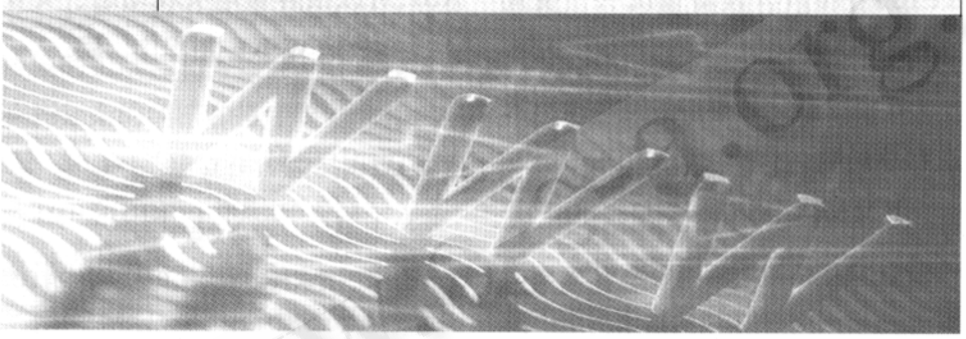
企业网络中 VLAN 的设计

张政宇 （中国石化股份公司茂名分公司 525000）

摘要 当今对于企事业单位的网络系统来说，VLAN已经成为网络建设中不可缺的一部分重要环节。本文通过案例的形式，详细介绍了企业 IP VLAN 的规划与划分。

关键词 企业网络 VLAN 设计



1 前言

VLAN即虚拟局域网。所谓VLAN亦是指处于不同物理位置的节点可以根据需要组成一个逻辑子网，即一个 VLAN 就是一个逻辑广播域，它可以扩展多个网络设备。VLAN 允许处于不同地理位置的网络用户加入一个逻辑子网中，共享一个广播域。通过对VLAN的创建可以控制广播风暴的产生，从而提高交换式网络的整体性能和安全性。

对于一个规模较大的企业来说，其下属有多个二级单位。一旦各单元的孤立的网络进行互连，出于对不同职能部门的管理、安全和整体网络的稳定运行，就涉及到了VLAN的划分。下面我们就该例对VLAN的划分做一详细的介绍。

2 需求分析

2.1 子网分析

(1) 该网络系统由三部分组成：公司、二级单位1、二级单位2，初始为三部分各自独立，未形成统一的网络环境。各网络系统的运行采用的是以交换技术为主的方式。

(2) 三网主干均采用的是千兆以太网技术，起点的高定位为企业的信息应用带来了高速、稳定、符合国际标准的网络平台。

(3) 公司中心交换机采用的是CISCO的CATALYST6506，带有三层路由的引擎使得企业网具有将来升级的能力。同时各二级单位的中心交换机采用的亦是CISCO的CATALYST4006。

(4) 各二级、三级交换机采用的是CISCO的CATALYT3500系列的交换机，原因为CATALYST3500系列交换机的高性能和可堆叠能力。

2.2 需求分析

(1) 三部分应公司的要求联网，使公司能对其下属单位有着更好、更直接、更有效率的管理并实现信息共享。网络的互连仍采用千兆带宽，但因三网均采用千兆以太网技术，为了不在主干形成瓶颈，因此各子网的互连采用TRUNK技术，即双千兆技术，使网络带宽达到4G，既增加了带宽，又提供了链路的冗余，提高了整体网络的高速、稳定、安全运行性能。

(2) 但由于网络规模的扩大化，信息流量的加大，人员的复杂化等原因，为企业网络的安全性、稳定性、高效率运行带来了新的隐患。由此引发了VLAN的划分，解决了企业该系列的隐患问题。

