维普资讯 http://www.cqvip.com

VLAN技术在校园网建设中的应用

杨永斌
(重庆工商大学计算机科学与信息工程学院　重庆400067)

摘　要　虚拟局域网(VLAN)不仅可以提高网络运行的效率,而且有利于网络安全和防止网络风暴,解决许多其他问题。第三层交换机的普及为VLAN的应用创造了条件。在实现网络升级改造中,采用VLAN技术可解决网络管理、扩容等问题,并可尽量发挥原有设备的作用,保护单位原有投资。本文详细探讨了VLAN技术在校园网建设中的应用。

关键词　虚拟局域网,网络,子网,校园网,策略,配置

The Application of VLAN Technique in Campus Network Building

YANG Yong-Bin
(College of Computer Science and Information engineer, Chongqing Technology and Business University, Chongqing400067)

Abstract　Virtual Local Area Network(VLAN)can not only increase the efficiency of network running, but also benefit network security and preventing network storms, and solve many other questions. The overreach of L3 switch creates the condition of VLAN application. In network upgrade and rebuilding, using VLAN technique can solve network management and network extending problem etc., and it can make the most use of inherence equipment, protect inhereance investment. The paper particularly discusses the application of VLAN technique in campus network building.

Keywords　Virtual local area network(VLAN), Network subnetwork, Campus network, Policy, Deploy

1　前言

校园网是高校实现数字化校园、现代化教学如无纸化办公、无纸化考试、远程教学等的基础。随着高校的不断发展及计算机应用系统的日益增加,高校的网络系统需要进行升级改造,以适应新的需求。在升级改造的过程中,传统的计算机局域网技术已难以适应业务发展的需要,VLAN技术为解决这一问题提供了一个很好的解决方案。并且随着网络硬件性能的不断提高、成本的不断降低,目前在校园网建设中,核心交换机都采用三层交换机,它能很好地支持虚拟局域网技术即VLAN,这对方便校园网的管理、保证校园网的高效可靠运行起到了非常重要的作用。

2　VLAN的定义

VLAN(Virtual Local Area Network)即虚拟局域网,是一种通过将局域网内的设备逻辑地而不是物理地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年颁布用于标准化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VLAN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。但由于它是逻辑的而不是物理的划分,所以同一个VLAN的各个工作站无需放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,即使是两台计算机有着相同的网段,如果它们没有相同的VLAN号,它们各自的广播流也不会相互转发,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,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,每个工作组就是一个虚拟局域网,其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。划分VLAN以后,各个VLAN之间是不能直接通讯的,它们之间的通讯需要由路由来完成,路由的实现可通过路由器或三层交换机来完成。

3　VLAN的优点

1.控制广播风暴。一个VLAN就是一个逻辑广播域,通过对VLAN的创建,隔离了广播,缩小了广播范围,可以控制广播风暴的产生。

2.提高网络整体安全性。通过路由访问列表和MAC地址分配等VLAN划分原则,可以控制用户访问权限和逻辑网段大小,将不同用户群划分在不同的VLAN,从而提高交换式网络的整体性能和安全性。

3.网络管理简单、直观。对于交互式以太网,如果对某些用户重新进行网段分配,需要网络管理员对网络系统的物理结构重新进行调整,甚至追加网络设备,增加网络管理的工作量。而对于采用VLAN技术的网络来说,一个VLAN可以根据部门职能、对象组或者应用将不同地理位置的网络用户划分为一个逻辑网段。在不改变网络物理连接的情况下可以任意地将工作站在工作组或子网间移动。利用虚拟网络技术,大大减轻了网络管理和维护工作的负担,降低了维护费用。在一个交换网络中,VLAN提供了网段和机构的弹性组合机制。

4　划分VLAN的策略及组建条件

从技术角度讲,VLAN的划分采取不同的原则或策略,一般有以下几种策略:

杨永斌　讲师,主要研究方向:计算机算法、计算机网络、数据库技术。

维普资讯 http://www.cqvip.com

基于端口的划分　这种划分是把一个或多个交换机的几个端口划分为一个逻辑组，被设定的端口都在同一个广播域中。例如，一个交换机的1、2、3、4端口被定义为VLAN1，同一个交换机的5、6、7、8端口定义为VLAN2。VLAN1、VLAN2内部的各个端口可以相互通信。这是最简单最有效的划分方法，配置过程简单明了。从目前来看，这种根据端口来划分VLAN的方式仍然是最常用的一种方式。

