第五章 系統實作與評估分析

ISP 在提供企業虛擬私有網路服務這項產品時，如何設計一個商業自動流程，能滿足企業客戶複雜的網路需求，增加企業資訊應用的彈性與創造其商業價值，並進一步降低企業管理的風險與成本，在 ISP 提供這項服務的同時，必需將企業網路的規劃、建置、維護、管理等流程做更專業有系統的設計與自動化，才能降低風險與成本，創造此項服務的商業收益。

根據上述的動機與目的，本論文的第三章提出了的企業網路需求分析，讓 ISP 業者瞭解企業客戶的真正需求與購買決策的方式，由此為 ISP 規劃一個具擴充性的 MPLS VPN 骨幹網路架構，能為企業客戶提供符合需求的 VPN 網路服務商品，並針對全球化趨勢，企業需要將其私有網路延伸至中國大陸與國際各地的情況，因而提出與國際 ISP 業者合作提供跨 ISP 的企業網路服務延伸架構，也因為 ISP 要提供如此複雜的網路服務商品組合(各種網路架構與加值服務應用)，所以希望將其統整在一個商業模組下以達成經濟規模，因此本論文提出企業網路需求選單的概念，延伸這樣的概念，在第四章提出 MPLS VPN 網管系統架構設計，主要的理論是根據以政策為基礎的網管技術，但經過簡化技術的複雜度，增加 ISP 產業實務的營運經驗，提出一個修正簡易實用的網管系統架構，並將服務的流程隱含於網管系統做集中控管。

最後本節根據第三章的需求分析與第四章的系統架構規劃，進一步製定出適當的資料表單，建立簡易的資料庫，安裝網管工具與撰寫簡易的 shell script 程式，開發出符合基本需求的網管系統之 prototype，並針對此一 prototype 做簡易的評估與分析。

5.1 MPLS VPN 網管系統實作

本論文提供一個統一且集中式的 Web-based 管理介面-Policy Manager，管理者只需在某一部個人電腦使用瀏覽器，即可透過 Policy Manager 做網路政策設定，並將政策配送至各個相關區域的 Policy Server，再透過 Policy Server 執行 telnet script 程式登入相關網路設備，自動設定網路設備的組態參數，毋需對所有網路設備逐一做設定，提供 ISP 網路業者完整的網路管理技術解決方案及模組化的系統軟體，希望能符合企業 VPN 網路管理之需求，本系統主要是簡化 IETF Policy-base 網路系統架構，包括三個主要模組角色，分別是 Policy

Manager、Policy Server 以及網路設備，在 Policy Manager 模組的部分，本論文只根據第四章規劃的 MPLS VPN 網路管理系統架構如【圖 4-4】，實作 VPN 服務的部分網管功能，實作環境請參考【圖 5-1】分述如后：

VPN Policy Manager

於 FreeBSD 作業系統平台上，開發 Policy Manager 程式模組，透過本系統提供的 Web-based 環境，管理者可以用圖形化的界面做網路政策的管理，本系統除提供網路政策編輯(policy editor)、Policy enable/disable、Traffic Monitor 等基本網路政策管理功能外，另結合 Mysql 資料庫提供網路政策資料庫(Policy DataBase)、網路政策監控(Policy Monitor)、網路政策報表(Policy Reporter)的資料分類儲存功能。

當企業客戶要加入新的 VPN 服務政策時，新的服務政策有可能與系統已存在的服務政策相衝突，因此政策管理系統必須在同一個客戶加入新政策的同時，進行政策一致性的確認工作，提醒管理者定出適當的政策規則，另一方面如果企業客戶的服務規格要異動時，系統必須制定相關的程序加以控管避免發生錯誤，所以以企業網路服務的產品狀態週期來說有新增、停用、暫斷、異動等情況發生，都必須有相對應的控制程序加以控管與執行。

Policy Server

於FreeBSD作業系統平台上，需先安裝網管相關工具如perl、zlib、gd、libpng、mrtg、ucd-snmp等模組，並開發Policy Server程式模組，提供執行Policy的能力，在實作中，利用MySQL做為資料庫的系統。由於Perl 可以利用SQL 的語法，經由DBI模組與資料庫溝通，得到我們所要的資料或是將資料記錄到資料庫裡，DBI模組並不知道要與何種資料庫溝通，但卻知道要如何去尋找且將DBD (Database Driver)模組載入，在透過DBD 進行連結，將所有關於網管政策與組態設定的資訊交由資料庫管理。Policy Server會將儲存在資料庫中的Policy Rules、Monitor Rules取出後，轉換成網路設備端(PEP)所能接受的格式，以telnet script程式傳送到網路設備端去執行。另外在Policy Server上也提供Monitor Daemon及Report Daemon，可依管理者的要求定時執行Policy或監控網路狀態。

網路設備端(PEP)

