Vlan 原理及典型应用

1．VLAN 的概念

VLAN（Virtual Local Area Network）是虚拟局域网的英文缩写，它将连接在同一个物理网络中的主机进行分组，使这些主机看起来就象连接在不同的网络中一样。

在 VLAN 的概念最早出现时，各个厂商纷纷推出自己的解决方案，互不兼容，各个厂商的交换机互相不能识别其他交换机的 VLAN。IEEE 802.1Q 是新的虚拟局域网标准，它统一了各个厂商的 VLAN 实现方案，使不同厂商的设备可以同时在一个网络中使用，各自的 VLAN 设置可以被其他设备所识别，符合 IEEE802.1Q 标准的交换机可以和其他交换机互通。

VLAN 可分为：基于端口的 VLAN、基于 MAC 地址的 VLAN、基于 IP 地址的 VLAN、基于 IP 子网的 VLAN、基于协议的 VLAN 和用户自定义的 VLAN。其中最常用的也是最基本的是基于端口的 VLAN，它按照接收端口来确定一个数据包的 VLAN 属性。

VLAN 的属性是指：当一个交换机端口接收到一个数据包时，确定这个数据包属于哪个 VLAN。

2．VLAN 的主要功能

2.1 VLAN 的主要作用是隔离广播域

将一个物理网络划分成多个逻辑上的 VLAN，可以将一个广播域划分成多个小的广播域，每个 VLAN 对应一个小的广播域，一个 VLAN 中的广播不能传播到其他的 VLAN，这样有效地控制广播风暴的发生。

通过 VLAN 可以非常灵活地将一个物理网络按照需求划分成多个逻辑子网。例如某公司由于各部门的业务不同以及安全的需求，可以按照市场部、工程部、财务部将公司的网络划分成三个不同的 VLAN，各部门不能直接访问。在这个网络中，一个部门网络的成员可以在不同的楼层，可以与不同的交换机端口相连，组网方式非常灵活。通过把公司网络划分成三个 VLAN，广播报文只限制在一个 VLAN 内传播，大大提高了网络的使用效率。

2.2 简化端站的移动、增加与更换

当一台终端站被移动到新的物理位置，它的属性可以从一台管理工作站上通过简单网络管理协议（SNMP）或用户接口菜单重新分配。若端站在同一 VLAN 中移动，在新的位置它将保持原有的属性。若端站移动到不同的 VLAN，那它将被赋予新的 VLAN 的属性。

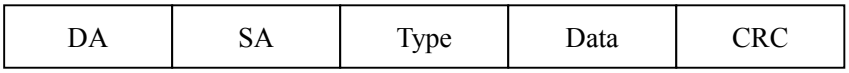
2.3 网络安全

把一个物理网络划分成若干个 VLANs，每个 VLAN 中的广播只能在本 VLAN 所属的交换机端口传播，提高整个网络的安全性。

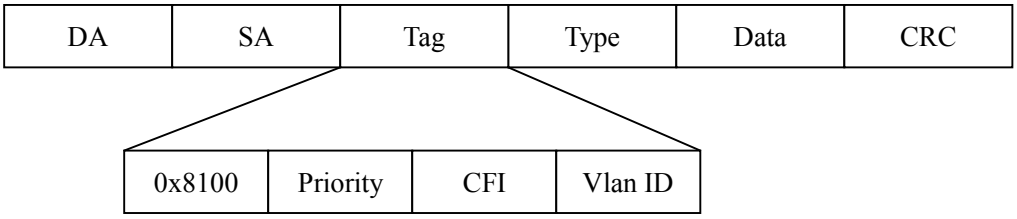
3．VLAN 的实现

3.1 IEEE802.1Q 标准帧格式

为了实现 VLAN，IEEE 802.1Q 标准定义了一种新的帧格式。它在标准的以太网帧的源 MAC 地址后面加入了一个 Tag header（4 字节），此格式用下图表示：



标准以太网帧格式



IEEE 802.1Q 标准帧格式

其中：
DA — 目的 MAC 地址；
SA — 源 MAC 地址；
Data — 帧中所携带的用户数据；
CRC — 循环冗余校验；
Priority — 用户优先级；
Vlan ID — 用来标识一个 VLAN 的 ID 号（取值范围为 1～4094）。加入 Tag 的目的是为了携带 VLAN 信息，表明这个数据帧属于哪个 VLAN，以确定数据帧的属性。

