目录

项目 1 组建局域网

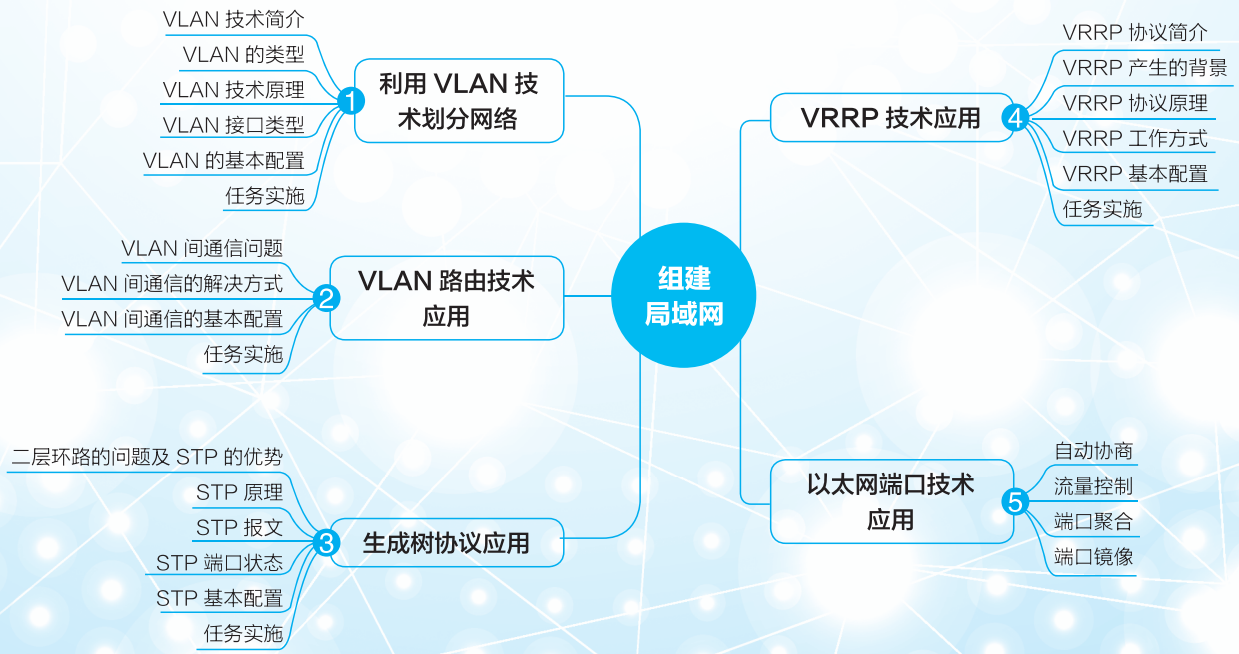
知识目标

1. 了解 VLAN 技术的基本概念。
2. 了解 VLAN 路由技术。
3. 了解生成树协议。
4. 了解 VRRP 技术。
5. 了解以太网端口技术。

技能目标

1. 学会二层 VLAN 组网方法。
2. 学会三层交换实现互联。
3. 学会 STP 任务实施。
4. 学会 VRRP 实现设备备份。
5. 学会以太网端口技术任务实施。

知识导图



笔记

项目导入

局域网（Local Area Network，LAN）是指在某一区域内由多台计算机互联而形成的计算机组，一般是在方圆几千米以内。在局域网内可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等操作。局域网是封闭型的，组机数量不受限制，可以由办公室内的两台计算机组成，也可以由一个公司内的上千台计算机组成。通过本项目的学习，读者可以自己组建局域网，实现文件共享等操作。

任务 1.1 利用 VLAN 技术划分网络

子任务 1.1.1 VLAN 技术简介

1. VLAN 的定义

VLAN（Virtual Local Area Network）的中文名为“虚拟局域网”。它是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术，主要应用于交换机和路由器中，但主流还是应用在交换机中。并不是所有交换机都具有此功能，只有 VLAN 协议的第二层以上的交换机才具有此功能，可以通过查看相应交换机的说明书得知。

2. VLAN 的作用与目的

早期的局域网（LAN）技术基于总线型结构，主要存在以下问题：

（1）若某时刻有多个节点同时试图发送消息，那么它们将产生冲突。

（2）从任意节点发出的消息都会发送到其他节点上，形成广播。

（3）所有主机共享一条传输通道，无法控制网络中的信息安全。

IEEE 于 1999 年颁布了用于标准化 VLAN 实现方案的 802.1Q 协议标准草案。VLAN 技术的出现，使得管理员可以根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于 VLAN 是从逻辑上而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同的物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

为了减少广播，需要在没有互访需求的主机之间进行隔离。路由器是基于三层 IP 地址信息来选择路由的，其连接两个网段时可以有效抑制广播报文的转发，但成本较高。因此人们设想在物理局域网上构建多个逻辑局域网，即 VLAN。

VLAN 将一个物理的 LAN 在逻辑上划分成多个广播域（多个 VLAN）。VLAN 内的主机间可以直接通信，而 VLAN 间不能直接互通。这样，广播报文被限制在一个 VLAN 内，提高了网络安全性。例如，同一个写字楼的不同企业客户，若建立各自独立的 LAN，企

业的网络投资成本将很高；若共用写字楼已有的 LAN，又会导致企业信息安全无法得到保证。而采用 VLAN，可以实现各企业客户共享 LAN 设施，同时又可保证其各自的网络信息安全。

笔记

图 1-1-1 是一个典型的 VLAN 应用组网图。3 台交换机可放置在不同的地点，比如写字楼的不同楼层。每台交换机又分别连接 3 台计算机，分别属于 3 个不同的 VLAN，即一个虚线框内表示一个 VLAN。

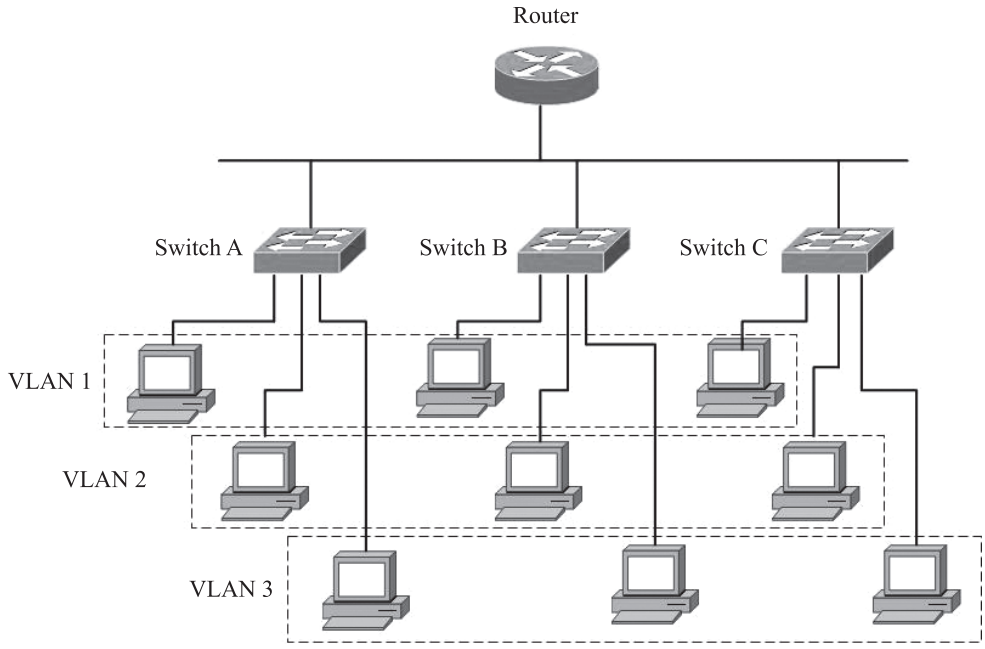
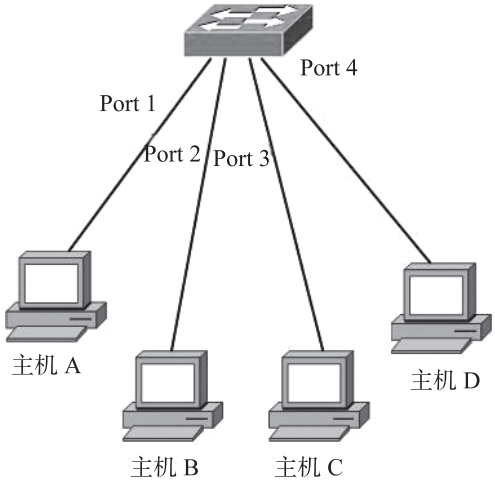


