IPv6在國防上的應用

作者/張俊榮 助理研究員

提要

目前網際網路(Internet)廣泛使用的網際網路通訊協定第四版(Internet Protocol Version 4, IPv4)在IP位址空間、點對點的移動性(Mobility)及點對點的安全性(Security)等漸漸暴露出了許多問題。而網際網路通訊協定第六版(Internet Protocol Version 6, IPv6)被稱為下一代網際網路協定，則是針對IPv4的問題，提出解決的方法，不僅可以提供龐大的IP位址空間，更可滿足國防網路上的每個人員、武器、裝備所需IP移動能力的需求及傳送國防機密資料安全性的保證。因此，國防網路實施IPv6是有其必要的。

前言

從應用與服務面來看，網際網路未來將以多媒體、高度安全性及高度行動能力支援爲基本的特性，IPv6完全具備上述特性的技術與能力。因此，IPv6將是下一代網際網路協定最好的選擇，也是並經之路①。而IPv6所具備的這些特性不僅可應用於商業化的網路，更可滿足保密性、安全性及移動性等要求甚高的國防網路的需求。

本篇文章首先針對IPv6的優勢作個簡介，並說明IPv6在國防上的應用，並進一步探討美國國防部IPv6發展狀況及其轉換(transition)計畫，最後就台灣IPv6發展狀況及行政院NICI IPv6標準測試實驗室作個說明。

IPv6的優勢

IPv6被稱爲下一代網際網路協定，它是由IETF(Internet Engineering Task Force)設計用來解決IPv4存在的一些問題與不足，例如IP位址不足、服務品質(Quality of Service)無

①「我國IPv6建置發展計畫辦公室」新聞稿，民國93年3月17日。

法獲得保障、安全性及移動性的限制等，並在許多方面提出了改進。與IPv4相比，IPv6具有許多新的特點，如簡化的標頭(header)格式、位址空間擴大、自動定址(Auto-configuration)功能、行動網際網路的支援、認證與加密的機制及服務品質的保證：

一、標頭簡化設計和標頭可擴展性設計

IPv6的標頭是由一個基本標頭和多個擴展標頭(Extension Header)構成。基本標頭具有固定的長度40位元組，固定的標頭長度有助於加快路由的速度，並且使路由器的硬體設計更加簡單，更方便未來直接使用硬體處理IP標頭資料加快路由的速度。除了基本標頭外，IPv6還定義了多種擴展標頭，使用者可以透過下一個標頭(Next header)的方式自行在標頭中指示下一個標頭的內容以利網路端或是接收端完成特定的工作，這使得IPv6變得極其靈活，能夠提供對多種應用的強力支援，同時又爲以後支援新的應用提供了可能②。

二、位址空間的擴大

IPv6將現有的IP位址長度由當前IPv4的32位元擴充到128位元，以支援未來數量龐大的網路節點。IPv6使用128個位元加以定址，預估未來從PDA到手機，甚至CD隨身聽、手錶等電子商品都將會有一個獨一無二的IP位址，可以透過網路取得更新資訊或進行遠端遙控等。

三、自動定址功能

在IPv4中動態主機配置協議(Dynamic Host Configuration Protocol,DHCP)實現了主機IP位址及其相關配置的自動設置。IPv6繼承了IPv4的這種自動配置功能，並將其稱爲全狀態自動配置(Stateful Auto-configuration)。除了全狀態自動配置，IPv6還採用了一種稱爲無狀態自動配置(Stateless Auto-configuration)的自動配置功能，這兩種自動配置功能都能自動將IP位址分配給用戶。只要機器一連接上網路便可自動設定IP位址，如此將可簡化網路斷線後的恢復，IP位址的發放與管理等複雜的管理問題，簡化了網路管理程序，降低了網路管理者的工作負擔，大幅降低網路管理成本。

四、行動網際網路支援

隨著科技的日新月異，Notebook PC、手持式設備(PDA、手機等)愈來愈多，人們對於網際網路支援行動能力的需求也愈來愈高，因此IPv6在設計上加入行動IP的功能，以利未來行動網際網路的支援，提供行動上網的服務。

