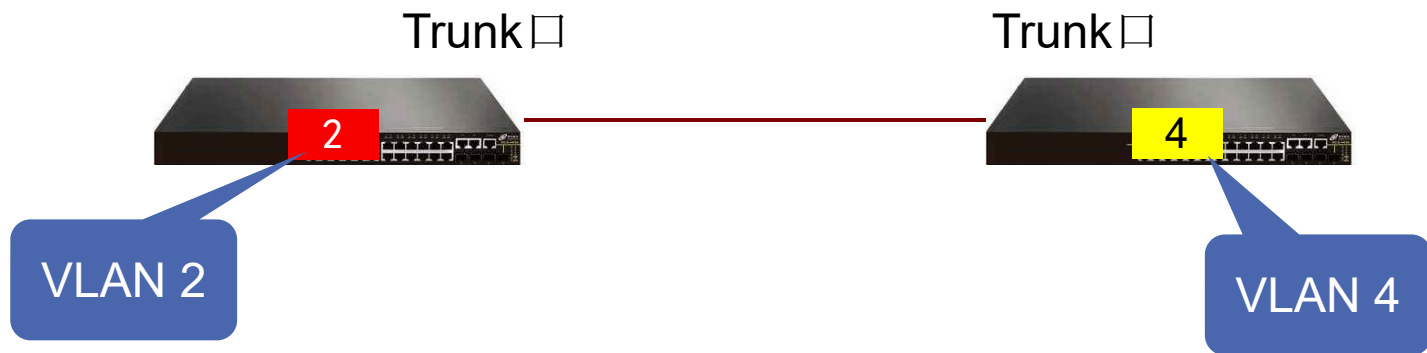
□ 认识Trunk接口

- 此处最关键的就是“交换机1和交换机2之间该如何连接才好呢？”
- 一种思路：在交换机1和交换机2上各设一个Access类型接口，并且让它们都属于VLAN 2，然后通过这两个Access接口把两台交换机级联起来，实现VLAN2中的计算机跨交换机通信。
- VLAN 4同理
 - 举例

VLAN接口的类型 —— Trunk接口

□ 认识Trunk接口

- 此处最关键的就是“交换机1和交换机2之间该如何连接才好呢？”
- 当VLAN跨交换机时，连接两个交换机的接口通常被设置成Trunk模式。
 - Trunk接口允许多个VLAN的流量通过，即Trunk接口的VID属性值可以是多个。（Access接口的VID属性值只有一个，且只能转发一个VLAN 的帧）。



VLAN接口的类型 —— Trunk接口

□ Trunk接口的应用

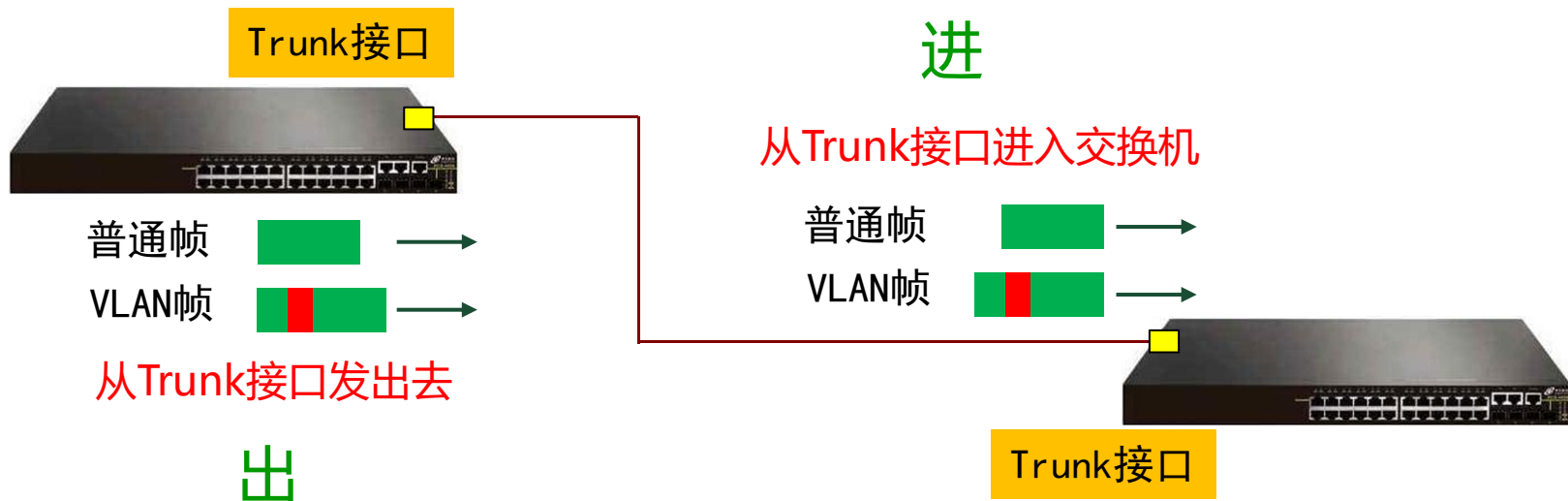
■ 注意：

- 虽然Trunk接口可以属于多个VLAN（即接口的VID属性值可以是多个），但Trunk接口PVID值只能有一个，且必须是VID属性值当中的一个。
- 缺省情况下，Trunk接口的PVID=1，它不会自动变化，但可以由管理员手工更改。（回忆一下：Access接口的PVID值，随着该接口所属VLAN的不同，其PVID值会自动变化）

VLAN接口的类型 —— Trunk接口

Trunk接口对进、出的数据帧的处理

- 数据帧进、出Trunk接口时，Trunk接口是如何在帧首部添加或去掉VLAN标签的？



VLAN接口的类型 —— Trunk接口

□ Trunk接口对进入数据帧的处理

■ 普通帧进入Trunk接口时：

- 这种情况比较少，因为Trunk接口通常连接另一台交换机的Trunk接口，因此收到的通常都是tagged帧。
- 当然，一些特殊情况下，一个Trunk接口也可能收到untagged帧（例如Trunk口连接计算机），此时，Trunk接口会在untagged帧上加上VLAN标签，标签中的VID值等于Trunk接口的PVID值（默认是1），然后将该帧转发到与PVID值相同的VLAN的其他接口（例如属于VLAN 1的其他接口）。
- 若管理员把trunk接口的PVID值改为100？

