我们学习过可以使用多个以太网交换机互连形成更大的广播域，但是随着用户主机接入的越来越多，可能需要加入更多的以太网交换机，广播域也会相应扩大，巨大的广播域会带来很多弊端：**广播风暴、难以管理和维护、潜在的安全问题。**

有的同学会有疑问：广播风暴真的那么容易发生吗？这个问题可以归结为网络中的广播帧很常见吗？

实际上网络中确实会经常出现广播帧，后续将学习到的协议比如ARP协议（已知IP地址，找出其相应的MAC地址）、路由信息协议RIP、动态主机配置协议DHCP等等。

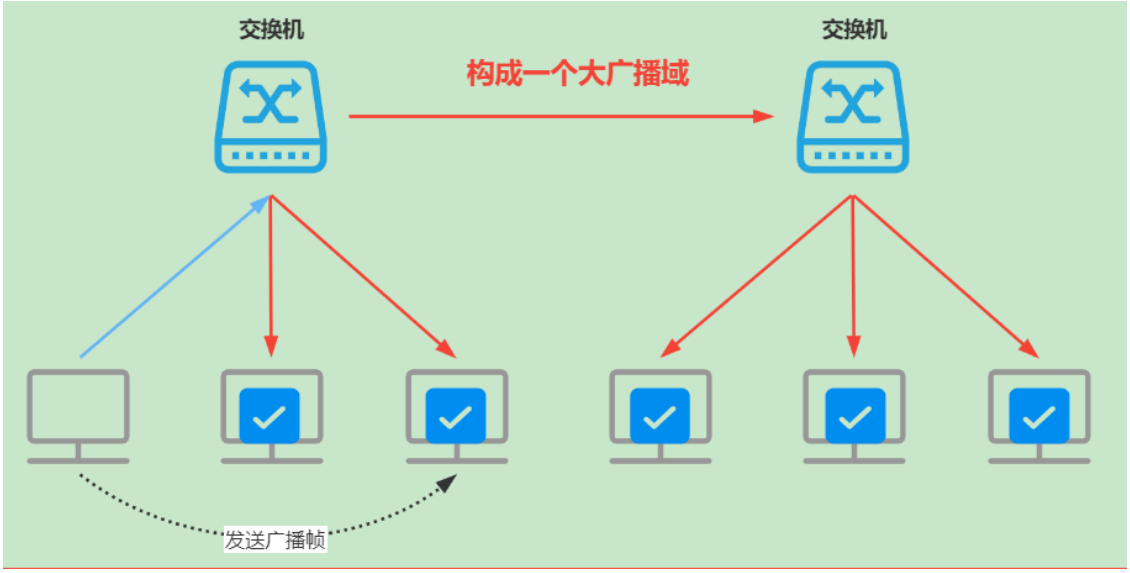
那么需要有一个方案可以来进行广播域的分隔，让一个无比巨大的广播域按照需求缩小为若干小的广播域，降低广播风暴带来的影响，方便进行网络管理，这个如何来做呢？

