政府網路及 e 政府網站
導入 IPv6 參考要點

新一代網際網路協定互通認證計畫
主持人：曾憲雄 博士
執行單位：財團法人台灣網路資訊中心
中華民國九十九年十月

1. 前言(Introduction)

本文件參考 IETF 國際標準[9]、IPv6 Forum IPv6 Ready Logo Program[2]、NIST 文件 A Profile for IPv6 in the U.S. Government[10]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，不在本文討論之範圍，文件將依據 IPv6 Ready Logo Program[2]之測試規範書不定期修正，期望提供更精確之資料。

本文後續章節將包含範圍、參考文件、IPv6 設備型態、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. 範圍(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. 參考文件(References)

[1]. IPv6 Forum, http://www.ipv6forum.org/

[2]. IPv6 Ready Logo Program, http://www.ipv6ready.org/, May 2007.

[3]. 台灣獲得 IPv6 Ready Logo 標章一覽表, http://interop.ipv6.org.tw/TaiwanIPv6ReadyLogoList.htm

[4]. 日本 TAHI 測試組織, http://www.tahi.org/

[5]. 美國 UNH IOL, http://www.iol.unh.edu/consortiums/ipv6/

[6]. 台灣 IPv6 標準測試實驗室, http://interop.ipv6.org.tw/

[7]. 韓國 TTA, http://www.tta.or.kr/English/new/main/index.htm

[8]. 北京 BII, http://www.biigroup.com/

[9]. The Internet Engineering Task Force, http://www.ietf.org/

[10]. A Profile for IPv6 in the U.S. Government – Version 1.0,

九十九年度「新一代網際網路協定互通認證計畫」

政府網路導入IPv6參考要點

壹、前言

截至 2010 年 10 月底全球位址管理機構 IANA(Internet Assigned Numbers Authority)保留而能分配使用的 IPv4 位址數量只剩 12 個 Class A(一個 Class A 等於 2^{24} 個位址)，不到總數的 5%。國際預期 IANA 的 IPv4 位址將於 2011 年中發放殆盡，接著亞太區網路資訊中心 APNIC 的 IPv4 位址將於 2012 年初消耗完畢，屆時台灣將進入位址枯竭時期，無法再獲得新的 IPv4 位址。為解決位址枯竭問題，並充分支援物件聯網需求，具有 128 位元位址的 IPv6 網路協定是唯一能徹底解決問題的方案，目前全世界的 IPv6 網路已快速發展中。為提供我國發展需求，也因應全球 IPv6 網路接軌的需要，各界都應及早佈局導入 IPv6。

推動 IPv6 的困難是 IPv6 與 IPv4 不相容，推動 IPv6 不是一件簡單的工作。目前全世界主要採用的方案是將既有網路升級為 IPv4/IPv6 雙協定網路，其做法是經由重新採購設備或進行韌體更版來升級網路設備，網站及網路應用程式則需要修改程式碼或調整系統設定，用戶端的部份相對簡單，大部分用戶的電腦作業系統已經支援雙協定。

貳、政府網路導入 IPv6 的理由

政府應有執行與領導 IPv6 建設的責任，政府部門的 IPv6 導入是整體 IPv6 發展的重要推力：

- 網際網路已深度影響國家經濟與民生社會的運作，持續維持網路的積極發展為政府的重大責任。
- 推動 IPv6 的建設對網路服務的發展與連續性至關重要，也是國家資訊網路實力是否繼續領先國際的重要關鍵。
- 基於 IPv6 網路未能立即創造商機，民營業界發展速度較慢，需要政府帶頭示範，宣示推動 IPv6 的決心，以加速整體的發展。
- 藉由政府網路及電子化政府網站服務導入 IPv6，將引導我國設備廠商、網路內容開發商及系統整合服務商早日投入相關產品及服務的研發與生產。
- 國際上已快速佈建及提供 IPv6 服務，我國政府單位及網站服務將面臨與 IPv6 用戶及 IPv6 服務連接互通的需求，須早日發展 IPv6，未雨綢繆。
- 網路相關設備均有一定之使用年限，如未把 IPv6 納入規格需求，汰舊換新之設備如不具 IPv6 功能，短期內將面臨重複投資的損失。

參、政府組織改造與資訊改造的機會

全球號碼資源組織（Number Resource Organization, NRO）主席 Axel Pawlik 呼籲所有網際網路相關產業必須立即推動及使用 IPv6，在 NRO 建議的行動綱領中，政府組織應該做的是扮演帶頭的角色，使政府網路的內容和服務可支援 IPv6，立即將 IPv6 的需求規格納入政府採購政策，乃是非常重要的關鍵。

政府組織即將改造精簡為 29 部會，並預定於民國 101 年啟動新架構，政府資訊組織未來將以「部」為資訊整合單位，組織改造後的行政院及各部會資訊組織，將統整各所屬機關成為集中式的資訊架構，新的資訊服務架構將帶動資訊系統朝大型化及集中化調整。另外，五都合併升格改制也將於民國 99 年底正式生效，許多相關資訊網路系統需要配合調整。

配合組織改造及五都升格，政府資訊網路及相關系統勢必進行規模不小的調整，趁此時機將 IPv6 網路支援納為資訊設備採購的必備規格將是重要的事情。配合資訊設備的汰舊換新、系統擴充及新系統建置，順勢導入 IPv6，是解決 IPv4 位址不足最經濟有效的方法。未來不管是配合組織調整或是推動各項數位化公共工程，政府部門採購網通設備都應將 IPv6 功能列為必要項目，資訊系統及 e 政府網站重整時，也應同步納入支援 IPv6 的考量。

肆、政府網路導入 IPv6 建議

目前全世界網路發展先進國家無不積極發展及佈建 IPv6 網路，美國聯邦政府已規定自 2010 年 7 月起美國政府各部門採購網路產品都必須符合 IPv6 支援標準 (US Government IPv6 Profile, USGv6)。美國電信暨資訊管理局於 2010 年 9 月 28 日公佈最新的 IPv6 發展策略，內容包括：

- 所有美國政府部門必須在 2012 年 9 月 30 日前將提供公眾使用的電子政府網站/電子郵件主機/網域名稱伺服器全部導入 IPv6 服務。
- 所有的美國政府部門必須在 2014 年 9 月 30 日前將所有內部網路移轉為純 IPv6 網路。
- 所有的美國政府部門必須立即指派一位負責執行 IPv6 移轉的主管。
- 所有美國政府部門新採購的資通訊設備必須符合 USGv6 的規範。

我國政府可參考美國做法，並配合政府資訊改造計畫的時程，制定我國政府網路導入 IPv6 綱要計畫，相關建議如下：

一、建議政府網路與政府網站帶頭導入 IPv6 以引導我國各界加速向 IPv6 移轉

世界各國大多優先推動政府網路向 IPv6 移轉，以作為整體 IPv6 發展的重要推力，政府網路向 IPv6 移轉可以帶動 IPv6 設備產業的發展，電子化政府網站的 IPv6 化則可以擴大 IPv6 內容服務的利用，創造 ISP 發展 IPv6 的誘因，並帶動民營 ICP 起而效尤。建議政府網路與政府網站帶頭導入 IPv6 以引導我國各界加速向 IPv6 移轉。

二、建議我國政府訂定並宣示電子化政府網站與政府網路導入 IPv6 時程表

建議參照美國政府時程，訂定並宣示我國政府網路導入 IPv6 時程表。其建議時程為 2012 年 12 月 31 日前依序完成中央政府網站導入 IPv4/IPv6 雙協定及地方政府網站導入 IPv4/IPv6 雙協定；並於 2014 年 12 月 31 日前依序完成中央政府內部網路導入 IPv4/IPv6 雙協定及地方政府內部網路導入 IPv4/IPv6 雙協定，各級政府單位應指定負責推動 IPv6 移轉的主管。

三、建議資訊、電腦及網路等資通訊設備應納入支援 IPv6 規格

建議我國政府參考美國 USGv6 的做法，訂定政府單位採購 IPv6 資通設備規範。在尚未制定規範之前，建議要求各公部門單位於資通設備汰舊換新時，應優先採購符合 IPv6 認證產品，包括 IPv6 Ready Logo 認證產品、DoD(美國國防部) IPv6 認證產品及 USGv6 認證產品。另外建議在台灣銀行中信局承辦之共同供應契約內，於資通設備清單增加 IPv6 專章，納入符合 IPv6 認證的設備，以供採購人員參考。

四、建議推動全面性之政府資訊人員 IPv6 技術教育訓練

IPv6 人才培訓是推動 IPv6 的關鍵工作之一，所有負責網路規劃、網路管理及軟體開發的資訊人員都迫切需要 IPv6 技術之養成訓練。建議行政院研究發展考核委員立即規劃通盤的政府資訊人員 IPv6 教育訓練，所有資訊人員應具備足夠的 IPv6 知識，財團法人台灣網路資訊中心及新一代網際網路協定認證計畫執行單位可以協助舉辦 IPv6 技術訓練課程。

五、建議網通相關之國家型計畫及政府研發案應立即納入支援 IPv6

建議檢討目前執行中或即將立案之網通相關國家型計畫，其網路通訊系統或作業平台應加入支援 IPv6 的規範。由各級政府部門或國營事業主導之資通訊系統研發案也應立即評估納入支援 IPv6 通訊協定，例如智慧感測、智慧電網等物聯網領域的計畫。另外如各單位適逢系統軟體開發或修改的需求，應納入對 IPv6 的支援，例如使用網域名稱取代網路位址，並使用支援 IPv6 的函數。

伍、政府各級機關導入 IPv6 參考要點

一、規劃 IPv6 導入方案

(一) 成立移轉工作小組，確認 IPv6 需求(含應用服務與建置範圍)，進行導入 IPv6 之規劃，詳細規劃方法可參考附錄二「RFFC 4057(中譯)」。

(二) 盤點網路設備及應用軟體，列出尚未支援 IPv6 的項目。

(三) 評估替換之硬體設備型號、應用軟體版本，規劃經費需求。

(四) 規劃 IPv6 位址分配原則，建議 GSN 以/48 網段配發各級政府單位 IPv6 位址，單位內如有規劃子網路需求，建議以/56 網段規劃子網路。

(五) 建議重新申請 IPv4/IPv6 雙協定線路，待各項網路應用轉移至雙協定線路，並提供穩定之服務，再廢除舊有 IPv4 線路，以完成平穩無縫之移轉。

(六) 撰寫導入 IPv6 作業計畫書，包括作業程序，參數設定腳本，服務中斷評估，異常撤退方案等。

二、執行 IPv6 導入方案

(一) 盤點既有軟硬體設備，評估支援 IPv6 的能力。大部分伺服器可直接支援 IPv6，部份路由器可藉由作業系統升級支援 IPv4/IPv6 雙協定。若舊有路由器無法升級或效能不足，則須採購新的路由器或增購新的模組界面。

(二) 進行 IPv4/IPv6 雙協定電路採購、施工安裝及連接至網路路由器，並調整及設定 IPv6 機房網路環境。

(三) 調整設定資安防火牆、代理伺服器、反向代理伺服器及負載平衡裝置(以上為依需要選用的設備)等網路設備，以支援 IPv4/IPv6 雙協定的需求。

(四) WWW /DNS/Email 伺服器作業系統升級或調整設定導入 IPv4/IPv6 雙協定，WWW 網頁內容及網路應用程式碼修改導入 IPv4/IPv6 雙協定。

(五) 調整內部網路架構與設定，導入 IPv4/IPv6 雙協定。

(六) 各項調整或建置工作，逐步進行功能測試，驗證原 IPv4 網路及 IPv6 網路之功能及品質符合原先之規劃。

三、撰寫系統建置報告

(一) 系統建置階段應逐步記錄 IPv6 環境參數、網路架構、問題排除等資料。

(二) 系統建置完畢應撰寫完工報告，詳細記載網路接線及系統設定等資料，作為後續系統維護參考資料。

陸、電子化政府網站及應用程式導入 IPv6 參考要點

一、作業系統建議採用 Linux 2.6.15(含)以上版本、FreeBSD Ver. 4.0(含)以上版本或 Windows server 2003(含)以上版本，以支援 IPv6 (參考附錄二表 3)。

二、申請及安裝 IPv6 線路或 IPv4/IPv6 雙協定線路，GSN 政府網際服務網在國內主要都會區已可以供裝 IPv6 線路或提供具備 IPv6 環境之資訊代管機房。

三、設定 DNS 支援 IPv6，包括設定 AAAA 記錄及設定 IPv6 位址反向查詢區域。

四、修改網頁相關程式碼，將不支援 IPv6 的函數及資料結構修改為同時支援 IPv4 及 IPv6。

五、應用程式盡量使用 Domain Name 的連結位址，減少 IP 位址的使用，但須考量到 DNS Server 的穩定性。

六、網頁程式修改要點如下：

(一) Html

HTML 語言裡的超連結位址，如果是以傳統 IPv4 的 IP 位址為連結，則必須改為 Domain Name 的連結位址。

(二) PHP

連結位址需將傳統 IPv4 之 IP 位址改成 Domain Name 的形式，在 PHP 程式設計中，網路存取獲得使用者(Client)之 IP 位址之函式語法如下，本函式同時支援 IPv4 及 IPv6：

```
$_SERVER['REMOTE_ADDR']
```

