# 第 3 章　交换机与虚拟局域网

## 3.1　学习目标

以太网已经变得越来越拥塞，主要是由于网络应用和网络用户的需求迅速增长。现在处于同一个以太网上的两个站点很容易就会使网络不堪重负。为了提高局域网的效率，交换技术就产生了。本章主要围绕交换技术来介绍交换机、交换式局域网以及虚拟局域网的知识。

- 掌握计算机与交换机的连接
- Console 端口的配置
- 掌握查看 MAC/端口映射表的方法
- 掌握建立和维护“端口/MAC 地址映射表”的原理
- 掌握“交换”局域网的特点
- 选择交换局域网的网络设备
- 掌握如何组建交换式局域网
- 掌握虚拟局域网的特点
- 掌握单个交换机的 VLAN 划分
- 掌握跨交换机的 VLAN 划分



## 3.2　交换机

### 3.2.1　基本知识

**1.交换机**

交换机是局域网中使用非常广泛的网络设备，它工作在数据链路层，属于数据链路层的交换设备。交换机的分类方法比较多，根据交换机所应用的局域网类型不同，可将交换机分为 10 Mb/s 以太网交换机、100 Mb/s 快速交换机、千兆交换机等。交换机如图 3.1 所示。

图 3.1　交换机

**2.交换机的工作原理**

典型的交换机就是以太网交换机。交换机是可以通过端口与端口之间的多个并发连接,实现多节点之间数据的并发传输。这种数据传输方式与集线器那种共享带宽的方式完全不同。在 2.3.3 节中,讲过 MAC 地址这部分知识。在交换机里存在一个“端口 MAC 地址映射表”,在这个表中,每个 MAC 地址都对应于交换机的一个唯一的端口。对应于图 3.2,交换机中的“端口 MAC 地址映射表”如表 3.1 所示。

表 3.1　　MAC 地址映射表

| MAC 地址 | 端口号 | 计时 |
|---|---|---|
| 01-13-AF-45-6E-7D （节点 A） | 3 | … |
| 01-13-AF-AC-1D-83（节点 B） | 4 | … |
| 12-3E-42-8D-91-28 （节点 C） | 4 | … |
| 12-3E-42-4C-7A-79 （节点 D） | 1 | … |
| 34-56-89-2A-4E-7F （节点 E） | 2 | … |
| …… | ….. | … |

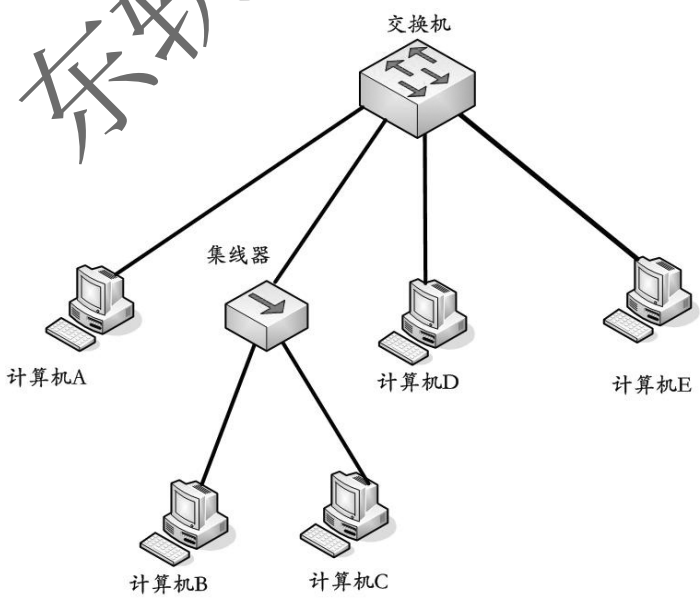


图 3.2　交换机连接的网络

如图 3.2，计算机 B、C 是通过集线器连接到交换机，而计算机 A、D 和 E 是直接连在交换机。根据表 3.1 和图 3.2，可以将计算机和端口的图描绘出来，如图 3.3 所示。

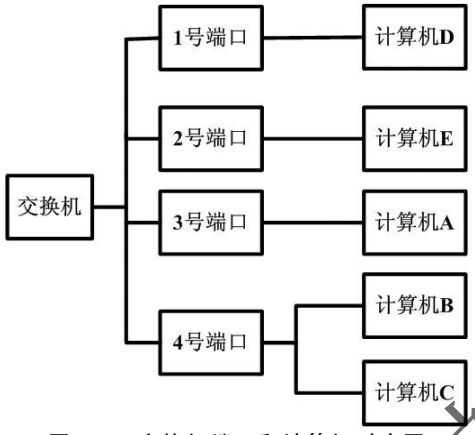


**图 3.3　交换机端口和计算机对应图**

如果计算机 D 要发送信息给计算机 E。计算机 D 首先将目的 MAC 地址指向计算机 E 的帧发往交换机。交换机接收该帧，并且检测到了目的 MAC 地址后，在交换机的“端口/MAC 地址表”中查找计算机 E 的端口号，即 2 号端口。这样，源主机 D(1 号端口)和目的主机 E(2 号端口)都已经确定，数据包的传送路径也只需要从 1 号端口通过交换机直接转发给 2 号端口。

如果同时计算机 A 要给计算机 B 发送信息，交换机的 3 号端口与 4 号端口也将建立一条连接，并将 3 号端口接收到的信息转发到 4 号端口。

这样，交换机在 1 号端口至 2 号端口和 3 号端口至 4 号端口之间就建立了两条并发的连接。计算机 A 和计算机 D 可以同时发送信息，计算机 B 和计算机 C 因为接在集线器连接的共享式以太网中，所以同时会收到计算机 A(3 号端口)的数据包。同样的，根据共享式以太网的原理，通过对目的 MAC 地址的识别，计算机 C 会抛弃掉数据包，计算机 B 留下数据包，数据传送完毕。

由此可以看出，交换机是利用这些并发连接，对接收到的数据信息进行转发和交换。

**3.交换机的功能**

(1)地址学习

以太网交换机利用“端口/MAC 地址映射表”进行信息的交换，因此“端口/MAC 地址映射表”的建立和维护就变得非常重要，因为一旦“端口/MAC 地址映射表”出现错误，就可能造成信息转发错误。那么“端口/MAC 地址映射表”是如何建立和维护的呢？

这里需要解决的问题一共有两个，一个是交换机如何知道哪台计算机连接到哪个端口；二是当计算机在交换机的端口之间移动时，交换机如何维护地址映射表。如果通过人工建立交换机的“端口/MAC 地址映射表”是非常不现实的，因为端口连接计算机的情况是经常改变的。因此，交换机应该自动建立“端口/MAC 地址映射表”。换句话来说，交换机应该动态建立和维护“端口/MAC 地址映射表”，我们将这种维护“端口/MAC 地址映射表”的方式称为“地址学习”。

“地址学习”具体是通过读取数据包的源地址和数据包进入交换机的哪一个端口，将源

地址和端口一一记录到交换机的“端口/MAC 地址映射表”，这样就建立了端口与 MAC 地址的对应关系。当得到对应关系后，交换机将检查地址映射表中是否已经存在该对应关系。如果不存在，就添加到“端口/MAC 地址映射表”，如果存在，就对该表项更新。