網路設備必須隨時接受Policy server的遠端控制，不需透過管理者在本機的手動設定，並讓新的設定能即時載入與生效。我們利用SSH 的方式，讓路由器的控制命令也是在一個安全的環境之中。此外由MRTG統計Router流量時，是透過 SNMP來取得資訊，由 MRTG 送出 SNMP查詢要求給Router，這時候我們稱此工作站叫做 SNMP Agent，而把 Router稱為 SNMP Server。SNMP查詢要求是使用 TCP 161 Port，SNMP Server 收到要求後會將要求的資訊以UDP 1024以後的Port傳送回SNMP Agent，另外為了讓網路設備能被Policy server控制管理必需設定的參數範例如下。

網路設備端網管監控功能啟動

- PE Router 的網管相關設定參數範例
  - ✓ 設定存取控制

    access-list 20 permit 192.168.1.99
  - ✓ 指定授權的網管主機查詢網路設備的狀態資料

    snmp-server community public RO 20
  - ✓ 將網路設備的trap傳送給指定授權的網管主機

    snmp-server host 192.168.1.99 public

    snmp-server enable traps

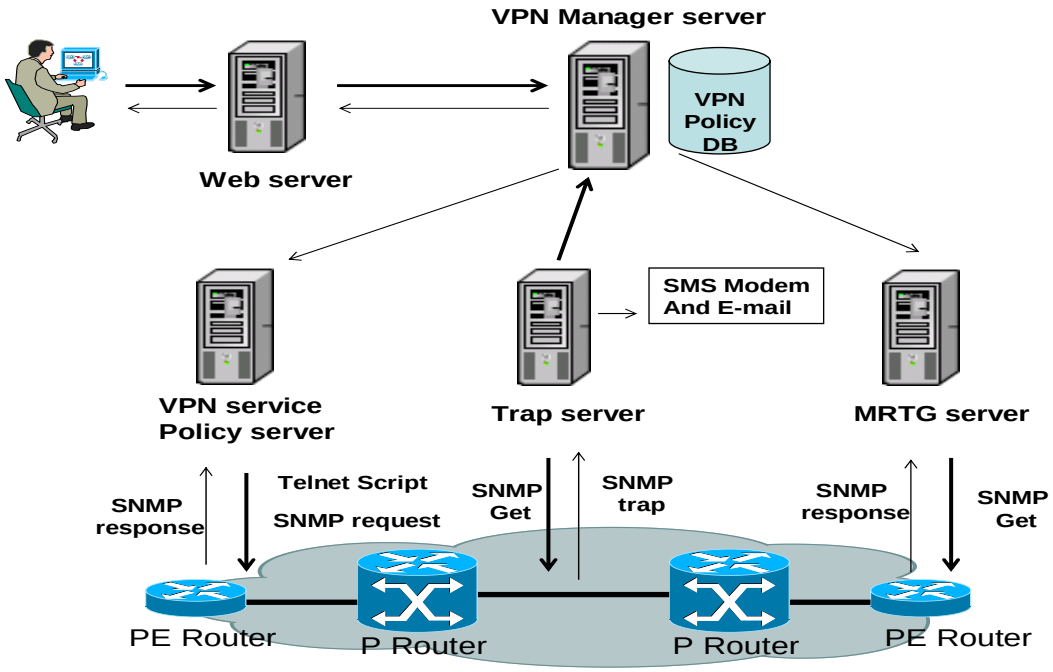
    snmp-server trap-source Loopback 0
  - ✓ 指定授權的網管主機使用CLI telnet script 設定網路設備參數

    line vty 0 4

    access-class 20 in
  - ✓ RMON even與alarm啟動設定參數

    rmon event 1 log trap get2seed description Rising owner config

    rmon alarm 1 ifEntry.10.1 60 delta rising-threshold 315000000 1 falling-threshold 285000000 owner config



【圖 5-1】網管系統實作環境

5.1.1 組態政策資料表建置

MPLS VPN 客戶設定參數資料表單欄位設計

本論文將網路組態資料儲存於資料庫中，我們使用 Mysql 的資料庫系統，主要用來提供管理者儲存已編輯完成的網路組態政策資料，及其他系統相關的網路設備資訊或設定參數等資料，而資料庫中主要 MPLS VPN 相關參數資料表單欄位規劃範例如【表 5-1】是記錄客戶單一節點線路種類及相關資訊，其中比較重要的是客戶編號、ADSL 附掛電話或專線編號、線路接入 ISP 的機房名稱、接入 ISP 端的設備 IP 位置與 Port 的位置、ADSL VCI/VPI 的值、實體線路介接 ISP 端與客戶端設備 WAN IP 位置、公司技聯絡人。

另一個資料表單是紀錄 MPLS VPN 相關網路組態資料如【表 5-2】所示，企業網路的拓樸架構、網路拓樸端別、MPLSVPN RD 與 RT 的值、與客戶端此節點對應 ISP 端的 PE Router 之 IP 位置、MPLS VPN RR 的 IP 位置、企業網路服務的種類等。

