TP-LINK®

802.1Q VLAN 技术白皮书

TP-LINK 管理型交换机

REV1.0.1
1910040617

目录

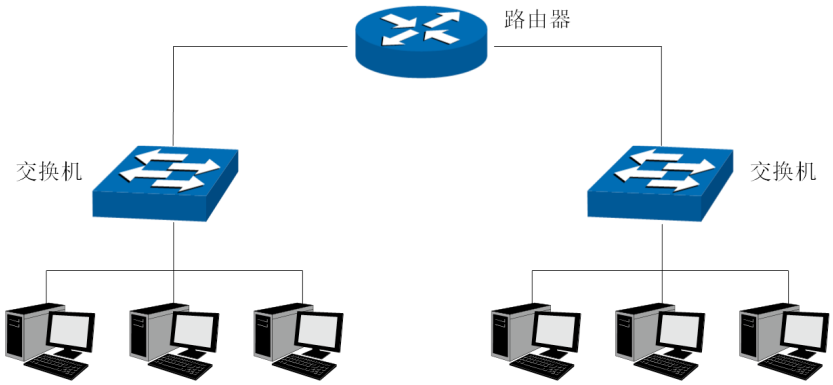
1 VLAN 概述

VLAN（Virtual Local Area Network，虚拟局域网）是一种将局域网设备从逻辑上划分成不同网段，从而实现虚拟工作组的数据交换技术。下面从 VLAN 的产生背景开始，详细介绍 VLAN 的相关概念和实际应用。

1.1 产生背景

二层交换机工作在数据链路层，在收到广播报文或未知的单播报文时，会向其他所有端口转发该报文，这样，我们可以认为一个二层交换机构成一个广播域，即广播帧能够直接到达的范围。若整个网络只有一个广播域，那么当某台设备发出广播报文时，其他所有设备都会收到该报文。随着网络中计算机数量的增多，广播报文的数量也会急剧增加，从而导致网络的传输效率下降。特别是当某个网络设备出现故障或者网络中出现环路时，广播信息会大量泛洪，从而导致广播风暴，使整个网络陷于瘫痪。因此，当网络中的设备数量增加到一定规模时，必须采取措施对网络进行分段，从而分隔广播域，减小这些潜在问题可能造成的不良影响。通过路由器，我们可以对网络进行分段，从而隔离广播域，如图 1–1 所示。

图 1–1　路由器划分网络

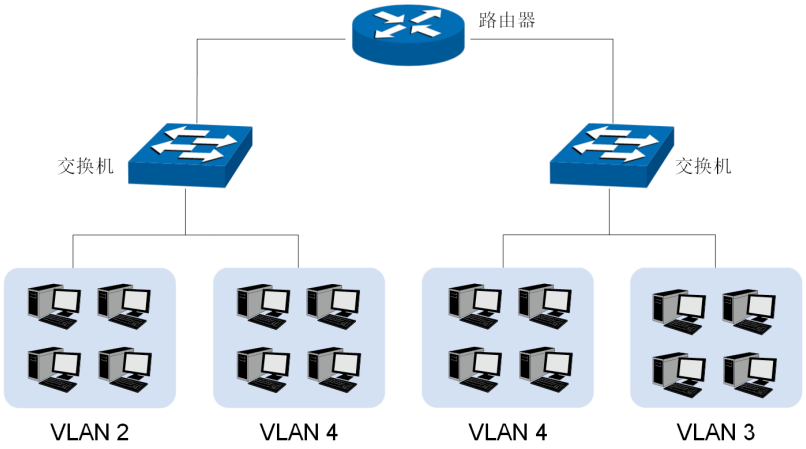


但是，这也不能解决同一交换机下的用户隔离。并且，随着网络的不断扩展，网络结构也日趋复杂，必须使用更多的路由器才能将不同的用户划分到各自的广播域中，而路由器数量的增多也会导致网络延时加长，网络数据传输速度下降。其次，不管从网络建设的成本还是管理上，这种方式都存在不足。

与路由器相比，交换机具有多个网络接口，通过它来分隔广播域，能使网络划分方式更加灵活，成本也相对更低。因此，VLAN 技术应运而生。利用 VLAN 技术，网络管理者可以根据实际应用需求，将局域网中的不同用户从逻辑上划分成不同的广播域，也就是 VLAN。VLAN 从逻辑上划分，不受物理位置的限制，一个 VLAN 包含的用户可以连接在同一台交换机上，也可以跨越交换机。如图 1–2 所示，一台路由器连接了两台二层交换机，交换机上划分了不

