108 年補助研究報告

『推動 IPv4/IPv6 雙軌普行方案』
期末報告

計畫補助機關：國家通訊傳播委員會

中華民國 108 年 12 月

108 年補助研究報告

GRB 系統編號：PG10804-0066

推動 IPv4/IPv6 雙軌普行方案

受補助單位

財團法人台灣網路資訊中心

計畫主持人

顧靜恆

研究人員

蔡更達、王彥傑、陳玟羽、許淑芳

研究期程：中華民國 108 年 01 月至 108 年 12 月

研究經費：新臺幣 694.5 萬元

中華民國 108 年 12 月

目　　次

附錄

表　次

圖　次

提　要

關鍵詞：網際網路、IPv4、IPv6、雙軌(Dual stack)

一、研究緣起

數位經濟為我國目前政策發展之關鍵重點，為有效推動我國數位經濟政策發展，行政院公布「數位國家.創新經濟發展方案」政策，因應數位創新帶來之超寬頻基礎建設與資通訊科技發展，帶來新型態數位經濟之崛起從國家策略角度預作規劃與整備。

「數位國家.創新經濟發展方案」的發展重點之一為主軸一：「數位創新基礎環境行動計畫」。本項政策目標希冀推動我國數位基磐建設發展，提昇寬頻基礎建設，其中，推動我國 IPv4/IPv6 雙軌普行使用是當前數位時代基礎建設中之重要一環。

全球提供 IPv6 連網服務趨勢近年來轉趨明顯，導入 IPv6 服務有其實質的必要性，其原因說明如下：

(一) 全球 IPv4位址已用罄，IASP 難以取得新 IPv4位址，為維持既有服務，導入 IPv6是必然的選擇。

(二) 導入 IPv6可減少 NAT 設備的投資，及減少使用 NAT 技術所產生的效能與維運障礙問題。

(三) 行動電信業者對 IP 地址需求大增。

(四) 開拓物聯網（IoT）創新業務需求。

(五) 內容網站透過 IPv6遞送比例逐年增加，此資料反應出支援 IPv6已經是世界潮流。

(六) IETF 已達成未來之新標準(RFC)皆以 IPv6為適用平台之共識，IPv6已成為未來技術主流與網路的根基。

因應國際IPv6發展潮流,世界各國皆在推動及發展 IPv6，藉由推動及完善國內 IPv6 網路環境及使用,建設台灣成為優質網路化社會的典範國家，並因應未來各項通訊傳播網路匯流科技發展之趨勢，創造台灣在國際資通訊科技競爭局勢中繼續領先之優勢，本計畫在推動我國 IPv6 發展之目標下，將包含：落實 IPv6 連網環境、強化 IPv6 連網安全及探索 IPv6 連網應用，三個方向進行。

二、研究方法及過程

為整合推動 IPv4/IPv6 雙軌普行，本計畫將具備以下三個工作項目,包括落實 IPv6 連網環境推動商用網路雙軌普行、

強化 IPv6 連網安全解析 ICP 網路安全防護平台架構，及探索 IPv6 連網應用研析物聯裝置標準及平台與應用。

(一) 落實 IPv6 連網環境推動商用網路雙軌普行

根據 107 年「我國 IPv4/v6 雙軌普行關鍵問題調查與可行解決方案研究」調查結果，本計畫將針對市售寬頻分享器和主要 IASP 連網環境規格需求探索及實際測試，以期能幫助業者掌握相關規格，提升市售設備預設開啟支援 IPv6 的可能性；擴大 IASP 業者支援 IPv4/IPv6 雙軌服務之調查，以掌握業者在支援 IPv6 網路服務的計畫，及進行 Cable 業者支援 IPv6 網路試用，為商用計畫做先行測試；並調研國際 IPv6 推動原因及經驗，以做為我國持續推動 IPv6 網路環境建置的參考。

(二) 強化 IPv6 連網安全解析 ICP 網路安全防護平台架構

國內 ICP 業者在支援 IPv6 上，因缺乏相關技術及人才，因此投入意願不高。為推展 ICP 業者提供 IPv6 網路服務的支援為目標，本計畫透過 ICP IPv4 / IPv6 平台架構雙協定網路安全防護差異解析及升級實際測試，研析 ICP 升級支援 IPv6 軟硬體設定相關資訊，強化 IPv4/IPv6 網路安全防護差異解析，並以實際輔導 ICP 業者做網站升級驗證案例，以提高相關業者投入網站升級的意願；另外開設 ICP

IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練，幫助 ICP 業者能更快速掌握 IPv4 和 IPv6 網站升級及網路安全防護平台架構的差異，及養成 IPv6 的技術團隊，幫助 ICP 業者朝向支援下一代網路服務環境前進。

(三) 探索 IPv6 連網應用研析物聯裝置標準及平台與應用

物聯網（IoT，Internet-of-Things）與 5G 等新技術的發展，相關技術及應用是近年來討論度相當高的話題，可預見未來將有更多的設備連上網路，IPv6 已經成為未來技術主流暨網路的根基。本計畫除了 IPv6 連網環境的基礎網路推動外，將研析物聯網、5G 和 IPv6 相關的技術及標準，以期能了解國內產業發展的需求，進而提升創新產業的動能為目標。計畫將透過蒐集與研析物聯網、5G 和 IPv6 相關的國際技術標準（RFC），以掌握國際標準的推展方向及進展；及物聯網平台與應用資料蒐集與研析國際 3 大物聯網平台相關資訊及應用案例，及對 IPv6 的支援狀況，以掌握物聯網的應用趨勢。

