**主题10 交换机的配置**

19组

组长：刘志君mf1532043

组员：刘轩宇 dz1532002

张心雨 mf1532095

王刚 mf1532063

彭楠 mf1532050

陈云林 mf1532017

摘要：

本文介绍了交换机的主要工作原理及其配置方法，主要包括三个部分，第一部分是交换机的原理介绍以及基本配置，第二部分是交换机中生成树的配置方法，第三部分是VLAN相关的配置方法。

交换（switching）是按照通信两端传输信息的需要，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由上的技术的统称。交换机根据工作位置的不同，可以分为广域网交换机和局域网交换机。广域的交换机（switch）就是一种在通信系统中完成信息交换功能的设备，它应用在数据链路层。交换机有多个端口，每个端口都具有桥接功能，可以连接一个局域网或一台高性能服务器或工作站。

关键词: 交换机、生成树、VLAN

**目 录**

[1.交换机的工作机制 3](#_Toc435343967)

[1.1交换机的工作原理 3](#_Toc435343968)

[1.1.1交换机工作主要机制 3](#_Toc435343969)

[1.1.2交换机结构 4](#_Toc435343970)

[1.2交换机的常规配置 5](#_Toc435343971)

[1.2.1基本概念 5](#_Toc435343972)

[1.2.2交换机口令配置 5](#_Toc435343973)

[1.2.3交换机VLAN相关配置 6](#_Toc435343974)

[1.2.4交换机网关，域名相关配置 6](#_Toc435343975)

[1.2.5交换机显示命令 7](#_Toc435343976)

[2.生成树协议 7](#_Toc435343977)

[2.1冗余拓扑概述 7](#_Toc435343978)

[2.2生成树概述 10](#_Toc435343979)

[2.3STP的机制 11](#_Toc435343980)

[2.3.1BPDU简介 11](#_Toc435343981)

[2.3.2桥(根交换机)和指定端口的选举过程 12](#_Toc435343982)

[2.3.3生成树的端口状态转换 13](#_Toc435343983)

[3虚拟局域网 14](#_Toc435343984)

[3.1使用vlan的原因 14](#_Toc435343985)

[3.2vlan技术 15](#_Toc435343986)

[3.2.1概述 15](#_Toc435343987)

[3.2.2VLAN的主要特征 16](#_Toc435343988)

[3.2.3VLAN的实现 17](#_Toc435343989)

[3.3静态vlan和动态vlan 18](#_Toc435343990)

[3.3.1静态VLAN 18](#_Toc435343991)

[3.3.2动态VLAN 19](#_Toc435343992)

[3.4vlan内主机之间的通信 19](#_Toc435343993)

[3.5vlan间的主机通信 19](#_Toc435343994)

[3.5.1通过路由器实现VLAN间的通信 20](#_Toc435343995)

[3.5.2用交换机代替路由器实现VLAN间的通信 20](#_Toc435343996)

[3.6vlan的配置 21](#_Toc435343997)

[3.6.1常见的VLAN配置类型 21](#_Toc435343998)

[3.6.2VLAN的配置过程 23](#_Toc435343999)

[3.7vlan之间的路由配置 27](#_Toc435344000)

[3.8三层交换机 28](#_Toc435344001)

[参考文献 31](#_Toc435344002)

# 1.交换机的工作机制

## 1.1交换机的工作原理

交换机是一种基于MAC（网卡的硬件地址）识别，能完成封装转发数据包功能的网络设备，交换机正如它的名字一样采用的是交换的工作模式，它可以“学习”网络中各个终端的MAC 地址，并把其存放在内部的MAC 地址表中，通过在数据帧的始发者和目标接收者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。

交换机拥有一条很高很快的背部总线和内部交换矩阵。交换机的所有端口均挂接在这条背部总线上，当控制电路接收到数据包后，处理端口会查找内存中的MAC 地址对照表以确定目的MAC 地址的网卡接在哪个端口上，通过内部交换矩阵直接将数据包传送到目的端口，而不是所有端口，交换机的这种工作方式较于集线器来说效率高，不浪费网络资源，因为它只是对目的地址传输数据，发送数据是其他节点很难侦听到所发送的信息。这也是交换机能很快取代集线器的重要原因之一。

交换机的另一个重要特点是它不像集线器一样每个端口共享带宽，它的每一个端口都是共享一部分交换机的总带宽，这样在速率上就对每个端口有个根本的保障。这样交换机就可以在同一时刻进行多个端口之间数据传输，每个端口都视为独立的网段，享有独立固定的带宽。无需同其他设备竞争使用。

交换机的目的是使得传输效率更高，它根据MAC 地址来进行判断，决定数据帧该送到目的地址的连接端口，而不打扰其他不相干的连接端口，如果内存中的地址表中不包含目的MAC 地址，交换机则会向所有端口广播这个数据包，找到后再将这个MAC地址加入到自己的MAC 地址表中，这样下次发送到这个地址时便不会发错[1][2][3][4]。

### 1.1.1交换机工作主要机制

地址表：端口地址表记录了端口下包含主机的MAC地址。端口地址表是交换机上电后自动建立的，保存在RAM中，并且自动维护。交换机隔离冲突域的原理是根据其端口地址表和转发决策决定的。

转发决策：交换机的转发决策有三种操作：丢弃、转发和扩散。丢弃：当本端口下的主机访问已知本端口下的主机时丢弃。转发：当某端口下的主机访问已知某端口下的主机时转发。扩散：当某端口下的主机访问未知端口下的主机时要扩散。每个操作都要记录下发包端的MAC地址，以备其它主机的访问。

生存期：生存期是端口地址列表中表项的寿命。每个表项在建立后开始进行倒记时，每次发送数据都要刷新记时。对于长期不发送数据主机，其MAC地址的表项在生存期结束时删除。所以端口地址表记录的总是最活动的主机的MAC地址。

三层路由：通常，普通的交换机只工作在数据链路层上，路由器则工作在网络层。而功能强大的三层交换机可同时工作在数据链路层和网络层，并根据 MAC地址或IP地址转发数据包。但是要注意到三层交换机并不能完全取代路由器，因为它主要是为了实现处于两个不同子网的Vlan进行通讯，而不是用来作数据传输的复杂路径选择。

