行政院所屬各機關因公出國人員出國報告書

（出國類別：實習）

赴澳洲實習

「寬頻遠端接取伺服器規劃設計與維運技術」報告

出國人 服務機關	職　　稱	姓　名
總公司技術處	副工程師	陳明欽
總公司網路處	助理工程師	江怡澤
北區分公司經營規劃處	工程師	陳清培
北區分公司網維處	副工程師	邱其添
北區分公司設計處	助理工程師	曾志元
中區分公司規劃設計處	副工程師	洪東生
中區分公司網路處	助理工程師	謝忠達
南區分公司網路處	股長	吳國賢
南區分公司台南營運處	專員	黃清忠
研究所網路維運支援技術研究室	副研究員	林世媛
研究所寬頻網路室	助理研究員	梁銘顯
研究所專線維運支援技術專案	助理研究員	梁居東
訓練所交換科	講師	黃春吉

出國地點：澳洲

出國期間：自 89 年 11 月 26 日至 12 月 9 日

報告日期：90 年 3 月 29 日

目　　錄

0. 摘要

1. 前言

為因應寬頻網路加值服務業者及服務供應商快速成長的大量需求，北電網路正式推出通訊產業界第一套寬頻網路服務的用戶彙接系統--Shasta 5000。由於其堅強的軟體與硬體設計，設備新增加之性能，更加符合了服務供應商用戶之要求以及提供高效能的網際網路所開發之關鍵性技術及發展應用。

中華電信公司為服務廣大的用戶並接受新固網業者的挑戰，特引進北電網路的 Shasta 5000 寬頻服務節點，藉以推出獨特且創新的加值服務業務，提供用戶全面性寬頻服務，滿足對目前和未來網路應用的需求，而此嶄新的寬頻加值服務更將會是未來服務供應商能否獲利與存活的關鍵。

2. 行程及實習內容紀要

為配合本公司引進Shasta 5000寬頻服務節點，奉交通部八十九年十一月十六日交人八十九字第〇六五三二三號函核准職等前往澳洲實習「寬頻遠端接取伺服器規劃設計與維運技術」，實習期間(含行程)自民國八十九年十一月二十六日至八十九年十二月九日為期十四天。本次實習課程計有：

Nortel Shasta 5000 BSN (3 天)

Nortel Shasta 5000 BSN Hands-on (2 天)

Nortel Passport 15K and ATM Integration (2 天)

IP Networking Overview (2 天)

3. Shasta 5000 BB-RAS 之系統架構及服務應用

Shasta 5000 BB-RAS又稱為Shasta Broadband Service Node簡稱Shasta BSN，以下就Shasta 5000之系統架構及服務應用作簡要之描述。

3.1 系統架構

3.1.1 硬體架構

(1) 概述

Shasta 5000之基座共有14個插槽，依據服務的需要，可由基座正面在不中斷電源下，插入或拔出不同組合的卡板，以提供不同的服務，基座之正面標示不同的顏色，以配合卡板之顏色，避免電路板誤插，卡板的種類如下：

- 控制管理卡(Control and Management Card，簡稱CMC) – 插槽13及14

  CMC卡負責基本系統運作、管理、路由及指定等功能。

- 用戶服務卡(Subscriber Service Card，簡稱SSC) – 插槽1 - 6及9 - 13

  SSC卡負責所有用戶服務。

- 交換結構卡(Switch Fabric Card，簡稱SFC) – 插槽7及8

  SFC卡提供ALC及SSC卡板間之ATM層互連。

- 線路卡(Line Card，簡稱LC) – 插槽1 - 6及9 - 13

  LC卡提供連接BSN之實體介面埠。

其中CMC及SFC卡板可配置為redundant架構，插槽5、6、9、10之基座標示為紅色，代表這些插槽可運作的能力為1.2Gbps，其餘插槽的能力為622Mbps。

Shasta 5000之基座及卡板外觀如圖3.1。

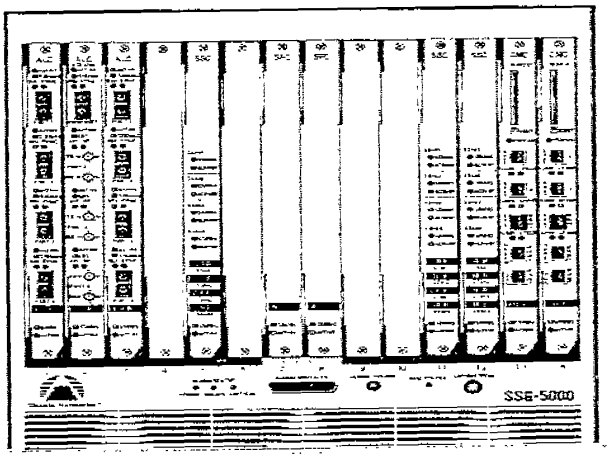


圖3.1 Shasta 5000外觀圖

(2) CMC 卡– 插槽 13 及 14

CMC卡除負責基本系統運作、管理、路由及指定等功能外，尚有：

- 包含Flash及硬碟設備供Shasta儲存作業系統及組態(configuration)檔案，也可選購PCMCIA卡作為備份儲存設備。
- 提供2個Ethernet用戶介面埠。
- 提供1個管理埠、1個串列modem埠及1個串列console埠。

工程設計規則如下：

- 每1套Shasta 5000只需一片CMC卡，另一片CMC卡是為了redundancy。
- 當只有1片CMC卡時，可插在插槽13或14，但插槽14只能插CMC卡。

- 當有2片CMC卡時，通常插在插槽14之CMC卡是active。
- CMC console埠需要使用一條serial management cable，一端以RJ-45接頭連接CMC卡，另一端以DB-25接頭連接工作站。
- 其外觀結構如圖3.2所示。

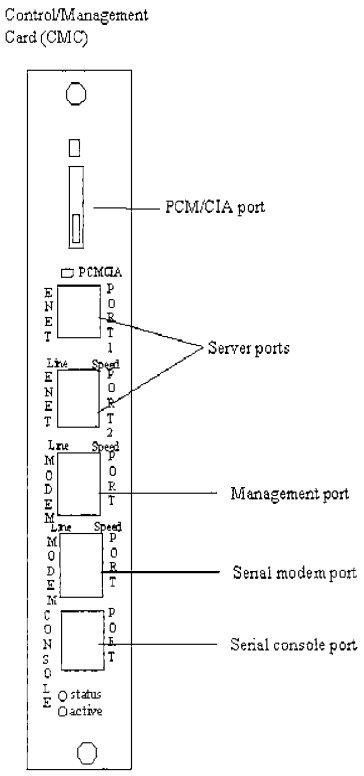


圖3.2 CMC外觀圖

(3) SSC 卡– 插槽 1 - 6 及 9 - 13

SSC卡提供所有用戶服務及訊務管理，SSC包含處理器陣列對每一個用戶執行個別服務及策略的操作。

SSC裝置4組用戶服務模組(Subscriber Service Module，簡稱

SSM)，由SSM提供用戶服務。

工程設計規則如下：

- 每1套Shasta 5000可裝設最高6片SSC卡，其中1片作為redundancy。
- 每1片SSC卡包含4組SSM，每1組SSM包含4組用戶服務處理器(Subscriber Service Processors，簡稱SSP)。
- SSM處理所有加密(encryption)
- 1個SSM每秒可route 176,000封包(packet)。
- 其外觀結構如圖3.3所示。

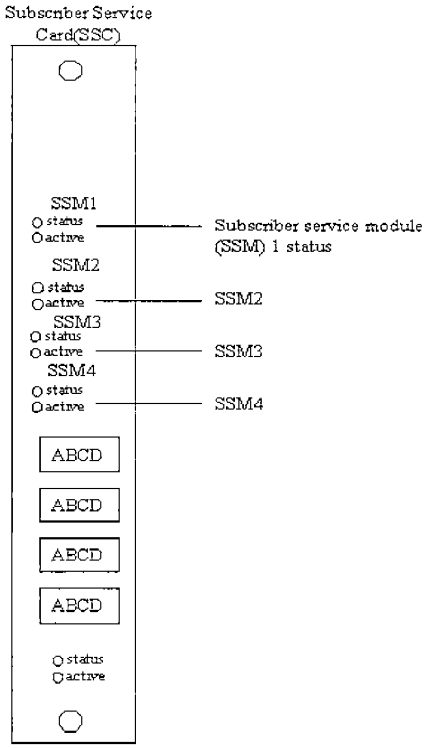


圖3.3 SSC外觀圖

(4) SFC 卡– 插槽 7 及 8

SFC卡提供ALC及SSC卡板間之ATM層互連及佇列(queuing)，其頻寬可達10Gbps。

工程設計規則如下：

- 插槽7及8只能插SFC卡，SFC卡以1：1方式運作，其中1片為redundancy。
- 可支援256,000VCs。
- 其外觀結構如圖3.4所示。

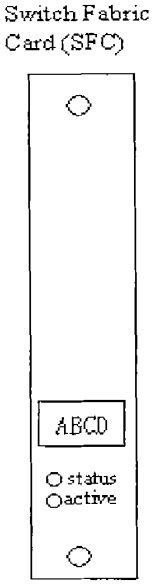


圖3.4　SFC外觀圖

- SFC卡以母子卡方式決定其可提供之頻寬大小，母卡頻寬為2.5Gbps，若所需頻寬大於2.5Gbps時，則可增加子卡，其規

則如下：

卡板選項	ATM頻寬	可用插槽
SFC母卡	2.5Gbps	11 - 14
2.5Gbps子卡	5.0Gbps	1 - 4、11 - 14
7.5Gbps子卡	10.0Gbps	所有插槽

(5) LC 卡– 插槽 1 - 6 及 9 - 13

LC卡提供連接BSN之實體介面埠，可供單模(Single-mode)、多模(Multimode)光纖及BNC同軸等連接。

所有LC卡均裝置有Intelligent Cell Parser(ICP)，ICP主要是將進入之訊務指引至適當的SSM，ICP由CMC得到用戶識別的組態資訊，再由新的資訊流的第一個封包來指引訊務。LC卡可有下列幾種類別卡板：

- OC-3 ALC：提供4個單模或多模OC-3光介面埠。
- DS3 ALC：提供1個單模或多模OC-3光介面埠及3個DS3同軸介面埠。
- E3 ALC：提供1個單模或多模OC-3光介面埠及3個E3同軸介面埠。
- OC-12c ALC：提供2個OC-12c光介面埠。
  - OC-12c卡板只能插於5、6、9、10插槽
  - 如果OC-12c卡板插在1 - 4、11 - 12及13時，只有埠2能運作，埠1無法使用。

• Channelized T3 LC：提供4個Channelized T3同軸介面埠。

• Fast Ethernet：提供8個Ethernet介面埠，每1個埠可在10M或100M Base-T運作。

(6) 資料流(Data Flow)

• Egress及Ingress訊務定義

Egress訊務：由網際網路流向用戶之訊務。

Ingress訊務：由用戶流向網際網路之訊務。

• Shasta 5000資料流程概述

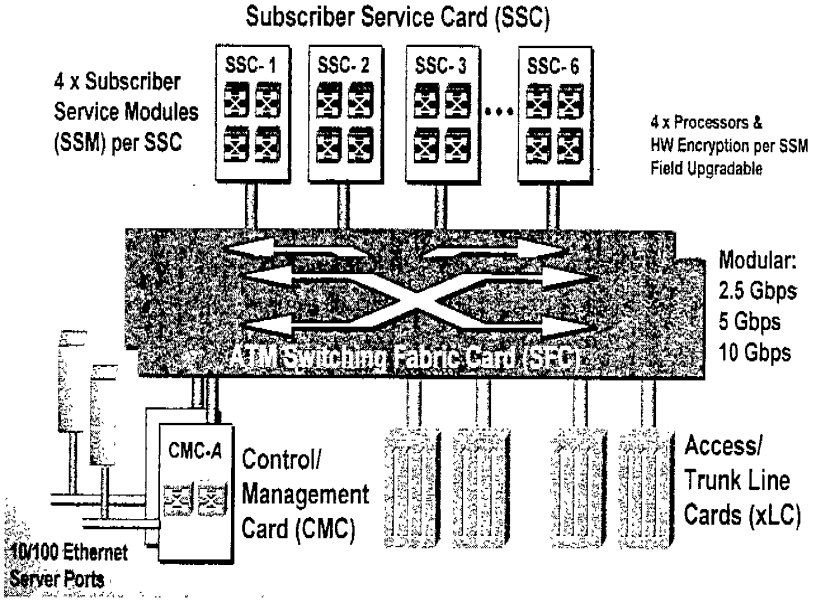


圖3.5 Shasta 5000資料流

依圖3.5來說明Shasta 5000資訊流的情況，資訊流的流程為ALC → SFC → SSC → SFC → ALC，以下分Ingress及Engress兩種情況分

別描述：

a. 由用戶至核心網路(接取/Ingress)

(a) 訊務經由 ALC 介面埠(或 CMC 之 ethernet 埠)進入 BSN。

(b) 訊務經由 ATM 背板轉至 SFC。

(c) SFC 將訊務轉至 SSC 作服務處理。

(d) SSC 提供服務後再將訊務轉至 SFC。

(e) SFC 將訊務轉至 ALC，經由介面埠出 BSN。

b. 由核心網路至用戶(中繼/Engress)

(a) 訊務經由 ALC 介面埠進入 BSN。

(b) 經由 ALC 之 ICP 將訊務送至 SFC，再轉至 SSC 上以個別用戶作處理之 SSM。

(c) SSM 處理後將訊務轉回 SFC，再經 ALC 之介面埠離開 BSN。

(7) 硬體錯誤(hardware fault)

Shasta 5000有AC/DC備援，下面對各項硬體錯誤來作敘述：

• SFC 錯誤：

Shasta 5000對SFC有1+1保護，但必須要裝有兩個SFC卡板，1個當主一個備援。

當主卡板發生問題時，馬上將服務切到備援卡板，資料損失率接近零(near-zero data loss)。

• CMC錯誤：

現存所有的sessions不會影響，但不能再增加新的session，所有sessions可以在3分鐘重建完畢

- SSM 錯誤：

故障SSMs上的對應用戶會被平均分擔至其他SSMs上。ssions從故障後開始切換的時間也可以加以設定

- ALC錯誤：

需要配合雙中繼(dual-trunk)的ATM switch 或Sonet ADM設備作備援的動作。

3.2 軟體架構

Shasta 5000軟體架構如圖3.6，包含：

- 服務創造系統(Service Creation System，簡稱SCS)伺服器
- SCS客戶端
- IP服務作業系統(IP Service Operating System，簡稱iSOS)
- 客戶網路管理(Customer Network Management，簡稱CNM)

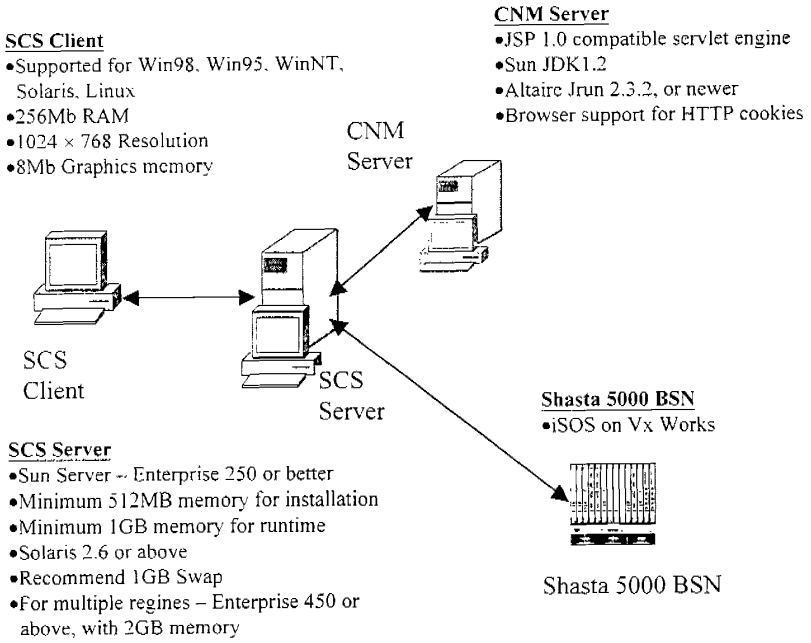


圖3.6　Shasta 5000軟體架構

(1) 服務創造系統(SCS)伺服器

SCS伺服器是一個多層架構，它分為ISP層(ISP tier)、設備擁有者層(Device Owner tier)及地區層(Region tier)，階層次架構如圖3.7，各層除負責其管理功能外，並與其它層一起工作。

- ISP層

ISP層包含Lightweight Directory Access Protocol(LDAP)目錄伺服器，LDAP伺服器的目錄中包含所有ISP的非裝置(non-device)特定資料，LDAP伺服器與設備擁有者層通訊並管理所有ISP層資訊，主要項目為所有用戶紀錄、radius profiles及服務策略。

註：絕不在LDAP層對用戶組態作改變，而是於設備擁有者層改變。

- 設備擁有者層

此層為管理網路的中心，它與ISP層與地區層通訊，主要含有domain伺服器，此伺服器維持地區的所有資訊，及裝置擁有者非裝置特定資訊，此非裝置特定資訊是所有地區所分享，所有SCS客戶端均為domain伺服器的客戶端。

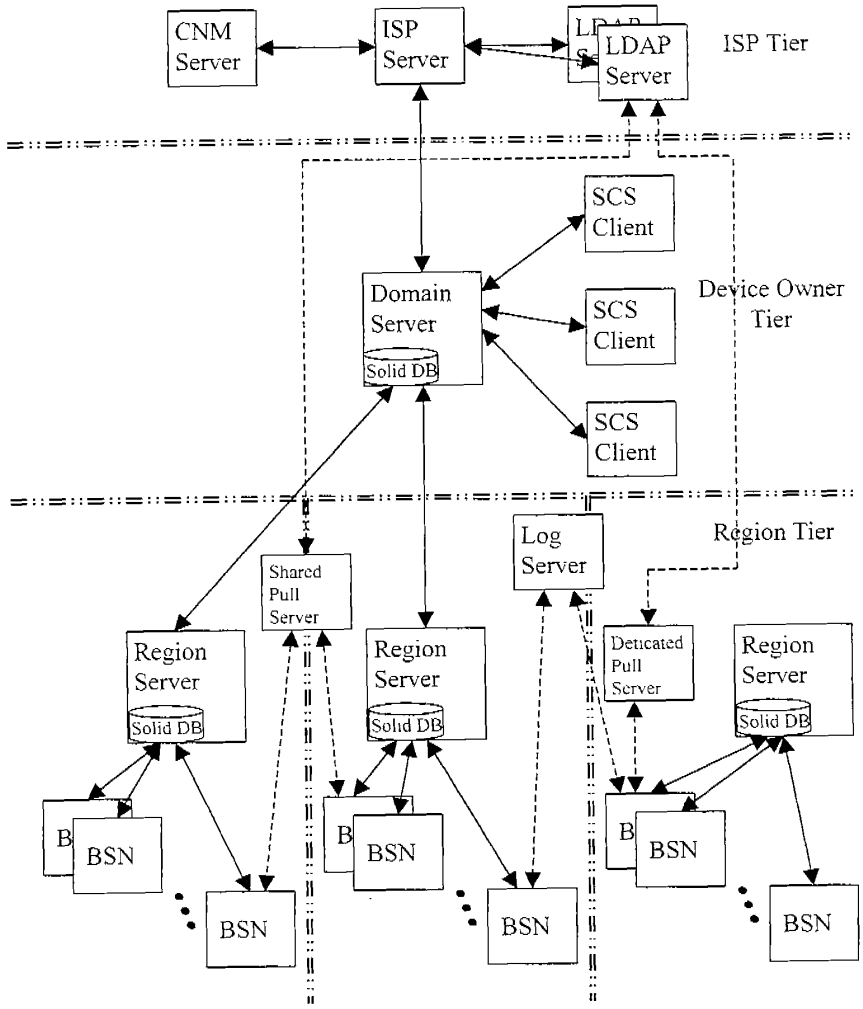


圖3.7　SCS軟體階層架構圖

- 地區層

地區層需向裝置擁有者層報告，此層可包含一或多個地區伺服器、pull伺服器及log伺服器。Shasta BSN直接向該地區伺服器報告，地區伺服器維持裝置特定資訊。

- Pull伺服器

Pull伺服器允許在PPP用戶login時，BSN查詢動態PPP用戶資訊，最多可有3個pull伺服器對1個BSN作組態，但只有1個pull伺服器會在任一給予的時間送出pull請求。

- Log伺服器

此伺服器收集所有裝置log並加以儲存，同時也收集用戶log(例如：統計及帳務log)且儲存為二位元檔案，最多可有3個log伺服器可被1個BSN定義並傳送log。

配置軟體於伺服器的一般規則如下：

- 配置所有層於1個伺服器。
- 在地區層的每一地區須有自己的伺服器。
- 地區伺服器可分享Pull及Log伺服器。
- 在裝置SCS軟體前，必須先在伺服器內安裝LDAP目錄。
- SCS客戶端在裝置擁有者層連接domain伺服器。

(2) IP 服務作業系統(iSOS)

iSOS軟體有三個主要部份用來運轉Shasta 5000，分別是：

- iSOS image – 作為個別電路板使用的作業系統。
- Configutions – 包含BSN使用的資訊，例如：ISPs、用戶及連接等。
- Data files – 包括logs及帳務。

有三個位置可以儲存軟體，分別是：

- Disk儲存 – BSN組態檔、logs及帳務等預設儲存位置。

- Flash儲存 – Image軟體預設儲存位置，依據啟動順序設定的不同，儲存於Flash將不同，如果系統是設定由tftp伺服器啟動，則CMC之images將仍在CMC，但其他卡片的images將下載至Flash。
- 備份儲存 – 選用的PCMCIA卡。

經由iSOS軟體與Shasta 5000互動必須經由iSOS指令稱為指令行介面(CLI)，CLI主要用於系統setup、診斷、組態證實及、檢視，要取得CLI指令的用法，可以：

- 查詢CLI User Guide。
- 下指令時鍵入"？"，系統會將可用的指令或參數由螢幕顯示出來。

註：絕不要在CLI建立或編輯組態檔案，因SCS伺服器在sync程序時會覆蓋他們。

(3) 客戶網路管理(CNM)

CNM是對ISP的用戶創造web-based網路管理應用的框架，利用CNM，用戶可以看到他們網路接取的組態、服務、logs及其他資訊。

3.3 服務應用

Shasta 5000主要是作為寬頻接取網路設備進入網際網路的遠端接取伺服器，並可提供多樣化的網路應用及用戶服務。

3.3.1 網路應用

Shasta 5000寬頻服務節點能夠在網路上提供許多的機能，說明以下：

(1) 用戶集合(Subscriber Aggregation)

作為用戶集合，Shasta 5000寬頻服務節點利用各種不同的技術接取輸入訊務，然後前送到ISP骨幹網路。如圖3.8所示。

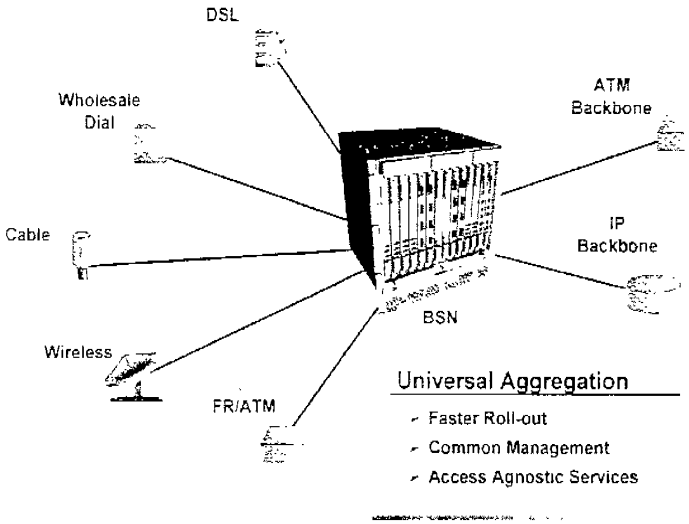


圖 3.8 用戶集合

§ 數位用戶迴路集合是從DSLAM(Digital Subscriber Loop Access Multiplexer)組合訊務並提供加值服務。即於現有的電話服務，由服務供應商提供基本的數位用戶迴路服務，利用ATM或快速乙太網路(Fast Ethernet, FE)上傳到ISP的核心網路。在Shasta 5000寬頻服務節點和用戶間的接取方式有如圖3.9所示，符合 RFC 1483B，具固定的且合法的IP位址，適用於固定制費率的用戶；如圖3.10所示，符合 RFC 1483B，必須由DHCP取得動態的IP位址，適用於計時制費率的用戶；如圖3.11所示，符合 RFC 1483R，針對企業用戶的需要，利用子網路設定固定的且合法的IP位址，其費率有如專線方式；如圖3.12所示，符合PPPoA，針對企業用戶擁有許多使用者的需要，從RADIUS取得一IP位址，並執行NAT，轉譯成企業內部網路IP位址到每一使用者，其費率有如撥接式的計時制方

式；如圖3.13所示，針對住宅用戶上網用，PC從RADIUS取得一IP位址，並透過PPP執行認證及計費，其費率採計時制方式；如圖3.14所示，針對VPN用戶上網用，PC向Shasta作認證後，建立L2TP隧道路由到公司，然後再做認證及計費，並由公司付費。

