第 3 章　交换技术及配置

交换技术是局域网中应用最为广泛的一种技术，交换式网络有效解决了共享式网络中存在的碰撞域问题，三层交换技术又成为局域网中子网间通信的最佳解决方案。本章主要围绕交换技术做以下几方面的介绍:

- 二层交换与三层交换
- VLAN 技术
- 链路聚合技术
- 生成树协议
- 交换技术应用案例分析
- 交换机配置

3.1　交换技术概述

局域网交换技术是为解决无法对共享式局域网提供有效的网段划分的问题而出现的，它可以使每个用户尽可能地分享到最大带宽，交换技术出现后得到了快速发展。目前二层交换技术与三层交换技术的应用已成为主流，四层以上交换功能也在一些高性能网络设备上出现。本节主要对二层、三层交换技术进行介绍。

3.1.1　二层交换技术

目前二层交换技术的发展比较成熟，二层交换机属于数据链路层设备，可以识别数据包中的 MAC 地址信息，根据 MAC 地址进行转发，并将这些 MAC 地址与对应的端口记录在自己内部的一个地址表中。具体的工作流程如下：

（1）当交换机从某个端口收到一个数据包时，它读取包头中的源 MAC 地址，这样它就知道源 MAC 地址的机器是连在哪个端口上的。

（2）读取包头中的目的 MAC 地址，并在地址表中查找相应的端口。

（3）如表中有与这个目的 MAC 地址对应的端口，把数据包直接复制到该端口上；如表中找不到相应的端口，则把数据包广播到所有端口上，当目的机器对源机器回应时，交换机又可以学习目的 MAC 地址与哪个端口对应，在下次传送数据时就不需要对所有端口进行广播了。

不断地循环这个过程，二层交换机可学习到全网的 MAC 地址信息，并建立和维护自己的地址表。

从二层交换机的工作原理可以得出以下三点：

（1）由于交换机对多数端口的数据进行同时交换，这就要求交换机具有很宽的交换总线带宽，如果二层交换机有 N 个端口，每个端口的带宽是 M，交换机总线带宽超过 N×M，交

换机就可以实现线速交换。

（2）学习端口连接的机器的 MAC 地址，写入地址表，地址表的大小（一般有两种表示方式：BEFFER RAM 和 MAC 表项数值）影响交换机的接入容量。

（3）二层交换机一般含有专门用于处理数据包转发的 ASIC （Application Specific Integrated Circuit）芯片，因此转发速度非常快。

局域网交换机的引入，使得网络站点间可独享带宽，消除了无谓的碰撞检测和出错重发，提高了传输效率，在交换机中可并行地维护几个独立的、互不影响的通信进程。在交换网络环境下，用户信息只在源结点与目的结点之间进行传送，其他结点是不可见的。但也有例外，如当某一结点在网上发送广播或组播时，或某一结点发送了一个交换机不认识的 MAC 地址的封包时，交换机上的所有结点都将收到这一广播信息。整个交换环境构成一个大的广播域。点到点是在第二层快速、有效地交换，但广播风暴会使网络的效率大打折扣。

3.1.2 三层交换技术

交换机的速度比路由器快得多，而且价格便宜得多。可以说，在网络系统的集成技术中，直接面向用户的第一层接口和第二层交换技术已取得令人满意的使用效果。交换式局域网技术使专用的带宽为用户独享，极大地提高了局域网的传输效率。但第二层交换技术也暴露出弱点：不能有效地解决广播风暴、异种网络互联、安全性控制等问题。作为网络核心、起到网间互联作用的路由器技术没有质的突破。当今绝大部分的企业网都已变成实施 TCP/IP 协议的 Web 技术的内联网，用户的数据往往越过本地网络在网际间传送，因此路由器常常不堪重负。传统的路由器基于软件，协议复杂，与局域网的速度相比，其数据传输效率较低。但同时它又作为网段（子网，VLAN）互联的枢纽，这就使传统的路由器技术面临严峻的挑战。随着 Internet/Intranet 的迅猛发展和 B/S（浏览器/服务器）计算模式的广泛应用，跨地域、跨网络的业务急剧增长，业界和用户深感传统的路由器在网络中的瓶颈效应日益严重，改进传统的路由技术迫在眉睫。其中一种解决方法是安装性能更强的超级路由器，但这样做开销太大，如果是建设交换网，这种投资显然是不合理的。

在这种情况下，一种新的路由技术应运而生，这就是第三层交换技术。第三层交换技术也称为 IP 交换技术、高速路由技术等。第三层交换技术是相对于传统交换的概念提出的。传统的交换技术是在 OSI 网络标准模型中的第二层——数据链路层进行操作的，而第三层交换技术则在网络模型的第三层中实现数据包的高速转发。简单地说，第三层交换技术就是第二层交换技术加第三层转发技术，这是一种利用第三层协议中的信息来加强第二层交换功能的机制。具有第三层交换功能的设备是一个带有第三层路由功能的第二层交换机，它是二者的有机结合，而不是把路由器设备的硬件及软件简单地叠加在局域网交换机上形成的。从硬件的实现上看，目前，第二层交换机的接口模块都是通过高速背板/总线（速率可高达几十 Gb/s）交换数据的。在第三层交换机中，与路由器有关的第三层路由硬件模块也插接在高速背板/总线上，这种方式使得路由模块可以与需要路由的其他模块间高速地交换数据，从而突破了传统的外接路由器接口速率的限制（10Mb/s～100Mb/s）。在软件方面，第三层交换机也有重大举措，它将传统的基于软件的路由器软件进行了界定，其作法是：

（1）对于数据封包的转发，如 IP/IPX 封包的转发，这些有规律的过程通过硬件得以高速实现。

（2）对于第三层路由软件，如路由信息的更新、路由表的维护、路由计算、路由的确定等功能，用优化、高效的软件实现。假设两个使用 IP 协议的站点通过第三层交换机进行通信，发送站点 A 在开始发送时已知目的站点的 IP 地址，但尚不知道在局域网上发送所需要的 MAC 地址。这就需要采用地址解析协议（ARP）来确定目的站点的 MAC 地址。发送站把自己的 IP 地址与目的站的 IP 地址比较，采用其软件中配置的子网掩码提取出网络地址来确定目的站点是否与自己在同一子网内。若目的站点 B 与发送站点 A 在同一子网内，A 广播一个 ARP 请求，B 返回其 MAC 地址，A 得到目的站点 B 的 MAC 地址后将这一地址缓存起来，并用此 MAC 地址封包转发数据，第二层交换模块查找 MAC 地址表确定将数据包发往的目的端口。若两个站点不在同一子网内，如发送站点 A 要与目的站点 C 通信，发送站点 A 要向默认网关发出 ARP（地址解析协议）封包，默认网关的 IP 地址已经在系统软件中设置。这个 IP 地址实际上对应第三层交换机的第三层交换模块。当发送站点 A 对默认网关的 IP 地址广播出一个 ARP 请求时，若第三层交换模块在以往的通信过程中已得到目的站点 C 的 MAC 地址，则向发送站点 A 回复 C 的 MAC 地址；否则第三层交换模块根据路由信息向目的站广播一个 ARP 请求，目的站点 C 得到此 ARP 请求后向第三层交换模块回复其 MAC 地址，第三层交换模块保存此地址并回复给发送站点 A。以后再进行 A 与 C 之间的数据包转发时，将用最终的目的站点的 MAC 地址封包，数据转发过程全部交给第二层交换处理，信息得以高速交换。

第三层交换具有以下突出特点：

（1）有机的硬件结合使得数据交换加速。

（2）优化的路由软件使得路由过程效率提高。

（3）除了必要的路由决定过程外，大部分数据转发过程由第二层交换处理。

（4）多个子网互联时只是与第三层交换模块的逻辑连接，不像传统的外接路由器那样需要增加端口，保护了用户的投资。

第三层交换的目标是，只要在源地址和目的地址之间有一条更为直接的第二层通路，就不经过路由器转发数据包。第三层交换使用第三层路由协议确定传送路径，此路径可以只用一次，也可以存储起来供以后使用，之后数据包通过一条虚电路绕过路由器快速发送。第三层交换技术的出现，解决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，解决了传统路由器因低速、复杂所造成的网络瓶颈问题。当然，第三层交换技术并不是网络交换机与路由器的简单叠加，而是二者的有机结合，从而形成一个集成的完整的解决方案。

传统的网络结构对用户应用所造成的限制，正是第三层交换技术要解决的关键问题。目前，市场上最高档路由器的最大处理能力为每秒 25 万个包，而最高档交换机的最大处理能力在每秒 1000 万个包以上，二者相差 40 倍。在交换网络中，尤其是大规模的交换网络中，没有路由功能是不可想象的。然而路由器的处理能力又限制了交换网络的速度，这就是第三层交换机要解决的问题。第三层交换机并没有像其他的二层交换机那样把广播封包扩散，第三层交换机之所以叫三层交换机是因为它们能看得懂第三层的信息，如 IP 地址、ARP 等。因此，三层交换机能洞悉某广播封包的目的何在，在没有把它扩散出去的情形下，满足了发出该广播封包的用户的需要（不管他们何子网里）。如果认为第三层交换机就是路由器，那也应称为超高速反传统路由器，因为第三层交换机没做任何“拆打”数据封包的工作，所有路过它的封包都不会被修改，并以交换的速度传到目的地。目前，第三层交换机距离成熟还有很长的路，像其他一些新技术一样，还有待进行其协议的标准化工作。目前很多厂商都宣称开发出了第三层交

换机，但经国际权威机构测试，各厂商的作法各异且不同第三层交换机的性能表现不同。另外，可能是基于各厂商占领市场的策略，目前的第三层交换机主要可交换路由 IP/IPX 协议，还不能处理其他一些有一定应用领域的专用协议。因此，有关专家认为，第三层交换技术是将来的主要网络集成技术，传统的路由器在一段时间内还会得以应用，但它将处于其力所能及的位置，那就是处于网络的边缘，进行速度受限的广域网互联、安全控制（防火墙）、专用协议的异构网络互联等。

3.2 VLAN 技术

VLAN（Virtual Local Area Network）即虚拟局域网，它是一种将局域网内的设备逻辑地而不是物理地划分成一个个网段的技术。这里的网段仅仅是逻辑网段的概念，而不是真正的物理网段。可以简单地将 VLAN 理解为是在一个物理网络上被逻辑地划分出来的逻辑网络。

