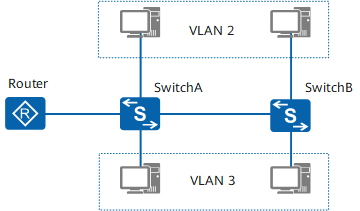
## 1 VLAN

### 1.1 VLAN简介

VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的LAN在逻辑上划分成多个广播域的通信技术。

早期以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detection）的共享通讯介质的数据网络通讯技术。当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至造成网络不可用等问题。通过交换机实现LAN互连虽然可以解决冲突严重的问题，但仍然不能隔离广播报文和提升网络质量。

在这种情况下出现了VLAN技术，这种技术可以把一个LAN划分成多个逻辑的VLAN，每个VLAN是一个广播域，VLAN内的主机间通信就和在一个LAN内一样，而VLAN间则不能直接互通，这样，广播报文就被限制在一个VLAN内。



如图是一个典型的VLAN应用组网图。两台交换机放置在不同的地点，比如写字楼的不同楼层。每台交换机分别连接两台计算机，他们分别属于两个不同的VLAN，比如不同的企业客户。

使用VLAN能给用户带来以下受益：

1. 限制广播域：广播域被限制在一个VLAN内，节省了带宽，提高了网络处理能力。

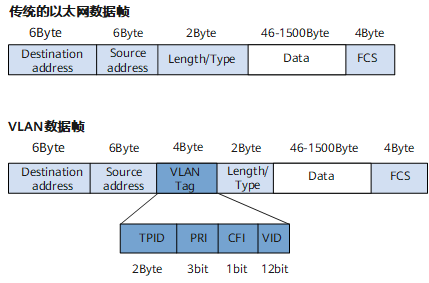
2. 增强局域网的安全性：不同VLAN内的报文在传输时是相互隔离的，即一个VLAN内的用户不能和其它VLAN内的用户直接通信。

3. 提高了网络的健壮性：故障被限制在一个VLAN内，本VLAN内的故障不会影响其他VLAN的正常工作。

4. 灵活构建虚拟工作组：用VLAN可以划分不同的用户到不同的工作组，同一工作组的用户也不必局限于某一固定的物理范围，网络构建和维护更方便灵活。

### 1.2 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，在以太网数据帧的目的MAC地址和源MAC地址字段之后、协议类型字段之前加入4个字节的VLAN标签（又称VLAN Tag，简称Tag），用以标识VLAN信息。如图所示。



VLAN标签包含4个字段，各字段含义如表所示：

| **字段** | **长度** | **含义** | **取值** |
| --- | --- | --- | --- |
| TPID | 2Byte | Tag Protocol Identifier（标签协议标识符），表示数据帧类型。 | 表示帧类型，取值为0x8100时表示IEEE 802.1Q的VLAN数据帧。如果不支持802.1Q的设备收到这样的帧，会将其丢弃。  各设备厂商可以自定义该字段的值。当邻居设备将TPID值配置为非0x8100时， 为了能够识别这样的报文，实现互通，必须在本设备上修改TPID值，确保和邻居设备的TPID值配置一致。 |
| PRI | 3bit | Priority，表示数据帧的802.1p优先级。 | 取值范围为0～7，值越大优先级越高。当网络阻塞时，交换机优先发送优先级高的数据帧。 |
| CFI | 1bit | Canonical Format Indicator（标准格式指示位），表示MAC地址在不同的传输介质中是否以标准格式进行封装，用于兼容以太网和令牌环网。 | CFI取值为0表示MAC地址以标准格式进行封装，为1表示以非标准格式封装。在以太网中，CFI的值为0。 |
| VID | 12bit | VLAN ID，表示该数据帧所属VLAN的编号。 | VLAN ID取值范围是0～4095。由于0和4095为协议保留取值，所以VLAN ID的有效取值范围是1～4094。 |