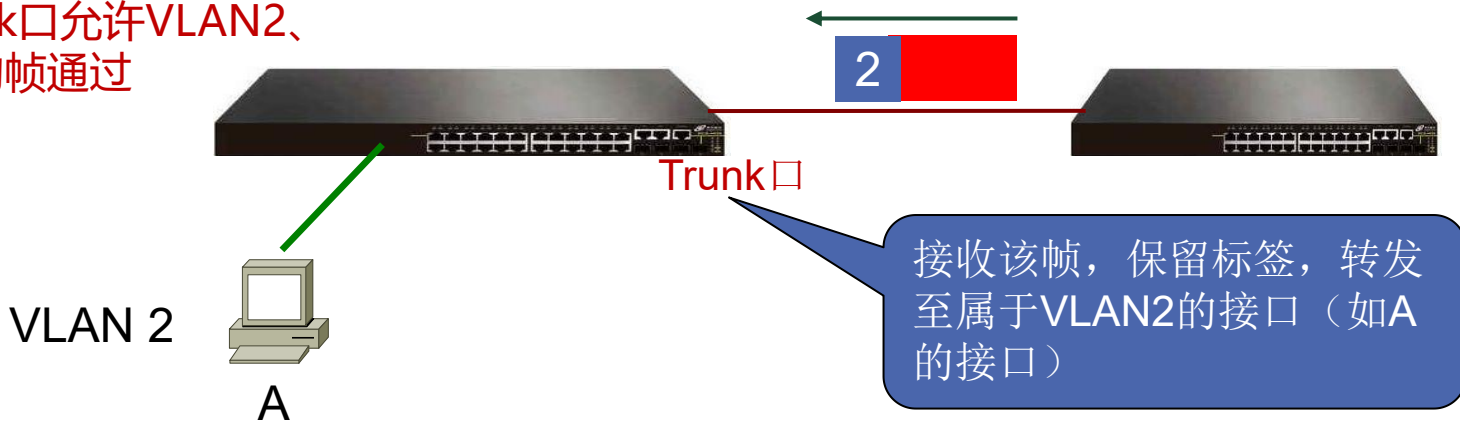
VLAN接口的类型 —— Trunk接口

Trunk接口对进入数据帧的处理

■ VLAN帧进入Trunk接口时：

- Trunk口收到VLAN帧（Tagged帧），若帧头VLAN标签中的VID值，在允许通过之列，则保留VLAN标签并将其转发到本交换机上属于相同VLAN的接口。

此处Trunk口允许VLAN2、
VLAN3的帧通过



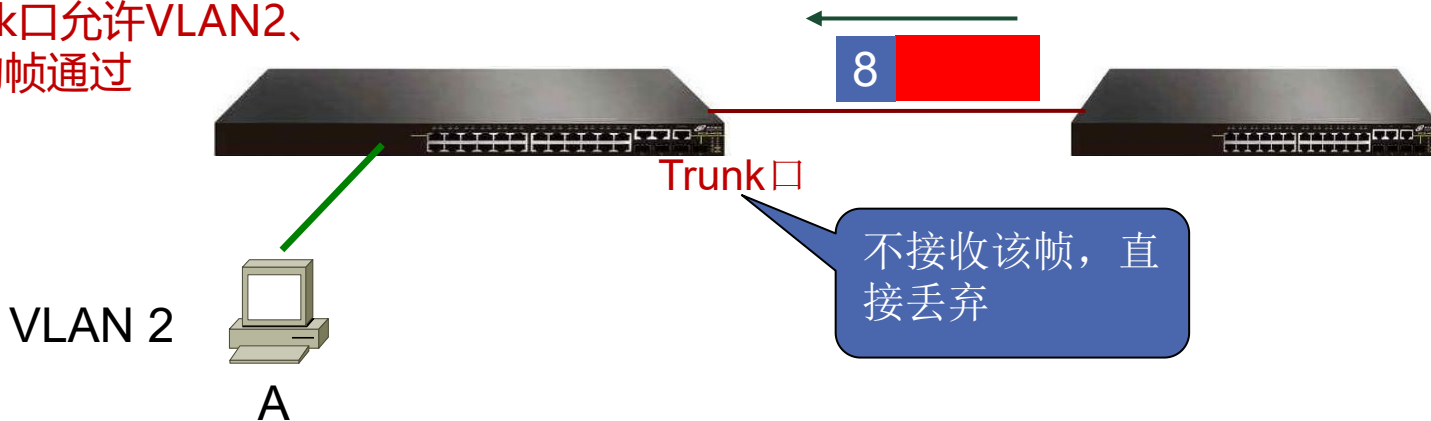
VLAN接口的类型 —— Trunk接口

□ Trunk接口对进入数据帧的处理

■ VLAN帧进入Trunk接口时：

- ▶ Trunk口收到VLAN帧（Tagged帧），若帧头VLAN标签中的VID值，不在允许通过之列，则直接丢弃。

此处Trunk口允许VLAN2、
VLAN3的帧通过



VLAN接口的类型 —— Trunk接口

□ Trunk接口对发出数据帧的处理

■ VLAN帧（即Tagged帧）从Trunk接口发出时：

- 对于帧VID=Trunk口PVID值的VLAN帧，去掉VLAN标签再发送出去；
- 对于帧VID≠Trunk口PVID值的VLAN帧，直接发送出去并保留VLAN标签。
- **注意：**由于Trunk接口的PVID值通常保持缺省值（即1），因此VLAN帧从trunk接口发出时，通常不去掉标签。