一、与神奇的路由器初见面！

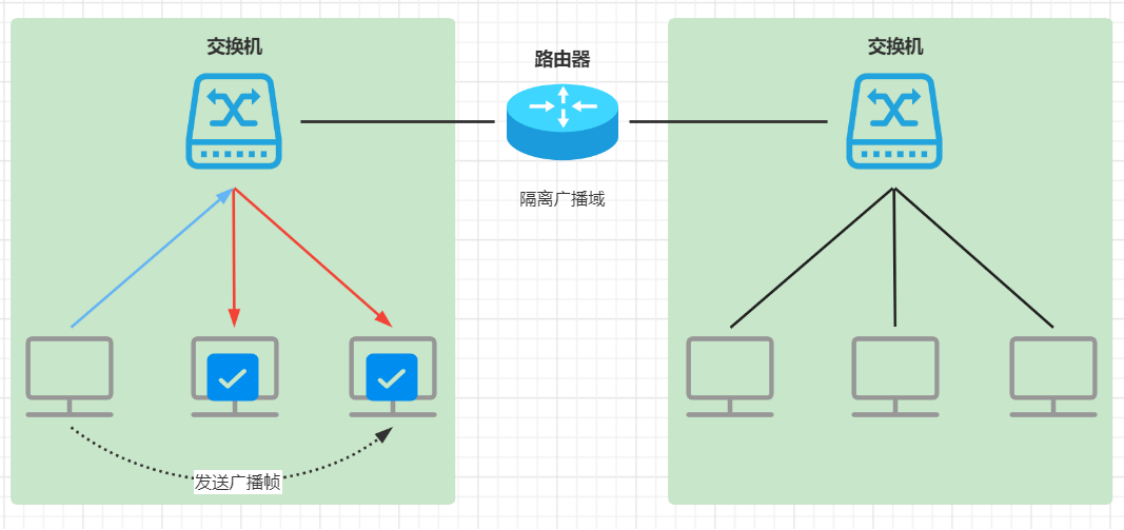
路由器是网络层的代表设备，我们暂且无需知道太多，只要知道：

由于路由器默认情况下不对广播数据包进行转发，因此路由器可以很自然地隔离广播域。

在只有交换机的情况下，两个交换机互联可将两个独立的广播域合并成一个大广播域：



如果加上路由器，可以将广播域进行隔绝：



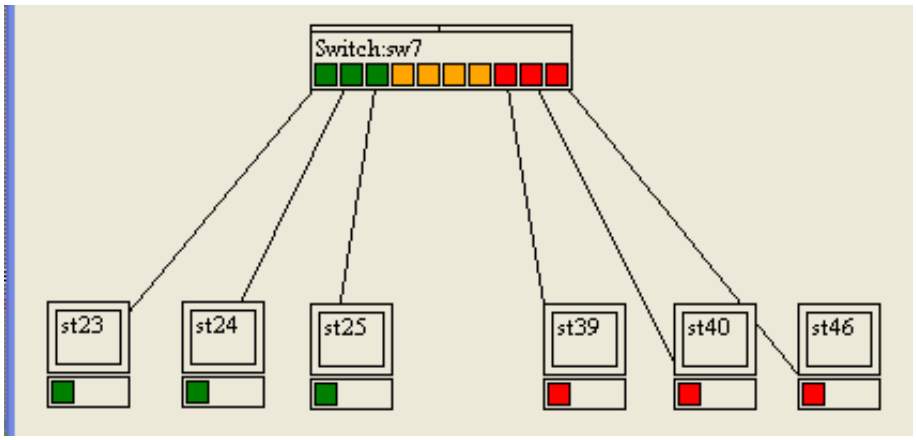
路由器强是强，但是价格成本高，在广大的局域网内部全部使用路由器来隔离广播域是不现实的，在这种情况下，虚拟局域网技术应运而生。

二、虚拟局域网VLAN概述！

LAN 是 Local Area Network 的缩写，表示“局域网”。VLAN 是 Virtual LAN 的缩写。因此 VLAN 就是虚拟局域网的意思。

VLAN 是一种技术。对于交换机来说，VLAN 就是将交换机的端口分隔到不同网络中的能力。简单来说就是分隔交换机的端口，这些被分隔开的端口不能再互相通信了。

假设我们的交换机有 10 个端口，上面连接了 6 台机器。我们希望前三台机器（在上图中是 23，24，25 这三台机器）可以互相通信，其他三台（在上图中是 39，40，46 这三台机器）也可以互相通信，但这两组机器不能跨组通信，彼此之间就好像被隔离了一样（因此是虚拟的分隔方式，而不是物理上的分隔）。



我们分别用绿色和红色标识这两个 VLAN。连接到属于绿色 VLAN 的端口的机器只能与绿色 VLAN 的机器进行通信。红色 VLAN 的情况也是一样。连接到绿色 VLAN 的机器无法与连接到红色 VLAN 的机器通信。

可以看到，通过vlan可将本来是一个大的广播域切分为了两个小的广播域，并且这两个小广播域内的主机之间在数据链路层上是不能直接互相通信的，这样，通过VLAN技术将不同用户在逻辑上进行了分组，做到了逻辑上的网络隔离，从而达到网络安全的目的。

可以想象，如果老师的网络和学生的网络在一起没有做隔离，一些怀有心思的学生通过一些手段可以登陆管理系统修改成绩，岂不是很糟糕?

三、VLAN的实现机制概述!