图 1-1-1　典型的 VLAN 应用组网图

子任务 1.1.2 VLAN 的类型

VLAN 的类型也可以理解为 VLAN 划分的方式，下面将逐一介绍。

（1）基于端口划分 VLAN，如图 1-1-2 所示。



VLAN 信息表

VLAN 10	VLAN 20	VLAN 30
Port 1	Port 2 Port 3	Port 4

图 1-1-2　基于端口划分 VLAN

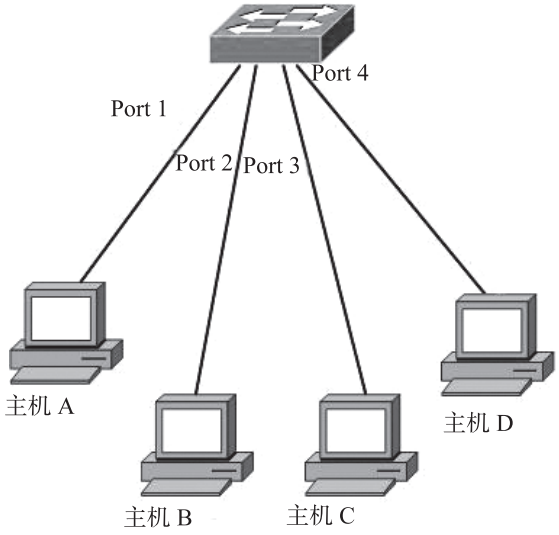
笔记

①原理：根据交换设备的端口编号来划分 VLAN。网络管理员给交换机的每个端口都配置不同的基于端口的 VLAN ID（Port-base VLAN ID，PVID）。当一个数据帧进入交换机端口时，如果没有带 VLAN 标签，且该端口上配置了 PVID，那么，该数据帧就会被打上端口的 PVID。如果进入的帧已经带有 VLAN 标签，那么交换机不会再增加 VLAN 标签，即使端口已经配置了 PVID。对 VLAN 帧的处理由端口类型决定。

②优点：定义成员简单。

③缺点：成员移动需重新配置 VLAN。

（2）基于 MAC 地址划分 VLAN，如图 1-1-3 所示。



VLAN 信息表

VLAN 10	VLAN 20	VLAN 30
主机 A MAC	主机 B MAC 主机 C MAC	主机 D MAC

图 1-1-3　基于 MAC 地址划分 VLAN

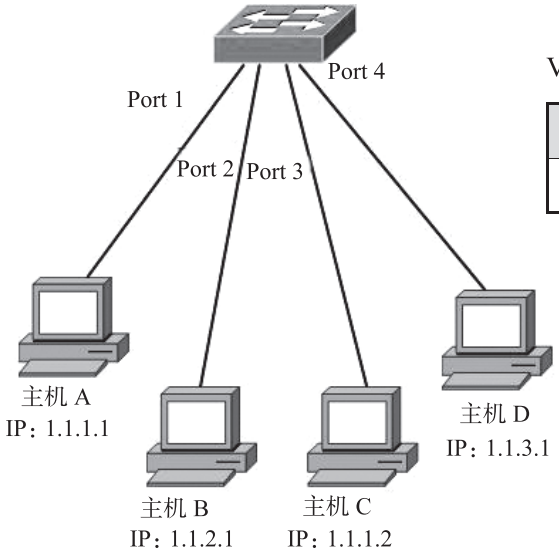
①原理：这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置其属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置。所以，可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN。这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户，配置是比较烦琐的，而且这种划分方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。另外，对于使用笔记本电脑的用户来说，他们的网卡可能会经常更换，这样，VLAN 就必须重新配置。

②优点：当终端用户的物理位置发生改变时，不需要重新配置 VLAN，提高了终端用户的安全性和接入的灵活性。

③缺点：只适用于网卡不经常更换、网络环境较简单的场景。另外，还需要预先定义网络中所有成员。

（3）基于子网划分 VLAN，如图 1-1-4 所示。

笔记



VLAN 信息表

VLAN 10	VLAN 20	VLAN 30
1.1.1.*	1.1.2.*	1.1.3.*

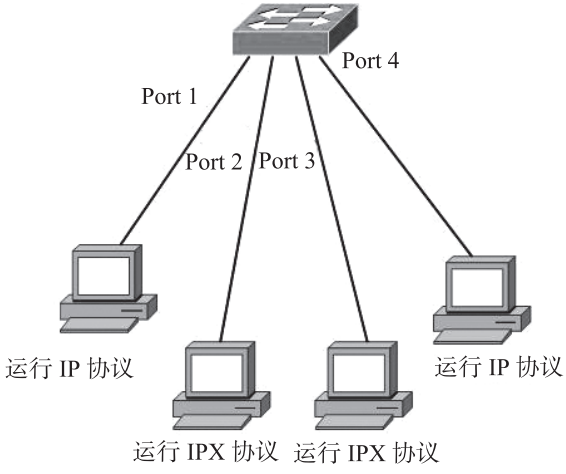
图 1-1-4　基于子网划分 VLAN

①原理：如果交换设备收到的是 untagged（不带 VLAN 标签）帧，交换设备会根据报文中的 IP 地址信息确定添加的 VLAN ID。

②优点：将指定网段或 IP 地址发出的报文在指定的 VLAN 中传输，减轻了网络管理者的任务量，且有利于管理。

③缺点：网络中的用户分布需要有规律，且要求多个用户在同一个网段中。

（4）基于协议划分 VLAN，如图 1-1-5 所示。



VLAN 信息表

VLAN 10	VLAN 20	VLAN 30
IP 协议号 …	IPX 协议号 …	

图 1-1-5　基于协议划分 VLAN

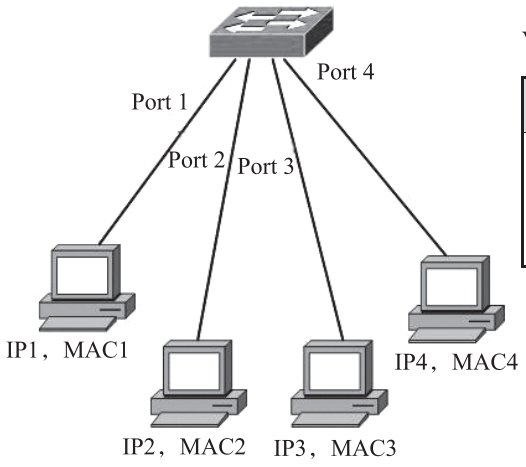
①原理：根据接口接收到的报文所属的协议（族）类型及封装格式来给报文分配不同的 VLAN ID。网络管理员需要配置以太网帧中的协议域和 VLAN ID 的映射关系表，如果收到的是 untagged（不带 VLAN 标签）帧，则依据该表添加 VLAN ID。目前，支持划分 VLAN 的协议有 IPv4、IPv6、IPX、AppleTalk（AT），封装格式有 Ethernet II、802.3 raw、802.2 LLC、802.2 SNAP。