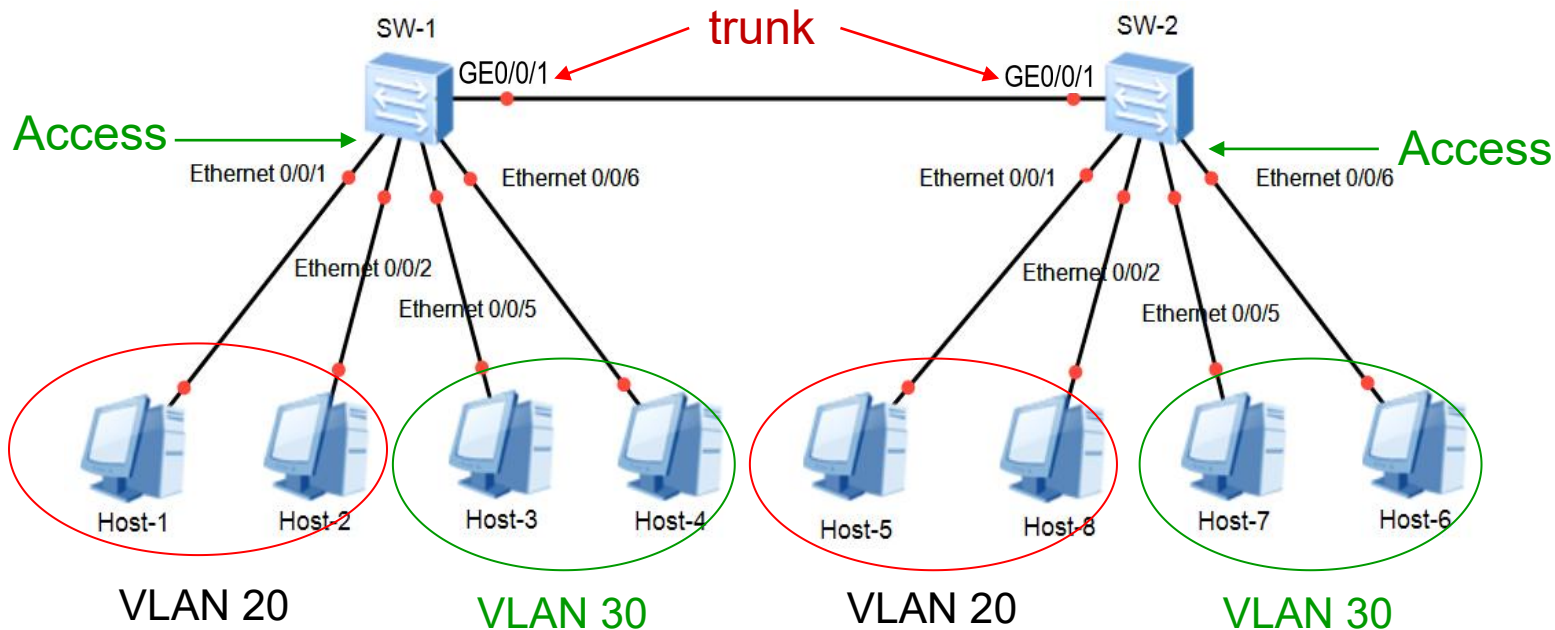
■ 普通帧从Trunk接口发出时：

- 普通帧进入配置VLAN的交换机后，都会被添加VLAN标签（包括VLAN 1），因此，无此情况；

操作案例：Access接口 和 Trunk接口的配置

操作案例：Access接口和Trunk接口的配置

- ❑ 交换机VLAN设置如图所示
- ❑ 将连接主机的接口设为Access口，交换机互连接口设为Trunk口



操作案例：Access接口 和 Trunk接口的配置

【在SW1上进行配置】 (SW2的配置同理)

//创建VLAN10和VLAN20

```
[SW-1]vlan batch 10 20 //创建VLAN20和VLAN30
```

//将Ethernet0/0/1和Ethernet0/0/2接口设置成Access类型并划入VLAN10

```
[SW-1]interface Ethernet 0/0/1
```

```
[SW-1-Ethernet0/0/1]port link-type access
```

```
[SW-1-Ethernet0/0/1]port default vlan 10
```

```
[SW-1]interface Ethernet0/0/2
```

```
[SW-1-Ethernet0/0/2]port link-type access
```

```
[SW-1-Ethernet0/0/2]port default vlan 10
```

//将Ethernet0/0/5和Ethernet0/0/6设成Access类型并划入VLAN20，操作同理

//将GEO/0/1接口设置成Trunk类型并允许VLAN10和VLAN20的数据帧通过

```
[SW-1]interface GigabitEthernet 0/0/1
```

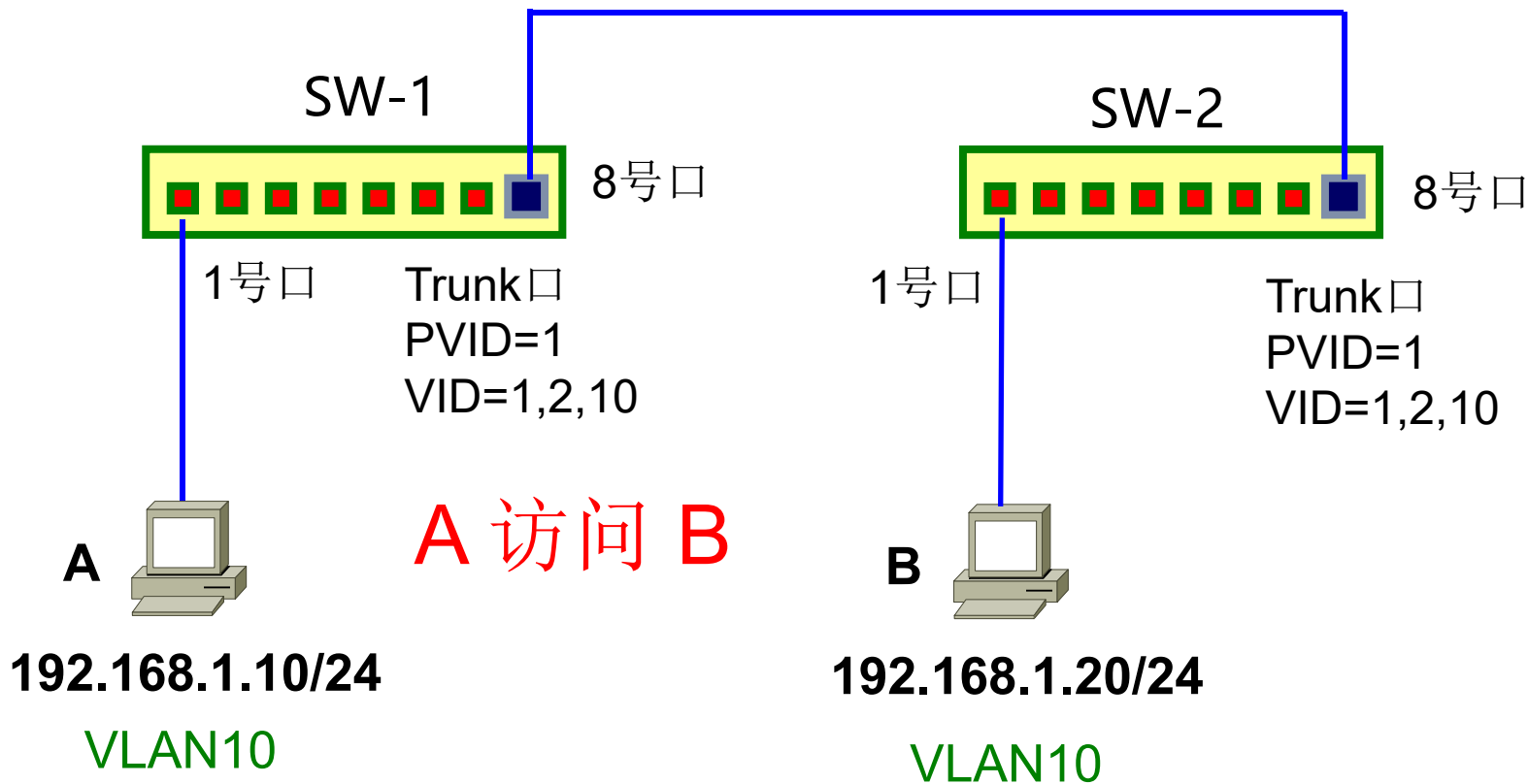
```
[SW-1-GigabitEthernet0/0/1]port link-type trunk
```

```
[SW-1-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20
```