交换机利用VLAN标签中的VID来识别数据帧所属的VLAN，广播帧只在同一VLAN内转发，这就将广播域限制在一个VLAN内。

在一个VLAN交换网络中，以太网帧主要有以下两种形式：

有标记帧（Tagged帧）：加入了4字节VLAN标签的帧。

无标记帧（Untagged帧）：原始的、未加入4字节VLAN标签的帧。

常用设备中：

用户主机、服务器、Hub、无管理型交换机只能收发Untagged帧。

交换机、路由器和AC既能收发Tagged帧，也能收发Untagged帧。

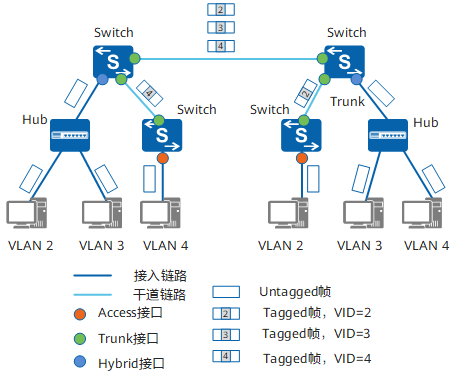
语音终端、AP等设备可以收发一个VLAN的Tagged帧或Untagged帧。

为了提高处理效率，交换机内部处理的数据帧一律都是Tagged帧。

### 1.3 接口的链路类型

交换机内部处理的数据帧一律都带有VLAN标签，而现网中交换机连接的设备有些只会收发Untagged帧，要与这些设备交互，就需要接口能够识别Untagged帧并在收发时给帧添加、剥除VLAN标签。同时，现网中属于同一个VLAN的用户可能会被连接在不同的交换机上，且跨越交换机的VLAN可能不止一个，如果需要用户间的互通，就需要交换机间的接口能够同时识别和发送多个VLAN的数据帧。

根据接口连接对象以及对收发数据帧处理的不同，一般来说分为3种接口链路类型：Access、Trunk和Hybrid，以适应不同的连接和组网。其中Access接口、Trunk接口和Hybrid接口如图所示。



#### 1.3.1 Access接口

Access接口一般用于和不能识别Tag的用户终端（如用户主机、服务器等）相连，或者不需要区分不同VLAN成员时使用。Access接口大部分情况只能收发Untagged帧，且只能为Untagged帧添加唯一VLAN的Tag。交换机内部只处理Tagged帧，所以Access接口需要给收到的数据帧添加VLAN Tag，也就必须配置缺省VLAN。配置缺省VLAN后，该Access接口也就加入了该VLAN。当Access接口收到带有Tag的帧，并且帧中VID与PVID相同时，Access接口也能接收并处理该帧。为了防止用户私自更改接口用途，接入其他交换设备，可以配置接口丢弃入方向带Tag的报文。

#### 1.3.2 Trunk接口

Trunk接口一般用于连接交换机、路由器、AP以及可同时收发Tagged帧和Untagged帧的语音终端。它可以允许多个VLAN的帧带Tag通过，但只允许一个VLAN的帧从该类接口上发出时不带Tag（即剥除Tag）。

#### 1.3.3 Hybrid接口

Hybrid接口既可以用于连接不能识别Tag的用户终端（如用户主机、服务器等）和网络设备（如Hub、无管理型交换机），也可以用于连接交换机、路由器以及可同时收发Tagged帧和Untagged帧的语音终端、AP。它可以允许多个VLAN的帧带Tag通过，且允许从该类接口发出的帧根据需要配置某些VLAN的帧带Tag（即不剥除Tag）、某些VLAN的帧不带Tag（即剥除Tag）。

### 1.4 缺省VLAN

缺省VLAN又称PVID（Port Default VLAN ID）。前面提到，交换机处理的数据帧都带Tag，当交换机收到Untagged帧时，就需要给该帧添加Tag，添加什么Tag，就由接口上的缺省VLAN决定。它的具体作用是：

当接口接收数据帧时，如果接口收到一个Untagged帧，交换机会根据PVID给此数据帧添加等于PVID的Tag，然后再交给交换机内部处理；如果接口收到一个Tagged帧，交换机则不会再给该帧添加接口上PVID对应的Tag。

