

第 3 章 交换与虚拟局域网

学习本章后需要掌握：

- 交换式以太网的特点
- 以太网交换机的工作过程和数据传输方式
- 以太网交换机的通信过滤、地址学习和生成树协议
- VLAN 的组网方法和特点

学习本章后需要动手：

- 组装简单的交换式以太网
- 配置以太网交换机
- 在交换式以太网上划分 VLAN

以太网变得越来越拥塞和不堪重负，一方面是由于网络应用和网络用户的迅速增长；另一方面则是由于快速 CPU 及快速网络操作系统的出现。现在，处于同一个以太网上的两个工作站就很容易使网络饱和。为了提高局域网的效率，交换技术应运而生了。

3.1 交换式以太网的提出

3.1.1 共享式以太网存在的问题

传统的共享式以太网是最简单、最便宜、最常用的一种局域网。但是在网络应用和组网过程中，共享式以太网也暴露出它的弱点。这些弱点包括如下方面。

- 覆盖的地理范围有限：按照 CSMA/CD 的有关规定，以太网覆盖的地理范围随网络速度的增加而减小。一旦网络速率固定下来，网络的覆盖范围也就固定下来。因此，只要两个结点处于同一个以太网中，它们之间的最大距离就不能超过某一固定值，不管它们之间的连接跨越一个集线器还是多个集线器。如果超过这个值，网络通信就会出现問題。
- 网络总带宽容量固定：传统的以太网是一个共享式的局域网，网络上的所有结点共享同一传输介质。在一个结点使用传输介质的过程中，另一个结点必须等待。因此，共享式以太网的固定带宽容量被网络上的所有结点共同拥有，随机占用。网络中的结点越多，每个结点平均可以使用的带宽越窄，网络的响应速度就会越

慢。例如,对于一个使用 100BASE-TX 技术的 100Mbps 以太网,如果连接 10 个结点,则每个结点平均带宽为 10Mbps;如果连接结点增加到 100 个,则每个结点平均带宽下降为 1Mbps。另外,在发送结点竞争共享介质的过程中,冲突和碰撞是不可避免的。冲突和碰撞会造成发送结点随机延迟和重发,进而浪费网络带宽。随着网络中结点数的增加,冲突和碰撞的概率必然加大,随之而来的带宽浪费也会变大。

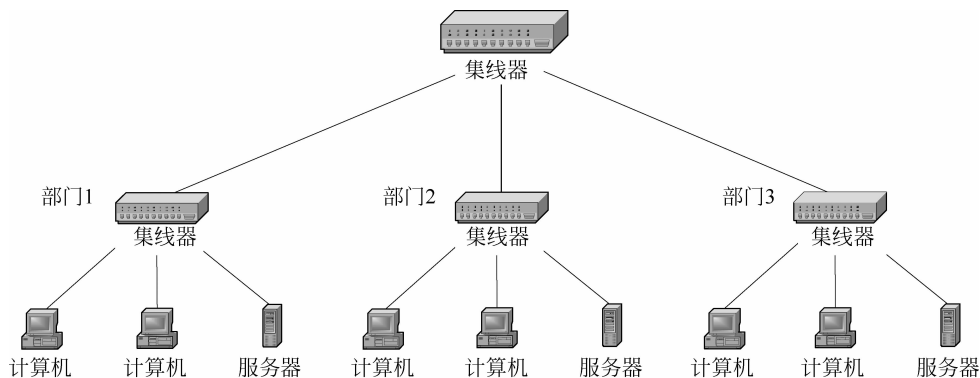
- 不能支持多种速率:网络应用是多种多样的。有的应用信息传输量小,低速网络就可以满足要求;而有的应用信息传输量大,要求快速的网络响应。不同速率的混合型组网不但有其存在的客观要求,而且可以提高组网的性能价格比。但是,由于传统以太网使用共享传输介质,因此网络中的设备必须保持相同的传输速率,否则一个设备发送的信息,另一个设备不可能正确接收。单一的共享式以太网不可能提供多种速率的设备支持。

3.1.2 交换的提出

通常,人们利用“分段”的方法解决共享式以太网存在的问题。所谓“分段”,就是将一个大型的以太网分割成两个或多个小型的以太网,每个段(分割后的每个小以太网)使用 CSMA/CD 介质访问控制方法维持段内用户的通信。段与段之间通过一种“交换”设备进行沟通。这种交换设备可以将一段接收到的信息,经过简单的处理转发给另一段。