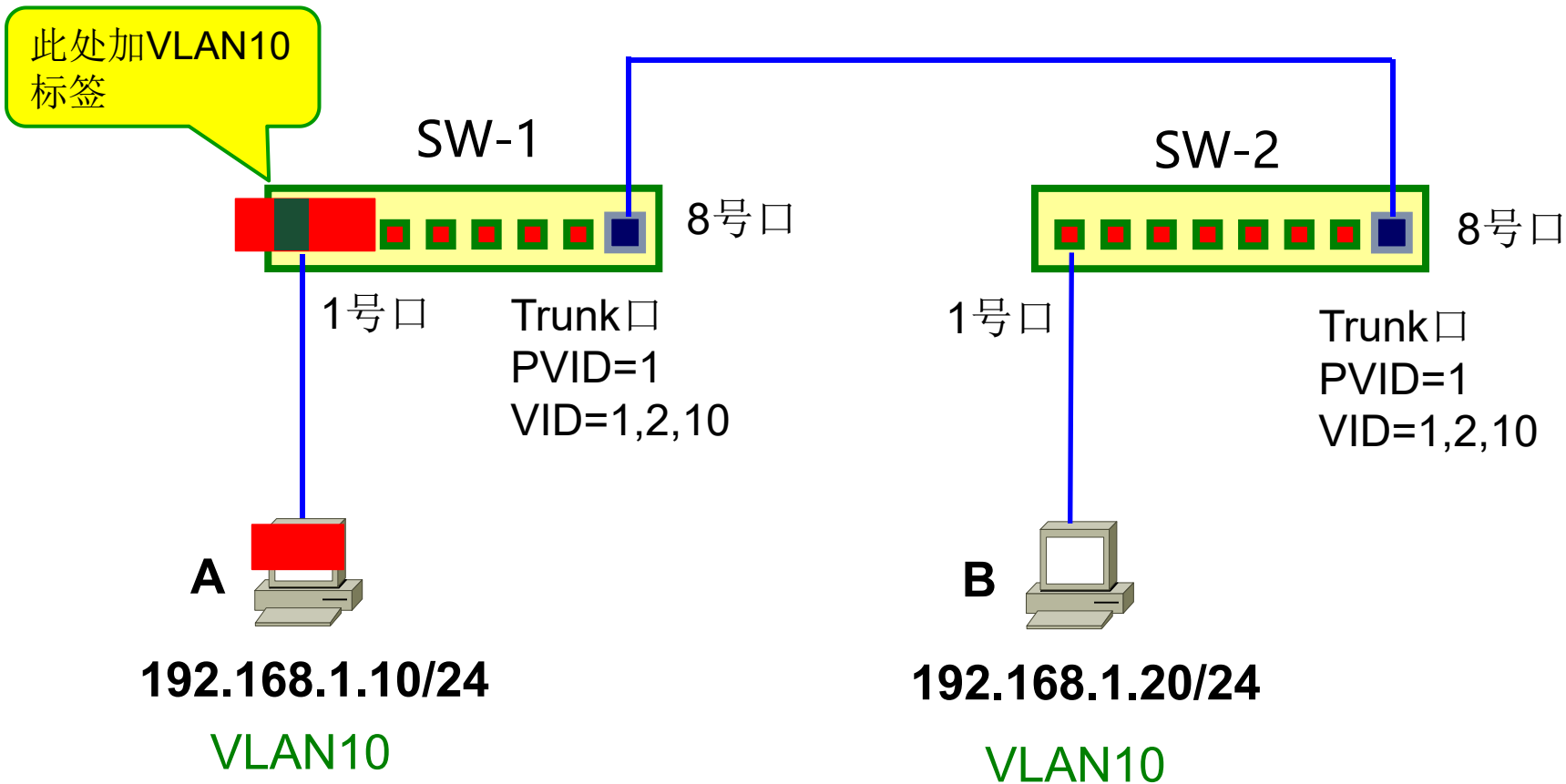
◆ 综合案例：

交换机划分VLAN后，Access接口和Trunk接口对通过的数据帧，加标签和去标签的过程。

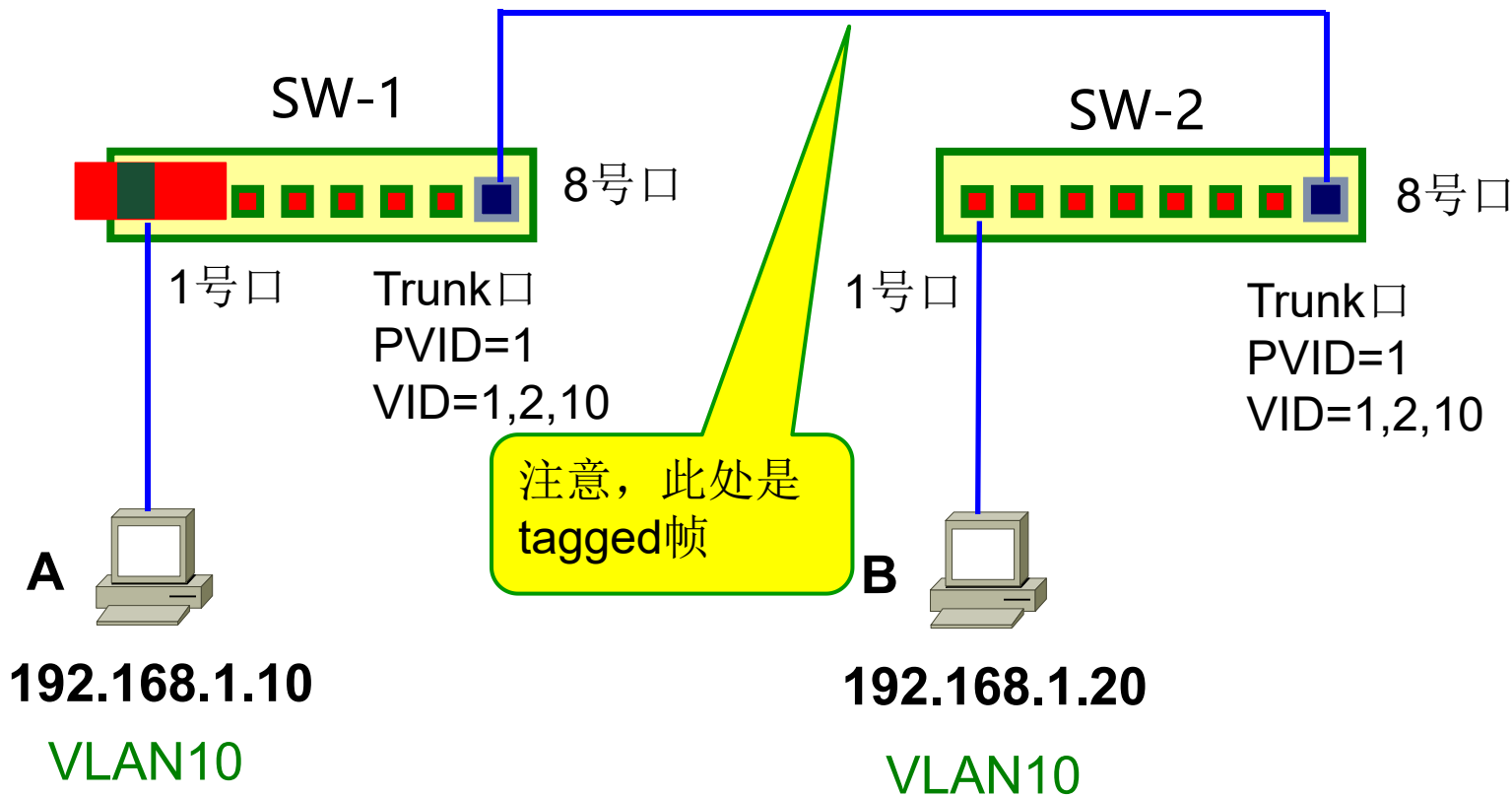
- 1号口都是Access口，属于VLAN10，其PVID值=VID值=10
