新的契機或危機？－談 IPv6 網路之安全威脅與防護

杜廣輝 / 財金資訊公司安控部高級工程師

一、前言

現今全球各地的人們可以打破地域限制，隨意瀏覽網頁，利用 LINE 等軟體進行即時通訊，觀賞 YouTube 上各類影音分享，林林種種全都拜網際網路蓬勃發展之賜；而構築整體網際網路架構的基石就是 TCP/IP 通訊協定，TCP 協定 (Transmission Control Protocol) 主要負責資料傳輸控制，以確保資料完整傳送至接收端。IP 通訊協定 (Internet Protocol) 則主要負責網路定址，針對網路上的節點 (node)，提供獨一無二的位址 (address)，以資判別。

現行通用的協定版本是 IPv4，位址表示方式是四個十進位制位元組的數字，中間以點分隔，例如 168.95.1.1。IPv4 規格自 1981 年於網路標準技術文件 RFC 791 公布使用至今，正面臨一個無法解決的問題 --IP 位址即將用盡。IPv4 位址編碼長度為 32 位元，理論上可使用的位址數量為 2^{32} 個，大約 42 億個左右，就其設計當年具備上網能力的電腦數量及使用者區域而言，應該是綽綽有餘，難以想像會有不足的一天。

然而，隨著網際網路應用蓬勃發展，個人電腦快速進入每個家庭，IP 位址需求日益增加，網路服務提供者 (Internet Service Provider，簡稱 ISP) 逐漸感受到壓力，遂開始縮減每一申請案件的 IP 配發數量。近年來，隨著行動裝置科技發展，具備上網能力的設備不再侷限於電腦，而配合無線及電信網路提供的便利服務，家電、智慧電表等各類設備、甚至汽車皆爭相配置上網能力，以突顯科技融入生活的無遠弗屆；加以智慧型手機及平板等個人行動設備大量普及，隨時隨地可連接網路。以這些設備與裝置的數量看來，全世界的 IP 需求量早已超過當初 IPv4 位址所能提供的上限。

目前我們仍然可以順利連上網際網路，感受不到 IP 位址耗盡的影響，最主要原因是網路位址轉換 (Network Address Translation，簡稱 NAT) 技術的應用減緩 IP 位址耗用速度，多部設備可以共用一個 IP 位址連線，大幅擴充網際網路上可使用的設備數量。然而，這項技術終將面臨不可逆的 IPv4 位址枯竭問題，因此科技界訂定了 IPv6 規格，希望以 128 位

元的位址編碼長度，提供 2^{128} 個位址，徹底解決位址不足的問題。以下舉例說明 IPv6 位址數量之大：以全球 70 億人口估算，每人可以分配到 4.86 × 10^{28} 個 IPv6 位址；由此可預見在我們有生之年，IP 位址枯竭的問題將不再發生。

在現今 IPv4 環境中，各類資訊安全事件層出不窮，駭客利用各種安全弱點，處心積慮企圖獲取有利資訊。轉換到新的 IPv6 協定後，雖然有較強的安全功能，卻無法樂觀以待，因為惡意攻擊者可能會趁新協定的防護機制尚未普及而發動攻擊。以下各節將分別從規格面、應用面及管理面說明 IPv6 的安全性議題，以供企業規劃導入 IPv6 安全防護之參考。

二、IPv6 規格簡介

在探討 IPv6 規格的安全議題前，先介紹 IPv6 的規格架構、位址表示及類型等基礎概念。

IPv6 的封包格式如圖 1 所示，Header 長度固定為 40 位元組。IPv6 簡化或取消以下 IPv4 之欄位：Header Length、Service Type、Identification、Flags、Fragment Offset、Header Checksum。

