第3章 局域网交换技术

本章以山西中北大学计算机科学技术学院网络工程改造项目为依托，介绍组建高效、安全局域网的交换技术。

熟悉局域网规划设计中需要应用的技术，熟悉网络安装中的各种网络设备，了解这些网络设备和交换技术在局域网应用中所承担的功能和作用。

图 3-1 展示了学校计算机科学技术学院网络中心工作场景。

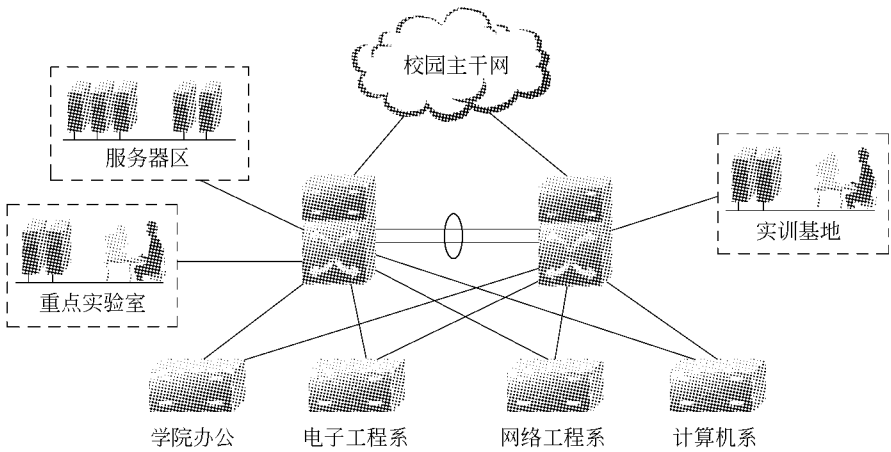

图 3-1 网络中心工作场景

学习完本章并完成练习之后，将了解到如下内容。

(1) 理解 VLAN 技术。

(2) 配置和管理 VLAN 技术。

(3) 学习局域网中的冗余拓扑。

(4) 了解局域网中的生成树协议。

(5) 了解 STP 收敛技术。

(6) 掌握快速生成树协议。

(7) 配置 STP 和 RSTP 技术。

(8) 掌握交换机端口聚合技术。

网络项目介绍

1. 项目背景

中北大学电子工程系、计算机科学技术系在学院改制前，都是独立建制单位，分别建有自己的网络，早期规划网络拓扑如图 3-2 所示。

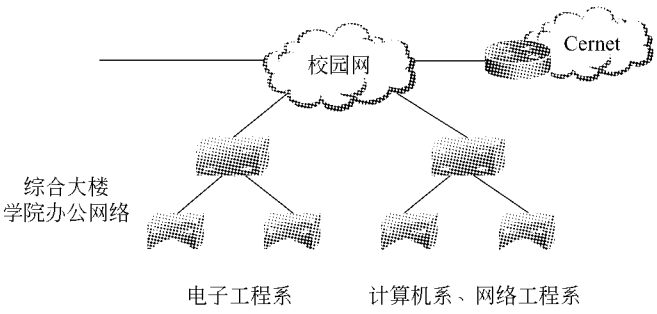

图 3-2　独立学院早期网络拓扑

学校为整合教学资源，把原电子工程系、计算机科学技术系及相关专业，在院系改制中合并成一个综合性的计算机科学技术学院。此外，为了改进传统的教学组织形式，利用网络多媒体技术教学，规范校园网络管理，现有的网络环境已不能满足日益增长的信息化管理和教学的需求，需改造升级校园主干网络，整合各学院目前的网络资源。

2. 业务需求分析

改造后学院网络应当达到如下目标。

(1) 教学办公自动化。建立信息化办公环境，学院所有办公室及实验室通过校园网，通过网络协同工作，获取信息资源，提高办公效率。

(2) 安全高效的网络性能。增加核心交换设备，主干采用光纤，提供高速数据转发。根据具体业务需要合理划分网络，保证教学、教务和学生实习网络的安全。采用必要的冗余技术保证网络的稳定。

(3) 便捷全面的网络服务。建立学院电子图书馆和 VOD 视频点播系统，共享资源。丰富教学的手段和方法，方便学生和教师对资料的查询、检索，提高学习和办公效率。

3. 网络规划思想

图 3-3 所示是新规划的学院网络拓扑结构。为保持网络的高速转发和稳定，在现有网络组织形式采用双核心结构。其次，为保证部门网络之间的独立性，各工作部门间按职能部门划分 VLAN，实现设备和链路安全冗余及负载平衡。

