

政府採購 IPv6 資通設備與軟體 規範建議書

交通部

中華民國 101 年 2 月

政府採購IPv6資通設備與軟體 規範建議書

目 錄

1. 前言(INTRODUCTION).....	4
2. 本文件適用對象(SCOPE)	4
3. IPV6 設備型態.....	4
4. USG IPV6 PROFILE 和國際 IPV6 READY LOGO 標章.....	5
4.1. 美國 USG IPV6 PROFILE 介紹	5
4.2. 國際 IPV6 READY LOGO 標章	8
5. 採購 IPV6 資通設備與軟體規範建議	11
5.1. IPV6 軟體規範建議	11
5.2. IPV6 主機採購規範建議.....	13
5.3. IPV6 路由器採購規範建議.....	13
5.4. IPV6 網路保護設備採購規範建議.....	14
5.5. IPV6 特殊設備規範建議.....	14
5.6. IPV6 家庭閘道器設備採購規範建議.....	14
6. IPV6 互連測試建議.....	15
7. IPV6 轉移技術及資通設備引進 IPV6 功能執行方案建議	15
7.1. IPV4/IPV6 雙協定(DUAL STACK)技術.....	16
7.2. 隧道(TUNNELING)技術	16
7.3. 轉換(TRANSLATION)技術	17
7.4. 資通設備升級 IPV6 功能執行方案建議.....	18
8. 結語與建議.....	19
9. 參考文件(REFERENCES).....	20
10. 附錄一 IPV6 功能需求規範建議表	21

圖目錄

圖 1 美國 USGv6 IPv6 PROFILE 角色關係圖	7
圖 2 國際 IPv6 READY LOGO 標章(左邊為 PHASE-1 銀質標章和右邊為 PHASE-2 金質標章).....	8
圖 3 IPv6 READY LOGO PHASE-1 國家統計表	9
圖 4 IPv6 READY LOGO PHASE-2 國家統計表	10
圖 5 IPv6 測試服務流程	15
圖 6 IPv6 轉移趨勢	19

表目錄

表 1 IPv6 READY LOGO PHASE-2 測試項目	10
表 2 作業系統及常用應用軟體支援 IPv6 功能一覽表	12
表 3 IPv4/IPv6 雙協定(DUAL STACK)技術優缺點比較表.....	16
表 4 IPv4/IPv6 隧道(TUNNELING)技術優缺點比較表	17
表 5 IPv4/IPv6 轉換(TRANSLATION)技術優缺點比較表	18

1. 前言(Introduction)

本文件參考 IETF 國際標準[10]、IPv6 Forum IPv6 Ready Logo Program[2]、美國 NIST 文件 A Profile for IPv6 in the U.S. Government[11]及設備實際成熟度，提供建置可維運的 IPv6 網路及服務的參考技術規範，可協助各機構擬定合宜之網路建置規劃，購置 IPv6 功能較齊備且通過標準驗證之設備，以確保網路建設之投資效益。

至於 IPv6 建置之必要性及網路演進策略方法，不在本文件討論之範圍，本文件將持續檢視 IPv6 Ready Logo Program 之測試規範書，提供更精確之資料。

本文件後續章節將包含範圍、參考文件、IPv6 設備型態、美國 USGv6 IPv6 Profile 和國際 IPv6 Ready Logo 標章、IPv6 主機規範建議、IPv6 路由設備規範建議、IPv6 網路安全設備規範建議、IPv6 互連測試建議、IPv6 轉移技術及結論。

2. 本文件適用對象(Scope)

所有未來將提供 IPv6 服務之組織或個人，包括政府單位、學校、企業等，可協助引進符合標準與實際需求之 IPv6 路由設備、相關服務節點及網路安全裝置等。

3. IPv6設備型態

IETF 定義(RFC 2460)只要實作 IPv6 的設備就稱為 IPv6 節點(IPv6 Node)。根據此定義，IPv6 節點可分為主機(Host)和路由器(Router)兩種型態；但實務上為了網路安全，可能在路由器和主機中間擺設一種特殊設備，可過濾、阻斷或修正網路封包。對路由器來說，此設備像主機；但對於主機來說，又像路由器。我們概稱這種設備為『IPv6 網路保護設備』(IPv6 Network Protected Device)。另外，為了因應各類家電及網路應用等產品(如攝影機、印表機等)僅具備簡易 IPv6 能力的設備，在 IPv6 Ready Logo Technical Committee(IPv6 Ready Program 之技術單位，專門負責技術規劃事宜)特別定義了一種稱之為特殊設備(Special Device)。

近來家庭網路興起，對於 IPv6 也有特殊需求，在 RFC 6204[14]中也定義了家用設備特殊之規範，可視為 Router 和 Host 的整合形式，整體來說還是屬於 Router，但差異在於 WAN 端具備 Host 行為，但 LAN 端具備 Router 行為，於本文件中定義為家庭閘道器(Home Gateway)

歸納上述五種類型設備定義如下：

- (1) 主機(Host)：不屬於路由器的任何網路節點(如個人電腦、伺服器)。
- (2) 路由器(Router)：用以轉送其目的位址非本身位址的 IPv6 封包之節點。
- (3) 網路保護設備(Network Protected Device, NPD)：包括防火牆和入侵偵測/保護設備，可以選擇性地攔阻或者修正網路流量。
- (4) 特殊設備 (Special Device)：僅具備簡易 IPv6 能力的網路應用設備，或是資源、環境受限制之 IPv6 感知網路元件。

- (5) 家庭閘道器(Home Gateway)：適合家用網路連上網際網路之設備，具備快速設定、即插即用之功能。

4. USG IPv6 Profile和國際IPv6 Ready Logo標章

4.1. 美國 USG IPv6 Profile 介紹

網際網路起源於美國國防部(Department of Defense)，美國聯邦政府為了延續網際網路的既有優勢，並且期望持續扮演世界工業火車頭的角色。美國白宮 Office of Management and Budget 委託美國商業部(Department of Commerce)下轄之國家標準與技術研究院(NIST)[12]成立專案計畫 USGv6 Test Program[11]，其目的在於制訂 USG IPv6 Profile 規範美國聯邦政府資通信設備必須具有 IPv6 能力，並確保 IPv6 資通信設備的品質與互通性，進而建立社會大眾對 IPv6 資通信設備的產品信心，以因應 IPv6 世界的到來。

在 USGv6 Test Program 初期，美國國家標準技術研究院(NIST)延用國際上已推行多年由 IPv6 Forum IPv6 Ready Logo Program 所擬訂的測試規範(Test Specification)來進行驗證測試，並以此基礎擴充發展出美國聯邦政府 USGv6 IPv6 資通信設備採購規範及測試規範，作為美國聯邦政府及全球產業界的溝通橋樑。

NIST USG IPv6 Profile[11]是美國政府為了協助聯邦政府單位導入 IPv6 技術規劃之指引，於 2008 年 7 月發行第一版(預計 2011 年底發佈第二版)。此 IPv6 Profile 規範適用於聯邦政府所有日後非機密(non classified)、非國家機密 (non national security) 之資訊系統。其內容定義：

(a)統一網路設備專用術語。

(b)最基本的必要 IPv6 能力並提供設定 profile 範本 (configuration profile)，以協助聯邦政府單位未來建置 IPv6 網路時，採購設備之參考。

(c)提供爾後美國政府機構相關需求之技術指導。

NIST IPv6 Profile 參考 USG DoD，IEEE，ISO/IEC 之規定，符合 IETF 標準之名詞規範(MUST、SHOULD、MAY)精神。

NIST IPv6 Profile 因為得涵蓋所有聯邦政府單位系統需求，在定義需求之用字遣詞之選用上特別故意保守模糊。不過，此規範不但保護聯邦政府單位系統及早期之 IPv6 投資也同時提升美國政府之 IPv6 技術標準，未來可以有效協助美國聯邦政府單位資訊安全系統制訂其 IPv6 技術標準。

USGv6 Test Program 主要將資通信設備分類為 Host、Router 與 Network Protection Devices(NPD)三種角色進行測試，其測試項目與測試方法皆依據 IETF 標準 RFC 擬訂，相關測試規範請參考[11]。USGv6 Test Program 目前總共囊括了 12 項功能之測試，測試範圍超過 150 篇 RFC，測試範圍包括了 Basic IPv6 Requirements、Stateless Address Autoconfiguration(SLAAC)、Address Architecture Requirements、Internet Key Exchange(IKEv2)、IPSecv3、Dynamic Host Configuration Protocol(DHCPv6)、Encapsulating Security Payload (ESP)、Open Shortest Path First(OSPFv3)等。

在 USGv6 Test Program 測試計劃當中，任何一項功能皆必須通過兩種性質不同的測試，分別為符合性測試與互連性測試，這與 IPv6 Ready Logo Program 測試方法一致，其中符合性測試主要針對通信協定的功能作驗證；而互連性測試則主要針對產品與其他廠牌機器在同一個網路環境中進行互連測試。對於一個成熟的商用產品而言，應用於實際的商用網路佈建與日常運作當中，能夠正常地與其他廠牌的產品互連互運為最基本之要求，因此通過互連性測試為首要考慮重點。

USG IPv6 Profile 規範終端設備(Host)須具備以下功能：

Method H1: USGv6-V1-Capable Host Requirements

- IPv6 Basic Requirements
- SLAAC - require support of stateless address auto-configuration.
- DHCP-Client - require support of stateful (DHCP) address auto-configuration
- Addressing Requirements
- IP Security Requirements
- IPSec-v3 - require support of the IP security architecture
- IKEv2 - require support for automated key management
- ESP - require support for encapsulating security payloads in IP
- Multicast Requirements
- Link Specific Technologies
- Link - require support of 1 or more link technologies

USG IPv6 Profile 規範路由器(Router)須具備以下功能：

Method R1: USGv6-V1-Capable Router Requirements

- IPv6 Basic Requirements
- DHCP-Client - require support of stateful (DHCP) address auto-configuration
- Addressing Requirements
- IP Security Requirements
- IPSec-v3 - require support of the IP security architecture
- IKEv2 - require support for automated key management
- ESP - require support for encapsulating security payloads in IP
- Network Management Requirements
- SNMP - require support of network management services
- Multicast Requirements
- Quality of Service Requirements
- DS - require support of Differentiated Services capabilities
- Link Specific Technologies
- Link - require support of 1 or more link technologies