我们用以太网MAC帧为例，以太网的MAC帧的模样我们再来回顾下，实际上就是插入了4字节的VLAN标记，如下图所示：

这个插入VLAN标识的帧叫做IEEE 802.1Q帧。

VLAN标记的最后12比特称为VLAN标识符VID，它唯一标志了以太网帧属于哪一个VLAN。VID的取值范围是0 ~ 4095，其中0和4095都不用来标识VLAN，因此用于表示VLAN的VID的有效取值范围是1 ~ 4094。

切记，IEEE 802.1Q帧是交换机来处理的，并不是用户主机来处理的：

- **当交换机收到普通以太网帧时，会将其插入4字节的VLAN标记转变为IEEE 802.1Q帧，简称打标签。**
- **当交换机转发IEEE 802.1Q帧时，可能会删除其4字节VLAN标记转为普通以太网帧，简称去标签，比如转发给用户主机时。**

因此可以通过此标识来判断是否是带VLAN标识的帧，并且可以通过此标识来确定该帧属于哪个VLAN。

四、一个简单的实际场景!

设想我们必须管理一所学校，包括一个管理部门，100 名老师和 1000 名学生。

此时，将交换机的端口分隔以便分开管理这三种人群（管理部门，老师，学生）就很有必要了。

这样才能保证学生无权访问管理部门的网络或老师的网络，而老师也无权访问管理部门的网络。

对于这个场景，与其购买 25 个拥有 48 个端口的小型交换机，不如购买 5 个拥有 256 个端口的大型交换机，布设起来简单一些。

除了网络分隔提供的安全性之外，这还使配置更加容易。如果我希望将一个端口从一个 VLAN 转到另一个 VLAN，只需在交换机上进行配置即可。我可以舒舒服服地端坐在我的网络管理员办公室里，用交换机的管理界面就可以完成所有这些操作，下图展示了一个交换机的管理界面：

Port	PVID	Port	PVID	Port	PVID	Port	PVID
1	1	2	1	3	1	4	1
5	2	6	2	7	2	8	1
9	1	10	1	11	1	12	1
13	4	14	4	15	1	16	4
17	1	18	1	19	1	20	1
21	1	22	1	23	1	24	1
25GT	3	26GT	3				

上图中，Port 那一列是对应端口（port 是“端口”的意思），而 PVID（华为交换机一般都这么叫） 那一列是对应 VLAN 的编号。我们可以看到每个端口都可以位于指定的 VLAN 中。

端口 1 是在 VLAN 1 中，而端口 5 则是在 VLAN 2 中。因此，连接到端口 1 的机器就没有办法和连接到端口 5 的机器互相通信。

那么，被分隔在一个 VLAN 中的机器真的就不能和另一个 VLAN 中的机器通信了吗？

不是完全不可能，但几乎是不可能。当然了，网络领域中几乎没有什么事情是完全不可能的。如果不可能的话，那估计也只是还没有人做到罢了。

对于 VLAN 来说，也是可以使属于两个 VLAN 的机器互相通信的，术语称为 VLAN Hopping 。hopping 表示“跳跃”，所以一般也称为 VLAN 跳跃。