学院各实验室根据地理位置接入所在系网络，通过 NAT 解决学生用机的 IP 地址扩

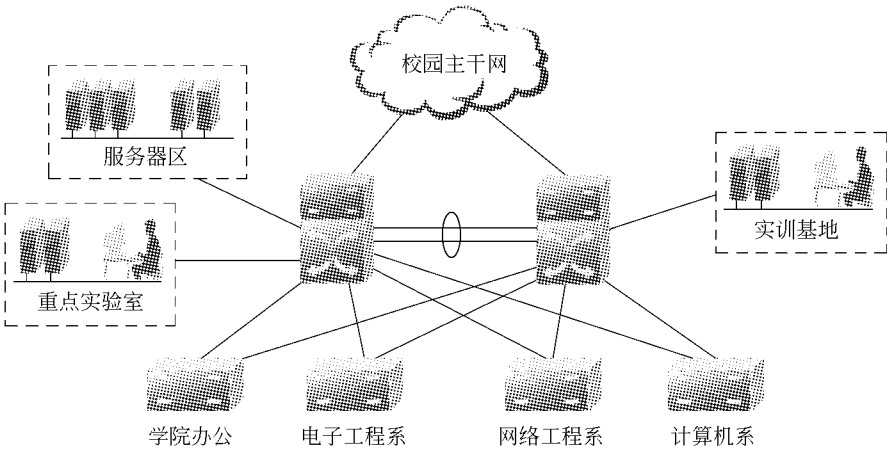

图 3-3　新规划的学院网络拓扑

容;学院重点实验室以及面对全校开放的计算机实训基地接入学院主干网络,保障接入点网络安全措施。

工作经历

自己最初的学校为实现无纸化办公,对校园网进行简单改造,增添了更多的设备。可网络中心的麻烦也接踵而来。由于设备的增多,学校网络的速度越来越慢,经常需要重启交换机设备才能恢复。此外,财务处的领导也来网络中心发牢骚,说财务处的计算机经常收到莫名的干扰……

各种因素促使自己去寻找网络发生使用不畅的原因,和安装的公司进行联系,网络公司说是校园网络扩大后广播带来的干扰,需要划分虚拟局域网才能解决。

图 3-4 所示的是中北大学一期校园网建设拓扑,图中虚线部分显示的区域是电子工程学院和计算机学院现有的网络安装场景:通过交换机把学院中所有的设备连为一体,在同一个交换网络中实现互联互通,满足了部门内部和部门之间信息化的建设需求。

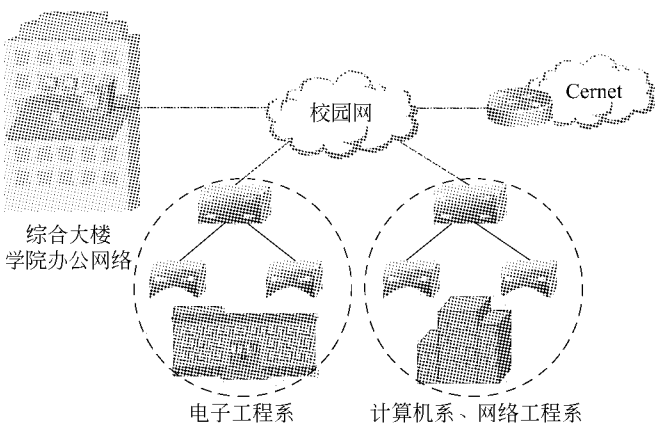

图 3-4　中北大学计算机科学技术学院网络 VLAN 改造技术

生活中虚拟局域网技术发生在图 3-4 所示虚线部分的网络场景。

通过前面的知识学习，已经对局域网的概念有了了解，局域网并不同于外界通信使用的 TCP/IP 协议体系，它是一种建立在传统以太网结构上的网络，除了使用 TCP/IP 协议外，它还涉及许多协议。

