兼具流量監測與虛擬位址應用之網路建置架構

范修維　　廖鴻圖　　伍啟錄

世新大學資訊管理學系　世新大學資訊管理學系　世新大學電算中心

fan@cc.shu.edu.tw　htliaw@cc.shu.edu.tw　rick@cc.shu.edu.tw

摘要

TANet 新骨幹採用乙太網路傳輸技術，讓各校得以使用 Gigabit Ethernet 進行界接，大幅提昇傳輸速率。為了避免高速網路被不當使用，申請 TANet 新骨幹的連線學校都必須進行網路流量監控，完成流量統計作業。不幸地，一些學校所採行的網路架構都僅能紀錄真實 IP 位址的流量，至於虛擬 IP 位址的傳輸紀錄就無從稽核，這些虛擬 IP 位址的電腦就成為問題追蹤的死角。本文中，我們將針對 TANet 最常用的網路設備，提出一套新的建置架構，不僅可以同時紀錄到真實及虛擬 IP 位址的流量，而且在未來加裝網路過濾設備 (如入侵偵測系統、網路防毒、電子郵件紀錄…) 時，也可以讓這些設備的加入或移除的時間降到最低。最重要的，這些架構都已成功地運行在本校的校園網路上，是個確實可行又具有彈性的建置方案。

關鍵字：TANet 新骨幹、網路架構、流量統計、虛擬位址。

Abstract

Today, TANet new backbone adapts the MAN architecture to let schools could use Gigabit Ethernet interface to connect and increase the transmit speed. For avoiding the unsuitable use of high speed network, the connected school which applied TANet new backbone must complete the task of network flow statistics. Unfortunately, some schools could only audit the flow of public IP addresses. In this paper, we propose a new architecture to audit the flow for public and private IP addresses. More importantly, this proposed architecture is a practical experience of our school. Therefore, it really is a suitable and flexible implementation strategy.

Keywords: TANet new backbone, network architecture, flow statistics, private address.

1. 前言

TANet 新骨幹開放 10/100/1000M 乙太網路界面讓各級學校進行界接，為了避免網路濫用而無法追查到來源，要求各校必須進行流量統計作業。各校必須先提出連線申請，並經審查通過後始可連線。在一些送審的學校架構中，我們發現虛擬位址的採用已是不可避免的趨勢，但是這些採用虛擬位址的學校，卻沒有辦法在流量統計中同時完成真實位址與虛擬位址的紀錄。仔細探究其原因，幾乎都是因為網路架構所造成的限制。大部分的學校只要經過適當的調整網路架構，這些問題就可克服。網路架構如果設計不當，不僅可能無法滿足功能面的需求，同時可能會耗費更高的建置成本。現在我們將一些規劃網路架構的重點及需求列舉如下：

1. 在穩定度的考量上，NAT 應採用 Router 級或 Core Switch 級的網路硬體設備，而不使用個人電腦或工作站以軟體的方式進行轉換 [3]。
2. 在效能的考量上，NAT 設備不應該成為網路流量的瓶頸。例如：當與 TANet 界接採用 Gigabit Ethernet 時，NAT 設備就必須支援到相同的速率，而不能僅支援到 Fast Ethernet 界面。
3. 在整個校園內，真實 IP 位址與虛擬 IP 位址應視為同等的校園 IP 位址，每個校內的伺服器都可以紀錄校內用戶端的 IP 位址，不管是真實 IP 位址還是虛擬 IP 位址。
4. 只有在出校園的 WAN 端出入閘口才加裝 NAT 轉換設備。轉換時，只轉換虛擬 IP 位址的部分，至於真實的 IP 位址則不受轉換影響可進行雙向連線之建立。
5. 在流量統計的應用時，必須紀錄 NAT 轉換之前的流量，而不是紀錄 NAT 轉換之後的流量，如此才能同時紀錄真實 IP 位址與虛擬 IP 位址的流量。
6. 在流量的收集上，必須只有一個流量的來源，使得我們在統計上僅需要採用一台流量統計伺服器即可進行統計。不應該分別針對真實 IP 位址及虛擬 IP 位址進行統計，造成資訊上無法整合，且浪費硬體資源。
7. 在取出網路流量時，不應該將真實 IP 位址的流量以及虛擬 IP 位址的流量分別取出，再利用集線器進行合併。利用集線器合併二者網路流量將可能導致封包的衝撞而使得統計值變得更不精確；再者，若網路已提昇至 Gigabit Ethernet 如此高速的界面，如何取得