【表 5-1】MPLS VPN 客戶(基本資料)表單欄位

No	Field Name	ADSL	Leased Line
1	客戶編號	M8805006	M8805006
2	附掛電話	27990000	N/A
3	專線號碼	N/A	6D-83150
4	線路類別	ADSL	LL
5	機房名稱	高雄機房	台北機房
6	聯單編號	A11111111	6D-83150
7	固網甲端出線位置	N/A	TNC1-TNE1-3333-DS1-2-8
8	固網乙端出線位置	N/A	N/A
9	ISP 機房出線位置一	N/A	B2-7
10	ISP 機房出線位置二	N/A	B2-8
11	設備 IP 位址	139.x.x.x	192.x.x.x
12	設備 Port 的位置	2/1	3
13	VPI 位置	1	N/A
14	VCI 位置	100	N/A
15	ISP 端 IP 位置	172.17.0.2	192.x.x.2
16	客戶端 IP 位置	172.17.0.1	192.x.x.1
17	公司聯絡人	Jason	Jason

【表 5-2】MPLS VPN 客戶(VPN 組態資料)表單欄位

No	Field Name	ADSL	Leased Line
1	網路拓樸	Full-Meshed	Full-Meshed
2	網路拓樸端別	general	general
3	VPN RR1 IP 位址	139.x.x.1	139.x.x.1
4	VPN RR2 IP 位址	139.x.x.2	139.x.x.2
5	VPN PE IP 位址	192.72.x.x	192.72.x.x
6	VPN RD 值	4780:8908102	4780:8908102
7	VPN RT 值	4780:890810200	4780:890810200
8	Service Type	intranet	intranet

5.1.2 網路組態設定實作

Telnet script自動設定模式

根據 DMTF 與 IETF 這兩組織提出的 Policy-based Network 的階層式系統架構說明(請參考 2.5.2)中建議，PDP 和 PEP 採用 Common Open Policy Service (COPS)作業協定來傳輸資料，但此協定還不普並且一般 ISP 企業內部網路有各種不同廠牌或型號及老舊設備的問題存在，為了能加強此一網管系統跨異質網路的能力並且為避免不同廠牌或型號的產品所提供的 MIB 參數值不一樣，造成必須要取得廠商所提供的私有 MIB 即時修改程式碼，才能提供服務的不便。

因此本論文使用的網路設備支援標準命令列介面（Command Line Interface, CLI）模式，可直接使用 telnet 來將所有的組態指令，以剪貼（copy/paste）的方式，將資料傳送到設備上。所以必須發展 shell script 程式，以外掛（plug-in）方式，提供系統使用，系統只需將必要的組態指令寫成檔案就可以了，即使是未來設備更新，只要支援標準的 CLI，即可使用 telnet script，管理者只要稍加修改組態指令以符合新設備，大大的增加網管系統的彈性與可擴充性。在開發程式時模擬整個連線過程，當網路設備送出控制碼，程式即會做出適當的回應，直到將全部資料取得或設定完成，結束連線等，其中必須利用 shell script 自動登入網路設備並自動輸入帳號和密碼，下面是部分的程式碼範例。

```
#!/usr/local/bin/expect --
> spawn telnet 139.170.1.253
> set passwd1 xxxxx
> set username xxx
> set timeout 10
> while 1 { expect {
>                 "Username:" { send "$username\r" }
>                 "word:" { send "$passwd1\r" }
>                 "#" { break }
>                 "Bad" { send_user " Bad password\r"; exit 1}
>                 timeout   { send_user " Timeout problem\r"; exit 2}
>               }}
>
> ####set global config for PE router ####
> send "\r"
> expect #
> send "config terminal\r"
> expect router(config)#
> send "ip vrf F8908102\r"
> expect router(config)#
> send "exit\r"
> expect #
> send "exit\r"
> exit
```