在局域网里，计算机要和彼此连接在一起的设备进行通信，并不是通过 IP 进行，而是通过网卡物理地址来进行。计算机物理地址是计算机网卡地址，网络在生产时就固化有全球唯一标识号，也称为 MAC 地址，因此通过 MAC 地址可以唯一标识网络中的任意一台计算机。根据局域网内通信协议规范，当一台计算机要与其他计算机通信时，首先查找另一台计算机的 MAC 地址，如图 3-5 所示，然后由网卡设备把需要通信的数据封装成数据帧的数据结构(类似于生活中书信的信封)，再通过网卡把数据发送出去。

图 3-5　查找本网络物理地址映射表

如果发送计算机的地址缓冲池中保存有对方计算机的 MAC 地址，这个过程按照以上过程直接封装、发送。但如果发送的计算机中没有保存通信方计算机的 MAC 地址，它必须把已知目标计算机的 IP 地址通过 ARP 协议(地址解析协议)在物理网络中广播出去。“广播”是局域网中计算机之间通信的方式，它能让和连接在同一网络中的任意一台计算机都能收到数据的通信方式。计算机收到数据后就会判断这条信息是不是发给自己的，如果是，就会返回应答，在这里它会返回自身地址。

当源计算机收到有效的回应时，它就得知了目标计算机的 MAC 地址，并把结果保存在系统的地址缓冲池里，下次传输数据时，就不需要再次发送广播了，这个地址缓冲池会定时刷新重建，以免造成数据冗余现象。然后由网卡设备把需要通信的数据封装成数据帧的数据结构，再通过网卡把数据发送出去。

3.1　虚拟局域网技术

3.1.1　局域网中的广播

在局域网中，设备之间的通信以三种方式进行：单播、组播和广播通信。在广播通信中，局域网中的每台主机都会接收到广播帧。如果中北大学整个校园网络仅有一个广播域，会影响到网络整体的传输性能。

图 3-6 所示是计算机科学技术学院使用多台二层交换机做接入的网络场景，一个由 3 台二层交换机(交换机 1～3)连接了大量客户机构成的网络。假设计算机 A 需要与计算机 B 通信，计算机 A 会通过 ARP 广播尝试获取计算机 B 的 MAC 地址，从而封装传输的数据帧。交换机 1、2、3 会转发该广播形成广播泛洪，如此一来学院中所有的网络都收到干扰，一方面广播消耗学院网络的带宽，另一方面还消耗计算机 CPU 的运算能力。

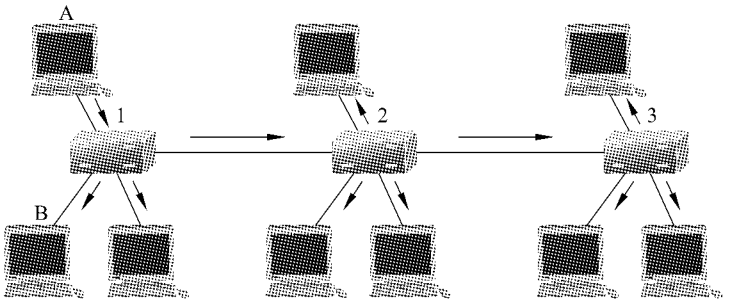

图 3-6　计算机科学技术学院网络广播示例

并且随着计算机科学技术学院网络设备的增加，学院网络内广播频率便会增加，网络传输效率会越来越低。因此，在进行计算机科学技术学院中内部新网络规划时，需要注意如何才能有效地分割广播，提高网络传输效率。

3.1.2　VLAN 技术概述

由于交换网络是以广播传输作为信息传输的核心，连接在一起的交换网络中存在广播、冲突和安全等因素的影响，因此造成了现有办公网络的工作速度缓慢，网络的安全性差。由于现有的网络中存在网络工作速度缓慢，网络内部干扰信息太多，网络的安全性差的情况，因此需要进行改造。

局域网作为当今网络不可或缺的组成部分，在网络应用中扮演着举足轻重的角色，但局域网内主机数日益增加带来了冲突、带宽浪费、安全等局域网中普遍存在的问题。通常，只有通过划分子网才可以隔离广播，但是 VLAN(Virtual Local Area Network，虚拟局域网)的出现打破了这个定律，用二层的技术解决三层的问题很是奇怪，但是的确做到了。VLAN 充分体现了现代网络技术的重要特征：高速、灵活、管理简便和扩展容易，是否具有 VLAN 功能是衡量局域网交换机的一项重要指标。