Gigabit Ethernet Hub 亦是個問題。

8. 紀錄網路流量時，不得造成流量的重複計算，例如：不可同時計算虛擬 IP 位址的流量以及 NAT Spool 真實 IP 位址的流量，這將導致網路流量的重複計算。
9. 在進行路由政策的規劃時，不僅要考慮流量統計及位址轉換的問題，同時也必須滿足 TANet 新骨幹連線申請的「不當資訊管制」要求，必須能處理 Transparent Proxy [5]的路由政策。
10. 在建置規劃上，應該也要考慮未來的擴充性及網路應用。例如：如果需要在校內 WAN 端出入閘口加裝流量管制設備或入侵偵測系統時，應該要能很容易地整合進來，並且這些設備也應該能同時管制或偵測到真實 IP 位址及虛擬 IP 位址。也就是說，這些設備應該裝在 NAT 轉換設備之內，而不是裝在 NAT 轉換設備之外。

經過實際的上線測試與調校，本校終於找出一個 TANet 新骨幹連線架構，不僅可以同時滿足上述的需求，而且建置成本也不甚高，非常適合即將申請或開始規劃 TANet 新骨幹連線申請的學校作為參考。在接下來的章節裡，我們將針對暨有的網路架構作探討，說明這些架構所存在的問題。針對這些問題，我們在第三節提出二個解決方案，分別應用於低階與高階的網路設備上，讓連線學校可按照其既有設備的功能選擇適當的建構方案。最後，我們將在第四節作簡單的結論。

2. 既有網路架構

圖 1 是典型的校園網路架構。校園內，以一台高階的 Core Switch 作為交換中心，其下以光纖連結至各大樓，再以 Access Switch 連接個人電腦。校內提供至少一台 Proxy Server，作為 WWW 瀏覽的快取及過濾。

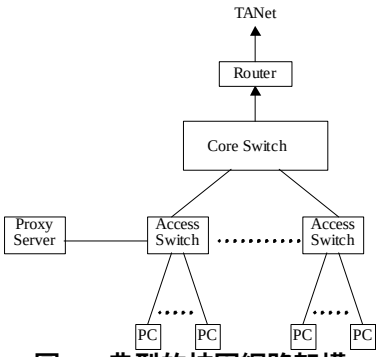

圖 1. 典型的校園網路架構

為了避免學生在宿舍架設地下網站，TANet 曾經建議各校將宿網改用虛擬 IP 位址。同時，一般的電腦教室也不會放置對外服務的伺服主機，因此也建議在電腦教室採用虛擬 IP 位址，以節省真實 IP 位址的需求。

在快速建置及降低成本的考量下，一些學校會考慮使用 Linux 等系統作為 NAT 轉換設備，並將 NAT 直接接在宿網的出入口，作為宿網的位址轉換。由於一般個人電腦僅提供 10/100 M RJ-45 界面，所以這個 NAT 設備會以二條 UTP 短線直接接上 Access Switch，再以 VLAN 的切割方式強迫宿網流量經過 NAT 的轉換 (如圖 2)。

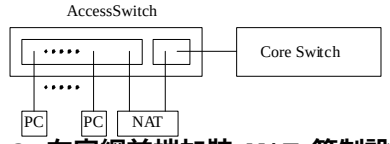

圖 2. 在宿網前端加裝 NAT 管制設備

在宿網之前加裝 NAT 裝置是個快速解決地下網站的方式，但卻不是最好的方式。第一個問題是該 NAT 容易成為宿網的瓶頸。目前大部分的校園網路都採用光纖作為骨幹線路，連接 Core Switch 及 Access Switch 大部分也都採用 Gigabit Ethernet。在 Access Switch 上，大部分只有二個 Gigabit Ethernet 界面，一個用來連接 Core Switch，另一個則用來作為串接擴充 Switch 之用。剩下的 Switch Port 都只是 10/100M 的 Fast Ethernet 界面，因此，即使 NAT 伺服器提供了 10/100/1000M 的乙太網路界面，最多也只有 100M 的速度，將大幅限制網路的傳輸效能。

