第3章

VLAN的配置

在了解了 VLAN 交换机的转发处理机制后，还需要掌握各种 VLAN 划分方式的基本配置，才能组建基本的局域网。

本章首先介绍各种 VLAN 划分方式的基本配置任务和配置命令，再通过介绍一些详细的配置示例，来进一步讲解各种 VLAN 划分方式的配置和组网应用。

3.1 本章目标

学习完本课程，应该能够：

- 应用 VLAN 交换机组建基本的局域网；
- 配置各种 VLAN 划分方式的交换机。

3.2 VLAN 的划分方式

VLAN 根据划分方式不同可以分为不同类型，最常见的 VLAN 类型为基于端口的 VLAN、基于协议的 VLAN 和基于 IP 子网的 VLAN。

基于端口的 VLAN 是最常用的 VLAN 划分方法。它按照设备端口来定义 VLAN 成员。将指定端口加入指定 VLAN 中之后，该端口就可以转发指定 VLAN 的数据帧。

基于协议的 VLAN 是根据端口接收到的帧所属的协议（簇）类型及封装格式来给帧分配不同的 VLAN ID。可用来划分 VLAN 的协议簇有 IP、IPX、AppleTalk 等，封装格式有 Ethernet Ⅱ、IEEE 802.3、IEEE 802.3/802.2 LLC、IEEE 802.3/802.2 SNAP 等。交换机从端口接收到以太网帧后，通过识别帧中的协议类型和封装格式来确定帧所属的 VLAN，然后将数据帧自动划分到指定的 VLAN 中传输。

基于 IP 子网的 VLAN 是以帧中 IP 包的源 IP 地址作为依据来进行划分的。设备从端口接收到帧后，根据帧中 IP 包的源 IP 地址，找到与现有 VLAN 的对应关系，然后自动划分到指定 VLAN 中转发。

如果交换机的某个端口下同时开启以上 3 种 VLAN，则默认情况下，VLAN 将按照基于 IP 子网的 VLAN、基于协议的 VLAN、基于端口的 VLAN 的先后顺序进行匹配。

图 3-1 所示为 VLAN 的匹配顺序流程图。图中，当交换机的以太网端口收到数据帧时，将采用以下方法处理。

（1）当收到的帧为 Tagged 帧时，如果端口允许携带该 VLAN 标记的帧通过，则正常转发；如果不允许，则丢弃该帧。

（2）当收到的帧为 Untagged 帧时，会按 IP 子网 VLAN 匹配方式进行匹配，依据帧的源地址来确定帧所属的 VLAN，如果匹配成功，将帧自动划分到指定 VLAN 中进行转发；如果

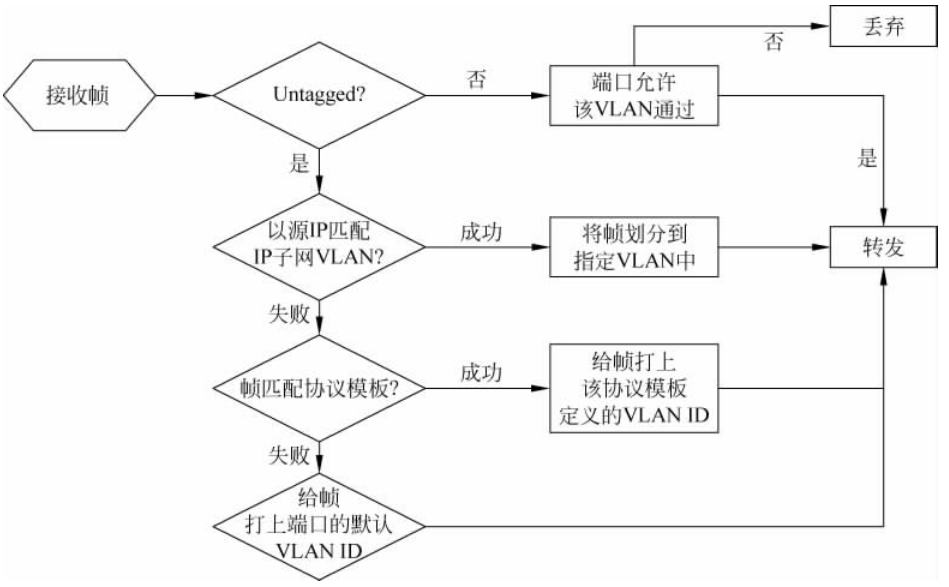

图 3-1 VLAN 的匹配顺序

匹配失败，则进行下一步处理。

(3) 按协议 VLAN 匹配方式进行匹配，如果帧匹配协议模板，则给帧打上由该协议模板定义的协议 VLAN 的 VLAN ID 进行转发；如果帧没有匹配协议模板，则给帧打上端口的默认 VLAN ID 进行转发。

