基于第三层VLAN技术的园区网实现

陈基雄（华中科技大学计算机科学系 430074）
蔡 霞（华中师范大学计算机科学系 430079）

摘要：本文结合华中科技大学东校区校园网（Huazhong University of Science & Technology Eastern Part Network）的例子讨论了基于第三层VLAN的园区网实现技术。文章先对HUSTEPNET的方案进行了介绍，然后讨论了该校园网中基于第三层的VLAN划分和路由策略，并提出了使用变长子网掩码来划分第三层VLAN的方法。

关键词：VLAN 第三层VLAN 变长子网掩码

随着计算机网络在全球的发展，各大企业、学校、科研机构纷纷建立自己的Intranet。如何合理的安排网络体系结构成为网络界关注的一个重要课题。基于VLAN的网络体系结构能够改善网络性能，控制广播域，提高网络的安全性。然而，目前广泛使用的基于第二层的VLAN，不仅管理复杂、自动配置能力和可扩展能力差，同时由于不具备路由能力，必须通过代价昂贵的路由器来实现VLAN之间的通信。为了解决这些问题，人们提出了第三层VLAN的概念。基于第三层的VLAN是用协议类型(如果支持多协议)或者网络层地址(例如IP网络的子网地址)来定义VLAN成员资格的VLAN划分方法。在基于第三层的VLAN中，VLAN的交换是依据交换机本地信息来进行的，如根据交换和路由表、端口和地址高速缓存器以及配置数据等来进行交换。用于交换的信息和VLAN的业务流都是基于第三层信息的，基于第三层的VLAN还同时具备交换能力和路由功能。

1 方案简介

华中科技大学东校区校园网采用美国Xylan公司的交换机产品，在校园网内部实现全交换。主干交换机由1台OmniSwitch 9WX（位于网络中心）、5台OmniStack 5024和2台OmniStack 4024组成，5台OmniStack 5024交换机分别位于教学楼、图书馆、行政楼、力学馆、水工馆，2台OmniStack 4024交换机位于规划院和成教楼。主干交换机之间采用8芯多模光纤连接成以OmniSwitch 9WX为中心的星型拓扑结构。

2 基于第三层VLAN的划分

在划分VLAN之前，需要明确一点，即在设置基于IP地址的VLAN时，我们可以将处于不同IP子网的IP放在同一个VLAN中，也可以一个VLAN只包含一IP子网。由于在传统上人们习惯于在不同的IP子网间谈及路由，这样不同VLAN间的数据交换，就可以看作是数据在不同的IP子网间路由，易于理解和掌握，因此，我们采用后一种方法来创建基于IP地址的VLAN。

我们根据地理位置和应用的角度将HUSTEPNET中使用TCP/IP协议的主机划分为16个基于IP的VLAN。如表1所示，基于安全考虑，我们将所讨论的IP地址的前16位设为192.168。

2.1 使用变长子网掩码（VLSM）的VLAN划分

我们在192.168.96.0这个C类地址中，使用变长子网掩码（Variable Length Subnet Mask，VLSM）的方法，划分了8个VLAN，这主要是从充分利用IP地址空间和安全及灵活性上的考虑。VLSM可以在每个子网上保留足够数量的主机的同时，将一个网分成若干个子网具有更大的灵活性。如果不使用VLSM，一个子网掩码将只能提供给一个网络，这样就限制了子网上的地址空间而且降低了灵活性。同时，不使用VLSM，还会引起以下矛盾，即如果按照能得到足够的子网数来选择掩码，你将难以在每个子网上配置足够多的主机；对主机来说也是一样，允许足

够的主机数的掩码就不会提供足够的子网空间。

将192.168.96.0这个C类地址空间划分成8个VLAN时，根据现有设施和条件有如下几点要求：

（1）交换机与路由器VLAN。占用两个IP地址，供中心交换机和路由器使用。所有出入境业务量都必须通过该VLAN，因为该VLAN只有两台主机，所以可以进一步缩小广播域，减少因广播而增加的开销。