- 8号口都是Trunk口，PVID值=1，允许VLAN 1、VLAN 2、VLAN 10的帧通过



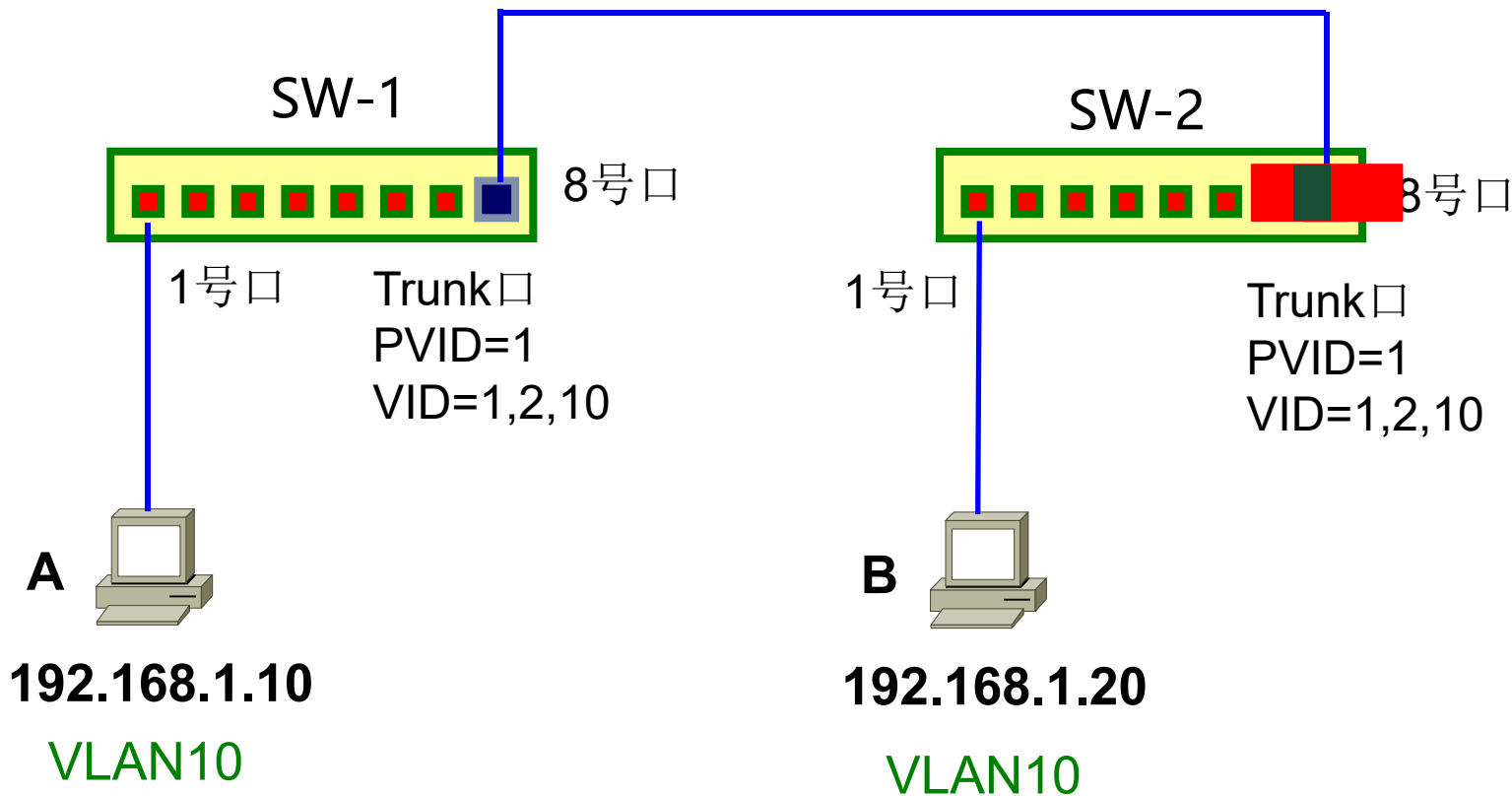
- PC-A发出普通帧，进入SW-1的1号口，普通帧被加上VLAN10的标签，使得该帧的VID=10