3.3 基于协议的 VLAN 基本配置

3.3.1 基于协议的 VLAN 配置任务

基于协议的 VLAN 是交换机可以对端口上收到的未携带 VLAN Tag 的报文进行分析，根据报文所属的协议(族)类型及封装格式将报文与用户设定的协议模板相匹配，为匹配成功的报文分配不同的 VLAN ID，实现将属于指定协议的数据自动分发到特定的 VLAN 中传输的功能。

可用来划分 VLAN 的协议有 IP、IPX、AppleTalk(AT)，封装格式有 Ethernet Ⅱ、IEEE 802.3 raw、IEEE 802.2 LLC、IEEE 802.2 SNAP 等。

协议 VLAN 由协议模板定义，在一个端口上可以同时关联多个协议模板。协议模板是用来匹配报文所属协议类型的标准，协议模板由“封装格式＋协议类型”组成，分为如下两种模板。

- 标准模板：指以 RFC 标准规定的协议封装格式和类型字段取值作为匹配条件的模板。
- 自定义模板：指以用户在命令中指定的封装格式和标识类型字段的取值作为匹配条件的模板。

基于协议的 VLAN 的配置任务如表 3-1 所示。

表 3-1 基于协议的 VLAN 的配置任务

操　作	命　令	说明
进入系统视图	system-view	—
进入 VLAN 视图	Vlan *vlan-id*	必选

续表

操　作	命　令	说明
配置基于协议的 VLAN 并指定协议模板	protocol-vlan[*protocol-index*]{at|ipv4|ipv6|ipx{ethernetii|llc|snap}|mode{ethernetii etype *etype-id*|llc{dsap *dsap-id*[ssap *ssap-id*]|ssap *ssap-id*}|snap etype *etype-id*}}	必选
进入二层以太网端口视图	interface *interface-type interface-number*	二者必选其一
进入端口组视图	port-group manual *port-group-name*	
配置端口的链路类型为 Hybrid 类型	port link-type hybrid	必选
允许基于协议的 VLAN 以 Untagged 方式通过 Hybrid 端口	port hybrid vlan *vlan-id-list* untagged	必选
配置 Hybrid 端口与基于协议的 VLAN 关联	port hybrid protocol-vlan vlan *vlan-id*{*protocol-index*[to *protocol-end*]|all}	必选

3.3.2 基于协议的 VLAN 配置命令

基于协议的 VLAN 只对 Hybrid 端口配置才有效。基于协议的 VLAN 主要配置命令如下。

(1) 默认情况下,没有配置任何协议模板。所以,首先在 VLAN 视图下配置基于协议的 VLAN,并指定协议模板。配置命令为:

protocol-vlan[*protocol-index*]{at|ipv4|ipv6|ipx{ethernetii|llc|snap}|mode{ethernetii etype *etype-id*|llc{dsap *dsap-id*[ssap *ssap-id*]|ssap *ssap-id*}|snap etype *etype-id*}}

其中主要参数含义如下。

- at:基于 AT(AppleTalk)协议的 VLAN。
- ipv4:基于 IPv4 协议的 VLAN。
- ipv6:基于 IPv6 协议的 VLAN。
- ipx:基于 IPX 协议的 VLAN。其中的 Ethernet Ⅱ、LLC、RAW 和 SNAP 为 IPX 的 4 种封装类型。
- mode:配置自定义协议模板。也可以分为 Ethernet Ⅱ、LLC、RAW 和 SNMP 4 种封装类型。
- ethernetii etype *etype-id*:匹配 Ethernet Ⅱ封装格式及相应的协议类型值。etype-id 表示入报文的协议类型值,取值范围为 0x0600～0xFFFF(除 0x0800、0x809B、0x8137、0x86DD 以外)。
- llc:以太网报文封装格式为 LLC。
- dsap *dsap-id*:目的服务接入点,取值范围为 00～0xFF。
- ssap *ssap-id*:源服务接入点,取值范围为 00～0xFF。
- snap etype *etype-id*:匹配 SNAP 封装格式及相应的协议类型值。etype-id 表示入报文的以太网类型,取值范围为 0x0600～0xFFFF,但不能是 SNAP 封装下的 IPX SNAP 类型。