(3) 对于VLAN的划分，应公司的需求，分为下列子网：

· 经理办子网

· 财务子网

· 供销子网

· 信息中心子网

· 其余划为一个子网

(4) IP地址范围为：192.168.0.0网段，所以对各VLAN的IP分配为：

· 经理办子网：192.168.1.0——192.168.2.0/22 GW: 192.168.1.1

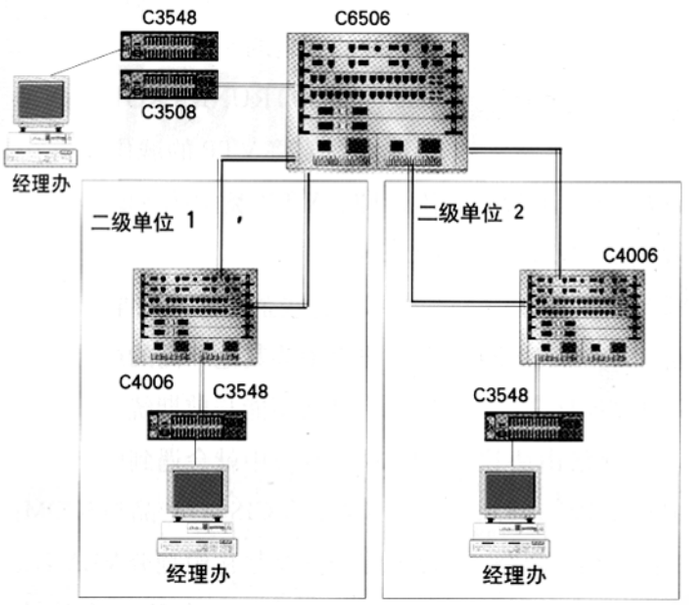
· 财务子网：192.168.3.0——192.168.5.0/22 GW: 192.168.3.1

· 供销子网：192.168.6.0——192.168.8.0/22 GW: 192.168.6.1

· 信息中心子网：192.168.7.0/24 GW: 192.168.7.1

· 服务器子网：192.168.100.0/24 GW: 192.168.100.1

· 其余子网：192.168.8.0——192.168.9.0/22 GW: 192.168.8.1



3 系统分析

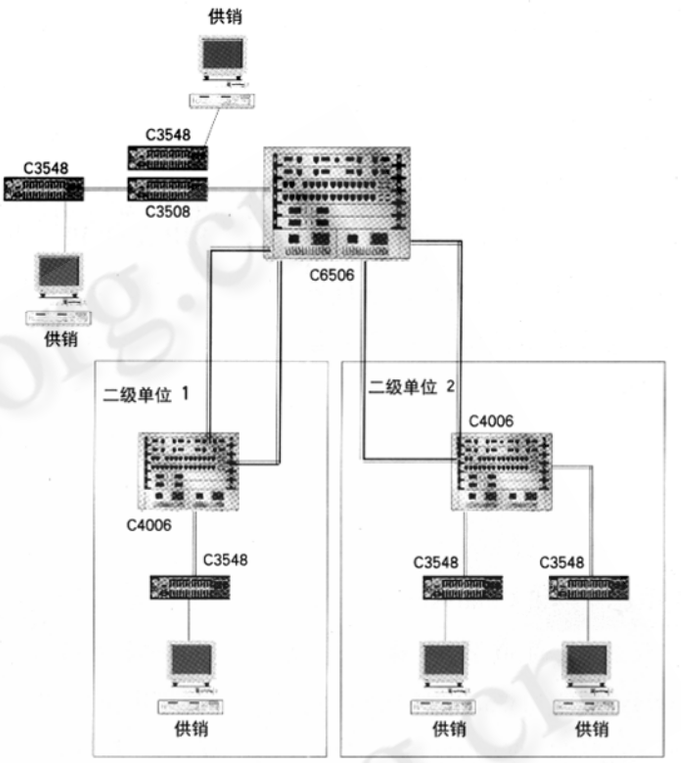
对于CISCO的产品划分VLAN主要是基于两种标准协议：ISL和802.1Q。ISL为CISCO自己研发设计的通用于所有CISCO网络产品的VLAN间互连封装协议，该协议针对CISCO网络设备的硬件平台在信息流的处理、多媒体应用的优化进行了合理有效的优化。而802.1Q协议则是IEEE802委员会于1996年发布的国际规范标准。

在这里我们所提到的案例中，因为所采用的均是CISCO的网络设备，故在进行VLAN间的互连时采用ISL的协议封装。对于不同产品的VLAN互连我们在后面会提到。

该系统分为三部分：分司、二级单位1、二级单位2，其各自有自己的网络系统。

公司中心交换机采用CISCO的Catalyst6506，其二级节点为Catalyst3508和Catalyst3548，Catalyst3508交换机具有8个千兆以太网，并且利用Catalyst3500系列交换机的堆叠能力，可以随时扩充工作站数量。边缘交换机采用有千兆模块的Catalyst3548。二级单位的中心交换机则采用了CISCO的Catalyst4006。其二级节点和边缘交换机采用的也是Catalyst3548。公司与各二级附属单位的连接采用ISL封装的TRUNK方式，以两组光纤连接(Catalyst6506与Catalyst4006之间)。如此既解决了VLAN间的互连，同时又提高了网络带宽、和系统的冗余，为三网互连提供了可靠保障。对于到Internet的连接，接口为公司的2MDDN专线接入。各二级单位亦通过公司的PROXY连接入Internet。Internet的管理由公司信息中心统一规划。

