路由登錄與代理伺服系統網路架構建置

黃仁竑、陳音竹、文志超、楊子民、陳重融
國立中正大學電算中心
rhhwang@cs.ccu.edu.tw
范國清、游象甫
國立中央大學電算中心
楊竹星、林福仁
國立中山大學電算中心
黃悅民
國立成功大學電算中心

摘要

台灣學術研究網路(TANet/I2)在國科會與教育部的推動下，自八十七年起已陸續建置完成並於八十八年正式啓用。而國家寬頻實驗網路(NBEN)也在國科會與中華電信研究所的共同努力下，也於八十八年開始提供寬頻實驗平台。加上原本的台灣學術網路(TANet)，使得路由登錄、代理伺服系統的管理與維運變得相當複雜。本研究之目的即是在提出一完整的服務計畫，利用完善的路由規劃、高效能的校園骨幹網路，讓雲嘉地區之大專院校、研究機構可以透過中正大學在 TANet/I2 上進行各項應用計畫，以改善研究環境、提昇研究效率、促進國際合作研究。而在此同時也可以將非學術研究的流量，如學生宿舍網路，排除在 TANet/I2 之外，以確保 TANet/I2 的正確使用。在此研究中，我們也提出整合多所學校，進行路由策略與代理伺服器相關議題的研究。我們研究路由管理與代理人架構，提供網路管理、路由設定、代理人設定之諮詢及相關之教育訓練。

一、前言

近年來，網際網路已是學術界資訊交換、傳佈的主要管道。然而由於網路爆炸性擴張，商業訊息到處充斥，使得學術界在網路的正常使用因而受到排擠，造成漫長的等待甚至無法使用。爲解決現今網際網路使用中所面臨而無法解決的問題，如：網路頻寬不足、資料未分流、重複垃圾資訊充斥、網路位址不足、欠缺網路安全支援、無法支援服務品保(Quality of Service)等，美國政府於 1996 年 10 月宣佈下一代網際網路(Next Generation Internet, NGI)計畫。美國國家科學基金會（National Science Foundation, NSF）爲配合 NGI 計畫，將於三年內投資三億美元，建構下一代網際網路，以高於目前網際網路一百至一千倍的速率，銜接美國境內一百個以上的主要研究單位，藉此開發落實新一代網路技術，並且刺激創新應用的成形。

爲了參與實現美國 NGI 計畫的機制，美國國家科學基金會(NSF) 於 1997 年 5 月宣佈 High Performance International Internet Services, HPIIS 計畫，開放其專供學術研究的骨幹網路—very High Speed Backbone Network Service, vBNS 與其他國家的對等研究網路連接，用以加速下一代網路相關技術與應用的跨國合作研究。容許各國在自付連線經費的前提下，連接美國重要的 NGI 參與單位，進行互惠的合作研究。申請銜接 vBNS 的條件爲：必須具備高速的國際專線（初期至少 10Mbps 五年內需達 155Mbps），同時必須提出具有研究價值的「應用計畫」。

若能參與銜接美國 NSF 的 vBNS 研究網路，不但可以抒解目前台灣學術網路(TANet)與國外連線的擁塞，也可爲國內學研各界建立與國際合作的暢通管道。有鑒於此，國家高速電腦中心在國科會國合處及各學術處的大力協助下，主動向國科會

提出「我國參與下一代高速研究網路連線計畫」，由高速電腦中心負責與中研院及教育部聯手增加 TANet 頻寬(由原 3Mbps 增至 45Mbps)，而由各學術處推薦具有研究價值的學界國際合作應用計畫。連線計畫書也於民國 86 年八月送美國 NSF 審核並於十一月通過，為全世界參與此一連線計畫的前五個國家之一。

目前此一台灣學術網路/研究網(TANet/I2) 之國際網路連線部分已於民國八十七年十月底正式連線，國內骨幹建置也以委外方式，由 APOL 亞太線上服務股份有限公司（Asia Pacific Online Service Inc.）負責建構與維運，已於八十八年五月底前正式啓用。

本研究之目的即是在提出一完整的服務計畫，利用完善的路由規劃、高效能的校園骨幹網路，讓雲嘉地區之大專院校、研究機構可以透過中正大學在 TANet/I2 上進行各項應用計畫，以改善研究環境、提昇研究效率、促進國際合作研究。而在此同時也可以將非學術研究的流量，如學生宿舍網路，排除在 TANet/I2 之外，以確保 TANet/I2 的正確使用。

在此研究中，我們也提出整合多所學校，進行路由策略與代理伺服器相關議題的研究。我們將研習路由管理與代理人架構，提供網路管理、路由設定、代理人設定之諮詢及相關之教育訓練。

二、TANet, TANet / I2 及 NBEN 網路架構及路由設定

2.1 TANet, TANet / I2 網路架構及路由設定

TANet/I2 主要是提供連線單位進行學術相關研究傳輸資料使用，故在路由上有嚴格限制，禁止過境交通經過 TANet/I2。由於 TANet/I2 骨幹是由亞太線上負責，在這邊我們只討論(1)POP 與 TANet/I2 骨幹路由器之間的路由策略; (2) 非 POP 之 TANet/I2 連線單位連接 TANet/I2 之問題。