VLAN 相当于 OSI 参考模型的第二层的广播域，能够将广播风暴控制在一个 VLAN 内部，划分 VLAN 后，由于广播域的缩小，网络中广播包消耗带宽所占的比例大大降低，网络的性能得到显著提高。不同的 VLAN 之间的数据传输通过网络层的路由来实现，因此使用 VLAN 技术，结合数据链路层和网络层的交换或路由设备可搭建安全可靠的网络。VLAN 与普通局域网最基本的差异体现在：VLAN 并不局限于某一网络或物理范围，VLAN 中的用户可以位于一个园区的任意位置，甚至位于不同的国家。可以根据网络用户的位置、作用、部门或根据网络用户所使用的应用程序和协议进行分组，网络管理员通过控制交换机的每个端口来控制网络用户对网络资源的访问，同时，VLAN 和第三层、第四层的交换的结合使用能够为网络提供较好的安全措施。

3.2.1 VLAN 产生的原因

既然物理 LAN 可以解决计算机互联通信问题，为什么还要在物理 LAN 上划分 VLAN 呢？原因有以下几个：

（1）基于网络性能的考虑。在传统的共享以太网和交换式以太网中，所有用户在同一个广播域内，会引起网络性能的下降，浪费可贵的带宽，而且对广播风暴的控制和网络安全只能在第三层设备上实现。VLAN 的划分可在第二层上限制广播范围，为解决冲突域、广播域及带宽问题提供了很好的解决方案。

（2）安全管理方面的需要。在一个网络中，由于地理位置和部门不同，对网络中相应的数据和资源就有不同的权限要求，如财务和人事部门的数据就不允许其他部门的人员看到或侦听到，以提高数据的安全性。在普通的二层设备上无法实现广播帧的隔离，只要人员在同一个基于二层的网络内，数据、资源就有可能不安全。利用 VLAN 技术限制不同工作组间的用户在二层之间互访，可很好地解决这个问题。

（3）基于组织结构的考虑。VLAN 的实施是通过软件实现的，因此，无需为改动计算机的逻辑关系而更改网络的布线和拓扑结构。VLAN 技术允许网络管理者将一个物理的 LAN 逻辑地划分为不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，同一 VLAN 内的各个工作站无需被放置在同一个物理空间里，只要按照不同部门划分，就可以满足在大中小型企业和校园网中避免地理位置的限制来实现组织结构的合理化分布。

从图 3-1 中可以看到工程部的 PC1、PC2、PC3 三台主机属于不同的楼层，在物理位置上并不相邻，但可通过划分 VLAN 使得它们成为同一个虚拟局域网的成员，从而达到信息共享的目的，而同楼层的其他主机反而不能直接通信。

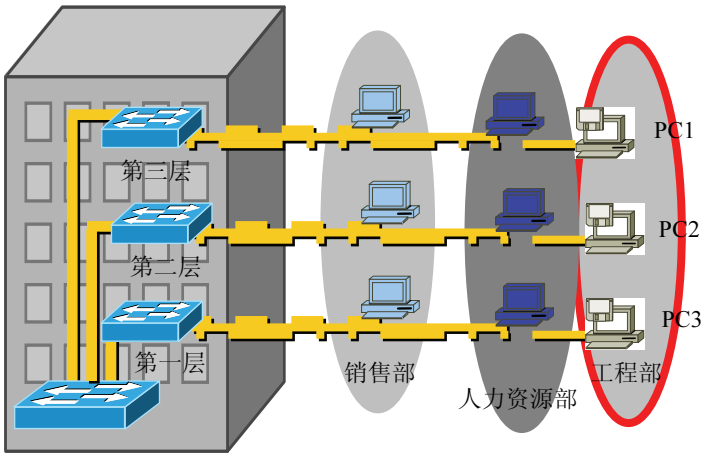
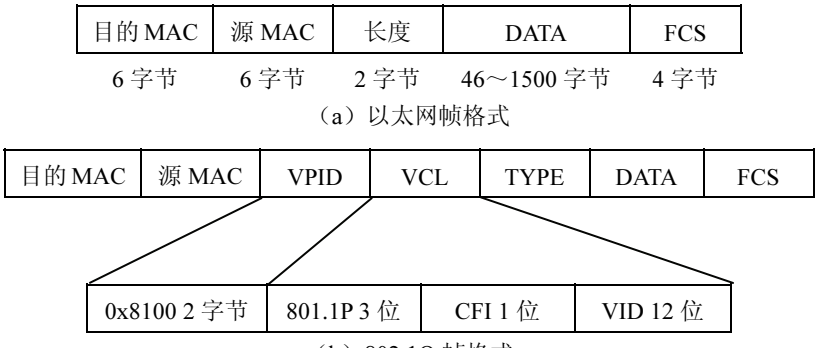


图 3-1　划分 VLAN 的局域网

3.2.2　VLAN 标准

1988 年 IEEE 批准了 802.3ac 标准，这个标准定义了以太网的帧格式的扩展，以便支持虚拟局域网。虚拟局域网允许在以太网的帧格式中插入一个 4 字节的标识符，称为 VLAN 标记（tag），用来指明发送该帧的工作站属于哪一个虚拟局域网。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

VLAN 标记字段的长度是 4 字节，插入在以太网 MAC 帧的源地址字段和长度/类型字段之间，如图 3-2 所示。VLAN 标记的前两个字节和原来的长度/类型字段的作用是一样的，但它总是设置为 0x8100，称为 802.1Q 标记类型。当数据链路层检测到 MAC 帧的源地址字段后面的长度/类型字段的值是 0x8100 时，就知道现在插入了 4 字节的 VLAN 标记。于是就接着检查后两个字节的内容。在后面的两个字节中，前 3 位是用户优先级字段，接着的 1 位是规范格式指示符 CFI，最后的 12 位是 VLAN 标识符 VID（VLAN ID），它唯一地标志了这个以太网帧属于哪一个 VLAN。



（a）以太网帧格式

（b）802.1Q 帧格式

图 3-2　以太网帧格式与 802.1Q 帧格式

3.2.3 VLAN 的划分方法

从概念上讲，可以根据各种分组规则划分 VLAN。但是，得到实际应用的分组规则包括三个，分别为：基于端口分类、基于 MAC 地址分类和基于 IP 地址分类。

1. 基于端口的 VLAN

根据 LAN 成员位于的交换机的端口进行分组，这样得到的 VLAN 称为基于端口的 VLAN。

基于端口的 VLAN 是划分虚拟局域网最简单、最有效的方法，也是最广泛使用的方法，它实际上是某些交换端口的集合，网络管理员只需要管理和配置交换端口，而不管交换机端口连接什么设备。这种划分方式的优点是定义 VLAN 成员时非常简单，只需对端口进行定义，缺点是如果某 VLAN 的用户离开了原来的端口，则需重新定义。基于端口的 VLAN 如图 3-3 所示。

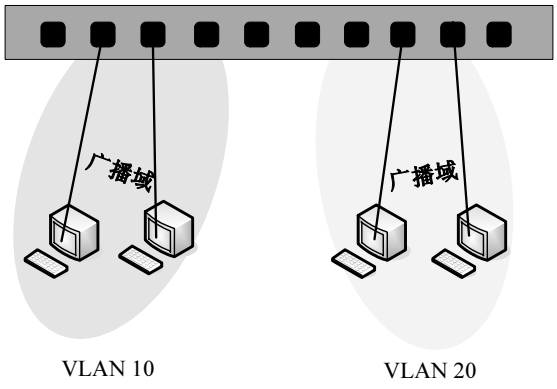


图 3-3 基于端口的 VLAN

2. 基于 MAC 地址的 VLAN

根据计算机网络接口的 MAC 地址进行分组，这样得到的 VLAN 称为基于 MAC 地址的 VLAN。

这种划分 VLAN 的方法根据每个主机的 MAC 地址来进行，即对每个 MAC 地址的主机都要配置它属于哪个组。这种划分 VLAN 的方法的最大优点是当用户的物理位置移动时，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，配置起来是非常累的。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，他们的网卡可能经常更换，这样，VLAN 就必须不停地配置。

3. 基于 IP 地址的 VLAN

根据与计算机网络接口卡关联的 IP 地址进行分组，这样得到的 VLAN 称为基于 IP 地址的 VLAN。

这种方法的优点是用户的物理位置改变了，不需要重新配置所属的 VLAN。而且这种方法不需要附加的帧标签来识别 VLAN，这样可以减少网络的通信量。缺点是效率低，因为检

查每个数据包的网络层地址是需要消耗处理时间的（相对于前两种方法），一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查 IP 帧头，则需要更高的技术，同时也更费时。

3.2.4　VLAN 内及 VLAN 间的通信

1. VLAN 内的通信

（1）Port VLAN 成员端口间的通信。Port VLAN 是基于端口的 VLAN，交换机的端口属性为 access 模式，一个交换机端口仅属于一个 VLAN，处于同一 VLAN 内的端口之间才能相互通信。如图 3-4 所示，在二层交换机上划分的端口 F0/1、F0/2 属于 VLAN 1，端口 F0/3 属于 VLAN 2。VLAN 1 和 VLAN 2 各自所属的端口间通信方式和一般的交换机一样，在未建立完整的 MAC 地址表之前，就将该帧广播到 VLAN 的各个端口上，只有目的地的工作站接受数据帧，其他端口则丢弃，同时交换机维护更改 MAC 地址表。这里的 VLAN 1 和 VLAN 2 之间是不能交换数据的。等交换机建立完整的 MAC 地址表后，相同 VLAN 中的成员端口之间交换数据可直接按地址对应的端口转发，而不必再将数据帧广播出去。

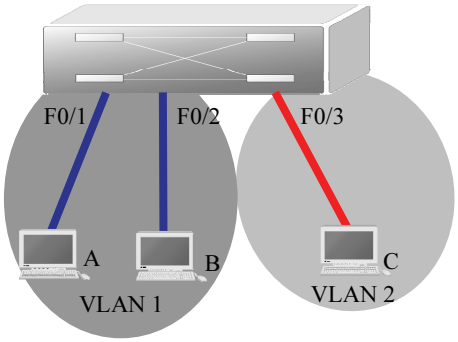


图 3-4　Port VLAN 成员端口间的通信

（2）Tag VLAN 成员端口间的通信。Port VLAN 只能实现在同一交换机上划分 VLAN，而 802.1Q 协议使跨交换机的相同 VLAN 端口间的通信成为可能。基于 802.1Q 的 Tag VLAN 用 VID 来划分不同的 VLAN，交换机的端口被划分为两种模式，一种为 access 模式，一种为 Trunk 模式，Trunk 端口属于所有 VLAN。在交换机之间用一条级联线，并将对应的端口设置为 Trunk，这条线路就可以承载交换机上所有 VLAN 的信息。Trunk 端口传输多个 VLAN 的信息，实现同一 VLAN 跨越不同的交换机。

当数据帧通过交换机时，交换机根据帧中 Tag 头（Tag Header）的 VID 信息来识别它们所在的 VLAN（如果帧中无 Tag 头，则根据帧所通过端口的默认 VID 信息来识别它们所在的 VLAN），这使得所有属于该 VLAN 的数据帧，不管是单播帧、多播帧还是广播帧，都将限制在该逻辑 VLAN 中传播。这将使组中主机相互之间能够通信，而不受其他主机的影响，如图 3-5 所示。