例如在图 3.2 中，假设“端口/MAC 地址映射表”中没有计算机 E 的 MAC 地址与交换机的端口对应关系。那么计算机 A 要向计算机 E 发送数据包，而交换机在 3 号端口接收到数据包之后，发现目的 MAC 地址(计算机 E)在“端口/MAC 地址映射表”中查询不到。为了保证数据包能够到达正确的目的地，交换机会向除了源端口(3 号端口)之外的所有端口发送这个数据包。当然，大家都知道，网络传输永远是双向的，当计算机 E 给计算机 A 发送回应数据包的时候，交换机就会捕捉到计算机 E 的 MAC 地址与端口的对应关系，就将这个对应关系存储到“端口/MAC 地址映射表”。

假设计算机 E 的端口发生改变，由 2 号端口换到了 5 号端口。则计算机 D 要给计算机 E 发送信息的时候，通过“端口/MAC 地址映射表”，将数据包发送到了 5 号端口，而却收不到 2 号端口的回应数据包，则证明此次数据传输失败。因此，计算机 D 重新发送数据包给交换机的所有端口，而计算机 D 在收到这个数据包并通过交换机 5 号端口回应数据包的时候，交换机将计算机 D 的 MAC 地址与 5 号端口的对应关系更新到交换机的“端口/MAC 地址映射表”。

在每次添加或更新地址映射表时，这个过程会增加一个计时器。所以，每个“端口/MAC 地址映射表”的映射表项在计时器的范围内，会存储在交换机中。如果在计时器溢出之前都没有再次学习到这个“端口/MAC 地址映射表”表项，则视为这个映射表项已经过期，交换机将其删除。这样，交换机就能维护一个实时更新的“端口/MAC 地址映射表”。

(2)通信过滤

交换机的“端口/MAC 地址映射表”建立之后，它就可以对通过的信息进行过滤了。这个“通信过滤”的过程，可以做以下详细描述。如图 3.4 所示，计算机 A 和 B 以及计算机 D 和 E 都是通过集线器连接，计算机 C 和 F 是直接连接交换机。

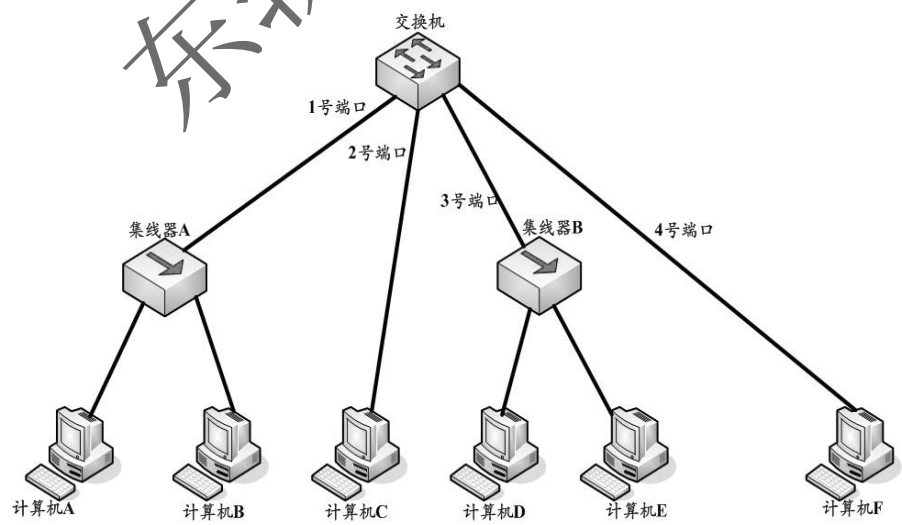


**图 3.4　网络拓扑图**

从前面讲到的交换机原理可以知道，如果计算机 A 要给计算机 C 发送数据包，通过“端

口/MAC 地址映射表”，信息只从交换机的 1 号端口传送到 2 号端口，而不再向 3、4 号端口转发。

如果计算机 A 要给计算机 B 发送数据包，交换机在 1 号接口收到数据包，而交换机发现目的端口与源端口一致，就不再转发数据包，直接把数据包抛弃，数据包就在集线器连接的局域网中传送。类似这样的过程就被称之为交换机的“通信过滤”。交换机的“通信过滤”能够避免网络上不必要的数据传输，减少了网络的通信负荷，为网络提供了更多的带宽，提高了网络的利用率。

**4.交换机的访问方式**

交换机的访问一般都支持四种方式：连接控制台方式、连接设备 AUX 端口方式、远程登录方式和 Web 配置方式。

(1)连接控制台方式

Console 端口是交换机提供的专用管理端口，可以通过相关的连接电缆，一端插入交换机的 Console 端口，另一端接入计算机的串口，以建立计算机与交换机的配置连接。通过 Console 端口连接并配置交换机是管理交换机必须经过的步骤，因为其他的管理和配置方式都需要先通过 Console 端口对交换机实施基本配置后才能进行。

不同品牌交换机的 Console 端口有不同的类型，但绝大多数都采用 RJ-45 端口，也有少数是串行端口。因此，要通过 Console 端口配置交换机就需要专门的 Console 连接线，Console 连接线主要有两种：一种是串行线，采用 DB-9 或 DB-25 的串行插口线；另一种是采用 RJ-45 接头的翻转线。图 3.5 展示了一台计算机终端通过控制台端口与交换机连接的实例。


**图 3.5　控制台访问方式**

(2)连接设备 AUX 方式

这种方式一般适用于远程移动用户的登录配置，有时候网络管理员因为一些实际情况需要经常在各个地方来回奔走。采用这种方式，如果管理员需要对网络设备进行远程配置操作，就可以通过 MODEM 连接设备的 AUX 端口，通过电话拨号的方式远程配置设备。

(3)远程登录方式(Telnet)

Telnet 也是网络管理员经常使用的配置方式之一。在实际网络环境中，网络的规模可能相当庞大，其地域覆盖甚至超过几十公里甚至上千公里。这种情况下，一个网络管理员是无法随时在设备面前对该设备实施配置操作的。通过 Telnet 方式，管理员就可以通过网络登录到远程设备上，像坐在设备面前一样轻松地完成配置。

(4)Web 配置方式

大多数的网络设备都支持 Web 的配置方式，像访问 WWW 一样，我们只需要打开 IE 浏

览器，直接输入交换机的管理地址（IP 地址），就能进入交换机的管理界面，如一些基于 Web 的管理软件 Cisco Work 或 HP Open View 等。Web 配置方式是基于 HTTP 协议的，这样网络管理员就能够从远程通过浏览器以图形化的界面方式来配置，因此具有操作直观、简便的优点。但是，由于 Web 配置在安全性方面不如前几种方式且管理功能有限，所以在大型网络管理中并不常见。