②优点：基于协议划分 VLAN，将网络中提供的服务类型与 VLAN 相绑定，方便管理和维护。

笔记

③缺点：需要对网络中所有的协议类型和 VLAN ID 的映射关系表进行初始配置。

（5）基于匹配策略划分 VLAN，如图 1-1-6 所示。



VLAN 信息表

VLAN 10	VLAN 20	VLAN 30
IP1+MAC1	IP2+MAC2+Port2 IP3+MAC3+Port3 …	IP4+MAC4+Port4 …

图 1-1-6　基于匹配策略划分 VLAN

①原理：基于 MAC 地址、IP 地址、端口组合策略划分 VLAN 是指在交换机上配置终端的 MAC 地址和 IP 地址，并与 VLAN 关联。只有符合条件的终端才能加入到指定的 VLAN 中。符合策略的终端加入到指定的 VLAN 中后，严禁修改 IP 地址或 MAC 地址，否则会导致终端从指定的 VLAN 中退出。

②优点：安全性非常高，基于 MAC 地址和 IP 地址成功划分 VLAN 后，禁止用户改变 IP 地址或 MAC 地址。相较于其他 VLAN 划分方式，基于 MAC 地址和 IP 地址组合策略划分 VLAN 是优先级最高的 VLAN 划分方式。

③缺点：针对每一条策略都需要手工配置。当设备同时支持多种方式时，一般情况下，优先使用顺序为：基于组合策略（优先级别最高）—基于子网—基于协议—基于 MAC 地址—基于端口（优先级别最低）。目前常用的是基于端口的方式。

子任务 1.1.3　VLAN 技术原理

VLAN 技术为了实现转发控制，在待转发的以太网帧中添加 VLAN 标签，然后设定交换机端口对该标签和帧的处理方式。处理方式包括丢弃帧、转发帧、添加标签、移除标签等，VLAN 通信基本原理如图 1-1-7 所示。

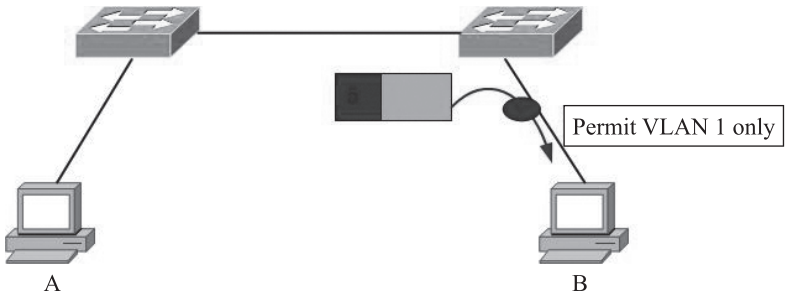


图 1-1-7　VLAN 通信基本原理

转发帧时，先检查以太网报文中携带的 VLAN 标签是否为该端口允许通过的标签，判断该以太网帧是否能够从端口转发。然后将 A 发出的所有以太网帧都加上标签 5，此后查询二层转发表，根据目的 MAC 地址将该帧转发到 B 连接的端口，由于在该端口配置了仅允许 VLAN 1 通过，所以 A 发出的帧将被丢弃。这就意味着支持 VLAN 技术的交换机转发以太网帧时不再仅仅依据目的 MAC 地址，同时还要考虑该端口的 VLAN 配置情况，从而实现对二层转发的控制。

接下来，对 VLAN 通信原理进行介绍。

1. VLAN 帧格式

IEEE 802.1Q 标准对 Ethernet 帧格式进行了修改，在源 MAC 地址字段和协议类型字段之间加入 4 B 的 802.1Q Tag，基于 802.1Q 的 VLAN 帧格式如图 1-1-8 所示。

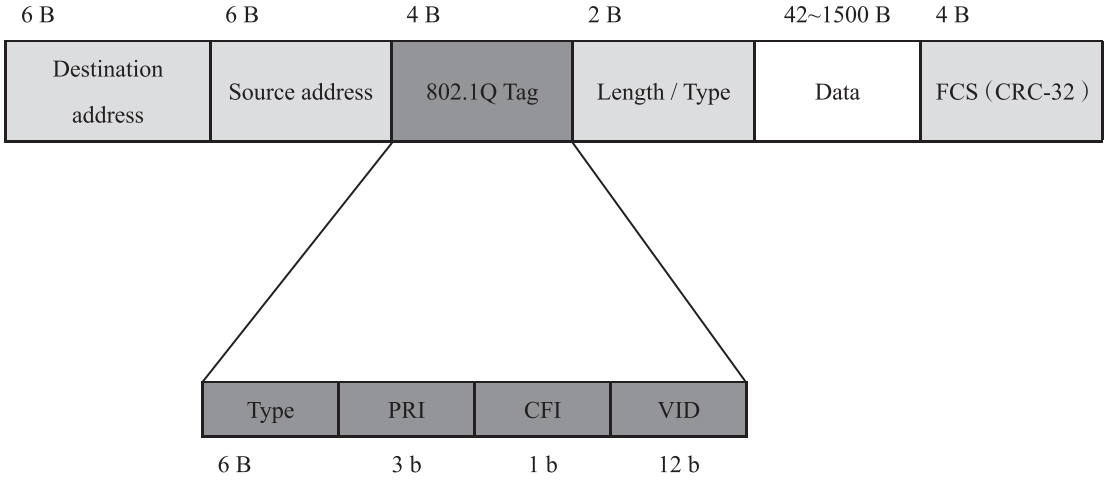


图 1-1-8　基于 802.1Q 的 VLAN 帧格式

802.1Q Tag 包含以下 4 个字段，含义如下：

（1）Type：长度为 2 B，表示帧类型。取值为 0x8100 时表示 802.1Q Tag 帧。如果不支持 802.1Q 的设备收到这样的帧，会将其丢弃。

（2）PRI：Priority，长度为 3 b，表示帧的优先级，取值范围为 0~7，值越大优先级越高。用于当交换机阻塞时，优先发送优先级高的数据帧。

（3）CFI：Canonical Format Indicator，长度为 1 b，表示 MAC 地址是否是经典格式。CFI 为 0 说明是经典格式，CFI 为 1 表示为非经典格式。用于区分以太网帧、FDDI（Fiber Distributed Digital Interface）帧和令牌环网帧。在以太网中，CFI 的值为 0。

（4）VID：VLAN ID，长度为 12 b，表示该帧所属的 VLAN。可配置的 VLAN ID 取值范围为 0~4 095，但是协议中规定 0 和 4 095 为保留的 VLAN ID，不能供用户使用。

使用 VLAN 标签后，在交换网络环境中，以太网的帧有以下两种格式：

（1）没有加上这 4 B 标识的，称为标准以太网帧（untagged frame）。

（2）加上 4 B 标识的，称为带有 VLAN 标记的帧（tagged frame）。

笔记

提示

本教材仅仅讨论 VLAN 标签中的 VLAN ID，对于其他字段暂不做研究。

笔记

2. VLAN 的转发流程

VLAN 技术通过以太网帧中的标签，结合交换机端口的 VLAN 配置，实现对报文转发的控制。假设交换机有两个端口 A 与 B，从某端口 A 收到以太网帧，如果转发表显示目的 MAC 地址存在于 B 端口下。引入 VLAN 后，该帧是否能从 B 端口转发出去，取决于以下两点。