同的 VLAN，若干主机通过交换机接入网络中，并分别属于不同的 VLAN。通过这样的划分，不同 VLAN 之间的设备就不能直接互相通信了。

图 1-2　VLAN 常用网络拓扑



1.2　VLAN 的优点

VLAN 在逻辑上把网络资源和网络用户按照一定的规则进行划分，其主要优点表现在以下几个方面：

- 提高网络性能。VLAN 技术把网络划分成逻辑上的不同广播域，将广播帧限制在 VLAN 中，从而避免了带宽的浪费，提高了网络处理能力。同时，VLAN 还能有效控制广播风暴的范围，减小此类网络问题所带来的损失。
- 方便网络管理。VLAN 将物理的局域网划分成了逻辑意义上的子网，不必考虑具体的物理位置。每一个 VLAN 都可以对应一个逻辑单位，如部门、项目组等，方便了企业或科研机构的管理。同时，这种划分方式增加了网络的灵活性，若某个用户从一个部门调到另一个部门，而办公位置没有发生改变，网络管理员只需对交换机等设备进行相应配置即可，而无需通过改变物理线路来将此用户接入到新部门中。
- 增强网络安全。不同 VLAN 内的设备要互相通信，必须通过路由器或三层交换机等设备。网络管理员可在三层设备上设置访问控制规则，确保 VLAN 内的数据不会被其他 VLAN 的设备窃听，从而提高了网络的安全性。

1.3　VLAN 的分类

根据不同的网络需求，可以选择不同的 VLAN 划分方式。目前我们最常用的 VLAN 划分方式是 802.1Q VLAN，这种方法配置比较简单，但当 VLAN 变更时，网络管理者的工作量较大。在 802.1Q VLAN 的基础上，我们可以添加一些标识，来实现其他几种 VLAN，比如 MAC VLAN、协议 VLAN 等。实现 VLAN 的方式多种多样，但几乎所有的这些实现方式都基于 IEEE 802.1Q 协议。本文档将详细介绍 802.1Q VLAN 的相关内容。

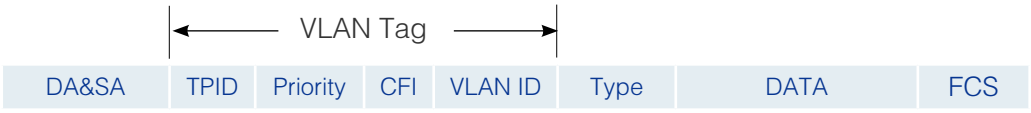
2 IEEE 802.1Q VLAN

IEEE 802.1Q 协议规定了 VLAN 的实现标准。过去各个厂商实现 VLAN 的方法并不完全相同，所以彼此无法兼容。IEEE 于 1999 年发布了用以规范 VLAN 实现方法的 IEEE 802.1Q 标准，进一步完善了 VLAN 的体系结构，统一了不同厂商的 VLAN 帧格式，从而使得不同厂商之间的 VLAN 互通成为可能。下面介绍 802.1Q 协议对 VLAN 帧格式提出的相应规范以及我司交换机的各端口类型。

2.1 VLAN 帧格式

为使交换机能够分辨不同 VLAN 的报文，IEEE 802.1Q 协议标准规定，在传统以太网数据帧中的 DA&SA（目的 MAC 地址和源 MAC 地址）之后封装 4 个字节的 802.1Q VLAN 标签，即 VLAN Tag，用以标识 VLAN 的相关信息，如图 2–3 所示。VLAN Tag 包含四个字段，分别是 TPID、Priority、CFI 和 VLAN ID。