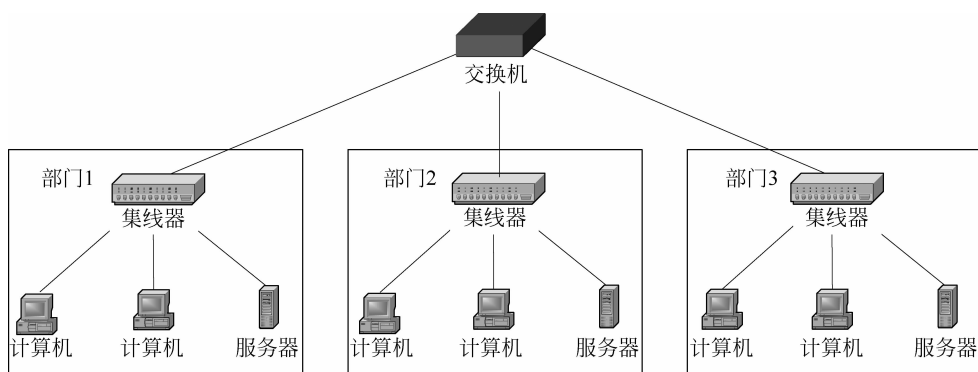
图 3-1 对一个较大的以太网进行了分段。其中图 3-1(a)给出了一个通过集线器级联组成的大型以太网。尽管部门 1、部门 2 和部门 3 都通过各自的集线器组网,但是由于使用共享式集线器连接各个部门的集线器,因此所构成的网络仍然属于一个大的以太网。这样,每台计算机发送的信息,将在全网流动,即使它访问的是本部门的服务器。

通常,部门内部计算机之间的相互访问是最频繁的。为了限制部门内部信息在全网流动,图 3-1(b)将整个大以太网分段,每个部门组成一个小的以太网,部门之间通过交换



(a) 通过集线器级联组成大型的共享以太网

图 3-1 使用交换设备对共享式以太网分段



(b) 通过交换设备将共享以太网分段

图 3-1(续)

设备相互连接。通过分段,既可以保证部门内部信息不会流至其他部门,又可以保证部门之间的信息交互。以太网结点的减少使冲突和碰撞的概率更小,网络的效率更高。不仅如此,分段之后各段可按需要选择自己的网络速率,组成性能价格比更高的网络。

交换设备有多种类型,局域网交换机、路由器等都可以作为交换设备。交换机工作于数据链路层,用于连接较为相似的网络(例如以太网—以太网);而路由器工作于互联层,可以实现异型网络的互联(例如以太网—帧中继)。

3.2 以太网交换机的工作原理

典型的局域网交换机是以太网交换机。以太网交换机可以通过交换机端口之间的多个并发连接,实现多结点之间数据的并发传输。这种并发数据传输方式与共享式以太网在某一时刻只允许一个结点占用共享信道的方式完全不同。

交换式以太网建立在以太网基础之上。利用以太网交换机组网,既可以将计算机直接连到交换机的端口上,也可以将它们连入一个网段,然后将这个网段连到交换机的端口。图 3-2 利用以太网交换机将两台服务器和两个以太网连成了一个交换式的局域网。如果将计算机直接连到交换机的端口,那么它将独享该端口提供的带宽;如果将以太网

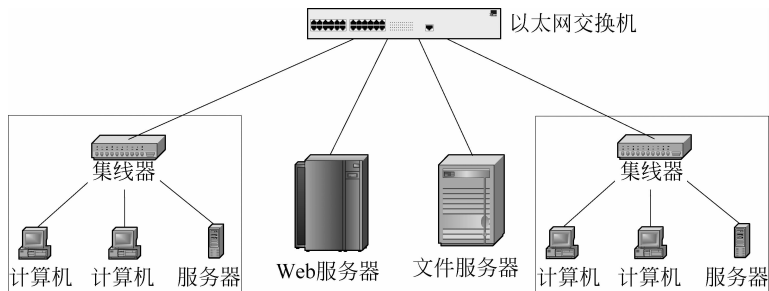


图 3-2 利用交换机连接计算机和以太网

连入交换机,那么该以太网上的所有计算机将共享交换机端口提供的带宽。

3.2.1 以太网交换机的工作过程

典型的交换机结构与工作过程如图 3-3 所示。图中的交换机有 6 个端口,其中端口 1、5、6 分别连接了结点 A、结点 D 和结点 E。结点 B 和结点 C 通过共享式以太网连入交换机的端口 4。于是,交换机“端口/MAC 地址映射表”就可以根据以上端口与结点 MAC 地址的对应关系建立起来。