這個問題還有解決的方法，如果 Core Switch 上具有空的 10/100/1000M 的乙太網路界面，就可以將 NAT 設備直接接在 Core Switch 上，透過 VLAN 的切割即可解決。不過，如果有多個 NAT 設備就要佔用多個 Core Switch 上的乙太網路界面，如此也要付出較高的成本作為代價。

除了上述效能的問題外，另一個問題則是連線來源不容易追蹤。例如：當宿網電腦大量使用 Proxy Server 去擷取檔案時 (如 FlashGet [2])，可能造成 Proxy Server 的過量負擔；或者，當宿網電腦感染了類似 Code Red [4]病毒而發作時，亦可能造成 Transparent Proxy Server 的沈重負擔。如果要透過系統 log 來找出用戶端的位址，將會得到 NAT Spool 的位址，而不是真正的用戶位址。

基於這二點理由，NAT 建置應儘量把位址轉換設備往外推，最好是安裝在學校 WAN 端的出入閘口 (如圖 3)。

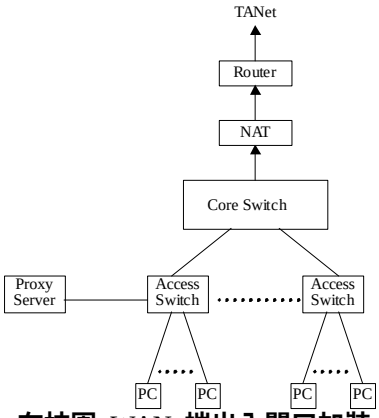

圖 3. 在校園 WAN 端出入閘口加裝 NAT

在校園 WAN 端出入閘口加裝 NAT 具有下列幾個好處：

1. 通常 LA N 的頻寬要比 WAN 的頻寬來得高，在 WAN 端加裝 NAT 設備並不會造成傳輸效能的重大影響。
2. 全校只需要使用一個 NAT 設備即可，不需要在宿網、電腦教室之前都加裝 NAT 設備，可以降低建置成本，並使維護更加容易。
3. 全校各個網路區段都可以使用虛擬 IP 位址，而不限定只有宿網或電腦教室，可以降低真實 IP 位址的需求。
4. 校園內的伺服器所紀錄到的用戶端 IP 位址就是真正的連線 IP 位址，而不是經過 NAT 轉換後的位址，對於問題的追查會更為容易。
5. 宿網內部亦可讓學生練習架站，服務對象也被限制為校內的使用者。如此不僅可達到讓學生練習架站的目的，又不致於影響到 TANet 的正常運作。

若要採用圖 3 的網路架構，必須要有下列先決條件：

1. NAT 界面的速度不應低於 WAN 端線路的速度，否則 NAT 設備將成為校園連外的瓶頸。
2. 該 NAT 設備必須具有部分轉換的功能，也就是說，當來源位址是真實 IP 位址時，不得被 NAT 設備作位址轉換。只有當來源 IP 位址是虛擬 IP 位址時，才進行位址轉換。

如果學校所申請的 TANet 連線速度在 100M 或以下時，第一個條件就影響不大。因為目前大部分的 NAT 設備都具有 10/100M 的傳輸界面，不會成為連外的傳輸瓶頸。但是如果學校所申請的 TANet 連線界面是 Gigabit Ethernet 時，這個條件就值得考慮了。因為具有 Gigabit Ethernet 界面的 NAT 網路設備 (Router 或 L3 Switch) 都非常昂貴，如何降低 NAT 建置成本是個重要因素。

至於第二個問題，如果所使用的 NAT 設備不具有部分轉換的能力，凡是經過 NAT 的網路封包都一律會進行位址轉換，此情形亦不適用於圖 3 的網路架構。因為在此情形下，就等於將全校所有電腦都打入虛擬 IP 位址，不僅使用上不方便，在管理上建立 NAT 對應表格亦非常費事耗時。

對於第二個問題，一些廠商提供了他們的解決方案：利用 Core Switch 的 Policy Route 來解決，也就是讓 NAT 設備的進、出兩端都接在 Core Switch 上，再利用路由政策來解決 NAT 的封包流向 (如圖 4)。