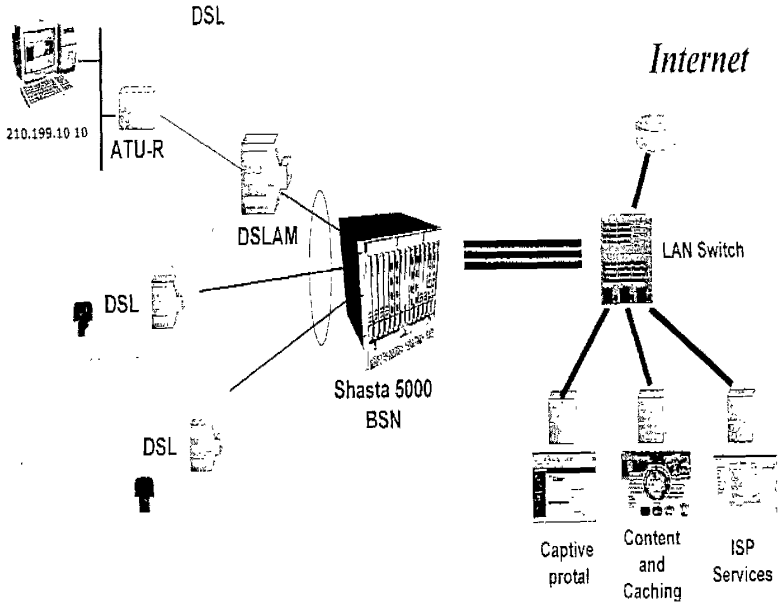


圖 3.9　RFC 1483B 固定的 IP 接取

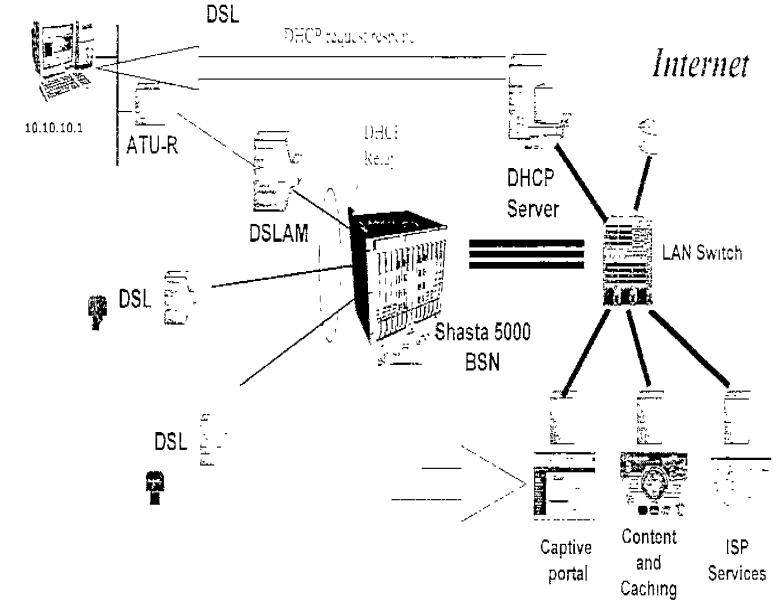


圖 3.10　RFC 1483B 動態的 IP 接取

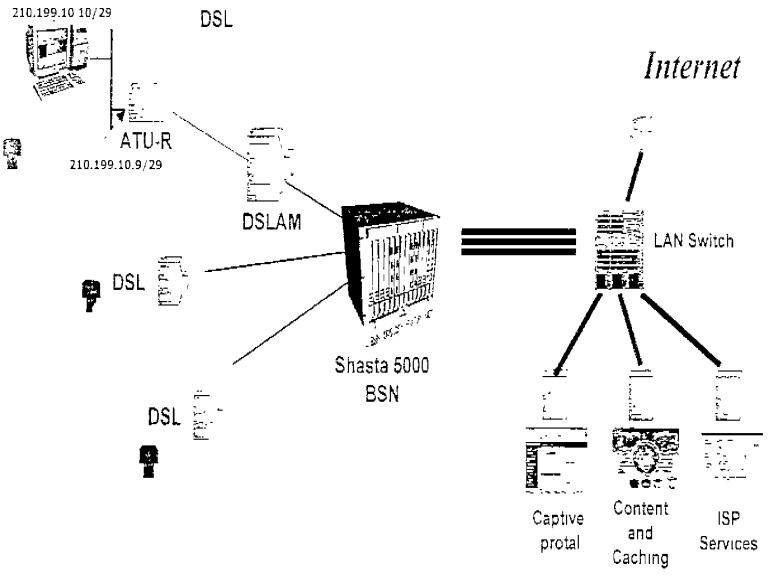


圖 3.11　RFC 1483R 接取

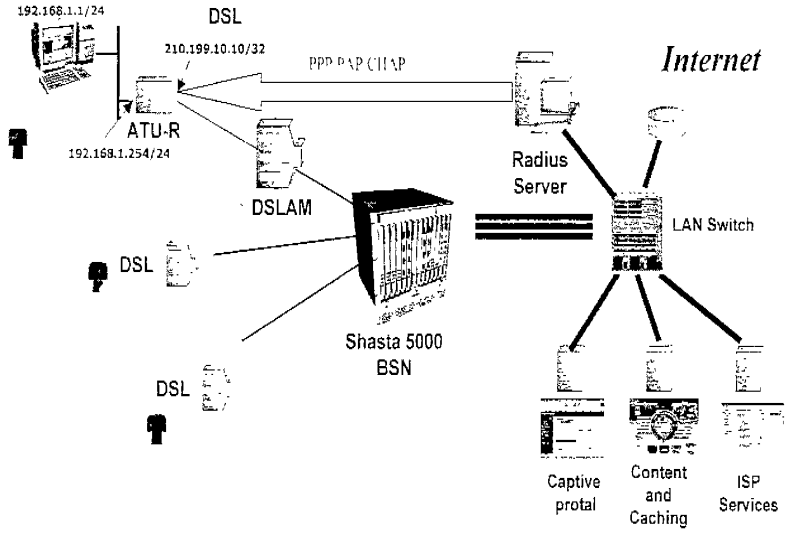


圖 3.12　PPPoA 接取

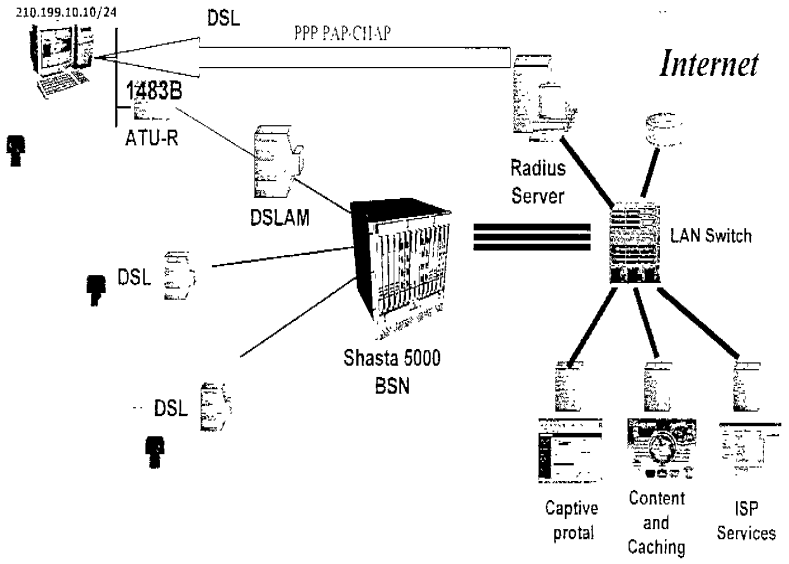


圖 3.13　住宅用戶接取

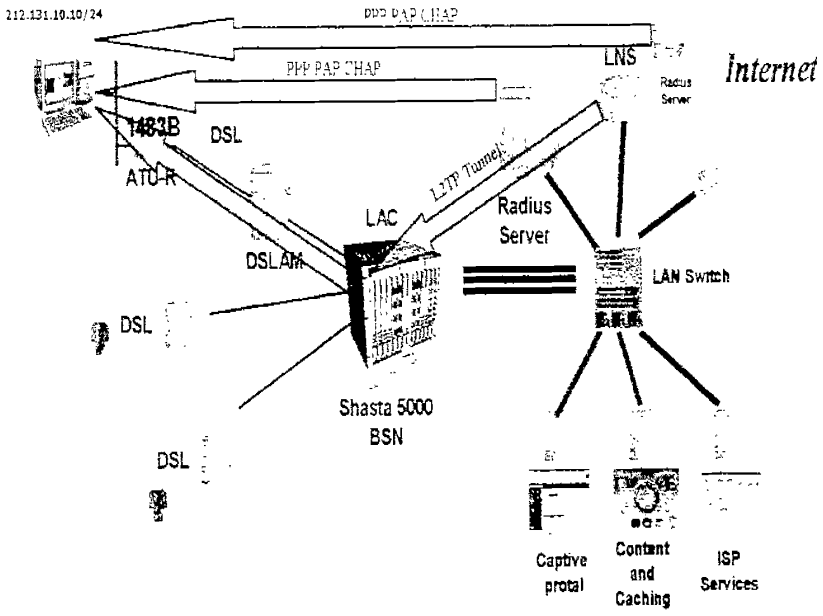


圖 3.14 VPN 用戶接取

§ Nortel 1M數據機，由 DMS交換機或UE9000提供。

§ 有線電視業者從纜線數據機(Cable Modem)頭端利用FE的上鏈直接連接到寬頻服務節點，供裝及計費可以是個別的IP位址或IP群，計費可以是計時制或以服務內容計價，如圖3.15所示。

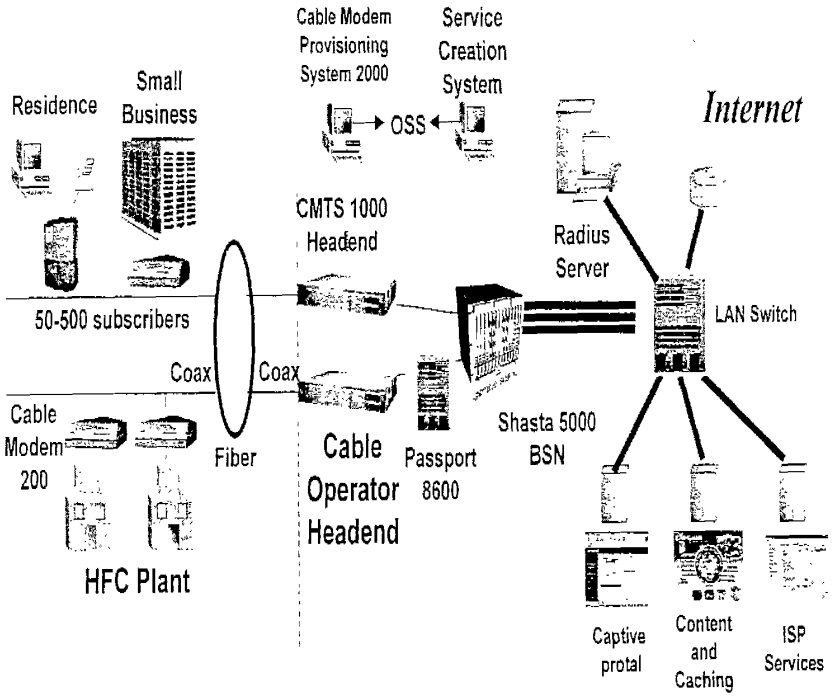


圖 3.15 有線電視接取

§ 撥接式用戶，包括類比式及ISDN的用戶，撥接到遠端接取伺服器(Remote Access Sever, RAS)如CVX-1800，再透過RADIUS(Remote Authentication Dial-In User Service)資料庫的辨識和認證服務，如圖3.16所示。

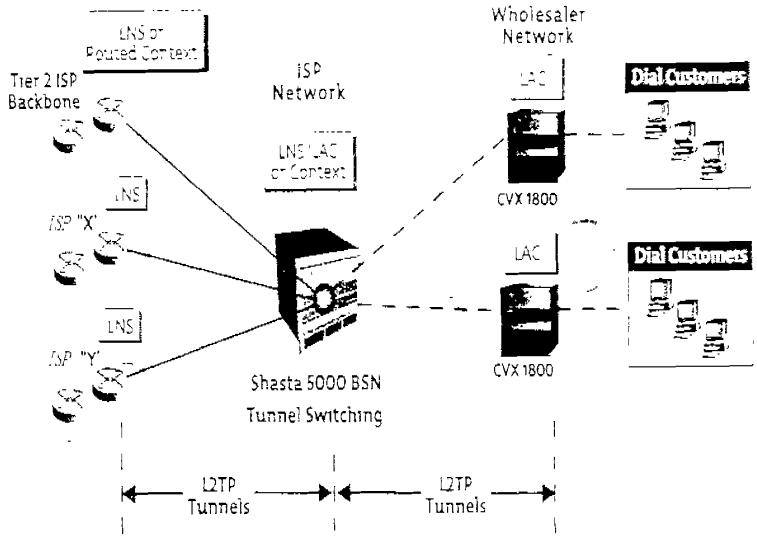


圖 3.16　撥接式用戶

§　無線用戶，連接到北電網路提供的CDMA的分封數據服務節點(Packet Data Service Node, PDSN)或GSM GPRS/EDGE 閘道節點(Gateway GPRS Support Node , GGSN)，提供高速的數據服務，如圖3.17，3.18所示。

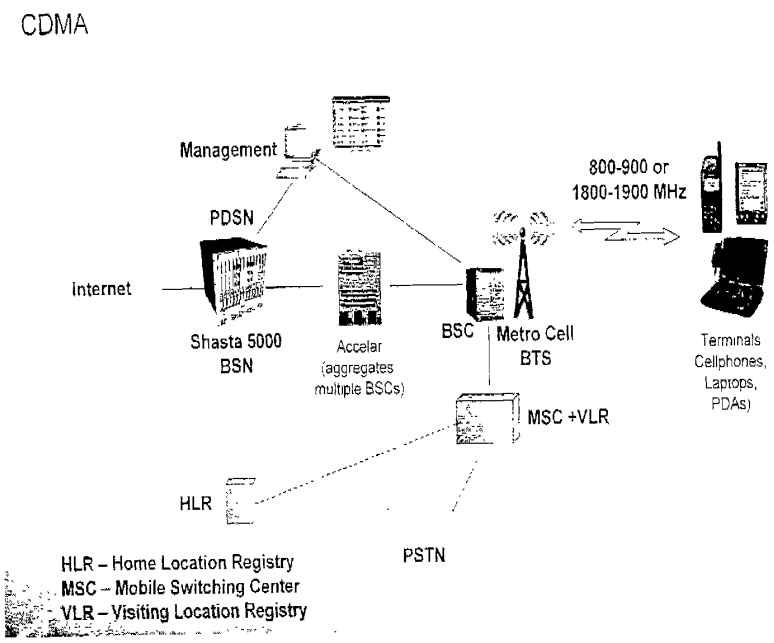


圖 3.17 CDMA 分封數據服務節點

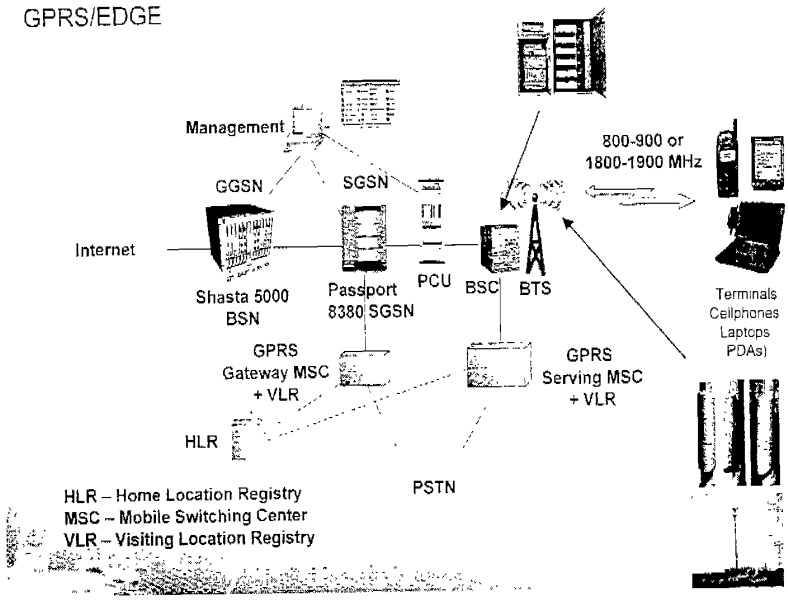


圖 3.18 GPRS/EDGE 閘道節點

(2) ISP 批發(ISP Wholesaling)

Shasta 5000寬頻服務節點能夠由個別的ISP或電信業者所擁有，且可分割成許多的虛擬路由器給個別的ISP，因此個別的ISP可建構自己的用戶資料及用戶服務，提供各種不同的接取批發模式，如圖3.19所示，並能夠控制寬頻服務節點的虛擬部份，目前Shasta 5000寬頻服務節點可支援64個ISPs。

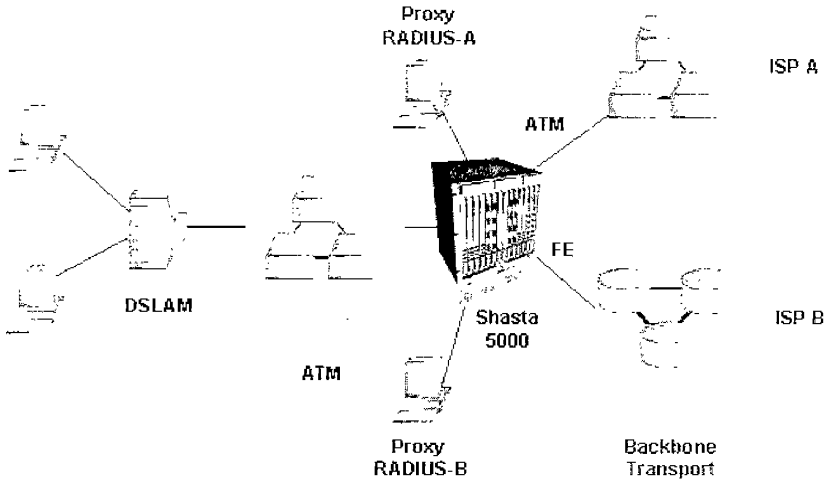


圖 3.19　ISP 批發

(3) ATM 服務節點(ATM Service Node)

伴隨著集合的用戶，Shasta 5000寬頻服務節點能夠配置成一ATM服務節點，除了提供寬頻服務，更增添許多加值服務，而提供給予用戶的加值服務，是以PVC(Permanent Virtual Circuit)或SVC(Switched Virtual Circuit)達成，如圖3.20所示。

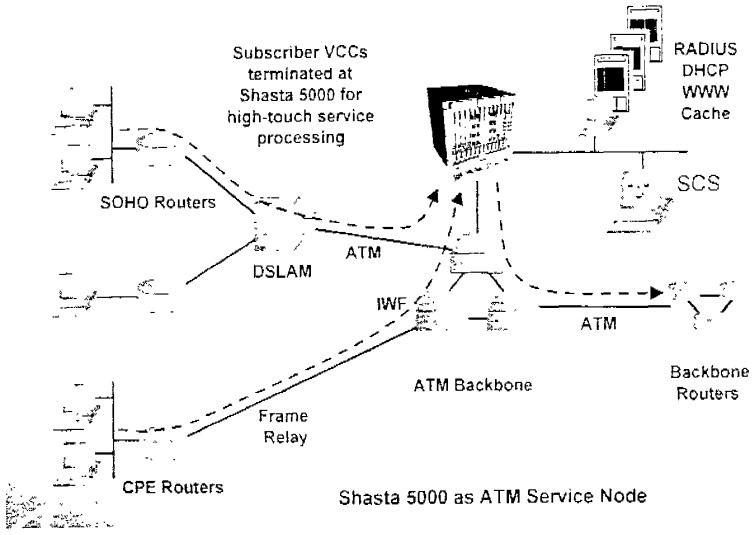


圖 3.20　ATM 服務節點

(4) 虛擬專用網路(VPN)

利用Shasta 5000寬頻網路節點建立可達到企業內部網路(Intranet)、虛擬專用路由網路(Virtual Private Routed Networks，VPRN)、虛擬撥接網路(Virtual Private Dialed Network, VPDN)、及虛擬專線(Virtual Leased Lines, VLL)環境之VPN，其示意如圖3.21所示，虛擬專用網路是利用穿隧提功訊務的流通，Shasta 5000寬頻網路節點將可扮演LAC(L2TP Access Concentrator)及LNS(L2TP Network Server)角色，並提供封包的加密與壓縮。

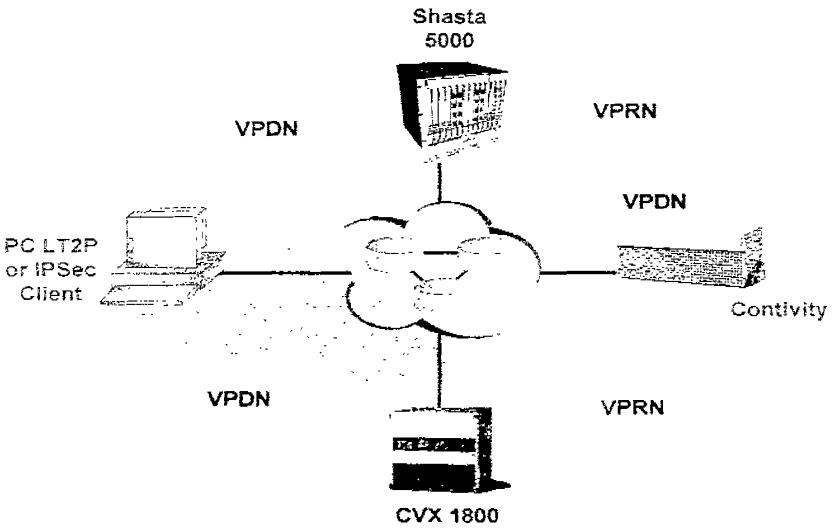


圖 3.21　虛擬專用網路

§ 虛擬的專用路由網路(Virtual Private Routed Networks，VPRN)：VPRN是一多服務地點的網路設計，可將服務擴展到供應商與用戶間或結盟企業間，Shasta 5000寬頻網路節點利用虛擬路由器所建立的路由表，解決私用及重疊的位址，並以IPSec作接續的安全機制，也提供用戶防火牆及網路位址轉譯功能，如圖3.22所示。

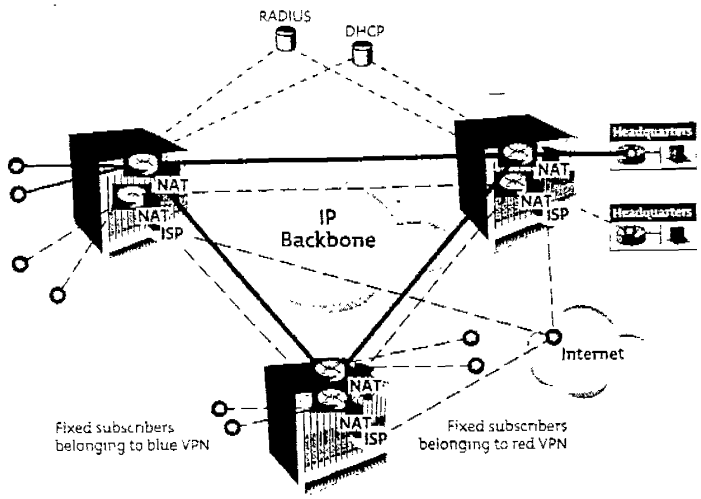


圖 3.22 虛擬專用路由網路

§ 虛擬專用撥接網路(Virtual Private Dialed Networks，VPDN)：使外勤之業務人員或通信量不多、連線時間不長之辦事處及在家上班族，可在遠端存取企業網路內部資源，連接至其企業網路，不論利用撥接、ISDN、數位用戶迴路或無線接取。Shasta 5000寬頻網路節點提供L2TP、LAC、LNS及IPSec功能，並結合北電網路其他產品提供更富彈性的服務，如圖3.23所示。

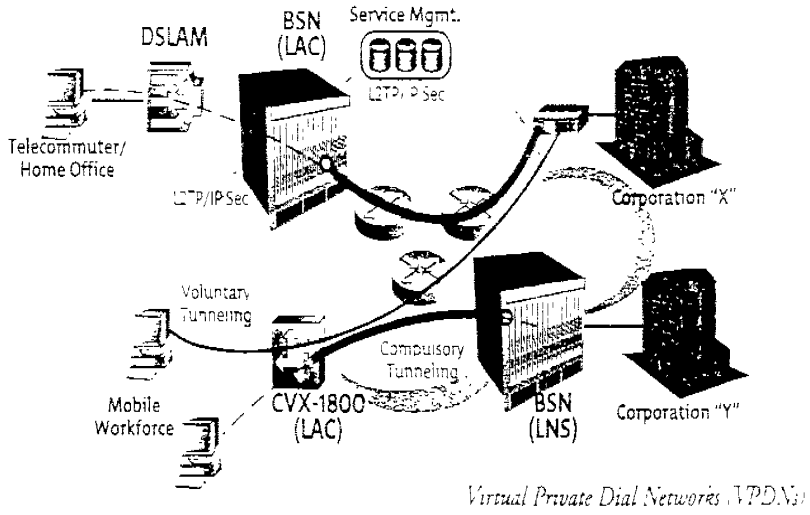


圖 3.23　虛擬撥接網路

§ 虛擬專線(Virtual Leased Lines VLL)：透過IP骨幹網路的IP穿隧連接兩個地點，雖然也仰賴IPSec，但其接續成本顯然比專線方式經濟，Shasta 5000寬頻網路節點目前提供具有DES/3DES加密的IPSec穿隧接續，如圖3.24所示。