## 3.2.2　任务实践

任务 1：交换机的配置模式共有几种？

任务解析：用表 3.2 来说明交换机的模式以及模式的命令。

**表 3.2　　交换机的模式**

| 模式名称 | | 命令 | 提示符 | 说明 |
|---|---|---|---|---|
| 用户模式 | | --- | Switch＞ | 普通用户操作级别 |
| 进入特权模式 | | enable | Switch # | 可以对设备配置并进入其他配置模式 |
| 全局配置模式 | | configure terminal | Switch（config）# | 配置交换机的全局参数 |
| 子模式 | 进入接口配置模式 | Switch（config）# interface f0/1 | Switch（config-if）# | 对交换机的某个接口配置 |
| | 进入线路配置模式 | Switch（config）# line console 0 | Switch（config-line）# | 对远程登录（telnet）等会话配置 |
| | 进入路由配置模式 | Switch（config）# router rip | Switch（config-router）# | 配置路由 |
| | 进入 VLAN 配置模式 | Switch（config）# vlan 3 | Switch（config-vlan）# | 配置 VLAN 参数 |

任务 2：怎样进入特权模式、全局配置模式？

任务解析：计算机连接到交换机，交换机正式启动后会直接进入用户模式，提示符是 Switch＞，具体步骤如下：

```
Switch>enable
Switch#config terminal
Switch(config)#
```

任务 3：怎样从全局配置模式退回到用户模式。

任务解析：

```
Switch(config)#exit
Switch#exit
Switch>
```

任务 4：交换机的时间通常对网络管理员来说非常重要，怎样设置交换机的系统时间？

任务解析：假设要将交换机的时间设置为 2014 年 2 月 16 日 13 点 40 分

```
Switch>enable
Switch#clock set 13:40:00 16 22014-2-16
```

设置完成后，在特权模式下通过命令“show clock”来显示交换机当前的时钟。

### 3.2.3 思考与练习

**一、选择题**

关于交换机的学习过程，下面（　　）是正确的。

A. 会在“MAC/端口地址映射表”中更新已知的目的 MAC 地址信息

B. 交换机智能地转发未知的目的 MAC 地址

C. 交换机可以学习广播 MAC 地址

D. 交换机丢弃未知的目的 MAC 地址

**二、实训练习**

练习：查看交换机的 MAC/端口映射表。

在这个实践环节中，首先要掌握计算机与交换机是如何连接的。交换机跟 PC 机不同，没有辅助设备（包括鼠标，键盘，显示器等）。因此，交换机要输入命令或者显示出结果，就要想办法将交换机连接到 PC 机，通过 PC 机来对交换机输入命令和输出结果。交换机的 console 端口和 console 线如图 3.6 和 3.7 所示。图 3.6 中的 console 线一端是 RJ45 接口，另一端是串口。RJ45 接口连接到 console 端口，串口连接到计算机。根据 console 端口不同，也可以适当调整。

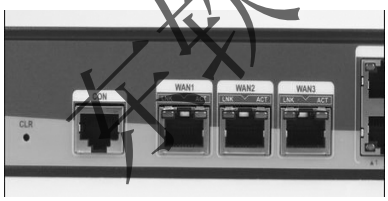


图 3.6　console 端口

图 3.7　Console 线

实验步骤如下：

（1）将计算机与交换机之间通过 console 线连接，如图 3.8 所示：


图 3.8　计算机与交换机通过 console 端口连接

（2）单击【开始】|【程序】|【附件】|【通讯】|【超级终端】，如图 3.9 所示，键入名称，单击确

定，进入下一步；

（3）由于是本地连接交换机，端口一定要选择 com 端口，如图 3.10 所示，单击【确定】，进入下一步；


图 3.9　超级终端


图 3.10　选择 com 端口

（4）在弹出的 com3 端口设置中，单击【还原为默认值】，单击【确定】，完成 PC 机与交换机的连接，弹出如下对话框，如图 3.11 所示：

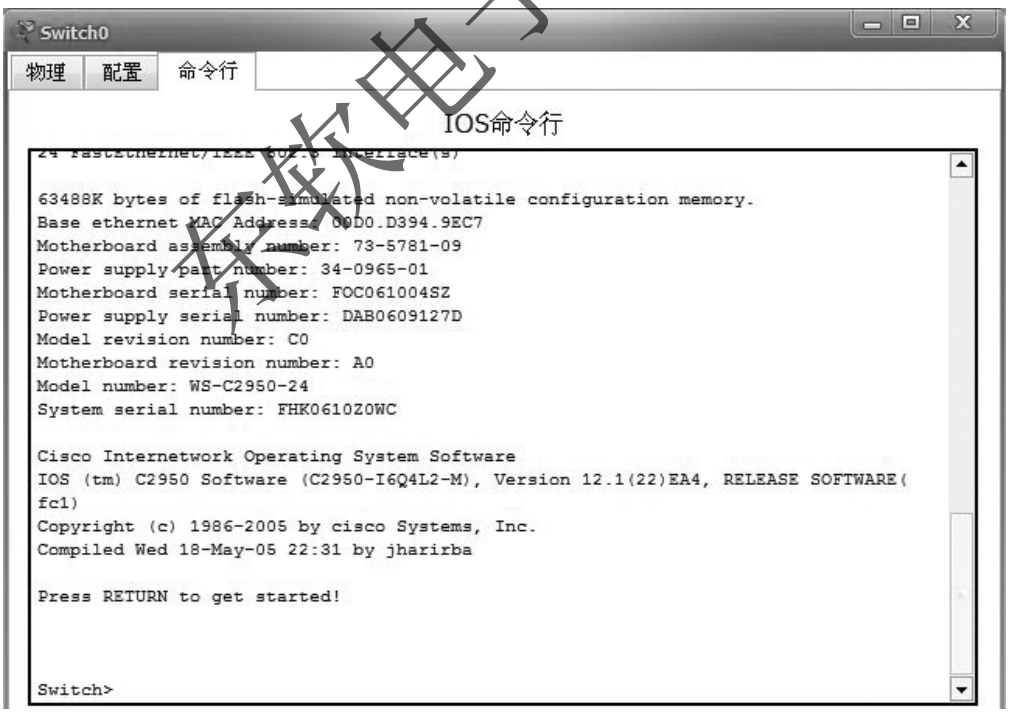


图 3.11　交换机启动

(5)输入命令“en”,进入交换机的特权模式;

(6)在“switch#”的提示符下,输入命令“show mac”,命令执行如图 3.12 所示。

```
Switch#show mac
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00e0.a342.2056    STATIC      Fa0/3
   1    00e0.a342.20e6    STATIC      Fa0/2
   1    00e0.a356.1a56    STATIC      Fa0/4
Switch#
```

图 3.12 MAC/端口映射表的执行

# 3.3 交换式局域网

## 3.3.1 基本知识

**1.为什么提出“交换式局域网”**

上一章中组建的局域网是共享式以太网,由集线器作为连接设备形成的以太网。传统的共享式以太网是最简单、最便宜、最常用的一种组网方式。但是,在网络应用和组网过程中,共享式以太网的最突出的缺点就是网络总带宽是固定的,网络上所有节点共享带宽。也就是说,在一个节点使用传输介质的时候,另一个节点就必须等待。因此,节点越多,速度越慢。例如:对于一个带宽为 100Mb/s 的共享式以太网,如果连接 10 个节点,则每个节点平均带宽为 10Mb/s。如果连接节点增加到 50 个,每个节点平均带宽将会降低为 2Mb/s。