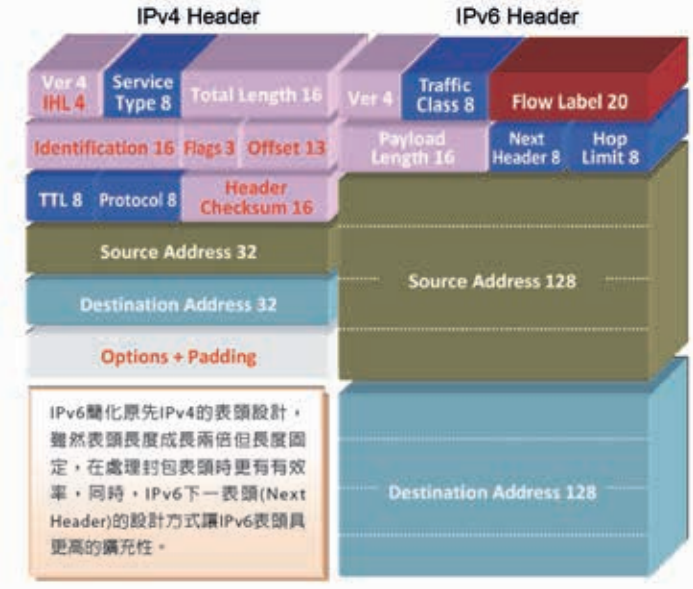


圖 1　IPv4 及 IPv6 封包格式

圖片來源：台灣網路資訊中心 IPv6 修練自學手冊

IPv6 位址長度為 128 位元，其前 64 位元稱為「網路前綴」(Prefix)，後 64 位元稱為「主機位址」；其表示方式是 16 位元為一組，分為 8 組，以冒號隔開，每組包含 4 位十六進位制數字，例如 2001:0db8:9095:02e5:0216:cbff:feb2:7474。若位址為 0，可以縮寫為 :0: 或 :: 等，其他細節請參考相關技術文件。

IPv6 的位址類型分為 Unicast（單播）、Anycast（任播）及 Multicast（群播）三種，與 IPv4 位址相較，取消 Broadcast（廣播）類型。

Unicast 為一對一網路封包傳送模式的位

址，又可分為以下三類；IPv6 較特殊的是同一張網路卡上可同時擁有這三類位址，以提供不同用途。

- Global：在全世界具有唯一性的位址，如同 IPv4 的公開位址 (Public Address)。
- Link-Local：僅在某一特定 Layer2 網路區段使用，不可被繞送至其他連結或網際網路上。位址格式為 fe80::/10，起首碼固定為 fe80，其後 64 位元係結合設備網路卡之 MAC (Media Access Control，媒體存取控制) 值，以 EUI-64 方式計算所得。因為網路卡 MAC 值是獨一無二的，所以轉換後所得的 Link-Local 位址也不會重複。
- Unique-Local：位址可於不同網路區段節點間繞送，但不可繞送至網際網路。位址格式為 fc00::/7。

Link-Local 及 Unique-Local 位址的概念就像 IPv4 的私有位址 (Private Address)，對於區域網路之間的通訊非常有用，尤其 Link-Local 是系統自動產生的位址，無須設定即可在區域網路之間互相溝通。

Multicast 適用於單一位址對多個位址的資料傳送，位址格式為 FF00::/8。Anycast 可供任何一個節點傳遞資料到距離最近的目的主機，以達到縮短傳輸時間的目的。

三、IPv6 規格面安全議題

IPv6 規格面的安全議題包含資源耗盡 DoS (Denial-of-service，服務阻斷) 攻擊、ND (Neighbor Discovery，芳鄰探索) 協定攻擊、ICMP (Internet Control Message Protocol，網際網路控制訊息協定) 連線開放、MTU (Maximum Transmission Unit，最大傳輸單位) 限制及 IPSec (Internet Protocol Security，網際網路安全協定) 使用等，逐一說明如下。

(一) 資源耗盡 DoS 攻擊

在 IPv4 環境中，如果將網路遮罩設定為 /24，路由器上可查詢的網路位址最多也只有 255 個；但是在 IPv6 環境中，網路遮罩如果設定為 /64，路由器上可查詢的 IP 數量將高達 2^{64} 個。如果駭客利用如此大量的 IP，不斷向路由器發出查詢要求 (如圖 2 所示)，路由器可能因大量位址查詢耗盡 CPU 及記憶體資源而無法正常作用，造成網路傳輸中斷。