五、認證與加密的機制

IPv4在設計之初並未考慮安全性問題，資料在網路上傳送並未使用安全機制，現今的網際網路極爲普遍，同時伴隨著大量具安全需求資訊之交換，安全性成爲網際網路必須面對的問題。爲了加強網際網路的安全性，1995年開始，IETF著手研究制定網際網路安全協定(IPSec)。IPSec是IPv4的一個選擇協定，在架設及管理上都是額外的負擔，而IPSec是IPv6的一個必須組成部分，使用者將不需透過額外的設備或軟體就可以對傳輸的資料進行認證及加密，達到網路安全的功效。

六、服務品質的保證

爲改善網際網路服務品質，IPv6封包表頭增加2個新的欄位，用以支援即時(Real

② 次世代網際網路標準協定-IPv6工研院電腦與通訊研究所資訊技術推廣部。

圖一　Global Information Grid構想示意圖③

Time)訊務的需求，包括訊務種類(Traffic Class)和訊務標記(Flow Label)，將有助於服務品質控制機制的設計。

IPv6在國防上的應用

以國防的需求來看，運用先進的通信技術建構一個安全可靠的通信網路，是捍衛國家安全的要件之一。因此，美國國防部在1999年提出建立全球資訊格網(Global Information Grid,GIG)的構想，如圖一所示。就是要讓全球任意兩點或多點之間可以進行資訊交流。其基礎是將有線、光纖、無線電、資料、太空通訊、視訊及多媒體服務等層級的通訊服務加以統合，以全球性的接收及使用爲目標，運用封包交換技術在網際網路中傳輸資料，提供共同使用者整合的資訊架構④。

然而現今使用的網際網路協定IPv4在使用上已出現窘境，美國國防部(Department of Defense, DoD)2003年6月9日發表的政策備忘錄更指出：使用了近30年的IPv4在位址空間、點對點的移動性及點對點的安全性等限制下，已無法滿足市場或軍方未來的需求，因此實施IPv6是有其必要的。

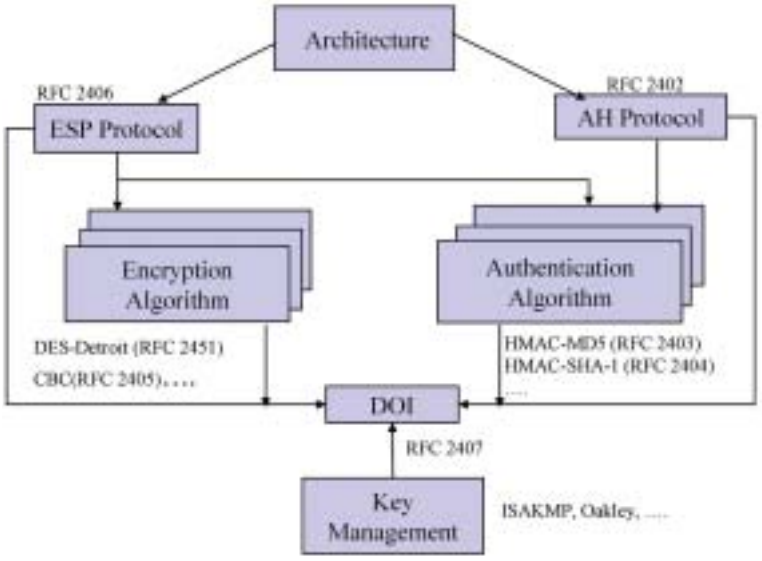
運用IPv6行動IP技術(Mobile IP)建構軍用的行動隨意網路，每一個前線單位均配有自己的IP，透過手持或配備在船艦、飛機上，可以傳輸數據資料，可以隨意連上區域網路，如果該單位移動到其他區域網路時，不需再重新登入，可以在機動的同時仍保持和網路連線，不會有機動的限制，如圖二所示。

再者，國防網路最重要的是安全性問題，沒有安全保障的網路不僅容易將國防機密資料被竊取或被僞造，嚴重的甚至影響國家安全。IPv4協定在設計上並沒有考慮安全性的問題，因此在國防網路上若使用IPv4協定傳送國防機密資料，將有非常高的風險。針對此一缺點，IETF於1995年提出IPSec第一版，包含認證標頭(Authentication Header,

