

# 學生宿舍網路管理與頻寬調節系統之研製

周文正

國立清華大學計算機與通訊中心

新竹市光復路二段 101 號

TEL : (03)5731122 , FAX : (03)5710776

E-Mail : [wjchou@cc.nthu.edu.tw](mailto:wjchou@cc.nthu.edu.tw)

## 摘要

近年來隨著網際網路快速成長，網路人口日益增多，網路頻寬使用量亦隨之快速提升。因此 TANet 與各校園主幹頻寬皆不斷逐年擴充更新，以滿足網際網路 WWW 各種影音聲光多媒體多元化的應用需求，然而不管是 TANet 主幹或校園網路，其絕大部份的頻寬卻由各校學生宿舍網路所佔用，其中高比例的使用人口、多媒體風行與擅自建置地下非法主機是主因。現況雖有主幹網路流量監測與告警，但仍未能徹底解決宿網濫用頻寬的老問題。除此之外，宿網茲因用戶異動頻繁與人口日漸增多，時有非法入侵他人系統，MAC 卡號與 IP 位址常被盜用，用戶缺乏自行檢測網路設備的工具，以及考慮網管運轉之方便性與時效性等。故本篇論文敘述以 WWW 為基礎的學生宿舍網路管理輔助系統(NMAS)的功能與應用經驗，嘗試解決上述有關問題，其中 NMAS 包括：用戶資訊管理、連線記錄追蹤、設備故障網路傳呼告警、用戶端網路埠流量自動監測、網路使用過量時實施間歇式停用的管理策略，以及相關查詢等功能，期以導正宿舍網路使用風氣，促進 TANet 與校園宿舍網路頻寬的有效運用與宿網管理績效。

**關鍵字：**網路管理、流量監測、頻寬調節、網路傳呼、全球資訊網

## 一、簡介

利用網路傳媒是目前學術研究、教育、生活不可少的基本設施，隨著網際網路的風行，網路人口日益增多，多媒體多元化的應用，導致網路頻寬使用量亦日益提升。如何確保網路暢通，以及如何迅速而有效地掌握網路情況，並適時處置與控制網路，勢必成為各網際網路服務者(ISP, Internet Service Provider)、電信網路提供者、以及企業內部網路(Intranet)維護者所面對之重要課題[1]。目前教育部與各區網中心，對 TANet 主幹進行流量監測與出國應用型態資流管控不遺餘力[2][3]，目前已發揮立竿見影之效。

近年來各大專院校極力推動校園網路的普及化固然重要，然而在校園扮演 ISP 角色的計算機中心，除了一般性行政業務電腦化、用戶帳號與儲存空間的管理、技術諮詢與支援、校園資訊網路建置與管理維護，以及提供 E-Mail、DNS、NEWS、WWW 等網際網路服務之外。常會面臨不容忽視的問題是：網路頻寬的有效運用與網路的維護效率。尤其最近 TANet 與各校園主幹頻寬皆不斷逐年擴充更新，以滿足網際網路 WWW 各種影音聲光多媒體多元化的應用需求，然而絕大部份的頻寬卻由各校學生宿舍網路所佔用，其中高比例的使用人口、多媒體風行與擅自建置地下非法主機是主要導因。雖目前已在 router 間執行阻隔網路芳鄰功能，但跨