所幸，目前允许 VLAN Hopping 的设计缺陷已经被修复了。

五、交换机之ACCESS端口！

实际上交换机的端口类型一般有以下三种：

- **Access**
- **Trunk**
- **Hybrid**

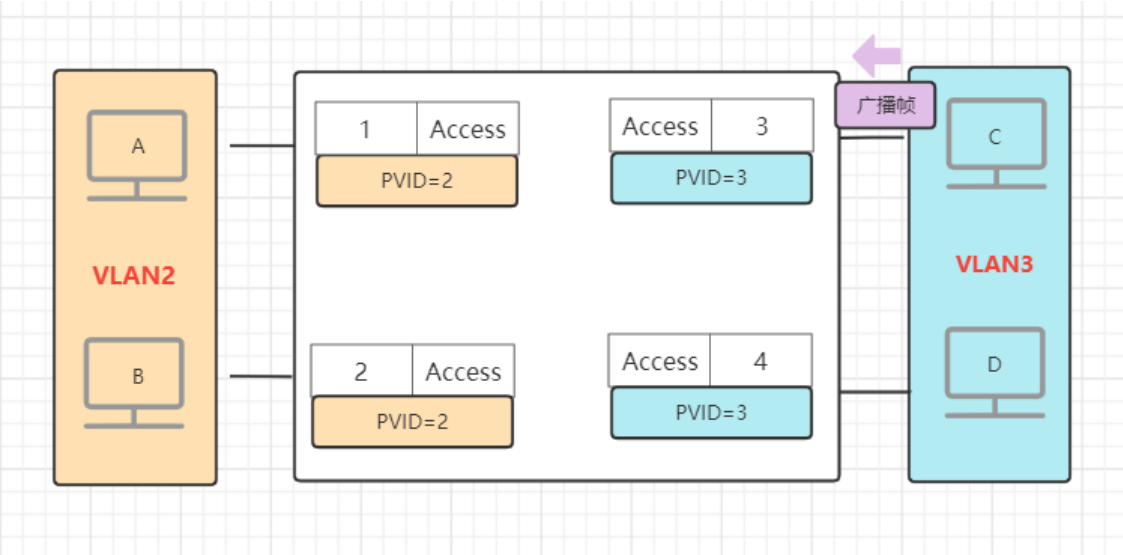
Access端口一般用于交换机连接用户计算机。

Access端口接收处理方法：一般只接受“未打标签”的普通以太网MAC帧，根据接收帧的端口的PVID给帧“打标签”，即插入4字节VLAN标记字段，字段中的VID取值与端口的PVID取值相等。

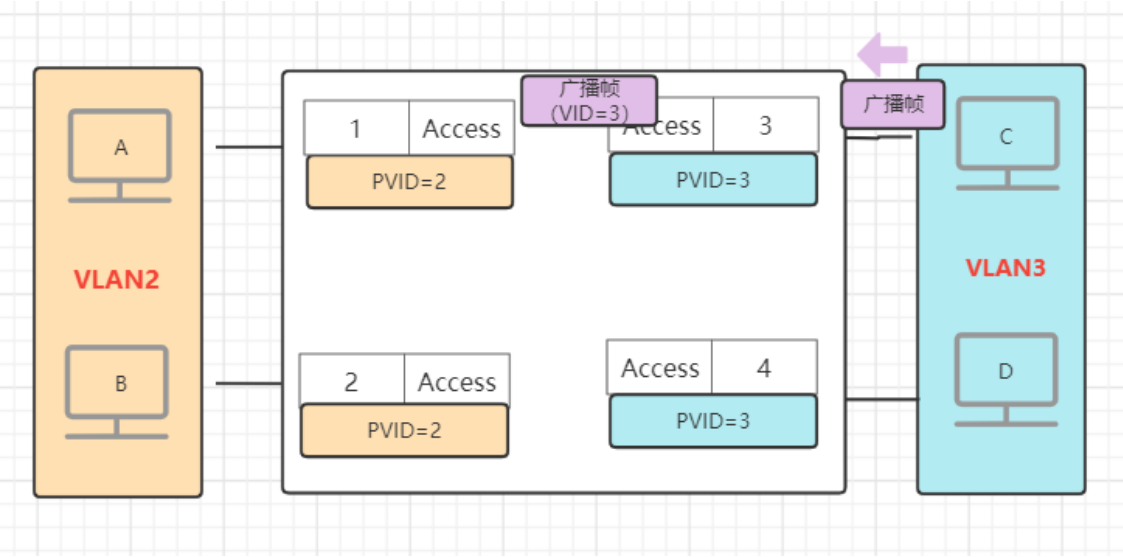
Access端口发送处理方法：打标签后的帧中携带VID广播到各个端口，其他各个端口判断自己的PVID和VID是否相等，若相等则“去标签”并转发该帧，否则不转发。

