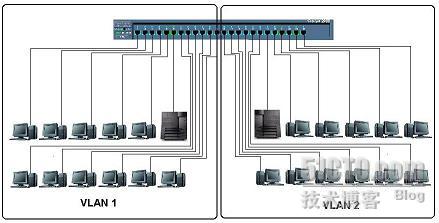
<http://liuxh.blog.51cto.com/225067/42345>

不把這麼多的計算機都放在一個網段中。原因有以下幾點：(1) IP地址衝突會把網管搞得暈頭轉向，而動態分配IP地址又會產生大量的廣播包，導致網絡傳輸效率下降。(2)任何網卡的損壞，都可能導致網絡風暴的發生，從而導致網絡癱瘓。(3)各種網絡協議被廣泛使用，導致網絡內充斥大量的廣播包，大大降低網絡的有效帶寬。(4)任何用戶都可以直接訪問所有的計算機，使惡意攻擊變得易如反掌，網絡沒有任何安全可言。

**一、什麼是VLAN**

虛擬網技術(VLAN ，Virtual Local Area Network)的誕生主要源於廣播。廣播在網絡中起著重要的作用，如發現新設備、調整網絡路徑、IP地址租賃等，許多網絡協議都要用到廣播。然而隨著網絡內計算機數量增多，廣播包的數量也急劇增加，當廣播包的數量占通訊總量30%時，網絡的傳輸效率將明顯下降。所以當局域網內的計算機達到一定數量後(通常限制在150~200台內)，通常採用劃分VLAN 的方式將網絡分隔開來，將一個大的廣播域劃分若干個小的廣播域，減小廣播造成的損害。

如何分隔廣播域呢？最簡單的方案是物理分隔，將完整的網絡物理地分隔成多個子網絡，再通過一個能夠隔離廣播的路由設備連接彼此。除物理分隔外，就是在交換機上採用邏輯分隔的方式，將一個大的局域網劃分為若干個小的虛擬子網(如圖2)，即VLAN，使每個子網都為一個單獨的廣播域，子網間通信通過三層設備。當VLAN在交換機上劃分後，不同VLAN 間的設備就如同是被物理地分割。也就是說，連接到同一交換機、然而處於不同VLAN 的設備，就如同被物理地連接到兩個位於不同網段的交換機上一樣，彼此間的通信要經過路由設備，否則他們間將無法得知對方的存在，將無法進行任何通信。

圖2劃分VLAN

**二、VLAN的重要意義**

VLAN 中的成員與其物理位置無關，可連接至同一台交換機，也可連接至不同交換機。

● 降低移動和變更的管理成本: 使用VLAN，當要把計算機從一個子網移到另一個子網時，只需在交換機上重新定義VLAN成員即可。尤其採用MAC地址動態劃分VLAN時，當用戶將計算機從一個交換機端口移動到另一個交換機端口，由於其網卡的MAC地址並不改變，所以交換機能夠自動跟踪該終端的MAC 地址，並自動將其納入定義的VLAN 中。

● 控制廣播: 所有的廣播都只在本VLAN 內進行，不會擴散到其他VLAN上，避免產生廣播風暴及在整個網絡的蔓延。

● 增強安全性: 交換機只能在同一VLAN內的端口間交換數據，不同VLAN的端口不能直接相互訪問。同時可在Trunk(中繼)中設置允許訪問的VLAN，限制未經允許的VLAN 訪問，保證VLAN只被授權的用戶訪問。

**三、VLAN的劃分方式**

對於新型的第二層交換器而言，VLAN堪稱近年來最重要的技術發展，大幅提升了網路管理的彈性及效能，尤其可大幅降低使用第三層路由通訊協定的必要性。

**VLAN的實作方式**

雖然VLAN一開始是針對第二層發展的技術，現在也逐漸延伸至第三層的應用。目前第二層以上的VLAN沒有業界標準，靠各廠商自行研發。802.1Q規格提供連接(Trunk)多臺交換器的VLAN功能，使橫跨多臺交換器的VLAN架構有可行性。  
劃分VLAN有多種方式，但使用最多的仍是基於端口的VLAN。不同廠商的交換機大多支持以下幾種VLAN 的劃分方式：

**Port-based VLAN**  
最簡單的實作方式，將交換器的連接埠指至特定的VLAN之中，如16埠交換器，可將8埠指定為「iThome」，另8埠為在同層樓的「PC Shopper」。假如有其它的集線器或交換器連結至對應特定VLAN的連接埠，也會成為該VLAN的一部分。管理者必須紀錄每個埠和VLAN的對應，而且如果將某臺電腦更換連接埠，也需要重新的設定。

