

淺談校園網路設計與應用

國立岡山高中

郭銘哲

一、前言

隨著網路技術及各項應用的不斷發展校園網路所必須涵蓋的使用範圍也越來越廣。而很不幸的是在一般中等以下學校(包含高中職)並沒有專職的網路管理人員。因此在校園中往往被界定為具備較佳的網路背景知識的人員就是資訊科的任教老師，也因此往往大家就必須兼任網管的工作。

但是網管的工作卻隨著網路功能的不斷增加及使用校園網路作為傳輸媒介的功能與設備日益增加而使得複雜度不斷升高，因此關於網路設計與相關應用就很值得討論囉!!以下就是個人的一些經驗談與淺見就教於各位先進。

二、常見校園網路應用

(一)Internet

網際網路(Internet)大概是校園中被需求度最高的網路服務，幾乎所有的個人電腦連上網路的主要目的就是使用網際網路的服務及存取網路資源。網際網路上常用的服務不外乎 WEB、FTP、E-MAIL 與即時通訊軟體等，只要有適當的頻寬規劃這些相關服務基本上都可以運作的很正常。

但是網際網路服務卻必須面對日益嚴重的攻擊事件，包括病毒攻擊、駭客入侵、網路釣魚、等日新月異的網路安全問題。而這些問題也已經不是傳統防火牆所能夠阻止或是對抗的。所幸相關網路設備廠商也不斷研發新的設備作為因應之道，例如日前頗為盛行的 UTM 設備就企圖以防火牆為基本功能加上入侵偵測、防毒、甚至網頁過濾等功能企圖畢其功於一役，一直到近期針對 Layer7 以網路行為做管控的設備則大為興起，於由於同樣以 80 port 或其他公用連接埠作為網路通訊及攻擊的軟體與模式越來越多，使得單純以連接埠作為偵測依據的方式已經不夠而必須進一步以網路行為作為判斷依據以辨識該行為是否為合法（允許）的網路通訊，而非攻擊或入侵。

(二)Intranet

企業(校園)內部網路(Intranet)所需提供的各項服務經常被視為理所當然，但是卻經常被忽視其對於網路管理的影響，一般的使用者往往僅在意 Internet 的服務是否順暢卻不了解 Intranet 所提供的服務內容及網路管理往往才是影響網路使用效率及生產效率的關鍵。特別是當我們越是對於校園 E 化的要求與依賴日深內部網路的管理與使用效益對於生產力(教學支援度)的影響就越大。以下則對於常見的校園網路服務做討論。

1.網路列印

網路列印也是另一項必備的網路服務，近年來所推出的印表機幾乎都內建網路列印伺服器，因此印表機也成為另一項必需佔用 IP 資源的網路服務。

2.圖書查詢系統

圖書查詢(管理)系統是另一項傳統但是網路使用日益吃重的服務項目，早期的圖書館查詢(管理)系統的使用僅限於有限範圍的區域網路(如圖書館內部)但是隨著網路普及不論是大專或中小學幾乎都要求必須能夠在校園內的任何網路端點可以進行館藏查詢的功能。因此圖書查詢系統也成爲另一項重要的網路服務。

3.網路電話

這裡所指的是校園內部所使用的內線電話，隨著網路日益普及且由於網路的擴充性即可操作性較傳統電話交換機更爲簡易且功能更多，加上對於管理單位而言更爲容易控管。因此有越來越多的使用者將傳統的校園分機更改爲以內部網路(RJ-45 佈線)爲主，實際上各大網路通訊設備(如 Cisco、Alcatel 等)也都積極拓展此一領域的產品。由於新一代的網路電話已經可以和現有區域網路完整的結合並且共用許多設備因此建置完整的內部網路電話服務門檻已日益降低(但是話機的價格依舊很高)

4.VOD&MOD

VOD 或 MOD 雖然發展的很早但是由於在一般中小學校內由於可供撥放影片的公用電腦不足，因此一直難以在課程教學之外成爲學生自行觀看吸收知識的管道，當然另一方面是是否校園內部能夠提供適當或具吸引力的內容也是另一項重要因素。但是隨著班級電腦日益普及的情況下，校園內部觀賞 VOD 或 MOD 影片將不再僅止於教師於課堂上的教學用途。相對的其所帶來的串流訊號流量也將大爲增加。