(三) ASP

ASP 程式語言取得客戶端的 IP 位址的方法可以使用下列語法取得客戶端的 IP 位址，本函式同時支援 IPv4 及 IPv6：

```
<%=Request.ServerVariables("REMOTE_ADDR")%>。
```

(四) ASP.NET

ASP.NET 程式語言取得客戶端的 IP 位址的方法可以類似下面語法來取得，本函式同時支援 IPv4 及 IPv6：

```
Your IP Address :<% Response.Write(Request.UserHostAddress)%>。
```

(五) JSP

JSP 程式語言取得客戶端的 IP 位址的方法可以使用下列語法取得客戶端的 IP 位址，本函式同時支援 IPv4 及 IPv6：

```
RemoteAddr: <%=request.getRemoteAddr()%>
<br>
RemoteHost: <%=request.getRemoteHost()%>
```

(六) 避免使用只支援 IPv4 程式碼。

1. 位址轉換功能應使用 inet_ntop()與 inet_pton()，可同時支援 IPv4/IPv6。
2. 主機名稱和 IP 位址解析應使用 getaddrinfo() 及 getnameinfo() 位址解析函數，避免使用 gethostbyname()、gethostbyaddr()、getservbyname()及 getservbyport()。
3. 發展與 IP 版本無關的程式碼，所有資料結構及 APIs 應該和 IP 版本無關，例如使用 Independent Structures 時應盡量避免使用 structs_in_addr, in6_addr, sockaddr_in, sockaddr_in6。

(七) 微軟工具(checkv4.exe)可檢查 IPv4 相關函數及參數，並提供相對應的 IPv6 函式。但是無法檢查 IP 位址相關的程式碼 (例如 IPv4 數字位址)。

七、SQL Server 已支援 IPv6 及 IPv4 兩種協定的連線。當 Windows 設定為 IPv6 SQL Server 時，元件會自動辨識，不需要特別的 SQL Server 組態。

八、在 IPv4 使用 Broadcast 的地方，在 IPv6 要改使用 Multicast。

九、注意 IPv6 的通則，例如最小的 IPv6 子網路遮罩通常為/64，IPv6 路由會通常會優於 IPv4 先被使用。

柒、IPv6 設備採購規範建議

國際大廠之設備大都已經通過 IPv6 Ready Logo 認證，我國資通信廠商設備也大都具備 IPv6 能力，將 IPv6 功能列入設備需求規範中，不必擔心無法獲得適當之設備，且應善用國際 IPv6 Ready Logo 標章，以降低採購人員撰寫設備規格書負擔，以及後續驗收之專業測試成本，詳細規範書請參考附錄二「IPv6 資通信設備功能需求規範建議書_V3.0」。

一、IPv6 主機 (Host) 設備應支援之規範建議如下：

(一) 必要項目：必須通過 IPv6 Ready Logo Phase-2 Core for Host 的測試規範。

(二) 安全選項：IPv6 Ready Logo Phase-2 IPSec for End-Node 的測試規範。

(三) 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。

(四) 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，可待市場設備普遍成熟時再納入考慮。

(五) DNS 選項：建議需支援 RFC 3596 DNS Extensions to Support IP Version 6。

(六) DHCPv6 選項：IPv6 Ready Logo Phase-2 DHCPv6 for Client，建議需支援 Client 模式，相關標準為 RFC 3315 Dynamic Host Config Protocol (DHCPv6)。

(七) 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。(目前大部分作業系統皆已經支援 IPv6)。

表一 IPv6 主機建議規範

編號	項目	規範建議
IPv6 主機 (Host) 必要規格		
1	核心項目	IPv6 Ready Logo Phase-2 Core for Host
IPv6 主機 (Host) 選項規格		
2	安全選項	IPv6 Ready Logo Phase-2 IPSec for End-Node
3	網管選項	IPv6 Ready Logo Phase-2 SNMP for Agent (以 SNMPv 2c 和 RFC 4293 IP MIB 為參考標準)
4	移動性選項	IPv6 Ready Logo Phase-2 Mobility for Mobile Node 或 Correspondent Node
5	DNS 選項	RFC 3596
6	DHCPv6 選項	IPv6 Ready Logo Phase-2 DHCPv6 for Client (支援 Client 模式，標準為 RFC 3315)
7	應用程式選項	SIP：IPv6 Ready Logo Phase-2 SIPv6 for User Agent Email、Web 及其他應用程式：必須同時支援 IPv4/IPv6 通訊協定

備註：選項項目請依據主機功能需求選列。

二、IPv6 路由器 (Router) 應支援之規範建議如下：

(一) 必要項目：必須通過 IPv6 Ready Logo Phase-2 Core for Router 測試規範。

(二) 安全選項： IPv6 Ready Logo Phase-2 IPSec for Secure Gateway 測試規範。

(三) 網管選項：IPv6 Ready Logo Phase-2 SNMP for Agent 的測試規範。建議以 SNMPv 2c 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。

(四) 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，可待市場設備普遍成熟時再納入考慮。

(五) DNS 選項：建議需支援 RFC 3596 DNS Extensions to Support IP Version 6。

(六) 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 RFC 3315 Dynamic Host Config Protocol (DHCPv6)。

(七) 路由選項：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 (RFC 2080)，而大容量 Router 建議需支援 OSPFv3 (RFC 5340)和 BGP-4 + (RFC 2545、RFC 4271)。

表二 IPv6 路由器建議規範

編號	項目	規範建議
IPv6 路由器 (Router) 必要規格		
1	基本項目	IPv6 Ready Logo Phase-2 Core for Router
IPv6 路由器 (Router) 選項規格		
2	安全選項	IPv6 Ready Logo Phase-2 IPSec for Secure Gateway
3	網管選項	IPv6 Ready Logo Phase-2 SNMP for Agent (以 SNMPv 2c 和 RFC 4293 IP MIB 為參考標準)
4	移動性選項	IPv6 Ready Logo Phase-2 Mobility for Home Agent
5	DNS 選項	RFC 3596
6	DHCPv6 選項	IPv6 Ready Logo Phase-2 DHCPv6 for Server (支援 Server 或 Relay Agent 模式，標準為 RFC 3315)
7	路由選項	根據路由器之容量及使用地點，決定適當通訊協定 SOHO Router：支援 RIPNG (RFC 2080) 大容量 Router：支援 OSPFv3 (RFC 5340)和 BGP-4+ (RFC 2545、RFC 4271)

備註：選項項目請依據主機功能需求選列。

三、其他建議如下：

(一) 有關 IPv6 網路保護設備規範，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。

(二) 目前 IPv6 Ready Logo Phase-2 無特殊設備定義，建議 IPv6 特殊設備需通過 IPv6 Ready Logo Phase-1 Special Device 的測試規範。

(三) 雖然第二層交換器 (Layer 2 Switch) 和 IP 層的運作理應無關，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)。

(四) 為了網路管理和服務供裝的需求，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。

附錄一、RFC 4057 (中譯)

目前在國際上 IPv6 已經從一門研究變成一項工作，一項不能不做的工作。除了技術上的創新與服務運用外，IETF 也討論出了許多轉移的建議，以下是根據 RFC4057 內容所提供的企業轉移建議，希望讀者可以依據此文件規畫自己公司的轉移方式。

這份建議文件描述 IPv6 在導入企業網路的解決方案，讀者可以根據這份文件再去定義各公司細部的 IPv6 導入計畫.在運用這份建議書規劃前，企業資訊管理單位需要先訂出 IPv4 與 IPv6 網路並存的期限，包含透過網路的各項商業應用服務和基本的 IPv6 基礎網路硬體建設時間。藉由本建議書的指引搭配國內相關 IPv6 實際佈署的資料與技術法人單位協助，相信每一個企業都能夠無痛轉移至 IPv6 的新世界。

1. 簡介

目前在國際上 IPv6 已經從一門研究變成一項工作，一項不能不做的工作。除了技術上的創新與服務運用外，IETF 也討論出了許多轉移的建議，以下是根據 RFC4057 內容所提供的企業轉移建議，希望讀者可以依據此文件規畫自己公司的轉移方式。

這份建議文件描述 IPv6 在導入企業網路的解決方案，讀者可以根據這份文件再去定義各公司細部的 IPv6 導入計畫.在運用這份建議書規劃前，企業資訊管理單位需要先訂出 IPv4 與 IPv6 網路並存的期限，包含透過網路的各項商業應用服務和基本的 IPv6 基礎網路硬體建設時間。藉由本建議書的指引搭配國內相關 IPv6 實際佈署的資料與技術法人單位協助，相信每一個企業都能夠無痛轉移至 IPv6 的新世界。從管理階層、網管人員和工程師都可以透過這份文件對企業將決定要使用 IPv6 之過度策略會有一定的了解，進而可以彼此協調如何無痛轉移甚至運用 IPv6 的優勢提供 multicast 服務。

以下描述三個基本的方案用來當作轉移範例，藉此提供明確的參考。

第一個方案假設企業決定要導入 IPv6 於現有的 IPv4 網路中。
第二個方案假設企業決定要因為某個特殊的 IPv6 應用服務所以需要取得 IPv6 連線。
第三個方案是假設企業在導入 IPv6 的同時建一個新的網路並與 IPv4 舊有節點共存。

本建議書中將討論以上 3 個明確的方案網路建構範例，所需要的網路節點元件及企業導入 IPv6 所需面對的挑戰也將會一起討論。在之入的支前管理部門需要討論在轉移的過程中如何確保原有 IPv4 的服務能夠繼續被使用，在 IPv6 網路運作後不同協定的服務轉換共通。相關的問題都會在本建議書中被討論或是找到解決的方向。但請注意一點，沒有一個解決方案能夠完整的提供一個企業進行轉移，細部的轉換、公司特有的服務與制度都需要在實際制定轉移計畫中考量。

2. 專有名詞

企業網路(Enterprise Network)

一個企業內的網路，可能是一個路由器或由多個路由器所組成的跨國網路。公司可以完全掌握內部的硬體與聯線。

網路連線服務提供商(Provider)
企業網路連接網際網路時所選擇的網路服務連線廠商，例如中華電信、亞太線上等。

具有 IPv6 連線能力
這裡指的具有 IPv6 連線能力代表了節點或網路可以同時支援 IPv4 與 IPv6 進行連線。

只具有 IPv4 連線能力
代表節點或網路只支援 IPv4 連線。

只具有 IPv6 連線能力
代表節點或網路只支援 IPv6 連線。

3. 基本轉移規畫

雖然各企業的需求不盡相同但還是可以粗分為三大類，根據這三大類網路的需求我們制定了三個基礎的轉移建議方案。特別要注意的是，在這三個基本方案中的 IPv6 網路節點都具有 IPv4/IPv6 的連線能力(現實的情況也是類似，大多數的作業系統都同時支援兩個協定)。

3.1 轉移基本方案的定義

・情境一
企業希望導入 dual-stack 雙協定於企業網路中，IPv6 與 IPv4 所包含的網路連線範圍與硬體架構將完全相同。

・假設
IPv4 與 IPv6 所使用的網路硬體架構相同。
・需求
在使用同樣網路硬體架構下，你需要了解到 IPv6 絕對會比表現的比 IPv4 好或是相同。IPv6 具有更好的安全性與多點傳遞功能，但是千萬不要假設硬體架構上的問題也能夠被解決。如果是 Layer2 的安全問題就不是 IPv6 所能夠解決的了。同時你必須要了解 IPv6 雖然架構簡單，但單位過去是否有存在 NAT 或是老舊的路由器，所以單純的更換企業入口路由器並不能馬上提供整個企業每一個角落 Ipv6 連線能力。

・情境二
企業針對某些特定的 IPv6 服務希望導入 IPv6 網路於某些企業內的區域。IT 部門所要負責的任務是提供有需要的單位 dual-stack 服務。

・假設
要確認所使用的新運用支援 IPv4/IPv6 的連線服務。而預定提供這項服務的相關軟硬體平台也需要支援 IPv6。

・需求

不需要影響到現有的 IPv4 網路。

・情境三

企業內具有只有 IPv6 連線能力的網路與部分 IPv4 連線能力的節點。這狀況發生在企業往往希望降低網路複雜度，所以會將網路盡量轉移到單一協定。當企業轉移至 IPv6 時，我們就需要設法讓原有 IPv4 的網路節點或服務能夠正常的運作

・假設

需要有效的 IPv6 網路架構，或是有效的透過定義一些時間表，支企業轉移畫

・需求

需要和思考舊有 IPv4 網路架構與節點如何透過 IPv6 網路互相連結，並與 IPv6 應用服務連接。

3.2. 轉移前需要確認的重要資訊

在著手改變整個網路導入 IPv6 之前，企業必須分析以下資訊確定轉移至 IPv6 網路之具體構想，以下數據將影響整個 IPv6 的導入計畫。

針對網路連線服務提供商需要討論

- IPv6 網路是否聯外
- 企業網路是單一區域或是分散在不同的地理位置上？
- 專用專線或是 VPN？
- 如果是不同區域的企業網路，要如何確保各分公司資訊交換的安全？
- 有多少個 IPv4 實體 IP 可供企業使用？
- 網路連線提供商有哪些 IPv6 的地址分配計劃可供選擇？
- 企業所需的 IPv6 遮罩長度(Prefix)與 IPv6 位址數量？
- 網路連線提供商是否會提供任何 IPv6 服務？
- 連接外部 IPv6 網路該採舉哪種路由協定？
- 公司的伺服器是否放在外部的網路服務提供商機房中？
- IPv6 是否使用與 IPv4 相同的連線線路去連接網際網路？