2. VLAN 之间的通信

VLAN 的划分是在二层设备也即二层交换机上实现的，但 VLAN 之间的通信要借助于三层网络设备即路由器或三层交换机实现。

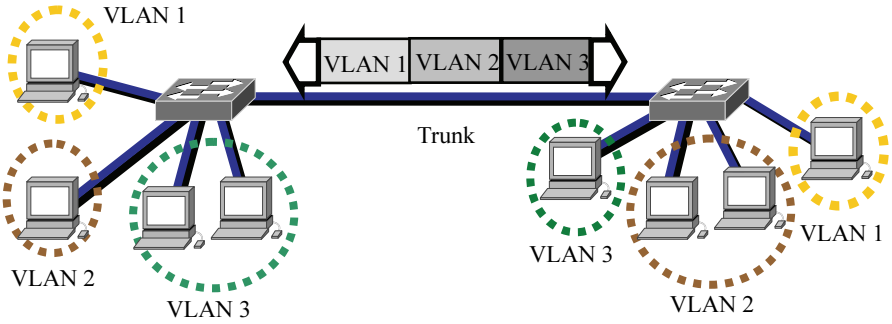


图 3-5　Tag VLAN 成员端口间的通信

（1）利用路由器实现 VLAN 间的通信。

在使用路由器进行 VLAN 间的路由时，与构建横跨多台交换机的 VLAN 时的情况类似，还会遇到该如何连接路由器与交换机的问题。当每个交换机上只有一个 VLAN 时，路由器和交换机的接线方式如图 3-6 所示，只需在路由器上设置路由就可以实现 3 个 VLAN 之间的通信。

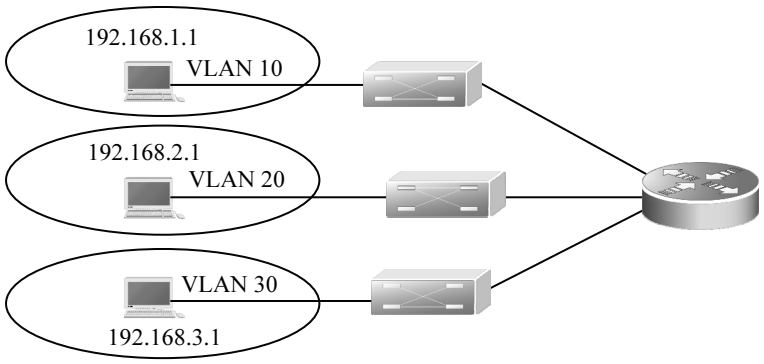


图 3-6　利用路由器实现 VLAN 间的通信

当每个交换机上有多个 VLAN 时，与路由器的连接方法大致有以下两种：

- 将路由器与交换机以 VLAN 为单位分别用网线相连。将交换机上用于和路由器互连的每个端口设为访问链接，然后分别用网线与路由器上的独立端口互连，如图 3-7 所示。

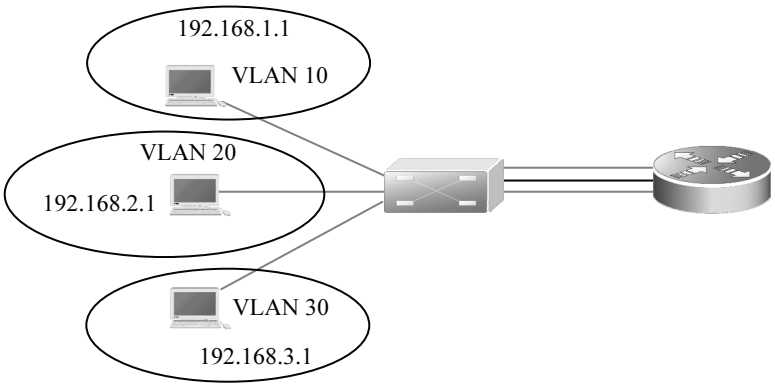


图 3-7　利用路由器实现 VLAN 间的通信

图 3-7 中的交换机上有 3 个 VLAN，就需要在交换机上预留 3 个端口用于与路由器互连，路由器上同样需要有 3 个端口，两者之间用 3 条网线分别连接。所以用这种方法，每增加一个新的 VLAN 都需要加设 1 个端口，两者之间用 1 条网线分别连接。每增加一个新的 VLAN，都需要消耗路由器的端口和交换机的访问链接，而且需要重新布设一条网线。而路由器，通常不会带有太多的 LAN 端口。新建 VLAN 时，为了对应增加 VLAN 所需的端口，就必须将路由器升级成带有多个 LAN 端口的高端产品，成本很高，且重新布线也会带来开销，所以这种方法不实用。

- 单臂路由解决思想。此方法使用一条链路连接多个 VLAN，通过在一个链路接口上划分子接口的技术来解决 VLAN 间通信问题。不论 VLAN 数目多少，都只用一条网线连接路由器与交换机，这需要用到干道链路。首先将用于连接路由器的交换机端口设为干道链路，路由器上的端口也必须支持干道链路，用于干道链路的协议必须相同。然后在路由器上定义对应各个 VLAN 的子接口（Sub Interface）。尽管实际上与交换机连接的物理端口只有一个，但在理论上可以把它分割为多个分别对应各个 VLAN 的虚拟端口（SVI），作为各个 VLAN 成员的网关。这样各个 VLAN 之间就可以利用路由器来实现数据交换了。单臂路由连接方法如图 3-8 所示。

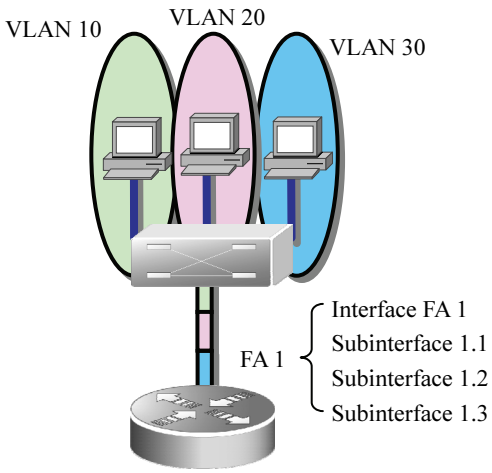


图 3-8　单臂路由连接方法

（2）利用三层交换机实现 VLAN 间的通信。

利用三层交换机的路由功能也可以实现 VLAN 间的通信，使用三层交换接口实现 VLAN 间的路由通信，可以使交换接口的成本大大降低。

在如图 3-9 所示的拓扑结构中，在二层交换机上分别划分 VLAN 10 和 VLAN 20，VLAN 10 的工作站的 IP 地址为 192.168.1.1；VLAN 20 的工作站的 IP 地址为 192.168.2.1。在三层交换机上创建各个 VLAN 的虚拟接口（SVI），并设置 IP 地址。然后将所有 VLAN 连接的工作站主机的网关指向该 SVI 的 IP 地址。具体操作如下：在三层交换机上划分 VLAN 10 和 VLAN 20，并设置 IP 地址分别为 192.168.1.10 和 192.168.2.10，然后将二层交换机的 VLAN 10 中的工作站网关设为 192.168.1.10，VLAN 20 的工作站网关设为 192.168.2.10。这样就利用三层交换机的虚拟接口（SVI）实现了不同 VLAN 间的通信。

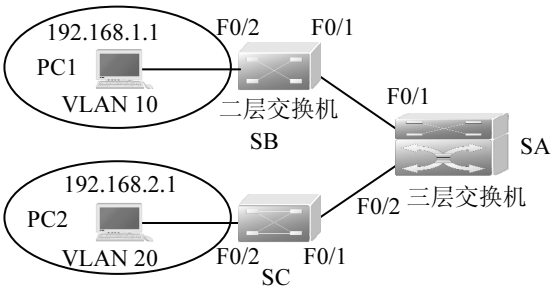


图 3-9　利用三层交换机实现 VLAN 间的通信

3.2.5　实现 VLAN

1. 划分 VLAN

首先，以图 3-4 为例，来看如何在二层交换机上实现 VLAN 划分。假设连接在二层交换机上的三台主机同属于一个 IP 网段 192.16.0.0/24。在不划分 VLAN 的情况下，三台主机之间是可以相互通信的。但现在要使 A 与 B 之间通信，A、B 不能与 C 通信，可以借助基于端口的 VLAN 使其实现。将 F0/1、F0/2 端口划分到 VLAN 1，将 F0/3 端口划分到 VLAN 2，过程分为两步。

第 1 步：创建 VLAN。

```
Switch#configure terminal
Switch(config)#vlan 1                          ! 创建 VLAN（查看 VLAN）
Switch (config-vlan)#exit                      ! 退出 VLAN 设置模式
Switch (config)#vlan 2
Switch(config-vlan)#exit
```

第 2 步：将端口划分到 VLAN 中去。

```
Switch (config)#interface fastethernet 0/1     ! 进入端口配置模式
Switch (config-if)#switchport access vlan 1    ! 将端口划分到 VLAN 中
Switch (config-if)#exit
Switch (config)#interface fastethernet 0/2
Switch (config-if)#switchport access vlan 1
Switch (config-if)#exit
Switch(config)#interface fastethernet 0/3
Switch (config-if)#switchport access vlan 2
Switch (config-if)#exit
```

至此，再次测试三者之间的连通性，会发现 A 与 B 之间可以通信，而 A、B 不能与 C 通信。

2. 实现 VLAN 间通信

3.2.4 节提到 VLAN 间的通信可以借助于三层交换机和路由器完成。使用三层交换机实现 VLAN 通信更为常见，下面以图 3-9 为例，介绍 VLAN 间通信的实现方法。

配置方法分为三步：①划分 VLAN，需在二层交换机端口进行设置；②VLAN 间通信，重点对三层交换机端口与虚拟端口进行设置；③主机配置，重点将主机的网关地址设置为三层交换机的虚拟端口地址。

第 1 步：划分 VLAN。

```
SB(config)#vlan 10
SB(config-vlan)#exit
SB(config)#interface fa 0/2
SB(config-if)#switchport access vlan 10
SB(config-if)#exit
SB(config)#
SB(config)#interface fa 0/1
SB(config-if)#switchport mode trunk
SB(config-if)#exit
SB(config)#
```

SC 以同样的方法设置。

第 2 步：VLAN 间的通信。

首先，将允许各 VLAN 通行的交换机端口设为 Trunk 模式。

```
SA(config)#interface fa 0/1
SA(config-if)#switchport mode trunk
SA(config-if)#exit
SA(config)#
```

