管理服務平台的最佳代表~

MPLS 虛擬私有網路服務

/台灣思科系統提供
電信事業群技術經理　錢小山

隨著網路經濟時代來臨、相關技術不斷進步、及使用需求急劇增加，多重協定標籤交換虛擬私有網路〔Multiprotocol Label Switching VPN, MPLS VPN〕技術的相關應用也日益多樣化，而 Cisco IOS 軟體中智慧型網路功能更已順應趨勢，升級支援 VPN 方面應用。因此，網路服務供應商可在 MPLS 基礎網路架構的加值型、共享式服務中獲得多種組合選擇，並以遠低於以往的價格來提供這些服務，讓許多企業用戶樂意將網路管理委外處理。

此外，服務供應商還可以運用 VPN Select 功能，在寬頻存取網路中，將客戶的 MPLS VPN 服務擴展到遠端用戶處，且無須考量其終端存取供應商之限制。而 Cisco 熱備用路由協定〔Hot Standby Routing Protocol，HSRP〕和虛擬路由器備援協定〔Virtual Router Redundancy Protocol，VRRP〕，目前也已應用於 MPLS 供應商端（PE）的路由器上，提供存取鏈結備援功能〔access link redundancy〕。此項雙主機功能不僅加速 MPLS VPN 服務的普及，搭配 Cisco IOS 軟體特殊功能，基本的 ping 和追蹤路徑功能亦可升級，以便讓服務供應商測試每條 VPN 網路連線的運作狀態。

VPN 資訊內容

PE 路由器的軟體功能除了可以探知 VPN 資料內容，並能區分不同用戶的 MPLS VPN 與處理網路流量，舉例來說，MPLS 技術中的其中一項獨到優勢即是僅需一台 PE 路由器，就可同時紀錄多個用戶的 VPN 路由/轉送（VPN routing/forwarding, VRF）表。由此可知，PE 路由器可把來自不同 VPN 的網路流量分隔開來，並保持隱密性。

目前，除了基本 MPLS VPN 連接和隱密性外，個別網路服務也受惠於 MPLS VPN 資料內容的讀取。使用這些功能，服務供應商可經濟有效的透過單一 PE 來為多個用戶提供額外管理服務，其項目如下：

- IP 位址管理，包括網路位址轉譯〔NAT〕和動態位址分配服務協定〔DHCP〕服務。
- 網際網路存取管理。
- VoIP 服務的離線呼叫功能。
- 在單點廣播 VPN 流量中傳送多點廣播流量。

為企業用戶帶來更多委外處理選擇

若把部份特定服務內容交由服務供應商之網路直接處理，將可為企業用戶帶來許多益處。而就 MPLS VPN 所衍生出的更多服務選擇來說，即可讓企業

享受由服務委外處理所帶來更大經濟規模效益的好處。舉例來說，一家擁有 5 或 10 個辦事處、而每各地點都只有 15 台電腦的企業管理者，為了節省專人管理 IP 位址相關業務之成本，必須審慎考量是否需由服務供應商來代替企業本身處理其特定執行內容，當然，這也是格外吸引中小型企業目光的重要特色。

因此，藉由採用支援 VPN 的 NAT 和 ODAP 服務，企業就可在服務供應商網路中，運用每個用戶所共同使用的共享式 DHCP 和 RADIUS 網路設備，且無需再花費額外管理成本。此外，企業還可將系統資源的升級當成是服務費用一部份，而不必支出多餘成本來升級或更替設備。

Cisco IOS 軟體呈現的嶄新功能

基本上，VPN 所擁有的先進網路服務，包括網路安全、點對點私密鏈結等，並可藉由其管理系統提供企業用戶一致性的鏈結、網管政策和安全鑰匙管理方式。而 Cisco IOS 軟體則具備支援 VPN 的監視、回報、入侵偵測和政策管理等功能，對於相關運作、功能及優勢，以下將做一簡單描述：

