中小型企業網路建置與應用之研究

Study of the Establishment and Applications of Small and Medium Sized Enterprise Network

林智祥
大同大學資訊工程研究所
jasonlin@ares.com.tw

包蒼龍
大同大學資訊工程研究所
tlpao@ttu.edu.tw

本文主要是在探討如何規劃建置一個具彈性的中小型企業網路環境與應用，使網路的規模可以隨著企業的成長與需求而逐步擴充。從企業網路架構的選擇到提供外部的安全網路連線，讓在外部的員工運用這個安全的網路，能方便與快速的存取公司內部資源。在企業網路上的應用方面則探討了網路電話的建置，讓企業本身的各據點之間能藉著網路電話的建置，降低彼此之間通話的電信費用支出。最後在資訊安全方面也提出一些考量與做法，讓企業網路環境能兼顧便利與安全。

***關鍵詞*—企業網路, 網路電話, 資訊安全**

In this study, we address the issues on how to design and implement a flexible network environment for small and medium size enterprises so that the network scale can gradually expand with the growth of the enterprise. We focus on the enterprise network structure planning and network security measure. This network can let employee access to enterprise resources conveniently and safely via a stable and secure network from outside. Meanwhile, this study will also discuss the voice services in the enterprise network. The enterprise and its branch offices can substantially lower their phone bill for inter-office communication. Lastly, we also outline considerations and suggestions for the information security, bringing both convenience and safety to the enterprise network environment.

Keywords: Enterprise network, Voice over IP, Information security

一、前言

研究動機

在高度競爭的商場裡，企業的競爭力是企業生存與獲利的重要關鍵，而現代企業的競爭力則在於面對每天各種複雜的資訊時，必須能夠快速的收集、統計與判斷並做出正確的決策，使企業的核心能力得到最佳的運用，企業的發展才能夠不斷前進。而在目前的環境裡，由於上游的產業、政府或是銀行單位等很多都已經電子化、網路化，所以舉凡從企業訊息、業務商機、政府公告、產品資料到郵件、訂單、匯款…等這些資訊也都能經由網路更快速取得與運用。根據以往的研究調查，中小型企業使用電子郵件的比率約達 98%，企業網站的建置也達到六成，這些數據都說明中小型企業藉著對網路的應用來提升競爭力是越來越倚重了[1]。另一方面隨著企業的成長，企業據點也可能會隨之增加，因此各據點之間網路聯繫也成為企業網路重要的一環，根據另一項研究報告，企業網路確實會創造企業的競爭優勢[2]，所以企業的電子化與網路化是必然的趨勢。

為了達到以上的目標，各企業對企業網路的建置需求日漸增加，但現今的各項網路技術卻也快速不斷地推陳出新，使得通常人數不多的中小型企業的資訊人員在受命建置企業專屬網路時，常因為本身沒有實際經驗或選擇了不

適當的產品而導致建置不符需求，甚至會有就不知道該如何下手而裹足不前。

研究目標

由於市場上企業網路規劃產品相當多，從企業內部網路到連接網際網路的運用，或是多據點的企業間網路，各式各樣的網路架構適合各種不同的環境與使用需求。

因為資金的關係，中小型企業的營運初期往往都是從很小的公司開始起步，這個時期的企業網路規模大概只能是一個小型區域網路搭配網際網路的基本架構，但是隨著企業的營運成長了，營業據點也開始增加的時候，各據點本身卻也只是自成一個小型企業區域網路，這個時期為了提升競爭力與達到企業內部資源的共享，就勢必要把各點的區域網路連結起來，以組成一個完整的企業網路。這個時期企業的規模變大了，可是企業主本身當然希望初期的各項設備投資都不浪費且具可擴充性，所以本文所要研究與探討的架構是在規劃符合這些原則下，能逐步擴大的企業網路架構。

基於上述需求，本文除了就一些較為典型而常被使用的網路架構提出說明之外，也透過實際建置的案例來探討各種企業網路的優缺點，同時說明這些企業網路架構所運用的場合。希望讓中小企業的資訊人員在遇到建置需求時，能經由參考本文的研究有比較清楚的考慮方向，並運用實際的案例內容與討論，選擇對各企業比較有利的建置架構。

本論文之架構如下，第二節就建置企業網路時所需之網路協定、技術等背景知識分別提出說明。第三節介紹幾種常見的企業網路架構，例如以實體線路來做區分的專線網路與交換式網路設備所組成的虛擬專屬網路或是以加密技術不同而區分的加密通道虛擬專屬網路等，並分別針對這些架構說明其特點，同時對企業網路中比較重要之網路電話語音之應用，提出一些不同的架構來解說。第四節我們提出了一個實際建置的案例來探討，如何在考量成本、線路穩定、可靠性與品質的要求下建置一套實用之企業網路。最後在第五節討論幾項在不久的將來，企業網路所可能遇到的應用與改變，以供企業的資訊從業人員可以進一步運用與探討。

