ADSL Proxy Server 建置與管理

范修維　廖鴻圖　邱孟佑　伍啟錄
世新大學資訊管理學系、世新大學電算中心
fan@cc.shu.edu.tw

摘要

目前 TANet 出國頻寬不足，導致各級學校對國外連線過於緩慢。為了解決出國連線緩慢的問題，各大專院校紛紛加裝 ADSL 線路連接 HiNet，以使用 HiNet 出國的頻寬。然而，一般學校往往只將 ADSL 線路作為 WWW Proxy，除此之外就未能再加以利用。事實上，這條線路還可以作為電子郵件的備援系統、DNS 代理查詢、NAT 位址轉換以及流量統計等服務，尤其是在 TANet 斷線時，更可突顯其優點。除了各大專院校自行加裝 ADSL 線路通往 HiNet 外，還可以在各區網中心設置，以供下游連線學校使用。由於 ADSL 線路的伺服器安裝與設定有別於一般的網路伺服主機，必須要經過許多步驟的設定才可完成。因此，本論文乃針對 ADSL 線路的利用提出建議方案，並提供參考設定指引，使得各校網路管理人員可以不必再經過太多的摸索階段即可有效地利用 ADSL 線路。

關鍵字：ADSL、Proxy、E-Mail、DNS、NAT、MRTG。

1. 前言

由於網路使用人口與日俱增，各級學校也鼓勵校內同仁及學生上網，因此網路頻寬的需求就日益迫切。雖然教育部已積極改善 TANet 內部頻寬，但是 TANet 對國外連線的頻寬仍然不足，導致國內各級學校與國外連線過於緩慢。為了解決出國頻寬不足的問題，各大專院校開始考慮加裝 ADSL 線路連接 HiNet，以利用 HiNet 的出國頻寬。不過在線路的使用上，各校往往僅侷限於 WWW Proxy 的應用，使得這條線路的效益沒有充分發揮，殊為可惜。

雖然 ADSL 線路可以解決 WWW 瀏覽速度的問題，但是對於電子郵件的收發仍舊沒有助益。目前 TANet 對出國頻寬進行管制，讓大部分的頻寬保留給 WWW Proxy 使用，剩餘的少數頻寬才提供給其它的網路應用。在此政策下，國內各級學校寄往國外的電子郵件就變得非常緩慢，經常一堆信件塞在 Mail Queue 中等待寄發，且寄發的過程又常常因為 Timeout 而必須重寄。不僅信件寄往國外非常困難，就連收取國外信件也非常緩慢。如果我們能將電子郵件的收發重導向由 ADSL 線路，不僅可以改善電子郵件收發的效能，還可作為電子郵件的備援系統。

雖然新增加了 ADSL 線路通往 HiNet，但是如果沒有經過特別的處理，當 TANet 斷線時，使用者仍然無法瀏覽網頁。最主要的問題就是校內的 DNS 系統仍然是走 TANet 線路，當 TANet 斷線時，當然無法查到網址所需要的 IP，因此就算擁有 WWW Proxy 也沒有用。此時，最佳的解決方案就是在 ADSL 線路上加裝 DNS 系統，作為 DNS 的 Cache Only 查詢[1]，而校內原有的 DNS 主機則可以使用 Forward 功能將 DNS 查詢導向到 ADSL 線路。因此，即使 TANet 斷線，仍然可以使用 ADSL 線路進行 WWW 的瀏覽。

若要充分利用 ADSL 通往 HiNet 的線路，可以再於該線路上加裝 NAT [2] 功能，使得在同網段的電腦都可以直接使用 ADSL 高速頻寬，此時不僅在 WWW 瀏覽可以暢行無阻，就連 TELNET、FTP 等網路服務都可以獲得改善。

當然，如果在 ADSL 線路上加裝 SNMP 的伺服程式，就可以使用 MRTG [3] 的統計能力來進行線路流量的監測，作為第二條線路擴充的評估依據。

雖然通往 HiNet 的 ADSL 線路具有多項頻寬改善的功能，但是並非所有學校都能自行申裝，有些學校是因為地理環境不允許，有些學校則是經費不足，尤其是中小學更面臨這方面的問題。這時，可由區網中心申裝 ADSL 線路，以供下游連線學校使用。即使只使用一條 ADSL 線路，下游學校也必能感受到比 TANet 直接出國的速度來得快些。當然，除了速度的改善之外，備援能力的增加也是另一項附加價值。