（1）该帧携带的 VLAN ID 是否被交换机创建。创建 VLAN 的方法有两种，管理员逐个添加或通过 GVRP（GARP VLAN Registration Protocol）协议自动生成。

（2）目的端口是否允许携带该 VLAN ID 的帧通过。端口允许通过的 VLAN 列表可以由管理员添加或使用 GVRP 协议动态注册，VLAN 转发流程如图 1-1-9 所示。

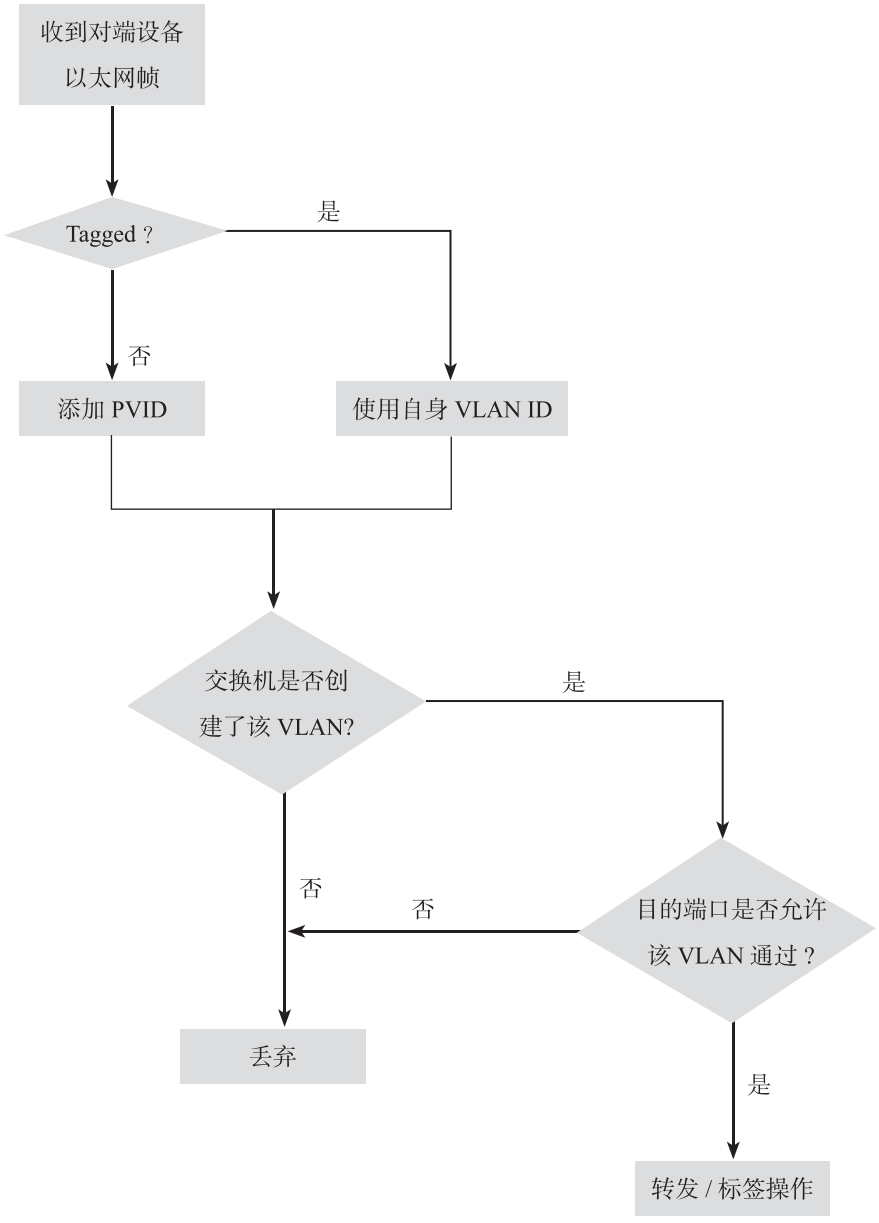


图 1-1-9　VLAN 转发流程

转发过程中，标签操作类型有以下两种：

（1）添加标签：对于 untagged frame，添加 PVID，在端口收到对端设备的帧后进行。

（2）移除标签：删除帧中的 VLAN 信息，以 untagged frame 的形式发送给对端设备。

子任务 1.1.4 VLAN 接口类型

为了提高处理效率，交换机内部的数据帧都带有 VLAN Tag，以方便统一处理。当一个数据帧进入交换机端口时，如果没有带 VLAN Tag，且该端口上配置了 PVID，那么，该数据帧就会被标记上端口的 PVID。如果数据帧已经带有 VLAN Tag，那么，即使端口已经配置了 PVID，交换机也不会再给数据帧标记 VLAN Tag。

由于端口类型不同，交换机对帧的处理过程也不同。接下来根据不同的端口类型分别介绍。

1. Access 端口

Access 端口一般用于连接主机，对于帧的处理如下。

（1）对接收不带 Tag 的报文处理：接收该报文，并打上默认 VLAN 的 Tag。

（2）对接收带 Tag 的报文处理：当 VLAN ID 与默认 VLAN ID 相同时，接收该报文；当 VLAN ID 与默认 VLAN ID 不同时，丢弃该报文。

（3）发送帧处理过程：先剥离帧的 PVID Tag，然后再发送。

2. Trunk 端口

Trunk 端口用于连接交换机，在交换机之间传递 Tagged Frame，可以自由设定允许通过多个 VLAN ID，这些 ID 可以与 PVID 相同，也可以不同。其对于帧的处理过程如下。

（1）对接收不带 Tag 的报文处理：打上默认的 VLAN ID，当默认 VLAN ID 在允许通过的 VLAN ID 列表中时，接收该报文，打上默认的 VLAN ID ；当默认 VLAN ID 不在允许通过的 VLAN ID 列表中时，丢弃该报文。

（2）对接收带 Tag 的报文处理：当 VLAN ID 在接口允许通过的 VLAN ID 列表中时，接收该报文；当 VLAN ID 不在接口允许通过的 VLAN ID 列表中时，丢弃该报文。

（3）发送帧处理过程：当 VLAN ID 与默认 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 与默认 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。

3. Hybrid 端口

Access 端口发往其他设备的报文都是 untagged frame，而 Ttrunk 端口仅在一种特定情况下才能发出 untagged frame，其他情况发出的都是 tagged frame。某些应用中，可能希望能够灵活地控制 VLAN 标签的移除。例如，在本交换机的上行设备不支持 VLAN 的情况下，希望实现各个用户端口的相互隔离。而 Hybrid 端口可以解决此问题。

（1）对接收不带 Tag 的报文处理：同 Trunk 端口。

（2）对接收带 Tag 的报文处理：同 Trunk 端口。

提示

正常情况下，交换机不会更改 tagged frame 中的 VLAN ID 的值。但某些设备支持特殊业务，可能提供更改 VLAN ID 的功能，此内容不在本教材讨论的范围之内。