針對企業運用服務需要討論

- 目前有哪些服務正在企業內使用中？
- 有哪些應用服務需第一優先支援 IPv6？
- 哪些應用服務可升級到 IPv6？
- 應用服務是否要同時支援 IPv4 和 IPv6？
- 企業軟硬體平台是否可以同時支援 IPv4 和 IPv6？
- 應用服務是否可以採用 NAT v4-v4 和 NAT v4-v6 進行轉換？
- 應用服務是否需要可以連上網際網路之實體 IP 位置？
- 應用服務採用 IPv4 和 IPv6 是否會有不同？
- 應用服務是否僅針對公司內部企業網路的使用者？

針對企業內資訊管理部門需要討論

- 管理網路的是自己公司的 IT 部門或是外包？
- 是否要支援遠端 VPN 連線？
- 是否需要跨分公司之間的連線？
- 是否需要支援網路行動性議題？(network mobility or NEMO)?
- IPv6 位址的規畫？
- 是否有詳細的資產管理資料庫，包含主機 IP/MAC 位址？
- 是否有企業內 IPv6 位址的分配流程
- 內部網路是否有執行 IPv6 路由協定的需求？
- 是否制訂了 IPv6 網路管理方針/程序？
- 是否制訂了 IPv6 網路品質管理方針/程序？
- 是否制訂了 IPv6 網路安全方針/程序？
- 是否有規劃企業內部的 IPv6 的教育訓練？
- 哪些運作中的服務或系統對於導入 IPv6 會有影響？
  - DNS 區域名稱伺服機
  - Management 管理軟體(SNMP tools)
  - Enterprise Network Servers Applications 企業網路服務應用
  - Mail Servers 郵件伺服器
  - High Availability Software for Nodes 節點可用性 高的軟體
  - Directory Services 目錄服務
- 是否所有的軟體或服務功能可升級到 IPv6？
- 如果沒有升級，有什麼可以替代？
- IPv6 對相關網路的硬體的影響？
  - Routers/switches 路由器/交換器
  - Printers/Faxes 印表機/傳真機
  - Firewalls 防火牆
  - Intrusion Detection 入侵偵測
  - Load balancers 負載平衡器
  - VPN Points of Entry/Exit 虛擬私有網路的進出
  - Security Servers and Services 保護網路安全的伺服器和服務
  - Network Storage Devices 網路儲存裝址裝置
- 是否這些硬體都可升級到可支援 IPv6？
- 如果沒有，有哪接替代方案

針對企業網路管理系統需要討論

- 網路管理應用需求？
- 安全性的管理需求
- 協定轉換軟硬體和管理的機制？
- 導入 IPv6 會有哪些新的管理需要？

針對 B2B 系統需要討論

- 哪些軟硬體平台需要升級支援 IPv6？
- 哪些網路站台入口和出口點是需要 IPv6？
- 哪些協定轉換機制需要導入以支援 IPv6？

- 有什麼方針/程序是需要支援 IPv6 轉換？
- 有什麼方針/程序是需要支援現存的 IPv4 節點和應用，使其互相運作

3.3. 實際上的規畫範例

以下將介紹三個實際上的轉移規畫範例，各位讀者可以參考 3.1、3.2、3.3 完成自己的轉移範例。藉由此舉可以找出自己企業網路對於 IPv6 導入所需要討論的議題。

範例網路 A

有著不同獨立區域分公司網路的大型企業網路系統

- 採用專線連接不同分公司的網路。
- 網路連線服務提供商提供 IPv4 地址。
- 網路連線提供商沒有提供 IPv6 服務。
- 網路連線提供商沒有提供私人租用線路服務
- 目前企業提供的服務
  - Internal Web/Mail.內部網路/郵件
  - File servers.檔案服務
  - Java applications.Java 服務
  - Collaborative development tools.合作發展工具
  - Enterprise Resource applications.企業資源應用服務
  - Multimedia applications.多媒體應用
  - Financial Enterprise applications.金融企業應用
  - Data Warehousing applications.資料倉儲應應用
  - Internal network operation:內部網路運作
  - In house operation of the network.在內部運作的網路
  - DHCP (v4)可用於一般使用者電腦;伺服器配置固定的網路位址
- 網路管理使用 SNMP
- 所有的路由器和交換器都可以升級到支援 IPv6。
- 現有的防火牆可以升級到支援 IPv6 的規則。
- 負載平衡器不支持 IPv6，同時升級途徑尚不清楚。
- IPv4 的私有地址空間是用來在企業內部。

範例網路 B

銀行使用大規模的跨國網路，支援線上轉換程序跨越多個網站與驗證管理，最終進入一個中央資料庫進行相關業務。

- 不需要外部連結
- 使用 VPN 連結各網站
- IPv4 私人地址空間與 NAT
- 網路連接到私密的交易中心
- 企業內所使用之應用
  - ATM transaction application.ATM 轉換應用
  - ATM management application.ATM 管理應用
  - Financial Software and Database.金融軟體和資料庫
- 部分工作站是會移動的，同時有從外部網路存取企業網路的需求

- 現存的防火牆可以升級支援 IPv6
- 負載平衡器不支持 IPv6，同時升級途徑尚不清楚。
- 需要識別和管理每個節點的 IP 地址與身分。

範例網路 C

一個安全防禦單位、緊急服務或是其他非常重要單位的網路

- 網路具有獨立的實體網路線路。
- 網路必須要能夠透過 AD Hoc 多點跳躍網路連結不同的子網路。
- 整個網路有移動的需求。
- 所有在網路內的節點也支援移動支援。
- 網路必須維持高可用性
- 網路需要管理由 Ad-hoc 網路連入之節點。
- 所有節點必需有能力支援無 DHCP 自動位址設定。
- 企業內所使用之應用
  - 多媒體串流可透過所有的節點傳遞聲音，影像和資料。
  - 在儲存和開啟檔案時可計算和分析資料。
  - 傳遞檔案的座標到感應裝置
  - 從所有的節點蒐集到資料和情報
- 所有的封包在點對點傳輸時必須加密
- 入侵偵測防禦系統必須存在於所有的網路的入口點。
- VPN 可被使用，但 NAT 被禁止使用。
- 節點必須可以透過 IPv6 網路存取現有的 IPv4 應用服務。

4. 網路重要架構元件需求

企業在導入 IPv6 將會需要增強部分網路架構元件或是增加佈署 IPv6 相關設備，這些網路設備與服務將需要認真的討論和認定為一種重要資源來管理。以下將針對重要的部分特別提出討論。

4.1. DNS

DNS 現在必須同時提供 IPv4 和 IPv6 服務能力，對於企業來說 DNS 不只是提供領域名稱的對應與轉換。在導入 IPv6 網路應用服務或將現有服務升級至 dual-stack 時，DNS 必須要配合做相關設定以確保連線進行。

4.2. Routing

內部和外部路由將被要求同支援 IPv4 和 IPv6 路由協議交換，進而在企業網路內提供 IPv6 與 IPv4 共存。企業將需要來確認 IPv6 路由拓撲在企業內的狀況，哪些與外部連接的介面、供應商網路、過渡機制都需要認真的討論。

4.3. Configuration of Hosts

IPv6 能夠提供全自動化的網路設定，但根據企業自己的需求也許會採用 DHCPv6 來進行位址設定控制。企業還需要確定如何完成從上游供應商的授權，以及如何這些授權到企業的 IPv6 網路。

4.4. Security

現有的企業在 IPv4 應該都有相關的安全方式，理論上 IPv6 並不會有太大的差異。企業 IT 管理單位需要檢視手上的資安工具是否支援 IPv6，同時檢視的範圍將包含了 B2B 網路。

4.5. Applications

現有的應用服務將需要移植或提供新的替代服務，確保同時提供 IPv4 和 IPv6 服務能力。

4.6. Network Management

新增的 IPv6 網路基礎設施元件需要被納入管理，企業網路運營中心將面臨一波新的需求。企業管理單位必須確認網路管理平台是否提供 IPv6 版本，同時需要規畫 IPv6 網路用以監控網路內的節點。最終網路管理需要考慮如何在只有 IPv6 的網路管理 IPv4 節點。

4.7. Address Planning

IPv6 提供了大量的位址與全新的規劃機會，企業資訊管理單位需要擬定 IP 申請發放的規定。同時為了應付 IPv6 導入初期的轉換需求，建議保留一組 IPv4 位址提供轉換服務使用。

5. 安全議題

最近安全議題已經成為企業與政府管理單位相當重視的問題，本規範書並沒有討論到這部分。IPv6 雖然提供了更好的點對點穿透性，但是並不會因此造成資安管理上的困難。過去有許多資安問題往往發生在躲在 NAT 後的節點，現在透過 IPv6 將可以進一步的將問題簡化。

附錄二、資通信設備 IPv6 功能需求規範建議書第 3.0 版

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，可協助各級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與方法，不在本文討論之範圍，文件將依據 IPv6 Ready Logo Program 之測試規範書不定期修正，期望提供更精確之規格資料。

本文將包含範圍、參考文件、IPv6 設備型態、USG IPv6 Profile 和國際 IPv6 Ready 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 轉移技術及資通信設備引進 IPv6 功能執行方案建議及結論。

2. 範圍(Scope)

所有未來將提供 IPv6 服務之組織或個人，包括政府單位、機關、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. 參考文件(References)

[1]. IPv6 Forum, http://www.ipv6forum.org/

[2]. IPv6 Ready Logo Program, http://www.ipv6ready.org/

[3]. 台灣獲得 IPv6 Ready Logo 銀質標章一覽表,
http://interop.ipv6.org.tw/TaiwanIPv6ReadyLogoListPhase1.htm

[4]. 台灣獲得 IPv6 Ready Logo 金質標章一覽表,
http://interop.ipv6.org.tw/TaiwanIPv6ReadyLogoListPhase2.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]. 台灣中華電信研究所 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]. RFC 4038 Application Aspects of IPv6 Transition.

4. 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 Committee 特別定義了一種稱之為特殊設備(Special Device)。歸納上述四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、伺服器等)。

(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。

5. USG IPv6 Profile 和國際 IPv6 Ready 標章

5.1. USG IPv6 Profile 介紹

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。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)統一之網路設備專用術語。

(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，可能進行採購之參考。

(c)提供爾後美國政府機構相關需求之技術指導。

NIST USG 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。

此規範並不適用上述之外之目的(實作或實驗室雛型系統建置等)。NIST USG IPv6 Profile 得涵蓋了所有聯邦政府單位系統需求，因此在定義需求之用字遣詞之選用上特別故意保守模糊。此規範不但保護聯邦政府單位系統且保障了 IPv6 投資，同時也提升美國政府之 IPv6 技術標準，未來可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。

5.2. 國際 IPv6 Ready 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 日特別召集全世界的 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 1　國際 IPv6 Ready 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 1 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 441 項產品通過認證，各國取得件數統計如圖 2 (2010/10/27 為止)，以臺灣地區為例，就已有獲得 70 項標章(詳細名單請參考[3])。

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 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、亞洲地區則有台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 478 項產品通過 Phase-2 認證，各國取得件數統計如圖 3 (2010/10/27 為止)，以臺灣地區為例，就已有獲得 69 項標章(詳細名單請參考[4])。