(2) 配置协议模板完成后,需要为协议 VLAN 添加端口并建立该端口与协议模板的关联。在端口视图下,配置 Hybrid 端口与基于协议的 VLAN 的关联。配置命令为:

port hybrid protocol-vlan vlan *vlan-id*{*protocol-index* [to *protocol-end*]|all}

3.3.3 基于协议的 VLAN 配置示例

图 3-2 所示为基于协议的 VLAN 配置示例，图中，PCA 与 PCC 协议为 IPv4，与 VLAN10 关联，PCB 与 PCD 的协议为 IPv6，与 VLAN20 关联，交换机之间使用 Trunk 端口相连，端口的默认 VLAN 是 VLAN1。

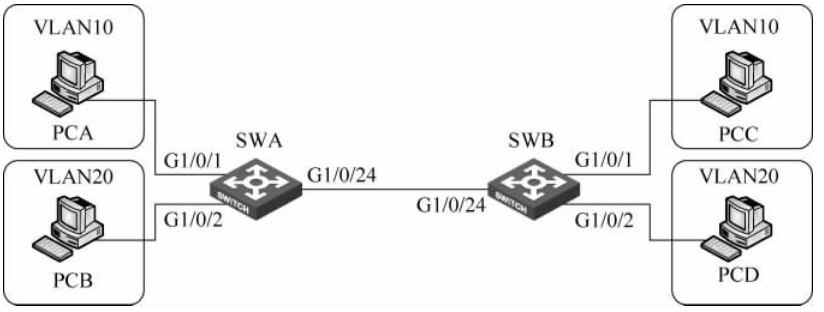

图 3-2 基于协议的 VLAN 配置示例

配置 SWA：

```
[SWA]vlan 10
[SWA-vlan10]protocol-vlan ipv4
[SWA-vlan10]quit
[SWA]vlan 20
[SWA-vlan20]protocol-vlan ipv6
[SWA-vlan20]quit
[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1]port link-type hybrid
[SWA-GigabitEthernet1/0/1]port hybrid vlan 10 20 untagged
[SWA-GigabitEthernet1/0/1]port hybrid protocol-vlan vlan 10 0
[SWA-GigabitEthernet1/0/1]port hybrid protocol-vlan vlan 20 0
[SWA-GigabitEthernet1/0/1]quit
[SWA]interface GigabitEthernet 1/0/2
[SWA-GigabitEthernet1/0/2]port link-type hybrid
[SWA-GigabitEthernet1/0/2]port hybrid vlan 10 20 untagged
[SWA-GigabitEthernet1/0/2]port hybrid protocol-vlan vlan 10 0
[SWA-GigabitEthernet1/0/2]port hybrid protocol-vlan vlan 20 0
[SWA-GigabitEthernet1/0/2]quit
[SWA]interface GigabitEthernet 1/0/24
[SWA-GigabitEthernet1/0/24]port link-type trunk
[SWA-GigabitEthernet1/0/24]port trunk permit vlan 10 20
```

配置 SWB：

```
[SWB]vlan 10
[SWB-vlan10]protocol-vlan ipv4
[SWB-vlan10]quit
[SWB]vlan 20
[SWB-vlan20]protocol-vlan ipv6
[SWB-vlan20]quit
[SWB]interface GigabitEthernet 1/0/1
[SWB-GigabitEthernet1/0/1]port link-type hybrid
[SWB-GigabitEthernet1/0/1]port hybrid vlan 10 20 untagged
[SWB-GigabitEthernet1/0/1]port hybrid protocol-vlan vlan 10 0
[SWB-GigabitEthernet1/0/1]port hybrid protocol-vlan vlan 20 0
```

```
[SWB-GigabitEthernet1/0/1]quit
[SWB]interface GigabitEthernet 1/0/2
[SWB-GigabitEthernet1/0/2]port link-type hybrid
[SWB-GigabitEthernet1/0/2]port hybrid vlan 10 20 untagged
[SWB-GigabitEthernet1/0/2]port hybrid protocol-vlan vlan 10 0
[SWB-GigabitEthernet1/0/2]port hybrid protocol-vlan vlan 20 0
[SWB-GigabitEthernet1/0/2]quit
[SWB]interface GigabitEthernet 1/0/24
[SWB-GigabitEthernet1/0/24]port link-type trunk
[SWB-GigabitEthernet1/0/24]port trunk permit vlan 10 20
```