基于MAC地址的划分　MAC地址其实就是网卡的标识符，每一块网卡的MAC地址都是唯一且固化在网卡上的。MAC地址由12位16进制数表示，前8位为厂商标识符，后4位为网卡标识。网络管理员可以按MAC地址把每个主机配置到它所属的组。这种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它交换机时，不用重新配置VLAN。

基于路由的划分　路由协议工作在网络层，相应的工作设备有路由器和路由交换机(三层交换机)。该方式允许一个VLAN跨越多个交换机，或一个端口位于多个VLAN中。

基于IP组播的划分　IP组播实际上也是一种VLAN的定义，即一个组播组就是一个VLAN，这种划分的方法将VLAN扩大到广域网，因而具有更大的灵活性，而且也很容易通过路由器进行扩展，当然这种方法不适应局域网，主要是效率不高。

基于策略的划分　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。

基于用户定义、非用户授权的划分　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。

组建VLAN的条件：VLAN是建立在物理网络基础上的一种逻辑子网，因此建立VLAN需要相应的支持VLAN技术的网络设备。当网络中的不同VLAN间进行相互通信时，需要路由的支持，这时需要增加路由设备。要实现路由功能，既可采用路由器，也可采用三层交换机来实现。

5　应用实例研究

假设某校拟进行校园网改造，以实现数字化校园建设的需求，将行政办公室、教学系部、教室、网络服务器系统甚至教师、学生寝室统统纳入整个校园网系统进行集中统一规划和管理。在整个网络改造中要充分利用现有设备，并且各部门之间的访问有一定的规定和限制，还要考虑今后网络系统的扩容的需求。

1. 系统拓扑结构：假如系统原有CISCO 3512XL、CISCO 3548XL、CISCO 2924XL交换机三台，拟新购买CISCO 2948G-L3交换机一台。为了成功进行系统改造，自然想到使用VLAN技术。根据目前情况，系统网络拓扑结构如图1所示：

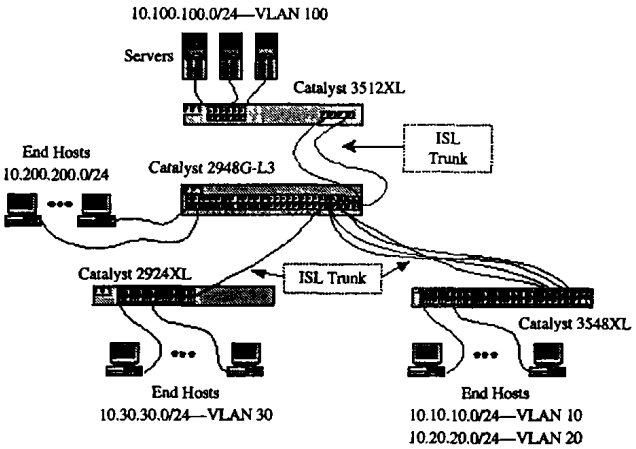

图1　系统拓扑结构

在此系统中，采用CISCO公司的2948G-L3交换机作为核心交换机，它提供了48个10/100M RJ45端口，2个千兆端口，每个端口均支持三层交换，它被配置成一个内部VLAN路由器。CISCO 2948G-L3和CISCO 3512XL之间通过两个千兆口相连，CISCO 2948G-L3和CISCO 3548XL之间用4个快速以太口相连，CISCO 2948G-L3和CISCO 2924XL之间通过一个快速以太口相连。整个系统划分成4个应用VLAN(VLAN10、VLAN20、VLAN30、VLAN100)和一个管理VLAN(即VLAN1)。

2. VLAN划分原则：根据系统需要，采用基于端口的划分方式，将不同部门的计算机划分在一个VLAN中。相应划分了四个应用VLAN：VLAN100包含了系统所有的服务器，VLAN10将行政办公室的工作站设在一个虚拟网中，VLAN-20主要是教学系部，VLAN30是教室、教室宿舍及学生寝食的专业虚拟网。