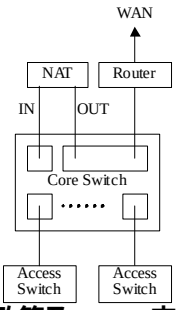

圖 4. 使用路由政策及 NAT 來解決部分位址轉換的功能

在圖 4 中，Core Switch 的 Default Gateway 指向對外的 Router，但是在 Core Switch 中使用 Policy Route 讓所有虛擬 IP 位址對外的封包均導入 NAT IN 的線路。NAT 在完成位址轉換後將封包直接送往對外的 Router (其中 NAT OUT 與 Router 設定在同一個 VLAN 上)。同樣地，在對外的 Router 上也設定路由政策，當封包從外界流入校內時，該 Router 就判斷是否目的位址是 NAT Spool 的位址範圍；如果是的話，就以路由政策導向 NAT OUT，否則就是一般的真實 IP 位址，直接送往 Core Switch 即可。

使用圖 4 的網路架構有個好處，其 NAT 設備不必具有部分位址轉換的功能，即使採用較低階的網路設備或伺服主機，只要具有 NAT 基礎轉換能力的功能，就足以勝任。

但是，這個網路架構在流量統計上卻出現了問題：我們無法同時統計到正確的真實 IP 位址與虛擬 IP 位址的網路流量。如果我們只針對 Core Switch 到 Router 之間的 VLAN 作監測，這樣就只能得到真實 IP 位址的流量；如果只針對 Core Switch 到 NAT IN 的 VLAN 作監測，就只能得到虛擬 IP 位址的流量；如果同時將這二者 VLAN 導出來進行監測，則 NAT Spool 的位址部分又會被重複計算。

不僅在流量統計上會造成問題，在流量的控

制及未來的應用上也會出現問題。例如：在此架構下，如果要加裝入侵偵測系統或頻寬管理器，就只能裝在 Core Switch 與 Router 之間，但這種作法將無法順利追蹤或管理到虛擬 IP 位址的電腦。

3. 解決方案

在我們所提出的解決方案中，將分為二種模式來探討，第一種是屬於較低階的作法：假設 Core Switch 不具有 NAT 能力，須使用外部 NAT 設備來作轉換，且該 NAT 也不具有部分位址轉換的能力，對外網路頻寬最高也僅達 100M bps 速率。這種解決方案適合於一般規模較小的學校使用。第二種則屬於較高階的作法，假設 Core Switch 已具有 NAT 轉換的能力，且連外的速率已達 1Gbps (Gigabit Ethernet)。這種解決方案適合於大專院校直接以 Core Switch 與 TANet 新骨幹作連接。

在第一種模式下，如果對外 Router 具有二個 LAN 連接埠，則可以直接使用圖 5 的架構來解決。Core Switch 及 Router 分別以路由政策的設定來達到分流的效果，也就是真實 IP 位址的網路封包走右邊 (Core Switch 直接接到 Router 的線路)，虛擬 IP 位址的網路封包則走左邊 (Core Switch 經 NAT 到 Router 的線路)。至於流量統計的工作，就使用 Core Switch 的 SPAN 功能直接將對外的二條線路的網路封包複製出來。

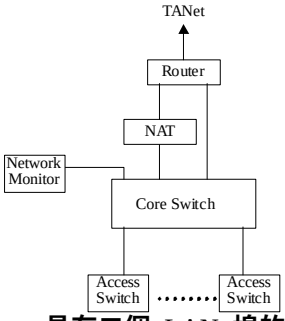

圖 5. Router 具有二個 LAN 埠的解決方案

如果 Router 僅具有一個 LAN 埠，或者另一個 LAN 埠要與 TANet 新骨幹串接，則 NAT 與 Router 之間就必須加裝 Switch 或 Hub 來擴充，感覺上就比較繁瑣 (如圖 6)。

事實上，界於 Router、NAT 以及 Core Switch 之間的連接設備 (Switch 或 Hub) 可以使用 Core Switch 的三個 Fast Ethernet 連接埠來取代，只要將那三個連接埠劃成獨立的 VLAN 即可 (不可在第三層建立對應界面)，如此即可使用單純的跳線來解決繁瑣的設備串接問題 (如圖 7)。

