

行政院及所屬各機關出國報告
(出國類別：實習)

赴加拿大參與「實習智慧型 IA 設備」報告

服務機關：中華電信研究所
出國人職稱：助理研究員
姓名：郭鴻志
出國地區：加拿大
出國期間：92/11/30-92/12/11
報告日期：92/12/18

H6/
CO9205053

系統識別號:C09205053

公務出國報告提要

頁數: 18 含附件: 否

報告名稱:

實習智慧型IA設備

主辦機關:

中華電信研究所

聯絡人/電話:

楊學文/03-4244218

出國人員:

郭鴻志 中華電信研究所 IA技術研究室 助理研究員

出國類別: 實習

出國地區: 加拿大

出國期間: 民國 92 年 11 月 30 日 -民國 92 年 12 月 11 日

報告日期: 民國 92 年 12 月 18 日

分類號/目: H6/電信 /

關鍵詞: 實習,智慧型,IA設備

內容摘要: 此研習係主要目的為Redback Networks的NetOp Policy Manager training，內容包含SmartEdge B-RAS/router產品功能，以及搭配NPM軟體後可達到的功能及其應用環境，如weblogin、service on demand、self-enrollment、service selection...等等。除此之外，亦包括軟體架構，原始程式碼的分析。期望藉著這次研習能深入瞭解其設計理念、軟硬體搭配架構，除了能夠利用這套系統自行客製化各式服務，甚至在應用在設備研發上，對於公司在減低維護成本或提供新型態服務能夠有所助益。

本文電子檔已上傳至出國報告資訊網

摘 要

關鍵字:

1. B-RAS : Broadband Remote Access Server (寬頻接取伺服器)
2. PNM : Policy-based Network Management (政策性網路管理)
3. NPM : NetOp Policy Manager (Redback 的 service creation 產品)
4. RADIUS : Remote Authentication Dial-In User Service
5. PPPoE : Point-to-Point Protocol over Ethernet
6. CLIPS : Client-Less IP Service (Redback 的名詞，指 DHCP/IP 服務)
7. SMS : (Redback 的 B-RAS 型號)
8. SE: Smart Edge (Redback 的 edge router 型號)

內容摘要:

此研習係主要目的為 Redback Networks 的 NetOp Policy Manager training，內容包含 SmartEdge B-RAS/router 產品功能，以及搭配 NPM 軟體後可達到的功能及其應用環境，如 weblogin、service on demand、self-enrollment、service selection...等等。除此之外，亦包括軟體架構，原始程式碼的分析。期望藉著這次研習能深入瞭解其設計理念、軟體搭配架構，除了能夠利用這套系統自行客製化各式服務，甚至在應用在設備研發上，對於公司在減低維運成本或提供新型態服務能夠有所助益。

目 次

壹、研習目的.....	1
貳、研習過程重點摘要.....	2
參、心得與建議.....	14
肆、附件.....	17

壹、研習目的

Redback 為一著重於 access network 的網路設備製造商，主要產品為 SMS 系列的 B-RAS 及 SE 系列的 edge router；其中 SE 系列 router 亦具備 B-RAS 的大部份功能，近來在市場上頗受歡迎。而 Redback 於 2000 年併購加拿大的軟體公司 Abatis Systems 成為其加拿大分公司，試圖將該公司原有之 service creation tool、portal service 等技術與其硬體平台做一整合。

本計劃在 service creation/management 方面投入相當心力，除了收集各種 open source 的解決方案之外，也已在本計劃自行研發的 6Switch 乙太網路交換器加入類似的功能，此外亦購入 Cisco、Redback 的系統研究。由於 Redback NPM 系統採取的作業系統和軟體架構較為開放，提供的課程包含 BRAS 與 NPM 軟體搭配技術、設計架構及原始程式碼分析，因此派員參與此研習。

參加此研習將有助於建立本公司 Policy-based Network Management 核心技術，有助於減少公司整體網路維運成本，並可應用於 FTTB 大樓網路代維代管等客戶所需的新服務上。

貳、研習重點摘要

研習課程:

1. 參訪 Redback Networks
與部份 TAC, R&D, SQA 人員會面，大致瞭解產品研發測試過程與上線後技術支援、bug reporting/tracking 等流程。
2. 公司概況及產品線簡介
簡單介紹公司營運狀況及其主力產品，包括 TDM 傳輸設備、SMS 系列 B-RAS、SE 系列 router... 等等。
3. Introduction to SmartEdge router
新一代的 edge router，強調其 intelligence、rich feature set 及 high performance。
4. Introduction to NetOp Policy Manager
可與 SMS 或 SE 搭配的 service creation 平台，可提供 weblogin、使用者自行註冊登錄、線上動態改變 user profile(如頻寬、QoS 參數...)、service selection... 等各式功能，並可透過資料庫管理介面修改已存在的 services 或是由使用者自行定義 services。
5. NPM Software architecture
介紹 NPM 的整體架構、內部模組以及各模組之間使用的通訊協定、運作方式及流程... 等等。

實驗室上機實習:

1. NPM installation & configuration NPM on Sun Solaris
2. NPM installation & configuration NPM on RedHat Linux
以上兩個部分是一切從頭：由作業系統的安裝開始，實際操作 NPM server 的安裝及設定方式。
3. SMS B-RAS setup
配合 NPM 所需環境，實地安裝及設定 SMS 1800 B-RAS。
4. SE-800 router setup
配合 NPM 所需環境，實地安裝及設定 SE 800 B-RAS。

5. PPPoE demo

以筆記型電腦模擬使用者連線，測試 PPPoE 的認證、計費等功能。

6. CLIPS demo

以筆記型電腦模擬使用者連線，利用 DHCP 方式連線，並可透過 Web 方式做使用者認證。

7. Bandwidth on demand demo

以筆記型電腦模擬使用者連線，由 Web 介面自行選擇不同的頻寬等級。

8. Service selection demo

以筆記型電腦模擬使用者連線，使用者可由 Web 介面自行選擇不同的 service。

9. Customization & database management

修改 web portal 畫面，以及透過資料庫管理介面，查詢或修改 services、使用者帳戶、使用者計費資訊...等資料。此外亦示範如何在更新版本時將舊有資料轉檔。

10. Trouble shooting

實習各式偵錯工具，包括透過 B-RAS/router 的 console 觀察 debug message；利用 ethereal 抓取封包；察看 apache、tomcat、radiator 等軟體套件的 log file；使用 Redback 提供的 database synchronization script 同步資料庫中的資料....。

11. Discussions

討論 NPM 的 scaliability、與 DHCP 搭配的問題、研發設備的通訊定協介面...等問題，以及未來 roadmap、版本更新、市場接受度等等。

參、心得整理與建議

1. 寬頻市場的進化

- (TCP) “Port”-based bandwidth limitation
- 演化的方向
 - DSLAM: Ethernet/IP, multicast
 - new last mile technology
 - layer two network
 - Intelligence moving closer to edge
 - opening network to ISP/ASP
 - head-end POP
- next generation broadband
 - two tier B-RAS
 - distributed: QoS, AAA, multicast...
 - centralized: “service mode”, policy, wholesale...
 - ATM → Ethernet/IP
 - Heavy QoS implementation (working w/ SIP, CAC...)
 - B-RAS interworking w/ edge devices

