第 3 章　交换机基础和配置

交换机的出现改变了传统共享式局域网中各个主机争用公共信道的方式，提高了网络的性能。交换机收到数据帧后，通过查找自身的端口地址表决定是进行转发还是过滤，并且交换机具有地址学习的功能。交换机转发数据帧的方式有直接交换方式、存储转发方式和改进的直接交换方式。交换机的性能主要靠转发方式、背板带宽、延迟、吞吐量等指标来衡量。交换机的常用配置是网络管理员必须掌握的一项内容。

3.1　交换机概述

交换机是现代局域网中用得最多的网络互联设备，它不仅可以进行网络互联，而且还具有很高的智能性，能对所连接的网络进行管理，提高网络的工作效率。熟练使用交换机的前提是了解交换机的工作原理、功能、分类、交换方式以及性能指标。

3.1.1　交换机的产生和工作原理

前面介绍的用同轴电缆构成的总线型以太网和用集线器构成的星型以太网，都属于共享式以太网。共享式以太网的特点是网络上所有的结点处于一个共同的冲突域，在同一时刻同一个冲突域中只有一台主机可以发送数据帧，其他主机都可以接收到，而且也只能接收数据，否则将产生冲突，导致发送失败。当同一个冲突域中的主机太多时，冲突将大幅增加，带宽和速度将显著下降。

为了克服网络规模和网络性能之间的矛盾，人们提出了以下 3 种解决方案：

(1)提高局域网的速度，将数据传输速率由 10 Mb/s 提高到 100 Mb/s，甚至 1 Gb/s、10 Gb/s，由此促进了高速局域网技术的研究与产品的开发。

(2)将一个大型的局域网划分为多个小型局域网，然后用网络互联设备进行连接，由此促进了网络互联技术的发展。

(3)将共享介质方式改为交换方式，由此促进了交换式局域网技术的发展。

交换式局域网的核心设备是局域网交换机。局域网交换机可以在它的多个端口之间建立多个并发连接。共享式局域网和交换式局域网在工作原理上的区别如图 3-1 所示。

1. 交换机的产生

为了隔离冲突域，最早使用的是网桥，后来交换机逐渐取代了网桥。网桥可以将两个或两个以上的局域网互联为一个逻辑局域网，使一个局域网中的用户可以通过网桥去访问另一个局域网的资源，实现局域网的互联，如图 3-2 所示。

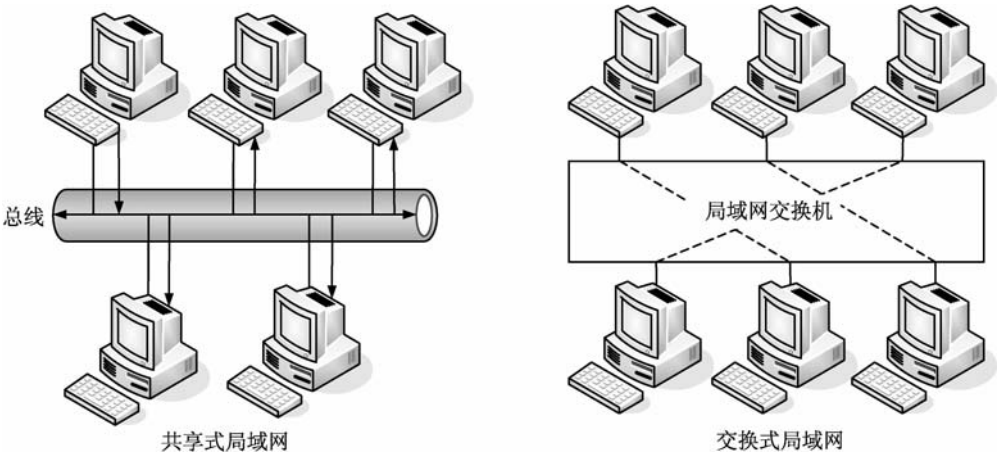

图 3-1　共享式局域网和交换式局域网在工作原理上的区别

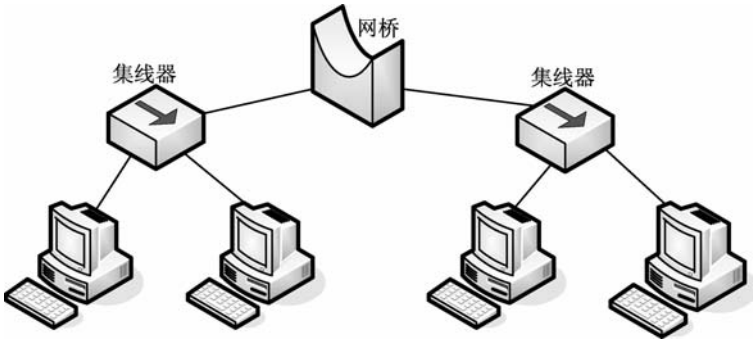

图 3-2　网桥连接两个局域网

网桥的工作原理已在第 1 章中进行了简单介绍，网桥虽能隔离冲突域，但不能隔离广播域，即网桥会广播未知目的数据帧，很容易形成广播风暴，导致无法正常通信或通信效率降低。

广播域是指广播帧所能到达的范围，连接在多个级联集线器上的所有设备构成了一个冲突域，同时也构成了一个广播域，此时冲突域和广播域是相同的。连接在网桥不同端口上的局域网分属于不同的冲突域，但都属于同一个广播域，即网桥的所有端口构成了一个广播域。冲突域和广播域的区别如图 3-3 所示。

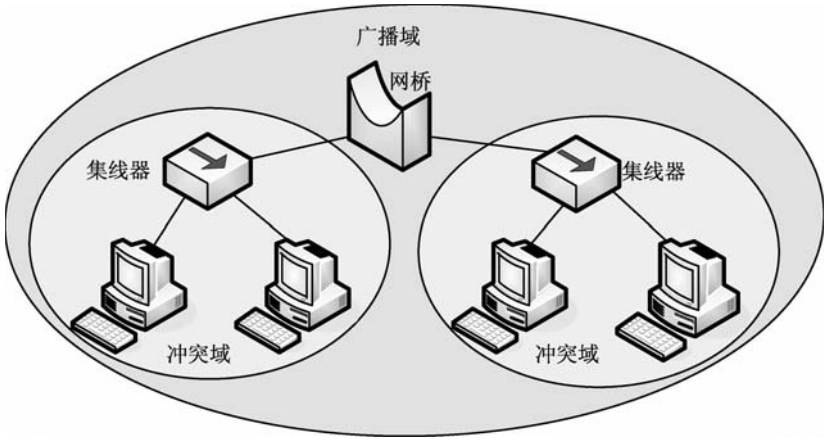

图 3-3　冲突域和广播域的区别

随着网络技术的发展，1995 年出现了最早的以太网交换机，交换机可以看做一个多端口网桥，使用的算法也基本相同，只是交换机的硬件厂商将算法进行固化，生产出了交换机的核心 ASIC 芯片，从而实现了基于硬件的线速交换机。

2. 交换机的工作原理

交换(switching)是按照通信两端传输信息的需要，是用人工或设备自动完成的方法把要传输的信息送到符合要求的相应路径上的技术的统称。广义的交换机，就是一种在通信系统中完成信息交换功能的设备。

在计算机网络系统中，交换式局域网是对共享式局域网的改进。交换式局域网中的交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有的端口都挂接在这条背部总线上，源端口收到数据包以后，会查找内存中的端口地址表以确定目的 MAC(网卡的硬件地址)的网卡挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口。如果数据包的目的 MAC 与端口的映射关系在端口地址表中不存在，将此数据包广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加到内部 MAC 地址表中。

使用交换机也可以把网络“分段”，通过对照 MAC 地址表，交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发，可以有效地隔离广播风暴，减少误包和错包的出现，避免共享冲突。

交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。当结点 A 向结点 D 发送数据时，结点 B 可同时向结点 C 发送数据，而且这两个传输都享有网络的全部带宽，都有着自己的虚拟连接。假设这里使用的是 10 Mb/s 的以太网交换机，那么该交换机这时的总流通量就是 2×10 Mb/s=20 Mb/s，而使用 10 Mb/s 的共享式 hub 时，一个 hub 的总流通量也不会超出 10 Mb/s。

总之，交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC 地址，并把其存放在端口地址表中，通过在数据帧的源端口和目标端口之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

目前，主流的交换机厂商有国外的 Cisco(思科)、3COM 等，国内的华为、神舟数码、D-LINK 等。

3.1.2 交换机的功能

交换机具备强大的交换处理能力，基本的功能有地址学习、帧的转发和过滤以及回路避免。目前，交换机还具备了一些新的功能，如对虚拟局域网(virtual local area network，VLAN)的支持、对链路汇聚的支持，甚至有的还具有防火墙的功能。

1. 地址学习

以太网交换机通过一段时间的学习，可以知道每一端口相连设备的 MAC 地址，并将地址同相应的端口映射起来存放在交换机缓存中的端口地址表中。地址的学习是通过监听所有流入的数据帧，再对源 MAC 地址进行检验完成的。

2. 帧的转发和过滤

当一个数据帧到达交换机后，如果目的地址在 MAC 地址表中有映射，就被转发到连接目的结点的端口，如果没有映射，则转发到其他所有端口，如果目的地址和源地址位于相同的端口，则进行过滤。

3. 回路避免

当交换机包括一个冗余回路时，以太网交换机通过生成树协议避免回路的产生，同时允许存在后备路径。

交换机除了能够连接同种类型的网络之外，还可以在不同类型的网络（如以太网和快速以太网）之间起到互联作用。如今许多交换机都能够提供支持快速以太网或 FDDI 等的高速连接端口，用于连接网络中的其他交换机或者为带宽占用量大的关键服务器提供附加带宽。

一般来说，交换机的每个端口都用来连接一个独立的网段，但是，有时为了提供更快的接入速度，还可以把一些重要的网络计算机直接连接到交换机的端口上。这样，网络的关键服务器和重要用户就拥有更快的接入速度，支持更大的信息流量。

3.1.3　交换机的分类

交换机的分类方法多种多样，下面介绍当前交换机的主流分类方法。

1. 根据网络覆盖范围划分

根据网络覆盖范围，可以将交换机分为广域网交换机和局域网交换机。

1）广域网交换机

广域网交换机主要应用于电信城域网互联、互联网接入等领域的广域网中，提供通信用的基础平台。

2）局域网交换机

局域网交换机最常见，主要应用于局域网，用于连接终端设备，如服务器、工作站、集线器、路由器、网络打印机等网络设备，提供高速独立的通信通道。

2. 根据传输介质和传输速度划分

在局域网交换机中，根据交换机使用的网络传输介质及传输速度的不同，可以分为以太网交换机、快速以太网交换机、千兆以太网交换机、万兆以太网交换机、ATM 交换机、FDDI 交换机等。

1）以太网交换机

“以太网交换机”是指带宽在 100 Mb/s 以下的以太网所用的交换机，后面介绍的“快速以太网交换机”、“千兆以太网交换机”和“万兆以太网交换机”也是以太网交换机，不过它们所采用的协议标准或者传输介质不一样，其接口形式也可能不一样。

以太网交换机可应用于大大小小的局域网，它的价格低，档次齐全。以太网包括 3 种网络接口——RJ-45、BNC 和 AUI，对应的传输介质分别为双绞线、细同轴电缆和粗同轴电缆。现在的以太网交换机一般都是 RJ-45 接口的，但是为了兼顾同轴电缆介质的网络连接，还会配上 BNC 或 AUI 接口。如图 3-4 所示的局域网交换机是一款带有 RJ-45 和 AUI 接口的以太网交换机产品实物图。

图 3-4 以太网交换机

2)快速以太网交换机

这种交换机用于 100 Mb/s 快速以太网。快速以太网是一种在普通双绞线或者光纤上实现 100 Mb/s 传输带宽的网络技术。现在的快速以太网交换机基本上还是以 10/100 Mb/s 自适应型为主。一般来说,快速以太网交换机通常所采用的介质也是双绞线,有的快速以太网交换机为了兼顾与其他光传输介质的网络互联,也留有少数的光纤接口。

3)千兆以太网交换机

千兆以太网交换机用于千兆以太网中,它的带宽可以达到 1 000 Mb/s。千兆以太网也称为"吉比特以太网"。千兆以太网交换机一般用于大型网络的骨干网段,采用光纤、双绞线两种传输介质,对应的接口为 SC 和 RJ-45 两种。

4)万兆以太网交换机

万兆以太网交换机用于万兆以太网的接入,它的带宽可以达到 10 Gb/s。万兆以太网采用光纤作为传输介质,因此,只有光纤接口。由于 10 Gb/s 以太网技术还处于研发初级阶段,价格也非常昂贵,所以,万兆以太网的实际应用还不是很普遍。如图 3-5 所示的是一款万兆以太网交换机产品实物图。

图 3-5 万兆以太网交换机

5)ATM 交换机

ATM 交换机是用于 ATM 网络的交换机产品。由于 ATM 网络技术独特,现在广泛用于电信、邮政网的主干网段,其交换机产品在市场上也很少看到。ATM 交换机的接口类型一般有以太网 RJ-45 接口和光纤接口两种。这两种接口适合于不同类型的网络之间进行互联。ATM 交换机的价格相对于以太网交换机来说要高很多,所以在普通局域网中极少使用。

6)FDDI 交换机

FDDI 技术是在快速以太网技术还没有开发出来之前开发的,它主要是为了解决 10 Mb/s 以太网和 16 Mb/s 令牌环网速度的局限,因为它的传输速度可达到 100 Mb/s。FDDI 技术采用光纤作为传输介质,比以双绞线为传输介质的网络成本高许多,所以随着快速以太网技术的成功开发,FDDI 技术也就失去了它的市场。