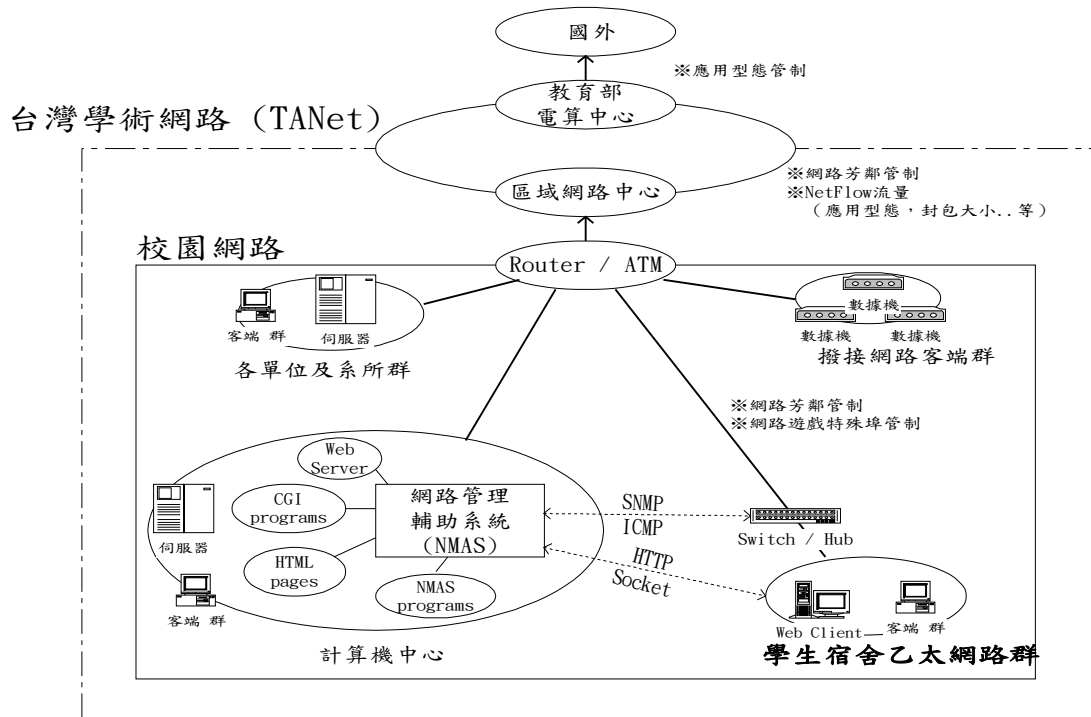
router之TCP/IP 應用(如 ftp 主機)與宿網內部網路芳鄰的資源共享仍是非常普遍。另一方面，雖能藉行政管理規章明定宿網內嚴禁擅自建立共享主機，以強化回歸宿網用戶應如同”撥接網路群”純屬客端(client)的角色，但主機的認定與取締方式仍有可議的空間。因此，我們在具有共享式的乙太區域網路架構下，進行用戶端網路流量自動計測，網路使用過量時實施間歇式停用的管理策略，期以杜絕宿網內建立諸如網路芳鄰與 ftp 主機，達到有效調節用戶端網路頻寬與發揮宿網應有的網路客端機能。

除此之外，宿網茲因用戶異動頻繁與人口日漸增多，時有非法入侵他人系統、MAC 卡號與 IP 位址也常被盜用、以及用戶自行檢測網路設備的工具仍嫌不足等問題。因此，實有需要宿網管理工具以常態記錄與管理用戶端的網路使用屬性資料，其中應該包括：用戶基本資料、用戶埠、網路連接設備埠、網路流量、MAC 卡號、IP 與 DNS 等項目。故本文之目的是敘述以 Web-Based 的學生宿舍網路管理輔助系統(Network Management Assistant system, NMAS) 之功能與應用經

驗，NMAS 的功能除了早期[4]原包括：用戶申請與管理、IP 與 DNS 管理、設備管理等功能改善之外、另加強網路設備存活偵測與即時通報、用戶端網路量測與統計、間歇式用戶端網路頻寬調節、用戶連接網路記錄之追蹤偵查，以及相關查詢等功能，期以促進 TANet 與校園宿舍網路頻寬的有效運用與宿網管理績效。

## 二、網路管理現況與 NMAS

整個 TANet 的连接組態是：校園區網→校園主幹→TANet 主幹，此形成階層式的網網相連，每階層網路皆需要透過 router 開道才能訊息交換，如圖(1)所示。TANet 各主幹區網中心無不終日盡職待命，不餘遺力以維持主幹正常運轉，同時大家也感受到網路使用頻寬日益不足，在現實的成本考量，不允許不斷以增加硬體線路來直接解決頻寬日益拮据的問題。目前最經濟之道無不透過主幹流量內容的統計分析，檢查是否有不當之應用存在，或是缺乏效率的頻寬濫用，再藉由進一步的管制措施，限制某些應用的傳輸，以確保其他應用的正常傳遞，是目前網際網