**2.解决共享式以太网所存在的问题**

通常人们解决复杂问题的时候,经常会采用“分而治之”的方法。为了解决共享式以太网中“共享带宽”的问题,就可以利用“分段”来解决这个问题。所谓“分段”,就是将一个大型的以太网分成多个小型的以太网。小型的以太网之间利用“交换”设备进行沟通。这种交换设备可以将在一个小型以太网接收到的信息经过简单的处理转发给另一个小型以太网。

图 3.13 是某企业的网络拓扑图,这是一个共享式以太网的例子。图中所示市场部、财务部和技术部都通过各自的集线器组网。图 3.13 中所示一个共享式集线器连接各部门的集线器,而构成了集线器级联并组成了大型共享式以太网。由于集线器发送信息的方式是广播发送,因此任何计算机之间传送信息都将流通于整个网络。

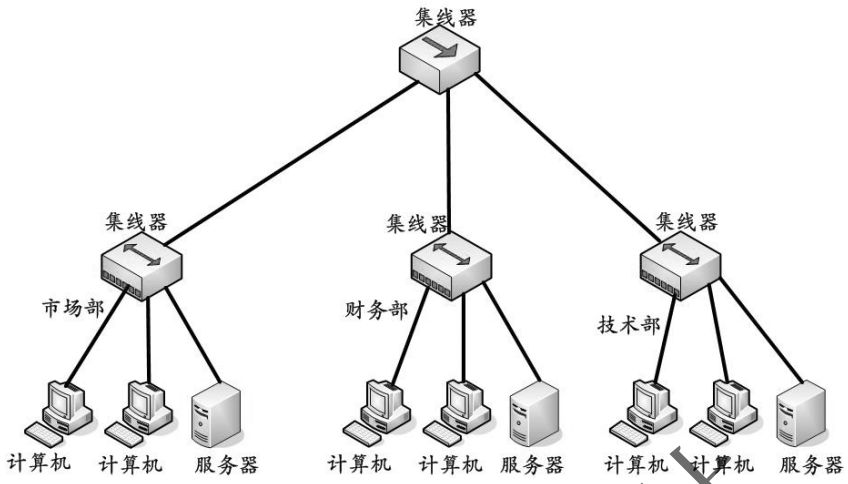


图 3.13　通过集线器级联组成大型的共享以太网

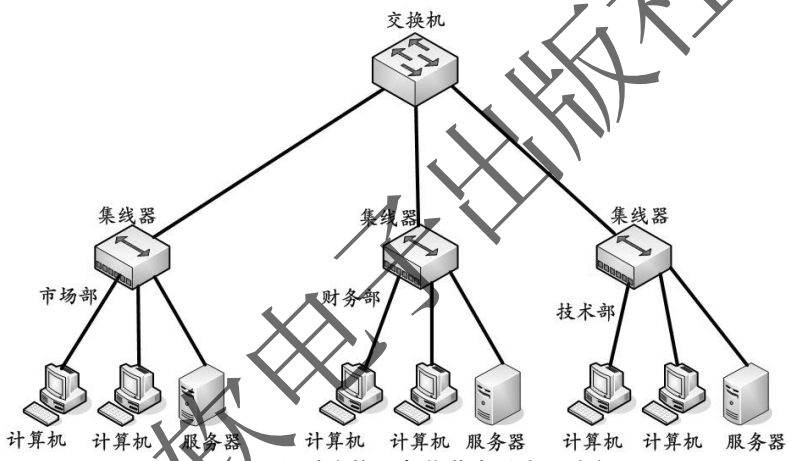


图 3.14　通过交换设备将共享以太网分段

通常，部门与部门之间的相互访问是最频繁的。为了限制部门内部计算机传送的信息在全网流动，就如图 3.14 所示将大型以太网分段。每个部门的计算机都组成了一个小型以太网，部门与部门之间的连接采用交换设备来完成。交换设备有很多类型，包括交换机、路由器等。交换机工作在数据链路层，也是交换式以太网的核心设备。路由器将在第五章中介绍。

## 3.3.2　任务实践

任务 1：集线器和交换机都是网络连接设备，他们有什么区别？

任务解析：集线器工作在物理层。集线器发送信息的形式是广播传送，即计算机 A、B、C 用集线器连接起来，A 如果想给 B 发送信息，A 先将信息传送给集线器，而集线器会将这些信息广播发送给 B 和 C。而计算机 B 判断数据包的目的地址与自己的地址吻合才把信息留下来，而计算机 C 将会把数据包丢弃，从而完成计算机 A 到计算机 B 的数据包传送。因此，集线器采用共享带宽的工作方式。

交换机：工作在数据链路层。传送信息的方式是端口与端口之间的传送。因此，交换机是独享带宽的。

任务 2：交换式局域网的交换方式有哪些？

任务解析：交换式局域网的交换方式一共有三种，分别是直接交换，存储转发交换和改进的直接交换。

直接交换：在直接交换的方式下，交换机要一边接收信息，一边检测信息。一旦检测到目的地，便将数据送到相应的端口，而不管数据是否出错，检测错误的任务也是由终端计算机来完成的。这种交换方式延迟时间短，但缺乏差错检测能力。

存储转发交换：交换机首先要完整地接收计算机发送的数据，并对数据进行差错检测。如果数据正确，才会根据目的地址将数据传送出去。但是这种交换方式会导致数据转发的延迟时间较长。

改进的直接交换：这种交换方式是将直接交换与存储转发交换结合起来，在接收到数据前 64 字节之后，就来检测数据是否正确，如果正确就转发出去。对于短数据来说，交换延迟与直接转发方式比较接近；而对于长数据来说，由于它只对数据前部的主要字段进行差错检测，交换延迟将会减少。

