第5章

IP地址及划分子网与VLAN

【学习目标】

划分子网与VLAN(虚拟局域网)是网络最基本的应用之一。学习本章后,应能深刻理解IP地址、广播域、冲突域和VLAN基本概念与作用;熟练掌握划分子网方法、可网管交换机与管理计算机连接及使用方法,体验单交换机划分VLAN过程,为将来学习专业核心课程《网络组建与互联》和《高级路由交换技术》奠定基础。

【重点难点】

IP地址结构及特殊IP地址含义;子网及子网掩码基本概念,子网划分方法;VLAN基本概念、可网管交换机与管理计算机连接及使用方法,单交换机划分VLAN方法。

5.1 IP地址相关知识

计算机网络中,存在着成千上百万台计算机,人们是如何区分网络中的计算机的呢?是通过计算机专用的"身份证号"——IP地址。

5.1.1 IP地址及作用

为了使接入Internet的众多计算机主机在通信时能够相互识别,接入Internet中的每一台主机都被分配有一个唯一的标识——32位二进制地址,该地址称为IP地址(Internet Protocol)。

IP地址是通过IP协议来实现的。IPv4(v4是版本号)协议保证了一个IP地址在Internet中对应唯一的一台主机;每台主机都必须有IP地址,每个IP地址都具有唯一性与通用地址格式。

所有IP地址都由国际组织NIC(Network Information Center)负责统一分配的,目前全世界共有三个这样的网络信息中心:InterNIC(负责美国及其他地区);ENIC(负责欧洲地区);APNIC(负责亚太地区)。我国申请IP地址要通过APNIC。APNIC的总部设在日本东京大学。

5.1.2 IP 地址结构及表示

在日常生活中要找某个地方，首先要知道这个地方的地址。实际上地址的表达方式中就包含了某种层次结构。

例如，河北工业职业技术学院的地址是“河北省石家庄市红旗大街 626 号”，该地址所包含的层次结构是：第一层，所在省份——河北省；第二层，所在城市——石家庄；第三层，所在街道——红旗大街；第四层，门牌号——626 号。

类似地，IP 地址也采用了层次结构的表达方式。

1. IP 地址的结构

IP 地址结构包含了两方面：网络 ID 和主机 ID，即 IP 地址＝网络 ID＋主机地址，如图 5-1-1 所示。

图 5-1-1 IP 地址由网络 ID 和主机 ID 两部分组成

图 5-1-1 中，网络 ID(又称网络号)，用于标识某个网段。在相同的一个网段中，所有 IP 地址的网络 ID 都相同。

主机 ID(又称主机号)，用于标识网段内的某个节点。在相同的一个网段中，所有 IP 地址的网络 ID 都相同，但所有 IP 地址的主机 ID 必须不相同。

说明：

“主机 ID 用于标识网段内的某个节点”，这里的“节点”是指网络内的一个节点，不能简单地理解为是一台计算机。实际上 IP 地址是分配给计算机网卡的，一台计算机可以有多个网卡，就可以有多个 IP 地址，一个网卡就是一个节点。

例如，有两台计算机，它们的 IP 地址分别是 192.168.100.2 和 192.168.100.3(它们都属于 C 类地址，后面有详细介绍)，则这两台计算机同属于一个网络 ID，即同属于一个网段，网络地址(即主机 ID 全为 0，属于特殊 IP 地址，后面有详细介绍)是：192.168.100.0，主机 ID 则分别是 2 和 3。

在一个网段内部，主机 ID 必须是唯一的。

说明：

①如果有多个 IP 地址的网络 ID 相同，则这些 IP 地址的设备是处于同一个网络中，它们之间的通信通过集线器或交换机连接即可；而且这些 IP 地址的主机 ID 必须各不相同，否则，IP 地址的网络 ID 相同、主机 ID 也相同，就一定会发生 IP 地址冲突。

②如果多个 IP 地址的网络 ID 不相同，则这些 IP 地址的设备不是处在同一个网络，它们之间的通信就需要通过路由器来实现。

2. IP 地址的表示

在 TCP/IP 协议中，IP 地址在计算机中采用 32 个二进制 bit 表示。

例 1：用二进制表示的 IP 地址是：10000000.00001010.00000010.00011110。

但是，使用二进制形式表示 IP 地址，非常不便于人们记忆。因此，通常把 32 位的 IP 地址

分成四段，每 8 个二进制 bit 为一段，每段二进制分别转换为人们习惯的十进制，并且用点隔开，这种表示 IP 地址的方法又称“点分十进制表示法”。

例如，在例 1 中用二进制表示的 IP 地址，可以用十进制的 128.10.2.30 表示，如图 5-1-2 所示。

二进制	10000000. 00001010. 00000010. 00011110
十进制	128 . 10 . 2 . 30

图 5-1-2　IP 地址的两种表示方式

说明：在 8 位二进制 bit 中最小的值是 00000000，与其对应的十进制数为 0；在 8 位二进制 bit 中最大的值是 11111111，与其对应的十进制数为 255。所以采用“点分十进制表示法”表示 IP 地址时，IP 地址每段数值的取值范围是 0～255。

5.1.3　IP 地址的分类

由于 IP 地址由 32 个二进制数组成，一共有 $2^{32}=4294967296$ 个 IP 地址，要想管理好这些数量庞大的 IP 地址是非常困难的。因此为了便于管理，Internet 管理委员会将 $2^{32}=4294967296$ 个 IP 地址分为了 A、B、C、D、E 五类地址。

在这五类地址的每一类中，又定义了网络 ID 和主机 ID 各占用总 32 位地址中的多少位。也就是说，在每一类的 IP 地址中规定了可以容纳多少个网络，以及在这些网络中可以容纳多少台主机。

在五类地址中，最常用的是 A～C 类，D～E 类很少用。D 类地址是多播地址或组播地址，用于实验室科研；E 类地址是保留地址，以备 IP 地址不够用。

1. A 类地址

如图 5-1-3 所示，A 类 IP 地址的第 1 字节表示网络 ID，后 3 个字节表示主机 ID。其中在网络 ID 的第 1 字节中，第 1 位为“0”，接下来的 7 位（第 2 位到第 8 位结束）表示网络 ID。

图 5-1-3　A 类地址

图 5-1-3 中，在 A 类地址的网络中，最大网络 ID 数共有 $2^7-1=126$ 个，即范围为 00000001～01111110，如果用十进制表示，则是在 1～126 之间（0 和 127 留作它用）；在每个网络 ID（网段）内，可容纳的最大主机数是 $2^{24}-2=16777214$ 台（可见是个庞大的网络）。

说明：$2^{24}-2$ 中的减 2 是因为：如果主机 ID 全为“0”（属于特殊的 IP 地址），则表示该地址是网络地址；主机 ID 全为“1”（属于特殊的 IP 地址），即表示是广播地址。这两个地址属于特殊 IP 地址（下面有具体介绍），一般不分配给主机，所以某个网段内的最大主机数应从所有主机数中减去网络地址和广播地址这两个地址。

例如，10.1.1.1、126.1.1.1 就是 A 类地址，其网络地址（主机 ID 全为 0）分别表示为 10.0.0.0、126.0.0.0。

如果第 1 位数大于 126，就不属于 A 类地址，如 192.1.1.1 就不属于 A 类地址。

2. B 类地址

如图 5-1-4 所示，B 类地址前 2 个字节表示网络 ID，后 2 个字节表示主机 ID。其中在网络 ID 的第 1 个字节的前 2 位设为“10”，接下来的 14 位（从第 3 位到第 16 位结束）表示网络 ID。

如果用十进制表示，B 类地址的第一个字节在 128～191 之间，即表示 B 类网络最大的网络 ID 允许有 16384 个，且每个网络 ID（网段）拥有 66534 个主机。

图 5-1-4　B 类地址

例如，172.168.1.1 就是 B 类地址，其网络地址（主机 ID 全为 0）是 172.168.0.0。

3. C 类地址

如图 5-1-5 所示，C 类地址前 3 个字节表示网络 ID，后 1 个字节表示主机 ID。其中在网络 ID 的第 1 个字节的前两位设为“110”，接下来的 21 位（从第 4 位到第 24 位结束）表示网络 ID。

C 类地址是最常用的地址。

图 5-1-5　C 类地址

如果用十进制表示，C 类地址的第 1 个字节在 192～223 之间，即表示 C 类网络最大的网络 ID 允许有 2097152 个，且每个网络 ID（网段）拥有 254 台主机。

例如，202.18.16.11 就是 C 类地址，其网络地址（主机 ID 全为 0）是 202.18.16.0，主机 ID 是 11。

如图 5-1-6 所示，是 IP 地址的五种分类方法示意图。

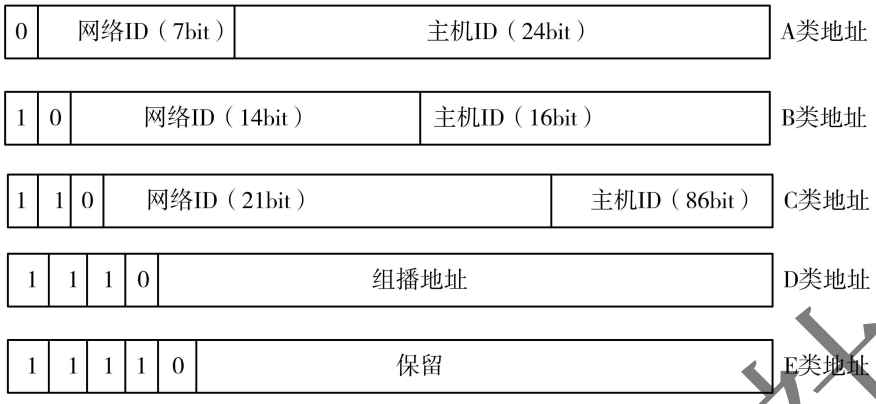

图 5-1-6　IP 地址的五种分类方法示意图

如表 5-1-1 所示，汇总了常用的 A、B、C 三类 IP 地址可以容纳的网络 ID 数和主机数。

表 5-1-1　　常用 A、B、C 三类 IP 地址可以容纳的网络 ID 数和主机数

类别	网络 ID 位数	主机 ID 位数	第 1 字节范围	网络地址长度	最大主机数目	地址范围	有效地址范围	网络规模
A	7	24	1～126	1B	1677214	0.0.0.0～127.255.255.255	1.0.0.1～126.255.255.254	大
B	14	16	128～191	2B	65534	128.0.0.0～191.255.255.255	128.1.0.1～191.254.255.254	中
C	21	8	192～223	3B	254	192.0.0.0～223.255.255.255	192.0.1.1～223.255.254.254	小

5.1.4　特殊 IP 地址

特殊 IP 地址是为特殊目的而保留的，不能用于标识网络设备。

下面介绍这些特殊的 IP 地址。

1. 私有地址与公有地址

IP 地址按不同的使用范围，可分为公有地址（又称公网地址）和私有地址（又称私网地址）。其中“公有地址”是可以直接连接互联网的 IP 地址，“私有地址”只能在某个企业或机构的内部网络（内部局域网）中使用。

（1）私有地址。

私有地址是不能够在互联网上使用的地址。

也就是说，如果在一个连接互联网的网络节点上使用了私有 IP 地址，那么该节点将不能和互联网上的任何其他节点通信，因为互联网的其他节点会认为该节点使用了一个非法的 IP 地址。

在 IP 地址的 A、B、C 类地址中，分别留出了三块 IP 地址空间（1 个 A 类地址段，16 个 B 类地址段，256 个 C 类地址段）作为私有的内部使用的地址。

表 5-1-2 列出了留出的内部私有地址。

表 5-1-2　　留出私有地址的 IP 地址空间

地址类	IP 地址空间	说明
A 类	10.0.0.0～10.255.255.255	A 类网络 ID 占 1 位，第 1 位是 10～10，因此只有 1 个 A 类地址
B 类	172.16.0.0～172.31.255.255	B 类网络 ID 占 2 位，第 2 位是 16～31，因此共有 16 个 B 类地址
C 类	192.168.0.0～192.168.255.255	C 类网络 ID 占 2 位，第 3 位是 0～255，因此一共有 256 个 C 类地址

由于私有 IP 地址无法直接连接互联网，因此，如果要使用私有地址将局域网连接到互联网，则需要将私有地址转换为公有地址。这如同一个单位的内部电话号码，只能在单位内部通话使用，如果要与单位外部通话，则必须通过单位的总机拨出。

将私有地址转换为公有地址的过程，称为网络地址转换（NAT，Network Address Translation），通常使用路由器执行 NAT 转换。

（2）需要私有地址的原因。

起原因就是 IP 地址资源的紧缺。由于私有地址可以在局域网内部重复使用，这样，就缓解了 IP 地址资源枯竭的危机。

前面已经介绍，IP 地址必须是唯一的，而且接入互联网的设备都必须有一个 IP 地址。IP v4 协议理论上支持 40 亿左右的公有 IP 地址，但事实上能够被利用的公有 IP 地址非常有限。如果每一台连接互联网的设备都需要一个公有 IP 地址，那么 IP v4 是绝对无法分配出这么多地址的。为此，采用私有地址仅供组织内部使用的方法，使组织内部主机无需唯一的公有 IP 地址，从而节约 IP 地址的资源。

例如，某单位需要管理 100 台计算机，要求这些计算机都能够连接到互联网。

理论上，该单位需要购买 100 个公有 IP 地址，才能在接入互联网后确保每一台计算机都有一个唯一的 IP 地址。

而事实上，该单位最少只需要购买一个公有 IP 地址即可。

简单地理解，如图 5-1-7 所示，在获得一个公有 IP 地址后（如 61.188.2.33），将该公有 IP 地址配置给路由器，至此，路由器就获得了一个独一无二的公有 IP 地址。而 100 台计算机组建了一个内部局域网，局域网内部使用的是私有 IP 地址（如 192.168.1.2～192.168.1.101）。再将 100 台计算机组建的局域网连接至路由器。此时，如果外界要给这 100 台计算机的其中一台发送信息，会先发送到路由器上，路由器会再转发给目标计算机，即路由器进行 NAT 转换。

说明：关于路由器的 NAT 功能，会在今后的专业课程中专门介绍。

对于规模大的网络，可以使用 A 类私有地址，可容纳 1600 万以上的私有地址；对于中型网络，可以使用 B 类私有地址，提供的地址超过 65000 个；小型企业和家庭网络一般使用单一的 C 类私有地址，最多可容纳 254 台主机。

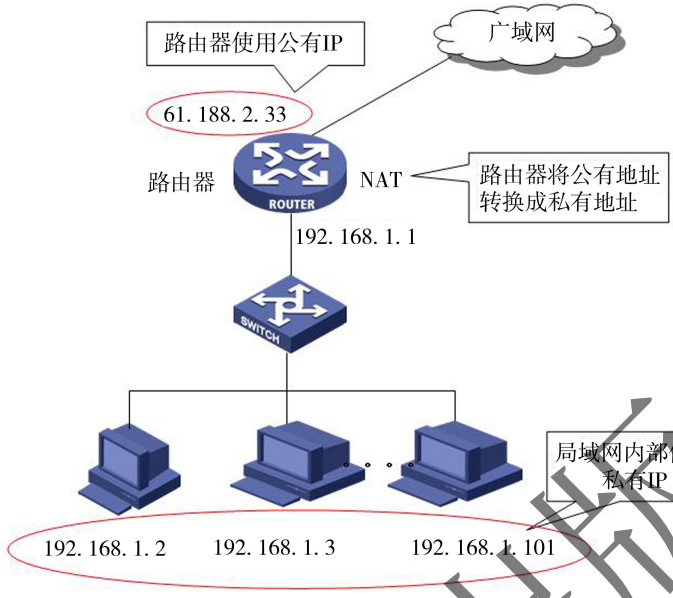

图 5-1-7　路由器进行 NAT 转换

(3)公有地址。

与私有地址相反,用于 Internet 中的 IP 地址称之为公有地址(Public Address),通过公有地址可直接访问互联网。

公有地址由 InterNIC(Internet Network Information Center 因特网信息中心)负责。

公有地址分类如表 5-1-3 所示。

表 5-1-3　　公有地址分类

类别	地址范围	私有地址	保留地址
A 类	1. 0. 0. 1～126. 255. 255. 254	10. 0. 0. 1～10. 255. 255. 254	127. 0. 0. 0～127. 255. 255. 255
B 类	128. 0. 0. 1～191. 255. 255. 254	172. 16. 0. 1～172. 31. 255. 254	169. 254. 0～169. 254. 255. 255
C 类	192. 0. 0. 1～223. 255. 255. 254	192. 168. 0. 1～192. 168. 255. 254	