2.1.1 TANet / I2 之網路架構

(1) TANet / I2 各 POP 所在地架構圖如圖一所示。

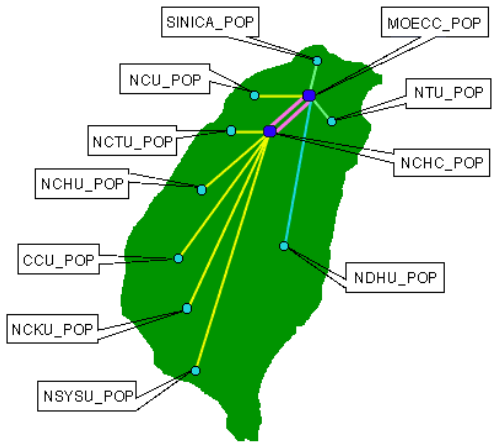
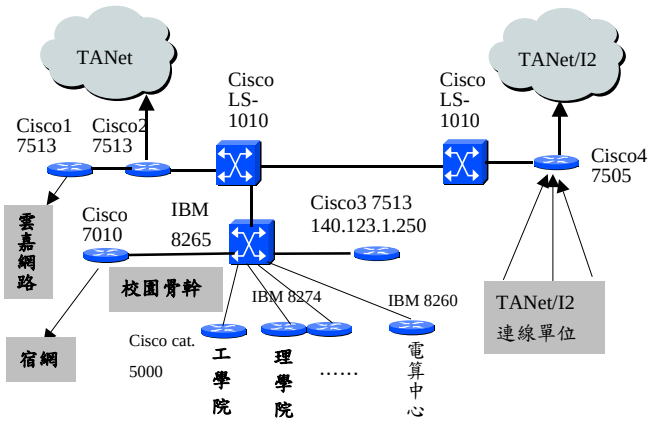


圖 1: TANet/TANet I2 骨幹架構圖

(2) 中正大學 TANet / I2 網路架構介紹

中正大學校園骨幹網路架構是以 IBM 8265 為中心所形成之 ATM 網路，如圖一所示。其中仲琦提供 TANet/I2 的機器為 Cisco 7505 router(Cisco4) 及 Cisco LS-1010 ATM switch。校園內各學院的 router 為 IBM 8274，以 ATM 介面與 IBM 8265 連接。另有一台 Cisco 7513 (Cisco3) (連接電算中心內部網路)也以 ATM 介面與 IBM 8265 連接。IBM 8265 為各 router 所形成之 ATM LANE 之 Server，且有 MMS 負責 routing 工作。

校園內與 TANet/I2 之 routing 交換是在 Cisco 7513 (Cisco3) 與 Cisco 7505 (Cisco4)間建立一 ATM PVP (Cisco3 IBM 8265 Cisco LS1010 Cisco LS1010 Cisco4)，並讓兩顆 Cisco 以 EIGRP 進行 routing 交換。Cisco 7505(cisco 4)只將 I2 的 routing table 給 Cisco 7513(cisco 3)，並不從 Cisco 7513(cisco 3) 學習中正大學以外之 routing information。Cisco 7513(cisco 3) 再將從 EIGRP 所學得之 I2 routing table 轉成 RIP 格式傳給校園內之工學院 (cisco cat.5000) 及電算中心 (IBM 8260) 之 routers，而其他學院之 routing 則是設 default rout 到 cisco3。如此，校園內往 I2 之交通便可經由 Cisco 7513 (Cisco3)轉至 Cisco 7505 (Cisco4)，再上 TANet/I2 骨幹。



圖二: 中正大學 TANet/I2 架構示意圖

但在 POP 內的學生宿舍網路的交通是不能過境 TANet/I2 骨幹的,所以在 POP 內必須做 policy routing。如上圖二所示，宿舍網路的交通與其他學院一樣是直接與 Cisco 7513 (Cisco 3) 路由器連接,故我們在 Cisco 3 上進行 policy routing，防止學生宿舍網路的交通過境 TANet/I2 的骨幹網路。

至於雲嘉地區其他單位的交通，目前是先到一顆獨立運作的雲嘉地區路由器(Cisco 7513)，再轉到 TANet 骨幹的 Cisco 7513 路由器上 TANet 骨幹網路。這些單位以後會分成 TANet/I2 連線單位及非 TANet/I2 連線單位。對 POP 的運作而言，並不會造成太多的負擔，因凡 TANet/I2 的連線單位，必須另以一路由器及專線連接 TANet/I2 的骨幹路由器來傳送 TANet/I2 的交通。如圖一所示，TANet/I2 連線單位可以直接連接上 Cisco 4 之路由器。所以凡是走舊的路線(即雲嘉地區路由器 TANet 骨幹路由器)的交通，不管是 TANet/I2 連線單位或非 TANet/I2 連線單位，均將在 TANet 骨幹的 Cisco 7513 路由器上，以 policy routing 方式，被禁止過境 TANet/I2 的骨幹網路。目前，雲科大已經接上 TANet/I2 了。

2.1.2 TANet/I2 路由政策及設定方法

(1) 背景：

Internet routing 分 inter-domain routing 和 intra-domain routing 兩個階層在一個 Autonomous System（AS）內的 routing 爲 intra-domain routing。目前最常用的 intra domain routing protocols 有 RIP，OSPF，EIGRP（Cisco proprietary）在不同的 AS 間的 routing 爲 inter-domain routing，目前使用的 protocol 爲 BGP4。

AS 的定義依網路的規劃各有不同。目前在 TANet 上之各區域網路中心的 Cisco 7513 routing 形成一個 AS。在由仲琦所提供服務的 TANet/I2 上各 POP 之 router 另形成一個 AS。但在 NBEN 上各 GigaPOP 各自形成一個 AS。當我們要將不同的網路（TANet，TANet/I2，NBEN）連接在一起時,彼此間的 routing 便變得相當複雜，特別是有 routing 限制（routing policy）時。

(2) 路由政策：

首先我們探討 TANet 與 TANet/I2 間的 routing policy 的問題。由於 TANet/I2 頻寬有限且與國外 I2 連接,故需限制可連接之 domain，除 POP 所在地之學校外，其餘機構必須經申請方可連上 TANet/I2，所以必須以 routing policy 加以限制。國高對於ＩＩ的管理政策是：與國外學校（只要有跟 vBNS 相連的學校）之交通是都是走ＩＩ出國，但各校需做好宿網隔離措施。而與國內學校之交通，只要該 GigaPOP 有隔離宿網，並做好 IP Summary，便可以走ＩＩ。