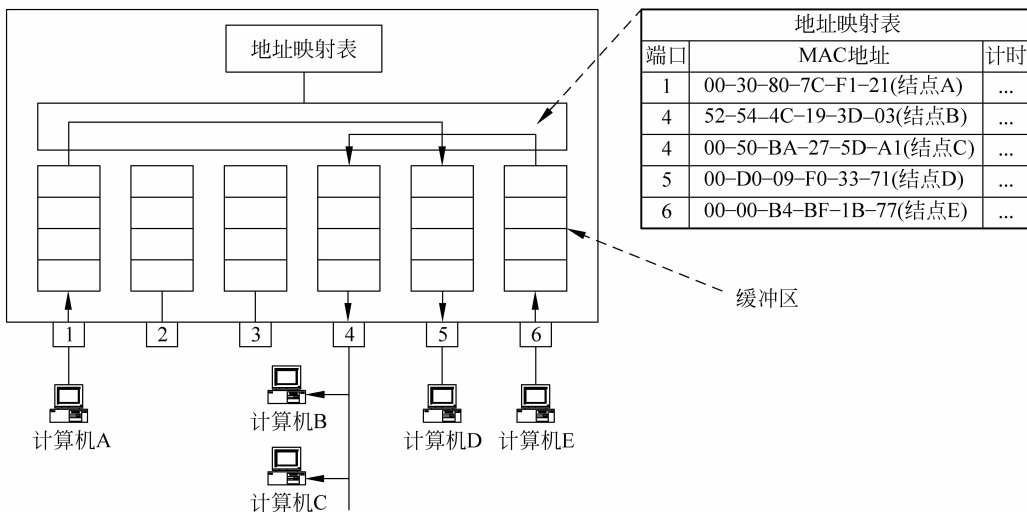


图 3-3 交换机的结构与工作过程

当结点 A 需要向结点 D 发送信息时,结点 A 首先将带有目的地址等于结点 D 的帧发往交换机端口 1。交换机接收该帧,并在检测到其目的地址等于结点 D 后,在交换机的“端口/MAC 地址映射表”中查找结点 D 所连接的端口号。一旦查到结点 D 所连接的端口号 5,交换机将在端口 1 与端口 5 之间建立连接,将信息转发到端口 5。

与此同时,结点 E 需要向结点 B 发送信息。于是,交换机的端口 6 与端口 4 也建立一条连接,并将端口 6 接收到的信息转发至端口 4。

这样,交换机在端口 1 至端口 5 和端口 6 至端口 4 之间建立了两条并发的连接。结点 A 和结点 E 可以同时发送信息,结点 D 和接入交换机端口 4 的以太网可以同时接收信息。根据需要,交换机的各端口之间可以建立多条并发连接。交换机利用这些并发连接,对通过交换机的数据信息进行转发和交换。

3.2.2 数据转发方式

以太网交换机的数据交换与转发方式可以分为直接交换、存储转发交换和改进的直接交换三类。

1. 直接交换

在直接交换方式中,交换机边接收边检测。一旦检测到目的地址字段就立即将该数据转发出去,不管这一数据是否出错。出错检测任务由结点主机完成。这种交换方式的优点是交换延迟时间短,缺点是缺乏差错检测能力,不支持不同输入/输出速率的端口之间的数据转发。

2. 存储转发交换

在存储转发方式中,交换机首先完整地接收站点发送的数据,然后对接收的数据进行差错检测。如果数据接收正确,那么交换机根据目的地址确定输出端口号,将数据转发出去。这种交换方式的优点是具有差错检测能力,能支持不同输入/输出速率端口之间的数据转发,缺点是交换延迟时间相对较长。

3. 改进的直接交换

改进的直接交换方式将直接交换与存储转发交换结合起来,在接收到数据的前64字节之后,判断数据的头部字段是否正确,如果正确则转发出去。这种方法对于短数据来说,交换延迟与直接交换方式比较接近;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,因此交换延迟将会明显减少。

3.2.3 地址学习

以太网交换机利用“端口/MAC地址映射表”进行信息交换,因此端口/MAC地址映射表的建立和维护显得相当重要。一旦地址映射表出现问题,就可能造成信息转发错误。那么,交换机中的地址映射表是怎样建立和维护的呢?