2. 直接广播地址和有限广播地址

广播地址是一种特殊形式的 IP 地址。

所谓“广播”,是指同时向某个网段上所有的主机发送信息。广播地址分两种:直接广播地址、有限广播地址。

(1)直接广播地址。

直接广播地址是:一个有效的网络 ID 和表示主机 ID 部分的 bit 位全为“1”,即它指定了网络 ID 所指定的网段中的“所有主机”。

也就是说,一个直接广播数据包将被发送到网络 ID 所指定网段内的所有主机。

例如,192. 45. 255. 255 就是 B 类地址中的一个直接广播地址。直接广播数据包被发送到网络地址为 192. 45. 0. 0 网段的所有主机。

类似地,168. 123. 255. 255、202. 118. 26. 255 也都是直接广播地址。

(2)有限广播地址。

有限广播地址(又称本地广播地址),即 IP 地址中 32 bit 二进制数全为“1”的 IP 地址(255.255.255.255)。有限广播将广播限制在本地网络范围内,它用于向本地网络中的所有主机发送有限广播数据包。

对本机来说,IP 地址 255.255.255.255 是指本网段内的所有主机。

当主机不知道本机所处的网络时(如主机的启动过程中),甚至连它自己的 IP 地址也还不知道时,只能采用有限广播方式,希望从网络 IP 地址服务器处获得一个 IP 地址。

任何情况下,路由器都会禁止转发目的地址为有限广播地址(255.255.255.255)的数据包,这样的数据包仅仅会出现在本地网络中。

说明:有限广播的数据包里不包含自己的 IP 地址,而直接广播包含自身的 IP 地址。

3.“0”地址

如果 IP 地址中 32 bit 二进制数全为“0”时(0.0.0.0),代表所有的主机,即表示整个网络。

它表示了这样的一个集合:所有不清楚的目的网络和目的主机。所谓“不清楚”是指既不知道网络 ID,也不知道主机 ID。

若主机想在本网内通信,但又不知道本网的网络 ID,那么可以利用 0.0.0.0 地址。

4.回送地址

127.x.x.x 即是回送地址。其中 x 可以是任何数。回送地址是指本机,即指将信息回传给自己。

回送地址主要用于网络软件测试以及本机进程间通信。无论什么程序,一旦使用回送地址发送数据,协议软件立即返回,不进行任何网络传输。

例如,使用 ping 127.1.1.1 命令,可以测试本机 TCP/IP 协议是否安装正确,如图 5-1-8 所示。

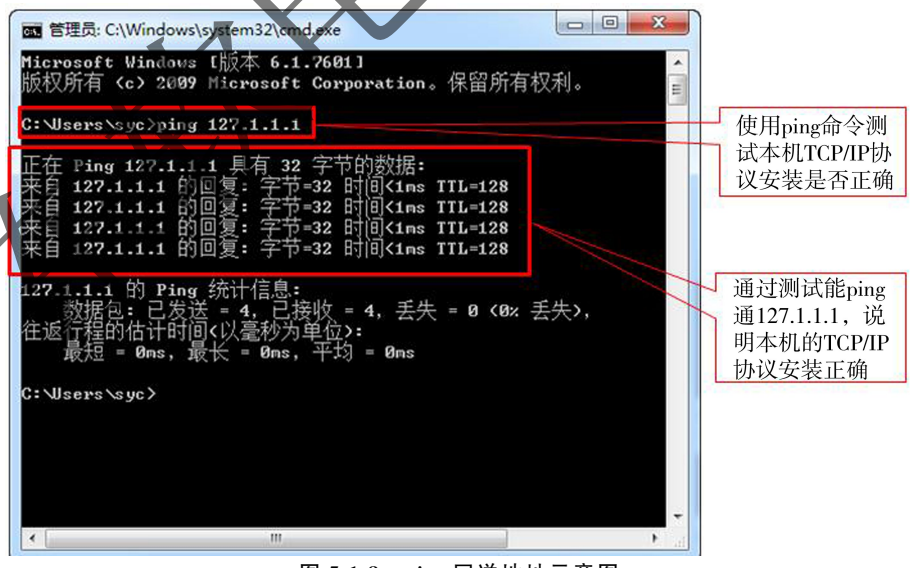

图 5-1-8 ping 回送地址示意图

5.小结

IP 地址根据网络 ID 和主机 ID 的数量分为 A、B、C 三类。

在一个网段中，它开始的第一个地址叫做“网络地址”（主机部分全为 0），最后一个地址叫“广播地址”（主机部分全为 1）。

例如，C 类 IP 地址 192.168.1.0 表示该网段的开始地址，即该网段的网络地址；192.168.1.255 表示该网段 192.168.1.0 的最后一个地址，即该网段的广播地址。这两个地址统属于特殊 IP 地址，不能分配给主机使用。

特殊地址及用途如表 5-1-4 所示。

表 5-1-4　　特殊用途地址

网络 ID	主机 ID	地址类型	用途
任意	全 0	网络地址	代表网络 ID 指定的网段
任意	全 1	直接广播地址	网络 ID 代表网段的所有节点
127	任意	回送地址	回环测试
全 0		所有网络	路由器用于指定默认路由
全 1		有限广播地址	只在本网络上进行广播（各路由器均不转发）

5.1.5　子网模式下的 IP 地址结构

IP 地址分为 A、B、C、D、E 五类，其中 A、B、C 三类地址最为常用。

通常，A 类地址分配给大型服务提供商使用，B 类地址分配给大公司使用，C 类地址分配给一般用户使用。但这样的分配方式会造成大量 IP 地址的浪费。

例如，一个 C 类地址最多可容纳 254 台主机，但如果主机数量只有 100 台，则多余的 254－100＝154 个 IP 地址将不能再使用，就被浪费掉了。因此，为了节省 IP 地址，将一个有类网络（A、B、C 类）再划分为若干个小网络。这样，便产生了子网与子网掩码。

“子网”是指把一个有类的网络地址，再划分成若干个小的网段，这些网段即称为子网。

如图 5-1-9 所示是一个子网模式下的地址结构。

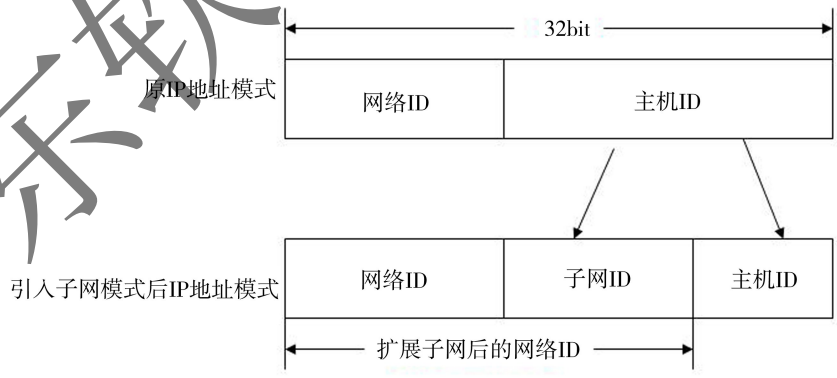

图 5-1-9　将主机 ID 部分进一步划分为子网 ID 和主机 ID

在划分子网以后，原 IP 地址模式变成了由三部分组成——网络 ID、子网 ID 和主机 ID。

在原来的 IP 地址模式中，网络 ID 部分就能够标识一个独立的物理网络，而引入子网模式后，需要网络 ID＋子网 ID 才能全局唯一地标识一个独立的物理网络。也就是说，子网的概念延伸了原网络 ID 部分，允许将一个网络分解为多个子网。

5.1.6 什么是子网掩码

随着子网的出现，使得扩展后的 IP 地址具有一定的内部层次结构，而且不再是按照标准地址（A 类、B 类、C 类等）来决定 IP 地址中的网络 ID，需要一个新的值来定义 IP 地址中哪部分是网络 ID，哪部分是主机 ID。这样，子网掩码应运而生。

子网掩码主要用于区分 IP 地址中的网络 ID 和主机 ID。它屏蔽了 IP 地址的主机部分，从而分离出网络 ID 和主机 ID。

说明：子网掩码可以理解为它是一部分透明，一部分不透明的纸条，不透明部分盖住主机 ID（掩住主机 ID），透明部分透出网络 ID。

子网掩码的格式同 IP 地址一样，是一个 32 位的二进制数，由连续的“1”和连续的“0”组成。为了理解的方便，也采用点分十进制表示。

子网掩码的定义为：对应于 IP 地址的网络 ID 部分，子网掩码的所有位都设为“1”，且“1”必须是连续的（即在连续的“1”之间不允许有“0”出现）；对应于 IP 地址的主机 ID 部分，子网掩码的所有位都设为“0”。

例如，IP 地址为 192.168.3.1，子网掩码为 255.255.255.0。

将 255.255.255.0 写成二进制形式，就如图 5-1-10 所示。

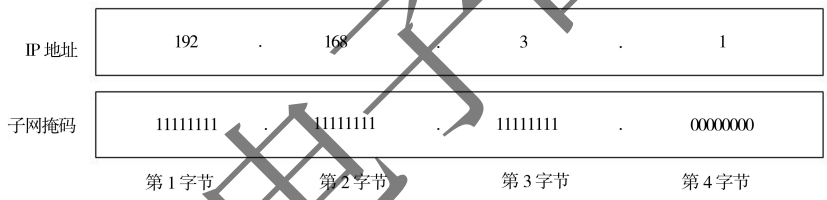

图 5-1-10　子网掩码分离出网络 ID 和主机 ID

图 5-1-10 中，子网掩码连续“1”的部分所对应的 IP 地址部分便是网络 ID，连续“0”部分所对应的 IP 地址部分便是主机 ID，即网络 ID 是 192.168.3（网络地址是 192.168.3.0），主机 ID 是 1。

对应地，A、B、C 类网络也都有自己缺省的子网掩码。

如图 5-1-11 所示，A 类网络的第 1 个字节表示网络 ID，因此其子网掩码是 255.0.0.0。

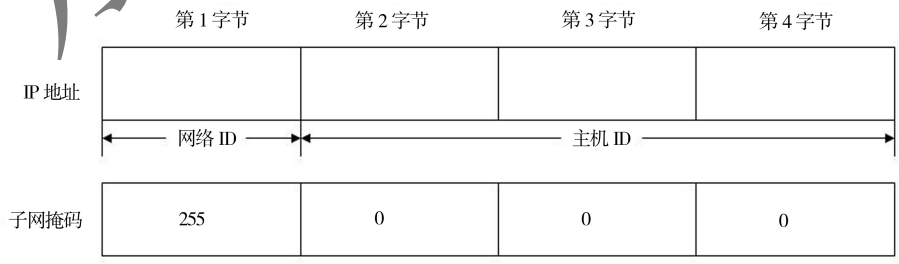

图 5-1-11　A 类网络的子网掩码

如图 5-1-12 所示，B 类网络的第 2 个字节表示网络 ID，因此其子网掩码是 255.255.0.0。

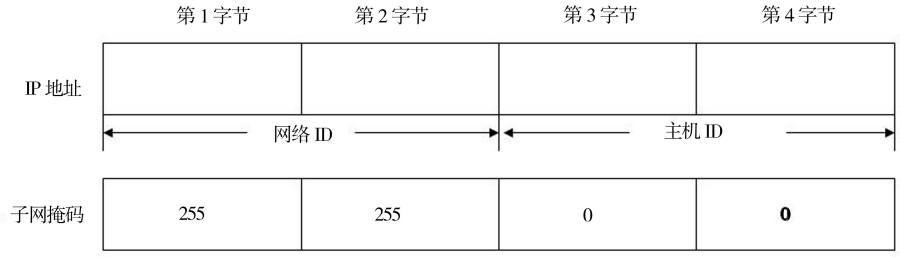

图 5-1-12　B 类网络的子网掩码

如图 5-1-13 所示，C 类网络的第 3 个字节表示网络 ID，因此其子网掩码是 255.255.255.0。

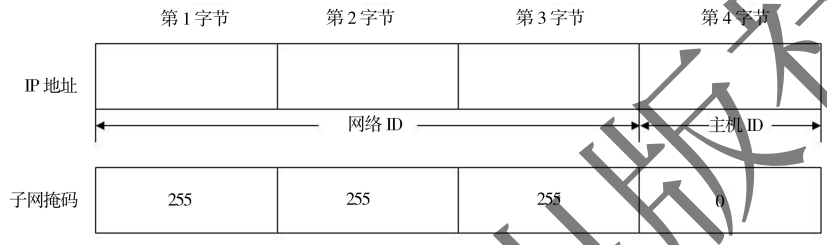

图 5-1-13　C 类网络的子网掩码

子网掩码还可以使用子网掩码中“1”的位数来表示。默认情况下，A 类地址为 8 位(8 位连续是“1”)，B 类地址为 16 位(16 位连续是“1”)，C 类地址为 24 位(24 位连续是“1”)。

例如，A 类的某个地址可表示为 12.10.10.3/8，这里的最后一个“8”是说明该地址的子网掩码有连续 8 位是“1”；而 199.42.26.0/28 表示网络地址是 199.42.26.0，子网掩码位数有连续 28 位是“1”。

5.1.7　用子网掩码求出网络 ID

公式：网络 ID＝IP 地址 and 子网掩码

即将 IP 地址和子网掩码进行布尔“与(and)”运算，所得结果即为网络 ID。

例如，网络中有一台主机的 IP 地址为 225.36.25.183，子网掩码为 255.255.255.240，则其网络 ID 是 225.36.25.176，运算过程如图 5-1-14 所示。

	点分十进制	二进制	
		网络ID	主机ID
IP地址	225.36.25.185	11100001 00100100 00011001 1011	0111
子网掩码	255.255.255.240	11111111 11111111 11111111 1111	0000
and运算结果	225.36.25.176	11100001 00100100 00011001 1011	0000

图 5-1-14　子网掩码的运算

说明：布尔“与(and)”运算：1and1＝1；1and0＝0；0and0＝0

5.1.8　IP 地址类别与子网掩码关系

例如：IP 地址是 2.1.1.1，子网掩码是 255.255.255.0，那么 IP 地址属于哪一类呢？正确答案是 A 类。

如图 5-1-15 所示，IP 地址的类别是根据分类原则进行划分的，而子网掩码 255.255.255.0 只是表示了在这个 A 类地址中，借用了主机 ID 的 2 个字节作为子网 ID。

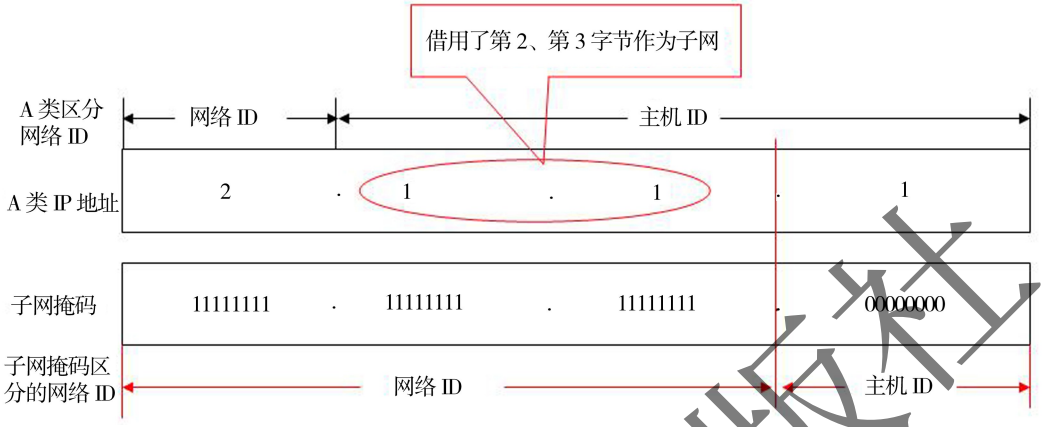

图 5-1-15　IP 地址类别与子网掩码关系

5.1.9　子网划分方法

子网的划分，实际上就是设计子网掩码的过程，即向 IP 地址中原来表示主机 ID 的 bit 位借位，作为子网 ID。

由于 C 类地址最常用，这里仅介绍 C 类地址的划分方法。

对于 C 类地址，它默认的子网掩码是 255.255.255.0，即默认可用主机数最大是 255－2＝253，即减去网络地址(255.255.255.0)和广播地址(255.255.255.255)这两个特殊地址。

但是，如果在一个小型局域网中，主机数量达不到 253 个，则可以根据要求，将 C 类地址的主机 ID 进行再划分，成为若个子网。也就是说，在一个 C 类地址主机 ID 的 8 位 bit 中，借位进行划分子网。这便是 C 类地址的子网划分。

子网划分实际上就是确定子网掩码。确定子网掩码就是要确定向原来表示主机 ID 的 bit 位要借多少位，即确定子网掩码连续“1”的个数。

注意：子网的 bit 位必须是由左到右进行定义，即中间不能跳位，要连续为“1”。

要进行子网划分，选择一个可用的子网掩码，就需要考虑及推断由这个子网掩码所决定的子网数量、有效主机数量等。下面五个问题是选择子网掩码时需要考虑及回答的问题：

(1)要划分多少个子网？

(2)每个子网中有多少个主机数？

(3)每个子网的网络地址(即每个网段的第一个地址)是什么？

(4)每个子网的广播地址(即每个网段的最后一个地址)是什么？

(5)每个子网中有效主机范围是什么？

说明：每个子网的网络地址是每个子网的第一个地址，每个子网的广播地址是每个子网的最后一个地址。

1. 确定划分子网数量

公式：划分子网数量＝2^x-2

其中 x 是向原表示主机 ID 所借的位数(主机位的从左到右),即掩码中连续“1”的个数。

例 1:如图 5-1-16 所示,IP 地址 192.168.5.1,子网掩码是 255.255.255.192;该子网掩码划分了多少个子网?