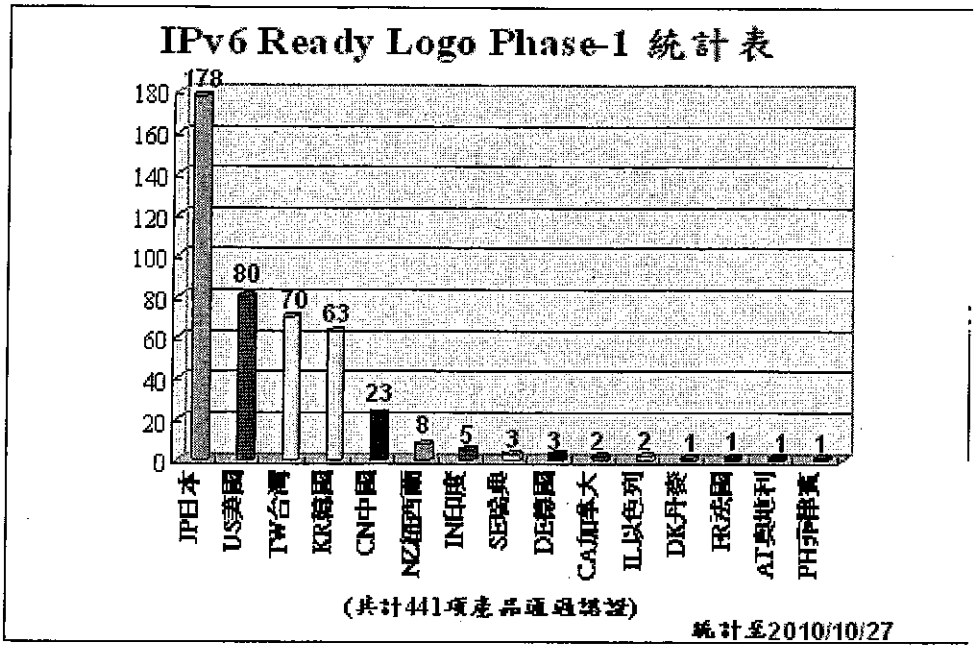


圖 2　IPv6 Ready Logo Phase-1 銀質標章統計表

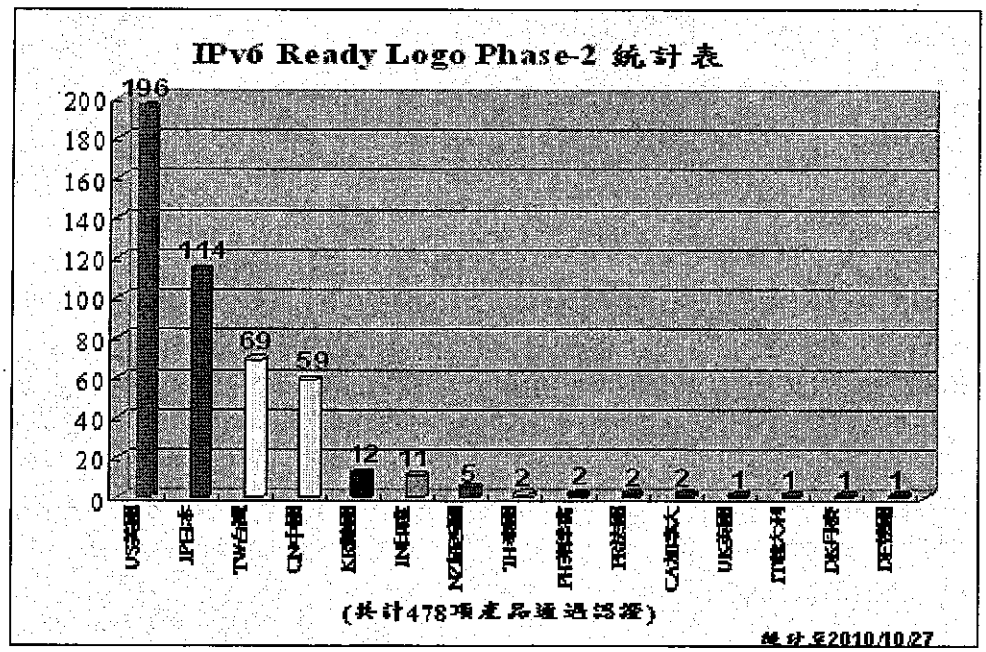


圖 3　IPv6 Ready Logo Phase-2 金質標章統計表

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 金質標章的技術門檻較高。Phase-2 測試項目現分成十大類，如表 1：IPv6 Core、IPSec、IKEv2、DHCPv6、SNMP、SIPv6、IMS、MLDv2、Mobile IPv6(MIPv6)、NEMO 及。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，可幫助申請者於自行下載、進行安裝與測試。

表 1　IPv6 Ready Logo Phase-2 金質標章測試項目(2010/09/01 更新)

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	測試工具	測試規格
P1/ P2 Core	必測	100%	V4.0.6 2010/04/26	v6eval 3.3.1 Self-Test(5.0.0)	V4.0.4 2010/03/22
IPSec	選測	100%	V1.10.0 2010/05/31	v6eval 3.3.1 IPsec_Self_Test_P2(1.10.0)	V1.10.0 2010/05/31
IKEv2 (NEW)	選測	100%	V1.1.0 2010/06/08	v6eval 3.3.1, koi 2.2.0 IKEv2_Self_Test(1.1.0)	V1.1.0 2010/06/08
DHCP	選測	100%	V1.1.2 2010/07/27	v6eval 3.3.1 self-test(1.1.0)	V1.1.0 2009/12/11
SNMP/ MIBs (NEW)	選測	100%	V1.0.3 2010/08/12	v6eval 3.3.1, koi 2.2.0 Net-SNMP 5.3.1 Perl Module SNMPv2C-AG 1.1.0	V1.0.4 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	v6eval 3.3.1, koi 2.2.0 Bind 9/ORTP/rtadvd ct-sip-ipv6-ua,-ep,-b2bua(2.0.2) -rg(2.0.0),-px(2.0.1)	V2.0.2 2010/07/22
IMS (NEW)	選測	100%	IMS UE V0.3.2 (Trial 2009/6/15)	v6eval 3.3.1, koi 2.2.0 ct-ims-ipv6-ue(2.1.0)	V0.3.1 (Trial 2009/6/15)
MLDv2 (NEW)	選測	100%	MLDv2 Router V1.0.0 (2009/12/04)	v6eval 3.3.1 ct-mldv2-router (1.0.5)	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	v6eval 3.3.1, ike-mipv6 1.0.5 ct-mipv6-cn(4.0.2) ct-mipv6-ha(4.0.7) ct-mipv6-mn(4.0.5)	V1.5.0 2007/11/08
NEMO	選測	100%	HA(v1.1.0) MR(v1.1.0) 2008/05/16	v6eval 3.3.1, ike-mipv6 1.0.5 ct-nemo-ha(1.0.2) ct-nemo-mr(1.0.2)	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 IPv6 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。Phase-1 及 Phase-2 之 IPv6 Core 符合性測試規格比較，如表 2。

表 2　Phase-1 及 Phase-2 之 IPv6 Core 符合性測試規格比較

IPv6 Ready Logo IPv6 Core 測試項目	Host		Router	
	Phase-1	Phase-2	Phase-1	Phase-2
RFC 2460 IPv6 Spec. RFC 5095 Deprecation of Type 0 Routing Headers in IPv6	30	54	40	79
RFC 4861 ND	116	236	113	150
RFC 4862 Stateless Address Auto-configuration	43	45	29	29
RFC 4443 ICMPv6	9	25	12	46
RFC 1981 Path MTU Discovery for IPv6	無	16	無	15

6. 規範建議

根據本文最後所之附表 7 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、NPD 和特殊設備之設備規範，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 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資通信廠商皆有相關產品獲得認證，且大部分作業系統及應用程式皆已支援 IPv6 功能，如表 3。

表 3　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	IPv6 版本需求	是否通過 IPv6 Ready Logo	
				Phase-1	Phase-2
微軟視窗作業系統及應用程式	Windows 2008	O.S.	支援		V
	Windows 2003	O.S.	支援	V	
	Windows XP	O.S.	SP1 及 SP2 均支援		
	Windows Vista	O.S.	支援	V	V
	Windows CE	O.S.	Ver. 4.1 以上	V	
	Windows 7	O.S.	支援		
	IIS	Web Server	Ver. 6.0 以上		
	Apache	Web server	Ver. 2.0 以上		
	sendmail	SMTP server	Ver. 8.10 以上		
	SQL server	Database	SQL Server 2005 以後		

	MySQL	Database	Ver. 4.1 以上		
Unix 作業系統及應用程式	FreeBSD	O.S.	Ver. 4.0 以上	V	V
	Linux	O.S.	Ver 2.6.15 以上	V	V
	NetBSD	O.S.	Ver. 1.5 以上		
	OpenBSD	O.S.	Ver. 3.9 以上		
	Novell	O.S.	Ver. 6.1 以上，Ver 8.0 佳	V	
	Sun Solaris	O.S. 同時支援 SPARC 及 x64 平台版本	Ver. 8 以上	V	
	IBM AIX	O.S., RS6000 的 AIX 5.2 以後版本	AIX 5.2 以上, (WAS 6.0 以上)	V	V
	HP	O.S., HP-UX	Ver. 11i 以上	V	V
	BIND	DNS server	Ver. 9.0 以上		
	IBM	Database	DB2 9 以上		
	PostgreSQL	Database	Ver. 8.3.1 以上		
	Oracle	Database	Ver. 10.1.3 以上		
MAC 作業系統	MAC OS X	O.S.	Ver. 10.2 以上		

6.1. IPv6 主機規範建議

IPv6 主機(Host)設備支援，建議如下: (請參閱附表 7)

(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)。

(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[12]。(目前大部分作業系統皆已經支援 IPv6)。

6.2. IPv6 路由器規範建議

IPv6 路由器(Router)支援，建議如下: (請參閱附表 7)

(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)。

(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)。

6.3. IPv6 網路保護設備規範建議

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。

6.4. 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。

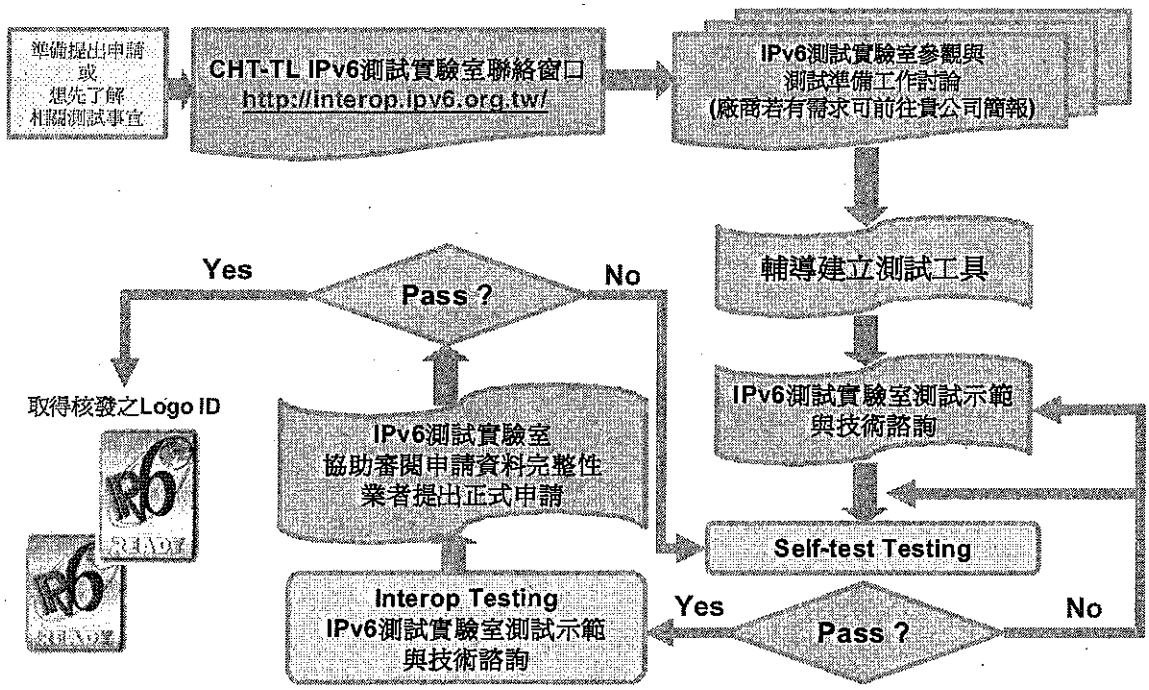
此外，第二層交換器(Layer 2 Switch)和第三層 IP 是無關的，但有些應用服務，如群播服務，為了效能理由，往往限制群播服務流的範圍，故需新增 MLD/MLDv2 Snooping 功能(RFC 4541)。且為了管理和供裝理由，第二層交換器通常需要一個管理介面，建議此管理介面需符合 IPv6 Ready Logo Phase-2 Core for Host 規範，未來更需符

合網管選項建議。

7. IPv6 互連測試建議

中華電信研究所於 2003 年起參加 IPv6 Ready Logo Program，並成立『中華電信研究所 IPv6 測試實驗室』，於 2003 年 7 月 1 日開始提供國內產業、學術及研究單位等進行 IPv6 通信協定測試服務，以達成推廣我國 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，為台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，建置 IPv6 Ready Logo Phase-1/Phase-2 符合性測試以及互連測試技術平台，提供臺灣地區 IPv6 Ready Logo Phase-1/Phase-2 認證服務。IPv6 測試服務流程，如圖 4 所示。



(符合性測試百分之百通過，始排定互連測試時間)

圖 4　Pv6 測試服務流程

8. IPv6 轉移技術及資通信設備引進 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 v6ops 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)、穿隧

(Tunneling)及轉換(Translation)等三大類技術，後續將介紹其優缺點，並建議資通信設備引進 IPv6 功能的執行策略。

8.1. 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 4 為雙協定技術優缺點比較表。

表 4　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
容易設置與易懂。	每個節點需 1 個 IPv6 位址及 1 個 IPv4 位址，兩者之間無關連。
端點對端點連線模式未遭破壞。	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。
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。	無法提供純 IPv4 主機與純 IPv6 主機的互通。

8.2. 穿隧(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。

穿遂技術可分為 6over4(RFC 2529)、6to4(RFC 3056)、Tunnel Broker(RFC 3053)、ISATAP(RFC 5214)及 Configured Tunnel(RFC 4213)，在此不多加贅述，表 5 為穿隧技術優缺點比較表。

表 5　IPv4/IPv6 穿隧(Tunneling)技術優缺點比較表

IPv4/IPv6 穿隧(Tunneling)轉移技術	
優點	缺點
節點對節點的連線方式未遭破壞。	需要 IPv4 網路架構。
利用現有 IPv4 網路，可降低成本。	無法解決 IPv4 位址不足的問題。
	封裝及解封裝增加網路額外負擔。
	需要人工的設定與維護，增加網管者沈重的工作負擔。

8.3. 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)及 A SOCKS-based IPv6/IPv4 Gateway Mechanism(RFC 3089)及 An IPv6-to-IPv4 Transport Relay Translator(RFC 3142)，相關技術在此不加贅述。

其中 NAT-PT 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。

NAT-PT 轉換器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 6 為轉換技術優缺點比較表。

表 6　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
NAT-PT 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。	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。
NAT-PT 的運作對 end-user 而言幾乎是透通的。	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。