(A) 首先是排除宿舍網路於 TANet/I2 之外;因大部分學校之宿網與一般研究教學之網路均屬於同一 class B 之 IP domain,所以必須靠校內 router 進行交通分流。也因此，交換出去給亞太線上（國高）的 routing table 不可以是一 class B 之 IP Domain。

(B)第二，教育部規定國內 POP 所在地之間的交通連線現在可以走 TANet/I2。因爲各校都會與亞太線上(國高)那邊的 router 做 routing table 的交換，若各校均將這樣龐大的 routing table 交換過去給國高，未經 IP summary,將使該國高路由器 load 很重。一般而言，因隔離宿網的關係，會使得交換出去的原始校內的 routing table 是零散的 class C，約會有 70 至 100 筆不等的 routing tables。故教育部規定各 POP 機構需先在校內將這 70-100 筆 routing table 作 IP Summary 成幾個 class C 之後，再將 routing table 送出去。

(3) 解決途徑：

這個地方要分成兩個部分來討論，一個是對外的（中正大學出 TANet/I2），另一個是中正大學校內的各單位之 ROUTER 如何設定。

(A) 將中正大學校內可以走Ｉ２的各單位（原則上只有宿網不能走）之 ip address 做個整理，利用 subnet mask 的方式 summary 起來。本校宿網網址爲：140.123.211.0 -- 140.123.225.0。將 CCU router-7513 (140.123.1.250) 做 routing summary 其作法如下：

```
# ip summary-address eigrp 110 140.123.0.0/17
# ip summary-address eigrp 110 140.123.128.0/18
# ip summary-address eigrp 110 140.123.192.0/20
# ip summary-address eigrp 110 140.123.208.0/23
# ip summary-address eigrp 110 140.123.210.0/24
# ip summary-address eigrp 110 140.123.226.0/23
# ip summary-address eigrp 110 140.123.228.0/22
# ip summary-address eigrp 110 140.123.232.0/21
# ip summary-address eigrp 110 140.123.240.0/20
```

故原來本校送出去的 ip address 約有 90 幾筆零散的 class C，經 summary 之後，只剩下 9 筆。

(B) 中正大學校內各學院之 routers 的設定：

由於由國高那邊（cisco 4）交換過來的 routing tables 很大，約有兩千多筆，故該不該將此多筆之資料與各學院之 routers 交換成爲一個問題；若要交換，則交由各學院之 routers 自己判斷該不該走 I2，但會造成各學院 routers 之 load 增加，若 routers 的處理速度本來就不快，更會造成速度嚴重下降，如此 bottleneck 是在各學院的 router 上：但若有都不交換，將校內的交通全部送到 cisco3 這顆 router 來判斷該不該走 I2，bottleneck 變成是在 cisco3 這科 router 上。

中正大學本來的作法是交通分流均交由各學院自己處理，故各學院之 routers (IBM 8274) 均接收由 cisco3 交換過來的 I2 routing tables，有兩千多筆，結果發現因 IBM 8274 load 太重，運作不良。後來，工學院換了新的 routers (Cisco CAT. 5000) 及電算中心也更換 爲 IBM 8260 之後，我們將上述作法取一折衷。使用舊的 IBM 8274 routers 的學院不接收 I2 routing tables，而是設一 default route 到 cisco3 這顆 router 上。而使用新的 routers 的工學院及電算中心，則是會跟 cisco3 交換 routing tables 過來，自己做交通的分流判斷。

(4) 路由設定結果測試及維護

定期作流量監控及 trace route，以掌握本校走 I2 的交通狀況，若流量突然變化很大，便跟亞太線上聯絡看看是否有出什麼問題。

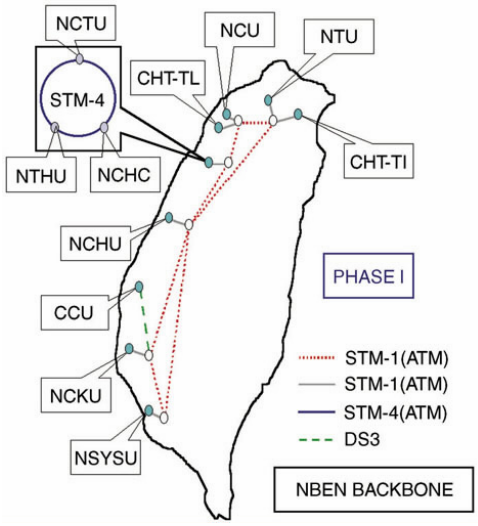
自動化路由診斷系統設計與實作：將於第四章說明。

2.2 NBEN 網路架構及路由設定

爲配合電信國家型科技計畫國家寬頻實驗網路之建置，在嘉雲地區以中正大學建置 GigaPop，連接國家實驗網路(NBEN)。GigaPop 之建置，是以新世代網際網路技術爲基礎，基本上必須具備寬頻網路良好的服務品質(QoS)，提供寬頻網路的技術發展及應用服務。

2.2.1 NBEN 之網路架構

(1) NBEN 各 GigaPOP 建置互連架構圖:

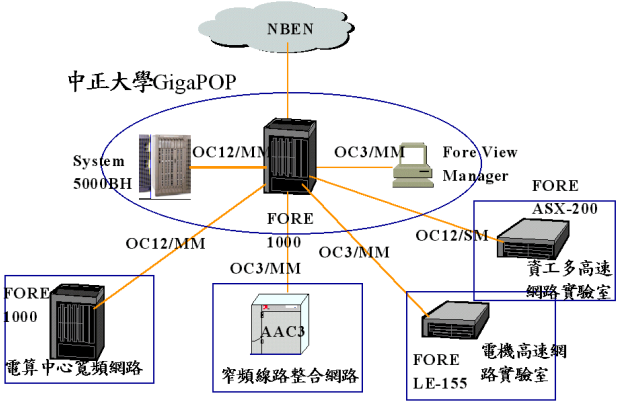


圖三: NBEN 架構圖

(2) 中正大學 GigaPOP / NBEN 網路架構介紹:

中正大學實驗網 GigaPOP 架構完成建置的網路系統，如圖三。目前已開始運作提供申請連線的使用單位皆爲本校，包括電機研究所高速網路實驗室、資工研究

所多媒體網路實驗室、電算中心寬頻遠距教學網與雲嘉區域窄頻專線遠距教學整合網路。電機實驗室使用一組 OC3c/155Mb 多模光纖連線至 Fore ATM Switch LE 155，另外使用一組 STM-1/155Mbps 單模光纖連線至 HP Protocol Analyzer 做量測分析。資工實驗室使用一組 OC12/622Mbps 單模光纖連線至 Fore ATM Switch ASX200，以提供多媒體資料庫查詢傳輸之用。電算中心使用一組 OC12/622Mbps 多模光纖連線至 Fore ATM Switch ASX1000 寬頻網路，可提供 AVA/ATV 遠距教學連線。電算中心整合雲嘉區域窄頻 FT-1 專線，使用一套多工介面中樞設備 AAC3 具備 OC3c/155Mb 多模光纖連線 GigaPOP/ATM，並且提供多阜 CSU/CSU 連線介面。



圖四：中正大學校園寬頻網路目前架構

2.2.2 NBEN 路由政策及設定方法

(1) 背景：

目前 NBEN 骨幹 routing 採取的是 intra-domain routing protocols: OSPF，在不同的 GigaPOP 間的路由節點，選定爲區域 (local area) 主要的邊界路由器 (Border router)，做爲匯集區域與對外路由的交換中心。

OSPF Area 的區域定義依網路的規劃階層各有不同架構，具有隔離內部與外界資訊的作用。目前在 NBEN 上之各區域網接中心的 Bay System 5000BH router 形成一個獨立 area (ID:211.73.*.0)，與相鄰骨幹 backbone area (ID:0.0.0.0)其它 OSPF area 交換最佳路由資訊。當我們要將（TANet，TANet/I2，NBEN）三個不同性質的網域連接在一起時，彼此間的 routing 如何選擇，特別是 routing policy 的制定有所規範，讓 routing 效率提高是我們所考量的依據，將在下面提出。

(2) 連線管理：

先前我們已探討 TANet 與 TANet/I2 間的 routing policy 的問題。由於 NBEN 的定位是屬於實驗性質，不像 TANet/I2 對頻寬需求與使用者類型限制有嚴格的規定，故只要有實驗需求即可申請連接各區域之 GigaPOP。。針對 NBEN 的路由管理政策是：POP 骨幹設備 ATM Switch 與 IP Router 以 OC-12/622Mbps 相連，整個環島骨幹是利用 Fore ASX1000 透過中華電信之 STM-1 實體線路互連，以 ATM 第二層協定 PNNI 爲基礎，所有交通流量都是 ATM cell 固定封包，但各校 GigaPOP 互連可使用頻寬，目前由國高與中華電信所管制。而與區域內研究教學單位之連線，只要該單位自備可連線的網路設備與線路，審核過則分配正式的 NBEN IP，便可以連上國家實驗網路。

(3) 路由政策：

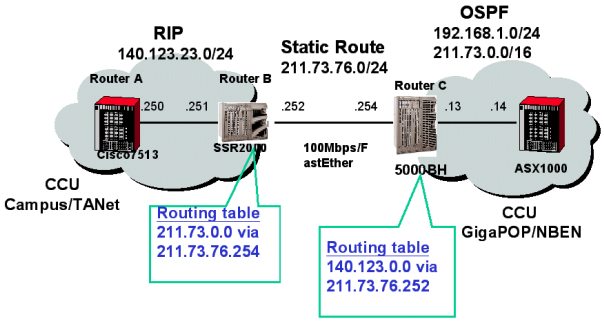
初期 NBEN 是封閉型的網路，禁止所有學校將部份 TANet 流量利用其寬頻線路過境，或與一般研究教學網路之 IP 混用，所以必須與校內 router 的連線分離，使兩者的 routing table 不能交換出去。

爲提高研究與管理的使用效率，國高決定開放從 TANet 上直接獲取 NBEN 的資源。在不影響 TANet 現有架構下的 routing 方式與保持良好的 performance，進行 NBEN 與 TANet 網路之間 Peering 的建置。做法分兩階段同時評估與實施，如下：

(A). 靜態路由(Static Route) —以實體連接方式來連接各 GigaPOP 內的 NBEN 與 TANet Router，利用空的 Fast Ethernet Module 上的埠來進行連線，以 Static Route 方式設定雙方的路由表。或以光纖連線來連接各 GigaPOP 內的 NBEN 與 TANet Router 上的 ATM Module，並建立點對點的 ATM PVC 虛擬路徑的方式連接。

(B). 動態路由 (Dynamic Route) — NBEN 與 TANet 分別屬於兩個獨立的實體網路，兩者以動態路由方式相連，目前最普遍的外部閘道協定(EGP)，大多採取 BGP(Border Gateway Protocol)。由於 NBEN 與 TANet 之骨幹 POP 節點構成一對一的對稱架構，對於兩者 AS 的規劃考慮採取階層式或平行式的路由交換，以降

低複雜性，達到最佳效率之目的。



圖五：NBEN 與 TANet 以 fast Ethernet 互連 Static Route

(4) 固定路由設定方式：

如圖五所示，在校園網路 TANet 部份，與中正 GigaPOP/NEBN 實驗網的連線是利用一台實驗 SSR2000 /Switch Router，在其 Fast Ethernet port 上分別接到兩端網路的路由器之 Ethernet 介面，然後在相關路由器設定兩端預定的固定路由。

