多條連外線路的對稱式路由策略

陳振庸、王鵬程、李乾麟、張永昌、柯守全*
修平技術學院、逢甲大學*
{jychen, pcwang, cllee, kenchang}@mail.hit.edu.tw, scke@fcu.edu.tw*

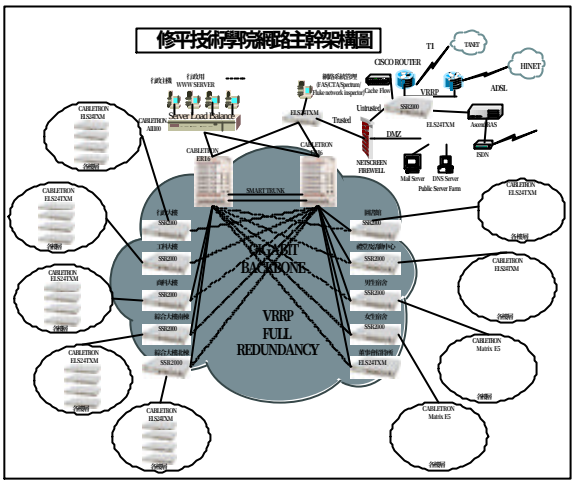
摘要

學術單位對連外頻寬的需求極為殷切，許多學校會利用有限經費租用其他 ISP 的線路做為替代線路，然而在 Routing 政策的限制下，替代線路大多呈現非對稱的使用型態，僅能用於紓解下傳的傳輸需求，對於上傳的需求還是只能利用 TANet 線路。為充分應用有限頻寬，我們利用 Static NAT、Dynamic NAT 及 Routing 機制，完成對稱式的路由策略的建置，在不影響原有網路服務亦不加劇 Router 負載情況下，開放上傳需求較高的服務如 Web、E-Mail 等，可以利用 ISP 所提供的 IP 對外提供服務，如此一方面充分應用有限頻寬，另一方面也提供更多管道的網路服務。

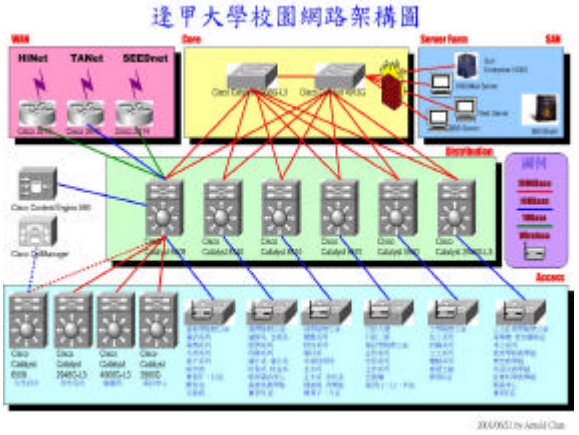
關鍵字：對稱式路由、網路管理

1. 動機

隨著資訊化與網路化的迅速成長，國內的網路人口迅速成長，加上全球資訊網、遠距教學等多媒體環境的成熟，使得網路頻寬的需求日益加劇。各級學校為了改善網路服務品質莫不投入經費積極建設校園網路，除了校園網路的建設外，租用 ISP 專線或 ADSL 線路來開闢多條連外線路亦相當普遍。以中部地區院校為例，修平技術學院校內已完成一個高可靠度而完整的 Gigabit 骨幹建置，連外線路則有 TANet T1、ADSL T1 及東訊 E1 等三條線路，如圖一所示 [1]，目前 ADSL 線路透過 Transparent Cache 來分擔 TANet 線路的 Web 流量；逢甲大學亦已完成校內高可靠度的 Gigabit 骨幹的建置，連外線路則有 TANet STM-1、TANet/I2 T1、HiNet T1、SEEDnet 128K 及 ADSL T1 等數條線路，HiNet T1 除了透過 Proxy Server 使用外，已開放一些網路服務，此外所有連外線路均透過 PAC 實施分流，如圖二所示 [2]。校內流量管理對電算中心人員而言都不是問題，而且頻寬也足以負荷，連外線路的管理反而較為頭痛，尤其頻寬有限又昂貴，如何達到最有效益的使用就格外重要了。