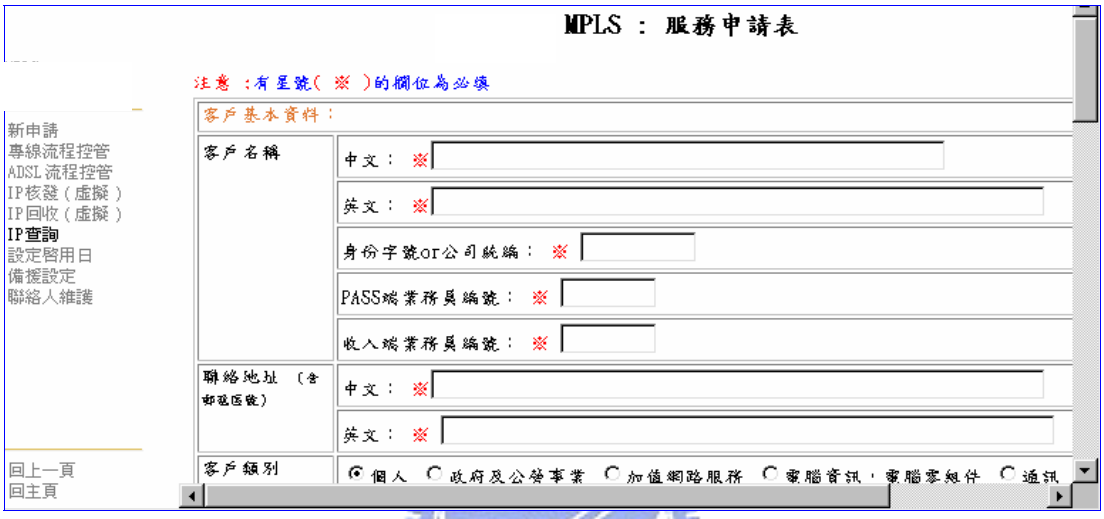
5.2 MPLS VPN 網管系統導入後效益

5.2.1 導入後定性的效益分析

網路組態自動設定管理系統

Policy based 的管理使網路管理人員由傳統的以網路和設備為中心的管理模式轉化為以業務為中心的管理模式，簡化管理過程，減輕對網管人員網管專

業知識和管理經驗的要求，同時也減少企業對網管人員技術培訓的開銷，透過圖解的使用者介面，用戶在設定配置時，將有對整體網路情況較好的觀察，因此能夠防止錯誤的發生。此外，系統將會提供一些分析資料(如網路利用率等)來幫助用戶在配置時能作出適當的決定。服務申請表主要是針對新客戶，填寫客戶基本資料及購買的網路服務種類數量等，請參考【圖 5-2】以作為連動客戶網路服務計費系統與網路管理系統的主要資訊，同時也是提供客服人員及業務人員服務客戶的基本資訊來源。



【圖 5-2】MPLS VPN 客戶服務申請表基本資料輸入圖

MPLS VPN 客戶連線資料輸入網頁，主要是輸入客戶 VPN 相關資料，請參考【圖 5-3】，例如 IP 範圍(系統有提示選單)、使用何種連線媒體建立 VPN 如 ADSL 或專線、網路拓樸架構為 Full-Mesh or Hub & Spoke、RD 與 RT 的參數值等。

【圖 5-3】MPLS VPN 客戶連線資料圖

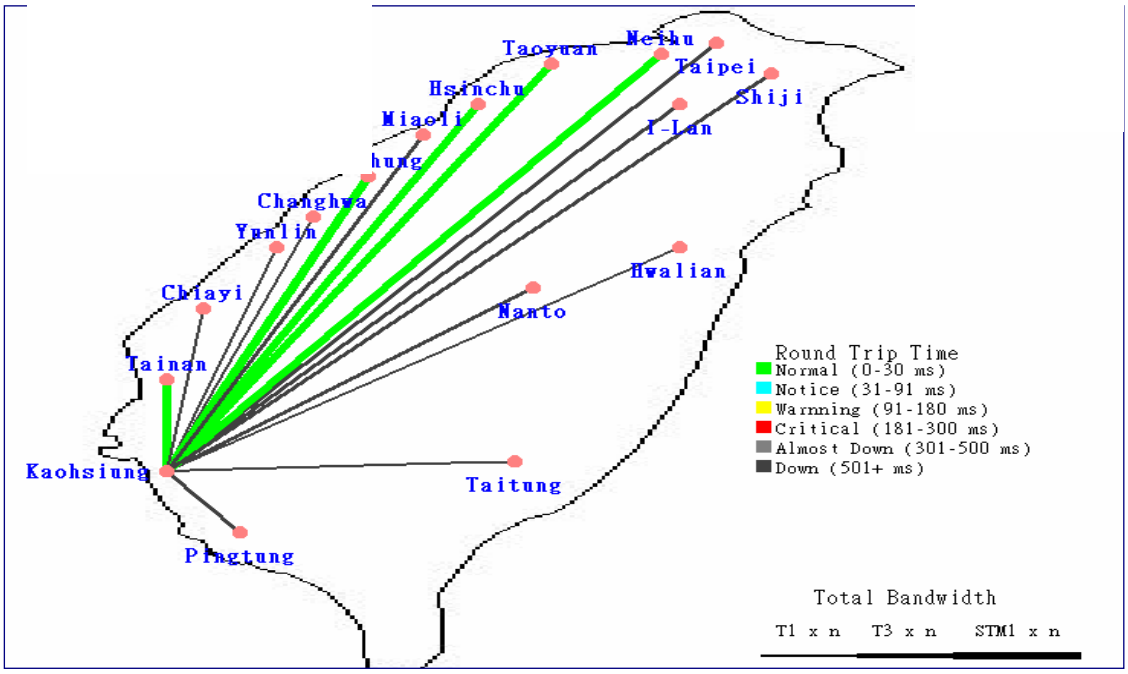
MPLS VPN 網路錯誤監控管理系統

基於瀏覽器的普及化，在使用者介面方面是以 Web based 為主，當瀏覽器升級時，系統不需要重新修改任何程式。在系統安全及管理方面，系統會預設一些不同級別的使用者，如：系統管理員、系統操作員等。他們將按照不同的使用者級別，而被授權執行不同的系統功能，如：系統登入許可權、網路修改許可權等。根據特定的網路系統需求，可以增加或減少額外的使用者。所用使用者帳號將會被加密及儲存在獨立的資料庫中。管理方面，系統能提供令使用者容易使用的介面來管理備份和還原等。