3.2 VLAN 中端口成员的确定

对于基于端口的 VLAN，属于这个 VLAN 的端口都被网络管理软件明确配置为这个 VLAN 的成员。

3.3 确定数据包的 VLAN 属性

对于带有 802.1Q Tag 的数据包，则直接根据数据包中所带标记确定其 VLAN 属性。对于未带有 Tag 的数据包，则交换机根据数据包内容和各 VLAN 具体规则确定其所属 VLAN。

3.4 VLAN 成员端口属性

VLAN 成员端口分为带标记(tagged)与不带标记(untagged)，可以通过网管来设置端口为带标记端口。一般当端口连接的设备支持 802.1Q 标准时将端口设置为带标记端口，当端口连接的设备不支持 802.1Q 时，设置端口为不带标记端口。

3.4.1 带标记端口

带标记端口即从该端口发出的所有数据包都必须带有该数据包所属 VLAN 标记。可设置该端口在接收数据包时是否丢弃不带标记的数据包或按各 VLAN 具体规则确定其所属 VLAN。

3.4.2 不带标记端口

不带标记端口即从该端口发出的所有数据包都不能带有该数据包所属 VLAN 标记。可设置该端口在接收数据包时是否丢弃带标记的数据包或按标记确定其 VLAN 属性。

3.5 端口的缺省 VLAN

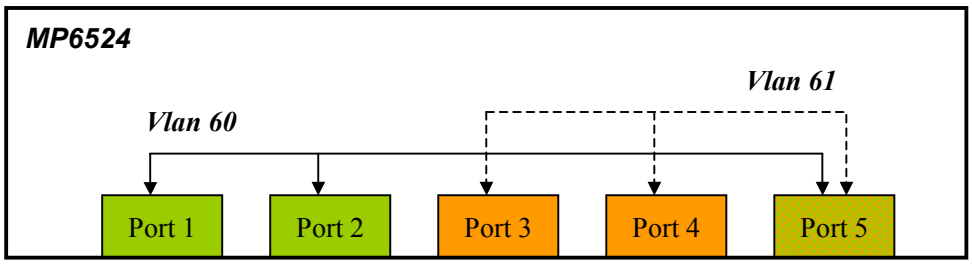
每个端口均可设置一个缺省 VLAN（PVid）。当交换机收到一个 Untagged 帧时，该帧就被指定为接收端口的缺省 VLAN。

4. Vlan 路由

在交换机中引入了 VLAN 的概念，通过在网络中划分 VLAN 可以实现广播域的隔离，大大提高了网络的性能；但是，却限制了一个 VLAN 中的用户访问其他 VLAN 中的用户。由于 VLAN 是第二层的技术，它在选路时使用的是以太网的 MAC 地址，所以没有办法实现 VLAN 之间的互访问。为解决这个问题，借鉴路由器的功能，引入 VLAN 间路由（三层交换机）功能。

路由交换机完成线速第三层交换采用的是一种“一次路由，多次交换”的思想。“一次路由”是指当第一次对此报文进行选路时，交给 CPU 中运行的路由协议（如：OSPF，RIP）来运算并给出路由信息，然后将此路由信息存储在交换芯片的 CACHE 表中，当发往该目的 IP 地址的报文再次进行路由时，由于 CACHE 表中已经有了该目的 IP 地址，因此数据包可以直接由硬件按照 CACHE 中该目的 IP 路由进行交换，以达到线速交换。

5. VLAN 设置举例



Vlan 60 包括：Port 1(Untagged) Port 2(tagged) Port 5(tagged)
Vlan 61 包括：Port 3(Untagged) Port 4(tagged) Port 5(tagged)

Port	1	2	3	4	5
缺省 Vlan	60	60	61	61	60

如果 Port 5 收到一个不带有 802.1Q Tag 的帧，因为在帧中没有指明该帧所属 Vlan，所以该帧被指定为 Port 5 的缺省 Vlan（Vlan 60）。依据交换机学习到的地址信息，该帧将可能被发送到相应的端口，或者因为交换机根据现存信息不能确定将向哪个和哪些端口转发而将该帧广播，但是此时的广播并不是向所有端口广播，而是由该帧所属 VLAN 决定，即向 Port 1、2 转发该帧。但 Port 1、2 转发的情况有所不同。

