# 旅館網路系統管理策略之研究

張展華
大同大學資訊工程學系
chanhua.chang@gmail.com

包蒼龍
大同大學資訊工程學系
tlpao@ttu.edu.tw

***摘要—本研究主要是探討旅館業的網路系統，旅館業力求讓住房客戶享受到最好的住宿及網路連線品質。本論文除了提出有效的旅館網路管理方式，也希望可以對於旅館住宿客群的區域網路存取控制及個人資訊安全性，提出有效的管理策略，藉由旅館業網路環境進行安全性相關的管理研究分析及實驗，以不影響原有架構的原則下，達到既便利又安全的旅館網路管理目的。本論文將針對旅館對於網路存取及住宿旅客的安全性存取管理策略做深入探討，希望有效解決住宿旅客使用網路之安全性問題，另外也能避免住宿旅客而造成旅館內部資訊應用系統的安全問題。***

***關鍵詞—旅館網路,網路管理,區域網路,VLAN***

**In this paper, we examine the network infrastructure and services used in the hotel chain. In the hotel business, to make the customers enjoying the best housing services and network connection quality are very important. In this paper, we propose an effective hotel network planning and management solution which can provide customers a secure and flexible network access. We will focus on the network management policies which can reduce the risk of network access even if the devices of the customers have no any defense mechanism installed. The policy shall also be able to protect the hotel administrative network so that the information system of the hotel will not be affected by the ill behaviors of the customer as well.**

**Keywords: Hotel network, Network management, VLAN.**

## 一、緒論

商務型訪客入住台灣各地的旅館，旅館業者為了提供便利的住宿環境，滿足各式各樣行動商務客及旅客的需求，衍生許多資訊應用及整合，提高住房的旅客舒適度及便利性。

但是在各種資訊應用進入旅館產業的同時，許多旅館業者大多忽略商務客或是一般旅客於住宿時使用資訊網路存取所帶來的資訊安全問題。

本論文研究的目的主要是提出具安全性的旅館客房區域網路管理方案，並藉由網路管理策略，主動提昇旅館客房住客個人電腦資訊的安全性，希望研究的結果可以做為旅館產業規劃網路資訊管理的參考，做為資訊化旅館之安全網路架構的基礎。

本文中我們將從相關文獻探討 VLAN 的標準協定，並針對 VLAN 的種類及協定作分析，同時也將針對本研究所使用到的相關頻寬管理、網路流量管理等相關設備及技術做介紹。

在測試驗證部份，經由網路管理之策略來規劃及設定 Switch VLAN、防火牆任意路由設定及存取測試、用戶端存取安全性測試及分析等的相關測試。

## 二、文獻探討

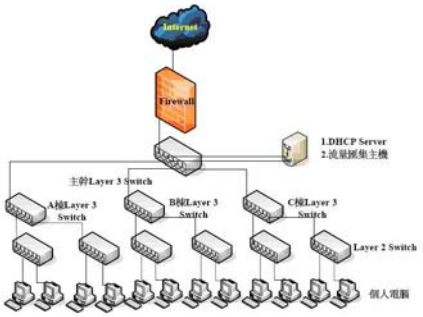
本節將探討旅館網路架構以及與其類似的校園宿舍網路及企業網路架構，相關的管理問題可作為互相比較之依據，由於在網路架構上有諸多相同的地方，因此本節中將對校園宿舍網路管理問題，企業網路管理上的應用以及旅館網路常見的問題進行探討。

### (一)網路管理於校園宿舍之應用

隨著網際網路應用的日漸普及與多樣化，校園宿舍中使用網路的普及率已達百分之百。然而經由網管資料分析得知，網路上所傳輸的訊息以

多媒體資料居多，網路使用者的行為模式也越來越複雜，如：P2P(Peer-to-Peer)、網路電視、串流影音等，使校園宿舍網路管理變得十分困難。因此，結合有效的管理政策以及合適的管理系統，用以解決上述問題將是校園資訊部門所必須面對的重大議題。

**校園宿舍網路管理**




圖一、常見的校園宿舍網路架構圖

圖一所示為常見的校園宿舍網路架構圖[8]，校園宿舍網路一般來說是每棟宿舍建築由一台或數台 Layer 3 Switch 連接至多台 Layer 2 Switch，再連結至宿舍中的個人電腦，宿舍網路佈線採用單一配線系統(Single Cabling System: SCS)，包含配線端子板、資訊插座、跳接線、連接線及 UTP 線等構成整體一致性之配線。

每一棟宿舍的 Layer 3 Switch 分別為每一層樓設定一個到數個虛擬區域網路(Virtual Local Area Network; VLAN) ，可以有效的控制廣播封包不會轉發到其他 VLAN 中。系統在執行 IP-MAC 對應和自動阻擋時，管理者只需對負責該網段的 Layer 3 Switch 下達管理指令即可，方便控制流量、簡化網絡管理、提高網絡的安全性。而在流量彙整及分析方面，則是在主幹的 Layer 3 Switch 上用 Mirror 的方式，將對外網路連接埠之流量複製到網管系統主機上，此一管理策略可以解決部份宿舍網路的問題，包括學生免除設定 IP 的困擾、避免 IP 衝突、自動阻擋流量異常之 IP、限制單一 IP 每天的流量等。

**常見的校園網路管理問題分析**

校園網路管理有許多常見的問題[9]：

**網路服務品質無法滿足**

由於 Multimedia 與 VoIP 等即時資訊傳遞的應用服務大量興起，除了加重網路負載外，亦無法滿足各個應用程式所需的網路服務品質要求。

**大流量電腦癱瘓整個校園網路**

由於層出不窮的電腦病毒，使用者很容易在不經意間中毒而產生大量垃圾封包，網路頻寬愈大，產生的垃圾封包量就愈驚人，除了佔用本身網段的頻寬外，亦危害到整個骨幹網路的正常運作，除此之外，P2P 軟體的濫用也可能造成大流量，大量的下載圖檔、MP3 或電影檔，同樣會造成網路使用不公平，讓成其他網路使用者的速度變慢。

**網路設備負載異常問題**

一般設備的中央處理器(Central Processing Unit，以下簡稱 CPU)的平均使用率很低，一旦中央處理器的平均使用率突然升高時，通常是網路上有異常的情況，大部分是蠕蟲爆發或改變網路架構造成迴圈（loop）所導致。