图 2–3 带有 VLAN Tag 的以太网帧



VLAN 标签中的四个字段分别标识了该数据帧不同的信息，下面通过表 2–1 对这四个字段进行具体的说明。

表 2–1 VLAN Tag 字段含义

TPID	Tag Protocol Identifier，标签协议标识符。占 16 位，表明这是一个添加了 IEEE 802.1Q 标签的数据帧，用于和未加 VLAN 标记的数据帧进行区别，缺省取值为 0x8100。
Priority	优先级。占 3 位，共有 0–7 八个优先级，数值越大优先级越高，当交换机阻塞时，该字段用于确定交换机优先发送哪个数据帧。
CFI	Canonical Format Indicator，标准格式指示位。占 1 位，用以兼容以太网和令牌环网。CFI 字段用来标识 MAC 地址是否以标准格式进行封装，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。在以太网中该值总为 0，表示以标准格式封装 MAC 地址。
VLAN ID	VLAN Identifier，VLAN 标识符，简称 VID。占 12 位，用来标识该报文所属的 VLAN 。VLAN ID 的取值范围为 0~4095，由于 0 和 4095 是保留值，通常不使用，所以取值范围一般为 1~4094。

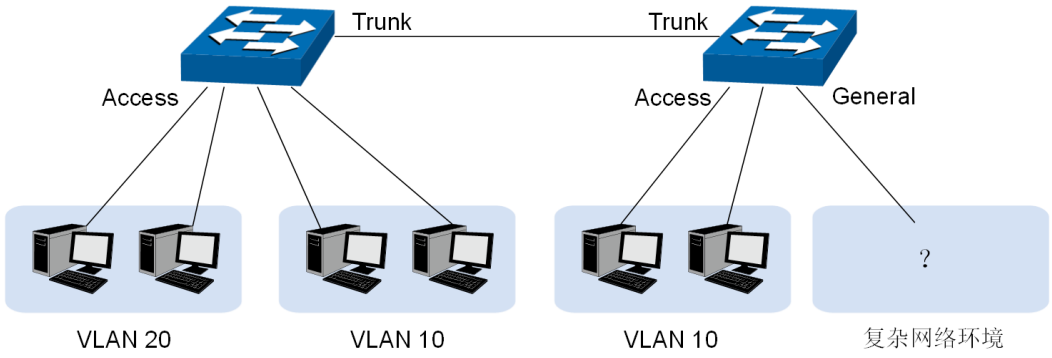
2.2 PVID

PVID（Port VLAN ID）用于表示端口默认所属的 VLAN，即缺省 VLAN。PVID 主要用于以下两种情形：当设备收到不带 Tag 的数据帧时，将根据 PVID 为数据帧插入 VLAN Tag；当设备接收到 UL 包或广播包的时候，由于 PVID 指定了端口默认所属的 VLAN，设备会将这些数据包在该端口的缺省 VLAN 内广播。

2.3 端口类型及数据进出口规则

我司交换机有三种类型的端口：Access 端口、Trunk 端口和 General 端口。通常我们需要根据端口所连接的设备来配置端口类型。下面通过图 2-4 所示的网络拓扑图具体介绍这几种不同类型的端口。

图 2-4 链路类型配置示意图



Access 端口

Access 端口只能属于 1 个 VLAN，出口规则为 UNTAG，也就是从该端口发送出去的数据帧不携带 VLAN Tag。Access 端口连接的多为不支持 VLAN 技术的终端设备，比如用户主机，如图 2-4 所示。

Trunk 端口

Trunk 端口可以属于多个 VLAN，出口规则为 TAG，也就是从该端口发送出去的数据帧会携带 VLAN Tag。Trunk 端口一般用于连接支持 VLAN 技术的网络设备，比如交换机或路由器。在实际网络中，VLAN 经常跨接在不同的通信设备上，如图 2-4 所示，此时需要将两台交换机相连的端口类型设置为 Trunk，以保证通信设备能区分不同 VLAN 的数据帧。

General 端口

General 端口可以属于多个 VLAN，出口规则可以根据该端口连接设备的实际情况灵活配置，既可以设置为带 Tag 发送报文，也可以设为不带 Tag 发送报文。因此，它既能用于网络设备之间的连接，也能用于网络设备和用户之间的连接。当与交换机相连的某个网络环境比较复

杂，无法判断网络中的设备是哪种类型，或者该网络中有多种类型的设备时，可将交换机和该网络相连端口类型设置为 General，如图 2–4 所示。

端口类型本质是通信设备接收和转发数据帧的处理方式。每一种类型的端口都有相应的数据进出口处理规则，入口规则表示接收数据帧时的处理方式，出口规则表示转发数据帧时的处理方式。表 2–2 介绍了三种类型端口的数据进出口处理规则。