整體來說，USG IPv6 Profile 測試規範的測試類別與測試範圍超過 IPv6 Ready Logo 測試規範。但針對 USG IPv6 Profile 的單一測試類別(如 F1-IPv6 Basic Requirements、F2-SLAAC、F7-Addr Arch Requirements、F16-IPSec-v3、F29-ESP 等)

當中的測試項目則略少於 IPv6 Ready Logo 相對應的測試項目 Core、IPSec。

美國國家標準技術研究院(NIST)為了確保各測試實驗室之測試能力以及測試水準，規定 USGv6 Test Program 之測試實驗室(Testing laboratories)必須通過 ISO 17025 實驗室認證，而認證測試實驗室機構(Accreditation organizations)必須通過 ISO 17011 以及與簽署 International Laboratory Accreditation (ILAC) Mutual Recognition Arrangement (MRA)協議，確保測試實驗室公信力。

USGv6 Test Program 為了確保各測試實驗室之測試能力與水準相當，故採取實驗室間比對(Interlaboratory Comparisons)的方式來驗證各實驗室測試能力，各實驗室須對相同測試樣品(Test Sample)進行測試，並將測試結果上傳至 USGv6 網站供大家參考比對，如測試結果有不一致或不合理的情形，將被要求改正，如此確保測試實驗室之測試能力以及測試結果的精確度。

依 NIST 公告，廠商須利用供應者符合性聲明 Supplier's Declaration of Conformity (SDoC)宣告商品之測試結果是否符合 USGv6 Test Program 要求。買方將來也可藉由 SDoC 當作購買 IPv6 商品之參考依據，如此消費者對於 IPv6 商品之品質與實際互連能力將更有信心。美國聯邦政府已於 2010 年 7 月要求政府採購 IPv6 設備必須符合 USG IPv6 Profile 設備規範。USGv6 Test Program 將扮演政府機構與產業界的橋樑以及幫消費者把關的角色。

美國 USGv6 IPv6 Profile 及 Test Program 和測試實驗室、採購單位之角色關係如圖 1 所示。

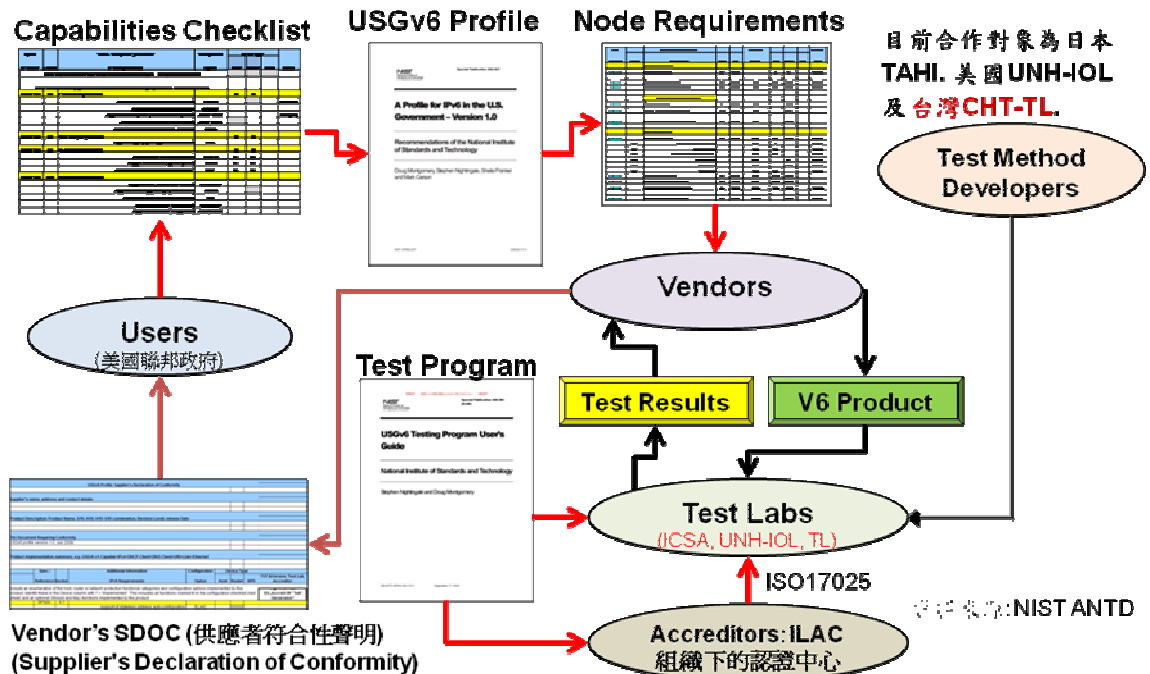


圖1 美國 USGv6 IPv6 Profile 角色關係圖

4.2. 國際 IPv6 Ready Logo 標章

國際 IPv6 Forum [1]為了協助大規模推廣 IPv6 網路技術與發展，於 2003 年 4 月 28 日特別召集全世界 IPv6 測試專家，共同組成 IPv6 Ready 標章委員會(IPv6 Ready Logo Committee)專門負責設計與制定 IPv6 符合性(Conformance)和互連性(Interoperability)測試規範，並成立國際特別工作組織 IPv6 Ready Logo Program(IPv6 Ready Logo 認證標章計畫)，負責推動與審核 IPv6 Ready Logo 業務。其目的在於給予使用者對於現在及未來使用 IPv6 的信心，督促設備廠商之設備符合 IPv6 標準，並提供 IPv6 相關測試套件及測試方法[2]。



圖2 國際 IPv6 Ready Logo 標章(左邊為 Phase-1 銀質標章和右邊為 Phase-2 金質標章)

目前 IPv6 Ready Logo 總共分成 Phase-1 及 Phase-2 (分別頒發銀質及金質標章，如圖 2所示)兩個階段實施：

Phase-1 主要有 94 項 IPv6 基本功能驗證測試，僅能保證最基本的 IPv6 功能及互通性。IPv6 Ready Logo Phase-1 自 2003 年 9 月 1 日正式開始實施以來，已成功地看到 IPv6 技術在全世界蓬勃發展。目前全球已有近 480 項產品通過認證，各國取得件數統計如圖 3(統計至 2011/12/31 日為止)，以本國臺灣為例，就已有獲得 75 項標章(詳細名單請參考[4])。IPv6 Ready Logo Phase-1 銀質標章已於 2011 年 11 月停止申請，原獲得銀質標章之 IPv6 產品將永久有效。

IPv6 Ready Logo Phase-1 統計表

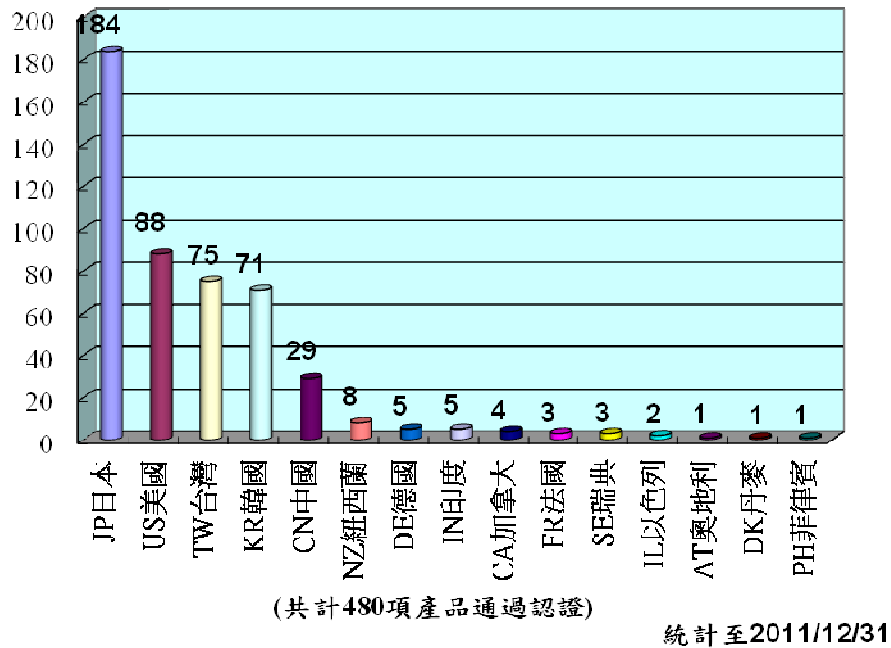


圖3 IPv6 Ready Logo Phase-1 國家統計表

為了進一步建立更高水準 IPv6 產品並贏得社會大眾對 IPv6 的信心，IPv6 Ready Logo 標章委員會乃進一步地研擬一套更嚴謹且完全符合 IETF 相關 IPv6 標準的測試規範。第二階段(Phase-2)為一國際性全方位 IPv6 測試計畫，主要由日本 TAHI[5]和美國 UNH(University of New Hampshire)互連測試實驗室 IOL(InterOperability Lab.)[6]共同負責制定、設計 IPv6 標準測試，並且獲得其它 IPv6 測試組織一致支持，如歐洲法國 IRISA、亞洲地區則有臺灣的中華電信研究所 IPv6 測試實驗室[7]、韓國的 TTA[8]以及中國大陸的 BII[9]等組織。此套測試標準不僅適合實務運作而且也可用於實際 IPv6 網路之建置。期望 IPv6 廠商能藉由第二階段(Phase-2)的實施而提昇改進他們原有 IPv6 產品功能，共同推動 IPv6 市場和建立社會大眾對 IPv6 產品的信心。自 2005 年 2 月 16 日正式開始實施，目前全球已有 675 項產品通過 Phase-2 認證，各國取得件數統計如圖 4(統計至 2011/12/31 日為止)，以本國臺灣為例，就已有獲得 126 項標章(詳細名單請參考[3])。