圖(1) 網路管理現況與 NMAS

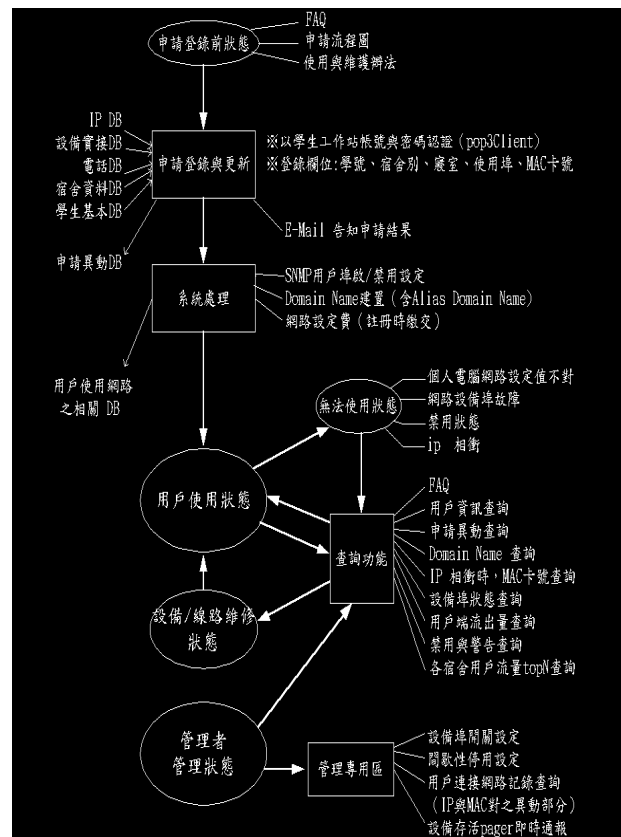
路上對於頻寬問題的常見作法[2][3]。例如：各區網中心對 TANet 主幹常利用 Cisco 所提供的 NetFlow，進行資料統計與應用型態分析(如 web、telnet、email、mail、dns 等)，進而在出國端依應用型態的不同實施分時分流的管制 [2][3]，目前已發揮立竿見影之效。

如圖(1)可知：在校園網路部份，可管控的樞紐要點是 router、switch/bridge，可藉由 access list 或 filtering/forwarding 的功能，針對 IP 或 MAC 卡號進行資流統計與管制，中央大學宿網管理就是一個成功的例子[5]。以清大宿網管理而言，目前除了用戶需經申請才能開啟網路設備埠(hub's port)准予使用之外，router 也已進行網路芳鄰與網路遊戲特殊埠管制，讓誇 router 的網路芳鄰之資流無法通行。然而由於網路多媒體易於分享(如 ftp 主機、網路芳鄰等)，導致宿網的多媒體資料(如圖片、VCD、網路電玩等)流通更為猖獗，使宿網內部 intranet 頻寬大部份仍被網路芳鄰與 ftp 所佔用。因此，若能消除非正當性用途的地下網路主機，讓大部份的宿網用戶角色回歸如同撥接網路群純屬客端(client)的角色，那麼善用宿網與主幹頻寬可望會有正面的效果。另一方面，雖能藉行政管理規章明定宿網內嚴禁擅自建立共享主機，但主機的認定與取締方式仍有灰色可議的空間。因此，清大 NMAS 嘗試實施自動監測用戶端網路埠的流出量，訂定違規次數，自動網路流量核驗，執行間歇式停用的管控策略，讓同學有自省自律的空間，畢竟有限的乙太網路頻寬是共享式的設施。

NMAS 對網路管理的角色分工而言，較著重處理 layer2 所能提供的資訊，由於較低階，因而較容易有效直接管制用戶端的網路使用。因此，NMAS 與主幹網路較高階的資料型態分析並未衝突，反而各有所司，互補互利。