笔记

（3）发送帧处理过程：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。

端口类型对比如表 1-1-1 所示。

表 1-1-1　端口类型对比

<table>
<tr><th rowspan="2">端口类型</th><th colspan="2">接收帧（IN）</th><th colspan="2" rowspan="2">发送帧（OUT）</th></tr>
<tr><th>不带有 Tag</th><th>带有 Tag</th></tr>
<tr><td>Access</td><td>打上本端口 PVID 后，接收</td><td>检查该帧所携带的 VID 是否与端口 PVID 相同
是：接收
否：丢弃</td><td colspan="2">剥离 Tag 后，发送</td></tr>
<tr><td rowspan="2">Trunk</td><td rowspan="2">打上端口 PVID，并检查该 PVID 是否为端口允许的 VLAN ID
是：接收
否：丢弃</td><td rowspan="2">检查该帧所携带的 VID 是否为端口允许的 VLAN ID
是：接收
否：丢弃</td><td colspan="2">检查该帧所携带的 VID 是否为接口允许的 VLAN ID</td></tr>
<tr><td>否：丢弃</td><td>是则检查该帧所携带的 VID 是否与接口 PVID 相同
是：剥离 Tag 后，发送
否：发送</td></tr>
<tr><td rowspan="2">Hybird</td><td rowspan="2">同 Trunk</td><td rowspan="2">同 Trunk</td><td colspan="2">检查该帧所携带的 VID 是否为接口允许的 VLAN ID</td></tr>
<tr><td>否：丢弃</td><td>是则检查是否配置剥离 Tag
是：剥离 Tag 后，发送
否：发送</td></tr>
<tr><td>备注</td><td colspan="4">对于端口允许的 VLAN ID 的配置
Trunk：port trunk allow-pass vlan {{vlan-id1 [to vlan-id2]}&<1-10>|all}
匹配以上 VID 的帧将被允许通过该端口
Hybird：port hybrid untagged vlan {{vlan-id1 [to vlan-id2]}&<1-10>|all}
匹配以上 VID 的帧将被允许通过该端口，且发送时剥离 Tag
port hybrid tagged vlan {{vlan-id1 [to vlan-id2]}&<1-10>|all}
匹配以上 VID 的帧将被允许通过该端口，且发送时保留 Tag
默认情况下，只有 VLAN 1 被允许，若端口为 Hybird，则属性为 untagged</td></tr>
</table>

在介绍完端口类型后，还需要说明的是，VLAN 内的链路分为接入链路（Access Link，一般为连接用户主机和交换机的链路）与干道链路（Trunk Link，一般为连接交换机和交换机的链路），链路类型如图 1-1-10 所示。对于上述各端口类型，Access 端口只能连接接入链路，Trunk 端口只能连接干道链路，Hybrid 端口既可以连接接入链路，又可以连接干道链路。

笔记

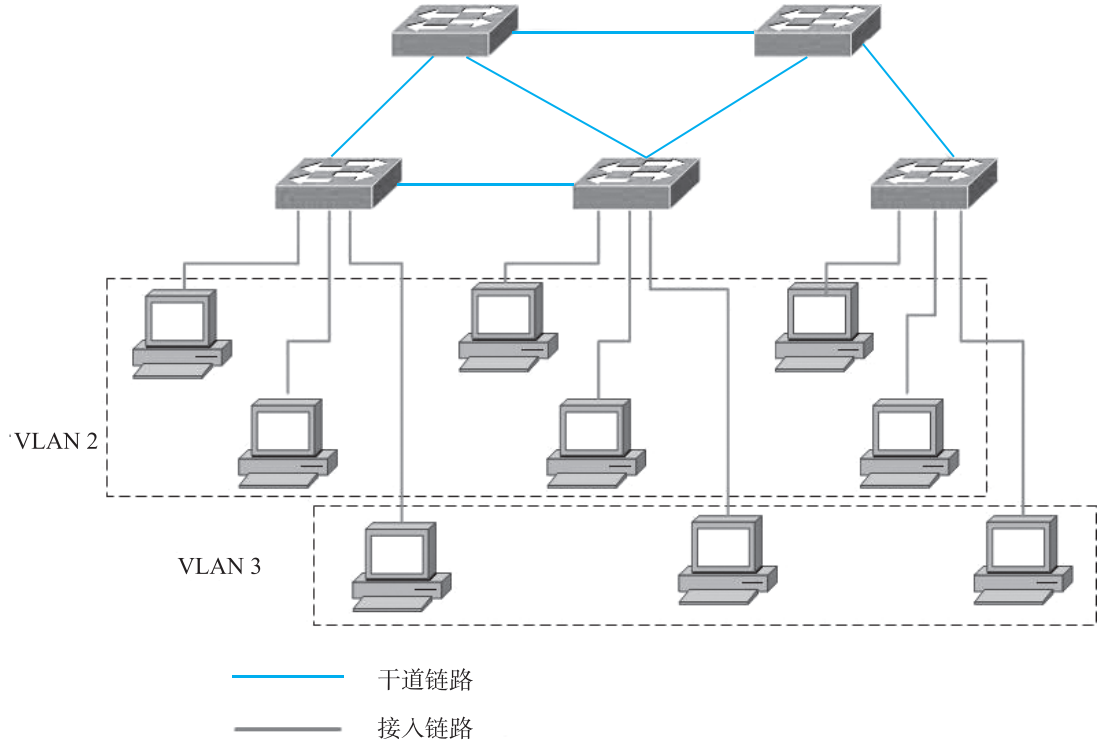


图 1-1-10　链路类型

子任务 1.1.5 VLAN 的基本配置

基于端口划分 VLAN 是最简单、最有效，也是最常见的划分方式。VLAN 常用命令及其作用如表 1-1-2 所示。

表 1-1-2　VLAN 常用命令及其作用

常用命令	视图	作用
vlan vlan-id VLAN ID 的范围 1~4 096	系统	创建 VLAN，进入 VLAN 视图
vlan batch {vlan-id1 [to vlan-id2]} &<1-10>	系统	批量创建 VLAN
interface interface-type interface-number	系统	进入指定接口
port link-type {access | hybrid | trunk | dot1q-tunnel}	系统	配置 VLAN 端口属性
port default vlan vlan-id	接口	将 Access 端口加入到指定的 VLAN 中
port interface-type {interface-number1 [to interface-number2]} &<1-10>	VLAN	批量将 Access 端口加入到指定的 VLAN 中
port trunk allow-pass vlan {{vlan-id1 [to vlan-id2]}&<1-10>|all}	接口	配置允许通过该 Trunk 接口的帧
port trunk pvid vlan vlan-id	接口	配置 Trunk 接口默认 VLAN ID

笔记

续表

常用命令	视图	作用
port hybrid untagged vlan {{vlan-id1 [to vlan-id2]}&<1-10>|all}	接口	指定发送时剥离 Tag 的帧
port hybrid tagged vlan {{vlan-id1 [to vlan-id2]}&<1-10>|all}	接口	指定发送时保留 Tag 的帧
undo port hybrid vlan {{vlan-id1 [to vlan-id2]}&<1-10>|all}	接口	移除原先允许通过该 Hybird 接口的帧
port hybrid pvid vlan vlan-id	接口	配置 Hybrid 端口默认 VLAN ID
display vlan [vlan-id [verbose]]	所有	查看 VLAN 相关信息
display interface [interface-type [interface-number]]	所有	查看接口信息
display port vlan [interface-type [interface-number]]	所有	查看基于端口划分 VLAN 的相关信息
display this	所有	查看该视图下相关配置