3. 根据应用层次划分

根据交换机所应用的网络层次,可以将网络交换机划分为企业级交换机、校园网交换机、部门级交换机、工作组交换机、桌面型交换机 5 种。

1)企业级交换机

企业级交换机属于一类高端交换机,一般采用模块化的结构,可作为企业网络骨干交换

机构建高速局域网，所以它通常应用于企业网络的最顶层。

企业级交换机可以提供用户化定制、优先级队列服务和网络安全控制，并能很快适应数据增长和改变的需要，从而满足用户的需求。对于有更多需求的网络，企业级交换机不仅能传送海量数据和控制信息，而且具有硬件冗余和软件可伸缩性特点，保证网络的可靠运行。这种交换机从它所处的位置可以看出它对网络的要求非同一般，至少在带宽、传输速率以及背板容量上要比一般交换机高出许多，所以企业级交换机一般都是千兆以上以太网交换机。企业级交换机所采用的端口一般都为光纤接口，这主要是为了保证交换机的高传输速率。通常认为，能支持 500 个信息点以上大型企业应用的交换机为企业级交换机。如图 3-6 所示的是友讯的一款模块化千兆以太网交换机，它属于企业级交换机范畴。

图 3-6　企业级交换机

2）校园网交换机

校园网交换机主要应用于较大型网络，一般作为网络的骨干交换机。这种交换机因通常用于分散的校园网而得名，其实它不只应用于校园网中，而是主要应用于物理距离分散的较大型网络中。这种交换机具有快速数据交换能力和全双工能力，可提供容错等智能特性，还支持扩充选项及第三层交换中的虚拟局域网等多种功能。

校园网交换机通常采用光纤或者同轴电缆作为传输介质，当然也就需提供 SC 光纤接口和 BNC 或者 AUI 同轴电缆接口。

3）部门级交换机

部门级交换机是面向部门级网络使用的交换机，一般具有较为突出的智能型特点，支持基于端口的虚拟局域网，可实现端口管理，可任意采用全双工或半双工传输模式，可对流量进行控制，有网络管理的功能，可通过 PC 机的串口或经过网络对交换机进行配置、监控和测试。如果作为骨干交换机，则一般认为支持 300 个信息点以下的中型企业的交换机为部门级交换机。这类交换机可以是固定配置，也可以是模块化配置，一般都同时具有双绞线接口和光纤接口。

4）工作组交换机

工作组交换机是传统集线器的理想替代产品，一般为固定配置，配有一定数目的 10Base-T 或 100Base-TX 双绞线接口。工作组交换机一般没有网络管理的功能，如果是作为骨干交换机，则一般认为支持 100 个信息点以下的交换机为工作组交换机。

5）桌面型交换机

桌面型交换机是一种最低档的交换机，它的端口数也较少（12 口以内，但不绝对），价格是最便宜的。这类交换机虽然只具备最基本的交换机特性，但是它具有交换机的通用优越性，广泛应用于小型企业或中型以上企业办公桌面。在传输速度上，目前桌面型交换机大都提供多个具有 10/100 Mb/s 自适应能力的端口。如图 3-7 所示是一款桌面型交换机产品的实物图。

图 3-7 桌面型交换机

4.根据交换机的端口结构划分

根据交换机的端口结构可以将交换机分为固定端口交换机和模块化交换机。其实还有一种是两者兼顾,那就是在提供基本固定端口的基础之上再配备一定的扩展插槽或模块。

1)固定端口交换机

固定端口交换机指的是带有的端口数量固定的交换机,这种交换机价格便宜,但由于它只能提供有限的端口和固定类型的接口,因此,无论从可连接的用户数量上,还是从可使用的传输介质上来讲都具有一定的局限性。

固定端口交换机在工作组中应用较多,一般适用于小型网络、桌面交换环境。目前,这种固定端口的交换机比较常见,一般的端口标准是 8 端口、16 端口和 24 端口。如图 3-8 所示是一款 24 端口的交换机产品实物图。

图 3-8 固定端口交换机

2)模块化交换机

模块化交换机虽然在价格上要贵很多,但是拥有更大的灵活性和可扩充性,用户可任意选择不同数量、不同速率和不同接口类型的模块,以适应千变万化的网络需求。而且模块化交换机大都有很强的容错能力,支持交换模块的冗余备份,并且往往拥有可热插拔的双电源,以保证交换机的电力供应。如图 3-9 所示为一款模块化快速以太网交换机产品实物图,具有 4 个可插拔模块,可根据实际需要灵活配置。

图 3-9 模块化交换机

在选择交换机时,应按照需要和经费综合考虑是选择模块化交换机还是固定端口交换机。一般来说,企业级交换机应考虑其扩充性、兼容性和排错性,因此,应当选用模块化交换机;而部门级交换机和工作组交换机则由于任务较为单一,故可采用简单的固定端口交换机。

5. 根据交换机工作的协议层划分

交换机工作的层次越高，其设备的技术性越高，性能也越好，档次也就越高。根据工作的协议层次，交换机可分为二层交换机、三层交换机和四层交换机。

1）二层交换机

二层交换机工作在数据链路层，依赖于数据链路层中的信息（如 MAC 地址）完成不同端口数据间的线速交换，主要功能包括物理编址、错误校验、帧序列以及数据流控制。二层交换机是最原始的交换技术产品，目前桌面型交换机一般属于这种类型，因为桌面型交换机一般来说所承担的工作复杂性不是很大，又处于网络的最基层，所以只需要提供最基本的数据链接功能。

目前，二层交换机由于价格便宜，功能符合中、小企业实际应用需求，因此，应用最为普遍，一般应用于小型企业或中型以上企业网络的桌面层次。要说明的是，所有的交换机在协议层次上来说都是向下兼容的，也就是说所有的交换机都能够工作在二层。

2）三层交换机

三层交换机工作在网络层，它比二层交换机功能更强，具有路由功能，可以将 IP 地址信息提供给网络路径选择，并可实现不同网段间数据的线速交换。当网络规模较大时，可以根据特殊应用需求划分为小而独立的虚拟局域网网段，以减小广播所造成的影响。通常这类交换机采用模块化结构，以适应灵活配置的需要。在大中型网络中，三层交换机已经成为基本配置设备。

3）四层交换机

四层交换机工作在传输层，直接面对具体应用。四层交换机用于实现对网络服务的快速访问。在四层交换机中，决定传输的依据不仅是 MAC 地址（第二层网桥）或源/目的地址（第三层路由），而且包括 TCP/UDP（第四层）应用端口号，被设计用于高速Intranet，四层交换机除了负载均衡功能外，还支持基于应用类型和用户 ID 的传输流控制功能。此外，四层交换机直接安放在服务器前端，它了解应用会话内容和用户权限，因而使它成为防止非授权访问服务器的理想平台。四层交换机支持传输层以下的所有协议，可根据端口号来区分数据包的应用类型，从而实现应用层的访问控制和服务质量保证。目前由于这种交换技术尚未真正成熟且产品价格昂贵，所以四层交换机在实际应用中还较少见。

6. 根据是否支持网络管理功能划分

根据交换机是否支持网络管理功能，可以将交换机分为“网管型”和“非网管型”两大类。网管型交换机的正面或背面一般有一个串口或并口，通过串口电缆或并口电缆可以把交换机和计算机连接起来，便于设置。

网管型交换机的任务就是使所有的网络资源处于良好的状态。网管型交换机产品提供了基于控制台（Console）端口、基于 Web 页面以及支持 Telnet 远程登录网络等多种网络管理的方式。因此，网络管理人员可以对该交换机的工作状态、网络运行状况进行本地或远程的实时监控，管理所有交换端口的工作状态和工作模式。网管型交换机支持 SNMP 协议。SNMP 协议由一整套简单的网络通信规范组成，可以完成所有基本的网络管理任务，对网络资源的需求量少，具备一些安全机制。SNMP 协议的工作机制非常简单，主要通过各种不同类型的消息，即协议数据单位（PDU）实现网络信息的交换。但是，网管型交换机相对于非网管型交换机来说要贵许多。

非网管型交换机是指不能通过管理端口执行监控交换机端口、划分 VLAN、设置 Trunk

端口等管理功能的交换机。

3.1.4 交换机的交换方式

交换机有直接交换、存储转发交换和改进的直接交换 3 种交换方式。

1. 直接交换方式

直接交换方式的以太网交换机只要检测到数据帧的目的地址字段，就启动内部的动态查找表查找相应的输出端口，在输入与输出交叉处接通，把数据帧直接转发到相应的端口，实现交换功能。这种方式的优点是延迟非常小，交换非常快，缺点是不提供错误检测能力，无法检查所传送的数据帧是否有误。由于没有缓存，所以不支持具有不同速率的输入输出端口之间的转发。

2. 存储转发交换方式

存储转发交换方式是计算机网络领域应用最为广泛的方式。交换机首先将接收到的数据帧存储起来，然后进行循环冗余码校验(CRC)，如果接收帧正确，则根据目的地址，确定端口号进行转发。这种方式的缺点是数据处理延时大，优点是可以对进入交换机的数据帧进行错误检测，有效地改善了网络性能，并且可以支持不同速率的端口间的转换，保持高速端口与低速端口间的协同工作。

3. 改进的直接交换方式

改进的直接交换方式是介于前两者之间的一种解决方案。它检查数据帧的长度是否够 64 字节：如果小于 64 字节，则丢弃该帧；如果大于 64 字节，则检查头部是否正确，正确则转发。它的数据处理速度比存储转发交换方式快，但比直接交换方式慢。这种方式对于短的数据帧来说，转发延时与直接交换方式接近；对于长的数据帧来说，由于只对帧的地址与控制字段进行了差错检测，因此，交换延时将比存储转发交换方式小。

3.1.5 交换机的主要技术参数

交换机的每一个技术参数都影响到交换机的性能和功能，其主要的技术指标有转发方式、背板带宽、延时、吞吐量、MAC 地址表大小、管理功能、生成树等。

1. 转发方式

转发方式分为直接交换方式、存储转发交换方式和改进的直接交换方式，各自的优缺点和应用场合在 3.1.4 中已经介绍过，应当根据需要进行选择。

2. 背板带宽

背板带宽标志交换机的数据交换能力。背板带宽越高，数据转发能力越强。在以背板总线为交换通道的交换机上，任何端口发送的数据都将放到总线上，并由总线传递给目标端口。这种情况下背板带宽是总线的带宽。模块化的交换一般采用交换矩阵，此时背板带宽指的是交换矩阵的总吞吐量。

3. 延时

延时是指从交换机接收到数据帧到开始向目的端口复制数据帧之间的时间间隔。有许多因素会影响延时大小，如转发技术等。采用直接交换方式的交换机有固定的延时。因为它不管数据帧的整体大小，而只根据目的地址来决定转发方向。采用存储转发交换技术的交换机，由于必须要接收完完整的数据包才开始转发，所以它的延时与数据包大小有关。数

据包大，则延时大；数据包小，则延时小。

4. 吞吐量

吞吐量体现了交换引擎的转发性能。目前，最流行的交换机为线速交换机。所谓线速交换，是指交换速度达到传输线路上的数据传输速度，能够最大限度地消除交换瓶颈。实现线速交换的核心是 ASIC 技术，用硬件实现协议解析和包转发，而不是传统的软件处理方式。

5. MAC 地址表大小

MAC 地址表大小是指交换机中的 MAC 地址表可以存储的 MAC 地址的数量，存储的 MAC 地址数量越多，数据转发的速率和效率也就越高。

MAC 地址表大小是由缓存容量的大小决定的，不同档次的交换机每个端口的 MAC 地址表大小也不同，档次越高，能够记住的 MAC 地址数量就越多。通常交换机只需要记忆 1 024 个MAC 地址就可以了，在具体选择时根据网络规模而定。

6. 管理功能

交换机的管理功能是指交换机如何控制用户访问交换机，以及用户对交换机的可视程度如何。通常，交换机厂商都提供管理软件或满足第三方管理软件远程管理交换机的功能。一般的交换机具有统计管理功能。而复杂一些的交换机会增加通过内置 RMON 组(mini-RMON)来支持 RMON 主动监视功能。有的交换机还允许外接 RMON 监视可选端口的网络状况。

7. 生成树

由于交换机实际上是多端口的透明网桥，所以交换机也存在“拓扑环”(topology loops)问题。某个网段的数据包通过某个桥接设备传输到另一个网段，而返回的数据包通过另一个桥接设备返回源地址。这种现象就叫“拓扑环”。一般来说，交换机采用生成树协议算法让网络中的每一个桥接设备相互知道，自动防止“拓扑环”现象。交换机通过将检测到的“拓扑环”中的某个端口断开，达到消除“拓扑环”的目的，维持网络中的拓扑树的完整性。在网络设计中，“拓扑环”常被推荐用于关键数据链路的冗余备份链路选择。所以，带有生成树协议支持的交换机可以用于连接网络中关键资源的交换冗余。

在选择交换机时，除了要考虑以上性能参数外，还要根据需要考虑交换机的端口数量(一般为 8 的倍数)、所支持的端口类型、是否支持虚拟局域网、是否有级联端口等因素。

3.2　交换机的常用配置

在交换式以太网中，交换机无疑是必不可少的设备。熟练地对交换机进行配置操作是作为网络管理员必须要掌握的知识和技能。

3.2.1　交换机配置基础

对交换机进行配置可分为本地配置和远程配置两种方式。本地配置采用本地控制台登录方式来实现，这种配置方式不占用交换机的带宽，因此，称为带外配置管理。在初始状态下，交换机还没有配置管理 IP 地址，所以只有采用本地配置方式来实现。远程配置是指通过网络对交换机进行配置管理，可以分为 3 种：Telnet 登录方式、Web 浏览器访问方式和

SNMP 远程管理方式。这 3 种方式均要通过网络传输，又称带内配置管理。

为了方便实现交换机的远程管理，在第一次配置交换机时，可以为其配置网络地址、设备名称等参数，并且有选择性地启用交换机上的 Telnet Server、Web Server、SNMP Agent 等服务，以便启用远程配置方式进行管理。

1. 本地配置

对于第一次配置交换机，必须采用本地配置，即采用本地控制台登录方式实现。在交换机上有一个 Console 端口，叫做控制台端口，符号 EIA/TIA RS-232C 是异步串行规范的配置口，通过它可实现对交换机的本地配置，并且可以查看和变更交换机的配置。通过 Console 端口连接并配置交换机是最常用、最基本的，也是网络管理员必须掌握的配置管理方式。