这里有两个问题需要解决:一是交换机怎样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,交换机怎样来维护地址映射表。显然,通过人工建立交换机的地址映射表是不切实际的,交换机应该采用一种策略自动建立地址映射表。

通常,以太网交换机利用“地址学习”法来动态建立和维护端口/MAC地址映射表。以太网交换机的地址学习是通过读取帧的源地址并记录帧进入交换机的端口进行的。当得到MAC地址与端口的对应关系后,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,交换机就将该对应关系添加到地址映射表;如果已经存在,交换机将更新该表项。因此,在以太网交换机中,地址是动态学习的。只要这个结点发送信息,交换机就能捕获到它的MAC地址与其所在端口的对应关系。

在每次添加或更新地址映射表的表项时,添加或更改的表项被赋予一个计时器。这使得该端口与MAC地址的对应关系能够存储一段时间。如果在计时器溢出之前没有再次捕获到该端口与MAC地址的对应关系,该表项将被交换机删除。通过移走过时的或旧的表项,可以使交换机维护好一个精确的和有用的地址映射表。

3.2.4 通信过滤

交换机建立起端口/MAC 地址映射表之后,它就可以对通过的信息进行过滤了。以太网交换机在地址学习的同时还检查每个帧,并基于帧中的目的地址做出是否转发或转发到何处的决定。

图 3-4 显示了两个以太网和两台计算机通过以太网交换机相互连接的示意图。通过一段时间的地址学习,交换机形成了图中所示的端口/MAC 地址映射表。

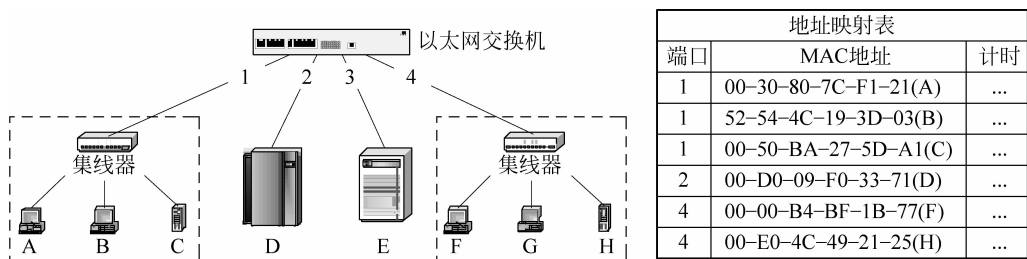


图 3-4 交换机的通信过滤

假设站点 A 需要向站点 F 发送数据,因为站点 A 通过集线器连接到交换机的端口 1,所以交换机从端口 1 读入数据,并通过地址映射表决定将该数据转发到哪个端口。在图 3-4 所示的地址映射表中,站点 F 与端口 4 相连。于是,交换机将信息转发到端口 4,不再向端口 1、端口 2 和端口 3 转发。

假设站点 A 需要向站点 C 发送数据,交换机同样在端口 1 接收该数据。通过搜索地址映射表,交换机发现站点 C 与端口 1 相连,与发送的源站点处于同一端口。遇到这种情况,交换机简单地将数据抛弃,不再进行转发。这样,数据信息被限制在本地流动。

以太网交换机隔离了本地信息,从而避免了网络上不必要的数据流动。这是交换机通信过滤的主要优点,也是它与集线器截然不同的地方。集线器需要在所有端口上重复所有的信号,每个与集线器相连的网段都将听到局域网上的所有信息流。而交换机所连的网段只听到发给它们的信息流,减少了局域网上总的通信负载,因此提供了更多的带宽。

但是,如果站点 A 需要向站点 G 发送信息,交换机在端口 1 读取信息后检索地址映射表,结果发现站点 G 在地址映射表中并不存在。在这种情况下,为了保证信息能够到达正确的目的地,交换机将向除端口 1 之外的所有端口转发信息。当然,一旦站点 G 发送信息,交换机就会捕获到它与端口的连接关系,并将得到的结果存储到地址映射表中。

