

IPv4 網址耗盡 是威脅、危險還是危機？ 迎接 IPv6 物聯新世界 The World Is Ready!

作者：思科院士 Fred Baker

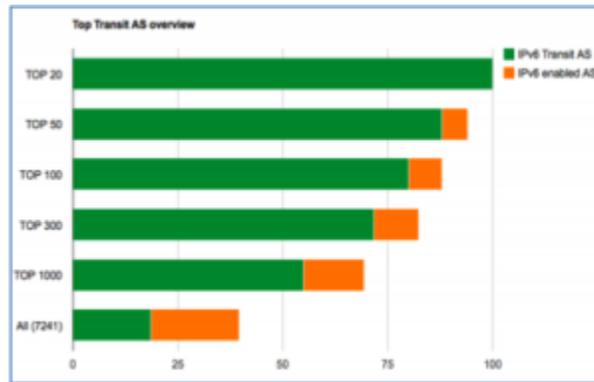
IPv4的耗盡究竟為企業帶來的是威脅、危險還是危機？就字面上解釋，「威脅」代表意圖使對方遭受痛苦、受傷、損壞或其他敵意行為。「危險」意指傾向或暴露在傷害或受傷、危機或嚴重危難的情況下。而「危機」則表示處在一連串事件的狀態下，而所有未來事件的發展，都存在著可能變好或變壞的轉折點。然而，IPv4網址的用盡，為企業帶來的是危機。

1990年在溫哥華的一場技術研討會中，一位名叫Frank Solensky的工程師便大膽預測，若按照當時分配IPv4網址空間使用的方式，到了1994年就面臨所有網址耗盡的問題。由於在當時的環境下，並沒有明確的解決方法，因此IPv4的耗盡對於所有依賴網路的事業體來說，都是一項巨大的威脅和危險。舉例來說，應用程式如全球資訊網 (World Wide Web)、檔案分享及YouTube影音網站等，都可能面臨成長的瓶頸，而我們也可能無法享受到過去這20年中，由科技的進步而帶來生活品質上的改善。所幸後來網址空間的分配方式改變，更有了私人網址空間及網路位址轉譯機制才得以使用IPv4至今。

儘管1990年代初期，已針對IPv4做了許多的改變，但當時的措施仍不足以維護網路或企業長期健全的發展，終究面臨IPv4瀕臨用盡的局面。這確實為組織、企業帶來了一些問題和麻煩，但對於網路的發展並不構成威脅，因為現在已有替代的協定，能支援現今網路上所運作的各種服務，並帶來發展各種新服務的機會。**現在的我們正處於一個轉捩點，唯有採取適當的行動，才不致讓IPv4用盡的問題構成進一步的威脅。**企業如能即早體察到這個危機，並進一步部署IPv6，便能持續穩健地發展網路相關的各種產品與服務。

目前的情況類似早年的「Y2K危機」，當時支援銀行業務與其他功能的軟體，皆以2位數字來記載當時的年份，但當1999年要跨入2000年時，即面臨19數字耗盡的危機，我們必需找出、修改、並驗證相關的軟體指令，並進行大型數據資料的修補，以將年份改由4位數字顯示。由於當時多數人察覺此問題並採取指定的修正動作，以致2000年1月實際通報的問題數量很少。如今網際網路也面臨了類似的危機，大家必須部署新的協定，並確保其服務能在此協定上運行，才能將問題化為最小。

歐洲網路協調中心（RIPE Network Coordination Centre, RIPE NCC）最近宣布近期將分派最後的IPv4 /8網址，和先前亞太網路資訊中心（APNIC）於2011年4月一樣，開始推動嚴格控管IPv4網址分發的策略。因此如果企業盼求區域網際網路註冊中心（包括APNIC、ARIN、RIPE等）分派IPv4網址空間，就會面臨問題，現有的解決方案就是轉換到IPv6。截至2012年6月8日，全球前1,000大網路服務商（ISP）有超過半數已經部署新網址技術，更有7,300家以上的服務商也加入轉換的行列。



而網路轉換的範疇不僅限於此，提供用戶端網路接取的服務商，包括NTT、Free、Orange、Comcast、及Time-Warner等業者都已公開其轉換的進度；大型內容供應商，包括谷歌與臉書等也都完成部署作業，並能在IPv4或IPv6上無縫的做連接或互換；電信業者，包括T-Mobile與中國移動通信等也都正在實驗關閉IPv4，僅採用IPv6的網路；大型企業，包括Bechtel、思科及其他企業也都正進行部署動作。欲得知自己的網路是否已轉換至IPv6，可參考<http://www.kame.net>網站，若您能看到網頁上方的烏龜在跳舞，即代表您正使用IPv6的網址。