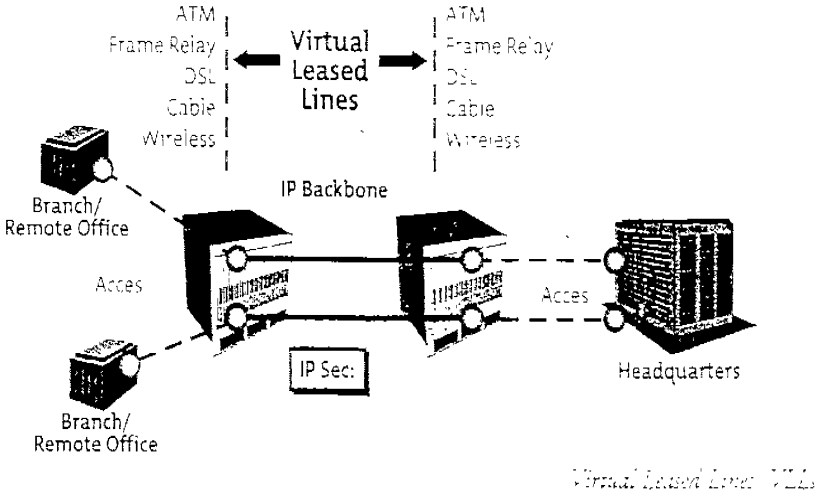


圖 3.24 虛擬專線

(5) 電子商務(E-Commerce)

透過Shasta 5000寬頻網路節點所提供的防火牆、加密及QoS機能，讓企業、經銷商、代理商間，經由完整的安全保密措施，使得電子商務活動，可以萬無一失，如圖3.25所示。

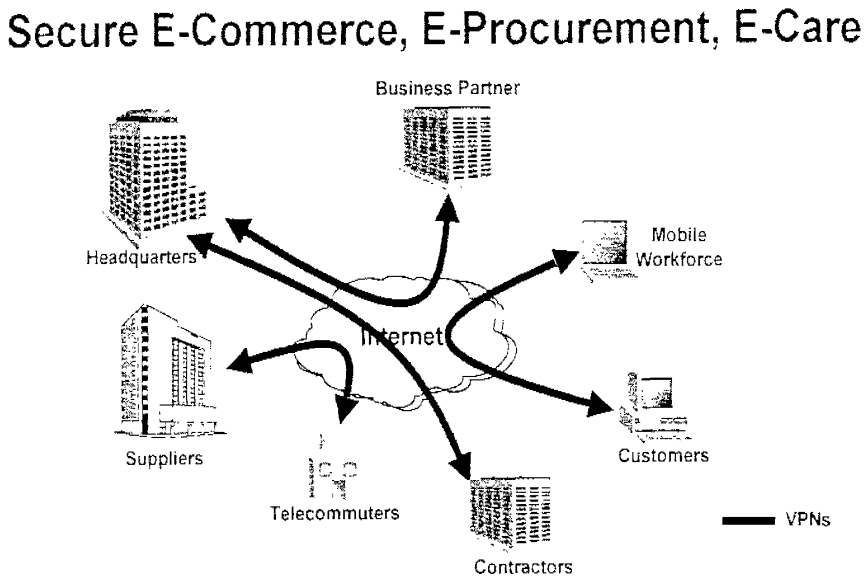


圖 3.25 電子商務

(6) 網際網路電話(Voice over IP, VoIP)

網際網路電話是不可錯失的商機，透過Shasta 5000寬頻網路節點所提供的安全機制及QoS機能，配合相關閘道的建立，讓用戶充分利用頻寬，提供經濟的網路電話，如圖3.26所示。

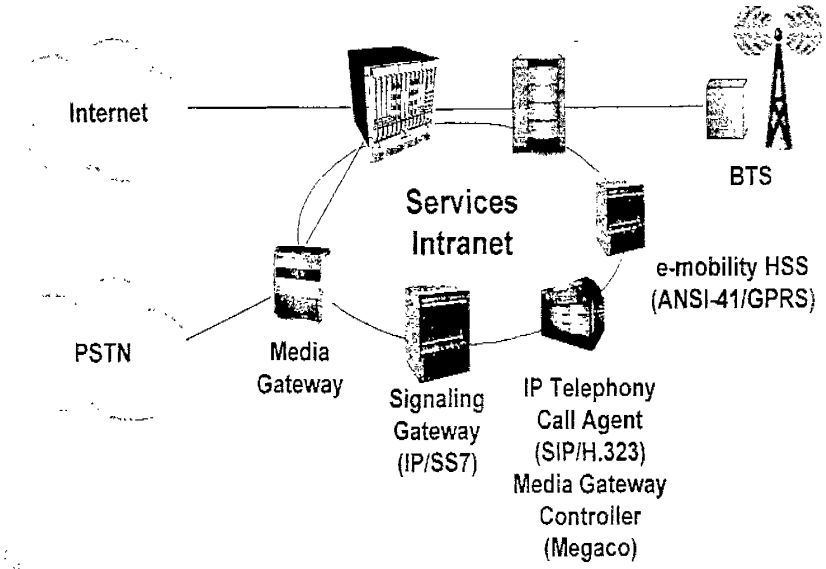


圖3.26　網際網路電話

(7) User Classes

Shasta 5000的使用者有Device owner及ISP owner，分別負責不同的功能接取設定：

• Device owner

Device owner負責Shasta 5000的實體組態設定及建構虛擬路由器--又稱為ISPs，其設定範圍如下：

- 在BSN建構Regions
- 設定BSN組態
- 建構ISP並指配使用者
- 建構接取及中繼連線(connection)

• ISP owner

ISP owner負責增刪用戶及指配連線的接取特性，ISP

owner也對每一個用戶設定其個別加值服務，其設定範圍如下：

- 增加ISP使用者
- 指配接取介面
- 設定中繼介面
- 設定路由
- 設定接取特性
- 指配用戶加值服務

3.3.2 用戶服務

藉由ISP定義用戶服務內容且其適用於以個別用戶或一群用戶為基礎。有三個服務元件之定義我們需要了解：

- 服務物件(Service Object)是網路物件或被應用在服務政策(Service Policy)之內的服務。物件(Object)可以按照需求被創造且包含IP通訊協定、用戶位址(Subscriber Address)或群(Group)等。
- 服務政策(Service Policy)即是定義了一些可以應用到個別用戶服務，服務政策可按照每一用戶的需求基礎為顧客訂製，例如防火牆(Firewall)或防詐騙政策(Anti-Spoofing Policy)等。
- 服務描述(Service Profile) 即是可以提供給用戶使用之一群被綁在一起的服務政策。

Shasta 5000創造和建置提供服務用戶皆須透過此三個完整服務元件，IP服務作業系統(iSOS：IP Services Operating System)可以提供辨別用戶服務之智慧運送可達數千的用戶。SCS

(Subscriber Creation System)是一個卓越的圖形使用介面(GUI-based)政策管理系統，它允許服務提供者容易地創造、包裝和建置按照市場現況及顧客的需求基礎為訂定之用戶服務描述，以提供每一個別用戶服務政策，如圖3.27所示。

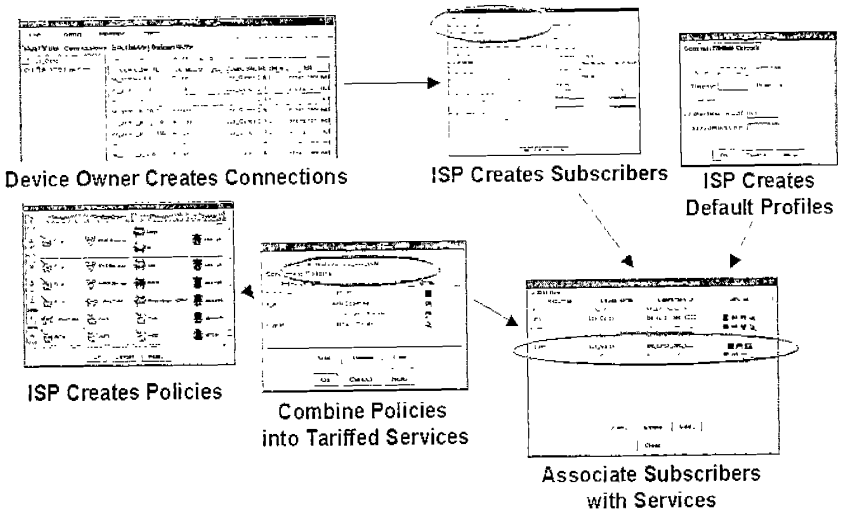


圖3.27　用戶供裝

服務被應用到用戶是在SSC(Subscriber Service Card)電路卡板中的SSM (Subscriber Service Module)執行，且其依據在SCS中所定用戶服務政策或服務描述定義，圖3.28為一些服務政策被應用之通訊量流程。

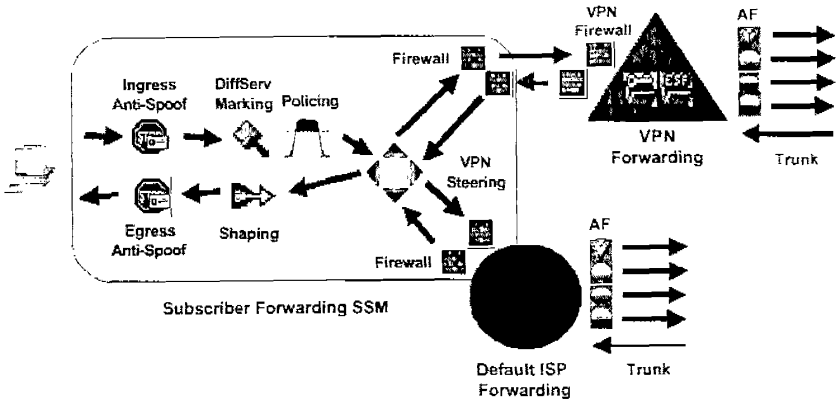


圖 3.28　用戶服務策略

Shasta 5000提供許多服務包括Security、DiffServ、Portal 、VPN...等服務，各種服務功能說明如下：

(1) 安全政策(防火牆)

安全性政策(Security Policy)即是放置於防火牆，主要是防止無用的或未授權的通訊量離開或者進入用戶的位置，可以執行封包過濾之規則和運用他們到不同用戶。它能夠使這管理者執行強大的封包過濾之規則，例如一個狀態式防火牆(stateful firewall)，且可維持每一 session 安全性狀態。譬如當系統識別到一個已知 VoIP session 開始，且在這對談的期間適用一套安全規則。Shasta 5000 允許以每一個用戶為基礎之下進而實現複雜的 stateful 防火牆。其示意如圖 3.29，而其設定如圖 3.30 所示。

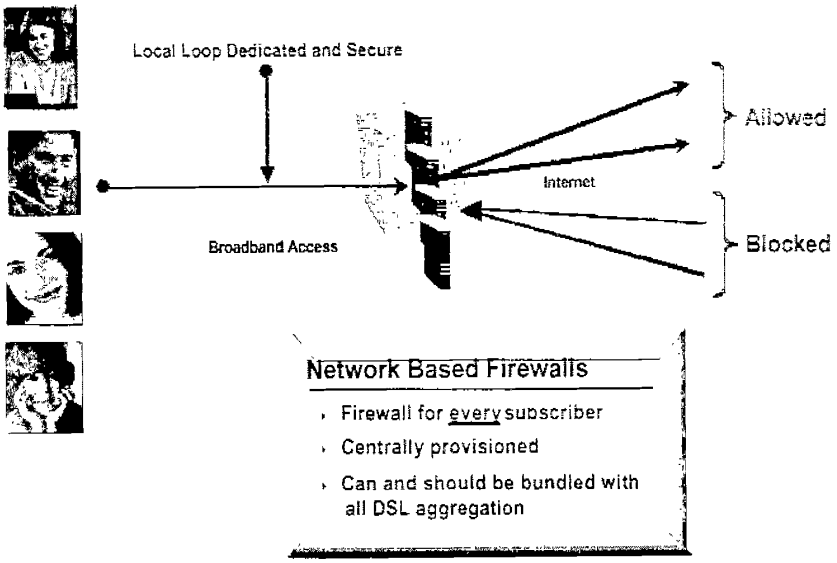


圖 3.29　防火牆

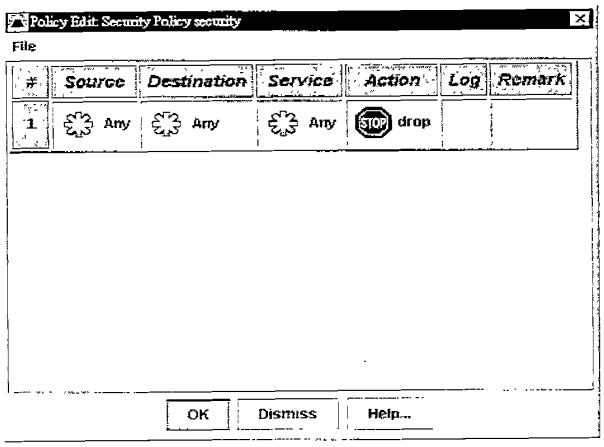


圖3.30　安全政策

(2) 分類服務(Diffserv)

分類服務允許提供用戶及有關帳單方面多變化層次的服務，譬如用戶可以有一個需求為語音(Voice)和資料(Data)通訊量，建置以一個較高優先序提供語音通訊量，允許保

證和管理一較高層次的服務。

分類服務每一hop保證向前進(AF：Assured Forwarding)之行為是依據IETF所定差異性服務(Differentiated Service)的結構。當服務形態(Type of Service，TOS)位元組被設定時，在網路核心之路由器將利用此位元組決定資料被排序等候或拋棄，通訊流量透過不同途徑傳送。

分類服務標示定義保證向前進AF等級從1到4，丟棄優先等級DP從1到3。

- AF為敘述通訊量傳送之相關的優先順序，利用AF等級有能力對應至ATM網路以達到ATM網路適當之服務品質QOS(Quality of Service)要求。
- DP為定義假如當網路發生擁擠時或用戶通訊量超過通訊量合約(Traffic Contract)時，如何適當的拋棄通訊量。

分類服務標示政策(DiffServ Marking Policy)應用到從Shasta 5000離開至網路的通訊量，Egress DiffServ標示政策(Egress DiffServ Marking Policy)應用到從Shasta 5000至用戶的通訊量。其設定如圖3.31所示。

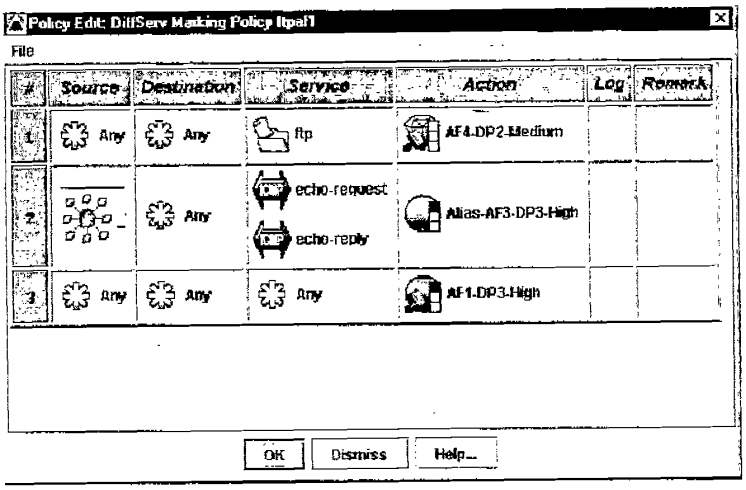


圖3.31　分類服務策略

(3) 話務控制(Traffic Shaping)

話務控制加值服務是被應用在用戶網路之方向，當較低優先序的應用正在傳送時，如電子郵件或FTP等應用，話務控制允許對特定任務之應用提供較高優先序和速率保證的傳送，例如ERP應用等。

話務控制政策利用Rate Weight、Rate Limit及Per Connection Rate Limit三項參數達成通訊量重整功能，且這些參數只有在當傳送鏈路發生擁擠時才有作用。

- Rate Weight決定在傳送鏈路發生擁擠時期所設定之通訊量類型(Traffic Type)能夠傳送佔用現成可用頻寬之百分比例。
- Rate Limit為在傳送鏈路發生擁擠時期所設定之通訊量類型之最大可用傳送頻寬。
- Per Connection Rate Limit是在傳送鏈路發生擁擠時期屬於所設定之通訊量類型每一連接(Connection)

最大可用傳送頻寬。

此通訊量重整功能識別IP訊務，且可以針對每一用戶為基礎在傳送鏈路發生擁擠時期，將其重整到一絕對頻寬(Absolute Bandwidth)和/或相對百分比頻寬。其設定如圖3.32所示。

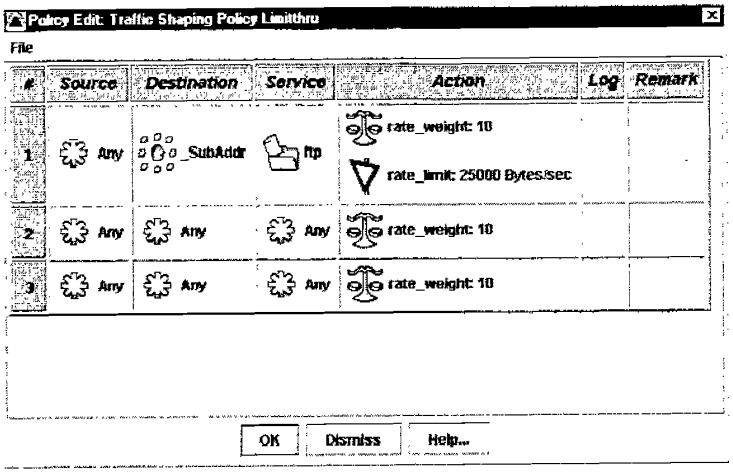


圖3.32　話務控制政策

(4) 訊務管理(Traffic Policing)

訊務管理允許定義一個用戶能夠送出之資料量來源的類型及其有關通訊量的數量多少。當用戶送出之資料通訊量超出可傳送契約所定之速率時，其功能仍可保護網路核心正常運作。

訊務管理功能利用在DiffServ標示的結果配合頻寬限度(Bandwidth Limit)，進而設定不同資料拋棄優先順序。Committed Rate、Committed Burst Size、Excess Burst Size、Peak Rate和Peak Burst Size Threshold等各項參數

配合適當符合之指令動作而被設定。指令動作類別分別為紅色、黃色、綠色來區別其間之不同，主要之指令動作如下：

- 通訊量之拋棄。
- 將通訊量置於適當的佇列(Queue)排列等候傳送。
- 改變通訊量之標示IP優先等級傳送。

各類服務政策定義之AF等級其速率和指令動作，須配合此AF1~AF4之設定提供服務。訊務管理有單速率三色標示(Single Rate Three Color Marking ; SRTCM)及雙速率三色標示(Two Rate Three Color Marking ; TRTCM)兩種模式運作，三色標示與速率之關係如下：

SRTCM (Single Rate Three Color Marking)，其設定如圖3.33所示。

- 紅色狀態：傳輸路徑中之通訊量大於(Committed Burst Size+Excess Burst Size)
- 黃色狀態：傳輸路徑中之通訊量大於Committed Burst Size，但是傳輸路徑中之通訊量小於(Committed Burst Size+Excess Burst Size)
- 綠色狀態：傳輸路徑中之通訊量小於Committed Burst Size

TRTCM (Two Rate Three Color Marking)，其設定如圖3.34所示。

- 紅色狀態：傳輸路徑中之通訊量大於Peak Burst Size

- 黃色狀態：傳輸路徑中之通訊量大於Committed Burst Size，但是傳輸路徑中之通訊量小於Peak Burst Size
- 綠色狀態：傳輸路徑中之通訊量小於Committed Burst Size

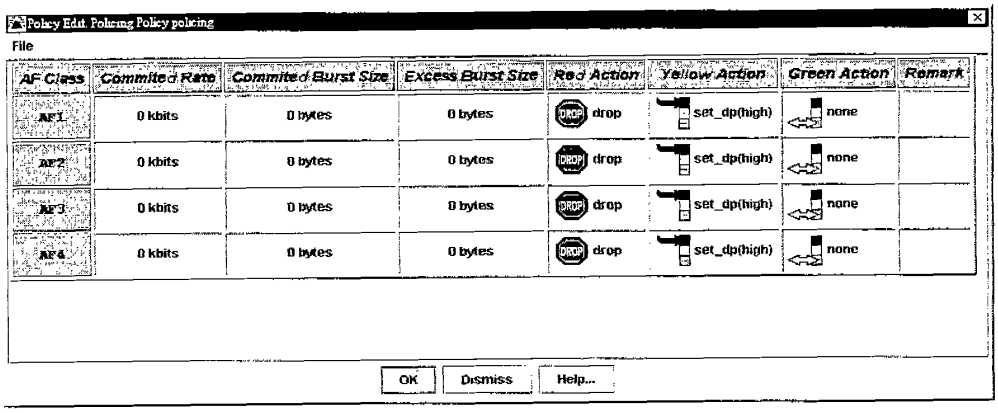


圖3.33　SRTCM 話務策略

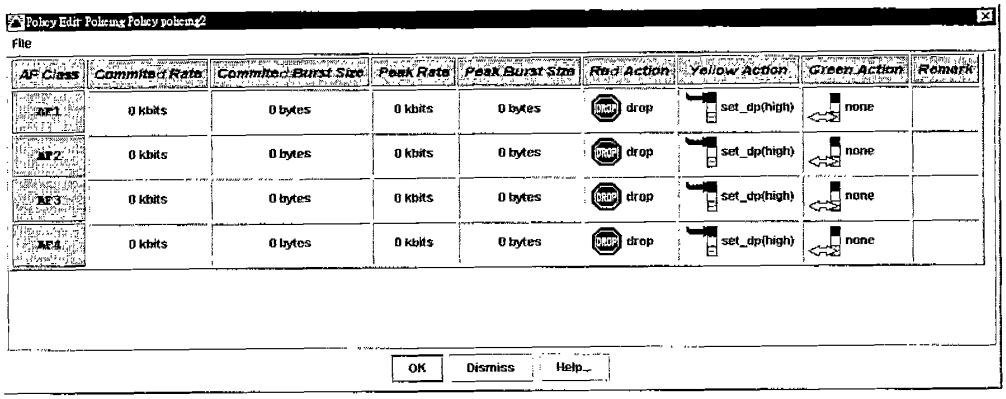


圖 3.34　TRTCM 話務策略

(5) 防詐騙(Anti-spoofing)

防詐騙確保可以保護防止從經由網際網路來冒充存取的第三者惡意用戶之攻擊，透過在用戶端鏈路過濾適當正確所期待的發送者位址內容之方式執行提供防詐騙功能。有兩種類型之防詐騙可以被建置，為Anti-spoofing及Ingrss anti-spoofing。

防詐騙政策(Anti-spoofing Policy)被用於保証收到從外部(網際網路)來之封包的發送者位址內容，不可以與用戶介面端本身所學習得知位址組群符合。若外來封包的發送者位址內容與用戶介面端之位址組群相符合，表示有第三者惡意用戶攻擊現象發生，則該封包將被拋棄之以防止影響用戶被攻擊。其設定如圖3.35所示。

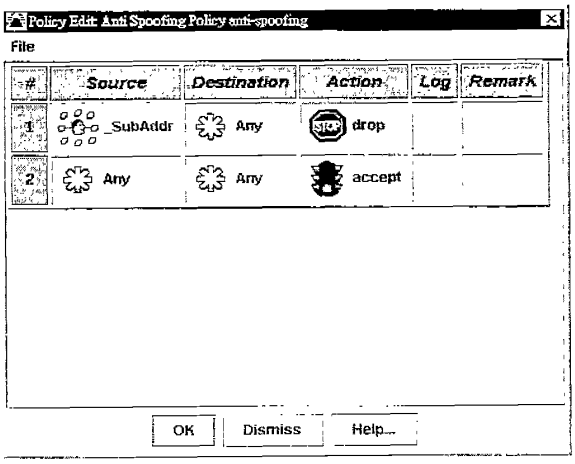


圖 3.35 防詐騙策略

入口防詐騙政策(Ingress Anti-spoofing Policy)被用於保証從用戶介面端收到之封包的發送者位址內容，必須與

用戶介面端本身所學習得知位址組群符合。若封包的發送者位址內容與用戶介面端之位址組群相不相符合，表示有第三者惡意用戶攻擊現象發生，則該封包將被拋棄之以防止影響用戶。其設定如圖3.36所示。