当接口发送数据帧时，如果发现此数据帧的Tag的VID值与PVID相同，则交换机会将Tag去掉，然后再从此接口发送出去。

每个接口都有一个缺省VLAN。

对于Access接口，缺省VLAN就是它允许通过的VLAN，修改接口允许通过的VLAN即可更改接口的缺省VLAN。

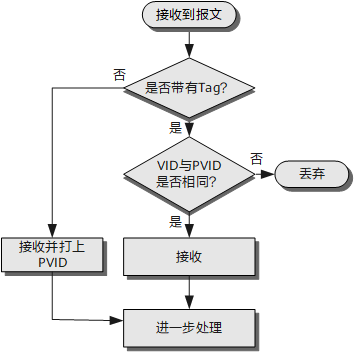
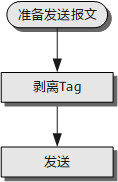
对于Trunk接口和Hybrid接口，一个接口可以允许多个VLAN通过，但是只能有一个缺省VLAN，修改接口允许通过的VLAN不会更改接口的缺省VLAN。

### 1.5 VLAN标签的添加和剥除

接口对收发的以太网数据帧添加或剥除VLAN标签的处理依据接口的接口类型和缺省VLAN。下面分别介绍Access接口、Trunk接口、Hybrid接口对收发数据帧的处理过程。

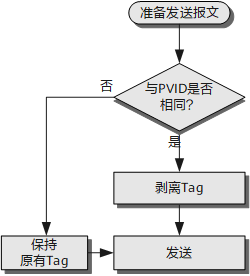
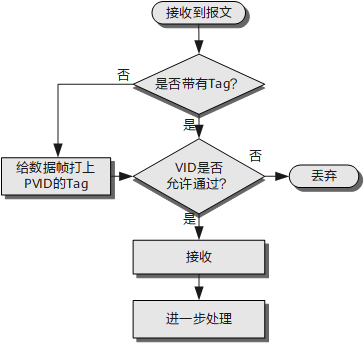
#### 1.5.1 Access接口

Access接口添加和剥除VLAN标签的处理如图所示。

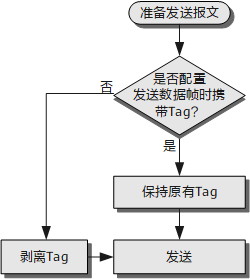
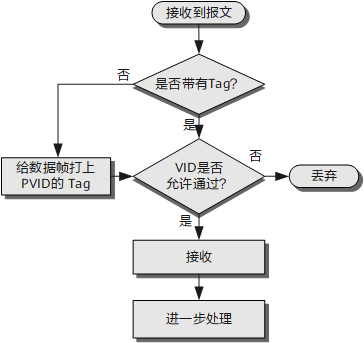
#### 1.5.2 Trunk接口

Trunk接口添加和剥除VLAN标签的处理如图所示。



#### 1.5.3 Hybrid接口

Hybrid接口添加和剥除VLAN标签的处理如[图4-8](https://support.huawei.com/enterprise/zh/doc/EDOC1100365040/f9b8a34a#fig_dc_cfg_vlan_100704)和[图4-9](https://support.huawei.com/enterprise/zh/doc/EDOC1100365040/f9b8a34a#fig_dc_cfg_vlan_100707)所示。



#### 1.5.4 不同类型接口添加或剥除VLAN标签的比较

| **接口类型** | **对接收不带Tag的报文处理** | **对接收带Tag的报文处理** | **发送帧处理过程** |
| --- | --- | --- | --- |
| Access接口 | 接收该报文，并打上缺省的VLAN ID。 | 当VLAN ID与缺省VLAN ID相同时，接收该报文。  当VLAN ID与缺省VLAN ID不同时，丢弃该报文。 | 先剥离帧的PVID Tag，然后再发送。 |
| Trunk接口 | 打上缺省的VLAN ID，当缺省VLAN ID在允许通过的VLAN ID列表里时，接收该报文。  打上缺省的VLAN ID，当缺省VLAN ID不在允许通过的VLAN ID列表里时，丢弃该报文。 | 当VLAN ID在接口允许通过的VLAN ID列表里时，接收该报文。  当VLAN ID不在接口允许通过的VLAN ID列表里时，丢弃该报文。 | 当VLAN ID与缺省VLAN ID相同，且是该接口允许通过的VLAN ID时，去掉Tag，发送该报文。  当VLAN ID与缺省VLAN ID不同，且是该接口允许通过的VLAN ID时，保持原有Tag，发送该报文。 |
| Hybrid接口 | 打上缺省的VLAN ID，当缺省VLAN ID在允许通过的VLAN ID列表里时，接收该报文。  打上缺省的VLAN ID，当缺省VLAN ID不在允许通过的VLAN ID列表里时，丢弃该报文。 | 当VLAN ID在接口允许通过的VLAN ID列表里时，接收该报文。  当VLAN ID不在接口允许通过的VLAN ID列表里时，丢弃该报文。 | 当VLAN ID是该接口允许通过的VLAN ID时，发送该报文。可以通过命令设置发送时是否携带Tag。 |