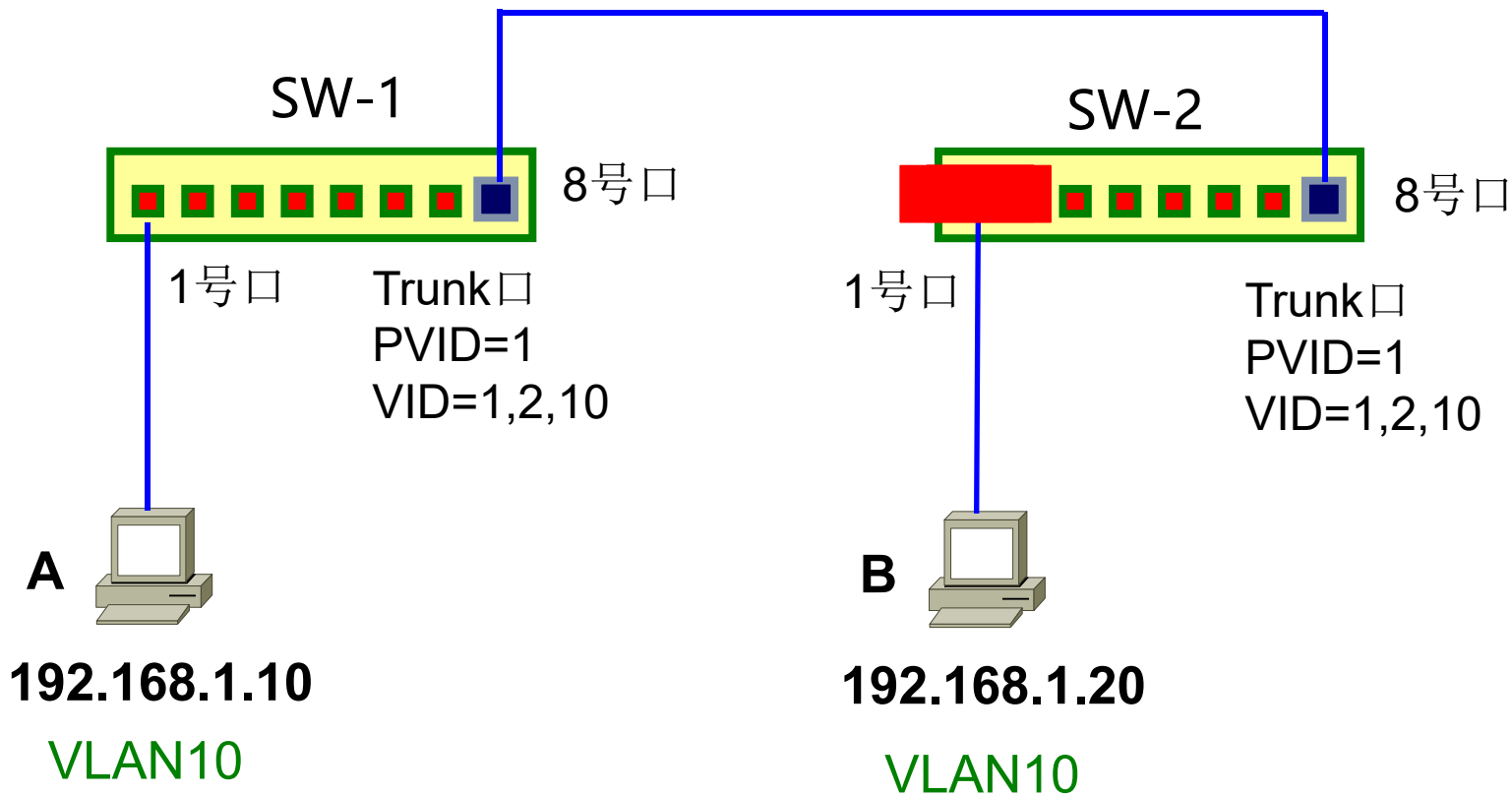
- 该tagged帧被转发至SW-1的8号口，由于8号口是Trunk口，且允许VLAN10的帧通过，且8号口PVID≠该帧的VID，因此，该帧被从8号口直接发出，不去掉标签。



- SW-2的8号口收到该tagged帧，由于8号口是Trunk口，且允许VLAN 10的帧通过，因此8号口不去掉该帧的VLAN标签，直接将其转发至VLAN 10的接口，此处，通过查询MAC地址表，将其发送到1号口。



- 该tagged帧从1号口发出，由于1号口是Access口，因此该tagged帧发出时，被去掉VLAN标签，变成普通帧，到达PC-B。



◆ 归纳：Access和Trunk接口对数据帧的处理

帧 接口	802.1Q帧（tagged帧）		普通帧 （untagged帧）	
	IN	Out	IN	Out
Trunk 接口	若允许通过，则接收，保持原有标签。 否则丢弃	若本接口的PVID=帧VID，则去掉帧中的VLAN标签，然后发出。 若本接口的PVID≠帧VID值，则直接发出，不去掉VLAN标签	按接口PVID值，添加VLAN标签	无此情况
Access 接口	若接口VID=帧VID则接收，否则丢弃	去掉标签，变为普通帧然后发出	按接口PVID值，添加VLAN标签	无此情况

接口的类型 —— Hybrid接口（自主学习）

VLAN接口的类型 —— Hybrid接口

□ 认识Hybrid接口

- 华为、H3C交换机的一种接口模式。
- Hybrid类型的接口既可以用来连接用户主机也可以用来连接其它交换机设备。



VLAN接口的类型 —— Hybrid接口

□ 认识Hybrid接口

■ 和Trunk接口 相同的是：

- Hybrid接口允许多个VLAN的帧通过，即它的接口VID属性值可以是多个；
- Hybrid接口的PVID值只能是一个，缺省是1，可以手工更改；
- Hybrid接口在接收数据时，处理方法也和Trunk接口一样
 - 对于tagged帧，若在允许通过之列的，接收，并保留标签；
 - 对于untagged帧，接收，加上VLAN标签，且帧中VID=接口PVID