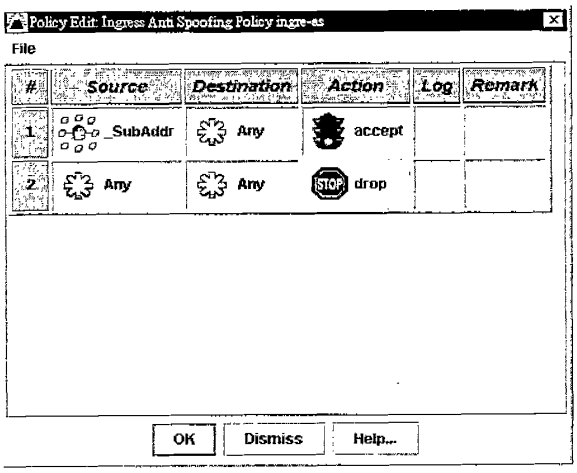


圖3.36　入口防詐騙策略

(6) 網路位址翻譯(Network Address Translation, NAT)

網路位址翻譯主要作用為允許公司使用私人專用位址空間，在他們內部的網路之內，諸如：10.x.x.x。且只使用公眾位址空間，在於與網際網路通信時使用。在工業上網路位址翻譯最初被認為是公眾位址空間的消耗問題，一個類似Ipv6將幫助減輕這問題之有潛力的解答方法。雖然網路位址翻譯可以讓公眾位址空間的使用減到最小，但是同時它產生很多問題。很多應用皆靠相同的IP位址被使用越過網路，假如IP位址被改變將導致這些應用無法正常運作將失敗。有兩類型最典型的網路位址轉換模式-靜態方式與動態方式。

- 靜態方式：私人專用位址到公眾位址空的對映是預先定義好或先建置好(Pre-configured)。其設定如圖

3.37所示。

- 動態方式：私人專用位址到公眾位址空的對映是自動的。

其他尚有PAT (Port Address Translation)或NAPT (Network Address Port Translation)等網路位址轉換方式，這些被使用以一對一的翻譯(One-to-one Translation)，NAT運作在資料所到達的輸出入埠，且產生一以輸出入埠為基礎的私人專用位址到公眾位址內部對映表。其設定如圖3.38所示。

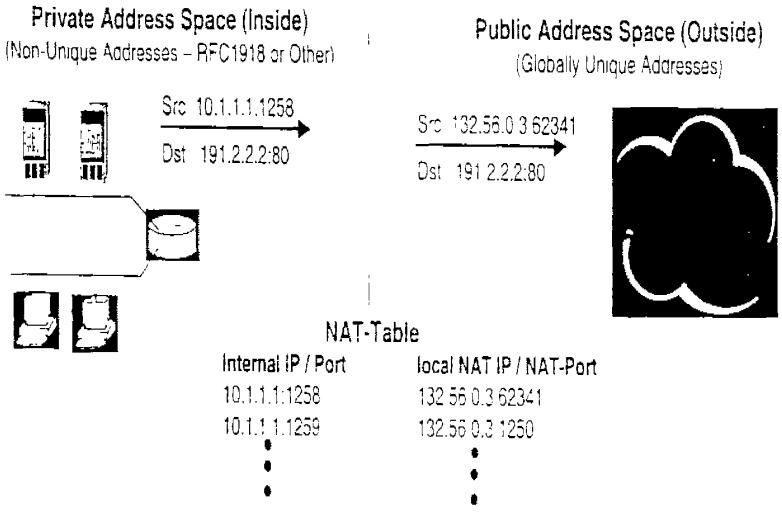


圖3.37 靜態的網路位址翻譯

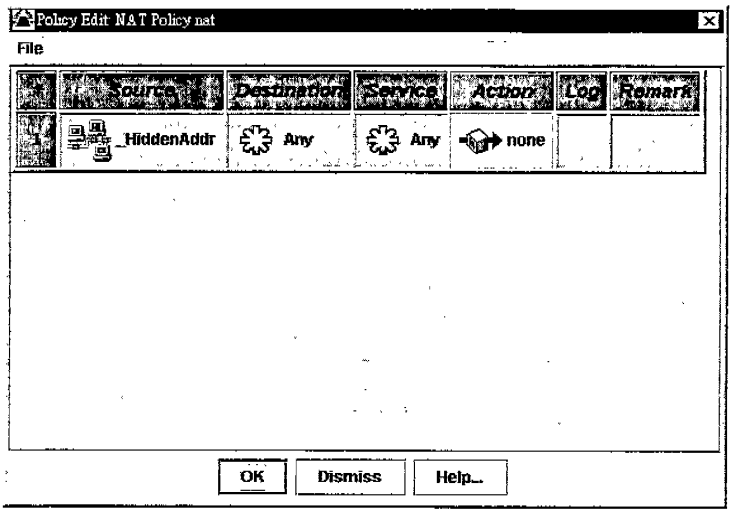


圖3.38　網路位址翻譯策略

(7) 計費(Accounting)

計費將追蹤用戶所發送和收到封包為多少，假如你的用戶有使用DiffServ之服務應用時且通過的通訊量已被標示完成，ISP能夠依據其服務位準辨別出那些通訊量和計算出這些封包數量。計費將依據通訊量其適當的標示個別分開計算封包與儲存於Bucket 0到Bucket 4中計算數量，任何通訊量無法匹配符合計費政策之封包，將被儲存在Bucket 0中計算數量。

當用戶利用DiffServ政策服務標示其通過之通訊量時，可以依據DiffServ政策服務標示分開這些通訊量進入不同計費儲存區。

在Shasta內部假如用戶通過之通訊量沒有標示，它將保證向前進等級預先被設定為AF Class 1且丟棄優先等級預先被設定為DP Class 1。假如沒有一個計費政策被設定，其通過之通訊量將被儲存於Bucket 0中計算數量。其設定如圖3.39所示。

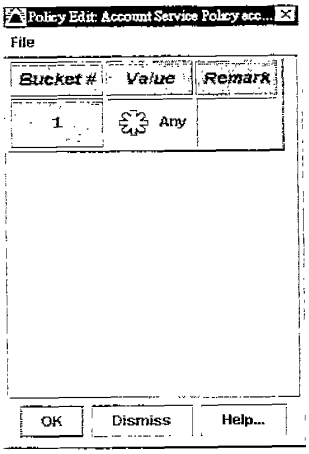


圖3.39 計費策略

(8) 強制入口服務(Captive Portal)

強制入口服務即將用戶的http請求從一個網頁位置轉移到事先建置好強制入口服務網頁位置。代替了用戶所期待看的網頁，用戶從這強制入口服務網頁位置將看事先安排好之特定網頁。然後經由強制入口服務網站下指令給Shasta 5000方式控制(從captive模式到non-captive模式之切換)，被攔截之網頁可再重新安排用戶至所期待看到的網頁。亦可配合由時間控制方式經過一段時間後，再強迫用戶轉移回到強制入口服務網頁位置將看事先安排好之特定網頁。其示意如圖3.40所示。

透過強制入口服務政策可使網路服務提供者對用戶端可以真正實際履行線內(in-line)入口網站之功能。其設定如圖3.41所示。

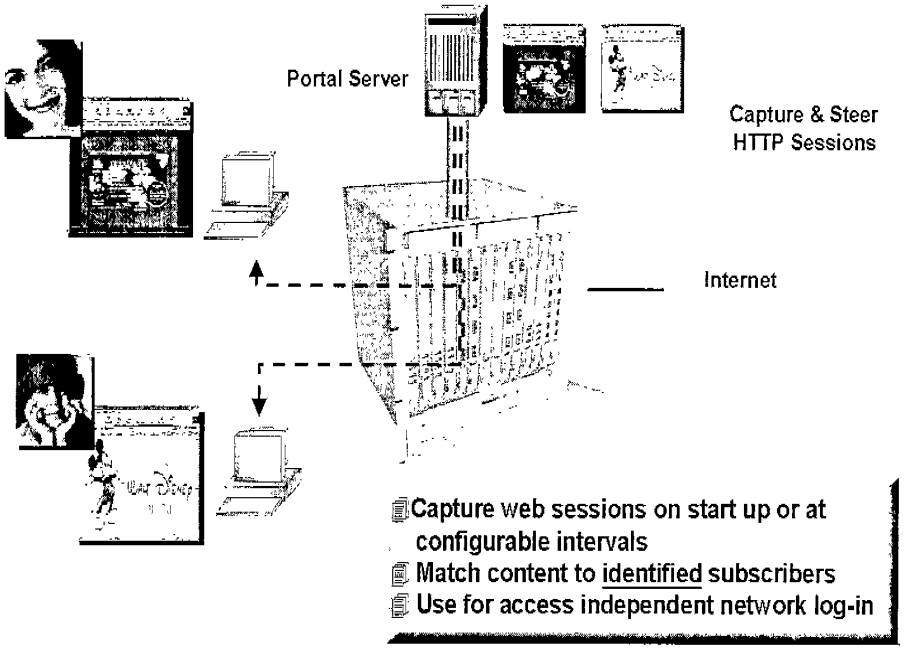


圖 3.40　強制入口服務

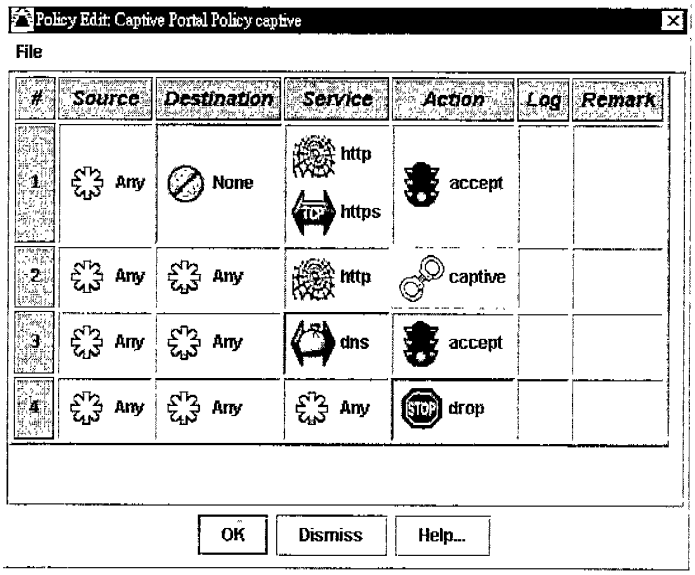


圖3.41　強制入口服務策略

(9) 網頁控制(Web Steering)

網頁控制允許服務提供者將用戶之http請求直接指到網快取記憶體(Web Cache)，將熱門流行之網頁儲存到這裡，所以可代替需要出網路上網際網路至該網頁時，減少所需資料往返和處理的網際網路遲延，如此用戶收到其請求之網頁直接從快取記憶體來。假如這網頁不在快取記憶體時，則將改由網際網路中取回。其示意如圖3.42所示。

網頁控制操控潛在能力包含NAT的支援，且當代理伺服器(Proxy Server)尚未共置(Co-located)於Shasta 5000內時，亦可提供增加安全(Security)保護機制。

網頁控制政策是以標準的rule-based格式方式訂定的，這些規則能加以指定哪些IP對談(經由指示特定的來源和目的地位址)會被進行網頁操控和哪些將不會。這些規則指至一特定"操縱"(steer)動作，同時必須指到一特定IP-farm之服務物件(Service Object)。

Shasta 5000同時也經由一些網頁操控服務，執行周期性測試IP-farm中全部成員是否正常工作。當有任何測試失敗時該IP位址從IP-farm中被移去，如此以致沒有新http請求將會再引導至測試失敗之IP位址處。IP-farm中剩餘成員將取代測試失敗的伺服器工作，當該proxy伺服器恢復正常時，且被重新安置(Reinstall)好則新http請求將再次引導至該伺服器加入服務，這種方式使其對短暫遠轉中斷有較佳之容忍度。其設定如圖3.43所示。

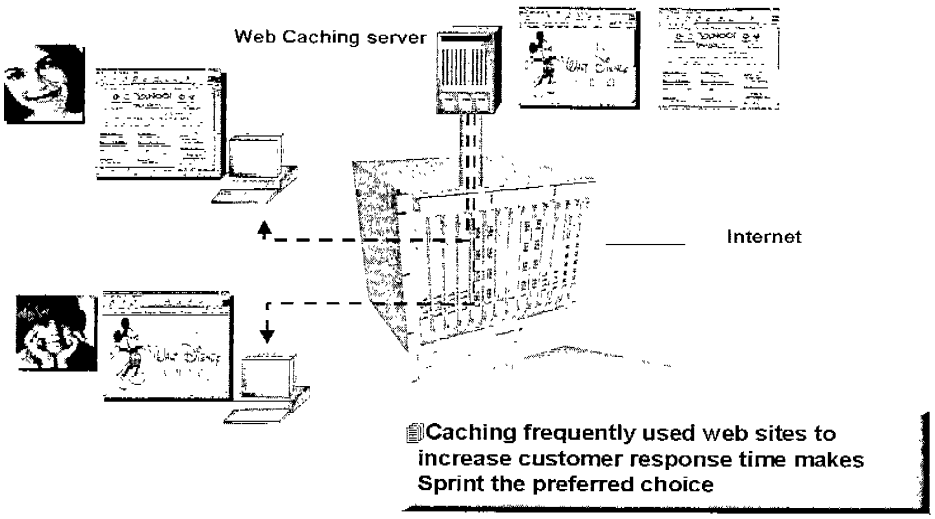


圖 3.42 網頁控制應用

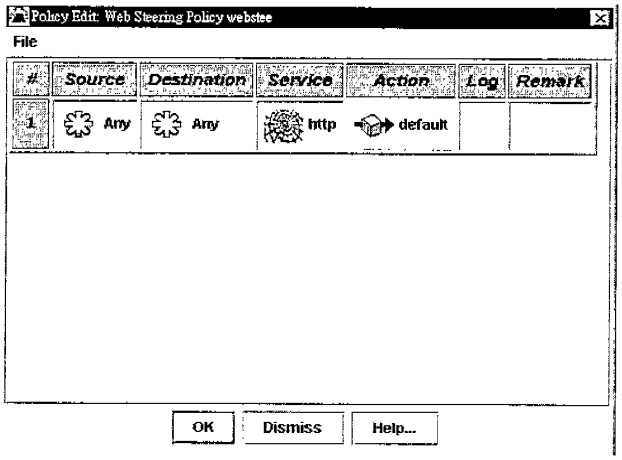


圖3.43 網頁控制策略

4. Shasta 5000 BB-RAS 之網路規劃設計

本公司BB-RAS主要是作為ADSL客戶進入網際網路的接取伺服器，也是寬頻網路提供加值服務的一個服務選擇Gateway，以下就BB-RAS在寬頻網路的規劃設計作簡要的描述。

4.1 初期 Shasta 5000 應用架構

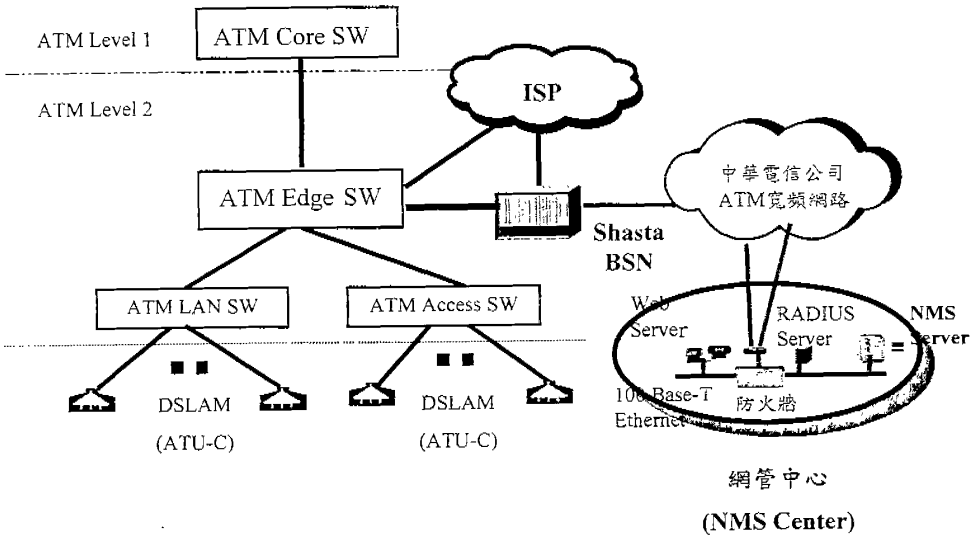


圖4.1　初期Shasta 5000應用架構

如圖4.1所示，Shasta 5000可用以選接ISP使用，初期引進時是為了ADSL計時制，避免ADSL用戶在更換ISP時，整條PVC必須重新設定的困擾，固接制ADSL仍由ATM SW.直接連線至ISP，由於HiNet已採購BB-RAS，且ISP均推出在同一地點無限時數上網之優惠措施，而ISP是靠VPI及VCI值識別用戶是否在同一地點上網，因此極力反對由區分公司提供BB-RAS，再連線至ISP之連接方式，但基於區分公司必須在Managed IP網路上作加值服務，也為了服務小ISP，因此，BB-RAS將結合新服務與上網之用途，提供另類之應用。

4.2 Shasta 5000 應用於 MCS 架構

多媒體通訊服務(MCS)應用架構是在原有架構上增設MCS相關設備包括網路介接設備、媒體伺服設備及服務管理系統等如圖4.2，並考慮ATM Access SW.直接與Shasta 5000連接，減少再經由Edge SW.連接，可減少ATM網路層級，增加供裝速度。

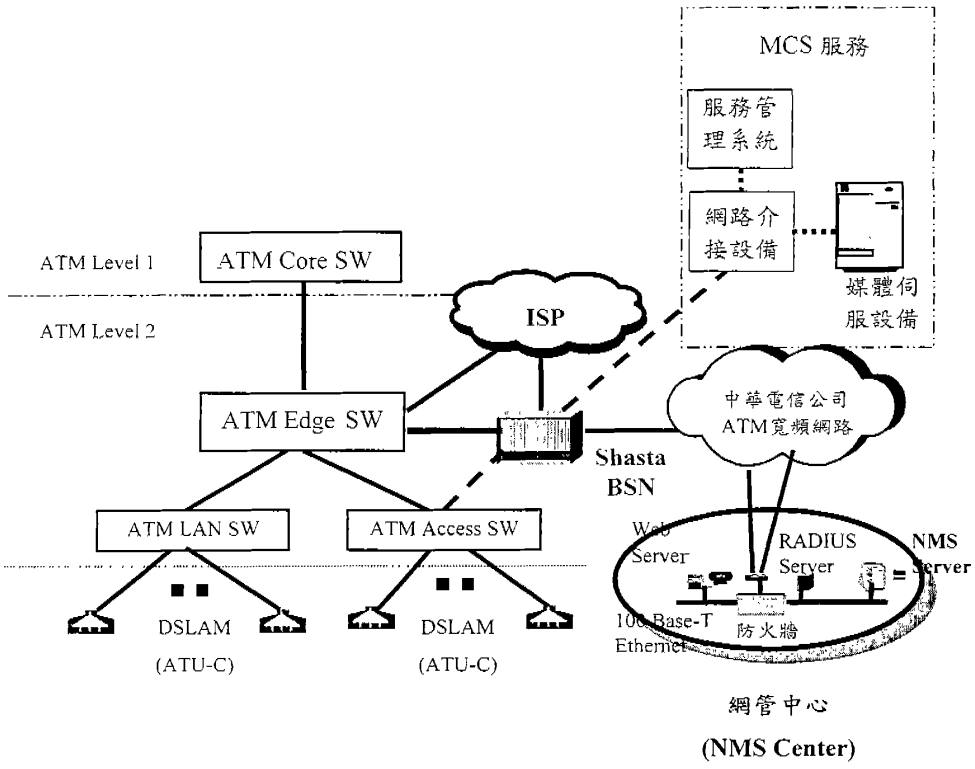


圖4.2　Shasta 5000應用於MCS架構

4.3 ATM – BB-RAS – ISP 及新服務最佳化網路架構

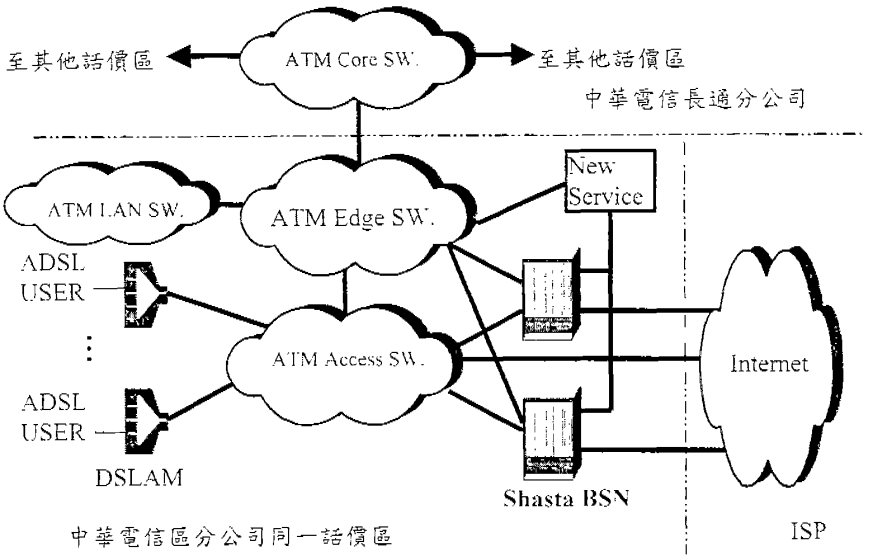


圖4.3 ATM – BB-RAS – ISP及新服務最佳化網路架構

ADSL在新業者競爭及降價優惠措施下，裝機量勢必大幅成長，隨著DSLAM可收容之ADSL數量增加，DSLAM 1條STM-1已可承載ADSL數1500路左右，與以往80～120路成長許多，因此ATM交換網路Edge及Access二層架構應有所改變，最佳之網路架構是由Access SW.收容DSLAM後直接與BB-RAS連線(GigaPop架構)，由BB-RAS來區分上網或接取新服務，某些固接式用戶可選擇由Access SW.直接連線至ISP，原收容於數據分公司BPX、LS1010或LAN SW.之DSLAM，則透過Edge SW.連線，網路架構如圖4.3。

目前Shasta 5000卡槽容量有限，無法由DSLAM直接連接Shasta BSN，倘若DSLAM可收容之ADSL數量再增加，且具備STM-4介面，而BB-RAS介面容量及處理能力也相對增加時，ATM Access SW.也可

直接由BB-RAS取代，以簡化網路層級，節省投資成本。

4.4 網管中心之架構設計

網管中心之架構如圖 4.4 所示。

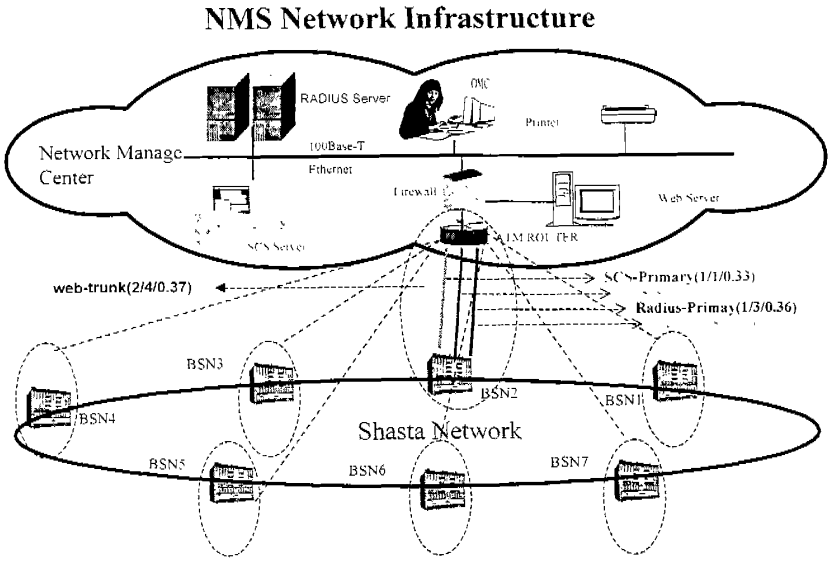
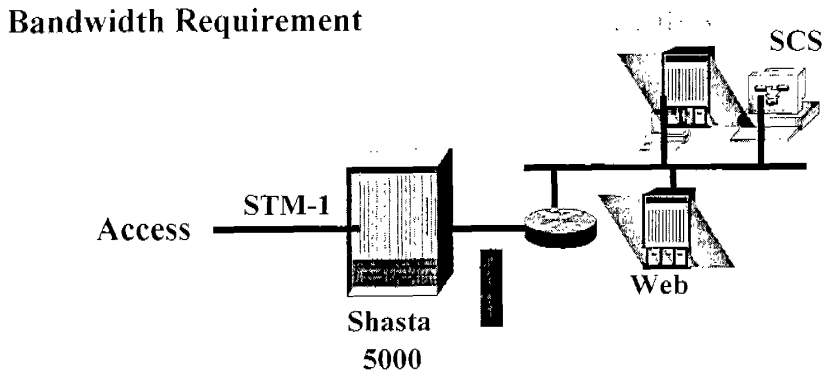


圖 4.4 網管中心之架構

4.5 Shasta 5000 至網管中心之訊務量估算



- 只針對 ADSL 服務所需之訊務量估算
- 於尖峰時段有**25%** 用戶上網
- 每一 STM-1 Access connection 服務 **2000** 用戶