三、重要發現

(一) 今年（108 年）針對 Cable 業者所做支援 IPv6 網路服務調查，完成的 20 家業者訪談結果，以台灣寬頻通訊最

為積極，後端網路設備支援 IPv6 建置已經完成，並於今年(108 年)6 月開放用戶申請試用，成為國內第一家 MSO 支援 IPv6 業者。目前尚屬少量用戶試用階段，對業者要進入商用階段提供大量用戶使用仍須做更多試驗及評估。

(二) 國內前 3 大行動電信業者包括中華電信、台灣大哥大及遠傳電信，去年（107 年）都已經支援 IPv6 連網服務，今年（108 年）初亞太電信也開啟支援 IPv6，而台灣之星預計於明年（109 年）初支援 IPv6 網路連線，預計國內 5 家電信業者將在 109 年初完成 IPv6 啟用計畫，完成行動通信網路全面升級。

(三) 針對 IASP 的調查結果來看，5 家行動電信業者都採用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶，以因應 IPv4 不足的問題，其中台灣大哥大(部分)、亞太電信及台灣之星 3 家業者所採用的 IP 位址共用的比例達到 1:64，增加網路犯罪偵查的複雜度。

(四) 固網的使用比例不論是終端使用者或企業用戶，IPv6 的使用比例仍不高，尤其以企業用戶使用比例更低，在網

路服務供應商仍有部分服務尚未支援的情況下，要推動企業網路支援 IPv6 仍存在相當大的阻力。

(五) 推動網站業者升級 IPv6 的第一大基本要素需要 IASP 所提供的各項網路服務能夠充分支援，否則容易在前期推廣 ICP 業者進行 IPv6 升級時，即遇到網路服務無法提供的障礙。

(六) 國內 IASP 所提供的網路服務多元，大部分業者尚未完成所有服務全面支援 IPv6，國內網路的基礎服務全面支援 IPv6 仍有一段路要走。

(七) 由國際大型 IASP 業者 Verizon 推動 IPv6 的經驗調查發現，在建置新系統時選擇導入 IPv6，減少後續更新的資金及人力成本支出。而 ICP 業者 Google 的經驗指出，支援 IPv6 需要相當的時間執行建置計畫，早期投入可以有更充足的時間準備及因應。Comcast 也認為佈建 IPv6 並非技術難度高，而是需要充足時間做準備。而 Facebook 進入商業市場運作時，就已經面臨市場 IPv4 缺乏的年代，為服務全球廣大使用者，支援 IPv6 是一定要進行的計畫。

四、主要建議事項

觀察國際 IPv6 發展趨勢，從去年（107 年）開始亞洲區除了我國之外，越南、馬來西亞及泰國等國家在 IPv6 連網比例也大幅成長，可見支援 IPv6 已經是國際共識，國內經過多年的努力去年（107 年）的成長驚人，以此基礎持續推動 IPv6 普及，以提供對新一代網路標準完善支援相當重要，根據計畫執行狀況所提建議如下：

(一) 立即可行之建議

1. 推動 IASP 各項服務支援 IPv6

根據 IASP 普查結果得知，IASP 除行動網路及固網的網路連線外，業者還經營其他各項服務如 PWLAN、IDC/Co-Location、雲端服務等，業者提供的服務是否支援 IPv6，也和 IPv6 是否能普及息息相關，持續積極推動業者各項服務支援 IPv6，對提升國內 IPv6 使用率有相當助益。

2. 手機預設開啟支援 IPv6

預計於明年（109 年）初國內 5 家行動網路服務業者全部支援 IPv6，在此基礎上推動手機業者能開啟預設支援 IPv6，以提高行動網路連線 IPv6 使用率。

3. 寬頻分享器

網通商品需支援 IPv6 必要規格及測試項目，並建議政府將 IPv6 規格納入共同供應契約，確保新採購之網通設備均能支援 IPv6。建置支援 IPv6 合規的網通商品型錄資料庫及建置推廣網站，提供消費者採購相關商品的參考依據。

(二) 中長期性建議

1. ICP 網站升級支援 IPv6

ICP 網站升級支援 IPv6 和 IASP 是否支援 IPv6 網路服務息息相關，如果可以和 IASP 業者合作向其客戶進行網站升級推廣，較能接觸到有機會成功升級 IPv6 的網站業者。

2. ICP IPv4/IPv6 升級及網路安全防護差異

台灣缺乏 IPv6 推廣文章，可以邀請部落客撰寫 IPv6 推廣及介紹文章，從概念、實作、創意、安全等各種角度切入，提供更多的網路用戶參考，有助於日後 IPv6 的應用普及與發展。或將國外授權的 IPv6 文章翻譯成中文之後，在 IPv6 推廣網站進行推廣。

3. 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單

建議將檢查清單放置在網站上，例如整合於 IPv6 推廣專區網頁，若有增添修改檢查清單的項目，並能更新以保持資料的正確性。

4. 推動 ICP 支援 IPv4/IPv6 雙軌服務

ICP 業者願意配合輔導做網站 IPv6 升級，除提供 IPv4/IPv6 雙軌服務外，業者也希望能有其他的收穫如增加網站曝光度，如果能有媒體曝光機會或許能吸引更多業者加入。

Abstract

The digital economy is the focus of National policy development. Aligning with the national policy directory "Digital Nation, Smart Island," the Taiwanese government has promoted the "Digital Nation & Innovative Economic Development Program (DIGI^{+})" which is intend to accelerate Industrial Innovation and create Smart Taiwan.One of the development priorities of the 〝Digital Innovation & Governance Initiative Committee〞 is to construct a beneficial infrastructure for digital innovation. Promoting the use of IPv4/IPv6 dual-track is an important part of the current digital infrastructure.