二、文獻探討

由於企業網路乃是專屬於企業本身使用，所以基本上就與公眾網路有所不同，建置企業網路，除了可以選擇專線網路架構之外，各種虛擬專屬網路的架構與技術也是本節探討的目標。在企業網路的應用方面，我們也針對電話語音的技術與語音壓縮規格做了簡要討論。

(一) VPN

VPN (Virtual Private Network)是虛擬私有網路的簡稱，VPN 雖然不是真的私有網路，但卻具有私有網路的功能，VPN 線路的連結方式和傳統「私有網路」實體線路的連結方式不同，但在運用上其作用和所達成的功能相同，故稱之為「虛擬」(Virtual）的私有網路。

傳統探討的 VPN 大都是指利用不同加密技術，透過網際網路所建置虛擬通道的 VPN，這種以加密方式建置的 VPN 如 SSL VPN 與 IPSec VPN，一般還以網路線路的連結架構來分類，如 Site to Site 和 End to Site 兩種，Site to Site 所指的是將分隔兩地的企業內部網路透過網際網路所做的 VPN 連接，End to Site 指的則是個別的行動設備與企業內部網路透過網際網路的 VPN 連接。但是現在的 VPN 則多了一些選擇，因為交換式骨幹網路的應用，使大部分的 ISP (Internet Service Provider，網際網路服務供應商)或 NSP (Network Service Provider，網路服務供應商)可以提供其骨幹網路設備來構成虛擬專屬連結 VPN，讓企業各據點的網路能經由這些

VPN 連接在一起，因此在 VPN 的端點之間的連結就沒有傳統專線網路所具備的點到點的固定線路，例如 MPLS (Multi-Protocol Label Switching，多重通訊協定標籤交換傳輸) VPN。

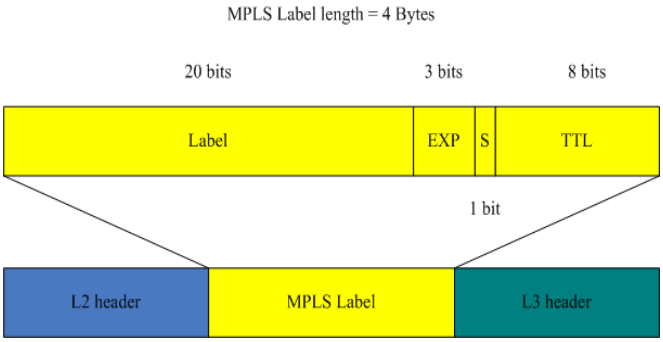
MPLS VPN

MPLS 是由 IETF 所發展出來的 IP 高速骨幹網路交換標準。其目的是要提供一個更具彈性、擴充性及效率更高的 IP 層交換技術。MPLS 是集成式的 IP Over ATM 技術，在 Frame Relay 及 ATM Switch 上結合路由功能，封包透過虛擬電路來傳送，只須在 OSI 第二層的資料連結層執行硬體式交換以取代第三層網路層的軟體式 IP 路由，使網路封包傳送的延遲時間減短，更適合多媒體訊息的傳送，增加網路傳輸的速度[3]。

MPLS 的運作原理是提供每個 IP 封包一個標籤，由此決定封包的路徑以及優先順序，與 MPLS 相容的路由器，在將封包轉送前，僅讀取封包標籤，無須讀取每個封包的 IP 位址以及表頭，迅速地將封包朝終點的路由器傳送，進而減少封包的延遲。

MPLS 整合了標籤交換架構與網路層路由機制的技術，最基本的概念是將進入 MPLS Network 之封包配置一個固定長度的標籤(Label)，在 MPLS 網路中封包會根據標籤做轉送，由標籤來決定封包在網路上的路徑，不會再看 Layer 3 的 IP 表頭。

圖一是 MPLS 標籤的格式與插入封包位置的圖示，MPLS Label 是一個 4 個位元組、固定長度、本地意義(locally-significant)的識別碼(Identifier)，標籤是被插入於封包的第二層資料連結層與第三層網路層表頭之間，其中標籤長度為 20 位元，紀錄 MPLS 標籤實際的值，EXP 長度為 3 位元，在網路傳遞時，做為封包要排程(Queuing)或是捨棄(Discard)的依據，也就是 MPLS 每個封包服務等級的紀錄之處，S (Stack) 則是支援階層式的標籤，最後的 TTL 則是提供 Time To Live 的功能[4]。