首先通过 Console 线将计算机和交换机进行物理连接。根据交换机 Console 端口的形式，将 Console 电缆线的一端连接到交换机的 Console 端口，另一端连接到计算机的串行口。然后在计算机上运行超级终端，即可实现将计算机模拟成交换机的一个终端，从而实现对交换机的访问和配置。

下面以建立一个名为 Switch 的超级终端为例说明本地配置过程。

(1)用一条串行线将控制台端口与计算机连接起来，该步骤有两种情况，取决于交换机的控制台端口类型。

Console 端口有两种端口形式：RJ-45 接口和 COM 端口形式。无论哪种端口，都需要通过专门的 Console 线连接至计算机的串行口，与交换机不同的 Console 端口相对应。Console 线分为 3 种。第一种是串行线，两端均为串行接口，分别插入计算机的串行口和交换机的 Console 端口。第二种是两端均为 RJ-45 接头的扁平线，这种连接线无法直接与计算机串行口连接，因此，还必须同时使用一个 RJ-45 to DB-9(或 RJ-45 to DB-25)适配器。通常情况下交换机自带一根 Console 线和相应的 DB-9 或 DB-25 适配器。第三种的一端是 RJ-45 接口，另一端是 COM 端口。

(2)在计算机上运行并设置超级终端软件(这里的操作系统为 Windows XP)。

首先，执行“开始”→“程序”→“附件”→“通讯”→“超级终端”命令，弹出超级终端的“连接描述”对话框，如图 3-10 所示。

接着，在超级终端的“连接描述”对话框中，输入新建连接的名称，如 Switch，单击“确定”按钮，弹出“连接到”对话框，如图 3-11 所示。

图 3-10 “连接描述”对话框

图 3-11 “连接到”对话框

然后，根据实际所用的计算机串行口号选择“连接时使用”的端口，单击“确定”按钮，出现端口属性设置对话框，如图 3-12 所示。

图 3-12　端口属性设置对话框

交换机控制台的默认波特率是 9 600，所以将端口属性设置为 9 600 波特率、8 位数据位、无奇偶校验、1 位停止位、无数据流控制。单击“确定”按钮，完成设置，即出现“超级终端”窗口，此时就可以通过命令来操控和配置交换机了，如图 3-13 所示。

图 3-13　交换机配置窗口

2. 远程配置

1）Telnet 方式

Telnet 协议是一种远程访问协议，可以用它登录到远程计算机、网络设备或专用的 TCP/IP 网络。在操作系统中都内置有 Telnet 客户端程序，可以用它来实现与远程交换机的通信。

在使用 Telnet 连接至交换机前，应当确认已经做好了以下准备工作：

- 在用于管理的计算机中安装有 TCP/IP 协议，并配置好了 IP 地址信息。
- 在被管理的交换机上已经配置好了 IP 地址信息。如果尚未配置 IP 地址信息，则必须通过 Console 端口进行配置。

- 在被管理的交换机上建立了具有管理权限的用户账户。如果没有建立新的账户，交换机默认的管理员账户为 Admin。

假设前面已经设置交换机的 IP 地址为 192.168.0.1，下面只介绍进入配置界面的步骤。

(1)单击“开始”按钮，选择“运行”菜单项，然后在弹出的对话框中输入“telnet 192.168.0.1”，如图 3-14 所示。如果为交换机配置了名称，则也可以直接在 Telnet 命令后面空一个空格后输入交换机的名称。

图 3-14 “运行”对话框

(2)输入完成后单击“确定”按钮，建立与远程交换机的连接。如图 3-15 所示为计算机通过 Telnet 命令与交换机建立连接时显示的界面。

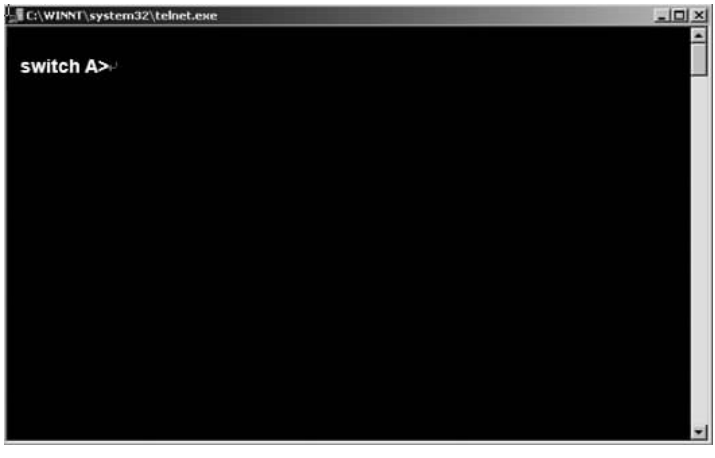

图 3-15 计算机与交换机建立连接界面

2)Web 浏览器方式

当利用 Console 端口为交换机设置好 IP 地址信息并启用 HTTP 服务后，即可通过 Web 浏览器访问交换机，并可通过浏览器修改交换机的各种参数并对交换机进行管理。在利用 Web 浏览器访问交换机之前，应确认已经做好以下准备工作：

- 在用于管理的计算机中安装 TCP/IP 协议，且在计算机和被管理的交换机上都已经配置好 IP 地址信息。
- 用于管理的计算机中安装有支持 Java 的 Web 浏览器，如 Internet Explorer 4.0 及以上版本、Netscape 4.0 及以上版本，以及 Oprea with Java。
- 在被管理的交换机上建立了拥有管理权限的用户账户和密码。
- 被管理交换机的 IOS 支持 HTTP 服务，并且已经启用了该服务。否则，应通过 Console 端口升级 IOS 或启用 HTTP 服务。

通过 Web 浏览器方式进行配置的方法如下：

(1)把计算机连接在交换机的一个普通端口上，在计算机上运行 Web 浏览器。在浏览器的地址栏中输入被管理交换机的 IP 地址(如 61.159.62.182)或为其指定的名称。按 Enter 键，弹出如图 3-16 所示对话框。

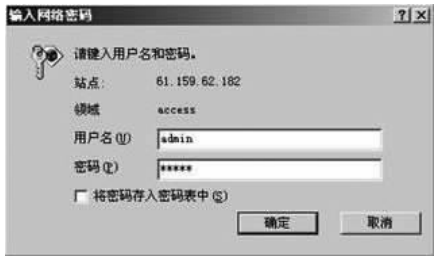

图 3-16　以 Web 浏览器方式登录交换机

(2)分别在“用户名”和“密码”框中输入拥有管理权限的用户名和密码。用户名和密码应当事先通过 Console 端口进行设置。

(3)单击“确定”按钮，即可建立与被管理交换机的连接，在 Web 浏览器中显示交换机的管理界面。

3.2.2　交换机的配置模式

交换机提供了用户模式与特权模式两种基本的命令执行级别，同时还提供了全局配置模式和特殊配置模式。其中，特殊配置模式又分为接口配置、Line 配置、VLAN 配置等多种类型，以允许用户对交换机进行全面的配置与管理。

1. 用户模式

当用户通过交换机的控制台或 Telnet 登录到交换机时，此时所处的命令执行模式就是用户模式。在该模式下，可以简单查看交换机的软、硬件版本信息，并进行简单的测试，但不能更改配置文件。

用户模式的提示符是：

```
Switch>
```

其中 Switch 是主机名，在该模式下直接输入“?”并按回车键，可获得该模式下允许执行的命令清单及相关说明，如：

```
Switch>?
```

若要获得某一命令的进一步帮助信息，可在命令之后加“?”，如：

```
Switch>show ?
```

在 Cisco IOS 中，可随时使用“?”来获得帮助。输入命令时可只输入命令的前几个字符，然后用 Tab 键自动补齐。

2. 特权模式

在用户模式下，执行 enable 命令，进入特权模式。在该模式下可以对交换机的配置文件进行管理，查看交换机的配置信息，进行网络测试与调试等。

特权模式的提示符为：

```
Switch#
```

在该模式下直接输入“?”并按 Enter 键，可获得该模式下允许执行的命令清单及相关说明。返回用户模式，可执行 exit 或 disable 命令，重新启动交换机可执行 reload 命令。

3. 全局配置模式

在特权模式下，执行 configure terminal 命令，则进入全局配置模式。在该模式下可以配置交换机的全局性参数(如主机名、登录信息等)。

全局配置模式的提示符为：

```
Switch(config)#
```

例如，若要设置交换机的名称为 st1，可使用 hostname 命令来设置，其配置命令为：

```
Switch(config)#hostname st1
St1(config)#
```

若要从全局配置模式返回特权模式，可执行 exit、end 命令或按 Ctrl+Z 组合键。

4. 接口配置模式

在全局配置模式下，执行 interface 命令，则进入接口配置模式。在该模式下，可以对选定的端口进行配置，并且只能执行配置交换机端口的命令。

接口配置模式的提示符为：

```
Switch(config-if)#
```

例如，若要设置交换机的 0 号模块上的第一个快速以太网端口的通信速率为 100 Mb/s，并采用全双工方式，则配置命令为：

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#speed 100
Switch(config-if)#duplex full
```

若要从接口配置模式退回全局配置模式，可执行 exit 命令。如果退回特权模式，可执行 end 命令或按 Ctrl+Z 组合键。

5. Line 配置模式

在全局配置模式下，执行 line vty 或 line console 命令，则进入 Line 配置模式。该模式主要用于对虚拟终端(vty)和控制台端口进行配置。

Line 配置模式的提示符为：

```
Switch(config-line)#
```

若要从 Line 配置模式退回全局配置模式，可执行 exit 命令。如果退回特权模式，可执行 end 命令或按 Ctrl+Z 组合键。

6. VLAN 配置模式

在特权模式下，执行 vlan database 命令，则进入 VLAN 配置模式。在该模式下可实现对 VLAN 的创建、修改或删除等配置操作。

VLAN 配置模式的提示符为：

```
Switch(vlan)#
```

若要从 VLAN 配置模式退回特权模式，可执行 exit 命令。

注意：(1)在使用命令对交换机进行各项配置时，一定要先进入到相应的配置模式下，因为交换机的配置命令只有在相应模式下才会有效。

(2)各模式的层次不可混淆。从接口模式不能直接进入 VLAN 模式，只能先使用 end 命令返回特权模式，再利用 VLAN 命令进入 VLAN 模式。

3.2.3　交换机基本配置命令

熟练掌握一定的交换机配置命令对一个网络管理员或工程师来说是十分必要的。下面详细介绍在命令界面下常用的命令，假设交换机的名称为 Switch。

1.模式转换命令

(1)enable：从用户模式进入特权模式。例如：

```
Switch>enable
Switch#
```

(2)disable：从特权模式退回用户模式。例如：

```
Switch#disable
Switch>
```

(3)configure：从特权模式进入全局配置模式。例如：

```
Switch#configure terminal
Switch(config)#
```

(4)interface：在全局模式下运行此命令，将选择一个端口进行设置，同时进入到接口配置模式。例如，以下命令是选中快速以太网端口 1：

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#
```

(5)exit：退回到上级命令模式。例如：

```
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

(6)end：直接从任何一种配置模式退回到特权模式。例如：

```
Switch(config-if)#end
Switch#
```

(7)vlan：在全局模式下运行此命令，将建立一个 VLAN，并进入 VLAN 配置模式。例如，要建立一个 vlan-id 为 10 的 VLAN，命令如下：

```
Switch(config)#vlan 10
Switch(config-vlan)#
```

2.配置主机名和管理 IP

1)配置主机名

为了管理方便，可以为一台交换机配置主机名来标识它。设置交换机的主机名可在全局模式下，通过 hostname 配置命令实现，其配置命令为：

```
Switch(config)#hostname hostname
```

其中，第一个 hostname 为配置命令，第二个 hostname 指的是为交换机配置的主机名。

默认情况下，交换机的主机名为 Switch。当网络中有多台交换机时，通常根据交换机的应用场所，为其设置一个具体的主机名。例如：

```
Switch(config)#hostname student        //将交换机主机名设为 student
Student(config)#exit
```

2)配置管理 IP 地址

在二层交换机中,IP 地址仅用于远程登录管理交换机,对于交换机的正常运行不是必需的。若没有配置管理 IP 地址,则交换机只能采用控制台端口进行本地配置和管理。

默认情况下,交换机的所有端口均属于 VLAN 1,VLAN 1 是交换机自动创建和管理的,不能由用户自己建立和删除。每个 VLAN 只有一个活动的管理地址。因此,对第二层交换机设置管理地址之前,首先应选择 VLAN 1 接口,然后再利用 ip address 配置命令设置管理 IP 地址,其配置命令为:

```
Switch(config)#interface vlan vlan-id
Switch(config-if)#ip address address netmask
```

其中,vlan-id 代表要选择配置的 VLAN 号,第二个 address 为设置的管理 IP 地址,netmask 为子网掩码。例如:

```
Student(config)#interface vlan 1
Student (config-if)#ip address 192.168.1.3 255.255.255.0
                                    //设置主机名为 student 的 IP 地址和子网掩码
Student (config-if)#ip default-gateway 192.168.1.1
                                    //设置主机名为 student 的缺省网关
```

interface vlan 配置命令用于访问指定的 VLAN 接口。二层交换机没有三层交换机功能强大,VLAN 间无法实现相互通信,VLAN 接口仅作为管理接口。

若要取消管理 IP 地址,选中 VLAN 1 接口,执行 no ip address 配置命令即可。

3.登录密码设置

1)控制台登录口令的设置

交换机的 Console 端口的编号为 0,通常需要利用该端口进行本地登录,以实现对交换机的配置和管理。为安全起见,应该为该端口的登录设置密码。配置命令为:

```
Switch(config)#line console 0                    //进入控制台端口的 line 配置模式
Switch(config-line)#password abc                 //设置本地登录密码 abc
Switch(config-line)#login                        //使密码生效
Switch(config-line)#end                          //返回特权模式
Switch#
```

2)配置远程登录密码

要想通过 Telnet 或 Web 方式来登录和管理交换机,除了要设置交换机的管理 IP 地址外,还要设置远程登录密码和交换机的特权密码。交换机支持多个虚拟终端,一般为 16 个(0～15),只有设置了密码,才允许远程登录。例如,对 0～3 条虚拟终端线路设置密码,则交换机就允许同时有 4 个 Telnet 登录连接,其配置命令为:

```
Switch(config)#line line vty 0 3                 //对 0～3 条虚拟终端线路进行设置
Switch(config-line)#password hello               //设置远程登录密码为 hello
Switch(config-line)#login                        //使密码生效
Switch(config-line)#end                          //返回特权模式
Switch#
```

3)特权模式密码设置

```
Switch(config)#enable password welcome           //设置特权模式密码为 welcome
Switch(config)#enable secret welcome             //设置特权模式密码为 welcome
```

两者的区别：第一种方式设置的密码是以明文方式存储的，第二种方式设置的密码是以加密方式存储的。前者设置的密码使用 show run 命令可见，后者则不可见。建议使用第二种方式设置特权模式密码。

4. 配置提示信息

当用户登录交换机时，可能需要告诉用户一些必要的信息。配置提示信息可以达到这一目的。

1）配置每日通知

用户通过本地或远程登录到交换机时，这些消息将会显示。在全局模式下，可以通过 banner 命令来设置每日通知信息：

```
Switch(config)#banner motd c message c
```

其中，c 为分界符，可以是任何字符。输入分界符后按 Enter 键在下一行输入文本，再次输入分界符并按 Enter 键结束文本的输入。message 为每日通知的信息，其中不能包含分界字符，并且不能超过 255 个字节。

2）配置登录标题

登录标题给登录交换机的用户提供一些常规的提示信息，显示在每日通知之后。设置命令为：

```
Switch(config)#banner login c message c
```

各个参数与设置每日通知信息命令相同。

例如，设置每日通知信息为“Happy new year!”，登录标题信息为“This is a cisco switch.”。

```
Switch(config)#banner motd #
Enter TEXT message. End with the character '#'.
Happy new year!
#
Switch(config)#banner login #
Enter TEXT message. End with the character '#'.
This is a cisco switch.
#
Switch(config)#end
Switch#logout                                    //退出登录状态
```

重新登录后会出现：

```
Happy new year!
This is a cisco switch.
User Access Verification
Password:
Switch>
```

5. 保存配置信息

交换机的当前配置文件 running-config 保存在 DRAM 中，当交换机断电时信息将丢失，所以配置好交换机后必须将配置文件保存到 NVRAM 中，文件名为 startup-config。其命令如下：

```
Switch#write memory
```

或

Switch#copy running-config startup-config

6.查看配置信息

使用 show 命令来显示交换机的相关配置。

1)查看交换机操作系统的版本

Switch#show version

2)查看交换机某接口的信息

Switch#show interface iftype mod/port

其中,iftype 代表端口类型,通常有 Ethernet、FastEthernet、GigabitEthernet 和 Ten Gigabit Ethernet 等。mod/port 代表端口所在的模块和在该模块中的编号。

例如,要查看 S3550 交换机 0 号模块的 24 号端口的信息,则查看命令为:

Switch#show interface fastethernet 0/24

显示结果如下:

Interface:fastethernet100BaseTX 0/24

Description:

Adminstatus:up

Operstatus:down

Hardware:10/100BaseTX

Mtu:1500

Lastchange:0d:0h:0m:0s

Adminduplex:auto

Operduplex:unknown

Adminspeed:auto

Operspeed:auto

FlowcontroladminStatus:Off

FlowcontroloperStatus:Off

Priority:0

Broadcast blocked:disable

Unknown multicast blocked:disable

Unknown unicast blocked:disable

3)显示接口 IP 信息

Switch#show ip interface brief

4)显示交换机 MAC 地址表

Switch#show mac-address-table

5)显示交换机正在运行的配置

Switch#show running-config

6)显示交换机存储在 NVROM 中的启动配置

Switch#show startup-config

提示:以上命令可以使用“show ?”来查看。

7.帮助命令

在交换机的所有命令中,有一个最基本的命令,那就是帮助命令“?”,在任何命令模式

下，只需输入“?”，即显示该命令模式下所有可用到的命令及其用途，这就是交换机的帮助命令。可以在一个命令和参数后面加“?”，以寻求相关的帮助。例如，想看一下在特权模式下有哪些命令可用，那么，可以在“#”提示符后输入“?”，并按 Enter 键。

另外，“?”还具有局部关键字查找功能。也就是说，如果只记得某个命令的前几个字符，那么，可以使用“?”让系统列出所有以该字符或字符串开头的命令。但是，在该字符或字符串与“?”之间不得有空格。例如，在特权模式下键入“C?”，系统将显示以 C 开头的所有命令。

还要说明的一点是，Cisco IOS 命令均支持缩写命令，也就是说，没有必要输入完整的命令和关键字，只要输入的命令所包含的字符长到足以与其他命令区别就够了。例如，可将 show configure 命令缩写为 sh conf，然后按 Enter 键即可。

8. 配置交换机接口

1）配置接口类型

交换机接口类型分为 Ethernet（10 Mb/s）、FastEthernet（10/100 Mb/s）、GigabitEthernet（1 000 Mb/s）。在实际配置接口时，交换机接口类型一定要写正确。一般可先用 show vlan 命令查看一下各接口的类型。在实际配置时，各接口类型可用前三个字符缩写。其命令格式为：

```
Switch(config)#interface type mod/port
```

其中，type 表示端口类型，通常有 Ethernet、FastEthernet 和 GigabitEthernet；mod 表示交换机的模块号；port 表示端口号。

2）配置接口描述、速度、双工模式

交换机有很多接口，在管理时可以为交换机的每个接口设置一个名字，方便记忆，可以用 description 命令来描述各个接口。其命令格式为：

```
Switch(config-if)#description string
```

其中，string 表示接口的描述信息。

duplex 命令用来配置接口的双工模式，其命令格式为：

```
Switch(config-if)#duplex {auto|full|half}
```

其中，auto 表示自动检测双工模式，full 表示全双工模式，half 表示半双工模式。

speed 命令用来配置交换机接口的速率，其命令格式为：

```
Switch(config-if)#speed {10|100|1000|auto}
```

其中，auto 表示自动接口速度，在 GigabitEthernet 接口上只能设为 1 000。

3）启用接口

交换机接口默认设置为关闭（shutdown），启用命令为：

```
Switch(config-if)#no shutdown
```

例如，要配置交换机 0 号模块上第一个快速以太网接口的名字为 teacher，接口模式为全双工，接口速率为 100 Mb/s，并启用该端口，其命令为：

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#description teacher
Switch(config-if)#duplex full
Switch(config-if)#speed 100
Switch(config-if)#no shutdown
```

3.3 桥接环路与生成树协议

随着交换技术在网络中的应用，保证各种网络终端包括服务器在内的设备间通信成为一项重要的任务，绝大多数情况下交换网络与交换设备之间采用多条链路连接，形成桥接环路来保证线路上的单点故障不会影响正常的网络通信，但交换机的基本工作原理导致这样的设计会在交换网络中产生严重的广播风暴。生成树协议是解决交换网络中链路冗余备份和产生广播风暴之间矛盾的重要技术。

另外，网络的关键设备之间由于受物理带宽的限制而产生通信瓶颈，解决的办法是在两个设备之间连接多条物理线路，采用 IEEE 802.3ad 标准将几个物理接口捆绑在一起而形成一个逻辑端口，从而达到增大带宽的目的。

3.3.1 冗余拓扑结构

组建计算机网络的目的是进行数据通信和资源共享，在网络中通常使用交换机作为网络连接设备。如某公司的销售部和财务部，这两个部门之间经常要进行通信：文件的共享、资料的传递、视频会议等。每个部门都通过一台交换机把本部门的主机连接起来，之后通过一根交叉线把两个部门的交换机连接起来，其网络拓扑结构如图 3-17 所示。这样，两个部门间的任何两台主机之间都能够进行通信。但如果连接两台交换机的交叉线或者端口出现了问题，就会导致两个部门间的通信中断，即出现单点故障的问题。

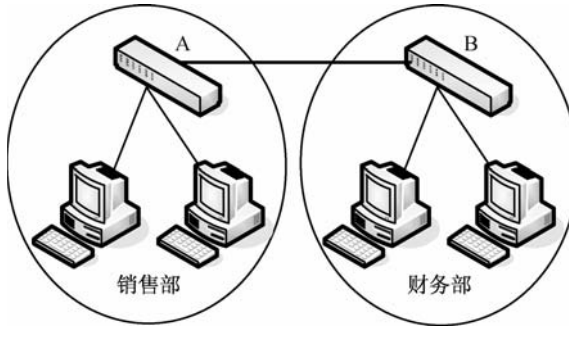

图 3-17 非冗余链路

为解决这种单点故障的问题，通常在进行网络拓扑时用冗余链路的办法来增强网络的健壮性，即在两个交换机之间再增加一条网线以作备份，如图 3-18 所示。

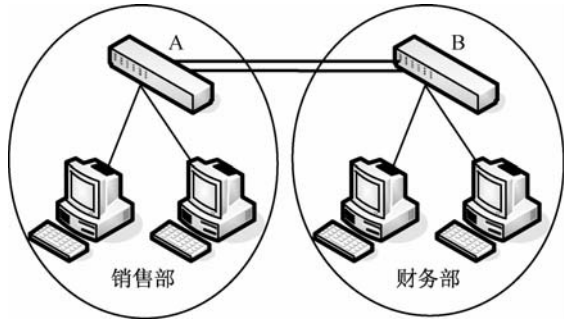

图 3-18 冗余链路

3.3.2　桥接环路的危害

如果两条网线同时连接到两个交换机的端口上，出现了网络环路，将产生广播风暴、多帧复制和 MAC 地址表不稳定等现象，严重影响网络正常运行。

1. 广播风暴

根据交换机的工作原理，在交换机中有一张 MAC 地址表，当接到一个帧时，则在此 MAC 地址表中寻找目的 MAC 地址对应的端口，如果找到，则将此帧直接转发到此端口上去；如果找不到，则向交换机的所有端口广播。假设销售部里的主机 A 发送一个广播帧，那么这个广播帧会传到财务部的网段上，从而又到达交换机 B 上，而交换机 B 会进行统一的操作。周而复始，在两个部门中这个广播包一直扩散，就形成了广播风暴。广播风暴会严重影响交换机性能，甚至会耗尽交换机的内存资源，最终耗尽所有带宽资源，阻塞网络通信。

2. 多帧复制

多帧复制是由于环路存在，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，严重时会导致网络连接的中断。假设主机 A 在交换机 A、B 初始化时，发出一个单播包给路由器，路由器首先收到一个由主机 A 发过来的数据包，而这个数据包会同时发向交换机 A、B。那么 A、B 交换机该如何处理这个单播包？它们会查找自己的 MAC 地址表，如果目的 MAC 地址在自己的 MAC 地址表中没有匹配的出口，那么交换机 A、B 会进行同样的操作——泛洪。那样路由器会通过交换机 A、B 的泛洪又收到多次同样的数据包。对于认证网络体系来说，同一时刻收到很多同样的数据包，就会给网络带来问题。

3. MAC 地址表不稳定

主机 A 在交换机 A、B 初始化时发一个单播包。对于交换机 A 来说，它从 prot1 端口收到一个单播帧，因为交换机在初始化时，MAC 地址表为空。这样交换机 A 会进行两个动作：一个是把这个数据帧泛洪，另一个是学习主机 A 的 MAC 地址，那么交换机 A 会认为自己的 port1 端口上连接了一台 MAC 地址为 A 的主机。而通过交换机 B 泛洪，由财务部门传递到交换机 A 的这个数据帧发到了 A 的 port2 端口上。那么此时交换机 A 又会认为自己的 port2 上也连接了一个 MAC 地址为 A 的主机。但是一台主机不可能同时连接到交换机的两个端口上，从而给网络带来问题。由于这一过程会导致 MAC 地址表的多次刷新，从而导致交换机内存资源被严重耗用，影响交换机的交换能力，使得整个网络的运行效率降低。

3.3.3　生成树协议

生成树协议(spanning tree protocol，STP)最初是由美国数字设备公司开发的，后经电气电子工程师学会进行修改，最终制定了相应的 IEEE 802.1d 标准。

1. 生成树协议的功能

为了保证网络的可靠性和稳定性，常常需要网络提供冗余拓扑结构，这样又会出现桥接环路，从而引起广播风暴、多帧复制、MAC 地址表不稳定等问题。因此，在网络中必须有一个机制来阻止环路的生成。

生成树协议的主要功能就是解决网络中由于备份连接所产生的环路问题。当网络中有

环路时，生成树协议通过生成树算法生成一个没有环路的网络。当交换机间存在多条链路时，只启动最主要的一条链路，而将其他链路都屏蔽掉，将其作为备用链路，当主链路存在问题时，这种算法会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。

生成树协议通过从软件层面修改网络物理拓扑结构来构建一个无环逻辑转发树形拓扑结构，发现故障并随之进行恢复，自动更新网络拓扑结构，使在任何时候都选择可能的最佳树形结构。它提供了物理线路的冗余连接，消除了网络风暴，从而提高了网络的稳定性和降低了网络故障的发生率。

在生成树协议发展过程中，不断克服以前的缺陷，开发新的特性，按照功能的改进情况，可以把生成树协议的发展过程划分为 3 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。

2. 生成树协议的端口状态

在生成树协议运行过程中，交换机的端口会经过一系列的状态。

- 阻塞(blocking)：刚开始启用端口后，端口不能接收或传输数据，不能学习帧的 MAC 地址，只能接收 BPDU。如果检测到一个回路，或者端口失去了根端口或指定端口的状态，就会返回到阻塞状态。
- 监听(listening)：一个端口成为一个根端口或指定端口，则转入监听状态。该端口不能接收或传输数据，也不能把 MAC 地址加入到它的地址表，只能接收或发送BPDU。
- 学习(learning)：在转发延时计时时间之后，端口进入学习状态。学习 MAC 地址并将其加入到它的 MAC 地址表中。此时该端口不能传输数据，但可以接收或发送 BPDU。
- 转发(forwarding)：在下一次转发延时计时时间之后，端口进入转发状态。现在端口能够接收并发送数据，接收并转发 BPDU，并开始学习 MAC 地址。
- 禁用(disabled)：为了管理目的端口，或者发生端口故障，将其关闭，不收发任何报文。