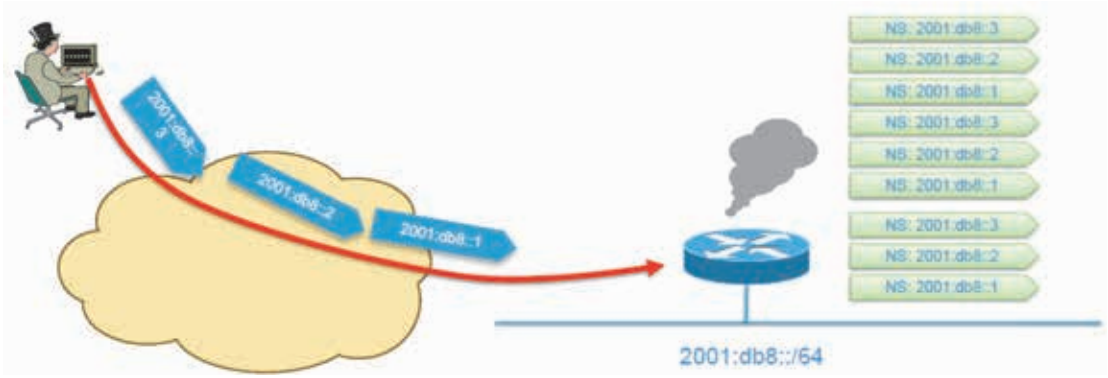


圖 2　資源耗盡 DoS 攻擊示意圖

調整路由器的設定可以防範此類攻擊：

1. **調整內建的位址查詢限制參數**。
2. **針對僅有點對點的連線，將網路遮罩設定為 /127**。
3. **建立 Access Control List，設定僅可查詢網路上已經存在的位址資訊**。

（二）ND 協定攻擊

IPv6 以 ND 取代 IPv4 的 ARP (Address Resolution Protocol，位址解析協定) 機制，做為探索網路內節點是否存在的協定。ND 主要功能包括可自動決定 IP 位址、IP 位址衝突偵測、Layer 2 位址解析、相鄰路由器及主機偵測 (如圖 3 及圖 4 所示) 等。ND 協定應用 ICMPv6 協定，為這些功能定義以下 6 種 ICMP type 回應值，以供溝通之用。

- Router solicitation (ICMPv6 type 133)
- Router advertisement (ICMPv6 type 134)
- Neighbor solicitation (ICMPv6 type 135)
- Neighbor advertisement (ICMPv6 type 136)
- Redirect (ICMPv6 type 137)
- Router Renumbering. (ICMPv6 Type 138)