3.2.5 生成树协议

集线器可以按照水平或树型结构进行级联。但是集线器的级联绝不能出现环路,否则发送的数据将在网中无休止地循环,造成整个网络的瘫痪。那么,图 3-5 所示的具有环

路的交换机级联网络是否可以正常工作呢？答案是肯定的。

实际上,以太网交换机除了按照上面所描述的转发机制对信息进行转发外,还执行一种称为生成树协议(spanning tree protocol)所规定的内容。通过实现生成树协议,交换机可以相互交换连接信息。利用这些信息,交换机将网络中的某些环路断开,从而在逻辑上形成一种树型的结构。交换机按照这种逻辑结构转发信息,保证网络上发送的信息不会绕环旋转。图 3-5 中的具有环路的网络形成的树型无环路逻辑结构如图 3-6 所示。最终,交换机的信息转发是按照这棵树进行的。

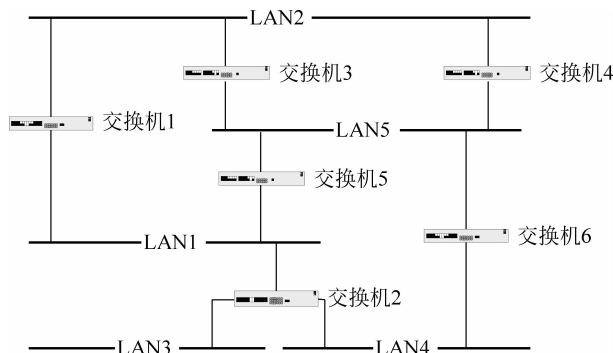


图 3-5 具有环路的交换机级联

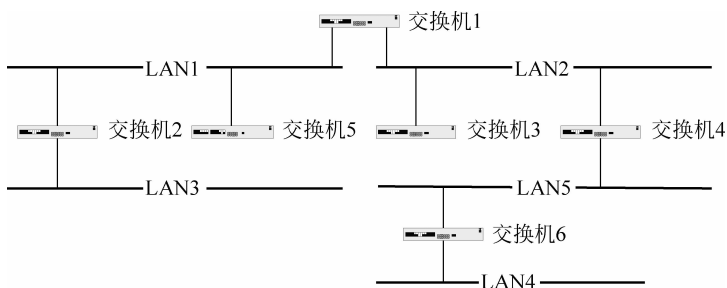


图 3-6 数据转发使用的逻辑树型结构

3.3 虚拟局域网 VLAN

所谓的虚拟局域网(virtual LAN,VLAN)就是将局域网上的用户或结点划分成若干个“逻辑工作组”,逻辑组的用户或结点可以根据功能、部门、应用等因素划分而无须考虑它们所处的物理位置。通常,通过以太网交换机就可以配置 VLAN。

3.3.1 共享式以太网与 VLAN

在传统的局域网中,一个工作组通常处于同一网段,每个网段可以是一个逻辑工作组。多个逻辑工作组之间通过交换机(或路由器)等互联设备交换数据,如图 3-7(a) 所

示。如果一个逻辑工作组的站点仅仅需要转移到另一个逻辑工作组(如从 LAN1 移动到 LAN3),那么需要将该计算机从一个集线器(如楼层 1 的集线器)撤出,连接到另一个集线器(如楼层 3 的集线器),即使它距离楼层 1 的集线器更近。如果一个逻辑工作组的站点(如 LAN1 中的站点)仅仅需要物理位置的移动(如从楼层 1 移动到楼层 3),那么为了保证该站点仍然隶属于原来的逻辑工作组 LAN1,它必须连接至楼层 1 的集线器,即使它连入楼层 3 的集线器更方便。在某些情况下,改变站点的物理位置或逻辑工作组甚至需要重新布线。因此,逻辑工作组的组成受到了站点所在网段物理位置的限制。

虚拟局域网 VLAN 建立在局域网交换机之上,它以软件方式实现逻辑工作组的划分与管理。因此,逻辑工作组的站点组成不受物理位置的限制,如图 3-7(b)所示。同一逻辑工作组的成员可以不必连接在同一个物理网段上。只要以太网交换机是互联的,它们既可以连接在同一个局域网交换机上,也可以连接在不同的局域网交换机上。当一个站点从一个逻辑工作组转移到另一个逻辑工作组时,只需要通过软件设定,而不需要改变它在网络中的物理位置;当一个站点从一个物理位置移动到另一个物理位置时(例如楼层 3 的计算机需要移动到楼层 1),只要将该计算机接入另一台交换机(例如一楼的交换机),通过交换机软件设置,这台计算机还可以成为原工作组的一员。同一个逻辑工作组的站点可以分布在不同的物理网段,但它们之间的通信就像在同一个物理网段一样。