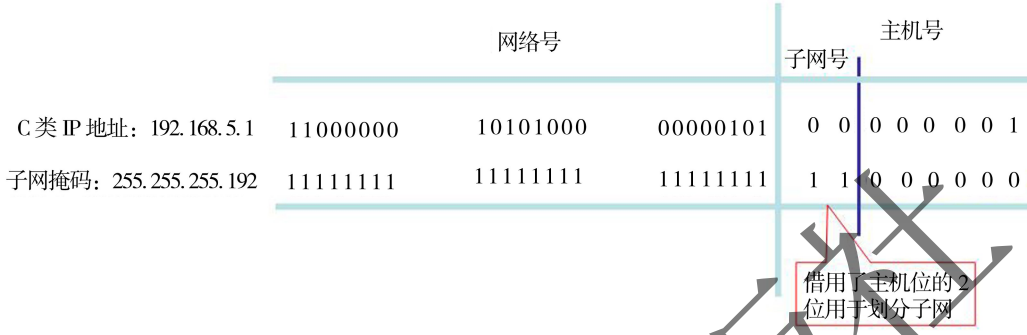

图 5-1-16　借用主机 2 位划分子网

图 5-1-16 中可看出,完整的子网掩码是 255.255.255.192,即在 C 类地址表示主机 ID 的 8 个 bit 中,从左到右借用 2 个 bit 位(子网掩码“1”的个数在主机位中是 2 位),即划分了 $2^2-2=2$ 个子网。

表 5-1-5 是 C 类地址子网划分表,表中列出了所有子网划分的可能。

表 5-1-5　　C 类地址子网划分表

子网位数	子网数量	主机位数	主机数量	子网掩码
2	4	6	62	255.255.255.192
3	8	5	30	255.255.255.224
4	16	4	14	255.255.255.240
5	32	3	6	255.255.255.248
6	64	2	2	255.255.255.252

2. 确定每个子网中的主机数量

公式:每个子网中主机数量$=2^y-2$

其中,y 是非掩码位的位数,即子网掩码中“0”的个数;减 2 是因为要减掉子网的网络地址和广播地址。

例 2:例 1 中主机位的子网掩码“11000000”中,“0”的个数决定了每个子网可以有 $2^6-2=64-2=62$ 台主机。

3. 确定每个子网的网络地址

每个子网的网络地址(每个子网的开始地址)是以掩码块大小做增量计算的。其中,掩码块大小=256−十进制的子网掩码。

例 3:例 1 中子网掩码是 255.255.255.192,则掩码块大小=256−192=64。因此,第一个子网网络地址是 192.168.10.64,第二个子网网络地址是 192.168.10.128。

4. 确定每个子网的广播地址

公式:每个子网的广播地址=下个子网号−1

例 4：在例 1 中，有两个广播地址：

第一个广播地址：下个子网网络地址－1＝128－1＝127，即 192.168.5.127；

第二个广播地址：下个子网网络地址－1＝(128＋64)－1＝191，即 192.168.5.191。

注意：最后子网的广播地址将总是 255。

5. 确定有效主机范围

公式：有效主机范围＝每个子网的网络地址＋1～每个子网的广播地址－1

即有效主机范围是介于各个子网之间的取值，并减去全“0”和全“1”的主机 ID。

例 5：例 1 中的有效主机范围是：

第一个子网主机地址范围是 192.168.5.65 ～192.168.10.126；

第二个子网主机地址范围是 192.168.5.129 ～192.168.10.190。

6. 小结

IP 地址 192.168.5.1，子网掩码 255.255.255.192，总结例 1～例 5，子网划分结果如下：

(1)根据子网掩码可分两个子网；

(2)两个子网的最大主机数可有：$2^6-2=62$ 个；

(3)两个子网的网络地址分别是：掩码增量＝256－192＝64，即第一个子网号是 192.168.5.64，第二个子网号是 192.168.5.128；

(4)广播地址：由于广播地址＝下个子网网络地址－1，因此两个子网的广播地址分别是 192.168.5.127 和 192.168.5.191；

(5)有效主机范围：

第一个子网主机地址范围是：192.168.5.65～192.168.5.126；

第二个子网主机地址范围是：192.168.5.129～192.168.5.190。

如图 5-1-17 所示是最终划分子网后的网络拓扑图。

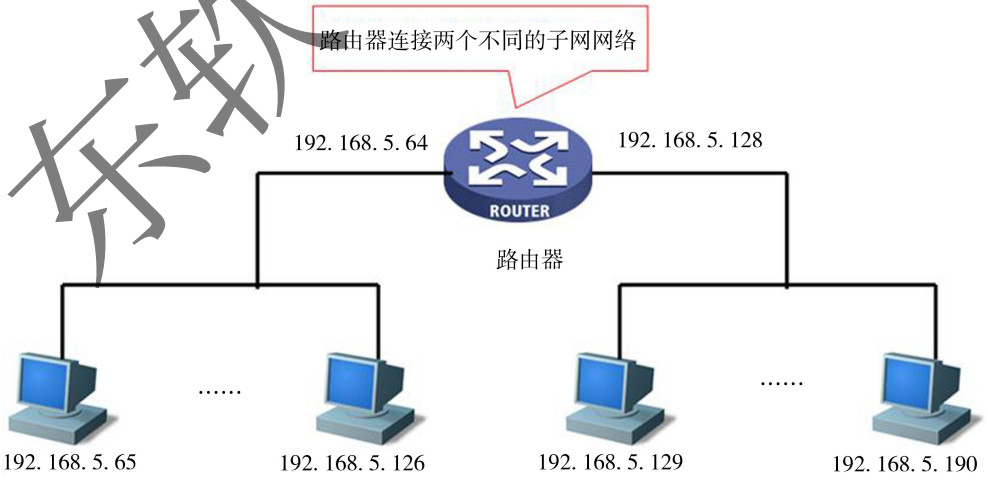

图 5-1-17　划分子网后的网络拓扑图

5.2　虚拟局域网相关知识

目前，交换机中大量使用了虚拟局域网（VLAN）技术。

VLAN 技术在后面有专门的专业课介绍，这里仅仅介绍 VLAN 相关基本概念。一提到 VLAN，一定会涉及广播域及广播风暴问题。

5.2.1　广播域与广播风暴

交换机虽然解决了冲突域的问题，即交换机隔离了冲突域，但交换机没有隔离广播域，交换机的所有端口依然处在同一个广播域。

1. 什么是广播域

在第 4 章中已介绍了什么是冲突域。冲突域是指所有设备所共享的介质范围。一个集线器的所有端口同处于一个冲突域，一个交换机的每一个端口是一个冲突域。

而广播域指的是能接收到广播数据包的主机范围（广播数据包通常采用广播地址发送，即主机 ID 全为“1”的地址）。

处于同一个网络的所有设备位于同一个广播域。也就是说，所有的广播信息会播发到网络的每一个端口（即使交换机也不能阻止广播信息的传播）。

从广播域的定义和交换机的特性可以看出，交换机的所有端口虽然在不同的冲突域，但仍然同处一个广播域。

在第 4 章已经介绍过，交换机的工作原理是依据 MAC 地址表做数据帧单点转发，因此，在转发数据时，每个端口所连接的计算机之间不受影响。但如果交换机在 MAC 地址表中没有找到 MAC 地址与端口映射，就需要发送广播给交换机端口连接的所有计算机，以此获得目标 MAC 地址与端口的映射关系。

也就是说，连接在交换机上的设备同处一个广播域，但不属于同一个冲突域，交换机的每个端口是一个冲突域，如图 5-2-1 所示。

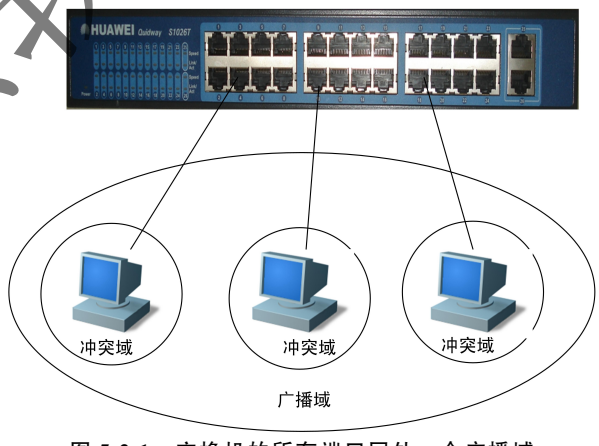

图 5-2-1　交换机的所有端口同处一个广播域

2. 什么是广播风暴

广播风暴是指大量广播数据充斥了网络，占用了大量的网络带宽，导致了网络无法正常运行，甚至造成了网络的彻底瘫痪。

理解帧的传输方式可帮助理解“广播风暴”。

帧的传输方式有单播帧（Unicast Frame）、多播帧（Multicast Frame）和广播帧（Broadcast Frame）。

（1）单播帧。

单播帧也称“点对点”通信。单播帧的接收和传递只在两个节点之间进行。

帧的目的 MAC 地址就是对方的 MAC 地址，网络设备（指交换机和路由器）根据帧中的目的 MAC 地址，将帧转发出去，如图 5-2-2 所示。

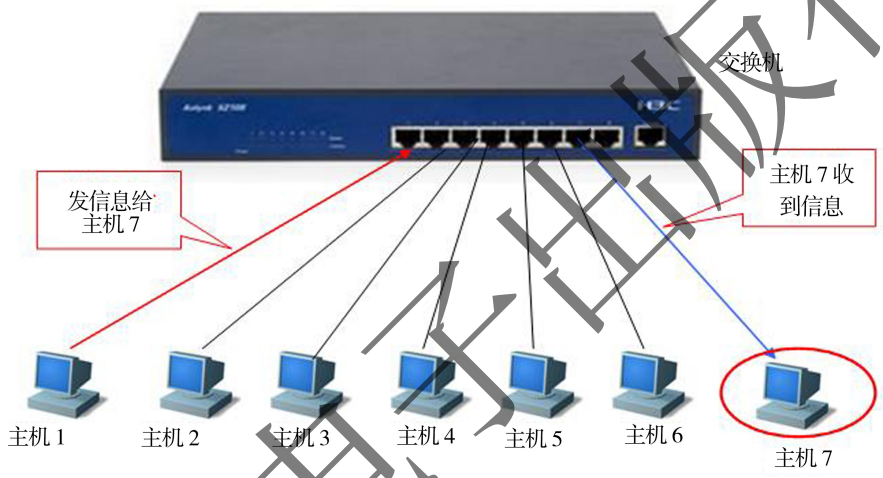

图 5-2-2　单播帧示意图

（2）多播帧。

多播帧可以理解为一个人向多个人（但不是所有人）说话。多播帧能够提高通话的效率。

多播帧占网络中的比重并不大，主要应用于网络设备内部通信、网上视频会议和网上视频点播等。多播帧示意图如图 5-2-3 所示。

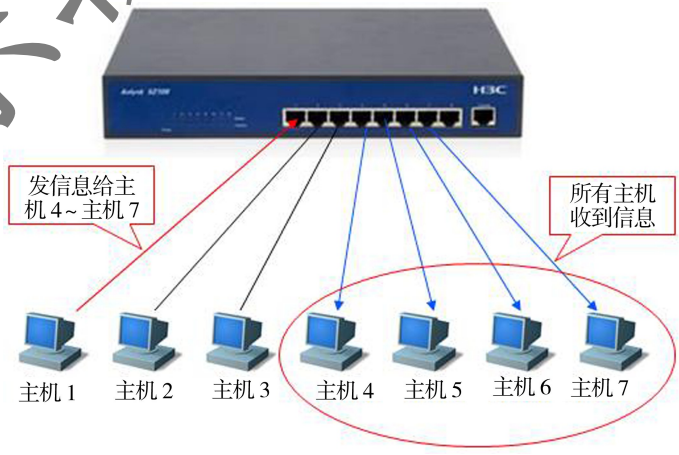

图 5-2-3　多播帧示意图

(3)广播帧。

广播帧可以理解为一个人对在场所有人说话。广播帧能够提高通话效率,信息一下子就可以传递到全体。

在广播帧中,帧中的目的 MAC 地址是“FF. FF. FF. FF. FF. FF”,代表网络上所有设备网卡的 MAC 地址,如图 5-2-4 所示。

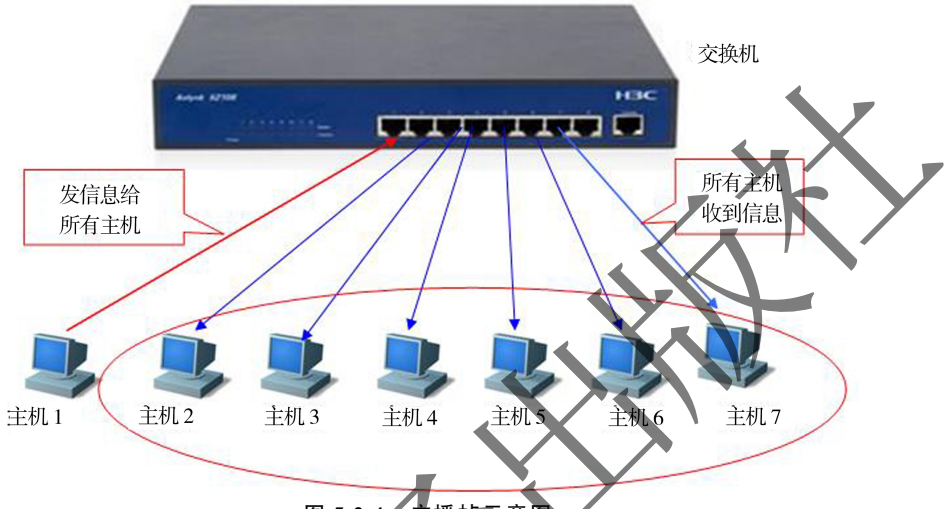

图 5-2-4　广播帧示意图

广播帧在网络中是必不可少的,它在网络中起着非常重要的作用,是作为发现未知设备的主要手段。

例如,交换机就是利用广播手段进行 MAC 地址学习的。同单播和多播相比,广播几乎占用了子网内网络的所有带宽。网络中不能长时间出现大量的广播帧,否则就会出现所谓的“广播风暴”,这如同在会场上只能有一个人发言,如果所有人都同时发言的话,就会造成会场一片混乱。

3. 引起广播风暴主要原因

引起广播风暴的原因有很多,主要原因有以下几点。

(1)网卡损坏造成:设备损坏的网卡,会不停地向交换机发送大量的数据包,产生了大量无用的数据包,导致了广播风暴的产生。

(2)网络环路造成:网络环路的产生,一般是由于一条物理网络线路的两端,同时接在了一台网络设备中。例如,将一条双绞线,两端插在同一个交换机的不同端口上,便导致了典型的网络环路。

(3)网络病毒造成:网络病毒的传播,会损耗大量的网络带宽,引起网络堵塞,引起广播风暴。

(4)黑客软件造成:黑客软件对内部网络进行攻击,也会引起广播风暴。

5.2.2　VLAN 基本概念

如上所述,广播风暴能导致网络性能下降,甚至网络瘫痪,那么怎样才能够避免广播风暴呢?