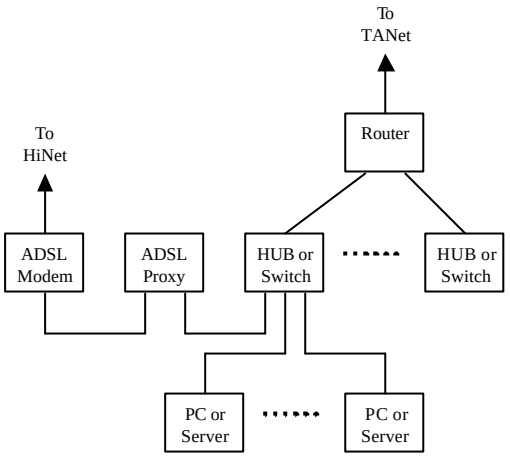
要獲得上述的效益，並不需要太多的硬體配置，除了 ADSL 線路及 ADSL Modem 之外，僅需提供一台電腦以提供各項服務。為了讓各校網路管理人員能更瞭解 ADSL Proxy 的使用方式，我們將各項功能的設定步驟列於第二節。對於區網中心加裝 ADSL Proxy，以及下游學校的使用方式，也於第三節提出我們的建議。最後，我們再針對此系統作簡單的結論。

2. 校內 ADSL Proxy 的設定

2-1 系統架構

當 ADSL 線路申裝後，中華電信會提供一個 ADSL Modem，一端連接電話線，一端則提供乙太網路界面。為充分利用該線路，我們找尋一台個人電腦作為 ADSL 的 Proxy Server (簡稱 ADSL Proxy)，其上安裝 Linux 作業系統以及 squid 套

件，即可提供全校師生作為 WWW 的 Proxy Server。在 ADSL Proxy 上安裝二片網路卡，一片連接 ADSL Modem，另一片則連接到校園網路的 Hub 或 Switch，而該 Hub/Switch 再透過路由器連接到校內其它網段。



圖一　ADSL 線路及 Proxy Server 與校園骨幹連接架構圖

為了方便後續的 NAT 使用，將網路界面 eth0 與 ADSL Modem 連接，並給予 HiNet 的 IP，例如：211.22.95.162，另一張網路界面 eth1 則與校園網路相連接，並給予 TANet 的 IP，例如：192.192.150.17。

2-2 基本路由設定

在 ADSL Proxy 上必須設定 Default Gateway，但是如果設定不當，則可能會讓系統變得非常緩慢，甚至無法使用。如果我們將 Default Gateway 設為校內的 Router，則 ADSL Proxy 將無法透過 ADSL Modem 去抓取資料，因此 ADSL Proxy 的 Default Gateway 勢必要指定為 ADSL Modem。此時，校內電腦在使用 ADSL Proxy 時就會面臨下列問題：

1. 如果校內電腦使用 ADSL Proxy 的 TANet 介面 (亦即 eth1) 作為瀏覽器的 Proxy Server 位址，則只有與 ADSL Proxy 相同網段的電腦可以使用，校內其它網段的電腦將無法使用。因為校內其它網段的電腦會送出網路封包到 ADSL Proxy 的 TANet 介面，但是 ADSL Proxy 卻會將結果由 HiNet 介面送出，導致其它網段的電腦無法使用。
2. 如果校內電腦使用 ADSL Proxy 的 HiNet 介面 (亦即 eth0) 作為瀏覽器的 Proxy Server 位址，則可以正常運作，但是速度將會變得異常緩慢，因為其所有網路請求將會透過 Router 的 WAN Port 送往 TANet，再轉往 HiNet，最後再由 ADSL Modem 進入 ADSL Proxy，而回應的網路傳輸也將反應繞一大圈才回到校內的個人電腦。

為解決上述的問題，可將校內的 IP 範圍以 Static Route 的方式鍵入 ADSL Proxy 中。亦即，在 /etc/rc.d/rc.local 尾端加入下列指令即可：

```
    /sbin/route  add  -net  192.192.148.0
netmask 255.255.255.0 gw 192.192.150.254
dev eth1
                        …
    /sbin/route  add  -net  192.192.159.0
netmask 255.255.255.0 gw 192.192.150.254
dev eth1
```

上述指令中，必須將「192.192.148.0」改為自己校內所擁有的網段，並且將「192.192.150.254」改為 ADSL Proxy 所在的 Router Port 位址。如果校內有多個網段，則必須將每個網段都加以設定。

在完成 ADSL Proxy 的路由設定後，校內師生即可將電腦的 Proxy Server 位址設為 ADSL Proxy 的 TANet 介面位址，如此就不會發生速度緩慢或根本無法使用的情形。

