1 VLAN 简介

1.1 VLAN 简介

1.1.1 VLAN 概述

传统的以太网是广播型网络，网络中的所有主机通过 HUB 或交换机相连，处在同一个广播域中。HUB 和交换机作为网络连接的基本设备，在转发功能方面有一定的局限性：

- HUB 是物理层设备，没有交换功能，接收到的报文会向除接收端口外的所有端口转发；
- 交换机是数据链路层设备，具备根据报文的目的 MAC 地址进行转发的能力，但在收到广播报文或未知单播报文（报文的目的 MAC 地址不在交换机 MAC 地址表中）时，也会向除接收端口之外的所有端口转发。

上述情况会造成以下的网络问题：

- 网络中可能存在着大量广播和未知单播报文，浪费网络资源。
- 网络中的主机收到大量并非以自身为目的地的报文，造成了严重的安全隐患。

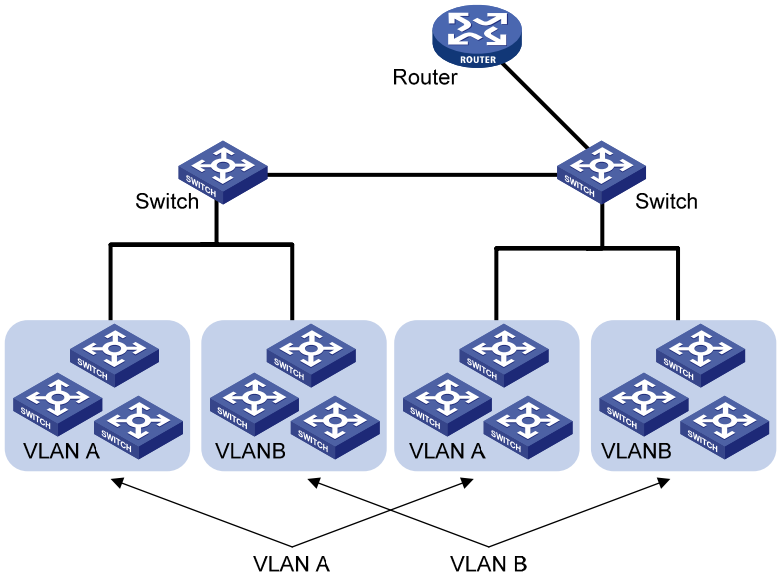
解决以上网络问题的根本方法就是隔离广播域。传统的方法是使用路由器，因为路由器是依据目的 IP 地址对报文进行转发，不会转发链路层的广播报文。但是路由器的成本较高，而且端口较少，无法细致地划分网络，所以使用路由器隔离广播域有很大的局限性。

为了解决以太网交换机在局域网中无法限制广播的问题，VLAN（Virtual Local Area Network，虚拟局域网）技术应运而生。

VLAN 的组成不受物理位置的限制，因此同一 VLAN 内的主机也无须放置在同一物理空间里。

如图1-1所示，VLAN把一个物理上的LAN划分成多个逻辑上的LAN，每个VLAN是一个广播域。VLAN内的主机间通过传统的以太网通信方式即可进行报文的交互，而处在不同VLAN内的主机之间如果需要通信，则必须通过路由器或三层交换机等网络层设备才能够实现。

图1-1 VLAN 组网示意图



1.1.2 VLAN 的优点

与传统以太网相比，VLAN 具有如下的优点：

- 控制广播域的范围：局域网内的广播报文被限制在一个 VLAN 内，节省了带宽，提高了网络处理能力。
- 增强了 LAN 的安全性：由于报文在数据链路层被 VLAN 划分的广播域所隔离，因此各个 VLAN 内的主机间不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。
- 灵活创建虚拟工作组：使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟工作组范围内移动时，不需要更改网络配置即可以正常访问网络。

1.1.3 VLAN 原理

1. VLAN Tag

为使交换机能够分辨不同 VLAN 的报文，需要在报文的数据链路层添加标识 VLAN 的字段。

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 Tag 的报文结构进行了统一规定。

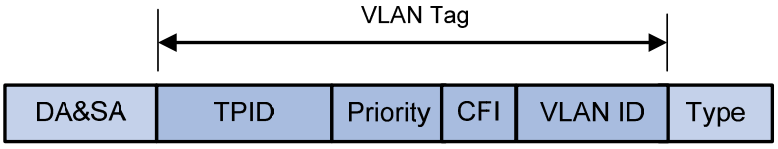
传统的以太网数据帧在目的MAC地址和源MAC地址之后封装上层协议的类型字段。如 图 1-2所示。