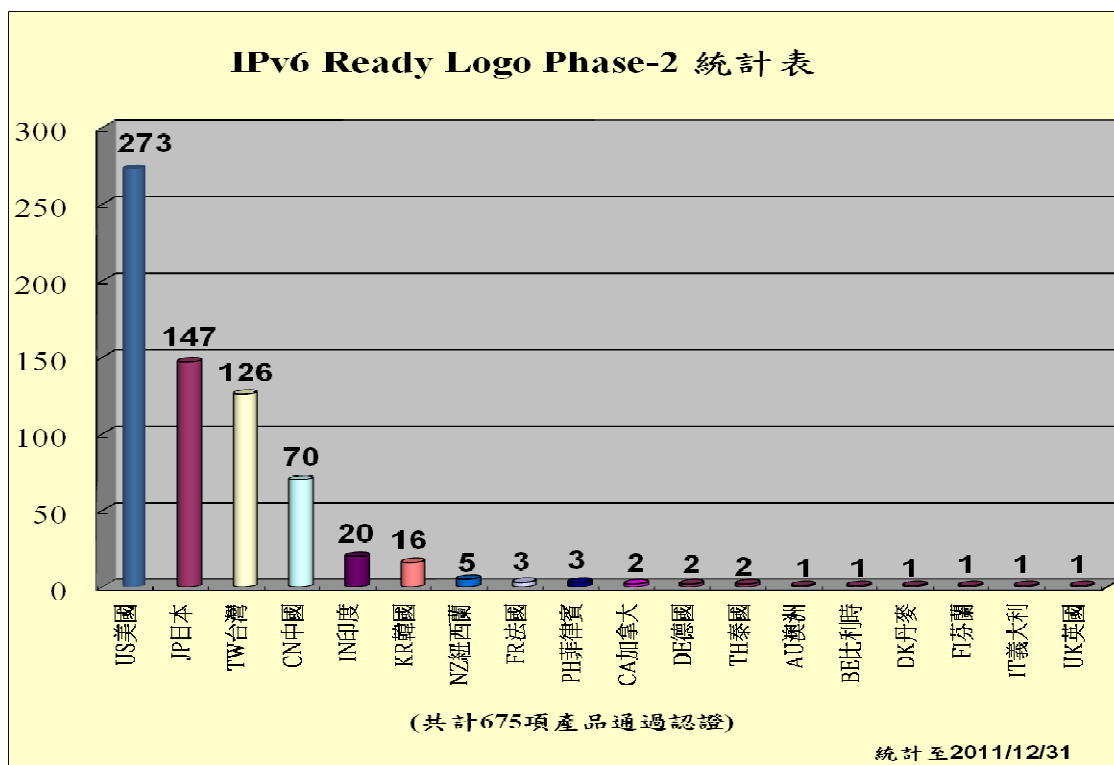


圖4 IPv6 Ready Logo Phase-2 國家統計表

IPv6 Ready Logo Phase-1 銀質標章為基本測試規範，目前著重於 Phase-2 推廣，Phase-1 為 Phase-2 之測試子集，換句話說 Phase-2 之金質標章技術門檻較高。Phase-2 測試項目現分成十大類，如表 1：IPv6 Core、IPSec、IKEv2、DHCPv6、SNMP/MIBs、SIPv6、IMS、MLDv2、Mobile IPv6(MIPv6)以及 NEMO。凡是欲申請取得 IPv6 Ready Logo Phase-2 金質標章者，皆應先通過 IPv6 Core 測試；其他測試項目皆為選擇性測試。每一類測試皆須通過符合性測試(Conformance)以及互連測試(Interoperability)。無論符合性測試以及互連測試，皆遵循其測試技術規格書(Test Specification)[2]。其中符合性測試已有開發自動化測試工具，可幫助申請者自行下載、進行安裝與測試。

表1 IPv6 Ready Logo Phase-2 測試項目

測試項目	必測與否	通過條件	符合性測試	互連測試
			測試規格	測試規格
P1/P2 Core	必測	100%	V4.0.6 2010/04/26	V4.0.4 2010/03/22
IPSec	選測	100%	V1.10.0 2010/05/31	V1.10.0 2010/05/31
IKEv2	選測	100%	V1.1.0 2010/06/08	V1.1.0 2010/06/08
DHCP	選測	100%	V1.1.3 2010/11/17	V1.1.0 2009/12/11
SNMP/	選測	100%	V1.0.3	V1.0.4

MIBs			2010/08/12	2010/08/20
SIP	選測	100%	Registrar V2.0.0 Proxy Server V2.0.1 UA, EP, B2BUA V2.0.2 2010/07/22	V2.0.2 2010/07/22
IMS	選測	100%	IMS UE V0.4.0 2010/10/15	V0.4.0 2010/10/15
MLDv2	選測	100%	MLDv2 Router V1.0.0 (2009/12/04)	V1.0.0 (2009/12/04)
MIPv6	選測	100%	CN(V3.2.0) HA(V3.2.0) MN(V3.2.0) 2007/11/08	V1.5.0 2007/11/08
NEMO	選測	100%	HA(v1.1.0) MR(v1.1.0) 2008/05/16	V1.1.0 2008/05/16

符合性測試主要是測試工具與待測物對接，連接在同一區域網段上，以驗證其功能是否達到 RFC 所規範之功能，並故意產生一些錯誤情況或是錯誤訊息給待測物，以測試待測物之錯誤處理能力，目前 IPv6 Core 參考標準為 RFC 2460、RFC4861、RFC 4862、RFC 4443、RFC5095 及 RFC 1981 共六篇。

互連測試主要是選擇兩種不同廠牌或來源之主機，以及兩種不同廠牌或來源之路由器進行測試，總共四種不同廠牌進行互連測試。待測物分別與此兩種主機及路由器，遵循互連測試規格書進行互連測試。

IPv6 Ready Logo Phase-2 Core 產品類別目前分成兩種，一為主機(Host)，另一為路由器(Router)。凡是 IPv6 產品，皆可測試，包括路由器、作業系統、通訊協定(Protocol Stack)、嵌入系統(embedded system)和特殊用途伺服器。

5. 採購IPv6資通設備與軟體規範建議

根據附錄一所示，IPv6 功能分為下列各類：IPv6 Core、Addressing、Link、IPSec、Mobility、Management、DHCPv6、Sockets、RADIUS、DNSv6、SIPv6、Routing、Transition 及 Multicasting。以下根據此分類，建議 IPv6 Host、Router、SPD、特殊設備和家庭開道器之設備規範，所有建議事項可根據實際需求進行適當修正。

使用國際 IPv6 Ready Logo 標章之優點為採購人員可簡單、快速的撰寫採購設備規格，後續的測試驗收可交由專屬測試實驗室負責，並可上網[2]查詢相關產品是否通過認證，目前全世界及本國知名網通廠商皆有相關產品獲得認證。

5.1. IPv6 軟體規範建議

大部分作業系統及應用程式皆已支援 IPv6 功能，但必須注意有些必需是指定的版本或某個版本以上的軟體，才支援 IPv6，如表 2 所示，Windows 2008 所有版本均支援 IPv6，FreeBSD 則必須是 4.0 版本或以上才支援 IPv6。

表2 作業系統及常用應用軟體支援 IPv6 功能一覽表

資訊系統平台	軟體	種類	支援 IPv6 版本	IPv6 Ready Logo 認證	
				Phase-1	Phase-2
微軟視窗作業系統及應用程式	Windows 2008	O.S.	全部支援		V
	Windows 2003	O.S.	全部支援	V	
	Windows XP	O.S.	SP1 及 SP2 均支援		
	Windows Vista	O.S.	全部支援	V	V
	Windows CE	O.S.	Ver. 4.1 或以上	V	
	Windows 7	O.S.	全部支援		V
	IIS	Web Server	Ver. 6.0 或以上		
	Apache	Web server	Ver. 2.0 或以上		
	sendmail	SMTP server	Ver. 8.10 或以上		
	SQL server	Database	SQL Server 2005 或以後		
Unix 作業系統及應用程式	FreeBSD	O.S.	Ver. 4.0 或以上	V	V
	Linux	O.S.	Ver. 2.4 或以上, Ver 2.6.15 佳	V	V
	NetBSD	O.S.	Ver. 1.5 或以上		
	OpenBSD	O.S.	Ver. 3.9 或以上		
	Novell	O.S.	Ver. 6.1 或以上, Ver 8.0 佳	V	
	Sun Solaris	O.S.	同時支援 SPARC 及 x64 平台版本, Ver. 8 或以上	V	
	IBM AIX	O.S.	RS6000, AIX 5.2 或以上, (WAS 6.0 以上)	V	V
	HP	O.S., HP-UX	Ver. 11i 或以上	V	V
	BIND	DNS server	Ver. 9.0 或以上		
	IBM	Database	DB2 9 或以上		
	PostgreSQL	Database	Ver. 8.3.1 或以上		
Oracle	Database	Ver. 10.1.3 或以上			
MAC 作業系統	MAC OS X	O.S.	Ver. 10.2 或以上		

5.2. IPv6 主機採購規範建議

IPv6 主機(Host)設備支援(伺服器屬於主機類別)，建議如下:(請參閱附錄一)

- (1) 必須通過 IPv6 Ready Logo Phase-2 Core for Host 的測試規範。
- (2) 安全選項：IPv6 Ready Logo Phase-2 IPsec for End-Node 的測試規範。
- (3) 網管選項：IPv6 Ready Logo Phase-2 SNMP for Agent 的測試規範(建議以 SNMPv2c 和 RFC 4293 IP MIB 為參考標準)。(惟考量網路演進趨勢，將有一段長時間之 IPv4/IPv6 並存時期，故可暫以提供 IPv4 SNMP 功能為近期之要求，待市場設備普遍成熟時再納入必要選項。目前標章只提供 Agent，Manager 則尚未提供)。
- (4) 移動性選項：IPv6 Ready Logo Phase-2 Mobility for Mobile Node 或 Correspondent Node 的測試規範，國際目前已有通過此規範之設備，唯數量不多(待市場設備普遍成熟時再納入考慮)。
- (5) DNS 選項：目前無 IPv6 Ready Logo 相關標準(已經列入下一階段 Phase-2 候選標章)，建議需支援 RFC3596 DNS Extensions to Support IP Version 6。
- (6) DHCPv6 選項：IPv6 Ready Logo Phase-2 DHCPv6 for Client，建議需支援 Client 模式，相關標準為 RFC3315 Dynamic Host Config Protocol (DHCPv6)。
- (7) 應用程式選項：目前已有 IPv6 Ready Logo Phase-2 SIPv6 for User Agent，但可考慮 email、Web 等服務或是註明相關應用程式必須同時支援 IPv4/IPv6 通訊協定[13]。(目前大部分作業系統皆已經支援 IPv6)。

其中(1)為必須支援，其餘(2)至(7)為所建議之選項，可依據不同用途勾選。

第二層交換器(Layer 2 Switch)和第三層 IP 是無關的，但有些應用服務，如群播服務，為了效能理由，往往限制群播服務流的範圍，故需新增 MLD/MLDv2 Snooping 功能(RFC 4541)。且為了管理和供裝理由，第二層交換器通常需要一個管理介面，建議此管理介面需符合 IPv6 Ready Logo Phase-2 Core for Host 規範，未來更需符合網管選項建議。