为了理解应用 VLAN 技术的必要性，了解在二层网络中所发现的问题是很重要的，二层网络中提出了如下的挑战。

(1) 一个平面、交换型的网络问题。在图 3-6 所示的一个“平面”的网络结构中，每台设备都可以看到被传输的广播数据包。因为每个端口都只在它自己的碰撞域中(一个端口就是一个碰撞域)，所以以太网通常的距离限制规则不再适用。这就导致了交换型网络变得很大，可以跨越几座建筑物，这样每个站点必须要处理的数据包数量就会不断增多。如果应用程序再发送广播数据包，情况就会更加恶化了。因为每个站点都要处理每个广

播数据包，就像这些数据包是要到这些站点去一样。

(2) 安全性。在二层网络环境中，提供安全性的保证不容易，因为每个站点可以访问所有的设备。

(3) 管理到目的地的多条路径。二层交换机不允许到目的地有冗余路径，而且也不能智能地对数据进行均衡负载。

当网络规模足够大，如同中北大学计算机科学技术学院网络，特别是降低平面网络中的广播率，是网络规划必须考虑的首要问题。降低网络内的广播流量就必须分隔广播域，通常采用把局域网分隔成几个子网段的方法，如图 3-7 所示。

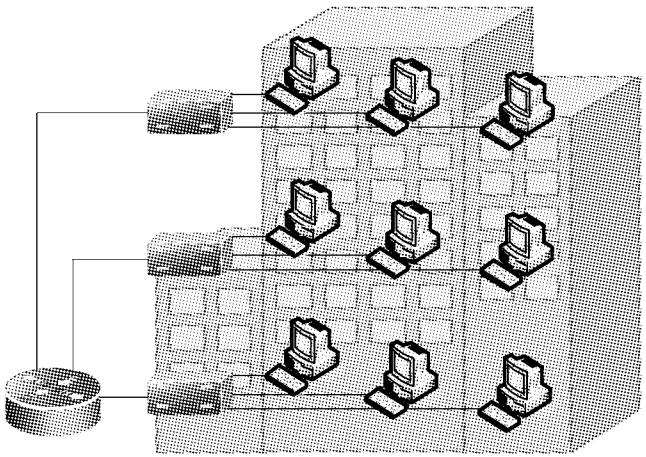

图 3-7　路由器分隔广播域示例

在早期局域网中只有通过路由器划分子网才可以隔离广播，而这种方式有着明显弊端，这主要是因为数据在从一个子网到另一个子网时，必须经过路由操作，导致网络数据传输速度的下降。交换机上虚拟局域网技术的出现，提供了替代路由器，解决广播、分隔子网的新方法。

VLAN 是一种通过将局域网内的设备逻辑地，而不是物理地划分成多个互不相干的子网络。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。可以将 VLAN 简单地理解为是在一个物理网络上逻辑地划分出来的逻辑网络。VLAN 内成员发出的数据帧，交换机只把其转发给同一 VLAN 内的成员，而不会发给该 VLAN 成员以外的计算机。

由于同一个 VLAN 内的广播包不会跑到别的 VLAN 中，VLAN 内的网内广播受到控制。VLAN 相当于 OSI 参考模型第二层的广播域，能够将广播流量控制在一个 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的提高。不同的 VLAN 之间的数据传输是通过第三层(网络层)的路由来实现的，因此使用 VLAN 技术，结合数据链路层和网络层的交换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。

图 3-8 所示网络拓扑是中北大学计算机科学技术学院内部网络，基于 VLAN 技术实

现广播域分隔的网络场景，分布在不同交换机上处室领导的交换机被划分到同一 VLAN 中，便于领导之间信息交流。

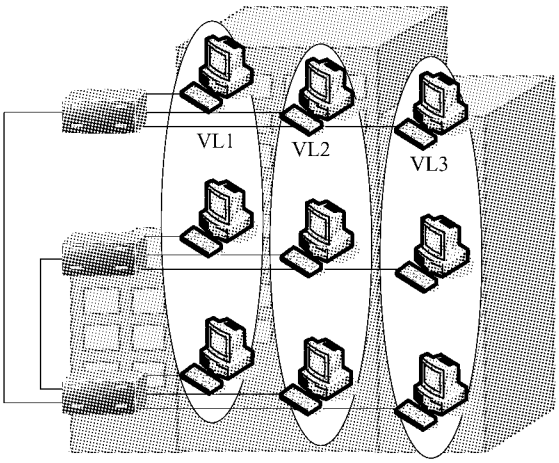

图 3-8　中北大学计算机科学学院内网 VLAN 规划

与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点和作用。

(1) 控制网络的广播风暴。由于实现了广播域分隔，VLAN 可以将广播风暴控制在一个 VLAN 内部，一个 VLAN 内的广播风暴不会影响其他 VLAN 的性能，网络中广播包消耗的带宽所占的比例大大降低，网络性能得到显著提高。