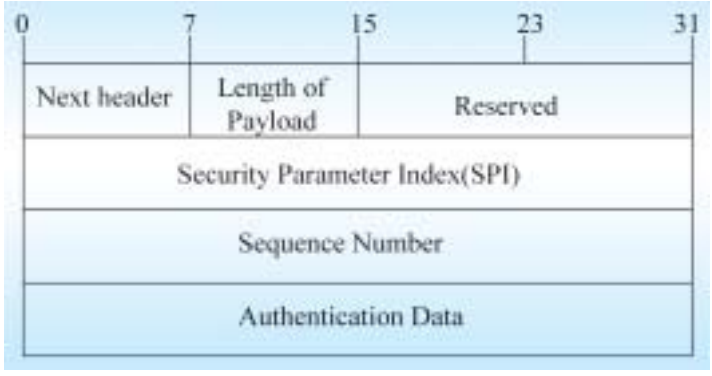
③ Building the Foundation: Net-Centric Operations and IPv6, Marilyn Kraus Architecture & Interoperability DoD Chief Information Officer, http://www.usipv6.com/2004santamonica/main.html.

④ 2003精實國防戰力科技研討會(二)，2004年1月14日。

圖二　行動IP網路示意圖⑤



圖三　IPSec規範架構圖⑥



圖四　認證標頭(AH)格式⑦

AH)與加密安全承載(Encapsulating Security Payload, ESP)。但金鑰的交換與管理並未定義。第二版於1998年11月提出，除了更新認證標頭與加密安全承載轉換的格式外，還加上了自動金鑰轉換機制、金鑰管理架構，與身分認證及加密演算法，可歸類爲七個部分，如圖三所示。

本文將針對認證標頭與加密安全承載作說明。認證標頭提供的功能包括資料完整性、來源身份認證和防止重播(replay)攻擊，但認證標頭並沒有提供加密功能，因此無法避免某些監視器分析你的資料流。而加密安全承載提供的功能包括資料保密性(confidentiality)、內部封包(Inner Packet)資料完整性、來源身份認證和防止重播攻擊。

認證標頭：認證機制可以用來辨識使用者、應用程式的身份和資料的完整性，以確保傳輸過程中並沒有遭到惡意竄改。認證標頭內部的欄位格式如圖四所示。

一、下一個標頭(Next Header)

⑤ 同註③。

⑥ S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," RFC2401, November 1998.

⑦ S. Kent, R. Atkinson, "IP Authentication Header," RFC2402, November 1998.

定義AH後面資料的類型。

二承載長度(Length of Payload)

認證資料欄位的長度。

三保留欄位(reserved)

保留供未來之用。

四安全參數索引(Security Parameter Index, SPI)

指明通訊的兩端事先約定所採用的身分驗證之演算法與其他參數。目前較常使用的演算法有雜湊訊息身份驗證代碼(Hashed Message Authentication Code, HMAC)-MD5及HMAC-SHA-1。

五序號(Sequence Number)

用來避免「重播攻擊(Replay Attack)」的事件發生。序號的產生方式是以遞增方式逐一累加。若遭受到重播攻擊時，有相同序號的封包會重複送達，系統便可由此得知攻擊事件發生。

六認證資料(Authentication Data)

配合安全參數索引(SPI)所提供的演算法所得到的完全檢查值ICV (Integrity Check Value)，無法成爲32 bits的整數倍時，用Padding來填補。

雜湊訊息身份驗證代碼是一種提供完整性和身份驗證的密鑰演算法。使用加密雜湊的身份驗證產生封包的數位簽名，它可以由接收者驗證。如果訊息在傳輸過程中被竄改，雜湊值也會改變，接收者發現雜湊值改變，表示IP封包的完整性已被破壞，IP封包就會遭到拒絕。目前較常使用的演算法有HMAC-MD5及HMAC-SHA-1，其中HMAC-MD5是產生128位數值的雜湊函數，HMAC-SHA-1是產生160位數值的雜湊函數，雖然HMAC-SHA-1比HMAC-MD5慢，但HMAC-SHA-1比HMAC-MD5的安全性更高。