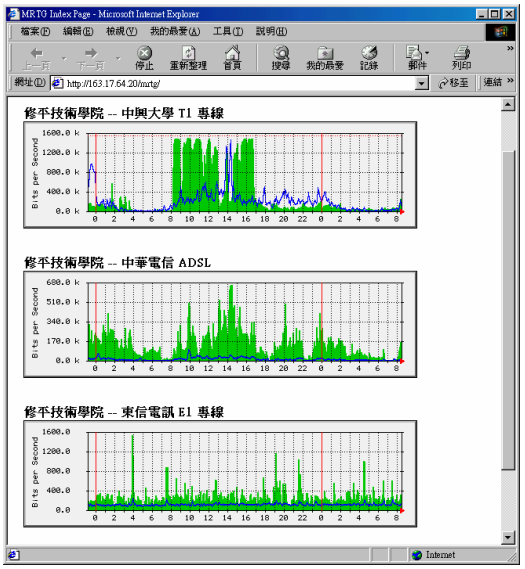
圖一 修平技術學院網路架構圖



圖二 逢甲大學網路架構圖

由於連外線路 Routing 的限制，各校租用的非 TANet 之替代線路所核發的 IP 極為有限，大多透過 Proxy Server 或 Policy Route [3,4]搭配 NAT/PAT [5,6] 使用該頻寬，因此傳輸型態幾乎都是非對稱式的，也就是以下載為主的傳輸型態，圖三所顯示的流量統計即可明顯看出各連外線路的使用型態。非對稱型態這對於 ADSL 類型的替代線路尚稱合理，但對於專線類型的替代線路則略覺上傳頻寬的浪費。修平及逢甲都租有專線類型的連外替代線路，每每碰到網路註冊選課或學期成績查詢等短暫但流量需求大的應用服務時，校外大量的存取使得 TANet 專線輸出幾乎維持滿載，替代線路應該要協助減輕

TANet 線路負擔才好，在此需求下我們積極嘗試各種技巧以便讓連外頻寬發揮更大效益。



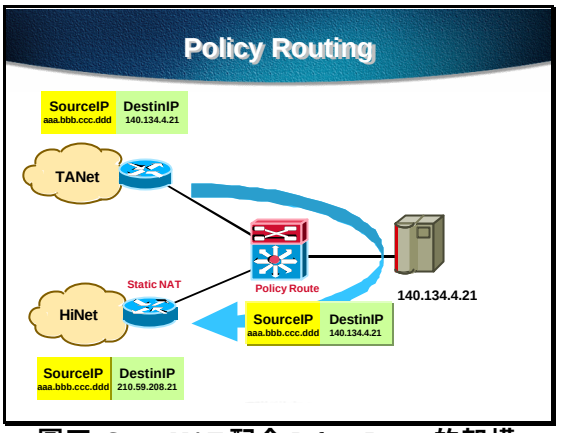
圖三 連外線路流量統計圖

2. 連外線路應用問題

以現在網際網路環境而言，電子郵件及全球資訊網網站已成為各校必備的網路服務項目，加上校務 e 化的需求漸增，Web-based 應用的便利性使得校務各項系統逐漸電腦化及網頁化蔚為趨勢，全校師生每日或多或少都會使用到網際網路，甚至已經成為日常生活的一部份，對網路傳輸品質的要求也就越來越高了，尤其是連外網路頻寬的建立、使用與管理，更是電算中心極為重要的工作項目之一。

連外線路的應用除了建置各項網路服務外，利用 Proxy Server 來加強與分擔網路傳輸負載是最常見的策略。如果建置有其他 ISP 替代線路的話，除了增加 Proxy Server 外，另外也可利用 Policy Route 搭配 NAT 來使用，讓更多的 IP 可以直接透過連外線路使用校外網路服務。如果是想利用替代線路提供校外網路服務如 E-Mail、Web 的話，最簡單的方式是在該範圍的 IP 網段上，直接建置相關的網路伺服器。這方法雖然簡單方便，但是必須要準備額外的伺服器軟硬體，不但增加了建置成本也增加了維護管理的成本，尤其是網站的維護涉及到內容一致性更是問題重重，即使用鏡射 Mirror 的方式，也必須注意所有網頁 URL 不能使用到固定的 IP。在逢甲大學 HiNet T1 線路替代路線上，我們就實際建置一部 Web 伺服器 (www.fcu.net.tw)，Mirror 逢甲大學網站 (www.fcu.edu.tw)的所有資訊，對外透過 HiNet 線路提供服務，Mirror 動作均利用夜間離峰時間，因此白天就可能出現網頁內容不一致的情況。此外此情況也僅較適合網頁完全集中的網站，超連結的 URL 即失去了應有的效果。

也有單位直接在網路服務的伺服器上增加建置一片網路介面，直接連接到替代路線網段上，成本要減輕很多，維護也較方便，但在 Default Route 的管理上卻十分麻煩，雖可以使用到替代路線提供網路服務，但是卻無法真的完全善用到各連外線路的頻寬。