5.校園安全監控系統

傳統的校園監控系統皆是以攝影機經由專用纜線(cable)將訊號回傳至監控主機，再經由監控主機將所拍攝之訊號加以儲存、顯示在監控螢幕上，甚至進一步由監控主機的網路連接埠接上現有內部網路，供使用者藉由網路端點隨處進行相關監控工作。但是新一代的網路監控系統將介由目前各單位普遍佈線密度最高的網路系統，讓各設別攝影機直接以 RJ-45 的端口與線路介接上鄰近的網路交換器(switch)，甚至是 POE 交換器更可直接省去電力配線的佈線工程，大幅降低建置成本。另一方面藉由無線訊號將監視器畫面進行傳送的方式也日漸普及對於校區範圍較爲廣大闊的校園在偏僻區域的使用具有極大的優勢。不論哪一種方式傳輸方式新一代網路安全監控系統在搭配已成爲網路節點的監控主機在整合大型網路儲存系統後將可更有效率的進行安全監控系統的管理。

6.校園電力監控系統

隨這地球暖化及氣候變遷的問題日益升高，節能減碳的需求也日益重要。因此各國紛紛發展電力監控，利用電腦網路的即時性與分佈密度對電力使用設備進行監控，藉由內部網路將各項監控數據自動傳回能源監控系統主機，並且可以在適當的營運規則下進行自動啓閉的功能，以達到節省能源之功效。

7.校園無線網路服務

校園無線網路也是已發展多年且臻於完善的網路系統，且日益普及，幾乎所有的校園都具備有無線上網的熱點，甚而可進行無線漫遊。但是無線網路由於較難進行完整安全防護所以是另一項隱憂。

8.校務行政系統

校務行政系統可以說是校園 E 化最初始的推手，不論是學籍系統、排課系統、社團管理、電子公文系統等皆是推動一波波校園 E 化的主要力量之一。但是現行多數校務行政系統相關系統隨著潮流的演進最終將逐步整合(例如 NAS、甚至 Google 文件共享)以達成進一步的資料整合。並且藉由「資料採礦」(例如藉由學籍系統進一步建立與分析學生學習成就與各項相關因素之間的關係與分析、或是不同科目間的學習成就之關連性)。推而廣之甚至包括教師教材的統合、互相引用及共同開發等皆可藉由整合性的系統管理進一步達到將教材與予以模組化，校內大型題庫的建立更是可以達到相互觀摩之效。並可做為新進教師之教育訓練教材。

9.其他應用服務(郵件服務、網路儲存)

郵件服務是各項網路服務中最基本之項目，但是由於近年垃圾郵件與病毒郵件的大量產生嚴重影響郵件系統的運行效率，以及使用者永遠嫌不夠的郵件空間需求下，郵件主機的服務逐漸由內部自行管理郵件主機改變成利用外部主機所提供的免費空間(最主要是 Google APPS)成為解決方案的選擇之一。但是對於必須進行內部郵件過濾的單位則相對不是那麼方便。

網路儲存是另一項在為來有極大成長空間的網路服務，但是一般的網路儲存設備不論是 NAS 或 SAN 對於一般中等學校都是不小的負擔，但是當資料必須被統一儲存時網路儲存是一項必要的選擇，但是唯有資料的整合與共享才能夠突顯網路儲存系統的價值，因此單純的作為各項系統的備份空間對於網路儲存系統並不能突顯其價值，而是奠基於資料共享與整合功能之效的網路儲存才能夠發揮其真正的效益。事實上就如同原端運算一樣，也許為來經由外部網路服務系統商所提供的網路儲存服務會取代目前機關內部自行建置的方式成為網路儲存的主流。其他如

