

新一代網路通信協定 IPV6

The next generation Internet Protocol—IPv6

臧意周

Yih-Jou Tzang

空軍航空技術學院軍事學科部專業專精組教官

Department of Professional Staff, Air Force Institute of Technology

摘要

隨著網際網路的流行與普及，現有網路通信協定所定義的 IPv4 位址範圍，很快就會不敷使用，預計在 2009~2010 年間將面臨分配使用完畢，因此使得 IPv6 的發展及推動越來越為迫切。又因為 IPv6 的發展所影響到的不只是網路、通信製造業、ISP 業者等，未來的佈建也將影響到我國整體的資訊、通信基礎建設的平台轉移。而國家的資訊、通信基礎建設成果，更關係著人民生活水準及產業的整體競爭力。因此，對新一代網際網路通信協定 IPv6，有其研究、探討與了解的必要性。

關鍵字：網際網路(Internet)、網路通信協定(IP)、IPv6、資訊基礎建設(NII)

Abstract

With the rapid development of Internet, people have been gradually recognizing the bottleneck of traditional IPv4 address and have been proposing “IPv6”, the next generation Internet protocol. However, using new technology may spend too much time and money while transferring for IPv4 to IPv6. In order to speed the spreading of new technology, the government should support it in many ways, including software, hardware and National Information Infrastructure (NII). If the development of IPv6 is successful, it will be a great benefit to many enterprises. For example: network service providers, Internet service providers (ISP) and telecommunication service providers. And the global competitiveness of Taiwan will be improved further in the future. Therefore, the researches and studies of the next generation Internet Protocol (IPv6) is important.

Keywords : Internet, Internet Protocol (IP), IPv6 (Internet Protocol Version 6), NII (National Information Infrastructure)

一、前言

由於這幾年來網際網路 (Internet) 的蓬勃發展，上網的人數也快速的增加。一九九〇年代初期網際網路開始走入家庭，用戶

數目在各種技術的推陳出新下 (其中以 HTTP 為基礎的瀏覽器與 BBS 最具代表性) 快速成長，後期又加入電子郵件、FTP 及 P2P 等誘人的全民應用，不但使得科技產業紛紛加入，原本興趣缺缺的傳統產業也

積極搶搭 Internet 列車，IP 位址的需求因而呈現爆炸性成長。此外在日常生活中，除了電腦可以上網以外，一些家電（如冷氣、冰箱）（可提供監控及遠端控制）、PDA、電話、手機．．．等等，也都將連接上網際網路視為其必要的基本功能了。

人類對於科技技術的要求提高及追求數位科技高品質、享受快速便捷的發展下，許多當初未被想到的使用形態都陸續出現，導致現在的網際網路規模，遠超過當初設計時的需求。而網際網路的運作，有一個不可或缺的要素，即 IP 位址，IP 位址相當於信封上的地址，網路上的資料在傳輸前，必須先加上原始及目的地 IP 位址後才送出，如此才能保障資料能順利送達。此種運作模式，使得原本網路網際使用的 IPv4 位址已經漸漸招架不住，所以許多這方面的專家和學者開始思考與探討這個問題，進而開始著手發展下一代的網際網路協定（IPng，Next Generation Internet Protocol），以解決這些問題以及應付未來的需求。而 IPv6 就是針對解決此一問題所衍生出來的，所以有些人將 IPv6 與下一代的網際網路畫上等號，也有許多人認為 IPv6 是歷史上最重大的網路及其技術的升級，在本篇文章中，將為各位詳細的介紹 IPv6 究竟是什麼。本論文的章節說明如下：第二部分探討 IPv6 的出現與發展；第三部分主題是 IPv6 與 IPv4 的比較；第四部分則主要探討的是 IPv6 定址方式；第五部分為結論，最後是參考文獻。

二、IPv6 的出現與發展

開始介紹 IPv6 之前，我們先回顧一下網路發展和網際網路通訊協定（IP，Internet Protocol）的歷史。在 1969 年美國國防部（DoD，Department of Defense）為了軍事的目委託了美國國防部高等研究計劃局（ARPA，Advanced Research Projects Agency）發展了一個雛型網路 ARPANet（現已經改由美國國防部通訊署 DCA，Defense Communications Agency

統籌管理，並且更名為 DARPA），研究出一套可以將不同製造公司、不同作業系統的網路，建立成一個像是網狀一樣的通訊網路，如此可以將大家擁有的資源，彼此互相分享、交換，後來這個運作方式就變成網際網路的創始，也奠定了今日的網際網路的模式，就是 TCP/IP（TCP，Transmission Control Protocol，就是中文的「傳輸控制通訊協定」；IP，Internet Protocol，就是中文的「網際網路通訊協定」），也就是我們最熟悉、最常在使用的網路通訊協定。