(I). Router A— Cisco 7513

建立一個指向各 GigaPOP 網域(211.73.0.0/16) 與 NBEN 骨幹 IP 網域(211.73.95.0/28)的路由表，Next hop 閘道是另一端相鄰的路由器介面。設定如下：

ip route 211.73.0.0 255.255.0.0 140.123.23.251

(II). Router B— SSR2000

分別建立固定路由指向到中正校園網路(140.123.0.0)與到實驗網 IP 骨幹與 GigaPOP 的 IP 網域。設定如下：

ip add route 211.73.0.0 255.255.0.0 gateway 211.73.76.254

ip add route 140.123.0.0 255.255.255.0 gateway 140.123.23.250

(III). Router C— System 2000BH

利用 Bay Router 管理程式 Site Manager 分別建立固定路由指向到中正校園網路(140.123.0.0)與到實驗網各校 GigaPOP 互連的校園網路 IP 網域。在其路由表可看到的固定路由所示如下：

Destination	Mask	Proto	Cost	NextHop
0.0.0.0	0.0.0.0	LOCAL	1	211.73.76.253
140.110.0.0	255.255.0.0	LOCAL	1	192.168.1.6
140.112.0.0	255.255.0.0	LOCAL	1	192.168.1.2
140.113.0.0	255.255.0.0	LOCAL	1	192.168.1.8
140.114.0.0	255.255.0.0	LOCAL	1	192.168.1.10
140.115.0.0	255.255.0.0	LOCAL	1	192.168.1.4
140.116.0.0	255.255.0.0	LOCAL	1	192.168.1.16
140.117.0.0	255.255.0.0	LOCAL	1	192.168.1.18
140.120.0.0	255.255.0.0	LOCAL	1	192.168.1.12
140.123.0.0	255.255.0.0	LOCAL	1	11.73.76.252
192.168.1.0	255.255.255.0	LOCAL	0	192.168.1.14
192.168.2.0	255.255.255.0	LOCAL	0	192.168.2.14

(5) 動態路由設定策略：

動態路由協定採取 BGP 的理由，主要考量在適度區隔兩個大型股幹網路 TANet I1/I2 學術暨研究網與 NEBN 實驗網的連線，在其內部分別有許多獨立區網中心與網接中心(POP)組成，提供該區域的特定連線服務。因此，可將之視爲一 ISP(Internet Service Provider)。所以動態路由協定 BGP 之設定策略，可選擇圖二中的中正校園網路 Router B (SSR2000)與中正 GigaPOP Router C (System5000)規劃成兩個相鄰的管理區域 peered AS。

2.3 TANet, TANet/I2, 與 NBEN 上使用 BGP 的需求

在台灣，學術網路是一個蘊藏有豐富網路資源的寶藏。幾乎所有網際網路的行爲模式都可在此學術網路的平台上觀察到。在台灣的網際網路環境日漸發達起來，各個 ISP 公司如雨後春筍般的出現，每家公司都想要和各個區網中心相接，已較佳較快的速度直接存取學術網路的資源，而使得區網中心的架構日漸複雜。

而各個區網中心面臨的挑戰將不是只有一項頻寬不足而已。而 Routing Entry 的管理將是區網中心所將面臨的一大挑戰。若 Routing Entry 管理失當，則將會衍生下列幾個困擾。

1. 路徑遺失:這是最常見到的狀況，而且也不太容易偵錯。在過去的管理經驗中，這種狀況還常發生，每次發生都得耗費大量的時間來除錯。這大部份由於 Routing Protocol 對於子網路作了錯誤的聚集所產生的。

2. 路徑指定錯誤會非最佳路徑:各種 Routing Protocol 互相溝通的結果會選出一條到目地的路徑。但在網狀架構的網路中，往往這條路徑不一定是我們所希望封包進行的路徑。這種狀況在跨幾個 AS 中最常見到的。例如中山到國家高速電腦中心有 Tanet 和 I2 兩條路徑。有些實驗，我們會希望封行經 Tanet 到國家高速電腦

中心。有些則希望封包由 I2 到國家高速電腦中心。甚至於希望某些來源的 IP 行經某段路徑。這在 IGP 的環境中不太容易達的到。

3. 無法做到負載平衡:前面提到，各家 ISP 公司都會希望和各區網中心連線，因此各 ISP 公司幾乎都會在各區網間有佈點，且願意提供線路給個學校來舒緩學術網路的擁塞狀況。如此，各個區網中間可能不只是一條路徑而已。例如中山到國高有 TANET 和 I2 兩條路徑，但對於路由器來講，它只會選擇一條路徑而已，很有可能會造成一條空的而另一條路徑滿載。

4. 在區網和各個 ISP 公司相接之後，網路的規模變大，網路變動的機率也跟著提高。而每次網路變動時，整個網路都會變的如前述般的不穩定，而收斂時間也隨之變大。若這整個網路是由同一個單位所負責的，則影響尚屬有限。若這個網路是由不同單位和 ISP 公司所構成的，那麼網路不穩定對各單位和 ISP 公司所構成的影響將會更加嚴重。因爲網路不穩定的責任無法劃明確劃分。

以上幾點，將是各區網中心所面臨的挑戰。爲了解決上述的問題, BGP 算是一個較好的解決方法。

BGP 的特性是各個自治系統之間皆有一顆邊界路由器(Boundry Router)，在各個邊界路由器之間執行 BGP。邊界路由器控管所有這個自治系統和對方自治系統的所有路由。

如此一來，有底下所述的一些好處:

1. 各個自治區內的路由表僅在自己的自治區中用 IGP 互相交換，而在自治區內的任何變動不會影響到其它的自治區。這一點算是最重要的。如此一來，就算 TANET 內部變動頻繁，也較不會影響到 I2 以及 NBEN 等其它的 Routing。因爲 TANET, I2 和 NBEN 上執行 BGP 可以有效的隔該 IGP 變動對其它 AS 自治區所造成的影響