### 三、NMAS 網管功能

NMAS 網管系統功能之設計考量，除了考慮網管功能本身是否能滿足各項自動化網路管理工作之需求之外，也需符合管理者與用戶在網路維運時各種操作上的方便性，因此，NMAS 是利用 WWW 環境開發的網路管理系統，不管用戶或管理者皆能藉由 Web 瀏覽器(browser)完成所有作業，NMAS 應用狀態與功能示意圖如圖(2)所示。



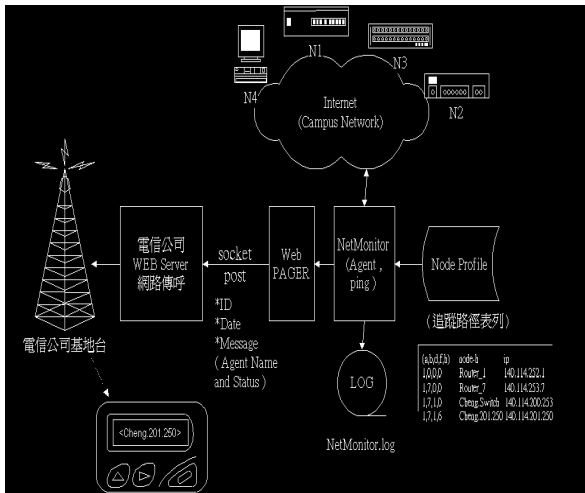
圖(2)NMAS 應用狀態與功能示意圖

以下列舉部份功能並進一步說明：

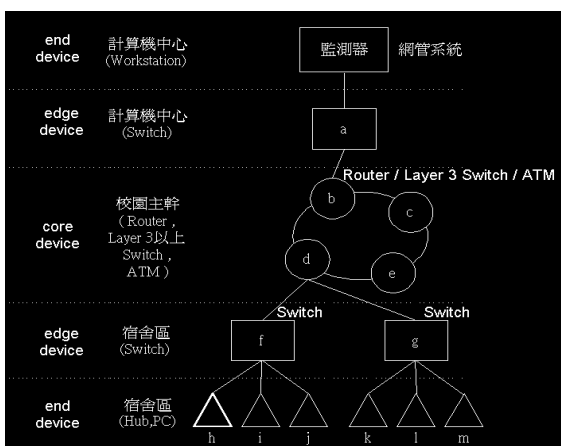
#### (1)設備故障即時通報

考慮網管運轉之方便性與時效上之立即性，網路故障發生時必須儘可能於最短的時間內將故障排除，以維持正常的網路服務。對網管系統而言，欲達到縮短故障時間的目標，應具備強而有力的設備故障即時通報功能[1]，以便能在發現故障時，藉由故障告警功能通報網管人員。現今網路設備無不透過

SNMP [6]網管軟體(manager) , 以週期性輪詢方式(Polling) 地監控分散各地的各被管設備(agent) , 若各地的設備點無回應或有異樣時, 設備會立即對網管系統回報(trap)事件, 或由網管主動監測以異樣顏色顯示狀況。因此, 為期改善管理者須終日守著網管系統才能得知網路設備存活狀況的缺點, 以及提高網路設備維護績效, 我們發展網路監控代理者程式, 隨時監測所管設備的存活狀況, 若有網路節點消失或回生時, 即可透過網路傳呼 (pager) 方式[7,8]通報網路設備現況, 其架構圖如圖(3)所示。



圖(3) 網路設備現況之網路傳呼通報架構圖



圖(4) 以網管系統為中心的階層結構圖

設備故障即時通報的方法如下：

(a) 建置以監測器為中心的節點連接路徑表列 (node profile), 以監測器為中心 (視為

根點), 展延至各方向的網點, 即可構成階層性結構的連接關係, 由根點至各受管節點稱為可追蹤路徑。如圖(4)所示, 例如受管 h 點的可追蹤路徑是 ( a,b,d,f,h ), j 點為 ( a,b,d,f,j )。