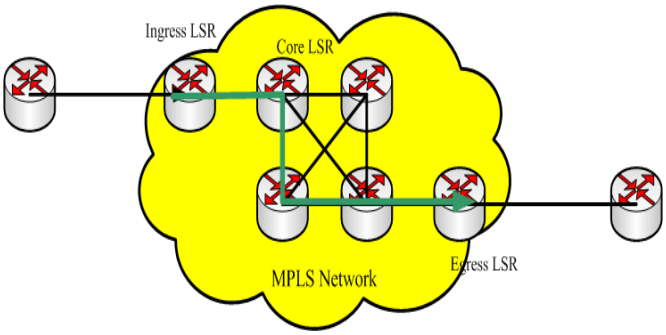
圖一、MPLS 標籤的格式與插入封包的位置

MPLS 網路是由多個具有標籤交換能力的路由器 LSR(Label Switch Router)互相連結所組成(見圖二)，根據在 MPLS 網路內扮演角色的不同 LSR 可以分為三種類型：

Ingress LSR：位於 MPLS 網路入口處的邊緣路由器，負責在進入 MPLS 網路的 IP 封包插入標籤(Insert)。

Core LSR：位於 MPLS 網路核心的核心路由器，負責做標籤轉換(Swap)。

Egress LSR：位於 MPLS 網路出口處的邊緣路由器，負責把要離開 MPLS 網路到一般 IP 網路的封包去除標籤(Remove)[5]。



圖二、MPLS 標籤遞送

SSL VPN

SSL VPN 是一種基於 SSL 通訊協定的 VPN 網路，幾乎所有作業系統都會具備的網頁瀏覽器中都會內含 SSL 通訊協定，因此使用者不用像使用 IPSec VPN 般需要安裝代理程式(agent)來處理加解密問題，只要使用作業系統內含的瀏覽器即可，所以 SSL VPN 又被稱為 Clientless VPN。

IPSec VPN

IPSec VPN 是一種基於 IPSec 協定的 VPN 網路，IPSec 協定是運作於 OSI 網路層的 VPN 通訊技術。大致上可以使用兩種架構的方式來建置 IPSec VPN，第一種架構是利用一個或是多個的 VPN Gateway 組成 VPN 通道，VPN Gateway 後端的使用者設備就可以利用這個通道與另個一 VPN Gateway 後端的使用者或是伺服器連接。第二種架構適用於企業外部員工的遠端存取方式，也就是在外部員工的電腦安裝 IPSec VPN Client 軟體，使外部員工也能連入企業內部網路來進行遠端存取的 VPN。

(二) VoIP

VoIP（Voice over IP）是透過 IP 網路傳輸語音資料的技術，IP 網路原先是設計用來傳遞資料封包，而 VoIP 包含了需要即時在 IP 網路上傳遞語音對的話封包。一般電話線路傳送的是類比語音訊號，但為了要在網際網路上傳輸則必須將聲音轉換成類比電訊號，接著加以數位化處理後藉由網路傳送。在接受端的程序則是反過來，將透過網路接收的數位訊號轉換回類比訊號，成為人耳能夠辨識的語音。VoIP 常用的協定有 H.323 與 SIP，而在語音壓縮部的技術則有 G.711、G.729、G.723.1 等。

H.323

H.323 系統是由終端器(Terminals)、閘道管理員(Gatekeepers)、閘道器(Gateways)、多點控制器(Multi-point Controllers)、多點控制單元(Multi-point Controller Units)等元件組成，雖然這些組成元件在邏輯上是相互分開的，但實際實作時是可以結合在一起的。

SIP

SIP 是由 IETF 於 1995 年針對網際網路電話所制訂出來的標準，目前最新的規格是規範在 RFC3261。SIP 是以 ASCII 文字資料為基礎，用來建立、維持與結束兩點或多點之間通訊應用程式層次之控制協定。如同其他的 VoIP 通訊協定，SIP 設計目的也是用來定義封包式資料電話網路中的訊號取樣(Single Sampling)與通訊階段管理工作。訊號取樣讓通訊內容能轉換成為數位化資訊，得以傳遞到網路各個地區，通訊階段管理則提供通話從開始到結束的所有狀態控制功能[6]。SIP 採用開放式架構，只要終端裝置可以連結上網，並能正確執行 SIP UA (User Agent)即可以進行通訊 [7]。

SIP 是一種點對點「Peer to Peer」的通訊協定，採用分散式架構，透過 URL 來命名位址與使用純文字格式來傳送訊息，使 SIP 能夠藉由網際網路模型的優點，來架構 VoIP 網路與應用程式，其組成元件如下：

(1)User Agents:

User Agents 是 SIP 網路環境中的終端設備，包含 User Agent Client (UAC)以及 User Agent Server (UAS)，UAC 負責建立請求(Request)，而 UAS 負責產生依照請求產生應答(Response)。每個 SIP User Agent 都包含 UAC 以及 UAS 的功能。

(2)SIP Proxy:

SIP Proxy 負責將 User Agent 或者其他的 SIP Proxy 所發出的請求代為傳遞到另外一個 SIP 元件。

(3)Redirect Server:

當 User Agent 或是 SIP Proxy 所發出的請求傳送到 Redirect Server 時，Redirect Server 回覆 Redirect 訊息，讓 User Agent 或者 SIP Proxy 知道需要將訊息重新導向至另一個 SIP 的元件。

(4)Registrar Server:

Registrar Server 提供給 User Agent 註冊的介面，以進行管理以及其他的服務，同時更新 Location Server 上的 User Agent 資訊或者更新其

他的資料庫訊息。

(5)Location Server:

Location Server 負責存放 User Agent 的註冊資訊，例如：URL、IP 位址等[8]。

語音壓縮技術 G.711、G.729、G.723.1

目前網路電話較常使用的語音壓縮技術為 G.711、G.729、G.723.1 等，其差異在於頻寬使用的多寡與重建之後的語音品質。如果企業採用 G.711，則每一通 VoIP 電話就需使用 64kbits/sec 頻寬，G.729 為 8kbits/sec，而 G.723.1 則是 6.3kbits/sec，不過傳送後重建的聲音品質當然也會有差異。因此企業須先決定在何種可接受的聲音品質之下評估最大同時通話數與 codec，據此估算出 VoIP 系統需要多少頻寬，例如企業希望容納 10 個人同時通話，並採用 G.711，所以大約需要 640k（10x64k），若採用 G.729，則減少為 80k（10x8k）。企業即可考量既有線路的頻寬、通話品質、增加 VoIP 是否會影響其他應用的效能等因素，綜合評估後，選擇最合適的語音壓縮技術。

三、系統架構

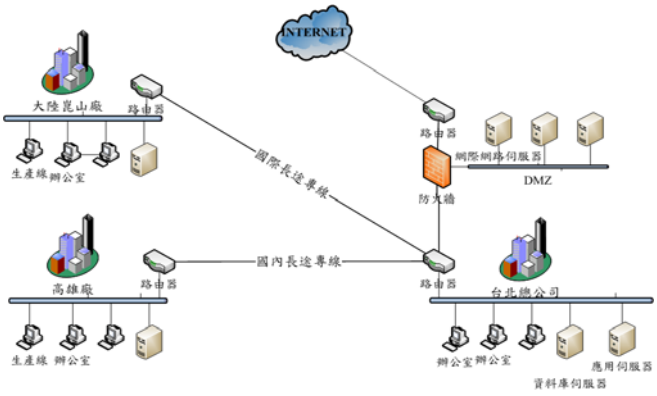
(一) 網路線路

基本架構

企業網路的環境根據使用的線路、設備與企業本身的需求可規劃出許多不同的架構，以下舉幾個實際的例子來加以說明。

(1) 專線企業網路

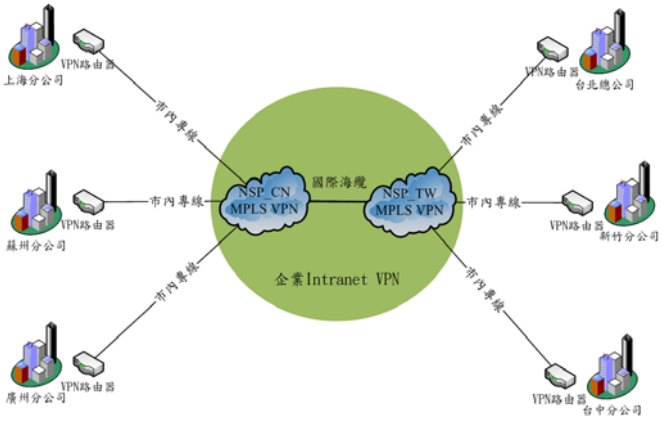
這個架構是直接使用實體專線線路連接，因此網路品質穩定，網路頻寬也完全能夠掌握，通常應用於跨區域企業網路上的資訊需要即時回應而不能有連線品質不穩定的時候採用，網路架構如圖三所示。但是這個架構的缺點是所有據點的網路都接回總公司，各據點之間的網路通訊都必須透過總公司的設備，因此如果總公司的設備故障，則所有據點間的網路都將中斷。



