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)

實習「專戶公司內部網路通信服務之整體需求規劃」報告書

服務機關：中華電信股份有限公司
中華電信股份有限公司
中華電信股份有限公司北區分公司
中華電信股份有限公司中區分公司
中華電信股份有限公司南區分公司

職　　稱：副工程師
副工程師
助理工程師
科長
科長

出 國 人：謝明璋
李憲慧
李俊傑
張坤昌
林來興

出國地點：美國

出國期間：89 年 11 月 15 日至 89 年 11 月 24 日

報告日期：90 年 02 月 19 日

—摘要—

由於網際網路的蓬勃發展及多媒體等應用服務的快速成長，企業為快速反應經營環境的變化，必須藉由網路科技的運用，改造既有經營模式與作業流程，來強化市場競爭力。電信業者也勢必要和企業客戶一起定義需求、規劃，量身訂製一個可以創造企業價值的網路，方是在這競爭的市場中，吸引新企業客戶、穩定老企業客戶的致勝之道。

此次奉派前往美國著名電信與系統公司，實習新一代 IP 寬頻網路之虛擬專用網路建置技術、IP 應用服務、市場趨勢、及相關產品等資訊，值此快速變遷的環境下，俾有助於為本公司專戶規劃符合其通信整體需求的專用網路。

本報告先針對專戶公司的通信服務需求面作一探討，接著說明其內部網路建置之整體規劃，主要涵概虛擬專用網路的演進、設計技術與考量、建置方式、以及服務應用層面考量等。

—目次—

壹、前言 1

貳、實習行程 2

參、專戶公司內部網路通信需求之探討 3

一、業者競爭之主要市場 → 專戶公司內部網路通信 3

二、專戶公司內部網路通信型態 3

三、專戶公司內部網路結構演變趨勢 5

四、其他事項 8

肆、專戶公司內部網路之建置規劃 9

一、不同市場不同需求 9

二、何謂虛擬專用網路 12

三、虛擬專用網路市場 13

四、專戶公司內部網路發展趨勢 15

五、VPN 網路設計技術 18

六、VPN 網路設計考量 22

七、VPN 網路建置方式 25

八、VPN 整體服務之規劃 29

伍、感想與建議 31

陸、附件參考資料 32

一、The Shasta 5000 BSN Applications 32

二、Nortel Networks Network-Based IP-VPN Solutions 46

三、Getting Ahead of the Networking Curve 49

壹、前言

職五人奉派前往美國實習「專戶公司內部網路通信服務之整體需求規劃」，承蒙北電網絡 (Nortel Networks) 及思科系統 (Cisco System) 等二家公司妥善安排，得以有系統的研討新一代 IP 寬頻網路之虛擬專用網路(Virtual Private Network, VPN)建置技術、IP 應用服務、市場趨勢、及相關產品等資訊，值此快速變遷的環境下，俾有助於為本公司專戶規劃符合其通信整體需求的專用網路。

由於網際網路的蓬勃發展及多媒體等應用服務的快速成長，企業為快速反應經營環境的變化，必須藉由網路科技的運用，改造既有經營模式與作業流程，來強化市場競爭力。依一般市調分析，企業對通信的期望主要是求改善內部通信和資訊分享以提高生產力、降低使用網路的通信成本、改善內／外部通信整合等方面著手；至於對電信服務的需求，將會有大量資訊傳送的頻寬要求；在資訊傳輸上，會要求保持暢通或是提供備援解決方案等可靠度；對於語音、數據、影像及各種系統的整合，則是需要保持服務應用的彈性與多樣性，並能提供企業內／外(Intranet／Extranet)的網路通信架構、電子商務平台、跨國通信等加值服務。由此窺知，電信業者勢必要和企業客戶一起定義需求、規劃，量身訂製一個可以創造企業價值的網路，方是在這競爭的市場中，吸引新企業客戶、穩定老企業客戶的致勝之道。

本報告的內容將先針對專戶公司的通信服務需求面作一探討，接著說明其內部網路建置之整體規劃，主要涵概虛擬專用網路的演進、設計技術與考量、建置方式、以及服務應用層面考量等，最後提出此行的感想與建議。

貳、實習行程

日　期	參 訪 單 位 與 實 習 項 目
11 月 15 日	往程，由台北飛往舊金山
11 月 16 ~ 18 日	娮參訪 Nortel Networks 位於 Santa Clara 之 IP Services Business Unit，研討： 鴱企業網路發展趨勢通信需求。 浑寬頻網路 IP VPN Services。 涋寬頻 IP 網路主力產品 Shasta 5000 Broadband Service Node (BSN)介紹。 (4)參觀 IP VPN Services 展示中心。 姶參訪 Nortel Networks 位於 Newark 之 Broadband Access Business Unit，研討： 鴱數位用戶迴路(DSL)市場趨勢。 浑寬頻接取網路主力產品 Universal Edge Intelligent Multiservice Access System (UE IMAS)介紹。
11 月 19 ~ 22 日	娮參訪 Cisco Systems 位於 San Jose 之 Executive Briefing Center，研討： 鴱 IP VPN for Enterprise Business Model。 浑 Content Delivery Network。 涋 Internet Data Center Business Model。 涤參觀 Internet Home Briefing Center。 姶參訪 Cisco Systems 之策略聯盟廠商 AboveNet 公司之 IDC 展示中心。
11 月 23 ~ 24 日	返程，由舊金山飛回台北

參、專戶公司內部網路通信服務需求之探討

一、業者競爭之主要市場 → 專戶公司內部網路通信

根據 Infonetics 市調公司所作調查結果，預測至 2001 年將超過 40% 的企業計劃利用虛擬專用網路(Virtual Private Network，VPN)的所有應用；另外，依 Yankee Group 公司所作調查結果，預測至 2003 年有 70% 的企業會利用 VPN 提供超過 90% 的數據通信。由上述的市場調查數據顯示，企業內部網路通信必是各電信業者急欲爭取的對象。

隨著全球電信自由化風潮興起，政府加快開放電信業務之腳步，電信服務市場逐漸由傳統的獨占，轉變為開放競爭；而專戶通信收入原本為本公司主要營收來源，現今面對三家民營業者加入固網市場行列，尤其將面臨固網業者急欲切入的強烈挑戰，如何整合語音、數據、視訊、與多媒體等服務，提供本公司專戶一完善、整合性高、多重服務網路功能整合之良好通信環境，是為本公司當前首要工作。

二、專戶公司內部網路通信型態

專戶服務著重於企業內部專有網路之規劃，以提供高頻寬、多點與多元化網路之應用，整合終端設備並提昇網路效益，提供企業虛擬網路電子商務專線服務與寬頻接取等整合性服務。

專戶公司內部通信包括有四種典型的應用，請參考圖 3-1：

芘遠端存取

企業公司為了提供機動性高之業務人員出差（國內、國外）、通訊量不多且連線時間不長之辦事處、或在家上班等員工可經由撥接方式遠端存取企業網路內部資源，員工透過公司通信網路而不

需打長途電話或付費專線回總公司，這方式可以幫公司省下大筆的開銷。

芧與分公司連線

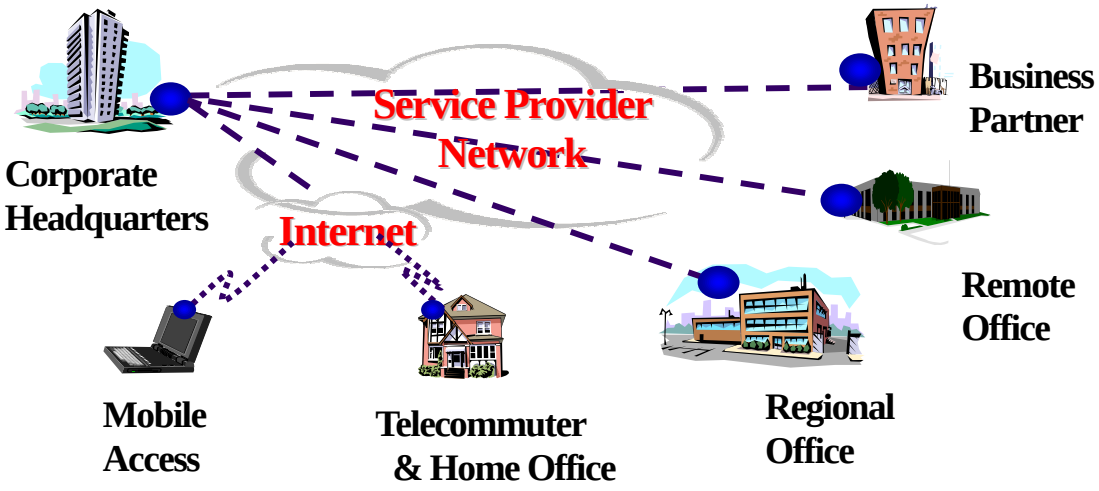
就是據點對據點的連線(Site-to-Site)，連接企業總部、各分公司、或遠端辦事處間通訊，達到私有網路之特性。