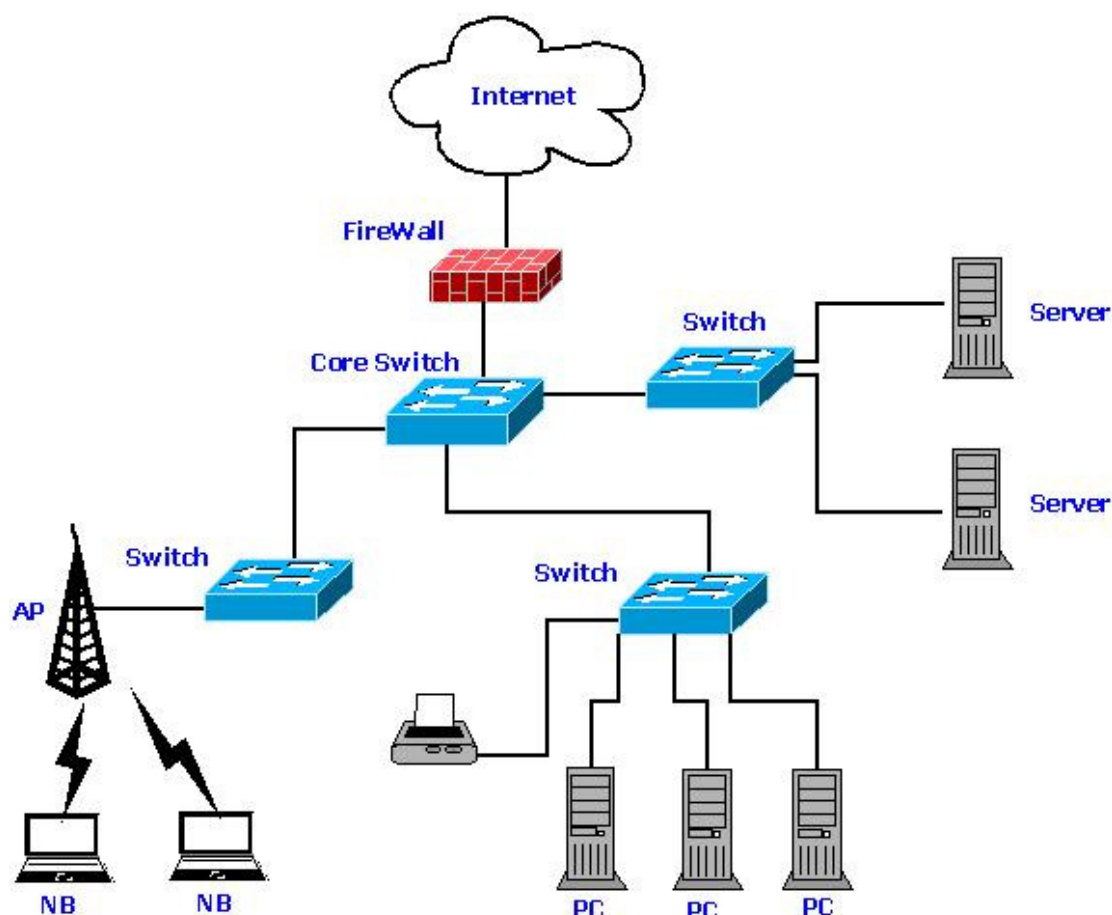
Google 所提供的「協作平台」專業版則可視為是一種另類的網路儲存系統，它同時具備超大儲存空間(25G)又可進行文件的共享與協作對於小型團體剖具吸引力，缺點是其對於超大型檔案如硬碟的映像檔(ISO)是無法儲存於其上的。

三、常見校園網路規劃類型

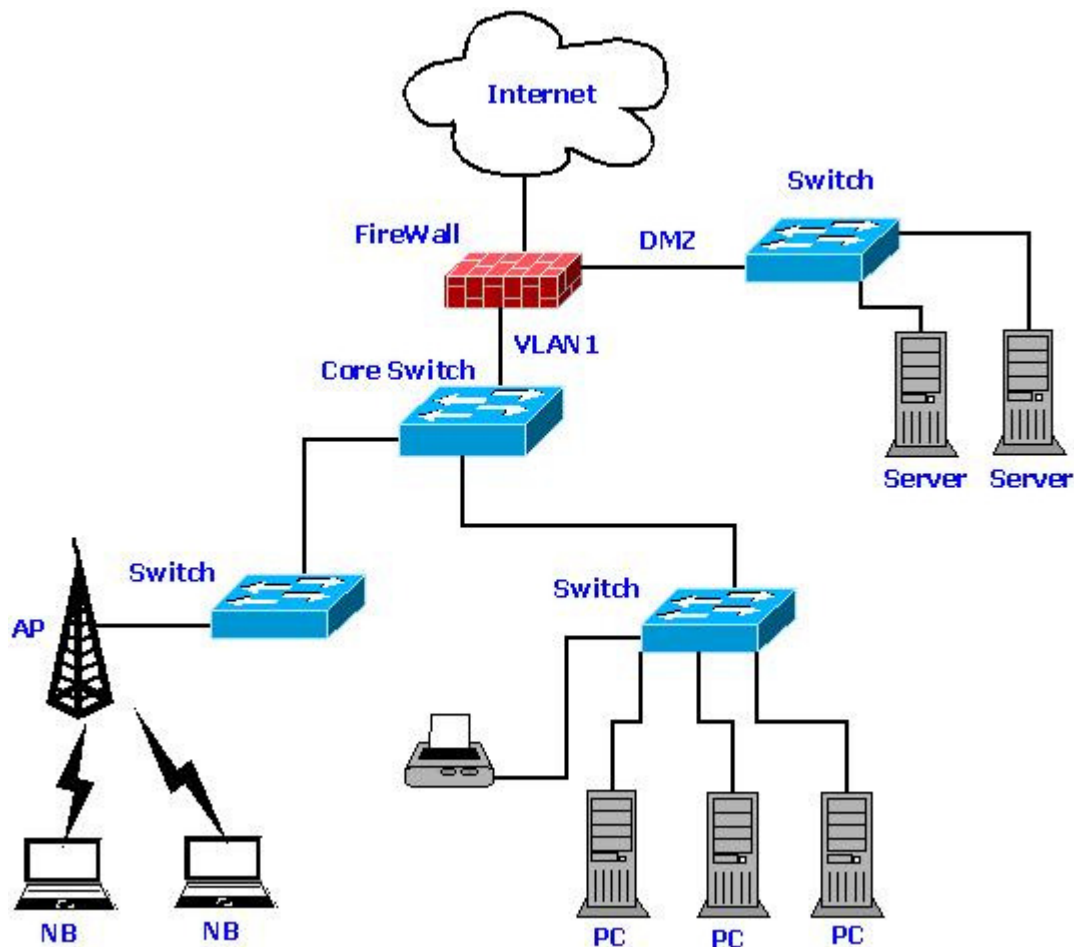
在討論完各項常見校園網路服務之後，藉由常見於校園的網路配置來思考如何將各項服務融入其中，討論其可能產生的優缺點。