下面举个简单的例子来配合理解Access端口。

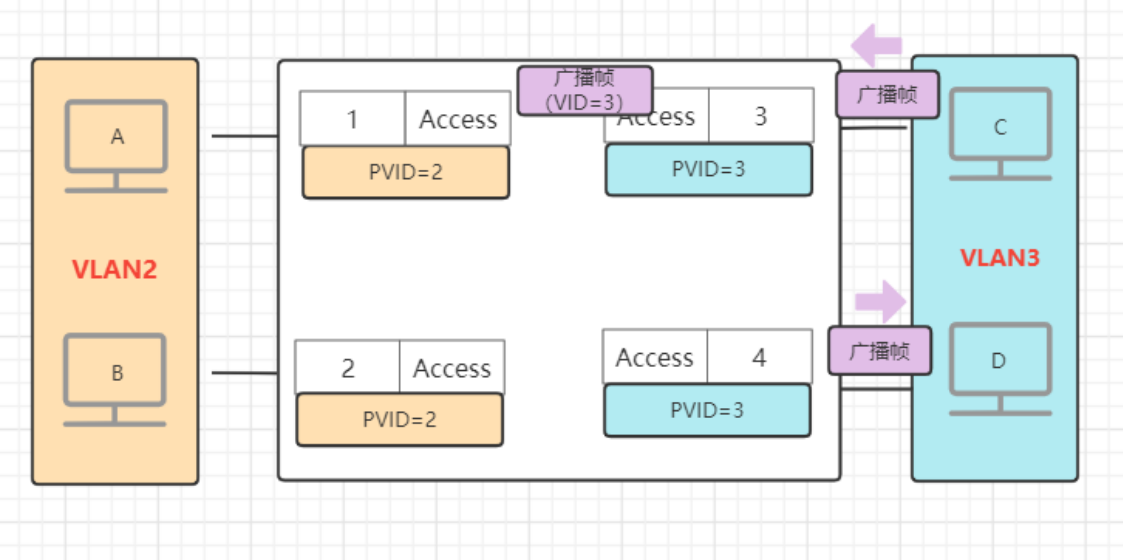
如下图所示，分为两个VLAN，一个是VLAN2，一个是VLAN3，连接的交换机端口都是Access端口，PVID如图进行了配置，我们假设主机C要发送一个广播帧：



该帧从交换机的端口3进入交换机，由于端口3的类型是Access，它会对接收到的未打标签的普通以太网MAC帧“打标签”，即插入4字节VLAN标记字段，由于端口3的PVID设置的是3，那么所插入的VLAN标记字段中的VID值也等于3.



广播出去后，发现端口4的PVID设置的值与VID相同，因此交换机会从端口4对帧进行“去标签”转发。



六、交换机之TRUNK端口！

Trunk端口一般用于交换机之间或交换机和路由器之间的互连，Trunk端口可以属于多个VLAN，用户可以设置Trunk端口的PVID值，**默认情况下Trunk端口的PVID值为1**。