(2) 提高网络的安全性。共享式局域网之所以很难保证网络的安全性，是因为广播形成的共享访问网络。而 VLAN 技术能限制个别用户的访问，控制广播组的大小和位置，而且不同的 VLAN 间的数据不能直接传输，需要通过第三层(网络层)路由技术来实现，结合网络层设备可以有效提高网络安全性。

(3) 简化网络管理。由于 VLAN 是逻辑而不是物理网络，在规划网络时可以避免地理位置的限制。网络管理员能借助于 VLAN 技术轻松管理整个网络，就像在本地使用局域网一样。

3.1.3　划分 VLAN 的技术

按照需要的不同，在交换机上划分 VLAN 的方法常见的有以下 4 种方式。

1. 根据端口划分 VLAN

许多 VLAN 厂商都利用交换机的端口来划分 VLAN 成员。被设定在共同 VLAN 中的端口都在同一个广播域中，如一台交换机的 1,2,3,4,5 端口被定义为虚拟网 VLAN 10，同一交换机的 6,7,8 端口组成虚拟网 VLAN 20。但是，这种根据端口划分虚拟网模式，将虚拟网 VLAN 技术限制在一台交换机上实现，跨交换机的同一虚拟网之间端口不能通信。

第二代基于端口 VLAN 技术，才实现允许在跨越多个交换机上划分同一 VLAN 技

术，不同交换机上的若干个端口可以组成同一个虚拟网，从而实现互访。

按照交换机端口来划分网络成员，其配置过程简单明了。因此，从目前来看，这种根据端口划分 VLAN 的方式仍然是最常用的一种方式。

2. 根据 MAC 地址划分 VLAN

这种划分 VLAN 的方法，是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 的方法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。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的话，配置的工作量非常大。而且这种划分方法也导致了交换机执行效率的降低。因为在每一个交换机的端口，都可能存在很多个 VLAN 组成员，这样就无法限制广播包。对于使用笔记本式计算机的用户来说，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，是根据每个主机的网络层地址或协议类型（如果支持多协议）划分，虽然这种划分方法是根据网络地址，如 IP 地址，但它不是路由，与网络层的路由毫无关系。

其优点是用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要。此外，这种方法不需要附加的帧标签来识别 VLAN，可以减少网络的通信量。

其缺点是效率低，因为检查每一个数据包的网络层地址需要消耗处理时间（相对于前面两种方法）。一般的交换机芯片都可以自动检查网络上数据包以太网帧头，但要让芯片能检查 IP 帧头，需要更高的技术，同时也更费时。当然，这与各个厂商的实现方法有关。

4. 根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义，即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，因此具有更大的灵活性，而且也很容易通过路由器进行扩展。当然，这种方法不适合局域网，主要是因为效率不高。

3.1.4 实现基于端口 VLAN 划分技术

基于端口 VLAN 是根据交换机端口来划分，是目前定义 VLAN 最广泛的方法。

基于端口 VLAN 是划分虚拟局域网最简单也最有效的方法，网络管理员只需要把交换机端口划分成不同端口集合（这些端口被指定为相同 VLAN ID），就可以管理和配置交换机，而不管交换机端口连接什么设备。如图 3-9 所示，VLAN 从逻辑上把一个局域网按

照交换机的端口划分成两个虚拟局域网，相应的终端系统划分为各自独立子网。

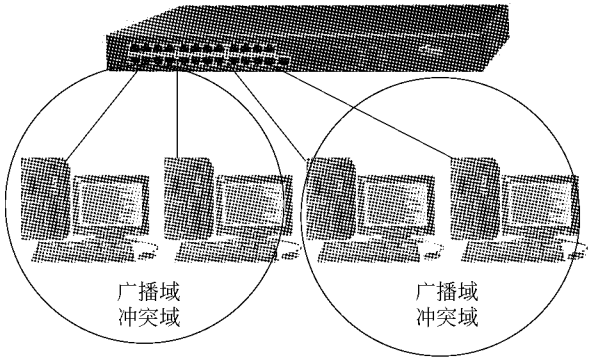

图 3-9　基于端口 Port VLAN 示例

基于端口 Port VLAN 在交换机上实现，分为两个步骤来实施：首先启用 VLAN 标识，然后将交换机端口指定到相应 VLAN 下。基于端口 VLAN 示意图如图 3-10 所示。