(b) 以 ping 依受管節點路徑表列, 求出是否應該藉由網路傳呼回報狀況。例如：有一受管節點的路徑為(a,b,d,f,h), 若 d、f、h 三節點故障時只通告 d 節點; 而不會通告 f、h 節點, 此只回報最臨近網管之受測點演算法如表(1)。

```

/* 回報最臨近網管之受測點演算法 */
for each T_node in Managed_NODE
## T_node = h
{
  get pathNode-list of T_node from NodeProfile
  ## pathNode-list(h) = (a,b,d,f,h)
  PreNode_status = "";
  for each Ping_Node in
    PreList(pathNode-list(T_node))
  ## PreList(pathNode-list(h)) = (a,b,d,f)
  {
    if ( ping_status(Ping_Node) == "alive")
  ## Ping_Node = a、b、d、f
  {
    PreNode_status = "down";
  }
}
if ((PreNode_status != "down") and
    (ping_status(T_node) == "down"))
{
  WebPagerCall("T_node DOWN !!");
}
if ((PreNode_status != "down") and
    (History_status(T_node) == "down"))
{
  WebPagerCall("T_node UP !!");
}
}

```

表(1)：回報最臨近網管之受測點演算法

(c) 以上 ping(agent ip) 只能檢測 agent Hub , 對同一工作群的其他非 agent Hub, 可藉 SNMP(agent IP, hubID , portNO) 方式監測。

## (2) 用戶資料查詢

對於扮演 ISP 角色的計算機中心, 能有網

路用戶的使用記錄資訊是很重要的，用戶資訊至少應包括：用戶基本資料(用戶碼、姓名、系所單位、E-Mail、聯絡電話等)、開始使用日期、用戶埠、網路連接設備埠(agentIP、hubID、portNO)、MAC、IP 與 DNS 等項目，完整的用戶資訊有助於日後網路管理維護與異狀追蹤。

### (3) IP 相衝時，以 MAC 查詢

NMAS 定期以 SNMP(agentIP, ObjectID) 至網路設備連接埠(hub's port) 蒐集用戶端殘留的 MAC 卡號，並建立設備位置與 MAC 卡號的對應關係。當用戶發覺別人 IP 與自己的相衝時，即可藉由對方的 MAC 卡號找出來源的設備位置與其使用者的基本資料。因此，儘管 MAC 卡號與 IP 位址易被盜用，而此種直接提供用戶端 MAC 卡號的用戶資料，有助於快速解決 IP 相衝問題。

### (4)設備埠狀態查詢

導致網路不通的原因很多，當網路不通時，能瞭解用戶所連設備是否正常是最基本的需求，尤其 NMAS 是以網路設備(hub)連接埠作為管制的物件。因此，能藉由用戶碼或設備位置，來查詢用戶端網路設備連接埠的開關(enable/partition)狀態，是有助於縮小診斷網路連線故障點的範圍。

### (5)用戶連接網路記錄之追蹤偵查

IP,MAC 異動查詢，NMAS 除記錄用戶端的流量之外，並會擷取用戶端流出的 MAC 卡號。另一方面可由 Router/Switch 的 ARP 表格內，存取 IP 與 MAC 二者的對應關係，常態追蹤建置用戶 IP 與 MAC 對(ip-mac pair)之異動時的歷史記錄，進而以 ARP's MAC 與 hub-port's MAC 作關係連結，找出當時的用戶資料。因此，當有用戶異常連網時，能以下列查詢方式，進行追蹤偵查用戶

連網記錄：

(a)以 MAC 卡號查詢其用戶名稱、使用設備埠、發生地點(寢室埠)、發生時間，以及 IP 對應等歷史記錄。

(b)以 IP 或用戶碼或使用設備埠，查詢上項所述的歷史記錄。

### (6)用戶流出量查詢

當用戶被 NMAS 警告或間歇式停用網路時，可藉由此功能充分瞭解自己的流出量，以除去心中疑慮，期以用戶自我節制調整或自行關閉共享主機。

### (7)禁用或警告查詢

提供用戶與網管人員瞭解網路管控的現況與歷史記錄，其中每筆記錄包括：實施日期、恢復使用網路的時間(expire time)，以及當時用戶符合管控條件的流量記錄。當網路不通時先得知停用狀態，有助於網路管理維護。