IPv4 address resources are gradually exhausted, and the IPv6 communications protocol allows room for the internet to scale with simplicity. As the prevalence of IPv6 increases globally, the evolution of the network to IPv6 has become an international consensus. After years of development, IPv6 has gradually matured in technical capabilities, and major telecommunications operators in various countries have started IPv6 commercial operations. The introduction of IPv6 services is required for the following reasons:

1. The IPv4 address has been exhausted and it is difficult for the IASP to obtain a new IPv4 address. In order to

maintain existing services, the introduction of IPv6 is an inevitable choice.

2. The introduction of IPv6 can reduce the investment of NAT devices and reduce the performance and maintenance barriers caused by the use of NAT technology.
3. Mobile operators have increased demand for IP addresses.
4. Internet of Things (IoT) innovative business needs.
5. The proportion of content sites delivered via IPv6 has increased year by year. This information reflects that support for IPv6 has become a worldwide trend.
6. The IETF has reached a consensus to accept IPv6 as the new future standard (RFC). IPv6 has become the foundation of future technology mainstreams and networks.

Responding to the international development trend of IPv6, the program is intent to promote the development of IPv6 and targets on three goals: construct IPv6 network environment, enhance IPv6 network security, and explore IPv6 network applications.

1. Construct IPv6 network environment

   The following are the tasks that the project will focus on:

   Based on the results of last year's survey, the project will investigate and test the needs of the most popular CPE equipment on the market and whether it meets the main IASP connection network environment specifications. Help industry manufacturers develop compliance specifications and encourage manufacturers to produce the IPv6-capable CPE devices by default.

   Survey the IASP industry's support for IPv4/IPv6 dual-stack services to make the network a connection service that supports IPv6. Work with network service providers in the cable industry to advance IP6-capable network connectivity trials to prepare for commercial projects.

   Investigate the reasons and experience of international IASP and ICP to promote IPv6. Reference as a national policy to continue to promote the establishment of an IPv6-enabled network environment

2. Enhance IPv6 network security

   Due to the lack of relevant technologies and talents, ICP are not willing to invest in upgrading to support IPv6. In

order to improve the ICP industry's willingness to provide IPv6 network services, the project will study the technologies required by ICP to support the upgrade of IPv4/IPv6 dual-stack protocols, including software and hardware upgrade settings and information security upgrades. The project also runs some practical cases to help ICP upgrade the site. It validates the functionality of the technical documentation and encourages more ICP to participate in IPv6-enabled connection upgrades.

In addition, the project will host some training courses on the ICP upgrade website to support the IPv4 / IPv6 dual-stack protocol connection network. The goal is to help ICP quickly understand the differences between IPv4 and IPv6 website architectures and to form an IPv6 technology development team.

3. Explore IPv6 network applications

   In addition to improving the network infrastructure to support IPv6 connectivity, the project will also examine technologies and standards related to the Internet of Things, 5G and IPv6 to understand the needs of domestic industrial development and further enhance innovation capabilities.

It will collect and analyze the Internet of Things, 5G and IPv6 related international technical standards (RFC) to grasp the direction and progress of international standards. It also collects innovative application cases based on the world's top three IoT platforms and investigates whether they support IPv6 connectivity.

This year, we surveyed 20 Cable operators to check if they have the ability to support IPv6 network services. Among them, TBC is the most active, and has completed support for IPv6 back-end network devices. In June of this year, TBC invited users to apply for trials and became the first MSO to support IPv6 network connections. Currently, users are required to apply for IPv6 network services for a small number of users to try, and TBC still needs more trials and evaluations to enter the commercial stage to provide a large number of users to obtain IPv6 connectivity services.

Last year, Chunghwa Telecom, Taiwan Mobile and FETnet have supported IPv6 network services. Since the beginning of this year, Asia Pacific Telecom has also begun to support IPv6, and TStar Telecom is expected to support IPv6 network connectivity by March 2020. It is expected that by next year, five mobile telecom operators will complete the IPv6

enablement plan and complete the comprehensive upgrade of the mobile communication network.

Due to the shortage of IPv4, some mobile operators have adopted an IP address sharing ratio of 1:64, which increases the complexity of cybercrime investigation.

The fixed network usage of end users or enterprise users with IPv6 functionality is still low, especially for enterprise users.If your network service provider still has some devices or services that are not yet supported, you will not be able to obtain an IPv6 network connection for end users or enterprise services.

The network services provided by IASP are diverse, and most operators have not completed all services to fully support IPv6. There is still a long way to go to fully support IPv6 in basic services.

A survey of IPv6 by Verizon found that introducing IPv6 when building a new system can reduce the capital and labor costs of subsequent updates. Google's experience points out that supporting IPv6 requires a lot of time to implement the construction plan, and early investment can have more time to prepare. Comcast has the same comment and experience as Google. As to Facebook, when it was founded, the shortage of IPv4 became more serious and IPv6 was steadily developing.

Therefore, Facebook had no choice but adopting IPv6. Enterprises adopting new technologies need to consider productivity、investment、competitiveness and user experience. From the experiences of Verizon、Comcast、Google and Facebook, IPv6 is obviously very helpful to them and it supports the Networking industry well.