整個 TCP/IP 很重要的一部份就網際網路通訊協定（IP），而目前網路所使用的網際網路通訊協定是在 1975 年開始討論，1981 年 9 月的 RFC 791（Internet Protocol）中所制定的 Version 4 版本（也就是 IPv4）。IPv4 從制訂、發展至今將近 30 年仍歷久不衰，主因是其具備協定架構簡單、開放及傳輸效率高等優點。而在這段時間內電腦的技術有很大的進步，同時很重要的是，網際網路也急速地普及化，使得目前不單單只有電腦可以連接上網際網路，而是你所能想像到的科技產品、汽車、相框、門窗、保全、甚至是國防上，都朝向可以連接上網際網路的方向發展中，這也讓整各網際網路規模更快速度的蓬勃發展。現今 IPv4 最常被討論到的問題就是網路位址（IP Address）已經不敷使用，可以稍微想想，若是家裡的家電或是手邊有的一些電子設備都可以連接上網路時，光是一個人，就需要多少個網路位址數。因此許為了解決 IPv4 位址不夠使用的問題，各式各樣的解決方案都因此出現，例如 DHCP、NAT、CIDR．．．等，雖然這些 IPv4 的延續策略，可以讓位址數短暫避開不夠使用的窘境，但根據一些專家的預測，再過幾年後，網際網路的應用會比現在更加熱絡、頻繁，也許將有更多沒有想到的應用，都會如雨後春筍般的冒出，此時這些解決方案也都會達到瓶頸、極限。而 IPv6 就是在這樣的時空環境當中討論所產生。



圖一 網路位址需求無所不在

在一九九〇年代初期，網際網路工程任務專案小組（IETF，Internet Engineering Task Force）開始研發一套新的標準和網際網路通訊協定，而在當時有許多的方案都相繼被提出，目的都是為了解決 IPv4 所面臨的位址數不足的問題。在 1993 年，IETF 成立了下一代網路領域（IPng Area），用來評估與研究各項方案的建議以及技術的可行性，同時做出適當的建言以加速新一代網際網路通訊協定的發展與制定。在 1995 年，由 S. Bradner 和 A. Mankin 所提出的 RFC 1752（The Recommendation for the IP Next Generation Protocol）文件中，對於三個 IPng 的提案做了評估，三項提案分別為 CATNIP（Common Architecture for the Internet）、TUBA（TCP/UDP with Bigger Address）、SIPP（Simple Internet Protocol Plus）。而在 RFC 1951 被提出，經過廣泛的討論之後，IETF 最後選擇 SIPP，並參考其他提案的優點，加上 128 位元的位址，以及自動設定的功能等，做為下一代網際網路通訊協定的發展基礎，同時將也將 SIPP 正是命名為 IPv6（Internet Protocol version 6）。也許有人會好奇的問，IPv4 之後為什麼不是命名為 IPv5 呢？主要的原因是版本的序號是由 IANA（Internet Assigned Numbers Authority）所管理的，而在 1990 年 10 月所提出的 RFC 1190（Experimental Internet Stream Protocol, Version 2 (ST-II)）已經使用了 IPv5，所以新一代的網際網路通訊協定也就只好依序變成 IPv6 了。

三、IPv6 與 IPv4 的比較

前面提到 IPv6 可以解決 IPv4 發展所面臨到的一些難題，但是究竟 IPv6 與 IPv4 差別在那，以下將敘述幾項 IPv6 與 IPv4 的主要不同點：

3.1 定址範圍

IPv6 最大的特色就是將位址的空間由原本 IPv4 的 32 個（ $4 * 8$ ）位元，擴增到 128 個（ $8 * 16$ ）位元，位置空間由 4,294,967,296 個（ 2^{32} 個）可能的位址，大幅增加到 340,282,266,920,938,463,374,607,431,768,211,465（ 2^{128} 個）個可能的位址，共增加了 2^{96} 倍，這將足以解決目前 IPv4 位址短缺的困擾。