5.3. IPv6 路由器採購規範建議

IPv6 路由器(Router)支援，建議如下:(請參閱附錄一)

- (1) 必須通過 IPv6 Ready Logo Phase-2 Core for Router 的測試規範。
- (2) 安全選項：IPv6 Ready Logo Phase-2 IPsec for Secure Gateway 的測試規範。
- (3) 網管選項：IPv6 Ready Logo Phase-2 SNMP for Agent 的測試規範(建議以 SNMPv2c 和 RFC 4293 IP MIB 為參考標準)。(惟考量網路演進趨勢，將有一

段長時間之 IPv4/IPv6 並存時期，故可暫以提供 IPv4 SNMP 功能為近期之要求，待市場設備普遍成熟時再納入必要選項。目前標章只提供 Agent，Manager 則尚未提供)。

- (4) 移動性選項：IPv6 Ready Logo Phase-2 Mobility for Home Agent 的測試規範，國際目前已有通過此規範之設備，唯數量不多(待市場設備普遍成熟時再納入考慮)。
- (5) DNS 選項：目前無 IPv6 Ready Logo 相關標準(已經列入下一階段 Phase-2 候選標章)，建議需支援 RFC3596 DNS Extensions to Support IP Version 6。
- (6) DHCPv6 選項：IPv6 Ready Logo Phase-2 DHCPv6 for Server，建議需支援 Server 或 Relay Agent 模式，相關標準為 RFC3315 Dynamic Host Config Protocol (DHCPv6)。
- (7) 路由選項：目前無 IPv6 Ready Logo 相關標準，但須根據路由器之容量及使用地點，決定適當通訊協定，通常 SOHO Router 只要支援 RIPNG(RFC2080)，而大容量 Router 建議需支援 OSPFv3(RFC 5340)和 BGP-4+(RFC2545、RFC4271)。

其中(1)為必須支援，其餘(2)至(7)為所建議之選項，可依據不同用途勾選，建議至少提供一種路由協定。

5.4. IPv6 網路保護設備採購規範建議

需通過 IPv6 Ready Logo Phase-2 for Core 認證，相關安全需求同 IPv4 之安全功能。

5.5. IPv6 特殊設備規範建議

因 IPv6 Ready Logo Phase-2 無特殊設備定義，故 IPv6 特殊設備僅需通過 IPv6 Ready Logo Phase-1 Special Device 的測試規範。

未來物聯網 IPv6 無線感知網路興起，如果實體層採用 802.15.4(Zigbee)，建議其設備必須符合 RFC 4944 Transmission of IPv6 Packets over IEEE 802.15.4 Networks 及 RFC 4919 IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs):Overview, Assumptions, Problem Statement, and Goals.之規範。

5.6. IPv6 家庭閘道器設備採購規範建議

因 IPv6 Ready Logo Phase-2 目前無此定義(進行中)，故建議目前此設備必須通過 RFC 6204[14]之標準，待未來此測項成為國際 IPv6 Ready Logo 標章後，再行直接採用。

6. IPv6互連測試建議

依據 2003 年行政院國家資訊與通信推動工作小組(National Information and Communication Initiative, 簡稱 NICI) IPv6 推動工作小組規劃，委由台灣網路資訊中心執行『IPv6 建置發展計畫』，並推動由標準測試分組中華電信研究所規劃建置『IPv6 測試實驗室』[7]，於 2003 年 7 月 1 日正式開始提供國內產業、學術及研究單位等進行 IPv6 通信協定測試服務，以達成推廣 IPv6 發展之目標。同時，中華電信研究所 IPv6 測試實驗室為國際 IPv6 Ready 標章委員會之創始會員，多次獲邀參加測試規範制訂及審核國際案件申請，為臺灣廠商的溝通橋樑及技術諮詢單位。自成立以來，已經協助國內產學研界獲得多項 IPv6 Ready Logo Phase-1/Phase-2 標章。

中華電信研究所 IPv6 測試實驗室著重於 Phase-2 標章推廣，並具備美國 USGv6 Test Lab 之資格，建置多樣化符合性測試以及互連性測試技術平台，提供臺灣地區 IPv6 Ready Logo Phase-2 認證服務及美國 USGv6 測試服務。IPv6 測試服務流程，如圖 5 所示。

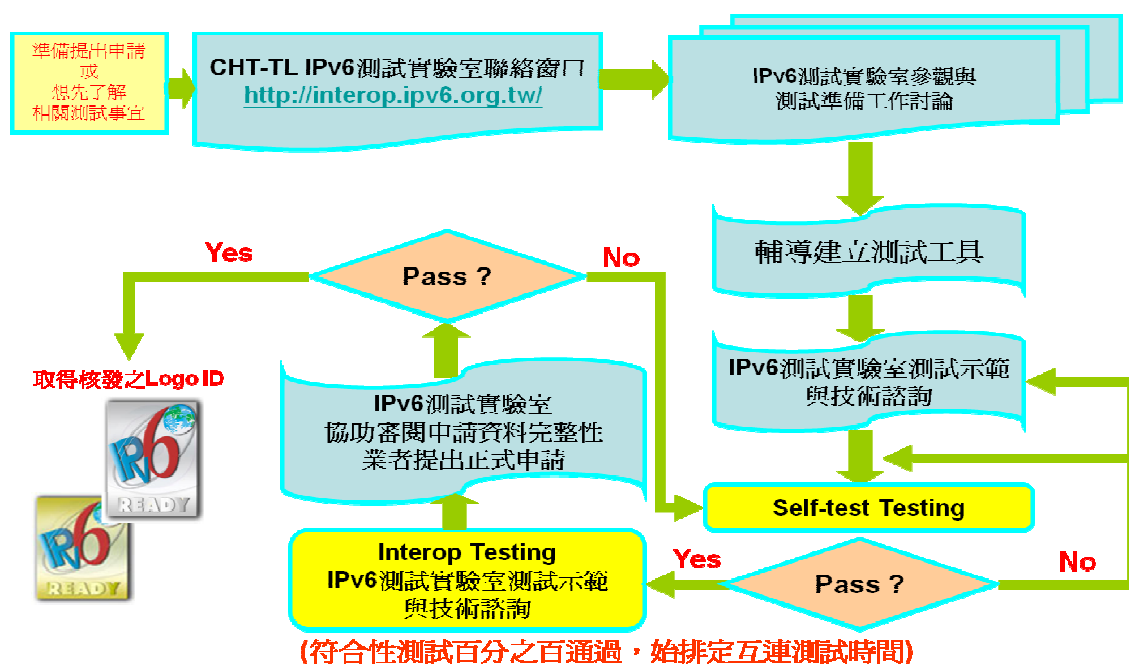


圖 5 IPv6 測試服務流程

有關國際 IPv6 Ready Logo 之互連測試可前往中華電信研究所 IPv6 測試實驗室[7] 進行相關服務。其他相關互連測試(如 Routing Protocol 等)，將視國際 IPv6 Forum 之規劃，陸續提供。

7. IPv6轉移技術及資通設備引進IPv6功能執行方案建議

由於全球網際網路的蓬勃發展，用戶數、路由器及應用服務伺服器數量非常龐大，轉移工程無疑是一項浩大工程。轉移時程並無法以約定的日期為基準日，進行全面的轉移。轉移的方式則是採漸進方式，在不影響現有網路服務下，依據網路現況靈活運用轉移機制，採循序漸進方式完成 IPv4 至 IPv6 的移轉。根據 IETF v6op 工作小

組及 RFC 4213 建議，轉移機制技術上分為三大類，IPv4/IPv6 雙協定(Dual Stack)、隧道(Tunneling)及轉換(Translation)等三大類技術，後續將介紹其優缺點，並建議資通設備引進 IPv6 功能的執行策略。

7.1. IPv4/IPv6 雙協定(Dual Stack)技術

所謂雙協定技術既是在同一台設備同時提供 IPv4 及 IPv6 處理能力，在 IPv4 轉移到 IPv6 過程的初期，所有具備 IPv6 處理能力的主機或路由器需配備 IPv4/IPv6 雙協定能力。此種 IPv4/IPv6 雙協定架構提供該 IPv6 設備可與既有的 IPv4 設備服務互連。

在轉移過程的最終階段，IPv4/IPv6 雙協定將由純 IPv6 協定取代，成為純 IPv6 主機或路由器。此轉移機制能使 IPv4 及 IPv6 的服務在同一網路上並行運作，讓轉移持續進行，而不影響整體原有 IPv4 網路的運作。

在 IPv4/IPv6 雙協定架構中，IPv4 層將被 IPv4/IPv6 雙協定層取代，而 TCP 與 UDP 層需升級至支援 IPv6，此種轉移方法非常簡潔明瞭，其主要缺失為主機或路由器需同時處理兩組位址，即 IPv4 位址及 IPv6 位址，降低處理效率，浪費記憶體空間，表 3 為雙協定技術優缺點比較表。

表3 IPv4/IPv6 雙協定(Dual Stack)技術優缺點比較表

IPv4/IPv6 雙協定(Dual Stack)轉移技術	
優點	缺點
<ol style="list-style-type: none"> 1. 容易設置與易懂。 2. 網路拓樸及端點對端點連線模式未遭破壞。 3. 雙協定主機可與其它雙協定主機、純 IPv4 主機或純 IPv6 主機互連。 	<ol style="list-style-type: none"> 1. 每個節點需 1 個 IPv6 位址及 1 個 IPv4 位址，兩者之間無關連。由於還是需要 IPv4 位址無法有效解決 IP 位址不足的問題。 2. 系統複雜度及負擔增加，需維持 2 個 IP 協定個別的路由資源及相關網管資訊。 3. 無法提供純 IPv4 主機與純 IPv6 主機的互通。

7.2. 隧道(Tunneling)技術

隧道(Tunnel)是一種利用 IPv4 封包及 IPv4 網路來傳送 IPv6 封包的技術。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，在 IPv6 發展初期，可節省大量建置成本。

IPv6 封包是在隧道起始點被封裝入 IPv4 封包的酬載 (payload) 中，而在隧道終結點被解封裝還原為 IPv6 封包，封裝/解封裝 IPv6 封包的起始點與終結點稱之為隧道端點。隧道端點必需是具備 IPv4/IPv6 雙協定的節點。