子任务 1.1.6 任务实施

1. 组网需求

如图 1-1-11 所示，SWA 的端口 E0/0/24 与 SWB 的端口 E0/0/24 相连。

SWA 的两个下行端口分别加入 VLAN 10 和 VLAN 20。

SWB 的一个下行接口加入 VLAN 10。

要求 VLAN 10 内的 PC 能够互相访问，VLAN 10 与 VLAN 20 内的 PC 不能够互相访问。

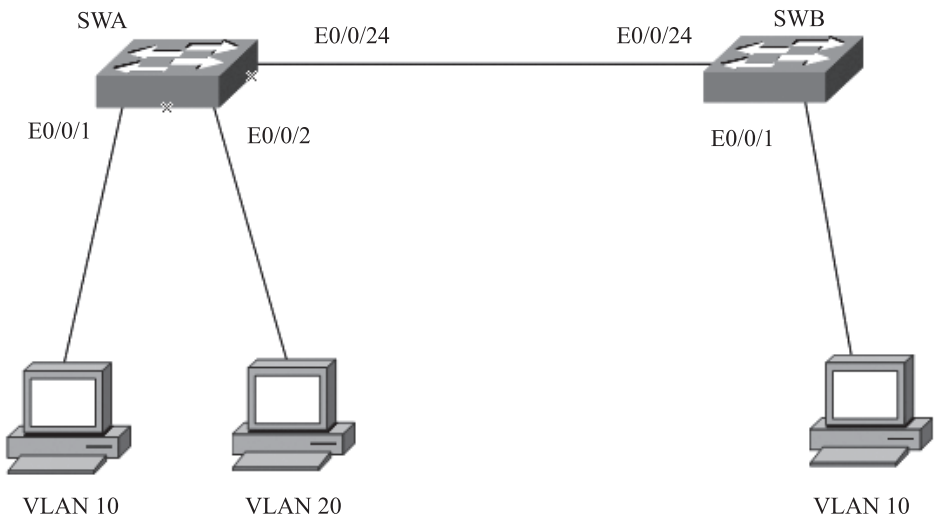


图 1-1-11　配置拓扑图

笔记

2. 配置思路

创建 VLAN，规划员工所属的 VLAN。

配置端口属性，确定设备连接对象。

关联端口和 VLAN。

3. 数据准备

为完成此配置实验，需准备如下的数据：

SWA 的端口 E0/0/1 属于 VLAN 10，E0/0/2 属于 VLAN 20，E0/0/24 为 Trunk，允许 VLAN 10、VLAN 20 通过。

SWB 的端口 E0/0/1 属于 VLAN 10，E0/0/24 为 Trunk，允许 VLAN 10、VLAN 20 通过。

4. 操作步骤

（1）配置 SWA。

```
# 创建 VLAN 10、VLAN 20
[SWA]vlan batch 10 20
# 配置端口属性
[SWA]interface Ethernet 0/0/1
[SWA-Ethernet0/0/1]port link-type access
[SWA-Ethernet0/0/1]port default vlan 10
[SWA-Ethernet0/0/1]quit
[SWA]interface Ethernet 0/0/2
[SWA-Ethernet0/0/2]port link-type access
[SWA-Ethernet0/0/2]port default vlan 20
[SWA-Ethernet0/0/2]quit
[SWA]interface Ethernet 0/0/24
[SWA-Ethernet0/0/24]port link-type trunk
[SWA-Ethernet0/0/24]port trunk allow-pass vlan 10 20
```

（2）配置 SWB。

配置过程类似 SWA，此处不再详述。

5. 验证配置结果

各个 PC 配置 IP 地址在同一网段即可。VLAN 10 内的 PC 可以互相 Ping 通，而 VLAN 10 与 VLAN 20 的 PC 不可以 Ping 通。

任务总结

通过本任务的实施，应掌握下列知识和技能：

（1）了解 VLAN 原理基础的概念和功能。

（2）了解 VLAN 原理基础的发展历程。

笔记

深入思考

（1）VLAN 的作用是什么？

（2）VLAN 划分的方式有哪些？

（3）VLAN 的端口类型有哪些？

任务 1.2 VLAN 路由技术应用

子任务 1.2.1 VLAN 间通信问题

通过划分 VLAN，可以隔离广播域，增强了安全性。但是，划分 VLAN 后，不同 VLAN 计算机之间的通信也相应地被阻止，VLAN 间通信问题如图 1-2-1 所示。这样一来，则背离了网络互联互通的原则。因此，我们迫切地需要一些技术与方法来解决 VLAN 间数据的通信。

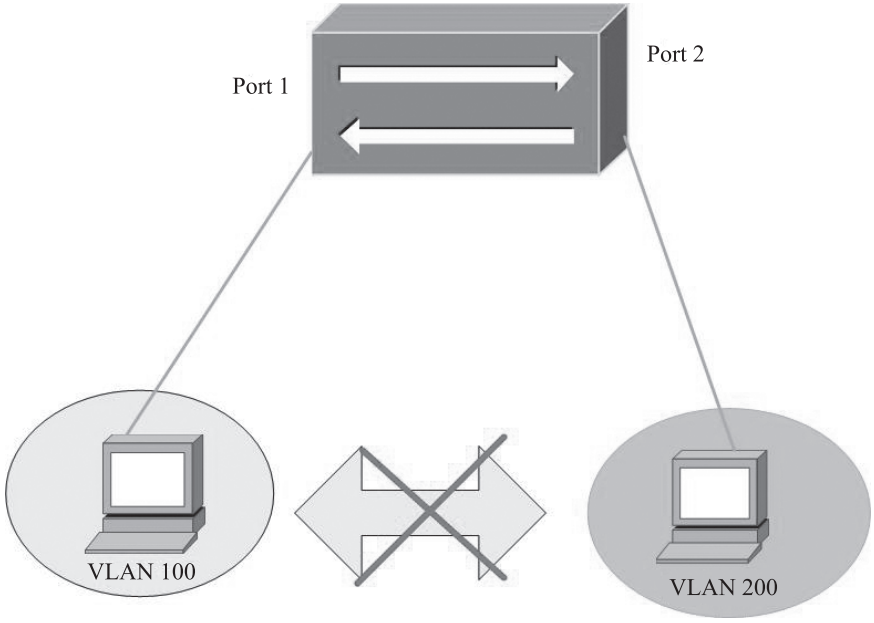


图 1-2-1 VLAN 间通信问题

一个 VLAN 就是一个广播域、局域网。由此可见，VLAN 间的通信就相当于不同网络之间的通信。所以，为了实现 VLAN 间的通信，必须借助于三层设备。VLAN 间的通信问题实质就是 VLAN 间的路由问题。

子任务 1.2.2 VLAN 间通信的解决方式

为了实现 VLAN 间的通信，通常可采用以下三种方式：

（1）每个 VLAN 一个物理连接。

（2）单臂路由。

（3）三层交换。

笔记

1. 每个 VLAN 一个物理连接

每个 VLAN 一个物理连接，就是为每个 VLAN 分配单独的路由器接口，如图 1-2-2 所示。每个物理接口就是对应 VLAN 的网关，VLAN 间的数据通信通过路由器进行三层路由，这样就可以实现 VLAN 之间相互通信。