3.2 標頭（Header）格式

IPv6 為了使得封包在網路傳輸的過程中，讓中間的網路設備處理的速度更快，在標頭格式的部份，將標頭的格式簡化，同時也將標頭由原本不固定長度變更為固定的共 40 個位元組的長度，但這樣的調整，勢必得將 IPv4 標頭做一些幅度的修改，於是 IPv6 將原來 IPv4 標頭中的一些欄位做了修訂。圖二為 IPv4 標頭的格式，圖二中綠色的部份是在 IPv6 標頭格式中，去除不用的欄位，而橘色的部份則是在 IPv6 標頭格式中被更名的欄位，原本的 Total Length 改成 Payload Length，Time to Live 改成 Hop Limit，另外 Protocol 則是被 Next Header 所取代。圖三為 IPv6 標頭的格式，其中灰色的部份，則是 IPv6 增加的欄位。

0 31 bits

Version	1HL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options + Padding				

圖二 IPv4 標頭的格式

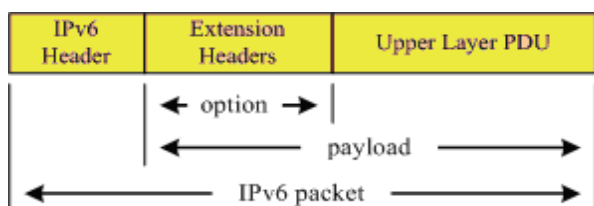
0 31 bits

Version (4 bits)	Traffic Class (8 bits)	Flow Label (20 bits)	
Payload Length (16 bits)		Next Header (8 bits)	Hop Limit (8 bits)
Source IP Address (128 bits)			
Destination IP Address (128 bits)			

圖三 IPv6 標頭的格式

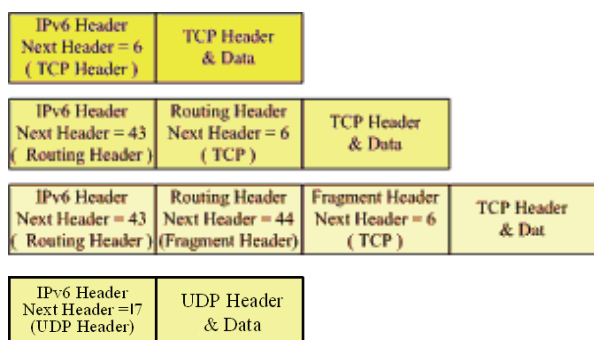
3.3 延伸擴充標頭 (Extension Headers)

選項 (Options) 在 IPv4 格式中是被整合於 IPv4 標頭中，但是在 IPv6 格式中，這些選項被放到延伸標頭中，如圖四所示。延伸標頭對於 IPv6 封包來說是可以有，也可以沒有的欄位，當需要有用到它時，它是利用串接的方式放置於 IPv6 標頭與資料 (Payload) 之間，這使得 IPv6 對於選項欄位變得十分彈性，當有新的選項被定義時，可以很輕易的加入進來，同時也讓 IPv6 的封包轉送效率大幅提升。



圖四 IPv6 封包結構

在 IPv6 標準中，IPv6 中的延伸標頭究竟是做什麼用途？此選擇性的網路層資訊被編碼在不同的延伸標頭內，並且可以由零個、一個或一個以上的延伸標頭，而每個延伸標頭類型則由前一個延伸標頭中的 Next Header 欄位來識別，欄位值 6 為 TCP 標頭，17 為 UDP 標頭，43 為路由標頭，44 為斷片標頭，如圖五所示。



圖五 延伸標頭使用方式

3.4 增加的安全性

一些資料安全方面的問題，在 IPv4 中是被歸類於必須在應用層解決，而在下層是不須要處理這方面的問題。但隨著實際的需求與技術的進步，由應用層來解決資料安全的設計方式，已經無法滿足現實的需求，因此在 IPv6 中利用它延伸標頭的特性，來達成對於認證的支援，同時對於資料完整性和資料保密性，一併做了規劃，也就是 IPv6 支援加密機制，以保證視頻、圖像傳送的完整性和私密性，將這些設計列入 IPv6 提供的功能當中。

3.5 資料流種類 (Traffic Class) 和資料流標籤 (Flow Labeling)

IPv6 在標頭增加兩項欄位資料流種類 (Traffic Class) 與資料流標籤 (Flow Label)，這二個欄位可用於初始節點的路由器去標示和區分不同 IP 封包類別和優先權，用來為 IP 封包提供不同形式的區別服務。這使得發送端可以將屬於相同的資料流 (Data Flow)、特別優先權或是有服務品質需求 (QoS, Quality of Service) 的封包，標上特定的種類 (Traffic Class) 或標籤 (Labeling)，這對於一些需要即時服務 (Real-time Service) 的應用，例如多媒體、網際網路視訊服務等，能夠對它們提供一定服務品質的保障。Payload Length (16 Bits)，則是用來記錄 Payload 的長度，以 Bytes 為計量單位。Hop Limit (8 Bits)，用來辨識封包是否要繼續向下傳送，每經過一個傳送點，Hop Limit 就會減一，當 Hop Limit 減到 0 而尚未到達目的位址時，這個封包逾時就會被丟棄。