### 3.3.3 思考与练习

**一、选择题**

1.（　　）设备无法解决冲突问题。

A. 集线器　　B. 交换机

C. 交换机和集线器　　D. 路由器和集线器

2. 关于交换机的学习过程，下面（　　）是正确的。

A. 会在“MAC/端口地址映射表”中更新已知的目的 MAC 地址信息

B. 交换机智能地转发未知的目的 MAC 地址

C. 交换机可以学习广播 MAC 地址

D. 交换机丢弃未知的目的 MAC 地址

**二、实训练习**

练习：在小型的企业中，办公自动化与局域网结合的应用非常广泛。现在要实现在企业局域网设置打印机共享，将打印机与一台计算机相连，通过其他的计算机实现打印服务应用。

实验步骤：

（1）通过交换机，将办公室的几台计算机连在一起，拓扑结构如图 3.15 所示（可以根据实际情况增加计算机的数量）；

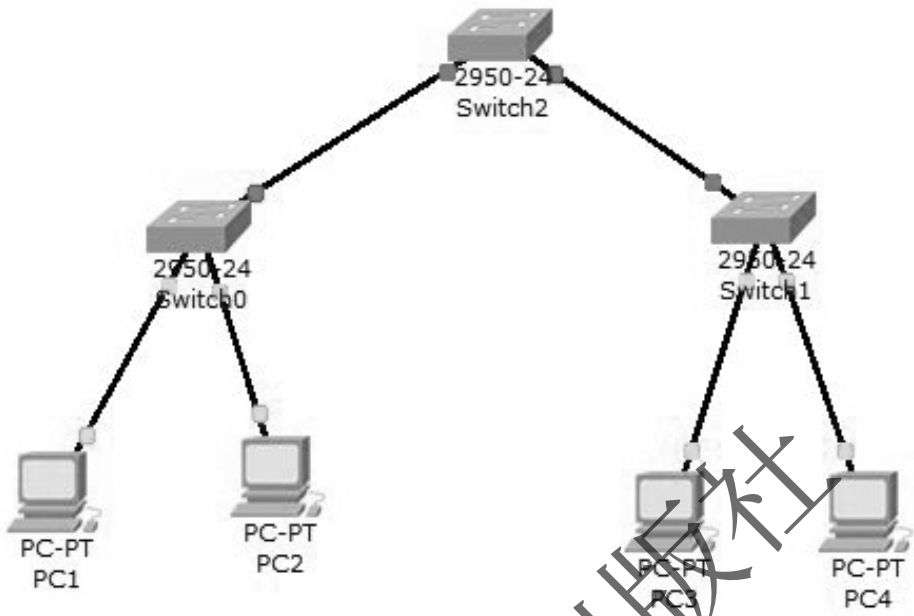


**图 3.15　某办公室网络拓扑图**

(2)将打印机与其中的一台计算机(PC1)连接,其余的 PC 机与 PC1 连接成交换式局域网,从而共享打印服务;

(3)打开控制面板,选择【打印机和传真】|【添加打印机】,如图 3.16 所示,单击【下一步】继续;

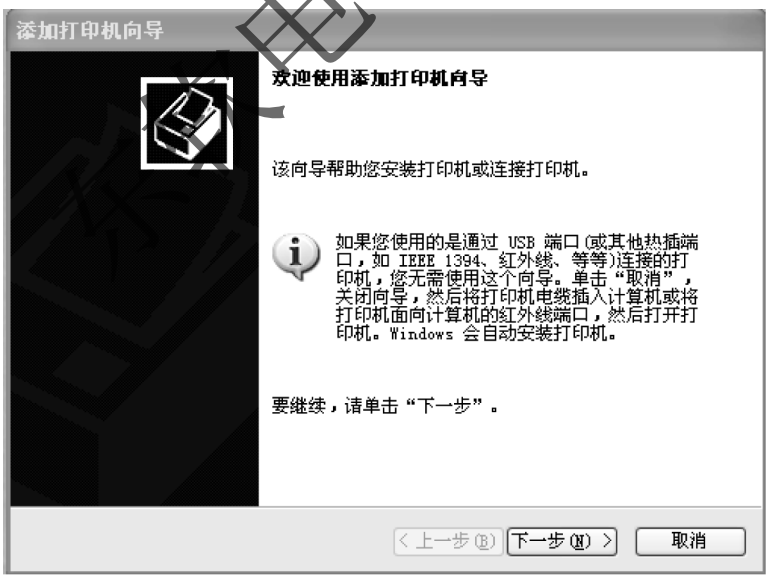


**图 3.16　设置共享打印(一)**

(4)选择网络打印机,如图 3.17 所示,单击【下一步】继续;

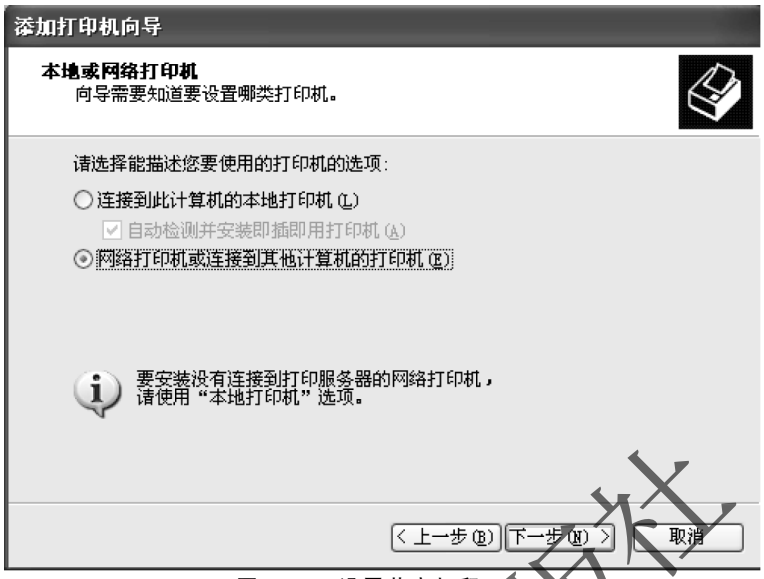


图 3.17 设置共享打印(二)

(5)选择浏览打印机,如图 3.18 所示,单击【下一步】继续;

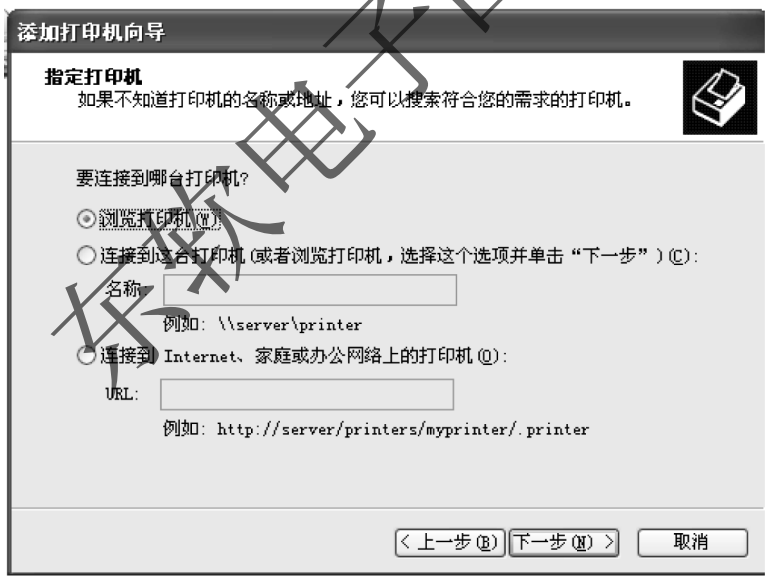


图 3.18 设置共享打印—浏览打印机

(6)选择你要选择的打印机的型号,单击【下一步】继续,添加打印机完成。


图 3.19　设置共享打印—选择打印机

(7)在局域网连接的计算机中,测试共享打印。

## 3.4　虚拟局域网

### 3.4.1　基本知识

所谓的虚拟局域网(VLAN,virtual LAN),就是将局域网上的计算机划分成若干个“逻辑组合”,这个逻辑组合可以根据功能、部门、职能等因素划分而无需考虑计算机所处的地理位置。

虚拟局域网可以在交换机上完成,以软件形式实现逻辑工作组的划分与管理。所以,局域网如果想划分虚拟局域网,跟计算机的物理位置无关。所以,虚拟局域网中的计算机可以不在一个网段中,只要交换机是互联的,逻辑组中的计算机可以连在一个交换机上,也可以连在不同的交换机上。计算机如果想从一个虚拟局域网转移到另一个虚拟局域网,只需要通过软件设定,而不需要改变它的物理位置。如果计算机的物理位置有所移动,只要通过交换机软件设置,这台计算机便可以成为原来的虚拟局域网中的一员。