配置完成后，交换机会把IPv4协议的数据帧划分为VLAN10，把IPv6协议的数据帧划分为VLAN20，PCA与PCC都被划分到VLAN10中且能够互通，PCB与PCD都被划分到VLAN20中且能够互通。

3.4 基于IP子网的VLAN基本配置

3.4.1 基于IP子网的VLAN配置任务

基于IP子网的VLAN是根据报文源IP地址及子网掩码来进行划分的。设备从端口接收到Untagged报文后，会根据报文的源地址来确定报文所属的VLAN，然后将报文自动划分到指定VLAN中传输。此特性主要用于将指定网段或IP地址发出的报文在指定的VLAN中传送。

不要把基于子网的VLAN和VLAN虚接口的IP配置搞混淆。

基于IP子网的VLAN的配置任务如表3-2所示。

表3-2 基于IP子网的VLAN配置任务

操 作	命 令	说明
进入系统视图	system-view	—
进入VLAN视图	Vlan *vlan-id*	必选
配置IP子网与当前VLAN的关联	ip-subnet-vlan[*ip-subnet-index*]ip *ip-address*[*mask*]	必选
进入二层以太网端口视图	interface *interface-type interface-number*	二者必选其一
进入端口组视图	port-group manual *port-group-name*	
配置端口的链路类型为Hybrid类型	port link-type hybrid	必选
允许基于IP子网的VLAN通过当前Hybrid端口	port hybrid vlan *vlan-id-list*{tagged|untagged}	必选
配置Hybrid端口与基于IP子网的VLAN关联	port hybrid ip-subnet-vlan vlan *vlan-id*	必选

3.4.2 基于IP子网的VLAN配置命令

基于IP子网的VLAN只对Hybrid端口配置有效，其主要配置命令如下。

(1) 在VLAN视图下配置当前VLAN与指定的IP子网关联。配置命令为：

ip-subnet-vlan [*ip-subnet-index*] ip *ip-address* [*mask*]

(2) 在以太网端口视图下，设置好当前端口为Hybrid类型且已经允许该VLAN通过后，还需要设定当前端口与基于IP子网的VLAN关联。配置命令为：

port hybrid ip-subnet-vlan vlan *vlan-id*

3.4.3 基于 IP 子网的 VLAN 配置示例

图 3-3 所示为基于 IP 子网的 VLAN 配置示例。图中，PCA 与 PCC 的网段为 10.10.10.0/24，与 VLAN10 关联，PCB 与 PCD 的 IP 网段为 20.20.20.0/24，与 VLAN20 关联，交换机之间使用 Trunk 端口相连，端口的默认 VLAN 是 VLAN1。