8.4. 資通信設備引進 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 5。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[12]。對於無原始碼之應用程式可考慮使用轉換技術(如 NAT-PT)來達成轉移之目的。

資通信設備引進 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。

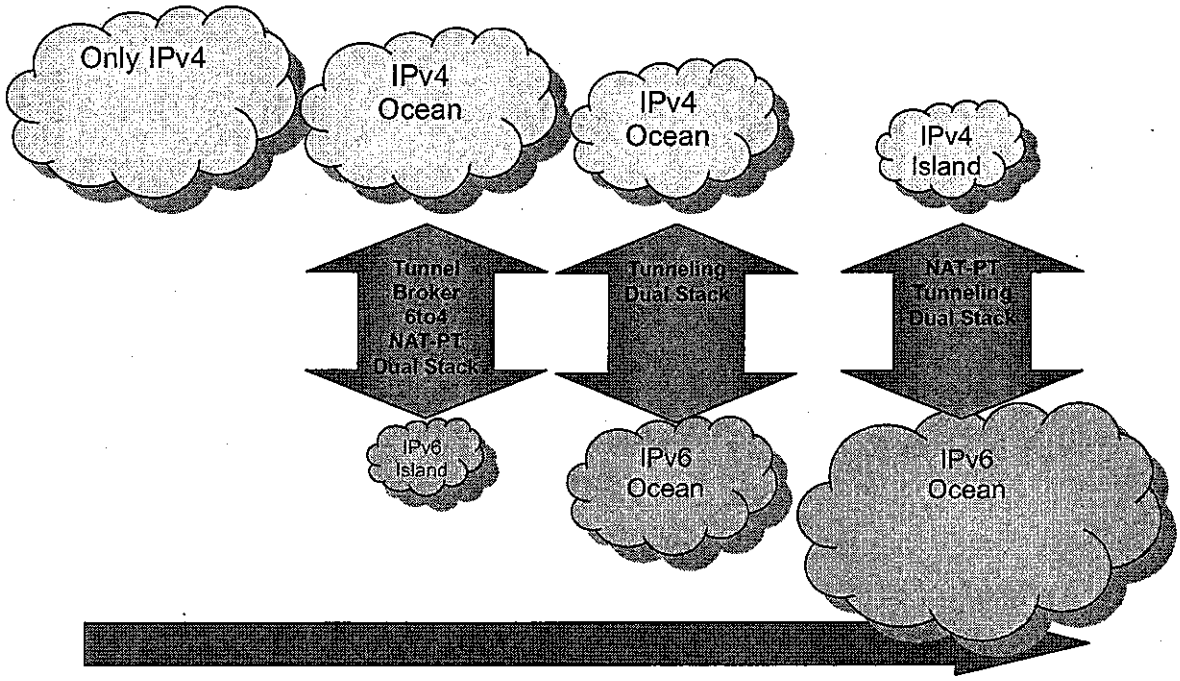


圖 5　IPv6 轉移趨勢

9. 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，根據國際組織統計預估 2011 年 IPv4 位址即將用盡。我們應該主動積極地面對此一困境，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，順勢引進 IPv6，降低投資風險。

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

本文著重於 IPv6 設備需求規範建議，重心集中於建立一個 IPv6 網路基礎建設所需的能力，未來將不定期更新，陸續增加各類設備之建議規範。

10. 致謝

本 IPv6 功能需求規範建議書之研究，首先感謝交通部郵電司及台灣網路資訊中心之指導與充分授權，另外對本產業發展分組及其他分組等相關同仁之努力，一併致上最誠摯之謝意。

表 7　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**

分類	RFCs				IPv6 Ready Logo Phase-1	IPv6 Ready Logo Phase-2	經濟部標檢局 CNS IPv6 標準	設備需求建議		
	編號	標題	狀態	時間				Host	Router	SPD
IPv6 Core										
IPv6 Core	**RFC2460**	Internet Protocol, Version 6 (IPv6) Specification	DRAFT STANDARD (Obsoletes RFC1883) (Updated by RFC5095)	1998/12	✓	✓	✓	M	M	
	RFC4861	Neighbor Discovery for IP version 6 (IPv6)	DRAFT STANDARD (Obsoletes RFC2461)	2007/09	✓	✓	✓	M	M	
	RFC4862	IPv6 Stateless Address Autoconfiguration	DRAFT STANDARD (Obsoletes RFC2462)	2007/09	✓	✓	✓	M	M	
	RFC4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	DRAFT STANDARD (Obsoletes RFC2463) (Updates RFC2780) (Updated by RFC4884)	2006/03	✓	✓	✓	M	M	
	RFC2464	Transmission of IPv6 Packets over Ethernet Networks	PROPOSED STANDARD (Obsoletes RFC1972)	1998/12	✓	✓	✓	M	M	
	RFC1981	Path MTU Discovery for IP version 6	PROPOSED STANDARD	1996/08		✓	✓	M	M	
	RFC4291	Internet Protocol Version 6 (IPv6) Addressing Architecture	DRAFT STANDARD (Obsoletes RFC3513)	2006/02		✓	✓	M	M	
	RFC3697	IPv6 Flow Label Specification.	PROPOSED STANDARD	2004/03				O	O	

	RFC5095	Deprecation of Type 0 Routing Headers in IPv6	PROPOSED STANDARD (Updates RFC2460, RFC4294)	2007/12		✓		**M**	**M**	
	RFC2675	IPv6 Jumbograms	PROPOSED STANDARD (Obsoletes RFC2147)	1999/08			✓	O	O	
	RFC3971	Secure Neighbour Discovery	PROPOSED STANDARD	2005/03				O	O	
	RFC3986	Uniform Resource Identifier (URI): Generic Syntax	STANDARD (Obsoletes RFC2732, RFC2396, RFC1808) (Updates RFC1738) (Also STD0066)	2005/01				O	O	
	RFC4884	Extended ICMP to Support Multi-Part Messages	PROPOSED STANDARD (Updates RFC0792, RFC4443)	2007/04				O	O	
	RFC4294	IPv6 Node Requirements	INFORMATIONAL (Updated by RFC5095)	2006/04				O	O	
	RFC5175	IPv6 Router Advertisement Flags Option	PROPOSED STANDARD (Obsoletes RFC5075)	2008/03				O	O	
Addressing	**RFC4007**	IPv6 Scoped Address Architecture	PROPOSED STANDARD	2005/03				O	O	
	RFC4193	Unique Local IPv6 Unicast Address	PROPOSED STANDARD	2005/10				O	O	
	RFC3879	Deprecating Site Local Addresses	PROPOSED STANDARD	2004/09				O	O	
	RFC3041	Privacy Extensions for IPv6 Stateless Address Autocon fig	PROPOSED STANDARD	2001/01				O	O	
	RFC3484	Default Address Selection for IPv6	PROPOSED STANDARD	2003/02				O	O	
	RFC3972	Cryptographically Generated Addresses (CGA)	PROPOSED STANDARD (Updated by RFC4581, RFC4982)	2005/03				O	O	
	RFC3587	IPv6 Global Unicast Address Format.	INFORMATIONAL (Obsoletes RFC2374)	2003/08			✓	O	O	
	RFC3595	Textual Conventions for IPv6 Flow Label	PROPOSED STANDARD	2003/09			✓	O	O	
	RFC5156	Special-Use IPv6 Addresses	INFORMATIONAL	2008/04				O	O	
Link	**RFC2467**	IPv6 over FDDI	PROPOSED STANDARD (Obsoletes RFC2019)	1998/12				O	O	
	RFC2470	Transmission of IPv6 Packets over Token Ring Networks	PROPOSED STANDARD	1998/12				O	O	

	RFC5072	IP Version 6 over PPP	DRAFT STANDARD (Obsoletes RFC2472)	2007/09				O	O	
	RFC5172	Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol	PROPOSED STANDARD (Obsoletes RFC2472)	2008/03				O	O	
	RFC2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks	PROPOSED STANDARD	1999/01				O	O	
	RFC2492	IPv6 over ATM Networks	PROPOSED STANDARD	1999/01				O	O	
	RFC2497	IPv6 over ARCnet	PROPOSED STANDARD	1999/01				O	O	
	RFC2590	IPv6 over Frame Relay	PROPOSED STANDARD	1999/05				O	O	
	RFC3146	IPv6 over IEEE 1394 Networks	PROPOSED STANDARD	2001/10				O	O	
	RFC3572	IPv6 over MAPOS (SONET/SDH)	INFORMATIONAL	2003/07				O	O	
	RFC4338	Transmission of IPv6 & IPv4 over Fibre Channel	PROPOSED STANDARD (Obsoletes RFC3831, RFC2625)	2006/01				O	O	
	RFC4919	IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs):Overview, Assumptions, Problem Statement, and Goals.	INFORMATIONAL	2007/08				O	O	
IPSec										
IPSec	**RFC4301**	Security Architecture for the Internet Protocol	PROPOSED STANDARD (Obsoletes RFC2401)	2005/12		✓		O+	O+	
	RFC4302	IP Authentication Header	PROPOSED STANDARD (Obsoletes RFC2402)	2005/12		✓		O+	O+	
	RFC2403	The Use of HMAC-MD5-96 within ESP and AH	PROPOSED STANDARD	1998/11		✓		O+	O+	
	RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH	PROPOSED STANDARD	1998/11		✓		O+	O+	
	RFC2405	The ESP DES-CBC Cipher Algorithm With Explicit IV	PROPOSED STANDARD	1998/11		✓		O+	O+	
	RFC4303	IP Encapsulating Security Payload (ESP)	PROPOSED STANDARD (Obsoletes RFC2406)	2005/12		✓		O+	O+	
	RFC4308	Cryptographic Suites for IPsec.	PROPOSED STANDARD	2005/12				O+	O+	

	RFC4310	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP).	PROPOSED STANDARD	2005/12				O+	O+	
	RFC2410	The NULL Encryption Algorithm and Its Use With IPsec	PROPOSED STANDARD	1998/11		✓		O+	O+	
	RFC2451	The ESP CBC-Mode Cipher Algorithms	PROPOSED STANDARD	1998/11		✓		O+	O+	
	RFC3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec	PROPOSED STANDARD	2003/09		✓		O+	O+	
	RFC3602	The AES-CBC Cipher Algorithm and Its Use with IPsec	PROPOSED STANDARD	2003/09		✓		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	2005/12				O+	O+	
	RFC4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).	PROPOSED STANDARD (Obsoletes RFC4305)	2007/04				O+	O+	
	RFC4306	Internet Key Exchange (IKEv2) Protocol.	PROPOSED STANDARD (Obsoletes RFC2407, RFC2408, RFC2409) (Updated by RFC5282)	2005/12				O+	O+	
	RFC5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol.	PROPOSED STANDARD (Updates RFC4306)	2008/08				O+	O+	
	RFC4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).	PROPOSED STANDARD	2005/12				O+	O+	
Mobility										
MIPv6	**RFC3775**	Mobility support in IPv6	PROPOSED STANDARD	2004/06		✓	✓	O+	O+	
	RFC3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	PROPOSED STANDARD (Updated by RFC4877)	2004/06		✓	✓	O+	O+	
	RFC4283	Mobile Node Identifier option for MIPV6	PROPOSED STANDARD	2005/11				O	O	

	RFC4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture.	PROPOSED STANDARD (Updates RFC3776)	2007/04				O	O	
	RFC5094	Mobile IPv6 Vendor Specific Option	PROPOSED STANDARD	2007/12				O	O	
	RFC5096	Mobile IPv6 Experimental Messages	PROPOSED STANDARD	2007/12				O	O	
	RFC5142	Mobility Header Home Agent Switch Message	PROPOSED STANDARD	2008/01				O	O	
	RFC5149	Service Selection for Mobile IPv6	INFORMATIONAL	2008/02				O	O	
	RFC5268	Mobile IPv6 Fast Handovers	PROPOSED STANDARD (Obsoletes RFC4068)	2008/06				O	O	
	RFC5269	Distributing a Symmetric Fast Mobile IPv6 (FMIPv6) Handover Key Using SEcure Neighbor Discovery (SEND)	PROPOSED STANDARD	2008/06				O	O	
	RFC5270	Mobile IPv6 Fast Handovers over IEEE 802.16e Networks	INFORMATIONAL	2008/06				O	O	
	RFC5271	Mobile IPv6 Fast Handovers for 3G CDMA Networks	INFORMATIONAL	2008/06				O	O	
	RFC5380	Hierarchical Mobile IPv6 (HMIPv6) Mobility Management.	PROPOSED STANDARD (Obsoletes RFC4140)	2008/10				O	O	
NEMO	**RFC3963**	Network Mobility (NEMO) Basic Support Protocol	PROPOSED STANDARD	2005/01		✓		O	O	
	RFC4908	Multi-homing for small scale fixed network Using Mobile IP and NEMO.	EXPERIMENTAL	2007/06				O	O	
Management										
SNMP	**RFC1157**	Simple Network Management Protocol (SNMP).	HISTORIC	1990/05				O+	O+	
	RFC2578	Structure of Management Information Version 2 (SMIv2)	STANDARD (Obsoletes RFC1902) (Also STD0058)	1999/04		✓		O+	O+	
	RFC2579	Textual Conventions for SMIv2	STANDARD (Obsoletes RFC1903) (Also STD0058)	1999/04		✓		O+	O+	
	RFC2580	Conformance Statements for SMIv2	STANDARD (Obsoletes RFC1904) (Also STD0058)	1999/04		✓		O+	O+	