2. NPM 系統需求

作業系統方面支援兩種常見的平台：

- PC : Redhat Linux 8.0 以上
- Sun workstation : Solaris 9

NPM 需要下列軟體套件運作，這些都是 opensource

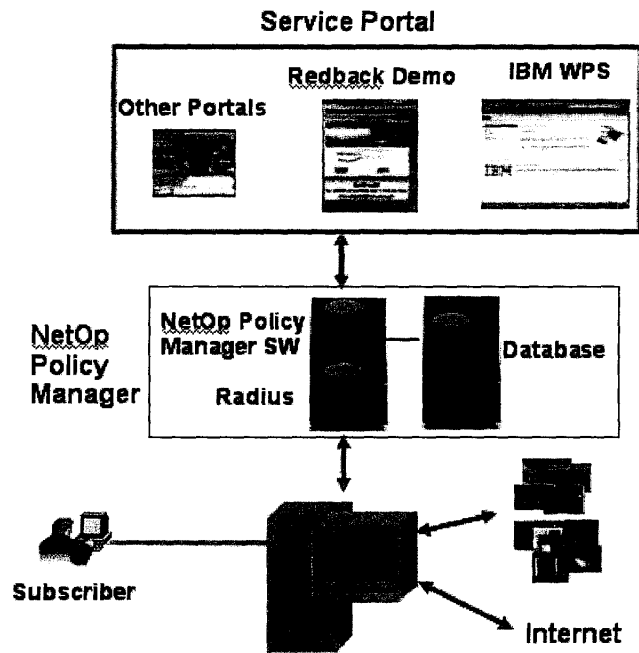
- Apache HTTP 2.0.40.8
- Apache Tomcat 4.1.18
- Java SDK 1.4.1.02

- MySQL 4.0.12.0
- Perl 5.8.0.55
- Radiator 3.6

另外有兩個 3rd party Java class, 提供 Tomcat server 發出 radius 及 snmp 呼叫的能力。

3. NPM 的組成

如圖一所示為 NPM 架構圖，大致可分成三層來看，最下層是使用者接入的設備(B-RAS 或 router)，如果以 PNM 的觀點來看，就是 PEP (Policy Enforcement Point)。中間層是 Policy manager，包括 database、authentication、accounting、決定使用者適用的 policy...，可以說是 NPM 的核心部分，也就是 PDP (Policy Decision Point)。最上層則是 http server、portal server 等，這一層的目的是呈現使用者介面。



圖一、NPM 架構

4. NPM 各部功能及通訊協定

事實上由前面可以看出 NPM 大多由 opensource software packages 組成，圖二所示為各模組之間的關係，以下就其各部功能做一簡介：

- Radiator RADIUS server (NetOp PM Radius)

Radiator 是 NPM 內建的一套 radius 伺服器軟體，負責認證、記錄計費資訊。事實上 Radiator 是一套商用的 opensource radius server，由 perl 撰寫而成，有開放出相當多的 APIs (Application Programming Interface)

可供使用者加上自訂功能，而且具備有 SQL database interface，可將資料置於外部資料庫。

- NetOpPM database MySQL 資料庫

MySQL 資料庫提供各種資料的記錄，比如 NAS 資訊、service 資訊、用戶資訊、計費資訊等。此資料庫透過 SQL 介面供 RADIUS server (Radiator)做認證、計費及 portal server (Tomcat)修改 service profile 使用。此外，管理者也可透過 MySQL 的 GUI 介面或是 CLI 介面直接對資料庫中的 table 管理。

- Apache Web server

Apache server 提供了一個基本的 web server 功能，接受 http 的請求，並 redirect 到 tomcat 的 port 上去。

- Tomcat server

Tomcat server 是實際上和用戶互動的部份，使用者透過 web browser 看到的畫面就是由 Tomcat server 所產生的。它會根據用戶認證的結果來決定是否要向 B-RAS/router 發出 SNMP set 來觸發 radius request。

這是 NPM 設計的特殊之處，不只是利用 RADIUS protocol 來做認證，也用來做 policy provisioning；但是因為 RADIUS 總是由 client initiated 的，所以需要