(1) MPLS VPN 骨幹網路品質監控系統

目前系統有兩個有效的方法，可以處理當警報發生時通知網管人員：視覺方法是在螢幕上出現各種顏色的圖案或聲音方法引起網管人員的注意，請參考【圖 5-4】另外我們將考慮另一個方法，告警管理例如：發送預設的消息至相關人員的 Email 及手機簡訊(SMS)即時通知。

網管人員可以更容易透過系統來一覽所有產生之斷線警報與骨幹網路品質不良事件，另外在螢幕上有固定的位置可以顯示即時的網路品質狀況 – 進各節點後可顯示該區目前有幾個緊急警告、重要警告、次要警告、事件警告及解除警告。當警報/事件未被告知接收時，警報/事件將會在螢幕上閃動。



【圖 5-4】MPLS VPN 骨幹網路即時監控系統

(2) MPLS VPN客戶端網路即時狀況查詢

可以透過 MPLS VPN 客戶端網路即時狀況查詢網頁，輸入客戶編號或客戶線路編號即可查尋客戶目前在各節點的線路資料、連接 PE Router 的 lookback IP address、Wan port 的 IP、客戶 IP 的網路區段、連接 ISP 端的機房位置、對外連線的即時狀況等資訊，請參考【圖 5-5】，方便工程人員做進一步判斷及處理網路問題。

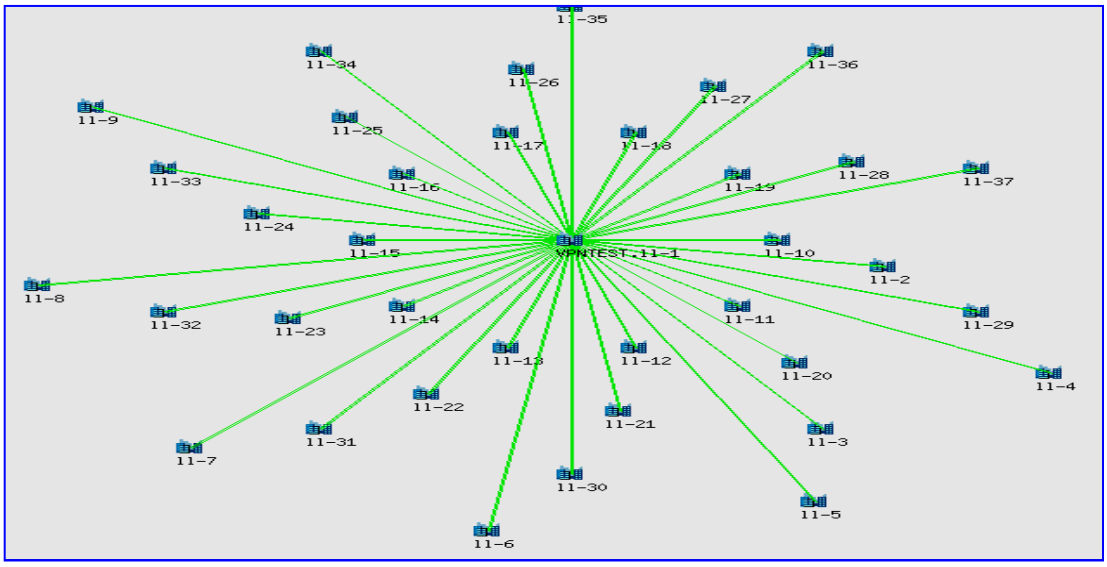
客戶編號	線路編號	設備 IP	WAN Port IP	IP 區段	所屬機房	對外連線狀態
F8908102	02-26274722	139.175.238.4	139.175.238.4	10.0.10.0-10.0.10.255 10.0.4.0-10.0.4.255	內湖機房	查詢
F8908102	02-26274722	139.175.238.4	139.175.238.4	10.0.10.0-10.0.10.255 10.0.4.0-10.0.4.255	內湖機房	查詢
F8908102	15-254	139.175.238.227	139.175.238.227	10.0.15.254-10.0.15.254	高雄機房	查詢
F8908102	150-254	139.175.238.130	139.175.238.130	10.0.150.254-10.0.150.254	台中機房	查詢
F8908102	3-254	139.175.238.4	139.175.238.4	10.0.3.254-10.0.3.254	內湖機房	查詢
F8908102	5-254	139.175.238.4	139.175.238.4	10.0.5.254-10.0.5.254	內湖機房	查詢
F8908102	KS-PE-S1-0	139.175.238.226	172.31.161.1	10.0.6.0-10.0.6.255	高雄機房	查詢