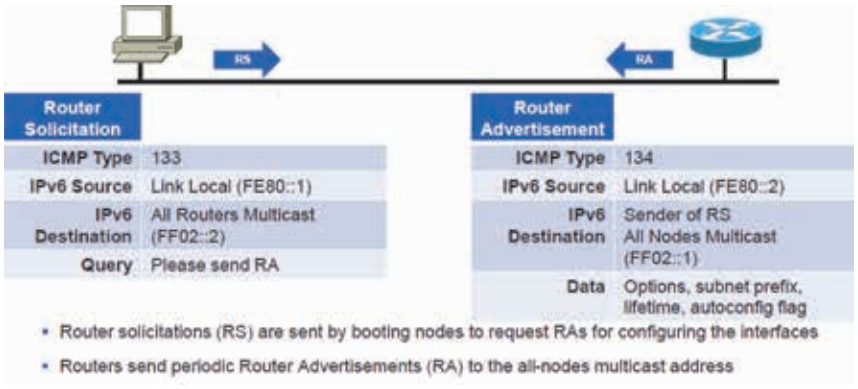


圖 3　相鄰路由器偵測

圖片來源：Cisco

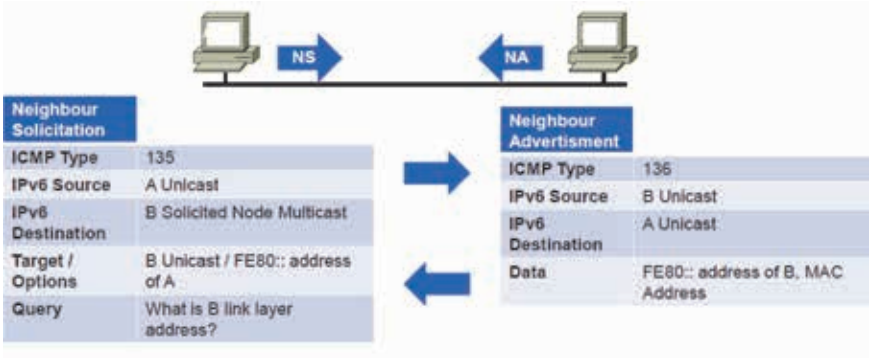


圖 4　相鄰主機偵測

圖片來源：Cisco

IPv6 的 ND 攻擊方式類似 IPv4 的 ARP 攻擊，可分為以下四種：

- **重導 (Redirect) 攻擊**：惡意系統將資料轉送至其他位置。
- **服務阻斷 (Denial-of-Service) 攻擊**：惡意系統阻止攻擊目標與其他網路節點間的溝通。
- **洪水服務阻斷 (Flooding Denial-of-Service) 攻擊**：惡意系統傳送大量資料至攻擊目標，使其不堪負荷。
- **偽冒 (Spoofing) 攻擊**：以假造的 IP 於網路中進行非法攻擊行為，造成破壞。

防範 ND 攻擊的最主要目標就是防止發生假冒 IP 的情形，可考慮針對 ND 通訊要求進行認證，確認是可信賴的端點後，再進行訊息交換。網路標準技術文件 RFC 3971 及 RFC 6494 的 Secure Neighbor Discovery (SeND) 協定對此提出三個選項 (option)：加密產生位址 (Cryptographically Generated Addresses，簡稱 CGA)、RSA 簽章 (RSA signature)、時間戳記與 Nonce (Timestamp and Nonce)。

SeND 機制實作於網路的終端節點，各節點須產生一組公鑰與私鑰，再利用 CGA 機制產生 IPv6 位址，以保證其位址擁有權；而以私鑰針對 ND 訊息所產生之 RSA 簽章係放在所有選項末端，確保訊息的機密性及完整性；至於時間戳記及 Nonce 選項則用以防止重送攻擊。

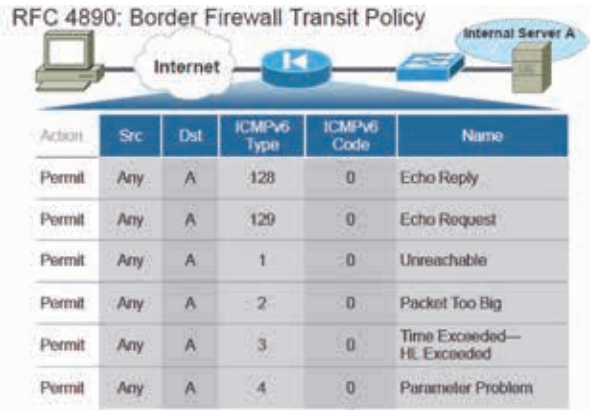
目前各作業系統 (如 Windows、Android、iOS 等) 並不支援 SeND 機制，僅主要網路設備廠商支援此協定，且加解密運算可能影響設備處理效能，建置時須審慎考量其適用範圍。

(三) ICMP 連線開放

ICMP 的主要功用為錯誤報告與診斷，在 TCP/IP 網路中發送控制訊息，提供通信環境中各種可能問題的資訊，管理者可透過該等訊息進行問題診斷，再據以採取適當的解決措施。在 IPv6 環境中，此協定被稱為 ICMPv6。

在設有防火牆的 IPv4 網路中，通常會阻斷大多數 ICMP 訊息的傳送，最主要原因是駭客可利用 ICMP 協定獲取網路異常原因等相關訊息，調整網路探測及攻擊方式，尤其外部稽核常要求金融機構介接網際網路的防火牆必須封鎖 PING (ICMP 的 Echo Request 及 Echo Reply 訊息) 連線封包。但是在 IPv6 的環境中，ND 協定須依據 ICMPv6 回應訊息，判斷路由器或主機是否存在，因此防火牆須允許 ICMPv6 封包通過。