3. 生成树协议的工作原理

为了实现 STP 的功能，交换机之间必须要进行一些信息的交流，这些信息交流单元就称为桥协议数据单元 BPDU。BPDU 是一种二层报文，其目的 MAC 地址是多播地址 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。该报文的数据区里携带了用于生成树计算的所有有用的信息，该报文的格式如表 3-1 所示。

表 3-1 BPDU 报文格式

ProtocolID(2)	Version(1)	Type(1)	Flag(1)	RootBID(8)	RootPathCost(4)
SenderBID(8)	PortID(2)	M-Age(2)	MaxAge(2)	HelloTime(2)	ForwardDelay(2)

各个参数说明如下：

- ProtocolID：协议 ID 号，该值总为 0，当前保留未使用。
- Version：版本，STP 的版本，数值大的被认为是最新定义的。
- Type：BPDU 类型。
- Flag：表示拓扑变化，值为 0 表示没变；值为 1 表示改变。
- RootBID：根交换机(RootBridge)的 ID，表示当前网络中的根交换机，由 2 字节的优

先级和 6 字节的 MAC 地址组成。

- RootPathCost：本交换机到根交换机的路径成本，即根路径成本。
- SenderBID：发送 BPDU 的网桥 ID。
- PortID：发送该报文的端口 ID，每个端口值都是唯一的。
- M-Age：BPDU 有效存活时间，从根交换机发出 BPDU 之后的跳数，每经过一个交换机都递减 1，所以它本质上是到达根交换机的跳数。
- MaxAge：保存 BPDU 的最长时间。交换机在将根交换机看做不可用之前保留根交换机 ID 的最长时间，最长为 20 s。
- HelloTime：发送 BPDU 的周期，默认为 2 s。
- ForwardDelay：转发延迟，指的是全网传输延迟。

网络中所有的交换机每隔一定的时间——HelloTime 就发送和接收 BPDU 数据帧，并且用它来检测生成树拓扑的状态，通过生成树算法得到生成树。其工作原理如下：

(1)在网络中选出一台根交换机。刚开始所有的交换机都认为自己是根交换机，交换机向本局域网广播发送配置 BPDU，具有最高优先级的交换机被选为根交换机，如果两个交换机有相同的优先级，拥有较小的 MAC 地址的交换机成为根交换机。

(2)每个交换机都计算出到根交换机的最短路径，在每个非根交换机上选出一个根口(RootPort)，即提供最短路径花费到根交换机的端口。

每个交换机端口都有一个根路径花费，根路径花费是该交换机到根交换机所经过的各个网段的路径花费总和。一台交换机中根路径花费的值最低的端口被选为根口，若多个端口的根路径花费相同，则具有最高优先级的端口为根口。路径花费由链路速度决定，由 IEEE 指定，如表 3-2 所示。

表 3-2　各种链路的路径花费

链路速度	路径花费
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

(3)在每个网段上选择一台交换机作为指定交换机，它属于该网段中根路径花费最少的交换机。把该网段和指定交换机连接起来的端口就是该网段的指定端口，该端口处理该段网络的流量。

注意：根口就不再参与指定端口的竞争，根交换机上的接口都是指定端口。

(4)根口和指定端口进入转发状态。其他非指定端口，即冗余端口处于阻塞状态。

这样，在决定了根交换机、交换机的根口以及每个网段的指定交换机和指定端口后，一个生成树的拓扑结构也就确定了。当交换机网络的生成树结构确定后，网络就稳定了。此时网络的状况为：网络中只有一台根交换机；每台非根交换机只有一个根口，每个网段只有一个指定端口，非根端口和非指定端口都处于阻塞状态而暂停使用，根端口和指定端口转发数据，被阻塞的端口不转发或丢弃数据。

4. 拓扑变化

拓扑信息在网络上传播有一个时间限制，这个时间限制是 M-Age。每个交换机存储来

自本网段选取端口的协议信息，并监视这些信息的存储时间。在正常稳定状态下，根交换机定期发送消息以保证拓扑信息不超时。

当某个交换机检测到拓扑变化时，它将以拓扑变化通知定时器的时间间隔，定期向根交换机方向的指定交换机发送拓扑变化通知，直到收到了指定交换机发来的确认拓扑变化信息。同时指定交换机重复以上过程，继续向根交换机方向的交换机发送拓扑变化通知。这样，拓扑变化的通知最终传到根交换机。根交换机收到这样一个通知，或其自身改变了拓扑结构，它将在一段时间内发送拓扑变化。所有交换机将收到新的配置消息，并根据信息对自己的地址表进行相应处理。然后所有交换机重新选举确定根交换机、根口、每个网段的指定交换机和指定端口，这样生成树的拓扑结构也就重新确定了。

5. 增强的 VLAN 的生成树

增强的 VLAN 的生成树(PVST+)为每个 VLAN 维护一个单独的生成树实例，默认情况下，在没有手工禁用 STP 的前提下，每个配置的 VLAN 都将运行单个生成树。PVST+能够以每个 VLAN 为基础提供负载均衡。

通常情况下，Catalyst 交换机 MAC 地址表最多可以容纳 1 024 个地址，MAC 地址表作为 VLAN 生成树中网桥 ID 的 MAC 地址部分。启用 MAC 地址缩减特性，使用了“系统 ID 扩展”附加字段，只能将交换机优先级指定为 4 096 的倍数。

通常情况下，辅助根所选用的优先级值是 8 192，实际情况下，可以有多台交换机担当备份根交换机。

为接口分配的路径花费越低，生成树也就越优先选择该接口，接口路径花费的取值范围是1～200 000 000。

6. 快速生成树协议

快速生成树协议(RSTP)能够显著加快重新计算生成树的速度，RSTP 不仅定义了其他端口角色，如替代端口、备份端口，而且还定义了 3 种端口状态：丢弃状态、学习状态和转发状态。

RSTP 802.1w 丢弃状态表示 802.1d STP 的禁用、阻塞和监听状态的合并。如果活跃的根端口发生故障，那么替代端口将成为根端口；如果现有的指定端口发生故障，那么备份端口将成为指定端口。当 RSTP 检测到网络中有一台交换机运行了 STP，则 RSTP 会自动降为 STP 来使用。如果指定端口在 3 个连续的 HelloTime 时间内没有接收到任何 BPDU，那么网桥将立即对协议信息进行老化处理。如果最大寿命计时器到期，那么协议也将立即被老化处理。在 RSTP 中，BPDU 的发送可以担当网桥之间的 keep-alive 机制。如果连续 3 次未收到 BPDU，那么网桥就相信它已经将到达邻接根网桥或指定网桥的连接丢失。

当链路发生转变的时候，边缘端口不会产生拓扑变更，如果边缘端口接收到 BPDU，那么它将立即放弃边缘端口的状态，并且成为一个正常的生成树端口。

默认情况下，如果端口工作在全双工模式，那么就认为它是点到点链路类型；如果端口工作在半双工模式，那么就认为它工作在共享介质之上。

3.3.4 生成树协议的配置命令

前面介绍了为什么使用 STP 以及 STP 的工作原理，下面以思科交换机为例介绍 STP 的主要配置命令。

1. 启动、关闭 STP

交换机的默认状态是关闭 STP，所以使用 STP 时，要先启动。启动 STP 的命令应在全局模式下进行。配置命令如下：

```
Switch(config)#spanning-tree
```

关闭 STP 的命令配置如下：

```
Switch(config)#no spanning-tree
```

2. 设置 STP 的类型

思科交换机支持的 STP 类型包括 PVST、PVST＋、Rapid-PVST＋、MISTP 和 MSTP 等。配置命令如下：

```
Switch(config)#spanning-tree mode {pvst|mst|rapid-pvst}
```

该命令设置 STP 类型默认为 PVST，若选 pvst 则允许 PVST＋；若选 mst 则允许 MSTP 和 RSTP；若选 rapid-pvst 则允许 Rapid-PVST＋。

3. 设置交换机的优先级

交换机的优先级决定哪个交换机为网络的根交换机，同时也关系到整个网络的拓扑结构。在交换机的选择中，先比较交换机的优先级，如果优先级数值小，则此交换机为根交换机。默认情况下所有交换机优先级均为 32 768，这样就要再比较交换机的 MAC 地址，但网络管理员很难知道哪个交换机的 MAC 地址最小，这样由 STP 选出来的交换机往往不是所希望的，不利于整个网络的稳定。为了更好地管理网络，使 STP 生成的逻辑树形网络与物理拓扑保持一致，往往把核心交换机指定为根交换机。因此，需要将核心交换机的优先级配置高一些，如 0 或 4 096 就可以了。交换机 STP 优先级的设置值有 16 个，都为 4 096 的整数倍。配置命令如下：

```
Switch(config)#spanning-tree priority priority
```

其中，第二个 priority 为优先级的取值，范围是 0～61 440，均为 4 096 的倍数，默认值为 32 768。

4. 设置端口的优先级

端口的优先级决定哪个端口为根口。高优先级（数值小）的端口成为根口，进入转发状态，低优先级（数值大）的端口进入 Discarding 状态。如果端口优先级一样，端口号小的那个进入转发状态。

要想人为指定哪个端口进入 Forwarding 状态，其配置命令为：

```
Switch(config)#spanning-tree port-priority priority
```

其中，priority 为端口的优先级，范围是 0～240，都为 16 的整数倍，默认值为 128。

如果要把端口的优先级恢复到默认值，其配置命令为：

```
Switch(config)#no spanning-tree port-priority
```

5. 设置端口的路径花费

端口的路径花费的设置关系到本交换机的根口的选择，默认值是系统自动计算的，速度高，花费小。配置命令如下：

```
Switch(config)#spanning-tree path cost
```

其中，cost 为端口的路径花费，范围是 0～200 000 000，默认值为根据 interface 的链路速率自动计算的数值，一般不需要改变。

6. 设置交换机发送 BPDU 的时间间隔

HelloTime 是交换机定时发送 BPDU 报文的时间间隔。配置命令如下：

```
Switch(config)#spanning-tree hello-time seconds
```

其中，seconds 为 HelloTime 的值，范围是 1～10 s，默认值为 2 s。

如果要把 HelloTime 恢复到默认值，其配置命令为：

```
Switch(config)#no spanning-tree hello-time
```

7. 设置端口状态改变的时间间隔

Forward-Delay Time 是端口状态改变的时间间隔。配置命令如下：

```
Switch(config)#spanning-tree forward-time seconds
```

其中，seconds 为 Forward Time 的值，范围是 4～30 s，默认值为 15 s。

如果要把 Forward-Delay Time 恢复到默认值，其配置命令为：

```
Switch(config)#no spanning-tree forward-time
```

8. 设置 BPDU 报文生存的最长时间

Max-Age Time 是 BPDU 报文消息生存的最长时间。配置命令如下：

```
Switch(config)#spanning-tree max-age seconds
```

其中，seconds 为 Max-age Time 的值，范围是 6～40 s，默认值为 20 s。

如果要把 Max-Age Time 恢复到默认值，其配置命令为：

```
Switch(config)#no spanning-tree max-age
```

9. 设置每秒钟最多发送的 BPDU 个数

Tx-Hold-Count 是每秒钟最多发送的 BPDU 个数。配置命令如下：

```
Switch(config)#spanning-tree tx-hold-count numbers
```

其中，numbers 为 Tx-Hold-Count 的值，范围是 1～10 个，默认值为 3 个。

10. 配置端口的连接类型

Link-type 是该端口的连接类型，主要有两种类型：point-to-point 和 shared。交换机会根据端口的双工状态来自动设置，全双工的端口就设 Link-type 为 point-to-point，半双工就设为 shared。当 Link-type 的值为 point-to-point 时，RSTP 能快速地收敛。当不设置该值时，也可以强制设置 Link-type 来决定端口的连接是不是点对点连接。配置命令如下：

```
Switch(config)#spanning-tree link-type point-to-point/shared
```

11. 显示设置信息

```
Switch#show spanning-tree                          //显示生成树的全部信息
Switch#show spanning-tree interface interface-id   //显示指定 interface 的信息
```

当 STP 配置完成后，可以回到特权模式下查看 STP 的全部信息和相关端口信息，根据显示的信息来判断配置是否达到要求。

3.4 三层交换机

三层交换机是指具备三层路由功能的交换机，其端口可以实现基于三层寻址的分组转发。传统的交换技术是在 OSI 参考模型中的数据链路层进行操作的，而三层交换技术是在 OSI 参考模型的第三层——网络层实现了数据包的高速转发。因此，三层交换技术就是二层交换技术加三层转发技术。

3.4.1　三层交换机概述

出于安全和管理方便等方面的考虑，VLAN 技术在网络中大量应用，不同 VLAN 间的通信要经过路由器转发，当局域网中数据流量很大时，路由器就成为了网络的瓶颈。

为了解决局域网的这个瓶颈问题，很多单位（如企业内部、学校和小区）建设局域网时都采用了三层交换机。三层交换机是一个具有三层交换功能的设备，是一个带有三层路由功能的二层交换机，它是交换机和路由器的有机结合，并不是简单地把路由器设备的硬件和软件叠加在局域网交换机上。

1. 三层交换机与路由器的区别

三层交换机和路由器都具有路由功能，但是三层交换机并不等于路由器，同时也不可能取代路由器。它们之间具体有下面几点区别。

1）主要功能不同

许多宽带路由器不仅具有路由功能，还提供了交换机端口、硬件防火墙功能，其目的是使设备适用面更广，使其更加实用。三层交换机是具备了一些基本的路由功能的交换机，但它的主要功能仍是数据交换。也就是说三层交换机同时具备了数据交换和路由转发两种功能，而路由器仅具有路由转发这一种功能。