	RFC3411	SNMP v3 Management Framework	STANDARD (Obsoletes RFC2571) (Updated by RFC5343) (Also STD0062)	2002/12				O	O	
	RFC3412	SNMP Message Process and Dispatch	STANDARD (Obsoletes RFC2572) (Also STD0062)	2002/12				O	O	
	RFC3413	SNMP Applications	STANDARD (Obsoletes RFC2573) (Also STD0062)	2002/12				O	O	
	RFC3414	User-based Security Model for SNMPv3	STANDARD (Obsoletes RFC2574) (Also STD0062)	2002/12				O	O	
	RFC3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).	STANDARD (Obsoletes RFC1905) (Also STD0062)	2002/12		✓		O+	O+	
	RFC3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).	STANDARD (Obsoletes RFC1907) (Also STD0062)	2002/12		✓		O+	O+	
MIBs	**RFC2863**	The Interfaces Group MIB.	DRAFT STANDARD (Obsoletes RFC2233)	2000/06				O	O	
	RFC3019	IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol	PROPOSED STANDARD	2001/01				O	O	
	RFC4087	MIB for IP Tunnels	PROPOSED STANDARD (Obsoletes RFC2667)	2005/06				O	O	
	RFC4022	Management Information Base for the Transmission Control Protocol (TCP).	PROPOSED STANDARD (Obsoletes RFC2452, RFC2012)	2005/03				O	O	
	RFC4113	Management Information Base for the User Datagram Protocol (UDP).	PROPOSED STANDARD (Obsoletes RFC2454, RFC2013)	2005/06				O	O	
	RFC4292	IP Forwarding Table MIB.	PROPOSED STANDARD (Obsoletes RFC2096)	2006/04				O	O	
	RFC4293	Management Information Base for the Internet Protocol (IP).	PROPOSED STANDARD (Obsoletes RFC2011, RFC2465, RFC2466)	2006/04		✓		O+	O+	
	RFC4292	IP Forwarding Table MIB.	PROPOSED STANDARD (Obsoletes RFC2096)	2006/04				O	O	

	RFC4668	RADIUS Authentication Client MIB for IPv6.	PROPOSED STANDARD (Obsoletes RFC2618)	2006/08				O	O	
	RFC4669	RADIUS Authentication Server MIB for IPv6.	PROPOSED STANDARD (Obsoletes RFC2619)	2006/08				O	O	
	RFC4670	RADIUS Accounting Client MIB for IPv6.	INFORMATIONAL (Obsoletes RFC2620)	2006/08				O	O	
	RFC4671	RADIUS Accounting Server MIB for IPv6.	INFORMATIONAL (Obsoletes RFC2621)	2006/08				O	O	
	RFC4807	IPsec Security Policy Database Configuration MIB.	PROPOSED STANDARD	2007/03				O	O	
	RFC4898	TCP Extended Statistics MIB.	PROPOSED STANDARD	2007/05				O	O	
	RFC5060	Protocol Independent Multicast MIB.	PROPOSED STANDARD	2008/01				O	O	
	RFC5132	IP Multicast MIB.	PROPOSED STANDARD (Obsoletes RFC2932)	2007/12				O	O	
	RFC5240	Protocol Independent Multicast (PIM) Bootstrap Router MIB	PROPOSED STANDARD	2008/06				O	O	
Application										
DHCPv6	**RFC3315**	Dynamic Host Config Protocol (DHCPv6)	PROPOSED STANDARD (Updated by RFC4361)	2003/07		✓	✓	O+	O+	
	RFC4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4).	PROPOSED STANDARD (Updates RFC2131, RFC2132, RFC3315)	2006/02				O	O	
	RFC3319	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers.	PROPOSED STANDARD	2003/07				O	O	
	RFC3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6.	PROPOSED STANDARD	2003/12				O	O	
	RFC3646	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	PROPOSED STANDARD	2003/12		✓		O	O	
	RFC3736	Stateless DHCP Service for IPv6	PROPOSED STANDARD	2004/04		✓		O	O	
	RFC3898	Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	PROPOSED STANDARD	2004/10				O	O	

	RFC4075	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6.	PROPOSED STANDARD	2005/05				O	O	
	RFC4076	Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	INFORMATIONAL	2005/05				O	O	
	RFC4242	Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).	PROPOSED STANDARD	2005/11				O	O	
	RFC4477	Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues.	INFORMATIONAL	2006/05				O	O	
	RFC4580	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option.	PROPOSED STANDARD	2006/06				O	O	
	RFC4649	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option.	PROPOSED STANDARD	2006/08				O	O	
	RFC4994	DHCPv6 Relay Agent Echo Request Option.	PROPOSED STANDARD	2007/09				O	O	
	RFC5007	DHCPv6 Leasequery	PROPOSED STANDARD	2007/09				O	O	
Sockets	**RFC3493**	Basic Socket Interface Extensions for IPv6.	INFORMATIONAL (Obsoletes RFC2553)	2003/02				O+	O+	
	RFC3542	Advanced Sockets Application Program Interface (API) for IPv6.	INFORMATIONAL (Obsoletes RFC2292)	2003/05				O	O	
	RFC4584	Extension to Sockets API for Mobile IPv6.	INFORMATIONAL	2006/07				O	O	
	RFC5014	IPv6 Socket API for Source Address Selection.	INFORMATIONAL	2007/09				O	O	
RADIUS	**RFC3162**	RADIUS and IPv6	PROPOSED STANDARD	2001/08				O+	O+	
	RFC4668	RADIUS Authentication Client MIB for IPv6.	PROPOSED STANDARD (Obsoletes RFC2618)	2006/08				O	O	
	RFC4669	RADIUS Authentication Server MIB for IPv6.	PROPOSED STANDARD (Obsoletes RFC2619)	2006/08				O	O	
	RFC4670	RADIUS Accounting Client MIB for IPv6.	INFORMATIONAL (Obsoletes RFC2620)	2006/08				O	O	
	RFC4671	RADIUS Accounting Server MIB for IPv6.	INFORMATIONAL (Obsoletes RFC2621)	2006/08				O	O	
	RFC5176	Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)	INFORMATIONAL (Obsoletes RFC3576)	2008/01				O	O	

DNSv6	**RFC3596**	DNS Extensions to Support IP Version 6.	DRAFT STANDARD (Obsoletes RFC3152, RFC1886)	2003/10			✓	O+	O+	
	RFC3901	DNS IPv6 Transport Operational Guidelines	BCP0091	2004/09				O	O	
	RFC4074	Common Misbehavior Against DNS Queries for IPv6 Addresses.	INFORMATIONAL	2005/05				O	O	
	RFC4472	Operational Considerations and Issues with IPv6 DNS.	INFORMATIONAL	2006/04				O	O	
	RFC5006	IPv6 Router Advertisement Option for DNS Configuration.	EXPERIMENTAL	2007/09				O	O	
SIPv6	**RFC3261**	SIP: Session Initiation Protocol	PROPOSED STANDARD (Obsoletes RFC2543) (Updated by RFC3265, RFC3853, RFC4320, RFC4916)	2002/06		✓		O+	O+	
	RFC3264	An Offer/Answer Model with Session Description Protocol	PROPOSED STANDARD (Obsoletes RFC2543)	2002/06				O	O	
	RFC4566	SDP: Session Description Protocol	PROPOSED STANDARD (Obsoletes RFC2327, RFC3266)	2006/07		✓		O	O	
	RFC2617	HTTP Authentication: Basic and Digest Access Authentication	DRAFT STANDARD (Obsoletes RFC2069)	1999/06				O	O	
	RFC3665	SIP Basic Call Flow Examples	BCP0075	2003/12				O	O	
	RFC5118	Session Initiation Protocol (SIP) Torture Test Messages for Internet Protocol Version 6 (IPv6)	INFORMATIONAL	2008/02				O	O	
Routing										
Routing	**RFC2080**	RIPng for IPv6.	PROPOSED STANDARD	1997/01					O+	
	RFC2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	PROPOSED STANDARD	1997/03					O+	
	RFC5340	OSPF for IPv6	PROPOSED STANDARD (Obsoletes RFC2740)	2008/07					O+	

	RFC5187	OSPFv3 Graceful Restart.	PROPOSED STANDARD	2008/06					O	
	RFC5243	OSPF Database Exchange Summary List Optimization.	INFORMATIONAL	2008/05					O	
	RFC5329	Traffic Engineering Extensions to OSPF Version 3.	PROPOSED STANDARD	2008/09					O	
	RFC2894	Router Renumbering for IPv6	PROPOSED STANDARD	2000/08					O	
	RFC4552	Authentication/Confidentiality for OSPFv3	PROPOSED STANDARD	2006/06					O	
	RFC4271	A Border Gateway Protocol 4 (BGP-4)	DRAFT STANDARD (Obsoletes RFC1771)	2006/01					O+	
	RFC1772	BGP Application in the Internet	DRAFT STANDARD (Obsoletes RFC1655)	1995/03					O	
	RFC4760	Multiprotocol Extensions for BGP-4.	DRAFT STANDARD (Obsoletes RFC2858)	2007/01					O+	
	RFC5308	Routing IPv6 with IS-IS.	PROPOSED STANDARD	2008/10					O	
	RFC4798	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE).	PROPOSED STANDARD	2007/02					O	
	RFC5120	M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)	PROPOSED STANDARD	2008/02					O	
	RFC5185	OSPF Multi-Area Adjacency	PROPOSED STANDARD	2008/05					O	
Transition										
Transition	**RFC2765**	Stateless IP/ICMP Translation Algorithm (SIIT)	PROPOSED STANDARD	2000/02				O	O	
	RFC2776	Network Address Translation - Protocol Translation (NAT-PT)	HISTORIC (Obsoleted by RFC4966) (Updated by RFC3152)	2000/02				O	O	
	RFC2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels.	PROPOSED STANDARD	1999/03				O	O	
	RFC3053	IPv6 Tunnel Broker.	INFORMATIONAL	2001/01				O	O	
	RFC4966	Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status.	INFORMATIONAL (Obsoletes RFC2766)	2007/07				O	O	

	RFC3056	Connection of IPv6 Domains via IPv4 Clouds (6to4)	PROPOSED STANDARD	2001/02				O+	O+	
	RFC4213	Transition Mechanisms for IPv6 Hosts and Routers	PROPOSED STANDARD (Obsoletes RFC2893)	2005/10			✓	O+	O+	
	RFC2473	Generic Packet Tunneling in IPv6	PROPOSED STANDARD	1998/12				O	O	
	RFC4798	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE).	PROPOSED STANDARD	2007/02				O	O	
	RFC4891	Using IPsec to Secure IPv6-in-IPv4 Tunnels	INFORMATIONAL	2007/05				O	O	
	RFC5158	6to4 Reverse DNS Delegation Specification	INFORMATIONAL	2008/03				O	O	
	RFC5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).	INFORMATIONAL (Obsoletes RFC4214)	2008/03				O	O	
Multicast										
Multicasting	**RFC2710**	Multicast Listener Discovery (MLD) for IPv6	PROPOSED STANDARD (Updated by RFC3590, RFC3810)	1999/10				O	O	
	RFC2711	IPv6 Router Alert Option	PROPOSED STANDARD	1999/10				O	O	
	RFC3810	MLD Version 2 for IPv6	PROPOSED STANDARD (Updates RFC2710) (Updated by FC4604)	2004/06				O+	O+	
	RFC4604	Using MLDv2 for Source Specifice Multicast (SSM)	PROPOSED STANDARD (Updates RFC3376, RFC3810)	2006/08				O+	O+	
	RFC3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol.	PROPOSED STANDARD (Updates RFC2710)	2003/09				O	O	
	RFC4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches.	INFORMATIONAL	2006/05				O	O	
	RFC4605	Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying").	PROPOSED STANDARD	2006/08				O	O	

	RFC4601	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised).	PROPOSED STANDARD (Obsoletes RFC2362) (Updated by RFC5059)	2006/08				O	O	
	RFC4602	Protocol Independent Multicast - Sparse Mode (PIM-SM) IETF Proposed Standard Requirements Analysis.	INFORMATIONAL	2006/08				O	O	
	RFC4609	Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements.	INFORMATIONAL	2006/10				O	O	
	RFC4610	Anycast-RP Using Protocol Independent Multicast (PIM).	PROPOSED STANDARD	2006/08				O	O	
	RFC4607	Source-Specific Multicast for IP.	PROPOSED STANDARD	2006/08				O	O	
	RFC5110	Overview of the Internet Multicast Routing Architecture	INFORMATIONAL	2008/01				O	O	
	RFC5186	Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction.	INFORMATIONAL	2006/05				O	O	

資通設備
IPv6功能需求規範建議書
第1.0版

發行機構：IPv6建置發展計畫標準測試分項計畫
執行單位：中華電信研究所
督導單位：交通部、IPv6建置發展計畫辦公室

中華民國九十六年五月製作

版本更新紀錄

版本	發行日期	摘要說明
第1.0版	2007年5月	初版

資通設備
IPv6功能需求規範建議書

目　錄

圖　目　錄

表　目　錄

http://www.nist.gov/

[11]. RFC 4038 Application Aspects of IPv6 Transition.