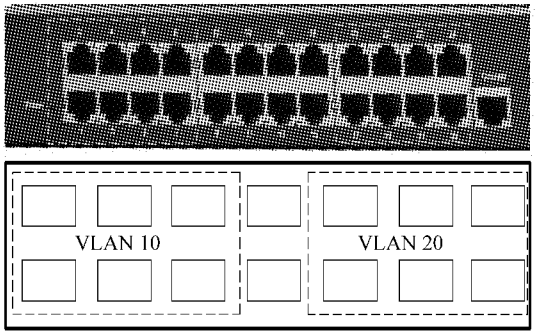

图 3-10　基于端口 VLAN，按端口划分 VLAN

1）基于端口划分 VLAN 命令

语法格式：

```
VLAN VLAN-id
```

该命令执行于全局配置模式下，是进入 VLAN 配置模式的导航命令。使用该命令的 no 选项，可以删除配置好的 VLAN：no VLAN VLAN-id 。需要注意的是，默认的 VLAN(VLAN 1)是不允许删除的。

```
Switch#
Switch#configure terminal
Switch(config)#VLAN 10                    !启用 VLAN 10
Switch(config)#name test                  !把 VLAN 10 命名为 test
Switch(config-VLAN)#
```

所有的交换机默认都有一个 VLAN 1，VLAN 1 是交换机的管理中心。在默认情况下，交换机所有的端口都属于 VLAN 1 管理。VLAN 1 不可以被删除。

2）指定端口到 VLAN 命令

语法格式

```
switchport access VLAN VLAN-id
no switchport access VLAN
```

该命令将一个端口设置为 statics access port，并将它指派为一个 VLAN 的成员端口。no 选项将该端口指派到默认 VLAN 中。需要注意的是，交换机端口的默认模式为 access，交换机默认的 VLAN 为 VLAN 1，VLAN 1 是一台交换机默认管理 VLAN。

如果输入的是一个新的 VLAN ID，则交换机会创建一个 VLAN，并将该端口设置为该 VLAN 的成员。如果输入的是已经存在的 VLAN ID，则增加 VLAN 的成员端口。

例如，将交换机 F0/5 端口指定到 VLAN 10 的配置如下。

```
Switch#
Switch#configure terminal
Switch(config)#interface fastEthernet 0/5          !打开交换机的接口 5
Switch(config-if)#switchport access VLAN 10        !把该接口分配到 VLAN 10 中
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#show VLAN                                   !查看 VLAN 配置信息
```

工程项目：单交换机划分虚拟局域网

【工程名称】

划分虚拟局域网

【目标技能】

划分基于端口 VLAN，实现本交换端口上连接的设备之间的安全隔离。

【材料准备】

二层交换机（1 台）；测试 PC(2～3 台)；网络连线(若干根)。

【工作场景】

图 3-11 所示的网络拓扑，是中北大学计算机科学技术学院网络建设中，教学行政楼中多个教研组部门之间的网络连接场景。由于不同教研组之间的计算机以前都连接在同一台交换机上，网络中由于广播等干扰，造成网络传输效率低下。

新规划网络时，提出希望通过实施虚拟局域网技术，保证不同教研组部门网络之间的计算机互相不进行干扰，实现隔离技术，提高网络传输效率。

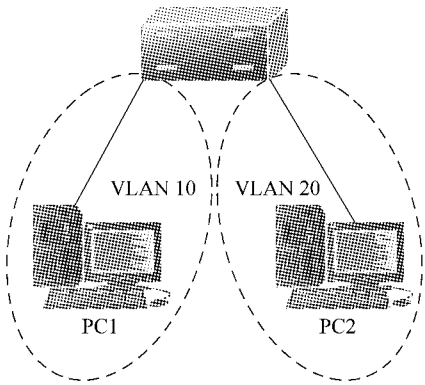

图 3-11　中北大学计算机科学技术学院教研组之间的网络隔离

【工作过程】

（1）在工作现场，如图 3-11 所示示意项目任