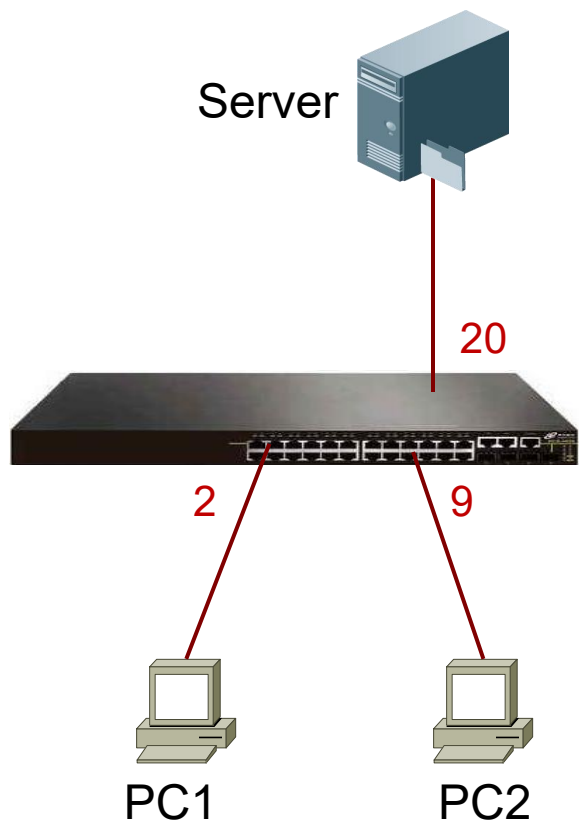
VLAN接口的类型 —— Hybrid接口

□ 认识Hybrid接口

■ 和Trunk接口不同的是：体现在向外发送tagged帧时的做法

- Hybrid接口在发出tagged帧时，可以设置成允许tagged帧不去掉VLAN标签直接发送出去（这一点依然与Trunk接口有相似之处）；
- Hybrid接口在发出tagged帧时，也可以设置成将tagged帧去掉VLAN标签变为普通帧后，再发送出去，而不论帧中的VID值是多少。（这一点与Trunk接口不同，Trunk接口只在接口PVID值=帧VID值时，去掉帧中的VLAN标签再发出）；

◆ 演示：Hybrid接口应用举例



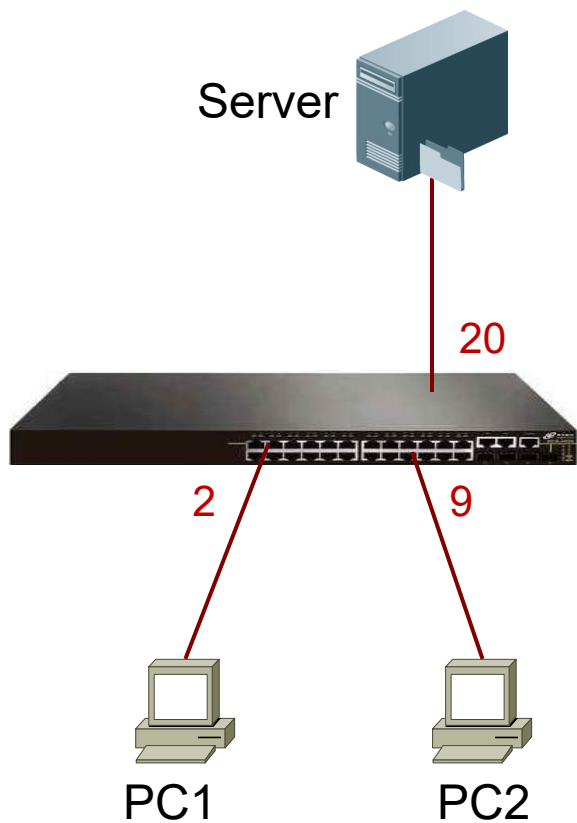
➤ 情景描述

PC1接入交换机的2号口，PC2接入交换机的9号口，服务器接入20号口。

➤ 要求

PC1和PC2之间不能互访，但都可以访问Server。

◆ 演示：Hybrid接口应用举例



□ 配置规划

➤ VLAN设计

- VLAN10、VLAN20、VLAN100

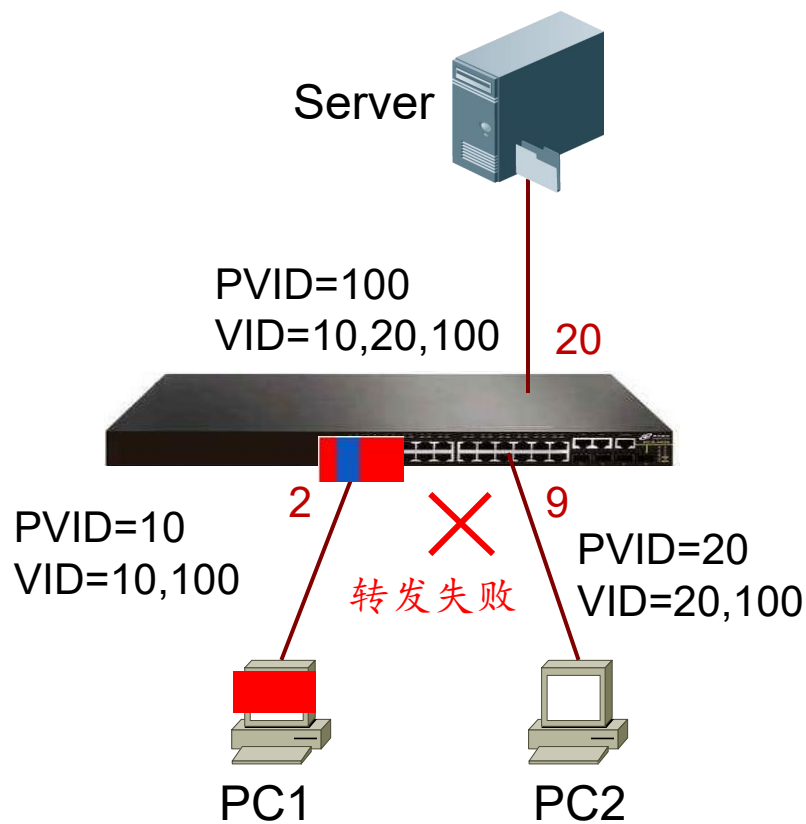
➤ 接口配置

- 2号口：Hybrid类型，
PVID=10 VID=10, 100
- 9号口：Hybrid类型
PVID=20 VID=20, 100
- 20号口：Hybrid类型
PVID=100 VID=10, 20, 100
- 2、9、20号口在发出VLAN帧时，
去掉VLAN标签