2）使用的场所不同

三层交换机主要是用于简单的局域网连接。正因如此，三层交换机的路由功能通常比较简单，路由路径远没有路由器那么复杂。

路由器是为了满足不同类型的网络连接，如局域网与广域网之间的连接、不同协议网络之间的连接等。不仅适用于同种协议的局域网间，更适用于不同协议的局域网与广域网间。

3）处理数据的方式不同

从技术上讲，路由器一般由基于微处理器的软件路由引擎执行数据包交换，而三层交换机通过硬件执行数据包交换。三层交换机在对第一个数据流进行路由后，将会产生一个 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再次路由，从而消除了路由器进行路由选择而造成网络延迟的问题，提高了数据包转发的效率。同时，三层交换机的路由查找是针对数据流的，它采用缓存技术，很容易利用 ASIC 技术来实现，因此，可以大大节约成本，并实现快速转发。而路由器的转发采用最长匹配的方式，实现复杂，通常使用软件来实现，转发效率较低。

总的来说，三层交换机与路由器之间存在着本质区别。在局域网中进行多子网连接，最好还是选用三层交换机，特别是在不同子网数据交换频繁的环境中。路由器虽然路由功能非常强大，但它的数据包转发效率远低于三层交换机，更适合于数据交换不很频繁的不同类型网络的互联。

2. 三层交换机的应用

在目前火爆的宽带网络建设中，三层交换机发挥着重要作用，一般被放置在企业网、校园网以及小区的中心和多个小区的汇聚层。三层交换机的出现，极大地改变了局域网的性能。正如路由器统治广域网一样，三层交换机将在今后主宰局域网。

很多网络的核心部分都用到三层交换机。三层交换机既有三层路由的功能，又具有二层交换的网络速度。三层交换机通过使用硬件交换机构实现了 IP 的路由功能，其优化的路由软件使得路由效率提高，解决了传统路由器软件路由的速度问题。因此，可以说三层交换

机具有“路由器的功能、交换机的性能”。

另外，连接子网少不了三层交换机。同一网络上的计算机如果超过一定数量（通常在200台左右，视通信协议而定），就很可能会因为网络上大量的广播而导致网络传输效率低下。为了避免在大型交换机上进行广播所引起的广播风暴，可将其进一步划分为多个VLAN。这样做将导致一个问题：VLAN之间的通信必须通过路由器来实现。但是传统路由器也难以胜任VLAN之间的通信任务，因为相对于局域网的网络流量来说，传统路由器的路由能力太弱，而且千兆级路由器的价格也是难以接受的。如果使用三层交换机上的千兆端口或百兆端口连接不同的子网或VLAN，就可以在保持性能的前提下，很经济地解决子网划分之后子网之间必须依赖路由器进行通信的问题，因此，三层交换机是连接子网的理想设备。

3. 三层交换机组网方案

三层交换机主要应用于局域网内部组网。例如，学校局域网、大型企业内部局域网和大型网吧的组网。下面是三层交换机的一个应用方案。

图3-19是一个标准的路由器作为主干结点的结构示意图。假如这个网络有1 000台主机和多个服务器，通过路由器和Internet连接。通常适应这种结构的路由器的分组处理速度达200～300 Kb/s。然而，这个网络在高峰时段要达到500～600 Kb/s。

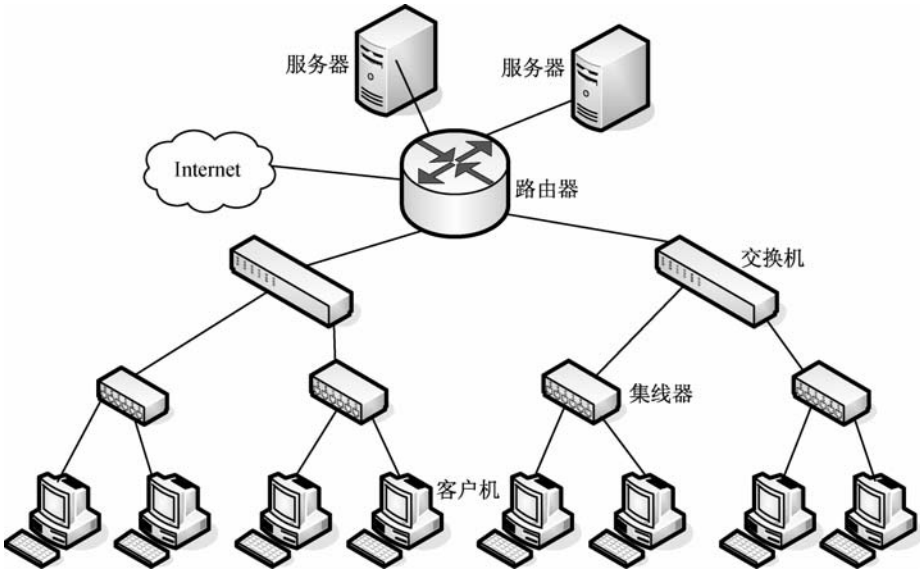

图3-19 路由器作为主干结点的网络结构

这种结构中，路由器不仅仅是连接的中心点，还是网络的瓶颈。为了解决这个问题，可以在主干部分增加一个三层交换机，如图3-20所示，这种配置能够提高网络的整体性能。因为三层交换机在服务器、路由器和交换机之间的分组交换能力平均可以达到1 Mb/s。一般情况下，一个网络系统内部的分组交换量应占80%，主要的分组交换任务由三层交换机完成，20%左右的与外部的通信量由路由器完成，这样的分工可以提高系统整体的效率。

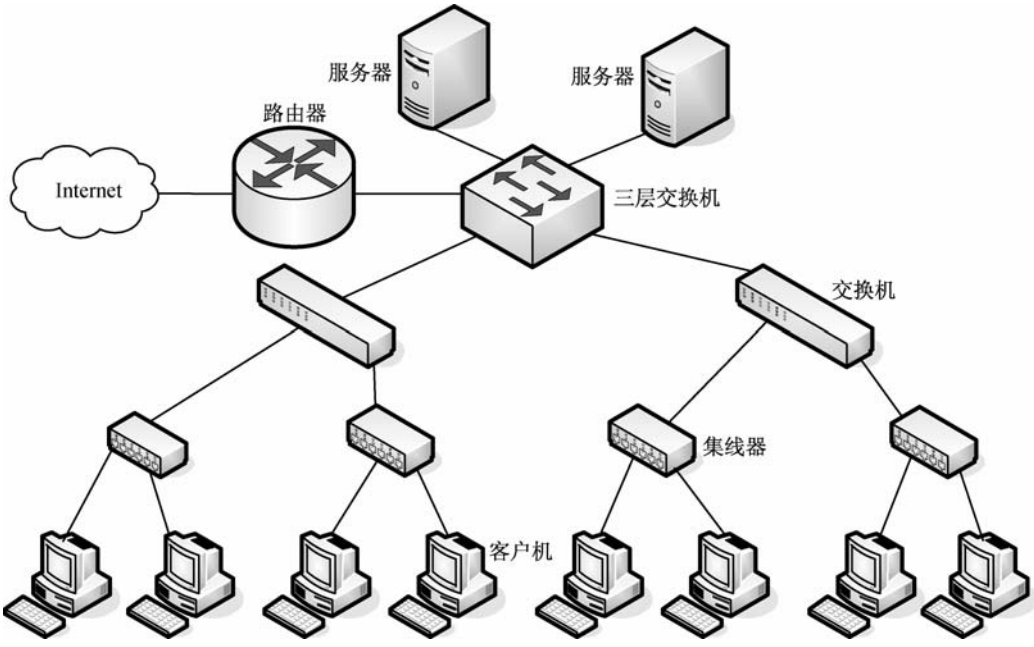

图 3-20　添加三层交换机后的网络结构

3.4.2　三层交换机的主要技术

传统路由器的各种功能都是由软件来实现的，并且可以通过软件升级来增强设备的功能，具有良好的扩展性和灵活性，但是配置复杂、价格高、吞吐量低。三层交换机在很大程度上弥补了这些缺点。三层交换机采用结构化、模块化的设计方法，仅仅针对 IP 协议采用专用集成电路实现交换和路由功能，限制特殊服务，软、硬件模块分工明确。

目前主要存在两类三层交换技术。

1. 报文到报文交换

报文到报文交换技术遵循这样一个过程，报文进入体系结构的第一层即物理接口，然后在第二层接受目的 MAC 检查，若能在第二层交换则进行第二层交换，否则进入第三层，在第三层，报文要经过路径确定、地址解析和某些特殊服务。处理完毕后报文已更新，确定合适的输出端口后，报文通过第一层传送到物理介质上。传统路由器是一种典型的符合第三层报文到报文交换技术的设备，它完全基于软件的工作机制所产生的固有缺陷已被现代基于硬件的三层交换技术所克服。

2. 流交换

在流交换中，第一个报文被分析以确定其是否标识一个“流”或者一组具有相同源地址或目的地址的报文。流交换节省了检查每一个报文要花费的处理时间。同一流中的后续报文则基于第二层的目的地址被交换。流交换需要两个技巧。第一个技巧是要识别第一个报文的一个特征标识流，这个流可以使其余报文走捷径，即第二层路径；第二个技巧是一旦建立通过网络的路径，就让流足够长以便利用捷径的优点。怎样检测流、识别属于特定流的报文，以及建立通过网络的流通路径随各厂商实现机制的不同而不同。目前出现了多种流交换技术，如 3COM 公司的快速 IP、Cisco 的多协议标记交换(MPLS)等。

除了上述一些技术之外，三层交换机还支持三层端口汇聚技术、网络时钟协议(NTP)等功能，在这里不再详述。随着三层交换相关技术的发展，三层交换机产品也有了进一步的细分，根据功能不同可以分为盒式百兆三层交换机、全千兆盒式三层交换机、机架式模块化三层交换机，以满足不同网络未来的需求。

3.5 VLAN 技术

虚拟局域网(VLAN)是将一组在物理位置上彼此分开的用户和计算机从逻辑上分成工作组群，构成一个广播域，在该广播域上的流量只有其成员才能收到。虽然在一个局域网中所有的计算机在物理线路上是连通的，但经过不同的 VLAN 配置后，可以使不同 VLAN 之间的计算机不能相互访问，实现了对不同组计算机之间的有效隔离。

3.5.1 VLAN 的概述

VLAN 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。这里的网段不是指真正的物理网段，而仅仅是逻辑网段的概念。

1. 使用 VLAN 的原因

VLAN 技术的出现，主要是为了解决交换机在进行局域网互联时无法限制广播和网络安全的问题。VLAN 技术在以太网帧的基础上增加了 VLAN 头，通过 VLAN ID 把一个 LAN 划分成多个逻辑的 LAN，即 VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间不能直接相互通信，这样，广播报文被限制在一个 VLAN 内。

2. VLAN 技术的应用

VLAN 技术主要应用于交换机和路由器中，但主流应用还是在交换机之中，并且只有具有 VLAN 协议的三层以上交换机才具有此功能。在共享网络中，一个物理的网段就是一个广播域。而在交换网络中，广播域可以是有一组任意选定的第二层网络地址(MAC 地址)组成的虚拟网段。这样，网络中工作组的划分可以突破共享网络中的地理位置限制，而完全根据管理功能来划分。同一个 VLAN 中的工作站，不论它们实际与哪个交换机连接，它们之间的通信就好像在独立的交换机上一样。

VLAN 对广播域的划分是通过交换机软件来完成的，它通过对用户分类来划分自己的用户群。例如，按项目组、部门或管理权限等进行划分。不需要调整物理连接、移动设备和线缆就能方便地组建逻辑网络，让设备或用户方便地在网络中移动。在划分 VLAN 的交换机上，每个端口都能够被赋予一个 VLAN 号，只有 VLAN 号相同的用户才同属于一个独立的广播域。如图 3-21 所示，网络中共划分了 3 个 VLAN，VLAN 中的数据帧和广播帧在各自的 VLAN 域内进行传输，不会直接到达其他区域。

3. VLAN 技术的优点

1)控制网络广播

使用 VLAN，可以将某个交换端口或用户赋予某一个特定的 VLAN 组，该 VLAN 组可以在一个交换网中，也可以跨接多个交换机，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。这样因广播所消耗的带宽占的比

例大大降低，网络性能得到显著改善，有效地减少了广播风暴的产生。

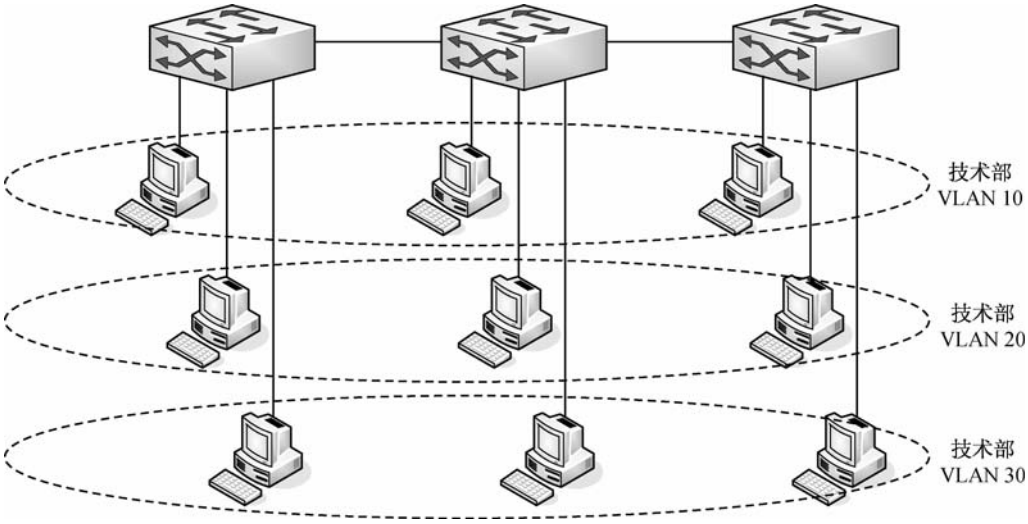

图 3-21　VLAN 的划分

2）增加了网络连接的灵活性

传统的网络技术中，网络内主机的移动、删除和增加都需要在物理位置上重新设置网络设备。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。