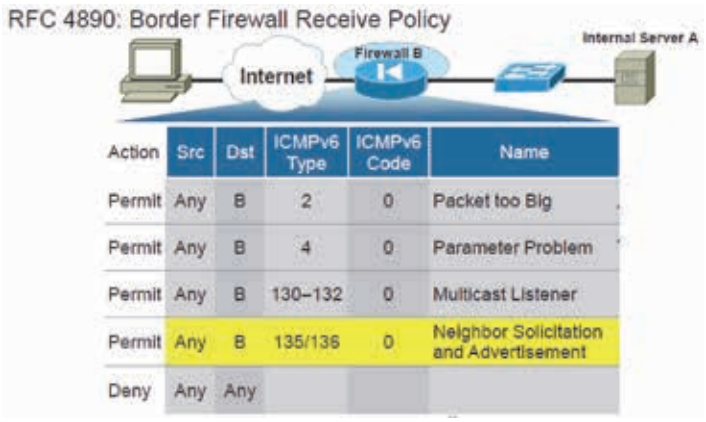
為防止 ICMPv6 訊息洩漏可能造成的影響，RFC 4980 針對防火牆可能需要開放的規則提出建議，即於實際設定時，應秉持最小化原則，針對防火牆規則的來源與目的端設定限制，盡可能設定明確的 IP 範圍，不應貪圖方便而設定為 Any，如圖 5 及圖 6 所示；介接網際網路的防火牆如有 Echo Request 及 Echo Reply 連線需求，則須進一步確認其必要性。



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	Unreachable
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—HL Exceeded
Permit	Any	A	4	0	Parameter Problem

圖 5　IPv6 防火牆傳輸規則

圖片來源：Cisco



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	135/136	0	Neighbor Solicitation and Advertisement
Deny	Any	Any			

圖 6　IPv6 防火牆接收規則

圖片來源：Cisco

(四) MTU 限制

MTU 是指網路上每一個封包所允許承載的最大資料位元組數。在 IPv4 中，MTU 最小為 576 位元組，最大為 1500 位元組；而 IPv6 中，MTU 最小為 1200 位元組，最大為 1500 位元組。

IPv4 及 IPv6 決定網路傳輸 MTU 值的方法亦不相同，IPv4 允許網路節點 (包括主機及路由器等) 對過大的封包進行分包的動作，待資料全部傳送至目標主機後，再組合成完整的資料。而 IPv6 為降低路由器的工作負擔，封包分包的動作只在送出資料的主機執行，網路上的節點透過 ICMPv6 訊息溝通，以 PMD (Path MTU Discovery) 機制，自動調整至最適合的 MTU 值，再傳送資料，其運作如圖 7 所示。

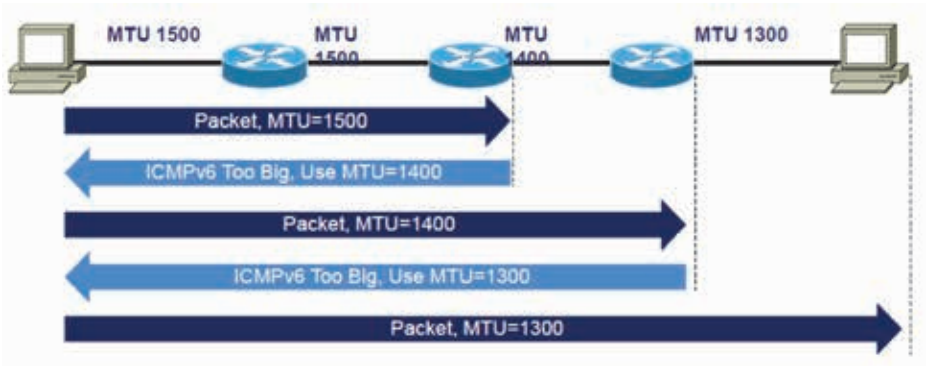


圖 7　PMD 運作示意圖

圖片來源：Cisco

為防止 PMD 機制失效，造成資料無法傳送，首先應確認主機是否手動設定 MTU，如有，應確認其值大於 IPv6 允許的最小值 1200 位元組；其次應確認網路上各節點是否支援 PMD，並替換不支援的設備，以免成為網路黑洞 (自動丟棄封包，且無任何錯誤訊息)。此外，防火牆或路由器的規則須允許傳送 ICMPv6 Type2 Code 0 (Packet Too Big)　資訊。