**IP 位址盜用欺騙問題**

因 IP 位址設定的特性，易被竊用，除了會造成 IP 位址衝突外，若僅以 IP 位址來稽核網路使用者，其正確性亦常令人質疑，因此，當網路用戶使用行為有爭議時，將衍生不少行政上或維護上的困擾。除此之外，當網路設備看到一個 MAC 位址使用多個 IP 位址的情形，被使用到的 IP 位址或是此 MAC 位址與閘道 IP 位址相衝時，將導致受害網段網路無法使用。

**校園流量管理及病毒攻擊防禦**

校園中因為網路頻寬的需求高，也使得網路管理更為複雜，頻寬管理及限制的議題經常被提出來討論，文獻中也有許多曾經被提出的研究成果。在流量管控部分， [11]之作者提出使用固定位址解析協定(Static Address Resolution Protocol)，來將 IP 位址與 MAC 位址做出對應，這樣可以避免使用者盜用他人 IP 位址的問題，也使 IP 的管理變得比較容易，但是校園內由於教學的需要，常常會有電腦移動而使該 MAC 位址不斷變換位置的狀況，所以此方法相對不太方便，同樣的於旅館網路中，因每日來來往往不同

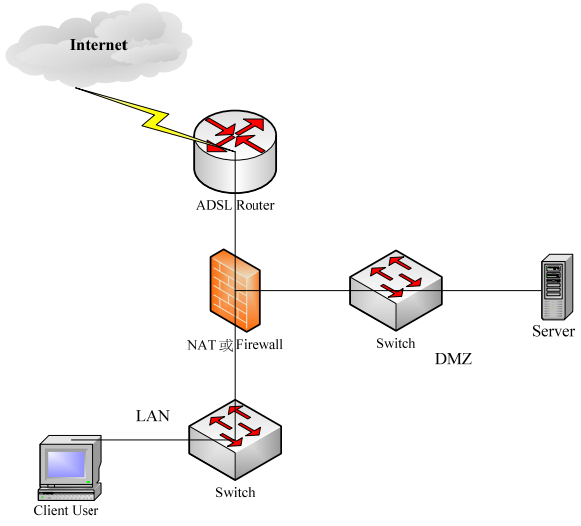
的住客，必然使 IP 與 MAC 資訊不停的更動，也不適合應用於旅館網路；除此之外，於文中有提到對於超過流量的 IP 位址切斷其對外傳輸，仍使其可以使用校內服務的作法於校園網路中使用確實可行，但若是於旅館網路使用，將造成客人使用上的問題與障礙，不過其對病毒攻擊的管理構想倒是值得作為旅館網路管理架構之參考。

(二)企業網路管理相關應用

企業網路的應用與旅館業網路的需求及應用有諸多的相似之處，網路管理問題亦有許多可供作參考的地方，以下列舉一些於中小企業為了網路管理之便而應用 VLAN 的時機與實例：

在小型企業的網路架構中，往往「一條 ADSL 線路」搭配「一台 IP 分享器或防火牆」與「幾個普通 Switch」就可以滿足其區域網路的應用以及使用網際網路功能。但若是 IT 人員面臨到需要管理較多數量的 PC 及 Server 以及需要加強網路安全以及網路效能時，最常遇到的做法就是規劃多個網路區段來滿足這樣的需求，想以事半功倍的方式來管理這類型的網路至少需要使用具備管理功能的 Layer 2 交換器。

圖二為一般常見的中小企業網路架構，由此圖可以瞭解到一些中小企業網路常見問題，來說明中小企業常見的 VLAN 應用來改善現有網路架構的方法。

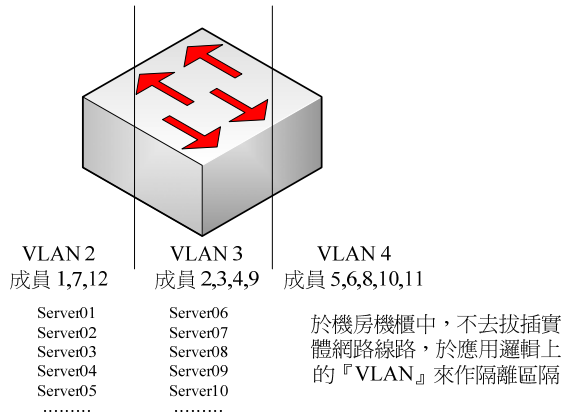



圖二、常見的中小企業網路架構圖

**機房機櫃放置伺服器的網路應用**

機房中所放置的主機，一般以伺服器居多，至於伺服器主機與網路設備的數量方面，一個機櫃一般預設只會搭配一個 Switch，這種方式衍生了一些問題。離如，假設機櫃內有多台伺服器，其中三台伺服器會對外提供服務，應該放在 DMZ 網路區；另外幾台伺服器只會對內提供服務，故放置在 LAN 區，這時若是沒有採用 VLAN 功能，想要切開這兩個網段只能採用實體的方式，也就是使用兩台 Switch 來隔離。

如圖三所示，倘若此時使用具備管理功能的 Switch 來建構，就可以使用邏輯的方式來切開兩個網段，甚至在往後的擴充性方面，不論增加伺服器主機、新增網段或切換主機所屬網段，都可以不需要進入機房插拔實體的網路線路。




圖三、機櫃放置伺服器的網路設備 VLAN 配置

**訪客專用網路與公司內使用網路區隔的需求應用**

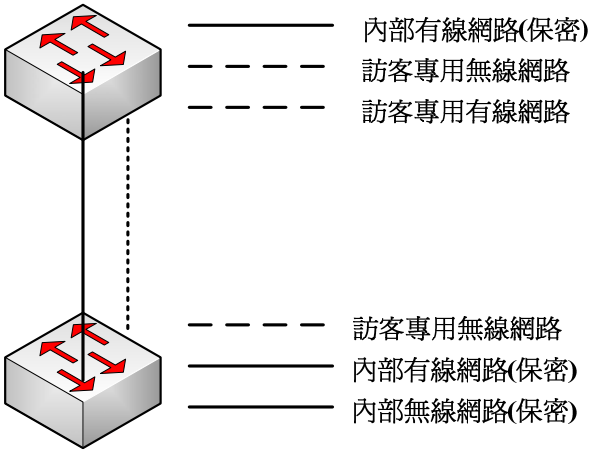
一般來說，企業常會遇到來訪的客戶使用自行攜帶的筆記型電腦透過企業線路上網，而最常使用到的網路區域應該算是會議室網路或是無線網路，但大多數的中小企業會議室網路或無線網路並未與公司內部網路區隔開來，這對於一些注重區域網路安全的中大型企業，通常是不允許這類情況發生，這時候可以使用 VLAN 方式來切割網段形成不同安全等級的網路。

