

VLAN

VLAN 概述

以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）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、性能显著下降甚至使网络不可用等问题。通过交换机实现LAN互联虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个LAN划分成多个逻辑的LAN——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，广播报文被限制在一个VLAN内，如图1所示。

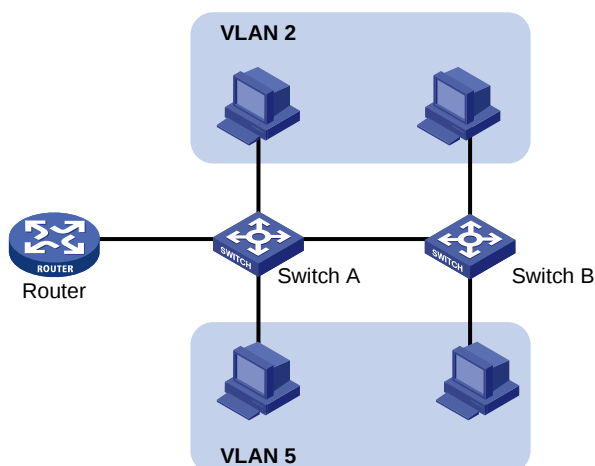


图1 VLAN 示意图

VLAN 的划分不受物理位置的限制：不在同一物理位置范围的主机可以属于同一个VLAN；一个VLAN包含的用户可以连接在同一个交换机上，也可以跨越交换机，甚至可以跨越路由器。

VLAN 的优点如下：

- 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。
- 增强局域网的安全性。VLAN间的二层报文是相互隔离的，即一个VLAN内的用户不能和其它VLAN内的用户直接通信，如果不同VLAN要进行通信，则需通过路由器或三层交换机等三层设备。

- 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。

VLAN 原理

要使网络设备能够分辨不同 VLAN 的报文，需要在报文中添加标识 VLAN 的字段。由于普通交换机工作在 OSI 模型的数据链路层，只能对报文的数据链路层封装进行识别。因此，如果添加识别字段，也需要添加到数据链路层封装中。

IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 IEEE 802.1Q 协议标准草案，对带有 VLAN 标识的报文结构进行了统一规定。

传统的以太网数据帧在目的 MAC 地址和源 MAC 地址之后封装的是上层协议的类型字段，如图 2 所示。

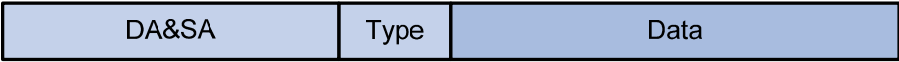


图2 传统以太网帧封装格式

其中 DA 表示目的 MAC 地址，SA 表示源 MAC 地址，Type 表示报文所属协议类型。

IEEE 802.1Q 协议规定在目的 MAC 地址和源 MAC 地址之后封装 4 个字节的 VLAN Tag，用以标识 VLAN 的相关信息。

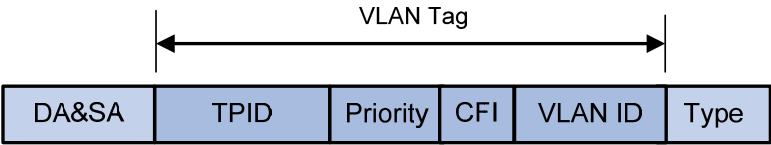


图3 VLAN Tag 的组成字段

如图 3 所示，VLAN Tag 包含四个字段，分别是 TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和 VLAN ID。

- TPID 用来判断本数据帧是否带有 VLAN Tag，长度为 16bit，缺省取值为 0x8100。
- Priority 表示报文的 802.1P 优先级，长度为 3bit，相关内容请参见“QoS 分册”中的“QoS 配置”。
- CFI 字段标识 MAC 地址在不同的传输介质中是否以标准格式进行封装，长度为 1bit，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，缺省取值为 0。
- VLAN ID 标识该报文所属 VLAN 的编号，长度为 12bit，取值范围为 0~4095。由于 0 和 4095 为协议保留取值，所以 VLAN ID 的取值范围为 1~4094。

网络设备利用 VLAN ID 来识别报文所属的 VLAN，根据报文是否携带 VLAN Tag 以及携带的 VLAN Tag 值，来对报文进行处理。