我们用两个交换机互连形成更大的网络，互连的交换机端口类型为Trunk端口。

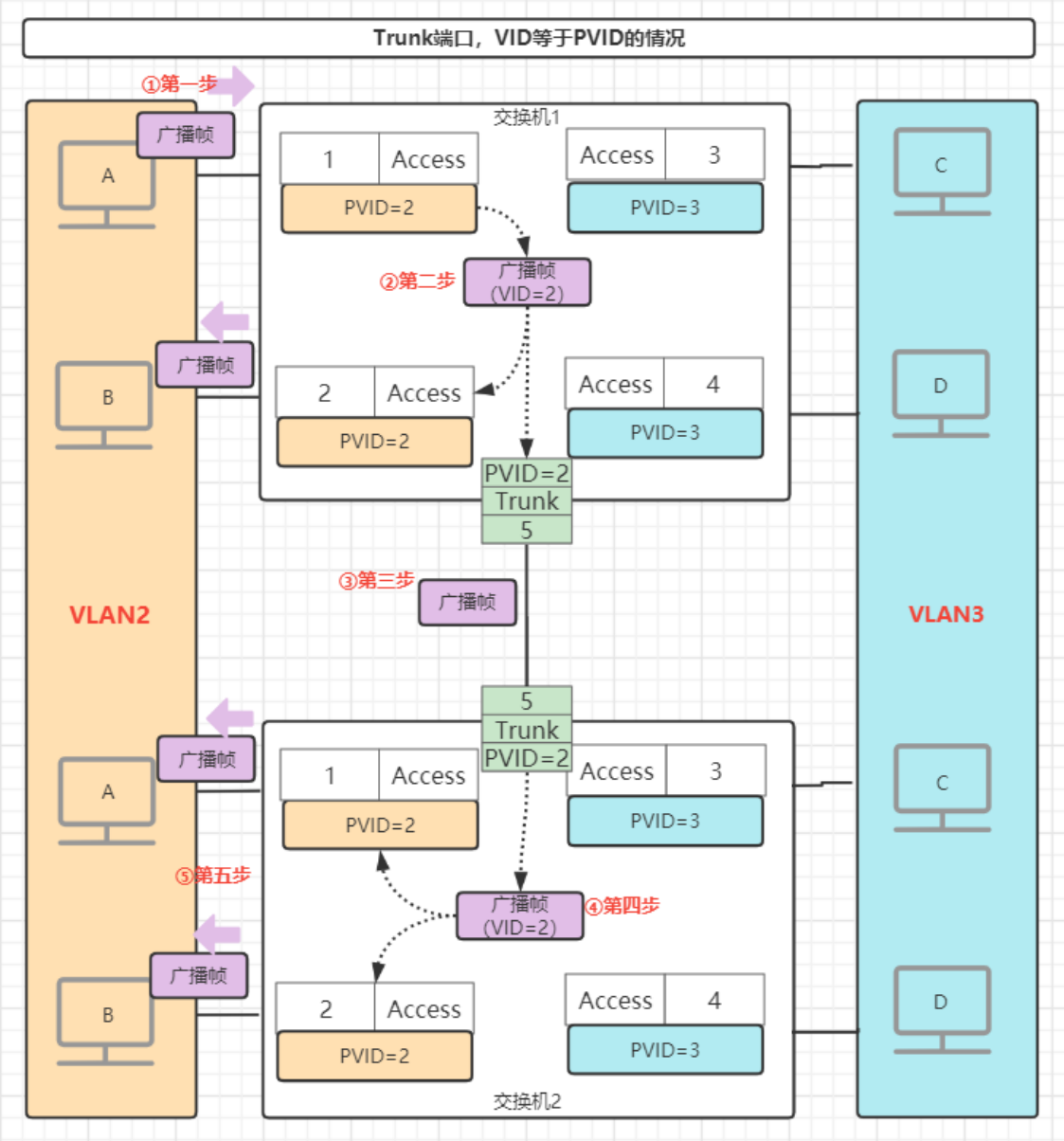
Trunk端口发送处理方法：

- 对于VID等于PVID的帧，”去标签“再转发。
- 对于VID不等于PVID的帧，直接转发。

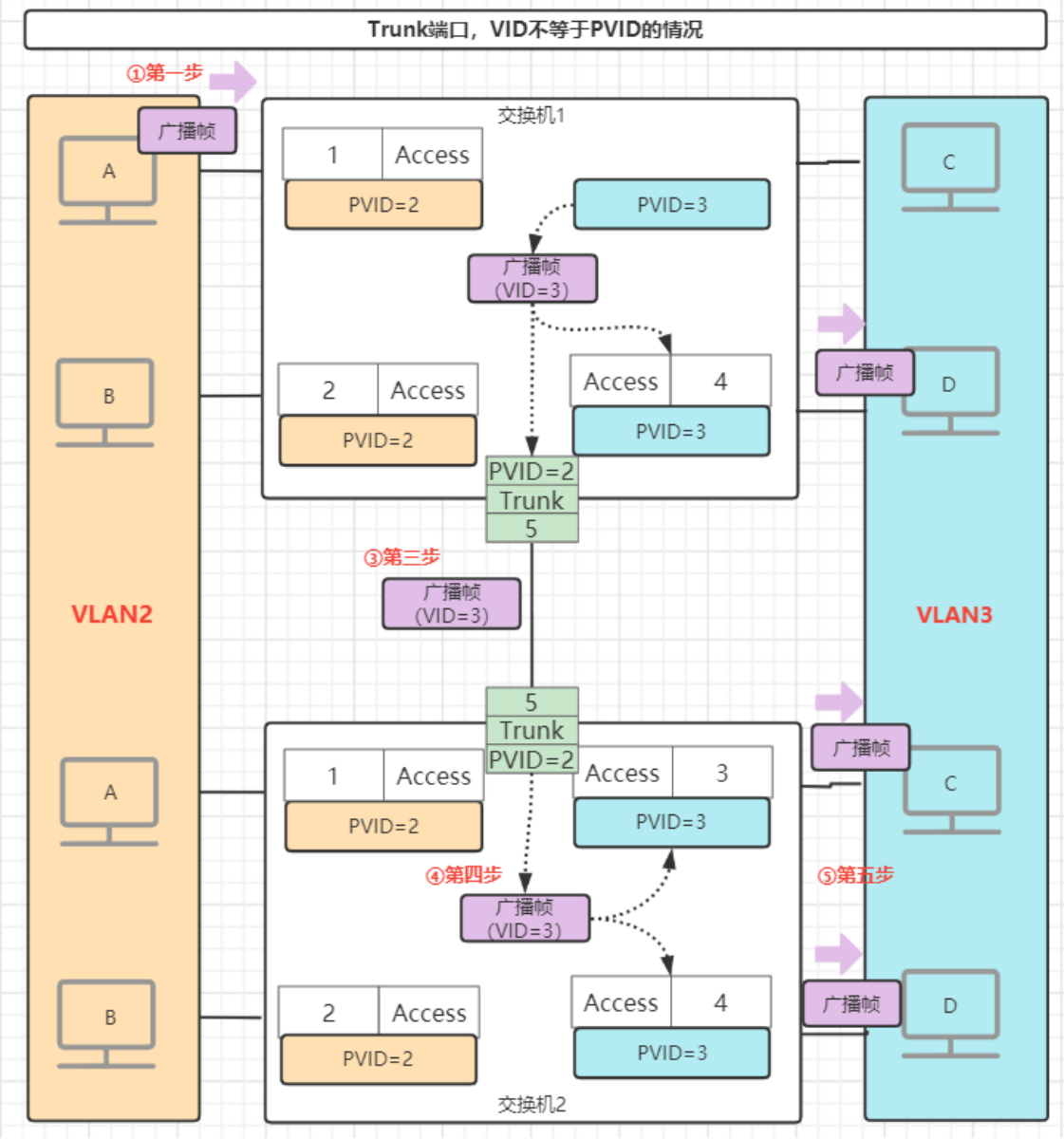
Trunk端口接收处理方法：

- 接收”未打标签“的帧，根据接收帧的端口的PVID给帧”打标签“，即插入4字节VLAN标记字段，字段中的VID取值与端口的PVID取值相等。
- 接收”已打标签“的帧，直接转发即可。

下面结合例子看看以上处理流程，首先看下VID等于PVID的情况：



- 第一步：假设是主机A发送的广播帧进入交换机1，由于主机A连接的端口是Access类型，并且PVID是2，所以封装新帧，VID等于2。
- 第二步、第三步：广播出去，发现端口2的PVID值也为2，因此接收；端口5是Trunk端口，并且PVID值也是2，则去标签转发。
- 第四步：进入交换机2，此时Trunk端口发现是未打标签的帧，根据接收帧的端口的PVID给帧”打标签“，即插入4字节VLAN标记字段，字段中的VID取值与端口的PVID取值相等，因此广播帧的VID等于2。
- 第五步：打完标签后广播，端口1和端口2接收，按照Access端口的发送逻辑进行“去标签”并转发该帧。



同理，只是区别在于第二步：