首先想到的就是减少广播域内的主机数量,缩小广播域。

虚拟局域网(VLAN,Virtual Local Area Network),是一种专门为隔离二层广播报文设计

的 VLAN 技术，是将局域网从逻辑上划分为不同的网段，而不是从物理上划分网段的技术。它是从逻辑上把网络资源和网络用户，按照一定的原则进行划分，把一个物理上的网络划分成多个小的逻辑网络，这些小的逻辑网络就形成了各自小的广播域，从而隔离了大的广播域。

下面是 VLAN 划分广播域的一个说明，分两部分。

如图 5-2-5 所示的是第一部分：如果将两个部门财务处、开发部的网络独立，则这两个部门不能互访，为了使这两个部门能相互访问，将这两个部门的网络设在一个网络中，且采用交换机将它们连接在一起，以便相互访问，但又产生了其他问题：增大了广播域和广播流量，即出现了广播风暴问题。

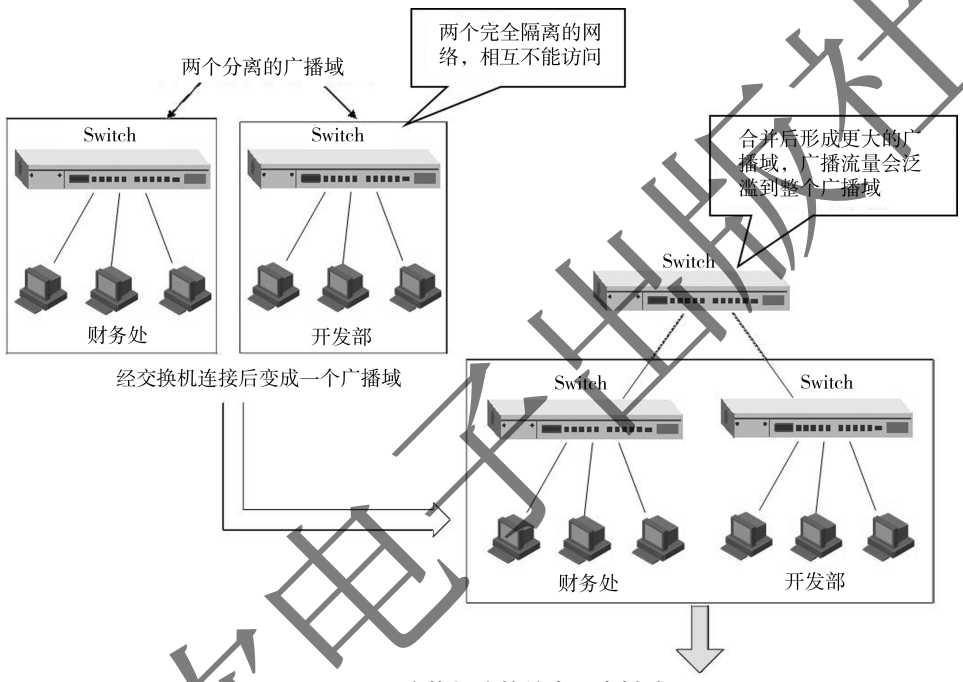

图 5-2-5　交换机连接扩大了广播域

如图 5-2-6 所示是第二部分：采用 VLAN 技术，使原来两个部门的一个物理网络，从逻辑上分为两个网络，即分隔了广播域，形成各自小的广播域，使广播报文不能跨越广播域传送。

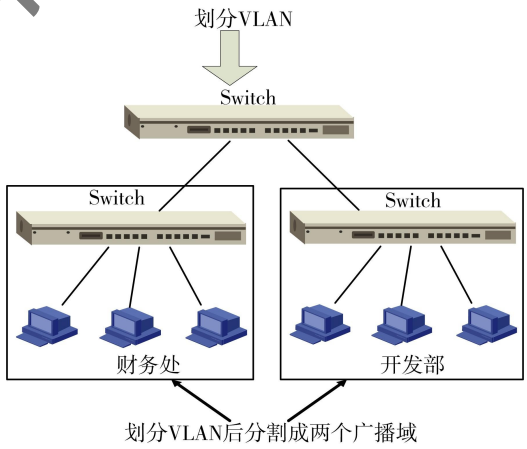

图 5-2-6　VLAN 从逻辑上分隔了两个广播域

又例如：如图 5-2-7 所示，如果财务处设在 1 楼，办公室设在 3 楼，开发部的一部分设在 3 楼，另一部分设在 6 楼。

对于这种分布在不同物理位置的部门，采用 VLAN 技术，可不改变任何布线、插拔交换机端口，即可轻松地对各部门进行广播域隔离。

图 5-2-7 中，将与财务处连接的交换机端口划到财务处的 VLAN1 中；将与办公室连接的交换机端口划到办公室的 VLAN2 中；将与开发部连接的交换机端口划到开发部的 VLAN3 中，即可分隔广播域了，非常简单方便，无需做任何物理改变。

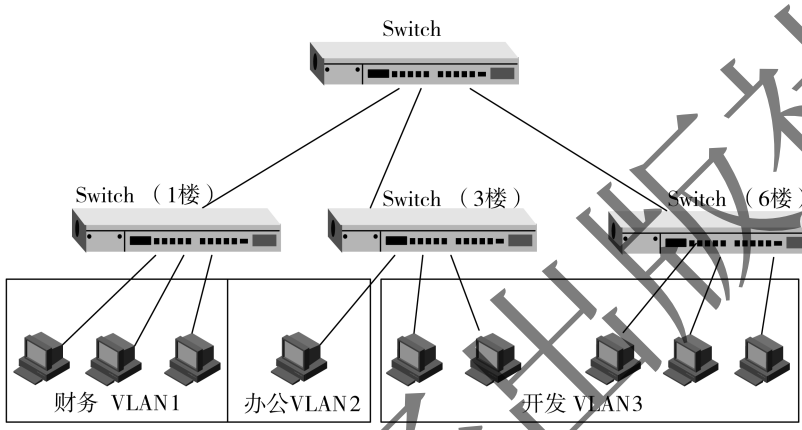

图 5-2-7　VLAN 解决一个部门位于多个地点问题示意图

VLAN 相关概念总结如下：

(1)VLAN 是一个在物理网络上，根据用途、工作组、应用等进行逻辑划分的虚拟局域网络，与用户的物理位置没有关系。

(2)VLAN 中的网络用户通过交换机进行通信。一个 VLAN 中的成员看不到另一个 VLAN 中的成员。

(3)VLAN 技术主要应用于交换机，但并不是所有交换机都具有此功能，只有支持 VLAN 协议的交换机才可使用此功能。

(4)一个 VLAN 内的主机想要同另一个 VLAN 内的主机进行通信时，必须通过三层设备(如路由器)才能实现。因为不同 VLAN 逻辑上就是不同的网络，不同的网络连接应采用路由器连接。

5.2.3　VLAN 主要功能

VLAN 主要功能有以下几方面。

(1)提高通信效果。同一个交换机上的设备，如果处于不同的 VLAN，彼此也不能互相通信。这样，通信流量被局限于本地的 VLAN 中，不会对其他 VLAN 产生干扰。

(2)控制广播风暴。处于同一个 VLAN 中的所有设备属于同一个广播域，处于不同 VLAN 中的设备，即使是在同一个交换机上，也不属于同一个广播域，从而在规模较大的网络中，消除了广播域产生的条件。

(3)确保网络安全。不同 VLAN 间无法随意进行访问，所以杜绝了广播信息的不安全性。

(4)简化网络管理。VLAN 使网络的组织更具灵活性，更改用户所属的 VLAN 不必换端

口和连接，只需修改交换机配置，将其划归到相应的 VLAN 中即可。

5.2.4 VLAN 划分方法分类

从技术角度讲，VLAN 划分可依据不同原则，一般主要有以下四种划分方法。

1. 基于端口划分 VLAN

这是根据交换机端口来定义 VLAN 成员。

每个交换机端口属于一个 VLAN，网络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。属于同一 VLAN 的端口可以不连续；一个 VALN 可以跨越多个以太网交换机。

基于端口划分 VLAN 是最简单，也是最有效的方法。

如图 5-2-8 所示是单交换机划分了两个 VLAN，不同 VLAN 之间的主机，彼此不连通。

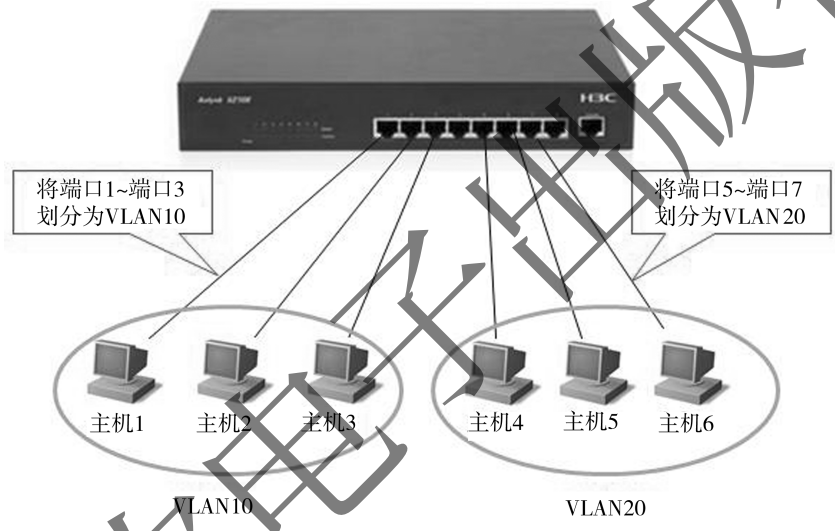

图 5-2-8 单交换机划分了两个 VLAN

2. 基于 MAC 地址划分 VLAN

这是根据每个主机的 MAC 地址来定义 VLAN 成员。

即对每个 MAC 地址的主机都配置它属于哪个组。这种方式的 VLAN 允许网络用户从一个物理位置移动到另一个物理位置时，自动保留其所属 VLAN 的成员身份。

这种 VLAN 划分方法最大的优点就是，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，因为它是基于用户，而不是基于交换机的端口。

3. 基于第三层协议划分 VLAN

这是根据网络层协议类型来定义 VLAN 成员的。

这种按网络层协议组成的 VLAN，可使广播域跨越多个 VLAN 交换机。这对那些希望针对具体应用和服务来组织用户的网络管理员来说是非常具有吸引力的。而且，用户可以在网络内部自由移动，其 VLAN 成员身份仍然保留不变。

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，而且可以根据协议类型来划分 VLAN。

4. 基于策略划分 VLAN

这是一种比较灵活有效的 VLAN 划分方法。是依据采用什么样的策略进行划分。目前常用的策略有：按 MAC 地址、按 IP 地址、按以太网协议类型和按网络应用等。

5.2.5　单交换机划分 VLAN 步骤

不同网络设备厂商生产的交换机配置命令不同，但原理和过程基本相同。下面以 H3C 公司的交换机为例，简单介绍如何使用单交换机进行基于端口的 VLAN 划分。

1. 连接并登录到交换机管理系统

第一次使用交换机，要登录到交换机管理系统进行配置和管理交换机。

首先，使用 Console 线的 RJ-45 接头一端连接交换机的 Console 口，Console 线的另一端串口接头连接管理计算机的串行口，如图 5-2-9 所示。

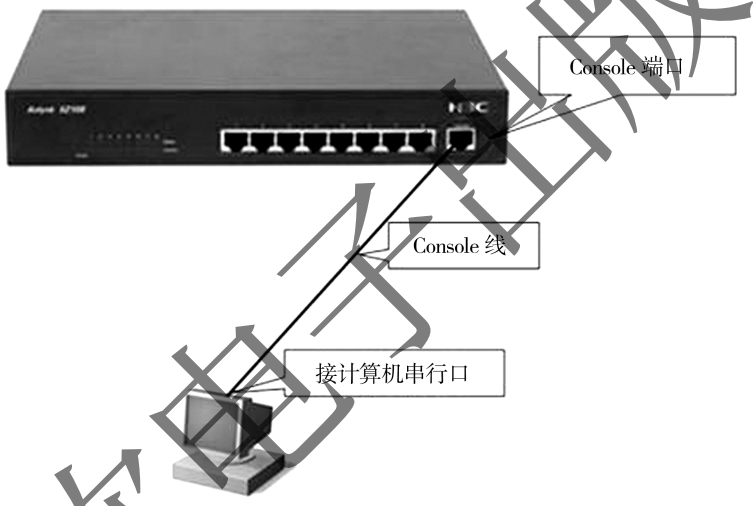

图 5-2-9　连接管理计算机与交换机

其次，运行管理计算机操作系统自带的“超级终端”程序，登录到交换机操作系统进行配置与管理。详见 5.4 任务案例 2。

2. 进入交换机视图

运行“超级终端”程序，登录到交换机操作系统后，首先进入交换机的“用户视图”模式。

H3C 交换机主要有四种视图模式：用户视图、系统视图、以太网端口视图和 VLAN 配置视图。

不同模式的视图只能执行该视图所允许的命令与操作。

(1)用户视图。

如图 5-2-10 所示，是进入交换机后默认的“用户视图”模式。

图 5-2-10 中，“用户视图”模式的提示符为尖括号(＜ ＞)。

“用户视图”模式下，只能查询交换机的一些基础信息，如版本号等。

图 5-2-10 “用户视图”模式

(2)系统视图。

如果要对交换机进行配置,必须通过“system-view”命令,从“用户视图”模式进入“系统视图”。“系统视图”提示符为中括号([ ])。

如图 5-2-11 所示,从“用户视图”模式(<H3C>)进入“系统视图”([H3C])。

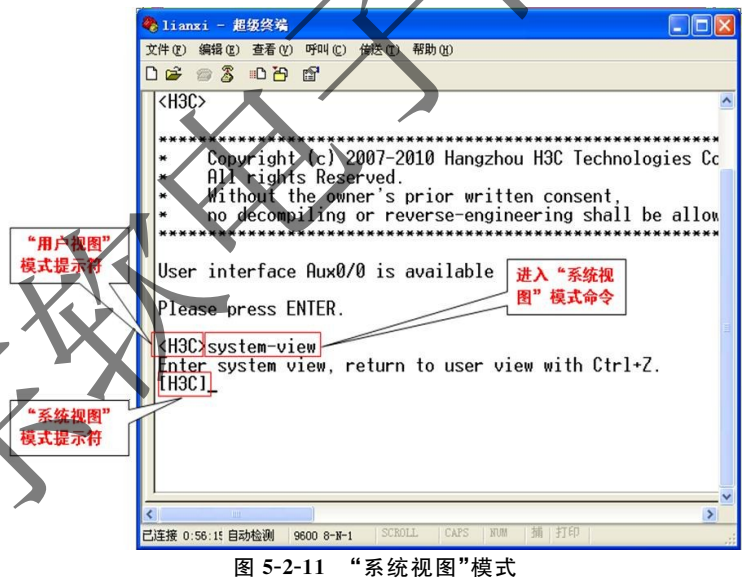

图 5-2-11 “系统视图”模式

(3)以太网端口视图。

如果要为交换机端口配置参数,要进入“以太网端口视图”模式。

“以太网端口视图”的提示符为中括号,且中括号内是对应的端口号。

如图 5-2-12 所示,是进入端口 1(ethenet 0/1 中的“0”是标识不同的交换机模块,“1”是表示该模块的端口号 1)的“以太网端口视图”模式命令及进入端口 1 后的“以太网端口视图”。