### (8)各宿舍 TOPN 查詢

顯示各宿舍用戶流出量的排行榜，反應宿舍網內資源共享的使用現況，提供網路社區用戶間的自律空間。畢竟在共享式有限頻寬的環境下，非必要性的網路傳輸是需要自律的。

### (9)設備埠啟禁設定

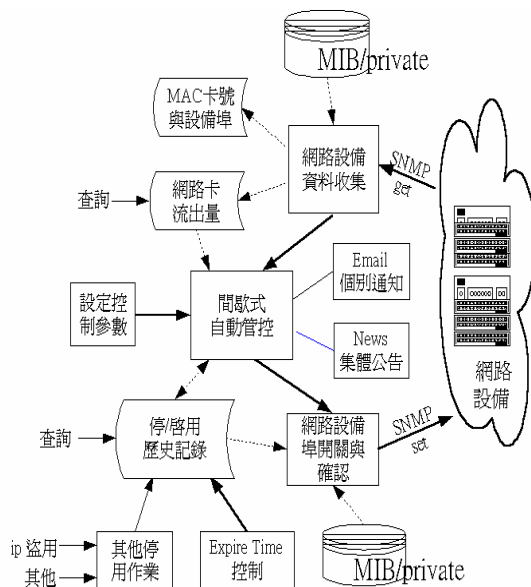
只允許管理者以用戶碼或用戶所用設備位置，再配合 community 字串，即可藉由 WEB 瀏覽器進行線上設備埠啟用或停用設定，在多用戶與多廠商設備的環境裡，此種作法可略去多重廠商傳統網管系統的牽究與不便。

### (10)間歇式宿網停用

各校宿舍網路已建多年，除了有前面所述網路頻寬濫用的問題之外，也會面臨宿網用戶逐年漸增與學校經費短缺的窘境，因此，

有效善用宿網內部頻寬以及發揮主幹應有的網路機能，實需要調節用戶網路頻寬的管理策略。基本上間歇式宿網停用的管理策略是：訂定違規流量、次數與懲罰方式，自動流量監測核驗，各別告警，公開告發，線上自動執行間歇式停用管控等措施。其頻寬管控功能與作業流程請參考圖(5)，間歇式宿網停用方法與步驟如下：

- (a).管理者設定間歇式控制參數，其中包括：警告與停用的關卡設限值 (threshold)、恢復時間與違規次數累計之處理等。以供系統執行管控之依據。
- (b).網路設備資料收集模組針對不同廠商設備(MIB)，每小時以 SNMP 監測各用戶設備埠(hub'sport)之流出量，並建立相關可分析與查詢的檔案格式。
- (c).管理者設定間歇式控制參數，其中包括：警告與停用的關卡設限值 (threshold)、恢復時間(expire time)與違規次數累計之處理等，以供系統執行管控之依據。



圖(5) 間歇式頻寬管控功能與作業流程

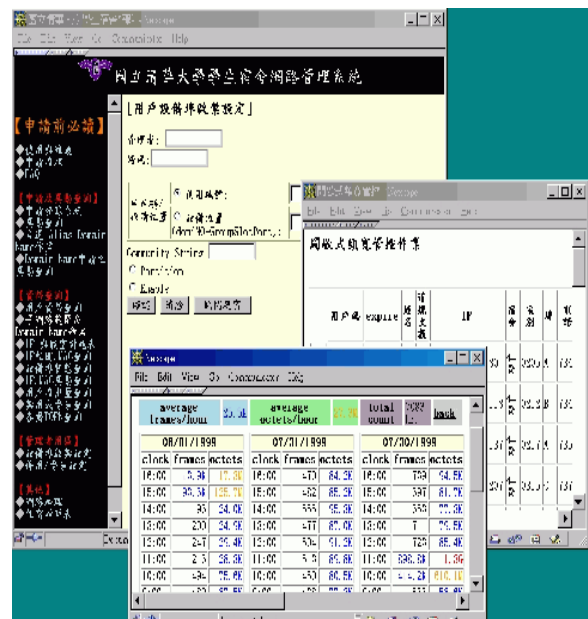
- (d).若用戶平常超過警告界定值，系統會自動以 E-Mail 告知用戶注意改善。經警告後用戶單位時間之平均流量仍超過停用界定