交换机的 F0/2 端口同理进行设置。

然后，设置虚拟接口 SVI，使该端口成为各个 VLAN 的网关。

```
SA(config)# interface vlan 10
SA(config-if)# ip address 192.168.1.254 255.255.255.0
SA(config-if)# no shutdown            ！开启端口
SA(config-if)# exit

SA(config)# interface vlan 20
SA(config-if)# ip address 192.168.2.254 255.255.255.0
SA(config-if)# no shutdown
SA(config-if)# exit
```

第三步：配置主机。

配置各主机的 IP 地址、子网掩码、网关。需注意 VLAN 之间的通信需要网关的支持，网关地址即为三层交换机的虚拟端口地址。

3.3　链路聚合技术

3.3.1　链路聚合

在局域网的应用中，由于数据通信量的快速增长，现有的百兆、千兆带宽对于交换机之间或交换机到高需求服务之间的通信往往不够用，如图 3-10 所示，于是出现了将多条物理链路当作一条逻辑链路使用的链路聚合技术，这时网络通信由聚合到逻辑链路中的所有物理链路共同承担。

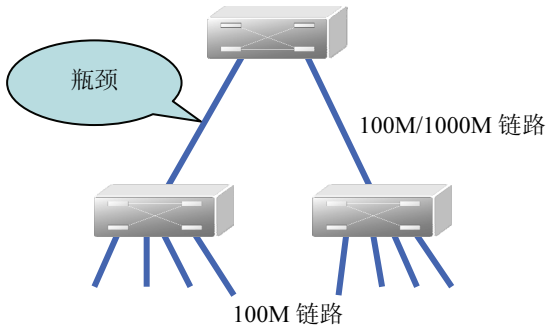


图 3-10　网络带宽存在瓶颈

IEEE 802.3ad 标准定义了将两个以上的千兆位以太网连接组合起来的方法，使高带宽网络连接实现负载共享、负载平衡，同时也提供了更好的可伸缩性服务。在链路聚合技术的支持下，网络传输的数据流被动态地分布到加入链路的各个端口，因此，在聚合链路中自动完成了对实际流经某个端口的数据管理。

把多个物理接口捆绑在一起可以形成一个简单的逻辑接口，这个逻辑接口称为一个 Aggregate Port（以下简称 AP）。AP 是链路带宽扩展的一个重要途径，符合 IEEE 802.3ad 标准。它可以把多个端口的带宽叠加起来使用，如全双工快速以太网端口形成的 AP 的最大带宽可以达到 800Mb/s，千兆以太网端口形成的 AP 的最大带宽可以达到 8Gb/s，如图 3-11 所示。

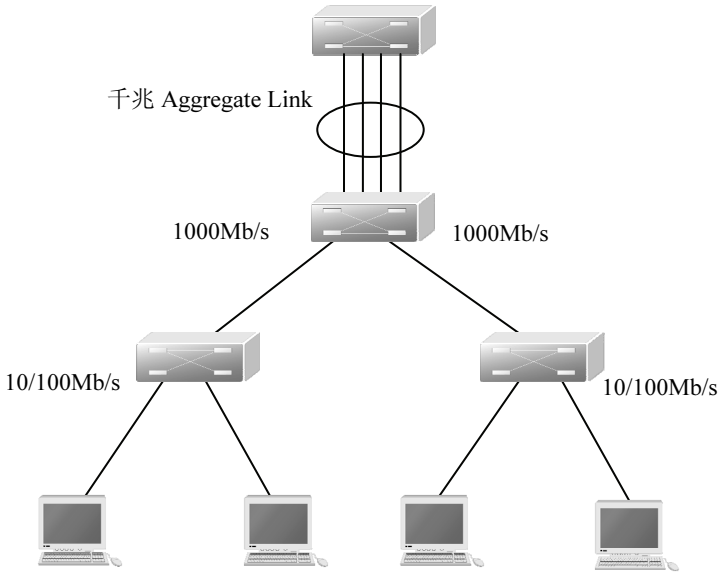


图 3-11　利用链路聚合增大带宽

这项标准适用于 10Mb/s、100Mb/s 和 1000Mb/s 以太网。聚合在一起的链路可以在一条单一的逻辑链路上组合使用上述传输速度，这就使用户在交换机之间有一个千兆端口以及 3 或 4 个 100M 端口时有更多的选择，可以以负担得起的方式逐渐增加带宽。链路聚合的另一个主要优点是可靠性。链路聚合技术在点到点链路上提供了固有的、自动的冗余性。如果链路使用的多个端口中的一个出现故障，网络传输的数据流可以动态地快速转向链路中其他工作正常的端

口进行传输。这种改向速度很快，当交换机得知介质访问控制地址已经被自动地从一个链路端口重新分配到同一链路中的另一端口时，改向就被触发了。然后这台交换机将数据发送到新的端口位置，并且在几乎不中断的情况下，网络得以继续运行。

总之，链路聚合将交换机上的多个端口在物理上连接起来，在逻辑上捆绑在一起形成一个拥有较大宽带的端口，形成一条干路，可以实现均衡负载，并提供冗余链路。

3.3.2　流量平衡

AP 根据报文的 MAC 地址或 IP 地址进行流量平衡，即把流量平均分配到 AP 的成员链路中。流量平衡可以根据源 MAC 地址、目的 MAC 地址或源 IP 地址/目的 IP 地址对进行。

源 MAC 地址流量平衡是指根据报文的源 MAC 地址把报文分配到各个链路中。不同的主机转发的链路不同，同一台主机的报文从同一个链路转发（交换机中学到的地址表不会发生变化）。目的 MAC 地址流量平衡是指根据报文的目的 MAC 地址把报文分配到各个链路中。同一目的主机的报文从同一个链路转发，不同目的主机的报文从不同的链路转发。可以用 Aggregateport Load-Balance 设定流量分配方式。

源 IP 地址/目的 IP 地址对流量平衡是指根据报文源 IP 与目的 IP 进行流量分配。不同的源 IP/目的 IP 对的报文通过不同的链路转发，同一源 IP/目的 IP 对的报文通过相同的链路转发，其他的源 IP/目的 IP 对的报文通过其他的链路转发。该流量平衡方式一般用于三层 AP。在此流量平衡模式下收到的如果是二层报文，则自动根据源 MAC/目的 MAC 对进行流量平衡。

在图 3-12 中，一个 AP 同路由器进行通信，交换机的 MAC 地址只有一个，为了让路由器与其他多台主机通信的流量能被多个链路分担，应设置为根据目的 MAC 进行流量平衡。

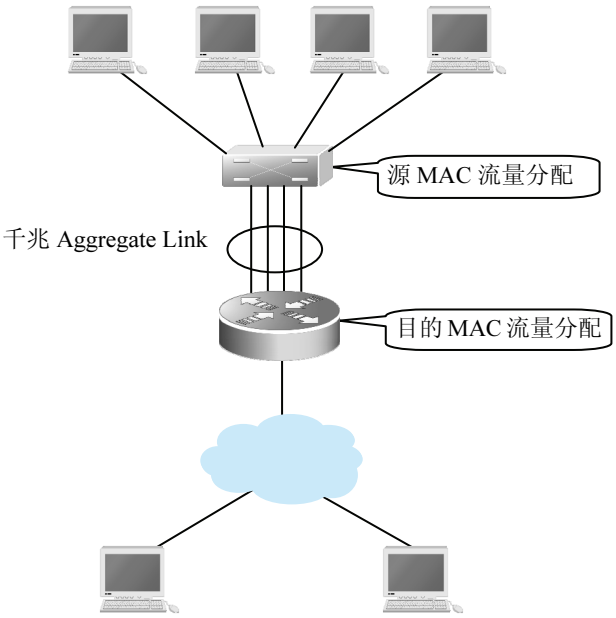


图 3-12　流量平衡

通常应根据不同的网络环境设置合适的流量分配方式，以便能把流量较均匀地分配到各个链路上，充分利用网络的带宽。

3.3.3 链路聚合的实现

链路聚合的实现可分为两步：①在交换机上配置端口聚合；②配置 AP 上的流量平衡算法。下面以图 3-13 为例，介绍链路聚合的具体配置方法。目标是在 SwitchA 与 SwitchB 之间的 F0/1 与 F0/2 端口上配置链路聚合。

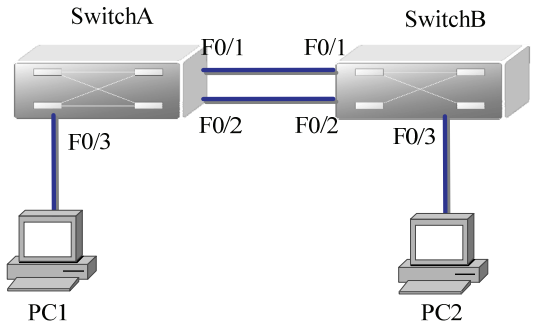


图 3-13 链路聚合拓扑图

首先，在交换机上配置端口聚合。

```
SwitchA(config)#interface aggregateport 1     //建立 ap 1
SwitchA (config-if)#switchport mode trunk     //设置 ap 1 的模式
SwitchA (config-if)#exit
SwitchA (config)#interface range fa 0/1-2     //进入到 0/1-2
SwitchA (config-if-range)#port-group 1        //配置 0/1-2 属于 ap 1
```

配置完后，看是否配置成功，用以下命令：

```
SwitchA (config-if-range)#show aggregateport 1 s     //查看
```

显示结果如下：

```
AggregatePort     MaxPorts     SwitchPort     Mode          Ports
-----------------  ----------  -------------  ----------    ---------------
AP1                4           Enabled        TRUNK         Fa0/1,Fa0/2
```

然后，配置 AP 上的流量平衡算法。

```
SwitchA (config)#aggregateport load-balance src-dst-mac
```

配置第二台交换机 SwitchB 的步骤是相同的。

经过测试，PC1 和 PC2 之间的一条线路断开后，两台计算机之间仍然可以通信。

若想删除 Ap1，使用以下命令：

```
SwitchA (config)#no interface aggregateport 1
```

3.4 生成树协议

3.4.1 交换网络中的冗余链路

在许多交换机或交换机设备组成的网络环境中，通常都会使用一些备份连接以提高网络的健壮性、稳定性。备份连接也称备份链路、冗余链路等。备份连接如图 3-14 所示，交换机

SW1 与交换机 SW3 的端口 1 之间的链路就是一个备份连接。在主链路（SW1 与 SW2 之间的链路或 SW2 到 SW3 之间的链路）出故障时，备份链路自动启用，从而提高网络的整体可靠性。