图1-2 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 表示上层协议的类型字段。

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1-3 VLAN Tag 的组成字段



如 图 1-3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：用来标识本数据帧是带有 VLAN Tag 的数据。该字段长度为 16bit，在 H3C 系列以太网交换机上缺省取值为协议规定的 0x8100。
- Priority：用来表示 802.1P 的优先级。该字段长度为 3bit，相关介绍和应用请参见本手册“QoS”部分的介绍。
- CFI：用来标识 MAC 地址是否以标准格式进行封装。该字段长度为 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：用来标识该报文所属 VLAN 的编号。该字段长度为 12bit，取值范围为 0～4095。由于 0 和 4095 通常不使用，所以 VLAN ID 的取值范围一般为 1～4094。

说明

这里的帧格式以Ethernet II型封装为例，以太网还支持 802.2/802.3 型封装。对于 802.2/802.3 型封装，VLAN Tag也会在目的MAC和源MAC地址字段之后进行封装。802.2/802.3 封装的具体格式请参见“1.3.2 以太网数据的封装格式”。

交换机利用VLAN ID来识别报文所属的VLAN，当接收到的报文不携带VLAN Tag时，交换机会为该报文封装带有接收端口缺省VLAN ID的VLAN Tag，将报文在接收端口的缺省VLAN中进行传输。有关端口缺省VLAN设置的内容，请参见 1.2.2 部分的介绍。

2. VLAN 的 MAC 地址学习机制

交换机是根据报文的目的 MAC 地址对报文进行转发的，因此交换机维护了一种记录 MAC 地址与端口对应关系的转发表来指导交换机进行转发，这个表称为 MAC 地址转发表。交换机将接收到的报文的源 MAC 地址以及接收端口记录到该表中，供后续报文转发使用，这个记录过程称为 MAC 地址的学习过程。

在配置了 VLAN 后，交换机的 MAC 地址学习方式分为两种：

- SVL（Shared VLAN Learning，共享 VLAN 学习）：交换机将所有 VLAN 中的端口学习到的 MAC 地址表项全部记录到一张共享的 MAC 地址转发表内，从任意 VLAN 内的任意端口接收的报文都参照此表中的信息进行转发。
- IVL（Independent VLAN Learning，独立 VLAN 学习）：交换机为每个 VLAN 维护独立的 MAC 地址转发表。由某个 VLAN 内的端口接收的报文，其源 MAC 地址只被记录到该 VLAN 的 MAC 地址转发表中，且报文的转发只以该表中的信息作为依据。

H3C S3100 系列以太网交换机目前采用 IVL 方式进行 MAC 地址学习。有关 MAC 地址转发表的更多内容，请参见本手册“MAC 地址转发表管理”部分的介绍。

1.1.4 VLAN 接口

不同 VLAN 间的主机不能直接通信，需要通过路由器或三层交换机等网络层设备进行转发，S3100 系列以太网交换机支持通过配置 VLAN 接口实现对报文进行三层转发的功能。

VLAN 接口是一种三层模式下的虚拟接口，主要用于实现 VLAN 间的三层互通，它不作为物理实体存在于交换机上。每个 VLAN 对应一个 VLAN 接口，该接口可以为本 VLAN 内端口收到的报文根据其目的 IP 地址在网络层进行转发。通常情况下，由于 VLAN 能够隔离广播域，因此每个 VLAN 也对应一个 IP 网段，VLAN 接口将作为该网段的网关对需要跨网段转发的报文进行基于 IP 地址的三层转发。

说明

H3C S3100 系列以太网交换机只支持配置一个 VLAN 接口，且该接口对应的 VLAN 需要先被配置为管理 VLAN，详情请参见“配置管理 VLAN”。

1.1.5 VLAN 类型

根据划分方式的不同，可以将 VLAN 分为不同类型，下面列出了 6 种最常见的 VLAN 类型：

- 基于端口的 VLAN

- 基于 MAC 地址的 VLAN
- 基于协议的 VLAN
- 基于 IP 子网的 VLAN
- 基于策略的 VLAN
- 其它 VLAN

目前 S3100 系列交换机支持基于端口的 VLAN 和基于协议的 VLAN。

1.2 基于端口的 VLAN

基于端口的 VLAN 是最简单的一种 VLAN 划分方法。用户可以将设备上的端口划分到不同的 VLAN 中，此后从某个端口接收的报文将只能在相应的 VLAN 内进行传输，从而实现广播域的隔离和虚拟工作组的划分。