除了上述應用之外，中大型企業難免會跨樓層，每一層也都有可能配備有會議室與無線網路基地台，在切割這類型網路的實做則是需將這些

需要被區隔的網路設備與網路孔號，利用具備管理功能的 Layer 2 Switch 將之隔離開來，來增強網路的實體安全性，至於跨樓層則透過 VLAN Trunk 的功能來銜接即可；若此時不使用 VLAN 區隔，而使用一般 Switch 替代的話，勢必會添購許多小型的 Switch，容易使得機房變得較凌亂造成架構較複雜等等缺點。

規劃這類型網路最繁雜的是遇到需要合中帶分、分中帶合的規格，例如會議室網路為了安全性而隔開使得無法存取區域網路，但卻有員工硬是需要從會議室網路來列印到內部網路的網路印表機，而這些需求並不是無法解決，像是使用帳號密碼認證方式存取網路（例如 802.1x 方式）只是通常需要較多的人力、物力來達成。

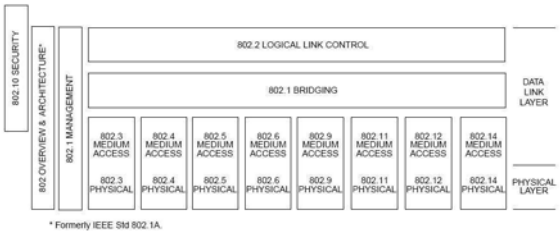
在 Layer 2 Switch 切割 VLAN 後，若有不同 VLAN 之間互通的需求時，可使用 Router 來解決這個需要（或是 Layer 3 Switch 也可以），所以切 VLAN 規劃成不同的子網路（Subnet）通常是為了未來應用路由器來連接，圖四為訪客專用網路與公司內網區隔示意圖。




圖四、訪客網路與公司內網區隔示意圖

(三)VLAN（Virtual Local Area Network）與 IEEE 802.1Q 標準規格

VLAN 標準係由 IEEE 定義在 802.1Q 中[3]，圖五所示為各相關標準及協定之關係圖。




圖五、IEEE 標準與相關協定關係圖

**VLAN 的種類劃分**

VLAN [5]，是由位於不同實體區域網段的設備組成。雖然 VLAN 所連接的設備來自不同的網段，但是相互之間可以進行直接通信，就好像處於同一網段中一樣。由於 VLAN 是將區域網內的設備採用邏輯方式而不是實體方式劃分成一個個獨立網段，所以它可以提供靈活的用戶及主機的管理、頻寬的分配以及網路資源最佳化等服務。

從技術角度來看，VLAN 一般有下列三種劃分的方法：基於 PORT 管理的 VLAN、基於 MAC ADDRESS 管理的 VLAN 以及基於協議的 VLAN。

**VLAN 技術的效益**

VLAN 技術中，一個 VLAN 即為一個邏輯子網，也是一個邏輯上的廣播域，他允許我們邏輯的子網劃分從而取代實體的子網劃分。通常用 VLAN 來提供更高的安全性和更加方便的管理。以下簡單介紹 VLAN 的優點和缺點，並簡單敘述 VLAN 技術的效益。

VLAN 的優點

(1) 控制網路廣播、增進網路效能

(2) 提高網路的安全性

(3) 用交換機代替路由器

(4) 方便網路管理

VLAN 的問題

(1) VLAN 之間傳輸的問題

(2) VLAN 的複雜性

(3) 路由器的負載能力

(4) 不能防止病毒的傳播

(四)旅館網路管理的問題

旅館網路和校園網路及企業網路在使用上因為需求不同，因此衍生出不同的網路管理問題及管理策略及不同的應用。

**旅館網路網管問題分析**

旅館網路管理有許多常見的問題，整理說明如下：

(1) 需提供有線網路存取隨插即用功能，避免造成訪客不方便

目前企業大多採用 DHCP 配發用戶端 IP 位址，但是對某些高階用戶而言，在公司的 IP 位址往往是固定，也必須透過固定的 IP 方可存取特殊權限。當此類型的訪客入住旅館之後，就必須要修改 IP 位址或是動態取得 IP 位址才能連線，對不太會操作的使用者而言，這些小變動就成為大負擔。有鑑於此，旅館網路便需做到「隨插即用」功能，無論客戶電腦上是否已經設定 IP 位址，旅館內的網路均會自動對應，讓使用者隨時可以連上網際網路。

(2) 住宿旅客自行攜帶網路設備，造成其他客房無法正常存取網路

旅館內經常有住宿客自行攜帶無線或是有線網路 IP 分享器接在住宿的房間內，若是旅館網路無法提供上述的任意網路存取功能，則當部份住客以 DHCP 取得的資訊是來自於客房網路住客安裝設備所發放，就會造成無法使用網路，旅館內的資訊人員也不易處理，畢竟旅館人員以服務為主，均以不打擾住宿中的客人為主要訴求，也因此在查修上十分困難。

(3) 住宿旅客電腦資訊安全問題，造成旅館網路異常

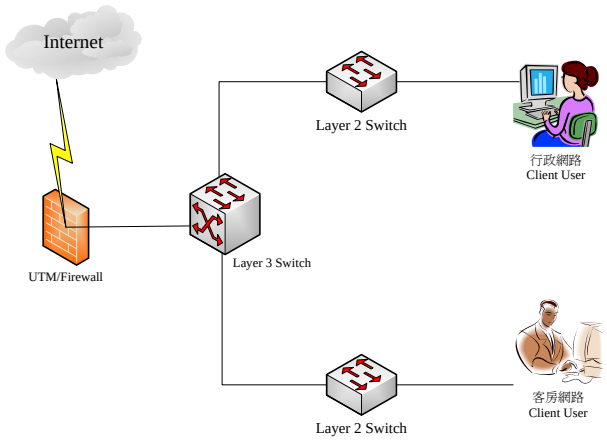
經常往來各地的商務旅客，攜帶筆記型電腦四處旅行，但並非所有電腦使用者都是資訊人員，對於資訊安全的認知通常不足，因此常有商務旅客電腦中毒後，於旅館客房網路廣播造成網路癱瘓，甚至有些商務旅客在無任何資訊安全的保護之下，電腦遭到其他住宿房客惡意竊取重要資料，不僅可能造成個人及公司資料的外漏，連帶的影響旅館的商譽。