3. VLAN配置：根据以上划分原则，划分的四个应用VLAN如表1所示：

表1

VLAN号	应用系统	网络地址	掩码	VLAN地址	交换机端口
VLAN100	服务器	10.100.100.0	255.255.255.0	10.1.1.2	CISCO 3512XL(1-12)
VLAN10	行政办公室	10.10.10.0	255.255.255.0	10.1.1.3	CISCO 3548XL(1-24)
VLAN20	教学系部	10.10.20.0	255.255.255.0	10.1.1.3	CISCO 3548XL(25-44)
VLAN30	教室	10.10.30.0	255.255.255.0	10.1.1.4	CISCO 2924XL(1-23)

VLAN1(管理VLAN)的网络地址为10.1.1.0，VLAN地址为10.1.1.1。

为了对各交换机及VLAN进行管理，需对交换机进行一系列配置。如配置各交换机的基本信息：在Catalyst 3512 XL、3548 XL和2924 X交换机上，需定义VLAN1管理接口、IP地址和网关，设IP分别为10.1.1.2、10.1.1.3、10.1.1.4，掩码为255.255.255.0，网关均为10.1.1.1。还需定义VLANs、将交换机端口分配至各VLAN，以及对交换机间的以太网连接、交换机间的ISL Trunks连接和Catalyst 2948G-L3的Bridge进行相应配置，限于篇幅，其具体方法从略。

6　设置VLAN中的计算机

位于VLAN中的计算机，除了设置本网段的IP地址外，如果想访问其他VLAN或其他网段的计算机和网络设备，需

维普资讯 http://www.cqvip.com

要在计算机中设置默认网关，其网关为本 VLAN 的接口地址。例如 VLAN10中的计算机，其网关应设置为10.1.1.3，掩码为255.255.255.0。

结束语 VLAN 采用多种方式配置于各种网络中，包括网络安全认证、使无线用户在802.11b 接入点漫游、隔离 IP 语音流在不同协议的网络中传输数据等虚拟局域网(VLAN)的出现打破了传统网络的许多固有观念，使网络结构变得灵活、方便。

参 考 文 献

1 [美]Interconnecting Cisco Network Devices Volume 1[M]. 技术资料
2 [美]Louis D.Rossi,等著. 詹文军,等译. Cisco 与 IP 寻址[M]. 北京:机械工业出版社,1999
3 [美]Cisco IOS Desktop Switching Software Configuration Guide [M]. 技术资料
4 2900XL VLAN config. http://www.chinaitlab.com/www/news/article_show.asp?id=3003

(上接第40页)

用层使用，与数据包的丢失率无关。

TESLA 的优点是产生和认证信息的计算量小、通信耗费低、发送端和接收端的缓冲需求小和系统的健壮性强。而缺点在于在认证之前，接收方需要提供缓存空间。一但信息量太大，就可能造成接收方丢包的情况出现。另外，接收方对缓存的要求可能会导致 DoS、拒绝服务等攻击。福州大学的刘传才等人对这种方案进行了一些改进，使之能够支持立即认证，即包一到接收方就能认证。同时还提出了密钥链的优化方法以及导出了密钥显密延迟的严格下界，使 TESLA 方法更实用。

3.2 流认证方案

R. Gennaro 等人首先提出了流签字方案：将待发送的信息分成一些消息链，每条链由若干的包组成。发送方只需对每条链的第一个包签字，链内的每一个包包含了下一个包的密码杂凑值，用于验证下一个包。但这种方案必须要有可靠组播的支持。C. K. Wong 等人改进了流签字方案，可部分解决包丢失问题，但附加的信息导致认证效率不高。