以太网交换机的端口链路类型可以分为三种：Access、Trunk、Hybrid。这三种端口在加入 VLAN 和对报文进行转发时会进行不同的处理。

基于端口的 VLAN 具有实现简单，易于管理的优点，适用于连接位置比较固定的用户。

1.2.1 以太网端口的链路类型

S3100 系列以太网交换机支持的以太网端口链路类型有三种：

- Access 类型：端口只能属于 1 个 VLAN，一般用于交换机与终端用户之间的连接；
- Trunk 类型：端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，一般用于交换机之间的连接；
- Hybrid 类型：端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。

说明

Hybrid 端口可以允许多个 VLAN 的报文发送时不携带标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不携带标签。

三种类型的端口可以共存在一台设备上，但 Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再设置为其他类型端口。例如：Trunk 端口不能直接被设置为 Hybrid 端口，只能先设为 Access 端口，再设置为 Hybrid 端口。

1.2.2 配置以太网端口的缺省 VLAN ID

Access 端口只能属于 1 个 VLAN，所以它的缺省 VLAN 就是它所在的 VLAN，不用设置；Hybrid 端口和 Trunk 端口可以属于多个 VLAN，所以需要设置端口的缺省 VLAN ID。

将端口加入VLAN并指定了端口的缺省VLAN后，三类端口对报文的接收和发送会有不同的处理方式，具体描述请参见 表 1-1、表 1-2和 表 1-3。

表1-1 Access 端口收发报文的处理

接收报文时的处理		发送报文时的处理
当接收到的报文不带 Tag 时	当接收到的报文带有 Tag 时	
接收该报文，并为报文添加缺省 VLAN 的 Tag	• 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	由于 VLAN ID 就是缺省 VLAN ID，不用设置，去掉 Tag 后发送

表1-2 Trunk 端口收发报文的处理

接收报文时的处理		发送报文时的处理
当接收到的报文不带 Tag 时	当接收到的报文带有 Tag 时	
• 当端口已经加入缺省 VLAN 时，为报文封装缺省 VLAN 的 Tag 并转发 • 当端口没有加入缺省 VLAN 时，丢弃该报文	• 当 VLAN ID 是该端口允许通过的 VLAN ID 时：接收该报文 • 当 VLAN ID 不是该端口允许通过的 VLAN ID 时：丢弃该报文	• 当 VLAN ID 与缺省 VLAN ID 相同时：去掉 Tag，发送该报文 • 当 VLAN ID 与缺省 VLAN ID 不同时：保持原有 Tag，发送该报文

表1-3 Hybrid 端口收发报文的处理

接收报文时的处理		发送报文时的处理
当接收到的报文不带 Tag 时	当接收到的报文带有 Tag 时	
• 当端口已经加入缺省 VLAN 时，为报文封装缺省 VLAN 的 Tag 并转发 • 当端口没有加入缺省 VLAN 时，丢弃该报文	• 当 VLAN ID 是该端口允许通过的 VLAN ID 时：接收该报文 • 当 VLAN ID 不是该端口允许通过的 VLAN ID 时：丢弃该报文	当报文中携带的 VLAN ID 是该端口允许通过的 VLAN ID 时，发送该报文，并可以通过 **port hybrid vlan** 命令配置端口在发送该 VLAN（包括缺省 VLAN）的报文时是否携带 Tag

注意

建议将本端 Hybrid 端口或 Trunk 端口的缺省 VLAN ID 和相连的对端交换机的 Hybrid 端口或 Trunk 端口的缺省 VLAN ID 配置为一致，否则端口可能无法正确转发报文。

1.2.3 将当前端口加入指定 VLAN

用户可以将当前以太网端口加入到指定的 VLAN 中。执行该配置以后，以太网端口就可以转发指定 VLAN 的报文，从而实现本交换机上的 VLAN 与对端交换机上相同 VLAN 的互通。