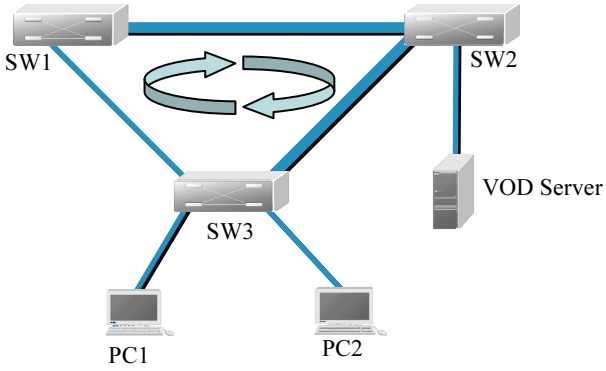


图 3-14　备份链路使网络存在环路

使用冗余链路能够为网络带来健壮性、稳定性和可靠性等好处，但是备份链路使网络存在环路。SW1-SW2-SW3 就是一个环路，环路是备份链路面临的最为严重的问题，环路将会导致广播风暴、多帧复制及 MAC 地址表的不稳定等问题。

（1）广播风暴。在一些较大型的网络中，当大量广播流（如 MAC 地址查询信息）同时在网络中传播时，就会发生数据包的碰撞。网络试图缓解这些碰撞并重传更多的数据包，结果导致全网的可用带宽减少，并最终使网络失去连接而瘫痪，这一过程称为广播风暴。

通常交换机对网络中的广播信息不会进行任何数据过滤，因为这些地址帧的信息不会出现在 MAC 层的源地址字段中。交换机总是直接将这些信息广播到所有端口，如果网络中存在环路，这些广播信息将在网络中不停地转发，直到导致交换机出现超负荷运转（如 CPU 过度使用，内存耗尽等）为止，最终将耗尽所有带宽资源、阻塞全网通信。

（2）多帧复制。如果网络中存在环路，目的主机可能会收到某个数据帧的多个副本，此时会导致上层协议在处理这些数据帧时无从选择，产生迷惑，不知道究竟该处理哪个帧。严重时还可能导致网络连接的中断。

（3）MAC 地址表的不稳定。当交换机连接不同网段时，将会出现通过不同端口接收到同一个广播帧的多个副本的问题。这一过程也会同时导致 MAC 地址表的多次刷新。这种持续的更新、刷新过程会严重耗费内存资源，影响该交换机的交换能力，同时降低整个网络的运行效率。严重时，将消耗掉整个网络资源，并最终造成网络瘫痪。

从以上可以看出，虽然备份链路带来许多好处，但同时环路的出现也带来了许多问题。所以在实际的局域网通信中，冗余链路的意思是准备两条以上的链路，当主链路不通时才启用备份链路。

3.4.2　生成树协议

为了解决冗余链路引起的问题，IEEE 通过了 IEEE 802.1d，即生成树协议。IEEE 802.1d 协议通过在交换机上运行一套复杂的算法使冗余端口置于“阻塞状态”，使得网络中的计算机在通信时只有一条链路生效，当这个链路出现故障时，IEEE 802.1d 协议将会重新计算出网络的最优链路，将处于阻塞状态的端口重新打开，从而确保网络连接稳定可靠。生成树协议和其

他协议一样，是随着网络的不断发展而不断更新换代的。在生成树协议的发展过程中，旧的缺陷不断被克服，新的特性不断被开发出来。一般可以把生成树协议的发展过程划分为三代。

- 第一代生成树协议：STP/RSTP。
- 第二代生成树协议：PVST/PVST+。
- 第三代生成树协议：MISTP/MSTP。

下面对第一代生成树协议（STP/RSTP）做详细介绍。

1. 生成树协议——IEEE 802.1d

生成树协议（Spanning Tree Protocol，STP）最初是由美国数字设备公司（Digital Equipment Corporation，DEC）开发的，后经电气电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）进行修改，最终制定了相应的 IEEE 802.1d 标准。STP 的主要功能是为了解决由于备份链路所产生的环路问题。

STP 的主要思路是当网络中存在备份链路时，只允许主链路激活，如果主链路因故障而被断开，备用链路才会被打开。STP 检测到网络上存在环路时，自动断开环路链路。当交换机间存在多条链路时，交换机的生成树算法只启动最主要的一条链路，而将其他链路都阻塞掉，将这些链路变为备用链路。当主链路出现问题时，生成树协议将自动启用备用链路接替主链路的工作，不需要任何人工干预。众所周知，自然界中生长的树是不会出现环路的，如果网络也能够像一棵树一样生长就不会出现环路。于是，STP 中定义了根交换机（Root Bridge）、根端口（Root Port）、指定端口（Designated Port）和路径开销（Path Cost）等概念，目的就在于通过构造一棵自然树的方法达到阻塞冗余环路的目的，同时实现链路备份和路径最优化。用于构造这棵树的算法称为生成树算法（Spanning Tree Algorithm，SPA）。

（1）STP 的基本概念。

要实现这些功能，交换机之间必须进行一些信息交流，这些信息交流单元就称为桥协议数据单元（Bridge Protocol Data Unit，BPDU）。STP BPDU 是一种二层报文，目的 MAC 是组播地址 01-80-C2-00-00-00，所有支持 STP 的交换机都会接收并处理收到的 BPDU 报文。该报文的数据区中携带了用于生成树计算的所有有用信息。包括：

- Bridge ID：每个交换机唯一的桥 ID，由桥优先级和端口号组成。
- Root Path Cost：交换机到根交换机的路径花费，以下简称根路径花费。
- PortID：每个端口的 ID，由端口优先级和端口号组成。
- BPDU：交换机之间通过交换 BPDU 帧来获得建立最佳树拓扑结构所需要的信息。这些帧以组播地址 01-80-C2-00-00-00 为目的地址。

每个 BPDU 由以下要素组成：

- Root Bridge ID：本交换机所认为的根交换机 ID。
- Root Path Cost：本交换机的根路径花费。
- Bridge ID：本交换机的桥 ID。
- Port ID：发送该报文端口的 ID。
- Message age：报文已存活的时间。
- Forward-Delay Time、Hello Time、Max-Age Time：三个协议规定的时间参数。

其他还有一些诸如表示发现网络拓扑变化、本端口状态的标志位。

当交换机的一个端口收到高优先级的 BPDU 时，在该端口保存这些信息，同时向所有端

口更新并传播信息。如果收到比自己低优先级的 BPDU，交换机就丢弃该信息。

这样的机制就使高优先级的信息在整个网络中进行传播，BPDU 的交流就有了下面的结果：

- 网络中选择了一个交换机作为根交换机（Root Bridge）。
- 除根交换机外的每个交换机都有一个根端口（Root Port），即提供最短路径到 Root Bridge 的端口。
- 每个交换机都计算出了到根交换机（Root Bridge）的最短路径。
- 每个 LAN 都有了指定交换机（Designated Bridge），位于该 LAN 与根交换机之间的最短路径中。指定交换机和 LAN 相连的端口称为指定端口（Designated Port）。
- 根端口（Root Port）和指定端口（Designated Port）进入转发（Forwarding）状态。
- 其他的冗余端口处于阻塞状态（Blocking State）。

（2）STP 的工作过程。

STP 的工作过程如图 3-15 所示。

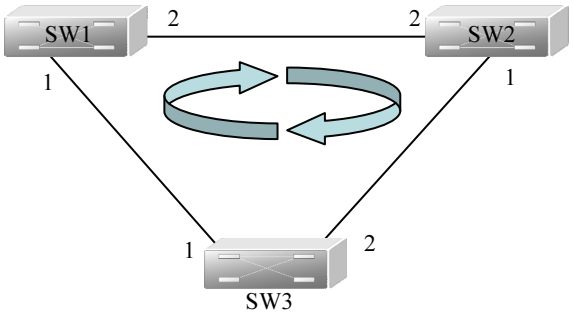


图 3-15　STP 的工作过程

首先进行根交换机的选举。选举依据是交换机优先级和交换机 MAC 地址组合成的桥 ID，桥 ID 最小的交换机将成为网络中的根交换机。在如图 3-14 所示的网络中，各交换机都以默认配置启动，在交换机优先级都一样（默认优先级为 32768）的情况下，MAC 地址最小的交换机成为根交换机，例如图 3-15 中的 SW1，它所有端口的角色都成为指定端口，进入转发状态。

然后，其他交换机将各自选择一条“最粗壮”的树枝作为到根交换机的路径，相应端口的角色就成为根端口。假设图 3-15 中的 SW2 和 SW1、SW3 之间的链路是千兆 GE 链路，SW1 和 SW3 之间的链路是百兆 FE 链路，SW3 从端口 1 到根交换机的路径开销的默认值是 19，而从端口 2 经过 SW2 到根交换机的路径开销是 4+4=8，所以端口 2 成为根端口，进入转发状态。同理，SW2 的端口 2 成为根端口，端口 1 成为指定端口，进入转发状态。

计算路径开销时，路径开销以时间为单位，如图 3-16 所示。计算标准如下：

带宽	IEEE 802.1d	IEEE 802.1w
10Mb/s	100	2000000
100Mb/s	19	200000
1000Mb/s	4	20000

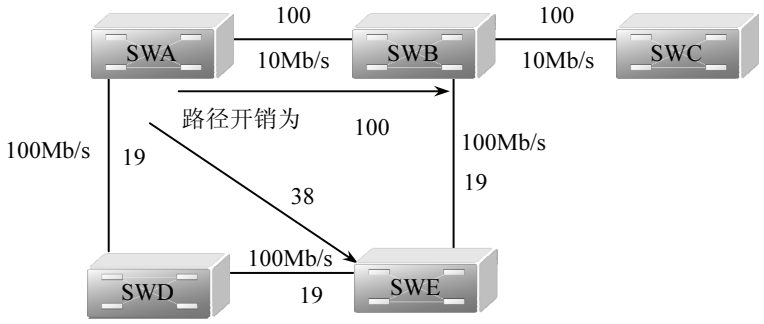


图 3-16　路径开销计算

根交换机和根端口都确定后一棵树就生成了，如图 3-17 中实线所示。下面的任务是裁剪冗余的环路。这个工作是通过阻塞非根交换机上的相应端口实现的，例如 SW3 的端口 1 的角色成为禁用端口，进入阻塞状态（如图中用“×”表示）。

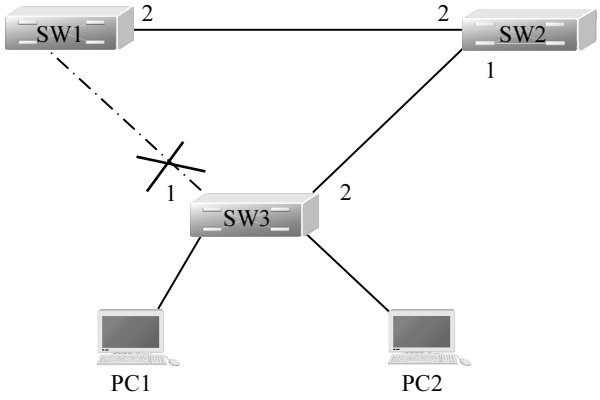


图 3-17　裁剪冗余的环路

（3）生成树的比较规则。

生成树的选举过程中，应遵循以下优先顺序选择最佳路径：

①比较 Root Path Cost；

②比较 Sender’s Bridge ID；

③比较 Sender’s Port ID；

④比较本交换机的 Port ID。

比较方法如图 3-18 所示。在图中，SWD 交换机为根交换机，假设图 3-18 中的所有链路均为百兆链路，且交换机均采用默认优先级 32768 和默认端口优先级 128。选择 C-ROOT 的最佳路径的步骤：因为交换机 A、B 的路径开销相等，比较交换机的 Root Path Cost，也就是 C-A-ROOT 和 C-B-ROOT 的路径开销，可以得知相等；比较交换机的 Sender’s Bridge ID，即比较发送给 C“BPDU”信息的交换机 A 与交换机 B 的 Bridge ID，由图 3-18 可知，A 的 Bridge ID 小于 B 的 Bridge ID，故 C 的 8 端口成为根端口，而与 B 相连的端口被阻塞掉，最佳路径为 C-A-ROOT。