圖三、專線企業網路

(2)Intranet MPLS VPN 企業網路

以兩岸企業據點間的網路連接為例，運用結合中國大陸與台灣兩地不同 NSP 各自的 MPLS VPN 來組成一個完整的企業網路。企業兩地的據點分別使用當地的短程市內專線連接上當地 NSP 網路機房，再透過 NSP 本身網路主幹的 MPLS VPN 來建立企業網路，至於兩個 NSP 之間則以國際海纜來連結，網路架構如圖四所示。

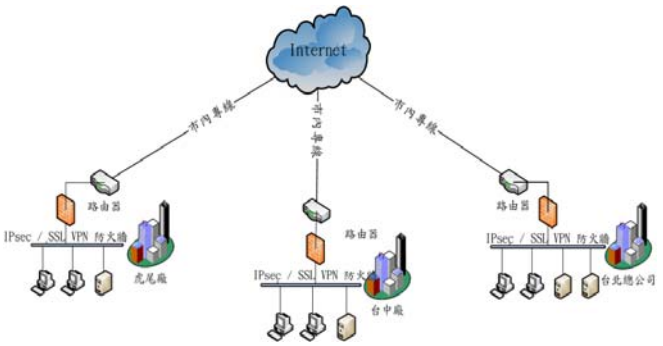


圖四、Intranet MPLS VPN 企業網路

(3)Internet IPSec VPN 企業網路

採用的架構是使用 IPSec VPN 設備，透過

Internet 的線路將各據點之網路連結成為 Site to Site 的 VPN，這個架構運作效能比較會受到 Internet 流量的影響，而且必須有支援 IPSec VPN 的網路設備，通常適用於較低網路頻寬要求的環境使用，網路架構如圖五所示。



圖五、Internet IPSec VPN 企業網路

優缺點比較

(1) 網路的穩定性

我們將就以上述提及的幾個實際例子來做網路品質穩定性的比較，依照使用的網路線路來評估，在「專線」架構的網路品質上，由於線路是完全專屬使用，因此也有比較穩定的可用頻寬。在「Intranet MPLS VPN」的網路架構上，雖然線路並不是專屬使用，但是 MPLS 是集成式的 IP Over ATM 技術，在 Frame Relay 及 ATM Switch 上結合路由功能，封包透過虛擬電路來傳送，以硬體式交換取代軟體式 IP 路由，整合了 IP 路由作業與第二層標籤交換作業為單一系統，使網路封包傳送延遲時間縮短，增加網路傳輸的速度，所以網路的穩定性也僅比專線稍低一些。至於「Internet IPSec VPN」則由於需經過 Internet 的公眾網路，所以在網路傳輸的品質上會因網路流量壅塞而受到影響。

(2)成本評估

成本可以分為第一次的建置成本與後續每月支出的線路成本來評估，建置成本包括設備成本與網路申請設定費用，但是以長期來評估，影響最大的應該是每個月的線路租金，因此成本的評估由高而低分別是「專線」、「Intranet MPLS VPN」、「Internet IPSec VPN」，以上各架構的優缺點比較，整理如表一所示。

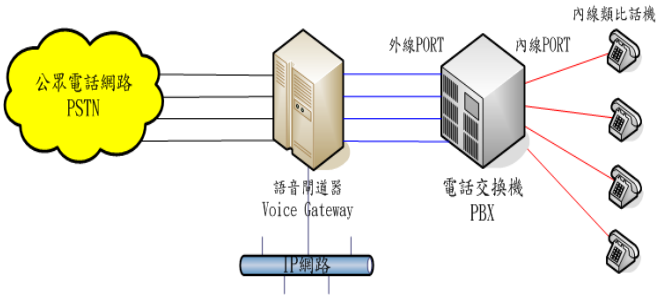
表一、各網路架構優缺點比較表

項目 \ 架構		專線式	MPLS VPN	IPSec VPN
成本	設備成本(一次性成本)	低	低	中
	每月租金	高	中	低
品質	可靠性	中	高	低
	穩定性	高	中	低

(二) VoIP

企業在企業網路上建置 VoIP 系統，可以在兩地將網路電話閘道器(VoIP Gateway)接入交換機或是話機，電話語音即可透過 Gateway 在 VPN 網路或 Internet 上傳送而達到通訊免費的效果。外地辦事處或出差人員同時可以使用 IP Phone 或 SIP 軟體電話與公司網內撥打。如果 Gateway 接上電信線路也可作遠端撥打或上車撥打之功能，可使在各地的電話機都可撥打節費系統。