茩 Extranet 的應用

透過存取控制與身份辦認服務，來認可或拒絕客戶、交易伙伴或關係企業，判定其是否能存取生意上所需用到的特定資訊。

苜上網存取

除了公司內部網路通信環境外，仍能使用網際網路的服務。

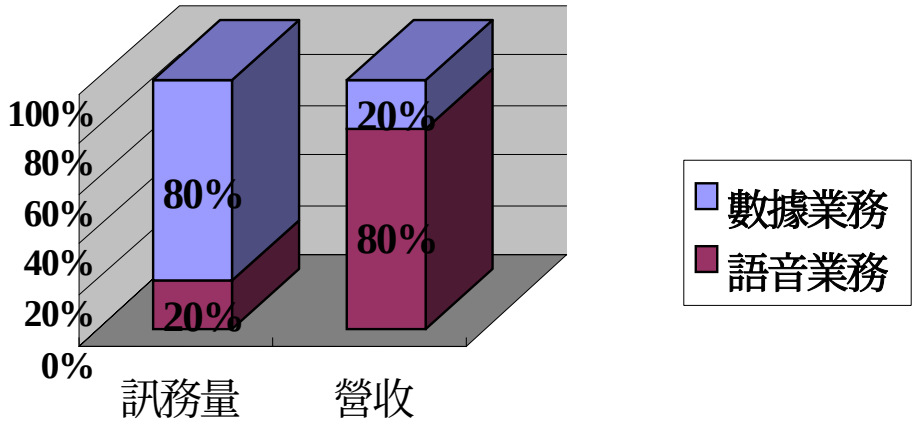


【圖 3-1】專戶公司內部網路通信對象

三、專戶公司內部網路結構演變趨勢

壵網路寬頻化

由於網際網路蓬勃發展造成數據業務快速發展，傳統電話業務與數據業務的服務將有革命性轉變，數據業務之訊務量將遠超過一般語音業務，依據北電網絡(Nortel Networks)公司之研究報告，在訊務量方面百分之八十來自數據業務，百分之二十來自語音業務，營收部分則反之，語音業務佔百分之八十，數據業務佔百分之二十，詳如圖 3-2，在此資訊快速起飛時代，如何快速傳遞資訊、獲得資訊、管理資訊與應用資訊，已成為企業競爭決勝之關鍵，因此高頻寬、穩定性佳、與保證服務品質之寬頻網路服務已為下一代網路(Next Generation Network，NGN)規劃趨勢。



資料來源：Nortel Networks (DEC 15 1999)

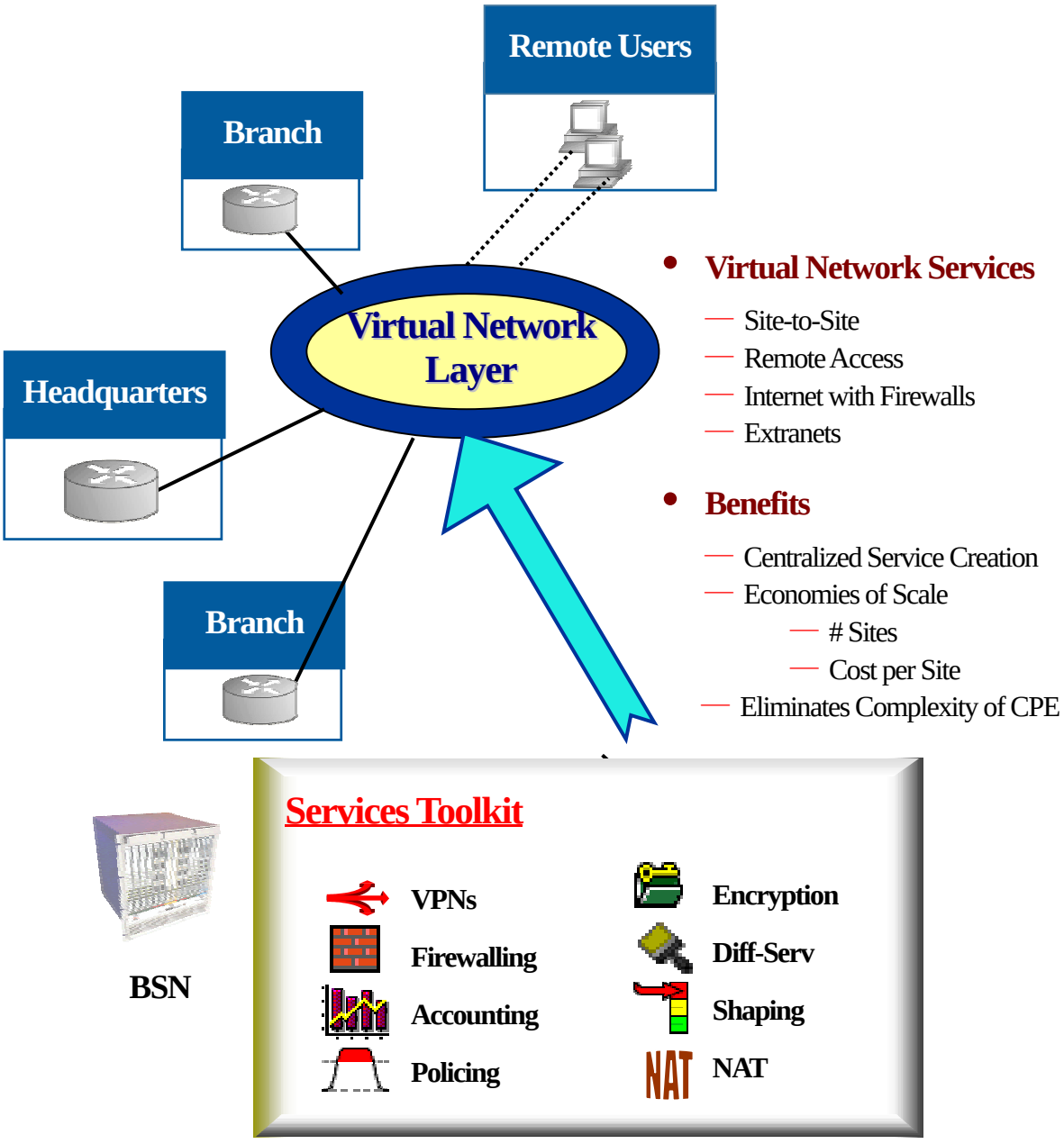
【圖 3-2】語音與數據業務訊務量與營收比較表

芧網路虛擬化

以往專戶建置該公司企業通信網路均採用數據專線(Leased Line)方式，透過向電信公司申裝數據專線及購買相關的通訊設備(如路由器等)，建構屬於自己的專用網路，可擁有較佳的安全性、效能、可靠度、及靈活的網路使用權；然而相對地必須付出較昂貴的營運成本，同時網路的備援性、加值服務提供也相對薄弱。

有鑑於數據傳輸需求日益增加，電信公司除提供數據專線建置服務，亦開始建構包括 X.25、訊框傳送(Frame Relay)、網際網路(Internet)、與非同步傳輸模式(Asynchronous Transfer Mode，ATM)等公眾數據網路供客戶選用，這種公眾數據網路除建設費、月租費較低廉外，更具有服務項目多樣化、備援性佳等特點。因此越來越多的企業為了在降低成本、提昇競爭力的前提下轉而使用公眾數據網路，不再租用長途數據專線來建構公司專用網路。

在公眾數據網路上透過指配固定的通道，可建構屬於企業的專有通信網路，由於在實體上，並無個別企業專用電路，而是大家共享，因此，虛擬專用網路的概念即應運而生。而北電網絡(Nortel Networks)公司所研發的智慧主力產品 Shasta 5000 BSN (Broadband Service Node)，是致力於使網路虛擬化的一個典型產品，其所提供的服務與效益如圖 3-3 所示。