由上面各类接口链路类型添加或剥除VLAN标签的处理过程可见，Access接口发出的数据帧肯定不带Tag，Trunk接口发出的数据帧只有一个VLAN的数据帧不带Tag，其他都带VLAN标签，Hybrid接口发出的数据帧可根据需要设置某些VLAN的数据帧带Tag，某些VLAN的数据帧不带Tag。

## 2 VLANIF接口

### 2.1背景信息

VLANIF接口是一种三层的逻辑接口，能实现不同VLAN间，不同网段的用户进行三层互通。由于配置较为简单，是实现VLAN间互通最常用的一种技术。

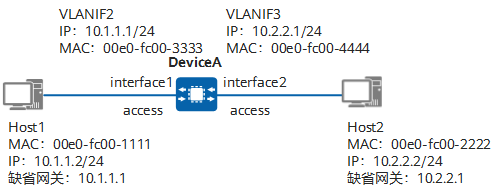
每个VLAN对应一个VLANIF接口，在为VLANIF接口配置IP地址后，该接口即可作为本VLAN内用户的缺省网关，对需要跨网段的报文进行基于IP地址的三层转发。

通过VLANIF接口实现VLAN间互通只适用于各个VLAN内主机处于不同网段的场景。

### 2.2不同VLAN间的互通原理

#### 2.2.1 通过VLANIF实现同设备VLAN间互访

如图所示，用户主机Host1和Host2连接在同台设备上，分别属于VLAN2和VLAN3，并位于不同的网段。在DeviceA上分别创建VLANIF2和VLANIF3并配置其IP地址，然后将用户主机的缺省网关设置为所属VLAN对应VLANIF接口的IP地址。



当用户主机Host1发送报文给用户主机Host2时，报文的发送过程如下（假设DeviceA上还未建立任何转发表项）。

host1判断目的IP地址跟自己的IP地址不在同一网段，因此，它发出请求网关MAC地址的ARP请求报文，目的IP为网关IP地址10.1.1.1，目的MAC为全F。

报文到达DeviceA的接口interface1，DeviceA给报文添加VID=2的Tag（Tag的VID=接口的PVID），然后将报文的“源MAC地址+VID+接口”的对应关系（00e0-fc00-1111， 2，interface1）添加进MAC表。

DeviceA检查报文是ARP请求报文，且目的IP是自己VLANIF2接口的IP地址，给Host1应答，并将VLANIF2接口的MAC地址00e0-fc00-3333封装在应答报文中，应答报文从interface1发出前，剥掉VID=2的Tag。同时，DeviceA会将Host1的IP地址与MAC地址的对应关系记录到ARP表。

Host1收到DeviceA的应答报文，将DeviceA的VLANIF2接口的IP地址与MAC地址对应关系记录到自己的ARP表中，并向DeviceA发送目的MAC为00e0-fc00-3333、目的IP为Host2的IP地址 10.2.2.2的报文。

报文到达DeviceA的接口interface1，同样给报文添加VID=2的Tag。

DeviceA根据报文的“源MAC地址+VID+接口”的对应关系更新MAC表，并比较报文的目的MAC地址与VLANIF2的MAC地址，发现两者相等，进行三层转发，根据目的IP查找三层转发表，没有找到匹配项，上送CPU查找路由表。

CPU根据报文的目的IP去找路由表，发现匹配了一个直连网段（VLANIF3对应的网段），于是继续查找ARP表，没有找到，DeviceA会在目的网段对应的VLAN3的所有接口发送ARP请求报文，目的IP是10.2.2.2。从接口interface2发出前，根据接口配置，剥掉VID=2的Tag。