值，管控模組會依其停用歷史記錄與系統控制參數，研判如何執行間歇式停用。系統同時以 E-Mail 告知各別用戶，News 集體公告處理情形。

- (e).恢復時間控制模組每天定時檢查停用記錄，若已到期限，即開啟設備埠恢復使用。
- (f).另提供其他停用作業介面，例如：IP 盜用等。
- (g).被處理的用戶可藉由 WWW 以用戶碼與密碼查詢自己一週內每一小時的流量細項，以助釐清疑慮。

#### 四、NMA 與作業範例

NMA 作業範例畫面請參考圖如(6)[9]。NMA 是以 HTML、CGI、perl5、JavaScript，以及 SDB (Simple Data Base) 為發展工具。其中 SDB 是 Berkeley DB File (以 HASH 為主檔；以 B-TREE 為索引檔) 使用 perl5 自行開發的共用模組(public module)，SDB 目前除了允許多重索引(multiple index)、複合鍵(compound key)、部份匹配(partial matching)等功能之外，另有公用服務程式協助 SDB 的維護。



圖(6) NMA 作業範例

在發展相關 CGI 程式時，除了可藉由用戶碼與密碼存放管制之外，有必要以瀏覽器的 IP 作為限制對象，其中必須考慮瀏覽器是否有無透過 proxy 主機存取，下面是 perl 簡單的範例片段：

```
if ($ENV{'HTTP_X_FORWARDED_FOR'} eq "")
# 若 HTTP_X_FORWARDED_FOR 環境變數是空字串，代表
# 瀏覽器
{ $REMOTEIP = $ENV{'REMOTE_ADDR'}; }
# 並無透過 proxy 主機存取，則環境變數 REMOTE_ADDR 的內
# 容即為瀏覽器的 IP
else
{ $REMOTEIP = $ENV{'HTTP_X_FORWARDED_FOR'}; }
#透過 proxy 主機存取時，環境變數
# HTTP_X_FORWARDED_FOR 的內容即是瀏覽器的 IP
```

至於相關 SNMP 程式的設計，目前清大宿網所用的乙太網路 Hub 有：Accton Hub、Synoptic Concentrator/Hub 與 Bay Hub 等設備。設計 SNMP 程式之前，須先依照所需功能找出標準 MIB[10]所定義的 Object ID 字串，再由 MIB browser (例如 EliteView 網管系統有提供) 測試驗證 Object ID 的可用性，有的受管設備 agent 並沒有完全符合標準 MIB，此時需由各廠商提供設備的私有 MIB 文件，經 MIB compiler 後，再以私有 Object ID 由 MIB browser 測試驗證，若經驗證無誤即可再藉由引含 public domain 所提供的 perl5 public module[11]，進行 SNMP perl 程式設計與測試，必要時再與 WWW CGI 程式結合。

目前 NMAS 部份功能仍繼續改良發展中，其無不追求更有效率簡便的管理與操作方式。經過上一學期的實地測試，針對間歇式宿網停用的功能部分，關卡設限值暫定為平均流出量為 5 天 5GigaBytes，即用戶連續 5 天每天平均有 5 小時 448kbps 的流出量 (448kbps\*60s\*60m\*5h=1G) 就假定是主

機，違規者會被警告或停用一段時間，被警告或停用的同學已有收斂自律的反應，並達到預警與嚇阻作用，惟控制參數標準的擬定(例如關卡設限的合理標準值)，有待進一步分析探討與調整的必要。