2-3 DNS 解析重導

當 TANet 發生斷線時，雖然校內 ADSL 線路維持在正常狀態，但校內仍無法正常使用 WWW 瀏覽器，最主要的問題就是在於 DNS 查詢。一般學校的 DNS 主機都配置在 TANet 上，所以 DNS 的查詢自然也會向 TANet 線路丟出，而當 TANet 斷線時，DNS 查詢自然無法完成。此時，如果將校內的 DNS 主機的查詢請求轉向到 ADSL Proxy，再由 ADSL Proxy 往 HiNet 線路進行查詢，就可以得到 DNS 的解析。

要完成這種 DNS 重導的設定，必須在 DNS 主機及 ADSL Proxy 上作設定。在 DNS 主機上，僅須在 /etc/named.conf 檔案內的 options 設定中加入 forwarders 即可，例如：

```
options {
    directory "/etc/named";
    pid-file  "/etc/named/named.pid";
    notify yes;
    forwarders {
          192.192.150.17;
    };
    allow-transfer {
          192.192.150.1;
          192.192.155.129;
    };
};
```

至於 ADSL Proxy 上僅需完成 DNS 的 Cache Only 設定即可，例如：在 /etc/named.conf 僅要設定下列敘述：

```
options {
    directory "/etc/named";
    pid-file  "/etc/named/named.pid";
};

zone "." in {
```

```
    type hint;
    file "named.root";
};
```

至於 DNS 系統的 Root Zone 則可由校內第一台 DNS 主機內拷貝（本例是放置於 /etc/named/named.root 檔案中）。

如果完成了 DNS 解析的重導，則在 TANet 斷線時，校內電腦仍可透過 ADSL 的 Proxy 功能進行 WWW 的瀏覽。

2-4 電子郵件外送重導

如果僅利用 ADSL 線路作為 WWW 的 Proxy，將可發現 ADSL 線路幾乎只有使用到下傳的頻寬，至於對外的頻寬則幾乎沒有用到 (這個現象可透過後述的 SNMP + MRTG 統計得到証實)。雖然 ADSL 是非對稱式的線路，但是在 1536K/ 384K 的線路上，仍有相當大的對外頻寬可用。

雖然 ADSL Proxy 解決了 WWW 瀏覽的問題，但是電子郵件的寄送仍過於緩慢。由於 TANet 對國外線路進行了頻寬限制，將大部分頻寬保留給 WWW 的 Proxy 使用，其餘的網路應用就只能擠在剩餘的頻寬裡。如果校內老師經常與國外通信，就會發現信件的寄送非常不易。對於電子郵件的管理者，也可以從 Mail Queue 中發現許多寄往國外的信件因逾時而重寄。如果我們把電子郵件系統的外送信件重導到 ADSL 線路，將可增快信件的寄出，又可降低原有學校對外的 TANet 頻寬需求，可謂一舉兩得。

若要將電子郵件系統的外送信件重導到 ADSL 線路，則必須在電子郵件主機及 ADSL Proxy 上面作設定。在電子郵件主機上，必須將 /etc/mail/sendmail.mc 中加入下列敘述：

```
    define(`SMART_HOST',
`hinet2.proxy.shu.edu.tw.')dnl
```

然後再重新產生 /etc/mail/sendmail.cf，並重新啟動 sendmail daemon 即可。如果在系統中沒有 /etc/mail/sendmail.mc，則可以自行到相關網站 [4] 取得。(注意：上述指令的頭尾引號是不相同的。)

至於 ADSL Proxy 上，也必須啟動電子郵件的服務，並開放郵件轉寄的權限。例如：若電子郵件主機的領域名稱為「cc.shu.edu.tw」，則必須在 /etc/mail/access 檔案中加入

```
    cc.shu.edu.tw  RELAY
```

敘述，然後在 /etc/mail 目錄下執行下列指令：

```
    makemap hash access < access
```

最後，再重新啟動 sendmail daemon 即可。

2-5 電子郵件備援系統

除了讓電子郵件系統的外送信件重導到 ADSL 線路外，我們也可以將收信的功能重導到 ADSL 線路，如此一來，不僅可加速國外電子郵件的接收，更可作為電子郵件收信的備援系統。即使 TANet 或 ADSL 線路其中任何一條線路故障，都還是可以接收到來自校外的信件。

若要完成此項功能，除了在電子郵件主機及 ADSL Proxy 要進行設定外，還必須在 DNS 系統上進行設定，其過程可能較為煩瑣。首先，必須在 DNS 系統上登記

```
cc.shu.edu.tw.   IN A 192.192.150.10
mail.shu.edu.tw. IN A 192.192.150.10
```