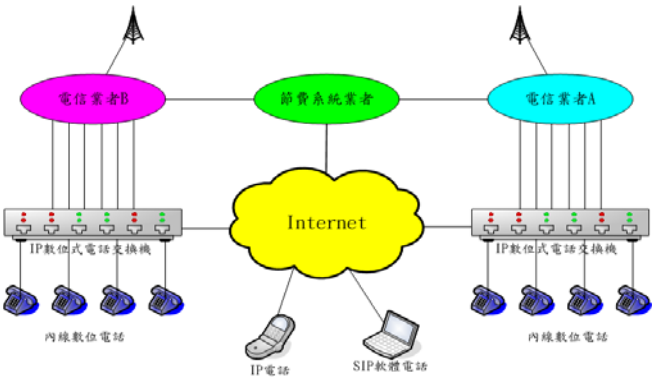
圖六是將一般類比的 PBX (Private Branch eXchange，電話交換機)連接語音閘道器的基本架構，在電話交換機後端的內線電話可以使用一般的類比電話機，是由傳統類比電話系統連接使用數位 IP 網路的最快也最便宜的做法。



圖六、電話交換機介接語音閘道器的基本架構

圖七則是使用 IP 話機時的架構，配合數位

式網路 IP 交換機，可以直接經由 Internet 的節費系統來連接其他的網路電話機，而達到降低電信費用的目標。



圖七、使用 IP PBX 或 IP Phone 的基本架構

優缺點比較

語音品質

以設備本身的通話品質來考量，除了採用的語音協定會影響通話品質之外，全數位式的 IP PBX 語音衰減較少，也能獲得比較好的通話品質，如果是使用類比交換機搭配 Voice Gateway，則需注意介面連接時的語音音量衰減問題。但是如果以網路的流量來考量，則不管是哪一種架構，都需注意所使用的通訊協定所佔用的頻寬，必須使網路上 Data 的流量不至於影響 Voice 流量的傳遞。

設備成本

通常企業的成本考量往往會主導建置案的設計，因此一般的企業在導入 VoIP 的環境時，多數會選擇保留原有設備的投資，所以比較常採用「交換機介接 Voice Gateway」的架構，這種架構比單純使用「IP PBX 或 IP Phone」的架構要節省較多設備投資的成本，另一方面在將來擴充話機時也能採購較便宜的類比話機。

(三) 企業網路的資安考量

防火牆的架設

在企業網路的環境裡，對外的網路上必須安裝防火牆來阻擋外界的惡意攻擊。而另一方面建置企業 VPN 之後，網路的範圍則隨著 VPN 更將延伸到相當大的範圍，因此要注意避免外來或內部的攻擊會透過 VPN 來影響其他端點，所以在各端點相互連接的線路上，也可以考慮加上一個防火牆來做阻隔保護的作用，如果企業內有使用無線網路，則無線網路上的防火牆與認證機制的設置更是必要。

採用 IPSec VPN 與 SSL VPN

在企業網路當中，如果規劃要讓員工可以由外部網路來存取企業網路的資源，則資源的安全考量就至為重要。一般我們可以依照需求與網路設備來規劃使用 IPSec VPN 或 SSL VPN。例如如果使用 Cisco 的防火牆，則可以規劃在員工的電腦中安裝使用 IPSec 協定的 Cisco VPN Client 軟體，使員工的電腦能夠在外部網路透過 VPN 直接連接企業網路。但是如果員工是派駐在各個客戶的辦公處所，則必須考量客戶本身的防火牆問題，因為有很多客戶為了保護其本身的商業機密或智慧財產，所以對外的網路連線經常多所限制，因此往往只有開放 WEB 能夠對外連線，此時採用 SSL VPN 的連線機制就是一個考慮的重點。

(四) 企業相關應用系統的備援

企業資料庫的備份

在企業相關應用系統中，最重要的當然是資料庫中的資料，因此按照一般的備援規劃，資料庫的定期備份必須確實執行，以往這些都是備份在當地的磁帶或磁碟中，再利用人工的方式帶到其他地點存放。

但是現在具有企業網路的企業，則更可以利用企業網路的方便性，資訊人員可以透過適當的備援設定，將備份的資料即時或定期地自動傳送至另一辦公室做異地備援以提升資料的安全性。

企業應用系統設備的備援

從另一方面來探討企業應用系統的備援，企業重要應用系統的不中斷使用也是一個考慮的重點。因此必須設計伺服器本身的備援機制，例如採用 HA (High Availability)的多伺服器架構、具 Cluster 架構的 Storage 等。如果企業的應用系統是影響其企業競爭力的重要關鍵，例如網購公司的購物網站或是金流伺服器等，除了資料需異地備援之外，企業這些重要的應用系統設備也必須考量異地備援，因此除了平日正常上線的系統設備外，在有企業網路連接的其他企業據點，也可以考量安裝備援設備以便隨時能接替上線，避免原本放置應用系統的企業據點或機房受到損壞時，整個企業之應用系統也隨之中斷。