3.6 位址自動組態隨插即用機制

IPv6 位址的隨插即用有自動組態有非狀態的自動組態 (Stateless Auto-configuration) 和狀態的自動組態 (Stateful Auto-configuration) 兩種。非狀態的自動組態是允許主機根據其本身網路卡卡號 (MAC Address) 自動產生位址，使得它可以與其他主機或路由器 (Router) 溝

通；而狀態組態則是透過 DHCP 伺服器搭配與主機位址。在 IPv4 位址上則必須了解基本的網路原理，然後對連接網路的設備作好正確的設定，才能成功的連上網際網路，這對於一些非電腦專業領域的人來說，仍顯得有些困難。而 IPv6 所提供的自動組態隨插即用方式，使得後續的一些數位家電或手持式設備，可以更簡易、甚至全自動化的連接上網際網路，這即是很重要的一項改進。

3.7 支援無線行動網際網路

IPv6 之發展目前以日本、韓國及歐洲國家最為積極，這幾個地區亦為第三代行動通信（3rd Generation Mobile Communication, 3G）等相關應用產業發展最為蓬勃之地，可望促使 3G 成為 IPv6 普及的關鍵應用。而大陸及印度為數眾多的人口，很可能是未來最迫切需要採用 IPv6 的國家。尤其大陸近兩年來，上網人口及行動電話用戶呈現快速成長的趨勢，相信未來結合 Mobile 應用的 IP 需求也將會特別殷切。

隨著這幾年來筆記型電腦或是手持式行動的設備普及，人們對於網際網路的行動能力需求也越益增加，因此 IPv6 當初在設計上也考慮到這點，於是在 IPv6 的標準中內建支援行動 IP（Mobile IP）的功能，使得在 IPv6 的環境下要行動上網更加方便。行動網際網路將成為全球無線寬頻應用市場之主流，未來網路節點設數量將會大幅增加，更加導致 IP 位址需求隨之成長。所以未來舉凡對物件導向（Object Orientation）、移動性（Mobility）及安全性（Security）等 IP 特性的市場需求，都將會是促成 IPv6 更為普及的原因。

3.8 芳鄰發現通訊協定

IPv6 的芳鄰發現（ND, Neighbor Discovery）通訊協定，是一組使用在 IPv6 訊息的網際網路控制訊息通訊協定（ICMPv6, Internet Control Message Protocol Version 6），它們管理相鄰節點之間的互動（同一連結上的節點）。芳鄰發現結合了位址解析協定（ARP, Address

Resolution Protocol）與 IPv4 網際網路控制訊息協定路由器發現（ICMPv4 Router Discovery）以及重導（ICMPv4 Redirect）等功能。

四、IPv6 定址方式

4.1 IPv6 位址表示法

在介紹 IPv6 定址的方式之前，我們得先介紹 IPv6 位址的表示法。在傳統 IPv4 的 32 位元位址，我們分別是以 8 個位元為界來劃分，然後用十進位來表示，並以句點作為分隔符號，例如 192.168.100.17、192.168.25.38 …等。但對於 IPv6 來說，若是使用同樣的方式來表達，其位址名稱將變成 192.168.100.17.119.67.8.11.23.123.42.21.11.71.83.1。這樣又長又難記的位址名稱，不但不容易理解更不方便使用。於是 IPv6 則是用 16 位元為界來劃分，然後用十六進位來表示，共有八組，並以冒號作為分隔符號，例如 21DA:0000:0000:02AA:0000:0000:0000:0008，上面的這個例子，還有更為簡便寫法 21DA:0:0:2AA:0:0:0:8，也就是可以省略每個區段中前置（Prefix）為零的部份。除了上述的表示法外，在當位址中有出現兩個以上為零的區段時，可以用雙冒號來取代一連串的零，同樣的以上面那個例子為例，它的精簡表示法為 21DA:0:0:2AA::8，因為此種的縮寫方式，只能在其中的一處被精簡，以避免產生模稜兩可（Ambiguity）的情況，一般是以多個零的部分，用雙冒號來取代。