**MAC Address-based VLAN**

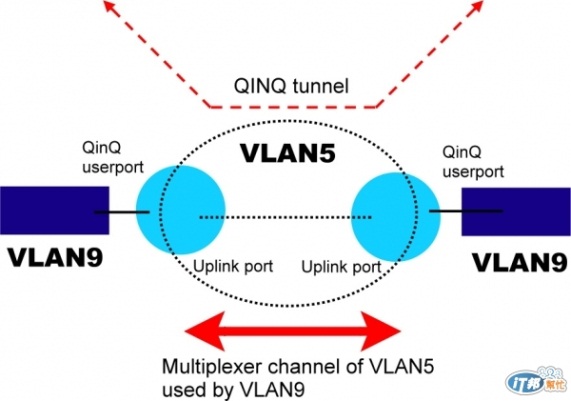
每張網卡都有獨立的MAC位址。透過紀錄每個MAC位址對應的VLAN，就算更動電腦的位置，也不要重新設定交換器，這對管理大量行動工作者相當的便利。不過缺點也很明顯，管理者要手動輸入每個MAC位址，尤其當網路卡或電腦發生故障或是被置換的時候，這都會造成管理上的困難。

**Tag-based VLAN**  
Tag-based VLAN在每個框包增加額外的欄位，指定不同的VLAN號碼，每個框包就屬於其指定的VLAN。目前Ethernet的VLAN標準802.1Q就是Tag-based VLAN。Tag-based VLAN實作上簡易、便於實作高數量及高效能的VLAN外，另一個優點在於便於達成某種程度的QoS，讓每個VLAN擁有不同的傳輸優先權。

**L3 Protocol-based VLAN**  
在一個區網內，可能有不同電腦執行不同的第三層通訊協定，所以可針對不同的通訊協定產生不同的VLAN，例如負責連外的Windows NT檔案伺服器採用IP，而負責對內的Novell Netware伺服器採用IPX，同時執行IP/IPX的用戶端則同時加入兩組VLAN。這樣做的優點是，除了只要不更動通訊協定即可任意更換實體位置，可針對不同的應用作網路頻寬的彈性規劃。不過判斷第三層通訊協定是消耗運算能量的工作，會降低交換器的效率。

**VLAN的限制**  
VLAN雖提升網路管理的彈性，不過對於提升網路效能卻有商榷的空間。當初VLAN技術發展有一個前提：80%的網路流量來自內部區網，而20%的流量則來自外部網路。隨著網際網路的興起，這個趨勢已經完全顛倒：往往80%的流量是對外的。在這種情況下，將不同需求的電腦組群化、使其共享資源的好處就已經消失大半，唯一比較明顯的好處就在於限制廣播風暴的影響。當然，不同的企業也會有不同的情況，像ISP可能如此，但金融業就大相逕庭。不過，基於管理上的優勢和彈性，VLAN對於企業網路依然有相當程度的貢獻，也勢必繼續扮演吃重的角色。

**QinQ VLAN簡易介紹**

QinQ VLAN簡略應用圖  
QinQ VLAN(IEEE802.1Q VLAN tunnel)是VLAN透過隧道穿越中間的VLAN到達另一個VLAN。IEEE802.1Q tag VLAN最多只能設定4096個group，但是透過QinQ VLAN，可設定到4096x4096個group。QinQ最明顯的特徵就是封包除了有4byte的tag標記外，又增加了4byte的tag標記，等於有2個Tag標記，其中一個標記就像是穿過隧道的通行證，而另一個標記就是另一個VLAN的門票。  
簡而明知的說QinQ是指將用戶內網 VLAN tag標記封裝在外網 VLAN tag標記中，使封包帶著兩層VLAN tag標記穿越ISP的骨幹網絡，在外網中只根據外層VLAN tag標記傳播，內網VLAN tag標記則被屏蔽。

不僅對封包進行了區分，而且由於內網VLAN tag標記被透明傳送，不同的用戶VLAN tag標記也能重複使用，只需要外層 VLAN tag標記在外網上的惟一即可，實際上也擴大了可利用VLAN tag標記的數量。  
在校園網絡中，可以根據這個原理，採用雙層VLAN tag標記技術構造多個的VLAN，實現用戶認證前port隔離和VLAN的隔離，從而達到有效減少廣播流量的目的。  
