

新一代公共圖書館網路規劃— 虛擬私有網路應用

Virtual Private Network for Public Libraries

張文熙

Shea-wenhsi Chang

國家檔案局籌備處資訊組

【摘要 Abstract】

目前國內公共圖書館網路規劃的方式是採取一個集中作業的中心，各分館或鄉鎮圖書館以不同速率的專線連入指定中心，再由這個中心連向所屬的台灣學術網路區網中心或縣網中心進入網際網路領域。傳統專線的運作方式在費用上與連線距離有關，距離越遠費用越高造成圖書館經營上的相當大的負擔。虛擬私有網路 (VPN, Virtual Private Network) 的運作方式基本上則是以透過現有的公眾網路透過適當的軟體技術，模擬成私有網路運作方式目的，除了可以節省通信經費外，透過虛擬私有網路建區分服務及保障網路服務品質 (QoS)，可以補足現行網際網路在通信控制上的缺失，本文旨在介紹虛擬私有網路的特性及基本概念，在未來公共圖書館網際網路的作業規劃上可以加以考量。

The paper is to introduce the concept of VPN (Virtual private network) briefly. Basically, virtual private network emulates leased lines and routed networks by software over public network, such as Internet. VPN can reduce overhead of dedicated lines to establish private connection with remote branches and offices. However, most of public library networks were connected directly by different kinds of traditional leased lines at the moment, so they have to endure high cost on communication for leased lines and low quality without better quality of services. On the other hand, QoS (Quality of Services) has become one of most

important issues for Internet services. It is very important for public libraries network planning to find out how to improve Internet services in public libraries in near future. VPN probably will be one of best solutions on this issue.

關鍵詞 (Keywords) : 公共圖書館 (Public Library)、圖書館網路 (Library Network)、圖書館自動化 (Library Automation)、虛擬私有網路 (Virtual Private Network)、區分服務 (Differentiated Services)

一、前言

圖書館自動化近年來在圖書館界全力地推動下有著非常令人驕傲的成績，除了在傳統圖書館的五大模組系統外，在圖書館內倡導網際網路資源應用，在全省各公共圖書館中圖書館界同道們的苦心隨處可見。為提供的免費網際網路服務，公共圖書館在對外的網際網路規劃也費盡了心力。通信上主要的困難在於公共圖書館通信經費來源有限，目前大多數的公共圖書館的作法均是在設備購置案中將三年的通信費用預估進去，和購入的設備保固年限一致，藉此暫時解決通信費用的問題。所幸隨著網際網路的重要性與日俱增，通信速率越來越高，通信的費用卻越來越低。同時隨著圖書館對資訊化服務的日益重視，及資訊媒體多元化的管理，相對地也陸續看到一些網路的規劃及作業上的問題，雖然短期之內不致於影響目前圖書館自動化作業，但是要進一步的有效利用頻寬從而提供更有效的服務方式，公共圖書館網路的規劃者有必要提早為下一代的網路應用進一步的思考。目前國內公共圖書館網路均是以使用數據專線連接的方式進行規劃。而公共圖書館網路規劃方式和學校及其他類型圖書館最大的不同處是在於廣域網路的使用，公共圖書館將各分散各地的單位（分館或鄉鎮圖書館）以不同類型的專線透過廣域網路連到集中的作業中心（文化中心或是總館），全時的提供連線作業服務。這樣的作業方式使得早期經費不足的圖書館無法支應高頻寬需求的網際網路查詢服務，因為專線計費很高而且和距離有直接的關係，只得以低速專線來應付必須的圖書館流通作業而略去網際網路其他的服務。這樣的情況一直到了 ADSL 非對稱數位迴路的方式上市後，提供物美價廉的通信方式才使得公共圖書館提供免費上網服務的可行性大為提高。但是傳統專線仍然存在，特別在文化中心對區網中心這一部分，另外已經使用專線連線作業的單位因為一時間無法汰換網路設備，所以到目前 ADSL 也沒有完全取代所有連線的單位。另外專線使用方式在同一時間內各連線單位是全時佔線的，對外線路永遠是固定出口，當連線單位間距離比較遠時，會有跨電路區的問題，造成收費比預期的高；並且所有的設備以分享的方式來佔用頻寬，無法讓重要的作業取得優先傳輸的權利。在這條專線上也不能作任何的服務或權限的限制，如果您在網路的管理上開始發現到上述問題時，則表示現行網際網路在控制服務能力上有缺憾，進而開始思考未來解決之道時，虛擬私有網路 (VPN, Virtual