表 2–2　端口的数据进出口处理规则

Access	接收报文时： 如果报文不带 Tag，则接收报文，并为报文添加缺省 VLAN 的 Tag； 如果报文带 Tag 且 VLAN ID ＝端口 PVID，则接收报文； 如果报文带 Tag 而 VLAN ID ≠端口 PVID，则丢弃报文。 发送报文时： 去掉 Tag 后，发送报文。
Trunk	接收报文时： 如果报文不带 Tag，则接收报文，并为报文添加缺省 VLAN 的 Tag； 如果报文带 Tag 且 VLAN ID 属于端口允许通过的 VLAN ID，则接收报文； 如果报文带 Tag 而 VLAN ID 不属于端口允许通过的 VLAN ID，则丢弃报文。 发送报文时： 转发端口默认 VLAN 的数据时去 tag 后发送报文，否则保持原 Tag 发送报文。（我司交换机 Trunk 端口出口规则不同机型有一定差异，详见各系列交换机配置指南）
General	接收报文时： 如果报文不带 Tag，则接收报文，为报文添加缺省 VLAN 的 Tag； 如果报文带 Tag 且 VLAN ID 属于端口允许通过的 VLAN ID，则接收报文； 如果报文带 Tag 而 VLAN ID 不属于端口允许通过的 VLAN ID，则丢弃报文。 发送报文时： 当出口规则配置为 TAG 时，保持原有 Tag 发送报文。 当出口规则配置为 UNTAG 时，去 Tag 后发送报文。

我司部分交换机仅有 General 端口，可灵活配置出口规则为 TAG 或 UNTAG。详情请见各交换机配置指南。

3 802.1Q VLAN 技术实现

3.1 VLAN 的 MAC 地址学习机制

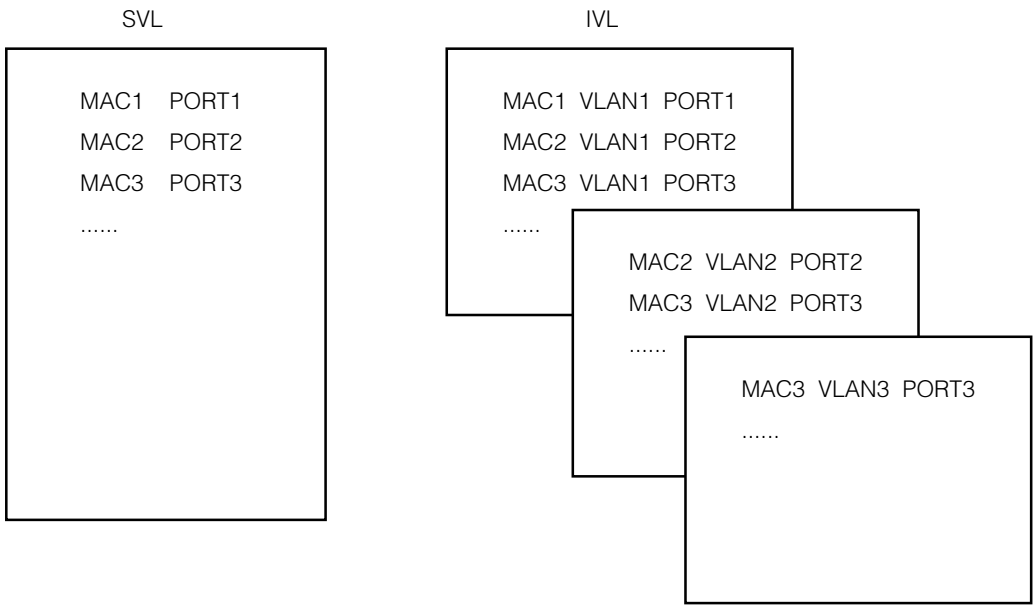
交换机是通过 VLAN ID 来区分识别不同 VLAN 的。对于支持 802.1Q VLAN 的交换机，其 MAC 地址表需同时维护 MAC 地址、转发端口和 VLAN ID 信息。其中，VLAN ID 信息将根据收到数据帧的 Tag 字段来确定，当收到的数据帧不带 Tag 时，则根据接收端口的缺省 VLAN 来确定。