4. 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 Committee 特別定義了一種稱之為特殊設備(Special Device)。歸納上述四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、伺服器等)。

(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。

5. 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 日特別召集全世界的 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 1 國際 IPv6 Ready 標章(左邊為 Phase I 銀質標章和右邊為 Phase II 金質標章)

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

Phase I 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 I 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 293 項產品通過認證，各國取得件數統計如圖 2 (2007/05/30 為止)，以臺灣地區為例，就已有獲得 44 項標章(詳細名單請參考[3])。

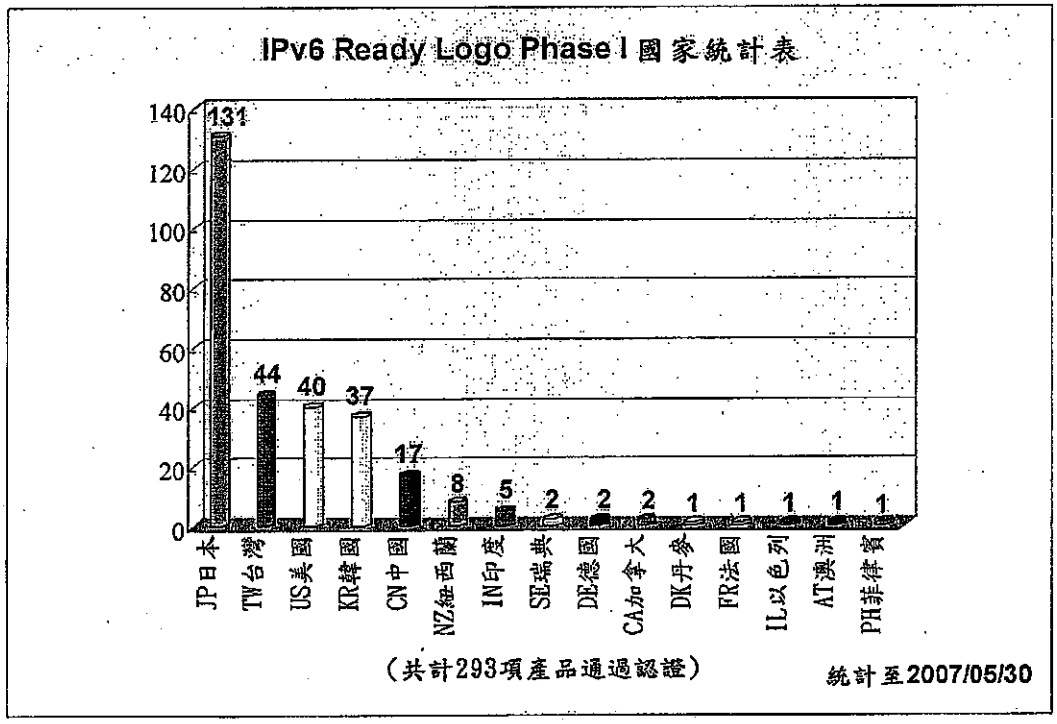


圖 2 IPv6 Ready Logo Phase I 國家統計表

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 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 II)為一國際性全方位 IPv6 測試計畫，主要由日本 TAHI[4]和美國 UNH(University of New Hampshire)互連

測試實驗室 IOL(InterOperability Lab.)[5]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 IRISIA、亞洲地區則有台灣的 NICI IPv6 標準測試實驗室[6]、韓國的 TTA[7]以及中國大陸的 BII[8]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 II)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 100 項產品通過 Phase II 認證，各國取得件數統計如圖 3(2007/05/30 為止)，以臺灣地區為例，就已有獲得 12 項標章(詳細名單請參考[3])。

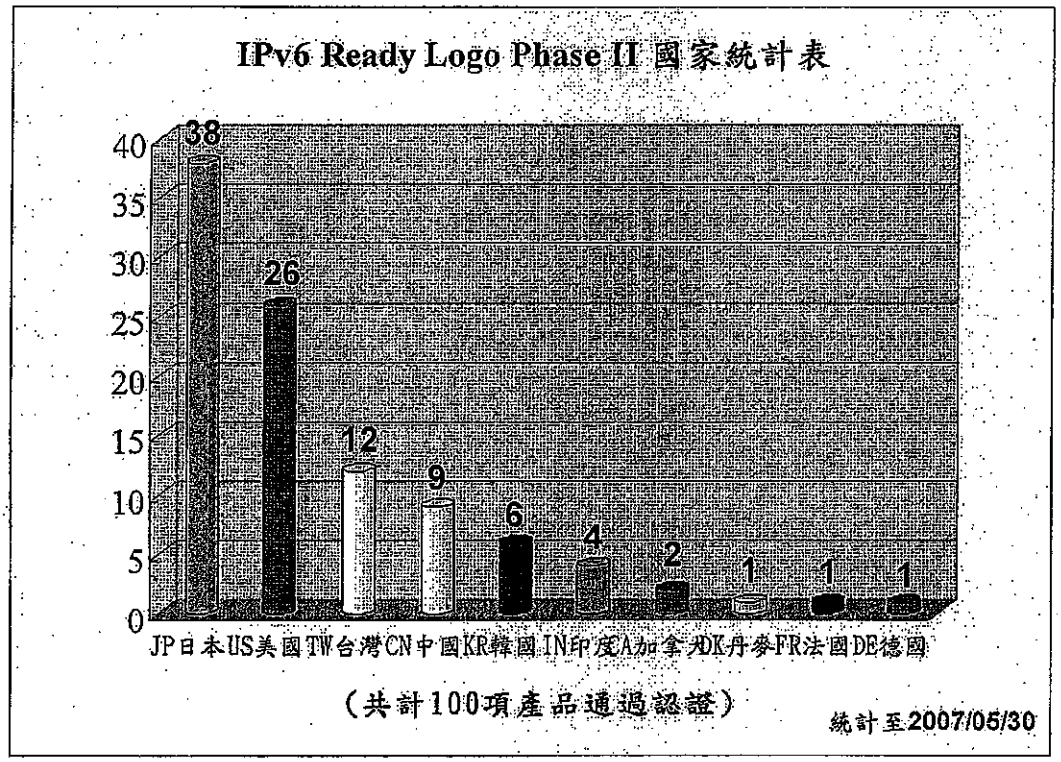


圖 3 IPv6 Ready Logo Phase II 國家統計表

IPv6 Ready Logo Phase I 銀質標章為基本測試規範，目前著重於 Phase II 推廣，Phase I 為 Phase II 之測試子集，換句話說 Phase II 之金質標章技術門檻較高。Phase II 測試項目現分成三大類，如表 1：IPv6 Core、Mobile IPv6(MIPv6)及 IPSec。凡是欲申請取得 IPv6 Ready Logo Phase II 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)。其中符合性測試已有開發自動化測試工具，可幫助申請者於自行下載、進行安裝與測試。

表 1 IPv6 Ready Logo Phase II 測試項目

測試項目	必測與否	符合性測試		互連測試
		通過條件	測試規格	測試規格
IPv6 Core	必測	100%	V3.8.10 2007/04/13	V2.8.4 2007/04/10
MIPv6	選測	100%	CN、HA、MN V3.1.5 2006/08/21	V1.4.3 2006/08/21
IPSec	選測	100%	V1.8.0 2007/04/27	V1.5.0 2007/04/27
NEMO	選測	100%	HA、MR V1.0.0 2007/01/22	V1.0.0 2007/01/22
DHCP	選測	100%	V1.0.0 2007/04/27	V1.0.1 2007/04/27
SIP	選測	100%	UA、Proxy Server V1.0.0 2007/04/27	V1.0.0 2007/04/27

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，參考標準為 RFC 2460、RFC2461、RFC 2462、RFC 2463 及 RFC 1981 共五篇。

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 II 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)、IPv6 實作(implementation)、嵌入系統(embedded system)和特殊用途伺服器。

Phase I 及 II 之 IPv6 Core 符合性測試規格比較，如表 2。

表 2 Phase I 及 II 之 IPv6 Core 符合性測試規格比較

IPv6 Ready Logo IPv6 Core 測試項目	Host		Router	
	Phase I	Phase II	Phase I	Phase II
RFC 2460 IPv6 Spec.	29	53	39	77
RFC 2461 ND	27	218	28	148
RFC 2462 Stateless Address Auto-configuration	26	41	14	26
RFC 2463 ICMPv6	12	21	13	40
RFC 1981 Path MTU Discovery for IPv6	無	15	無	14

6. 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 和特殊設備之設備規範。

6.1. IPv6 主機規範建議

IPv6 主機(Host)設備支援，建議如下: (請參閱附錄一)

(1) 必須通過 IPv6 Ready Logo Phase II Core for Host 的測試規範。

(2) 安全選項：IPv6 Ready Logo Phase II IPSec for End-Node 的測試規範。

(3) 網管選項：目前無 IPv6 Ready Logo 相關標準(已經列入下一階段 Phase II 候選標章)，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 Ready Logo 標章確立及市場設備普遍成熟時再納入必要選項)。

(4) 移動性選項：IPv6 Ready Logo Phase II 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。

(5) DNS 選項：目前無 IPv6 Ready Logo 相關標準(已經列入下一階段 Phase II 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 II 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 II 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。(目前大部分作業系統皆已經支援 IPv6)。

6.2. IPv6 路由器規範建議

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 II Core for Router 的測試規範。

(2) 安全選項：IPv6 Ready Logo Phase II IPSec for Secure Gateway 的測試規範。

(3) 網管選項：目前無 IPv6 Ready Logo 相關標準(已經列入下一階段 Phase II 候選標章)，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 Ready Logo 標章確立及市場設備普遍成熟時再納入必要選項)

(4) 移動性選項：IPv6 Ready Logo Phase II 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。

(5) DNS 選項：目前無 IPv6 Ready Logo 相關標準(已經列入下一階段 Phase II 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 II 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 2740)和 BGP-4+(RFC2545、RFC4271)。

6.3. IPv6 網路保護設備規範建議

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

6.4. IPv6 特殊設備規範建議

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

此外，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 II Core for Host 規範，未來更需符合網管選項建議。

7. IPv6互連測試建議

依據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『IPv6 建置發展計畫』規劃，委由標準測試分組中華電信研究所規劃建置『NICI IPv6 標準測試實驗室』，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，NICI IPv6 標準測試實驗室為國際 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，為台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 I/Phase II 標章。

NICI IPv6 標準測試實驗室著重於 Phase II 標章推廣，建置 IPv6 Ready Logo Phase I/Phase II 符合性測試以及互連測試技術平台，提供臺灣地區 IPv6 Ready Logo Phase I/Phase II 認證服務。NICI IPv6 標準測試服務流程，如圖 4所示。

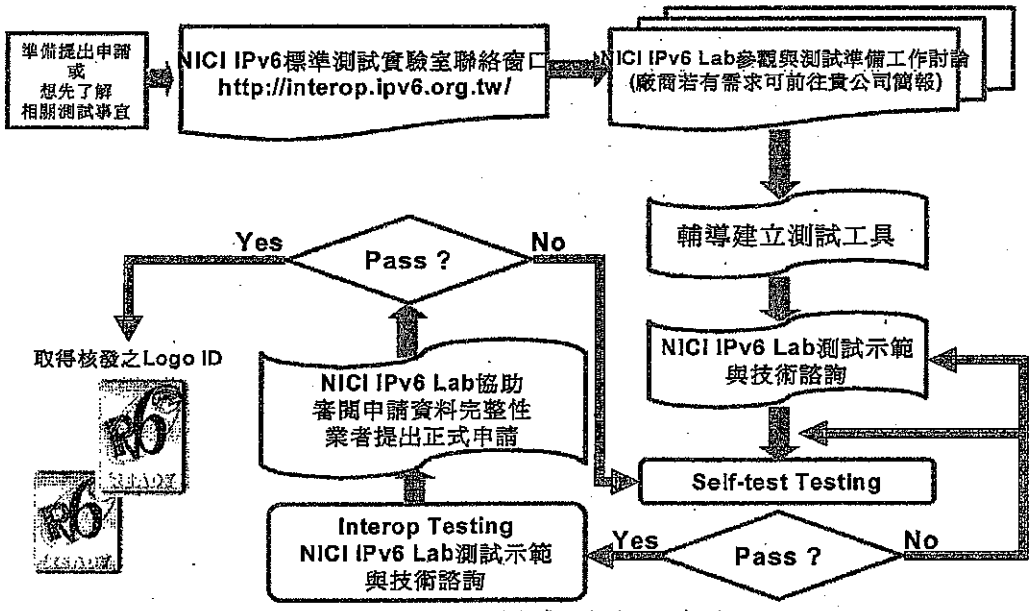


圖 4 NICI IPv6 標準測試服務流程

有關 IPv6 Ready Logo 之互連測試可前往 NICI IPv6 標準測試實驗室[6]進行相關服務。其他相關互連測試(如 Routing Protocol 等)，將視國際 IPv6 Forum 之腳步，陸續提供。

8. 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 雙協定堆疊(Dual Stack)、穿隧(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。

8.1. IPv4/IPv6 雙協定堆疊(Dual Stack)

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 雙協定堆疊。此種 IPv4/IPv6 雙協定堆疊架構提供該 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 雙協定堆疊將由純 IPv6 協定堆疊取代，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 雙協定堆疊架構中，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為雙協定堆疊技術優缺點比較表。