网管功能：一台交换机所支持的管理程度反映了该设备的可管理性与可操作性。带网管功能的交换机可对每个端口的流量进行监测，设置每个端口的速率，关闭/打开端口连接。通过对交换机端口进行监测，便于对网络业务流量的区分和迅速进行网络故障定义，提高了网络的可管理性。

端口聚合：这是一种封装技术，它是一条点到点的链路，链路的两端可以都是交换机，也可以是交换机和路由器，还可以是主机和交换机或路由器。基于端口汇聚（Trunk）功能，允许交换机与交换机、交换机与路由器、主机与交换机或路由器之间通过两个或多个端口并行连接同时传输以提供更高带宽、更大吞吐量， 大幅度提供整个网络能力。

### 1.1.2交换机结构

级联方式：这是最常用的一种组网方式，它通过交换机上的级联口（UpLink）进行连接。需要注意的是交换机不能无限制级联，超过一定数量的交换机进行级联，最终会引起广播风暴，导致网络性能严重下降。

聚合方式：前面我们已接触到端口聚合的特点，此种方式相当于用多个端口同时进行级联，它提供了更高的互联带宽和线路冗余，使网络具有一定的可靠性。

堆叠方式：交换机的堆叠是扩展端口最快捷、最便利的方式，同时堆叠后的带宽是单一交换机端口速率的几十倍。但是，并不是所有的交换机都支持堆叠的，这取决于交换机的品牌、型号是否支持堆叠；并且还需要使用专门的堆叠电缆和堆叠模块；最后还要注意同一叠堆中的交换机必须是同一品牌。

分层方式：这种方式一般应用于比较复杂的交换机结构中，按照功能可划分为：接入层、汇聚层、核心层。

作为网络的重要连接设备，交换机在实际使用中相当频繁。对于一般家庭用户而言，比较复杂的应用就是交换机的级联结构了；而三层路由、堆叠等高级应用一般在企业中应用较多。

## 1.2交换机的常规配置

### 1.2.1基本概念

IOS:互联网操作系统，也就是交换机和路由器中用的操作系统

VLAN:虚拟lan

VTP:VLAN TRUNK PROTOCOL

DHCP:动态主机配置协议

ACL:访问控制列表

用户模式hostname# ；

特权模式hostname(config)# ；

全局配置模式hostname(config-if)# ；

### 1.2.2交换机口令配置

switch>enable ；进入特权模式switch#config terminal ；进入全局配置模式switch(config)#hostname csico ；设置交换机的主机名switch(config)#enable secret csico1 ；设置特权加密口令switch(config)#enable password csico8 ；设置特权非密口令switch(config)#line console 0 ；进入控制台口switch(config-line)#line vty 0 4 ；进入虚拟终端switch(config-line)#login ；虚拟终端允许登录switch(config-line)#password csico6 ；设置虚拟终端登录口令csico6switch#exit ；返回命令

### 1.2.3交换机VLAN相关配置

switch#vlan database ；进入VLAN设置switch(vlan)#vlan 2 ；建VLAN 2switch(vlan)#vlan 3 name vlan3 ；建VLAN 3并命名为vlan3switch(vlan)#no vlan 2 ；删vlan 2switch(config)#int f0/1 ；进入端口1switch(config)#speed ? 查看speed命令的子命令switch(config)#speed 100 设置该端口速率为100mb/s (10/auto)switch(config)#duplex ? 查看duplex的子命令switch(config)#duplex full 设置该端口为全双工(auto/half)switch(config)#description TO\_PC1 这是该端口描述为TO\_PC1switch(config-if)#switchport access vlan 2 ；当前端口加入vlan 2switch(config-if)#switchport mode trunk ；设置为trunk模式(access模式)switch(config-if)#switchport trunk allowed vlan 1，2 ；设置允许的vlanswitch(config-if)#switchport trunk encap dot1q ；设置vlan 中继switch(config)#vtp domain vtpserver ；设置vtp域名相同switch(config)#vtp password ；设置发vtp密码switch(config)#vtp server ；设置vtp服务器模式switch(config)#vtp client ；设置vtp客户机模式

### 1.2.4交换机网关，域名相关配置

switch(config)#interface vlan 1 ；进入vlan 1switch(config-if)#ip address 192.168.1.1 255.255.255.0 ；设置IP地址switch(config)#ip default-gateway 192.168.1.6 ；设置默认网关switch(config)#ip domain-name cisco.com 设置域名switch(config)#ip name-server 192.168.1.18 设置域名服务器switch(config)#mac-address-table? 查看mac-address-table的子命令switch(config)#mac-address-table aging-time 100 设置超时时间为100msswitch(config)#mac-address-table permanent 0000.0c01.bbcc f0/3 加入永久地址在f0/3端口switch(config)#mac-address-table restricted static 0000.0c02.bbcc f0/6 f0/7 加入静态地址目标端口f0/6源端口f0/7switch(config)#endswitch#show mac-address-table 查看整个MAC地址表switch#clear mac-address-table restricted static 清除限制性静态地址

### 1.2.5交换机显示命令

switch#write ；保存配置信息switch#show vtp ；查看vtp配置信息switch#show run ；查看当前配置信息switch#show vlan ；查看vlan配置信息switch#show interface ；查看端口信息switch#show int f0/0 ；查看指定端口信息switch#show int f0/0 status；查看指定端口状态switch#dir flash: ；查看闪存

# 2.生成树协议

## 2.1冗余拓扑概述

访问文件服务器、数据库、因特网、企业内部网和企业外部网，这些对于商业成功有着关键作用。如果网络瘫痪了，生产就会蒙受损失，顾客就会不满。因此，在如今的网络工程设计中，冗余设计是考验一个网络稳定的关键环节，链路冗余使网络具有了容错功能，但如何在冗余设计中避免“网络环路”的危害呢？

冗余拓扑（Redundant Topologies）的目标是消除由于单点故障引起的网络中断。这就和我们每天上班途经的公路一样，如果正在进行道路维修的话，我们同样可以通过绕行来到达目的地。[5]如图2.1中所示，网段2中的所有客户端在交换机出现故障时，网络应用不会受到影响。交换机A如果出现故障，网络流量依然可以通过交换机B到达服务器和路由器。