【圖 3-3】網路虛擬化示意圖

四、其他事項

艽通信品質

—瞭解據點分佈情況。

—瞭解服務接續需求，包括稽延時間(Latency)、效能(Performance)、及障礙復原時間。

—瞭解服務等級(Class of Service，CoS)需求。

—瞭解備援(Backup)計畫。

—高訊務量據點之負載平衡措施(Load Balancing)考量。

—瞭解建置、營運之成本預算。

芧安全策略

—提供行動用戶、遠端存取用戶之身份驗證(Authentication)及授權(Authorization)方式為何。

—據點之間設備交換資料前如何認證。

—重要資料在傳輸過程要如何加解密(Encryption & Decryption)，密鑰(Key)如何管理。

—有防火牆(Firewall)功能需求？要如何規劃？

茎管理策略

—如何提供一個可支援控制網路服務之單純化的維運管理策略或準則。

—要自行管理或委外(Outsourcing)管理。

肆、專戶公司內部網路之建置規劃

一、不同市場不同需求

企業依其本身的規模大小、分散據點多少、通信型態等會有不同網路建置規劃，圖 4-1 是針對美國企業建置其網路的市場分析，大致可歸類為下列兩種類型。

艼大企業—少數客戶群

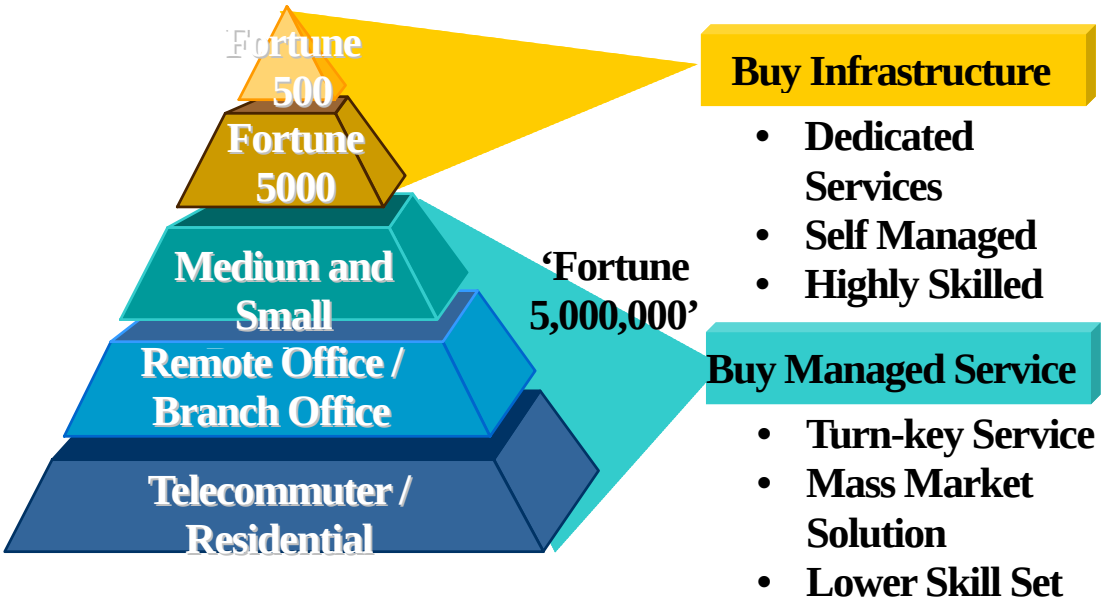
娮建置專用企業網路提供專屬服務，可以同網／異網(On-Off Net)擷取服務。

娮擁有技術層次較高的專業人員，可以自行管理網路。

婓擁有自己的 PBX 系統。

芧中小企業—多數客戶群

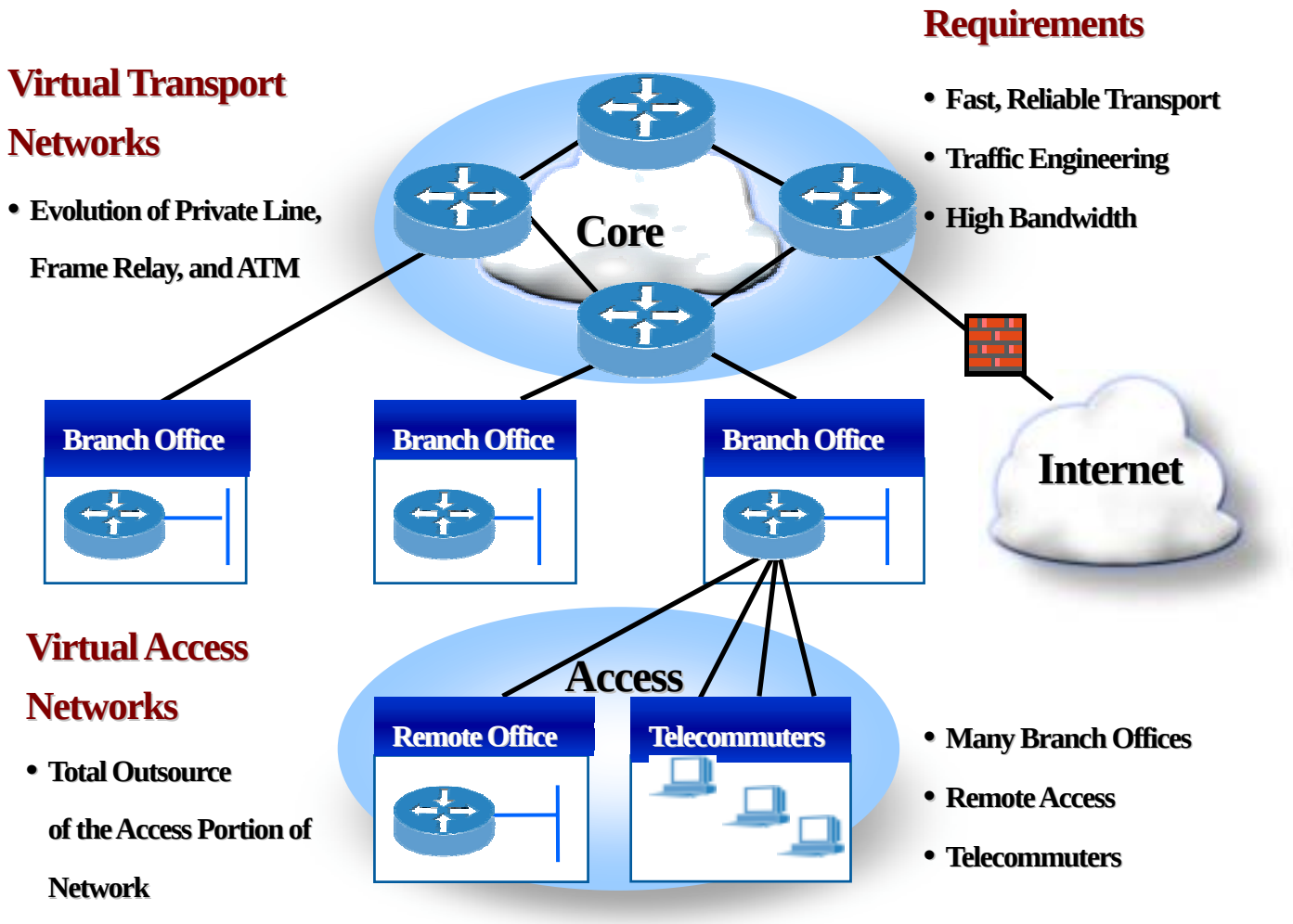
本身不具有高層次的專業技術人員，大致採取購買電信業者公眾網路(如 PSTN/Centrex 系統)現有大眾化解決方案之管理服務。