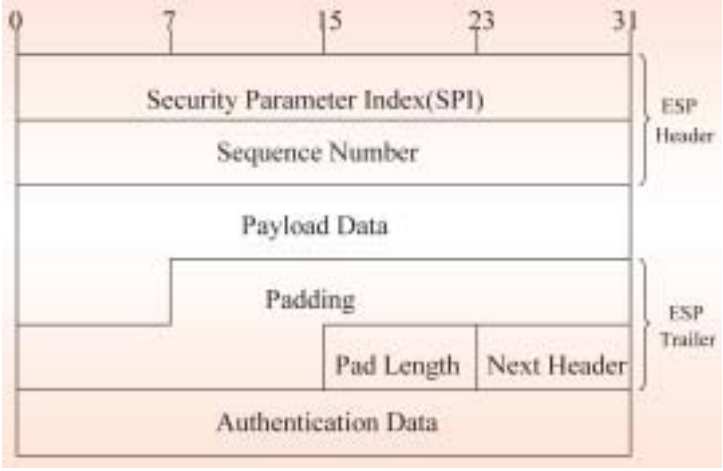
加密安全承載：主要的作用是加密保護資料，並將加密的資料放在IP ESP裡的資料區部分。ESP所使用的保密技術是DES(Data Encryption Standard)或是Triple-DES。DES是1970年代中期由美國IBM公司所發展，且被定爲美國的國家標準(NIST FIPS PUB 46)。目前NIST正在審查新一代的資料加密標準(Advanced Encryption Standard, AES)。加密安全承載內部的欄位格式如圖五所示。

一安全參數索引

指明通訊的兩端事先約定所採用的加密演算法與其他參數。

二序號

用來避免「重播攻擊」的事件發生。序號的產生方式是以遞增方式逐一累加。若遭受到重播攻擊時，若有相同序號的封包會重複送達，系統便可由此得知攻擊事件發生。

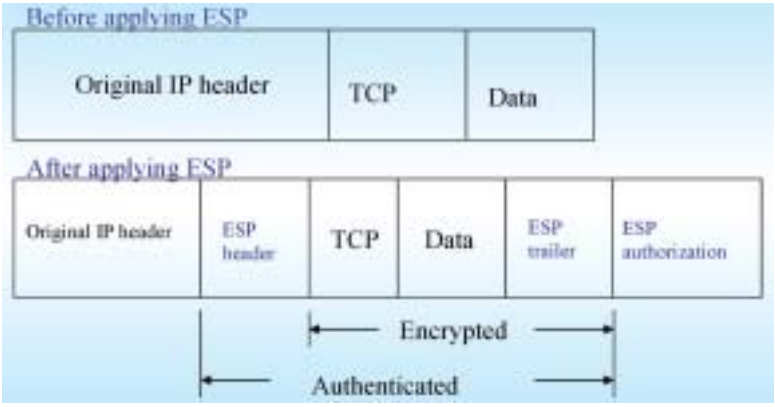


圖五　加密安全承載(ESP)格式⑧

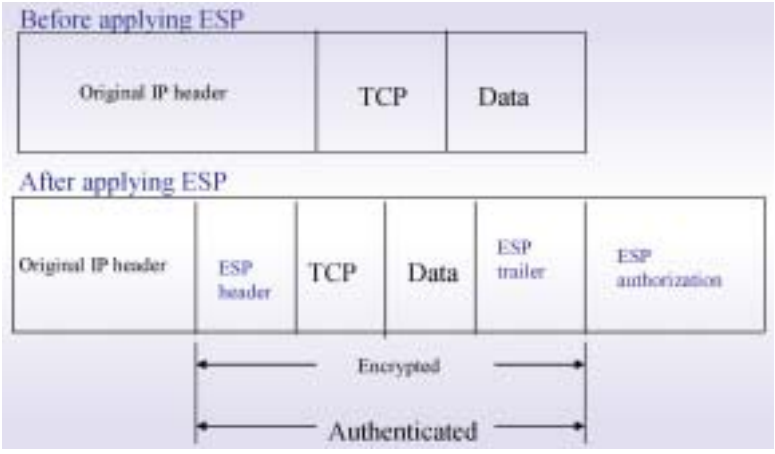
⑧ S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC2406, November 1998.