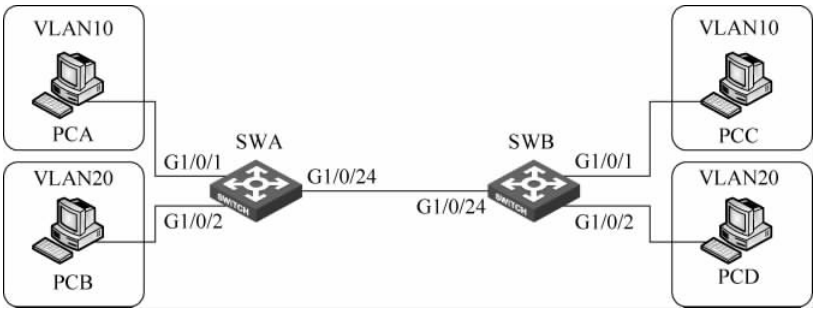

图 3-3 基于 IP 子网的 VLAN 配置示例

配置 SWA：

```
[SWA]vlan 10
[SWA-vlan10]ip-subnet-vlan ip 10.10.10.0 255.255.255.0
[SWA-vlan10]quit
[SWA]vlan 20
[SWA-vlan20]ip-subnet-vlan ip 20.20.20.0 255.255.255.0
[SWA-vlan20]quit
[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1]port link-type hybrid
[SWA-GigabitEthernet1/0/1]port hybrid vlan 10 20 untagged
[SWA-GigabitEthernet1/0/1]port hybrid ip-subnet-vlan vlan 10
[SWA-GigabitEthernet1/0/1]port hybrid ip-subnet-vlan vlan 20
[SWA-GigabitEthernet1/0/1]quit
[SWA]interface GigabitEthernet 1/0/2
[SWA-GigabitEthernet1/0/2]port link-type hybrid
[SWA-GigabitEthernet1/0/2]port hybrid vlan 10 20 untagged
[SWA-GigabitEthernet1/0/2]port hybrid ip-subnet-vlan vlan 10
[SWA-GigabitEthernet1/0/2]port hybrid ip-subnet-vlan vlan 20
[SWA-GigabitEthernet1/0/2]quit
[SWA]interface GigabitEthernet 1/0/24
[SWA-GigabitEthernet1/0/24]port link-type trunk
[SWA-GigabitEthernet1/0/24]port trunk permit vlan 10 20
```

配置 SWB：

```
[SWB]vlan 10
[SWB-vlan10]ip-subnet-vlan ip 10.10.10.0 255.255.255.0
[SWB-vlan10]quit
[SWB]vlan 20
[SWB-vlan20]ip-subnet-vlan ip 20.20.20.0 255.255.255.0
[SWB-vlan20]quit
[SWB]interface GigabitEthernet 1/0/1
[SWB-GigabitEthernet1/0/1]port link-type hybrid
[SWB-GigabitEthernet1/0/1]port hybrid vlan 10 20 untagged
```

```
[SWB-GigabitEthernet1/0/1]port hybrid ip-subnet-vlan vlan 10
[SWB-GigabitEthernet1/0/1]port hybrid ip-subnet-vlan vlan 20
[SWB-GigabitEthernet1/0/1]quit
[SWB]interface GigabitEthernet 1/0/2
[SWB-GigabitEthernet1/0/2]port link-type hybrid
[SWB-GigabitEthernet1/0/2]port hybrid vlan 10 20 untagged
[SWB-GigabitEthernet1/0/2]port hybrid ip-subnet-vlan vlan 10
[SWB-GigabitEthernet1/0/2]port hybrid ip-subnet-vlan vlan 20
[SWB-GigabitEthernet1/0/2]quit
[SWB]interface GigabitEthernet 1/0/24
[SWB-GigabitEthernet1/0/24]port link-type trunk
[SWB-GigabitEthernet1/0/24]port trunk permit vlan 10 20
```

配置完成后，交换机会把 10.10.10.0/24 网段的数据帧划分为 VLAN10，把 20.20.20.0/24 网段的数据帧划分为 VLAN20，PCA 与 PCC 都被划分到 VLAN10 中且能够互通，PCB 与 PCD 都被划分到 VLAN20 中且能够互通。

3.5 本章总结

（1）默认情况下，VLAN 将按照基于 IP 子网的 VLAN、基于协议的 VLAN、基于端口的 VLAN 的先后顺序进行匹配。

（2）基于协议的 VLAN 和基于 IP 子网的 VLAN 只对 Hybrid 端口配置有效。

3.6 习题和答案

3.6.1 习题

（1）基于协议的 VLAN 对（　　）类型的端口配置有效。

A. Access 端口　　B. Trunk 端口

C. Hybrid 端口　　D. 以上端口都可以

（2）VLAN 的划分包含（　　）方式。

A. 基于端口划分　　B. 基于协议划分

C. 基于 IP 地址划分　　D. 基于 IP 子网划分

3.6.2 习题答案

（1）C　（2）ABD

第4章

VLAN扩展技术

VLAN技术的成熟应用带来了很多的便利，但在实际使用过程中，VLAN技术还有或多或少的应用场景无法适应。因此针对这些特殊应用，VLAN也与时俱进，不断地扩展新技术来满足各种应用需求。

4.1 本章目标

学习完本课程，应该能够：

- 熟悉Private VLAN的基本原理和配置；
- 熟悉Super VLAN的基本原理和配置。

4.2 Private VLAN技术的原理和配置

4.2.1 Private VLAN技术介绍

随着以太网技术的快速发展，很多运营商采用LAN接入小区宽带。基于用户安全和管理计费等方面考虑，运营商一般要求接入用户互相隔离。VLAN是天然的隔离手段，于是很自然的一个想法是每个用户1个VLAN。但是，根据IEEE 802.1Q协议规定，设备最大可使用的VLAN资源为4094个。对于运营商的设备来说，如果每个用户1个VLAN，4094个VLAN远远不够，而且，为每个只包含1个用户的VLAN配置第三层接口，将耗费大量的IP地址和部署成本。