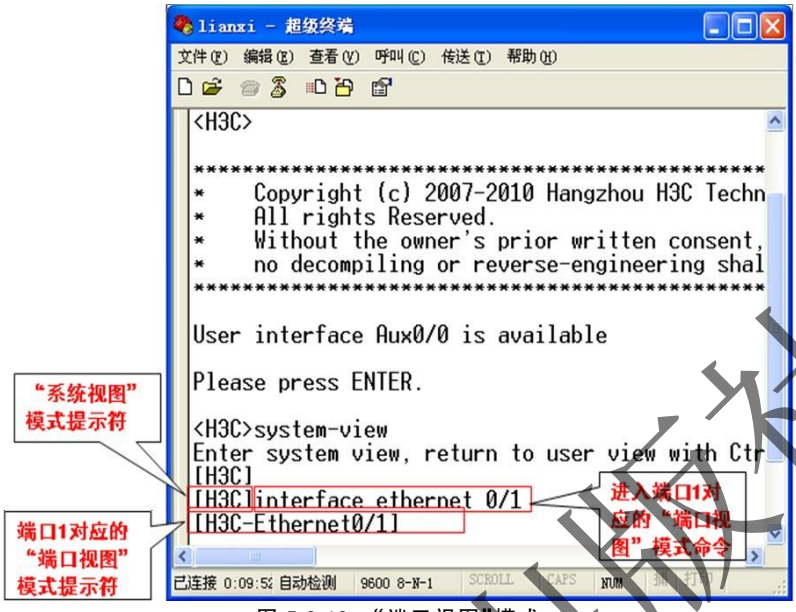

图 5-2-12　"端口视图"模式

(4)VLAN 配置视图。

"VLAN 配置视图"模式下,可设置所对应的 VLAN 的相关参数。

如图 5-2-13 所示是进入 VLAN10 的"VLAN 配置视图"。

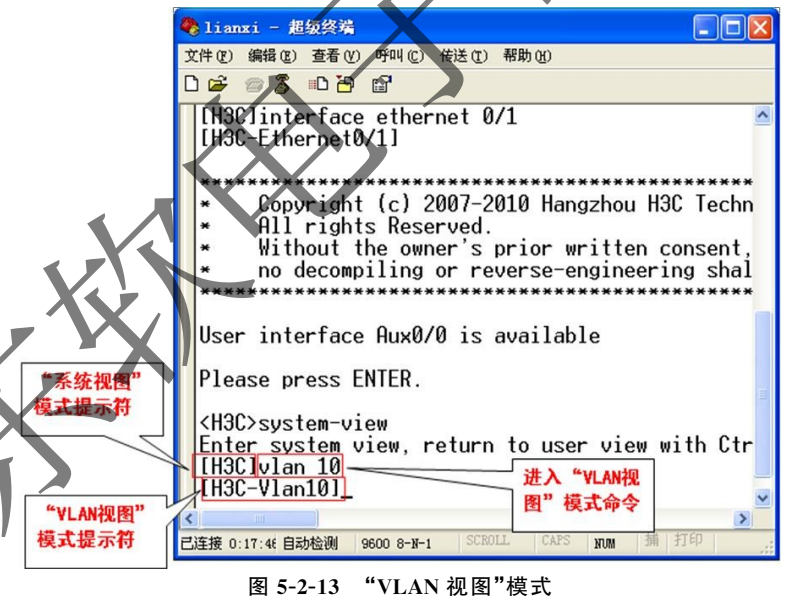

图 5-2-13　"VLAN 视图"模式

3. 查看交换机 VLAN 状态

第一次使用交换机,要首先查看交换机当前的 VLAN 状态,了解 VLAN 设置情况。

步骤 1:进入交换机"系统视图"界面。

命令格式:system-view(在"用户视图"模式下)

如图 5-2-14 所示,从"用户视图"进入"系统视图"模式。

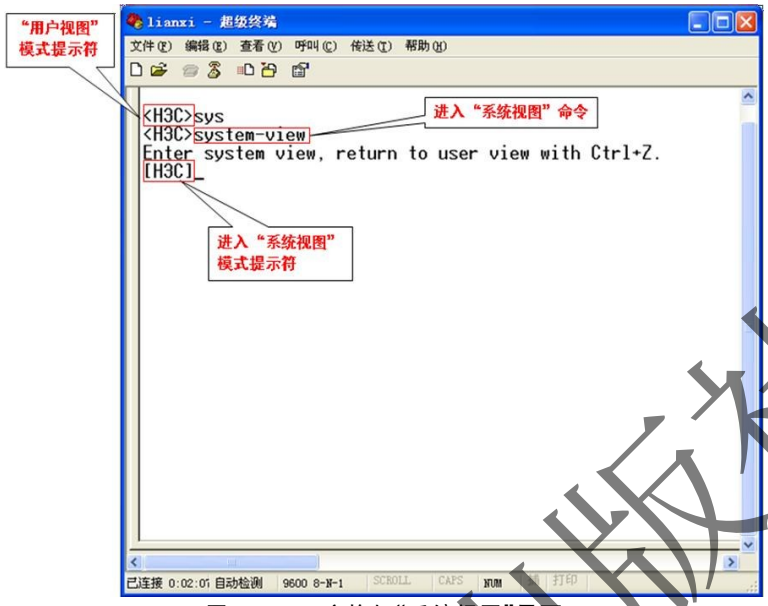

图 5-2-14 交换机"系统视图"界面

步骤 2:查看当前交换机中 VLAN 状态。

命令格式:display vlan(在"系统视图"模式下)

在划分 VLAN 之前,应首先了解交换机当前 VLAN 状态。

如图 5-2-15 所示,查看当前 VLAN,且结果是仅有默认 VLAN1。

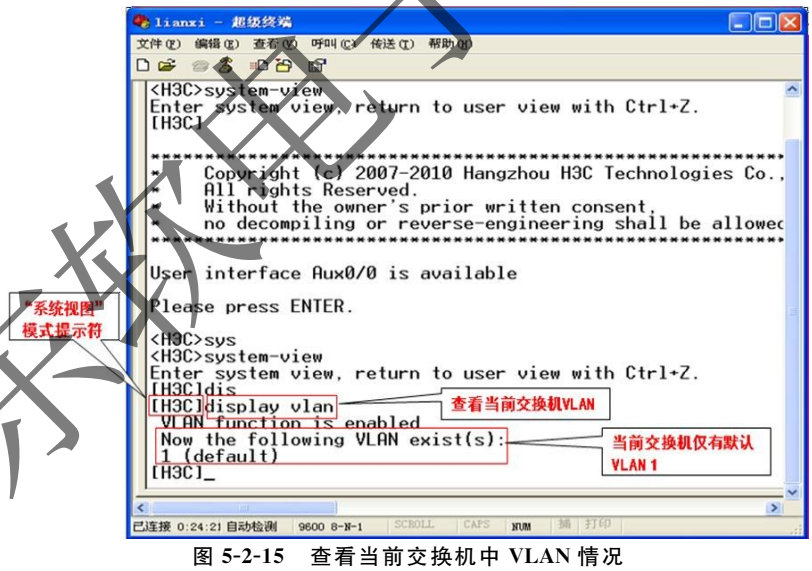

图 5-2-15 查看当前交换机中 VLAN 情况

4. 创建所需的 VLAN

命令格式:VLAN 数字号码(在"系统视图"模式下)

其中"数字号码"代表要新创建的 VLAN 号码。

如图 5-2-16 所示,创建了一个 VLAN10。

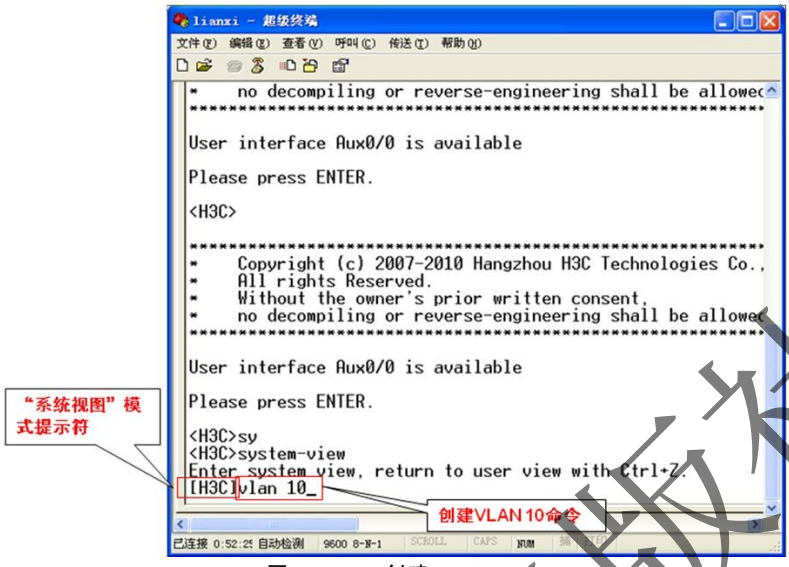

图 5-2-16　创建 VLAN10

5. 将对应交换机端口号加入 VLAN 中

命令格式：port 端口号(在“VLAN 视图”下)

在“VLAN 视图”模式下，把要加入到某个 VLAN 的交换机端口(可以是多个)加入到指定的 VLAN 中。

如图 5-2-17 所示，将端口 1 加入到 VLAN10 中。

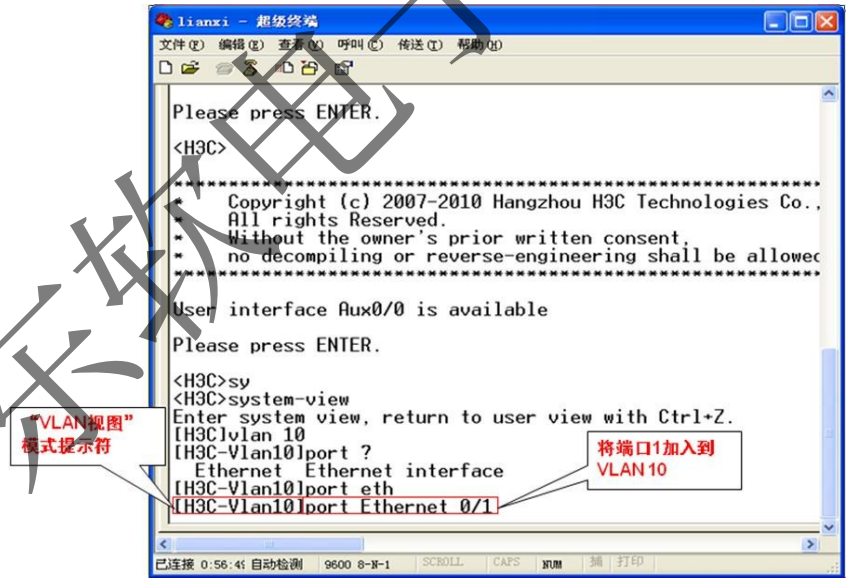

图 5-2-17　将端口加入到 VLAN10

6. 再次查看交换机端口状态

重复第 3 步，目的是检查命令是否起作用。

如图 5-2-18 所示，在 VLAN10 的“VLAN 视图”模式下，使用命令查看 VLAN 状态。

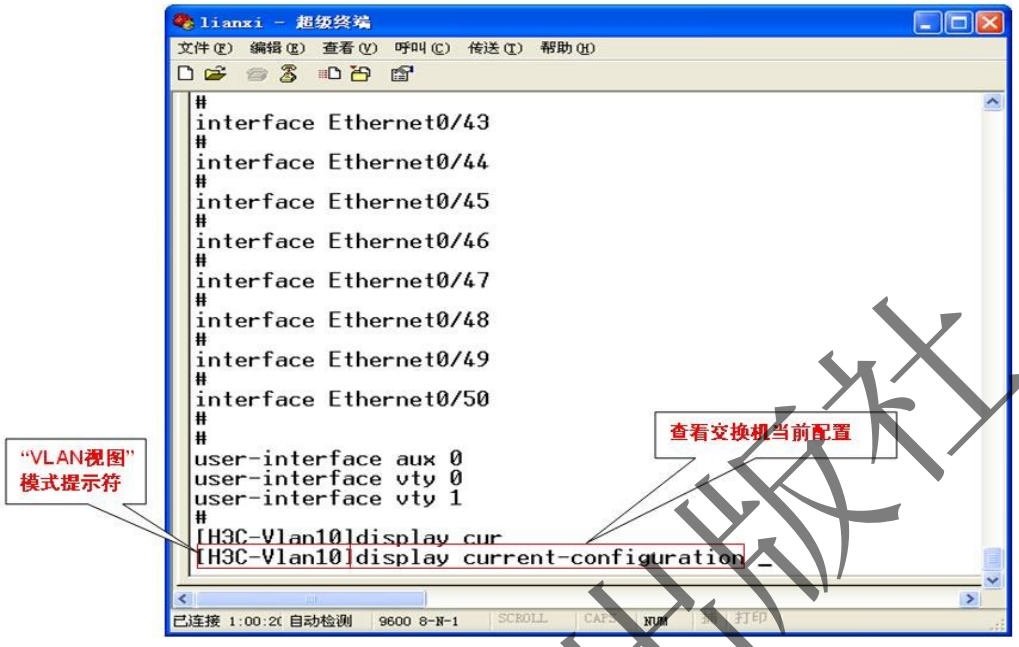

图 5-2-18 查看划分 VLAN10 的信息

如图 5-2-19 所示，显示已建成 VLAN10，且端口 1 在 VLAN10 中。

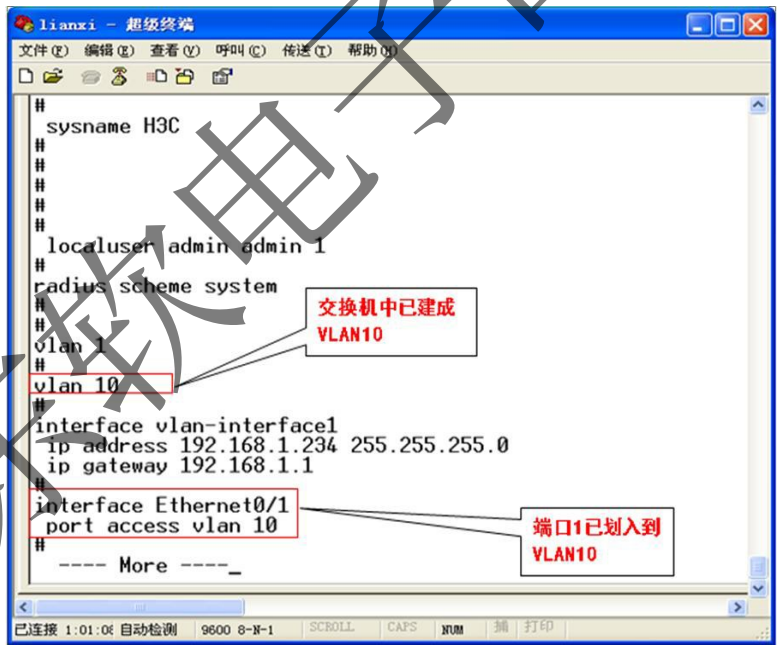

图 5-2-19 设置后交换机状态

7. 退出设置

命令格式：quit(在任何视图均可，该命令退出当前视图并返回上一级视图)

如图 5-2-20 所示，一直退出到“用户视图“模式下。

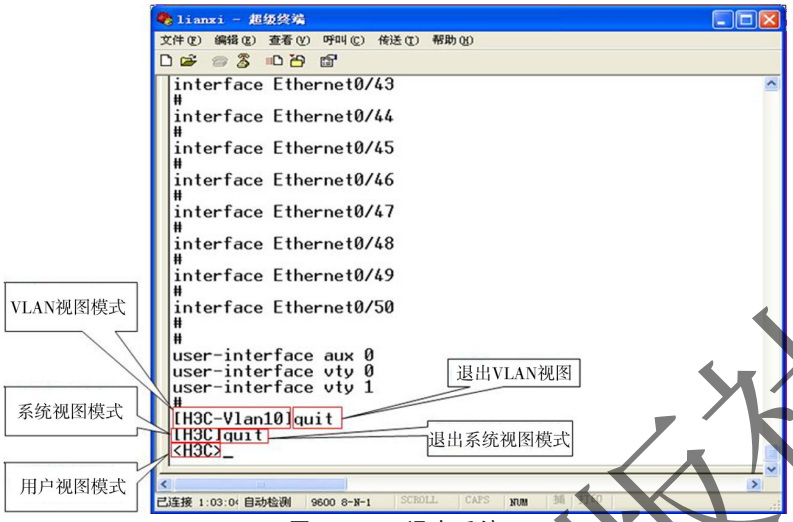

图 5-2-20　退出系统

表 5-2-1 显示了 H3C 配置 VLAN 主要步骤及命令。

表 5-2-1　　H3C 配置 VLAN 主要步骤及命令

步骤	命令	命令当前视图	说明
1	system-view	用户视图	进入交换机“系统视图”模式
2	display vlan	系统视图	显示当前交换机中 VLAN 状态
3	VLAN 数字号	系统视图	创建所需 VLAN 号
4	port 端口号	VLAN 视图	将端口号加入当前 VLAN 中
5	display currrent-configuration	VLAN 视图	查看当前交换机状态及配置命令是否生效

8. 举例

例如，要在一个交换机上创建两个 VLAN：VLAN10 和 VLAN20，将端口 2～5 加入到 VLAN10，将端口 8 加入到 VLAN20，则主要命令及步骤如表 5-2-2 所示。

