虚拟局域网VLAN在企业网管理的应用思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_99_9A_E6_8B_9F_E5_B1_80_E5_c101_644010.htm 1.VLAN介绍 所谓VLAN 是指处于不同物理位置的节点根据需要组成不同的逻辑子网，即一个VLAN 就是一个逻辑广播域，它可以覆盖多个网络设备。VLAN 允许处于不同地理位置的网络用户加入到一个逻辑子网中，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。同一个VLAN 中的端口可以接受VLAN 中的广播包，别的VLAN 中的端口则接收不到。 2. VLAN在网络管理中的应用 该集团公司下属公司多，业务种类多，根据业务发展需要，经过认真规划，将联网后的统一网络划分为30个VLAN。划分原则为：集团本部以楼层为单位进行VLAN 划分，各下属公司以业务的不同来划分VLAN，不同的VLan具有不同的安全级别。其中生产用机及各种服务器所在的VLAN 具有的安全级别较高。同时利用Cisco 6509自身的访问控制功能，设置访问列表对特定的VLAN用户进行保护，对特定的端口 135、445、1434等进行控制，保证了整个网络中各个VLAN 用户的安全隔离。VLAN划分的有4种策略：基于端口的VLAN划分、基于MAC地址的VLAN划分、基于路由的VLAN 划分、基于策略的VLAN 划分。该集团采用的方式是基于端口的VLAN划分的方式。 基于端口的VLAN划分是最简单、最有效的划分方法。该方法只需网络管理员对网络设备的交换机端口进行重新分配即可，不用考虑该端口所连接的设备。在交换机投入运行前就把它的物理端口根据需要划

分给指定的VLAN 并分配给用户。这种划分使网络管理员能够随时掌握网络的负载情况，有利于网络的优化使用，并具有较高的安全性，虽然在一定程度上增加了管理员的工作量。举例来说，集团下属公司分布在不同城不同的地理位置，但考虑到方便管理，这些公司的OA服务器均使用一个VLAN的IP.对需要其他权限的OA服务器单独分配其他网段的IP，所有这些网络应用的实现均是依靠基于交换机端口VLAN 的划分来实现的。另一方面，对静态VLAN 技术的应用(即基于端口的VLAN 划分)来说，交换机不能分辨出被盗用IP地址的非法接人。一个用户盗用同一子网某特权用户的IP地址后就可以伪装成这个VLAN 的特权用户，非法访问网络中的服务器，并造成IP地址的冲突。为了解决这个问题，就利用用户一般不会改变计算机MA C地址的特点，采用了对大部分用户的IP地址和MA C地址与交换机端口绑定的方法， 弥补了静态VLAN 的这一缺陷，有效地防止了这种情况的发生。满足了对不同VLAN设置不同访问权限，那么VLAN与VLAN之间又是如何实现相互间的访问呢? 在一般的二层交换机组成的网络中，VLAN 实现了网络流量的分割，不同的VLAN 间是不能互相通信的。要实现VLAN 间的通信必须借助：1)路由器来实现.2)三层交换机。下属公司采用的是使用三层交换机的方式。利用三层交换机实现VLAN 间通信，三层交换机是将第二层交换机和第三层路由器两者的优势有机而智能化地结合起来，可在各个层次提供线速性能。三层交换机内，分别设置了交换机模块和路由器模块.而内置的路由模块与交换模块类似，也使用ASIC硬件处理路由。因此，与传统的路由器相比，可以实现高速路由。并且，路由与交换模块是汇聚链

接的，由于是内部连接，可以确保相当大的带宽。用三层交换机的路由功能来实现VLAN 间的通信。 核心交换机选用Cisco 6509三层交换机，接人层交换机选择了Cisco 3750和Cisco 2950系列交换机，其中Cisco 3750交换机为带路由功能的三层交换机，用于数据流量较大的分局，而Cisco 2950为二层交换机，主要用于通过千兆光纤与中心交换机的直接连接，通过这样的连接方式，整个局域网就能很好的协同工作。VLAN 对于网络使用者来说是完全透明的，用户感觉不到使用中与交换式网络有任何的差别，但对于网络管理人员则有很大的不同，因为这主要取决于VLAN 的几点优势。 (1)控制广播风暴 网络管理必须解决因大量广播信息带来带宽消耗的问题。VLAN 作为一种网络分段技术， 可将广播风暴限制在一个VLAN 内部，避免影响其他网段。与传统局域网相比，VLAN 能够更加有效地利用带宽。在VLAN 中，网络被逻辑地分割成广播域，由VLAN 成员所发送的信息帧或数据包仅在VLAN 内的成员之间传送，而不是向网上的所有工作站发送。这样可减少主干网的流量，提高网络速度。 (2)增强网络的安全性 共享式LAN上的广播必然会产生安全性问题，因为网络上的所有用户都能监测到流经的业务，用户只要插入任一活动端口就可访问网段上的广播包。采用VLAN提供的安全机制，可以限制特定用户的访问，控制广播组的大小和位置，甚至锁定网络成员的MA C地址，这样，就限制了未经安全许可的用户和网络成员对网络的使用。 (3)增强网络管理 采用VLAN技术，使用VLAN管理程序可对整个网络进行集中管理，能够更容易地实现网络的管理性。用户可以根据业务需要快速组建和调整 VLAN。当链路拥挤时，利用管理程序

能够重新分配业务。管理程序还能够提供有关工作组的业务量、广播行为以及统计特性等的详尽报告。对于网络管理员来说，所有这些网络配置和管理工作都是透明的。VLAN 变动时，用户无需了解网络的接线情况和协议是如何重新设置的。另外在使用VLAN 划分后，也较好的解决了客户机随意使用IP地址的问题，因为某台计算机是属于某个特定的VLAN的，如果设置其他VLAN的IP地址，则是不能接人局域网的。3结语 局域网通过使用VLAN 划分技术，在安全性和稳定性方面都有了很大的提升，为各种业务的开展提供了可靠的保证，总之VLAN技术在集团公司网络管理中的重要性是不容忽视的。 