第一章 計畫執行狀況與檢討

第一節 計畫執行內容說明

一、 背景分析

數位經濟為我國目前政策發展之關鍵重點，為有效推動我國數位經濟政策發展，行政院公布「數位國家.創新經濟發展方案」政策，因應數位創新帶來之超寬頻基礎建設與資通訊科技發展，帶來新型態數位經濟之崛起從國家策略角度預作規劃與整備。

「數位國家.創新經濟發展方案」的發展重點之一為主軸一：「數位創新基礎環境行動計畫」。本項政策目標希冀推動我國數位基磐建設發展，提昇寬頻基礎建設，其中，推動我國 IPv4/IPv6 雙軌普行使用是當前數位時代基礎建設中之重要一環。

全球提供 IPv6 連網服務趨勢近年來轉趨明顯，導入 IPv6 服務有其實質的必要性，其原因說明如下[1] ：

(一) IPv4位址枯竭：全球 IPv4位址已用罄，IASP 難以取得新 IPv4 位址，為維持既有服務，導入 IPv6是必然的選擇。

(二) 解決 NAT 的問題：導入 IPv6可減少 NAT 設備的投資，僅提供 IPv4網路服務需持續更新 NAT 等設備，反而增加 IASP 之支出。且使用 NAT 技術會有效能與維運障礙問題，增加 IASP 人力的負擔。

(三) 行動網路發展需求：行動電信業者對 IP 地址需求大增，近年

來因智慧型手機及平板電腦等行動式裝置快速增加，而行動式裝置所具備的基本特性為隨時在線（always-on）及上網時間長，要同時提供大量的行動式裝置上網，就必須有足量的 IP 才能提供相對應的服務，以滿足客戶的需求。

(四) 開拓物聯網（IoT）創新業務：因應新產業創新服務需求，為建立物聯網創新服務之通訊環境，需符合物聯網裝置的特性，包含高安全性、高移動性、隨插即用、IP 隨時在線等，產業 IP 需求將隨著服務之擴張而增加。物聯網的發展勢必增加對 IP 的需求，若不提前布局支援 IPv6，可能失去下一代網路應用發展的先機。

(五) 內容網站透過 IPv6遞送比例逐年增加：根據 Alexa 量測統計資料顯示，全球前1,000大流量網站，到107年已經有28%網站內容可透過 IPv6遞送，相較106年的23%網站內容可透過 IPv6遞送，又增加5%的網站業者支援 IPv6連結，此資料反應出支援 IPv6已經是世界潮流，為了符合我國推動數位經濟的願景，建全的 IPv6連網環境乃是數位經濟的基礎，因此佔有相當的重要性。

(六) IETF 已達成未來之新標準(RFC)皆以 IPv6為適用平台之共識，IPv6已成為未來技術主流與網路的根基。

因應國際 IPv6 發展潮流，世界各國皆在推動及發展 IPv6，藉由推動及完善國內 IPv6 網路環境及使用，建設台灣成為優質網路化社會的典範國家，並因應未來各項通訊傳播網路匯流科技發展之趨勢，創造台灣在國際資通訊科技競爭局勢中繼續領先之優勢，本計畫在推動

我國 IPv6 發展之目標下，將包含：落實 IPv6 連網環境、強化 IPv6 連網安全及探索 IPv6 連網應用，三個方向進行。

為整合推動 IPv4/IPv6 雙軌普行，本計畫將具備以下三個工作項目，包括落實 IPv6 連網環境推動商用網路雙軌普行、強化 IPv6 連網安全解析 ICP 網路安全防護平台架構，及探索 IPv6 連網應用研析物聯裝置標準及平台與應用。下圖所示為本計畫進行 IPv4/IPv6 雙軌普行推動方向：

圖 1、IPv4/IPv6 雙軌普行推動方向

本計畫藉由持續普查連網全路徑上各連網環節 IPv6 支援情形及遭遇之困難，解析 ICP 網路安全防護平台架構，並研析物聯裝置標準及平台與應用，以確保我國數位通訊傳播基礎建設發展及國人數位資訊流通或普用與世界先進國家同步，促進國內數位經濟發展。

(一) 商用網路雙軌普行發展

由於全球 IPv4 位址已用罄，網際網路接取服務業者（Internet Access Service Provider，IASP）難以取得新 IPv4 位址，國際目前

IPv6 之使用率以 IPv6 瀏覽 Google 網站之用戶佔比在西元 2018 年（107 年）底已經達到將近 27%，預估西元 2019 年（108 年）將達到 34%，表示 IPv6 之國際生態系已經趨於健全；而隨著網路應用蓬勃發展，僅提供 IPv4 網路服務，將限制 IASP 之業務擴張的可能性。

台灣在 106 年底 IPv6 使用者比例僅 0.38%，排名全球第 67，至 107 年 12 月已經達到約 29%，全球排名躍升至第 6 名，成長速度於 107 年度創下世界第一。成長主因為中華電信固網和行動網路的接取服務於 107 年起已經對用戶預設開通支援 IPv6，遠傳電信和台灣大哥大行動網路於 107 年下半年起對於用戶也採取逐步開通 IPv6 網路服務，台灣主要大型 IASP 業者對用戶提供 IPv6 服務，對我國 IPv6 連網的使用比例有很大的提升。除了 3 家主要 IASP 業者預設開通 IPv6 服務之外，尚有 Cable 業者和部分行動網路 IASP 尚未開通 IPv6 服務，針對這些業者進行訪談調查，以了解其推動時程規劃和所遭遇的困難，為後續推動 IPv6 普及工作之重點項目之一。