2. 透過 BGP，區網中心可以決定自己開放那些網段到其它如 I2, NBEN 的網段上，而不會造成所有的網段皆由 TANET 或 I2 灌進來. 目前 I2 上的作法是在各校接 I2 的路由器上過濾宿網，並且 I2 也在各校的 7505 上做宿網 Routing 的過濾，此種作法會造成一些路徑被過濾掉，而無任何錯誤訊息。如果能夠嘗試換成 BGP 來溝通，則各區網就可以隨時掌握那些網路藉 TANET，那些網路段可以藉著 I2，而 I2 和 NBEN 就可以當做過境的 AS。

三、TANet 路由伺服器架設及管理

3.1 背景

目前 TANet 上之 proxy 採階層式，且強制到各縣市網路 proxy 之建置與設定，在骨幹及出國線路上又有保留頻寬，所以運作相當有效率。目前 proxy 之階層分三層，最上層爲教育部之 proxy(也可用中研院之 proxy)。第二層爲 TANet 各區網中心之 proxy。第三層則爲各縣市之網路中心之 proxy。各區網中心校園內大都也有建置第三層之 proxy。爲了承受大量負載，各層之 proxy 可以使用一台以上之工作站來建構。以中正大學爲例，第二層之 proxy(雲嘉區網 proxy) 是由三台跑 FreeBSD 作業系統之高效能 PC 組成。爲保留頻寬，第二層以上之 proxy 是使用 168.28.x.x 之 IP address。

3.2 所遭遇之問題

目前各區網中心的第二層 proxy 因連接各縣市第三層 proxy，大部份交通非屬 TANet/I2 之交通流量，所以不應走 TANet/I2 骨幹。屬於 TANet/I2 單位之第三層 proxy 雖可走 TANet/I2 骨幹，但因其 parent 爲各區網中心的第二層之 proxy，若無特別設定，此 proxy 在 cache 中找不到的資料，會向其 parent 要。但第二層 proxy 無法直接走 TANet/I2，所以在效能上無法提昇。 (目前向外宣告之 proxy IP 有 163.28.8.0/21 ， 163.28.48.0/28 ， 163.28.48.32/28 ， 163.28.48.64/28 ， 163.28.129.0/24 ， 163.28.130.0/24 ， 163.28.160.0/24，163.28.175.0/24。)

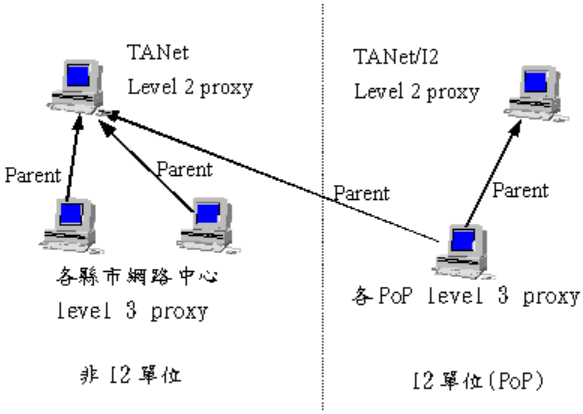
3.3 解決途徑

對於 proxy 的問題，我們提出以下的根本解決方法。我們覺得第二層的 proxy 應分 I2 和非 I2 兩部份。原 TANet 在各區網中心的 proxy 維持其原運作方式，負責非 I2 交通之 proxy 角色。我們提出在 TANet/I2 之各 PoP 設置另一個第二層之

proxy，負責 I2 交通之 proxy 角色。我們提出的架構如下圖六所示。其中原 TANet level 2 proxy IP 爲 163.28.x.x。此部份之 IP address 不用加入向國外 I2 網路宣告之 IP table 中，因其仍負責非 I2 網路的 proxy。TANet level 2 proxy 對外維持走原 TANet 骨幹所預留之頻寬。我們建議在 TANet/I2 PoP 內另建置一屬 I2 之 level 2 proxy，其 IP 使用 PoP 內之 IP (如中正使用 140.123.x.x)。因各 PoP 出國可走 TANet/I2 骨幹，所以此 proxy 若需 retrieve 國外 I2 之資料，也是可以走 TANet/I2。TANet/I2 對外國宣告之 IP 就不用爲 proxy 而做任何特殊之更動。

在設定上，原 TANet level 2 proxy 及各縣市網路中心之 level 3 proxy (非 I2 單位)均不用做任何改變。唯一改變設定的是 I2 連線單位所建置的 level 3 proxy。以中正大學爲例，目前校園內 level 3 proxy 設定其 parent 爲區網的 level 2 proxy (level 2 proxy 因有許多台，所以目前採 round robin 方式輪流 service)。當 level 3 proxy 無 client 端所需要之資料，它會先向其 parent 查詢。若 parent 也都沒有，則改以 client-service 方式由 parent 以 proxy 角色向 level 1 proxy 要資料(或直接至資料 source 要)。

我們建議將 level 3 proxy 的設定改爲依資料 source 的 IP domain 來決定向那一個 parent (TANet or TANet/I2 level 2 proxy) 要資料。若是屬 I2 的 IP domain，則向 TANet/I2 level 2 proxy 查詢，否則就向 TANet level 2 proxy 查詢。初期我們將在中央、中正、成大、中山各建置一 TANet/I2 level 2 proxy，並彼此設定爲 sibling 關係。實驗測試成功後，再建議國科會高速電腦中心建置一台 TANet/I2 level 1 proxy。這樣的架構，其優點包括: (1) 所有 client 端的 proxy 不需做任何的改變，就可以達到交通分流。(2)原 TANet proxy 不需做任何改變。(3)對於需要走 TANet/I2 的交通確實可以走 TANet/I2 骨幹。比較麻煩的是 I2 連線單位的 level 3 proxy 的設定需要知道那些 IP domain 需要跟那一個 level 2 proxy 查詢。下面 3.5 小節我們將提出一個可以自動由 I2 routing table 轉成 proxy 設定檔的方法。



圖六: TANet/I2 proxy 新架構

3.4 Squid Proxy 介紹

(1) Squid 與階層設定相關之指令簡介:

Squid 的指令很多，這邊只針對其中跟階層架構相關之設定方法做介紹。

(A) parents 與 children 或 cache peer 間的設定：
(I) cache_peer (hostname) (type) (http_port) (icp_port): To specify other caches in a hierarchy
(II) cache_peer_domain (cache_host) (domain) : To limit the domains for which a neighbor cache will be queried.
(III) Neighbor_type_domain (hostname) (parent|sibling) (domain) (domain) : You can treat some domains differently than the default neighbor type specified on the “cache_peer” line.