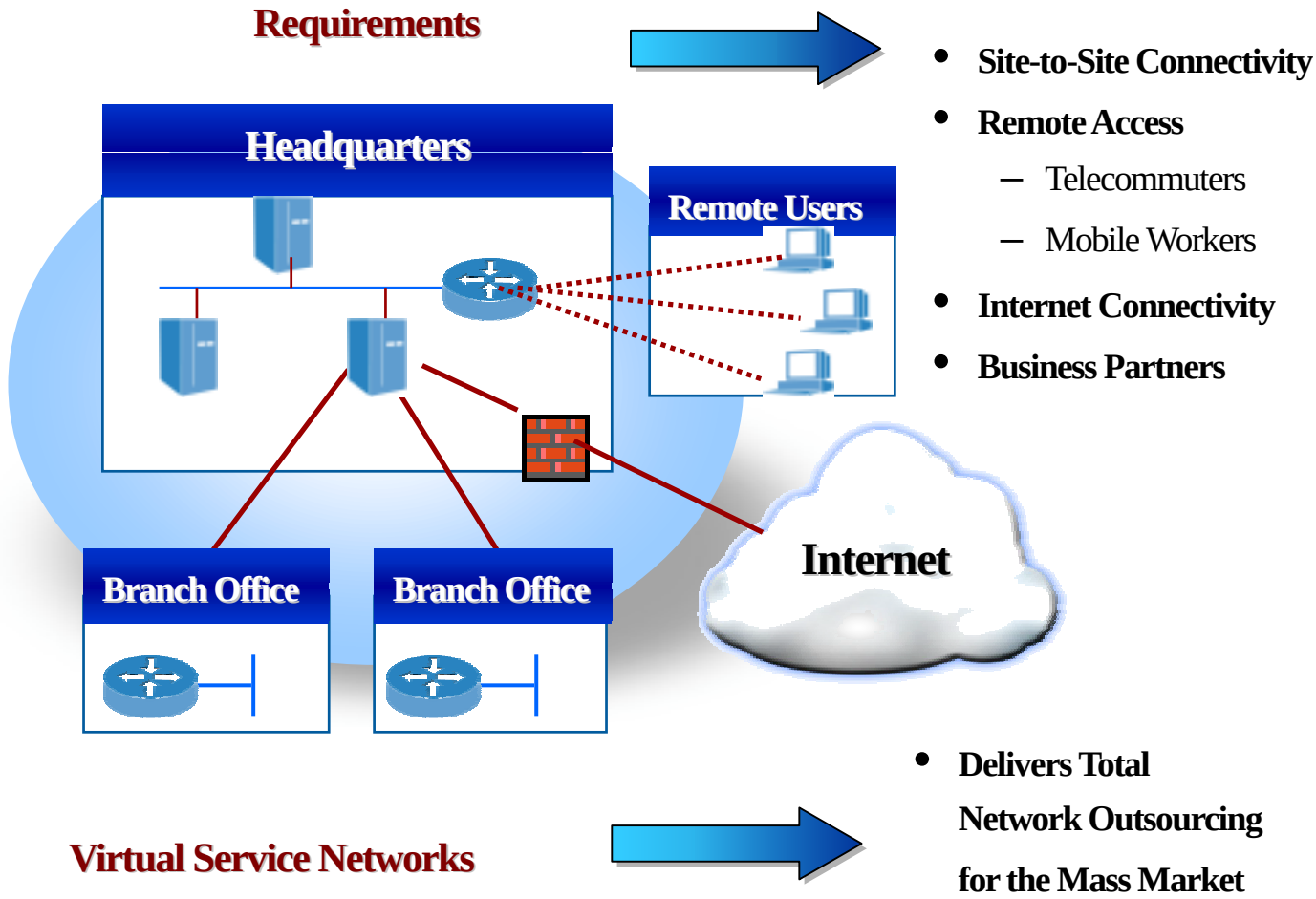
【圖 4-1】企業網路建置的市場結構

圖 4-2 是大企業建置其網路的示意圖。

圖 4-3 是中小企業建置其網路的示意圖。



【圖 4-2】大企業網路示意圖



【圖 4-3】中小企業網路示意圖

二、何謂虛擬專用網路

虛擬專用網路(Virtual Private Network, VPN), 就是“ 在公眾網路上建立屬於自己企業公司內部的專有網路“ 。也就是說, 不再使用長途數據專線建立公司內部通信網路, 而是在網際網路或其他公眾數據網路上, 為自己的企業量身訂做一個最符合自己需求、自己可以控制的網路, 透過這專用網路, 可以安全地傳送私人資訊。企業採用 VPN 網路規劃可以節省昂貴的出租專線費用及網路基礎建設成本。

目前推出的VPN種類繁多, 有在智慧型網路(Intelligent Network, IN)上建置純語音的IN VPN, 有使用在行動領域的MVPN, 及有以數據為主的CPE VPN等。然因網際網路的蓬勃發展, IP儼然成為未來下一代網路的共通語言, 服務提供者莫不積極建置IP寬頻骨幹網路、接取網路、用戶端網路與應用軟體等, 然後企業可在此公眾網路架構上透過下層共享資源而非使用個別專屬的實體線路及通訊服務, 利用 IP 設備來建置具有資料私密與安全性、獨立的定址空間與路由能力、並於其上提供具私有性 IP 服務之IP VPN。

三、虛擬專用網路市場

如前一章節所述，企業內部網路通信是各電信業者急欲爭取的對象，但是到底虛擬專用網路市場商機有多大？下面是幾家公司所作的市場預測，雖然數據顯示結果差距頗大(可能預測包括軟、硬體設備及提供的服務之切入點不同)，但也不失參考價值。

芘依據 IDC1999 年 3 月的報告，VPN 市場到公元 2002 年將達 7 億美元。

芧 Dataquest 甚至更樂觀預測至 2001 年 VPN 市場將達 8.986 億美元，詳表 4-1。

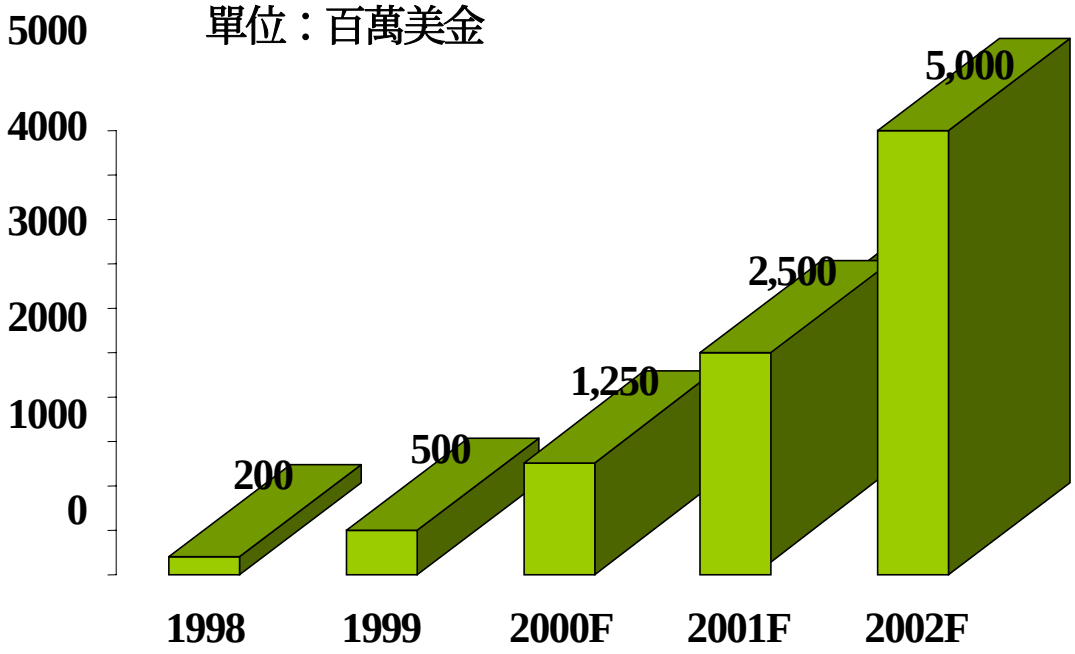
單位：百萬美金

年 項 目	**1998**	**1999**	**2000**	**2001**
營收	**114.9**	**358.4**	**603.7**	**898.6**
年成長率		**312%**	**168%**	**149%**

資料來源：Dataquest (1999 年 7 月)

【表 4-1】1998-2001 年 VPN 市場預測

茎 Fuji-Keizai 預測美國至 2002 年 IP VPN 市場將達 50 億美元，詳圖 4-4。



資料來源：Fuji-Keizai USA (1999/08)

【圖 4-4】美國 IP VPN 市場規模預測

四、專戶公司內部網路發展趨勢

由於寬頻網路已是現行通訊網路的基礎，而且企業競爭優勢也已從製造、財務管理之爭，移轉到高效能的企業專用網路科技戰，並積極規劃、建置網路以提昇公司營運效益，創造公司新市場機會，因此企業建置其內部網路主要視當時技術成熟度有下列方式。

芷傳統企業專用網路—目前主流

娮數據專線網路

在總公司與各分公司間採用專線建構專戶公司內部企業網路，每個據點均需有路由器(Router)、DTE、DCE 等設備。

姶非同步傳輸模式(ATM)／訊框傳送(Frame Relay)網路

骨幹網路採用 ATM／Frame Relay 網路，接取網路部分採用專線或非對稱數位用戶迴路(Asymmetric Digital Subscriber Line, ADSL)，其主要特性有：

皰可提供端點對端點之頻寬保證 QoS。

浧藉由固接式虛擬線路(Permanent Virtual Circuit, PVC)提供VPN間之區隔，一般可不需另外對資料加密。

淯必須在Frame Relay／ATM PVC、或ATM SVC(Switched Virtual Circuit)上建置VPN，網路架構受限。

涋ATM SVC有擴充時效(Scalability)問題。

泌使用者變動時(加入、退出、及移動)，須對所有端點設定，使得設定維護PVC耗時。

浮服務提供者只提供網路第二層虛擬線路(Virtual Circuit，VC)，使用者需自行設定路由表(Routing Tables)，服務提供者不

易提供加值服務。

芧 IP VPN 網路—未來趨勢

隨著網際網路快速發展，網路 IP 化已成為趨勢，未來可能是”Everything is over IP”，透過 IP 可以立即與世界上任何一個使用網際網路的單位連結。是故電信網路與電腦網路將整合成單一 IP Based 寬頻網路，而現有的電信網路都可以介接至 IP 寬頻網路上。利用 IP 設備來建置 IP VPN 網路是不可避免之發展趨勢，未來企業網路將是建構在 IP 寬頻網路上擁有自主權的私有專用網路，而非 Frame Relay 或 ATM 等提供固接式虛擬線路(PVC)服務的網路。