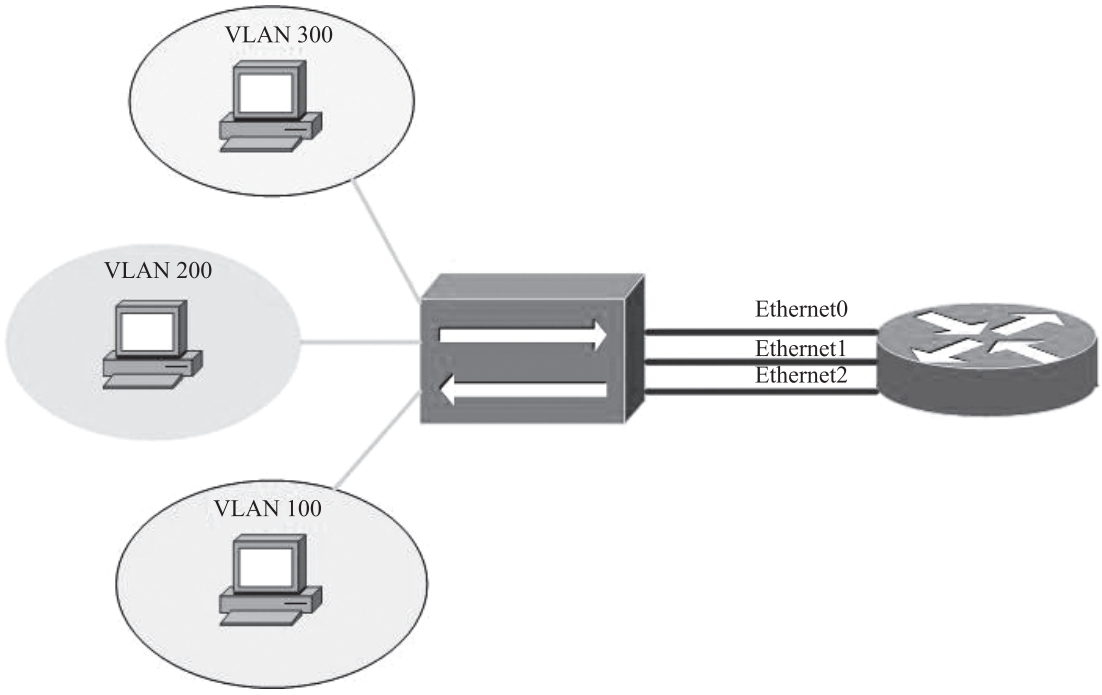


图 1-2-2　为每个 VLAN 分配单独的路由器接口

但是，随着每个交换机上 VLAN 数量的增加，按照上述 VLAN 间路由的实现方式必然需要大量的路由器接口。出于成本的考虑，一般不用这种方案来解决 VLAN 间路由选路问题。此外，某些 VLAN 之间可能不需要经常进行通信，这样会导致路由器的接口未被充分利用。

2. 单臂路由

为了解决物理接口需求过大的问题，在 VLAN 技术的发展中，出现了一种名为单臂路由的技术，用于实现 VLAN 间的通信。即通过在路由器的一个接口上配置子接口（或“逻辑接口”，并不存在真正物理接口）的方式，实现原来相互隔离的不同 VLAN 之间的互联互通。

单臂路由技术实现方式，如图 1-2-3 所示，路由器仅仅提供一个以太网接口，而在该接口下提供 3 个子接口分别作为 3 个 VLAN 用户的默认网关。当 VLAN 100 的用户需要与其他 VLAN 的用户进行通信时，该用户只需将数据包发送给默认网关，默认网关修改数据帧的 VLAN 标签后再发送至目的主机所在的 VLAN 中，即可完成 VLAN 间的通信。

笔记

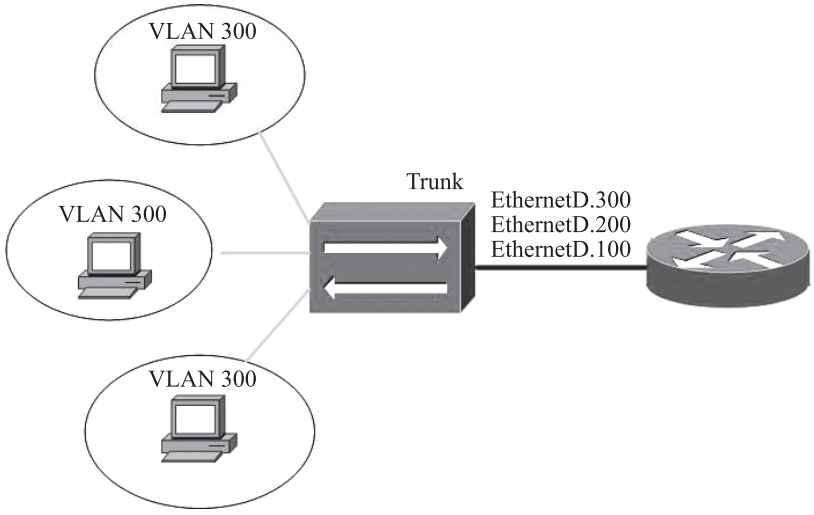


图 1-2-3　单臂路由技术实现方式

但是，这种方式也有很大的问题，当 VLAN 间的数据流量过大时，路由器与交换机之间的链路将成为网络的瓶颈。

3. 三层交换

三层交换技术就是二层交换技术 + 三层转发技术。它打破了局域网中网段划分之后，网段中的子网必须依赖路由器进行管理的局面，解决了传统路由器低速与复杂所造成的网络瓶颈问题。

在实际网络搭建中，三层交换技术成为解决 VLAN 间通信的首选方式，三层交换技术实现方式如图 1-2-4 所示。

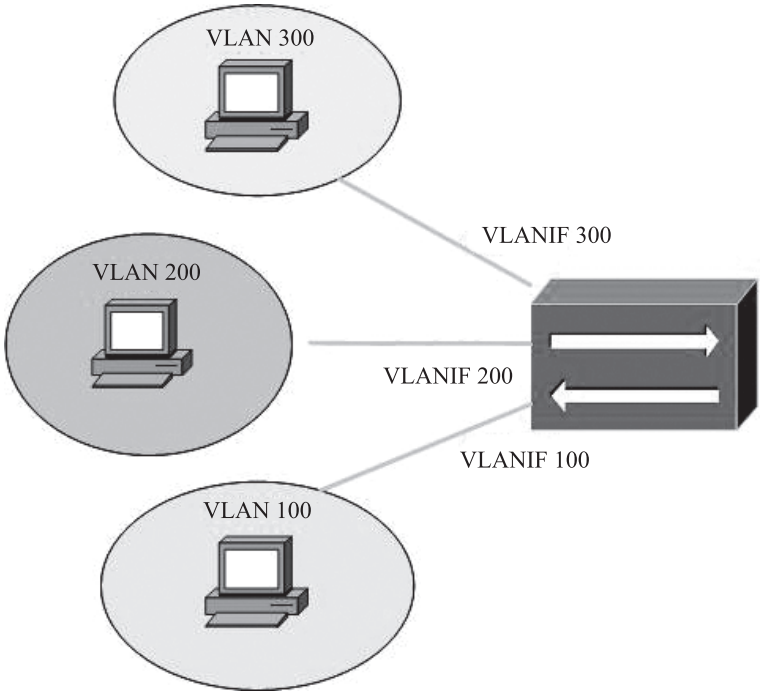


图 1-2-4　三层交换技术实现方式

三层交换机基本工作原理：三层交换机通过路由表传输第一个数据流后，会产生一个

MAC 地址与 IP 地址的映射表。当同样的数据流再次通过时，将根据此表直接从二层通过，而不是通过三层，从而消除了路由器进行路由选择而造成的网络延迟，提高了数据包转发效率。也称之为一次路由，多次交换。另外，为了保证第一次数据流通过路由表正常转发，路由表中必须有正确的路由表项。因此必须在三层交换机上部署三层接口，并部署路由协议，实现三层路由可达。VLANIF 接口也由此而产生，该接口为逻辑接口。