表 5-2-2　　按要求创建 VLAN 主要命令及步骤

步骤	命令	说明
1	system-view	进入“系统视图”
2	display currrent-configuration display vlan	显示当前交换机端口状态； 显示当前交换机中 VLAN 情况
3	VLAN10	在“系统视图”下创建 VLAN10，并进入“VLAN 视图 ”
4	port ethe0/2 to ethe10/5	在“VLAN 视图”下，将端口 2～5 加入到 VLAN10（“ethe0/2”中的“ethe0/”是标识不同的交换机模块，“2”是表示该模块的端口号 2）
5	VLAN20	创建 VLAN20 并进入“VLAN 视图”
6	port ethe0/8	在“VLAN 视图”下将端口 8 加入到 VLAN20
7	display currrent-configuration	在“系统视图”下再次显示当前交换机端口状态，查看配置命令是否生效

5.3 任务案例1——划分子网

【任务描述】对一个C类地址，划分出四个子网，目的是熟练子网划分方法。

【任务要求】学院新建了四个机房，每个机房有25台PC机，有一个C类IP地址192.168.10.0，子网掩码是255.255.255.0；现要求将每个机房划为一个子网，确定出每个机房的网络ID、主机地址范围、广播地址和子网掩码。

【任务分析】本任务的核心是确定子网掩码。确定子网掩码后，即可根据相关公式，分别求出每个子网的主机数量、网络地址、广播地址和主机地址范围。

5.3.1 划分子网的步骤及公式

从“5.1.9 子网划分方法”得知，划分子网的步骤及公式如下：

步骤1：确定划分子网数量。公式是：划分子网数量$=2^{N}-2$

步骤2：确定每个子网中的主机数量。公式是：主机数量$=2^{n}-2$

步骤3：确定有效的子网网络地址。首先确定“掩码块大小”，掩码块大小$=256-$十进制的子网掩码；再以“掩码块大小”做增量，依次确定每个子网的网络地址。

步骤4：确定每个子网的广播地址。公式是：广播地址＝下个子网网络地址－1

步骤5：确定每个子网的有效主机范围。公式是：有效主机范围＝各子网的网络地址＋1～各子网的广播地址号－1

下面依据以上步骤划分子网。

5.3.2 确定子网向主机位要借的位数

根据给出的C类IP地址192.168.10.0和掩码255.255.255.0，其对应的二进制形式如图5-3-1所示。

	网络号			主机号
C类IP地址：192.168.10.0	11000000	10101000	00001010	0 0 0 0 0 0 0 0
子网掩码：255.255.255.0	11111111	11111111	11111111	0 0 0 0 0 0 0 0

图5-3-1 IP地址和掩码的二进制表示

由于条件是要划分四个子网，根据公式：子网数量＝$2^x-2=4$，即 x＝3。

也就是说，要在主机 ID 的 8 位 bit 中借 3 位 bit（即，子网掩码中“1”的个数是 3）用于子网 ID，如图 5-3-2 所示。

	网络ID			子网号	主机ID
C类IP地址：192.168.10.0	1100000	1010100	0000101	0 0 0	0 0 0 0
子网掩码：255.255.255.0	11111111	11111111	1111111	1 1 1	0 0 0 0

图 5-3-2　在主机 ID 的 8 位 bit 中借 3 位 bit 用于划分子网

5.3.3　确定子网掩码

确定了子网位数是 3 位后，即主机位数也就确定为 8－3＝5 位。

这样，借位后的新子网掩码也就确定了：255.255.255.224，如图 5-3-3 所示。

	网络ID			子网号	主机ID
C类IP地址：192.168.10.0	1100000	1010100	0000101	0 0 0	0 0 0 0
子网掩码：255.255.255.0	11111111	11111111	1111111	1 1 1	0 0 0 0
借位后子网掩码：255.255.255.224	11111111	11111111	11111111	1 1 1	0 0 0 0

图 5-3-3　确定借位后的子网掩码

5.3.4　确定各子网有效的网络地址

各有效子网网络地址是以掩码块大小做增量计算。其中，掩码块大小＝256－十进制的子网掩码。

由于新的子网掩码是 255.255.255.224，因此掩码块大小＝256－224＝32，由此确定出各子网的网络地址：

第一个子网的网络地址：192.168.10.32

第二个子网的网络地址：192.168.10.64

第三个子网的网络地址：192.168.10.96

第四个子网的网络地址：192.168.10.128

5.3.5　确定每个子网的广播地址

公式：广播地址＝下个子网网络地址－1

确定各子网的广播地址如表 5-3-1 所示。

表 5-3-1　　各子网的广播地址

序号	各子网网络地址	各子网广播地址
1	192.168.10.32	192.168.10.63
2	192.168.10.64	192.168.10.95
3	192.168.10.96	192.168.10.127
4	192.168.10.128	192.168.10.159

5.3.6　确定各个子网的有效主机范围

公式：有效主机范围＝各子网的网网络地址＋1～各子网的广播地址号－1

确定出各个子网的有效主机范围，以及网络 ID、广播地址如表 5-3-2 所示。

表 5-3-2　　各个子网的有效主机范围、网络 ID、广播地址

序号	各子网网络地址	各子网广播地址	各子网有效主机地址范围
1	192.168.10.32	192.168.10.63	192.168.10.33～192.168.10.62
2	192.168.10.64	192.168.10.95	192.168.10.65～192.168.10.94
3	192.168.10.96	192.168.10.127	192.168.10.97～192.168.10.126
4	192.168.10.128	192.168.10.159	192.168.10.129～192.168.10.158
5	192.168.10.160	192.168.10.191	192.168.10.161～192.168.10.190
6	192.168.10.192	192.168.10.223	192.168.10.193～192.168.10.222

说明：表中第 5、6 条记录仅供参考。

5.4　任务案例 2——登录可网管交换机

【任务描述】通过交换机的 Console 口配置及管理交换机，目的是熟悉可网管交换机的连接与管理。

【任务要求】以 H3C 交换机为例，用交换机的 Console 口登录交换机管理界面。

【任务分析】对于可网管交换机，第一次使用时，一般要通过交换机的 Console 口进行配置与管理交换机。

5.4.1　连接与管理交换机

通过前面学习可知，交换机可分为可网管交换机和不可网管交换机，可网管交换机主要用于中小型局域网中。

可网管交换机一般是通过交换机的 Console 口连接和管理，首先运行“超级终端”程序和管理计算机建立连接，连接成功后即登录到交换机的管理界面。再根据不同交换机产品（如 H3C、思科、锐捷等）的命令系列，对交换机进行设置及管理。

将 Console 线的 RJ-45 接头端连接交换机上的 Console 口；将 Console 线另一端的串行口连接管理计算机的串行口。

5.4.2　运行“超级终端”建立和交换机的连接

“超级终端”程序用于管理计算机和交换机建立连接。

1. 运行“超级终端”程序

如图 5-4-1 所示，单击“开始→程序→附件→通讯”，鼠标左键单击“超级终端”选项，运行“超级终端”程序。

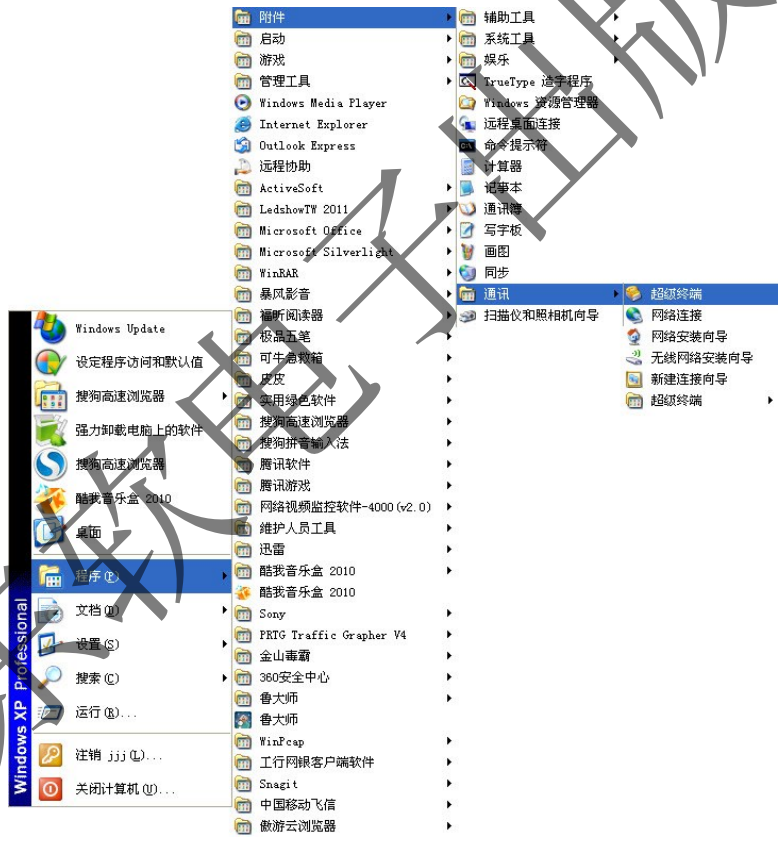

图 5-4-1　运行“超级终端”程序

2. 设置“超级终端”程序

(1)为新建连接命名。

打开“超级终端”，界面如图 5-4-2 所示。在“超级终端”的“连接描述”窗口中，为新建的管理计算机与交换机连接输入名称（可任意设置），在本例中输入“lianxi”。

图 5-4-2　为新连接命名

（2）设置“国家、区号”等参数。

如图 5-4-3 所示，在“连接到”窗口中，“连接时使用”选项中选择“COM1”（本例交换机和管理计算机连接的串行口是“COM1”口，如果是连接在 COM2 口上，则要选择“COM2”），其他“国家、区号、电话号码”等参数按默认选择即可。

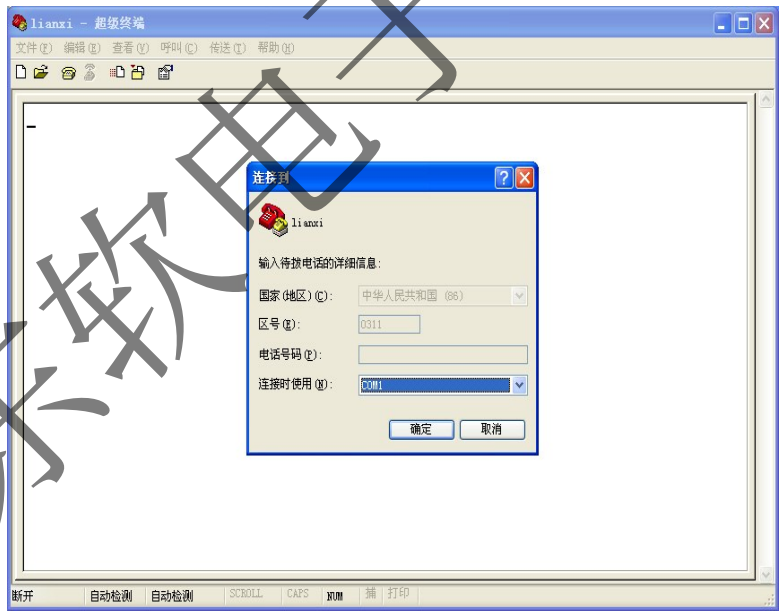

图 5-4-3　设置“连接到”各项参数

（3）设置“COM1”属性。

如图 5-4-4 所示，在“COM1 属性”设置窗口中，用鼠标左键单击“还原为默认值”按钮，将初始参数更改为默认值。

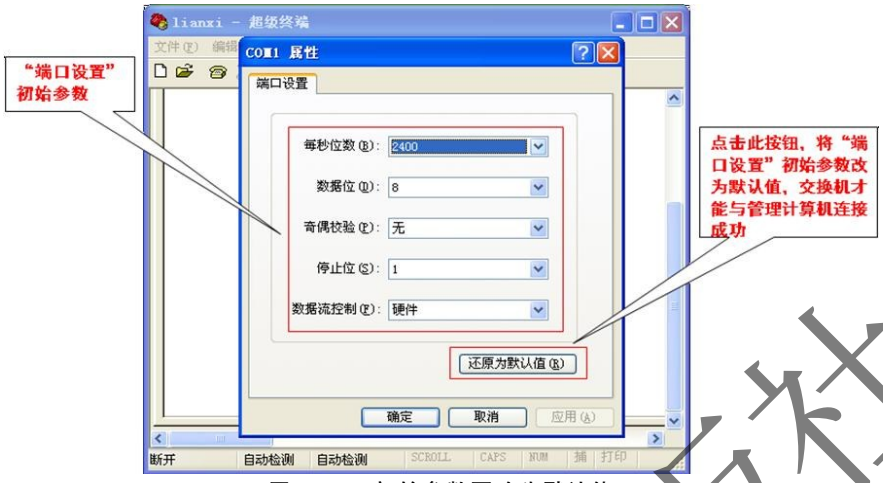

图 5-4-4　初始参数更改为默认值

如图 5-4-5 所示为“COM1 属性”窗口中初始参数更改为默认值后的状态。

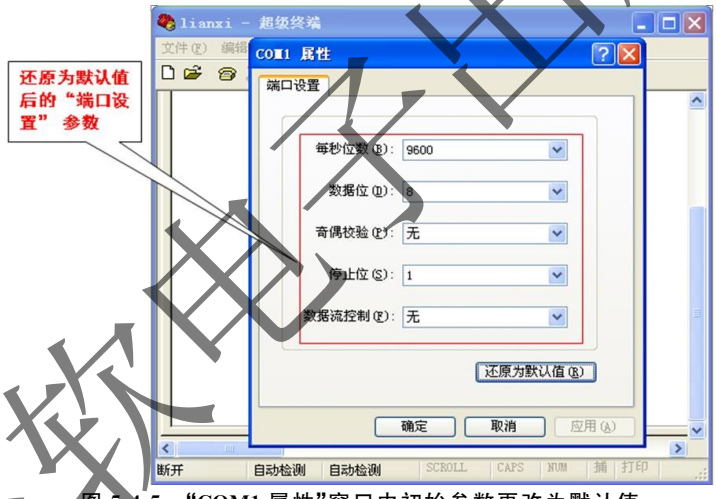

图 5-4-5　“COM1 属性”窗口中初始参数更改为默认值

5.4.3　登录交换机管理界面

完成以上步骤后，在“超级终端”窗口按“回车”键即可进入交换机管理窗口，如图 5-4-6 所示。

进入交换机管理界面后，即可按不同设备的命令进行交换机的设置及管理。

说明：不同设备的交换机管理界面与使用的配置命令是不同的，但以上步骤相同。

图 5-4-6　进入交换机管理窗口

5.5　任务案例 3——单交换机划分 VLAN

【任务描述】创建两个不同的 VLAN，使同一个网段原本连通的两台计算机在加入到不同的 VLAN 后，再测试，变为不通。通过该任务要求了解创建 VLAN 过程，深刻理解 VLAN 的基本概念及作用。

【任务要求】以 H3C 交换机为例：

(1)将一台交换机与两台计算机连接；

(2)将两台计算机设置为一个网段，用 ping 命令测试连通性；

(3)创建两个 VLAN，VLAN10 和 VLAN20，将测试连通的计算机分别加入到不同的 VLAN 中；

(4)再测试不同 VLAN 中的计算机，是否连通。

【任务分析】本任务的精髓是要体验和理解一台交换机、相同网段，但不同的 VLAN，彼此之间互不相通，这就是 VLAN 的意义。即 VLAN 是将一个物理网络分隔成逻辑上不同的网络，因此，IP 地址处在一个网段的两台计算机本应该是相通的，但经过划分了不同的 VLAN 后变得不相通了。

5.5.1　创建 VLAN 之前测试

在创建 VLAN 之前，首先要保证相连的计算机是互通的。

(1)在创建 VLAN 之前，要确保进行连接的两台计算机的 IP 设在一个网段，如设置主机 1 的 IP 地址是：192.168.1.11，设置主机 2 的 IP 地址是 192.168.1.16，计算机 IP 地址设置可参考以前章节相关内容。

(2)用一台交换机连接这两台计算机。将主机 1 通过网线连接到交换机的端口 1，将主机 2 通过网线连接到交换机的端口 9。在没有设置任何 VLAN 情况下，交换机的所有端口都属于默认 VLAN 1，且主机 1 与主机 2 属于同一网段。

(3)使用 ping 命令验证主机 1 和主机 2 的连通性。默认情况下交换机所有端口都属于默

认 VLAN 1，即主机 1 连接的端口 1 与主机 2 连接的端口 9 同属于 VLAN1，且主机 1 与主机 2 属于同一网段，所以主机 1 和主机 2 可互通，如图 5-5-1 所示。