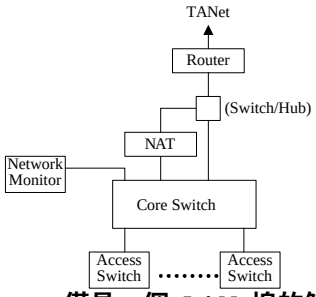

圖 6. Router 僅具一個 LAN 埠的解決方案

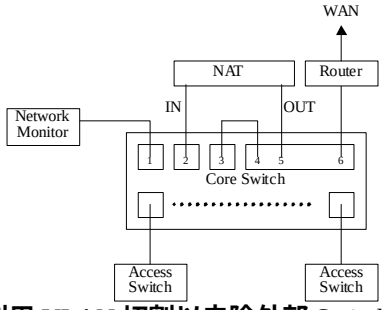

圖 7. 利用 VLAN 切割以去除外部 Switch 的需求

注意到圖 7 中，Core Switch 的第 3 及第 4 個連接埠使用了跳接短線，看起來似乎具有 loopback 的效果。這個 loopback 短線不能移除，也不能將第 3 埠與 4/5/6 三埠的 VLAN 作合併，否則網路架構將會退化成圖 4，也就無法作準確的流量統計了。

在流量統計上，利用 Switch Port 1 作為 SPAN 的導出埠，同時監看第 2 及第 3 埠的流量狀態。在此架構下，可能會收到來自第 4/5/6 埠 VLAN 的 ARP 廣播封包，但這個對我們的流量統計幾乎不構成影響。

圖 7 的網路架構在本校已實際運用了一年多，在尚未連接到 TANet 新骨幹時，本校就是採用這種網路架構，一切運行都非常正常。

如果要考慮未來的擴充性，例如加裝主動式入侵偵測系統或頻寬管理器，這些裝置就可以插入 Core Switch 與 NAT/Router 之間，此時網路架構就如圖 8。同樣地，所增加的 Switch 或 Hub 亦可用圖 7 的技巧來取代。

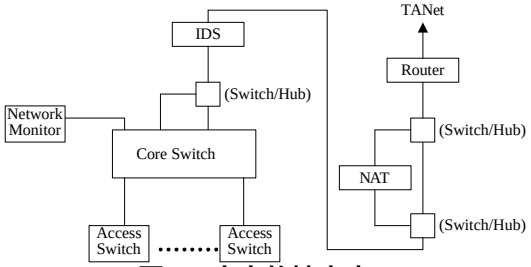

圖 8. 未來的擴充應用

接著，我們要討論第二種模式，也就是假設

Core Switch 已具有 NAT 的轉換能力 (如 Cisco 6509 Multi-Layer Switch)，並且假設學校將以該 Switch 的 Gigabit Ethernet 連接埠直接與 TANet 新骨幹串接。

在 1Gbps 高速的需求下，具有這種連接界面的網路設備都非常昂貴 (如 Cisco 7200 系列)。若改用伺服器 (Linux + 2 GB Ports) 的解法，其 NAT 的穩定度及效能可能不比硬體網路設備來得佳。因此，我們沒有理由使用外掛的 NAT 設備而捨棄 Core Switch 的 NAT 轉換功能。

如果不考慮流量統計的問題，直接使用高階 Core Switch 就可以與 TANet 新骨幹的連接，當然，NAT 的部分位址轉換也可以在 Core Switch 中完成 (如圖 9)。

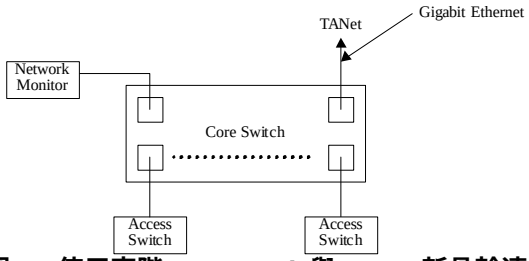

圖 9. 使用高階 Core Switch 與 TANet 新骨幹連接

在圖 9 中，使用 SPAN 功能將通往 TANet 的所有網路封包都複製到 Network Monitor 上，但這裡所得到的網路封包都是經過 NAT 轉換之後的結果，因此無法得到 NAT 轉換之前的虛擬 IP 位址流量統計。