4.2 IPv6 前置碼格式

IPv6 的位址是採階層式架構，可以分成數個副欄位，所以顯得非常有彈性，典型的 IPv6 位址包含三個部份：前面為全球路由前置碼（Global Routing Prefix），緊接下來在後面的是子網路識別碼（Subnet ID）以及最後的是介面識別碼等三個部份。RFC 2373（IP Version 6 Addressing Architecture）中列出許多的前置碼格式（

FP, Format Prefix), 透過前置碼格式可以用來區別特殊的 IPv6 位址, 例如鏈路本機位址、區域本機位址和多點傳播位址等, 表一列出了目前已經被配置的 IPv6 位址。

表一 已被配置的 IPv6 位址

配置	前置碼格式 (FP)
保留	0000 0000
保留給 NSAP 配置	0000 001
保留給 IPX 配置	0000 010
鏈路本機 (Link-local) 單點傳播位址	1111 1110 10
地區本機 (Site-local) 單點傳播位址	1111 1110 11
多點傳播 (Multicast) 位址	1111 1111
可聚集的全球單點傳播位址	001
迴路位址	00...1(128 bits)

4.3 IPv6 傳送位址的類型

在傳送位址的類型方面, IPv6 的傳送位址主要分為三大類, 其中單點傳播位址與 IPv4 的單點傳播位址概念相同, 而 IPv6 取消了原來在 IPv4 中的廣播 (Broadcast) 位址, 改由多重傳播 (Multicast) 位址取代之。除此之外, IPv6 較特別的是加入了 IETF 所提出的新類型位址, 任一傳播 (Anycast) 位址。任一傳播位址是 IPv6 獨有的位址類型。下面將針對三大類傳送位址類型做簡單的介紹:

4.3.1 單點傳播 (Unicast)

單點傳播位址適用於單一介面的位址, 帶有單點傳播位址的封包會傳送到具有該位址的介面 (網路卡)。而在 RFC 2373 中允許多個介面使用同一個位址, 但對於網路拓撲來說這些介面是可以看為單一介面。在同一鏈路上的不同節點, 不應配給它們相同的介面識別碼; 若具有多介面的網路節點要使用相同的介面識別碼時, 其必要條件就是這些介面須分別接在不同的子網路上。



圖六 單點傳播

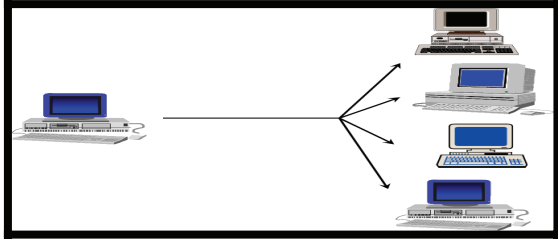
4.3.2 多重傳播 (Multicast)

多重傳播位址適用於一組介面的位址, 帶有多重傳播位址的封包會傳送到具有該位址的群組中所有介面。也就是說, 特定的一群主機可以組成一個群組, 而這一個群組中所有成員都會具有相同的多重傳播位址, 所以要傳播給群組中所有成員的封包時, 只要在目的端位置填入該群組的多重傳播位址, 群組中所有成員就能夠都收得到此一封包。

在 IPv6 的 128 位元位址格式中, 多重傳播位址表示法以 FF (十六進位) 為首並包括旗標 (Flags), 範圍 (Scope) 和群組 ID 等三欄位, 旗標欄位中包含了四個位元, 當中前三個位元保留為將來使用, 其預設值為 0, 而第四個位元稱為 T (Transient) 位元, 當 T=0, 代表一個永久被指定眾所周知的多重傳播位址, 例如: 位址 FF02::1, 為永久性的多重傳播位址, 代表一個連線範圍裡所有節點的多重傳播位址。而 T=1, 代表了非永久性的多重傳播位址, 例如: 位址 FF12::A:B:C 為一個網路連線範圍內, 群組為 A:B:C 的暫時性多重傳播位址。當群組會議結束後, 此位址可被重新指定到其他群組。而範圍欄位是一個四個位元的欄位, 它是用來指定多重傳播群組成員的區域範圍。多重傳播 ID 欄位則是用來識別多點傳播群組。

多重傳播的應用可分為一對多、多對多及無線網路環境的應用。在一對多的應用, 群組裡會有一個信認伺服器, 將多點傳播的資料傳送給群組的其他成員。在多對多的應用裡, 群組內的成員其身份可以是傳送者與接收者, 只有合法的成員才能存取多重傳播資料。對於無線網路的技術日漸成熟, 多重傳播的應用自然因應而生, 例如: 行動線上遊戲、行動遠距教學及行動視訊會議...等。多重傳播在無線開放空間環境下所遇到的問題與可能解決的方法就更複雜。在無線環境下, 其頻寬不像有線環境那麼大, 因此在成員管理及路由資訊更新等方法, 需要進一步考慮其對頻寬的影響。此外, 無線環境