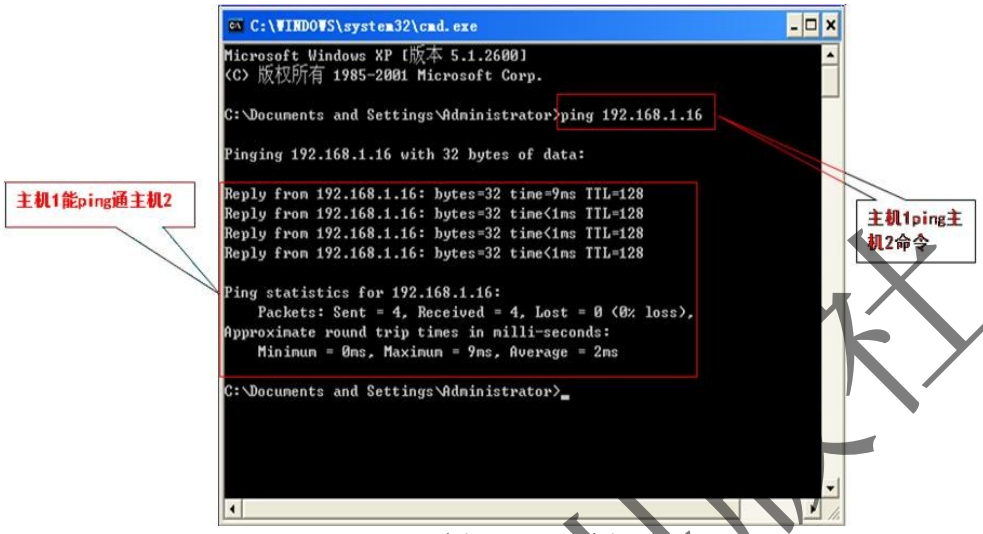

图 5-5-1　主机 1 ping 通主机 2

5.5.2　用 Console 口和交换机建立连接

按 5.4 节介绍的内容，使用 Console 线将交换机的 Console 口和管理计算机的 COM1 口建立连接。运行“超级终端”程序进入交换机“系统模式”。

5.5.3　查看交换机当前状态

通过“超级终端”进入交换机管理界面时，首先进入的是交换机默认视图的“用户视图”（<H3C>为提示符）；输入“system-view”命令进入“系统视图”（提示符由<H3C>变为[H3C]）。

命令如下：

（1）<H3C> system-view（在“用户视图”下进入“系统视图”），如图 5-5-2 所示。

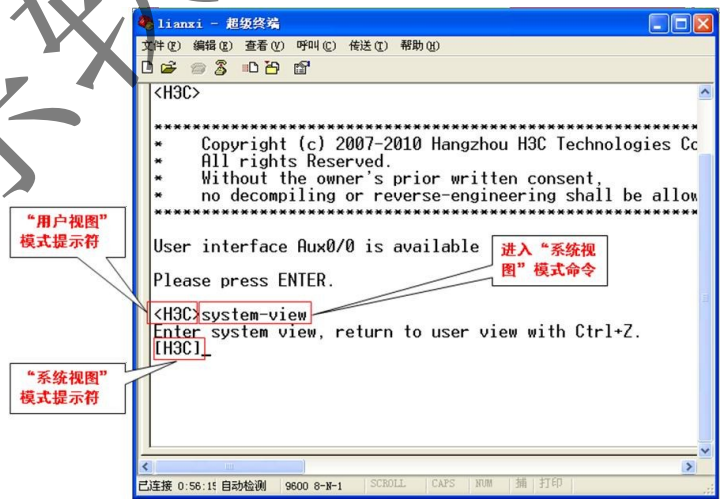

图 5-5-2　进入“系统视图”模式

(2)在“系统视图”查看交换机当前 VLAN 状态([H3C] display vlan),如图 5-5-3 所示。查看结果是当前交换机 VLAN 只有默认的 VLAN1。

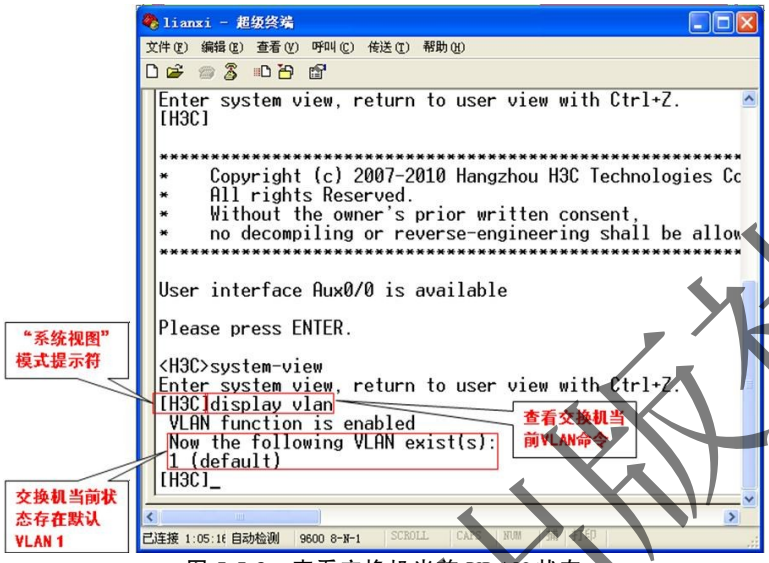

图 5-5-3 查看交换机当前 VLAN 状态

5.5.4 创建不同 VLAN

本例中,要创建两个 VLAN:VLAN10 和 VLAN20。

为了便于比较,要保证创建 VLAN 之前测试的两台计算机的连接端口和 IP 地址等所有条件不变。连接示意图如图 5-5-4 所示。

说明:本任务是以两台计算机为例,实际上,一台计算机就代表了 VLAN 内的多台计算机。

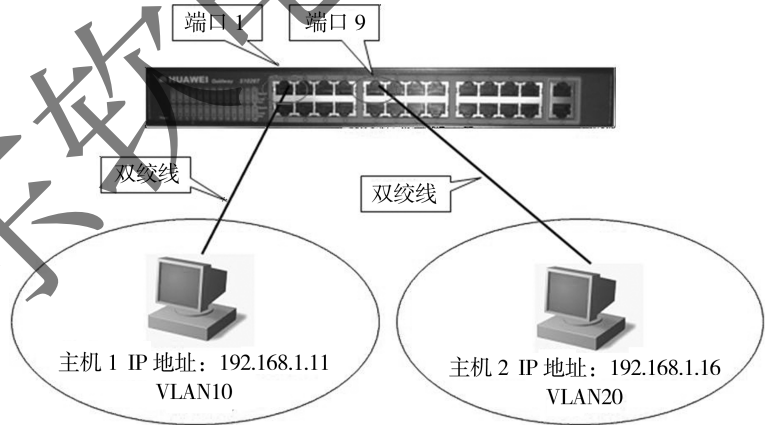

图 5-5-4 一台交换机上连接两台主机

1. 新建 VLAN10

在交换机“系统视图”模式下,使用“VLAN10”命令建立 VLAN10,如图 5-5-5 所示。建立 VLAN10 后,自动进入“VLAN10 视图”模式。

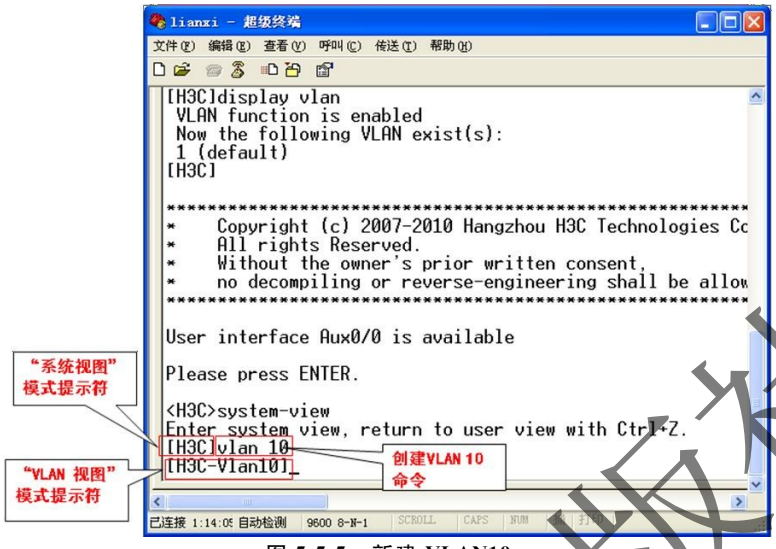

图 5-5-5　新建 VLAN10

2. 将交换机端口划入对应 VLAN10

如图 5-5-6 所示，在“VLAN 视图”模式下使用“port 端口”命令将交换机的 1 端口划入到 VLAN10 中。

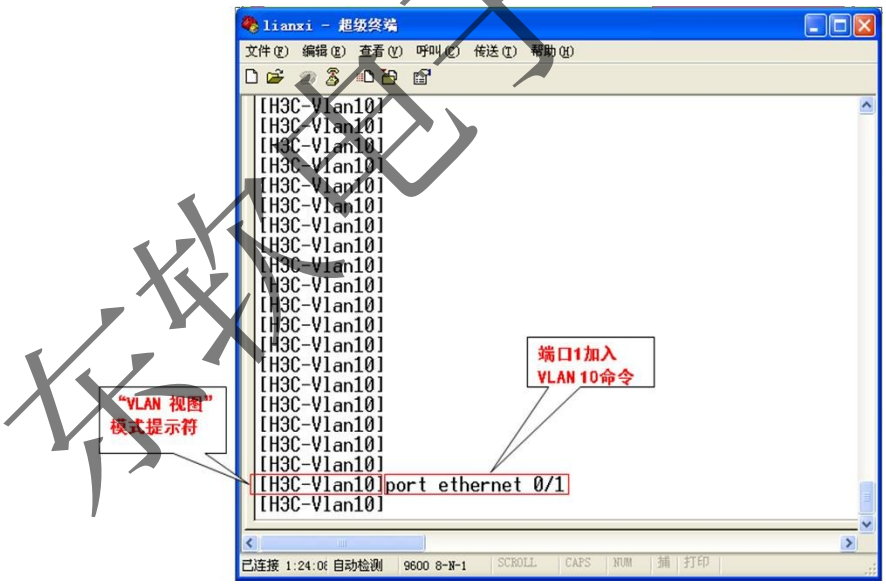

图 5-5-6　交换机端口划入对应 VLAN10

3. 查看命令后结果

如图 5-5-7 所示，查看当前交换机状态。

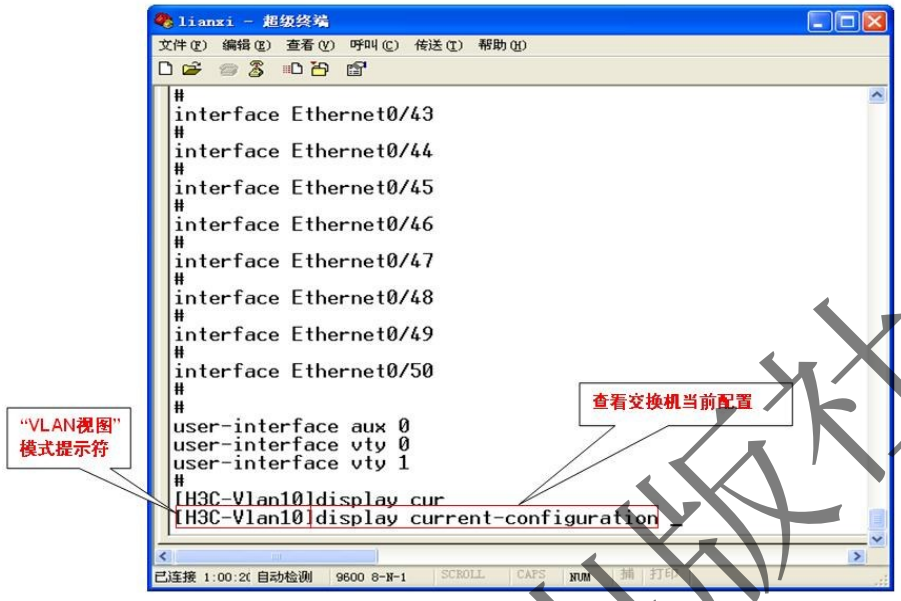

图 5-5-7 划分 VLAN 后查看交换机当前配置

如图 5-5-8 所示，显示端口 1 已加入到 VLAN10 中。

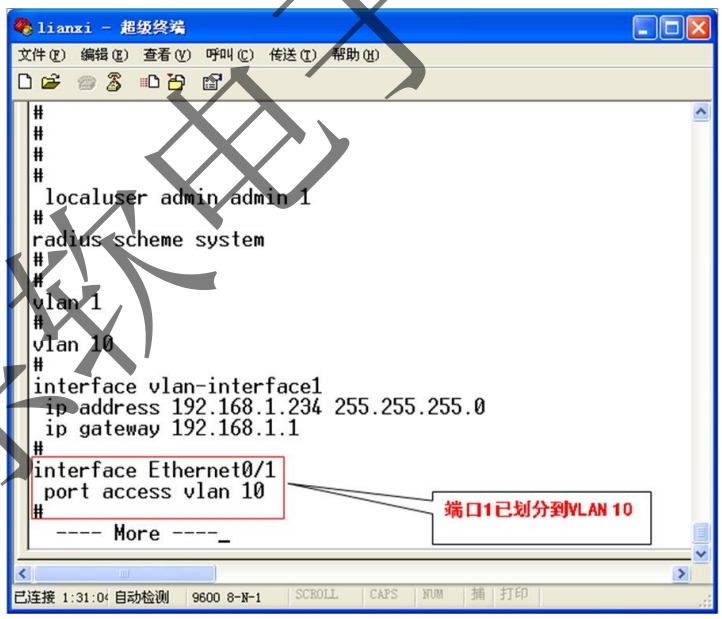

图 5-5-8 端口 1 已加入到 VLAN10 中

4. 查看划分好的 VLAN

在交换机“系统视图”模式下，使用命令“display vlan”，查看交换机当前存在的 VLAN，看是否设置有效。如图 5-5-9 所示，交换机有两个 VLAN：VLAN10 和 VLAN1。

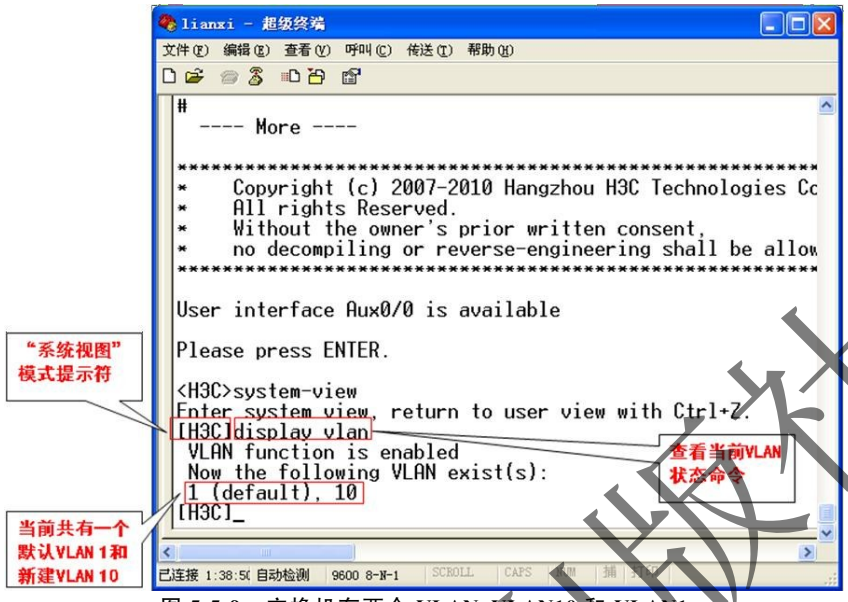

图 5-5-9　交换机有两个 VLAN：VLAN10 和 VLAN1

5. 新建 VLAN20

新建 VLAN20 与新建 VLAN10 所用命令与操作类似，具体命令如表 5-5-1 所示。

表 5-5-1　　创建 VLAN20 命令与步骤

步骤	命令	命令当前视图	说明
1	vlan20	系统视图	创建 VLAN20
2	portEthernet 0/9	VLAN 视图	将端口号 9 加入当前 VLAN20 中
3	Display current-configuration	系统视图	查看交换机当前配置

5.5.5　验证不同 VLAN 中的主机不能进行通信

到目前为止，计算机的 IP 地址没有变，仍为同一网段；端口物理位置也没有变；仅仅是在交换机上做了以下设置：

(1)新建了 VLAN10 和 VLAN20；

(2)将端口 1 加入到 VLAN10；端口 9 加入到 VLAN20。

此时，主机 1 处于 VLAN10，主机 2 处于 VLAN20，这两台主机处于不同的 VLAN 之中。即通过划分 VLAN，使这两台主机变成处于不同的逻辑网络之中，所以它们之间也就不能进行通信，也就是主机 1 无法 ping 通主机 2，如图 5-5-10 所示。