(一)單一 C 級 (Class C) 網路

單一 C 級網路常見於多數的學校，特別是規模不大的學校幾乎都是以一個 C 級網路作為網路規劃的依據與使用範疇。其基本的設定也最為單純簡單，依照使用的需求又可區分為下列兩種形式。1.具備 DMZ 區域放置公共服務伺服器，並建置虛擬網段供內部網路使用。2.所有設備皆放置於內網並無 DMZ 區及虛擬網段供內部網路使用。分別圖示如下：



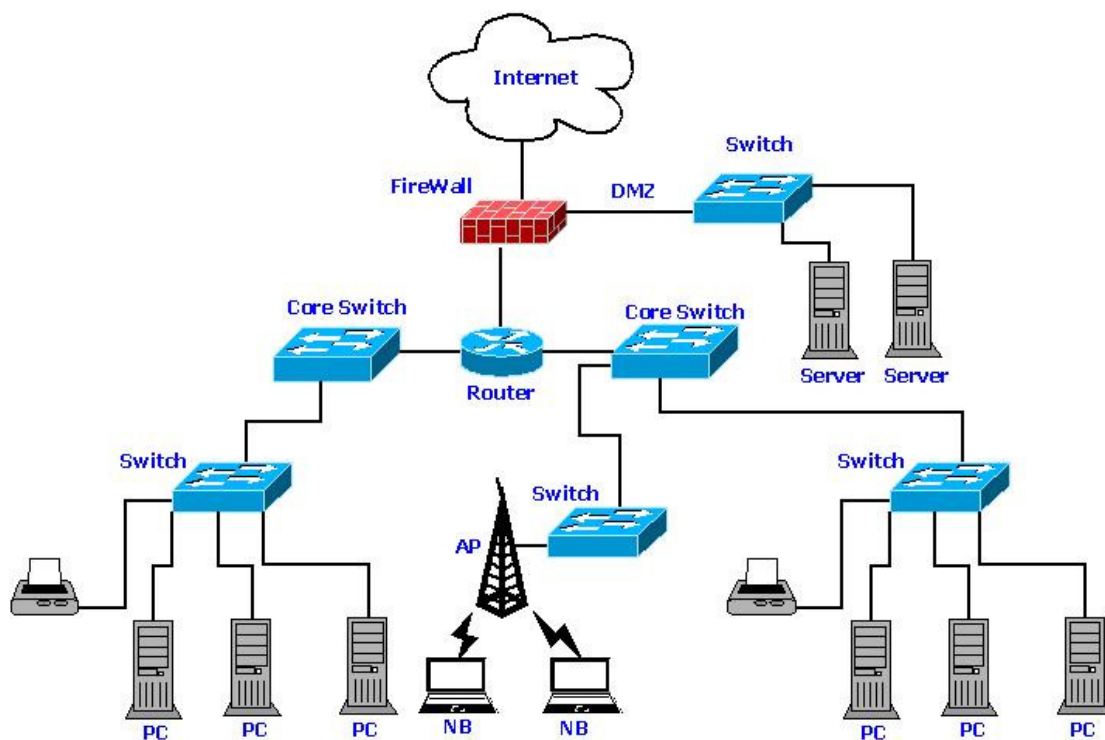
本圖中的所有網路設備皆直接賦予實體 IP 並以一個 Class C 為所以為使用原則，包括公用網路服務伺服器(WWW、E-mail 等)皆置於內網中。但是在此一方案下，容易造成 IP 不足的情況以及內部 PC 容易對公用網路服務伺服器發動攻擊。