Host2收到ARP请求报文，发现请求IP是自己的IP地址，就发送ARP应答报文，将自己的MAC地址包含在其中。同时，将VLANIF3的MAC地址与IP地址的对应关系记录到自己的ARP表中。

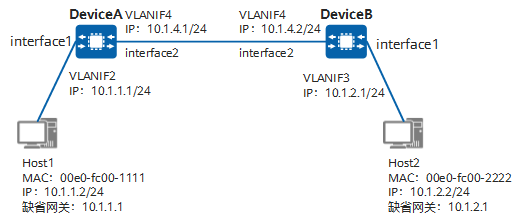
DeviceA的接口interface2收到Host2的ARP应答报文后，给报文添加VID=3的Tag，并将Host2的MAC和IP的对应关系记录到自己的ARP表中。然后，将Host1的报文转发给Host2，发送前，同样剥离报文中的Tag。同时，将Host2的IP地址、MAC地址、VID及出接口的对应关系记录到三层转发表中。

至此，Host1完成对Host2的单向访问。Host2访问Host1的过程与此类似。

#### 2.2.2 通过VLANIF实现跨设备VLAN间互访

由于VLANIF接口的IP地址只能在设备上生成直连路由，当不同VLAN的用户跨多台设备互访时，除配置VLANIF接口的IP地址外，还需要配置静态路由或运行动态路由协议。

如图所示，用户主机Host1和Host2连接在不同的设备上，分别属于VLAN2和VLAN3，并位于不同的网段。主机与设备之间使用Access接口，设备之间使用Trunk接口。在DeviceA上分别创建VLANIF2和VLANIF4，配置其IP地址为10.1.1.1和10.1.4.1；在DeviceB上分别创建VLANIF3和VLANIF4，配置其IP地址为10.1.2.1和10.1.4.2，并在DeviceA和DeviceB上分别配置静态路由。DeviceA上静态路由的目的网段是10.1.2.0/24，下一跳是10.1.4.2；DeviceB上静态路由的目的网段是10.1.1.0/24，下一跳是10.1.4.1。



当用户主机Host1发送报文给用户主机Host2时，报文的发送过程如下（假设DeviceA和DeviceB上还未建立任何转发表项）。

与同设备VLAN间互通（VLANIF接口）的步骤1～6一样，经过“Host1比较目的IP地址—>Host1查ARP表—>Host1获取网关MAC地址—>Host1将发给Host2的报文送到DeviceA—>DeviceA查MAC表—>DeviceA查三层转发表”的过程，DeviceA上送CPU查找路由表。

DeviceA的CPU根据报文的目的IP 10.1.2.2去找路由表，发现匹配了一条静态路由，目的网段是10.1.2.0/24的下一跳IP地址为10.1.4.2，于是继续查找ARP表，没有找到，DeviceA会在下一跳IP地址对应的VLAN4的所有接口广播ARP请求报文，目的IP是10.1.4.2。报文从DeviceA的接口interface2发出前，根据接口配置，发送该ARP请求报文到DeviceB的interface2接口，不会剥除报文的Tag。

ARP请求报文到达DeviceB后，发现目的IP为VLANIF4接口的IP地址，给DeviceA回应，填写VLANIF4接口的MAC地址。

DeviceB的ARP响应报文从其interface2直接发送到DeviceA，DeviceA接收后，记录VLANIF4的MAC地址与IP地址的对应关系到ARP表项。

DeviceA将Host1的报文转发给DeviceB，报文的目的MAC修改为DeviceB的VLANIF4接口的MAC地址，源MAC地址修改自己的VLANIF4接口的MAC地址，并将刚用到的转发信息记录在三层转发表中（10.1.2.0/24， 下一跳IP的MAC地址， 出口VLAN， 出接口）。同样，报文是直接转发到DeviceB的interface2接口。

DeviceB收到DeviceA转发的Host1的报文后，与同设备VLAN间互通（VLANIF接口）的步骤6～9一样，经过“查MAC表—>查三层转发表—>送CPU—>匹配直连路由—>查ARP表并获取Host2的MAC地址—>将Host1的报文转发给Host2”的过程，同时将Host2的IP地址、MAC地址、出口VLAN、出接口记录到三层转发表项。

至此，Host1完成对Host2的单向访问。Host2访问Host1的过程与此类似。