此外，根據 106 年市售網通產品的市場調查結果發現，目前銷售前 20 名的網通商品，主要以寬頻分享器為主，由調查結果發現國內所銷售的寬頻分享器，在 IPv6 的支援比例上尚未過半，其主要原因是網通商品具有產品週期長的特性，市面上仍有多項舊款產品為熱門商品，而舊款產品具備支援 IPv6 功能的商品較少，因此拉低了整體支援 IPv6 的比例。

部分市售網通產品雖然於規格中宣稱支援 IPv6，但一般消費者在購買安裝後，是否能順利連通為我們關切的議題。經過挑選部分熱銷產品進行實際測試之後，發現部分產品雖然宣稱支援 IPv6，

但和中華電信採用 PPPoE 規格不合，IPv6 依然無法連通；另外統計商品是否預設開啟設定支援 IPv6，目前只有 D-Link(友訊) 一個廠牌所生產的商品可達到預設支援，這對一般消費者實際能使用到支援 IPv6 網路的比例變得更低，除需要更積極的協調業者於市售產品中支援 IPv6，並需與 IASP 之 IPv6 服務介接進行實際測試，將結果反應給網通產品業者，亦是現階段推動 IPv4/IPv6 雙軌普及的重要工作。

本項工作將依 107 年研究結果，針對問題推行解決方案，並依實際成效調整，以持續推動我國連網環境達到 IPv4/IPv6 雙軌普行的目標。

(二) ICP 網路安全防護平台架構

107 年執行 IPv4/IPv6 雙軌普行研究調查顯示，普行障礙主要關鍵瓶頸包括網路接取服務(IASP)、網路內容應用服務(ICP)及網通產品等 3 方面。為建立完整 IPv6 生態系，以創造發展網路應用服務之基礎，推動台灣 ICP 業者啟用 IPv6 服務是重要的工作環節之一。

針對台灣 ICP 業者啟用 IPv6 服務的比例尚低，並且在三項關鍵瓶頸中對 IPv6 的支援比例最低，經由 Alexa 的統計資料得知台灣民眾最常瀏覽的前 100 大網站，調查其使用 IP 屬於台灣申請取得的有 27 家，經測試後發現已支援 IPv6 連線服務之 ICP 只有 6 家，支援 IPv6 比例為 22.2%。另外由於 ICP 網站多架設於 IDC，經查此 27 家 ICP 網站是分別架設於 7 家不同 IDC 業者，包括國家發展委員會的 GSN，以及 6 家民營業者。經調查 GSN 及其中 5 家民營業者已經對其 ICP 客戶提供 IPv6 服務，由此得知 IDC 業者支援

IPv6 整備完成的比例相當高。因此 ICP 業者在 IPv6 支援程度低的關鍵問題，主要在於 ICP 業者的支援意願及業者本身技術和維運上的考量。

107 年執行 IPv4/IPv6 雙軌普行研究案調查前，台灣 IASP 對 IPv6 服務的支援與提供，一直還是停留在觀望試用期，真正的商用計畫一直未真正實現，因此台灣 ICP 業者多認為台灣環境並未成熟，且以目前大多數 ICP 業者並未有 IPv4 缺乏的狀況，因此對啟動 IPv6 的需求更無法感受其必要性。但在 107 年計畫執行推動期間，中華電信固網及台灣 3 大行動電信業者，陸續啟動 IPv6 連網服務，台灣 107 年更名列全球 IPv6 連網成長率的第一名，因此透過對 ICP 業者問卷調查及面訪機會，對業者傳達台灣 IPv6 的發展狀況及進展，有 ICP 業者在 107 年中華電信開通 IPv6 連網服務後，也開始提供 IPv6 連網服務；其他的 21 家 ICP 業者中，部分業者在訪談過後，也已經和 IDC 詢問相關訊息並開始進行規劃。

107 年在 ICP 業者不提供 IPv6 服務的困難點調查中發現，有 ICP 業者提出是因業者本身建置維運及網路管理的技術能力或人力不足，且 IPv6 網路安全防護設定和 IPv4 不同，支援 IPv4/IPv6 雙軌並行，形成業者對網路安全問題上的疑慮。因此幫助 ICP 業者做 IPv4/IPv6 雙協定網路安全防護平台架構分析，建立其 IPv6 相關技術能力，培育技術人才，將可降低業者所需投入心力，增加業者投入的意願。

(三) 物聯裝置標準及平台與應用發展

物聯網（IoT，Internet-of-Things）、5G 等新技術的發展，持續朝向萬物聯網的方向推進，未來將有更多的設備連上網路，因此

也對 IP 位址之需求持續增加。IETF 已達成未來之新標準(RFC)皆以 IPv6 為適用平台之共識,IPv6 已成未來技術主流暨網路的根基。除了 IPv6 連網環境的基礎網路推動計畫外，如何創新為下一代的網路新產業鋪路，對國家未來經濟發展至關重要，為蓄積技術能量加強創新產業連結，及對新技術與應用的瞭解及掌握，持續對物聯網、5G 與 IPv6 相關的技術有更深入的了解，政府應扮演國內物聯網、5G 和 IPv6 產業之統合協調與推動的角色，引領國內產業的發展，提升創新產業的動能，創造對 IPv6 新一代網路的需求，同時開拓出 IPv6 的產業價值鏈,提昇業者進行網路升級 IPv6 之意願，協助突破國內 IPv6 推動的困境。為對物聯網、5G 與 IPv6 相關的技術及平台與應用有更深入的了解,並掌握技術的發展動向，本計畫透過蒐集及研析相關 RFC 和參與相關國際技術與應用會議及展覽，以強化技術能量，充分掌握技術及產業發展的脈動。