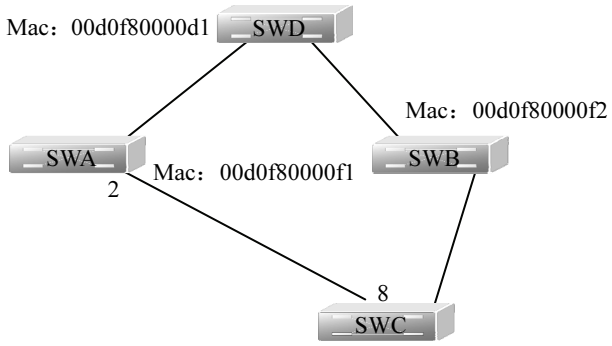


图 3-18　生成树的比较规则

如图 3-19 所示，如果交换机 A 与交换机 C 间增加了一条备份链路，而给 C 发送 BPDU 信息的都是 A，这时就要比较 Sender’s Port ID 了，由于端口 1 与端口 2 的优先级相同（均为默认值），而编号为 1 的端口号更小更优先，故 C 的端口 7 成为根端口，端口 8 被阻塞掉，则最佳路径为 C-7-1-A-ROOT。

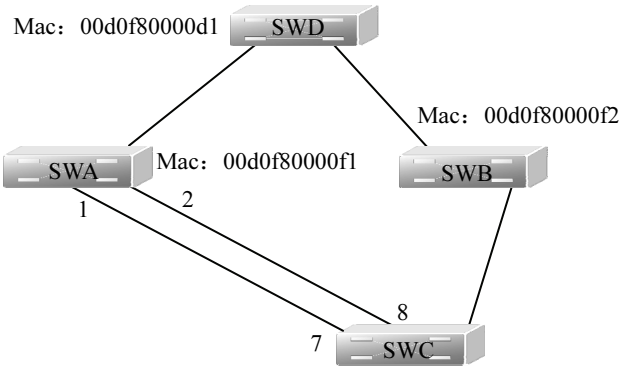


图 3-19　交换机 A 与 C 间增加一条备份链路

如图 3-20 所示，如果交换机 A、C 之间增加了一个 HUB 连接，这时就要比较本交换机的 Port ID，由于端口 6 和 7 的优先级相同，则端口编号小的端口 6 优先成为根端口，而端口 7、8 被阻塞掉，最佳路径为 C-6-HUB-1-ROOT。

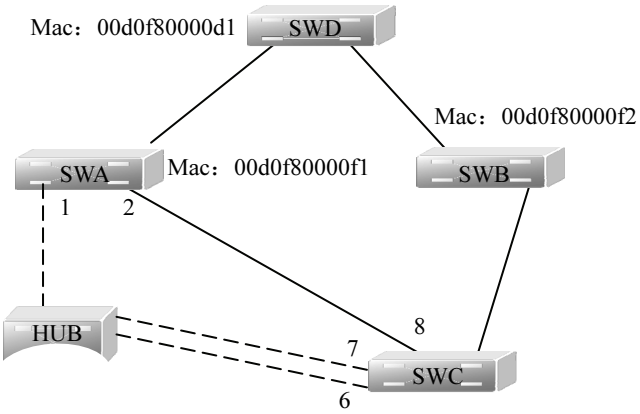


图 3-20　交换机 A、C 之间增加一个 HUB 连接

（4）STP 的缺点。

STP 解决了交换链路的冗余问题。但是，随着应用的深入和网络技术的发展，它的缺点在应用中也暴露出来。STP 的缺陷主要表现在收敛速度上。

当拓扑发生变化，新的 BPDU 要经过一定的时延才能传播到整个网络，这个时延称为 Forward Delay，协议的默认时延值是 15 秒。在所有交换机收到这个变化的消息之前，若旧拓扑结构中处于转发的端口还没有发现自己应该在新的拓扑中停止转发，则可能在网络中形成临时环路。为了解决临时环路的问题，生成树使用了一种定时器策略，即在端口从阻塞状态到转发状态中间加上一个只学习 MAC 地址但不参与转发的中间状态，两次状态切换的时间长度都是 Forward Delay，这样就可以确保在拓扑变化的时候不会产生临时环路。但是，这个看似良好的解决方案实际上带来的却是至少两倍 Forward Delay 的收敛时间。图 3-21 中描述了影响到整个生成树性能的三个计时器。

- Hello timer（BPDU 发送间隔）：定时发送 BPDU 报文的时间间隔，默认为 2 秒。
- Forward-Delay timer（发送延迟）：端口状态改变的时间间隔。当 RSTP 协议以兼容 STP 协议模式运行时，端口从 Listening 转向 Learning，或者从 Learning 转向 Forwarding 状态的时间间隔，默认为 15 秒。
- Max-Age timer（最大保留时间）：BPDU 报文消息生存的最长时间，超出这个时间，报文消息将被丢弃，默认为 20 秒。

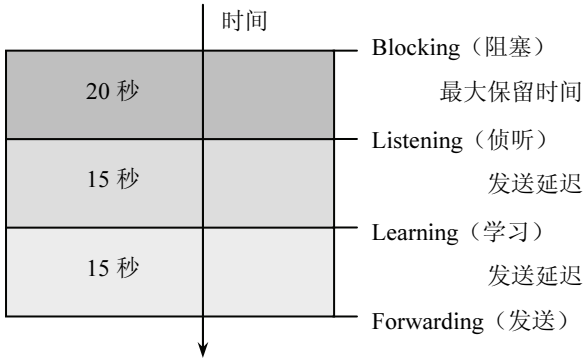


图 3-21　影响生成树性能的三个计时器

生成树经过一段时间（默认值为 50 秒左右）后，所有端口要么进入转发状态，要么进入阻塞状态。STP BPDU 仍然会定时（默认每隔 2 秒）从各个交换机的指定端口发出，以维护链路的状态。如果网络拓扑结构发生变化，生成树会重新计算，端口状态也会随之改变。

2. 快速生成树协议（Rapid Spanning Tree Protocol，RSTP）

（1）快速生成树协议 RSTP 的改进之处。

在 IEEE 802.1d 协议的基础之上进行一些改进，就产生了 IEEE 802.1w 协议。IEEE 802.1d 解决了因链路闭合引起的死循环问题，但生成树的收敛时间比较长，可能需要花费 50 秒钟。对于以前的网络来说，50 秒的阻断是可以接受的，毕竟那时人们对网络依赖性不强，但是现在情况不同了，人们对网络的依赖性越来越强，50 秒的网络故障足以带来巨大的损失，因此 IEEE 802.1w 协议问世了。RSTP 在 STP 的基础上做了三点重要改进，使得收敛速度快得多（最快 1 秒以内）。IEEE 802.1w 协议使收敛过程由原来的 50 秒减少为现在的大约 1 秒，因此

IEEE 802.1w 又称为“快速生成树协议”。

第一点改进：为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口（Backup Port）两种角色，当根端口/指定端口失效时，替换端口/备份端口就会无时延地进入转发状态。图 3-22 中的所有交换机都运行 RSTP，SwitchA 是根交换机，假设 SwitchB 的端口 1 是根端口，端口 2 将能够识别这种拓扑结构，成为根端口的替换端口，进入阻塞状态。在端口 1 所在链路失效的情况下，端口 2 能够立即进入转发状态，无需等待两倍的 Forward Delay 时间。

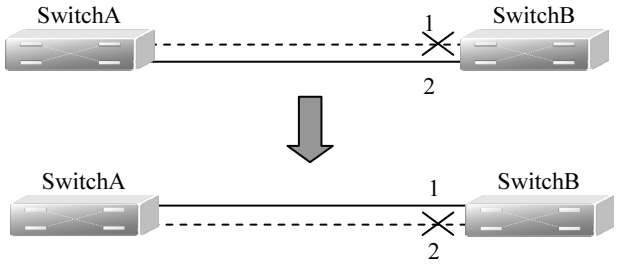


图 3-22　RSTP 的第一点改进

第二点改进：在只连接了两个交换端口的点对点链路中，指定端口只需与下游交换机进行一次握手就可以无时延地进入转发状态。如果是连接了三个以上交换机的共享链路，下游交换机不会响应上游指定端口发出的握手请求，只能等待两倍 Forward Delay 时间进入转发状态。

第三点改进：直接与终端相连而不是将其他交换机相连的端口定义为边缘端口（Edge Port）。边缘端口可以直接进入转发状态，不需要任何延时。由于交换机无法知道端口是否直接与终端相连，所以需要人工配置。

（2）端口角色和端口状态。

每个端口都在网络中扮演一个角色（Port Role），用来体现它在网络拓扑中的不同作用。

- Root Port：根端口，是指具有到根交换机最短路径的端口。
- Designated Port：指定端口，每个 LAN 通过该端口连接到根交换机。
- Alternate Port：根端口的替换口，一旦根端口失效，该端口就立刻变为根端口。
- Backup Port：指定端口的备份口，当一个交换机有两个端口都连接在一个 LAN 上，高优先级的端口为 Designated Port，低优先级的端口为 Backup Port。
- Undesignated Port：当前不处于活动状态的端口，OperState 为 down 的端口都被分配了这个角色。

RP=Root Port，DP=Designated Port，AP=Alternate Port，BP=Backup Port。在没有特别说明的情况下，端口优先级从左到右递减。

如图 3-23 所示为各个端口角色的示意图。

每个端口由三个状态（Port State）来表示是否转发数据包，从而控制整个生成树拓扑结构。

- Discarding：既不对收到的帧进行转发，也不进行源 MAC 地址学习。
- Learning：不对收到的帧进行转发，但进行源 MAC 地址学习，这是个过渡状态。
- Forwarding：既对收到的帧进行转发，也进行源 MAC 地址的学习。

对一个已经稳定的网络拓扑，只有 Root Port 和 Designated Port 才会进入 Forwarding 状态，其他端口只能处于 Discarding 状态。