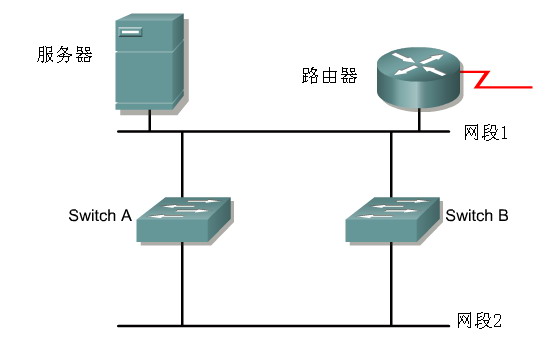
[](http://new.51cto.com/files/uploadimg/20080716/170304564.jpg)

图2.1

容错性通过冗余来实现。冗余指的是多于和大于一般情况和正常情况下所应该有的冗余设计可以贯穿整个三层结构（核心、汇聚、接入），每个冗余设计都有针对性，可以选择其中一部分或几部分应用到网络中以针对重要的应用系统。万一网络中某条路径失效时，冗余链路可以提供另一条物理路径。可采用链路聚合（IEEE 802.3ad）实现“端口级”冗余，以克服某个端口或线路引起的故障；也可采用生成树协议（IEEE 802.1d）提供“设备级”的冗余连接。

交换机学习连接到其端口设备的MAC地址，以便于工作数据能够正确转发到目的地。在交换机获得设备的MAC地址之前，它会把未知的目的地的帧泛洪出去，广播和多播也会被泛洪出去。所以，冗余交换拓扑也会导致广播风暴、帧的反复重传和MAC地址表不稳定的问题。

从生成树的发展历程来看，透明网桥转发数据帧时，如果有环路，数据帧将会在环路中来回传递，大量增生数据帧，形成广播风暴。如图8-2所示，显示了一个核心的数据区域的多环形网络。

多环形网络可以实现任何一条链路出现问题都不影响应用，但在环形交换网络中很容易出现“广播风暴”。出现“广播风暴”主要有两种原因：广播和电缆中断引发环路。

图2.2中说明广播环路的形成。网络两台交换和两台主机，两台交换机之间环形连接，如果没有启用生成树，主机A向主机B发送广播帧。

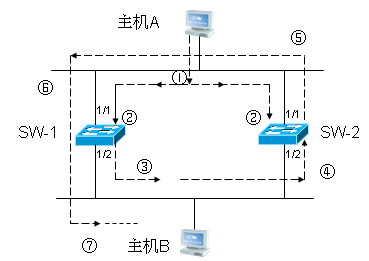
[](http://new.51cto.com/files/uploadimg/20080716/170417301.jpg)

图2.2

假设两台交换机均没有运行生成树，主机A发送MAC为FF-FF-FF-FF-FF-FF 的广播帧①，由于以太网络是星形或总线形，广播同时发送到SW-1和SW-2上②，当广播帧达到SW-1 1/1端口时，SW-1通过端口1/2将该广播帧发送给SW-2 的1/2口③④，SW-2通过1/1端口又将该广播帧发给SW的1/1 端口⑤⑥，SW-1将该数据帧继续通过1/2端口继续发给SW-2 的1/2口⑦，这样一个环路形成；另外我们注意到，第一个广播帧也发给SW-2的1/1，SW-2也一样将该广播帧发给SW-1，这样双向广播形成。

常见的环路主要是广播环路引起，然而，单播也能引发环路，图2.3显示了该环路引发的流程。

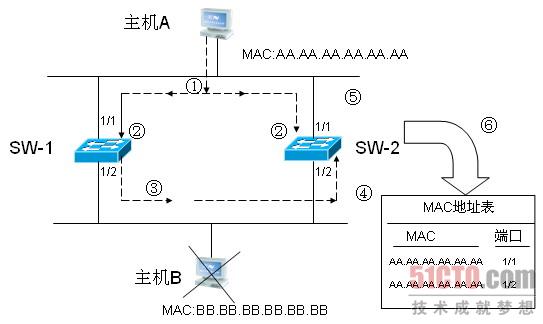
[](http://new.51cto.com/files/uploadimg/20080716/170716891.jpg)

图2.3

假设主机A发送一个Ping单一包给主机B①，数据包将同时发送到SW-1和SW-2的1/1端口上②，这时主机B临时关机，这是在SW-2上，主机B 的MAC地址从MAC地址表中被释放，这是SW-1的MAC表内没有主机B的MAC地址，直接将该数据包发送给SW-2 的1/2端口③、④，SW-2收到SW-1来的数据包，这时就有可能出现两种情况：

SW-2将广播该数据帧，应该主机B的MAC地址是新学到的，又重新从1/1口发送到回去⑤，这样环路产生。

SW-2从端口 1/2收到源地址为AA.AA.AA.AA.AA.AA的数据包，这是SW-2错误的更新他的MAC地址表，误认为主机A从1/2端口学到⑥，造成网络无法正常通信。

## 2.2生成树概述

生成树(Spanning Tree)协议, 说白了就是让网络中的所有交换机形成一个第二层的无环网络. 这是有必要的. 因为实际网络中交换机往往需要多条链路来实现冗余, 让网络不至于因单点故障而中断通信, 因此一个交换机可能需要有多条不同的链路连接到某个端口. 很明显, 这样就造成了网络是环状的(画个图就理解了). 然而, 交换机的特性是只划分冲突域而不划分广播域, 因此这种环状实际上是不允许出现在多个交换机的拓扑中的.

很简单的也很容易出现的一个问题就是广播风暴. 其实就是两个交换机A和B通过两条链路连接, 这就是一个最简单的环路. 当A收到一个广播, 很自然的要向其它所有端口发送. 由于存在环路, 很自然, A的这个端口会收到同样的广播, 然后又重复刚才的操作, 向所有其它端口发送. 这是无法停止的. 可以想象, 当网络比较大的时候, 这种广播会引起所有的交换机同时发送一样的广播包, 导致阻塞链路甚至使交换机down掉. 这就是广播风暴.

很明显, 要解决这种问题只能有一种方法, 就是让存在环路的网络变成没有环路的网络, 也就是让某些冗余的链路暂时不能工作, 而作为正常链路的备份, 当正常链路失效的时候再启用冗余链路. 而生成树协议就是为了达到这个目的.

## 2.3STP的机制

STP的运行一般是自动的, 也就是说当交换机启动就开始运行这协议了. 生成树协议包含了一个叫做网桥协议数据单元(BPDU), 所有的生成树协议相关信息都背包含在BPDU中, BPDU是交换机启动后自动发送的, 默认间隔为2秒. 所有交换机用它来:

(1)选择一台交换机作为生成树的根交换机;

(2)计算它到根交换机的最短路径并确定根端口;

(3)在每一个LAN网段(即交换机端口隔离的网段), 选举一个指定端口, 只有指定端口和跟端口才能连接该网段和外部的通信. 同一网段的其它端口都处于阻塞状态, 不能通信.