3）增强局域网的安全性

传统网络中，同一子网的用户在网络层很难实施安全措施。引入 VLAN 以后，不同 VLAN 内的报文在传输时是相互隔离的，即一个 VLAN 内的用户不能和其他 VLAN 内的用户直接通信，如果不同的 VLAN 要进行通信，则需要通过路由器或三层交换机等第三层设备。

3.5.2　VLAN 的划分

根据定义 VLAN 成员关系的不同，VLAN 可以划分为 6 种。不同种类的 VLAN 适用于不同的场合，但目前应用最广泛的是基于端口的 VLAN。

1. 根据端口来划分 VLAN

基于端口的 VLAN 划分是虚拟局域网最简单、最有效的方法。按交换机的端口来划分，管理员只需要管理和配置交换端口，而不管交换端口连接什么设备。被设定的端口都在同一个广播域中。例如，一个交换机的 1～5 端口被定义为 VLAN 10，同一交换机的 6～8 端口被定义为 VLAN 20。这样做允许各端口之间的通信，并允许共享型网络的升级。但是，这种划分模式将 VLAN 限制在了一台交换机上。第二代端口 VLAN 技术允许跨越多个交换机的多个不同端口划分 VLAN，不同交换机上的若干端口可以组成同一个 VLAN。

以交换机端口来划分网络成员只需定义端口，非常灵活，简单明了。但是连接到某 VLAN 上的用户离开原来的端口，到一个新的交换机的端口，就要重新定义其所属的 VLAN。

2. 根据 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据连接在交换机端口上的工作站或服务器的 MAC 地址来

划分,即管理员对每个 MAC 地址对应的主机都需要配置它属于哪个组。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,一般认为这种根据 MAC 地址划分的方法是基于用户的 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的话,工作量是非常大的。而且这种划分的方法也会导致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。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. 根据网络层划分 VLAN

这种划分 VLAN 的方法有两种含义:一是不同的协议可以组成不同的 VLAN,例如,IPVLAN、IPXVLAN 等;二是不同的网络地址网段组成不同的 VLAN,例如,不同的 IP 网段划分成不同的 VLAN。也就是说交换机是根据协议类型(如果支持多协议)或网络层地址来划分的,虽然这种划分是根据网络地址(如 IP 地址)进行的,但它不是路由,与网络层的路由毫无关系。

基于网络层的 VLAN 按传输协议划分网段,因而可以控制广播,提高性能,用户可以在网络内部自由移动而不用重新配置自己的工作站。这种方式继承了基于端口的 VLAN 和基于 MAC 地址的 VLAN 的优点,配置方便灵活,与基于 MAC 地址的 VLAN 相比,更实用。它的缺点是:交换机必须能读懂数据包的第三层信息,分析其协议类型;基于网络层的 VLAN 需要分析协议或地址格式并进行相应的转换,影响交换机的速度和性能;交换机初始配置的工作量太大。

4. 根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义,它认为一个组播组就是一个 VLAN。这种划分的方法将 VLAN 扩大到了广域网,因此,这种方法具有更大的灵活性,而且也很容易通过路由器进行扩展,但是这种方法不适合局域网,主要是效率不高。

5. 基于规则的 VLAN

基于规则的 VLAN 也称基于策略的 VLAN,它具有自动配置的能力,能够把相关的用户连成一体,在逻辑划分上称为“关系网络”,是一种最灵活的 VLAN 划分方法。

采用这种方法,整个网络可以非常方便地通过路由器扩展网络规模。有的产品还支持一个端口上的主机分别属于不同的 VLAN,这在交换机与共享式 hub 共存的环境中显得尤为重要。自动配置 VLAN 时,交换机中软件自动检查进入交换机端口的广播信息的 IP 源地址,然后软件自动将这个端口分配给一个由 IP 子网映射成的 VLAN。

6. 按用户定义、非用户授权划分 VLAN

根据用户定义、非用户授权来划分 VLAN,是指为了适应特别的 VLAN 网络,根据具体的网络用户的特别要求来定义和设计 VLAN,而且可以让非 VLAN 群体用户访问 VLAN,但是需要提供用户密码,在得到 VLAN 管理的认证后才可以访问一个 VLAN。

使用 VLAN 的一个重要的工作就是前期对网络进行规划与设计。例如,整个网络的广播如何配置,哪些机器在一个 VLAN 中,各自的 IP 地址、子网掩码如何分配,VLAN 之间如何相互通信(路由的设计)等问题。只有规划设计好了,才能够在配置和以后的使用维护时更加方便和容易。实际应用中可能多种划分方法混合使用,使得网络管理更加灵活。

3.5.3　VLAN 的配置

在进行 VLAN 配置时，首先应根据应用需求，规划设计网络拓扑结构，划分 VLAN 和分配 IP 地址，接着才开始具体的配置，最后还要进行调试，查看、修改配置信息，确保配置合理正确。

遵循 IEEE 802.1q 标准，VLAN 以 VLAN ID 来标识，最多支持 250 个 VLAN(VLAN ID 范围是 1～4 094)。VLAN 1 是由交换机自动创建的，是默认配置，不能被删除，其他的 VLAN ID 可以添加、删除、修改。

加入或移除一个 VLAN 时可以通过接口模式来配置一个端口的 VLAN 成员类型。VLAN 成员类型有 Access 端口和 Trunk 端口两种。一个 Access 端口只能属于一个 VLAN，并且是通过手工设置指定 VLAN 的。交换机上的所有端口默认都是 Access 端口，属于 VLAN 1。一个 Trunk 端口，在默认情况下属于本交换机的所有 VLAN，它能够转发所有 VLAN 的帧，但是可以通过设置许可 VLAN 列表(allowed-VLANs)来加以限制。

1. 在同一个交换机上创建 VLAN

首先要用控制线连接计算机和交换机 Console 端口，再用直通线连接计算机和交换机的端口，打开交换机电源。

创建 VLAN 时，需要给出 VLAN 号，在特权模式下输入：

```
Switch# vlan database
Switch(vlan)# vlan 100
```

返回特权模式，进入全局配置模式，再进入端口配置模式，将交换机的端口加入 VLAN 中(以交换机端口 5 为例)。

```
Switch(config)# interface fastethernet 0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
```

在计算机上用 ping 命令测试 VLAN 的配置，验证接入不同 VLAN 的计算机之间无法通信。

从 VLAN 中取消交换机端口(按上面过程，先进入端口配置模式)：

```
Switch(config-if)# no switchport access vlan 100
```

从 VLAN 数据库中删除 VLAN 100

```
Switch# vlan database
Switch(vlan)# no vlan 100
```

2. 创建跨越交换机的 VLAN

在不同交换机之间配置 VLAN 时，需要使用 VTP。VTP(VLAN trunking protocol)就是用来解决具有 VLAN 的多台交换机互联环境下保持各交换机上 VLAN 设置一致的协议。VTP 可以在同一个 VTP 管理域(也称为 VLAN 管理域)中的交换机之间传递 VLAN 的配置信息，从而使得各交换机的 VLAN 配置一致。这样不仅减小了配置工作量，降低了配置出错的可能性，同时还可以支持较大的网络。

VTP 的操作共有 3 种模式：服务器(server)模式、客户(client)模式、透明(transparent)模式。在服务器模式下可以建立、修改和删除 VLAN 及配置其他关于整个 VTP 管理域的参数。在客户机模式下可以接收和发送域中交换机 VLAN 的最新配置信息，从而保持与交换

机 VLAN 配置的同步。在透明模式下交换机不参与本域中 VLAN 配置的同步，仅传递本域中其他交换机的 VTP 广播信息。

当交换机处于服务器或透明模式时，管理员可以增加、修改和删除 VLAN 的相关配置，而在客户机模式时是不可以的。设置命令如下：

```
Switch# vlan database
Switch(vlan)# vtp domain domain-name
Switch(vlan)# vtp {server|client|transparent}
```

在不同交换机上设置同一个 VLAN 时，它们的 VTP 域名和 VLAN ID 必须相同，在交换机之间交换 VLAN 信息时，需要设置级联端口，并需要将级联端口 Trunk 打开。Trunk 端口属于所有的 VLAN。配置命令如下：

```
Switch(config)# interface fastethernet 0/24
Switch(config-if)# switchport trunk encapsulation dotlq
Switch(config-if)# switchport mode trunk
```

需要注意的是，trunking 技术允许任何一个 VLAN 的信息从一条电缆上通过，相当于在一条物理连接上绑定了多条逻辑链路，或者说相当于一条导管，任何 VLAN 信息都可以流经它。VLAN trunking 能只用一条线连接多个甚至所有 VLAN，用来区分数据帧所属 VLAN 的方法是：当数据帧通过 Trunk 离开交换机时，交换机给来自每个 VLAN 的数据帧的头部加上一个唯一的标志，标明其所属的 VLAN，从而使得收到数据帧的交换机通过辨别这个标志就能知道数据帧来自哪个 VLAN。

实现 VLAN trunking 主要有两种方法：

(1)使用 IEEE 802.1q trunking 协议，该协议是国际标准，并且得到了所有厂家支持。

(2)使用 Cisco 私有的 ISL(inter-switch link)协议，只有部分 Cisco 设备上支持该协议。

下面通过举例说明在多个交换机上创建 VLAN 的方法。

【例 3-1】 网络拓扑图如图 3-22 所示，分别在交换机 SwitchA 和 SwitchB 上创建 VLAN 100，将相应的交换机端口配置到 VLAN 100 中。

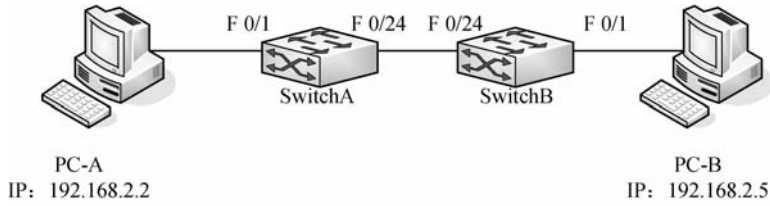

图 3-22 跨越交换机创建 VLAN

具体操作步骤如下：

```
SwitchA#show vlan
SwitchA#vlan database
SwitchA(vlan)#vtp domain vd1
SwitchA(vlan)#vlan 100
```

返回特权模式，再进入全局配置模式，选择加入 VLAN 100 的交换机端口 1，进入端口配置模式。

```
SwitchA#configure terminal
```

```
SwitchA(config)#interface fastethernet 0/1
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 100
```

选择用作 Trunk 的端口 24，进入端口配置模式。

```
SwitchA(config)#interface fastethernet 0/24
SwitchA(config-if)#switchport mode trunk
```

在交换机 SwitchB 上重复上述步骤，把端口号 1 也加入到同一个 VLAN 中，并将端口 24 的 Trunk 功能打开 。

最后，用 ping 命令验证。

3. VLAN 间的通信配置

除了三层交换外，单臂路由器方法在 VLAN 间通信时具有非常重要的实际意义，下面通过实例介绍单臂路由器的配置方法。

【例 3-2】 网络拓扑图如图 3-23 所示，采用一台路由器 Router1，两台交换机（一台为三层交换机 SwitchA，另一台为二层交换机 SwitchB）。两台计算机 PC-A 和 PC-B 通过直通线分别与交换机 SwitchA 和 SwitchB 连接。设置两个 VLAN：VLAN 20 和 VLAN 30。

SwitchA 交换机的端口 23、24 设置为 Trunk 端口，端口 1、2、3、4 配置到 VLAN 20，端口 5、6、7、8 配置到 VLAN 30。SwitchB 交换机的端口 24 设置为 Trunk 端口，端口 1、2、3、4 配置到 VLAN 20，端口 5、6、7、8 配置到 VLAN 30。

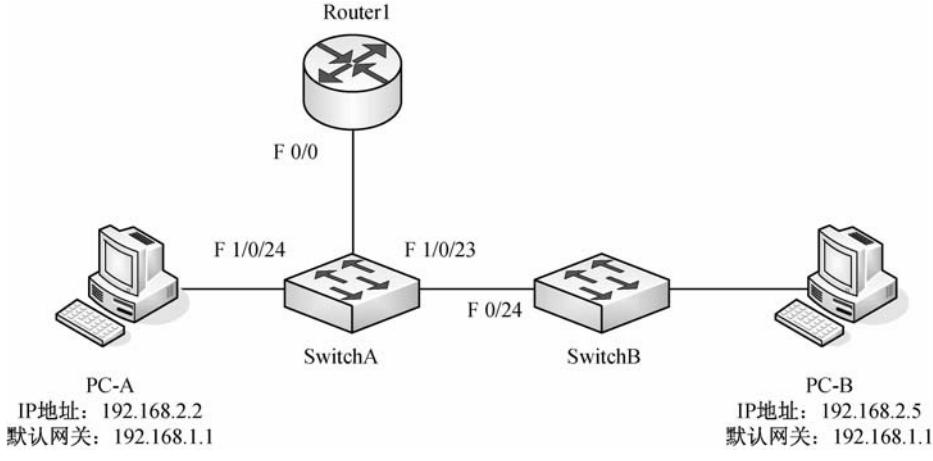

图 3-23　VLAN 间的通信

具体操作步骤如下：

(1)对 SwitchA 的操作：

```
SwitchA#vlan database
SwitchA(vlan)#vlan 20 name market
SwitchA(vlan)#vlan 30 name develop
SwitchA(vlan)#vtp server
SwitchA(vlan)#exit
SwitchA#configure terminal
SwitchA(config)#interface fastethernet 1/0/1-4
```

```
SwitchA(config-if-range)#switchport access vlan 20
SwitchA(config-if-range)#interface range fastethernet 1/0/5-8
SwitchA(config-if-range)#switchport access vlan 30
SwitchA(config)#interface fasterethernet 1/0/24
SwitchA(config-if)#switchport trunk encapsulation dotlq
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#exit
SwitchA(config)#interface fastethernet 1/0/23
SwitchA(config-if)#switchport trunk encapsulation dotlq
SwitchA(config-if)#switchport mode trunk
SwitchA#show vlan brief
```