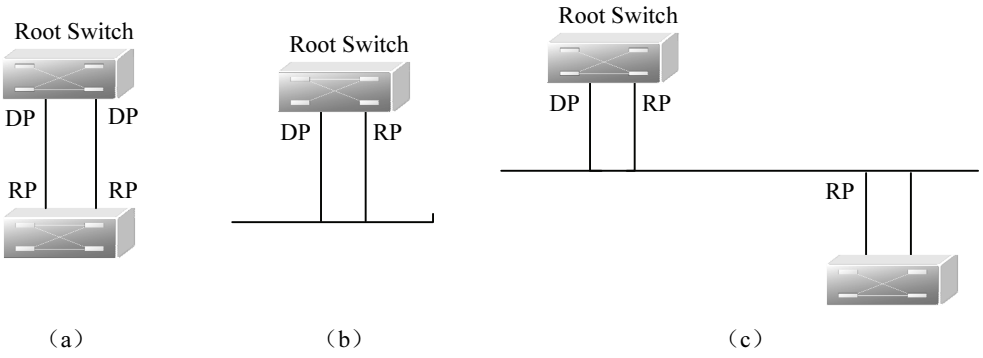


图 3-23　RSTP 中的端口角色

（3）网络拓扑树的生成。

下面说明 STP、RSTP 如何将杂乱的网络拓扑生成一个树型结构。如图 3-24 所示，假设 SwitchA、B、C 的 Bridge ID 是递增的，即 SwitchA 的优先级最高。A 与 B 间为千兆链路，B 和 C 间为百兆链路，A 和 C 间为十兆链路。SwitchA 作为该网络的骨干交换机，对 SwitchB 和 SwitchC 都做了链路冗余。显然，如果让这些链路都生效会产生广播风暴。

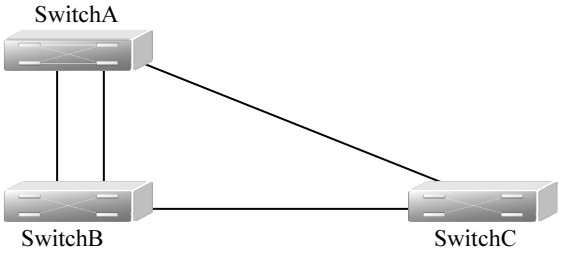


图 3-24　由三台交换机连接而成的环路拓扑

如果这三台交换机都打开了 Spanning Tree 协议，它们通过交换 BPDU 选出根交换机（Root Bridge）为 SwitchA。SwitchB 发现有两个端口都连在 SwitchA 上，它选出优先级最高的端口为 Root Port，另一个端口就被选为 Alternate Port。SwitchC 发现它既可以通过 B 到 A，也可以直接到 A，该交换机通过计算发现：即使通过 B 到 A 的链路花费也比直接到 A 的低，于是 SwitchC 选择与 B 相连的端口为 Root Port，与 A 相连的端口为 Alternate Port。选择好端口角色（Port Role）后，各个端口就进入相应的状态，如图 3-25 所示。

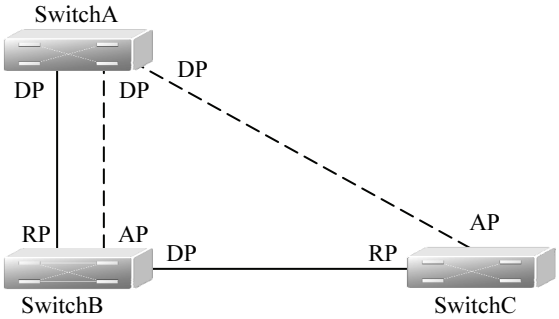


图 3-25　三台交换机都打开了 Spanning Tree 协议

如果 SwitchA 和 SwitchB 之间的活动链路出了故障，备份链路就会立即产生作用，如图 3-26 所示。

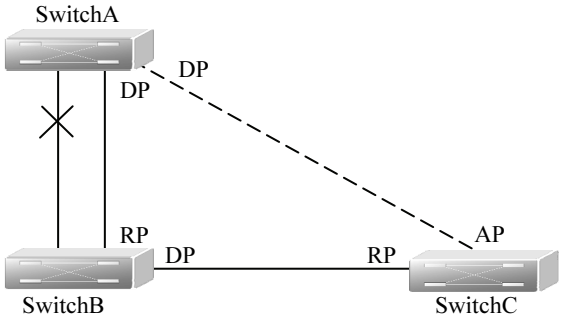


图 3-26　交换机 A 和交换机 B 之间的活动链路出了故障

如果 SwitchB 和 SwitchC 之间的链路出了故障，SwitchC 就会自动把 Alternate Port 转为 Root Port，如图 3-27 所示。

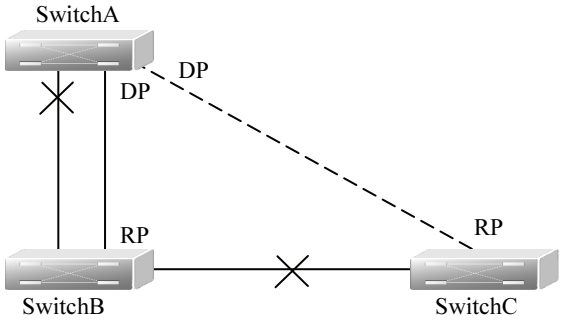


图 3-27　交换机 B、C 之间的活动链路出了故障

（4）RSTP 与 STP 的兼容性。

RSTP 保证了在交换机或端口发生故障后，能迅速地恢复网络连接。一个新的根端口可快速地转换到转发端口状态。局域网中的交换机之间显式的应答使指定的端口可以快速地转换到转发端口状态。

在理想条件下，RSTP 应当是网络中使用的默认生成树协议。由于 STP 与 RSTP 之间的兼容性，使得由 STP 到 RSTP 的转换是无缝的。

RSTP 协议可以与 STP 协议完全兼容，RSTP 协议会根据收到的 BPDU 版本号自动判断与之相连的交换机是支持 STP 协议还是支持 RSTP 协议，如果是与 STP 交换机互联就只能按 STP 的 Forwarding 方法，过 30 秒再 Forwarding，无法发挥 RSTP 的最大功效。

（5）RSTP 的拓扑变化机制。

在 RSTP 中，拓扑结构变更只在非边缘端口进入转发状态时发生，当某条链路出现故障断开时，不会像 802.1d 一样引起拓扑结构变更。

802.1w 的拓扑结构变更通知（TCN）功能不同于 802.1d，它减少了数据的溢流。在 802.1d 中，TCN 被单播至根交换机，然后组播至所有交换机，802.1d 中 TCN 的接收使交换机转发表中的所有内容快速失效，无论交换机转发拓扑结构是否使转发表受到影响。

相比之下，RSTP 明确地告知交换机，溢出除了经由 TCN 接收端口了解到的内容外的所有内容，优化了该流程。TCN 行为的这一改变极大地降低了拓扑结构变更过程中 MAC 地址的溢出量，当网络拓扑结构发生变化以后立刻转发（收敛时间小于 1 秒）。

3.4.3 生成树的实现举例

在此，以图 3-28 所示结构为例，说明生成树的实现方法。为了提高网络的可靠性，用两条链路将交换机互连，同时要求在交换机上做快速生成树协议配置，使网络避免环路。以两台 S2126 交换机为例，两台交换机分别命名为 SwitchA、SwitchB。PC1 和 PC2 在同一网段，假设 IP 地址分别为 192.168.0.137、192.168.0.136，网络掩码为 255.255.255.0。

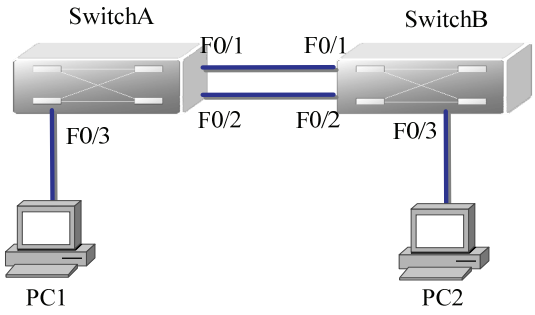


图 3-28 生成树拓扑图

通过观察不难发现，图 3-28 与图 3-13 是一样的，所以在这里需要提示的是，当看到网络拓扑图当中出现双链接时，要根据具体情况判断是冗余链路还是链路聚合，虽然形态上一致，但实现原理是不一样的。

在本案例中，有三个关键点：交换机 Trunk 端口的配置、配置生成树协议、设置交换机的优先级。

首先，对交换机进行基本配置。

```
Switch#configure terminal
Switch(config)#hostname SwitchA
SwitchA(config)#vlan 10
SwitchA(config)#interface fastethernet 0/3
SwitchA(config-if)#switchport access vlan 10
SwitchA(config-if)#exit
SwitchA(config)#interface range fastethernet 0/1-2
SwitchA(config-if-range)#switchport mode trunk
```

SwitchB 做与 SwitchA 相同的配置。

然后，配置快速生成树协议。

```
SwitchA#configure terminal
SwitchA(config)#spanning-tree
SwitchA(config)#spanning-tree mode rstp
```

验证测试：

```
SwitchA#show spanning-tree                    ！验证快速生成树协议已经开启
```

SwitchB 与 SwitchA 上述操作相同。

第三步，设置交换机的优先级，指定 SwitchA 为根交换机。

```
SwitchA(config)#spanning-tree priority 4096        ！设置交换机优先级为 4096
```

验证测试：

```
SwitchA#show spanning-tree                         ！验证 SwitchA 的优先级
```

SwitchB 与 SwitchA 上述操作相同。

最后，按图 3-28 所示连接网络设备，并配置 PC1、PC2 的 IP 地址、子网掩码，进行验证测试。

验证交换机 SwitchB 的端口 1 和端口 2 的状态。

```
SwitchB#show spanning-tree interface fastethernet 0/1
SwitchB#show spanning-tree interface fastethernet 0/2
```

如果 SwitchA 与 SwitchB 的端口 F0/1 之间的链路 down 掉，验证交换机 SwitchB 的端口 2 的状态，并观察状态转换时间。

```
SwitchB#show spanning-tree interface fastethernet 0/2
```

如果 SwitchA 与 SwitchB 之间的一条链路 down 掉（如拔掉网线），验证 PC1 与 PC2 是否仍能互相 ping 通，并观察 ping 的丢包情况。

```
PC1 上：ping 192.168.0.136                         ！观察连通性
PC1 上：ping 192.168.0.136 -t                      ！观察丢包情况
```