在配置了 VLAN 后，交换机的 MAC 地址学习方式有两种：

- SVL（Shared VLAN Learning，共享式 VLAN 学习）：MAC 地址表项全部记录到一张共享的 MAC 地址转发表中，一个 MAC 地址在整张表中是唯一的。当交换机收到数据帧时会先进行 MAC 地址查询，然后再进行后续的 VLAN 查询。
- 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，因此 MAC 地址表在逻辑上可以看成根据 VLAN 信息被分成了多张地址表。某个 VLAN 的成员端口接收到数据帧时，其源 MAC 地址只被记录到该 VLAN 的 MAC 地址转发表中，且只依据该表中的信息转发数据帧。

图 3–1 简要表示了这两种 MAC 地址学习机制。在 SVL 中，所有 MAC 地址被记录到同一张表中，且一个 MAC 地址只能属于一个 VLAN；在 IVL 中，我们可以从逻辑上认为每个 VLAN 单独拥有一张地址表，一个 MAC 地址可以同时记录到不同 VLAN 的表项中。

图 3–1　MAC 地址学习机制



我司在售交换机均为 IVL 交换机，因此在后续介绍中均以 IVL 交换机为例来介绍 802.1Q VLAN 的实现原理。IVL 交换机二层转发的基本流程如下：

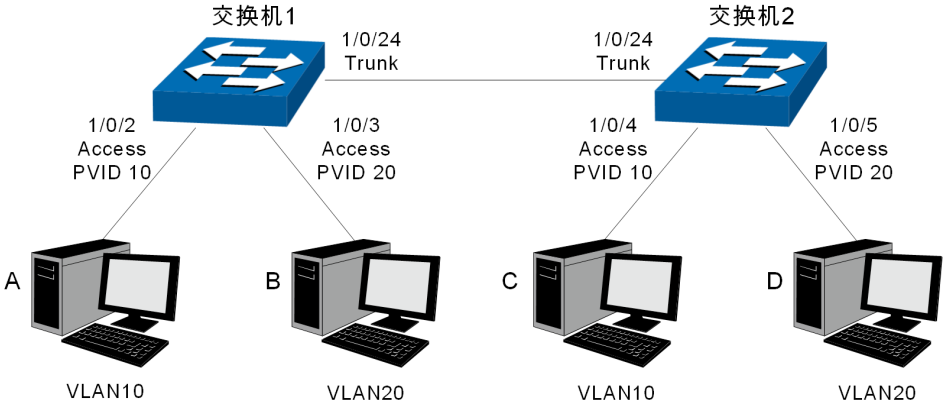
1) 收到数据帧后，根据其源 MAC 地址和 VLAN ID 信息添加或更新 MAC 地址表项。

2) 根据目的 MAC 地址和 VLAN ID 信息查找 MAC 地址表项。如果没有找到匹配项，则将数据帧在 VLAN ID 对应的 VLAN 内广播；如果能找到匹配表项，则将数据帧向表项中对应的端口进行转发。

3.2 VLAN 内的通信

下面通过一个示例来讲解同一 VLAN 内的设备进行通信的过程。在两台出厂设置的交换机上分别创建两个 VLAN，VLAN10 和 VLAN20，并分别设置交换机与主机相连的端口类型为 Access，两台交换机相连的端口类型为 Trunk。将交换机 1 的端口 2 加入 VLAN10，端口 3 加入 VLAN20，端口 24 同时加入 VLAN10 和 VLAN20；将交换机 2 的端口 4 加入 VLAN10，端口 5 加入 VLAN20，端口 24 同时加入 VLAN10 和 VLAN20，如图 3-2 所示。

图 3-2 跨交换机的 VLAN 内通信



主机 A 与主机 C 第一次通信的过程如下：

1) 主机 A 向交换机 1 发送一个不带 VLAN Tag 的数据帧，交换机 1 的 Access 端口接收该数据帧后，由于该端口的 PVID 值为 10，故为数据帧添加一个带有 VLAN ID=10 的标签。

2) 由于交换机 1 的 MAC 地址表中暂时还没有该数据帧对应的 MAC 地址信息，故将数据帧中的源 MAC 地址、VLAN ID 信息以及对应的端口号 2 添加到 MAC 地址表中，并将该数据帧在 VLAN 10 内广播。