## 三、網路管理策略研究與限制問題分析

本節將以本研究所做的網路管理機制、網路架構和流程及分析比較等三方面作詳細說明與介紹。

(一)研究程序與架構

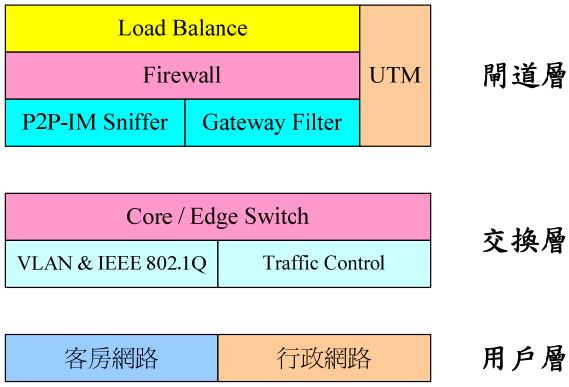
本研究的架構分析，主要分為連鎖旅館行政網路管理和旅館客房網路管理，以此兩者進行管理研究架構之建構與分析，並分析出架構之優缺點。本研究除了參考相關文獻外，亦將架設模擬環境進行實際測試，驗證本研究在相關旅館等服務業進行網路管理之可行性，圖六為旅館網路架構圖。




圖六、旅館網路架構圖

(二)VLAN 網路管理策略

本篇研究所提出的，如果要實現於連鎖旅館業中，需要相關網路設備或伺服器來搭配管理，圖七所示為研究中需應用到的相關資訊設備，架構中包括閘道層、交換層及用戶層。



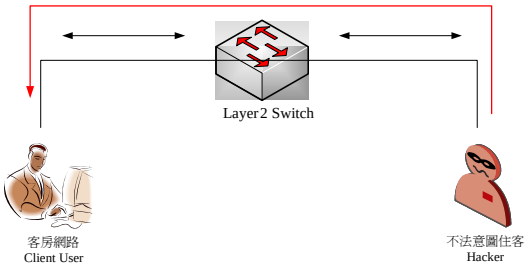

圖七、VLAN 網路管理策略

**閘道層**

在一般企業網路中與網際網路介接的設備為網路閘道器，於本研究中，我們將統一稱為閘道器。閘道層包含了 Load Balance、Firewall、P2P-IM Sniffer 以及 Gateway Filter，而具備這樣整合性功能的閘道器，一般稱之為 UTM，（Unified Threat Management），即『整合式威脅管理』，顧名思義就是將威脅統一且集中地做控制與管理，目的在於區分單一資安防禦設備如：防火牆、入侵偵測系統、防毒閘道等等系統，惟現今資安廠商為因應市場需求以及積極跨越其他資安領域之市場考量下，各家廠商均利用自行研發或採取併購方式加強設備在功能上之提升與增加服務種類。

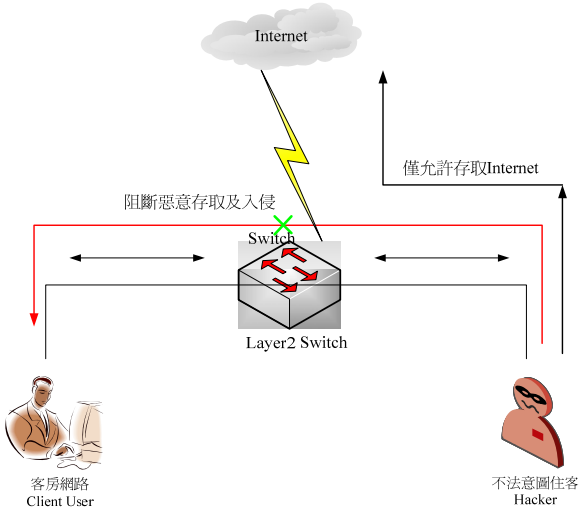
**交換層**

於網路交換層中，我們將考慮的是 Edge 與 Core Switch 的安全性管理，一般區域網路存取原則上都是希望彼此能互通聯繫，交流資訊，然而在旅館客用網路裡，這種方式是有其安全性的隱憂存在，舉例來說，圖八為一般旅館網路架構，於 Edge 端之下有各式各樣的使用者，有一般的住客，也可能有不法意圖的住客存在，若是旅館住宿客本身資訊安全觀念不足，很可能被不法意圖的住客惡意破壞或是竊取資料。



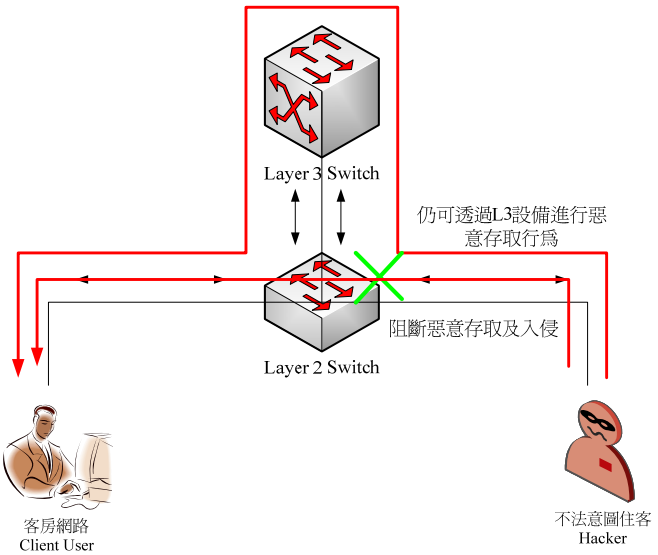

圖八、一般旅館客房網路無法阻斷惡意攻擊示意圖

若是在 Edge 於網路交換層設備上，設定好適當的存取控制協定，有效率的阻斷不法意圖住客的惡意存取，使其僅可正常存取網際網路資源而不能存取其他住房，將可減低資訊安全的問題。如圖九所示，不法意圖的住客企圖存取鄰近住宿客的電腦，於 Switch 上已不被允許而阻斷，僅可正常存取網際網路資源。