4.5.1 SCS Server In-band 訊務量

假設於尖峰時段有**25%** 用戶欲登錄上網，每一筆用戶資料查詢約需**2.3Kbytes**

NO users per Shasta = *NO of user per STM-1 * Number of Access*

= 2000 * 1 = 2000

Active users per time = *NO users per Shasta * (% of active user/100)*

= 2000 * 0.25 = 500 users

NO of users log on at a time = *Active users per time * (% of user try to log on/100)*

= 500 * 0.25 = 125 users

Size required for in-band = NO of users log on at a time* Traffic of each query

= 125 * 2.3K

= 287.5Kbytes

Traffic flow in bits = Size required *for in-band * 8 bits*

= 287.5K * 8

= **2.3Mbit**

4.5.2 Web Server 訊務量

假設於尖峰時段有**50%** 用戶正在上網，Web Content = 30Kbytes (basic homepage without a lots of graphics used)

Active users per time = *NO users per Shasta * (% of active user/100)*

= 2000 * 0.25 = 500 users

NO user access Web Server/time = NO of users /Shasta * % users access Web Server

= 500 * 50%

= 250

Size for Web Server Access = NO user access Web Server/time * Web Content

= 250 * 30Kbyte

= **7500Kbyte** or **7.5Mbyte**

Traffic Flow in Bits = *Size for Web Server Access * 8 bits*

= 7.5M * 8 = **60Mbit**

4.5.3 RADIUS Server 訊務量

Radius 訊務量與SCS Server 訊務量應相當接近故假設為2.3M

4.5.4 Total 訊務量估算

Total Traffic Required = SCS Server + Radius Server + Web Access

= 2.3M +2.3M + 60M = 64.6M

Bandwidth (Kbit/s)	**Duration (Second)**
3230	20
4306	15
6460	10
12920	5
64600	1

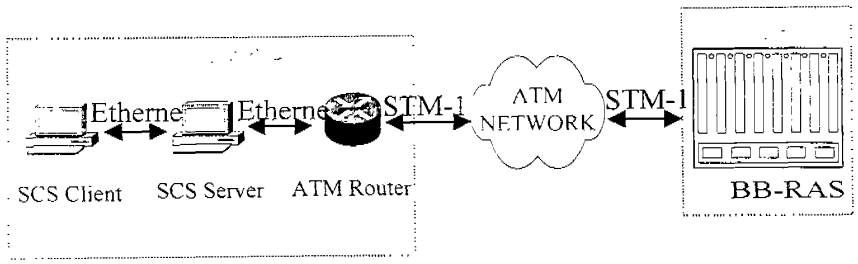
5. Shasta 5000 BB-RAS 之 O&M

5.1 IN BAND 管理與 OUT OF BAND 管理方式

每部 Shasta 5000 與他的網管中心連接可以有下列兩種不同的方式－In-Band 與 Out Of Band：

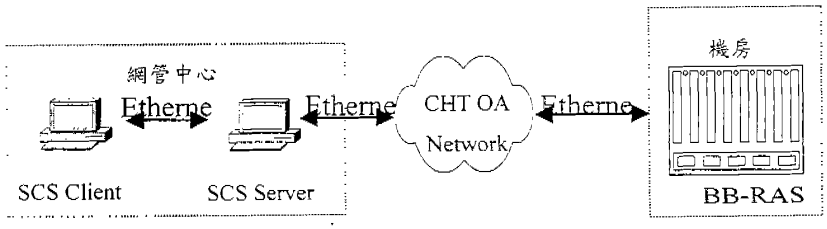
(1)In-Band 方式：

透過 ATM 連線經 ATM 網路與網管中心相連，與一般用戶相同佔用 LC 卡板上的一個 VC 值，測試架構如下：



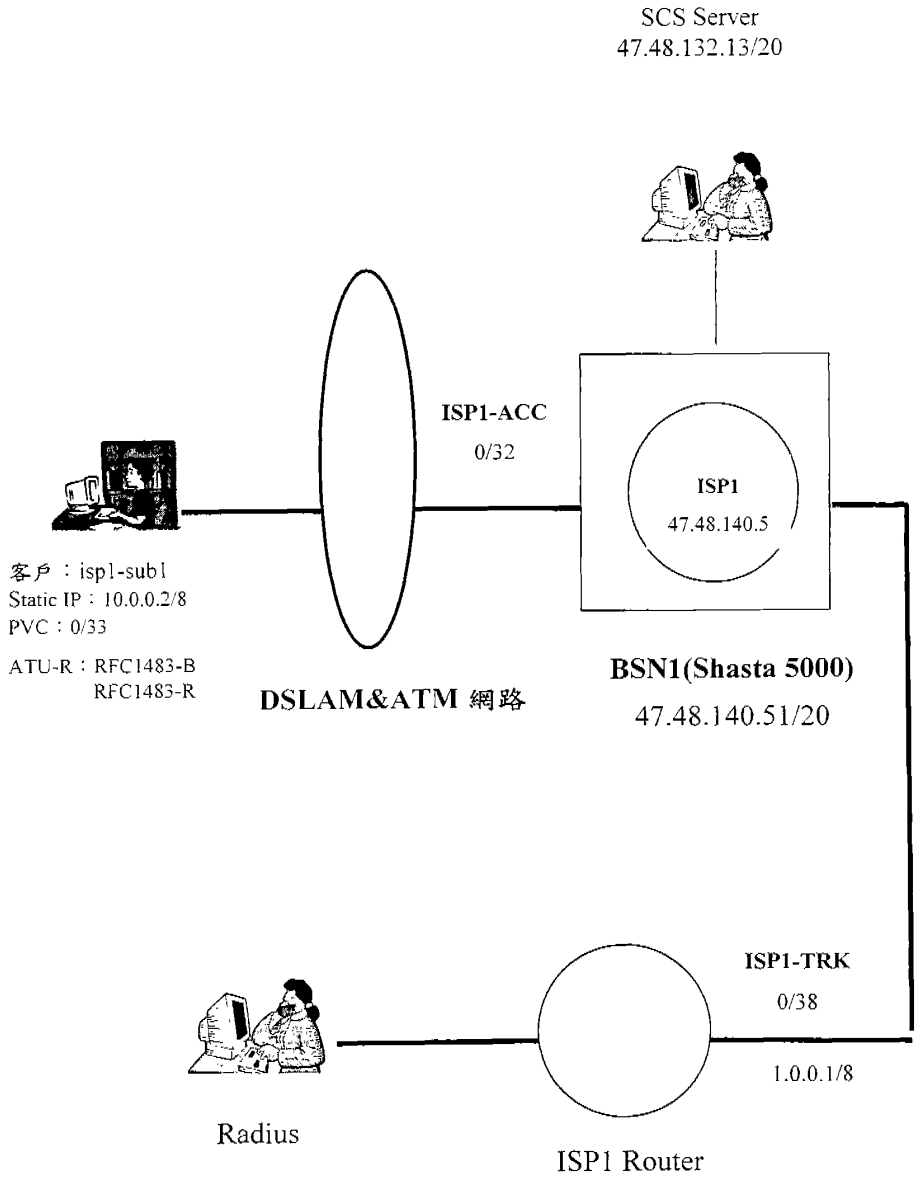
(2)Out Of Band 方式

在 Shasta 5000 上的 CMC 卡板上有一個網管的 Ethernet Port (現在已有 100 Base-T fast Ethernet 埠)，透過此埠與網管相連接並不額外佔用一個 ATM VC 值，稱之。測試架構如下：



5.2 O&M 實例

（一）網路架構



（二）建置步驟

以 **device owner** log in to the SCS server

a. Add and configure regions and BSNs SCS

進入 Device Manager 視窗依以下資料建置

SCS user name	5.2.1 Device_owner
SCS password	**do**
SCS Server IP address	47.48.132.13
Region Name	Training（可自訂）
Region number	1
Region IP address	47.48.132.13
BSNdevice name	BSN1
BSN device IP address	47.48.140.51

b. Configure cards and ports

進入 Device manager，在 BSN icon 按滑鼠右鍵後帶出 Configuration-Device 視窗，加入 CMC、SFC、SSC、及 ALC（含 port）等電路板設備。

c. Add and configure an ISP

進入 ISP Manager 視窗依以下資料建置

ISP name	Isp1
ISP IP address	47.48.140.5 (須與 BSN 1 同一網段)
ISP user name	Isp1
ISP user password	Isp1
ISP user profile	Isp_user
ISP device(s)	BSN 1

d. Add and configure access and trunk connections

(1)Access connections 提供客戶至 BSN 的連線(Encapsulation

Type: 1483-LLC-B

(2)Trunk connections 提供 BSN 至 ISPs 的連線(Encapsulation Type: 1483-LLC-R

進入 Connection Manager 依以下資料建置

1st Trunk Connection ID/Slot/Port/VPI/VCI	Isp1-trky/12/2/0/32
2nd Trunk Connection ID/Slot/Port/VPI/VCI	
3nd Trunk Connection ID/Slot/Port/VPI/VCI	
Access Connection ID/Slot/Port/VPI/VCI	Isp1-acc/12/2/0/38
ISP user password	Isp1
ISP user profile	Isp_user
ISP device(s)	BSN1

以 **ISP Owner** log in to the SCS server 作以下步驟

e. Configure an ISP dedicated subscriber（客戶）

(1) 進 Connection Manager 點選 Connection icon 確認 access and trunk 均已建妥。

(2) 進入 Subscriber Manager 依以下資料建置

User name：isp1-sub1

Domain：isp1

Customer：isp

IP address& Netmusk：10.0.0.2/8（須與 BSN1 access-side interface 同網段）

f. Configure trunk interfaces and OSPF（或 RIP）routing

以 **ISP user** log in to the SCS server

進入 Device Manager 視窗依以下資料建置

ISP Default Address：1.0.0.254

Local IP Addr&Netmusk：1.0.0.1/8

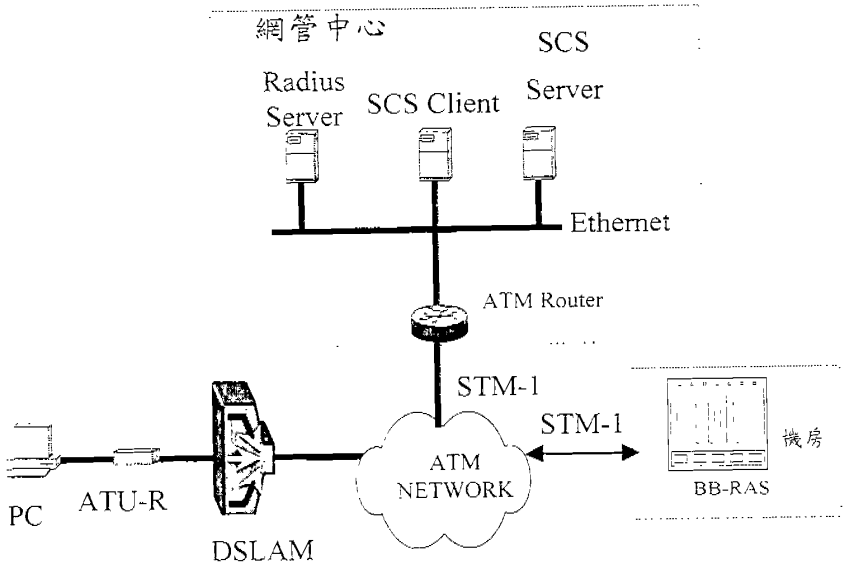
5.3 Shasta 5000 BB-RAS 之驗收測試

5.3.1 封裝協定測試

測試目的: 驗證 BB-RAS 設備是否提供 PPPoA、PPPoE、RFC 1483 – Bridged、Routed 等封裝協定。

相關規格: ME3010-1 2.3.1 封裝協定格式

測試架構:



測試環境:

a. ATM Network、DSLAM 一套、ATU-R 一台(support PPPoA)、PC 一台。

b. BB-RAS、ATM Router、SCS Server、SCS Client、Radius Server、PPPoE 連線軟體一套。

測試設備: None

初始設定:

1. SCS Server 於網管中心透過 ATM Router 連接上 ATM NETWORK。
2. BB-RAS 於各機房透過 STM-1 光纜連接上 ATM NETWORK。
3. ATU-R 用戶經由 DSLAM 透過 ATM Network 連接上 BB-RAS。
4. 設定 ATU-R 與 DSLAM 介接。

測試結果:

項次	測試步驟	預期測試結果
1	a、 透過 SCS Client 設定 BB-RAS 於 DSLAM 與 BB-RAS 間建立 access connection、封裝協定為 PPP/ATM b、 設定 BB-RAS 於 ATM Router 與 BB-RAS 間建立 trunk connection, 封裝協定為 RFC-1483-R c、 設定 BB-RAS, 建立 PPP 用戶 d、 ATU-R 用戶可成功連線上網, Ping 通 ATM Router	用戶可使用 PPPoA 方式順利連線表示本系統支援 PPPoA 封裝協定
2	a、 設定 DSLAM 與 BB-RAS 介接, 封裝協定為 RFC-1483-B。 b、 於網管中心，透過 SCS Client 於 BB-RAS 建立 Connection c、 建立 PPPoE Tunnel profile d、 建立 PPPoE 用戶 e、 用戶使用 PPPoE 連線軟體上線	用戶可使用 PPPoE 軟體順利連線表示本系統支援 PPPoE 封裝協定
3	a、 建立 ISP trunk connection 連接至 ISP 端，使 用 1483-LLC-R 封裝屬性 。 b、 建立 Access connection 連接至 DSLAM 用戶端，使用	用戶可順利連線，表示支援 RFC 1483 Bridging 及 RFC 1483 Routing 封裝模式。

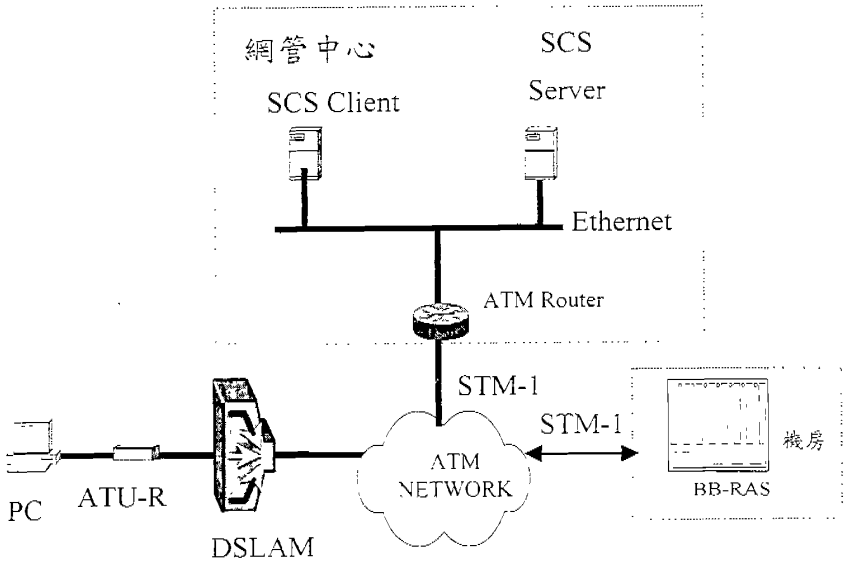
	1483-LLC-B 屬性。
	c、 用戶使用 PPPoE 連線軟體上線。

5.3.2 PPPoE 連線測試

測試目的: 驗證 BB-RAS 設備是否具備 PPPoE 連線方式。

相關規格: ME3010-1 2.4 PPPoE 連線

測試架構:



測試環境:

a. ATM Network、DSLAM 一套、ATU-R 一台、PC 一台。

b. BB-RAS、ATM Router、SCS Server、SCS Client、PPPoE 連線軟體一套。

測試設備: None

初始設定:

1. SCS Server 於網管中心透過 ATM Router 連接上 ATM NETWORK。
2. BB-RAS 於各機房透過 STM-1 光纜連接上 ATM NETWORK。
3. ATU-R 用戶經由 DSLAM 透過 ATM Network 連接上 BB-RAS。
4. 設定 ATU-R 與 DSLAM 介接。
5. 設定 DSLAM 與 BB-RAS 介接，封裝協定為 RFC-1483-B。

測試結果:

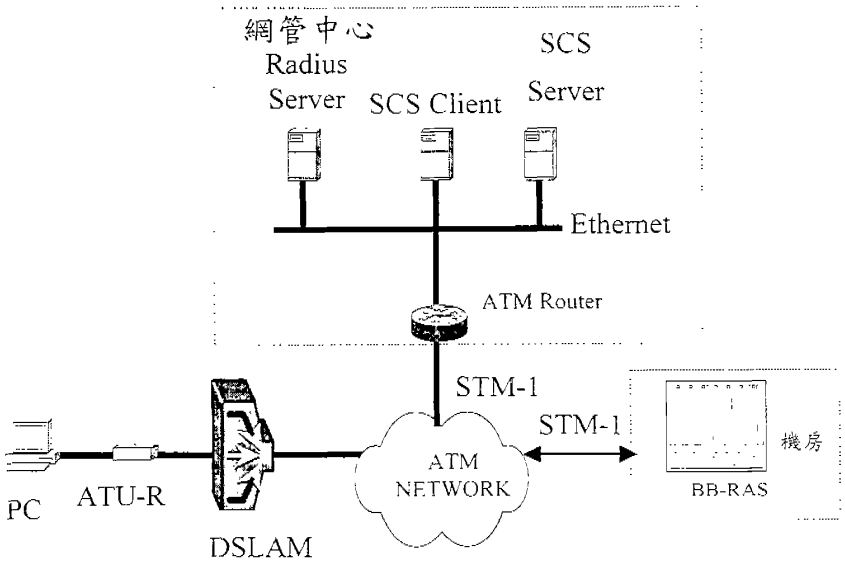
項次	測試步驟	預期測試結果
1	a. 透過 SCS Client 設定 BB-RAS 於 DSLAM 與 BB-RAS 間建立 access connection，封裝協定為 RFC-1483-B b. 設定 BB-RAS 於 ATM Router 與 BB-RAS 間建立 trunk connection，封裝協定為 RFC-1483-R c. 設定 BB-RAS，建立 PPPoE Tunnel profile d. 設定 BB-RAS，建立 PPPoE 用戶 e. ATU-R 用戶使用 PPPoE 連線軟體上線 f. ATU-R 用戶可成功連線上網，Ping 通 ATM Router	用戶可使用 PPPoE 軟體順利連線

5.3.3 PPPoA 連線測試

測試目的: 驗證 BB-RAS 設備是否具備 PPPoA 連線方式。

相關規格: ME3010-1 2.4 PPPoA 連線

測試架構:



測試環境:

a. ATM Network、DSLAM 一套、ATU-R 一台、PC 一台。

b. BB-RAS、ATM Router、SCS Server、SCS Client、Radius Server。

測試設備: None

初始設定:

1. 以 Device Owner 登入 SCS Server 建 PPP/ATM(即 PPPoA)封裝方式之連線。
2. 登出 Device Owner 後，以 ISP 之身分建立以上述連線 Connection Template 之用戶。
3. 於 Radius Server 建立用戶之 profile "sub_pppoa" (PAP/CHAP) 並指定其 Address 。
4. 設定 PC 及 ADSL router 相關之設定。
5. 於 BB-RAS 設定 Reachability 指向用戶所屬之 Domain。

測試結果:

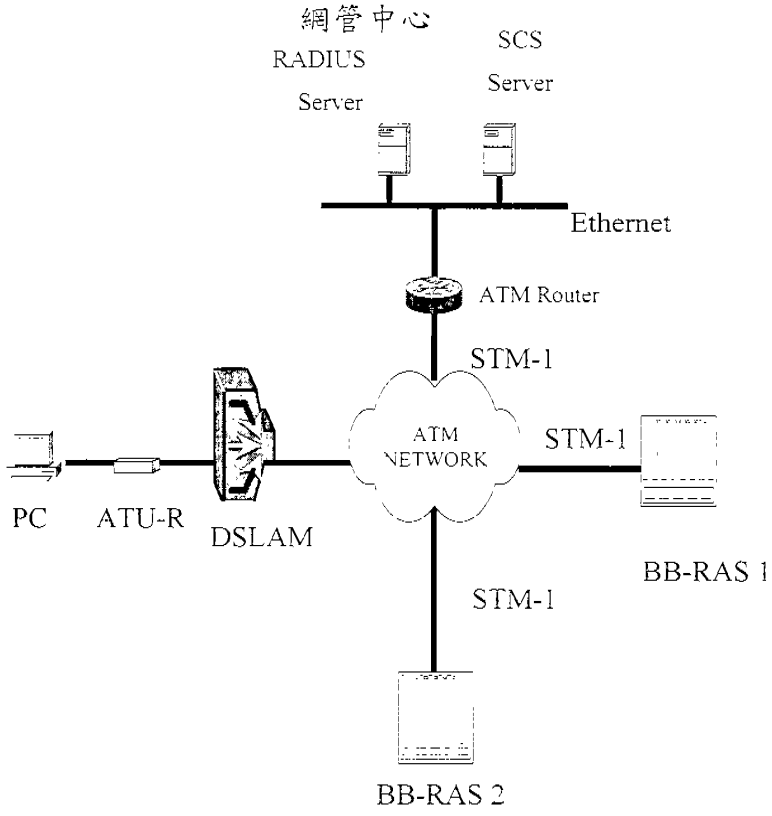
項次	測試步驟	預期測試結果
1	a. 透過 SCS Client 設定 BB-RAS 於 DSLAM 與 BB-RAS 間建立 access connection、封裝協定為 PPP/ATM b. 設定 BB-RAS 於 ATM Router 與 BB-RAS 間建立 trunk connection, 封裝協定為 RFC-1483-R c. 設定 BB-RAS, 建立 PPP 用戶 d. ATU-R 用戶可成功連線上網、Ping 通 ATM Router	用戶可使用 PPPoA 方式順利連線

5.3.4 橋接(Bridging)與燧接(Tunneling)測試

測試目的: 驗證 BB-RAS 設備之是否具備 L2TP 功能。

相關規格: ME3010-2.3.3 橋接(Bridging)與隧接(Tunneling)

測試架構:



測試環境:

a. ATM Network、DSLAM 一套、ATU-R 一台、PC 一台

b. BB-RAS 二台、ATM Router、SCS Server、Radius Server、PPPoE 軟體

測試設備: None

初始設定:

1. SCS Server 於網管中心透過 ATM Router 連接上 ATM NETWORK。
2. BB-RAS 於各機房透過 STM-1 光纜連接上 ATM NETWORK。
3. ATU-R 用戶經由 DSLAM 透過 ATM Network 連接上 BB-RAS。
4. 設定 ATU-R 與 DSLAM 介接。
5. 設定 DSLAM 與 BB-RAS 介接，封裝協定為 RFC-1483-B。

測試結果:

項次	測試步驟	預期測試結果
1	a. 將連接上 DSLAM 與 BB-RAS(BB-RAS 1)之 connection 設定為 access connection b. 任選連上 ATM Network 之另一台 BB-RAS(BB-RAS 2)，設定此二台 BB-RAS 間之 connection 為 trunk connection c. BB-RAS 1 端設定為 L2TP 之 LAC Mode、BB-RAS 2 端設定為 L2TP 之 LNS Mode。 d. 於 BB-RAS 設定 subscriber 為 l2tp 狀態。 e. ADSL 用戶透過 PPPoE 連線軟體上網，要求 BB-RAS 1 與 BB-RAS 2 間建立 L2TP Tunnel f. 分別檢查 BB-RAS 1 與 BB-RAS 2 之 connection 狀態，均顯示存在 l2tp connection g. BB-RAS 2 端取消 L2TP 之 LNS Mode 設定 h. ADSL 用戶透過 PPPoE 連線軟體	本系統提供 L2TP Tunnel Connection 功能

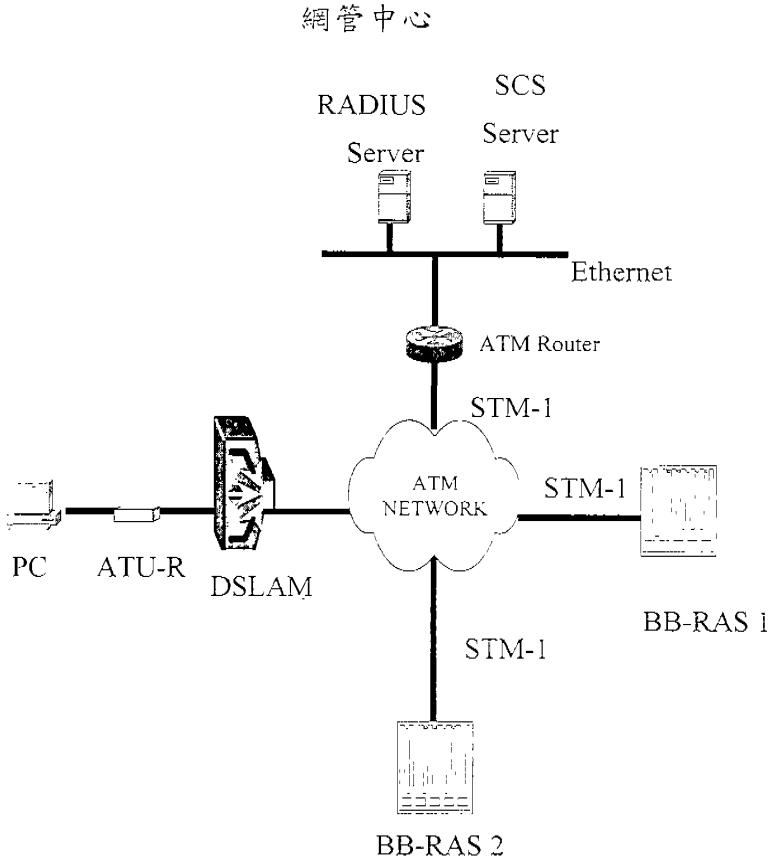
	連線因 BB-RAS 1 與 BB-RAS 2 間無法成功建立 L2TP Tunnel 而連線失敗。	