促使這麼多網路需要轉換至IPv6有幾項原因：對ISP來說，其替代方案是在自己的網路中使用網路位址轉換器，然而這麼做會讓其業務更複雜且難以營運，而且除非透過主機託管供應商，不然根本無法為企業用戶提供服務。印度、非洲、南美洲、及中亞等地區的網路早在幾年前就曾這麼做，但現在已改弦易轍。對於內容供應商來說，其生存係仰賴於找到用戶及他們當前的位置，但網路位址轉譯卻會阻礙基本商務資訊的傳輸。對於行動電信業者而言，由於多年來飽受內部轉譯問題所苦，這給了他們簡化網路的機會。它讓企業能更有效率地管理其網路，更容易看到錯誤進行除錯，重新把網址空間分派給LAN，以減少付出的資源和人力。對於家用寬頻網路而言，上述情況都有涉及一些，因此一個通用的位址空間會為上述各方面帶來許多的好處。

此外，我們每個人特別是企業與家庭使用者，都將面臨無法存取內容的威脅。若部署IPv6網路，我們仍能透過NAT64轉譯器連結到純IPv4網路的內容，但若其他一方把IPv4關掉或置於NAT的後方（不論是電信級或非電信級），那麼我們僅能用到IPv4網路中的服務，無法存取他們的內容，原因和我們曾經認為IPv4 NAT能帶來安全防護一樣。位址複用（address multiplexing）的問題，將讓我們無法聯絡上客戶與商務夥伴，且他們也無法聯絡上我們，這將讓情況變成一場危機，雖然不致讓網路及企業滅亡。但不採取行動的必然結果，就好比不用助聽器導致聽力喪失，整個世界將變得異常安靜且無趣，因為會完全聽不到重要的聲音。

隨著IPv6的推出，就不再需要藉由狀態型網路位址轉譯器，讓IPv4位址空間共存。或許有些人會擔心網路因此變得不安全，但位址轉譯器確也不見得能帶來安全，因為在轉譯的同時雖會形成邊界安全策略，讓人難以從網域外面啟動傳輸階段進入網域，但這樣的策略並不普遍被業界採用亦缺乏效率，因為大多數的攻擊主要都是從防火牆後面發動。因此，透過能執行安全策略的防火牆，將比位址轉譯器來得必要且有用。

轉換至IPv6是網際網路發展必然的途徑，然而IPv4仍會共存好一陣子才會完全被汰換，就如同成長曲線一樣。根據RIPE NCC的報告指出，目前全球宣佈採用IPv6協定的比例約占15%，若成長到28%時，電信網路的價值會和系統連網使用者數量的平方成正比，並牽動進一步的部署。當採用比例達70%時，市場就會接近飽和，技術便會開始下滑，此階段如同業界開始討論要全面關閉公眾網路骨幹上的IPv4之時。

我們預估將在5年內就會達到70%的飽和度，因為包括像是筆電、家用路由器等設備，大約都已過了一半的使用年限。目前消費者使用的作業系統，包括MacOSX、Windows(Vista和之後更新的系統)、FreeBSD、及Linux都支援IPv6。若消費者在2007年1月之後所購買的電腦，皆已支援IPv6，除非故意關閉這項功能。而目前尚未採用IPv6技術的消費電腦，包括X-box、舊款手機、及使用Windows XP系統的電腦。微軟在2014年4月後就不再支援XP，有些XP的使用者甚至已面臨必須升級的壓力。而家用閘道器則遠落在後頭，直到最近一、兩年出廠的機種才剛開始支援IPv6，有些產品甚至仍有舊技術留下的問題。目前使用Linksys、Netgear、及D-Link路由器等設備，且若還在正常壽命約5年之內，消費者可透過升級的動作來支援IPv6。

有人問IPv6為何不能和IPv4回溯相容？這個問題的真正焦點應是IPv4並不能和任何架構前向相容。因為若IPv6有誤，也無法藉由調整舊有的協定來取代。然而，可預期的是，當IPv6用盡時，我們將會需要完全不同的設計，因為屆時大環境的需求也會有所變化。若真如此，我們就無法從現在預測未來新科技的面貌，但在那之前，網路將會因其他不一樣的原因完全汰換掉IPv6。