## 五、結論

本論文敘述清大 WWW-based 宿網管理系統之功能與應用經驗，其中 NMAS 有下列特點：

1. 用戶需經申請才能開啟網路設備埠准予使用，充分掌握用戶基本資料，便於事後管理與使用付費。
2. 準確記錄用戶上線記錄，遇有異狀網路連線，有助於追蹤偵查，達到示警防範作用。
3. 儘管 MAC 卡號與 IP 位址易被盜用，仍能提供精確的 MAC 用戶查詢，有助於快速改善 IP 相衝問題。
4. 即時監控通報網路設備的存活狀況，縮短待修等候時間，以提高網路使用率。
5. 即時提供用戶端網路設備連接埠的開關狀態，有助於用戶自行診斷，以降低維護工時。
6. 準確量測用戶端網路埠的流出量，實施宿網間歇式停用的管理策略，配合相關流量與警/停用之查詢，讓同學有自省自律的空間，以期杜絕擅自架設非法主機與過度使用網路芳鄰，導正宿舍網路使用風氣。進而有效調節用戶使用網路頻寬，藉此促進 TANet、校園與宿舍網路頻寬之有效運用。

NMAS 對網路管理的角色分工而言，目前較著重處理 layer2 所能提供的資訊，由於較低階，因而較容易有效直接管制用戶端的網路使用。其與主幹網路較高階的資料型態之限時分流並未衝突，反而各有所司互補互

利。但就系統維護而言，當某宿舍的設備廠牌型號與組態變更時，NMAS 的 SNMP 程式部分需緊隨更新，才能發揮應有的網管效果，畢竟 NMAS 網路資料管理與用戶端設備息息相關。

任何業務之推展，需擬訂或修正適於實況技術之管理制度與發展所需之應用系統環境，才能發揮管理上應有之預期效果。現階段在未有新的可行與管理方案(例如：宿網設獨立 private ip 透過 VPN 分向分流分頻等)之前，若各校皆能消除非正當性用途的地下網路主機，讓大部份的宿網用戶角色回歸如同撥接網路群純屬客端的角色，那麼善用宿網與主幹頻寬可望會有正面的效果。

#### 參考文獻

- [1]. 陳彥錚、林正森、羅中奇等(1998 年 10 月),“利用 WWW 技術開發 HiNet 網路管理系統—HiView”, 第四屆台灣區網際網路研討會 (Tanet'98), p.3c-15 ~ 3c-23.
- [2]. 劉大川、張傑生、楊子翔(1998 年 10 月),“台灣學術網路出國線路壅塞狀況之分析研究”, 第四屆台灣區網際網路研討會 (Tanet'98), p.5c-15 ~ 1c-26.
- [3]. 蕭漢威、陳年興(1998 年 10 月),“網路流量統計分析及其管理意函”, 第四屆台灣區網際網路研討會 (Tanet'98), p.5c-1 ~ 1c-14.
- [4]. 周文正, (1995 年 10 月),“學生宿舍網路管理環境的建立”, 第一屆台灣區網際網路研討會 (Tanet'95).
- [5]. 包元輝、戴元任、曾黎明(1998 年 10 月),“網路自動化管理系統之研究發展及應用”, 第四屆台灣區網際網路研討會 (Tanet'98), p.1c-15 ~ 1c-23. RFC 1157, “Simple Network Management Protocol(SNMP)”
- [6]. 孫三為、王亮惟、莊德政、梁冠雄、林怡年、許家彰等(1998 年 10 月),“整合網際網路與無線通訊之訊息服務 (HiAir)”, 第四屆台灣區網際網路研討會 (Tanet'98), p.6a-15 ~6c-20
- [7]. ALPHA Call 網上傳呼, <http://www.pager.com.tw/web/webtopager/webcall.asp>
- [8]. NMAS , <http://thccx11.cc.nthu.edu.tw/~dormnet/dormnetMgr.html>
- [9]. RFC 1213 , “Management Information Base version II (MIB-II)”
- [10]. Simon Leinen, “SNMP support for Perl 5”,
11. <http://www.switch.ch/misc/leinen/snmp/perl/>.