图4-1所示为Private VLAN技术的产生背景——运营商小区宽带接入典型组网。图中，采用LAN方式接入的小区宽带用户的主要应用是上互联网，用户之间相互隔离，每个用户1个VLAN，用户数远远大于4094个VLAN，VLAN数量限制了更多用户的接入需求。

VLAN ID主要消耗在接入层，对于运营商来说，如果既能够保证接入层用户之间相互隔离，又能将接入层的VLAN ID屏蔽，只可见汇聚层的VLAN ID，则4094个VLAN是够用的。为了解决上述问题，Private VLAN技术应运而生。

Private VLAN采用二层VLAN结构，它在同一台设备上设置Primary VLAN和Secondary VLAN两类VLAN。功能如下。

(1) Primary VLAN用于上行连接，不同的Secondary VLAN关联到同一个Primary VLAN。上行连接的设备只知道Primary VLAN，而不必关心Secondary VLAN，简化了网络配置，节省了VLAN资源。

(2) Secondary VLAN用于连接用户，Secondary VLAN之间二层帧互相隔离。如果希望实现同一Primary VLAN下Secondary VLAN用户之间互通，可以通过配置上行设备的本地

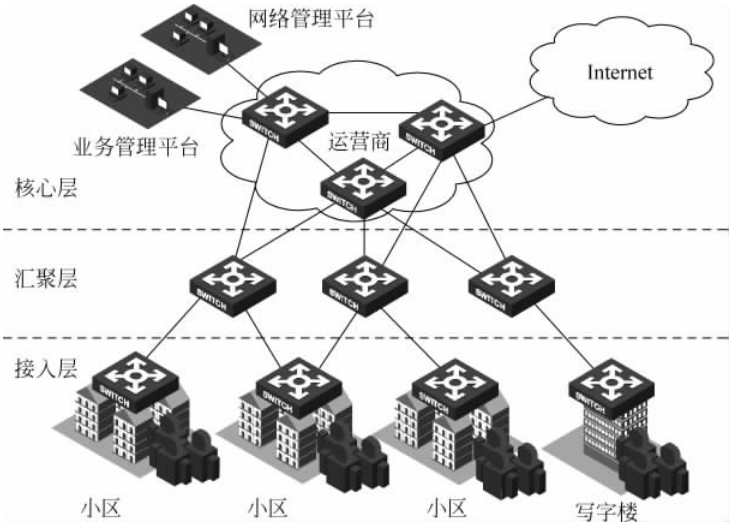

图 4-1 Private VLAN 技术的产生背景

代理 ARP 功能来实现三层报文的互通。

(3) 一个 Primary VLAN 可以和多个 Secondary VLAN 相对应,理论上每个 Primary VLAN 可以包含 4094 个 Secondary VLAN,所以相当于提供了 4094×4094 个 VLAN。Primary VLAN 下面的 Secondary VLAN 对上行设备不可见。

下面通过一个简单的应用来描述 Private VLAN 的技术特点,图 4-2 所示为 Private VLAN 技术的简单应用。图中,SWA 为三层交换机,是 SWB 的上行设备,SWB 为支持 Private VLAN 功能的交换机。在 SWB 上开启 Private VLAN 功能,并配置 VLAN10 为 Primary VLAN,VLAN2、VLAN3 和 VLAN4 为 Secondary VLAN,VLAN2、VLAN3 和 VLAN4 都映射到 VLAN10。

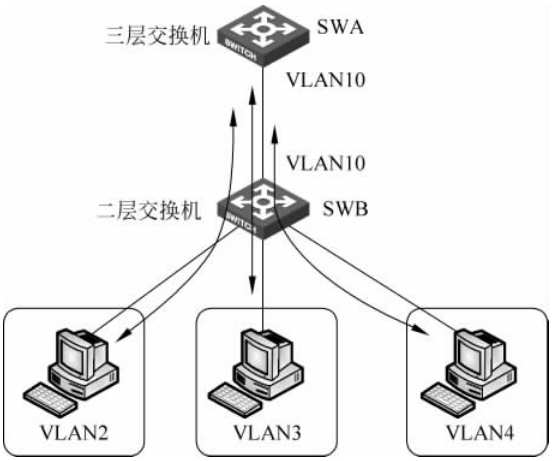

图 4-2 Primary VLAN 技术功能

在 SWB 上完成 Private VLAN 配置后,SWB 上的 VLAN2、VLAN3 和 VLAN4 都可以和 SWA 互通,对于上层设备 SWA 来说,只需识别下层交换机 SWB 的 VLAN10,而不必关心 VLAN10 中包含的 VLAN2、VLAN3 和 VLAN4;SWB 上的 VLAN2、VLAN3、VLAN4 间通