- **MPLS VPN 的 NAT 功能：**服務供應商可以在網路中安裝單一個網路閘道器，將多個 VPN 用戶的私有 IP 位址（private IP address）轉換成在公眾網際網路中使用，且是全球唯一的 IP 位址。經過這個動作，這項功能則會將指定的 IP 位址和 VPN 資訊相互聯繫，並引導公眾網際網路傳回的流量送到正確的用戶網路中。

就企業用戶觀點，支援 VPN 的 NAT 服務可讓多重服務聚集在一起，例如：可在單一存取線路上提供企業網路與網際網路的鏈結，以及為離線用戶將 VoIP 訊務轉送到公眾電話網路之中。藉由減少分散的網際網路連線，而使用專線線路數和路由器埠數，用戶可減少每個月重複的服務項目，以及成本支出。

- **MPLS VPN 的 ODAP 功能：**這項功能讓跨越多個 VPN 的 IP 位址管理機制可自動化處理，並同時維持現有企業 IP 位址規劃的完整性。目前服務供應商必須為每個用戶的 VPN 分別提供 DHCP 或 RADIUS 伺服器（或者企業必須自行提供），一旦設備容量達到上限時，新的位址就必須用手動方式來增加。相對的，在管理分享服務〔Managed Shared Services〕中，單一 Cisco DHCP 伺服器不僅可用來為多個 VPN 的用戶設定 IP 位址，而且，一旦設備的定址超過上限時，MPLS 的 ODAP 功能就會自動啟動擴增整體位址庫（address pool）的程序，向 DHCP 或 RADIUS 伺服器要求新的位址庫。

- **多點廣播 VPN 功能：**管理分享服務〔Managed Shared Services〕解決方案的模組讓 IP 多點廣播服務可在 MPLS VPN 上傳送。大多數需經常性向多個分散用戶群傳送內容的組織單位都會使用多點廣播技術，因為這可讓他們因應用戶數變化，並解決串流傳輸時頻寬需求的問題。多點廣播網路藉由將單一封包串流送到群組位址（group address），而不是將封包複製成好幾份後，送到多個終端位址。雖然 MPLS VPN 標準現在並沒提到如何處理多點廣播訊務，但是到目前為止，支援這些功能的機制都必須在有參與 MPLS VPN 的用戶端

（CE）路由器間，設立一個完全網狀的一般性路徑選擇封裝（Generic Route Encapsulation，GRE）通道。

結論

在早期建設中，MPLS VPN 主要被當成一種比虛擬電路、Layer-2 VPN 用戶服務更便宜的方法，來為企業提供網狀企業網路連接之用。而 MPLS VPN 更為經濟有效益的主要原因，則是因為其採用非連線導向的 IP 位址資訊來進行封包傳送的動作，而不需要企業通訊兩端之間，在事前建立連線導向的虛擬電路。大型企業除可向傳統電信業者租用專線服務外，也能透過新興網路服務供應商之共享數據網路，租用包括訊框傳送網路(Frame-Relay)、非同步傳輸網路(ATM)、甚至是網際網路(Internet)來建構電子商務的通訊傳輸平台。

MPLS 已應用在 Cisco 140 個服務供應商網路之中，MPLS 會被採用的另一個因素是它為服務供應商帶來聚集的好處。依循 Cisco IOS 軟體加強功能，已讓 MPLS 骨幹網路可在一個聚集的多重協定核心中支援 IP 網路服務，以及傳統的 Layer 2 服務。這些 Layer 2 服務包括了：Frame Relay、ATM、乙太網路、點對點協定序列連線，和高階資料鏈結(HDLC)控制電路模擬服務。

由於 MPLS 擁有多樣化的功能且不斷新增，因此已成為一服務創新平台，不僅能滿足客戶對於網路安全性、服務品質控制、高彈性與可擴充性的需要，也將持續穩定發展，與下一代光纖通訊網路技術相互結合。當然，服務供應商的利基也會因此而擴增，以便提供企業用戶更豐富的委外處理服務項目。