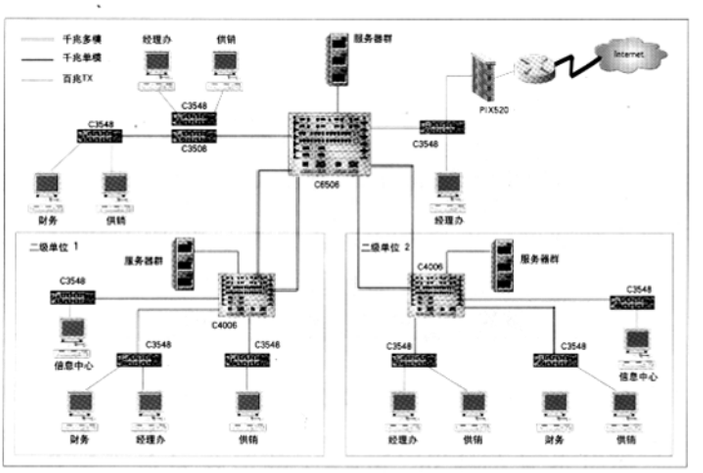
由于本案例中关于VLAN的划分扩展了各个交换机，所以交换机之间的连接都必须采用TRUNK的方式经理办和供销子网代表了VLAN划分中的两种问题：扩展交换机VLAN的划分和端口VLAN的划分，下面就经理办和供销虚网对各虚网做一介绍：



3.1 经理办虚网

由于经理办公工作站所在LAN交换机均有其他VLAN的工作站存在，即该交换机划分了多个VLAN，所以该交换机与其上层交换机之间的连接必须采用TRUNK方式：

- 公司Catalyst3508——Catalyst6506
- 二级单位1的Catalyst3548——Catalyst4006
- 二级单位2的Catalyst3548——Catalyst4006



3.2 供销虚网

对于一个交换机扩展多个VLAN的时候，前面提到了该交换机与其上层交换机间必须采用TRUNK方式连接，但在供销的虚网划分中，在二级单位1中的供销独立于一个LAN交换机Catalyst3548，所以在这里，Catalyst3548与二级中心交换机Catalyst4006只需采用正常的交换式连接即可，对于此部分供销VLAN的划分，只要在Catalyst4006上针对与Catalyst3548连接的端口进行划分即可。也就是前面提到的基于端口的VLAN的划分。

3.3 路由列表

上面对VLAN之间的连接我们已经做了阐述，因为两个Catalyst4006与主中心交换机Catalyst6506间采用的是双光纤通道式连接，屏蔽了Catalyst406与Catalyst6506间的线路故障的产生，所以对整体网络的路由进行基于Catalyst6506的集中式管理。下面我们对VLAN之间的路由做一个介绍。

在主中心交换机Catalyst6506上设置VLAN路由：

- 经理办虚网：192.168.1.1/22
- 财务虚网：192.168.3.1/22
- 供销虚网：192.168.6.1/22
- 信息中心虚网：192.168.7.1/24
- 其余虚网：192.168.8.1/22

在中心交换机上设置路由协议RIP或OSPF，并指定网段192.168.0.0。在全局配置模式下执行如下命令：

router rip

network 192.168.0.0

注意事项：

(1) 在这里需要注意的是：因为整个公司的网络系统的VLAN的划分是作为一个整体结构来设计的，所以为了保持VLAN列表的一致性，例如当二级单位1的VLAN有所变化时，二级单位的VLAN列表也会有所变化，这时就需要该Catalyst4006对整体网络的其他部分进行广播，以达到VLAN的列表的一致性。所以在设置VTP(VLAN TRUNK PROTOCOL)时要注意，要将VTP的域作为一个整体，即：VTP类型为SERVER和CLIENT。

(2) 有些企业建网较早，所选用的网络设备为其他厂商的产品，而后期的产品又不能与前期统一，这样在VLAN的划分中就会遇到些问题。

例如：在CISCO产品与3COM产品的混合网络结构中划分VLAN，对于CISCO网络设备的TRUNK的封装协议则必须采用802.1Q，以达到与3COM的通信。虽然两者之间可以建立VLAN的正常划分和正常的应用，但由于交换机都具有自学习的能力，以致两者之间的协调配合较差。当两者之间的连接发生变化时，必须在CISCO交换机上使用命令(clear counter)进行清除，方可达到两者的重新协调工作。■