3) 交换机 1 的 Trunk 端口 24 属于 VLAN10，故该端口接收数据帧，保持 VLAN ID=10 的标签，并从该端口转发给交换机 2。

4) 交换机 2 的 Trunk 端口 24 也属于 VLAN 10，故该端口接收数据帧。交换机 2 查询自己的 MAC 地址表，发现不存在该表项，故将数据帧中的源 MAC 地址、VLAN ID 信息以及对应的端口号 24 添加到自己的 MAC 地址表中，并将该数据帧在 VLAN 10 内广播。

5) 交换机 2 的 Access 端口 4 属于 VLAN10，故该端口接收数据帧，并将帧中的 VLAN 标签去掉后转发给主机 C。此外，由于主机 C 会给交换机返回信息，故交换机也会将主机 C 的 MAC 地址以及对应的端口号添加到地址表中。

这样，跨交换机的 VLAN 内通信就完成了。当主机 A 和主机 C 再次进行通信的时候，就能直接通过查询 MAC 地址表进行数据转发了。同样的，主机 B 与主机 D 之间也可以通过这样的过程实现 VLAN 内的通信。

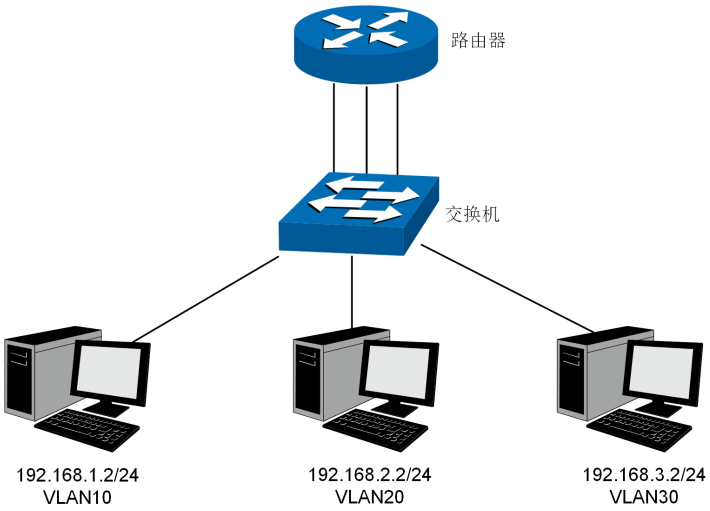
3.3 不同 VLAN 间的通信

同一个 VLAN 中的设备可以进行数据链路层的通信，而不同 VLAN 之间的设备通信则需要建立在网络层的基础上。一般有两种方法来实现 VLAN 之间的通信：通过路由器和通过三层交换机。下面分别介绍这两种实现不同 VLAN 之间通信的方法。

3.3.1 通过路由器实现 VLAN 间通信

路由器和交换机的连接方式有两种。一种是把路由器的不同物理接口分别连接到交换机上的每个 VLAN，并将交换机上与路由器相连的端口设置为相应 VLAN 的访问链路，如图 3–3 所示。

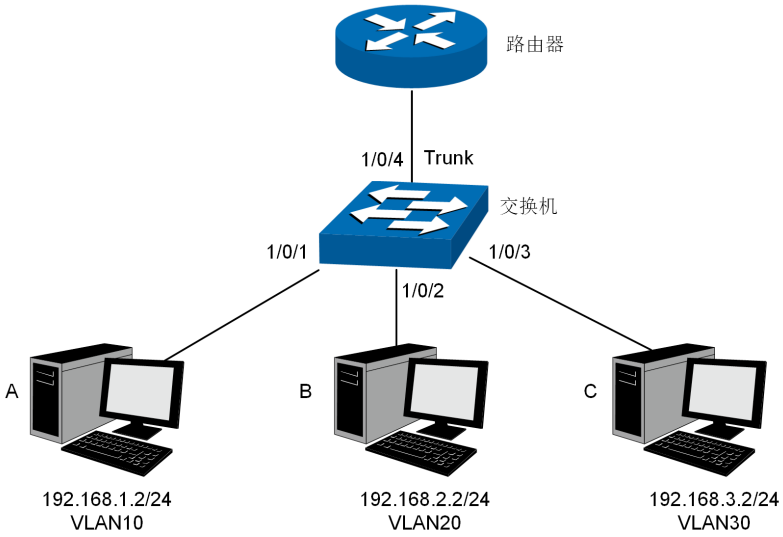
图 3–3 通过路由器实现 VLAN 间通信



这种连接方法比较简单，但是网络扩展难度大。每增加一个新的 VLAN，都需要消耗路由器和交换机上的端口，而且还需要重新布设一条网线。而路由器较交换机而言，所提供的端口较少，这使得网络管理的成本增加，因此不推荐此方法。