圖 4-5 是企業引入傳統 VPN 與 IP VPN 費用比較，其實採用 IP VPN 通訊除了成本降低外，尚有其他顯著效益，下列列出主要好處。

娮營運成本降低，包含

—設備建置成本。

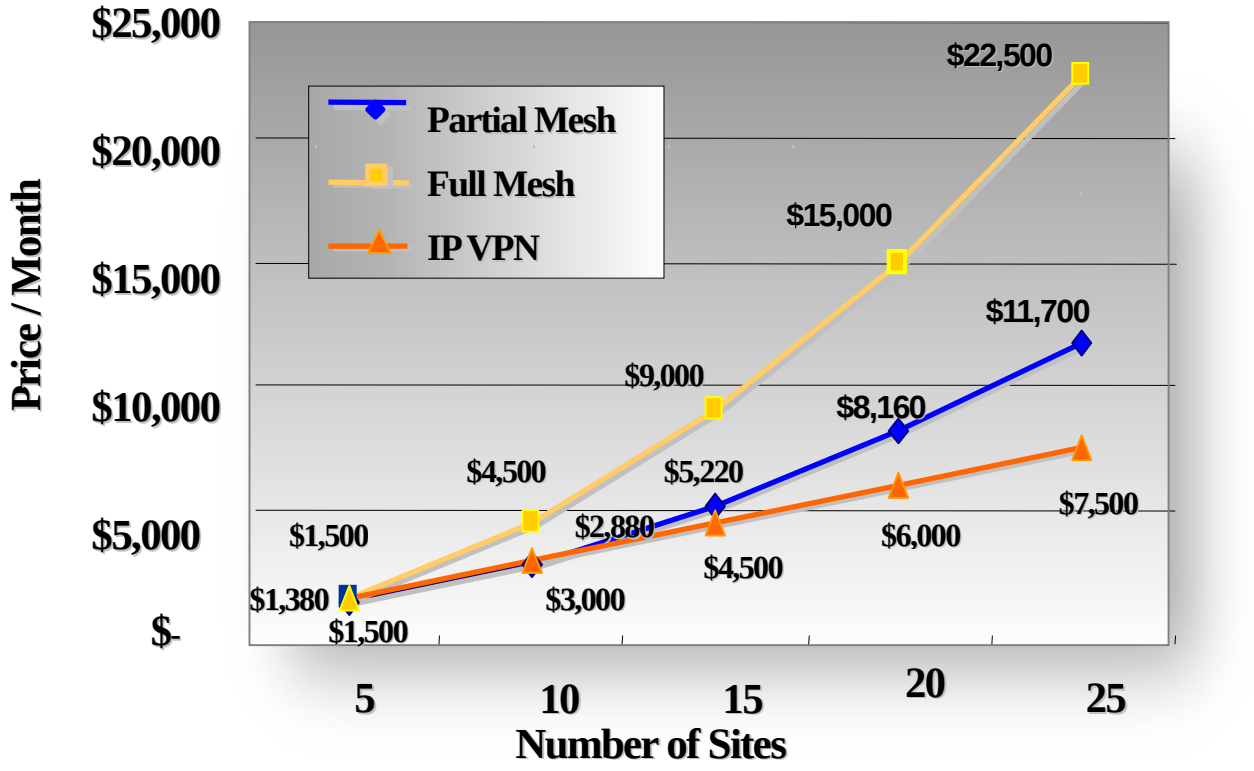
—網路維護成本。

—通訊費用成本。

姶極佳的網路組態彈性，可隨時依需要調整，快速反映企業結盟策略。

婓與網際網路比較，通訊之私密性較佳。

娆可將VPN管理及設備建置、升級外包給服務提供者，提供客戶快速切入市場之時效能力。



Sites	Number of total VC or connections			Pricing Assumptions
	Partial Mesh	Full Mesh	IP VPN	Frame Relay:
5	8	10	5	$180/port
10	18	45	10	$60/PVC
15	42	105	15	IP VPN:
20	76	190	20	$300/port
25	120	300	25	

資料來源：Nortel Networks

【圖 4-5】Frame Relay VPN 與 IP VPN 費用比較

五、VPN 網路設計技術

在公眾 IP 骨幹網路上建置一個具有如同傳統 VPN 之服務品質(QoS)和安全策略的 VPN，必須要探討穿隧(Tunneling)、安全(Security)、訊務量規劃(Traffic Engineering)、策略管理(Policy Management)等主要技術。

艼穿隧技術(Tunneling)

穿隧技術是為了將私有數據網路的資料在公眾數據網路上傳輸，所發展出來的一種資料打包方式(Encapsulation)，亦即在公眾網路上建立一條秘密通道。IETF 從 1995 年起，陸續公佈許多網路安全之相關技術標準，這些標準統稱為 IPSec (IP Security，RFC1825 ~ 1829，RFC1851，RFC2085，RFC2104) 。

在 IP 環境下使用穿隧技術建立虛擬鏈路的通信協定主要有：IPSec、MPLS(Multi Protocol Label Switching)、GRE(Generic Routing Encapsulation)、PPTP(Point-to-Point Tunneling Protocol)、及 L2TP(Layer 2 Tunneling Protocol)等六種。不論是 Site-to-Site VPNs 或 Remote Access VPNs，IPSec、PPTP、L2TP 是三種常用的穿隧技術，其中 IPSec 為第三層的穿隧技術，專門為 IP 所設計，不但符合現有 IPv4 的環境，同時也是 IPv6 的標準，它也是 IEIF 所制定的業界標準；PPTP 與 L2TP 均為第二層的穿隧技術，適合具有 IP/IPX/AppleTalk 等多種協定的環境。IPSec、PPTP、L2TP 三者，最大的不同在於，運用 IPSec 的技術，使用者可以同時使用 Internet 與 VPN 的多點傳輸功能(包括 Internet/Intranet/Extranet/Remote Access 等)，而 PPTP 及 L2TP 只能執行點對點 VPN 的功能，無法同時執行 Internet 的應用，使用時較不方便。

芧安全技術(Security)

在 IP VPN 環境上駭客是很容易借由 IP 服務非法入侵，因此為確保公司的資源與服務僅供有權限使用者擷取，安全策略是不得不考慮的問題，其主要措施不外是資料加解密(Encryption & Decryption)、密鑰管理(Key management)、身分確認(Authentication)等技術。

一、加解密技術(Encryption & Decryption)

為確保私有之資料於傳輸過程中，不會被其他人瀏覽、竊取或篡改，所有的封包在傳輸過程中均需加密，當封包傳送到私有數據網路後，再將封包解密。封包於傳輸過程中，即使遭到駭客竊取，駭客只能看到一些無意義的的亂碼。如果駭客想看到封包內的資料，他必須先破解該封包的密鑰(Encryption Key)。隨著加密技術與密鑰長度的不同，駭客破解密鑰所需的設備與時間便有所不同。例如：使用 SSL(Secure Socket Layer)技術，密鑰長度為 40 bits，以現在的 PC 不到一秒就可破解；而 56-bits 的 DES(Data Encryption Standard)，以一般的 PC 大概要幾十年才能破解；112bits 的 Triple DES(3DES)，現在則被視為無法破解。

加解密技術可概分為兩大類，

- 對稱式密碼學(Symmetric Cryptography)，又稱密鑰式密碼學(Secret-key Cryptography)。
- 非對稱式密碼學(Asymmetric Cyptography)，又稱公用鑰匙密碼學(Public-key Cryptography)。

對稱式的加解密技術，加密與解密均使用同一把鑰匙。大家所熟知的 DES、RC2 即為對稱式的加密技術。非對稱式的加解密技術，加密與解密使用不同的鑰匙，其中以 RSA 最常被採用。由於對稱式密碼演算法的運算速度較非對稱式密碼演算法快

(約差 100 ~ 1000 倍)，所以現行之加密標準均採用 DES 或 3DES 做為加解密所用的演算法。部份 VPN 之設備廠商(如 VPNet Technologies Inc.)則採用對稱式加上非對稱式的融合(Hybird)密鑰管理功能，達成網路上密鑰的交換與管理，以此方式不但可提供較快的傳輸速度，也有更好的保密功能，也更難破解。

㈥密鑰管理技術(Key Management)

駭客如果想要解讀封包，必需先破解加解密所用之密鑰(Key)。如果駭客無法截取密鑰，他只能使用窮舉法來破解，如此便會大幅減少資料被竊取的可能性。因此如何在 IP VPN 網路上安全地傳遞密鑰，而不被駭客竊取，這就是密鑰管理的主要任務。

現行常用密鑰管理的技術又可分為 SKIP(Simple Key management for IP)與 ISAKMP/Oakley (又稱為 IKE)兩種。

㈦據點設備與使用者身分確認(Site and User Authentication)