下，因為使用者的位置變動性高，在路由方面更形複雜。另一方面，在無線環境下，封包的遺失率更高，而且封包是傳送在開放空間，所有人都可以存取，因此，封包傳遞的可靠更須要加以考慮。

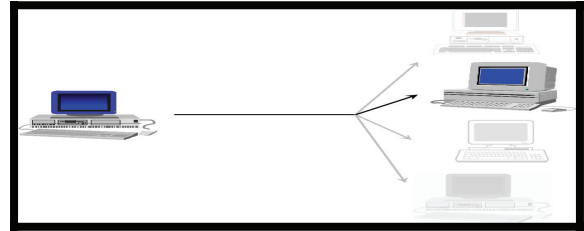


圖七 多點傳播

多重傳播路由協定，一般是採取階層式的架構，在一個網路內部網域內使用 Distance Vector Multicast Routing Protocol (DVMRP)、Multicast Open Shortest Path First (MOSPF)、Protocol Independent Multicast (PIM)。而對於網域間的多重傳播通訊則使用 Multicast Source Discovery Protocol (MSDP)、Multiprotocol extensions for BGP-4 (MBGP) 或 Border Gateway Multicast Protocol (BGMP) 做路由。

4.3.3 任一傳播 (Anycast)

任一傳播位址適用於一組介面的位址，並且這些介面通常都是屬於不同的節點，帶有任一傳播位址的封包會傳送到具有該位址的群組中某一個介面。此種傳播位址與多點傳播位址的功能十分相似，但不同的時，多重傳播會將封包傳送給群組中所有的成員，而任一傳播位址則只會傳送到最近的（或代價最少的）一個成員，而這邊所謂的最近並非實體（physical）網路位置上的最近，而是邏輯（Logic）網路上的最近或是負荷最輕的一個介面。任一播送位址現階段只適合配置給 IPv6 網路中之路由器使用，而不分配給網路主機。



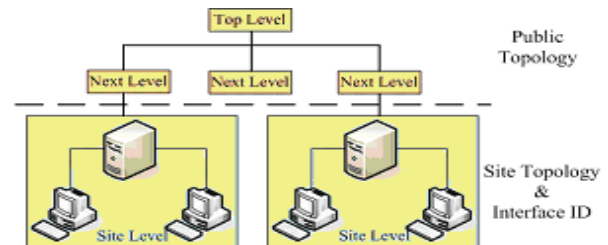
圖八 任一傳播

4.4 IPv6 位址範圍

IPv6 的傳送位址除了上述的三種類型外，根據其使用的範圍還可以再向下細分為全球單點傳播位址（Global Unicast Address）、鏈路本機單點傳播位址（Link-local Unicast Address）、區域本機單點傳播位址（Site-local Unicast Address）和特殊位址等。而下面將針對上述幾種位址做簡單的介紹：

4.4.1 全球單點傳播位址

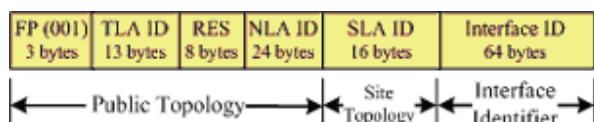
全球單點傳播位址是提供給 IPv6 節點來連上網際網路的位址，也就是說全球單點傳播位址是一種可以全球路由和連線的位址。全球單點傳播位址的格式支援目前以提供者為基礎的路由集合和新的以交換為基礎的路徑集合，此外 IPv6 位址很重要的一個特色就是階層式的聚集概念，階層式位址架構使得位址分配及維護管理都變得容易，同時也可促進路由選擇的效率。全球單點傳播位址的前置碼格式為 001，並且是由三個部份所組成，公共拓撲（Public Topology）、區域拓撲（Site Topology）和介面識別碼（Interface Identifier）。



圖九 IPv6 位址階層概念

全球單點傳播位址分成三個部份的主要目的是讓支援長途網路業者（Long Haul

Providers)，及其下所接的多層次網路提供者 (Multiple Levels of Providers)，乃至於使用者均能具備有分配位址之能力。而全球單點傳播位址格式如下：