圖九、Edge 端阻斷不法存取示意圖

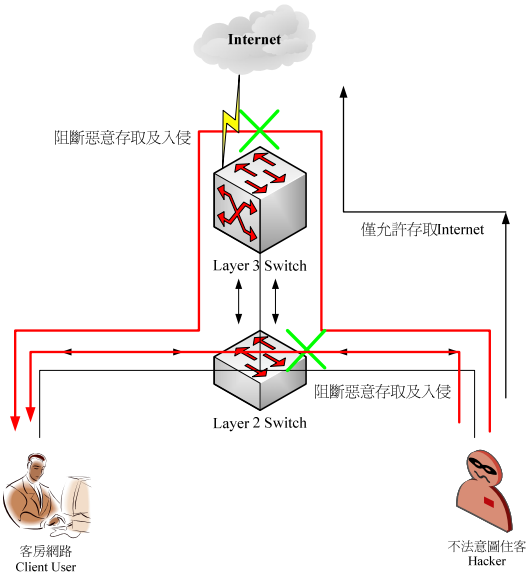
然而，若僅僅是在 Edge 於網路交換層設備上，設定存取控制協定，當網路架構較為複雜的情況下，可能會有 Core 端的收容設備，此時若是忽略了 Core 端的安全設定，仍舊無法阻斷不法意圖住客的惡意存取，依舊會有資訊安全上的隱憂，如圖十所示，不法意圖的住客企圖存取鄰近住宿客的電腦，於 Edge 端 Switch 上已不被允許而阻斷，但是透過 Core 端設備後，還是有機會竊取或是破壞其他客房使用者的資訊設備。




圖十、較為複雜的旅館網路無法阻斷惡意存取示意圖

因此除了在 Edge 端於網路交換層設備上設定存取控制協定之外，Core 端的網路交換層設備也要有相當的存取控制，方可有效的阻斷不法意

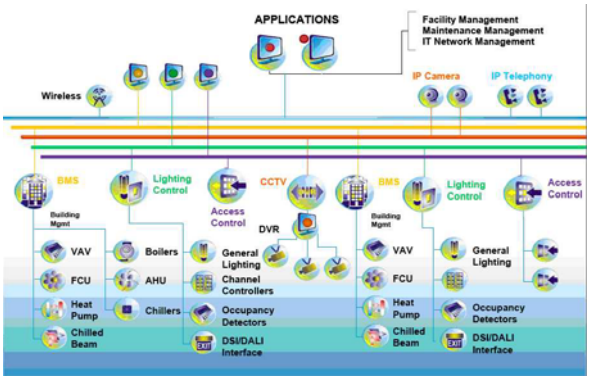
圖住客的惡意存取，如此便可杜絕資訊安全上的隱憂，如圖十一所示，不法意圖的住客企圖存取鄰近住宿客的電腦，於 Edge 端 Switch 上已不被允許而阻斷，當存取路徑試圖透過 Core 端設備進行存取時，亦被 Core 端設備阻攔，此時存取者僅可正常存取網際網路資源，而無法竊取或是破壞其他客房使用者的資訊設備。




圖十一、Core 端阻斷不法存取示意圖

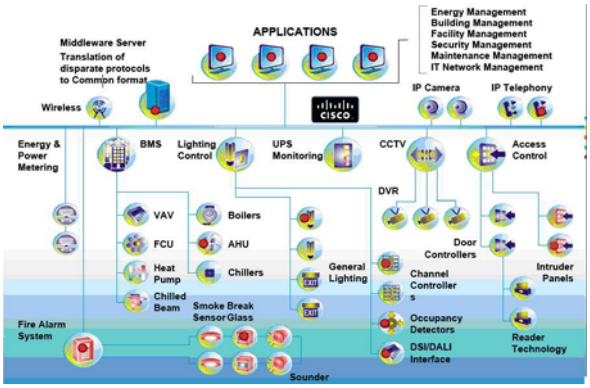
**用戶層**

旅館網路的客房資訊應用相當廣泛，過去旅館網路需因應各種不同的使用需求，使得旅館網路採用多種型態的網路，圖十二為以往旅館用戶層示意圖。




圖十二、過去多種型態的旅館網路用戶層示意圖

因為科技的日新月異，許多資訊化應用不斷的導入傳統產業及服務業，因此旅館客房資訊應用逐漸走向 IP 網路化，使得旅館網路朝向共用 IP 的網路平台架構發展，圖十三為 IP 網路化旅館用戶層的示意圖。



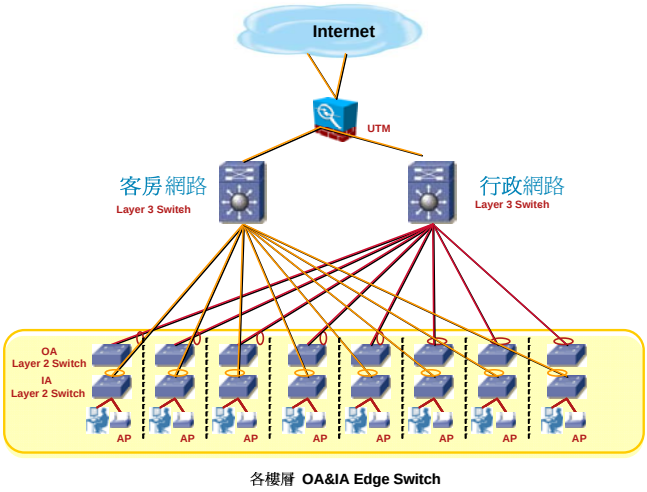

圖十三、共用 IP 的網路平台旅館用戶層示意圖

旅館服務業為了迎合各種不同的住客需求，也為了滿足各式各樣的行動商務旅客的需求，進而衍生出多元化的資訊應用及整合，以提高住房的旅客舒適度及提供各式各樣的資訊服務。

因此，針對旅館用戶層的管理策略，主要考量點以滿足所有旅客的需求為優先，避免對旅館用戶層作過多的限制，但在滿足使用需求的同時，仍需考慮到安全性的議題。

(三)旅館客用網路管理架構

本研究所提出的管理架構，主要是管理服務業中連鎖旅館業，客房與客房間，客房與行政網路之間存取的安全性問題。除此之外，由於客房網路諸多的資訊設備整合應用，導致網段內廣播封包情況嚴重，因此，為提高旅館客房網路之安全性，將旅館行政網路與客房網路系統各自獨立，讓兩個網路系統彼此不互通，彼此不受影響，以網路獨立來強化安全性。客房與客房之間，彼此也不互通，採行的管理方法，係藉由 Private Vlan Edge 技術，將每個客房網路區隔開，保護外來的顧客使用者的資訊安全，同時 Private Vlan Edge 技術可防止 IA 網路 IP/MAC 攻擊事件產生，如：非法架設 DHCP Server、IP 衝突、MAC 攻擊等資安事件，確保客用網路的穩定性與安全性。由於 Private Vlan Edge 封包資訊到 L3 設備時，設備與設備間，彼此仍可互通，因此在 L3 Switch 上仍需再制定 VLAN ACL 管理策略讓彼此不互通，圖十四為管理策略下的『旅館行政網路及客房網路管理架構圖』。