笔记

子任务 1.2.3　VLAN 间通信的基本配置

VLAN 间通信常用配置命令及其作用如表 1-2-1 所示。

表 1-2-1　VLAN 间通信常用配置命令及其作用

常用命令	视图	作用
interface interface-type interface-number	系统	进入指定接口
ip address ip-address {mask|mask-length} [sub]	接口	配置接口 IP 地址
control-vid vid { dot1q-termination | qinq-termination }	子接口	指定子接口控制 VLAN ID，用于标识不同子接口
dot1q termination vid vid	子接口	配置子接口对一层 Tag 报文的终结功能。必须结合 control-vid 命令使用
display ip interface [brief] [interface-type interface-number]	所有	查看接口与 IP 相关的配置和统计信息或者简要信息
display ip routing-table	所有	查看路由表

子任务 1.2.4　任务实施

1. 通过配置以太网子接口实现 VLAN 间的通信

（1）组网需求。

单臂路由配置拓扑如图 1-2-5 所示，RTA 的接口 Eth1/0/0 与 SWA 上行口相连（Eth 也可以用 E 或 Ethernet 表示）。

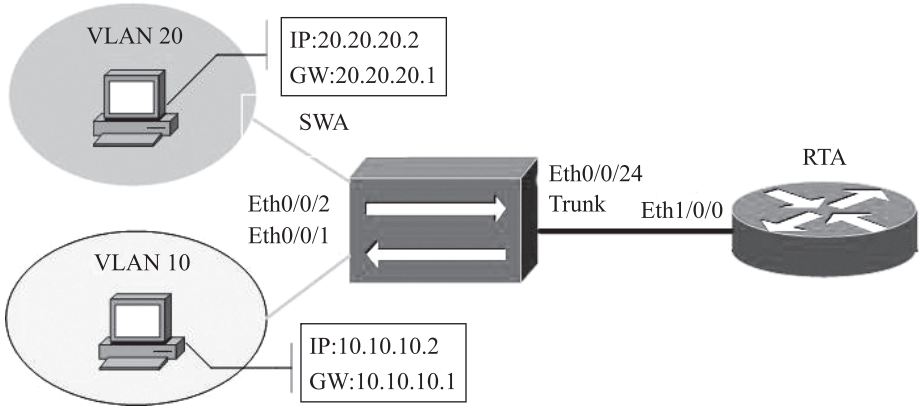


图 1-2-5　单臂路由配置拓扑

笔记

SWA 的两个下行接口分别加入 VLAN 10 和 VLAN 20。

要求 VLAN 10 内的 PC 与 VLAN 20 内的 PC 能够互相访问。

（2）配置思路。

启用路由器接口的子接口。

配置各子接口的封装方式均采用 802.1Q。

配置各子接口所属的 VLAN ID。

配置各子接口的 IP 地址。

（3）数据准备。

为完成此配置实验，需准备如下的数据：

以太网子接口 Eth1/0/0.1 和 Eth1/0/0.2 的 VLAN ID 为 10 和 20。

以太网子接口 Eth1/0/0.1 和 Eth1/0/0.2 的 IP 地址为 10.10.10.1 和 20.20.20.1。

SWA 上行接口设置为 Trunk。

SWA 下行接口分别加入 VLAN 10 与 VLAN 20。

（4）操作步骤。

配置好交换机和 PC 后完成下面子接口的配置。

①配置 RTA 上对应 VLAN 10 的子接口。

```
# 创建并配置以太网子接口 Eth1/0/0.1
[RTA] interface ethernet 1/0/0.1
[RTA-Ethernet1/0/0.1]control-vid 100 dot1q-termination
[RTA-Ethernet1/0/0.1]dot1q termination vid 10
[RTA-Ethernet1/0/0.1]ip address 10.10.10.1 24
[RTA-Ethernet1/0/0.1]quit
```

②配置 RTA 上对应 VLAN 20 的子接口。

```
# 创建并配置以太网子接口 Eth1/0/0.2
[RTA] interface ethernet 1/0/1.1
[RTA-Ethernet1/0/0.2]control-vid 200 dot1q-termination
[RTA-Ethernet1/0/0.2]dot1q termination vid 20
[RTA-Ethernet1/0/0.2]ip address 20.20.20.1 24
[RTA-Ethernet1/0/0.2]quit
```

（5）检查配置结果。

在 VLAN 10 中的 PC 上配置默认网关为 Eth1/0/0.1 接口的 IP 地址 10.10.10.1/24。

在 VLAN 20 中的 PC 上配置默认网关为 Eth1/0/0.2 接口的 IP 地址 20.20.20.1/24。

配置完成后，VLAN 10 内的 PC 1 与 VLAN 20 内的 PC 2 能够互相访问。

2. 通过配置三层交换机实现不同 VLAN 间的通信

（1）组网需求。

配置三层交换机 VLAN 间的通信如图 1-2-6 所示，SWA 的接口 E0/0/1 与 E0/0/2 分别

与两台 PC 相连。

SWA 的下行接口 Eth0/0/1 加入 VLAN 10，下行接口 Eth0/0/2 加入 VLAN 20。

要求 VLAN 10 内的 PC 与 VLAN 20 内的 PC 能够互相 Ping 通。

笔记

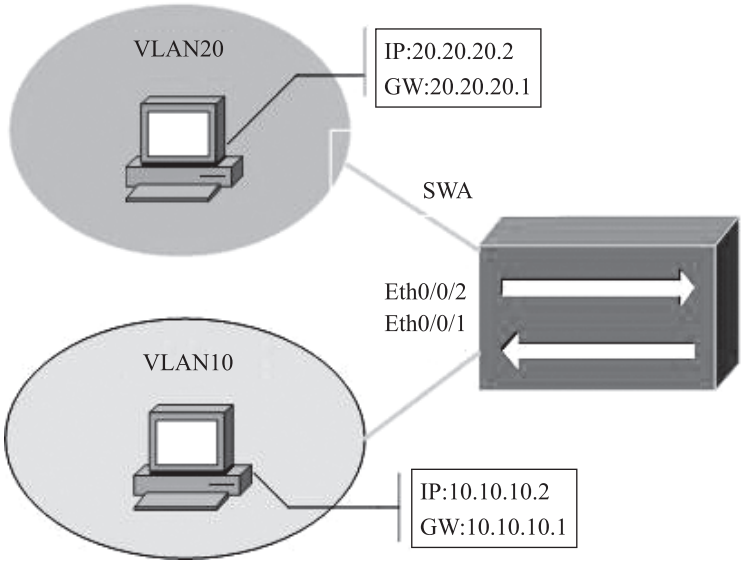


图 1-2-6　配置三层交换机 VLAN 间的通信

（2）配置思路。

启用 VLANIF 接口。

配置 VLANIF 接口 IP 地址。

（3）数据准备。

为完成此配置实验，需准备如下的数据：

在 SWA 上配置接口 Eth0/0/1 加入 VLAN 10。

在 SWA 上配置接口 Eth0/0/2 加入 VLAN 20。

在 SWA 上配置 VLANIF 10 的 IP 地址为 10.10.10.1/24。

在 SWA 上配置 VLANIF 20 的 IP 地址为 20.20.20.1/24。

（4）操作步骤。

```
# 创建 VLAN
[Router]vlan batch 10 20
# 配置接口加入 VLAN
配置略
# 配置 VLANIF 接口的 IP 地址
[SWA]interface vlanif 10
[SWA-Vlanif10]ip address 10.10.10.1 24
[SWA-Vlanif10]quit
[SWA]interface vlanif 20
[SWA-Vlanif20]ip address 20.20.20.1 24
[SWA-Vlanif20]quit
```