搭配 SNMP 做觸發的動作。

- DHCP server

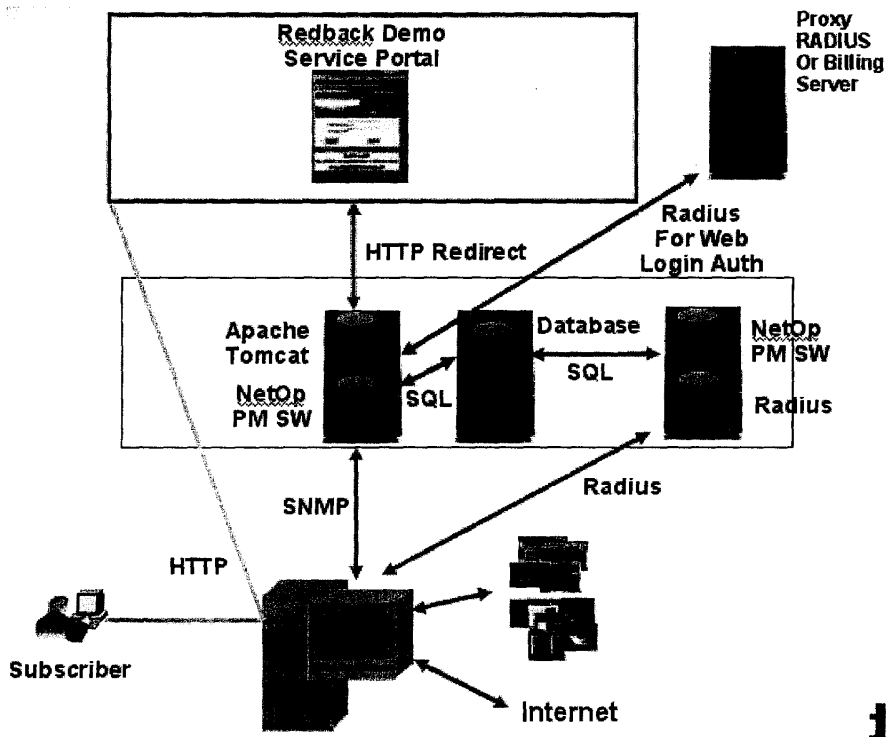
DHCP server 用來動態配發 IP 及相關參數給使用者。

嚴格說起來 DHCP server 並不算是 NPM 的一個元

件，尤其是使用 Smart Edge router 時，因為該設備僅

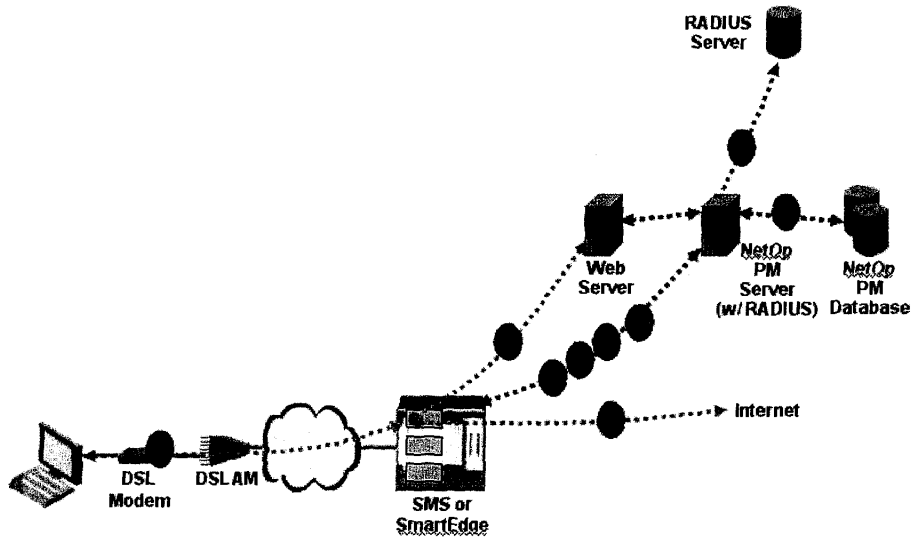
支援 DHCP proxy，並無內建 DHCP server。一般最常

見的 DHCP server 是使用 ISC DHCPd。

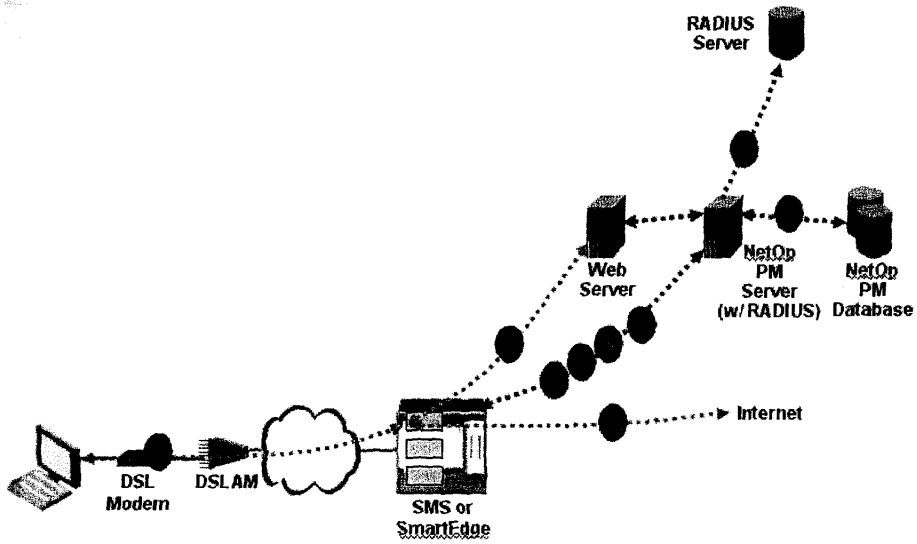


圖二、NPM 使用的通訊協定

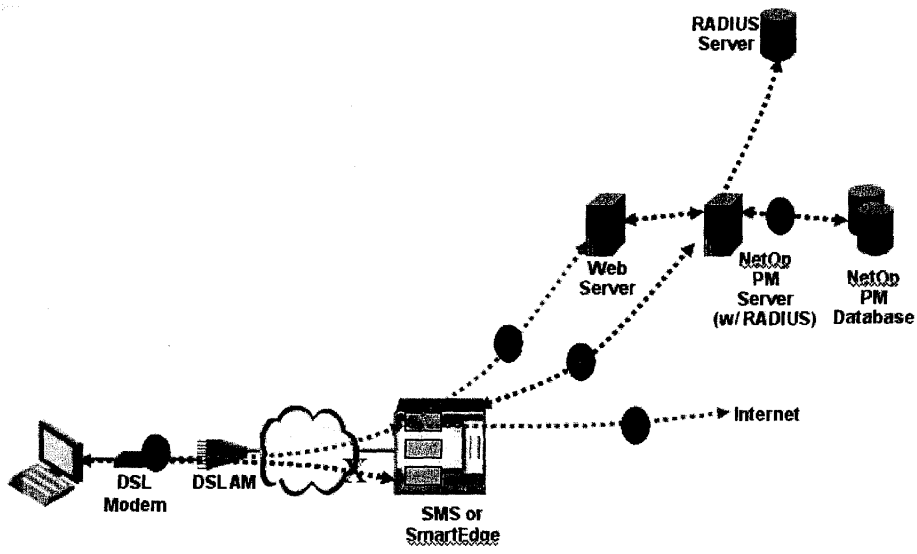
5. 各種服務應用模式



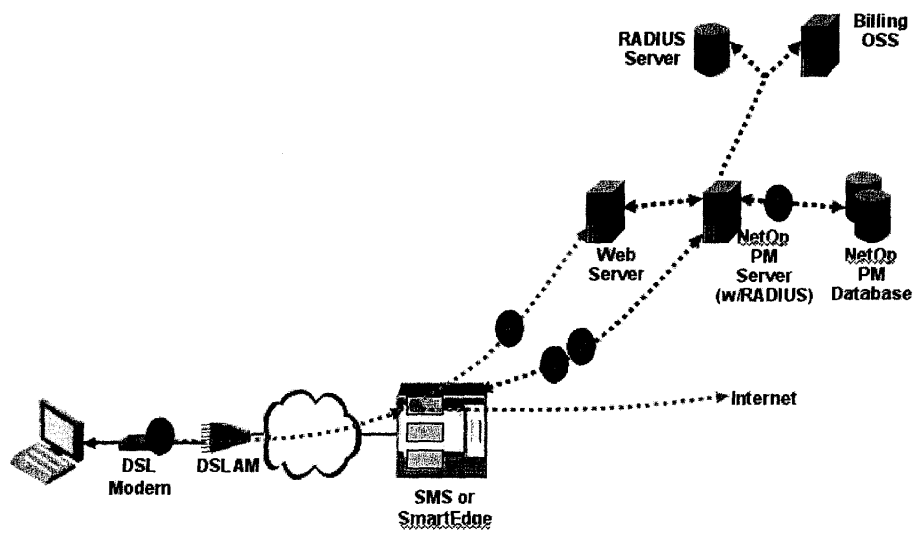
圖三、Weblogin service



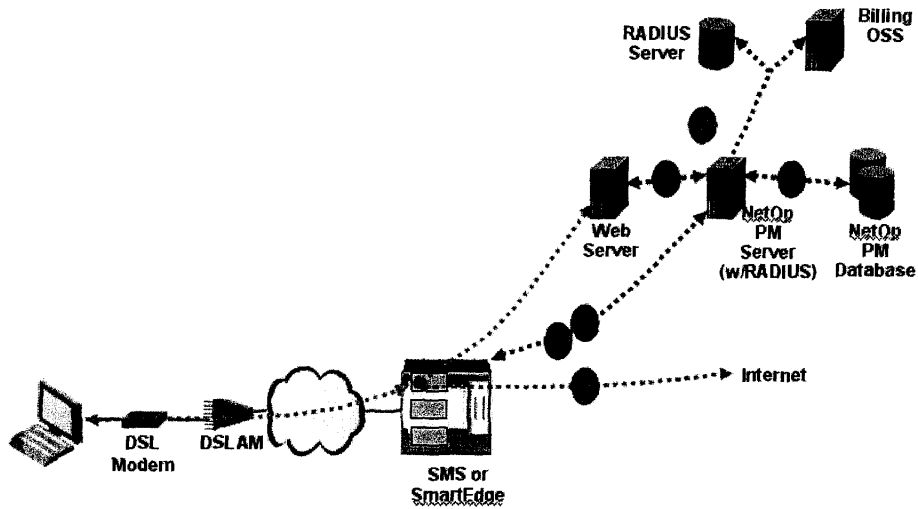
圖四、Bandwidth on demand service



圖五、service selection service