圖十四、旅館行政網路及客房網路管理架構

(四)旅館客房網路管理的策略

為避免客房的特定使用者佔用大多數頻寬，對於客房頻寬管理的問題，提出三種管理方法：

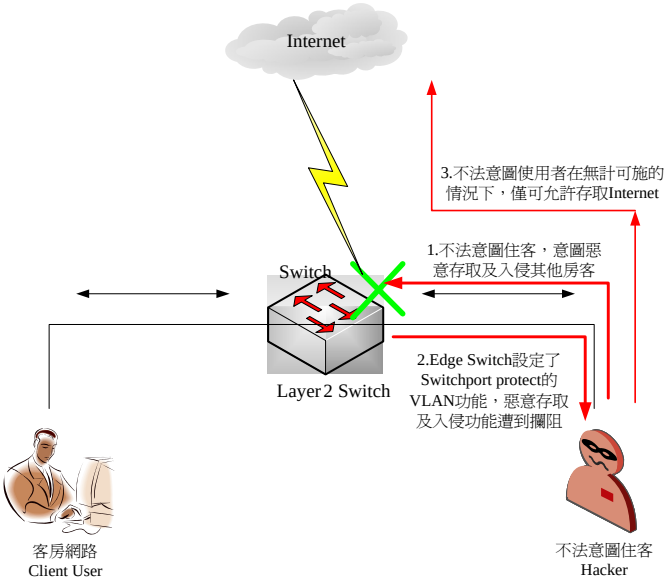
By Port：藉由 Service-Policy 機制，可針對 Interface 限制每一個客房頻寬使用大小，防止頻寬資源被少數人或不重要的流量所獨佔，以保障每個使用者連線的基本頻寬。

By Service：需針對特定的服務(如：WEB、E-Mail、 Peer to Peer)制定不同的頻寬管理政策，進而達到有效頻寬管理。

管理上還可以採行雙層式頻寬管理， 亦即結合上述兩者來作管理。

(五) VLAN 網路管理的運作流程

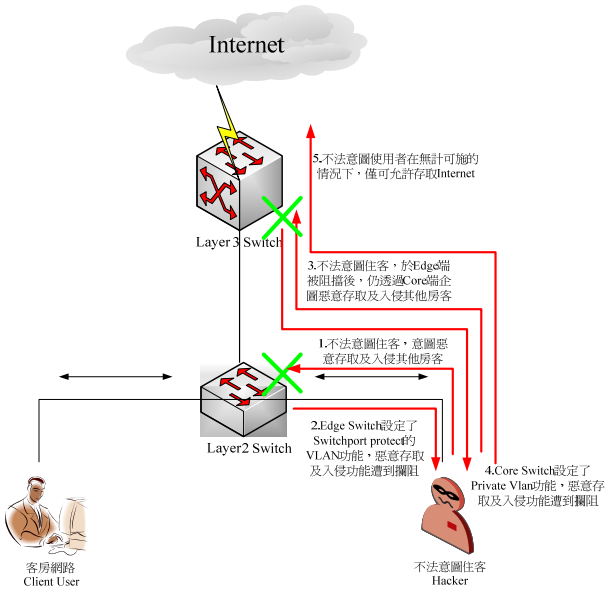
圖十五為 VLAN Edge 端運作流程圖，不法意圖住客意圖惡意存取及入侵其他房客，Edge Switch 設定了 Switch-port protect 的 VLAN 功能，惡意存取及入侵功能遭到攔阻，不法意圖使用者，僅可允許存取 Internet。




圖十五、VLAN Edge 端運作流程

**VLAN Core 端運作流程**

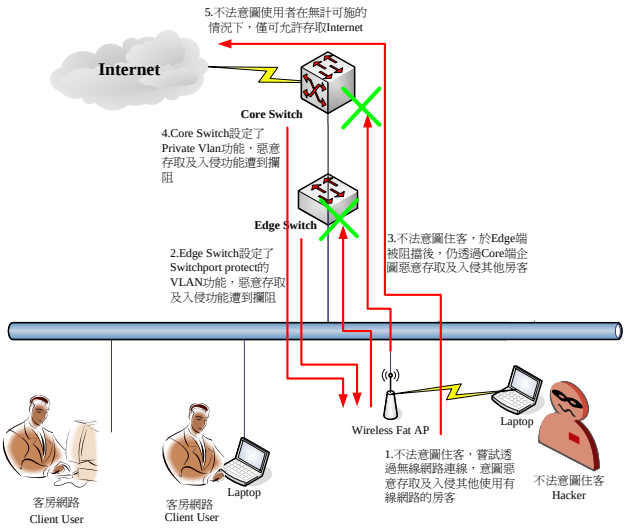
圖十六為 VLAN Core 端運作流程圖。不法意圖住客，意圖惡意存取及入侵其他房客。Edge Switch 設定了 Switch-port protect 的 VLAN 功能，惡意存取及入侵功能遭到攔阻。不法意圖住客，於 Edge 端被阻擋後，仍透過 Core 端企圖惡意存取及入侵其他房客。Core Switch 設定了 Private Vlan 功能，惡意存取及入侵功能遭到攔阻不法意圖使用者，僅可允許存取 Internet。




圖十六、VLAN Core 端運作流程

**VLAN 於 Wireless AP 端運作流程**

圖十七為 VLAN 於 Wireless AP 端運作流程圖。不法意圖住客，嘗試透過無線網路連線，意圖惡意存取及入侵其他使用有線網路的房客 Edge Switch 設定了 Switch-port protect 的 VLAN 功能，惡意存取及入侵功能遭到攔阻，不法意圖住客於 Edge 端被阻擋後，仍透過 Core 端企圖惡意存取及入侵其他房客。Core Switch 設定了 Private Vlan 功能，惡意存取及入侵功能遭到攔阻，不法意圖使用者，僅可透過 Wireless AP 連線允許存取 Internet。