（1）Port 1 是 Untagged 端口，因此在发送时该帧将不会带 802.1Q Tag。

（2）Port 2 是 tagged 端口，因此在发送时交换机将会给该帧加上 802.1Q Tag，指明该帧所属 Vlan 为 60。

如果端口 5 收到一个带有有效 802.1Q Tag 的帧，则交换机可以直接从帧中读出该帧的 VLAN 属性。在这样的条件下，端口的缺省 VLAN 在确定帧的 VLAN 时不再起作用。假设 Tag 指明该帧所属 Vlan 为 61。依据交换机学习到的地址信息，该帧将可能被发送到相应的端口，或者因为交换机根据现存信息不能确定将向哪个和哪些端口转发而将该帧广播，但是此时的广播并不是向所有端口广播，而是由该帧所属 VLAN 决定，即向端口 3、4 转发该帧。但端口 3、4 转发的情况有所不同。

（1）Port 3 是 Untagged 端口，因此在发送时该帧将不会带 802.1Q Tag。

（2）Port 4 是 tagged 端口，因此在发送时交换机将会给该帧加上 802.1Q Tag，指明该帧所属 Vlan 为 61。

6. VLAN 典型应用

在实际应用中，通常有这样几种情况：

（1）端口所连接的是一台普通的计算机。

通常将这种端口划分在某一个 VLAN，我们需要做如下设置：

确定该端口设置为 Untagged 端口且缺省 VLAN 为这台计算机所在的 VLAN。

确定该 VLAN 的成员中包含这个端口。

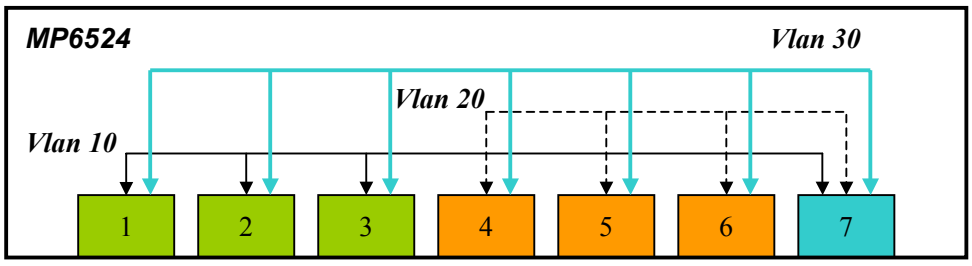
（2）端口所连接的是共享的网络设备，如服务器、打印机、路由器等。

这些设备通常有一些特殊要求，它们要能够被许多其他 VLAN 的计算机访问。配置这些端口所需的操作要复杂一些：

确定端口所在 VLAN 的成员中包含所有它要与之互通的端口。

确定所有的与它有互通需求的 VLAN 的成员中包含这个端口。

举例：计算机分为两组，两组之间互相不需要通信，但两组共享一台服务器。



Vlan ID	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7
10	Untagged	Untagged	Untagged	—	—	—	Untagged
20	—	—	—	Untagged	Untagged	Untagged	Untagged
30	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged
PVid	10	10	10	20	20	20	30

其中，PVid 表示端口默认 VLAN ID。

当连接在 Port 2 的计算机要访问服务器的时候，计算机传送给服务器的数据通过 Port 2 被交换机接收。数据帧中不包含 802.1Q Tag，因此交换机把数据帧标记为 VLAN 10。VLAN 10 的成员中包含了 Port 7，所以该数据帧可以被发送到 Port 7 并被服务器所接收。当服务器有回送的数据时，发出的数据通过 Port 7 进入交换机。同样因为数据帧不包含 802.1Q Tag，交换机将帧标记为 VLAN 30。VLAN 30 的成员端口中包含了 VLAN 10 的所有端口，所以 Port 2 的计算机能够收到来自服务器的数据。

而当连接在 Port 2 的计算机要发送数据给连接在 Port 4 的计算机时，数据通过 Port 2 被交换机接收。数据帧中不包含 802.1Q Tag，因此交换机把数据帧标记为 VLAN 10。VLAN 10 中不包含 Port 4，所以该数据帧不会被发送到 Port 4。由此可知，VLAN 10 中的 Port 1、2、3 不会与 VLAN 20 中的 Port 4、5、6 通信，但 VLAN 10 和 VLAN 20 中的端口均可分别与 VLAN 30 中的端口互相通信。