（2）管理VLAN。占用9个IP地址，供8台交换机管理和1台网管工作站的管理用。

（3）服务器VLAN。目前有3台主机，供WWW、DNS、FTP、E-mail服务用，以后随着应用的开展，服务器数量将有所增加。

（4）网络中心NIC（Network Information Center）部和NOC（Network Operation Center）各有两个VLAN，每个VLAN主机数预留为20台。

（5）培训中心有28台主机，供网络培训用。

表1 WHUCINET中基于IP的VLAN划分

VLAN	VLAN名称	网络号	子网掩码	虚拟路由器地址	描述
1	Switch-Router VLAN	96.4	255.255.255.252	96.5	WX与路由器
2	Management VLAN	96.16	255.255.255.240	96.17	管理VLAN
3	Server VLAN	96.32	255.255.255.224	96.62	服务器VLAN
4	NIC VLAN1	96.64	255.255.255.224	96.94	IC VLAN1
5	NIC VLAN2	96.96	255.255.255.224	96.126	IC VLAN2
6	NOC VLAN1	96.128	255.255.255.224	96.158	OC VLAN1
7	NOC VLAN2	96.160	255.255.255.224	96.190	OC VLAN2
8	Training Center VLAN	96.192	255.255.255.224	96.222	培训中心VLAN
9	Computer Center VLAN	97.0	255.255.255.224	97.254	计算机中心VLAN
10	Teaching Building VLAN	98.0	255.255.255.0	98.254	教学楼VLAN
11	Library VLAN	99.0	255.255.255.0	99.254	图书馆VLAN
12	Office Building VLAN	100.0	255.255.255.0	100.254	行政楼VLAN
13	Physical Building VLAN	101.0	255.255.255.0	101.254	物理楼VLAN
14	Dynamics Building VLAN	102.0	255.255.255.0	102.254	力学馆VLAN
15	Waterworks VLAN	103.0	255.255.255.0	103.254	水工馆VLAN
16	Educational Admin VLAN	104.0	255.255.255.0	104.254	教务管理VLAN

根据以上要求，我们需要把192.168.96.0这个C类地址空间分成8个子网，这些子网的主机数要求分别为：2、9、3、20、20、20、20、28。如果没有VLSM，可有两种选择：

① 使用掩码255.255.255.224，将地址分成各有32台主机的8个子网，但由于192.168.96.0～31和192.168.96.224～255分别作为使用该掩码时的网络号和广播地址，所以实际上可用子网数为6个。

② 使用掩码255.255.255.240，将地址分成各有16台主机的16个子网，其实际上可用子网数为14个。这两种选择显然都难以满足我们实际的需要。

因此，我们先用掩码255.255.255.224，将地址空间分为8个32台主机的子网，由于192.168.96.0～31是该掩码的网络号，所以我们再用掩码255.255.255.240将192.168.96.0～31分为2个16台主机的子网，而这样细分后192.168.96.0～15又是掩码255.255.255.240的网络号，故再使用掩码255.255.255.252将这16个地址为4个4台主机的子网。至此，已经可以全部满足我们提出的划分要求了。表2说明了如何按前所述划分地址空间。

表2 使用VLSM把网络地址空间划分为不同大小的子网

	4地址		16地址（掩码255.255.255.240）
		32地址	（掩码255.255.255.224）
		32地址	（掩码255.255.255.224）
		32地址	（掩码255.255.255.224）
		32地址	（掩码255.255.255.224）
		32地址	（掩码255.255.255.224）
		32地址	（掩码255.255.255.224）

VLSM的另一个优点是可在一定程度上防止IP地址的盗用，一般IP地址盗用是盲目的，若盗用者将IP地址改为该IP子网的一个IP后，由于它的子网掩码与VLAN中的定义不符，它将不能被该VLAN的自动成员识别算法所识别，因此不能上网。

在使用VLSM还应注意一个问题，即不是所有的路由协议都能处理VLSM，RIP I和IGRP（Interior Gateway Routing Protocol，内部网关选路协议，Cisco专用）在路由更新时不传送子网掩码，于是在处理VLSM划分的子网时存在问题。因此，应选用RIP II、OSPF、EIGRP（Enhanced Internet Gateway Routing Protocol，增强的因特网网关选路协议，Cisco专用）作为VLAN的路由协议。