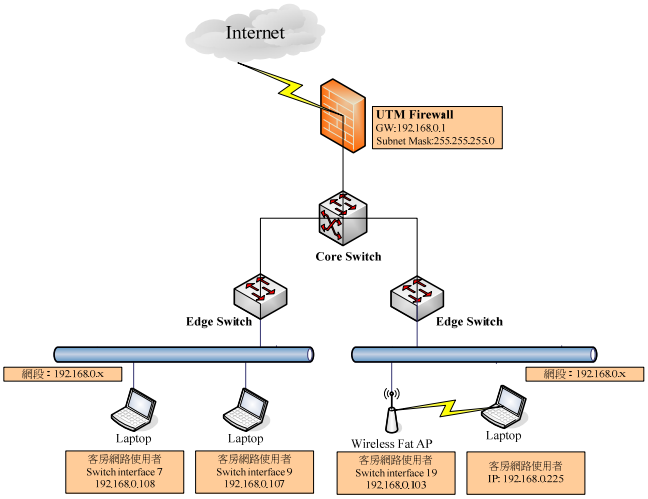

圖十七、VLAN 於 Wireless AP 端運作流程

## 四、建制研究架構與環境實測

(一)VLAN 網路管理架構

本研究中的 Private VLAN 網路管理策略架構環境，如圖十八所示，防火牆設備對外連接了一條 Internet 線路，防火牆的限制上目前設定為內對外可以任意存取，不作任何限制。在 Firewall 之下串接了一台 Layer 3 層級的 Core Switch，與 Core Switch 串接的部份分別連接兩台 Layer 2 層級的 Edge Switch，兩部 Edge 端設備之下，分別連接了筆記型電腦及無線 AP 站台。

Core / Edge Switch 端設定了 Private LAN 及 Switch-port protect 的存取限制規則，將禁止所有用戶端彼此互相存取，所有用戶端只能連線至 Firewall 後，存取網際網路資訊，而連線 Wireless fat AP 的使用者，亦不可對網段內其他實體線路用戶進行存取，Wireless fat AP 內的使用者則不在此限。




圖十八、VLAN 網路管理實測網路環境架構圖

(二)旅館網路管理實測環境

在實測環境中，分別針對 Core / Edge Switch 端進行 Private VLAN 的存取限制規則設定，以及能連線至 Firewall 後，存取網際網路資訊，而連線 Wireless fat AP 的使用者，亦不可對網段內其他用戶進行存取。

**Edge Switch 設定**

在測試環境中，首先針對 Edge switch 測試部份作說明，我們於 switch 上的 interface FastEthernet0/7 port 上，連接了一部筆記型電腦，IP 設定為 192.168.0.108，另外在 interface FastEthernet0/9 port 上，連接了另外一部筆記型電腦，IP 設定為 192.168.0.107，單機作業系統均為 Windows XP，無安裝任何軟體防火牆。

一般的 VLAN 設定方式需針對所有的 Port Interface 進行設定，賦予特定的 VLAN ID 作 VLAN 區隔，作法較為繁複且維護不易，在閱讀了相關的指令集後，找到一個更好的指令可以取代且可以達到我們所需要的功能。於 switch 上的 interface FastEthernet0/7 port 及 interface FastEthernet0/9 port 上，我們下達了 switchport protected 的指令，此一指令將可達到我們所需要的安全性設定功能。

**Core Switch 設定**

接下來針對 Core switch 測試部份作說明，我們於 switch 上的 interface GigabitEthernet1/0/1 port，連接了 firewall，interface GigabitEthernet1/0/27 port 連接了測試用的 PC，interface GigabitEthernet1/0/48 port 上則連接了 Edge switch。

我們於 Edge 端設定了針對連接 port 的安全性指令後，仍需要在 Core 端進行安全性的設定，方可有效杜絕用戶端透過 Core 端連結後，仍可透通存取其他 port 口連結的用戶，傳統賦予特定的 VLAN ID 作 VLAN 區隔作法在此不太適用，因為繁複且維護不易的情況仍舊存在，若是已旅館客房數來作分割，動輒數百間的旅館房間，VLAN ID 的維護將使網路維護人員非常難以維護，因此在閱讀了相關的技術文件後，取得了更好的指令可以取代且可以達到我們所需要的功能。於 switch 上的 interface GigabitEthernet1/0/1 上，我們下達了 switchport private-vlan mapping 223 224 及 switchport mode private-vlan promiscuous 兩指令，此種指令格式屬於 gateway type，連接聯外的 gateway 設備如防火牆，若需要給所有設備串接通聯則都需使用這類型的 VLAN TYPE。另外我們於 interface GigabitEthernet1/0/27 及 interface GigabitEthernet1/0/48 上下達了 switchport private-vlan host-association 223 224 及 switchport mode private-vlan host 指令，switchport mode private-vlan host 指令與 Edge 端 switch 使用的指令 swtich-port Protect 功能類似，經過這樣的設定過程後，則可得到所需要的安全性設定功能。

**Wireless AP 設定**

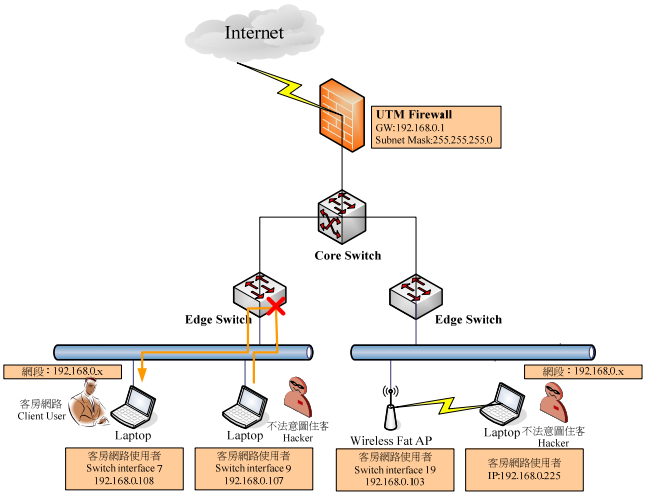
在測試環境中，針對 Edge switch 連結 Wireless 的測試部份作說明，我們於 switch 上的 interface FastEthernet0/19 port 上，連接了一部 wireless fat-AP，AP 的 IP 設定為 192.168.0.103，設備將不提供 DHCP 發放功能，所有 IP 發放作業均由 UTM 處理，同樣的我們於 switch 上的 interface FastEthernet0/19 port 上，我們下達了 switchport protected 的指令，此一指令將可確保由使用 wireless 連結旅館網路的使用者，仍會在我們所需要的安全性設定功能範圍管轄。