(B) Access Controls 的指令---- acl，http_access，icp_access，miss_access。
(註:You will define an ACL first, and then deny or allow access to a function of the cache.)設定方式如下：
(I) acl aclname acltype string1
(II) acl aclname acltype “file”
(III) acl aclname src ip-address/netmask
(IV) acl aclname dst ip-address/netmask
(V) acl aclname srcdomain (domain)
(VI) acl aclname dstdomain (domain)
(VII) http_access (allow|deny) ([!]aclname)
(VIII) icp_access (allow|deny) ([!]aclname)
(IX) miss_access (allow|deny) ([!]aclname)
(X) cache_peer_access (cache_host) (allow|deny) ([!]aclname)

3.5 實際設定

(1) 目前中正大學對 I2 PROXY 的架構是除原來 3 台 proxy servers 外，尚設有一台 level 2 proxy server 專門處理 I2 cache。
(2) 由於有 I2cache 專門處理屬於 I2 的資料，故若 clients 跟 level3 要屬於 I2 上的資料，只跟 i2cache proxy server 要。其設定方式如下：

於 level3 之 config.設

```
cache_peer_access proxy.ccu.edu.tw deny i2-map
cache_peer_access cache.ccu.edu.tw deny i2-map
cache_peer_access cache2.ccu.edu.tw deny i2-map
```

(3) 上面設定方法中有一 i2-map 檔案，這個檔案就是由 I2 routing table 轉過來的，其流程如下：
(A) 在 Level 2 proxy server 端

(I) 在 I2 Cache 上跑 routed 接收由 router (140.123.16.250) 所送出來的 routing table 的資料，再透過 perl 程式轉換成 squid 所需要的 acl 檔案格式，儲存爲 i2map file。在 i2 cache 上重新執行 squid -k reconfigure。將所需執行程式（如下）丟到 cron 去執行，每小時執行一次。

```
#!/bin/csh
cd /root/i2r
set interface=xl1
set net="^140\.123"
set file=i2.routing
set prog=./transform.pl
netstat -rn|grep -v default|grep interface|grep -v $net|$prog > $file
/usr/local/squid/bin/squid -k reconfigure
cp i2.routing /usr/local/www/data/i2.routing
```

(B) Level 3 proxy server 端

(I) 在 ccu-proxy 端把 i2cache 產生出來的 i2map file 抓到 ccu-proxy reconfigure 一次。

(II) 將所需執行程式(如下)丟到 cron 去執行，每小時執行一次。

```
#!/bin/csh
cd /root/i2
rm i2.routing
/usr/local/bin/wget -q http://i2cache.ccu.edu.tw/i2.routing/usr/local/squid/bin/squid -k reconfigure#!/bin/csh
set interface=xl1
set net="^140\.123"
set file=i2.routing
set prog=./transform.pl
netstat -rn|grep -v default|grep $interface|grep -v $net|$prog > $file•#!/usr/local/bin/perl

#####################################
##### parser.pl
##### 將文字輸入(STDIN)的第一欄
#####(以空白分開)轉爲 IP 表示，並在最
#####後加入 bit 數.
##### Coder: Nidalap
##### Update:Mar 16,2000
#####################################

my($ip, @ip, $bits, $new_bits, @line);

@line = <STDIN>;
foreach $line (@line) {
  $new_bits = 0;
  $line =~ s/\n//;
  ($ip) = split(/\s+/, $line);
  ($ip, $bits) = split(/\//, $ip);
  $new_bits=$bits    if($bits != 0);
      ## 保留原有 bits 值(如果有的話)
  next    if($ip eq "");
  ($ip[0], $ip[1], $ip[2], $ip[3]) = split(/\./, $ip);
  foreach $ele (@ip) {
      $ele="0"    if($ele eq "");
      $new_bits+=8        if(($bits==0)    and ($ele != 0));
## 計算 bits 值(如果原先沒有)
  }

print("$ip[0].$ip[1].$ip[2].$ip[3]/$new_bits\n");
}
```

四、Web-based 自動設定、警示與偵錯工具製作

4.1 TANet/I2 Routing 問題

因爲目前校園網路中，有了 TANet 和 TANet/I2 兩個骨幹網路出外，因爲 TANet/I2 爲一個研究網路，所以在 routing 上有著許多了規則和限制。也使得校園網路的 Routing Table 變得複雜和容易出錯。所以我們希望可以藉著監控校園網路中各個 Router 的運作，當 Router 有異常狀況時可以立即的以 e-mail 的方式通知網路管理者。另我們也將建立一個 Web 介面的

監控環境，讓管理者可以方便迅速的得知校園網路的狀況。

為了達到管理監控校園網路的 Routing，因為校園網路的 Routers 負責了整個校園網路的運作，為了網路安全上的考量，我們並不在 Router 內放一個 agent 或者直接跟 Router 連線讀取相關的資料的方法，因為這樣可能會造成 Router 的效能下降或者是安全上的漏洞。而是藉由著架設一台監控的機器在校園網路 Routers 之間的 LAN 上面，在上面收取 RIP 的封包，藉由 RIP 封包的分析進而達到了解校園網路運作的狀況。

在這邊我們所採用都是免費的自由軟體，利用 Apache server 提供一個網頁的管理環境，而 MySQL 提供一個簡單易用的資料庫讓我們存取 Routing 相關的資料，PHP 則是方便我們打造出一個符合我們需求的網頁。