### 2.3.1BPDU简介

PDU是运行STP的交换机之间交换的消息帧。BPDU内包含了STP所需的路径和优先级信息，STP便利用这些信息来确定根桥以及到根桥的路径。

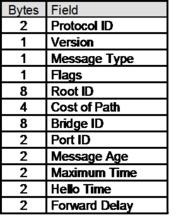


图2.4

Root ID:本交换机当前"承认"的根桥, 在网络未稳定前, 每收到更低BID网桥发来的BPDU, 该交换机都会将自己发送的BPDU中Root ID字段替换成这个更低的BID(注意不是直接转发这个BPDU). 网络稳定后, 网络中所有BPDU的Root ID都是变成一样的了.

Bridge ID:本交换机的BID, 在选举指定端口时使用, 通过它也了解了哪些交换机在同一LAN中.

Root Path Cost:达到根桥的成本, 在选举指定端口时使用.

Port ID:端口ID, 选举指定端口时, 在当通过前面三个条件不能判断时使用端口ID判断(其实就是判断同一交换机的不同端口, 当这些端口在一个LAN中时).

### 2.3.2桥(根交换机)和指定端口的选举过程

根桥的选举可以用一个字来形容: 低. 即比较谁的Bridge ID最低谁就是跟桥. BID由两部分组成: 优先值和MAC地址, 先比较优先值再比较MAC地址. 默认优先值是一样的. 所以如果想人工干预跟桥选举, 就可以设置低的优先值.

所有的交换机如何都得知谁的BID最低呢?当然是通过BPDU. 如前面所说, 所有交换机刚启动的时候均处于侦听状态, 即不发送用户数据, 发送和接收BPDU.

如图，首先, 广播自己的BPDU, 其中包含一些重要的字段(详见下面的指定端口选举). 最初的BPDU中BID字段和Root ID字段均为本交换机的BID. 在之后的过程那个中,每个交换机如果收到的BPDU中的Root ID比自己的Root ID低, 则将这个Root ID替换当前自己发送的BPDU中的Root ID并继续广播,通过这个过程, 最终所有的交换机都接收和发送相同Root ID的BPDU, 而这个BPDU的Root ID就是跟桥的BID.

选择了跟桥以后, 就开始选举指定端口. 指定端口按顺序判断Root ID, Root Path Cost, BID和Port ID, 并选出最低的值作为该网段的指定端口. 另外, 每个交换机上有一个根端口, 该端口是交换机上Root Path Cost最低的端口, 也就是该交换机上离跟桥最近的端口. Root Path Cost是在BPDU接收端口上进行累加的(注意: 发送端口不参与), 如果该端口连接到快速以太网, 则该端口要累加19.[6]根桥, 指定端口和根端口选举完毕后, 进入学习状态, 然后进入转发状态. 剩下的端口直接进入阻塞状态.

### 2.3.3生成树的端口状态转换

指定端口和根端口选举完毕后, 进入学习状态, 然后进入转发状态. 剩下的端口直接进入阻塞状态.

可以把生成树协议中交换机通信数据分为两类, 一类是BPDU包, 另一类是用户数据.所有端口在任意状态均会发送BPDU以获得同样的拓扑.在这个基础上, 可以把生成树协议中的交换机端口分为5种状态:



图2.5

（1）侦听状态：处于这个状态, 持续15秒, 期间不发送用户数据.这个状态下生成树完成根桥,指定端口和根端口的选举.

（2）学习状态:侦听状态后,根端口和指定端口进入学习状态,这个状态还是不转发用户数据,而只通过收到的用户数据学习该端口下都有那些MAC地址, 从而建立MAC映射表. 持续15秒.

（3）阻塞状态:侦听状态后, 非根端口和指定端口直接进入这个状态. 只接收用户数据包和BPDU, 不进行转发. 当20秒内未收到BPDU后, 重新进入侦听状态.

（4）转发状态:学习状态后, 根端口和指定端口进入转发状态. 这时指定端口开始转发所有的BPDU和用户数据.

（5）禁止状态:不转发用户数据和BPDU, 可以理解成不参与协议了.[7]

生成树收敛是指交换机处于转发或阻塞状态, 而不存在侦听或者学习状态. 因为这时候生成树是稳定的.

当网络拓扑产生变化需要重新计算生成树, 到网络重新收敛, 通常需要20+15+15=50秒. 而如果直接连接的链路失效(如直连端口失效), 能被CDP直接检测到, 因此不需要20秒的生存时间, 重新收敛只需要30秒.

# 3虚拟局域网

## 3.1使用vlan的原因

VLAN是一种用逻辑的定义方法，把两个或更多的连在交换网络上的终端规划在一起。这种逻辑定义方法可以延伸到多个交换机。被规划在一起的终端，可以通过几种网络设置来规划。好像任何一种网络技术一样，了解在您的网络上存在的VLAN的特性，是有效地管理网络一个非常重要的一节。这可令您更精确的设定VLAN并在事故发生时减少故障诊断的时间。

采用VLAN的主要原因有几个：如控制广播域的范围，网络安全，第三层地址的管理，和网络资源的集中管理。

1) 控制广播域的范围

当一个广播域内的设备增加时，在广播域内设备的广播频率便会相对增加。广播率的提高，对设备的效率会有很大的影响，因为每一个设备都必须中断其CPU正在处理的业务，来处理收到的广播包，以决定是否需要对包内的数据作进一步处理。这种中断降低了CPU处理正常业务的效率，增长了完成这些业务的时间。

VLAN一个非常重要的好处是在一个VLAN内的广播包不会跑到别的VLAN上去。通过限制一个VLAN 上的设备数目，在一个VLAN 上的广播率便可受到控制。一个正常的广播率应该平均每秒不超过30 个广播包。

2) 网络安全

有很多时候，网管人员需要限制对本地网络中一个或多个特别设备的接入。如果所有的设备都在同一个广播域内，便很难执行这种限制。通过建立多个广播域，可以通过地址过滤和建立连接认可地址表来实现该限制。