（3）端口连接的是支持 802.1Q 的交换机

当多个 VLAN 跨越几个交换机时，在这样的连接上通常会支持多个 VLAN 的互通。
这类端口包含在所有的要通过该端口互通的 VLAN 的成员中。
端口的缺省 VLAN 的 VLAN ID 与对面交换机端口的相同。
端口设置为 Tagged 端口。

说明

如果端口连接的也是交换机但不能支持 802.1Q VLAN，或者就是一台 HUB，这种情况下就不能将该端口设置为 Tagged，而应该设置为 Untagged，否则发送出去的帧将有可能无法被对面交换机和 HUB 连接的计算机识别。另外，连接在对面的交换机和 HUB 上的设备都将被认为是属于同一个 VLAN（即这个端口的缺省 VLAN）。

7. VLAN 组网方案示例

7.1 确定需求

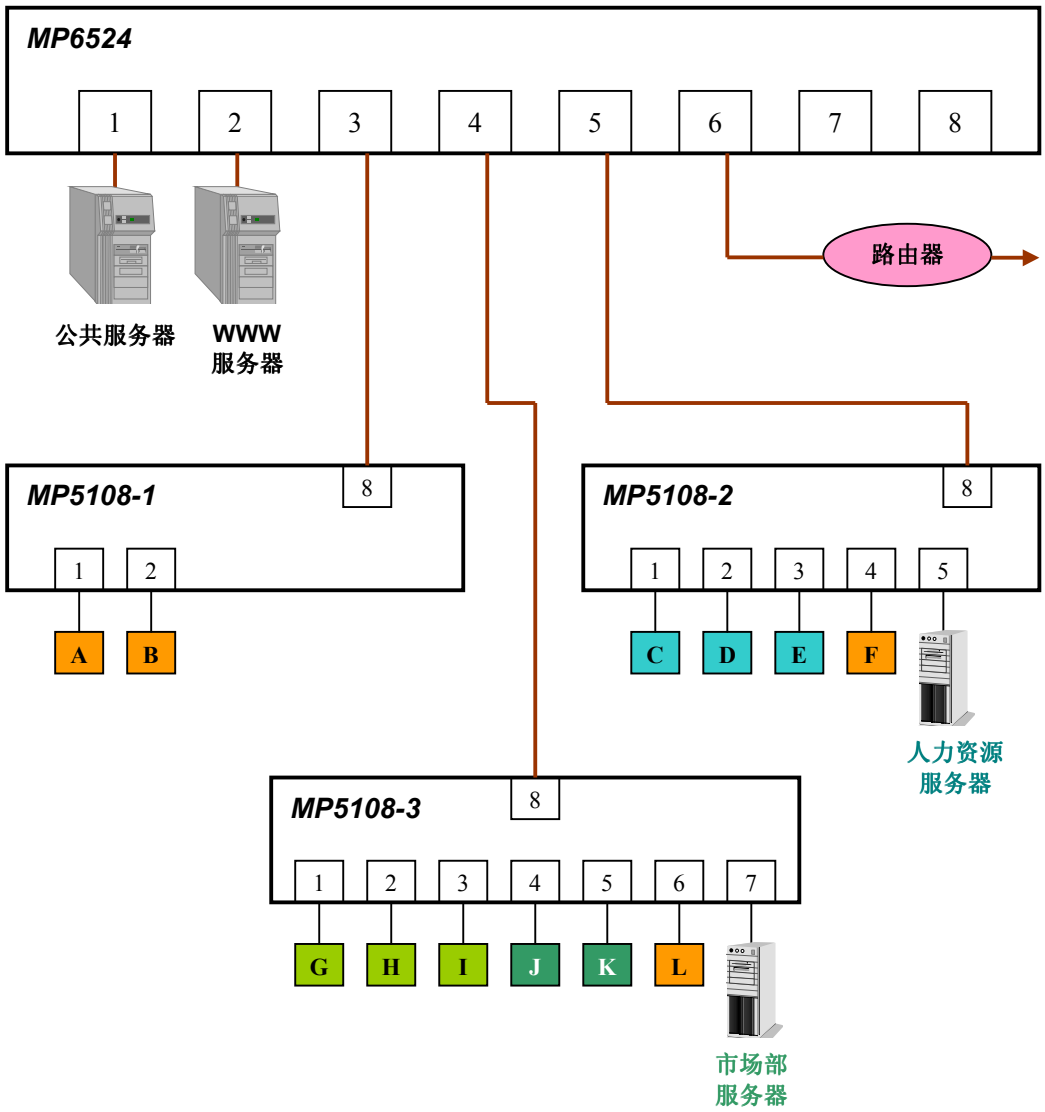


图 7.1 组网示例

确定 VLAN 之前首先要明确需求，根据具体应用的需要将联网用户划分若干个组，明确组与组之间的互通关系。此处以 MP6524、MP5108 为例。上图的组网示例，组与组之间的互通关系假定如下表所示。

主机	部门	交换机	端口	说明
A	管理	MP5108-1	1	可与管理部互相访问
B	管理	MP5108-1	2	同上
C	人力资源	MP5108-2	1	可与人力资源部和管理部 F 互相访问
D	人力资源	MP5108-2	2	同上
E	人力资源	MP5108-2	3	同上
F	管理	MP5108-2	4	可与管理部和人力资源部互相访问
人力资源服务器		MP5108-2	5	可被人力资源部 C、D、E 访问

G	国内市场	MP5108-3	1	可与国内市场部、管理部的 L 互相访问
H	国内市场	MP5108-3	2	同上
I	国内市场	MP5108-3	3	同上
J	国际市场	MP5108-3	4	可与国际市场部、管理部的 L 互相访问
K	国际市场	MP5108-3	5	同上
L	管理	MP5108-3	6	可与国内、国际市场部互相访问
市场部服务器	市场	MP5108-3	7	可被 G、H、I、J、K 访问