虚拟局域网可以通过交换机的接口来划分,如果按照这种方式划分 VLAN,那么一旦接口改变,VLAN 也随之会发生变化。虚拟局域网也可以通过 MAC 地址、逻辑地址或数据包的协议类型来划分,按照这些方式来划分 VLAN,VLAN 不会因为计算机的接口改变而改变,只要计算机中的网卡不改变,VLAN 就不会发生变化。因此,VLAN 就有静态和动态之分。

**1.VLAN 组网方式**

VLAN 可以根据部门、功能或应用来划分,而不需要考虑用户的物理位置。简单的说,

可以利用划分端口的方式来分配 VLAN。且 VLAN 的组网方式主要包括静态 VLAN 和动态 VLAN。

(1)静态 VLAN

静态 VLAN 是将以太网交换机上的一些端口划分给一个 VLAN。如果不用人工的方式去改变 VLAN,VLAN 就不会改变。在图 3.20 中,在配置 VLAN 时,以太网交换机端口 3、4、5 可以组成 VLAN1,同时以太网交换机端口 1、2、6、7、8、9 组成 VLAN2。

虚拟局域网可以在一个交换机上来实现,也可以跨交换机来划分 VLAN。如图 3.21 交换机 A 的 12、13、16 号端口和交换机 B 中的 3 号和 11 号端口配置形成 VLAN1;交换机 A 中的 2、8、10 号端口和交换机 B 中的 4、6、16 号端口形成 VLAN2。如何跨交换机划分 VLAN,将在练习环节中详细阐述。

①静态 VLAN 的优点:划分方式比较简单,容易实现。

②静态 VLAN 的缺点:不适应地理位置的变化。如果局域网中的计算机要移动位置,交换机的端口也会改变。这样,原来的 VLAN 就会发生变化。

因此,静态 VLAN 比较适合计算机位置相对稳定的情况。

(2)动态 VLAN

动态 VLAN 就是指根据用户的 MAC 地址、逻辑地址和数据包的协议类型来决定计算机属于哪一个 VLAN。也就是说,交换机上 VLAN 端口是动态分配的。若以 MAC 地址来划分 VLAN,可以通过指定哪些 MAC 地址的计算机划分在哪一个 VLAN。

例如,MAC 地址为 01-32-56-4A-6B-0E、53-4C-1A-67-98-32 和 43-77-9D-1E-2F-42 的计算机属于 VLAN1,而不必关心这些计算机连接交换机的哪些端口。所以,无论计算机的地理位置如何改变,只要计算机的 MAC 地址不变,它所属的 VLAN 就不会改变,所以网络管理员不必因为计算机的地理位置改变而重新配置 VLAN。

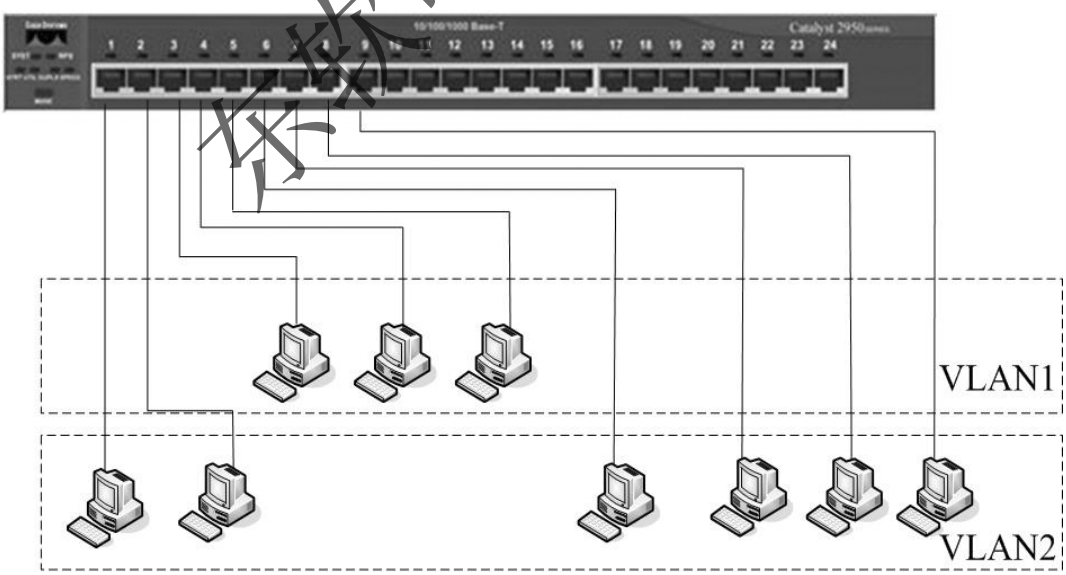


图 3.20 在单个交换机划分 VLAN

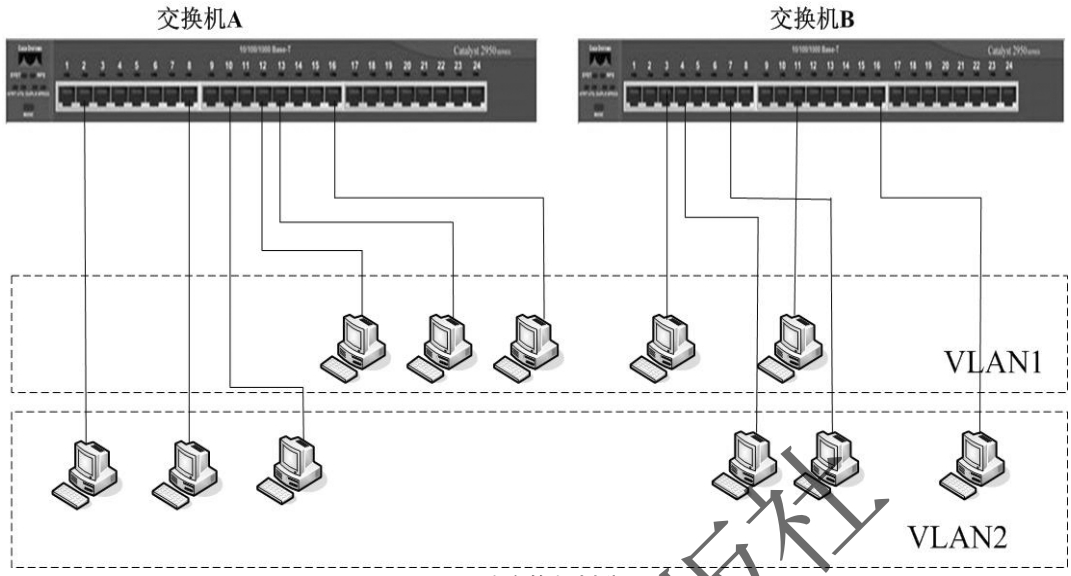


图 3.21　跨交换机划分 VLAN

**2.VLAN 的优点**

(1)控制广播风暴

广播存在于任何网络中,而且广播数据包数量增多就会形成广播风暴。一旦产生广播风暴,就会造成网络拥堵,大大降低了网络的利用率。因此为了要提高网络效率就要限制网络上的广播,将网络划分为多个 VLAN 就可以减少参与广播风暴的设备数量。局域网分段可以防止广播风暴波及整个网络。使用 VLAN,可以将某个交换机端口或用户赋于某一个特定的 VLAN,该 VLAN 可以在一个交换网中跨接多个交换机,在一个 VLAN 中的广播不会送到 VLAN 之外。同样,相邻的端口不会收到其他 VLAN 产生的广播。这样可以减少广播流量,释放带宽供用户应用,减少广播的产生。