数据包要跨越一个VLAN必须通过一个3层路由设备。这种路由设备让网管人员可以定义设备间的接入。这种接入控制功能的使用，可以控制和监视对敏感资源设备的接入。

3) 第三层地址管理

一个很常见的设计，是把同类型的设备，规划在同一个IP子网。例如把打印机安排在同一个IP子网上，属于会计部的工作站和服务器却在另一个子网。在逻辑上这样好像很合理，但在一个大型企业网络上，这种构想没有VLAN是无法实现的。

4) 网络资源的集中管理

假定我们把所有的打印机都规划在一个子网上，而每一个打印机都必须在同一个广播域里。这样等于需要在每一个楼层上，分别安装交换机。这些交换机都需要光缆和铜缆的连接，而这些打印机子网都需要连接到自己的专用路由器端口上。

利用VLAN，可以让打印机和网络中的其他设备连接到同一个交换机，分享同一条互联的电缆或光纤链路、同一个路由器端口。

## 3.2vlan技术

### 3.2.1概述

VLAN（Virtual Local Area Network）即虚拟局域网[8]，是一种通过将局域网内的设备逻辑地址而不是物理地址划分成一个个网段从而实现虚拟工作组的新兴技术。IEEE于1999年颁布了用以标准化VLAN实现方案的802.1Q协议标准草案。

VLAN技术允许网络管理者将一个物理的LAN逻辑地划分成不同的广播域（或称虚拟LAN，即VLAN），每一个VLAN都包含一组有着相同需求的计算机工作站，与物理上形成的LAN有着相同的属性。但由于它是逻辑地而不是物理地划分，所以同一个VLAN内的各个工作站无须被放置在同一个物理空间里，即这些工作站不一定属于同一个物理LAN网段。一个VLAN内部的广播和单播流量都不会转发到其他VLAN中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

VLAN是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了VLAN头，用VLAN ID把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

### 3.2.2VLAN的主要特征

1) 所有成员组成一个VLAN。同一个VLAN中的所有成员共同组成一个独立于物理位置而具有相同逻辑的广播域，共享一个VLAN标志，组成一个虚拟局域网络。

2) 成员间首发广播包的特点是同一个VLAN中的所有成员均能受到同一个VLAN中的其它成员发送来的每一个广播包，但收不到其它VLAN

中成员的广播包。

3) 成员间通信的特点是同一个VLAN中的所有成员之间的通信，通过VLAN交换机可以直接进行，不需要路由支持；不同VLAN成员之间不能直接通信，无论采用传统路由器方式还是虚拟路由方式，均需要通过路由支持才能进行。

4) 便于工作组优化组合。控制通信活动，隔离广播数据顺化网络管理，方便工作组优化组合。VLAN中的成员只要拥有一个VLAN ID，就可以不受物理位置的限制，随意移动工作站的位置。

5) 网络安全性强。通过路由访问列表、MAC地址分配等VLAN划分原则，可以控制用户的访问权限和逻辑网段的大小。VLAN交换机就像是一道道屏风，只有具备VLAN成员资格的分组数据才能通过，这比用计算机服务器做防火墙要安全得多，增加了网络的安全性，提高了网络的整体安全能力。

6) 网络性能高。网络带宽得到充分利用，网络性能大大提高。

7) 网络管理简单、直观。

### 3.2.3VLAN的实现

1) 基于端口划分的VLAN [9]

这种划分VLAN的方法是根据以太网交换机的端口来划分，比如Quidway S3526的1~4端口为VLAN 10，5~17为VLAN 20，18~24为VLAN 30，当然，这些属于同一VLAN的端口可以不连续，如何配置，由管理员决定，如果有多个交换机，例如，可以指定交换机 1 的1~6端口和交换机 2 的1~4端口为同一VLAN，即同一VLAN可以跨越数个以太网交换机，根据端口划分是目前定义VLAN的最广泛的方法，IEEE 802.1Q规定了依据以太网交换机的端口来划分VLAN的国际标准。

这种划分的方法的优点是定义VLAN成员时非常简单，只要将所有的端口都指定义一下就可以了。它的缺点是如果VLAN A的用户离开了原来的端口，到了一个新的交换机的某个端口，那么就必须重新定义。

2) 基于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地址的主机都配置他属于哪个组。这种划分VLAN的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，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，配置是非常累的。而且这种划分的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组的成员，这样就无法限制广播包了。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，这样，VLAN就必须不停的配置。

3) 基于网络层划分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)划分的，虽然这种划分方法是根据网络地址，比如IP地址，但它不是路由，与网络层的路由毫无关系。它虽然查看每个数据包的IP地址，但由于不是路由，所以，没有RIP，OSPF等路由协议，而是根据生成树算法进行桥交换，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，这对网络管理者来说很重要，还有，这种方法不需要附加的帧标签来识别VLAN，这样可以减少网络的通信量。

这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的(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的以太网祯头，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[10]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，当然这种方法不适合局域网，主要是效率不高。

## 3.3静态vlan和动态vlan

### 3.3.1静态VLAN

静态VLAN提供基于端口的成员资格，在这里，交换机端口被分配给某些特定的VLAN。终端用户设备根据它们所连人的物理交换机端口而成为一个VLAN中的成员。对于这些终端设备,不需要握手联络或独特的VLAN成员关系协议；当它们连入一个端口时，会自动进行VLAN互连。正常情况下，终端设备甚至不会注意到该VLAN的存在。交换机端口和它的VLAN完全可以看做和用于其他任何网段，好像和其他“本地连接”的成员连在一根网线上。

由于交换机端口是通过网络管理员的人工操作而分配给VLAN的，因而将这种VLAN称为静态VLAN。单一一台交换机上的端口也可以分配和组并到许多VLAN中。即使是连在同一台交换机上的两台设备，如果它们分属于不同的VLAN端口，通信量也不会在它们之间传送。如果我们想要在两个VLAN之间通信，就要利用一台第3层设备来路由分组，或使用一台第2层设备来桥接（bridge）分组。

一般而言，端口和VLAN之间的成员资格是在交换机的硬件中处理的，这种硬件有一个专用的应用集成电路（ASIC）。由于所有的端口映像都是在硬件级上完成，无须复杂的表项查找，因而这种成员关系能提供性能优良的通信功能。