IP VPN 網路上有眾多的使用者與設備，如何正確地辨識合法之使用者與設備，使屬於自己單位的人員與設備能互相連通，構成一個虛擬專用網路(VPN)，並讓非用戶無法進入系統，這就是使用者與設備身分確認技術所要解決的問題。辨識合法使用者的方法很多，最常使用的是使用者名稱與密碼或卡片式兩段認證等方式。設備認證則需仰賴由電子證書核發單位(Certificate Authority)所發出之 X.509 電子證書(Certificate)。設備交換資料前，須先確認彼此的身份，藉著出示彼此的電子證書，雙方將此證書比對，如果比對正確，雙方才開始交換資料，反之，則不交換。藉由這個方式，即使網路上有同一廠牌的機器，因為其電子證書不同，除非安裝時藉由網路管理程式接受設備的電

子證書，將其視為同一 VPN 之合法設備，否則兩個設備還是無法連通。

㈡訊務量規劃(Traffic Engineering)

如同傳統的 WAN 網路，在 IP 寬頻的骨幹網路也需要有新的工具來提供訊務規劃，譬如：資料封包在進入 IP 骨幹網路前需要分類和加上標記、接取網路的出口頻寬(Egress Bandwidth)要依資料重要性作公平合理地分配、標記資料在這共享網路擁塞處根據服務提供者所付服務水準協議書(Service Level Agreement，SLA)提供服務等。

㈢策略管理(Policy Management)

在 IP 寬頻網路中，企業網路的連線數會隨著 VPN 數量級數增加，因此不能再以傳統網路組態和設備監控方式來管理 IP 企業專用網路，而必須要有一個能提供具有彈性、以策略導向的端對端 VPN 管理(End-to-End Policy-Based VPN Management)。

藉由上述的 VPN 技術，企業可以迅速建構一個屬於自己的 IP 企業專用網路，享受到公眾數據網路與私人數據網路的優點。除此之外，更能將企業內／外部網路(Intranet／Extranet)及遠端存取／上網存取(Remote Access／Internet Access)功能等整合於 IP VPN 環境下，使企業節省許多設備購置費用、長途數據線路月租費、撥接線路費用及後續管理維護成本，增進工作效能與員工生產力，提高企業整體的競爭力。

六、VPN 網路設計考量

要規劃專戶的企業網路，當然須依其網路需求再配合各種準則，選擇最佳方案提供給專戶，本節是針對設計 VPN 網路的主要問題考量準則加以描述。

☑ 定址問題(Addressing Issues)

☑ 路由規劃問題(Routing Issues)

☑ 安全機制(Security Issues)

☑ 服務品質(Quality of Service，QoS)

☑ 網路擴充性(Scalability)

☑ 網路管理(Network Management)

☑ 現有 VPN 網路移轉(Migration from pre-VPN Networks)

艾定址問題

娟 IP-VPN 之 IP 位址應妥善規劃

毫對外採用公用 IP(Public IP) 位址，由於公用 IP 為有價資源，網路設計規劃時應盡量減少使用。

淨公司內部採用私有 IP(Private IP) 位址，需依公司據點數及各據點所需之 IP 數量妥作 IP 分配及子網路切割。

姶需有網路位址轉換 (Network Address Translation，NAT)機制作 Public IP 及 Private IP 間位址轉換。

芧路由規劃問題

設計時需考量總公司、分公司及各據點間訊務流量情形及公司預

算，作適當路徑路線規劃。對於高訊務量之點提供負載平衡(Load Balancing)措施，重要路由則需提供備援電路或動態路由規劃(Dynamic Routing)，將資訊安全、快速的傳送到指定地點。

㈡安全機制

VPN 應用於 Extranet 時，由於採用 Public IP 網路，給予入侵者、竊聽者非法滲入企業內部網路之機會，為避免公司內部機密資訊被有心者竊取，規劃設計時，需有防火牆(Firewall)及入侵者偵測系統(Intrusion Detection System，IDS)等安全機制方面考量。另外在新增設備或功能時，很可能因一時疏忽，導致網路安全機制遭受破壞，因此，在執行設計時需慎重考慮的要素有：

- 新增設備或功能是否容易遭受非法者入侵？
- 密碼資訊是否曝露於外，讓竊取有機可乘？
- 是否內部網路對入侵者防禦較為脆弱？
- 是否外部網路之使用者在進入網路前均有經過授權與認證？

㈢服務品質

㈠依據客戶通訊種類及頻寬需求不同，提供不同等級服務。

㈡ VPN 提供者應提供差異性服務(Differential Service，Diff-Serv)之服務水準協議書(Service Level Agreement，SLA)供客戶選擇。SLA 服務標準內容，包括在供裝建設、頻寬效能、服務可用率、障礙通知及報表提供等方面提供保證及罰款規定等。

㈢ VPN 提供者須能提供 SLA 監視之工具，供客戶佐證參考。

艹網路擴充性

一個良好的 VPN 規劃，將吸引企業客戶之注意焦點，隨著企業據點之擴充及頻寬需求之增加，應能即時提供網路擴充。因此，網路設計規劃除需考慮實體連接架構、設備間路由需求、彈性及負載分攤外，網路擴充性亦為重要考量因素。

第網路管理

企業公司內部各部門採用之 VPN 設備不同，其功能及管理方式亦有不同，客戶最需要的是如何提供一整合式應用管理系統，因此，除了本身網路管理功能外，更應提供客戶一整合式應用客戶管理服務系統。

茎現有 VPN 網路移轉

對於企業公司內部已建有廣域網路或撥接網路，或已裝設有路由器、防火牆等設備連接至網際網路之情況時，在導入新的 VPN 規劃案時，必須考量和現有設備之相互支援性，儘量在對現有網路維運衝擊最小情況下移轉。