Private Network) 出現了；它就是一種可行的方式，藉此向各位同道介紹或許可以作為未來在公共圖書館網路規劃方式的參考。

二、傳統專線的問題

當大部分的讀者在上網瀏覽網頁時，可能流通櫃台有讀者正因為賠款的問題和館員起了衝突，館員因此要立刻連回中心主機做進一步系統查證時，在現有的網際網路架構下並不會因為問題的急迫性而優先傳送，同時為了做進一步查證所必須傳遞的資料可能涉及較高隱私的問題，網際網路並不會在傳輸上對這些資料作例外的處理，仍然是以和其他的資料一視同仁平分固定的網路頻寬。又如果在作業的同時可能有某要員正在準備民代質詢的資料時，因為其他的使用者也正在使用，對外網路在滿載的情形下使得他的作業受到影響，即便他想以高價來取得暫時保證頻寬以維持一定的速度卻無法做到。這些幾個假設的情形說明了現有網際網路的服務形式中缺乏有效的服務品質保證機制。

國內大部分公共圖書館的總館或分館都是採用租用專線來向外連接，大部分的公共圖書館使用的架構是，分館（或是鄉鎮圖書館）連到文化中心（文化局）圖書館透過專線集中資料流向台灣學術網路的區網中心或縣網中心進入網際網路的世界。租用專線的原始用意，就是節省自行佈線的經費，但是租用專線的使用方式是點對點，一對一的模式，觀念上和自行佈線是一樣的，不論您用不用價格是一定的。換言之在不用的時候會價格照常計算。但是如果公共圖書館使用一般的公用網路（如電話網路）撥接使用時也有缺點，為了省錢不傳送資料就斷線，這時又有再撥等待的問題，對即時作業為主的流通台就不太適用。另外，目前各地方公共圖書館網路連結的方式都是以將專線集中到同一個點（文化中心或總館），特別在主從架構的應用環境更成熟後未來可以會有新服務需求產生需要由分館對分館直接連接，在這種情況下以現有架構上必須透過中心分別和這兩個館連線溝通，可能會不如直接另拉一條線去連接這兩個館來得有效率。如果分館彼此的連接需要越來越重要的話，分館越來越多時為解決分館間連線問題，連線數會和分館數的平方數正成正比，這樣一來專線線路成長量對公共圖書館而言太大很容易就無法負擔，這些問題就形成了應用虛擬私有網路的基本理論基礎，如何以公用線路的價格以虛擬連結的方式去達成私有專屬線路服務品質的目的就是未來在網路應用的新走向。

三、頻寬是有限的

網路應用的越廣，使用者對網路的要求越來越高。雖然網路技術也一直隨著使用者的需

求跟進，但頻寬最終是有限的。圖書館要如何規劃網路，讓使用者始終可以滿足頻寬的需求是一個很困難的課題。對讀者及圖書館而言，過去都缺乏頻寬危機意識的觀念，一般認為只是單純通信費的問題，只要有足夠的經費就可以解決通信上的問題。但實際上會有可能將來因為需求量大增，根本不可能有專屬線路給您使用的情形發生，通信媒體本身也有物理性質上的極限。對已有高速專線의圖書館未來有可能處在長期忍受高費率低享受之事實。另外在網際網路的發展應用層面越來越高，不僅需求高保密、高頻寬，更要有服務品質 (QoS) 之保障，這樣的網路應用需求開始在電子商務領域被提出來，很明顯地在電子化政府及圖書館電子化服務也開始有相同的需求，因為電子商務交易的方式在政府服務一樣是非常重要的部分。因為網路建設之速度永遠趕不上使用者增加之速度，加上現有網際網路使用之通訊協定並無頻寬保證之機制，這使得網路更容易擁塞，因此有可能反而降低上網之意願。這種情形在通信經費短少的鄉鎮圖書館以低速 14.4 k 專線連線作業的情形很容易體會。如何提昇網路服務品質應該是公共圖書館網路規劃的下一個主要課題。