（五）IPSec 使用

IPSec 針對連線資料傳輸進行認證及加密，以確保資料的機密性及完整性，是維護 IP 層通信安全的機制。IPSec 運作主要有兩個步驟：第一、傳送端與目的端必須使用 IKE (Internet Key Exchange) 建立安全聯結 (Security Associations)；第二、IPSec 針對要傳送的封包以加密演算法及 Key 加密後傳送。IPSec 有兩種實作模式：AH (Authentication Header) 及 ESP (Encapsulating Security Payload)，AH 用以確認封包的完整性與不可否認性，ESP 定義封包加密及完整性認證標準，兼具驗證與加密之功能。

IPv4 環境可視實際需求導入 IPSec 機制，而 IPv6 於最初設計時雖將 IPSec 設定為必須建置的強制性安全機制，但 2011 年發布的 RFC 6434 則未要求強制導入，而是認為“IPsec SHOULD be supported by all IPv6 nodes”。

雖然許多企業仍認為應該全面導入 IPSec 機制，以加密保護網路之資料傳遞，卻可能忽略以下問題：

1. IPSec 是點對點間的加密技術，如果有 n 個設備要互相連線，則須儲存 n^2 個連線資訊，且資料的傳輸接收都須耗費 CPU 資源進行加解密，許多運算及儲存能力不足的設備 (如手機) 將無法順利傳輸。
2. IPSec 可利用通訊兩端設備所預先輸入的一組共享 key，以 IKE 機制產製連線 key，但網際網路通訊的另一端可能是未知對象，難以預先建置共享 key，如要利用公開金鑰架構 (PKI) 進行 IPSec 認證，又涉及憑證管理及更新等問題，並非一般使用者可容易瞭解並自行設定的作業。

最重要的是，如果 IPSec 的建立有問題，代表所有網際網路連線皆無法成功，對使用者將造成極大不便，凡此種種皆可能是導致 IPv6 架構調整修正 IPSec 角色的重要原因。

四、IPv6 應用面安全議題

目前常見的木馬程式、病毒、蠕蟲等威脅皆建構於網路的應用層，而 IP 協定位於網路層，由 IPv4 轉換至 IPv6 並無法消除這些針對應用程式的攻擊行為，只是有可能因為 IPv6 位址數量龐大而減緩其擴散速度。其他如封包側錄、服務阻斷、分散式服務阻斷、私架設備或中間人等攻擊方式，也不會因為改用 IPv6 而有所不同。

五、IPv6 管理面安全議題

導入 IPv6 協定時，必須考量企業運作相關安全議題。全新的企業才有可能一次全面導入 IPv6，大多數企業仍須逐步轉換，IPv4 與 IPv6 兩種協定並存的過渡時期受限於許多因素，只要網際網路或內部環境中還有使用需求，IPv4 位址就不會消失，有人預估網際網路上的 IPv4 位址到西元 2025 年才可能完全退場。在兩種協定並存的情況下，必須考量下列議題：

（一）定義 IPv6 導入範圍

IPv6 主要是為解決網際網路位址缺乏的問題，對於企業內部的衝擊較小，因此規劃 IPv6 轉換必須評估導入的範圍，以估算確實完成轉換所需的人力、物力及財力，不只完成

技術轉換，亦應兼顧安全性。

（二）無須使用 IPv6 之設備，應關閉 IPv6 協定

有些作業系統 (如 Windows 2012) 於網路啓動後，即自動啓動 IPv6 協定，而 IPv6 協定啓用後，設備即自動計算出一個 Link-Local 位址，可與同一網路區段內的其他 IPv6 設備互通，可能在管理者不知情的情況下，成為惡意攻擊或入侵的對象。因此，設備管理人員應檢查並確認資訊環境中的設備現況，以免產生資安漏洞。