此外，我们还可以采用单臂路由的方式来实现 VLAN 之间的通信。这种方法是在路由器与交换机相连的那个物理端口上定义多个逻辑子接口，也就是从逻辑上将它分为多个虚拟端口。一个子接口连接一个 VLAN，每个子接口配置相应 VLAN 内的 IP 地址，并封装 802.1Q 协议。同时，在交换机上把与路由器相连的端口设置为 Trunk 端口。在这种方法中，路由器只使用一个端口连接到交换网络中，因此被称为单臂路由，如图 3–4 所示。

图 3-4　通过单臂路由方式实现 VLAN 间通信



该网络拓扑包含了 3 台主机、一台交换机和一台路由器，路由器和交换机之间配置中继链路 Trunk，交换机上设置了 3 个 VLAN，分别是 VLAN10，VLAN20 和 VLAN30。

当 VLAN10 中的主机 A 向 VLAN20 中的主机 B 发送信息时，交换机端口 1 收到主机 A 发出的数据帧，查询自己的 MAC 地址表，然后将数据帧从 Trunk 端口 4 转发出去，并为数据帧添加 VLAN ID=10 的标签。路由器收到数据帧后，发现它属于 VLAN10，因此把它交给负责 VLAN10 的子接口，该接口判断数据帧应发往负责 VLAN20 的子接口。负责 VLAN20 的子接口再为数据帧添加 VLAN ID=20 的标签并发回给交换机。交换机收到该数据后查询 MAC 地址表，去掉数据帧中的 VLAN 标签，将它从端口 2 发送给主机 B。这样主机 B 就接收到了主机 A 发给它的信息。可以看到，通过路由器进行 VLAN 之间的通信时，信息传输经过以下过程：发送者 –> 交换机 –> 路由器 –> 交换机 –> 接收者，即使通信的双方处在同一台交换机上，也必须经过这样的过程。

一般这种拓扑适用于小型网络，在已有的二层交换机的基础上，只需要购买一台路由器就能实现不同 VLAN 之间的通信。

3.3.2　通过三层交换机实现 VLAN 间通信

使用路由器来实现 VLAN 之间的通信，VLAN 之间的流量会集中到路由器和交换机互连的中继链路部分，这部分就容易成为速度的瓶颈。而三层交换机采用的是“一次路由，多次转发”的机制，能实现数据的高速转发，因此采用三层交换机来实现 VLAN 之间的通信更适合用于中大型网络，此时三层交换机可作为整个网络的核心。图 3-5 所示即为通过三层交换机进行 VLAN 之间通信的一个简单示意图。