雖然同樣以一個 Class C 為使用限度，但是藉由防火牆及核心交換器(Core Switch)設定一內部網路 VLAN 將公用網路服務伺服器以 DMZ 的方式做區分，可同時讓公用網路服務伺服器區隔於內外網路，減低遭到內部 PC 攻擊的風險。

(二) 多個 C 級網路

一般多見於較大型的學校或是高職等。兩個 C 級網路之間需使用 Router(或具備 Router 功能的 Layer3 Switch) 做互相連結與封包的轉送。同樣依照使用的需求又可區分為下列兩種形式。1.具備 DMZ 區域放置公共服務伺服器，並建置虛擬網段供內部網路使用。2.所有設備皆放置於內網並無 DMZ 區及虛擬網段供內部網路使用。但是具備多個 C 級網路的單位較少因此在此不做詳細討論。



(三) 單一 C 級網路使用數個 VLAN

多數的學校由於僅具備單一 C 級網路，因此在使用網路傳送資料的設備逐漸增加的情況下就會面臨 IP 不夠使用的窘境，而且不同使用目的與功能的網路傳輸也日益增加，全部使用同一個 C 級網路作為傳輸路徑也會使得交換器

(switch) 經常處於高負載的情況不利於通訊的品質與效能。因此對於不同使用目的賦予不同的 VLAN 作為傳輸之用可大幅提升通訊品質，並減少傳輸錯誤及降低交換器 (switch) 的負擔。隨著新一代交換器 (Layer2 or Layer3 皆然) 幾乎都支援 802.1Q 的網路協定，利用 Ports Group 的方式進行 VLAN 的對應可以穿過多層的交換器達到資料的分流的目的。讓原有同一套的網路系統同時包容多項網路服務的資料流。

例如：某校想要使用的 Intranet 網路服務包括：1.校務行政系統、2.辦公室網路列印、3.圖書管理系統、4.VOD&MOD、5.郵件服務、6.網路儲存、7.無線網路、8. 校園電力監控系統、9.校園安全監控系統、10.校內網路電話。

需使用網路的設備包含有行政單位使用之個人電腦 50 台與網路列印設備 20 共有 70 台，教師辦公室共有個人電腦 70 台與網路列印設備 10 共有 80 台，班級電腦 45 台，另專科教室中電腦教室共 4 間共約 155 台設備，其他各專科教室具有 1-10 台不等的設備共 20 台。教師使用無線上網之筆電約 20 台。其他需使用網路之相關設備包含網路話機 150 台，校園電力監控設備 50 個端點，校園安全監控之網路攝影機 60 支等。

若統計其設備使用需求可發現，其需要使用網路並藉之進行管理的設備高達 650 台(支)之多，尚不包含需提供各項網路服務之伺服器主機共 16 部。因此絕非單

一 C 級網路或是兩個 C 級網路所能夠提供足夠的 IP 進行網路配置。這時就必須藉助 VLAN 的協助將所有的設備與服務進行資料的分流與區隔，但為避免重複建置多套實體網路配線，因此適當的 VLAN 分配即可有效的讓所有的需求皆能達成。假設將所有網路服務與需使用該項服務的設備進行分類與對應。