二、 計畫動機及主題

下圖所示為推動 IPv4/IPv6 雙軌普行方案計畫工作架構，以下將就各分項說明：

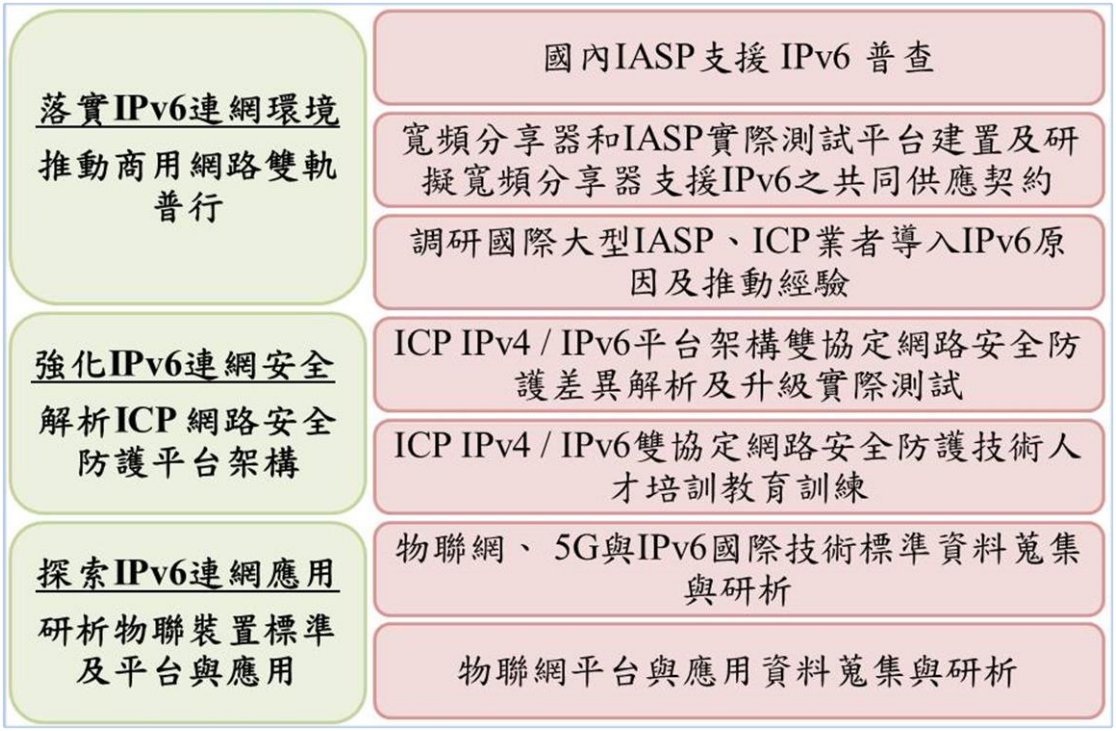

圖 2、推動 IPv4/IPv6 雙軌普行方案工作架構

(一) 落實 IPv6 連網環境推動商用網路雙軌普行

本分項計畫為國家通訊傳播委員會 107 年度「我國 IPv4/IPv6 雙軌普行關鍵問題調查與可行解決方案研究計畫」之延續推動計畫。根據前項研究成果，包括：

1. 依據 WiFi AP、WiFi adaptor、寬頻分享器、路由器、L3 Switch、Home Gateway 等市售前 20 名網通產品市場銷售資訊及支援 IPv6 和 PPPoE 的狀況調查。銷售前 20 名的商品主要為兩大類，第一類為寬頻分享器，第二類為 WiFi adaptor（無線網路

卡)，其中寬頻分享器和連網環境是否設定支援 IPv6 相關。由 107 度計畫調查結果得知國內市售網通商品中的寬頻分享器，支援 IPv6 的比例仍低。

2. 依據國內市場銷售量前 3 名之手機和平板電腦廠牌，及其支援 IPv6 狀況調查，得知國內市售手機和平板電腦，支援 IPv6 的比例高。

3. 依據固網及行動網路 IASP 整備程度、IPv6 連通狀況及相關設定、以及國內 IPv6 使用比例及成長趨勢調查，得知 3 大行動網路業者於 107 年陸續提供 IPv6 網路連線商業運轉服務。

4. 依據臺灣主要網站業者支援 IPv6 情形，及業者相關規劃，了解主要網站業者支援 IPv6 之意願及所遭遇的困難。得知 IDC 提供 IPv6 網路服務的比例整備程度高，但 ICP 提供 IPv6 網路連線服務的支援程度低。

依據 107 年 IPv4/IPv6 雙軌普行關鍵問題之研究結果，IASP 開通 IPv6 服務，對 IPv6 的使用比例具有關鍵性的影響，108 年研究計畫將依 107 年研究結果，針對關鍵問題推行解決方案，並依實際成效調整。

關鍵問題解決方案之推動，將針對使用者設備、及擴大 IASP 業者支援 IPv4/IPv6 雙軌服務之調查，以充分掌握業者的規劃進度，並提升我國之 IPv6 使用率與國際同步，朝向建立我國 IPv6 完整生態系之目標。