➤ IP地址规划

- 192.168.0.0/24

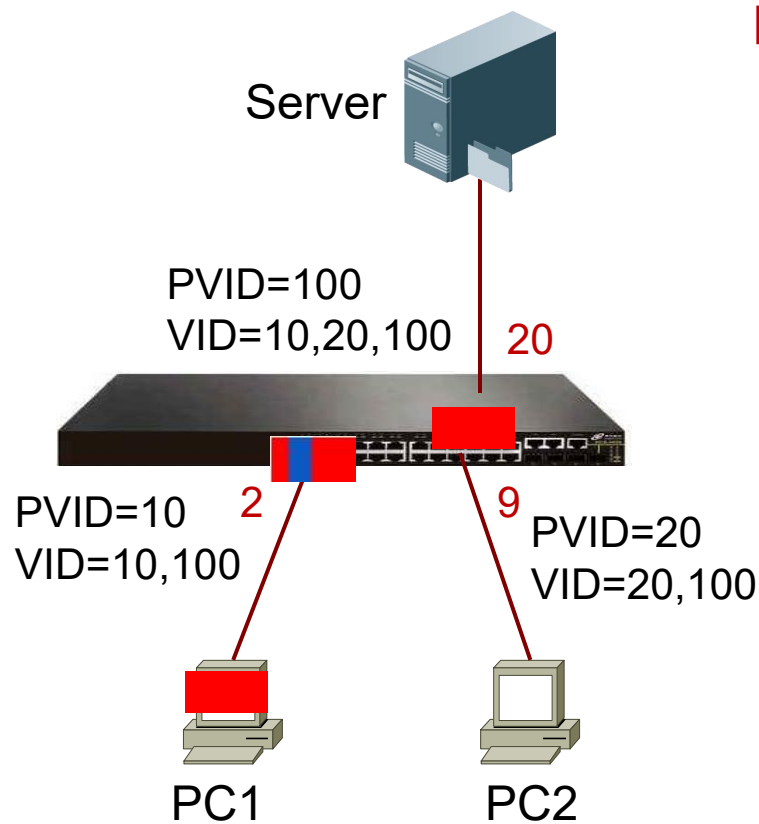
◆ 演示：Hybrid接口应用举例



□ 通信分析1：PC1 访问 PC2

1. PC1发出普通帧，到达2号口；
2. 2号口添加VLAN标签，标签VID=PVID=10；
3. 交换机查看MAC地址表，发现目的MAC所对应接口（即9号口）的VID属性值包括20和100，不包括10，因此无法转发至9号口；
4. 访问失败，符合题目要求

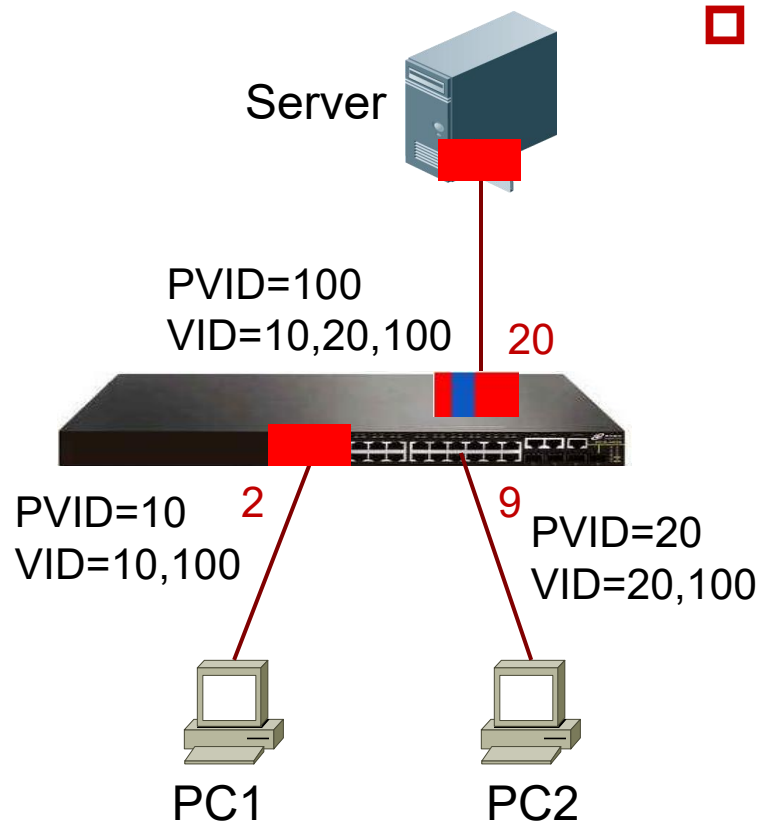
◆ 演示：Hybrid接口应用举例



□ 通信分析2：PC1 访问 Server

1. PC1发出普通帧，到达2号口；
2. 2号口添加VLAN标签，标签VID=PVID=10；
3. 交换机查看MAC地址表，发现目的MAC所对应接口（即20号口）的VID属性值包括10、20和100，因此转发至20号口；
4. 根据规划及配置，VLAN帧在从20号口发出时，要去掉VLAN标签，所以，变为普通帧发至Server。

◆ 演示：Hybrid接口应用举例



□ 通信分析2：PC1 访问 Server（返回）

1. Server发出确认报文（普通帧），到达20号口；
2. 20号口添加VLAN标签，标签VID=PVID=100；
3. 交换机查看MAC地址表，发现目的MAC所对应接口（即2号口）的VID属性值包括10、和100，因此转发至2号口；
4. 根据配置，VLAN帧在从2号口发出时要去掉VLAN标签，所以，变为普通帧发出。
5. 访问成功！符合题目要求

第3讲 虚拟局域网

完