圖十 全球單點傳播位址格式

FP：全球單點傳播位址的前置碼

TLA ID：頂層 (Top-Level) 聚集識別碼

RES：保留供未來使用

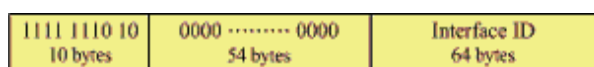
NLA ID：下一層 (Next-Level) 聚集識別碼

SLA ID：區域層 (Site-Level) 聚集識別碼

Interface ID：介面識別碼

4.4.2 鏈路本機單點傳播位址

鏈路本機單點傳播位址相當於微軟公司 Windows 系統上使用 169.254.0.0/16 字首自動組態的 IPv4 位址。鏈路本機單點傳播位址前置碼為 1111 1110 10，路由器不會轉送來源端或目的端位址為鏈路本機單點傳播位址的封包，也就是說此位址只能用於沒有路由器的 IPv6 網路中。通常來說鏈路本機單點傳播位址都是由自動組態程序所產生，因為鏈路本機單點傳播位址是 IPv6 芳鄰找尋中必要的位址，相當於 IPv4 中的網路卡位址。鏈路本機單點傳播位址格式如下：



圖十一 鏈路本機單點傳播位址格式

4.4.3 區域本機單點傳播位址

區域本機單點傳播位址相當於 IPv4 中的私有位址 (Private Address) 空間，10.x.x.x/8、172.16.x.x/12 和 192.168.x.x/16。區域本機單點傳播位址前置碼為 1111 1110 11，路由器不會轉送來源端或目的端位址為區域本機單點傳播位址的封包，也就是說此位址只能用於私有的區域網路。區域本機位址的使用是將封包的傳送，侷限於某一網域內部，一個連接外部網路的子網路間道路由器，不應

該將發送端位址或目的端位址中任一為區域本機位址型態的封包，轉出此子網路外部。區域本機單點傳播位址與鏈路本機單點傳播位址最大的差別在於，鏈路本機單點傳播位址是透過自動組態程序所產生的，而區域本機單點傳播位址則是必須透過一些受管理的位址組態程序來設定，例如手動設定等。區域本機單點傳播位址格式如下：



圖十二 區域本機單點傳播位址格式

4.4.4 特殊位址

在 IPv6 中還有一些特殊位址，例如不指定的 (Unspecified) 位址、迴路 (Loopback) 位址……等。

● 不指定的位址

不指定的位址其值為 0：0：0：0：0：0：0：0：0，也有人稱為全零 (All-Zeros) 位址，也可以縮寫為：：。不指定的位址與 IPv4 中的 0.0.0.0 意義相同，都是用來表示位址不在，所以這個位址不該動態或固定給網路介面，或是做為封包目的端位址。

● 迴路位址

迴路位址其值為 0：0：0：0：0：0：0：1，也可以縮寫為：：1。迴路位址與 IPv4 中的 127.0.0.1 意義相同，都是用來將封包傳送到協定堆疊 (Protocol Stack)，而不是實際傳送到網路上，通常用來檢測協定堆疊是否正常的運作，所以這個位址亦不該動態或固定給網路介面。

五、結論

目前 IPv6 的建置仍在持續增進當中，雖然純 IPv6 的應用還不夠多，但是如果對此新興科技有興趣，可到台灣 IPv6 論壇網站瀏覽看看，你會看到一些在 IPv4 不曾見過的新奇的應用產品 (如 IP 遙控器車、IPv6 檯燈、IPv6 行動終端機、IPv6 家電……等)。我國 IPv6 建置工作從 2001 年

就已正式展開，鑑於 IPv6 對未來網路及其他產業發展的重要性，行政院資訊通信發展小組（NICI）已於 2002 年將 IPv6 的建置發展列為六年國建「數位台灣」計畫重點項目。美國國防部也公告於 2003 年 10 月起，採購的網路設備需支援 IPv6 功能。2004 年開始，日本與美國相繼成立具有驗測 IPv6 功能設備的認證機構，並推廣至各國企業的設備，期望能為通信、電腦、資訊家電等相關業者共同開發 IPv6 應用。日本政府為了鼓勵電信及 ISP 業者建構 IPv6 網路，甚至提出設備採購稅金減免及零利率或低利率貸款等政策。而中國大陸對 IP 位址的需求隨著上網人口急遽發展與日俱增（目前僅次於美國，居世界第二），自 1998 年即開始發展及推動 IPv6，目前有許多的大型軟硬體研究及網路建置計劃執行中。在歐洲，歐盟委員會（EU Commission）已正式建議各國政府及工業界支持 IPv6，2001 年更在歐盟行政系統下成立 IPv6 任務工作小組（IPv6 Task Force），為歐洲地區規劃整體 IPv6 發展藍圖。自此可以看的出來，它會是資訊及相關產業發展與應用的趨勢，政府現正積極的主導推動，未來 IPv6 勢必會全面取代現有的 IPv4，應用於生活中各類型的資訊與通信產品中。