根據 107 年調查結果，網通商品寬頻分享器能預設開啟支援 IPv4/IPv6，且符合 PPPoEv4/v6 並採用單一帳號密碼的產品比例不高，寬頻分享器業者反映，因缺乏各 IASP 所採用的數據機(Modem)，無法建立完整的實際測試平台，缺乏驗證機制，以確認商品合乎消費市場需求，因此業者不願意採取主動預設開啟 IPv6 連網的機制。因此本計畫延續 107 年的調查結果，目標在協助業者建立相關環境，供業者實際測試商品是否符合 IASP 規格，幫助消除寬頻分享器業者的擔憂，提高業者在國內市場銷售商品能預設開啟支援 IPv6 連網的機制。

綜合以上 107 年的調查結論，為持續推動我國 IPv4/IPv6 雙軌普行連網服務，本分項之研究主題包括：

1. 國內 IASP 支援 IPv6 普查：

由於 107 年計畫對於國內 IASP 支援 IPv6 的調查，只針對國內 3 大行動業者及中華電信固網服務進行調查，108 年將擴大進行調查，針對 IASP 所經營的不同業務，依業者現有之 IPv6 位址使用情境，分為固網、行動網路、公眾無線區域網路（Public Wireless Local Area Network，PWLAN）、有線電視（Cable）、網路數據中心（Internet Data Center，IDC）、及雲端機房等類別，對業者支援 IPv6 之整備狀況，進行普查，以掌握我國 IPv6 之網路基礎環境建置現況。除了 IPv6 的整備狀況調查外，同時將針對有提供網域名稱快取伺服器（DNS cache server）之 IASP 業者對 DNSSEC 的準備情況進行調查，以對業者在網路資訊安全防護的認證機制採行狀況進行了解。

2. 寬頻分享器和 IASP 實際測試平台建置及研擬寬頻分享器支援 IPv6 之共同供應契約：

整理網通商品之寬頻分享器支援 IPv6 並符合 PPPoE 的規範，以及建立寬頻分享器符合支援 IPv6 規範標準測試項目及驗證環境，透過寬頻分享器和 IASP 實際測試平台，使業者有依循準則及驗證環境，並進一步建議政府將符合支援 IPv6 規範及標準項目納入共同供應契約，提升業者生產銷售支援 IPv6，並預設開啟支援 IPv6 的設備商品之意願。

3. 調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗：

除了推動國內 IPv4/IPv6 普行工作項目之外，將透過調查研究國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗，以了解國際推動 IPv6 普及的動力及建置過程，作為國內推動 IPv4/IPv6 雙軌連網服務普及的參考。

(二) 強化 IPv6 連網安全解析 ICP 網路安全防護平台架構

由 107 的調查結果顯示，目前 ICP 業者對支援 IPv6 的意願不高主要的原因可歸納如下：

1. 缺乏支援 IPv6 的誘因：目前 ICP 業者的 IPv4 位址充足，且投入建置支援 IPv6 並無法增加相對應的收入。

2. 開發部門人力不足，且缺乏熟悉網路 IPv6 建置的技術人才。

3. IPv4 和 IPv6 網路通訊協定並不相容，過渡時期必須同時支援 IPv4 及 IPv6 系統共存，對 ICP 業者而言，增加網路系統管理

的複雜度，擔心網站連線不通，網頁內容無法顯示，網站回應速度變慢等可能風險，且 IPv6 網路安全防護設定不同於 IPv4，業者擔心網站遭受攻擊，危及網站營運的穩定度。

國內 ICP 業者在支援 IPv6 上，因缺乏相關技術及人才，因此投入意願不高。為推展 ICP 業者對使用者提供 IPv6 網路服務的支援，以期增加支援 IPv4/IPv6 之應用網站為目標，如果能提升業者在建置 IPv6 網路服務上的相關技術能量，縮短業者投入的時程，才能提高其投入建置支援 IPv6 的意願。因此本計畫以透過網路安全防護平台架構研析，及技術人才培育的方法，幫助 ICP 業者能更快速掌握 IPv4 和 IPv6 網路安全防護平台架構的差異，及養成 IPv6 的技術團隊，幫助 ICP 業者朝向支援下一代網路服務環境前進。

綜合以上所描述的計畫推展目標，因此將本分項之研究內容分為以下主題，包括：

1. ICP IPv4/IPv6 平台架構雙協定網路安全防護差異解析及升級實際測試：

   因應 ICP 業者支援 IPv6 疑慮，分析 IPv4 及 IPv6 網路雙協定平台在安全架構設計上的差異，建立 IPv4/IPv6 平台架構雙協定網路安全手冊及檢查項目清單，能快速完成基礎檢測項目，降低 ICP 業者支援 IPv6 的阻力及縮短業者摸索的過程。並實際輔導 ICP 業者做網站支援 IPv4/IPv6 雙軌網路服務升級，以提供相關業者做為參考案例。

2. ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練：

透過提供 ICP 業者技術人才培訓課程及技術研討的方式，幫助業者快速累積相關技術及人才培育，並建立國內 IPv6 所需的技術人才庫，達到資源共享，以幫助業者減少需要投入的人力及資源，提高業者支援 IPv6 的意願。

(三) 探索 IPv6 連網應用研析物聯裝置標準及平台與應用

為了解物聯網、5G 與 IPv6 相關的技術、以及平台與應用的發展動向，透過收集及研析相關 RFC 和參與國際相關技術與應用會議，以充分掌握技術及產業發展的脈動。因此，本分項之研究主題包括：