表 3 IPv4/IPv6 雙協定堆疊(Dual Stack)技術優缺點比較表

IPv4/IPv6 雙協定堆疊(Dual Stack)轉移技術	
優點	缺點
容易設置與易懂。	擴展性(scalability)差。因為每個節點需 1 個 IPv6 位址及 1 個 IPv4 位址。
端點對端點連線模式未遭破壞。	系統複雜度及負擔增加，需維持 2 個 IP 協定個別的 routing table 及

	相關網管資訊。
雙堆疊主機可與其它雙協定堆疊主機、純 IPv4 主機或純 IPv6 主機互連。	無法提供純 IPv4 主機與純 IPv6 主機的互通。

8.2. 穿隧(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 雙協定堆疊的節點。

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 與 IPv6 間的連線。

隧道技術可分為 6over4(RFC 2529)、6to4(RFC 3056)、Tunnel Broker(RFC 3053)、ISATAP(RFC 4214)及 Configured Tunnel(RFC 4213)，在此不多加贅述，表 4為穿隧技術優缺點比較表。

表 4 IPv4/IPv6 穿隧(Tunneling)技術優缺點比較表

IPv4/IPv6 穿隧(Tunneling)轉移技術	
優點	缺點
節點對節點的連線方式未遭破壞。	需要 IPv4 網路架構。
利用現有 IPv4 網路，可降低成本。	無法解決 IPv4 位址不足的問題。
	封裝及解封裝增加網路額外負擔。
	需要人工的設定與維護，增加網管者沈重的工作負擔。

8.3. 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)及 A SOCKS-based IPv6/IPv4 Gateway Mechanism(RFC 3089)及 An IPv6-to-IPv4 Transport Relay Translator(RFC 3142)，相關技術在此不加贅述。

其中 NAT-PT 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 可充當兩者的翻譯官。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。

NAT-PT 轉換器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
NAT-PT 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。	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。
NAT-PT 的運作對 end-user 而言幾乎是透通的。	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。

8.4. 資通設備引進 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 雙協定堆疊網路，甚至只提供 IPv6 網路及服務，如圖 5。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 雙協定堆疊，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[11]。對於無原始碼之應用程式可考慮使用轉換技術(如 NAT-PT)來達成轉移之目的。

資通設備引進 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 雙堆疊之功能。
(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。

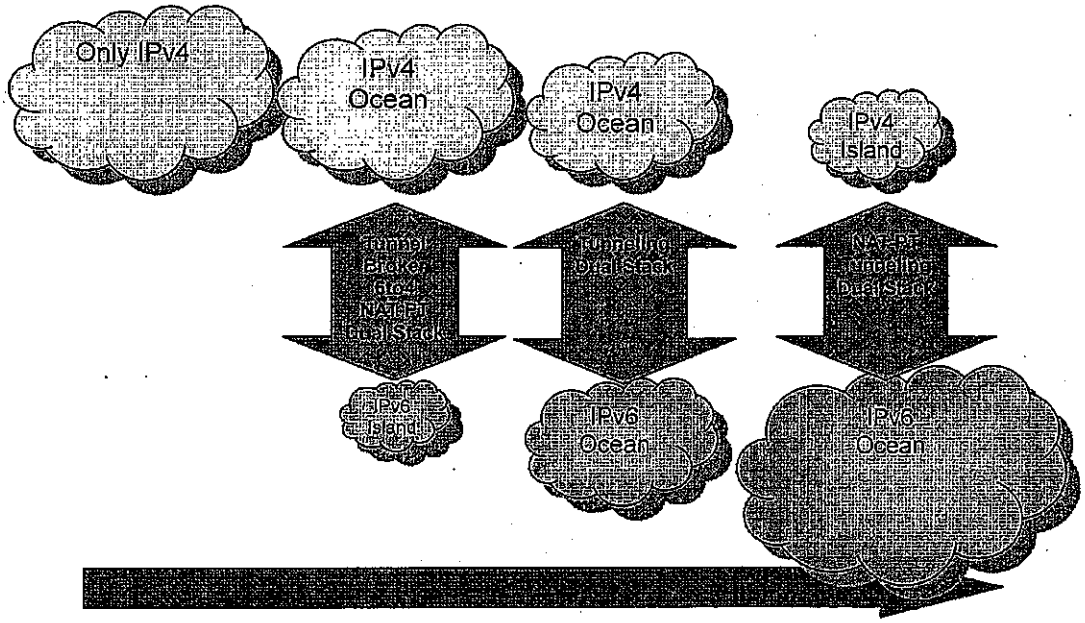


圖 5 IPv6 轉移趨勢

9. 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，根據國際組織統計預估 2009~2015 年間 IPv4 位址即可能用盡。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。

本文著重於 IPv6 設備需求規範建議。在此版本中，把重心集中於建立一個核心 IPv6 網路基礎建設所需的能力，未來將不定期更新，陸續增加各類設備之建議規範。

10. 致謝

本 IPv6 功能需求規範建議書之研究，首先感謝交通部郵電司及台灣網路資訊中心之指導與充分授權，另外對本分組及其他分組等相關同仁之努力，一併致上最誠摯之謝意。

11. 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 I 不支援、Phase II 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

分類	RFCs		IPv6 Ready Logo Phase I	IPv6 Ready Logo Phase II	經濟部標檢局 CNS IPv6 標準	設備需求建議		
						Host	Router	SPD
IPv6 Core								
IPv6 Core	RFC2460	Internet Protocol, Version 6 (IPv6) Specification	✓	✓	✓	M	M	
	RFC2461	Neighbor Discovery for IP Version 6 (IPv6)	✓	✓	✓	M	M	
	RFC2462	IPv6 Stateless Address Autoconfiguration	✓	✓	✓	M	M	
	RFC4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	✓	✓	✓	M	M	
	RFC2464	Transmission of IPv6 Packets over Ethernet Networks	✓	✓	✓	M	M	
	RFC1981	Path MTU Discovery for IP version 6		✓	✓	M	M	
	RFC4291	Internet Protocol Version 6 (IPv6) Addressing Architecture		✓	✓	M	M	
	RFC3697	IPv6 Flow Label Specification.				O	O	
	RFC2675	IPv6 Jumbograms			✓	O	O	
	RFC3971	Secure Neighbour Discovery				O	O	
	RFC3986	Uniform Resource Identifier (URI): Generic Syntax.				O	O	
Addressing	RFC4007	IPv6 Scoped Address Architecture				O	O	
	RFC4193	Unique Local IPv6 Unicast Address				O	O	

	RFC3879	Deprecating Site Local Addresses				O	O	
	RFC3041	Privacy Extensions for IPv6 Stateless Address Autocon fig				O	O	
	RFC3484	Default Address Selection for IPv6				O	O	
	RFC3972	Cryptographically Generated Addresses (CGA)				O	O	
	RFC3587	IPv6 Global Unicast Address Format.			✓	O	O	
	RFC3595	Textual Conventions for IPv6 Flow Label			✓	O	O	
Link	**RFC2467**	IPv6 over FDDI				O	O	
	RFC2472	IPv6 Over PPP				O	O	
	RFC2491	IPv6 over Non-Broadcast Multiple Access (NBMA) networks				O	O	
	RFC2492	IPv6 over ATM Networks				O	O	
	RFC2497	IPv6 over ARCnet				O	O	
	RFC2590	IPv6 over Frame Relay				O	O	
	RFC3146	IPv6 over IEEE 1394 Networks				O	O	
	RFC3572	IPv6 over MAPOS (SONET/SDH)				O	O	
	RFC4338	Transmission of IPv6 & IPv4 over Fibre Channel				O	O	
IPSec								
IPSec	**RFC2401**	Security Architecture for the Internet Protocol		✓		O+	O+	
	RFC2402	IP Authentication Header		✓		O+	O+	
	RFC2403	The Use of HMAC-MD5-96 within ESP and AH		✓		O+	O+	
	RFC2404	The Use of HMAC-SHA-1-96 within ESP and AH		✓		O+	O+	
	RFC2405	The ESP DES-CBC Cipher Algorithm With Explicit IV		✓		O+	O+	
	RFC2406	IP Encapsulating Security Payload (ESP)		✓		O+	O+	

	RFC2410	The NULL Encryption Algorithm and Its Use With IPsec		✓		O+	O+	
	RFC2451	The ESP CBC-Mode Cipher Algorithms		✓		O+	O+	
	RFC3566	The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec		✓		O+	O+	
	RFC3602	The AES-CBC Cipher Algorithm and Its Use with IPsec		✓		O+	O+	
Mobility								
MIPv6	**RFC3775**	Mobility support in IPv6		✓	✓	O+	O+	
	RFC3776	Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents		✓	✓	O+	O+	
	RFC4283	Mobile Node Identifier option for MIPV6				O	O	
Management								
SNMP	**RFC1157**	Simple Network Management Protocol (SNMP).				O+	O+	
	RFC3411	SNMP v3 Management Framework				O	O	
	RFC3412	SNMP Message Process and Dispatch				O	O	
	RFC3413	SNMP Applications				O	O	
	RFC3414	User-based Security Model for SNMPv3				O	O	
	RFC3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).				O+	O+	
	RFC3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).				O	O	
MIBs	**RFC2863**	The Interfaces Group MIB.				O	O	
	RFC3019	IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol				O	O	
	RFC4087	MIB for IP Tunnels				O	O	

	RFC4022	Management Information Base for the Transmission Control Protocol (TCP).				O	O	
	RFC4113	Management Information Base for the User Datagram Protocol (UDP).				O	O	
	RFC4292	IP Forwarding Table MIB.				O	O	
	RFC4293	Management Information Base for the Internet Protocol (IP).				O+	O+	
Application								
DHCP v6	**RFC3315**	Dynamic Host Config Protocol (DHCPv6)			✓	O+	O+	
	RFC3319	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers.				O	O	
	RFC3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6.				O	O	
	RFC3646	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).				O	O	
	RFC3736	Stateless DHCP Service for IPv6				O	O	
	RFC3898	Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).				O	O	
	RFC4075	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6.				O	O	
	RFC4076	Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6).				O	O	
	RFC4242	Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6 (DHCPv6).				O	O	
	RFC4477	Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues.				O	O	

	RFC4580	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option.				O	O	
	RFC4649	Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option.				O	O	
Sockets	RFC3493	Basic Socket Interface Extensions for IPv6.				O+	O+	
	RFC3542	Advanced Sockets Application Program Interface (API) for IPv6.				O	O	
	RFC4584	Extension to Sockets API for Mobile IPv6.				O	O	
RADIUS	RFC3162	RADIUS and IPv6				O+	O+	
	RFC4668	RADIUS Authentication Client MIB for IPv6.				O	O	
	RFC4669	RADIUS Authentication Server MIB for IPv6.				O	O	
	RFC4670	RADIUS Accounting Client MIB for IPv6.				O	O	
	RFC4671	RADIUS Accounting Server MIB for IPv6.				O	O	
DNSv6	RFC3596	DNS Extensions to Support IP Version 6.			✓	O+	O+	
	RFC3901	DNS IPv6 Transport Operational Guidelines				O	O	
	RFC4074	Common Misbehavior Against DNS Queries for IPv6 Addresses.				O	O	
	RFC4472	Operational Considerations and Issues with IPv6 DNS.				O	O	
SIPv6	RFC3261	SIP: Session Initiation Protocol				O+	O+	
	RFC3264	An Offer/Answer Model with Session Description Protocol				O	O	
	RFC4566	SDP: Session Description Protocol				O	O	
	RFC2671	HTTP Authentication: Basic and Digest Access Authentication				O	O	

	RFC3665	SIP Basic Call Flow Examples				O	O	
Routing								
	RFC2080	RIPng for IPv6.					O+	
	RFC2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing					O+	
	RFC2740	OSPF for IPv6					O+	
	RFC2894	Router Renumbering for IPv6					O	
	RFC4552	Authentication/Confidentiality for OSPFv3					O	
	RFC4271	BGP-4					O+	
	RFC1772	BGP Application in the Internet					O	
	RFC2858	BGP Multi-Protocol Extensions					O+	
Transition								
	RFC2765	Stateless IP/ICMP Translation Algorithm (SIIT)				O	O	
	RFC2776	Network Address Translation - Protocol Translation (NAT-PT)				O	O	
	RFC3056	Connection of IPv6 Domains via IPv4 Clouds (6to4)				O+	O+	
	RFC4213	Transition Mechanisms for IPv6 Hosts and Routers			✓	O+	O+	
	RFC2473	Generic Packet Tunneling in IPv6				O	O	
	RFC4798	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE).				O	O	
Multicast								
Multicasting	**RFC2710**	Multicast Listener Discovery (MLD) for IPv6				O	O	
	RFC2711	IPv6 Router Alert Option				O	O	
	RFC3810	MLD Version 2 for IPv6				O+	O+	

	RFC4604	Using MLDv2 for Source Specifice Multicast (SSM)				O+	O+	
	RFC3590	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol.				O	O	
	RFC4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches.				O	O	
	RFC4605	Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying").				O	O	
	RFC4601	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised).				O	O	
	RFC4602	Protocol Independent Multicast - Sparse Mode (PIM-SM) IETF Proposed Standard Requirements Analysis.				O	O	
	RFC4609	Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements.				O	O	
	RFC4610	Anycast-RP Using Protocol Independent Multicast (PIM).				O	O	
	RFC4607	Source-Specific Multicast for IP.				O	O	