(三)旅館客房網路管理實測結果

本篇論文所討論之網路管理策略，實測的結果將於本節依續以 Edge / Core 端及使用 wireless AP 連線後的測試結果進行說明。

**Edge Switch 端存取安全性測試結果**

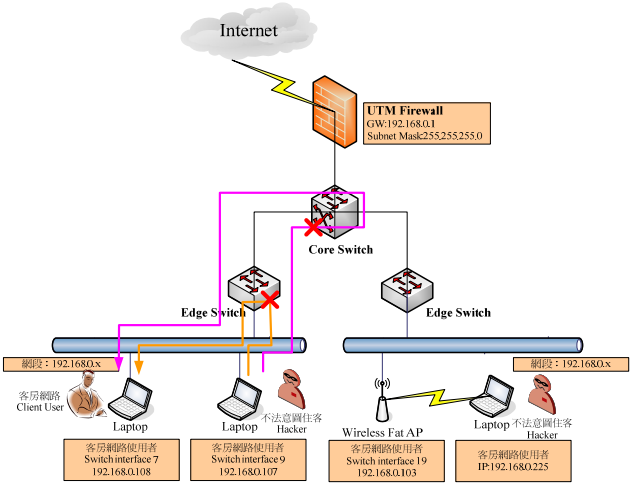
如圖十九所示，住客企圖竊取鄰近客房商業住客的電腦資訊，在進行安全性設定之後，就算住宿的商業住客本身沒有足夠的資安防護觀念，因為旅館內的安全機制，可避免發生資訊安全的問題。




圖十九、模擬客房住客入侵其他住客測試遭到攔阻示意圖

**Core Switch 端存取安全性測試結果**

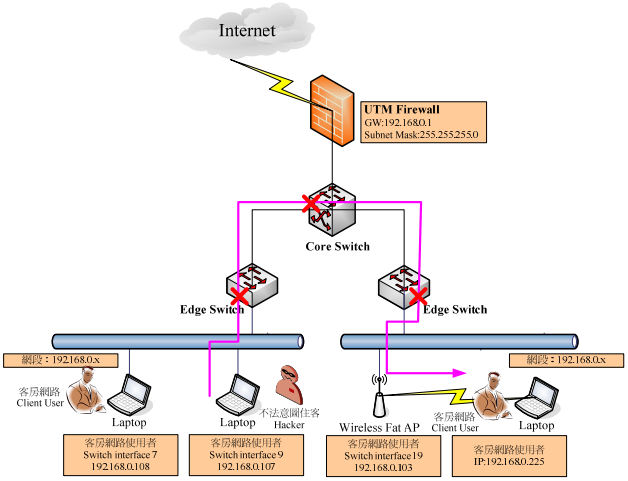
如圖二十所示，住客企圖竊取鄰近客房商業住客的電腦資訊，在進行安全性設定之後，就算住宿的商業住客本身沒有足夠的資安防護觀念，因為旅館內的安全機制，降低了資訊安全的疑慮。




圖二十、模擬不法意圖住客透過 Core 端入侵其他住客測試遭到攔阻示意圖

**Wireless AP 端存取安全性測試結果**

如圖二十一所示，不法意圖住客企圖透過網路連線無線網路網段，竊取鄰近客房商業住客的電腦資訊，在進行安全性設定之後，就算住宿的商業住客本身沒有足夠的資安防護觀念，因為旅館內的安全機制，避免了可能的入侵行為。




圖二十一、模擬不法意圖住客企圖連線無線網路用戶住客測試遭到攔阻示意圖

## 五、研究結論及未來展望

旅館客房網路系統是一個應用廣泛且複雜的系統，因此在管理上除了要顧及各方面的應用整合之外，安全性網路系統的管理更是一個重要的課題，從本篇論文中我們了解以 IEEE 802.1Q 標準作為架構基礎的管理特性及需求，進而討論出相對應的網路管理策略，使我們可以在維持網路服務品質的同時，兼顧到旅館資訊系統的安全性及住宿旅客的資料安全及保密性，為了易於管理及維護，建置擬擬的管理架構進行測試及分析，來驗證及實驗出期望的結果。

本篇論文重點在於參考各種 VLAN 網路架設之經驗及應用，如校園網路中宿舍網路架構之經驗、中小企業應用 VLAN 之案例等，規劃建置出適合旅館網路的應用，解決日益繁重的資訊管理問題。但使用 Wireless fat-AP 所衍生的資訊安全問題仍舊未能在本研究中解決，若需要解決無線網路使用者彼此之間的資訊安全問題，仍需使用成本較高的 thin-AP 架構，方能得到期望的資訊安全管理層級，未來在研究上仍需對這方面的研究多加琢磨，以求得成本較低且具備安全性的無線網路架構。

## 六、參考文獻

[1] Adam Laurie ,「用電視可駭入旅館房客資訊」，http://www.zdnet.com.tw/news/software/0,2000085678,20100603,00.htm

[2] Cisco Systems website, Inc., http://www.cisco.com/.

[3] IEEE,“IEEE 802.1Q Standard, ” http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf.

[4] R. Venkateswaran, “Virtual Private Networks,” *IEEE Trans. Potencials*, pp.11-15, Feb. 2001.

[5] “Virtual LAN (VLAN),” http://en.wikipedia.org/wiki/VLAN

[6] 方盈，TCP/IP 通訊協定-理論與實務，初版，台北市，博碩，1997.

[7] 黃武隆，校園宿舍的網路管理及建置以南華大學宿網為例，南華大學資訊管理研究所碩士論文，2002.

[8] 姜文忠、廖述益、施銘亮,「網頁式校園宿舍網路管理資訊系統規劃與建置」, TANET 2007.

[9] 張慶龍、楊智淵、徐正哲,「以分層公平頻寬使用考量之校園網路管理架構設計與實現」, TANET 2006

[10] 劉大川、陳昌盛,「規劃新一代的校園宿舍網路」, TANET 2008

[11] 嚴嘉錚、楊靖宇,「流量管理及病毒攻擊防禦整合系統之建置」, TANET 2003.