【圖 5-5】MPLS VPN 客戶端網路即時狀況查詢系統

(3) MPLS VPN 客戶端網路拓樸架構即時監控系統

圖像顯示網路架構:使用 SNMP 搜集網路中的配置資訊，根據規劃與配置精確的顯示網路的拓樸圖以不同的圖代表網路上各種裝置，請參考【圖 5-6】正確的顯示網路上各種裝置的配置資料可以支援自動發現功能，如 cisco 路由器及其連接的網路幹線，可針對網路的部份細節加以放大顯示，操作簡易的圖像介面。

使用者可以清楚地瞭解到整個網路的結構。另外，使用者在主頁上可以選擇使用拓樸映圖裝置、放大圖形或功能選擇系統，用來配置或監控整個網路系統。因此，使用者可以無須牢記任何裝置化低階的指令，它們將會被下拉及點選等這些簡單的動作取替。



【圖 5-6】客戶端網路拓樸即時監控系統

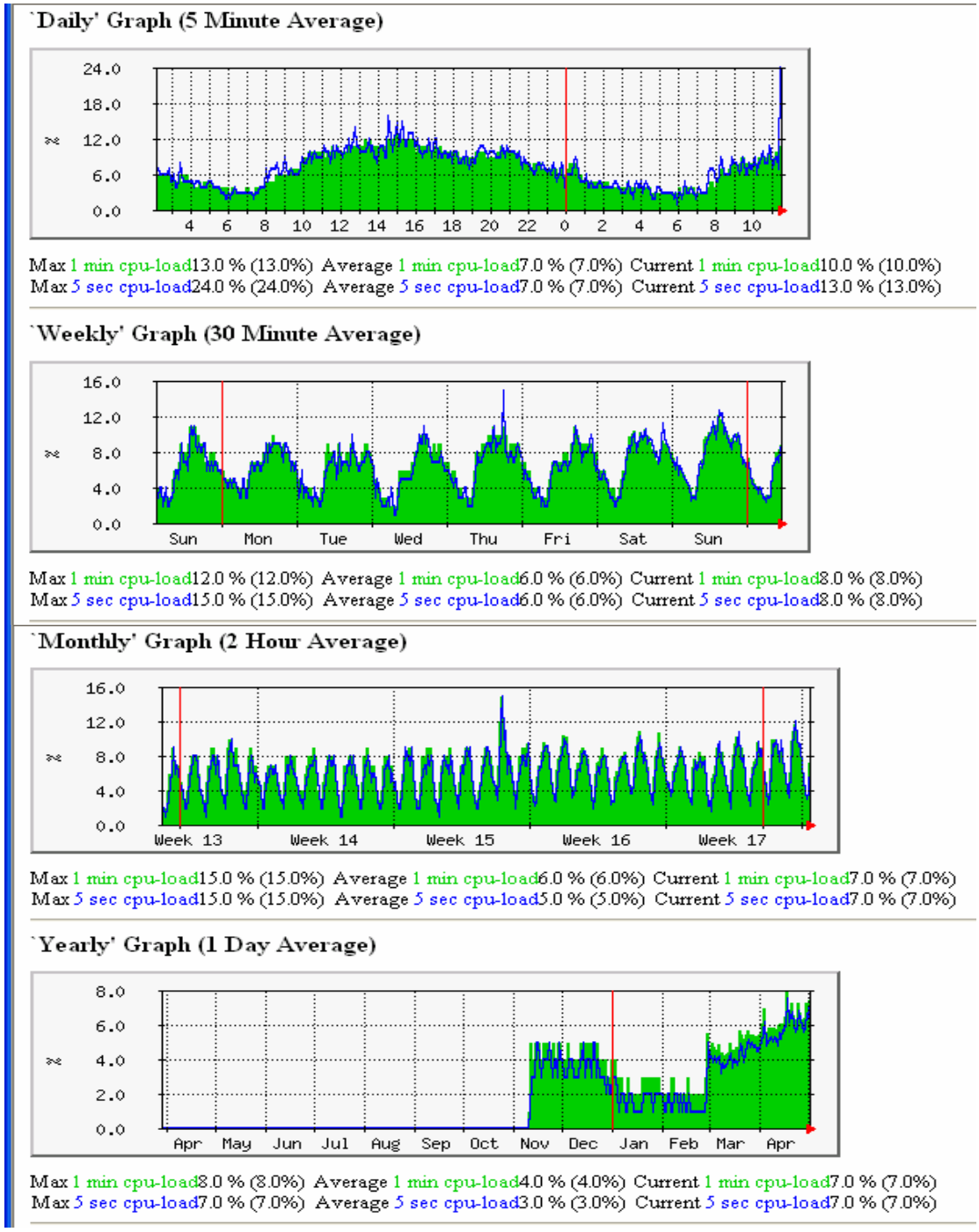
(4) 全省 PE Router 設備性能即時監控系統

系統能提供以目錄和圖表來表示的即時及統計報告。它們包括網路統計報告，CPU 使用率、Free Memory 剩餘大小、PE Router Uplink 的頻寬使用率、Packet Loss 等相關的資料，請參考【圖 5-7】。所有資料能在自定的格式內拿取，因此能把資料轉移到其他軟體再作進一步的分析和報導。當 ISP 拿到這些有用的資料，可以決定如何去修改網路政策分配封包流量分佈、平衡負載安排、網路資源再分配等作出判斷。此外，亦可以找出如資料流程量之瓶頸、在不同時間範圍內的網路使用率等。