其中第一行是原來的電子郵件主機名稱，第二行則是內部轉信時使用，在後續的電子郵件主機及 ADSL Proxy 設定中將會用到。除了上述二個名稱外，ADSL Proxy 的二個網路介面也都要設定名稱：

```
hinet2.proxy.shu.edu.tw. IN A 192.192.150.17
hinet2.mail.shu.edu.tw.  IN A 211.22.95.162
```

前一項設定是針對 ADSL Proxy 的 TANet 介面，後一項設定是針對 ADSL Proxy 的 HiNet 介面。前一項名稱是提供給校內師生作為 Proxy Server 設定時使用，在電子郵件收信的備援上沒有用處；後者則是用來接收外界的電子郵件，對校內電腦而言並無作用。最後，必須再設定 MX 紀錄以達到收信的備援：

```
cc.shu.edu.tw. IN MX 30 hinet2.mail.shu.edu.tw.
cc.shu.edu.tw. IN MX 50 cc.shu.edu.tw.
```

加入這二項設定後，會讓信件由 ADSL Proxy 的線路接收，但是一旦 ADSL 線路出問題時，信件會自動由原來的電子郵件主機接收。

在電子郵件主機上，必須在 /etc/mail/local-host-names 中加入二道敘述：

```
    cc.shu.edu.tw
    mail.shu.edu.tw
```

加了這二道敘述後，電子郵件主機就可接收寄至這二個名稱的信件。

至於 ADSL Proxy 上，則必須將 /etc/mail/sendmai.mc 檔案加入下列敘述

```
    FEATURE(`relay_based_on_MX')dnl
    FEATURE(`virtusertable')dnl
```

並且重新產生 /etc/mail/sendmail.cf 檔。接著在 /etc/mail/virtusertable 中加入下列敘述

```
    @cc.shu.edu.tw    %1@mail.shu.edu.tw
```

注意，中間不可使用空白，須使用 <TAB> 鍵。完

成設定後，再於 /etc/mail 目錄中鍵入下列指令

```
makemap hash virtusertable < virtusertable
```

接著，必須在 /etc/mail/local-host-names 中加入代收信件的主機名稱

```
cc.shu.edu.tw
```

最後再重新啟動 sendmail daemon 即可。

2-6 NAT 設定

如果在 ADSL Proxy 上增加 NAT 的設定，則在校內與 ADSL Proxy 相同網段的電腦或主機都可以將 Default Gateway 設為 ADSL Proxy 的 TANet 界面，然後使用其 NAT 功能直接走 ADSL 線路與外界連絡。如此一來，不僅只有 WWW 的瀏覽可以加快，就連 TELNET、FTP 等功能都可享受到更高的連線速度。

如果要使用 NAT 的功能，必須要注意將 eth0 網路卡指定為連接 HiNet 介面，並將 eth1 網路卡連接為 TANet 介面，因為在啟動 NAT 之後，封包會由 eth1 到 eth0 作 NAT 轉換。如果二個介面指定不正確，NAT 將無法正常運作。要啟動 ADSL Proxy 的 NAT 功能其實很簡單，只要在 /etc/rc.d/rc.local 尾端加入下列敘述即可：

```
    echo 1 > /proc/sys/net/ipv4/ip_forward
    /sbin/ipchains -P forward DENY
    /sbin/ipchains    -A    forward    -s
192.192.150.0/24 -j MASQ
    /sbin/modprobe ip_masq_ftp
```

最後一行是為了讓 NAT 可以轉換 FTP 的功能而設定的。如果要讓 NAT 通過更多的網路應用，請自行增加[B]。另外，上述第三行的「192.192.150.0」網段須改為 ADSL Proxy 的 TANet 介面所處的網段。

除了 ADSL Proxy 設定之外，其餘的個人電腦也必須設定，只要將個人電腦的 Default Gateway 設為 192.192.150.17 (ADSL Proxy 的 TANet 介面位址) 即可。

2-7 流量統計

為了充分掌握 ADSL 線路的頻寬運用情形，可在 ADSL Proxy 上啟動 snmpd。如此一來，就可以利用 MRTG [C] 流量統計軟體來統計 ADSL Proxy 的流量。統計時，不妨針對 TANet 介面及 HiNet 介面分別作統計，更能掌握到 ADSL Proxy 所帶來的效益。

3. 區網及下游學校的設定

如果學校礙於經費考量，無法自行在校內加裝 ADSL 線路連接 HiNet 時，也可考慮由區網中心申裝，並開放給所屬下游連線學校使用。此時，區網中心的 ADSL Proxy 要進行下列設定：