三Payload Data

ESP加密的範圍可以是整個IP Datagram或者只是上層TCP, UDP或ICMP資料，完全決定於使用是隧道模式(Tunnel Mode)或傳送模式(Transport Mode)。若爲隧道模式則Payload Data爲完整的IP資料封包之密文，若爲傳送模式則Payload Data爲IP資料封包的資料部份之密文。ESP傳送模式，如圖六所示。ESP隧道模式，如圖七所示。



圖六　ESP傳送模式格式⑨



圖七　ESP隧道模式格式⑩

四附加位元組(padding)

加密演算法要求明文(cleartext)必須是某個位元組的整數倍，則我們可利用此欄位將明文擴充到所需要的長度大小。

五附加位元組長度(Pad Length)

計算前一個附加位元組的長度。

六下一個標頭

定義承載資料欄位之中的第一個標頭格式ESP Header後面資料的類型，可能是TCP或是IP標頭。

七認證資料(Authentication Data)

包含爲了檢查自此ESP Packet減去認證標頭後計算的Packet安全性之完全檢查值(Integrity Check Value, ICV)，無法成爲32 bits的整數倍時，用Padding來填補。

IPV6在國防上的應用最重要的考量點在於安全性，藉由自動的金鑰轉換機制及金鑰的管理，進行身分認證及承載資料安全加密，達到網路安全的功效。考慮未來國防網路的需求，IPv6 128位元數量龐大的位址空間，使得國防網路上的每個人員、武器、裝備與任何主機都可以取得獨一無二的Global IPv6位址，結合IPv6 Mobility的技術與IPv6 IPSec認證加密技術，使得國軍任何軍種、任何部隊、任何人員都能隨時隨地的移動及動態的收集資料，且對資料進行認證及加密的情況下彼此傳遞資料並進行情報的交換，進而串聯成一個巨大的國防網路，達到制敵