- 第二步、第三步：广播出去，发现端口3、4的PVID值也为3，因此接收；端口5是Trunk端口，并且PVID值是2，则按照规则直接转发即可，无需进行去标签操作。
- 第四步：进入交换机2，此时Trunk端口接收”已打标签“的帧，直接转发即可。

有个小问题：那为什么规则不简单粗暴点呢？Trunk端口直接转发不就可以了吗，为什么还要在VID等于PVID时”去标签“再转发呢？这不是多此一举吗？

对此存疑，我想应该是为了兼容Trunk端口直连用户主机的情况吧，当来了一个帧后，主机即可处理此端口对应PVID的帧，因为它做了去标签处理，是一个普通的MAC帧，如果PVID和VID不一致的帧，主机无法解析并丢弃此帧即可，达到了与Access端口类似的目的。

欢迎读者朋友们提出正确的原因，谢谢。。。

七、交换机之Hybrid端口!

由上面我们知道，连接主机的交换机端口应该设置为Access类型，交换机之间互连的端口应设置为Trunk类型。

Hybrid端口是华为交换机私有类型，既可用于交换机之间或交换机与路由器之间的互连（同Trunk端口），也可以用于交换机和用户主机之间的互连（同Access类型）。

Hybrid端口与Trunk端口基本类似，比如Hybrid端口可用于多个VLAN，比如用户可设置Hybrid端口的PVID值，默认情况下Hybrid端口值为1，都与Trunk端口一样。

不同点是Hybrid端口发送处理方法，查看帧的VID是否在端口的“去标签”列表中：

- 若存在，则“去标签”后转发；
- 若不存在，则直接转发；

Hybrid端口接收处理方法同Trunk端口，不赘述。