### 3.3.2动态VLAN

动态VLAN[11]是根据终端用户设备的MAC地址来定义成员资格的。当设备连人一个交换机端口时，该交换机必须查询它的一个数据库以建立VLAN的成员资格。因此，网络管理员必须先把用户的MAC地址分配到VLAN成员资格策略服务器(VMPS，VLAN Membership Policy Server)的数据库中的一个VLAN上。

对Cisco交换机而言，动态VLAN是用如Ciscoworks 2000或Ciscoworks for Switched Internetworks（CWSI）的网络管理工具来建立和进行管理的。动态VLAN对终端用户来说具有更大的灵活性和可移动性，但要求有更多的管理方面的开销。

## 3.4vlan内主机之间的通信

在VLAN内的通信，是通过数据帧头中指定通信目标的MAC地址来完成的。而为了获取MAC地址，TCP/IP协议下使用ARP地址协议解析MAC地址的方法是通过广播报文来实现的，如果广播报文无法到达目的地，那么就无从解析MAC地址，亦即无法直接通信。

## 3.5vlan间的主机通信

当计算机分属不同的VLAN时，就意味着分属不同的广播域，自然收不到彼此的广播报文。因此，属于不同VLAN的计算机之间无法直接互相通信。为了能够在VLAN间通信，需要利用OSI参照模型中更高一层——网络层的信息(IP地址)来进行路由。在目前的网络互连设备中能完成路由功能的设备主要有路由器和三层以上的交换机。

### 3.5.1通过路由器实现VLAN间的通信

使用路由器实现VLAN间通信时，路由器与交换机的连接方式有两种。第一种通过路由器的不同物理接口与交换机上的每个VLAN分别连接。第二种通过路由器的逻辑子接口与交换机的各个VLAN连接。

**通过路由器的不同物理接口与交换机上的每个VLAN分别连接。**

这种方式的优点是管理简单，缺点是网络扩展难度大。每增加一个新的VLAN，都需要消耗路由器的端口和交换机上的访问链接，而且还需要重新布设一条网线。而路由器，通常不会带有太多LAN接口的。新建VLAN时，为了对应增加的VLAN所需的端口，就必须将路由器升级成带有多个LAN接口的高端产品，这部分成本、还有重新布线所带来的开销，都使得这种接线法成为一种不受欢迎的办法。

**通过路由器的逻辑子接口与交换机的各个VLAN连接。**

这种连接方式要求路由器和交换机的端口都支持汇聚链接，且双方用于汇聚链路的协议自然也必须相同。接着在路由器上定义对应各个VLAN的逻辑子接口E1.1和E1.2。由于这种方式是靠在一个物理端口上设置多个逻辑子接口的方式实现网络扩展，因此网络扩展比较容易且成本较低，只是对路由器的配置要复杂一些。

### 3.5.2用交换机代替路由器实现VLAN间的通信

目前市场上有许多三层以上的交换机，在这些交换机中，厂家通过硬件或软件的方式将路由功能集成到交换机中，交换机主要用于园区网中，园区网中的路由比较简单，但要求数据交换的速度较快，因此在大型园区网中用交换机代替路由器已是不争的事实。用交换机代替路由器实现VLAN间通信的方式也有两种，其一，就是启用交换机的路由功能，这种方式的实现方法可采用以上介绍的路由器方式的任一种。其二，是利用某些高端交换机所支持的专用VLAN功能来实现VLAN间的通信。下面就对这种方式作重点介绍。

专用VALN将端口分为混杂端口、隔离端口和群体端口三类，只有混杂端口能够和路由器或三层交换机连接。对应混杂端口的VLAN称为Primary VLAN，它可以和映射到混杂端口的所有隔离VLAN(Isolated VLAN)的端口及群体VLAN(Community VLAN)的

端口通信。Community VLAN的端口除了可以和Primary VLAN通信外，内部端口间也可以相互通信。Isolated VLAN内的端口只能和Primary VLAN的端口通信外，内部端口间是互相隔离的。

专用VLAN在城域网建设中得到了广泛的应用，一个专用VLAN 不需要多个VLAN和IP子网就提供了具备第二层数据通信安全性的连接，所有的用户都接入专用VLAN，从而实现了所有用户与缺省网关的连接，而与专用VLAN内的其它用户没有任何访问，专用VLAN同样具有控制广播域的作用。

## 3.6vlan的配置

### 3.6.1常见的VLAN配置类型

**基于端口划分的Vlan**

这是最常应用的一种VLAN划分方法，应用也最为广泛、最有效，适用于任何大小的网络。这种划分VLAN的方法是根据以太网交换机的交换端口来划分的，它是将VLAN交换机上的物理端口和VLAN交换机内部的PVC（永久虚电路）端口分成若干个组，每个组构成一个虚拟网，相当于一个独立的VLAN交换机。对于不同部门需要互访时，可通过路由器转发，并配合基于MAC地址的端口过滤。对某站点的访问路径上最靠近该站点的交换机、路由交换机或路由器的相应端口上，设定可通过的MAC地址集。这样就可以防止非法入侵者从内部盗用IP地址从其他可接入点入侵的可能。

从这种划分方法本身我们可以看出，这种划分的方法的优点是定义VLAN成员时非常简单，只要将所有的端口都定义为相应的VLAN组即可。适合于任何大小的网络。它的缺点是如果某用户离开了原来的端口，到了一个新的交换机的某个端口，必须重新定义。

**基于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地址的主机都配置他属于哪个组，它实现的机制就是每一块网卡都对应唯一的MAC地址，VLAN交换机跟踪属于VLAN MAC的地址。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。

由这种划分的机制可以看出，这种VLAN的划分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，因为它是基于用户，而不是基于交换机的端口。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，配置是非常累的，所以这种划分方法通常适用于小型局域网。而且这种划分的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组的成员，保存了许多用户的MAC地址，查询起来相当不容易。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就必须经常配置。

**基于网络层协议划分VALAN**

VLAN按网络层协议来划分，可分为IP、IPX、DECnet、AppleTalk、Banyan等VLAN网络。这种按网络层协议来组成的VLAN，可使广播域跨越多个VLAN交换机。这对于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，但其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，这对网络管理者来说很重要，还有，这种方法不需要附加的帧标签来识别VLAN，这样可以减少网络的通信量。这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的(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的以太网祯头，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。

**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IP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，主要适合于不在同一地理范围的局域网用户组成一个VLAN，不适合局域网，主要是效率不高。