过传统的 VLAN 技术实现二层隔离，也可以在上行设备 SWA 上配置本地代理 ARP 功能实现三层报文的互通。

其实，Private VLAN 功能是利用了 Hybrid 类型端口的灵活性以及 VLAN 间的 MAC 地址同步技术来实现的。

Hybrid 端口在转发数据时，可以按照需要进行多个 VLAN 数据流量的发送和接收，可以根据需要决定发送数据帧时是否携带 IEEE 802.1Q 标签。正因为这一灵活性，Hybrid 端口可以用于交换机之间的连接，也可用于连接用户计算机。

下面通过一个抽象的模型图来说明 Private VLAN 技术的基本原理。交换机的端口和所属 VLAN 如图 4-3 中 SWB 所示，SWB 上 Port1、Port2 和 Port3 这 3 个端口都设定为 Hybrid 类型，Port1 允许 VLAN2、VLAN10 的数据帧通过，Port2 允许 VLAN3、VLAN10 的数据帧通过，Port3 允许 VLAN2、VLAN3 和 VLAN10 的数据帧通过，所有发出去的数据帧都不携带 IEEE 802.1Q 标签。配置完成后，PCA 可以和 SWA 互通，PCB 可以和 SWA 互通，而 PCA 和 PCB 之间隔离。

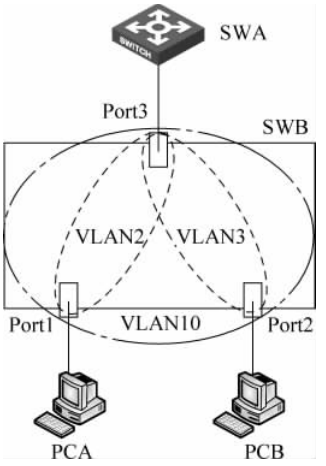

图 4-3 Private VLAN 技术基本原理

如果仔细分析不难发现，交换机在转发时会存在一个较为严重的问题。按照需求，如图 4-3 所示 SWB 的 3 个端口的 PVID 应该分别为 VLAN2、VLAN3 和 VLAN10。一开始 PCA 发送 ARP 请求到 Port1，解析 SWA（网关）的 MAC 地址，PCA 的 MAC 地址被学习到 SWB 的 VLAN2 中，SWB 没能匹配到 SWA 的 MAC 地址表项，只能在 VLAN2 的广播域内广播，因 Port3 允许 VLAN2 的数据帧通过，所以此广播帧会从 Port3 转发出去，SWA 会接收到。

当 SWA 返回的 ARP 响应到达 SWB 的 Port3 时（源 MAC 为 MAC_SWA，目的 MAC 地址为 MAC_PCA），SWA 的 MAC 地址将被学习到 SWB 的 VLAN10 中，SWB 会给报文添加 Tag，VLAN ID 为 10（即端口的默认 VLAN ID），然后以“MAC_PCA＋VLAN10”为条件去查询 MAC 地址表。由于找不到相应的表项，该报文会在 VLAN10 内广播，并最终从 Port1 和 Port2 发送出去。

同理，每次上行和下行的报文都需要广播才能到达目的地。当 Secondary VLAN 和 Primary VLAN 包含的端口较多时，这样的处理方式会占用大量的带宽资源，大大降低了交换机的转发性能，而且不安全（广播报文容易被截获和侦听）。通过 MAC 地址同步机制可以解决这个问题。

Primary VLAN 的 MAC 地址同步机制有如下两种。

（1）Secondary VLAN 到 Primary VLAN 的同步，即下行端口在 Secondary VLAN 内学习到的 MAC 地址都同步到 Primary VLAN 内，而出端口则保持不变。

（2）Primary VLAN 到 Secondary VLAN 的同步，即上行端口在 Primary VLAN 学习到的 MAC 地址同步到所有的 Secondary VLAN 内，而出端口则保持不变。

如下信息即是交换机 MAC 地址表同步后的结果：