图 3–5　三层交换实现 VLAN 之间通信

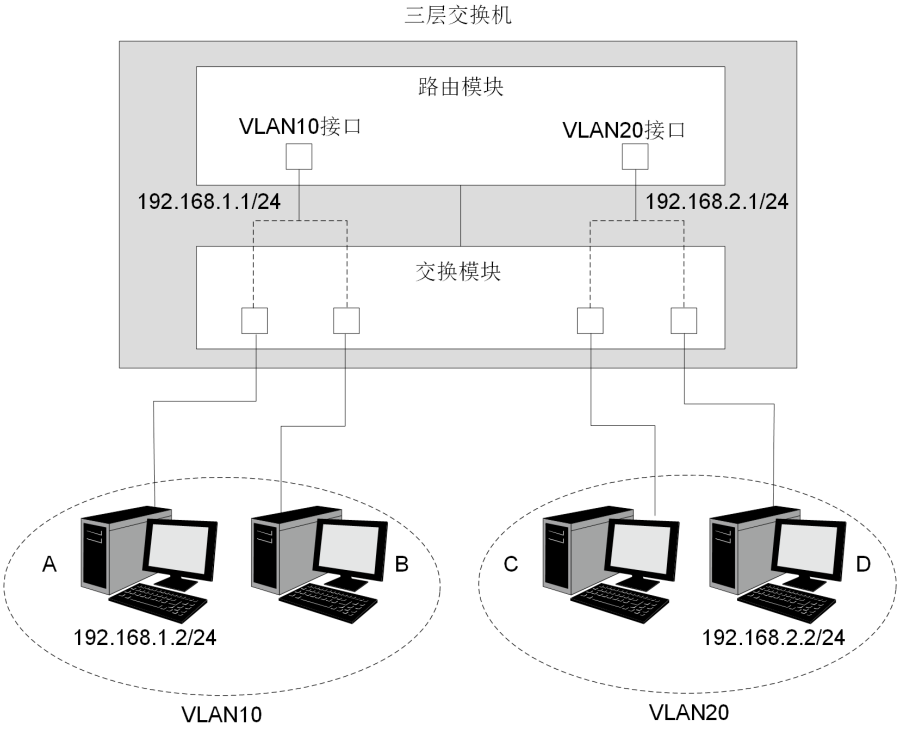


图 3–5 中，有一个三层交换机，连接了 4 台主机，分别属于 VLAN10 和 VLAN20。当主机 A（192.168.1.2）与主机 D（192.168.2.2）要通信时，主机 A 发送一个数据帧。三层交换机的交换模块接收该数据帧之后查询 MAC 地址表，为它添加一个 VLAN ID=10 的标签，然后转发给路由模块。路由模块接收数据帧后会通过 VLAN 信息判断将此数据交给 VLAN10 接口来处理。VLAN10 接口判断将数据帧交给 VLAN20 接口，VLAN20 接口再将数据帧转发回交换模块，最终数据帧中的 VLAN 信息被去掉后转发到主机 D。

可以看到，三层交换机进行 VLAN 间通信也会经过“发送者 –> 交换模块 –> 路由模块 –> 交换模块 –> 接收者”这样几个过程。但三层交换机一旦转发过一组目的 IP 相同的数据包之后，就会把该信息缓存，以后相同的数据包就能进行直接转发，而不需要通过路由处理了。由于交换模块对于数据包的二层转发速率远高于三层的路由模块，因此，通过三层交换机实现 VLAN 之间的通信能极大提高网络的数据转发效率，从而解决网络瓶颈的问题。

4 VLAN 设计方法

VLAN 的设计可从以下三个方面来考虑：确定 VLAN 类型，划分 VLAN 成员，规划 VLAN 间路由。

1) 确定 VLAN 类型。设计 VLAN 的首要任务是确定使用哪种 VLAN 类型。我们经常使用的是 802.1Q VLAN，这种 VLAN 的划分方法比较简单直接，实用性也比较强。我司交换机还提供 MAC VLAN、协议 VLAN 等 VLAN 划分类型。

2) 划分 VLAN 成员。确定 VLAN 类型之后，要规划好将哪些用户划分到哪个 VLAN 中，最好是在建网的同时将 VLAN 成员的划分作为一个因素综合考虑进工程中，这样能充分考虑 VLAN 的需求，全盘规划好网络结构。在网络建成之后，如果用户有了新需求，则有可能需要对原有结构做出适应性的改变。

3) 规划 VLAN 间路由。VLAN 的设计很大程度上和路由的规划密切相关，其中最直观的就是 IP 子网的划分。一般有如下几种情况：

   - 同一 IP 子网的成员属于不同的 VLAN。当一个 IP 子网的范围还不能足够细分工作组时，可以采用 VLAN 将其中的成员划分到更小的组里面，此时，不需要为这些 VLAN 的成员指定路由，因为他们已经在同一个子网了。
   - 同一 VLAN 的成员属于不同 IP 子网。这种划分方式主要适用于那些地理位置较远但需求相近的用户组，此时他们之间的路由就要使用 IP 子网间的路由。
   - 不同的 VLAN 和 IP 子网一一对应，即一个 IP 子网的成员都属于一个 VLAN。此时，VLAN 之间的路由与 IP 子网之间的路由重合。

5 参考文献

IEEE Std 802.1Q–2005

张蒲生 . 局域网技术 . 北京 : 人民邮电出版社 ,2007

鲍蓉 . 网络工程教程 . 北京 : 中国电力出版社 ,2008

晋玉星 . 计算机网络技术 . 北京 : 科学出版社 ,2012

Marina Smith.Virtual LANs. 北京 ; 清华大学出版社 ,2000

声明