七、VPN 網路建置方式

茊 CPE Based VPN

婧在客戶端採用 VPN 設備，利用穿隧技術如 IPSec、L2TP、PPTP、GRE 等建立 VPN 環境，其特性為：

匏網路架構可跨越不同的 ISP、NSP 業者整合，只要網路層能提供 IP 網路，而不需考慮其間的互通性及安全性，建置方式快速而且有彈性。

滒 QoS 需由骨幹網路提供。

淯客戶端需自行建設 VPN 設備或以 Outsourcing 方式委託給 ISP、NSP 建置。

涋各據點間通常需採 Full Mesh 方式建立隧道(Tunnel)，容量有限。

姵建立隧道的設備一般採用三種方式提供：

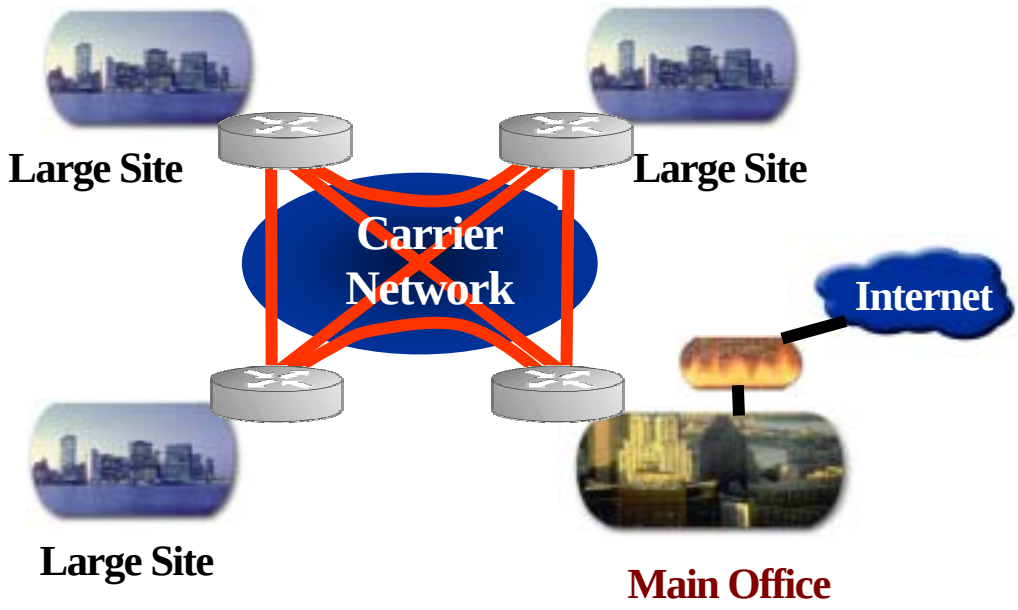
匏單機設備—效能、穩定性較高，不需仰賴作業平台。

滒在路由器、防火牆上附加建立隧道之功能。

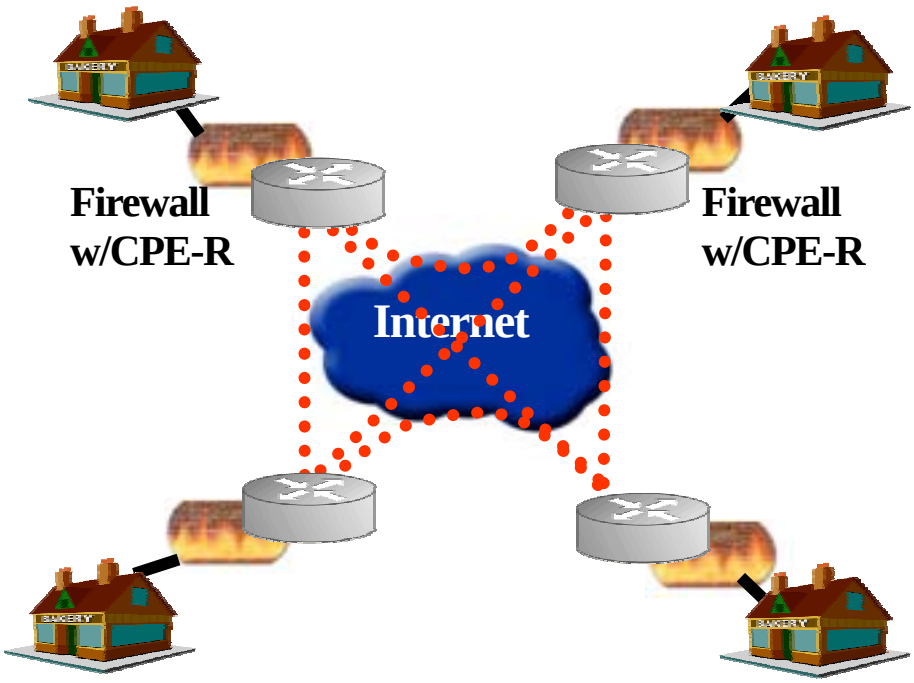
淯純軟體方式—如 MS Windows2000。

圖 4-6 以 Frame Relay 為骨幹網路之 CPE Based VPN 網路架構圖，目前為中大型企業採用，CPE 路由器具有管理多重連接功能，且可有效以 PVC 連接各大據點。

圖 4-7 是目前小型企業大致採用的以網際網路為骨幹所建置之 CPE Based VPN 網路架構圖，是以 IPSec 穿隧技術建立隧道連接各點，具有簡單、成本低優勢，只要有接取網際網路設備，就很容易加入 VPN。



【圖 4-6】CPE Based VPN (Frame Relay)



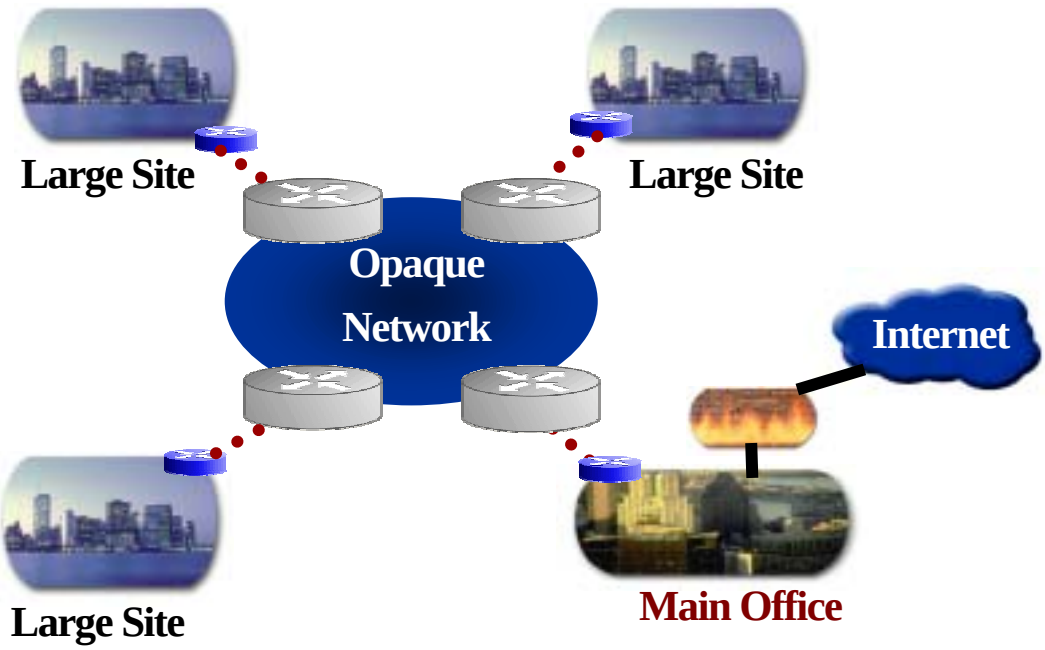
【圖 4-7】CPE Based VPN (Internet)

苧 Network Based VPN

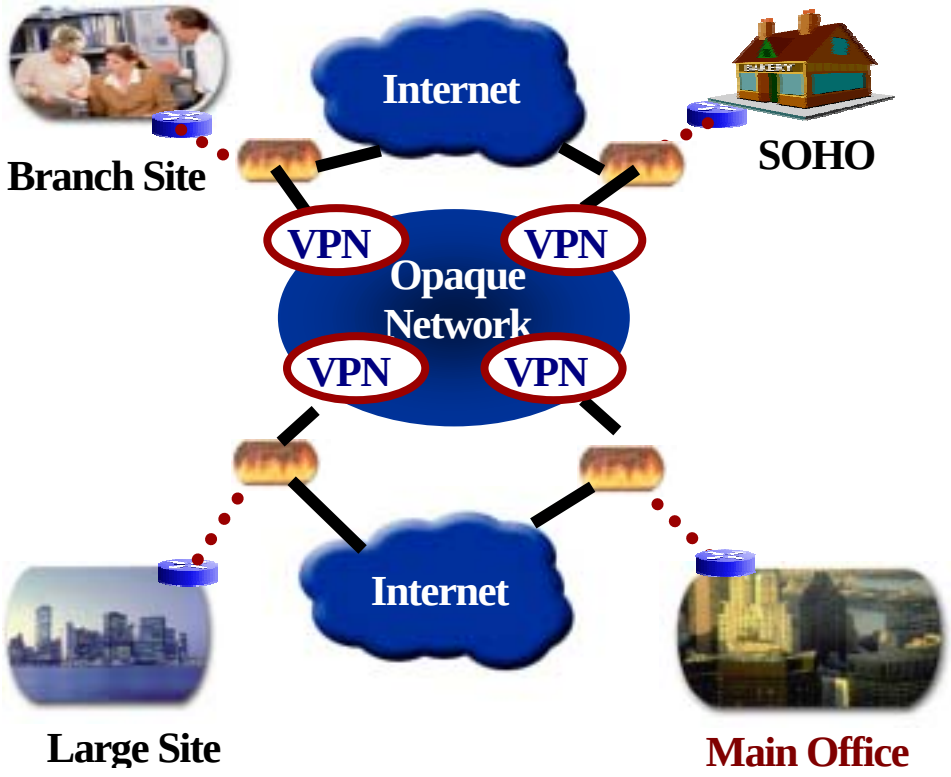
Network Based VPN 網路架構不同於 CPE Based VPN 以 CPE 設備建置 VPN，Network Based VPN 是由服務提供者之核心網路架構提供，VPN 之運作完全委託給 ISP 或 NSP 業者。採用 Network Based VPN 網路架構時，可同時提供如防火牆、內部資訊管理、頻寬管制、權限管制、網路管理、或是 VoIP(Voice over IP)等服務，Network Based VPN 為最適合 ISP 或 NSP 業者切入 VPN 服務市場，惟在面對不同 ISP 或 NSP 業者或是不同網路架構時，需考慮複雜的互通性、信任度及拆帳的問題。

Network Based VPN 是一個客戶並不再意的黑箱網路(Opaque Network)，而且每個據點不像 CPE Based VPN 客戶需自行設定端對端路徑，如圖 4-8 所示。圖 4-9 主要強調是由服務提供者負責將 VPN 與網際網路綁在一起，因此訊務不必全要透過總公司上網。