(2)对 Router1 的操作：

```
Router1#configure terminal
Router1(config)#interface fastethernet 0/0
Router1(config-if)#no shutdown
Router1(config-if)#interface fastethernet 0/0.2
Router1(config-subif)#encapsulation dotlq 20
Router1(config-subif)#ip address 192.168.1.1 255.255.255.0
Router1(config-subif)#no shutdown
Router1(config-subif)#interface fastethernet 0/0.3
Router1(config-subif)#encapusulation dotlq 30
Router1(config-subif)#ip address 192.168.2.1 255.255.255.0
Router1(config-subif)#no shutdown
Router1(config-subif)#exit
```

(3)对 SwitchB 的操作：

```
SwitchB#vlan database
SwitchB(vlan)#vtp client
SwitchB(vlan)#exit
SwitchB#show vlan brief
SwitchB#configure terminal
SwitchB(config)#interface fastethernet 0/24
SwitchB(config-if)#switchport mode trunk
SwitchB(config)#interface range fastethernet 1/0/1-4
SwitchB(config-if-range)#switchport access vlan 20
SwitchB(config-if-range)#interface range fastethernet 1/0/5-8
SwitchB(config-if-range)#switchport access vlan 30
SwitchB(config-if)#exit
```

实　训　一

一、实训目的

掌握常用的交换机配置命令，理解交换机各种不同工作模式之间的切换技术。

二、实训背景

假设你是某公司新进的一名网络管理员，负责网络中心的设备管理工作，要求熟悉公司的网络产品，公司采用全系列锐捷网络产品，要求登录配置交换机，掌握交换机的命令操作。

三、实训设备

- S2126G 交换机 1 台。
- 主机 1 台。
- 控制 PC1 台。
- 直通线 1 根。
- 控制台电缆 1 根。

四、拓扑图

网络拓扑图如图 3-24 所示。

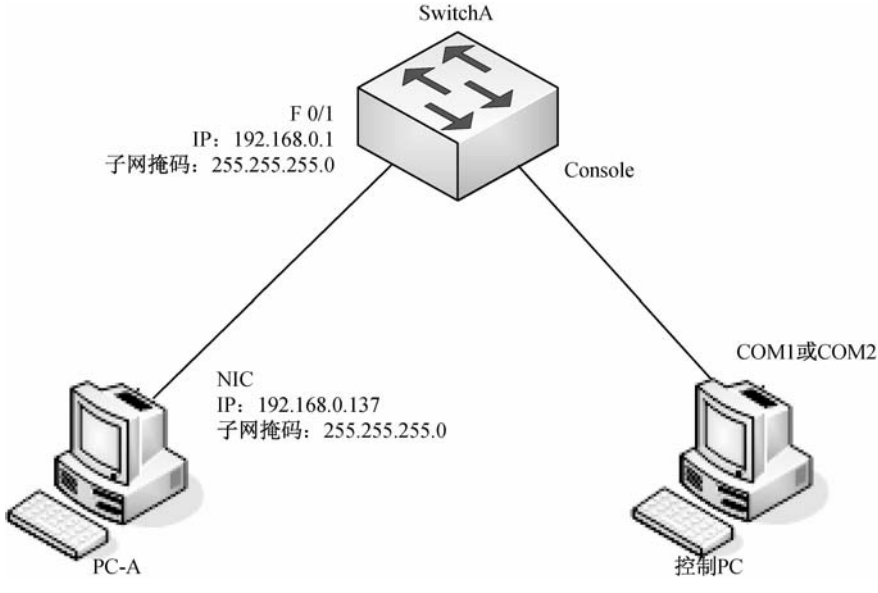

图 3-24　交换机基本配置网络拓扑图

五、实训内容及步骤

(1)按照 3.2.1 节中本地配置的方法打开超级终端，为使用配置命令作好准备。

(2)各种配置模式的切换。

```
SwitchA>enable                                  //进入特权模式
SwitchA#show ?                                  //查看可用的命令
SwitchA#configure terminal                      //进入全局配置模式
SwitchA(config)#interface fastethernet 0/1      //进入交换机 F 0/1 的端口模式
```

```
SwitchA(config-if)#
SwitchA(config-if)#exit                          //退回到上一级操作模式
SwitchA(config)#

SwitchA(config-if)#end                           //直接退回到特权模式
SwitchA#
```

(3)交换机设备名称、管理地址、本地登录口令、远程登录口令以及特权模式口令的配置。

```
SwitchA>enable
SwitchA#configure terminal                       //进入全局配置模式
SwitchA(config)#hostname teacher                 //配置交换机名称为 teacher
Teacher(config)#interface vlan1
Teacher(config-if)#no shutdown                   //开启交换机管理端口
Teacher(config-if)#ip address 192.168.0.1 255.255.255.0
                                                 //配置交换机 IP 地址
Teacher(config-if)#exit
Teacher(config)#line console 0
Teacher(config-line)#passward bddlmm             //设置本地登录密码 bddlmm
Teacher(config-line)#login                       //使密码生效
Teacher(config-line)#exit                        //返回全局配置模式
Teacher(config)#line vty 0 3                     //对 0～3 条虚拟终端线路进行设置
Teacher(config-line)#password ycdlmm             //设置远程登录密码 ycdlmm
Teacher(config-line)#login                       //使密码生效
Teacher(config-line)#exit                        //返回全局配置模式
Teacher(config)#enable secret tqmsmm             //设置特权模式密码为 tqmsmm
```

(4)交换机端口参数的配置。

```
Teacher>enable
Teacher#config terminal
Teacher(config)#interface fastethernet 0/1       //进入 F 0/1 的端口模式
Teacher(config-if)#speed 10                      //配置 F 0/1 的端口速率是 10 Mb/s
Teacher(config-if)#duplex half                   //端口全双工模式改为半双工模式
Teacher(config-if)#end
```

(5)保存各种配置信息。

```
Teacher#copy running-config startup-config
```

(6)查看各种配置信息。

```
Teacher#show interface fastethernet 0/1          //查看交换机端口信息
Teacher#show version                             //查看交换机的各项信息
Teacher#show running-config                      //查看交换机的当前生效的配置信息
```

(7)交换机远程登录的验证。

配置主机 PC-A 的 IP 地址为 192.168.0.137,首先用 ping 命令验证 PC-A 与交换机是

否连通，命令为 ping 192.168.0.1，ping 通之后在主机上进行远程登录：

```
C:＞telnet 192.168.0.1
Password
S2126＞
```

注意事项：(1)交换机命令可以简写，但简写时必须能够唯一区别该命令。

(2)交换机每个操作模式下有各自的命令，不能跨模式工作。

(3)配置设备名称的有效字符是 22 个字节。

(4)show running-config 是查看当前生效的配置信息，该信息存储在 RAM 中，但交换机断电或重新启动时会生成新的配置信息。

实　训　二

一、实训目的

掌握使用三层交换机实现 VLAN 间通信的配置方法，实现网络的连通性，从而使信息实现共享和传递，进一步理解三层交换机的工作原理。

二、实训背景

假设某公司有两个主要部门：销售部和技术部。其中，销售部的 PC 机分散连接在 2 台交换机上，部门内部需要互相进行通信。另外，销售部和技术部之间也需要进行相互通信。现在要求通过三层交换机的配置来实现这一目标。

三、实训设备

- 交换机 2 台，二层交换机 1 台，三层交换机 1 台。
- PC 主机 3 台，运行 Windows 2003/XP 操作系统，要求安装有超级终端程序。
- 直通线 3 根，交叉线 1 根。

四、拓扑图

网络拓扑图如图 3-25 所示。

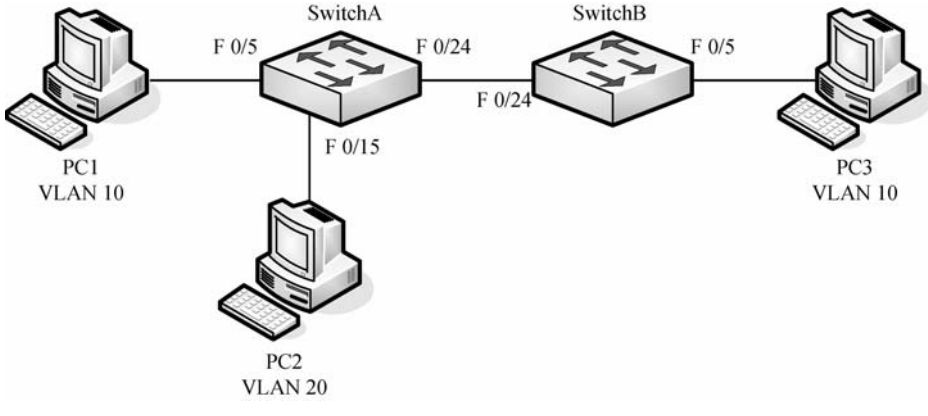

图 3-25　三层交换机实现 VLAN 间通信的网络拓扑图

五、实训内容及步骤

(1)在交换机 SwitchA 上创建 VLAN 10,并将 F 0/5 端口划分到 VLAN 10 中,代码如下:

```
SwitchA(config-vlan)#name sales                    //创建 VLAN 10 并命名为 sales
SwitchA(config-vlan)#exit
SwitchA(config)#interface fastethernet 0/5         //进入接口配置模式
SwitchA(config-if)#switchport access vlan 10       //将 F 0/5 端口划分到 VLAN 10 中
SwitchA(config-if)#end
SwitchA#show vlan id 10
```

(2)在交换机 SwitchA 上创建 VLAN 20,并将 F 0/15 端口划分到 VLAN 20 中,代码如下:

```
SwitchA#configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#name technical
SwitchA(config-vlan)#exit
SwitchA(config)#interface fastethernet 0/15
SwitchA(config-if)#switchport access vlan 20
SwitchA(config-if)#end
SwitchA#show vlan id 20
```

(3)将交换机 SwitchA 上与 SwitchB 相连的端口(假设为 F 0/24 端口)设置为 Trunk 模式,代码如下:

```
SwitchA#configure terminal
SwitchA(config)#interface fastethernet 0/24
SwitchA(config-if)#switchport mode trunk
                                   //将 fastethernet 0/24 端口设置为 Trunk 模式
SwitchA(config-if)#end
SwitchA#show interface fastethernet 0/24 switchport
```

(4)在交换机 SwitchB 上创建 VLAN 10,并将 F 0/5 端口划分到 VLAN 10 中,代码如下:

```
SwitchB(config)#vlan 10
SwitchB(config-vlan)#name sales
SwitchB(config-vlan)#exit
SwitchB(config)#interface fastethernet 0/5         //进入接口配置模式
SwitchB(config-if)#switchport access vlan 10
SwitchB(config-if)#end
SwitchB#show vlan id 10
```

(5)将交换机 SwitchB 上与 SwitchA 相连的端口(假设为 F 0/24 端口)设置为 Trunk 模式,代码如下:

```
SwitchB#configure terminal
SwitchB(config)#interface fastethernet 0/24        //进入接口配置模式
```

```
SwitchB(config-if)#switchport mode trunk
                                        //将 fastethernet 0/24 端口设置为 Trunk 模式
SwitchB(config-if)#end
SwitchB#show interface fastethernet F 0/24 switchport
```

(6)将 PC1 连接到 SwitchA 的 F 0/5 端口,PC2 连接到 SwitchA 的 F 0/15 端口,PC3 连接到 SwitchB 的 F 0/5 端口,使用 ping 命令分别验证 PC1 与 PC3 能互相通信,但 PC2 与 PC3 不能互相通信。

已设置 PC1 的 IP 为 192.168.1.151,PC2 的 IP 为 192.168.1.152,PC3 的 IP 为 192.168.1.153,则有代码如下 :

```
C:\> ping 192.168.1.153          //在 PC1 的命令行方式下验证能 ping 通 PC3
C:\> ping 192.168.1.153          //在 PC2 的命令行方式下验证不能 ping 通 PC3
```

(7)设置三层交换机 VLAN 间通信,代码如下:

```
SwitchA(config)#interface vlan 10          //创建虚拟接口 VLAN 10
SwitchA(config-if)#ip address 192.168.10.254 255.255.255.0
                        //配置虚拟接口 VLAN 10 的地址为 192.168.10.254
SwitchA(config-if)#exit                    //返回到全局配置模式
SwitchA(config)#interface vlan 20          //创建虚拟接口 VLAN 20
SwitchA(config-if)#ip address 192.168.20.254 255.255.255.0
                        //配置虚拟接口 VLAN 20 的地址为 192.168.20.254
```

(8)修改 PC1 和 PC3 的默认网关为:192.168.10.254,PC2 的默认网关为:192.168.20.254。修改相应的 IP 值:PC1 的 IP 为 192.168.10.151,PC2 的 IP 为 192.168.20.152,PC3 的 IP 为 192.168.10.153,则有代码如下:

```
C:\> ping 192.168.20.152         //在 PC1 的命令行方式下验证能 ping 通 PC2
C:\> ping 192.168.20.152         //在 PC3 的命令行方式下验证能 ping 通 PC2
```

测试结果:通过三层交换机 SwitchB,实现了 SwitchA 上位于不同 VLAN 内的主机可以互相 ping 通。

本 章 小 结

本章从交换机的基础知识出发,首先讲解了交换机的工作原理、功能、分类方法、交换技术和主要的技术参数,接着详细介绍了交换机的配置模式和常用的配置命令,然后对生成树协议的功能和工作原理进行了阐述,最后介绍了三层交换机的概念及其 VLAN 应用。学习完本章内容,可以使读者对交换机有一个详细的了解和认识,并能够利用交换机进行基本的网络配置和管理,达到符合网络管理员基本要求的目的。

习　题　3

1.什么是交换机?交换机的工作原理是什么?

2. 交换机的交换方式有哪几种？各自的特点是什么？
3. 交换机的主要性能指标有哪些？
4. 交换机的主要分类方法有哪些？
5. 通过什么方式可以配置交换机？
6. 交换机的配置模式之间的切换命令有哪些？
7. 生成树协议的作用是什么？简述其工作原理。
8. 三层交换机的特点是什么？主要技术有哪些？
9. 什么是 VLAN？VLAN 技术的优点有哪些？
10. VLAN 的划分方法有哪些？