(2)安全

增强局域网的安全性,含有敏感数据的用户组可与网络的其余部分隔离,从而降低泄露机密信息的可能性。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,如果不同 VLAN 要进行通信,则需要通过路由器或三层交换机等三层设备。

(3)成本降低

假设一个小型企业存在技术部、开发部、市场部、财务部、办公室、宣传部等部门,每个部门大概有 3～4 人。在组建这个企业局域网的时候,希望每个部门都属于一个小型网络。如果想要物理实现,那么每个部门都需要一台交换机来完成整个企业局域网的配置。这样,就需要 6 台以上的交换机,且每个部门都只有 3～4 台计算机,所以成本会大大增加。如果能够用一台或两台交换机将他们所有机器连接在一起,用划分 VLAN 的方法来使每个部门成为独立的逻辑组合,同样可以达到企业的需求,成本还可以大大降低。

(4)应用管理

VLAN 将用户和网络设备聚合到一起,以支持商业需求或地域上的需求。通过职能划

分,项目管理或特殊应用的处理都变得十分方便,例如可以轻松管理教师的电子教学开发平台。此外,也很容易确定升级网络服务的影响范围。

(5)增加网络连接的灵活性

借助 VLAN 技术,能将不同地点、不同网络、不同用户组合在一起,形成一个虚拟的网络环境,就像使用本地局域网一样方便、灵活、有效。VLAN 可以降低移动或变更工作站地理位置的管理费用,特别是一些业务情况经常有变动的公司。但如果使用了 VLAN 之后,这部分管理费用就可以大大降低。

**3.VTP 协议**

VTP(VLAN Trunk Protocol)是一种消息协议,是由 Cisco 公司开发的私有协议,目前华为等品牌交换机也支持 VTP 协议。用于在 VTP 域内同步 VLAN 信息,而不需要在每个交换机上配置相同的 VLAN 信息,从而实现 VLAN 配置的一致性。在一台交换机(设置为 VTP Server)上配置一个新的 VLAN 信息,则该信息将自动传播到本域内的所有交换机,从而减少在多台设备上配置同一信息的工作量,且方便了管理。VTP 信息只能在 Trunk 端口中传播。

任何一台运行 VTP 协议的交换机可以配置成以下三种模式:

①VTP Server:维护该 VTP 域中所有 VLAN 信息列表,可以增加、删除或修改 VLAN。

②VTP Client:维护该 VTP 域中所有 VLAN 信息列表,不能增加、删除或修改 VLAN,任何变化的信息必须从 VTP Server 发送的报文中接收。

③VTP Transparent:不参与 VTP 工作,虽然忽略所有接收到的 VTP 信息,但能够将接收到的 VTP 报文转发出去。它只拥有本设备上的 VLAN 信息。

其中,VTP Server 和 VTP Client 必须处于同一个 VTP 域,而且一个交换机只能位于一个 VTP 域中。默认交换机是 VTP Server 模式。

注意:交换机之间或交换机与路由器互联用的端口就称为 Trunk 端口。Trunk 端口是用来在不同的交换机之间进行连接,以保证跨多个交换机的同一个 VLAN 的成员能够互相通讯。

**例 3-1** VLAN 中继协议(VTP)用于在大型交换网络中简化 VLAN 的管理。按照 VTP 协议,交换机的运行模式分为 3 种:服务器、客户机和透明模式。下面关于 VTP 协议的描述中,错误的是(　　)。(摘自 2009 年网络工程师真题)

A. 交换机在服务器模式下能创建、添加、删除和修改 VLAN 配置

B. 一个管理域中只能有一个服务器

C. 在透明模式下可以进行 VLAN 配置,但不能向其它交换机传输配置信息

D. 交换机在客户模式下不允许创建、修改或删除 VLAN

试题解析:VTP 从不要求一个管理域中只能有一个服务器。所以答案是 B。

**例 3-2** 新交换机出厂时的默认配置是(　　)。(摘自 2009 年全国计算机技术与软件专业技术资格(水平)考试网络工程师真题)

A. 预配置为 VLAN1,VTP 模式为服务器

B. 预配置为 VLAN1,VTP 模式为客户机

C. 预配置为 VLAN0，VTP 模式为服务器

D. 预配置为 VLAN0，VTP 模式为客户机

试题解析：在默认的情况下，交换机将所有接口都划分到 VLAN1 中，而 VTP 模式默认为服务器。所以答案是 A。

## 3.4.2　任务实践

任务：现有交换机一台，要求 2、3、4、5 号端口属于编号为 13 的 VLAN。请详细阐述 VLAN 划分的步骤。

任务解析：划分 VLAN 的步骤如下：

(1)查看目前 VLAN 的划分情况；

(2)新建一个编号为 13 的 VLAN；

(3)将 2、3、4、5 号端口添加到编号为 13 的 VLAN。

注意：在交换机没有划分任何 VLAN 的情况下，交换机有一个默认的 VLAN，编号为 1，且所有的接口都属于 VLAN1。

## 3.4.3　思考与练习

**一、选择题**

1. 能进入 VLAN 配置状态的交换机命令是(　　)。(摘自全国计算机技术与软件专业技术资格(水平)考试网络工程师考试试题)

A. 2950(config)# vtp pruning　　B. 2950# vlan database

C. 2950(config)# vtp server　　D. 2950(config)# vtp mode

2. 关于虚拟局域网(VLAN)，下面(　　)是错误的。

A. VLAN 是一个广播域　　B. VLAN 是一个用户逻辑组

C. VLAN 与位置相关　　D. VLAN 是一个子网

**二、实训练习**

练习 1：单交换机的 VLAN 划分

此实验项目将同一个交换机连接的 PC 机划分为两个 VLAN，使得同一个 VLAN 的两台 PC 机能够通信，而不同 VLAN 的两台 PC 机无法通信。在交换机上创建两个 VLAN，将 PC1 和 PC2 划分到 VLAN10 中，将 PC3 和 PC4 划分到 VLAN20 中，在交换机上新建 VLAN10 和 VLAN20。实验步骤如下：

(1)查看目前 VLAN 的划分情况

在交换机输入指令中，在特权模式下输入“show vlan”的命令，查看目前 VLAN 的划分情况，如图 3.22 所示。默认情况下 24 个端口都在 vlan1 中。

```
Switch>en
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
```

**图 3.22 查看 VLAN**

```
Switch#config terminal      --- 进入全局配置模式
Switch(config)#vlan 10      ----创建编号为 10 的 vlan
Switch(config-vlan)#exit    ----退回到全局配置模式
Switch(config)#vlan 20      ----创建编号为 20 的 vlan
```