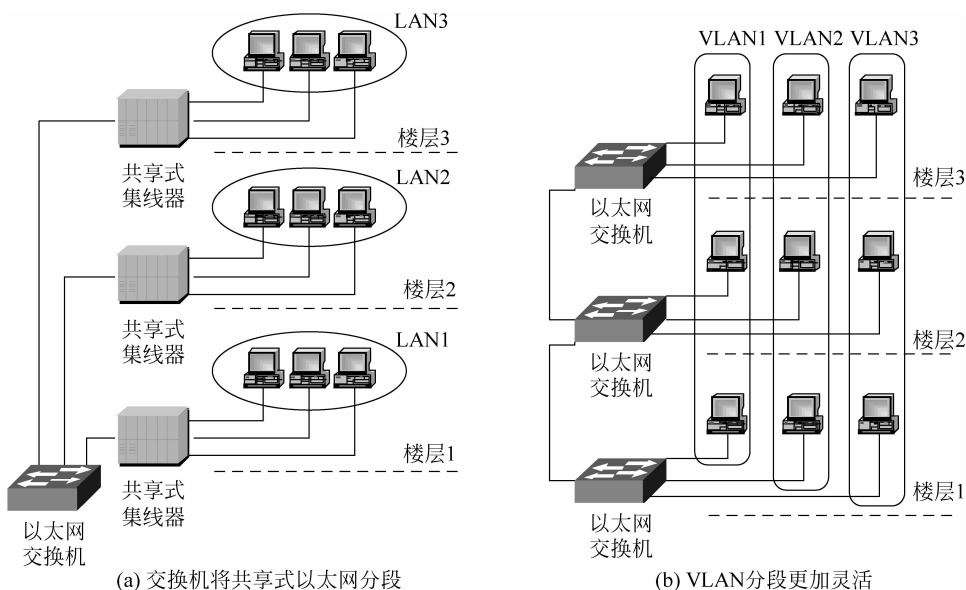


图 3-7 共享式以太网与 VLAN 的比较

3.3.2 VLAN 的组网方法

VLAN 的划分可以根据功能、部门或应用而无须考虑用户的物理位置。以太网交换机的每个端口都可以分配给一个 VLAN。分配给同一个 VLAN 的端口共享广播域(一个站点发送希望所有站点接收的广播信息,同一 VLAN 中的所有站点都可以接收到),分

配给不同 VLAN 的端口不共享广播域,这将全面提高网络的性能。

VLAN 的组网方法包括静态 VLAN、动态 VLAN 两种。

1. 静态 VLAN

静态 VLAN 就是静态地将以太网交换机上的一些端口划分给一个 VLAN。这些端口一直保持这种配置关系直到人工改变它们。

在图 3-8 所示的 VLAN 配置中,以太网交换机端口 1、端口 2、端口 6 和端口 7 组成 VLAN1,端口 3、端口 4、端口 5 组成 VLAN2。

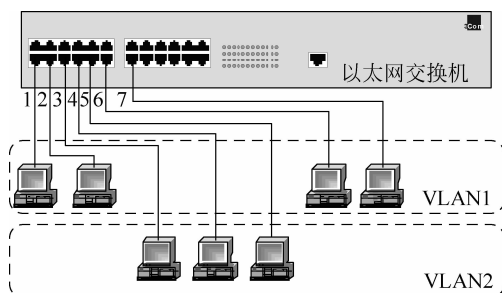


图 3-8 在单一交换机上配置 VLAN

虚拟局域网既可以在单台交换机中实现,也可以跨越多台交换机。在图 3-9 中, VLAN 的配置跨越两台交换机。以太网交换机 1 的端口 2、端口 4、端口 6 和以太网交换机 2 的端口 1、端口 2、端口 4、端口 6 组成 VLAN1,以太网交换机 1 的端口 1、端口 3、端口 5、端口 7 和以太网交换机 2 的端口 3、端口 5、端口 7 组成 VLAN2。