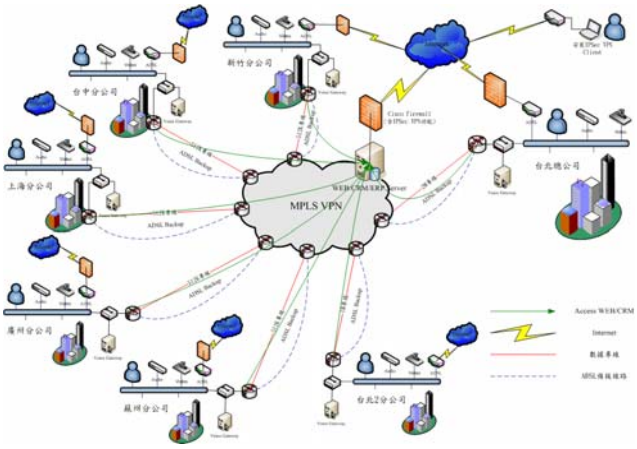
一條以上的網路通道備援

目前很多企業當已經非常倚重網路的使用，許多重要的資料來源都必須經由網路取得，企業內部的區域網路在維護上比較沒有疑慮，但是在跨區域的網路線路上，則必須有良好的備援規劃才行。例如日常會使用的 email 系統，如果對外網路中斷，則許多重要的資訊可能無法即時取得，就會影響業務之推展，根據經驗在對外網路斷線之後，一般情況下員工大約在幾分鐘之內就會反映 email 不正常，如果反映的人員是老闆或是有重要資料要傳遞的業務人員，則負責網路的資訊人員的壓力就會很大，所以網路的規劃必須有備援線路機制，當一條線路中斷時，必須能藉由人工手動或是設備自動切換到另一條線路上，建置企業網路也具有一部分的備援功能，因為每個企業據點都有網路連接，當 A 據點對外網路中斷時，就可以將其以更改網路路由的方式暫時切換藉由 B 據點的對外網路上網。

四、架構建置與分析

本節以一個中小型企業實際建置 VPN 與 VoIP 的案例來做詳細分析，在線路上不採用昂貴的點對點長途專線與 IPLC (International Private Leased Circuit，國際長途專線)或最低廉的 Internet IPSec VPN，而是採用較便宜但仍有一定頻寬品質的 MPLS VPN。如此建置成本不但降低，同時在線路品質穩定性的條件上也有相當好的保障。

此架構另一個好處是因為採用的 MPLS VPN 架構非常具有彈性，只要各據點利用 Local 專線或 ADSL 與當地的 NSP 機房連線即可，所以不管是小型企業的單一據點或是中型企業的多據點連接，在其辦公室據點的擴充上比較有彈性。本系統的 VPN 架構基本上是使用 NSP 本身的骨幹網路來建置 MPLS VPN，從每一個辦公室以專線連接到 NSP 的當地機房，再由各機房的路由器設定互相聯結為一個完整的 MPLS VPN，如圖八所示。



圖八、網路環境的建置

因為 MPLS VPN 的網路主要是由網路服務供應商的骨幹網路所組成，包含邊緣路由器與核心標籤交換路由器，因此所有的 MPLS VPN 路由設定皆由網路服務供應商依據骨幹網路的連結來加以設定，企業本身只需針對本身各據點的 IP 網段，分別於客戶端路由器加上 IP 路由即可。

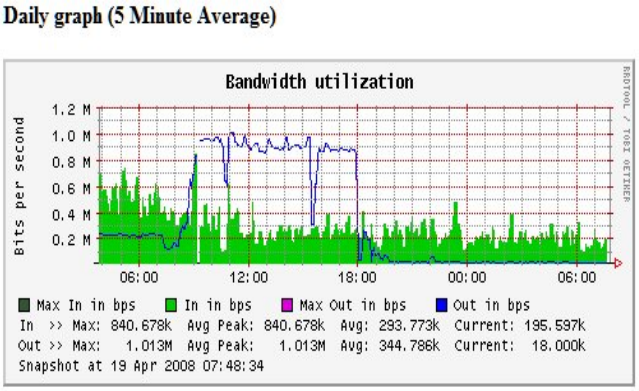
在提供員工連進企業內部網路的 VPN 部分是採用 IPSec VPN，利用防火牆做為 IPSec VPN Server，並結合在防火牆 DMZ 區裡一台 Radius 伺服器做登入驗證。當員工要使用 IPSec VPN 時，必須先在其電腦安裝 VPN Client 軟體，並針對防火牆的 VPN 環境參數做相對應的設定。

