多重標籤交換協定 (MPLS)之安全應用解析

台灣思科系統提供/
台灣思科系統電信事業部技術經理 錢小山

隨著網路安全越來越受到重視，目前很多企業都考慮如何將傳統 Layer 2 虛擬私有網路，如：非同步傳輸模式（Asynchronous Transfer Mode，ATM），或是訊框中繼（Frame Relay），轉換成以多重標籤交換協定（Multiprotocol Label Switching ，MPLS）為基礎的服務。由於多重標籤交換協定已成為提供虛擬私有網路（Virtual Private Network，VPN）服務中，愈來愈普及的技術，因此多重標籤交換協定架構的安全問題也愈受重視。本文將介紹多重標籤交換協定/邊界閘道器協定（Border Gateway protocol，BGP）的虛擬私有網路架構，從安全角度探討多重標籤交換協定架構安全的整體狀況，並與傳統 Layer 2 服務比較，提供服務供應商及企業關於多重標籤交換協定架構安全之建議。

多重標籤交換協定網路安全性的需求

現今許多服務供應商與客戶，常將以多重標籤交換協定為基礎的網路解決方案與傳統 Layer 2 虛擬私有網路解決方案相互比較，如訊框中繼與非同步傳輸模式等。以下將針對多重標籤交換協定的安全性分別探討：

- **位址空間（Address Space）與路由區隔**

在多重標籤交換協定服務中，兩個沒有相互連接的虛擬私有網路位址空間（Address Space）是屬於完全獨立性質，也就是說，兩個不相連的虛擬私有網路，可運用 10/8 網路而不會彼此干擾。

- **隱藏多重標籤交換協定核心架構**

一般來說，外部網路（網際網路或是任何相連虛擬私有網路）是無法看見多重標籤交換協定核心網路的內部結構，即使看得見，也不會導致安全問題。

- **對攻擊的抵抗**

攻擊有兩種基本形式：一是癱瘓服務攻擊，使獲授權使用者，無法使用網路資源。二是侵入式攻擊（Intrusions），使未獲授權使用者，可以進入使用網路資源。

表一：兩種基本攻擊形式

	有存取管道	無存取管道
獲授權用戶	正常	癱瘓服務
無授權用戶	侵入	正常

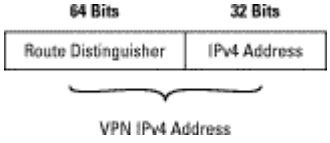
以表一內所描述的侵入式攻擊而言，目前已有兩種基本網路保護方式。第一，強化可能被濫用之協定（例如路由器的 Telnet）；第二，結合封包篩選，或使用防火牆以及隱藏位址方式，使網路不易進入。相較之下，癱瘓服務式攻擊則較容易執行，只要知道一個網際網路位址，駭克即可攻擊主機；而唯一使網路不會因遭受攻擊而癱瘓的方法，即是透過封包篩選與隱藏位址，讓駭客無法取得資料。

多重標籤交換協定的安全性分析

以下我們將就前述幾個安全性考量，來分析多重標籤交換協定的架構。

- **位址空間與路由區隔**

- **圖一：VPN IPv4 位址的格式**



多重標籤交換協定允許不同的虛擬私有網路使用相同位址空間，而使用的方法是在原本 IPv4 位址前面，加上一個 64 位元路由識別碼 (Route Distinguisher，RD)，使它成為唯一位址。這種延伸的位址又稱為虛擬私有網路 IPv4 位址，如圖一所示。所以客戶在使用多重標籤交換協定服務時，並不用改變其現有網路中的位址設定。

而每個供應商端的路由器中，分別為其所連結的虛擬私有網路維護了一份虛擬路由及轉送表 (Virtual Routing and Forwarding instance，VRF)。供應商端路由器中每一份虛擬路由及轉送表都記錄該虛擬私有網路所執行的通訊協定，以及資料傳輸路徑。因為每一個虛擬私有網路的路由結果，都分別記錄在不同的虛擬路由及轉送表中，所以供應商端路由器所連結的各個虛擬私有網路間，並不會相互影響。

在多重標籤交換協定核心與供應商端的路由器之間，要達到這種虛擬私有網路的區隔，可在多重邊界閘道器通訊協定(Multiprotocol BGP, MP-BGP)中，加入一個唯一的虛擬私有網路識別碼。因為核心網路中的虛擬私有網路依靠多重邊界