我們的研究分五個部份進行。第一、二部份的目的是要提供一個方便的管理者查詢介面。後面三個部份的工作是偵測網路路由異常。如果有意常出現的話，立即 Mail 通知系統管理員。以下對每一部份，分別加以說明。

(一) 因為現在校園網路對外有著兩個路徑，所以我們有需要知道某一個特定的 Destination 是經由哪個路徑連接的。於是我們提供 Web 的介面查詢特定的 Destination 所經過的路由為 TANet 或 TANet/I2。

(二) 藉由我們在校園網路 Router 所存在的 LAN 上面，打開 Linux 中的 roued，可以就由這一個 route daemon，來收集校園網路的整個 Routing Table，知道哪些路由是屬於 TANet，哪些是屬於 TANet/I2。我們於是可以將校園網路的 Routing Table 顯示在 WWW 上面，並可以分別顯示 TANet 和 TANet/I2 的 Routing Table，而且:
   (1) 在 Routing Table 過大時，視為異常現象，立即通知系統管理者。
   (2) 可對 Routing Table 中的各個欄位做收尋、排序。

(三) 要偵測網路路由異常，我們首先先確立一個最容易檢查出異常的，就是當一個 Router 當掉或者不再運做時，這樣整個網路運作一定會出現問題。所以我們利用程式檢查校園網路所有的 Router 是否 alive。

(四) 以目前網路運作的狀況，因為有了 TANet/I2 的加入，使得整個 Routing Table 所紀錄的項目變多，但是根據我們的觀察大概數目會維持在 1000~1500 筆左右。所以當 Routing Table 紀錄的項目過多或過少時，則表示有異常的狀況發生。所以我們利用程式自動偵測 Routing Table 的大小是否超過一個合理的範圍。

(五) 目前存在校內的的路由分兩大部分，一是經過普通的學術網路 TANet，另一個是經過研究網 TANet/I2，因為 TANet/I2 定位在研究網，所以在這邊會有一些路由的規則在區分流量，所以現在校園網路需要做到，可以經由 TANet/I2 的封包就經由 TANet/I2，而其他的就不能經由 TANet/I2。所以當有不正確的路由發生時要能夠立即偵測出。所以，我們需要從 TANet/I2 的 Router 的 Routing Table，然後監測校園網路中其他 Router 所送出的 RIP 的封包，在我們收入的 RIP 當中，到 TANet/I2 的單位所紀錄的 Metric 值應該是要大於重 TANet/I2 的 Router 所得到的 Metric，如果小於獲等於的話則表示有異常發生。我們利用程式自動比較監控的 RIP 封包，檢查其紀錄的 Destination 和 Metric 值是跟 TANet 和 TANet/I2 的 Routing Table 比較，是否有不正確的紀錄。

4.2 代理伺服器

現在本校中 TANet 與 TANet/I2 的分流已經完成，經由 routed 取得的 TANet/I2 IP address 經由幾個 shell script 的轉換，目前已經加入 level 3 proxy server 的 cache_peer_aceess list，因此要經由 TANet/I2 的 HTTP request 封包，要經過 proxy 檢查，才能進入，若是不屬於 TANet/I2 研究網路的封包，則因為沒有選擇權而經由 TANet 出國。

以目前學校的 porxy 架構來看，可以分為 level2 及 level3 的 proxy，而 level2

的 proxy 又分兩種，一種經由 TANet/I2 到國外之學術研究單位，而其他 request 則經由 TANet 出國，因此在 proxy 的設定上會較爲費事而且有錯的機會極大，此外，因爲 level3 的的 proxy 不僅要處理校園使用者的眾多的 request，還要負責辨別其 request 是否是要到 I2 研究單位所在之網路，負荷沈重，因此隨時能掌握 proxy server 狀況也是相當的重要。

由上面的說明，我們延伸出以下之研究議題：

(一) proxy server 監控與管理，偵測 porxy server 失效或當機的狀況，我們可以利用校園中的一部電腦，經由 corn 來跑 client 或是 echoping 等測試軟體，測試並分析 porxy 所傳回的訊息，若是 proxy 出現 timeout 或當機的現象，則在站上公告並寄信給該 porxy 的系統管理者。如此，便可確實的瞭解 proxy 運作不正常的狀況，並加以控制。

(二) 以目前的學校的架構爲核心，發展出一套方便有效的 web 介面管理程式，管理 proxy server 的設定檔—squid.conf。目前主要的想法是在 proxy sever 上利用 cgi 程式來讀取與設定 squid.conf，經過整理之後以 web 介面的形式呈現出來。使得目前的 proxy server 的設定更容易瞭解與操作。使得管理人員可以清楚的瞭解目前 proxy server 的設定情況，將目前所設定的 cache peer 的屬性，位置、參數列出；此外，對於 access list 屬性，名稱能做分類與管理，使得管理人員處理大量的 access list 不至於無所適從，此外，對於將 TANET 與 TANET/I2 的 request 做分流的 cache_peer_acl 及其他的變數，也可以分類觀察與設定，因此，經由這些 web 介面的工具管理程式，網路管理人員的負擔將會降低，設定出錯的機會也會減少。

(三) 監控程式部分將與設定程式結合，當監控程式發現校園中的 proxy server 出問題時，將自動透過設定程式，將有問題的 parent 或 sibling 設定移除，使得網路上的使用者不會 request 到出問題的 proxy，增加網路的服務品質與使用效率。

五、結論

在本論文中，我們對目前兩個新的骨幹網路(國家寬頻實驗網路及台灣學術研究網路)與台灣學術網路連接時，所衍生的路由策略及代理伺服器的問題，提出了可以正常維運的策略。我們也針對維運上所遇到的困難，提出利用背景程式，讓管理者在路由交換及代理器發生問題時，可以收到示警訊息，並透過全球資訊網的介面，讓管理者可以進行設定與查詢的工作。