按照拓扑图连接网络时注意，两台交换机都配置快速生成树协议后，再将两台交换机连接起来。如果先连线再配置会造成广播风暴，影响交换机的正常工作。

3.5　交换技术综合应用案例

下面将综合有关交换技术设计一个组网案例，以此说明交换技术的应用与配置方法。

假设一中型公司有多个部门，其中包括销售部、市场推广部、财务部及总经理室等，现要组建自己的办公网络，组建需求如下：

（1）公司内部员工可以通过网络互相交流，各部门之间又相对独立。

（2）保证销售部门的员工能够全部接入网络，并且要保障接入交换机的工作效率。

（3）保证财务部门接入网络时不因线路问题而出现不能访问的情况。

（4）保证市场推广部利用网络高速传输文件。

为满足该公司的正常业务需要，可做以下设计：

（1）考虑该公司为中型规模，采用两层结构化设计，省略分布层，选用一中档三层交换机（SW-L3）作为核心层交换机，接入层交换机选用普通二层交换机（S2126），直接将接入交换机与三层交换机相连。

（2）为实现公司内部员工可以通过网络互相交流，各部门之间又相对独立，可以部门为单位划分 VLAN，如将销售部设为 VLAN 10，市场推广部设为 VLAN 2，财务部设为 VLAN 11，其他部门类推，在二层交换机上实现，并借助三层交换机实现 VLAN 之间的通信。

（3）为保证财务部门接入网络时不因线路问题而出现不能访问的情况，可在通向核心交换机的线路上采用冗余链路。

（4）在接入层上利用交换机堆叠技术保证销售部门的员工能够全部接入网络且保障接入交换机的工作效率。

（5）为使市场推广部利用网络高速传输文件，在通向核心层的链路上应用链路聚合技术。

（6）考虑到总经理在公司中的特殊性，可将总经理室主机（VLAN 99）直接接入网络核心层。

基于以上考虑，可得出网络组建方案如图 3-29 所示。

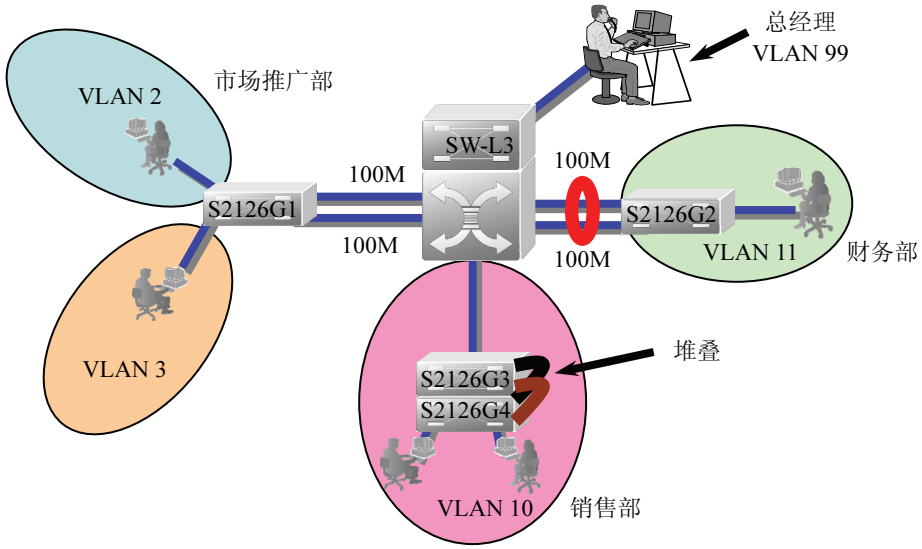


图 3-29　网络组建拓扑图

设计方案确定后，下面要做的事便是对各设备进行安装、连接及配置，使设备可正常工作。各设备的地址配置及接口连接情况可参考表 3-1，VLAN 分配情况见表 3-2。

表 3-1　设备地址及接口连接表

设备名称	设备地址	接口连接
SW-L3	VLAN 2：192.168.2.1/24	F0/1 连接 S2126G1 F0/1
	VLAN 3：192.168.3.1/24	F0/2 连接 S2126G1 F0/2
	VLAN 10：192.168.10.1/24	F0/23 连接 S2126G3 F0/23 F0/24 连接 S2126G3 F0/24
	VLAN 11：192.168.11.1/24	F0/11（VLAN 11）连接 S2126G2 F0/1
	VLAN 99：192.168.99.1/24	F0/9（VLAN 99）连接总经理 PC
S2126G1		F0/1 连接 SW-L3 F0/1
		F0/2 连接 SW-L3 F0/2
S2126G3		F0/23 连接 SW-L3 F0/23
		F0/24 连接 SW-L3 F0/24
S2126G2		F0/1 连接 SW-L3 F0/11
S2126G4		S2126G4 与 S2126G3 堆叠
总经理 PC	IP：192.168.99.99/24	网卡与 SW-L3 F0/9 连接

表 3-2　VLAN 分配表

设备名称	VLAN ID	接口分配
SW-L3	VLAN 11	F0/11（VLAN 11）
	VLAN 99	F0/9（VLAN 99）
S2126G1	VLAN 2	F0/3～F0/11
	VLAN 3	F0/12～F0/24
S2126G2	VLAN 11	F0/1～F0/22
S2126G3	VLAN 10	全部接口分配到 VLAN 10
S2126G4		

下面来看如何配置设备。

（1）划分 VLAN。

第 1 步：在相关交换机上创建 VLAN，并将接口划分到相关的 VLAN 中。

```
S2126G1(config)#vlan 2
S2126G1(config- vlan)#exit
S2126G1(config)#vlan 3
S2126G1(config- vlan)#exit
S2126G1(config)#interface range fastethernet 0/3-11
S2126G1(config-if-range)#switchport access vlan 2
S2126G1(config-if-range)#exit
S2126G1(config)#interface range fastethernet 0/12-24
S2126G1(config-if-range)#switchport access vlan 3
```

其他二层交换机配置略。

要注意的是，在三层交换机 SW-L3 上同样要建立相关 VLAN，并将相应接口加入到相应 VLAN。

第 2 步：在核心交换机上开启 VLAN 间的路由。

```
SW-L3(config)#interface vlan 2                          ! 创建虚拟接口 VLAN 2
SW-L3(config-if)#ip address 192.168.2.1 255.255.255.0   ! 为虚拟接口 VLAN 2 配置 IP
SW-L3(config-if)#no shutdown
SW-L3(config-if)#exit
SW-L3(config)#interface vlan 3
SW-L3(config-if)#ip address 192.168.3.1 255.255.255.0
SW-L3(config-if)#no shutdown
SW-L3(config-if)#exit
SW-L3(config)#interface vlan 10
SW-L3(config-if)#ip address 192.168.10.1 255.255.255.0
SW-L3(config-if)#no shutdown
SW-L3(config-if)#exit
SW-L3(config)#interface vlan 11
SW-L3(config-if)#ip address 192.168.11.1 255.255.255.0
SW-L3(config-if)#no shutdown
```

```
SW-L3(config-if)#exit
SW-L3(config)#interface vlan 99
SW-L3(config-if)#ip address 192.168.99.1 255.255.255.0
SW-L3(config-if)#no shutdown
SW-L3(config-if)#exit
```

说明：虚拟接口的 IP 地址就是该接口所对应 VLAN 中的主机的网关地址。

（2）将销售部 S2126G3 与 S2126G4 上的堆叠模块用堆叠线缆连接起来。

这里不需要配置交换机，只需要根据堆叠规则对交换机正确连接就可以了。连接方式为：S2126G3 的 UP 端口与 S2126G4 的 DOWN 端口相连，S2126G3 的 DOWN 端口与 S2126G4 的 UP 端口相连。

（3）建立财务部冗余链路。

第 1 步：建立 S2126G2 与 SW-L3 之间的双链路。

```
S2126G2(config)#interface range fastethernet 0/1-2
S2126G2(config-if-range)#switchport mode trunk
SW-L3(config)#interface range fastethernet 0/1-2
SW-L3(config-if-range)#switchport mode trunk
```

第 2 步：S2126G2 与 SW-L3 运行快速生成树协议 RSTP。

```
S2126G2(config)#spannning-tree
S2126G2(config)#spanning-tree mode rstp
SW-L3(config)#spanning-tree
SW-L3(config)#spanning-tree mode rstp
```

（4）建立市场推广部聚合链路。

第 1 步：建立 S2126G1 与 SW-L3 之间的双链路。将 S2126G1 的 F0/1、F0/2 与 SW-L3 的 F0/1、F0/2 级联。

第 2 步：建立 S2126G1 与 SW-L3 之间的聚合链路。

```
S2126G1(config)#interface range fastethernet 0/1-2
S2126G1(config-if-range)#port-group 1
SW-L3(config)#interface range fastethernet 0/1-2
SW-L3(config-if-range)# port-group 1
```

至此，完成所有的设置，用户的需求已完全满足，可运行相关命令查看设置情况。

```
SW-L3#show spanning-tree                ！查看生成树协议
SW-L3#show aggregateport summary        ！查看聚合端口
SW-L3#show vlan                         ！查看 VLAN
SW-L3#show ip route                     ！查看路由表
```

为测试网络运行是否正常，可使用最经典的方法，在一台主机上运行 ping 命令，看是否能与目标主机 ping 通即可。

一、填空题

1．由于交换机对多数端口的数据进行同时交换，这就要求交换机具有很宽的交换总线带宽，如果二层

交换机有 N 个端口，每个端口的带宽是 M，交换机总线带宽超过_____，交换机就可以实现线速交换。

2．传统的交换技术是在 OSI 网络标准模型中的第二层（数据链路层）进行操作的，而第三层交换技术则在网络模型的_____层中实现数据包的高速转发。简单地说，第三层交换技术就是第二层交换技术加第三层转发技术，这是一种利用第三层协议中的信息来加强第二层交换功能的机制。

3．VLAN 标记字段的长度是_____字节，插入在以太网 MAC 帧的源地址字段和长度/类型字段之间。

4．下面对 VLAN 的描述，错误的是_____。

A．虚拟局域网 VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组

B．这些网段具有某些共同的需求

C．每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的工作站是属于哪一个 VLAN

D．VLAN 是一种新型局域网

5．链路聚合将交换机上的多个端口在物理上连接起来，在逻辑上捆绑在一起形成一个拥有较大宽带的端口，形成一条干路，可以实现 _____，并提供冗余链路。

二、简答题

1．试述二层交换与三层交换各自的特点。

2．三层交换机与路由器有何异同点？

3．VLAN 的划分方法有哪些？

4．说明 Port VLAN 和 Tag VLAN 的不同之处，并写出它们的配置方法。

5．简述 VLAN 之间进行通信的方法。

6．链路聚合的作用是什么？

7．生成树协议是为了解决什么问题？简要说明其工作原理。

8．请说出以下命令的作用：

（1）Switch (config)#aggregateport load-balance src-dst-mac

（2）Switch (config)# interface vlan 10

（3）SwitchA(config)#spanning-tree mode rstp

9．尝试为自己所在学校、企业或部门设计一个交换网络，并进行相应配置，使其满足所有用户的需求。