圖四 Static NAT 配合 Policy Route 的架構

除了建置相關的網路伺服器外，我們第二個測試建置的方法為 Static NAT 搭配 Policy Route，如圖四所示。這方法設定、建置及維護都非常簡便，也很快就建立起網路服務來，但是很快的我們也發現 Router 負載因 Policy Route 而大增，且這種做法為非對稱式的 Routing 做法，也產生了一些其他的使用問題，使得效果極為有限且網路服務也不能太多。以逢甲大學為例，如圖二所顯示的網路架構圖，因全校性之網路伺服主機均已建置 Gigabit 介面直接建置在網路核心，在計劃讓辦公室自動化系統 Notes 伺服器可以利用 HiNet T1 專線傳輸時，建置的方式步驟如下：

1. 先在連接 HiNet 專線的 Router 上建立一個 Static NAT，讓 Notes 伺服器可以對應一個 HiNet 所核發的 IP。

2. 在骨幹交換器 Catalyst 6509 上建置 Policy Route，因 Gigabit 骨幹雙迴路的關係，必須比對由 Vlan 1 及 Vlan 2 所進入的封包，判斷 Source IP 及 Destination IP。當 Source 為 Notes Server 而 Destination 為校內 IP 時，維持原 Routing 路線，但若 Source 為 Notes Server，而 Destination 為校外 IP 時，則將 Next Hop 設定為 HiNet Router。

```
HiNet Router：
  ip nat inside source static
    140.134.4.21 210.59.208.21
  !
  interface Ethernet0/0
    ip nat inside
  !
  interface Serial0/0
    ip nat outside
  !
```

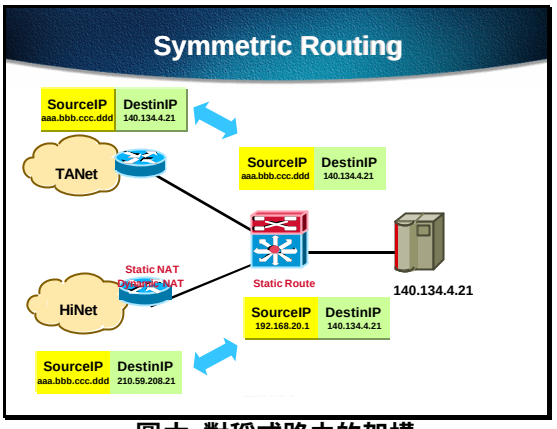
```
Core Router：
    interface vlan1
      ip policy route-map FCUoaRoute
    interface vlan2
      ip policy route-map FCUoaRoute
    !
    ip access-list extended FCUoa
      permit ip host 140.134.4.21
              140.134.0.0 0.0.255.255
    ip access-list extended FCUoaHi
      permit ip host 140.134.4.21 any
    !
    route-map FCUoaRoute permit 10
      match ip address FCUoa
    !
    route-map FCUoaRoute permit 20
      match ip address FCUoaHi
      set ip next-hop 210.59.208.253
```

圖五 Static NAT 及 Policy Route 設定資料

Static NAT 與 Policy Route 方式相關網路設備設定資料如圖五所示。此方法可免除額外網路伺服器的建置與維護成本，有需要增減網路服務時，只要調整 Static NAT 的對應資料，另外調整 Policy Route 的 Source IP 對應即可，維護上並不需要太多管理負擔。

3. 對稱式路由

Static NAT 搭配 Policy Route 的方法雖然可以利用連外替代路線建立網路服務，但是衍生許多使用與管理上的問題。首先是骨幹交換器負載亟劇增高，由於 Policy Route 所判斷封包 Source 及 Destination 的位置均在 Gigabit 骨幹介面上，因此流量本身即非常高，每個封包都要經過 Source 與 Destination IP 的檢查，對網路設備的負擔可想而知。第二個問題是 Policy Route 本身強迫將符合條件的流量轉往替代路線的 Router，而該 Router 輸出前透過 Static NAT 的設定，會將該 Source IP 轉為 ISP 所核發的 IP 地址，造成使用者由校外經 TANet 的存取，封包回傳卻經由非 TANet 的替代線路且 Source IP 並不一致，對網路正常存取便會造成莫大問題，也間接造成該網路資源校外僅能透過替代路線存取的反效果。



圖六 對稱式路由的架構

由於 Static NAT 配合 Policy Route 所產生的問題，我們最後改採用 Static NAT、Dynamic NAT 及一般 Routing 方式構築成對稱式路由(Symmetric Routing)的環境來，如圖六所示。同樣以逢甲大學 Note Server 服務為例，建置方式步驟如下：

1. 先在連接 HiNet 專線的 Router 上建立一個 Static NAT，讓 Notes 伺服器可以對應一個 HiNet 所核發的 IP，也就是將 Inside Local 的 IP 轉為 Inside Global 的 IP。