屬於同時對內與對外提供的網路服務：校務行政系統、網路儲存、郵件服務。對應之使用設備包含所有的個人電腦與筆記型電腦。

屬於僅對內服務的部份：辦公室網路列印、圖書管理系統、VOD&MOD、無線網路。對應之使用設備包含所有的個人電腦與筆記型電腦。

屬於校內特定用途的服務：校園電力監控系統、校園安全監控系統、校內網路電話等。

再將上述各項服務與對應之設備加以整理後可繪製如下圖的網路規劃圖。

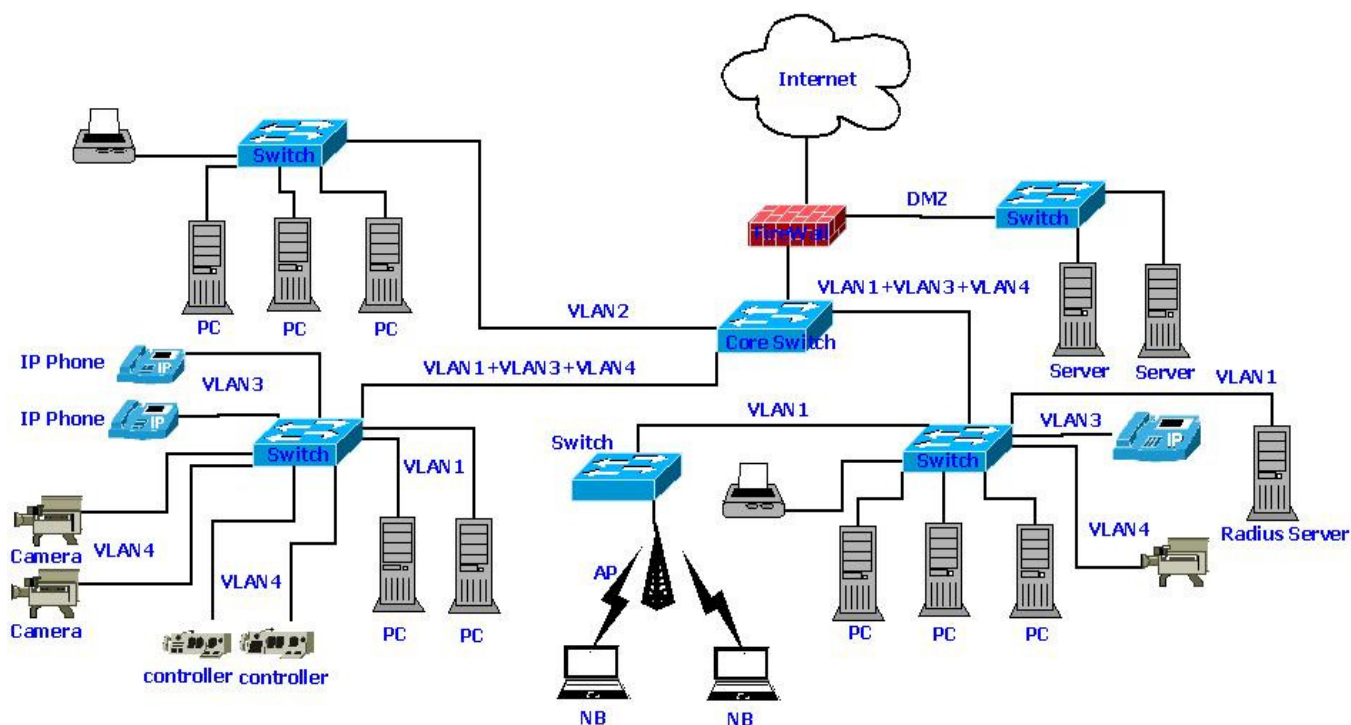
說明如下：

VLAN1：所有辦公室設備與無線網路配置於此，並且建置 Radius Server 作為無線網路認證之用。

VLAN2：所有電腦教室與專科教室之設備配置於此。

VLAN3：網路電話。

VLAN4：校園安全監控與電力監控設備。



實體的設定與配置則直接在各交換器上以不同的 Ports Group 對應不同的 VLAN，並將所有的訊號送至 Core Switch 做最終的交換工作。因此相對 Core Switch 的性能必須極佳方能承擔此重任。藉由如此的配置之後可達到各項設備皆猶如模組一般，能夠快速的對應或配置於實際所需之地點。

四、結語

網路的各項功能與應用日新月異，因此各項技術與相關設備也不斷推陳出新，僅就在下在校園內的一些網路管理經驗與淺見加以整理與大家一同分享並就教於各位先進，也期望我的一點經驗可以提供給大家一些參考價值。

五、參考資料

- (1)資訊工業策進會中文化部門(譯)(1997)。 TCP/IP Illustrated,Volume 1 中譯本。台北市：和碩科技文化。
- (2)陳冠銘(2003)。最新網路原理與應用。台北市：金禾資訊。
- (3)CCNA 訓練教材(2008)。Cisco : US。