**按策略划分VLAN**

基于策略组成的VLAN能实现多种分配方法，包括VLAN交换机端口、MAC地址、IP地址、网络层协议等。网络管理人员可根据自己的管理模式和本单位的需求来决定选择哪种类型的VLAN。

**按用户定义、非用户授权换分VLAN**

基于用户定义、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加入一个VLAN。

### 3.6.2VLAN的配置过程

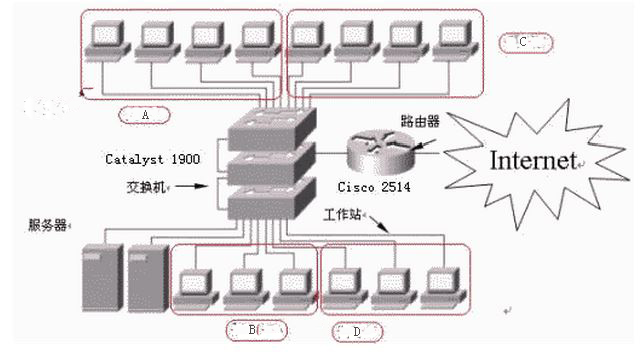


图3.1

网络基本结构为：整个网络中干部分采用3台Catalyst 1900网管型交换机(分别命名为Switch1、Switch2、Switch3)。一台Cisco 2514路由器，整个网络都通过路由器Cisco 2514与外部互联网进行连接。所连接的用户主要分布于四个部分A、B、C、D区。

各VLAN组所对应的网段如下表所示：

|  |  |  |
| --- | --- | --- |
| VLAN号 | VLAN名 | 端口号 |
| 2 | A | Switch1 2-21 |
| 3 | B | Switch2 2-16 |
| 4 | C | Switch3 2-9 |
| 5 | D | Switch3 10-21 |

图3.2

VLAN的配置过程其实非常简单，只需两步：（1）为各VLAN组命名；（2）把相应的VLAN对应到相应的交换机端口。

下面是具体的配置过程：

第1步：设置好超级终端，连接上1900交换机，通过超级终端配置交换机的VLAN，连接成功后出现如下所示的主配置界面（交换机在此之前已完成了基本信息的配置）：

1 user(s) now active on Management Console.

User Interface Menu

[M] Menus

[K] Command Line

[I] IP Configuration

Enter Selection:

第2步：单击"K"按键，选择主界面菜单中"[K] Command Line"选项 ，进入如下命令行配置界面：

CLI session with the switch is open.

To end the CLI session,enter [Exit ].    >

此时我们进入了交换机的普通用户模式，就象路由器一样，这种模式只能查看现在的配置，不能更改配置，并且能够使用的命令很有限。所以我们必须进入"特权模式"。

第3步：在上一步">"提示符下输入进入特权模式命令"enable"，进入特权模式，命令格式为">enable"，此时就进入了交换机配置的特权模式提示符：

#config t

  Enter configuration commands,one per line.End with CNTL/Z

(config)#

 第4步：为了安全和方便起见，我们分别给这3个Catalyst 1900交换机起个名字，并且设置特权模式的登陆密码。下面仅以Switch1为例进行介绍。配置代码如下：

(config)#hostname Switch1

Switch1(config)# enable password level 15 XXXXXX

Switch1(config)#

第5步：设置VLAN名称。因四个VLAN分属于不同的交换机，VLAN命名的命令为" vlan vlan号 name vlan名称 ，在Switch1、Switch2、Switch3、交换机上配置2、3、4、5号VLAN的代码为：

Switch1 (config)#vlan 2 name A

Switch2 (config)#vlan 3 name B

Switch3 (config)#vlan 4 name C

Switch3 (config)#vlan 5 name D

第6步：上一步我们对各交换机配置了VLAN组，现在要把这些VLAN对应于表1所规定的交换机端口号。对应端口号的命令是"vlan-membership static/ dynamic VLAN号 "。在这个命令中"static"(静态)和"dynamic"(动态)分配方式两者必须选择一个，不过通常都是选择"static"(静态)方式。VLAN端口号应用配置如下：

名为"Switch1"的交换机的VLAN端口号配置如下：

Switch1(config)#int e0/2

Switch1(config-if)#vlan-membership static 2

Switch1(config-if)#int e0/3

Switch1(config-if)#vlan-membership static 2

Switch1(config-if)#int e0/4

Switch1(config-if)#vlan-membership static 2

 ……

Switch1(config-if)#int e0/20

Switch(config-if)#vlan-membership static 2

Switch1(config-if)#int e0/21

Switch1(config-if)#vlan-membership static 2

Switch1(config-if)#

名为"Switch2"的交换机的VLAN端口号配置如下：

Switch2(config)#int e0/2

Switch2(config-if)#vlan-membership static 3

Switch2(config-if)#int e0/3

Switch2(config-if)#vlan-membership static 3

Switch2(config-if)#int e0/4

Switch2(config-if)#vlan-membership static 3

   ……

Switch2(config-if)#int e0/15

Switch2(config-if)#vlan-membership static 3

Switch2(config-if)#int e0/16

Switch2(config-if)#vlan-membership static 3

Switch2(config-if)#

名为"Switch3"的交换机的VLAN端口号配置如下(它包括两个VLAN组的配置)，先看VLAN 4的配置代码：

Switch3(config)#int e0/2

Switch3(config-if)#vlan-membership static 4

Switch3(config-if)#int e0/3

Switch3(config-if)#vlan-membership static 4

Switch3(config-if)#int e0/4

Switch3(config-if)#vlan-membership static 4

 ……

Switch3(config-if)#int e0/8

Switch3(config-if)#vlan-membership static 4

Switch3(config-if)#int e0/9

Switch3(config-if)#vlan-membership static 4

Switch3(config-if)#

下面是VLAN5的配置代码：

Switch3(config)#int e0/10

Switch3(config-if)#vlan-membership static 5

Switch3(config-if)#int e0/11

Switch3(config-if)#vlan-membership static 5

Switch3(config-if)#int e0/12

Switch3(config-if)#vlan-membership static 5

  ……

Switch3(config-if)#int e0/20

Switch3(config-if)#vlan-membership static 5

Switch3(config-if)#int e0/21

Switch3(config-if)#vlan-membership static 5

Switch3(config-if)#

为了验证我们的配置，可以在特权模式使用"show vlan"命令显示出刚才所做的配置，检查一下是否正确。

## 3.7vlan之间的路由配置

当我们使用路由器实现VLAN 间通信时，路由器与交换机的连接方式有两种。第一种是通过路由器的不同物理接口与交换机上的每个VLAN分别连接。第二种是通过路由器的物理接口的逻辑子接口与交换机的各个VLAN连接。