公共服务器		MP6524	1	可被所有用户访问，但不能从外部通过路由器访问
WWW 服务器		MP6524	2	可被所有用户访问
路由器		MP6524	6	可被所有用户访问

表 7.1 需求关系表

MP5108-3 通过其端口 8 连接至 MP6524 的端口 3；
MP5108-3 通过其端口 8 连接至 MP6524 的端口 5；
MP5108-3 通过其端口 8 连接至 MP6524 的端口 4。

7.2 划分 VLAN

总的来说，划分 VLAN 就是将连接到网络上的主机划分为若干个组。

分组的原则是：同组的主机之间的互通需求相同，所有联网的主机都被划分到某一个组中。

经分析，在本例中将联网主机划分为如下 8 个组，实现 8 个 VLAN，如下表所示。

组	包含主机
国内市场	G、H、I
国际市场	J、K
管理	A、B、F、L
人力资源	C、D、E
市场部服务器	市场部服务器
人力资源部服务器	人力资源部服务器
公共服务器	公共服务器
WWW 与路由器	WWW 服务器、路由器

表 7.2 VLAN 划分表

7.3 为 VLAN 确定 Vlan ID

在交换机内部划分不同 VLAN 的标志就是各个 VLAN 的 VLAN ID（802.1Q VID）不同。理论上说，每一个 VLAN 应该分配不同的 ID。但在实际应用中，如果我们将多个 VLAN 分配同样的 VID，在某些特定条件下也是允许的。

VLAN ID 是区分不同 VLAN 的唯一标识。如果两个 VLAN 的实现不存在交叉点（即任何一台交换机上都不需要同时实现的 VLAN），那么两个 VLAN 就可以共用相同的 VLAN ID。

我们可以利用下面的表格来帮助分析，如下表所示。

VLAN		是否需要在如下交换机上实现			
组	VLAN ID	MP5108-1	MP5108-2	MP5108-3	MP6524
国内市场	**2**			√	√
国际市场	**3**			√	√
管理	**4**	√	√	√	√
人力资源	**5**		√		√
市场部服务器	**6**			√	
人力资源部服务器	**6**		√		
公共服务器	**7**	√	√	√	√
WWW 与路由器	**8**	√	√	√	√