5.3.5 應用服務之動態服務選擇測試

測試目的: ADSL 用戶依其意願 (如user name@domain name) 動態更換服務提供者 (ISP 或 ICP) 時，購方維運單位無須重新調定 PVC 電路或 BB-RAS，即可依用戶意願選擇不同服務提供者 (ISP 或 ICP) 上網接取服務。

相關規格: 工程設計書動態服務選擇

測試架構:



測試環境:

a. ATM Network、DSLAM 一台、ATU-R 一台、PC 一台

b. BB-RAS 二台、ATM Router、SCS Server、Radius Server

測試設備: None

初始設定:

1. SCS Server 於網管中心透過 ATM Router 連接上 ATM NETWORK。
2. BB-RAS 於各機房透過 STM-1 光纜連接上 ATM NETWORK。
3. ATU-R 用戶經由 DSLAM 透過 ATM Network 連接上 BB-RAS。
4. 設定 ATU-R 與 DSLAM 介接。
5. 設定 DSLAM 與 BB-RAS 介接, 封裝協定為 RFC-1483-B。

測試結果:

項次	測試步驟	預期測試結果
1	a. 系統設定 2 個 ISP(ISP1、ISP2), 及設定 access connection 由 BB-RAS 1 連接到 DSLAM b. 設定 ISP 1 trunk connection 連接到 ATM Router, 即以 ATM Router 模擬 ISP 1, ISP 2 trunk connection 連接到 BB-RAS 2, 即以 BB-RAS 2 模擬 ISP 2 c. 設定 ISP Subscriber group 及用戶 d. Radius server 設定 2 個 ISP(ISP1 ISP2)，且設定其 domain，與 user-name，password。 Isp1.com ->user-name=isp1 ->password Isp2.com ->user-name=isp2 ->password e、 ATU-R 用戶(PC)輸入 isp1@isp1.com 可連線到 ISP1，Ping isp1 router(ATM Router)。	ATU-R 用戶依其意願動態更換服務提供者

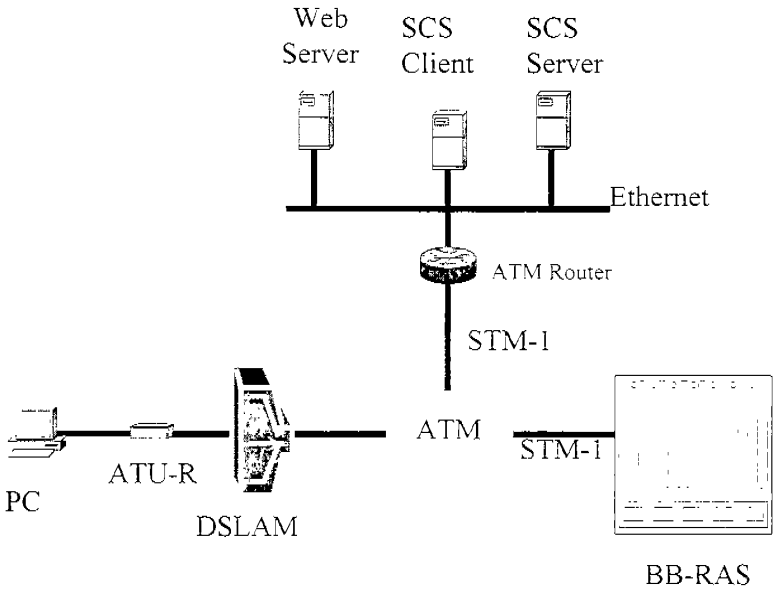
	f、 ATU-R 用戶(PC)斷線。 g、 ATU-R 用戶(PC2)輸入 isp2@isp2.com 可連線到 ISP2，Ping isp2 router(BB-RAS 2)。	

5.3.6 Portal Service 測試

測試目的: 驗證 BB-RAS 設備之 Portal Service 功能是否符合器材規格之規範

相關規格: 工程設計書: 12.5 其他加值服務

測試架構:



測試環境:

a. ATM Network、DSLAM 一台、ATU-R 一台、PC 一台

b. BB-RAS、ATM Router、SCS Server、SCS Client、Web Server、PPPoE 軟體

測試設備: PC 一台

初始設定:

1. Web Server 於網管中心透過 ATM Router 連接上 ATM NETWORK。
2. BB-RAS 於各機房透過 STM-1 光纖連接上 ATM NETWORK。
3. ATU-R 用戶經由 DSLAM 透過 ATM Network 連接上 BB-RAS。
4. 設定 ATU-R 與 DSLAM 介接。
5. 設定 DSLAM 與 BB-RAS 介接, 封裝協定為 RFC-1483-B。

測試結果:

項次	測試步驟	預期測試結果
1	a. 透過 SCS Client 建立一 ISP, 設定 BB-RAS 於 DSLAM 與 BB-RAS 間建立 access connection, 封裝協定為 RFC-1483-B b. 設定 BB-RAS 於 ATM Router 與 BB-RAS 間建立 trunk connection, 封裝協定為 RFC-1483-R c. 設定 BB-RAS, 建立 PPPoE Tunnel profile d. 設定 BB-RAS, 建立 Captive Portal Service Policy e. 設定 BB-RAS, 建立 PPPoE 用戶並選擇 Captive Portal Service f. ATU-R 用戶使用 PPPoE 連線軟體上線 g. 通過認證測試後，建立 Connection。 h. 在 ATU-R 用戶 PC 上執行 Web browser 軟體。 i. 於 Browser 任意輸入 URL。 j. 不論用戶其 URL 為何,均會被本系統(BB-RAS)抓取而 redirect 到內定	本系統具備 Portal Screen 服務功能

	之 Web Server 而提供 Portal Screen 服務	
2	a. 使用 SCS Client 建立 2 個 ISP(ISP1、ISP2)並建立 PPPoE 之 ISP Select 相關設定 b. 分別於 2 個 ISP 建立 Captive Portal 並指定為不同之 Web cgi 程式 c. 用戶使用 PPPoE 連線上網並開啟 Browser, sub@isp1 將 redirect 到 isp1 之 Web cgi 畫面, sub@isp2 將 redirect 到 isp2 之 Web cgi 畫面	本系統可依 domain name 而 pump 不同之 Portal Screen 畫面
3	a. 接續 1. 設定 Captive Portal 之 Session Timeout 為 1 分鐘(step 8) b. ATU-R 用戶使用 Browser 而為 Captive Portal redirect 到 Web Server 且於一段時間 release 到正常網站 c. 1 分鐘後, reload web page 則此網頁將再次被 Captive Portal 抓住而回到 Portal Screen	本系統可於 release 到正常網頁一段時間後, 再次抓回 Portal Screen 畫面

6. Shasta 5000 BB-RAS 網路管理系統運作

6.1 Shasta 5000 BB-RAS 網管功能概要

Shasta 5000網管系統，主要設備包括NMS Server、RADIUS Server、WEB Server及網管終端設備等。網管系統相關設備能在權限範圍內，以圖型化介面 (GUI) 管理各分公司所轄寬頻伺服器網路資源及服務，並提供組態管理、錯誤管理、效能管理、安全管理、計費管理、Web Login 管理、認證、授權與計費等功能。網管系統透過 ATM 寬頻交換網路，用以傳遞 BB-RAS 網管訊息及計費資料 (CDR) 之路由採 Active-Standby Redundancy 架構，路由作切換時網管系統不會中斷服務。

Shasta 5000之網管系統硬體採用SUN Server平台，軟體為Shasta SCS Server及SCS Client。SCS Server安裝於網管Server，而SCS Client則安裝於網管終端設備。SCS (Service Creation System) Server為Multi-tier架構。SCS Server之架構，如圖6-1：

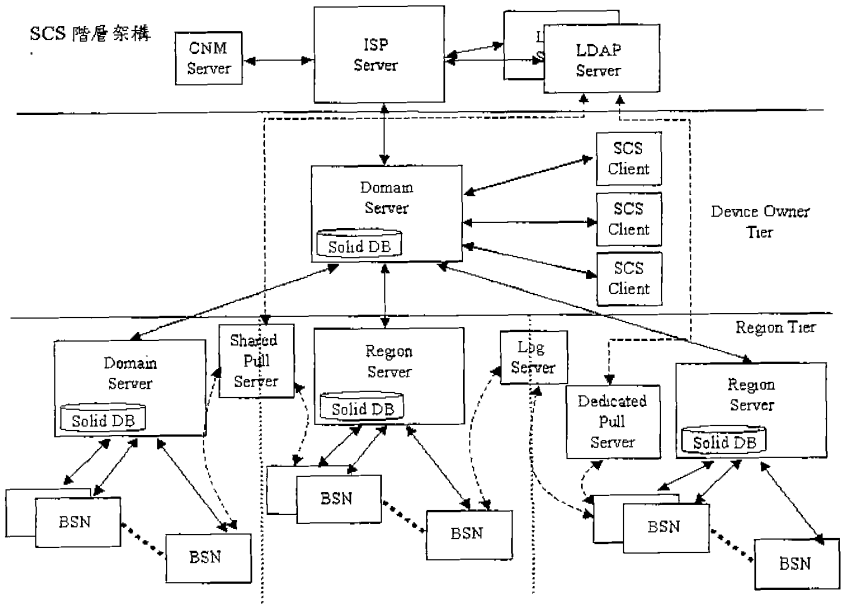


圖6-1、 SCS 架構

6.2 NMS 之系統架構及其功能

此次三區分公司之BB-RAS寬頻遠端伺服器建設工程，北區建設7套、中區建設6套、南區建設12套、訓練所建設1套，合計26套。係由南方資訊公司得標，所提供之產品為NORTEL公司之Shasta 5000，以下簡要說明Shasta 5000 網路管理系統(NMS)之架構及其功能。

6.2.1 區分公司寬頻伺服器架構

本案之BB-RAS主要用途為提供寬頻用戶選擇服務型態或欲接取之ISP網路，BB_RAS置於ATM Edge Switch後端，介接於寬頻用戶迴路接取網路上，支援用戶管理、寬頻網際網路與虛擬專用路由器(Virtual Router)機能等服務應用，區分公司寬頻伺服器網路架構，如圖6-2:

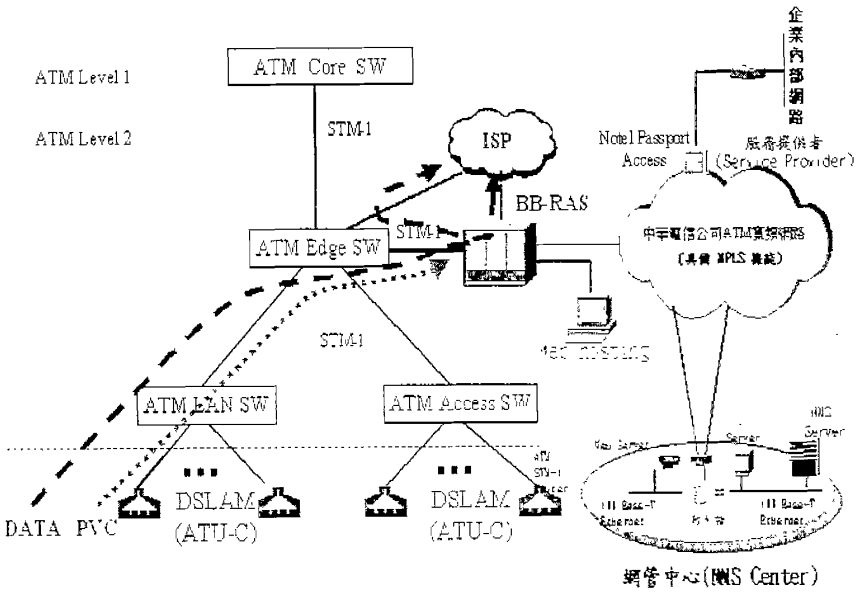


圖 6-2、 區分公司寬頻伺服器網路架構

6.2.2 三區分公司 BB-RAS Shasta 5000 網管系統架構

本次區分公司之BB-RAS建設工程，三區各自設有網管系統，網管架構採用 In-band 方式，經由本公司之 ATM 寬頻交換網路管理各區分公司所轄寬頻伺服器，且三區網管中心之 RADIUS Server可經由ATM 寬頻交換網路 PVC 電路或 MPLS 機能，以 TCP/IP 通訊規約互連，達到資料查詢認證功能，以提供用戶漫遊認證功能。三區之Shasta 5000 網管系統架構說明如下：

(1) 北區 Shasta 5000 網管系統架構說明

北區之網管系統設置於東六網管中心，由分公司網管處一科負責監控，並於士林劍潭(電子維運中心)設置遠端維護中心；東六網管中心監控北區所轄東四、南二、板橋、石牌、中壢普義、新竹關東及宜蘭中央等七個BB-RAS。北區Shasta 5000 網管系統架構，如圖6-3:

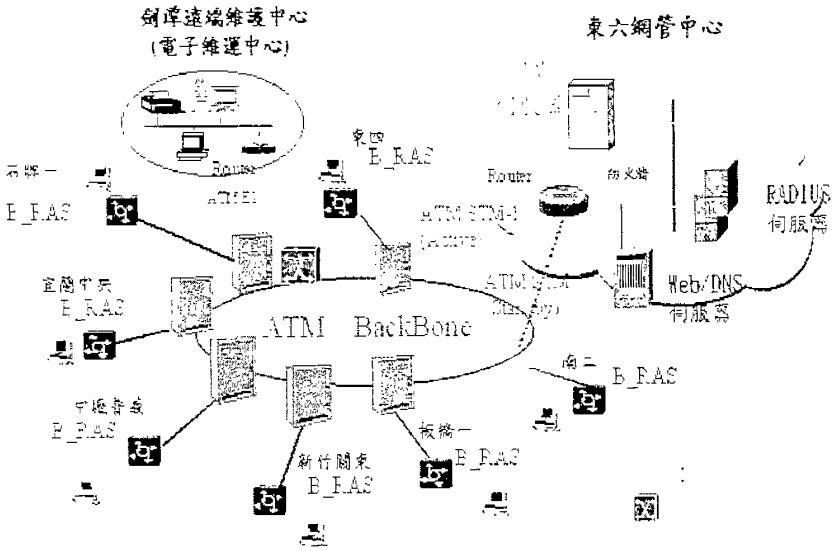


圖 6-3、 北區 Shasta 5000 網管系統架構

(2) 中區 BB-RAS 網管系統架構說明

中區之網管系統設置於南台中公館機房，由南台中營運處負責監控；公館機房網管中心監控中區所轄南台中公館、北台中民權、苗栗、彰化、南投南崗及雲林斗六等六個BB-RAS。中區Shasta 5000 網管系統架構，如圖6-4:

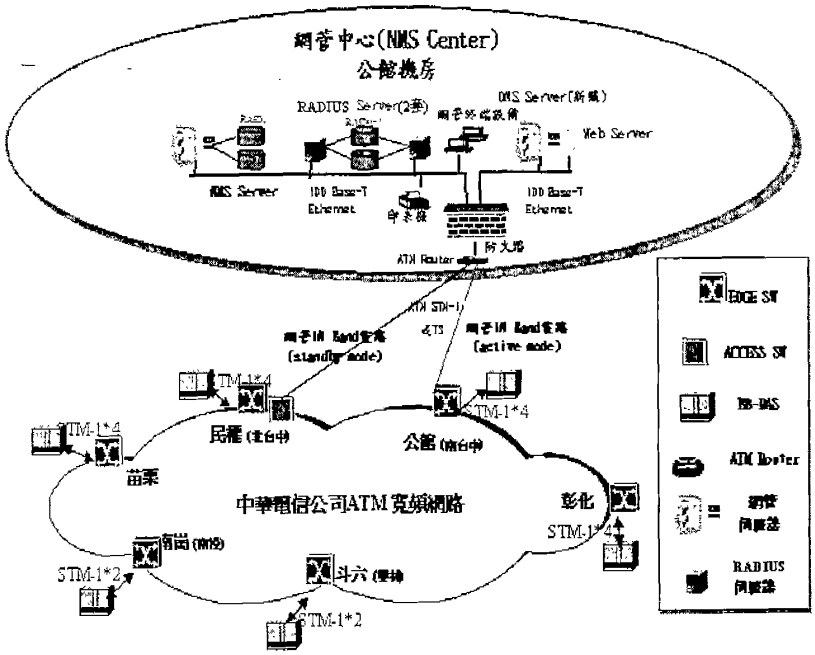


圖 6-4、 中區 Shasta 5000 網管系統架構

(3) 南區 BB-RAS 網管系統架構說明

南區之網管系統設置於網四科建工機房，由分公司網路處四科負責監控；建工機房網管中心監控南區所轄南高雄中山、北高雄民族、鳳山、台南延平、台南小康、台南道爺、新營民治、嘉義新厝、屏東建國、台東、澎湖馬公及金門金城等十二個BB-RAS。南區Shasta 5000 網管系統架構，如圖 6-5:

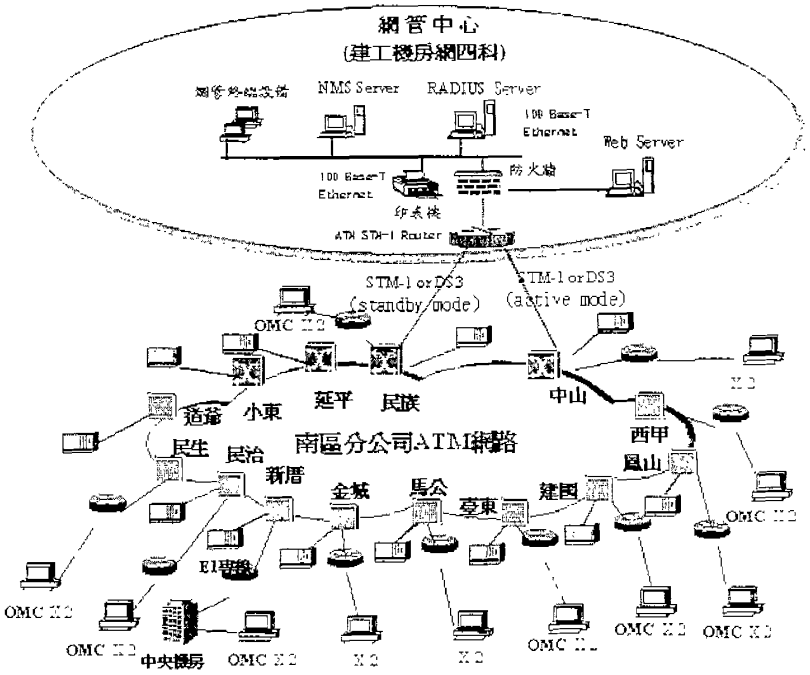


圖 6-5、 南區 Shasta 5000 網管系統架構

6.3 Shasta 5000 BB-RAS 之網路管理功能

Shasta 5000網管系統 (SCS Server) 為一圖形化的網路管理及供裝服務管理。SCS Server提供了以下網管系統之主要功能：

(1) 組態管理 (Configuration Management)

- 提供組態資料庫之設定、詢問、更新、備份(Backup)、回復等能力。
- 具備圖形化使用者介面以進行設定作業。
- 提供與用戶及服務提供者相關的服務參數設定程序，如服務政策(Policies)與服務品質Profiles。
- Configure the Shasta 5000：
  - Add and configure Regions and BSNs within SCS
  - Configure cards and ports on a BSN
  - Add and configure an ISP
  - Add and configure trunk and access connections

(2) 錯誤管理 (Fault Management)

- 具備告警(Alarm)信號與事件之顯示、維護與資料庫更新之能力。
- 提供磁碟空間以儲存告警信號與事件，並提供瀏覽、排程(Schedule)與過濾告警信號與事件至一特定檔案之能力。
- 對於網管系統相關設備，即時提供可聽(Audio)及可視(Visual)之告警顯示超即時報表。
- 於SCS Client連上網管GUI畫面，進入Alarm Manager與Device Manager之Monitoring功能，以檢視BB-RAS之告警，而對BB-RAS進行Fault Management。

(3) 效能管理 (Performance Management)

- 具備設定與取回(Retrieve)系統主機各項效能監控與流量量測資訊之能力，且可將前述各項資訊儲存於磁碟供後續處理。
- 於SCS Client連上網管GUI畫面，進入Device Manager之Viewing Static功能，可查詢BB-RAS之CPU效能、流量狀況等資料，而對BB-RAS進行Performance Management。

(4) 安全性管理 (Security Management)

- 提供 device_owner&isp、device_owner 和 isp等三種網路存取等級之設定，並只允許網路管理系統之系統管理者修改安全性等級之設定。
- 以 device_owner 權限 Login SCS Server, 進入 User Manager 功能可對 BB-RAS 之使用者權限進行管理。
- device_owner 存取等級可建立 ISP、Connection 等資料, 而 isp 存取等級可建立 Subscriber 等用戶資料, device_owner&isp 則均可存取。
- 提供Event Log紀錄使用者行為狀況，可依時間標戳(Time Stamp)紀錄使用者行為，並可將該使用狀況紀錄至一特定檔案。

(5) 用戶計費統計管理 (Accounting Management)

- 記錄每一用戶使用時間及傳送資料量等計費資訊，可直接或透過RADIUS-Proxy方式以提供本地或遠端 RADIUS伺服器進行計費作業。

(6) 具備 In-Band Management 功能

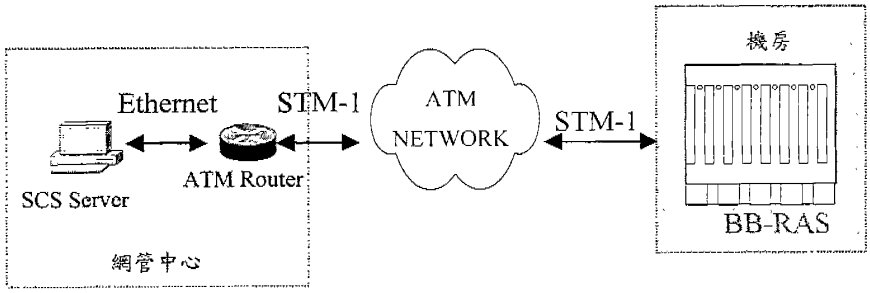
- SCS Server 可透過 ATM 網路，對 BB-RAS 作 In-Band 管理。

(7) 具備 Out-Of-Band Management 功能

- SCS Server 亦可透過 CHT Intranet 網路，對 BB-RAS 作 Out-Of-Band 管理。

(8) 具備系統載入及再啟動功能

- 網管系統具備系統載入及再啟動功能，系統重新啟動後能正常運作並保留原有設定。
- SCS Server 可對所監控之 BB-RAS 作系統載入重新啟動(Reload)。
- 亦可對 SCS Server 本身作 Reboot，首先啟動 LDAP Server，再啟動 SCS Server。



6.4 Shasta 5000 BB-RAS與安全管理

SCS 在安全管理上提供了 3 種使用者權限來管理 Shasta 5000：

(1) DO (Device Owner) 權限

- SCS 所管理 Shasta 5000 設備的擁有者

(2) ISP (Internet Services Provider) 權限

- ISP 利用 Shasta 5000 設備來提供服務給用戶但並不擁有 Shasta 5000 設備

(3) DO&ISP 權限

- SCS 所管理 Shasta 5000 設備的擁有者並且也同時是 ISP

SCS 提供了 12 種管理經理(Manager)來做為網路管理的服務，這 12 種管理經理分別為:

(1) Device Manager

- Device Manager擁有Shasta 5000設備元件供裝(Provision)設定功能的權限。設備供裝設定功能包含新增，刪除，和更改 Nodes, Slots 組態和Card組態，Access 和 Trunk Interfaces和 Routing組態，並且也能新增，刪除，和更改Alarms 和 Statistics組態.。

(2) ISP Manager

- ISP Manager 擁有新增，刪除，和更改 ISP 權限。

(3) Connection Manager

- Connection Manager 擁有新增，刪除，和更改 Trunk 及 Access Connections 權限。

(4) Bulk Connections Manager

- Bulk Connection Manager 擁有新增，刪除，和更改大量 Connection 權限。

(5) Access Property Manager

- Access Property Manager 擁有新增，刪除，和更改 RADIUS、DHCP、PPP、IPEC、IKE profiles，及新增，刪除，和更改 ISP FQDN、VLL、Connection Template、Tunnels 等等物件權限。

(6) Service Policy Manager

- Service Policy Managerr 擁有新增，刪除，和更改 Service Policy profile，包含 Security, Anti-Spoofing, Ingress Anti-Spoofing, DiffServ Marking, Traffic Shaping, Captive Portal and Policing Policies 權限。

(7) Subscriber Manager

- Subscriber Manager擁有新增，刪除，和更改用戶權限。

(8) User Manager

- User Manager 擁有新增，刪除，和更改 SCS 使用者權限。

(9) Alarm Manager

- Alarm Manager 是用來管理 Shasta 5000 之告警。

(10) Route Properties Manager

- Route Properties Manager 擁有新增，刪除，和更改路由設定權限。

(11) VPN Manager

- VPN Manager 擁有新增，刪除，和更改 VPN 權限。

(12) Logs Manager

- Logs Manager 適用來管理用戶的服務記錄資料

SCS 根據使用者不同的權限提供不同的網路管理範圍。如下表格所示:

(1) Table 6-1. Manager Windows versus User Types

Manager	(2) DO	DO & ISP	ISP
Device Manager	X	X	X
ISP Manager	X	X	
Access Properties Manager	X (部份)	X	X
Service Policy Manager	X (部份)	X	X
Connection Manager	X	X	
Bulk Connection Manager	X	X	
User Manager	X	X	X
Subscriber Manager		X	X
Alarm Manager	X	X	X
Route Properties Manage	X	X	X
VPN Manager		X	X
Log Manager		X	X

7. Shasta 5000 之 IP VPN

7.1 IP VPN 概要

Passport 7K/15K之IP VPN是靠虛擬路由器(Virtual Router, VR) 、Virtual Connection Group (VCG) 、Point-To-Multipoint(PTMP) tunneling、與Multiple Protocol Label Switch(MPLS)等元件來完成的，以下將對這些元件作一摘要說明，同時也將針對Passport中使用之IP路由協定加以說明。

7.1.1 虛擬路由器

虛擬路由器提供一實體路由器的軟體模擬器。經由虛擬路由器，Passport的節點轉送封包到正確的目的地，並靠著對每一客戶維持一獨立且分離的路由表格來區隔客戶的訊務量。從本公司的觀點而言，每一IP VPN是由一組虛擬路由器組合而成的；此外，每一獨立的客戶端虛擬路由器可支援許多VPN用戶地區。

Passport 使用客戶端虛擬路由器、管理虛擬路由器、與VCG來實作IP VPN解決方案。一IP VPN包括一個或多個客戶端虛擬路由器且可延伸至多個Passport節點，本公司對每一客戶端指派一客戶端虛擬路由器用以連接客戶端網路。因此，每一客戶端虛擬路由器在一個Passport節點代表一個獨立且分離的VPN地區。對每一企業客戶網路而言，客戶端虛擬路由器提供一獨立且分離的路由表格；因為客戶訊務量資料只被擁有該VPN的企業客戶之專屬客戶端虛擬路由器所處理，所以當在共有之交換機與傳輸資源下仍可與其他客戶區別以達成路由能力的保證。每一客戶端虛擬路由器靠Virtual Private Identifier(VPI)來識別其屬於那一VPN，而在Passport

節點上的每一虛擬路由器的VPI ID是唯一的；從網路管理的觀點而言，屬於相同IP VPN的所有客戶端虛擬路由器通過許多Passport節點擁有相同的VPI ID是非常重要的。

管理虛擬路由器可視為一特殊的虛擬路由器。他提供連接Passport節點的單一進入點，並允許管理在該節點上的所有虛擬路由器。可透過外部的存取服務如telnet、ftp、或FMIP在管理虛擬路由器的TCP agent上執行，也可透過SNMP agent的方式來管理。Passport節點內定第一個虛擬路由器作為管理虛擬路由器，一但啟動該設定時，不可以更改其他的虛擬路由器作為管理虛擬路由器之用。

7.1.2 VCG

VCG亦可視為一特殊的虛擬路由器。在典型的Passport IP VPN實作上，CPE路由器連接分配給該企業的客戶端虛擬路由器，在Passport節點之每一客戶端虛擬路由器連接至一屬於該交換機所共通的虛擬路由器，稱之為VCG。如圖7.1所示，他不但從戶端虛擬路由器中聚集訊務量且提供在該節點上的所有客戶訊務量連接至WAN的單一對外連接。連接所有Passport節點的這些VCG不但提供所有IP的功能，同時也經由PTMP的 IP tunnel提供在同一IP VPN內的客戶端虛擬路由器之間的連接。本公司建設時在骨幹網路上連接每一Passport節點之VCG以達成完全連接，因為VCG允許在骨幹網路上聚集第二層的電路連接，故當本公司需要增加一新的客戶端虛擬路由器到計有網路時，骨幹網路上的規劃仍然不受影響而不需更動。本公司可在Passport節點上規劃使用超過一個以上的VCG，每個VCG指派管理部分的客戶端虛擬路由器以降低記憶體的使用效率與提升訊務量。

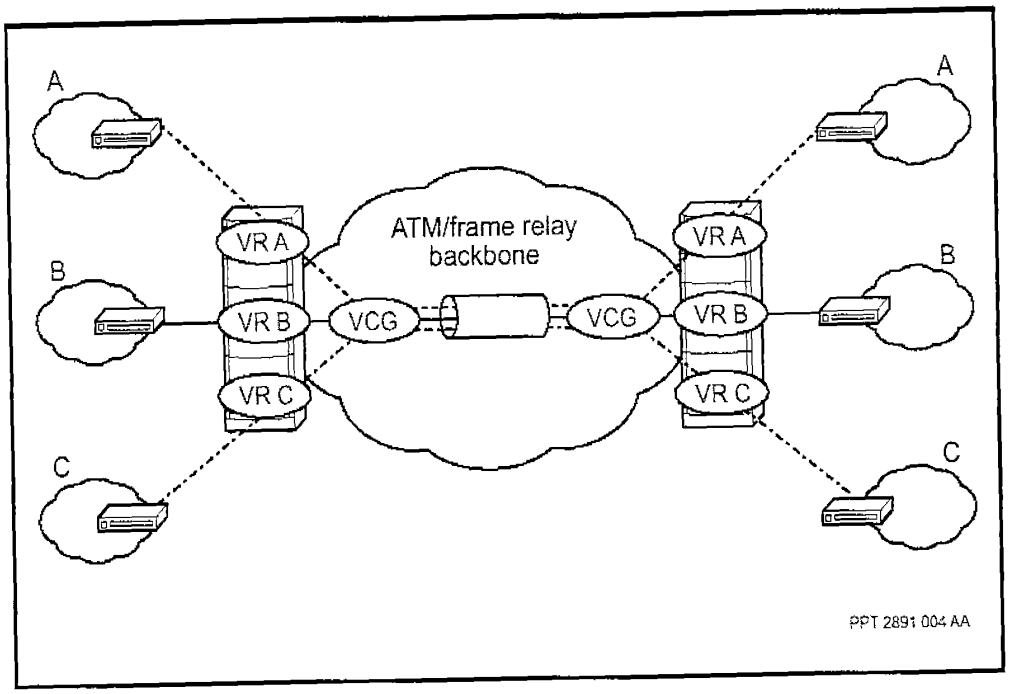


圖 7.1 Passport IP VPN 之 VCG 示意圖

7.1.3 PTMP tunneling

如圖7.2所示，Passport IP VPN服務使用PTMP tunneling提供在不同Passport節點間的客戶端虛擬路由器之相互連接。為了達成完全的site-to-site連接目的，本公司必須在IP VPN內每一客戶端虛擬路由器之PTMP tunnel規劃起始與多重目的位址。客戶端虛擬路由器在ingress端執行IP in IP tunnel encapsulation(RFC 2003)，在egress端則是執行decapsulation。

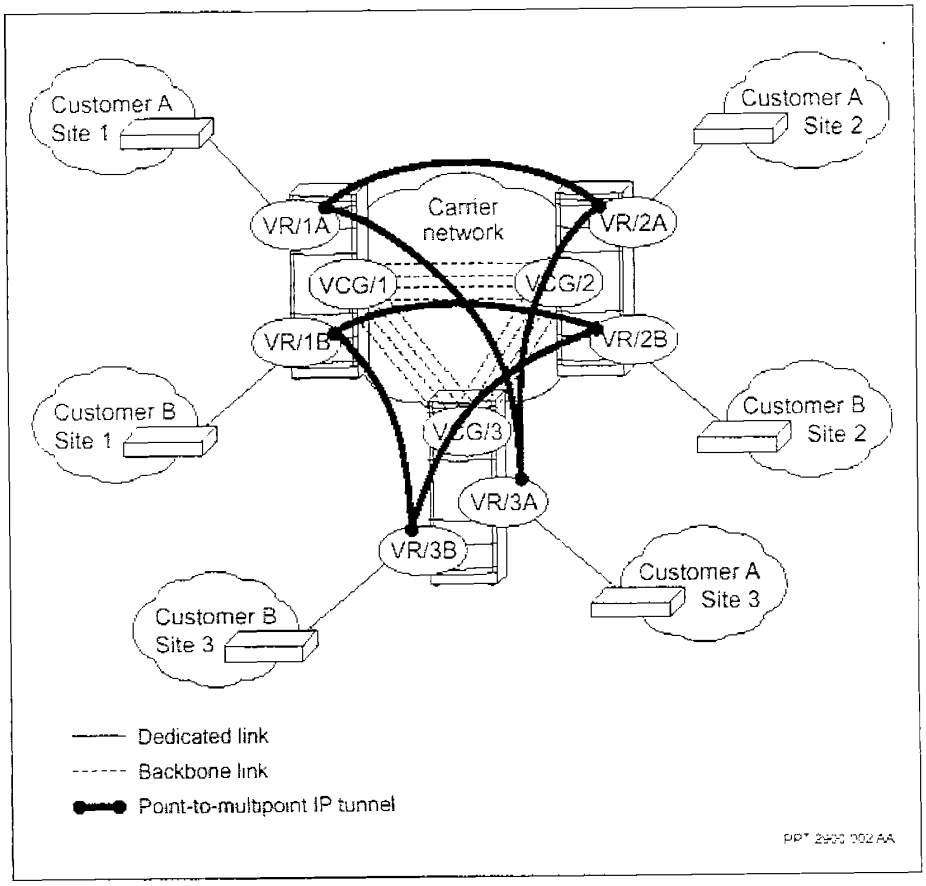


圖 7.2 Passport IP VPN 之 PTMP tunneling 示意圖

7.1.4 MPLS

MPLS是Passport在第三階段IP VPN解決方案中才會提供的元件。在此應用中，經由本公司公眾網路設定MPLS之Label Switched Path(LSP)提供VCG間的連接，LSP可以經由IP

路由協定資訊來設定，且經由明確的路由路徑事先規劃。它的好處是使得網路規劃工程容易，且提供單層的路由路徑。當在骨幹網路上使用MPLS時，VCG被視為是Label Edge Router(LER) ，f且可建立介於本地VCG LER與相對應遠端客戶之VCG LER間的LSP。當IP 訊息封包到達本地VCG LER時，在ATM第二層表頭內會插入一MPLS的標記，且會在IP訊息封包中附加一空的shim表頭；然後這些IP訊息封包會透過在LSP所經過的所有LSR間進行標記交換，直到到達相對應遠端客戶之VCG LER為止。到達目的地時，最外層包含標記的表頭會被移除，且IP tunnel表頭會用以指明相對應客戶端虛擬路由器的tunnel輸出點。如此一來，原始的IP訊息封包送給給相對應客戶端虛擬路由器，而正常的IP路由則可到達最後的目的地。

7.1.5 IP 路由協定

如圖7.3所示，Passport客戶端虛擬路由器與VCG可以分別執行不同的轉送表格以確保在不同VPN間的隔離，每一虛擬路由器的IP轉送表格和路由資料庫仍然與在該節點的其他每一個虛擬路由器保持分開。Passport的虛擬路由器支援靜態與動態的路由協定，例如RIP v1、RIP v2、OSPF、與BGP-4等。每一客戶端虛擬路由器從所連接的CPE 設備透過靜態路由或IGP學得路由資訊，也支援從企業網路中學得動態路由資訊。本公司必須規劃在客戶端虛擬路由器的路由協定以便接收這些資訊。BGP-4的同層連接提供在IP VPN內的到達資訊，客戶端虛擬路由器可轉送在骨幹網路中CPE 設備經由IBGP同層連接所學得的路由資訊。IBGP同層連接是位於IP tunnel的輸出點，傳遞路由資訊給屬於相同VPN的所有客戶端

虛擬路由器。

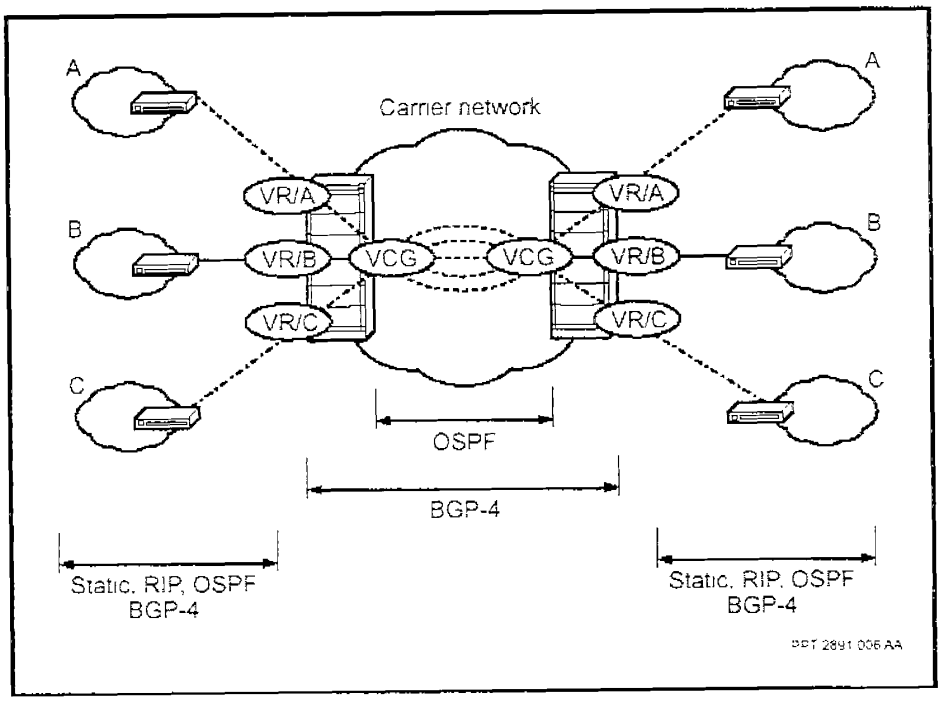


圖 7.3 Passport IP VPN 之 IP 路由協定示意圖

7.2 IP VPN 之建立

Passport VR-VR VPN 的建立步驟如下：

1. 在 IP VPN 中對每一客戶建立一虛擬路由器
2. 透過本公司網路連接在 IP VPN 內的客戶端虛擬路由器
3. 在每一客戶端 VPN 地區內規劃 IP 存取媒介
4. 規劃對該 IP VPN 的 IP COS
5. (可有可無)增加另一個 VPN 地區到現有的 IP VPN

在此狀況下，每一分配給客戶的虛擬路由器與在相同VPN的其他虛擬路由器相互連接，為了達到全部連接，Nortel建議在這些客戶端虛擬路由器間使用完全虛擬電路連接，但此建議並非必須的。

Passport VCG-based VPN 的建立步驟如下：

1. 在連接客戶端的每一 Passport 節點建立一 VCG
2. 透過本公司網路連接這些 VCG
3. 在 VPN 地區規劃客戶端虛擬路由器
4. 在客戶端虛擬路由器間規劃 PTMP IP tunnel
5. 在 IP tunnel 輸出點間規劃路由散佈
6. 規劃被動式 OSPF 介面
7. 規劃客戶存取介面
8. 規劃 IP 存取媒介

在此狀況下，每一分配給客戶的虛擬路由器與在相同VPN的其他虛擬路由器以PTMP tunnel的方式相互連接，VCG聚集了所有在Passport節點上的客戶訊務量並透過共通的骨幹網路連接出去。

7.3 IP VPN Class Of Services (COS)

圖7.4是Passport之COS示意圖，IP COS市透過電信業者在客戶端虛擬路由器的ingress port基於政策需求來執行IP訊息封包分類來達成的。分類法則包括：第二層分類、TOS分類、與流程分類。分類完成後可依IP訊息封包針對TOS/Diffserv欄位做標記，標記政策是由egress port來決定的。

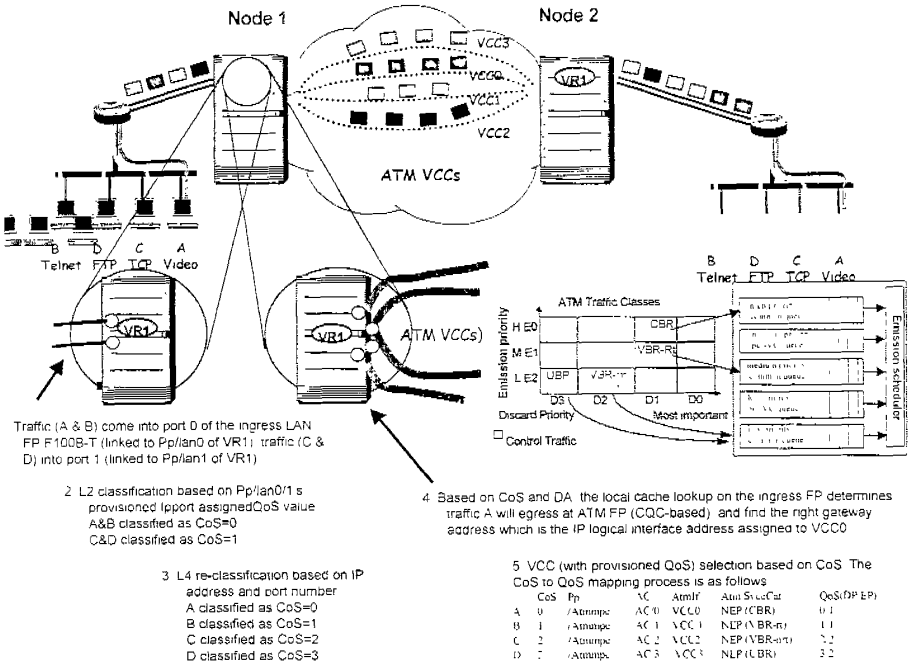


圖 7.4 Passport 7K/15K 之 COS 示意圖

基於服務應用、客戶指明政策、與Diffserv標記特性之Passport的COS支援兩種狀況：靜態(在第二層)與動態(在第三層)。靜態(在第二層)之IP COS對應如圖7.5所示，在此應用中經由frame Relay的DLCI或ATM的PVC透過客戶指明IP COS的方式連接CPE端的路由器與某一特定的VR。一如往常CPE端的路由器透過PVC或DLCI傳送訊息，一但訊息到達VR時，VR會依照客戶當初申請時對該PVC所定義之IP COS來對所接收到的訊息封包加以分類；所有透過PVC連接到VR的訊息封包將會對應到相同的IP COS，在骨幹網路中VCG的egress port的IP COS政策會定應如何將IP COS對應到ATM PVC或MPLS LSP上。

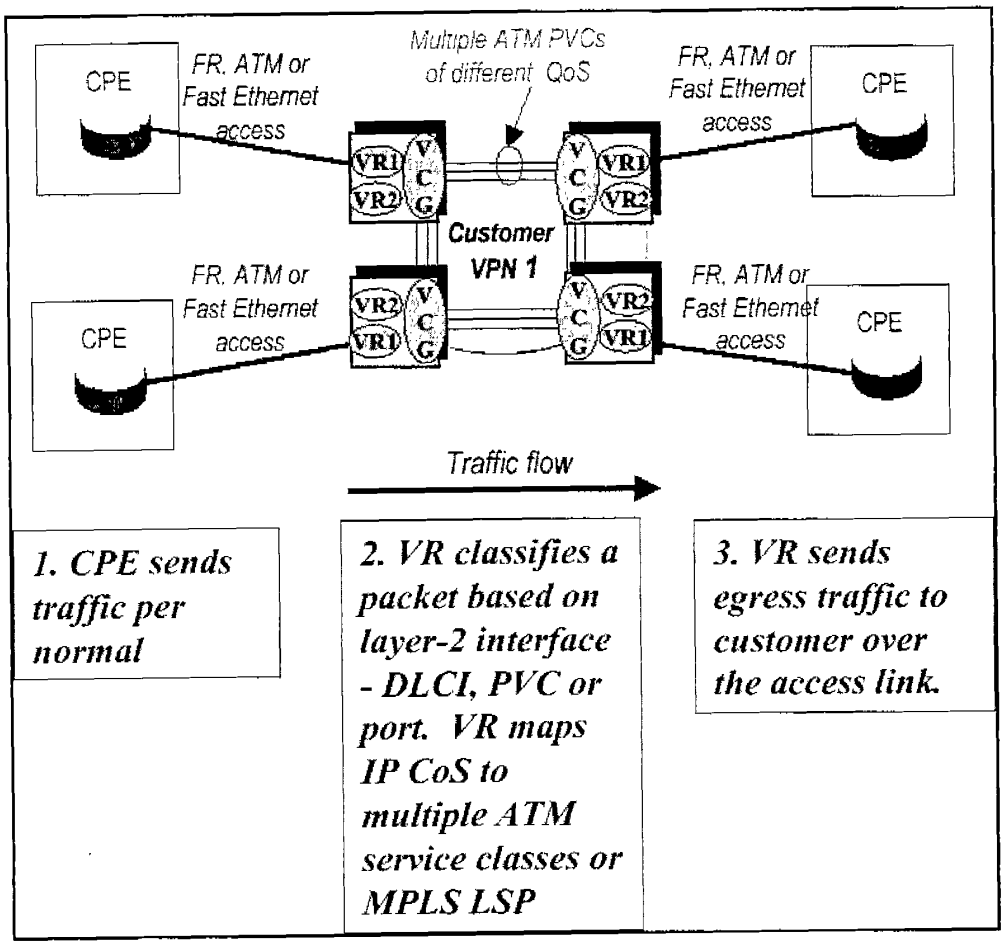


圖 7.5 靜態(在第二層)之 IP COS 對應

動態(在第三層)之IP COS對應如圖7.6所示，在此應用中，訊息封包可以動態地被識別或區分。有一些方法可用於分類，包括應用名稱、來源IP位址、目的IP位址、來源IP協定port、目的IP協定port、與CPE (路由器或主機)Diffserv欄位標記等方法可以使用。應用名稱可以在訊息封包中使用TCP/UDP port來識別例如使用TCP port 20來識別FTP訊息封包，也可以由port數目與IP位址組合來識別一特

定的flow。

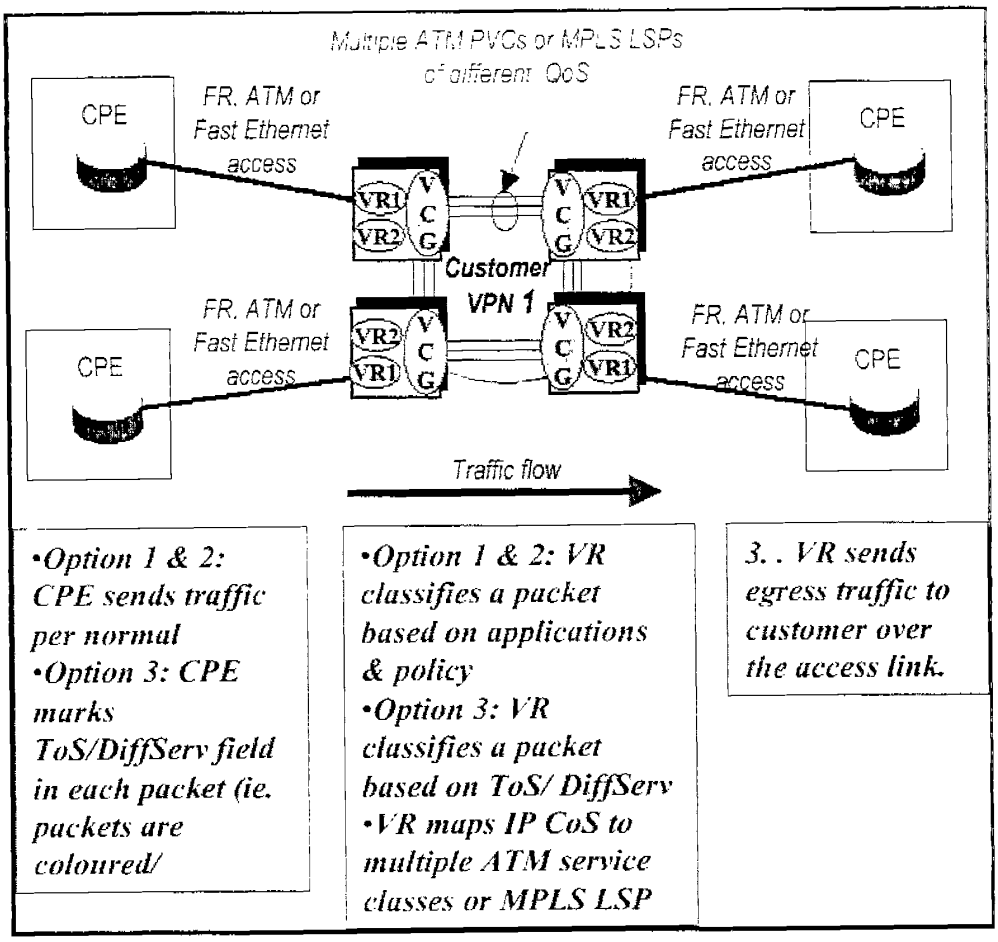


圖 7.6 動態(在第三層)之 IP COS 對應

7.4 Passport 之 IP VPN 支援狀況

Passport之IP VPN支援狀況分為三個階段，第一階段(2000年10月)提供以客戶端虛擬路由器(Virtual Router, VR)與專用虛擬電路為主(virtual circuit, VC)。如圖7.7所示，工作平台是Passport 7K；可提供IP COS、多重客戶端虛擬路由器、與對每一客戶擁有專用虛擬電路；軟體版本是R5.1與PCR 1.2；硬體卡版需要CP2卡、以PM2為