隧道可依據其建立的機制，分為自動式隧道與預設式隧道兩種。在自動式隧道方法中，封裝、目的地位址的抽取及隧道建立等動作是自動被完成的，不需人工的個別設定。在預設式隧道的建立過程中，隧道終結點的 IPv4 位址必需以人工方式個別預先設定。不同的 IPv6 網段及其相對映隧道終結點的 IPv4 位址等資訊均需事先取得，並加以人工方式設定後，方能夠建立 IPv6 網路間的連線。

隧道技術可分為 6over4(RFC 2529)、6to4(RFC 3056)、Tunnel Broker(RFC 3053)、ISATAP(RFC 5214)、Configured Tunnel(RFC 4213)及 6rd(RFC 55969)，在此不多加贅述，表 4 為隧道技術優缺點比較表。

表4 IPv4/IPv6 隧道(Tunneling)技術優缺點比較表

IPv4/IPv6 隧道(Tunneling)轉移技術	
優點	缺點
<ol style="list-style-type: none"> 1. 節點對節點的連線方式未遭破壞。 2. 利用現有 IPv4 網路，可降低成本。 3. 快速建立服務。 	<ol style="list-style-type: none"> 1. 需要 IPv4 網路架構。 2. 無法解決 IPv4 位址不足的問題。 3. 封裝及解封裝增加網路額外負擔。 4. 需要人工的設定與維護，增加網管者沈重的工作負擔。 5. 自動隧道技術容易產生資安問題。

7.3. 轉換(Translation)技術

IPv6 轉換技術可分為 SIIT(RFC 2765)、Network Address Translation-Protocol Translation(NAT-PT, RFC 2766)、Bump-In-Stack (BIS, RFC 2767)、Bump-In-API(BIA, RFC 3338)、A SOCKS-based IPv6/IPv4 Gateway Mechanism(RFC 3089)、An IPv6-to-IPv4 Transport Relay Translator(RFC 3142)、NAT64(RFC 6146)及 DNS64(RFC 6147)，相關技術在此不加贅述。

轉換機制提供給 IPv4 網域的純 IPv4 節點與 IPv6 網域的純 IPv6 節點達成連線的需求。NAT-PT 是位址及通訊協定轉換器，因為 IPv4 與 IPv6 封包在格式及內容定義上不同，兩者形同雞同鴨講，無法直接溝通，而 NAT-PT 可充當兩者的翻譯器。NAT-PT 的功能主要為位址轉換及協定轉換，在位址轉換方面，是將 IPv4 位址轉換為 IPv6 位址，反之亦然，但由於 NAT-PT 雙向協定非常複雜，造成實作上和 DNS 機制運作的困難，目前此協定已於 2007 年 7 月遭到廢除(RFC 4966)，由 2011 年 4 月制訂的 NAT64(RFC 6146)及 DNS64(RFC 6147)取代，和 NAT-PT 最大差異為只支援 IPv6 啟始連結 IPv4 資源，簡化通訊協定流程。

所有轉換機制無法處理封包酬載中位址的轉換，而有些應用程式是利用封包酬載來傳送位址資料，例如 DNS、FTP 等應用程式，這類應用就需要借助應用層閘道器

(Application Level Gateway, ALG), 例如 DNS-ALG、FTP-ALG 等, 將封包酬載中的位址做適當的 IPv4/IPv6 位址轉換以及通訊協定轉換, 達成應用層雙向互連, 表 5 為轉換技術優缺點比較表。

表5 IPv4/IPv6 轉換(Translation)技術優缺點比較表

IPv4/IPv6 轉換(Translation)技術 NAT-PT	
優點	缺點
1. 可建構在 IPv4 與 IPv6 網路交界位置, 提供純 IPv4 與純 IPv6 間的通訊, 免除將主機升級為雙 IP 協定堆疊的麻煩。 2. 運作對 end-user 而言幾乎是透通的。	1. 經由 NAT-PT 處理的 session, 在整個 session 過程中, 所有封包均需流經此 NAT-PT。因此 NAT-PT 轉換器可能成為網路運作的瓶頸點, 會危及整體網路運作。 2. 需借助 DNS-ALG、FTP-ALG 以及各種應用程式 ALG(Application Layer Gateway)方能處理封包酬載中位址的轉換, 達成應用層雙向互連。

7.4. 資通設備升級 IPv6 功能執行方案建議

未來網路會從只提供 IPv4 網路轉移至同時提供 IPv4/IPv6 雙協定網路, 甚至只提供 IPv6 網路及服務, 如圖 6。建議使用 Dual Stack 和 Tunneling 技術, 善加利用網路設備汰舊換新之時機, 降低設備採購成本, 順勢導入 IPv6 技術, 讓新購之網路節點同時支援 IPv4/IPv6 雙協定, 同時修正應用程式使其發展成為和 IP 層無關之應用程式, 即同時支援 IPv4 和 IPv6 之應用程式[13]。對於無原始碼之應用程式可考慮使用轉換技術(如 NAT64)來達成轉移之目的。

資通設備升級 IPv6 功能執行方案建議如下：

- (1) 檢視現有軟硬體設備支援 IPv6 之現況。
- (2) 新建置之設備必須加入支援 IPv6 功能選項。
- (3) 資訊系統規劃 OS 升版時, 必須要求同時支援 IPv4/IPv6 雙協定之功能。
- (4) 檢視應用軟體支援 IPv6 之現況, 無法升級之系統應擬定未來升級之計畫。
- (5) 注意引進 IPv6 帶來資安議題。

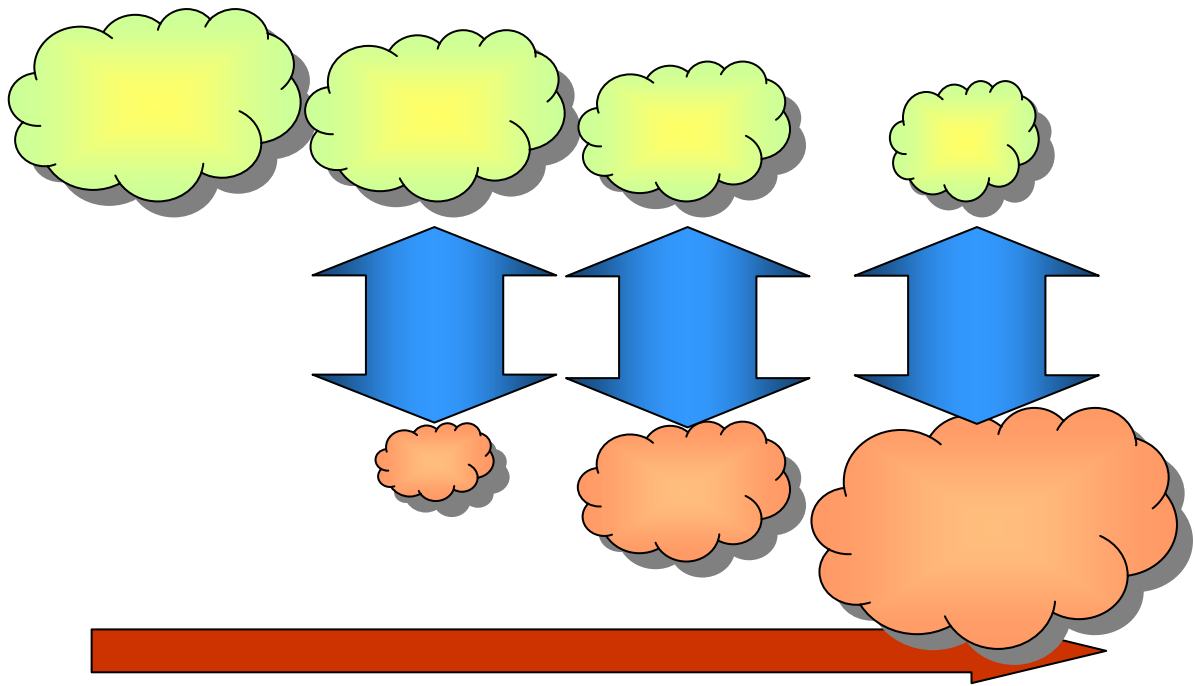


圖6 IPv6 轉移趨勢

8. 結語與建議

近來全球寬頻網路及行動寬頻服務蓬勃發展，IP 位址的需求量迅速成長，國際網路位置分配機構 IANA(Internet Assigned Numbers Authority)已於 2011 年 2 月 3 日宣佈無 IPv4 位址可供分配，而亞太地區 IP 資源分配機構 APNIC(Asia Pacific Network Information Centre, 亞太網路資訊中心)也於 2011 年 4 月 15 日啟動最後 Class A 位址發放機制，所有亞太地區之 ISP 最多只能再獲得 1024 個 IPv4 位址。我們應該主動積極地面對此困境，及早做好引進 IPv6 之準備。在 IPv6 服務未正式導入之際，應該著重於網路 IPv6 化能力，相關網路應該利用設備汰換，順便引進 IPv6，降低投資風險。

而從 Ready Logo 通過之設備不難發現，國際大廠之設備大都已經通過 Ready Logo 之認證，同時我國網通廠商之設備也都具備 IPv6 能力，將 IPv6 功能列入設備需求規範中，不必擔心因此無法獲得適當設備之困擾，且應善用國際 IPv6 Ready Logo 標章，適時導入，降低採購人員撰寫設備規格書之負擔及後續驗收之專業測試成本。

本文件著重於 IPv6 設備需求規範建議。在此版本中，把重心集中於建立一個 IPv6 網路基礎建設所需的能力，未來將持續檢視國際發展情勢，檢討各類設備與軟體之建議規範。

9. 參考文件(References)

- [1]. IPv6 Forum, <http://www.ipv6forum.org/>
- [2]. IPv6 Ready Logo Program, <http://www.ipv6ready.org/>
- [3]. 臺灣獲得 IPv6 Ready Logo 金質標章一覽表 ,
<http://interop.ipv6.org.tw/TaiwanIPv6ReadyLogoListPhase2.htm>
- [4]. 臺灣獲得 IPv6 Ready Logo 銀質標章一覽表 ,
<http://interop.ipv6.org.tw/TaiwanIPv6ReadyLogoListPhase1.htm>
- [5]. 日本 TAHI 測試組織, <http://www.tahi.org/>
- [6]. 美國 UNH IOL, <http://www.iol.unh.edu/consortiums/ipv6/>
- [7]. 臺灣 IPv6 測試實驗室, <http://interop.ipv6.org.tw/>
- [8]. 韓國 TTA, <http://www.tta.or.kr/English/new/main/index.htm>
- [9]. 北京 BII, <http://www.biigroup.com/>
- [10]. The Internet Engineering Task Force, <http://www.ietf.org/>
- [11]. A Profile for IPv6 in the U.S. Government – Version 1.0, NIST Special Publication 500-267, July 2008
<http://www.antd.nist.gov/usgv6/usgv6-v1.pdf>
- [12]. National Institute of Standards and Technology,
<http://www.nist.gov/index.html>
- [13]. RFC 4038, Application Aspects of IPv6 Transition, March 2005
- [14]. RFC 6204, Basic Requirements for IPv6 Customer Edge Routers, April 2011