⑨ 同註⑧。
⑩ 同註⑧。

機先的功效。

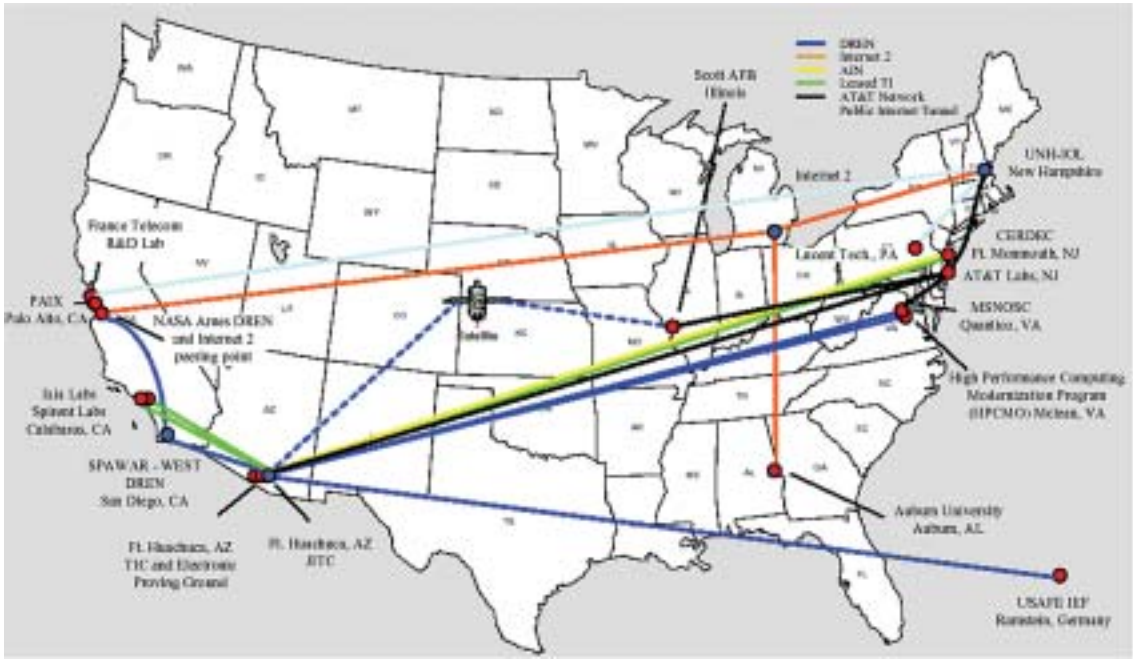
美國國防部與Moonv6合作計畫概述

即使IPv4位址相當充裕的美國軍方也體認到IPv6的優越性，於2003年6月中旬美國國防部簡報上，負責網路和資訊的副部長John Stenbit表示美國國防部將在2008年前將網路基礎設施遷移到IPv6上，凡是在2003年10月份以後替換的設備必須相容IPv6。

因此，美國國防部與北美IPv6工作組(North American IPv6 Task Force, NAv6TF)、美國新罕布夏大學(University of New Hampshire Interoperability Laboratory, UNHIOL)、網際網路服務商及設備製造商共同合作發起名爲Moonv6的網路，作爲美國國防部與網際網路服務商測試下一代網際網路協定IPv6的實驗平台，其網路佈線如圖八所示。

2003年10月，Moonv6進行了爲期10天的IPv6第一階段測試，共有30多家國際著名廠商參與，在試驗中新漢普敦大學的網址和軍方網址連接起來，測試項目包括FTP, Telnet以及視訊會議應用。美國國防部、UNH、NAv6TF對其第一階段測試結果感到滿意。

2004年3月底，Moonv6進行了爲期13天的第二階段測試，20多個軟、硬體產品廠商參加了測試。Moonv6完成的測試包括：QoS、防火牆(firewall)、移動IPv6、DNS、路由協定以及IPv6在10G高速連接時的性能。新罕布夏互通實驗室負責視察測試工作的本．舒爾茨介紹：「測試結果證實IPv6支援的防火牆確實名副其實。支援IPv6的路由器能夠實現不同等級的資料並給予不同的優先順序。」測試完成後，該網路仍將繼續存在，以實現與全球各IPv6網路的連接，作爲服務於產業、ISPs以及美國軍方的實驗平



圖八　Moonv6網路 ⑪

⑪ Ben Schultz/Roswell Dixon, Moonv6 network test event North American IPv6 Summit, 2004.

台。北美IPv6工作組主席Jim Bound先生表示：「下一步，我們計劃建設實際的IPv6骨幹網路，用於IPv6安全、多媒體以及漫遊設備的產品前期測試。」

美國國防部IPv6發展狀況與轉換規劃

美國國防部於2003年6月9日發表了一份「IPv6備忘錄」，提出了在美國軍方規劃實施的全球資訊格網中全面部署IPv6的重要決策，並作出了300億美元以上的IT預算，並且從2003年10月起，其300億美元的IT預算將只能用來購買支援相容IPv6技術的軟體或硬體設備。2003年6月30日美國防部國防資訊系統局的一篇文章「國防部的IPv6」指出，未來作戰系統必將以IP網路爲中心，網路將散佈到世界的各個角落，各種武器系統、資訊系統和指揮控制系統將透過網路連繫在一起，而IPv6具有IPv4所沒有的絕對優勢，包括足夠大的位址空間、改善點對點的安全性(End-to-end Security)、可動態進行地址分配的特性、促進行動通訊(Mobile Communication)的便利、提高服務品質(Quality of Service)的機制以及降低系統管理(System Management)的負擔。這些優勢以及美軍對未來作戰的考慮，美國防部已具體提出了IPv6的進度安排：