如果要取得 NAT 轉換之前的網路封包，就不可以讓校內對校外的網路封包直接送往 WAN 端，必須將這些封包送往中繼站，然後再對這個中繼站作 SPAN 監控流量。例如：我們可以在 Core Switch 上新增一個 Vlan (如圖 10)，將所有校內往校外的封包都送往此 Vlan，然後再由 Vlan2 送至 TANet；同樣地，當 Vlan2 收到來自 TANet 的封包時，也先送往此新增的 Vlan，然後再傳送到正確的目的地。

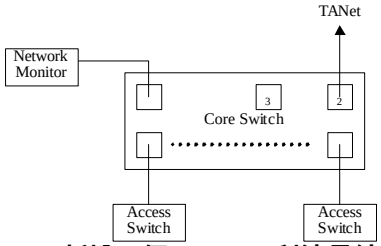

圖 10. 新增一個 Vlan 以利流量統計

理論上，這個構想應該可以解決流量統計的問題，但不幸地，在實際的 Cisco 6509 Multi-Layer Switch 上卻無法運作。不過，就算可以正常運作，這個構架在擴充上也有所限制，未來如果要與入侵偵測系統或頻寬管理器結合，也會面臨無法處理虛擬 IP 位址的問題。

按照圖 10 的架構加以修改，藉由一個外部的 L3 Switch，分別連接 Core Switch 的二個獨立 Vlan，這個問題就可迎刃而解。在圖 11 中，L3 Switch 分別與 Core Switch 的 Vlan3 與 Vlan4 相連接，而 Vlan2 則與 TANet 相連接。所有校內通往 TANet 的網路封包都以 Access Switch→Vlan4→L3 Switch→Vlan3→Vlan2→TANet 的方式傳遞；同樣地，當 TANet 的網路封包流入校園內部時，即按照相反的流向進行。

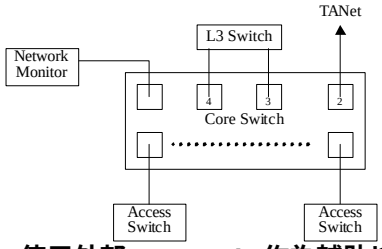

圖 11. 使用外部 L3 Switch 作為輔助以解決 NAT 與流量統計的問題

為了能確保網路封包的流向能按照我們的需求進行，必須設定適當的路由政策。首先，將連接 TANet 新骨幹的 Switch 位址設為 Default Gateway，讓所有對外的封包最後都能從 Vlan2 送往 TANet。接著，設定一組路由政策，供校內所有 Vlan 使用。Core Switch 路由政策如下：若網路封包的目的地是校內位址，則不作更改，直接送往目的地所對應的 Vlan；其餘的網路封包都送往 L3 Switch 的 Vlan4 界面。L3 Switch 只作簡單的靜態路由設定：若網路封包的目的位址是校內，則送往 Core Switch 的 Vlan4 界面，否則以 Default Route 送往 Core Switch 的 Vlan3 界面。在 Core Switch 的 Vlan3 上必須設成 NAT Inside，並且指定 NAT Source 位址為校內的虛擬 IP 位址。在 Core Switch 的 Vlan2 上則設為 NAT Outside。此外，還須在 Vlan2 上加入路由政策，讓所有進入校園的網路封包都送往 L3 Switch 的 Vlan3 界面 (可參考[1]的重要設定)。

完成上述路由政策的設定後，所有往來校內與校外的網路封包都一定會流經 L3 Switch，所以，只要將 Core Switch 連接 L3 Switch 的任何一個界面以 SPAN 方式重導網路封包，就可以讓 Network Monitor 接收到往來校內與校外之間的封包，而且包含了所有的真實 IP 位址封包與虛擬 IP 位址的封包。