【圖 5-7】全省 PE Router 設備即時監控系統

(5) 網路流量統計

網路流量統計對於企業 VPN 網路的狀態是一項重要的指標，可以瞭解目前及過去網路尖峰與離峰時刻的使用狀況，進而掌握網路的流量負載，以達到監測網路流量的目的，請參考【圖 5-8】。掌握企業 VPN 網路中每個節點的網路流量與網路連線狀態，可以做為改善舊有網路環境的建置缺失，如網路流量的頻寬分配，可提供是否將頻寬加大或限制某些流量的參考。



【圖 5-8】網路流量統計圖

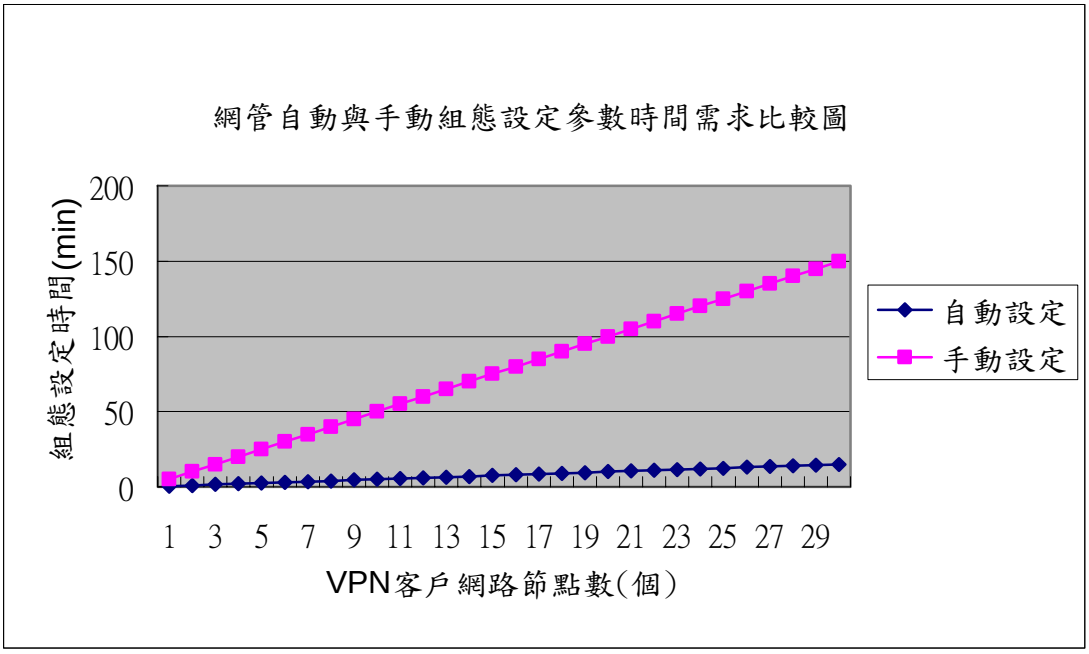
5.2.2 導入後定量的效益分析

MPLS VPN 網路組態設定管理系統

利用此 Web based 網管配置系統，從進入相關選單網頁輸入各類參數，到完成建立 MPLS VPN 客戶單一網路節點的過程平均大約需 0.5min，此外測試當從網頁上按下傳送後到參數設定到 PE Router 的反應時間大約 1~2 second，然而

工程師使用傳統方式 telnet 遠端登入 PE Router 做手動參數設定，整個過程平均大約需 5min，之所以有這些差距是因為工程人員用傳統方式 telnet 遠端登入 PE Router 做手動設定時，需要根據路由器 IOS 軟體的語法下指令並設定參數值，然而使用 Policy-based 的網管系統時，使用者只需輸入主要的參數值，系統會自動將其參數值整合已編輯好的政策規則後，再轉換成路由器 IOS 軟體可接受的語法格式，並且傳送給各節點相關 PE Router 完成設定。

如果 VPN 客戶網路的節點數很少的話，用手動設定與自動設定差別可能不大，但如果網路節點數有 5 點以上組態設定所需時間就有很大的差距，請參考【圖 5-9】的比較可知如果當 VPN 客戶的節點數有 30 個節點，使用自動設定大約維持在 12min 內可完成設定，但使用手動設定大約要花 150min 才能完成，所以使用這套系統只需傳統手動設定所需時間的 1/10 即可。