10. 附錄一 IPv6功能需求規範建議表

符號說明：

- 1 *表示支援、空白表示不支援 (如 RFC 1981 Phase-1 不支援、Phase-2 支援)
- 2 M：必須支援此標準、O+：分類必須支援此標準(如 DHCPv6 的 RFC3315)、O:可選
- 3 RFC 紅色+底線表示 3.0 版更新之資料

2011/04/30 製表

分類	RFCs				IPv6 Ready Logo Phase-1	IPv6 Ready Logo Phase-2	經濟部標檢局 CNS IPv6 標準	美國 USGv6	設備需求建議			
	編號	標題	狀態	時間					Host	Router	SPD	HG
IPv6 Core												
IPv6 Core	RFC1981	Path MTU Discovery for IP version 6	PROPOSED STANDARD	Aug-96		*	*	*	M	M		
	RFC2460	Internet Protocol, Version 6 (IPv6) Specification	DRAFT STANDARD (Obsoletes RFC1883) (Updated by RFC5095)	Dec-98	*	*	*	*	M	M		
	RFC2464	Transmission of IPv6 Packets over Ethernet Networks	PROPOSED STANDARD (Obsoletes RFC1972)	Dec-98	*	*	*	*	M	M		
	RFC2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.	PROPOSED STANDARD (Obsoletes RFC1455, RFC1349) (Updated by RFC3168, RFC3260)	Dec-98		*		*	O	O		
	RFC2675	IPv6 Jumbograms	PROPOSED STANDARD (Obsoletes RFC2147)	Aug-99			*	*	O	O		
	RFC3697	IPv6 Flow Label Specification.	PROPOSED STANDARD	Mar-04					O	O		
	RFC3971	Secure Neighbour Discovery	PROPOSED STANDARD	Mar-05				*	O	O		
	RFC3986	Uniform Resource Identifier (URI): Generic Syntax	STANDARD (Obsoletes RFC2732, RFC2396, RFC1808) (Updates RFC1738) (Also STD0066)	Jan-05				*	O	O		
	RFC4291	Internet Protocol Version 6 (IPv6) Addressing Architecture	DRAFT STANDARD (Obsoletes RFC3513)	Feb-06		*	*	*	M	M		
	RFC4294	IPv6 Node Requirements	INFORMATIONAL (Updated by RFC5095)	Apr-06					O	O		

	RFC4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	DRAFT STANDARD (Obsoletes RFC2463) (Updates RFC2780) (Updated by RFC4884)	Mar-06	*	*	*	*	M	M		
	RFC4861	Neighbor Discovery for IP version 6 (IPv6)	DRAFT STANDARD (Obsoletes RFC2461)	Sep-07	*	*	*	*	M	M		
	RFC4862	IPv6 Stateless Address Autoconfiguration	DRAFT STANDARD (Obsoletes RFC2462)	Sep-07	*	*	*	*	M	M		
	RFC4884	Extended ICMP to Support Multi-Part Messages	PROPOSED STANDARD (Updates RFC0792, RFC4443)	Apr-07				*	O	O		
	RFC5095	Deprecation of Type 0 Routing Headers in IPv6	PROPOSED STANDARD (Updates RFC2460, RFC4294)	Dec-07		*		*	M	M		
	RFC5175	IPv6 Router Advertisement Flags Option	PROPOSED STANDARD (Obsoletes RFC5075)	Mar-08				*	O	O		
	RFC6204	Basic Requirements for IPv6 Customer Edge Routers.	INFORMATIONAL	Apr-11								M
Addressing	RFC2526	Reserved IPv6 Subnet Anycast Addresses	PROPOSED STANDARD	Mar-99				*	O	O		
	RFC3041	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	PROPOSED STANDARD (Obsoleted by RFC4941)	Jan-01								
	RFC3484	Default Address Selection for IPv6	PROPOSED STANDARD	Feb-03				*	O+	O+		
	RFC3587	IPv6 Global Unicast Address Format.	INFORMATIONAL (Obsoletes RFC2374)	Aug-03			*		O+	O+		
	RFC3595	Textual Conventions for IPv6 Flow Label	PROPOSED STANDARD	Sep-03			*		O	O		
	RFC3879	Deprecating Site Local Addresses	PROPOSED STANDARD	Sep-04				*	O+	O+		
	RFC3972	Cryptographically Generated Addresses (CGA)	PROPOSED STANDARD (Updated by RFC4581, RFC4982)	Mar-05				*	O	O		
	RFC4007	IPv6 Scoped Address Architecture	PROPOSED STANDARD	Mar-05				*	O	O		
	RFC4193	Unique Local IPv6 Unicast Address	PROPOSED STANDARD	Oct-05				*	O	O		
	RFC4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6.	DRAFT STANDARD (Obsoletes RFC3041)	Sep-07				*	O	O		
	RFC5156	Special-Use IPv6 Addresses	INFORMATIONAL	Apr-08					O	O		
	RFC5375	IPv6 Unicast Address Assignment Considerations	INFORMATIONAL	Dec-08					O	O		
	RFC5952	A Recommendation for IPv6 Address Text Representation	PROPOSED STANDARD (Updates RFC4291)	Aug-10					O	O		
	RFC6177	IPv6 Address Assignment to End Sites.	BEST CURRENT PRACTICE (Also BCP0157) (Obsoletes RFC3177)	Mar-11					O	O		

Link	RFC2467	IPv6 over FDDI	PROPOSED STANDARD (Obsoletes RFC2019)	Dec-98			*	O	O		
	RFC2470	Transmission of IPv6 Packets over Token Ring Networks	PROPOSED STANDARD	Dec-98				O	O		
	RFC2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks	PROPOSED STANDARD	Jan-99			*	O	O		
	RFC2492	IPv6 over ATM Networks	PROPOSED STANDARD	Jan-99			*	O	O		
	RFC2497	IPv6 over ARCnet	PROPOSED STANDARD	Jan-99			*	O	O		
	RFC2590	IPv6 over Frame Relay	PROPOSED STANDARD	May-99			*	O	O		
	RFC3146	IPv6 over IEEE 1394 Networks	PROPOSED STANDARD	Oct-01			*	O	O		
	RFC3572	IPv6 over MAPOS (SONET/SDH)	INFORMATIONAL	Jul-03				O	O		
	RFC4338	Transmission of IPv6 & IPv4 over Fibre Channel	PROPOSED STANDARD (Obsoletes RFC3831, RFC2625)	Jan-06			*	O	O		
	RFC4919	IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs):Overview, Assumptions, Problem Statement, and Goals.	INFORMATIONAL	Aug-07				O	O		
	RFC4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks.	PROPOSED STANDARD	Sep-07			*	O	O		
	RFC5072	IP Version 6 over PPP	DRAFT STANDARD (Obsoletes RFC2472)	Sep-07			*	O	O		
	RFC5121	Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks	PROPOSED STANDARD	Feb-08				O	O		
RFC5172	Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol	PROPOSED STANDARD (Obsoletes RFC2472)	Mar-08				O	O			
RFC5692	Transmission of IP over Ethernet over IEEE 802.16 Networks	PROPOSED STANDARD	Oct-09				O	O			
IPSec											
IPSec	RFC2403	The Use of HMAC-MD5-96 within ESP and AH	PROPOSED STANDARD	Nov-98		*		*	O+	O+	
	RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH	PROPOSED STANDARD	Nov-98		*		*	O+	O+	
	RFC2405	The ESP DES-CBC Cipher Algorithm With Explicit IV	PROPOSED STANDARD	Nov-98		*		*	O+	O+	
	RFC2410	The NULL Encryption Algorithm and Its Use With IPsec	PROPOSED STANDARD	Nov-98		*		*	O+	O+	
	RFC2451	The ESP CBC-Mode Cipher Algorithms	PROPOSED STANDARD	Nov-98		*		*	O+	O+	
	RFC3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec	PROPOSED STANDARD	Sep-03		*		*	O+	O+	
	RFC3602	The AES-CBC Cipher Algorithm and Its Use with IPsec	PROPOSED STANDARD	Sep-03		*		*	O+	O+	

	RFC3686	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP).	PROPOSED STANDARD	Jan-04		*		*	O+	O+		
	RFC4301	Security Architecture for the Internet Protocol	PROPOSED STANDARD (Obsoletes RFC2401)	Dec-05		*		*	O+	O+		
	RFC4302	IP Authentication Header	PROPOSED STANDARD (Obsoletes RFC2402)	Dec-05		*		*	O+	O+		
	RFC4303	IP Encapsulating Security Payload (ESP)	PROPOSED STANDARD (Obsoletes RFC2406)	Dec-05		*			O+	O+		
	RFC4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).	PROPOSED STANDARD (Obsoletes RFC2402, RFC2406) (Obsoleted by RFC4835)	Dec-05		*		*	O+	O+		
	RFC4308	Cryptographic Suites for IPsec.	PROPOSED STANDARD	Dec-05				*	O	O		
	RFC4310	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP).	PROPOSED STANDARD	Dec-05					O	O		
	RFC4312	The Camellia Cipher Algorithm and Its Use With IPsec.	PROPOSED STANDARD	Dec-05		*			O+	O+		
	RFC4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).	PROPOSED STANDARD (Obsoletes RFC4305)	Apr-07				*	O	O		
	RFC4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec.	PROPOSED STANDARD	May-07		*		*	O+	O+		
IKEv2	RFC4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP).	PROPOSED STANDARD	Dec-05					O	O		
	RFC4306	Internet Key Exchange (IKEv2) Protocol.	PROPOSED STANDARD (Obsoletes RFC2407, RFC2408, RFC2409) (Updated by RFC5282)	Dec-05		*		*	O+	O+		
	RFC4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).	PROPOSED STANDARD	Dec-05		*		*	O+	O+		
	RFC4718	IKEv2 Clarifications and Implementation Guidelines.	INFORMATIONAL (Obsoleted by RFC5996)	Oct-06		*			O	O		
	RFC4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).	PROPOSED STANDARD (Obsoletes RFC4305)	Apr-07					O	O		
	RFC5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol.	PROPOSED STANDARD (Updates RFC4306)	Aug-08					O	O		