1. 系統架構：
   仍然使用二張網路卡，將連接 TANet 的介面位址或對應的領域名稱公佈給下游學校，作為 WWW Proxy 使用。如果要提供電子郵件的備援服務，則必須再將連接 HiNet 的介面位址或對應的領域名稱公佈給下游學校，作為 DNS 的 MX 紀錄設定之用。
2. 基本路由設定：
   必須將所有下游連線學校的 IP 範圍都加入 ADSL Proxy 的 Static Route 中。
3. DNS 重導：
   不需要進行額外設定，只需完成 DNS 的 Cache Only 即可。
4. 電子郵件外送重導：
   在 /etc/mail/access 中加入下游學校的 SMTP 主機名稱，以提供 RELAY 服務。
5. 電子郵件備援：
   必須在 DNS 系統中指定 ADSL Proxy 的 HiNet 介面所對應的領域名稱，並修改 /etc/mail/sendmai.mc ，以產生新的 /etc/mail/sendmail.cf 設定檔，再於 /etc/mail/local-host-names 中加入下游學校的收信主機，並且在 /etc/mail/virtusertable 加入信件重導向的設定。
6. NAT 設定：
   此項功能無法提供下游學校使用。
7. 流量統計：
   此項功能無額外新增設定，僅須啟動 snmpd，並使用 MRTG 軟體進行流量統計即可。

至於下游連線學校，若要使用區網中心的 ADSL Proxy，則必須配合下列設定：

1. 系統架構：
   此部分與連線學校無關。
2. 基本路由設定：
   此部分與連線學校無關。
3. DNS 重導：
   當 TANet 斷線時，但連線學校與區網中心還保持連線狀態的話，可在校內的 DNS 主機加入 Forwarders 項目，再重新啟動 named，就可完成 DNS 重導的功能。
4. 電子郵件外送重導：
   在 /etc/mail/sendmail.mc 增加 SMART_HOST 的定義，並產生新的 /etc/mail/sendmail.cf 檔，再重新啟動 sendmail daemon 即可。
5. 電子郵件備援：
   必須在 DNS 上將收信主機取另一個名稱，以提供 ADSL Proxy 作內部信件的轉寄，並且定義 MX 紀錄，讓信件可由 ADSL Proxy 及原來的電子郵件主機共同收取。此外，在

/etc/mail/local-host-names 檔案中，必須將電子郵件主機的二個名稱都加入，才可以收信。

6. NAT 設定：
   此項功能下游學校無法使用。
7. 流量統計：
   此部分與連線學校無關。

除了上述各功能外，我們也建議下游連線學校自建 WWW Proxy Server，利用 squid [5] 的階層式架構來向區網中心的 ADSL Proxy 取得 WWW 的資料，這樣就可避免下游學校的電腦都直接將 WWW Proxy 指向區網中心，造成新的網路瓶頸。

4. 附加的功能

如果經常對電子郵件的 Mail Queue 作觀察，可能會發現某些主機經常連不上去，造成待送信件的累積及重試，例如：mail.pager.com.tw，使用者喜歡在自己收到信件時，同時將信件 forward 到該主機，而該主機卻經常無法連上，導致 Mail Queue 中產生一堆寄往該主機的信件。

如果校內已將 SMTP 重導向到 ADSL Proxy 上，則只要在 ADSL Proxy 上作簡單的設定即可過濾這些信件而不再對外發送。設定方法很簡單，只要在 ADSL Proxy 上的 /etc/mail/virtusertable 中加入

```
@mail.pager.com.tw     /dev/null
```

就可把寄往該主機的信件丟棄。

5. 結論

利用 ADSL 線路通往 HiNet 已是目前各校解決出國頻寬不足的普遍方案，但是 ADSL Proxy 伺服器的架設對網路管理者而言卻是新的嘗試。並非所有的網路管理者對各項設定都很熟，因此在架設 ADSL Proxy 伺服器時往往需要歷經許多摸索的階段。其實，經驗是可以傳承的，往往一些小小的提示都可以讓管理者避免許多無謂的嘗試。

本文提供了一些 ADSL 線路的利用方法及其設定方式，主要目的乃提供尚未申裝 ADSL 線路的學校作為參考。至於已申裝 ADSL 線路的學校，也可參考本文所敘的利用方式，評估是否仍有更多的改善空間。對於區網中心而言，也可重新思考要如何提供給下游連線學校更多的服務。

參考文獻

[1] http://dnsrd.nctu.edu.tw/

[2] http://metalab.unc.edu/mdw/HOWTO/IP-Masquerade-HOWTO.html

[3] http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

[4] http://www.sendmail.org/

[5] http://www.squid.org/