表 7.3 网络用户分组与交换机关系表

至此，网络建设的总体规划工作就完成了，剩下的工作就是具体的交换机配置。

7.4 为每台交换机确定 VLAN

根据表 7.3，我们可以确定每一台交换机上面应该实现的 VLAN，配置如下所示。

交换机	组	VLAN ID
MP5108-1	管理	**4**
	公共服务器	**7**
	WWW 与路由器	**8**
MP5108-2	管理	**4**
	人力资源	**5**
	人力资源服务器	**6**
	公共服务器	**7**
	WWW 与路由器	**8**
MP5108-3	国内市场	**2**
	国际市场	**3**
	管理	**4**
	市场部服务器	**6**
	公共服务器	**7**
	WWW 与路由器	**8**
MP6524	国内市场	**2**
	国际市场	**3**
	管理	**4**
	人力资源	**5**
	公共服务器	**7**
	WWW 与路由器	**8**

表 7.4 交换机 VLAN ID 配置表

7.5 确定 VLAN 成员及端口属性

VLAN 成员包含允许接收该 VLAN 的广播帧的端口，凡是与该 VLAN 的主机有互通需求的端口都应该包含在该 VLAN 成员中。

端口属性确定该端口输出数据帧是否带 802.1Q Tag。对于直接连接主机的端口，应设置

为 Untagged；对于连接支持 802.1Q VLAN 的局域网交换机的端口应该设置为 Tagged。

交换机	VLAN ID	VLAN 成员端口及属性								
		1	2	3	4	5	6	7	8	…
MP5108-1	**4**	**U**	**U**	—	—	—	—	—	**M**	—
	7	**U**	**U**	—	—	—	—	—	**M**	—
	8	**U**	**U**	—	—	—	—	—	**M**	—
MP5108-2	**4**	**U**	**U**	**U**	**U**	—	—	—	**M**	—
	5	**U**	**U**	**U**	**U**	**U**	—	—	**M**	—
	6	**U**	**U**	**U**	—	**U**	—	—	—	—
	7	**U**	**U**	**U**	**U**	—	—	—	**M**	—
	8	**U**	**U**	**U**	**U**	—	—	—	**M**	—
MP5108-3	**2**	**U**	**U**	**U**	—	—	**U**	**U**	**M**	—
	3	—	—	—	**U**	**U**	**U**	**U**	**M**	—
	4	**U**	**U**	**U**	**U**	**U**	**U**		**M**	—
	6	**U**	**U**	**U**	**U**	**U**	—	**U**	—	—
	7	**U**	**U**	**U**	**U**	**U**	**U**		**M**	—
	8	**U**	**U**	**U**	**U**	**U**	**U**		**M**	—
MP6524	**2**	**U**	**U**	—	**M**	—	**U**	—	—	—
	3	**U**	**U**	—	**M**	—	**U**	—	—	—
	4	**U**	**U**	**M**	**M**	**M**	**U**	—	—	—
	5	**U**	**U**	—	—	**M**	**U**	—	—	—
	7	**U**	—	**M**	**M**	**M**	—	—	—	—
	8	—	**U**	**M**	**M**	**M**	**U**	—	—	—

表 7.5 交换机 VLAN 成员端口及端口属性配置表

说明

U 表示 VLAN 成员包括该端口，端口属性为 Untagged（输出数据帧不带 802.1Q Tag）；

M 表示 VLAN 成员包括该端口，端口属性为 Tagged（输出数据帧带 802.1Q Tag）；

— 表示 VLAN 成员不包括该端口。

7.6 确定端口缺省 VLAN ID

对于直接连接主机的端口，应设置为该主机所属的 VLAN；对于连接支持 802.1Q VLAN 的交换机的端口应该使该端口设置与对端的交换机端口的设置在 802.1Q 级别上相一致。

交换机	端口	缺省 VLAN ID
MP5108-1	**1**	**4**
	2	**4**
	8	**7**
MP5108-2	**1**	**5**
	2	**5**
	3	**5**
	4	**4**
	5	**6**
	8	**7**
MP5108-3	**1**	**2**
	2	**2**
	3	**2**
	4	**3**
	5	**3**
	6	**4**
	7	**6**
	8	**7**
MP6524	**1**	**7**
	2	**8**
	3	**7**
	4	**7**
	5	**7**
	6	**8**

表 7.6 交换机端口缺省 VLAN ID 配置表

【撰稿】严华
【时间】2001.10