除了網路流量的統計外，對於未來的擴充應用也非常方便。例如，當我們欲加裝主動式入侵偵測系統或頻寬管理器，可以很容易地加入或移

除這些新增的設備。在架構上，我們可以按照圖 12(a) 或圖 12(b) 進行實體設備的連接。這二者之間的實際線路接法完全相同，所不同的部分僅在於系統的設定。在圖 12(a) 中，我們新增一個 Vlan5 以連接外部 IDS 系統，將原來 Core Switch 上 Vlan4 界面的位址移除，並將該位址指定給 Vlan5 界面，如此即完成 IDS 的插入。當然，若因為某種因素而必須移除 IDS 時，可以再將 Vlan5 界面的位址移回到 Vlan4 界面即可。所以，只要系統建置完成後，要新增或移除 IDS 系統僅需要針對 L3 的設定作修改即可。至於圖 12(b) 的方式就更簡單了，只要針對連接埠的 Vlan 對應作變更，即可動態地加入或移除 IDS 系統。換言之，整個設定也僅需要在 L2 部分作修改即可。

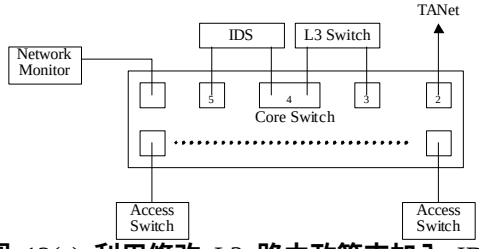

圖 12(a) 利用修改 L3 路由政策來加入 IDS

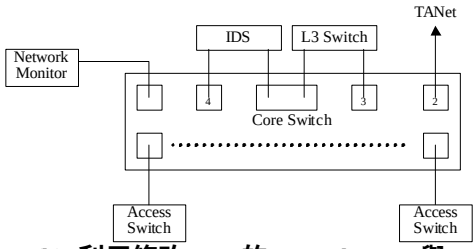

圖 12(b) 利用修改 L3 的 Switch Port 與 Vlan 對應來加入 IDS

除了未來的入侵偵測系統或頻寬管理器之類的應用外，對於網路監控也有很大的幫助。目前我們所採用的網路流量統計大多數屬於 Sniff Based 技術 (Attach 模式)，這種方式的好處是不會影響網路傳輸的效能，但缺點是無法保証可以 100% 地捕捉到所有的網路封包。雖然這個影響在流量的統計分析上差異不大，但是如果要進行 Layer 7 的分析時，遺漏封包就可能導致無法重組整個傳輸過程。此時，只有將 Sniff Based 的方式改為 Pass Through 方式，也就是強迫將所有的網路封包都必須流經 Layer 7 Monitor，再由該 Monitor 作封包 Forwarding 的工作，如此才能保証所有的封包都不會遺漏。若要將外部的 Monitor 由原來的 Attach 模式改為 Pass Through 模式，在本網路架構上可以很容易地施行。

自從本校申請 TANet 新骨幹的連線申請後，就開始規劃這種新的網路架構。目前本校已成功地利用 Cisco 6509 Multi-Layer Switch 直接與 TANet 新骨幹連接，並且採用 Gigabit Ethernet 作為連接界面，運作至今都非常順暢。

4. 結論

如果要同時作到虛擬位址的應用以及完整的流量統計，沒有經過精心的規劃是很難兩全其美的。本文中，特別針對二種網路設備的層次來作規劃，一種是適合於網路設備較為低階的環境，另一種則是適合於網路設備較為高階的環境。不管是在哪一種環境，我們都可以在校園內讓真實 IP 位址與虛擬 IP 位址混合使用，並且可以在校園 WAN 端出入口處正確地進行網路流量的統計，包含真實 IP 位址與虛擬 IP 位址。這二種網路架構都經過本校正式上線運行測試，是個實際可行的解決方案。

目前 TANet 新骨幹採用 Cisco 6509 Multi-Layer Switch 作為核心交換器，許多學校也跟隨採用相同的設備連上 TANet 新骨幹。本文所提供的高階網路設備環境正是以此設備作為對象，如果這些學校尚無法同時兼顧虛擬位址應用與網路流量統計者，可直接套用本文的網路架構，以獲得立即的成效。至於其他學校網路設備與本文所提不同者，本文亦可提供設計上的參考，以期找出流量統計與虛擬位址應用二者兼顧的網路架構。

參考文獻

1. http://cc.shu.edu.tw/~nm/sample.txt
2. http://www.amazesoft.com/
3. http://www.netfilter.org/documentation/HOWTO/NAT-HOWTO.html
4. http://www.symantec.com/avcenter/venc/data/codered.worm.html
5. http://www.tldp.org/HOWTO/TransparentProxy.html