四、何謂虛擬私有網路

虛擬私有網路 (Virtual Private Network, VPN) 的觀念是要在現有單一網際網路上邏輯性的區分多個虛擬的私有網路，並利用隧道 (tunnel) 之觀念提供保密之通訊和服務品質之保證 (QoS, Quality of Service)。觀念上很簡單就是如同每個虛擬私有網路就像馬路，在馬路上劃分不同的車道 (隧道) 一樣，有公車專用道也有機車專用道，不同車道作不同的管制。

Ferguson, P 和 Huston, G 就 VPN 下一個定義¹，架構於公共非私有存取模式的網路環境下，分割出特定的部分去組成子網路，同時允許這些子網路內的節點彼此互相通訊；而這些節點、通信連結與相關的網路協定就構成 VPN 的實體架構。簡單的說 VPN 就是在公共網路基礎架構 (如 Internet) 上所架構出的私有網路。為何需要以虛擬的方式來建置私有網路服務呢？很顯然是因為價格考量是一項主要的因素，因為現有公眾線路的使用可以節省高額の佈線成本，如果可以透過軟體的方式完成私有網路可以專屬某一特定使用者的特性就可以解決這個問題，這樣的需求顯然是網路演變之必然趨勢。而虛擬私有網路在技術也有不同的形式，有模擬專線的方式，也有模擬可繞路的網路方式，但基本上都會符合上述對虛擬私有網路的定義。

1 Ferguson, P. and Huston, G., "What is a VPN?", April 1 1998, <http://www.employees.org:80/~ferguson/vpn.pdf>

五、確保通訊服務品質

網際網路目前存在一個相當重要的問題，就是目前整個網際路缺乏有效的服務品質保證機制。而虛擬私有網路要建置在網際網路中，一樣會碰到相同的問題，這使得問題的難度變得更高。IETF（Internet Engineering Task Force）組織中之 Integrated and Differentiated services working group 已有相關之討論議題，如 RSVP 之觀念，但也只能保證路由器到路由器（router-to-router）的服務品質。不像 ATM Forum 所提之流量管理（Traffic Management）中可以保證端點到端點（end-to-end）的服務品質。在而在網際網路之訊務皆為不可準確預測的環境下，在虛擬私有網路中提供 QoS 就目前來看雖然是大勢所趨但並不是很簡單的，不過對於公共圖書館的規劃者了解這個方向應該就足夠了。

六、區分服務 (Differentiated service) 的概念

圖書館在網路化之後，分館與分館之間、分館與總館之間、加上不同的單位間的館際互動使得網路運作的方式隨之複雜。例如國立台中圖書館所規劃的全國共同性資料庫就是一個很好的例子。這種作業方式其實就是所謂企業子網或是網內網路 (Intranet) 及企業連網 (Extranet) 觀念的應用。在這種環境下資訊流通管道的效率與資訊安全的考量就更形重要。虛擬私有網路 (VPN) 在這一類的服務規劃就相當適合，成為解決這類問題的有效方案，很自然地 VPN 就成為最近網際網路發展中的熱門技術。

目前在網際網路服務上只提供所謂的全力資料傳送 (best effort data delivery) 服務品質 (Quality of Service)，但是往往在網際網路的應用上會發生一些臨時性的特殊區求而受限於這種全力資料傳送的模式而使不上力，像是前面所說的要員的資料查詢需求等。為了能夠擴大網際網路在即時應用服務的功能，那麼就必須修改網際網路架構使能支援即時服務品質，同時控制端點對端點之封包延遲才可能改善通信服務品質。IETF 組織首先提出整體性服務架構 (Integrated Service Architecture)，利用 RSVP (ReSerVation Protocol) 協定依據訊流規格 (flow specification) 來保留網路資源，以保證此訊流之服務品質要求。然而，於此架構下，所有路由器及主機皆需對每一訊流保留一份訊流狀態而造成比例分配的 (scaling) 問題。因此，區分服務架構 (Differentiated Service Architecture) 繼而被提出，此架構介於目前網際網路所謂的全力傳送及利用 RSVP 之整體性服務間，不但使網路能滿足各種異質應用之需求，藉此訂定不同之收費標準，同時解決網路使用比例分配 (Scaling) 的問題。目前 IETF 下有正式的 DiffServ 工作小組，負責制定有關區分服務相關標準。而這種區分服務的觀念對圖書館網路應用的影響可能包含不同優先順序的傳送權利，及搭配而來的收費