（三）網路防護設備應支援 IPv6 功能

防火牆、弱點掃描及入侵偵測防禦等系統須支援及解析 IPv6 連線資訊，才能發揮適當的資訊揭露、連線阻絕等防護功能。系統管理人員應檢視並瞭解各設備的功能或版本限制，例如：防火牆系統版本是否具有完整的防護及記錄功能？是否只能支援路由或透通模式？如發現功能有所不足，應進行適當的調整或提升，才能發揮完全防護的功效。

（四）IP 的分配及控管

由於 IPv6 網段的 IP 數量龐大，較佳處理方式是減少每一個網段所含的 IP 數量，只使用網路遮罩 /118 (相當於一個網路遮罩 /22 的 IPv4 子網路所包含的主機數量)，並明確配置所有位址，以免剩餘太多空的位址遭駭客利用，降低發生資安問題的可能性。

（五）PCI 合規性

信用卡交易處理相關機構自西元 2015 年起，必須符合 PCI DSS (Payment Card Industry Data Security Standard，支付卡業務資料安全標準) 第 3.0 版之規範，其中 Requirement 1.3.8 內容如下：

Do not disclose private IP addresses and routing information to unauthorized parties.

– *Note: Methods to obscure IP addressing may include, but are not limited to: Network Address Translation (NAT) ...*

– *The controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.*

PCI DSS 規範內部 IP 及路由不可洩漏至未被授權者，然而，DMZ (Demilitarized Zone) 主機的 IPv6 位址如果是使用 ISP 派發的 Global 位址，就可能將位址傳至網際網路，與 PCI 之規範有所衝突。Cisco 公司認為可採行應用程式代理機制、ACL 連線過濾或嚴格過濾 BGP 路由資訊等方式，以符合 PCI DSS 之要求。

（六）人員訓練

資訊人員缺乏 IPv6 相關技術知識及實務經驗，也可能導致資安問題，尤其為同時支援兩種協定，不僅工作負荷加重，也容易陷入兩種協定技術互相糾纏不清的迷思。充分而良好的訓練可提升人員技術知能，熟悉兩種協定不同的運作方式，可正確完成系統設備維護、應用程式開發、網路或資安問題查測等維運作業，以消弭資安風險，確保業務持續運作。

六、結語

IPv4 及 IPv6 是兩種截然不同的技術規格，對於新技術的發展及導入，除瞭解相關技術細節及應用方式外，資訊安全所面臨的衝擊更不容忽視。依以上章節的分析結果，除新舊規格差異所產生的新興資安議題外，眾多資安威脅其實早已存在於 IPv4 環境，IPv6 環境亦無法倖免。

IPv6 的導入，對於企業之資訊安全看似一項危機，惟如能針對本文所提及之各類安全議題，審慎評估相關需求，並據以採行適當之防護措施，降低資安問題發生機率，經由事前規劃、事中監控及事後檢核的管理機制，必能化危機為轉機，順利與網際網路新世界接軌。

※ 參考文獻 / 資料來源：

1. 財團法人台灣網路資訊中心，IPv6 升級實做技術手冊第 1.1 版，中華民國 101 年 11 月。
2. IPv6 修練自學手冊，台灣網路資訊中心編著。
3. GSN IPv6 資安問題白皮書，徐武孝，中華民國 98 年 10 月。
4. IPv6 Security Threats and Mitigations，錢小山，December 2013。
5. Guidelines for the Secure Deployment of IPv6, NIST, December 2010。
6. Eric Vyncke, IPv6 Security: Threats and Mitigation, Cisco Live, 2014。
7. Dean Robertshaw, Understanding IPv6, Cisco Live, 2014。
8. Cisco, Cisco IOS IPv6 Configuration Guide, 2009。
9. Carlos E. Caicedo , James B.D. Joshi and Summit R. Tuladhar, IPv6 Security Challenges, IEEE Xplore, September 2009。
10. http://en.wikipedia.org/wiki/Wikipedia，維基百科。