	RFC5739	IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)	EXPERIMENTAL	Feb-10						O	O		
	RFC5996	Internet Key Exchange Protocol Version 2 (IKEv2)	PROPOSED STANDARD (Obsoletes RFC4306, RFC4718) (Updated by RFC5998)	Sep-10						O	O		
	RFC5998	An Extension for EAP-Only Authentication in IKEv2.	PROPOSED STANDARD (Updates RFC5996)	Sep-10						O	O		
Mobility													
MIPv6	RFC3775	Mobility support in IPv6	PROPOSED STANDARD	Jun-04		*	*	*		O+	O+		
	RFC3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	PROPOSED STANDARD (Updated by RFC4877)	Jun-04		*	*			O+	O+		
	RFC4283	Mobile Node Identifier option for MIPv6	PROPOSED STANDARD	Nov-05				*		O	O		
	RFC4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture.	PROPOSED STANDARD (Updates RFC3776)	Apr-07		*		*		O	O		
	RFC5094	Mobile IPv6 Vendor Specific Option	PROPOSED STANDARD	Dec-07						O	O		
	RFC5096	Mobile IPv6 Experimental Messages	PROPOSED STANDARD	Dec-07						O	O		
	RFC5142	Mobility Header Home Agent Switch Message	PROPOSED STANDARD	Jan-08						O	O		
	RFC5149	Service Selection for Mobile IPv6	INFORMATIONAL	Feb-08						O	O		
	RFC5268	Mobile IPv6 Fast Handovers	PROPOSED STANDARD (Obsoletes RFC4068) (Obsoleted by RFC5568)	Jun-08									
	RFC5269	Distributing a Symmetric Fast Mobile IPv6 (FMIPv6) Handover Key Using SEcure Neighbor Discovery (SEND)	PROPOSED STANDARD	Jun-08						O	O		
	RFC5270	Mobile IPv6 Fast Handovers over IEEE 802.16e Networks	INFORMATIONAL	Jun-08						O	O		
	RFC5271	Mobile IPv6 Fast Handovers for 3G CDMA Networks	INFORMATIONAL	Jun-08						O	O		
	RFC5380	Hierarchical Mobile IPv6 (HMIPv6) Mobility Management.	PROPOSED STANDARD (Obsoletes RFC4140)	Oct-08						O	O		
	RFC5419	Why the Authentication Data Suboption is Needed for Mobile IPv6 (MIPv6)	INFORMATIONAL	Jan-09						O	O		
	RFC5447	Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction.	PROPOSED STANDARD	Feb-09						O	O		
RFC5555	Mobile IPv6 Support for Dual Stack Hosts and Routers.	PROPOSED STANDARD	Jun-09						O	O			
RFC5568	Mobile IPv6 Fast Handovers	PROPOSED STANDARD (Obsoletes RFC5268)	Jul-09						O	O			

	RFC5844	IPv4 Support for Proxy Mobile IPv6	PROPOSED STANDARD	May-10					O	O		
	RFC5845	Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6	PROPOSED STANDARD	Jun-10					O	O		
	RFC5846	Binding Revocation for IPv6 Mobility	PROPOSED STANDARD	Jun-10					O	O		
	RFC5847	Heartbeat Mechanism for Proxy Mobile IPv6	PROPOSED STANDARD	Jun-10					O	O		
	RFC6097	Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6.	INFORMATIONAL	Feb-11					O	O		
	RFC6224	Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains.	INFORMATIONAL	Apr-11					O	O		
NEMO	RFC3963	Network Mobility (NEMO) Basic Support Protocol	PROPOSED STANDARD	Jan-05		*		*	O	O		
	RFC4908	Multi-homing for small scale fixed network Using Mobile IP and NEMO.	EXPERIMENTAL	Jun-07					O	O		
	RFC6089	Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support.	PROPOSED STANDARD (Updates RFC5648)	Jan-11					O	O		
Management												
SNMP	RFC1157	Simple Network Management Protocol (SNMP).	HISTORIC	May-90					O	O		
	RFC2578	Structure of Management Information Version 2 (SMIPv2)	STANDARD (Obsoletes RFC1902) (Also STD0058)	Apr-99		*			O+	O+		
	RFC2579	Textual Conventions for SMIPv2	STANDARD (Obsoletes RFC1903) (Also STD0058)	Apr-99		*			O+	O+		
	RFC2580	Conformance Statements for SMIPv2	STANDARD (Obsoletes RFC1904) (Also STD0058)	Apr-99		*			O+	O+		
	RFC3411	SNMP v3 Management Framework	STANDARD (Obsoletes RFC2571) (Updated by RFC5343) (Also STD0062)	Dec-02				*	O	O		
	RFC3412	SNMP Message Process and Dispatch	STANDARD (Obsoletes RFC2572) (Also STD0062)	Dec-02				*	O	O		
	RFC3413	SNMP Applications	STANDARD (Obsoletes RFC2573) (Also STD0062)	Dec-02				*	O	O		
	RFC3414	User-based Security Model for SNMPv3	STANDARD (Obsoletes RFC2574) (Also STD0062)	Dec-02				*	O	O		
	RFC3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).	STANDARD (Obsoletes RFC2575) (Also STD0062)	Dec-02					O	O		

	RFC3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).	STANDARD (Obsoletes RFC1905) (Also STD0062)	Dec-02		*			O+	O+		
	RFC3417	Transport Mappings for the Simple Network Management Protocol (SNMP).	STANDARD (Obsoletes RFC1906) (Updated by RFC4789, RFC5590) (Also STD0062)	Dec-02					O	O		
	RFC3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).	STANDARD (Obsoletes RFC1907) (Also STD0062)	Dec-02		*			O+	O+		
	RFC5343	Simple Network Management Protocol (SNMP) Context EngineID Discovery.	PROPOSED STANDARD (Updates RFC3411)	Sep-08					O	O		
MIBs	RFC2863	The Interfaces Group MIB.	DRAFT STANDARD (Obsoletes RFC2233)	Jun-00					O	O		
	RFC4022	Management Information Base for the Transmission Control Protocol (TCP).	PROPOSED STANDARD (Obsoletes RFC2452, RFC2012)	Mar-05			*		O	O		
	RFC4087	MIB for IP Tunnels	PROPOSED STANDARD (Obsoletes RFC2667)	Jun-05			*		O	O		
	RFC4113	Management Information Base for the User Datagram Protocol (UDP).	PROPOSED STANDARD (Obsoletes RFC2454, RFC2013)	Jun-05			*		O	O		
	RFC4292	IP Forwarding Table MIB.	PROPOSED STANDARD (Obsoletes RFC2096)	Apr-06			*		O	O		
	RFC4293	Management Information Base for the Internet Protocol (IP).	PROPOSED STANDARD (Obsoletes RFC2011, RFC2465, RFC2466)	Apr-06		*		*	O+	O+		
	RFC4295	Mobile IPv6 Management Information Base.	PROPOSED STANDARD	Apr-06				*	O	O		
	RFC4668	RADIUS Authentication Client MIB for IPv6.	PROPOSED STANDARD (Obsoletes RFC2618)	Aug-06					O	O		
	RFC4669	RADIUS Authentication Server MIB for IPv6.	PROPOSED STANDARD (Obsoletes RFC2619)	Aug-06					O	O		
	RFC4670	RADIUS Accounting Client MIB for IPv6.	INFORMATIONAL (Obsoletes RFC2620)	Aug-06					O	O		
	RFC4671	RADIUS Accounting Server MIB for IPv6.	INFORMATIONAL (Obsoletes RFC2621)	Aug-06					O	O		
	RFC4807	IPsec Security Policy Database Configuration MIB.	PROPOSED STANDARD	Mar-07				*	O	O		
	RFC4898	TCP Extended Statistics MIB.	PROPOSED STANDARD	May-07					O	O		
	RFC5060	Protocol Independent Multicast MIB.	PROPOSED STANDARD	Jan-08					O	O		
RFC5132	IP Multicast MIB.	PROPOSED STANDARD (Obsoletes RFC2932)	Dec-07					O	O			
RFC5240	Protocol Independent Multicast (PIM) Bootstrap Router MIB	PROPOSED STANDARD	Jun-08					O	O			

	RFC5324	MIB for Fibre-Channel Security Protocols (FC-SP)	PROPOSED STANDARD	Sep-08					O	O		
	RFC5519	Multicast Group Membership Discovery MIB.	PROPOSED STANDARD (Obsoletes RFC2933, RFC3019)	Apr-09					O	O		
	RFC5643	Management Information Base for OSPFv3	PROPOSED STANDARD	Oct-09					O	O		
Application												
DHCPv6	RFC3315	Dynamic Host Config Protocol (DHCPv6)	PROPOSED STANDARD (Updated by RFC4361)	Jul-03		*	*	*	O+	O+		
	RFC3319	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers.	PROPOSED STANDARD	Jul-03					O	O		
	RFC3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6.	PROPOSED STANDARD	Dec-03		*		*	O	O		
	RFC3646	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	PROPOSED STANDARD	Dec-03		*			O	O		
	RFC3736	Stateless DHCP Service for IPv6	PROPOSED STANDARD	Apr-04		*		*	O	O		
	RFC3898	Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	PROPOSED STANDARD	Oct-04					O	O		
	RFC4075	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6.	PROPOSED STANDARD	May-05					O	O		
	RFC4076	Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	INFORMATIONAL	May-05					O	O		
	RFC4242	Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	PROPOSED STANDARD	Nov-05					O	O		
	RFC4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4).	PROPOSED STANDARD (Updates RFC2131, RFC2132, RFC3315)	Feb-06				*	O	O		
	RFC4477	Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues.	INFORMATIONAL	May-06					O	O		
	RFC4580	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option.	PROPOSED STANDARD	Jun-06					O	O		
RFC4649	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option.	PROPOSED STANDARD	Aug-06					O	O			
RFC4994	DHCPv6 Relay Agent Echo Request Option.	PROPOSED STANDARD	Sep-07					O	O			