方式，服務越高者收費越高。ISP 業者可能對收費區分的部分更有興趣，實際上許多 ISP 也都在這個方向去做。

七、VPN 的效益與缺點

圖書館可能會需要利用 VPN 的技術，透過現有的 Internet 連結來與其他圖書館或資料供應商作資源分享與資訊交換，在兼顧效率與安全的情況下能夠降低連網的費用的考量這些形成發展 VPN 有利的環境。和傳統私有數據網路 (PDN) 來作比較，VPN 因為使用公眾數據網路作為通訊的通道，所使用的頻寬、路由器、網路管理設備人力等均是與他人分享使用，不但設備、頻寬的利用效率高，同時使用者的成本也可以大幅的降低。傳統的大型公共圖書館要將分散各地的分館連結成一個網內網內網路，以便能分享各館資源或便於館內部資訊的傳遞時，傳統的做法是使用專線將要連結的各點連結，這種做法的缺點是：專線的費用與頻寬和距離有關，當要連結的兩點距離遙遠時，專線的費用便變得非常昂貴。當規模持續變大，要連的節點增加時，如果要將各節點完全連結，所需要的專線數將與節點數的平方成正比，這使得大型的網內網路 (intranet) 變得不可行；但若僅用少數專線將節點作串接，當其中某一個節點或專線故障時，將造成整個子網被分成兩個或兩個以上造成彼此無法通信，而虛擬網路就比較有彈性，可以選擇替代的路徑。同時利用專線建置網路，網路供應商只提供電路，用戶本身必須管理眾多的網路設備如路由器等，而這些管理成本相當高。當然虛擬網路不是沒有缺點的它會受中繼網路影響；但未來將可配合 RSVP 協定²做到虛擬專線 (virtual lease line)，以提高網路效率。

另外目前在大多數的文化中心等級的圖書館所提供撥接的服務，過去是以服務讀者上網為主，但是因為 ISP 的興起，撥接服務對圖書館而言吃力而不討好，主要使用來提供館員或維護工程師作在需要時從遠端撥接進行系統問題的處理。傳統的做法是由圖書館申請若干個門號，並購置撥接設備（如終端機伺服器）、建置使用者資料庫與安全控管資料，這種作法同樣有很大的缺點：用戶必須購置並維護撥接設備、單獨支付門號的費用、設備管理維護的人力費用以及可能需付長途電話費用。使用 VPN 技術的虛擬撥接服務 (VPDN, Virtual Private Dialup Network) 與一般撥接服務除了在建置成本和維護費用減少之外，需多一道 IP Dialing 的手續。兩相比較雖然 VPN 因有 overhead（通信成本）的關係，效率較差；但是若中繼網路速度快，且使用者是以連結區域網路方式取得網路存取權，則可以提高效率。而與現有的公眾網路直接連線相比較（如 Internet）VPN 可以提供強度不同層級的安

2 A. Mankin, F. Baker, S. Bradner, M. O'Dell, A. Romanow, A. Weinrib, L. Zhang, "Resource ReSerVation Protocol(RSVP) Version 1", RFC 2208, Sep. 1997

全機制，這個就是目前一般撥接服務控管方式作不到的部分。

八、VPN 的分類

只要滿足前述的 VPN 定義都是 VPN 的一種，換言之 VPN 可以不同的形式存在。可以依照建構 VPN 所使用的協定或依 VPN 的服務模式對 VPN 來加以分類。就依照建構 VPN 所使用的協定來分類，VPN 可分類為以 IP 協定為基礎的虛擬私有網路和非 IP 協定為基礎的虛擬私有網路。IP Based VPN 和 Non-IP Based VPN 兩大類。就前一類而言又可細分為網路層虛擬私有網路 (Network Layer VPN)、傳輸層虛擬私有網路 (Transport Layer VPN) 和應用層虛擬私有網路 (Application Layer VPN) 三類。