Access 端口只能加入到 1 个 VLAN 中，Hybrid 端口和 Trunk 端口可以加入到多个 VLAN 中。

说明

在将 Access 端口或 Hybrid 端口加入到指定的 VLAN 前，指定的 VLAN 必须已经创建。

1.3 基于协议的 VLAN

说明

在 S3100 系列以太网交换机中，只有 S3100-EI 系列交换机支持协议 VLAN 功能。

1.3.1 基于协议的 VLAN 概述

基于协议的 VLAN 也称为协议 VLAN（为方便描述，下文将统称为协议 VLAN），是另一种 VLAN 划分方法。通过配置协议 VLAN，交换机可以对端口上收到的未携带 VLAN Tag 的报文进行分析，根据不同的封装格式及特殊字段的数值将报文与用户设定的协议模板相匹配，为匹配成功的报文添加相应的 VLAN Tag，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。

此特性主要用于将网络中提供的服务类型与 VLAN 相绑定，方便管理和维护。

1.3.2 以太网数据的封装格式

为清楚地了解交换机对报文协议的识别过程，先简要介绍一下以太网常用的数据封装格式。

1. Ethernet II 与 802.2/802.3 封装

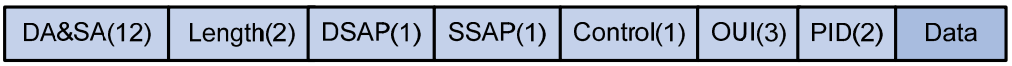
目前以太网的报文封装主要有两种类型，分别为 Ethernet II 型和 802.2/802.3 型，分别由 RFC894 和 RFC1042 规定。两种报文的封装格式如下：

- Ethernet II 型

图1-4 Ethernet II 型报文封装格式

- 802.2/802.3 型

图1-5 802.2/802.3 型报文封装格式



DA、SA 分别表示报文的目的 MAC 地址和源 MAC 地址，括号中的数字表示此字段的长度，单位为字节。

由于以太网报文的最大长度为 1500 字节，转换成 16 进制数字为 0x05DC，所以 802.2/802.3 封装的 Length 字段取值范围为 0x0000～0x05DC。

而 Ethernet II 型封装中的 Type 字段取值范围为 0x0600～0xFFFF。

Type 或 Length 字段取值为 0x05DD～0x05FF 的报文将被认为是非法报文，交换机将直接丢弃。

交换机根据这两个字段的取值范围的不同来区分 Ethernet II 型和 802.2/802.3 型报文。

1.3.3 各种协议支持的封装格式

802.2/802.3 型封装格式又分为 802.3 raw、802.2 LLC和 802.2 SNAP三种扩展封装格式，表 1-4 列出了各种协议所支持的封装格式，括号中为该协议的协议类型值。

表1-4 各种协议支持的封装格式

封装 / 协议	Ethernet II	802.3 raw	802.2 LLC	802.2 SNAP
IP（0x0800）	支持	不支持	不支持	支持
IPX（0x8137）	支持	支持	支持	支持
AppleTalk（0x809B）	支持	不支持	不支持	支持

注意

目前 S3100 系列以太网交换机只支持对 EtherentII 型封装的报文协议类型进行匹配，不支持对 802.2/802.3 型及其扩展封装的报文协议类型进行匹配。

1.3.4 协议 VLAN 的实现方式

S3100 系列以太网交换机通过协议模板来匹配报文，实现根据报文的协议将报文划分到不同 VLAN 中传输的功能。

协议模板是用来匹配报文所属协议类型的标准，协议模版由“封装格式+协议类型”组成，分为标准模板和自定义模板两种：

- 标准模板是指以 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。
- 自定义模板是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。

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。协议 VLAN 内的端口需要根据报文协议的不同，为各种报文封装不同 VLAN 的 Tag，即该端口需要属于多个 VLAN。而且，由于该端口连接客户端，普通客户端无法处理携带 VLAN Tag 的报文，所以需要该端口在发送所有报文时去掉 VLAN Tag。综上所述，在向协议 VLAN 内添加端口并建立端口与协议模板的关联之前，需要将端口配置为 Hybrid 端口，并配置该端口在转发来自所有协议 VLAN 的报文时采取去除 VLAN Tag 的操作。