Yongsu Park 等人提出了基于树链的高效流认证方案(ESAS)。这种方案将要发送的消息分为若干消息块(每 n 个消息块分为一组)，对于每 n 个消息块，发送方构造出一棵认证树。认证树的结构如图1所示。树中每个结点都对应一个值。其中，叶结点的值表示每个消息块的 hash 函数值，其他中间结点的值和它的儿子结点有关。例如，图1中的叶结点 $e_{0\text{-}0}$ 和 $e_{1\text{-}1}$ 分别对应消息块 M_0 和 M_1，分支结点 $e_{0\text{-}1}$ 的值则和 $e_{0\text{-}0}$、$e_{1\text{-}1}$ 的值有关。对于每棵认证树，发送方生成 n 个包(每个包由对应的消息块和根据认证树产生的附加值组成)，每产生一个包立刻发送给接收者。当一组的所有包都发送完以后，发送方再传输整个组的签字包。发送方对于下一个组又重复这个过程。当接收方收到某一组的签字包和这组中的某些消息包后，就可以进行认证了。

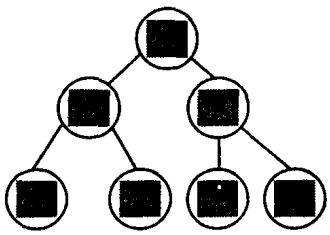

图1 ESAS 中的认证树

和 R. Gennaro 的方案相比，在通信量相同的情况下，ESAS 有更高的验证概率和较低的通信成本。而和 C. K. Wong 提出的方案相比，ESAS 的通信量和计算量更低，在特定的情况下，它的验证概率接近1(C. K. Wong 方案的验证概率为1)。

3.3 基于不对称消息认证码 MAC 的认证技术

MAC 技术是指用一个密钥生成一个小的数据块追加在消息的后面发送。它的前提条件是假定通信双方共享一个密钥 K。由于 MAC 不会进行类似加密过程的反向计算，所以这种鉴别是较难攻破的。但通信双方共享单密钥的方式不适合进行组播源认证，任何拥有密钥 K 的可能接收者都可以假冒发送者发送消息。

R. Canetti 等人提出了一种不对称的 MAC 认证方法(如图2所示)。它使发送者拥有所有接收者的密钥集合，每个接收者和发送者共享其中的一个子集。发送者根据每个接收者的密钥生成一个 MAC 值，将这些 MAC 值附加在消息上一起发送，而接收者则用他所拥有的密钥验证对应的 MAC 值。如果这些 MAC 值不正确，接收者就拒绝接收这一消息。

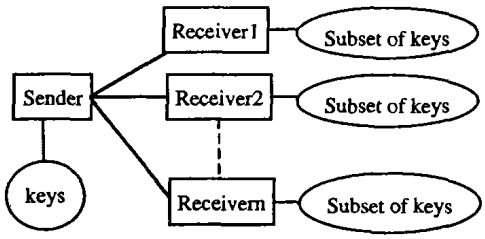

图2 不对称的 MAC 认证

在基于不对称消息认证码 MAC 的认证技术中，如果一个接收者不知道其他接收者的密钥，则无法伪造 MAC 进行欺骗。和公钥签名相比，这种认证方法可大大缩短签名时间，验证时间和优化的 RSA 公钥签名类似。但这种方案没有提供抗抵赖服务，而且需要安全的密钥分配技术的支持。

结束语 组播源认证是组播通信面临的主要安全问题之一。在组播源认证的解决方案中，很多方案都只考虑了单一发送者的情况。但在组播的实际应用中，很多时候组播的发送者是动态变化的，组成员即可能是消息的发送者，也可能是消息的接收者。这是我们在设计组播源认证方案时应该进一步考虑的问题。另外，要更好地解决组播源认证，还需要和其他相关技术、协议联系起来，如密钥管理方案和可靠组播协议等。

参 考 文 献

1 Perrig A, Canetti R, Tygar J, Song D X. Efficient authentication and signing of multicast streams over lossy channels. In: IEEE Symposium on Security Application Conference, 1997
2 Perrig A, Canetti R, Tygar J, Song D. The tesla broadcast authentication protocol. RSA CryptoBytes, Summer, 2002,5
3 Gennaro R, Rohargi P. How to sign digital streams. In: Burton. S, Kaliski, J eds. Advancesin CryptologyCRYPTO'97, Berlin: Springer-Verlag, 1997
4 Wong C K, Lam S S. Digital signatures for flows and multicasts, In: Proc. of IEEE ICNP'98, Oct. 1998
5 谢希仁. 计算机网络. 电子工业出版社,1999