2. 在 HiNet 專線 Router 上建立一個 Dynamic NAT 的 Pool，讓校外存取的來源 IP 轉換為 RFC 所許可的 Private IP 範圍 [7]，也就是將 Outside Global 的 IP 轉為 Outside Local 的 IP。

3. 在骨幹交換器 Catalyst 6509 上增加一個 Static Route，Destination 為 Dynamic NAT 所分配的 Private IP，Next Hop 設定為 HiNet Router。

建置對稱式路由環境其原理事實上非常單純，將校外經由 ISP 所傳入的流量封包，除了 Destination IP 根據 Static NAT 轉成校內網路伺服器的真正使用之 IP 外，亦同時將 Source IP 透過 Dynamic NAT 轉換成另一個 Private IP，再連接到校內的網路伺服器。回傳封包則因骨幹交換器的 Static Route 設定，回傳封包會傳輸回替代路線的 Router。當封包是由 TANet 傳入的話，因為 Source IP 並未轉換為 Private IP，因此回傳封包根據 Routing 查詢仍經由 TANet 輸出，而達到對稱式路由的效果。相關設定資料如圖七所示：

```
HiNet Router：
    ip nat translation timeout 120
    ip nat pool NAToutaddr
          192.168.20.1 192.168.20.254
          netmask 255.255.255.0
    ip nat inside source static
          140.134.4.21 210.59.208.21
```

```
        ip nat outside source list natin
              pool NAToutaddr
        !
        interface Ethernet0/0
          ip nat inside
        !
        interface Serial0/0
          ip nat outside
        !
        ip access-list extended natin
          permit ip any host 210.59.208.21

    Core Router：
        ip route 192.168.20.0
            255.255.255.0 210.59.208.253
```

圖七 對稱式路由的設定資料

採用對稱式路由來建置替代路線的網路服務，較之 Policy Route 的方式有許多優點，最明顯的是大幅降低骨幹交換器的 CPU 負載。當使用 Policy Route 時，因當時設備為 Cisco Catalyst 5500，Routing 模組 RSM 本身的處理效率就不高，導致 CPU 負載約為 60%左右，但改用 Static Route 後 CPU 負載降低到 10%以下。第二是可以避免封包在 Policy Route 情況下被強迫往替代路線傳輸，因此由 TANet 線路來的存取需求，封包 Routing 還是會由 TANet 傳輸回去；由替代路線來的存取，封包 Routing 也會由該替代路線傳輸回去，符合對稱式的要求，亦可避免因 IP 變化而影響網路服務的使用。第三是維護管理方便，在 Policy Route 做法中，增減網路服務必須要修改替代路線 Router 及骨幹交換器之相關設定，在對稱式路由的環境下則只要修改替代路線 Router 設定即可，也就是增加一個 Static NAT 對應資料，另外在 access-list 上調整 Permit 的 IP 範圍。

4. 結語

連外線路成本昂貴， 如何達到最大的使用效益，一直是電算中心網管人員最重要的工作項目之一。為充分應用有限頻寬，我們利用 Static、Dynamic NAT 及 Static Routing 機制，完成對稱式的路由策略的建置，在不影響原有網路服務亦不加劇 Router 負載情況下，開放上傳需求較高的服務如 Web、E-Mail 等，可以利用 ISP 所提供的 IP 對外提供服務，如此一方面充分應用有限頻寬，另一方面也提供更多管道的網路服務。而在骨幹交換器負載降低的情況下，適度在少數 Gigabit 骨幹之介面上，建立 Policy Route，讓連外線路的使用更多樣化。

5. 參考資料

[1] 張永昌, 王鵬程, "修平技術學院高速校園網路系統報告書", Mar. 2001

[2] 陳振庸, "逢甲大學校園網路架構圖", *http://madonna.cc.fcu.edu.tw/arch/FCUnet20010621.jpg*, Jun. 2001

[3] Cisco Systems, "Understanding Policy Routing," *http://www.cisco.com/warp/public/105/36.pdf*

[4] Cisco Systems, "Policy-Based Routing: The Need to Define Routing Policy," *http://www.cisco.com/warp/public/techno/protocol/tech/policy_wp.pdf*

[5] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," *RFC 1631*, May 1994

[6] Cisco Systems, "Cisco IOS Network Address Translation (NAT) Overview," http://www.cisco.com/warp/customer/cc/pd/iosw/ioft/ionetn/prodlit/1195_pp.pdf

[7] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot and E. Lear, "Address Allocation for Private Internets," *RFC 1918*, Feb. 1996