圖六、self-enrollment service (1)



圖七、self-enrollment service (2)

6. 與技術人員討論的 Q&A

- **Q:** DHCP server 怎麼做 redundancy/load-balance ?

A: SE800 沒有內建 DHCP server，而且僅支援針對一個 DHCP server 做 DHCP proxy，在下個版本的 firmware 才會支援多個 servers。在 Korean Telcom 的建置案中，目前的做法是利用一台 Layer 4 switch 擺在 DHCP servers 前面做 loadbalancing / redundancy。

- **Q:** DHCP timeout 的問題，如何決定合理的 lease time ?

A: SE800 上的 DHCP proxy 和一般的 DHCP relay 不同，使用者看到的 DHCP server 是 SE800；因此可利用不對稱

的方式設定，在 DHCP server 還是設定很長的 lease time (如 3 天)，但是在 SE800 上設成比較短的 lease time (如 10 分鐘)；如此即可避免 lease time 太短造成 flooding。

- **Q:** NPM 是否 scalable ?

A: 是的，NPM 的架構非常的 scalable，在 B-RAS 上你可以設定最多 5 筆的 RADIUS server，然後 B-RAS 會自動在這 5 個 server 之間 round-robin，而這些 Radiator 可以跑在同一部 NPM server 機器上的不同 TCP port，當然也可以擴充成為多台 NPM servers；這些 NPM servers 後端可以連結到同一個 MySQL database。

- **Q:** 如何讓分散各地的 site 集中使用同一個 portal server 以便管理？

A: 在目前的 firmware 版本你必需在 SE800 上設定 GRE tunnel，將 http traffic 導至遠端的 SE800；在下一個版本，我們會提供 http redirection，可以把 http request 導至任意的 URL，甚至附加一些變數在 URL 上。因此事情會變得更簡單。[那麼，在 portal server 也不需要做 D-NAT 了?]
是的，使用 http redirection 就不必做 D-NAT。