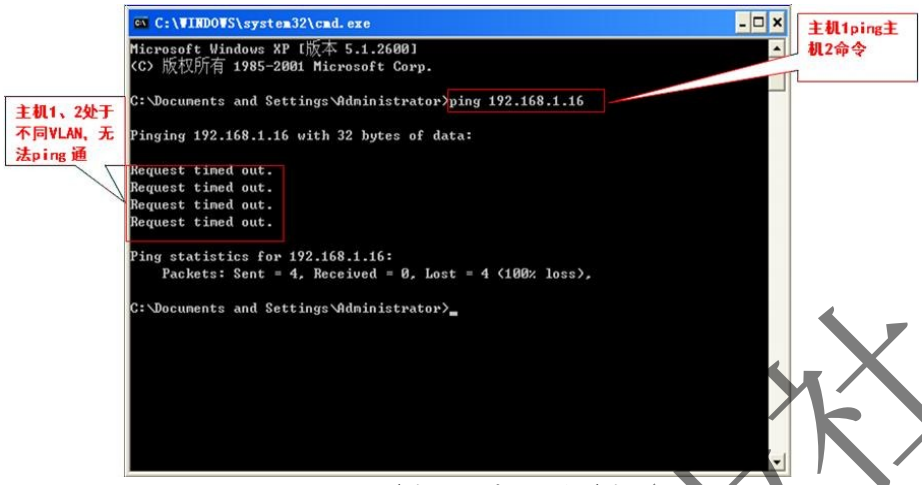

图 5-5-10　主机 1 无法 ping 通主机 2

5.6　知识拓展：ARP(地址解析协议)基本知识

在局域网中，通过 ARP 协议完成将 IP 地址转换为第二层物理地址(即 MAC 地址)。ARP 协议对网络安全也具有重要的意义。

5.6.1　什么是 ARP

ARP(Address Resolution Protocol)即地址解析协议，是一个位于 TCP/IP 协议栈中的低层协议，负责将某个 IP 地址解析成对应的 MAC 地址。

ARP 协议是指主机在发送帧前(前面已经学习过，帧是在数据链路层的传输数据单元)将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的。

说明：在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。

5.6.2　ARP 表及维护过程

每台计算机都在各自的高速缓存区(cache)中存放一张 IP 地址到 MAC 地址的转换表，该表称为 ARP 表。计算机初始启动时，主机的 ARP 表均为空。

如图 5-6-1 所示为 ARP 表建立及维护的主要过程。

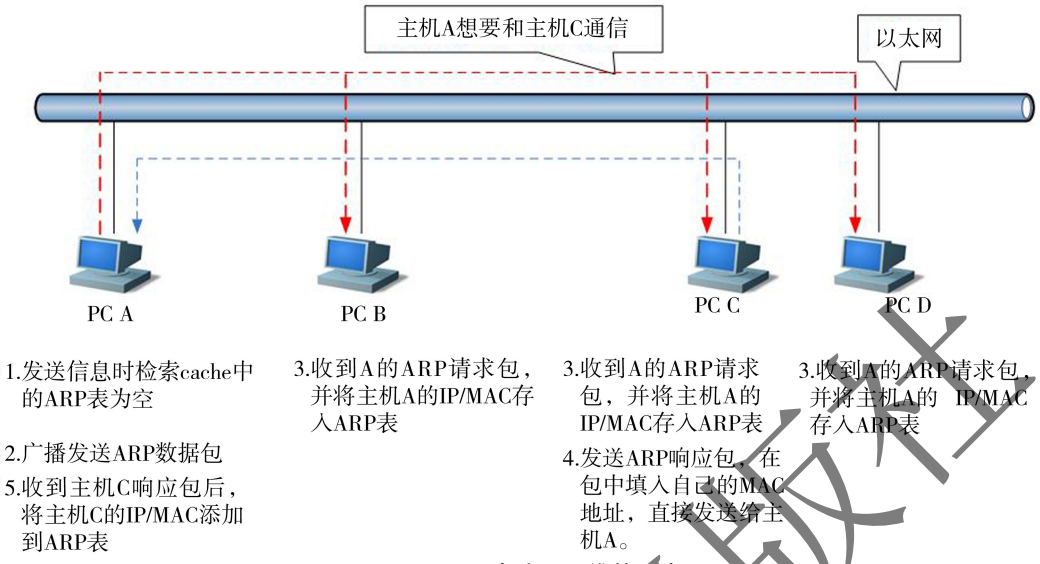

图 5-6-1　ARP 表建立及维护示意图

(1)如果主机 A 要和主机 C 通信,首先检索自己(主机 A)cache 中的 ARP 表,看其中是否有与主机 C 对应的 ARP 表项。

(2)如果找到,则直接利用该 ARP 表项中的 MAC 值把 IP 数据包封装成帧,发送给主机 C;如果在 ARP 表中找不到对应的地址项,则创建一个 ARP 请求数据包,并以广播的方式发送(把以太帧的目的地址设置为 FF-FF-FF-FF-FF-FF)。ARP 请求数据包中有需要查询的主机 C 的 IP 地址,以及主机 A 自己的 IP 地址和 MAC 地址。

(3)包括主机 C 在内的所有主机都收到 A 的 ARP 请求包,然后将主机 A 的 IP 地址与 MAC 地址的映射关系存入各自的 ARP 表中。

(4)主机 C 创建一个 ARP 响应包,在包中填入自己的 MAC 地址,直接发送给主机 A。

(5)主机 A 收到响应后,从包中提取出所需查询的 IP 地址及其对应的 MAC 地址,添加到自己的 ARP 表中。并根据该 MAC 地址所需要发送的数据包封装成帧发送出去。

说明:ARP 表的内容是定期更新的,如果一条 ARP 表项很久没有使用了,则它将被从 ARP 表中删除。

5.6.3　ARP(地址解析协议)工作过程

在同一个局域网的子网中,主机之间互相传送信息时,需要的地址是 MAC 地址,而不是 IP 地址。主机每次发送数据时,都要将 IP 地址转换成 MAC 地址。由于每个主机的网卡都有唯一的 MAC 地址,所以数据可以准确发送到目的地址。

例如,如图 5-6-2 所示,假设在一个以太网上的四台计算机,分别是计算机 PCA、PCB、PCC、PCD,通过 TCP/IP 协议进行通信,那么双方的数据链路层必须知道对方的 MAC 地址。

(1)当主机 A 要与 IP 地址为 192.168.4.4 的主机 C 通信时(如主机 A ping 主机 C),主机 A 会先检查自己缓存内的 ARP 表中是否有主机 C 的 MAC 地址。如果没有,主机 A 会发送一

个 ARP 请求广播包，此广播包内包含着目标主机的 IP 地址，也就是主机 C 的 IP 地址。

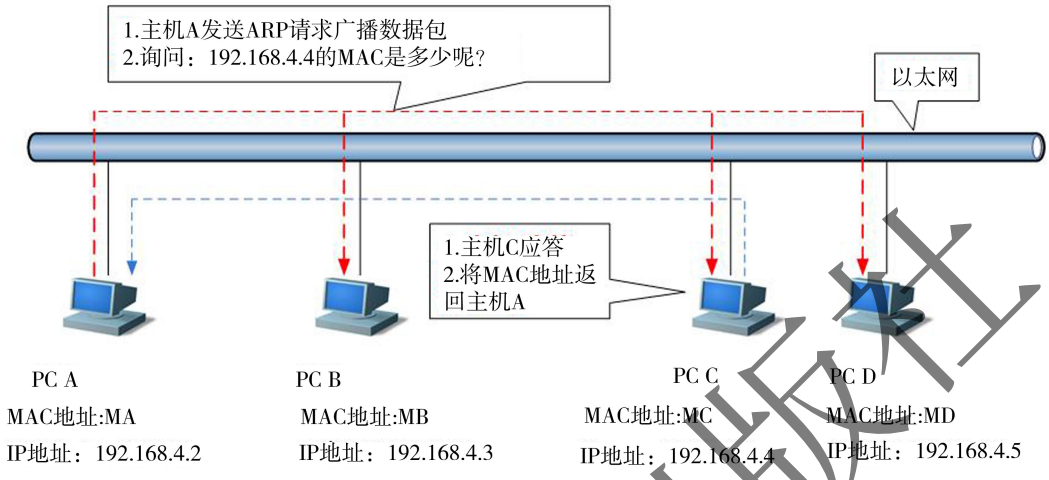

图 5-6-2　ARP(地址解析协议)工作过程示意图

(2)当主机 C 收到此广播后，会将自己的 MAC 地址利用 ARP 协议响应包返回给主机 A，并更新自己的 ARP 缓存，也就是同时将主机 A 的 IP 地址/MAC 地址映射保存起来，以供后面使用。

(3)主机 A 在得到主机 C 的 MAC 地址后，就可以与主机 C 通信了，即把 IP 数据包封装成帧，发送给主机 C。同时，主机 A 也将主机 C 的 IP 地址/MAC 地址映射保存在自己的 ARP 表内。

【本章小结】

本章重点详细介绍了 IP 地址、子网掩码及子网划分的相关基本概念及子网划分方法；介绍了可网管的交换机如何连接及进入交换机管理系统。简要介绍了 VLAN 的相关基本概念、单交换机的 VLAN 划分方法，为将来交换机进一步的专业学习奠定了基础。

在“知识拓展”中，主要介绍了 ARP(地址解析协议)的基本知识，进一步理解 MAC 地址与 IP 地址及关系。

本章通过三个案例，分别详细介绍了如何根据要求划分多个子网；如何通过交换机的 Console 口，使用“超级终端”进行配置交换机；如何利用单交换机实现基于端口的 VLAN 划分，充分体验和理解 VLAN 的基本概念及功能。

本章小结图如图 5-7-1 所示。

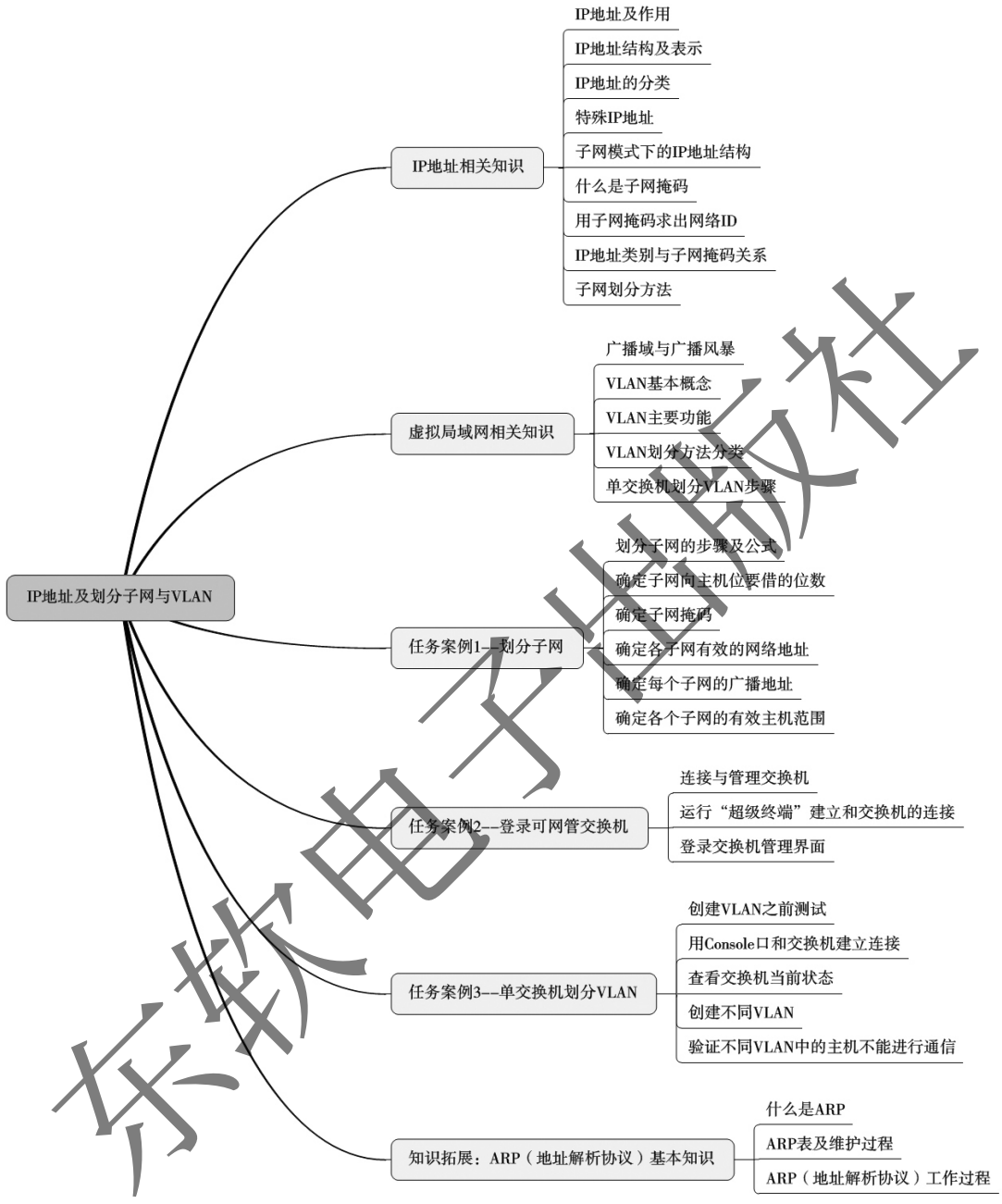

图 5-7-1　本章内容结构

【思考与练习】

1. IP 地址的构成、表示与分类分别是什么？IP 地址的作用是什么？

2. 什么是子网？什么是子网掩码？子网掩码的作用是什么？

3. IP 地址分为哪几类？它们各自适用于什么情况？

4. IP 地址有哪几种特殊地址？各自的含义是什么？

5. 什么是网络 ID？什么是主机 ID？什么是网络地址？什么是广播地址？

6. IP 地址类别与子网掩码的关系是什么？

7. 什么是冲突域？什么是广播域？两者有什么区别？

8. 什么是广播风暴？引起广播风暴的因素有哪些？如何降低广播风暴带来的影响？

9. 什么是 VLAN？VLAN 主要功能是什么？

【单元测试】

一、填空

1. IP 地址的结构包含(　　)和(　　)。

2. IP 地址分为(　　)、(　　)、(　　)、(　　)和(　　)五类。

3. 连接在交换机上的计算机都同处一个(　　)，但不属于同一(　　)，交换机的每个端口就是一个(　　)。

4. 相同 VLAN 的主机可以(　　)，不同 VLAN 的主机不能(　　)。

5. VLAN 和物理网络(　　)。

6. IP 地址 219.25.23.56 的默认子网掩码有(　　)位。

7. IP 地址为 211.116.18.10，掩码为 255.255.255.252，其广播地址为(　　)。

二、选择题

1. 192.168.5.255 代表的是(　　)

A. 主机地址　　B. 网络地址

C. 广播地址　　D. 组播地址

2. C 类网段 192.168.1.0 最有可能的主机地址是(　　)。(提示：去掉特殊 IP 地址)

A. 254　　B. 256

C. 1024　　D. 16

3. 对于 IP 地址为 202.93.120.6 的主机来说，其网络 ID 为(　　)。

A. 202.93.120　　B. 202.93.120.6

C. 202.93.120.0　　D. 6

4. 下面有效的 IP 地址是(　　)。

A. 202.280.120　　B. 192.256.120.6

C. 192.93.120.0　　D. 285.93.120.0

5. 默认情况下，交换机上所有端口属于 VLAN(　　)。

A. 0　　B. 1

C. 1024　　D. 8081

6. 下面两台主机位于同一个网络中的是(　　)。

A. IP 地址:192.168.1.160,子网掩码:255.255.255.224 的主机

B. IP 地址:192.168.1.240,子网掩码:255.255.255.224 的主机

C. IP 地址:192.168.1.154,子网掩码:255.255.255.224 的主机

D. IP 地址:192.168.1.190,子网掩码:255.255.255.224 的主机

二、简述题

1. 子网掩码与 IP 地址的关系是什么?

2. 子网划分的主要步骤是什么?

3. 单交换机划分 VLAN 的一般步骤是什么?

三、练习题

有一个 C 类地址网段:192.168.5.0,子网掩码:255.255.255.0,要求划分为 16 个子网:给出每个子网的网络地址、广播地址和各子网的有效主机地址范围。