2.2 跨主干的VLAN

在表1的VLAN中，教务管理VLAN是跨主干的，并且是根据实际应用来划分的虚网。基于本校区教务管理系统的开发与应用，教务科与各系教学秘书之间在网上进行教学计划的上报、考试成绩上报、教务通知下发等工作。该教务管理系统是在Netscape Livewire for NT平台下开发的，其服务器放置在教务科。各系教学秘书使用的计算机与该服务器在同一VLAN（教务管理VLAN）中，由于地理位置分布情况，该VLAN跨越了校园网主干。

以后我们将陆续开发教学管理相关的系统，如考试成绩连机查询系统、公共选修课报名系统等，进一步充分利用校园网资源。

在创建了16个基于IP地址规则的VLAN之后，我们又根据原有的Novell NetWare局域网划分了4个VLAN，以满足原有局域网上网需要。

出于安全考虑，我们还在划分VLAN的过程中使用了第二层VLAN与第三层VLAN相结合的划分方法。如财务处、组织部等部门（表6.1中未列出），必须严格防止非法用户侵入，因此，在划分VLAN时，先采用基于IP地址规则的划分方法，然后再给该VLAN加入另外两个规则--MAC地址规则和端口规则，将IP地址及MAC地址和交换机端口绑定，一定程度上防止了非法侵入。

3 VLAN的路由策略

我们在创建VLAN时已经定义了该VLAN虚拟路由器的IP地址，见表1。这个地址实际上是虚拟路由器端口的IP地址，在该VLAN内的所有IP，要实现跨VLAN的访问，都必须经过该路由端口进行路由。如计算机中心（VLAN 9）的一台主机X（IP地址为192.168.97.5），要访问服务器VLAN（VLAN 3）中的某服务器(192.168.96.33)，它的路由跳数将如表3所示。交换机发现主机X要访问的目的IP不在其同一VLAN，因此，将数据包传给主机X所在VLAN的虚拟路由器端口192.168.97.254，虚拟路由器查找路由表，发现目的IP属于服务器VLAN，因此将数据包转发服务器VLAN的虚拟路由器端口192.168.96.62，该端口再将数据包发给目的IP。

表3 路由实例

跳数	源IP	目的IP
1	192.168.97.5	192.168.97.254
2	192.168.97.254	192.168.96.62
3	192.168.96.62	192.168.96.33

为了减轻中心交换机的路由压力，保证路由的负载平衡，我们启用OmniStack 5024的第三层交换能力，使得整个校园网内部路由处于分布式路由状态。这样，本地交换机内部VLAN之间的数据交换可以不通过中心第三层交换机OmniSwitch 9WX进行路由，而直接在本地交换机上实现路由，减轻了中心第三层交换机的路由压力，进一步提高网络的性能。

在校园网的路由协议选择上，我们使用RIP II作为其路由协议。这不仅因为RIP II较RIP I有很大改进，而且由于我们使用了变长子网掩码划分VLAN，RIP I不能够解决子网掩码的传送问题。

同时，为了在路由中增强冗余度，我们在为VLAN设置路由端口后，给每一个VLAN加入了静态路由，由于虚拟路由器的路由表实际上是第三层交换机中所维护的路由表的一部分，所以，只须给交换机设置一条静态路由即可。如给图书馆5024的交换机增加一条静态路由，路由的源IP地址设置为0.0.0.0，下一跳（Next Hop）IP地址设置为192.168.96.17（中心交换机的虚拟路由器IP地址）。在原有链路失效的情况下，静态路由将会自动启用，增强了网络的稳定性。■

参考文献

1 Virtual LAN Communications, http://cio.cisco.com/warp/public/641/13.html

2 Cisco Systems Inc., ''Cisco VLAN Roadmap'', http://www.cisco.com/warp/public/538/7.html, Apr 15 1999

3 金培权，"第三层交换技术浅析"，微型机与应用，1998.12