- **Q:** 關於 ADSL forum 中提到的 Smart CPE 概念，你們有計劃實作嗎？如果我們要設計一個 Smart CPE，並置於 NPM 的架構中，如果利用單晶片控制器如 8051，加上嵌入式 TCP/IP protocol 並實作 RADIUS，你認為可行嗎？

A: 我們目前並沒有計劃生產 CPE 設備，但是就大樓或是小區域用戶而言，我們希望能用 SE400 來取代 IPDSLAM 的地位。

至於 protocol 方面有三選擇，第一，使用 RADIUS 協定，這對整個架構的變動最小，但是你們就必須在 CPE 設備上實作 TCP/IP stack 及 RADIUS 協定。第二，我們目前正在規劃一種全新的 protocol 叫 SUP (subscriber update protocol)，它的目的是用於 SE800 (B-RAS) 和 SE400 (remote B-RAS) 之間的溝通；我們的研發人員正在草擬這個標準，並試圖讓它標準化；SUP 通訊協定在我們的計劃裡，但是目前還不會出現在我們的產品 roadmap 上。第三種是使用你們自訂的私有協定，它的好處可能是在實作上比 RADIUS 簡單，但是你必須在 NPM 加上你自己的 driver code。

- **Q:** 為何使用 Radius protocol 做為 policy management 的 protocol，IETF 不是有訂定 COPS protocol 嗎?

A: 因為 Radius 是 proven technology，你可以在世界各地看到許多成熟的應用；而且它很簡單、scalable，又具有延伸性，你只要定義自有的 VSA (Vender Specific Attribute)，就可以做任意的擴充。[但 COPS 也可以定義 PIBs，而且 COPS 是 PNM 的標準，不是嗎?] 沒錯，但是相對地，COPS 相當複雜，我還沒有看到任何一個成功的應用案例。

7. 心得

軟體發展趨勢

GNU/Linux、opensource 在軟體發展的過程所佔的角色愈來愈重要，在過去可能只是利用 opensource 的開發工具如 gcc 來做發展，但近來有愈來愈多的軟體是建構在 opensource packages 之上，這些趨勢都是必需多加以注意的，此外，也要瞭解各種 license 的內容，以免在商品化的階段違法。

產品的價值

NPM 雖然大部份由 opensource 組成，但其價值在於提出整體架構，並且整合各部軟體，最重要的是有一個穩定的硬體設備與之搭配。在與 Redback 的 R&D、SQA 人員會談時，可以知道其產品也是經過很長一段時間不斷測試，甚至透過客戶的回報來修正才漸漸穩定。一旦作業平台建立起來，配合完整的通報流程，後續開發增值功能就變得容易許多；相形之下，如果老是把立即性的市場擺在第一位，其結果往往是過度倚賴廠商的 total solution，並且大量壓縮測試的時程，再加上沒有完整的通報體系，這樣的模式很難得到一個成熟或是有延續性的產品。

擺脫舊思維

RAIDUS protocol 是大家早已熟悉的協定，但是應用在 policy provisioning，卻是很特別的想法，即使它有一些缺點如無法由 client initialite、因為使用 UDP 所以不容易做 load balance 以及 attribute 長度有限制；但是這些缺點都可以改善。著眼其穩定性、普遍接受度以及擴充性，再加上原有的認證計費用途，搭配 SNMP 使用，確實是比 COPS 較佳的選擇。

新型態服務

隨著網路及用戶的成長，以及 FTTB 市場的興，採用 PPPoE 做為的接取方式的缺點逐漸顯露出來，如網路邏輯拓樸的瓶頸點、multicast、維護多種版本的 PPPoE client、PPPoE client 授權費用...等等，如果換成 DHCP (以 Redback 的術語叫 CLIPS)的接取方式，看起來優點是遠多於缺點；即使需要做類似撥接制的機制，也可以搭配 weblogin 技術使用。目前國內市場已有多家 ISP 開始上線 DHCP 接取方式，也有不少廠商正在評估試用 NPM 系統，其影響不可不注意！

肆、附件

Redback Networks 實驗室一景