在語音設備架構的部分，則在考慮降低建置成本的需求之下，採用 Voice Gateway 直接連接各辦公室原有 PBX 的方式來達成 VoIP 的建置。因此依照各辦公室電話交換機現有的外線卡與內線卡的 Port 容量、電話線路的數量、預估使用人數的多寡等來決定 Voice Gateway 所需要使用的 Port 數，初估每個辦公室使用 8 Ports，則語音最高使用 50.4K (8×6.3k)的頻寬。如此各辦公室的話機、PBX 均不需更換，話機直接使用原類比話機即可，優點是使用者的使用習慣完全不變，使建置的阻力減少，而且在話機的汰購成本上，類比話機也比數位話機便宜很多。

網路流量的分析

利用 Network Sniffer 軟體收集網路的流量來做分析，一條 T1 專線的流量大約可以到達 1.544Mbps，由流量圖九來觀察網路的尖峰流量大約在都發生在早上 9 點至下午 6 點的上班時間，最大流量高達 1.013Mbps，因此大約還有 400kbps 的餘裕頻寬。

在語音的流量方面，因 Voice Gateway 的語音壓縮採用 G723.1，每個 Voice Gateway 有 8 個 ports，所以語音所需最大頻寬僅 50.4Kbps。根據這個流量觀察的結果來分析目前網路頻寬並不會影響語音的傳輸。但是如果後續的觀察有發現網路流量將近 1.5Mbps 時，則為了保持一定水準的通話品質，則必需採取頻寬管制的措施以保障語音的正常傳送。



圖九、網路流量

話務流量的分析

建置時在成本的考量之下，各線路並未配置頻寬管理設備，因為原本預測 Voice 的使用量達到最高時所占用的頻寬僅 50.4Kbps，所以在 T1 專線具有 1.544Mbps 的網路頻寬下，預估 Data 的傳送並不會對語音有明顯的影響。但是根據建置完成之後實際傳送資料封包的測試顯示，當兩個辦公室之間在做檔案傳送時，Data 的傳送量在瞬間會達到高峰，此時 Voice 的使用狀況就會有斷斷續續的情況出現，這種情況同時也會依照 Data 所傳輸的方向而有單方聽不到對方聲音的情形產生，因此為了確保語音的正常傳送，在這些線路上應該還是需要搭配頻寬管制的設備或軟體，才能避免發生語音傳送斷斷續續的情況出現。

五、結論與未來發展

由於企業的競爭力日益仰賴資訊的運用，因此企業網路在未來會更加重要與普及，目前網路供應商提供的網路架構與產品很多，由此次的建置經驗可以了解其中的 MPLS VPN 網路是一個性能優越且能彈性擴充的網路架構，很適合企業規模也具有彈性擴展空間與必需對花費成本比較有限制的中小型企業採用。

企業網路在電話語音節費的運用方面，因為行動電話結合行動上網的趨勢，目前已經開

始有業者將手機的行動上網結合企業 VPN 的 VoIP 環境來加以運用，只要企業的 VoIP 網路有安裝網路電話設備，則在公司外面的員工就可以透過手機的網路電話軟體直接以網內互打的方式撥回公司，如此就不會有通信費用的產生，再搭配其他節費系統的運用，就可以節省企業大量的電信費用支出。

以往企業的資料備援都是利用磁帶或磁碟備份之後，再運至其他地點存放，但是目前已經有許多企業開始利用企業網路的彈性優點，將重要企業資料即時或定時的透過企業網路備份到其他不同的企業據點儲存，但是將來更進一步的做法則因為企業網路的建置，企業另一方面同時也可以在各據點建立備援的機器設備，使備援系統隨時能在不同的據點啟用，使影響企業競爭力的重要營業系統能達到不中斷的目標。

六、參考文獻

[1] 蔡連發，中小企業網路應用程度與競爭力關係之研究，輔仁大學資訊管理學系碩士論文，Jun. 2004

[2] 陳坤成，企業網路引進 Extranet 對創造競爭優勢的影響，雲林科技大學資訊管理系碩士論文，Jun. 2002

[3] 王鍵義，”淺談 IP 與 ATM 技術的結合 — MPLS”， 中華顧問工程司

[4] 劉有順，多協議標記交換網路界接服務品質保證之研究，元智大學資訊工程學系碩士論文，Jun. 2002

[5] Seednet 教室，”MPLS 概論”， http://eservice.seed.net.tw/class/class0801c.html

[6] 劉文楨，” SIP VoIP 系統簡介”，中華電信訓練所

[7] 邱冠霖，在 VoIP 環境下對管線搜尋演算法之研究與實作，靜宜大學資訊管理學系碩士論文，Jul. 2005

[8] 陳政良， H.323 與 SIP 之 VoIP 閘道器架構探討，亞東技術學院資訊與通訊工程研究所碩士論文，Jun. 2005