【圖 5-9】自動與手動組態設定時間需求比較

MPLS VPN 網路錯誤監控管理系統

(1) 客戶線路品質監控效能分析

線路品質監控主要項目包含(1)Lease line/ADSL 斷線(透過 Trap)，(2)線路產生嚴重 Error，(3)Reachable 發生問題，(4)Delay time>180ms，(5)Packet Loss > 20%，(6)Bandwidth Utilization> 80%。通知方式包括(a)手機簡訊(SMS)通知，(b)不同頻率 E-mail 通知相關人員，通知的反應時間皆可在 1~5min

內可收到，通知成功率在手機簡訊(SMS)部分，因為瞬間大量時會有 GSM 局端擁塞問題發生，造成部分簡訊遺失所以成功率只有 97%，而在 E-mail 通知方面成功率都在 99%，請參考【表 5-3】，以上數據是根據簡訊主機與 mail 主機 log 統計得知，另外也有監控客戶線路頻寬使用率如果過高，所購買頻寬使用率 > 80%時，透過 E-mail 通知該地工程與業務每天一次，使業務通知客戶加買頻寬以維持好的網路品質。同時針對客戶不同等級流量監控，提供 MRTG 流量圖。

【表 5-3】客戶線路品質監控效能分析

網管監控 / 客戶端 / 通知方式 / 線路問題種類	手機簡訊(SMS)通知監控中心工程人員	E-mail 通知監控中心工程人員	E-mail 通知當地工程及 Hub 端工程人員
斷線 /Error(reliability)(透過 Trap)	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%
Reachable/Delay time/ Packet Loss	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%
Bandwidth Utilization > 80%			E-mail 通知該地工程及業務每天一次

(2) MPLS VPN骨幹網路品質監控效能分析

為了要提供給 MPLS VPN 客戶網路品質的保證，我們針對(1)MPLS 網路中的 PE Router 本身對外的網路品質及(2)PE2PE Qos 的監控，以確保 VPN 客戶 end-to-end 中經過 ISP MPLS 骨幹網路的品質能維持在 SLA 定訂標準的範圍內。在前者的監控項目包括：PE Router Uplink Port down、Packet loss > 10% Bandwidth Utilization > 80%、Reliability < 252 及發生 Unreachable 時發出簡訊或 E-mail 通知，在後者的監控項目包括：監控從台北端和高雄端分別到各節點 PE 路由器的品質--Packet loss > 10%、Delay Time > 80ms 及發生 Unreachable 時發出簡訊或 E-mail 通知，通知的反應時間及成功比率請參考【表 5-4】。

【表 5-4】MPLS VPN 骨幹網路品質監控效能分析

網管監控通知方式 / 骨幹網路品質監控種類	手機簡訊(SMS)通知監控中心工程人員	E-mail 通知監控中心工程人員	E-mail 通知當地工程及骨幹工程人員
全省各 PE Router	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%
PE2PE Qos 監控	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%

(3) MPLS VPN 路由資訊監控效能分析

VPN 客戶的網路發生問題，不一定是線路問題造成，有時是因為路由資訊發生錯誤或是路由資訊遺失，因此對於 MPLS VPN 路由資訊做定期確認工作，偵測是否有異常現象發生，所以首先對 RR2PE 與 PE2RR MP-BGP Session 做監控，看看是否 Session down，如果發生 Session down 客戶 VPN 各節點的路由資訊就無法交換，即使客戶線路正常網路也是不通的，另外更進一步監測在各節點的 PE Router，比較目前客戶 VPN 路由資訊是否與原始資料庫的資料是否相同，相異則發出簡訊或 E-mail 通知，通知的反應時間及成功比率請參考【表 5-5】。

【表 5-5】MPLS VPN 路由資訊監控效能分析

網管監控通知方式 / 骨幹網路路由資訊種類	手機簡訊(SMS)通知監控中心工程人員	E-mail 通知監控中心工程人員	E-mail 通知當地工程及骨幹工程人員
RR2PE 與 PE2RR MP-BGP Session 監控	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%
PE Router 及 RR Router 上客戶之 VPN 路由資訊是否正常	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%

(4) MPLS VPN骨幹網路設備監控效能分析

針對 MPLS VPN 相關重要網路設備如 PE Router、RR Router、ASBR Router(建立 inter-AS MPLS VPN 時於其他 ISP MPLS 網路界接的路由器)，做基本的效能監測以防止路由器因負載太高而當機，主要的監控項目有 CPU Loading > 50%、Free Memory < 5Mbytes、Unreachable(從台北及高雄網管主機分別做 ping 1 次/5sec)等，如果發生異常則發出簡訊或 E-mail 通知，通知的反應時間及成功比率請參考【表 5-6】。

【表 5-6】MPLS VPN 骨幹網路設備監控效能分析

網管監控通知方式 / 骨幹網路設備種類及監控項目	手機簡訊通知監控中心工程人員	E-mail 通知監控中心工程人員	E-mail 通知當地工程及骨幹工程人員
各點 PE Router 監控	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%
RR Router 監控	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%
ASBR Router 監控	可在 1~5 分鐘內收到，成功率 97%	可在 1~5 分鐘內收到，成功率 99%	每三十分鐘一次，成功率 99%