1.通过路由器的不同物理接口与交换机上的每个VLAN分别连接。假设我们使用cisco 2621路由器的两个快速以太网接口来连接上表的两个VLAN，简单的配置如下:

router2621 (config)# interface fa0 /0

router2621 (config-if)# ip address 192. 168. 10. 1 255.255. 255. 0

router2621 (config-if)# no shutdown

router2621 (config-if)# exit

router2621 (config) interface fa0 /1

router2621 (config-if)# ip address 192. 168. 11. 1 255.255. 255. 0

router2621 (config-if)# no shutdown

这种方式的优点是配置和管理简单，缺点是网络扩展难度大。每增加一个VLAN 就必须增加一个路由器的物理接口，当VLAN增加到几十个时，这种实现方式几乎不可能。

2.通过路由器的物理接口的逻辑子接口与交换机上的每个VLAN分别连接。

假设我们使用cisco 2621的快速以太网接口的逻辑子接口来实现，简单的配置如下:

router2621 (config)# interface fa0 /0

router2621 (config-if)# no shutdown

router2621 (config-if)# exit

router2621 (config)# interface fa0 /0. 10

router2621 (config-if)# encapsulation dot1q 10

router2621 (config-if)# ip address 192. 168. 10. 1 255.255. 255. 0

router2621 (config-if)# no shutdown

router2621 (config-if)# exit

router2621 (config)# interface fa0 /0. 11

router2621 (config-if)# encapsulation dot1q 11

router2621 (config-if)# ip address 192. 168. 11. 1 255.255. 255. 0

router2621 (config-if)# no shutdown

这种方案的优点是可扩充性好，增加VLAN时只需要增加逻辑子接口的数量即可，理论上可以达到很大的VLAN之间路由的扩充。它的缺点是: 所有的VLAN都在一个100Mbit/S的物理接口上路由容易造成带宽不足；由于使用了Trunk，路由器还要产生额外的开销。

## 3.8三层交换机

三层交换机就是内部集成了路由处理器的交换机。这种情况下，路由处理器位于交换机的某块线路卡上。现在的交换机的趋势是将路由处理器集成在交换机引擎相同的模块上，交换机的背板(交换机内部使用的高速交换通道)提供了交换机和路由处理器之间的通信路径。从技术上，交换机的内部路由处理器使用的数据流和外部路由器与交换机配合工作时的数据流类似。在交换机的背板上有连接交换机和路由处理器的Trunk，它为三层交换机提供了两种关键的优势:

A. 速度

B. 集成性

所以我们在有条件的情况下，基本上都是采用了三层交换机来实现VLAN 之间的路由功能。下面就举一个在Cisco 4006-L3三层交换机上配置V LAN之间路由的例子(假设L3模块位于交换机的插槽5中)：

Cisco 4006> (enable) set vtp domain xcc

Cisco 4006> (enable) set vtp mode server

Cisco 4006> (enable) set interface sc0 up (打开管理接口)

Cisco 4006> (enable) set interface sc0 1 192. 168. 1. 2 /24(设置管理接口的ip地址)

Cisco 4006> (enable) set ip route default 192. 168. 1. 1

Cisco 4006> (enable) set port channel 5 /1- 2 mode on

Cisco 4006> (enable) set vlan 1 5 /1-2

Cisco 4006> (enable) set trunk 5 /1 no negotiate dot1q 1-1005

Cisco 4006> (enable) session 5

Router-L3 (config)# interface port- channel1

Router-L3 (config-if)# no shutdown

Router-L3 (config-if)# exit

Router-L3 (config)# interface Giga bit Ether net 3

Router-L3 (config-if)# channel-group 1

Router-L3 (config-if)# exit

Router-L3 (config)# interface Giga bit Ether net 4

Router-L3 (config-if)# channel- group 1

Router-L3 (config-if)# exit

Router-L3 (config)# interface port- channel1. 1

Router-L3 (config-subif)# encapsulation dot1q 1 native (封装do t1q协议)

Router-L3 (config- subif)# ip address 192. 168. 1. 1 255.255. 255. 0

Router-L3 (config- subif)# exit

Router-L3 (config )# interface port- cha nnel1. 10

Router-L3 (config- subif)# encapsulation dot1q 10

Router-L3 (config - subif) # ip address 192. 168. 10. 1 255. 255. 255. 0

Router-L3 (config- subif)# exit

Router-L3 (config)# interface port- channel1. 11

Router-L3 (config- subif )# encapsulation dot 1q 11

Router-L3 (config - subif) # ip address 192. 168. 11. 1 255. 255. 255. 0

# 参考文献

1. 王廷尧《以太网技术及应用》北京：人民邮电出版社
2. Rich seifert 《千兆以太网技术与应用》郎波译北京：机械工业出版社
3. 罗庆超《二层交换机转发帧的原理和实现》2004
4. 李勇敢《浅谈集线器与交换机的区别》.内江科技.2005
5. 《生成树协议及其优化策略》 张欣
6. 《生成树协STP》http://blog.sina.com.cn/s/blog\_701074a60100lh3z.html
7. 生成树协议的详解 http://blog.163.com/yang\_h\_h/blog/static/4903699201110910371712/
8. IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks. IEEE802.1Q-1998.
9. Wang Xiaoying, Zhao Hai, Guan Mo, Guo Chengguang, Wang Jing. Research and Implementation of VLAN Based on Service. Conference Record / IEEE Global Telecommunications Conference, v5, 2003:67-84.
10. D.MePherson, B.Dykes, RFC3O69:VLAN Aggregation for Efficient IP Address Allocation, 2001.
11. Mihui Kim, Kijoon Chae. Dynamic VLAN registration mechanism on EoMPLS. Communications. 2003. APCC 2003. The 9th Asia-Pacific Conference on. Volume 1, 21-24, Sept. 2003: 208-212.
12. Cisco Networking Academy Program. CCNP思科网络技术学院教程(第七学期)多层交换[M ].北京: 人民邮电出版社. 2003.
13. 张卫,王能.计算机网络工程.清华大学出版社. 2004.
14. Boson Netsim 5. 31模拟软件帮助文档。