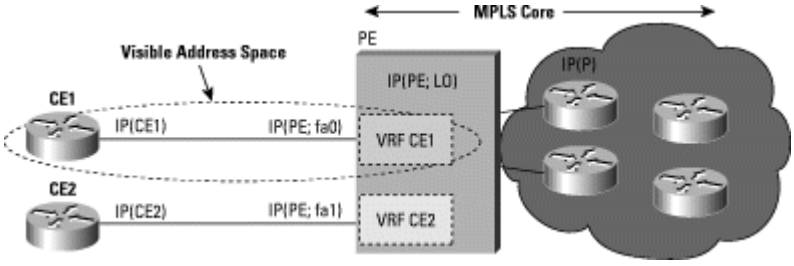
閘道器通訊協定來交換資料，而這只會傳送到供應商端路由器中，不會傳送到核心網路，所以跨越多重標籤交換協定網路的虛擬私有網路就可各自獨立運作。

- **隱藏多重標籤交換協定的核心架構**

網路供應商與客戶通常都不希望他們的網路拓僕曝露給外界知道，以保護網路安全，使駭客難以攻擊。如果駭客不知道目標位址，便只能靠猜測或是情報來獲得位址資料加以攻擊。

圖二顯示核心網路位址是不會被外界看到的，但是供應商端路由器（Provider Edge Router，PE Router）上其他位址，就不屬於該虛擬私有網路安全保護範圍。

圖二：隱藏網路核心基礎架構



總之，在單純 MPLS-VPN 的服務中，若無其他網際網路存取路徑，位址資訊就不會暴露給第三者知道，換句話說，若多重標籤交換協定網路沒有和網際網路連結，安全性是等同於訊框中繼或是非同步傳輸模式。但如果多重標籤交換協定網路和網際網路連結，就會暴露至少一個位址給服務供應商，如此位址也等於讓外界知道。

- **抵抗駭客的攻擊**

其他可能攻擊方式，就屬直接攻擊多重標籤交換協定的核心，然後再由核心攻擊其他虛擬私有網路。針對多重標籤交換協定核心的攻擊有兩種基本的方式：

- 直接攻擊供應商端的路由器
- 攻擊多重標籤交換協定傳訊機制（Signaling Mechanisms）(大部分是路由機制)

而若要攻擊多重標籤交換協定網路中的設備，首先要知道設備位址，但多重標籤交換協定核心架構對於外界而言，通常都是隱藏的。所以攻擊者並不知道網路核心中任何路由器位址，也無法攻擊其隨意猜測的位址，因為對於多重標籤交換協定的核心而言，每個虛擬私有網路位址空間都是獨立的，因此就算是駭客能猜到核心 IP 位址，這個封包仍舊無法抵達核心路由器。

大致看來，駭客不可能由某個虛擬私有網路入侵到其他虛擬私有網路或多重標籤交換協定核心，但理論上卻可能利用路由協定（Routing Protocol）的弱點對

供應商攻擊，以影響其他虛擬私有網路客戶，所以必須確保供應商端路由器安全無虞，才能保護所有與之相連的網路使用者。

- **標籤仿冒**

在多重標籤交換協定網路中，資料封包的傳送不是由 IP 位址來決定，而是根據供應商端路由器加在封包上的標籤而定。因此，理論上攻擊者可以仿冒多重標籤交換協定封包的標籤資料，以進行駭客攻擊。而客戶端傳送資料給供應端時，是使用 IP 通訊協定而非多重標籤交換協定，傳輸時所需要的資訊是由供應商端路由器執行，根據其路由設定，供應商端路由器會產生一個標籤放置在資料封包前端，以說明資料封包的來源及去向。因此對於所有進入多重標籤交換協定網路的介面來說，只需要 IP 封包，而不需標籤封包。所以，為了安全考量，供應商端路由器永遠不應該接受由客戶端路由器傳來具有標籤的封包。就 Cisco 路由器而言，所有經過客戶端路由器傳來含有標籤的封包都會被棄置。因此在供應商端路由器拒絕接受任何有標籤封包的情況下，便不可能由外界加入標籤仿冒。

接下來還有一種可能受攻擊的情況，就是駭客將仿冒 IP 位址的封包送到多重標籤交換協定網路中。不過如前所述，在供應商端路由器中，每一個虛擬私有網路位址空間都是獨立的，各自擁有自己的虛擬私有網路表，這種攻擊方式最多只能傷害到發送攻擊封包來源的虛擬私有網路，所以多重標籤交換協定網路便不會有漏洞存在。

結論

以Cisco標籤交換（Label Switching）技術為基礎的多重標籤交換協定，是專為解決今日服務供應商所面對的問題所設計，亦即是如何建立彈性十足的網路基礎，以提供IP加值服務。多重標籤交換協定的標籤轉遞機制，不但能簡化複雜網路中的 IP 流量路由問題，更能輕鬆提供可靈活擴充的 IP 加值服務。Cisco在多重標籤交換協定及Cisco IOS軟體和新興的開放式標準的應用方面，更獨具長才，可為企業在建構 IP 服務方面提供基礎。