一2002年至2004年IPv6協議標準化，並進行大規模試驗(Moonv6網路)。

二2005年至2007年，IPv6和IPv4協議並行。

三2008年實現美國本土全面的IPv6化⑫。

台灣IPv6發展狀況

爲實現國內IPv6網際網路環境，並加速國內IPv6軟硬體研發、網路互連及測試、骨幹建設及推廣應用。行政院國家資訊通訊發展推動小組(National Information Communication Initiative, NICI)於2002年1月正式成立「IPv6推動工作小組」，由交通部電信總局局長擔任總召集人，小組成員包括台灣網路資訊中心(Taiwan Network Information Center, TWNIC)、國科會、經濟部、電信國家型計畫辦公室、各大學與研究機構、資策會、工研院電通所、中研院、國家高速電腦中心、中華電信、相關固網及ISP業者。各成員依照單位屬性組成「骨幹建設」、「研究發展」、「標準測試」及「應用推廣」等四個分組，由各分組擬定推動目標及工作重點項目，定期召開會議並向NICI報告工作成果。

在應用推廣分組方面，台灣網路資訊中心在國內舉辦多次IPv6研討會，進行教育推廣與宣傳外，更在TWNIC成立IPv6工作小組積極進行IPv6推動工作，並加入國際IPv6 Forum成爲會員，協助傳遞許多國際IPv6發展寶貴的訊息給國內IPv6領域之學者專家參考。

在標準測試分組方面，NICI IPv6推動工作小組於2003年7月1日特別成立IPv6標準測試分組，並在中華電信研究所建立「NICI IPv6標準測試實驗室」，提供國內廠商研製IPv6網路設備、用戶設備等相關產品所需之測試、驗證測試及各種設備之互連，進而探討各級學校和產業界移轉到IPv6所需要的各種解決方案，測試各種資訊應用能否順利於IPv6環境中執行，致力建立 IPv6標準測試之相關技術，以建立國家級技術與應用驗證中

⑫「國防部的IPv6」，美國國防部資訊系統局，2003年6月30日。

心，達到促進產業升級與提昇 IPv6科技研究水準之目標。除此之外，更積極爭取加入國際IPv6 Forum IPv6 Ready Logo委員會以協助我國業者取得重要參考資訊，協助國內廠商進行申請IPv6 Ready Phase I標章之認證測試。在IPv6標準測試實驗室之設備及技術支援下，臺灣業界已有六項產品順利取得IPv6 Ready Phase I標章，與美日大廠產品媲美。

目前NICI IPv6標準測試所提供之服務項目包括：

一IPv6符合性測試(Conformance Test)。

二IPv6效能測試(Performance Test)。

三IPv6互連測試(interoperability)。

NICI IPv6標準測試實驗室依循之規範：

一IETF IPv6相關RFCs。

二3GPP/3GPP2相關標準。

三IPv6 Forum/IPv6 Ready Logo。

四Committee相關決議。

民間方面，2002年4月11日成立「台灣IPv6論壇」(IPv6 Forum Taiwan)，由工研院電通所出面召集廠商，獲得近 20家資訊通訊廠商如Hinet、亞旭、友訊與智邦等業者及ISP加入，如此一來，結合政府與民間的力量，共同進行IPv6推動計畫，以期整合產、官、學、研界資源，同步推動IPv6建置計畫，俾使我國即早邁入IPv6資訊網路新紀元。

行政院國家資訊通信基本建設小組總召集人蔡清彥表示，為實現IPv6網際網路環境，「IPv6推動工作小組」已正式研擬「加速寬頻網路建設－我國IPv6建設中程發展計畫」，並正式宣示IPv6為我國網際網路建設之重要工作計畫項目。預計至96年漸進達成以下目標：

一學術網路骨幹92年度達100%支援IPv6；國內ISP業者網路至96年度達100%支援IPv6。

二國內網路相關軟硬體於96年度皆能支援IPv6。

三於94年度建置完成國內IPv4至IPv6轉換機制。

四於95年度完成建立符合標準規範的IPv6測試驗證中心。

五每年(92-96年度)舉辦國內及國際性大型IPv6研討會各一次。

六92年度台灣擁有IPv6位址之ISP數達5家、93年度15家、94年度30家、95年度達50家，96年度達100%。

IPv4/IPv6的轉換(Transition)