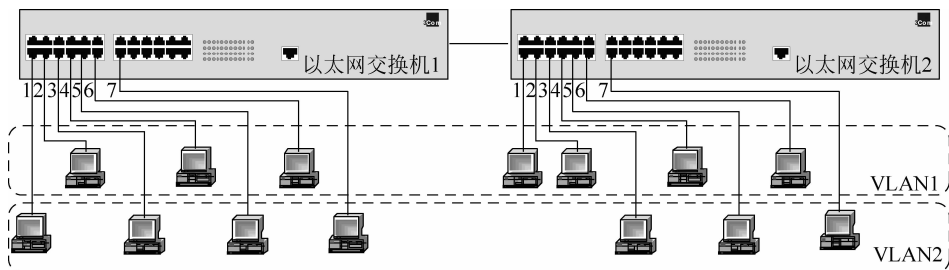


图 3-9 VLAN 可以跨越多台交换机

尽管静态 VLAN 需要网络管理员通过配置交换机软件来改变连接,但它们有良好的安全性,配置简单并可以直接监控,因此很受网络管理员的欢迎。特别是站点设备位置相对稳定时,应用静态 VLAN 是一种最佳选择。

2. 动态 VLAN

所谓的动态 VLAN 是指交换机上 VLAN 端口是动态分配的。通常,动态分配的原则以 MAC 地址、逻辑地址或数据包的协议类型为基础。

如果以 MAC 地址为基础分配 VLAN,网络管理员可以通过指定具有哪些 MAC 地

址的计算机属于哪一个 VLAN 进行配置(例如 MAC 地址为 00-30-80-7C-F1-21、52-54-4C-19-3D-03 和 00-50-BA-27-5D-A1 的计算机属于 VLAN1),不管这些计算机连接到哪个交换机的端口。这样,如果计算机从一个位置移动到另一个位置,连接的端口从一个端口换到另一个端口,只要计算机的 MAC 地址不变(计算机使用的网卡不变),它仍将属于原 VLAN 的成员,不需网络管理员对交换机软件进行重新配置。

3.3.3 VLAN 的优点

1. 减少网络管理开销

部门重组和人员流动是网络管理员最头痛的事情之一,也是管理网络的最大开销之一。在有些情况下,部门重组和人员流动不但需要重新布线,而且需要重新配置网络设备。

VLAN 为控制这些改变和减少网络设备的重新配置提供了一个有效的方法。当 VLAN 的站点从一个位置移到另一个位置时,如果它们还在同一个 VLAN 中并且仍可以连接到交换机端口,那么这些站点本身就无须改变。位置的改变只需简单地将站点插入另一个交换机端口并对该端口进行配置。

2. 控制广播活动

广播在每个网络中都存在。广播的频率依赖于网络应用类型、服务器类型、逻辑段数目及网络资源的使用方法。虽然在过去几年里网络应用被很好地封装以减少它们发送广播包的数量,但是多媒体技术的应用又会不可避免地产生广播和组播。

大量的广播可以形成广播风暴,致使整个网络瘫痪。我们必须采取一些措施来预防广播带来的问题。尽管以太网交换机可以利用端口/MAC 地址映射表减少网络流量,但却不能控制广播数据包在所有端口的传播。VLAN 的使用在保持了交换机良好性能的同时,可以保护网络免受潜在广播风暴的危害。

一个 VLAN 中的广播流量不会传输到该 VLAN 之外,邻近的端口和 VLAN 也不会受到其他 VLAN 产生的任何广播信息,如图 3-10 所示。VLAN 越小,VLAN 中受广播活动影响的用户就越少。这种配置方式大大减少了广播流量,为用户的实际流量释放了带宽,弥补了局域网易受广播风暴影响的弱点。

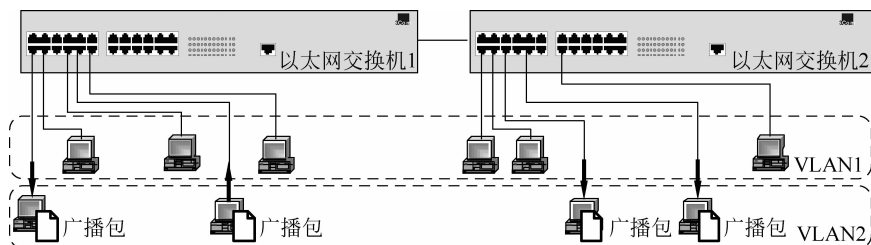


图 3-10 利用 VLAN 限制广播包的传播范围