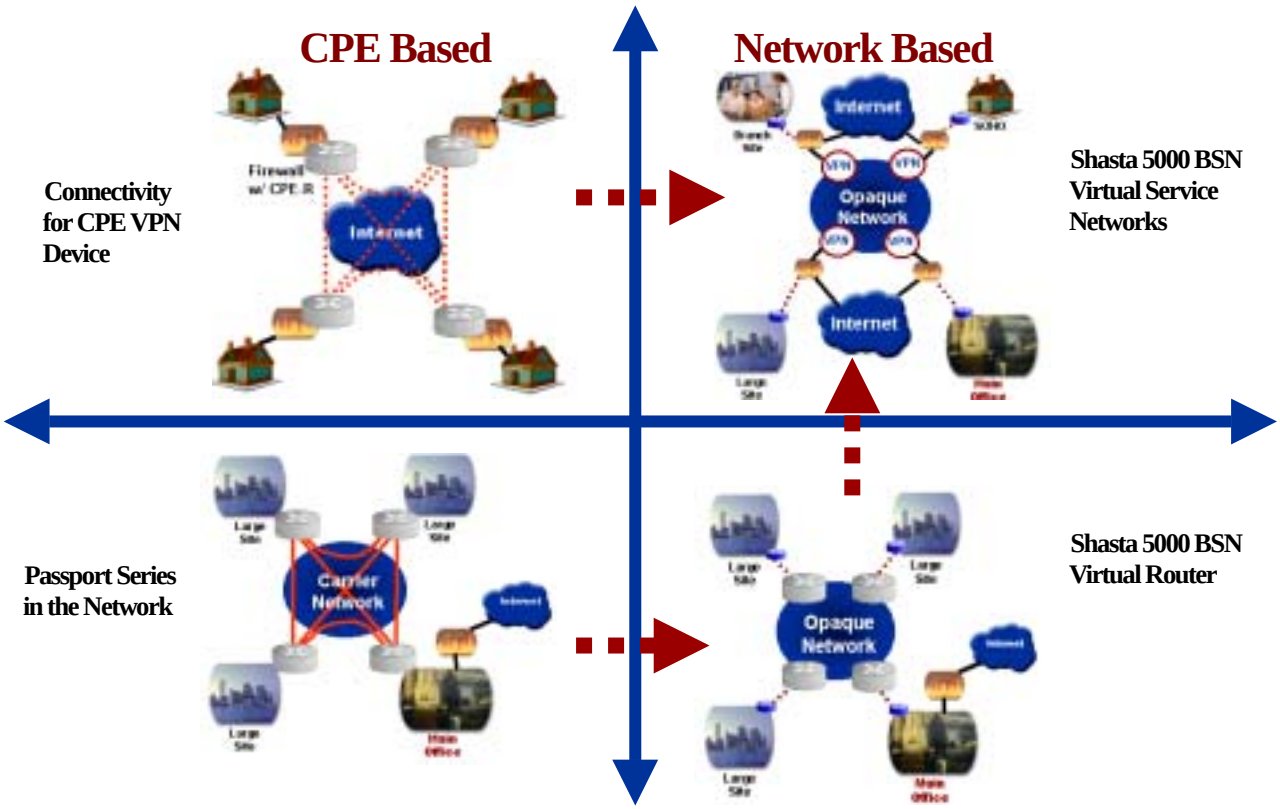
圖 4-10 顯示 Nortel Networks 使用在 VPN 的各種產品系列。



【圖 4-8】Network Based VPN (Private Only)



【圖 4-9】Network Based VPN (VPN + Internet)



【圖 4-10】

八、VPN 整體服務之規劃

企業利用寬頻 IP 網路建置 IP VPN 環境後，當然會依其需求量身訂製各種不同的服務運用。目前 IP VPN 環境所能提供的服務類型如圖 4-11 所示，至於要如何規劃專戶公司內部網路之整體服務方案，可依下列三個層面考量。

艼基本服務層面

—根據專戶公司通信需求,建議採用適當的服務等級(Class of Service，CoS)。

—接取方式(專線、ADSL、．．．)。

—規劃語音、數據、影像整合性應用服務。

—提供網路用戶終端設備(CPE)軟、硬體之諮詢及規劃服務。

芓加值服務層面

—利用網際網路及 CTI 等相關技術，整合專戶公司之電話與數據網路，規劃全方位網際網路客戶服務中心。

—規劃動態即時之視訊會議、遠距教學、隨選視訊等多媒體通訊服務。

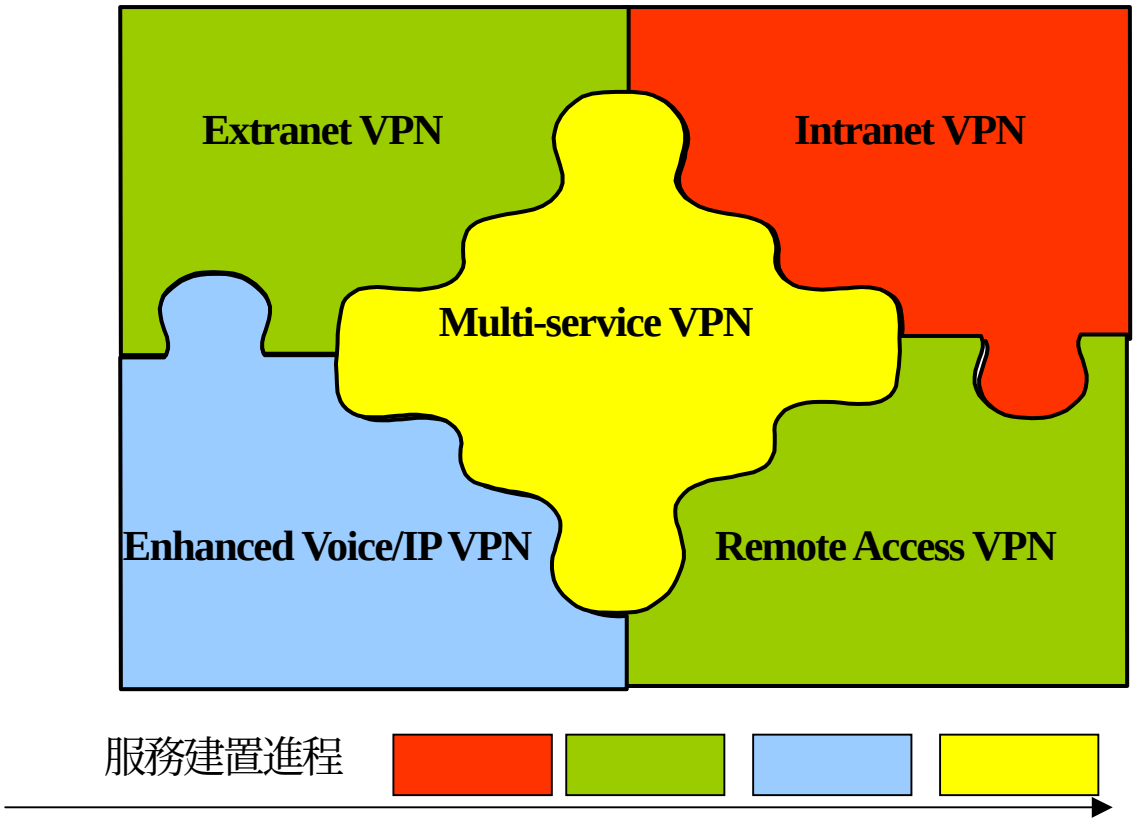
—規劃電子郵件、影像、語音、傳真等整合性訊息服務。

芏配套服務層面

本層面主要著重在委外服務(Outsourcing)，包括

—網頁、電子商務、資訊、通信網路等代客設計與建設。

—設備代管(Co-location)。



【圖 4-11】**IP VPN** 服務類型

伍、感想與建議

面臨固網業者即將營運之際，而且直接從新一代技術 IP 寬頻網路切入，使本公司頓失優勢；另一方面，企業客戶必成它們主攻目標市場應是勿庸置疑。因此本公司要在這競爭的環境中，避免又處於挨打的局面，必須重新思索一套可攻可守的策略，來開拓與鞏固我們的企業客戶市場，在此有幾點建議可供參酌。

一、加強專業技術及行銷人才之引進與培育

民營大哥大業者行銷策略之威力與效果，本公司必有錐心之痛的感受，加上本公司員工平均年齡過於老化，非得積極注入有技術專才、行銷專長背景的新血輪不可，並進一步加強員工專業訓練，以活化公司迎接新的挑戰，為公司開創新契機，再創事業第二春。

二、積極落實整體性、多元化的服務目標

要在這競爭的市場中，吸引新企業客戶、穩定老企業客戶，提供企業整體服務是當務之急。以往這方面本公司視為禁臠之地的用戶終端設備(CPE)領域、服務不夠多樣化、新服務推出時程過長等，常使公司失去很多商機，甚至流失客戶。以上種種現象，本公司可和相關設備廠商或服務提供者廠商，以交換持股、投資方式建立上下游之垂直分工或水平分工的關係，甚至自己成立子公司，致能充分滿足企業客戶的整體需求。

三、以企業集團導向為專戶服務對象

由於電信環境、市場趨勢的發展，使得企業客戶不再滿足於傳統電信業務的服務；另一方面，企業公司集團化的走向也越來越明顯，因此企業本身的通信需求，必會由早期各公司自建的思考模式朝向以集團整體需求方向規劃。如是本公司的專案經理若能順

勢調整儘量以集團類別來服務，這樣企業集團化後也符合單一窗口的精神，而且也更能掌握企業客戶具體的需求，達到事半功倍的效果。

陸、附件參考資料

(本部分未轉為電子檔)