目前的IPv4網路應用非常廣泛與普及，IPv6網路如何與IPv4網路進行正常通信，必須開發出IPv4/IPv6互通技術以保證IPv4能夠平穩過渡到IPv6。為此IETF下一代轉移工作小組(Internet Engineering Task Force Next Generation Transition Working Group, IETF NGTrans WG)訂定了一系列的標準，目前已經出現了多種過渡技術和互通方案，這些技術各有特點，用於解決不同過渡時期、不同環境的轉移依據：

一雙協定堆疊(Dual-stack)

IPv4和IPv6最直接相容的方式就是雙協定堆疊，也就是節點同時具備IPv4和IPv6的Protocol Stack。當與IPv4節點(IPv4-only)連接時，使用IPv4通訊協定；當與IPv6節點(IPv6-only)連接時，使用IPv6通訊協定，達到互通的目的。

這種方式對IPv4和IPv6提供了完全的相容，但由於需要雙路由設備，增加了網路的複雜度，卻依然無法解決IPv4地址耗盡的問題。

二IPv6-over-IPv4隧接(Tunneling)

隧接是一種利用IPv4封包及IPv4網路來傳送IPv6封包的技術。當網路兩端是IPv6節點，兩節點連接時中間需跨越IPv4網路，可使用此方法來連接。在從純IPv4網路環境變遷到純IPv6網路的過程中，藉著建立隧道(tunnel)的方法，可使得IPv6封包得以穿越IPv4涵蓋的網路，達成與遠端IPv6端點連線的需求。其方法是在兩節點間建立IPv4 tunnel，IPv6封包是在隧接起始點被封裝(encapsulate)入IPv4封包的酬載中，而在隧接終點處被解封裝(decapsulate)還原爲IPv6封包，封裝/解封裝IPv6封包的起始與終結點稱之爲隧接端點。隧接端點必須是具備IPv4/IPv6雙協定堆疊的節點。目前隧道建立的方式主要有預設式隧接(Configured Tunnel)、自動式隧接(Automatic Tunnel)、6to4、6over4、隧接代理者(Tunnel Broker)等方式來完成。隧道技術巧妙地利用了現有的IPv4網路，雖然提供了一種使IPv6的節點間能夠在過渡期間通信的方法，卻不能解決IPv6節點與IPv4節點間互通的問題。

三網路位址轉換及協定轉換(NAT-PT)

NAT-PT(Network Address Translation-Protocol Translation)，適用於IPv4-only節點與IPv6-only節點之間的通訊，此方法並未藉助雙協定堆疊或是隧接的機制來完成。NAT-PT必須將封包的相關欄位做相對應的轉換(即IPv4轉爲IPv6、或是IPv6轉爲IPv4)，如IP位址、傳輸代碼(如TCP/UDP Port No、ICMP Query Id等)、header checksum等，酬載部分也應配合需要進行修改，由於IPv4和IPv6的封包欄位在與格式上有些差距，因此NAT-PT轉換有其侷限性。

IPv4網路過渡到IPv6網路，在不同的過渡階段、不同的網路環境應採用不同的過渡技術和機制。現有的過渡機制各有其優缺點和各自不同的適用範圍，評估不同的過渡階段及應用的範圍，合理選擇轉換機制，才能更順利地以較小的代價實現IPv4網路向IPv6的平穩過渡。

結論

美國國防部負責網路和資訊集成的副部長John Stenbit於2003年6月17日宣布：「凡是在十月份以後替換的設備必須相容IPv6，並且在2008年以前，國防部相關的IPv4網絡將完全遷移到IPv6上」，他強調這將是軍隊裝備的一次的革新，Stenbit表示IPv6之所以能引起軍隊的注意是因爲它能夠提昇端對端的安全性和網路服務質量，這樣就能確保資料通過網路準確地到達指定的目的地。而在現有的IPv4系統中，這些是不被保證的。而且軍隊也要和那些準備升級到IPv6商業組織保持同步。

作者簡介

張俊榮，私立中原大學電機系、私立中原大學電子所碩士。曾任工程師。現任中華電信研究所助理研究員。