至於 IPv4 與 IPv6 轉換的過程中，並不是瞬間可達的，因為這樣重大的轉換，將會影響數以百萬的網路設備，以及所有相關的使用者，所以它必須經過逐步轉移而成，整個原有網際網路先是以 IPv4 為主要通訊協定，而 IPv6 則是一些實驗性質的區域網路。進入下一階段後，才開始有部份的網際網路以 IPv6 為主，不過整個網際網路的環境，還是 IPv4 居多，雖然 IPv6 已經開始涵蓋了一些區域，不過仍就是屬於少數。到了主流階段，IPv6 將開始成為主要的通訊協定，而 IPv4 則只剩一些還無法順利轉換的環境下才會使用。最後到了完成階段，IPv4 將會消失不見，整個網際網路環境都將為 IPv6 所取代而正式成為 IPv6 的天下。在轉

換過程中，大部分的時間 IPv4 與 IPv6 將會共存於網際網路中，因此造就了兩者間互通或者是轉換的機制，以確保在這段轉換過程的平順。本文希望透過上述這些對於 IPv6 的簡介，能夠多一個管道帶給大家對 IPv6 了解，讓大家對於下一代網路協定 IPv6 能有一些基本的認識。

參考文獻

- 1.RFC 2460 — “Internet Protocol, Version 6 (IPv6) Specification”。
- 2.RFC 2373 — “IPv6 Addressing Architecture”
- 3.RFC 2461 — “Neighbor Discovery for IP Version 6 (IPv6)”。
- 4.RFC 2463 — “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)”。
- 5.RFC 2236 — “Internet Group Management Protocol Version 2 (IGMPv2)”。
- 6.RFC 3170 — “Internet Group Management Protocol Version 3 (IGMPv3)”。
- 7.RFC 2710 — “Multicast Listener Discovery (MLD) for IPv6”。
- 8.RFC 3056 — “Connection of IPv6 Domains via IPv4 Clouds”。
- 9.RFC 2893 — “Transition Mechanisms for IPv6 Hosts and Router”。
- 10.RFC 2473 — “Generic Packet Tunneling in IPv6 Specification”。
- 11.RFC 3756 — “IPv6 Neighbor Discovery (ND) Trust Models and Threats”。
- 12.RFC 1075 — “Distance Vector Multicast Routing Protocol (DVMRP)”。
- 13.RFC 1584 — “Multicast extensions to OSPF (MOSPF)”。
14. “Protocol Independent Multicast (PIM) Sparse Mode : Motivations and

- architecture,” draft-ietf-pim-arch-05.txt。
- 15.RFC 2283 — “Multiprotocol extensions for BGP-4”。
16. “Multicast Source Discovery Protocol (MSDP) ,” draft-ietf-msdp-spec-06.txt。
17. “Border Gateway Multicast Protocol (BGMP) ,” draft-ietf-bgmp-spec-01.txt。
- 18.Upkar Varshney, “Multicast Over Wireless Networks,” Communications of ACM, Vol.45, No.12, Dec. 2002。
- 19.Hirorai. R. , Yoshifuji. H. , “Problems on IPv4-IPv6 Network Transition,” International Symposium on Applications and the Internet Workshops (SAINT) 2006, 23-27 Jan. 2006。
20. “IPv6 解析”，美商歐萊禮，ISBN: 9867794-11-7。
- 21.Internet Engineering Task Force (IETF) <http://www.ietf.org/>。
- 22.6Bone, <http://www.6bone.net>。
- 23.台灣 IPv6 RFC http://www.ipv6.org.tw/rfc/ipv6_rfcs.html。
- 24.台灣 TANET2, <http://www.tanet2.net.tw/index.html>。
- 25.TWNIC 國家高速網路與計算中心 IPv6 網址核發分配表 <http://rms.twnic.net.tw/twnic/User/Member/Search/IPv6Allocated.jsp>。
- 26.台灣 IPv6 論壇, <http://www.ipv6.org.tw>。
- 27.台灣 HiNet IPv6, <http://www.ipv6.hinet.net>。
- 28.台灣微軟 IPv6 論壇, <http://www.microsoft.com/taiwan/technet/community/columns>。