	<u>RFC5007</u>	DHCPv6 Leasequery	PROPOSED STANDARD	Sep-07						O	O		
	<u>RFC5460</u>	DHCPv6 Bulk Leasequery.	PROPOSED STANDARD	Feb-09						O	O		
	<u>RFC5678</u>	Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Options for IEEE 802.21 Mobility Services (MoS) Discovery.	PROPOSED STANDARD	Dec-09						O	O		
	<u>RFC5908</u>	Network Time Protocol (NTP) Server Option for DHCPv6	PROPOSED STANDARD	Jun-10						O	O		
	<u>RFC5970</u>	DHCPv6 Options for Network Boot	PROPOSED STANDARD	Sep-10						O	O		
	<u>RFC6153</u>	DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery.	PROPOSED STANDARD	Feb-11						O	O		
Sockets	<u>RFC3493</u>	Basic Socket Interface Extensions for IPv6.	INFORMATIONAL (Obsoletes RFC2553)	Feb-03				*		O+	O+		
	<u>RFC3542</u>	Advanced Sockets Application Program Interface (API) for IPv6.	INFORMATIONAL (Obsoletes RFC2292)	May-03				*		O	O		
	<u>RFC4584</u>	Extension to Sockets API for Mobile IPv6.	INFORMATIONAL	Jul-06				*		O	O		
	<u>RFC5014</u>	IPv6 Socket API for Source Address Selection.	INFORMATIONAL	Sep-07				*		O	O		
RADIUS	<u>RFC3162</u>	RADIUS and IPv6	PROPOSED STANDARD	Aug-01						O+	O+		
	<u>RFC4668</u>	RADIUS Authentication Client MIB for IPv6.	PROPOSED STANDARD (Obsoletes RFC2618)	Aug-06						O	O		
	<u>RFC4669</u>	RADIUS Authentication Server MIB for IPv6.	PROPOSED STANDARD (Obsoletes RFC2619)	Aug-06						O	O		
	<u>RFC4670</u>	RADIUS Accounting Client MIB for IPv6.	INFORMATIONAL (Obsoletes RFC2620)	Aug-06						O	O		
	<u>RFC4671</u>	RADIUS Accounting Server MIB for IPv6.	INFORMATIONAL (Obsoletes RFC2621)	Aug-06						O	O		
	<u>RFC4818</u>	RADIUS Delegated-IPv6-Prefix Attribute.	PROPOSED STANDARD	Apr-07						O	O		
	<u>RFC5176</u>	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	INFORMATIONAL (Obsoletes RFC3576)	Jan-08						O	O		
	<u>RFC5778</u>	Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction	PROPOSED STANDARD	Feb-10						O	O		
	<u>RFC5779</u>	Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server	PROPOSED STANDARD	Feb-10						O	O		
DNSv6	<u>RFC2874</u>	DNS Extensions to Support IPv6 Address Aggregation and Renumbering	EXPERIMENTAL (Updates RFC1886) (Updated by RFC3152, RFC3226, RFC3363, RFC3364)	Jul-00						O	O		

	RFC3363	Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS).	INFORMATIONAL (Updates RFC2673, RFC2874)	Aug-02					O	O		
	RFC3364	Tradeoffs in Domain Name System (DNS) Support for Internet Protocol version 6 (IPv6).	INFORMATIONAL (Updates RFC2673, RFC2874)	Aug-02					O	O		
	RFC3596	DNS Extensions to Support IP Version 6.	DRAFT STANDARD (Obsoletes RFC3152, RFC1886)	Oct-03			*	*	O+	O+		
	RFC3901	DNS IPv6 Transport Operational Guidelines	BCP0091	Sep-04					O	O		
	RFC4074	Common Misbehavior Against DNS Queries for IPv6 Addresses.	INFORMATIONAL	May-05					O	O		
	RFC4472	Operational Considerations and Issues with IPv6 DNS.	INFORMATIONAL	Apr-06					O	O		
	RFC5006	IPv6 Router Advertisement Option for DNS Configuration.	EXPERIMENTAL (Obsoleted by RFC6106)	Sep-07								
	RFC6106	IPv6 Router Advertisement Options for DNS Configuration	PROPOSED STANDARD (Obsoletes RFC5006)	Nov-10					O	O		
SIPv6	RFC2617	HTTP Authentication: Basic and Digest Access Authentication	DRAFT STANDARD (Obsoletes RFC2069)	Jun-99		*			O	O		
	RFC3261	SIP: Session Initiation Protocol	PROPOSED STANDARD (Obsoletes RFC2543) (Updated by RFC3265, RFC3853, RFC4320, RFC4916)	Jun-02		*			O+	O+		
	RFC3264	An Offer/Answer Model with Session Description Protocol	PROPOSED STANDARD (Obsoletes RFC2543)	Jun-02		*			O	O		
	RFC3665	SIP Basic Call Flow Examples	BCP0075	Dec-03		*			O	O		
	RFC4566	SDP: Session Description Protocol	PROPOSED STANDARD (Obsoletes RFC2327, RFC3266)	Jul-06		*			O	O		
	RFC5118	Session Initiation Protocol (SIP) Torture Test Messages for Internet Protocol Version 6 (IPv6)	INFORMATIONAL	Feb-08					O	O		
	RFC6157	IPv6 Transition in the Session Initiation Protocol (SIP).	PROPOSED STANDARD (Updates RFC3264)	Apr-11					O	O		
Others	RFC5101	Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information	PROPOSED STANDARD	Jan-08					O	O		
	RFC5321	Simple Mail Transfer Protocol	DRAFT STANDARD (Obsoletes RFC2821) (Updates RFC1123)	Oct-08					O	O		

RFC5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	PROPOSED STANDARD (Obsoletes RFC3768)	Mar-10							O		
RFC5855	Nameservers for IPv4 and IPv6 Reverse Zones	BEST CURRENT PRACTICE (Also BCP0155)	May-10						O	O		
RFC5881	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)	PROPOSED STANDARD	Jun-10						O	O		
RFC5905	Network Time Protocol Version 4: Protocol and Algorithms Specification.	PROPOSED STANDARD (Obsoletes RFC1305, RFC4330)	Jun-10						O	O		
RFC5986	Discovering the Local Location Information Server (LIS)	PROPOSED STANDARD	Sep-10						O	O		
RFC6059	Simple Procedures for Detecting Network Attachment in IPv6	PROPOSED STANDARD	Nov-10						O	O		

Routing

RFC1772	BGP Application in the Internet	DRAFT STANDARD (Obsoletes RFC1655)	Mar-95				*			O		
RFC2080	RIPng for IPv6.	PROPOSED STANDARD	Jan-97							O+		
RFC2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	PROPOSED STANDARD	Mar-97				*			O+		
RFC2894	Router Renumbering for IPv6	PROPOSED STANDARD	Aug-00							O		
RFC4271	A Border Gateway Protocol 4 (BGP-4)	DRAFT STANDARD (Obsoletes RFC1771)	Jan-06				*			O+		
RFC4552	Authentication/Confidentiality for OSPFv3	PROPOSED STANDARD	Jun-06				*			O		
RFC4760	Multiprotocol Extensions for BGP-4.	DRAFT STANDARD (Obsoletes RFC2858)	Jan-07				*			O+		
RFC4798	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE).	PROPOSED STANDARD	Feb-07							O		
RFC5120	M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)	PROPOSED STANDARD	Feb-08							O		
RFC5185	OSPF Multi-Area Adjacency	PROPOSED STANDARD	May-08							O		
RFC5187	OSPFv3 Graceful Restart.	PROPOSED STANDARD	Jun-08							O		
RFC5243	OSPF Database Exchange Summary List Optimization.	INFORMATIONAL	May-08							O		
RFC5308	Routing IPv6 with IS-IS.	PROPOSED STANDARD	Oct-08							O		
RFC5329	Traffic Engineering Extensions to OSPF Version 3.	PROPOSED STANDARD	Sep-08							O		
RFC5340	OSPF for IPv6	PROPOSED STANDARD (Obsoletes RFC2740)	Jul-08				*			O+		
RFC5838	Support of Address Families in OSPFv3	PROPOSED STANDARD	Apr-10							O		

	RFC6146	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers.	PROPOSED STANDARD	Apr-11					O	O		
	RFC6147	DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers.	PROPOSED STANDARD	Apr-11					O	O		
	RFC6156	Traversal Using Relays around NAT (TURN) Extension for IPv6.	PROPOSED STANDARD	Apr-11					O	O		
Multicast												
Multicasting	RFC2710	Multicast Listener Discovery (MLD) for IPv6	PROPOSED STANDARD (Updated by RFC3590, RFC3810)	Oct-99					O	O		
	RFC2711	IPv6 Router Alert Option	PROPOSED STANDARD	Oct-99			*		O	O		
	RFC3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol.	PROPOSED STANDARD (Updates RFC2710)	Sep-03					O	O		
	RFC3810	MLD Version 2 for IPv6	PROPOSED STANDARD (Updates RFC2710) (Updated by FC4604)	Jun-04		*		*	O+	O+		
	RFC4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches.	INFORMATIONAL	May-06					O	O		
	RFC4601	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised).	PROPOSED STANDARD (Obsoletes RFC2362) (Updated by RFC5059)	Aug-06				*		O		
	RFC4602	Protocol Independent Multicast - Sparse Mode (PIM-SM) IETF Proposed Standard Requirements Analysis.	INFORMATIONAL	Aug-06						O		
	RFC4604	Using MLDv2 for Source Specific Multicast (SSM)	PROPOSED STANDARD (Updates RFC3376, RFC3810)	Aug-06		*		*	O+	O+		
	RFC4605	Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying").	PROPOSED STANDARD	Aug-06					O	O		
	RFC4607	Source-Specific Multicast for IP.	PROPOSED STANDARD	Aug-06				*	O	O		
	RFC4609	Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements.	INFORMATIONAL	Oct-06				*		O		
	RFC4610	Anycast-RP Using Protocol Independent Multicast (PIM).	PROPOSED STANDARD	Aug-06						O		
RFC5059	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM).	PROPOSED STANDARD (Obsoletes RFC2362)	Jan-08						O			

		(Updates RFC4601)									
RFC5110	Overview of the Internet Multicast Routing Architecture	INFORMATIONAL	Jan-08						O		
RFC5186	Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction.	INFORMATIONAL	May-06					O	O		
RFC5796	Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages.	PROPOSED STANDARD (Updates RFC4601)	Mar-10						O		
RFC6085	Address Mapping of IPv6 Multicast Packets on Ethernet.	PROPOSED STANDARD (Updates RFC2464)	Jan-11					O	O		
RFC6224	Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 (PMIPv6) Domains.	INFORMATIONAL	Apr-11						O		