系统自动为 vlan10 和 vlan20 分别起名字为 VLAN0010 和 VLAN0020。网络拓扑及 VLAN 划分情况如图 3.23 所示。

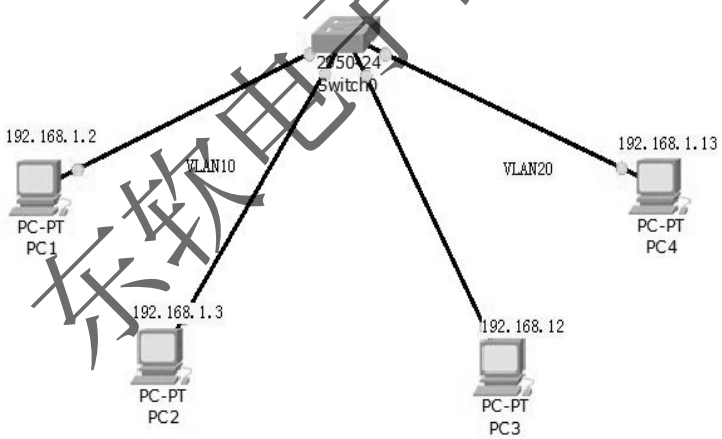


**图 3.23 VLAN 划分示意图**

(2)在交换机上向各个 VLAN 内添加端口。分别将 PC1 和 PC2 所连接的 Fa0/1 和 Fa0/2 接口添加到 VLAN10,将 PC3 和 PC4 所连接的 Fa0/3 和 Fa0/4 接口划入 Vlan20。代码如下:

```
Switch(config)#interface f0/1
Switch(config-if)#switchport access vlan 10
```

将 PC1 连接的 Fa0/1 分配给 vlan10。

```
Switch(config-if)#exit
Switch(config)#int f0/2
Switch(config-if)switchport access vlan 10
Switch(config)#int f0/3
```

```
Switch(config-if)switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int f0/4
Switch(config-if)switchport access vlan 20
```

再次退回到特权模式，查看 vlan 的划分情况，如图 3.24 所示。

```
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   VLAN0010                          active    Fa0/1, Fa0/2
20   VLAN0020                          active    Fa0/3, Fa0/4
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
```

**图 3.24　查看划分后的 VLAN 情况**

(3)测试 PC1 和 PC3 的连通性，通过测试的结果，发现两台计算机不能通信。

(4)经过以上配置以及测试，证明 vlan 划分成功。

练习 2：跨交换机的 VLAN 划分

按照图 3.25 来搭建网络，2 台交换机分别与 2 台 PC 机用直通线互联，Switch1 的 f0/1 和 f0/6 连接 PC1 和 PC2，Switch2 的 f0/1 和 f0/6 连接 PC3 和 PC4。两台交换机分别用各自的 f0/20 号端口用交叉线互联。现在要将 PC1 和 PC3 划分到 VLAN10 中，PC2 和 PC4 划分到 VLAN20 中。

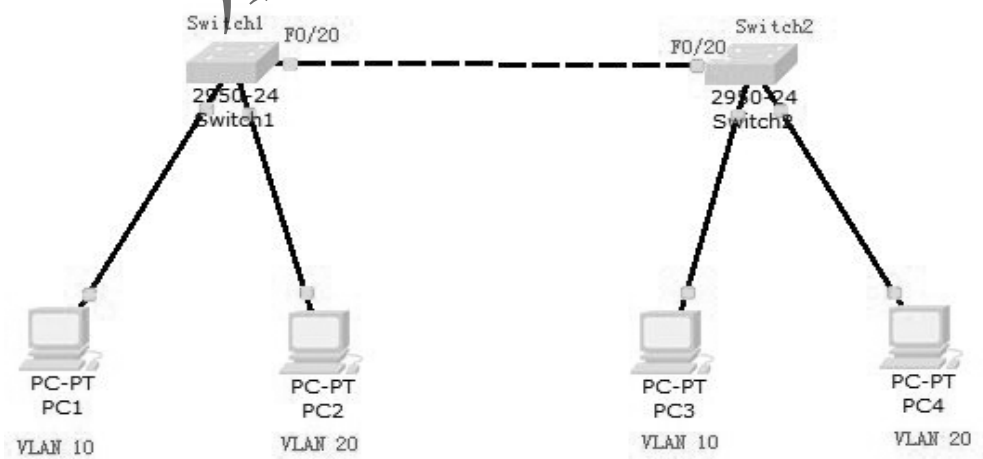


**图 3.25　跨交换机的 vlan 划分**

跨交换机实现 VLAN 划分的步骤如下：

(1)交换机 1 上创建 VTP 域，设置为 VTP Server，创建 VLAN10 和 VLAN20；

(2)交换机 2 上创建相同 VTP 域，并设置为 VTP Client；

(3)分别打开 Switch1 和 Switch2 的 f0/20 接口功能；

(4)在各自的交换机上分配接口，也就是在 Switch1 的 1 号接口分配到 VLAN10，Switch1 的 6 号接口分配到 VLAN20。将 Switch2 的 1 号接口分配到 VLAN20，Switch2 的 6 号接口分配到 VLAN20。

(5)利用连通性来测试 VLAN 的划分情况。

具体实施步骤如下：

(1)打开 Cisco Packet Tracer，按照图 3.25 来搭建网络的拓扑结构。

(2)配置 4 台 PC 机的 IP 地址。

(3)利用 ping 命令来测试连通性。

(4)打开 Switch1 和 Switch2 各自 F0/20 端口的 Trunk 功能，代码如下：

```
Switch1(config)#int f0/20
Switch1(config-if)#switchport mode trunk
```

(5)配置 Switch1，创建 VTP 域，名字为 exam。并设置 Switch1 为 VTP 的 Server，代码如下：

```
Switch1(config)#vtp domain exam
```

(6)配置 Switch2，创建相同的 VTP 域，并设置为 VTP Clietn 模式；

```
Switch2(config)#vtp domain exam
Switch2(config)#vtp mode client
```

(7)配置 Switch1，创建 vlan10 和 vlan20，同时在 Switch2 输入命令 show vlan，查看 vlan 的划分情况，如图 3.26 所示。

```
Switch2#
Switch2#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
10   VLAN0010                          active
20   VLAN0020                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
```

图 3.26 查看 vlan

(8)配置 switch1,添加 F0/1 接口到 vlan10,F0/6 接口到 Vlan20。同样配置 switch2,添加 F0/1 接口到 vlan10,F0/6 接口到 vlan20,如图 3.27 和 3.28 所示。

```
%SYS-5-CONFIG_I: Configured from console by console

Switch1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
10   VLAN0010                         active    Fa0/1
20   VLAN0020                         active    Fa0/6
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
 --More--
```

图 3.27　在 switch1 上查看 vlan 划分情况

```
Switch2#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
10   VLAN0010                         active    Fa0/1
20   VLAN0020                         active    Fa0/6
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
 --More--
```

图 3.28　switch2 上查看 vlan 划分情况

(9)测试 PC1 和 PC2 的连通性,经过测试,可以得知 PC1 和 PC2 无法连通。

(10)经过以上配置及测试情况证明,跨交换机 vlan 划分成功。

## 3.5 小结

本章首先介绍了交换机的工作原理以及访问方式,之后将为什么提出“交换式局域网”的问题引出来,并给予解决。本章的重点内容是虚拟局域网,包括虚拟局域网的基本知识,以及单交换机的 VLAN 划分和多交换机的 VLAN 划分。虚拟局域网在网络管理员的工作中频繁应用,应重点掌握。