而非 IP 協定為基礎的虛擬私有網路 Non-IP Based VPN 主要包括有 Frame Relay Based VPN 與 ATM Based VPN 兩種。IP Based VPN 和 Non-IP Based VPN 主要的差別是前者 VPN 的鏈結是透過網路層 (network layer) 或網路層之上的協定建立 Tunnel 來完成 VPN 的功能，而後者是藉由資料鏈結層 (data link layer) 建立一個虛擬電路 (virtual circuit) 來完成。比較簡單的說法是根據 OSI 的七層網路協定，IP 是網路層協定，使用網路層以上的虛擬私有網路就是以 IP 為基礎的。因此網路層在傳遞上的特性，要必須透過如 RSVP 等協定來達成控制其網路服務品質 (QoS) 作法上比較困難，後者則要提供網路服務品質保證較容易，但相對的在網路組態、管理和擴充性上較為困難，因本文重點不在說明 VPN 技術故不在此加以詳述。

九、VPN 相關產品

要使用虛擬私有網路的方式來建構公共圖書館網路，必須要選擇具備 VPN 能力的相關產品才能完成。就筆者所了解的部分以國外廠商開發的產品為主，國產品尚少見到，未來應該會有更多不同等級的產品可供選擇。建置 VPN 的產品可分為硬體與軟體兩種不同的方式。目前國外各大型網路設備廠商多已經有這類的硬體產品上市，如 Bay Network 的 Extranet Switch Series，CISCO 的 1720 VPN Router，3COM 的 PathBuilder Series 等。目前 VPN 設備銷售方式多是和路由器及防火牆與相結合，也就是在原有的繞路功能或防火牆功能外，附加上 VPN 的功能。而以軟體的方式開發的 VPN 服務軟體套件，可以在用戶端的軟體平台，如 NT 或 Unix 等作業系統平台上運作，利用軟體建立各別的資料通道 (tunnel) 來達成 VPN 的功能。軟體的優點是價格較便宜，缺點則是使用軟體執行 VPN 相關功能如繞路和資料加密 data encryption 等效率會較差。使用者在建構時可以自行考量。

十、國內外 ISP/VPN 市場狀況

國外的 ISP 業者多已提供或正計劃提供 VPN 服務，以 AT&T 為例即以 Frame Relay 為網路的基礎架構提供 VPN 相關服務。國內的中華電信、SeedNet、HtNet(仲琦資訊)、TTN(台灣電信網路)等 ISP，目前也已開始提供 VPN 服務。各家在應用策略上有些不同，有興趣的讀者可以親洽這些 ISP 去了解會取得比較深入的答案。大致上有提供虛擬撥接(VPDN)的服務及針對以企業用戶為主，利用 Frame Relay 作為網路骨幹，提供 VPDN 和 VPRN(Virtual Private Routed Network)服務。也有提供以交換技術為主 switching based VPN 給提供企業用戶包含網路連結與電話語音的整合方案。個人以為圖書館對網路服務供應商而言和其他的企業體沒有什麼不同，差別只是在傳送資料的內容有所不同而已。個人以為公共圖書館網路連線的方式並非是一成不變的，公共圖書館在未來應該對選擇最佳網路供應商作規劃上的考量，因為有虛擬私有網路的技術可以取代目前直接連線方式，又可以提高服務品質。

十一、結論

虛擬私有網路的架構模式也許對大部分的圖書館館員是一個新的名詞，個人以為在圖書館館員的立場不必深入了解這樣的技術內容，但是為提供整個公共圖書館有更好的網路服務品質，館員們卻有必要去了解的它在應用範圍。因為資訊市場的技術瞬息萬變，館員們時時保持對網路市場資訊的掌握程度是維持圖書館服務品質的不二法門。未來在網際網路的應用上一定會出現更多各類交易行為，圖書館也可能會提供許多付費的服務，例如線上資料庫的列印，或是讀者透過圖書館的網路去進行這類的網路活動，如何提供資料安全的控制，這些都有待館員們去思考的。筆者認為虛擬私有網路應該可以在公共圖書館網路規劃上有應用的空間，期待各位同道能夠對此加以指正。

參考資料：

1. Bryan Gleeson, Arthur Lin, Shasta Networks Inc. A framework for IP based Virtual Private Networks, *Internet Engineering Task Force INTERNET DRAFT* September, 1998
2. 曹志誠，王培元，虛擬專線網路於電子商務之應用，《中央資電博士班電子商務課程報告》88,1,5