基礎的SBIC卡、CQC卡、與ILS forwarderd卡；客戶端存取支援IP over LAN(Ethernet)與IP over WAN(PPP、FRS、與ATM)；網路骨幹支援IP over WAN(FRS與ATM)；路由協定支援static/RIP/在CPE路由器與客戶端虛擬路由器間使用OSPF/在同一VPN內的客戶端虛擬路由器間使用BGP。

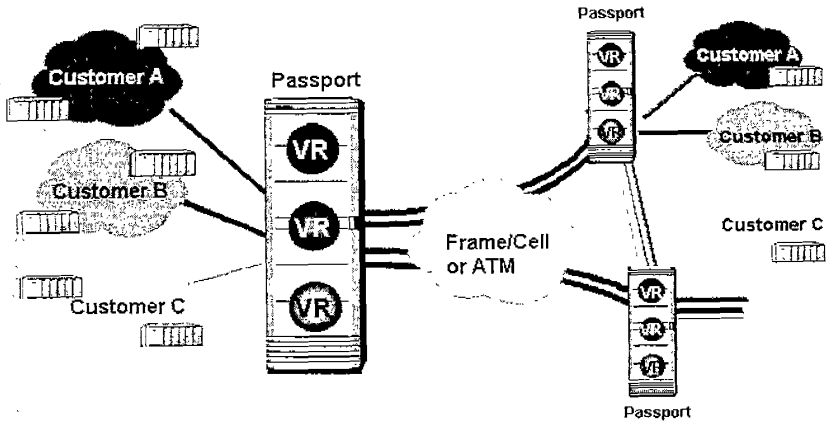


圖 7.7 以客戶端虛擬路由器(Virtual Router, VR)與專用虛擬電路為主之 IP VPN

第二階段(2001年1月)提供以VCG與PTMP tunneling為主。如圖7.8所示，工作平台是Passport 7K或Passport 15K；可提供IP COS、多重客戶端虛擬路由器、PTMP tunneling、與對所有客戶擁有共享虛擬電路；軟體版本是對Passport 7K是PCR1.3與PCR 2.0或更高版本，對Passport 15K是PCR 2.0或更高版本；硬體卡版對Passport 7K是需要CP2卡、以PM2為基礎的SBIC卡、ATM IP FP卡(PQC1.0/2.0)、與MSA32卡(PQC2.0)，對Passport 15K是需要CP3卡、以PM2為基礎的SBIC卡、ATM IP FP卡(PQC1.0/2.0)、與MSAS卡(PQC2.0)；客戶端存取支援IP over WAN(PPP、FRS、與ATM)、

IP over LAN(Ethernet)只支援在Passport 7K上 ；網路骨幹支援IP over WAN(FRS與ATM) ；路由協定支援static/RIP/在CPE路由器與客戶端虛擬路由器間使用OSPF/在同一VPN內的客戶端虛擬路由器間使用BGP(EBGP或IBGP)/在網路內所有VCG間使用IGP。

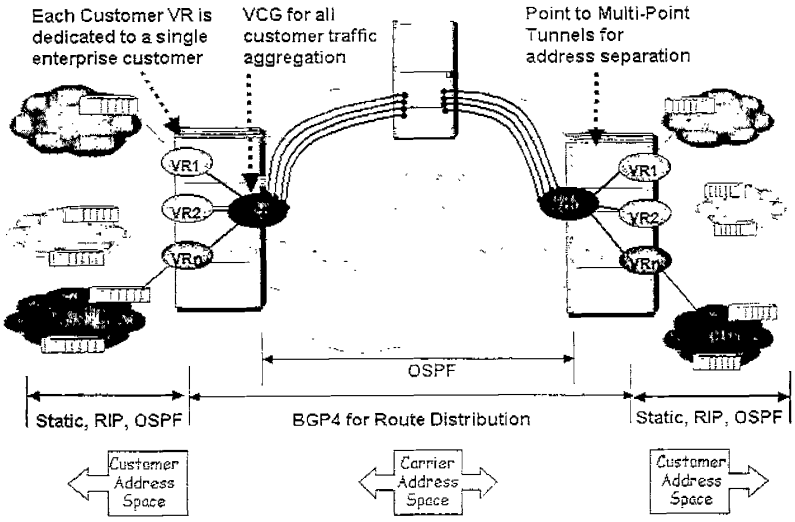


圖 7.8 以 VCG 與 PTMP tunneling 為主之 IP VPN

第三階段(2001年6月)提供以VCG與MPLS為主。如圖7.9所示，工作平台是Passport 7K或Passport 15K；可提供IP COS、多重客戶端虛擬路由器、PTMP tunneling、與對所有客戶擁有共享虛擬電路、MPLS；軟體版本是PCR 2.1或更高版本；硬體卡版對Passport 7K是需要CP2卡、ATM IP FP卡、與MSA32卡，對Passport 15K是需要CP3卡、ATM IP FP卡、與MSAS卡；客戶端存取支援IP over WAN(PPP、FRS、與ATM)；網路骨幹支援IP over WAN(FRS與ATM) ；路由協定支援static/RIP/在CPE路由器與客戶端虛擬路由器間使用OSPF/在同一VPN內的客戶端虛擬路由器間使用BGP(EBGP

或IBGP)/在網路內所有VCG間使用IGP。

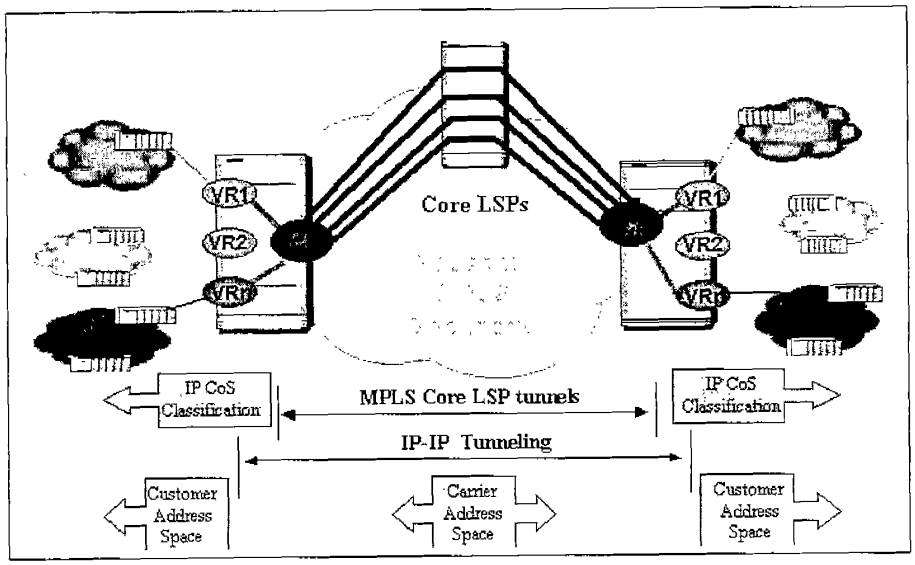


圖 7.9 以 VCG 與 MPLS 為主之 IP VPN

7.5 澳洲電信(Telstra)之 IP VPN 應用

澳洲電信之IP VPN應用服務稱之為Data Mode of Operation(DMO) ，其目的在發展一下一代具有可擴充性、高可靠性、與高保密性等特性的共通多重服務網路基礎建設。如圖7.10所示，IP VPN網路的主要元件是採用Nortel networks的Passport 7K、Passport 15K、與Shasta 5000所組合而成：主要需求是確定新的基礎建設可提供可變通性以滿足不斷改變中的用戶需求，同時確保營運成本保持最低與投資成本經由用戶成長而逐步增加。

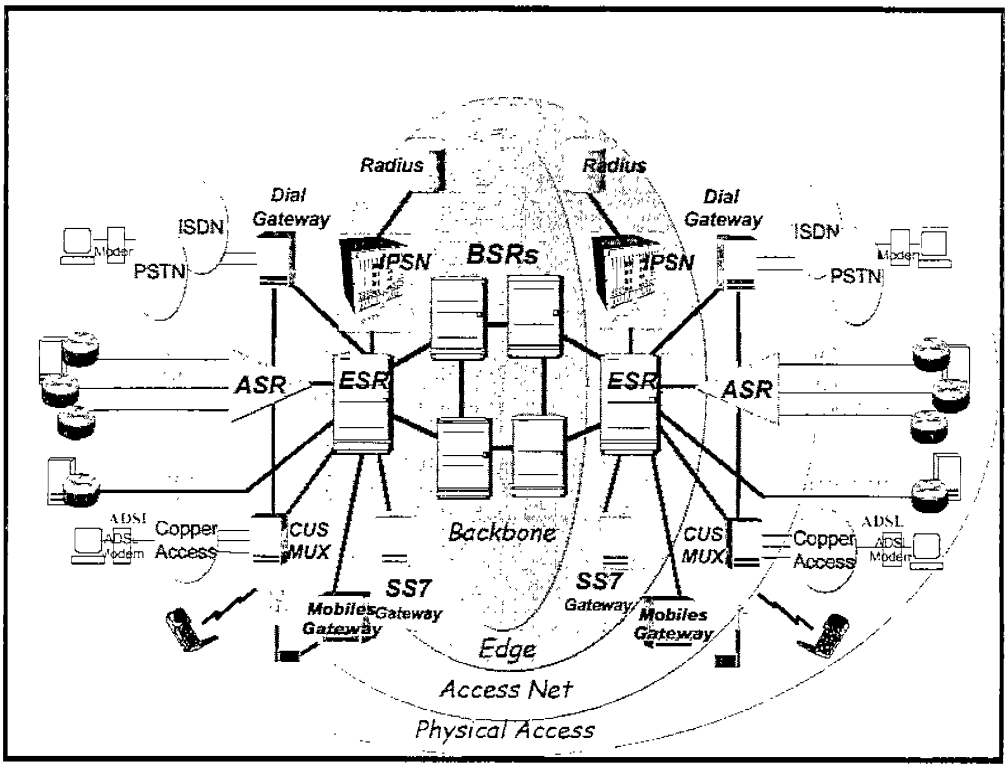


圖 7.10 Telstra 之 DMO 網路架構圖

共通DMO網路之功能性架構是由三種階層組合而成的，分別是Backbone、Edge、與Access。此階層式架構用以達成最大的可變通性、功能性、可擴充性、與可管理性之目的。DMO網路的Backbone層是採用Passport 15K作為Backbone Switch Router(BSR) ，在網路階層的最高層中這些BSR透過2.5Gbps與622Mbps的傳輸媒介相互連接。建設初期這些Passport 15K將以高速ATM SW為主，然而未來將支援高速IP路由與引進MPLS技術。

DMO網路的Edge層是由Edge Switch Router(ESR) 、IP Service Nodes(IPSNs)、SS7信號閘道器、與Radius伺服器所組成。建設初期ESR是採用Passport 7K但最後將視用戶訊務量成長而逐步汰換

至Passport 15K。IPSN是採用Shasta 5000以統一動態存取與提供虛擬IP能力來降低網路成本。DMO網路的Edge層是最複雜的一層，它提供複雜的IP特性、支援與接取網路和授權伺服器互相網路介接、和提供與PSTN網路間的信號網路介接。

DMO網路的Access層是由Access Switch Router(ASR)包含Passport 7K的Frame Relay與ATM接取與撥接閘道器提供撥接接取與ADSL接取之用戶多工器所組成。Access層提供網路中不同的接取服務的用戶聚集與集縮，當接取技術演進或新的接取技術成熟時，適當的接取閘道器將會建設在Access層。最後，實體Access層透過不同種類的傳輸媒介如銅線、光纖、無線、PSTN、ISDN、或ADSL來介接用戶設備。

8. Shasta 5000 BB-RAS 之 AAA 管理

8.1 Radius 通訊協定

Shasta 5000之用戶計費統計管理主要是與Radius 伺服器配合運作的，故首先必須要對Radius通訊協定有一基本認識。AAA 是Authentication、Authorization、Accounting 的簡寫。Authentication 就是一般我們講的身分辨認，通常就是檢查使用者帳號跟密碼；Authorization 就是將系統資源區分等級，要使用某種資源必須先得到相對應的授權，權限不夠時則無法使用；Accounting 就是記錄使用者使用的資源、時段，作為計費、收費的依據。

Radius伺服器可配合許多現有使用者認證技術。例如PPP的PAP(Password Authentication Protocol，密碼認證協定)技術、CHAP(Challenge Handshake Authentication Protocol，查問性握手驗證協定)、與SecurID記號認證系統。PAP較易使用，但安全性較低。在PAP協定中，使用者輸入未加密、文字格式的密碼至RAS；RAS將其加密後傳至RADIUS伺服器，RADIUS伺服器再將其解密，並將密碼與其資料庫進行比對。CHAP方式是RAS先請使用者證明自己的身份，方法是RAS先隨機產生一個隨機數字，並傳給使用者，使用者的PPP客戶端程式會用這一數字加密，產生一個摘要。這個摘要會先送給RAS，再轉送給RADIUS伺服器；接著RADIUS伺服器會用使用者正確的密碼，也換算出一個摘要。如果兩個摘要相同，表示宣稱自己是某使用者的人，已通過RADIUS伺服器的認證。SecurID記號認證系統，經由記號式(Token)的動態密碼技術，為因應不同等級認證需求，數位認證(Digital certificate)及認證機關(Certificate Authority，CA)；CA是一值得信賴的協力組織，而該組織則負責確認使用者的身份，CA同時也保存了數位認證及公開基鑰(Public encryption key)等資料。

Shasta 5000支援的標準Radius屬性資料如表8.1所示，而屬於

Shasta 5000特有的屬性資料則如表8.2所示。所有計費資料是儲存在Shasta 5000的非揮發性記憶體內並且經由Radius通訊協定再一固定的時間內傳送給Radius伺服器。Shasta 5000本身是扮演Radius客戶端的角色，它與Radius伺服器間的連接可以透過本地附接的Ehternet port(在CMC卡上) 或透過ATM PVC的方式進行。

Attribute Name	Num	Access-Response	Access-Request	Accounting Request START	Accounting Request STOP	Note	Release
User-Name	1	Maybe	Yes	Yes	Yes	Username@ispname or username only if trimdomain is selected.	1.1
User-Password	2	No	Yes	No	No	PAP password	1.1
Chap-password	3	No	Yes	No	No	Chap response	1.1
NAS-IP-address	4	No	Yes	Yes	Yes	ISP IP address	1.1
Service-Type	6	Yes	Yes	No	No		1.1
Framed-Protocol	7	Yes	Yes	No	No	PPP	1.1
Framed-IP-Address	8	Yes	Yes	Yes	Yes (2.0)		1.1
Framed-IP-Netmask	9	Yes	No	Yes	Yes (2.0)		1.1
Framed-MTU	12	Yes	No	No	No		1.1
Login-Ser	15	Yes	Yes	No	No	For telnet	2.0

vice					authentication	
Reply-Message	18	Yes	No	No	No	1.1
Framed-Route	22	Yes	No	No	No	The format should contain a destination prefix in dotted quad form, optionally followed by a slash and a decimal length specifier stating how many high order bits of the prefix should be used. We ignore any gateway address. For example: 129.3.3.0/24	2.0
State	24	Yes	Yes	No	No	Used for access-challenge	1.5
Class	25	Yes	No	Yes	Yes		1.1
Session-Timeout	27	Yes	No	No	No	Only for PPP user	1.1
Idle-Timeout	28	Yes	No	No	No	Only for PPP user	1.1
Called-Station-Id	30	No	Yes	No	No	Only for PPP/L2TP	2.0
Calling-Station-Id	31	No	Yes	Yes	Yes	The format of this field is: 4 bytes of	1.5

						hostname (truncated if hostname is longer than 4), 2 digits of slot, 1 digit of port, 3 digits of VPI, 5 digits of VCI. Total is 15 bytes. When the ppp session is over Ethernet, VPI and VCI field are both 0. When the ppp session comes in on a LNS, we use LAC's AVP.	
Acct-Status-Type	40	No	No	Yes	Yes		1.1
Acct-Input-Octets	42	No	No	No	Yes		1.1
Acct-Output-Octets	43	No	No	No	Yes		1.1
Acct-Session-Id	44	No	Yes (2.1)	Yes	Yes	Encoded as RFC 2138.	1.1
Acct-Authentic	45	No	No	Yes	Yes		1.1
Acct-Session-Time	46	No	No	No	Yes		1.1
Acct-Input-Packets	47	No	No	No	Yes		1.1
Acct-Output-Packe	48	No	No	No	Yes		1.1

ts							
Acct-Termination-Cause	49	No	No	No	Yes		1.1
Acct-Input-Gigawords	52	No	No	No	Yes		1.5
Acct-Output-Gigawords	53	No	No	No	Yes		1.5
Event-Timestamp	55	No	No	Yes	Yes		1.5
Tunnel-Type	64	Yes	No	Yes	Yes	Only L2TP is supported	2.0
Tunnel-Medium-Type	65	Yes	No	Yes	Yes	Only IPv4 is supported	2.0
Tunnel-Client-Endpoint	66	Yes	No	Yes	Yes	Ignored on BSN.	2.0
Tunnel-Server-Endpoint	67	Yes	No	Yes	Yes	Dotted IP address format	2.0
Acct-Tunnel-Connection	68	No	No	Yes	Yes	<Initiated-Tunnel-ID>-<Responder-Tunnel-ID>	2.0
Tunnel-Password	69	Yes	No	No	No	Max. Length 15 characters	2.0
Tunnel-Preference	83	Yes	No	No	No	Lower preference takes higher priority	2.0
Acct-Interim-Interval	85	Yes	No	No	No		1.5

Tunnel-Client-Auth-ID	90	Yes	No	No	No	Max. Length 32 characters	2.0
Tunnel-Server-Auth-ID	91	Yes	No	No	No	Max. Length 32 characters	2.0

表 8.1 Shasta 5000 支援的標準 Radius 屬性資料

Shasta Vendor Id is 3199.

Attribute name	Num	Access-Response	Access-Request	Release	Comments
User Privilege	1	Yes	No	1.5	Used to specify the user privilege level for telnet users. It is an integer with three values possible values: 0: user privilege 1: super-user privilege 2: super-super-user privilege
Service Profile	2	Yes	No	2.0	Used to specify which pre-configured service profile should be applied to the subscriber
VPN Name	3	Yes	No	2.0	Used to specify which VPRN the subscriber belongs to.

表 8.2 Shasta 5000 特有的屬性資料

8.2 負載分擔與備份

Shasta 5000使用時可定義一串的Radius 伺服器，依照排列的先後次序決定優先順序。Shasta 5000首先送出AAA需求給主伺服器(編號為0)，假如在時限到時未得到回應，Shasta 5000會嘗試再次發出需求給主伺服器，如仍舊未在時限內得到回應，Shasta 5000則會嘗試送給備份伺服器，此過程將會持續下去直到下列事件之一

發生為止：

1.Shasta 5000從其中一個Radius 伺服器中得到回應

2.到達Radius伺服器所設定的最大重新嘗試次數(通常是3)

換言之，一但送給Radius 主伺服器的需求超過時限時，即會在次伺服器(編號大於0)中啟動輪詢機制，一直到最大重新嘗試次數到達為止。

Shasta 5000對於多重Radius 主伺服器則額外支援負載分擔機制。Shasta 5000可規劃使用多個Radius 主伺服器(編號為0) ，目前可使用的限制是8個主伺服器。假如在Radius的定義中使用多個Radius 主伺服器與次伺服器時，Shasta 5000將會在主伺服器使用負載分擔與次伺服器間使用輪詢機制並用於選擇適當的Radius伺服器。舉例來說，假設規劃使用三個主伺服器(編號為0)—PA,PB,PC與兩個次伺服器—SA, SB。當Shasta 5000發出需求時，首先會送給PA，如先前所述在開始嘗試次伺服器SA與SB之前會再發出第二次需求給PA；第二次當Shasta 5000發出需求時則轉由PB來服務，同理在確定PB故障後才會嘗試次伺服器SA與SB；第三次當Shasta 5000發出需求時則轉由PC來服務，如此巡迴下去成為負載分擔。

上述機制的例外條件是當STOP需求(session STOP或tunnel STOP) 產生時，Shasta 5000的AAA機制中將嘗試送STOP需求給與當初發送START需求相對應的伺服器。同時將處理下列狀況：

1. STOP需求可對應到與當初發出START需求相符合的伺服器，但卻得不到伺服器的回應。此時，將立即使用輪詢機制傳送STOP需求給下一個伺服器。

2.當Shasta 5000接收到STOP需求時，找不到相對應符合的伺服器。此時，Shasta 5000將提供負載分擔與輪詢機制並開始傳送STOP需求給主伺服器。

8.3 位址分配

在Shasta 5000內每一ISP可有一內定的sgroup與許多次要的sgroup，每一sgroup由許多不同範圍的位址構成的位址區(address pool)所組成。每一用戶通常分配給一個sgroup，並使用該sgroup所定義的位址區。在該位址區內，第一個定義的位址範圍總是首先被使用；在尚未使用完第一個定義的位址範圍之前，其餘定義的位址範圍是不被允許使用的，且使用法則並非使用者可以決定的。假如某一位址使用完畢並釋放出來，該位址將會放在分配區的最後面，如此一來，每次用戶簽入時得到的位址都會與前一次不同，即使在此期間並無其他用戶簽入時亦同。

8.4 Radius 切斷(Disconnect)

Shasta 5000內定將從radius伺服器UDP port 1700中接收Radius切斷訊息。當使用此功能時，Radius伺服器扮演session切斷的起始者(initiator)的角色。Radius伺服器可以指定一特定的Session Id或IP位址切斷Shasta 5000中的某一特定session，如果在其中指明某一用戶名稱則會將Shasta 5000中刪除與該用戶相對應之所有session。目前，Lucent/Ascend與Alcatel的Radius伺服器產品支援此一功能；本公司所買的Radius伺服器是lucent的NavisRadius，該軟體係同型產品中功能最完備，效能最佳的系統，該軟體採用Java script方式撰寫，可隨使用者需求自行修改並增加新功能，故可支援此功能。為了滿足此功能，Shasta 5000需設定：

1. Radius 設定中需將"Enable disconnect" flag 設定成"ON"
2. 切斷需求必須從 Radius 設定中的某一 Radius 伺服器中啟動

假使沒有滿足以上的狀況，此需求會被視為未經授權且該特定

的session不會在Shasta 5K中被刪除掉。在Radius伺服器端與客戶端(Shasta 5000)中交換的訊息是使用三個新的Radius碼(Ascend的專用碼)—40(Disconnect Request),41(Disconnect ACK))與42(Disconnect NAK) ；假使session成功的在Shasta 5000中被刪除掉，客戶端會發出ACK給Radius伺服器；否則，客戶端會發出NAK給Radius伺服器。

9. 實習心得與建議

- Shasta 5000寬頻服務節點的引進，配合ATM骨幹網路及接取網路的建設，將可以開發新的服務，藉以擴大市場，增加營收，滿足用戶需求。而新服務的開發應具創造性和使用者需求與生活習性相關，具有市場發展潛力，符合寬頻，跨網路整合、個人化及企業化服務的特性，結合本公司的既有網路優勢，提供個人化、套裝式的服務，讓用戶可以自行控制、管理自己的服務設定；提供Any2Any，不拘任何型式的通信型態；提供無所不在的服務，讓用戶可以透過任何的終端設備取得個人的通信服務。
- 在面對未來固網業者的競爭下，本公司提供給客戶的服務也要不斷的推陳出新才可在市場上取得領先的地位。IP VPN 是本公司的利器之一，本公司應隨時注意此技術的最新發展趨勢，擬妥相關對策，同時積極培育相關規劃、建設、與維運人才，並及早規劃與推出在此骨幹網路架構下的新服務諸如 MCS、WCS、與 UMS 等以因應未來更嚴峻的挑戰。
- IP VPN 是本公司提供相當於專線網路服務給客戶但實際上卻是使用共享的公眾骨幹網路的一種管理性的 IP 服務。Passport ATM SW 是本公司在提供 IP VPN 服務中所採用的設備，它不但可以讓本公司提供給客戶多重選擇的 IP 服務，也可與 Shasta 5K 結合在一起提供企業網路連接、Network Address Translation(NAT)、防火牆、加密/解密等先進的 IP 服務。
- 寬頻網路設備大部份都是 Data Com 產品，目前較無法做到百分之百的穩定性(如 Active/Standby 設計，當 Active Fail 而切換至 Standby 時，或多或少都會有一些 Out-Of-Service 狀態)，其維運機制亦不如交換機般之嚴謹(如 Diagnostic 及 Trouble Shooting 方面)，但若運轉異常或當機時，其影響所及卻較交換機嚴重許多，因此寬頻網路之維運工作是絕對不能忽視的。縱使目前寬頻網路

之維運有上述不盡完美之處，但仍應面對並予以克服，及早培育相關之維運技術與人才，備足所需之維護用料(或與廠商簽訂維護合約)，引進必要之測試工具與儀器，更重要的應積極培訓寬頻應用服務之開發人才(或以策略聯盟方式辦理)，期能在各相關單位之群策群力下，使得寬頻網路之建設、維運和應用服務之推展能順利圓滿。