1. 物聯網、5G 與 IPv6 國際技術標準資料蒐集與研析：

收集及研析物聯網、5G 與 IPv6 相關的國際技術標準(RFC)，以掌握國際標準的推展方向及進展等資訊。

2. 物聯網平台與應用資料蒐集與研析：

蒐集及研析國際 3 大物聯網平台相關資訊及技術發展情況，解析物聯網平台的架構及國內外相關應用發展趨勢，以及調查各大物聯網平台對 IPv6 的支援狀況。

三、 工作架構與施行方法

依據計畫目標，本計畫架構將包含以下三個分項：

- 分項一：推動商用網路雙軌普行；
- 分項二：解析 ICP 網路安全防護平台架構；
- 分項三：研析物聯裝置標準及平台與應用。

以下將就計畫執行內容，依照各分項工作架構與施行方法說明。

(一) 分項一：推動商用網路雙軌普行

本分項計畫為接續 107 年調查結果，持續推動更多的業者加入支援 IPv6 連網服務的行列，透過擴大 IASP 支援 IPv6 的調查、訂定寬頻分享器商品符合支援 IPv6 的規範和標準測試項目、及調研國際 IASP、ICP 業者導入 IPv6 原因及推動經驗等方面，朝向推動增加支援 IPv4/IPv6 雙軌連網服務之 IASP 業者，及使用者設備普遍支援 IPv6 連網功能的方向前進，以期能達到提高國人 IPv6 連網比例的目標前進。下圖為推動商用網路雙軌普行工作項目，以下將就分項工作說明：

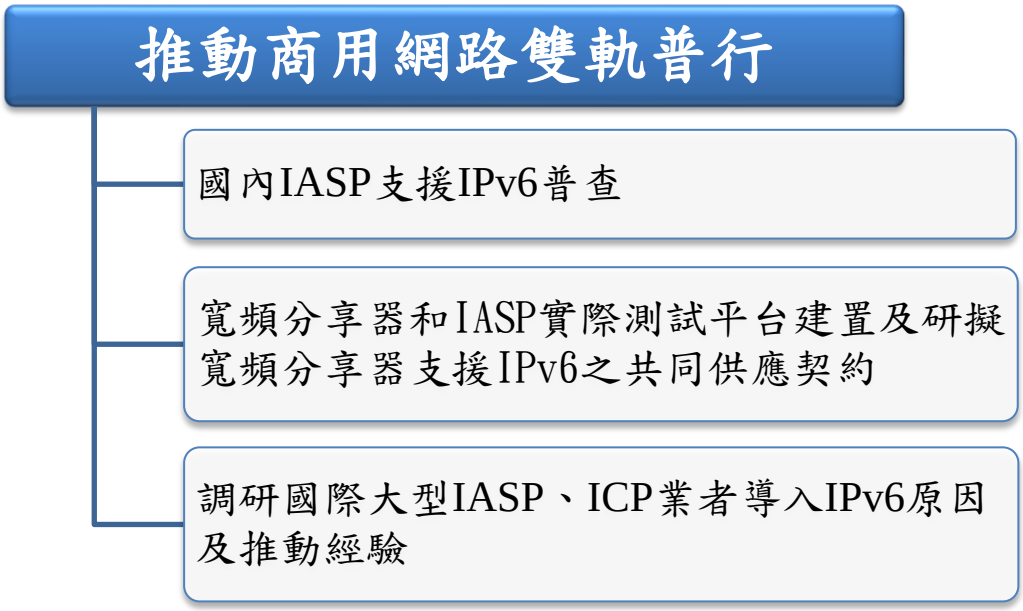

圖 3、商用網路雙軌普行推動工作項目

1. 國內 IASP 支援 IPv6 普查

國內 IASP 支援 IPv6 的普查工作項目，根據業者 IPv6 位址使用情境，將依固網（如動態分配用、固定用戶種類別）、行動網路、公眾無線區域網路（Public Wireless Local Area Network，PWLAN）、有線電視（Cable）、網路數據中心（Internet Data Center，IDC）、及雲端機房等類別進行調查。

IASP 支援 IPv6 調查工作主要是採用問卷調查，並輔以面訪方式進行。此項工作的重點為，針對國內 IASP 業者，調查其在 IPv6 的整備現況及預定商轉的計畫。

問卷調查法是研究團隊運用統一設計的問卷向被選取的調查對象瞭解情況或徵詢意見的調查方法。此調查的目的為詢問 IASP 業者關於各種網路服務支援 IPv6 的準備情形及時程，及該服務之設備支援 IPv6 之程度。除此之外並將安排對業者進行面訪，以期能更深入了解業者的想法、及所遭遇的困難，並可藉此

機會做雙向溝通，收集更多資訊以做為政策研擬的參考。

除了對 IPv6 連網服務的調查外，本計畫也將對有建置網域名稱快取伺服器（DNS Cache Server）的 IASP 業者，調查其在啟用 DNSSEC 驗證的準備情形，以了解國內網路安全防護的佈建狀況，並加強業者對資訊安全的重視。

另外針對 Cable 業者的部分，在本計畫執行中希望能從問卷及面訪調查結果中，找出在 IPv6 設備建置狀況較佳的業者中，選定至少 1 個合作對象，輔導其進行 IPv4/IPv6 雙軌連網服務的試用，透過先期試用的測試，收集 Cable 網路服務支援 IPv6 連網可能遭遇的問題，為商用計畫開通 IPv6 連網服務預先打下基礎。

本項計畫內容除 IASP 調查之外，亦將開發一個手機設定 IPv6 之 APP，並設置 IPv6 推廣專區網站，透過調查及推廣二方面，持續推動國內 IPv6 網路服務的普及。

依據上列所述將國內 IASP 支援 IPv6 普查工作分為 5 個子項目，下圖顯示此項工作下各分項內容，及各子項目工作執行程序：

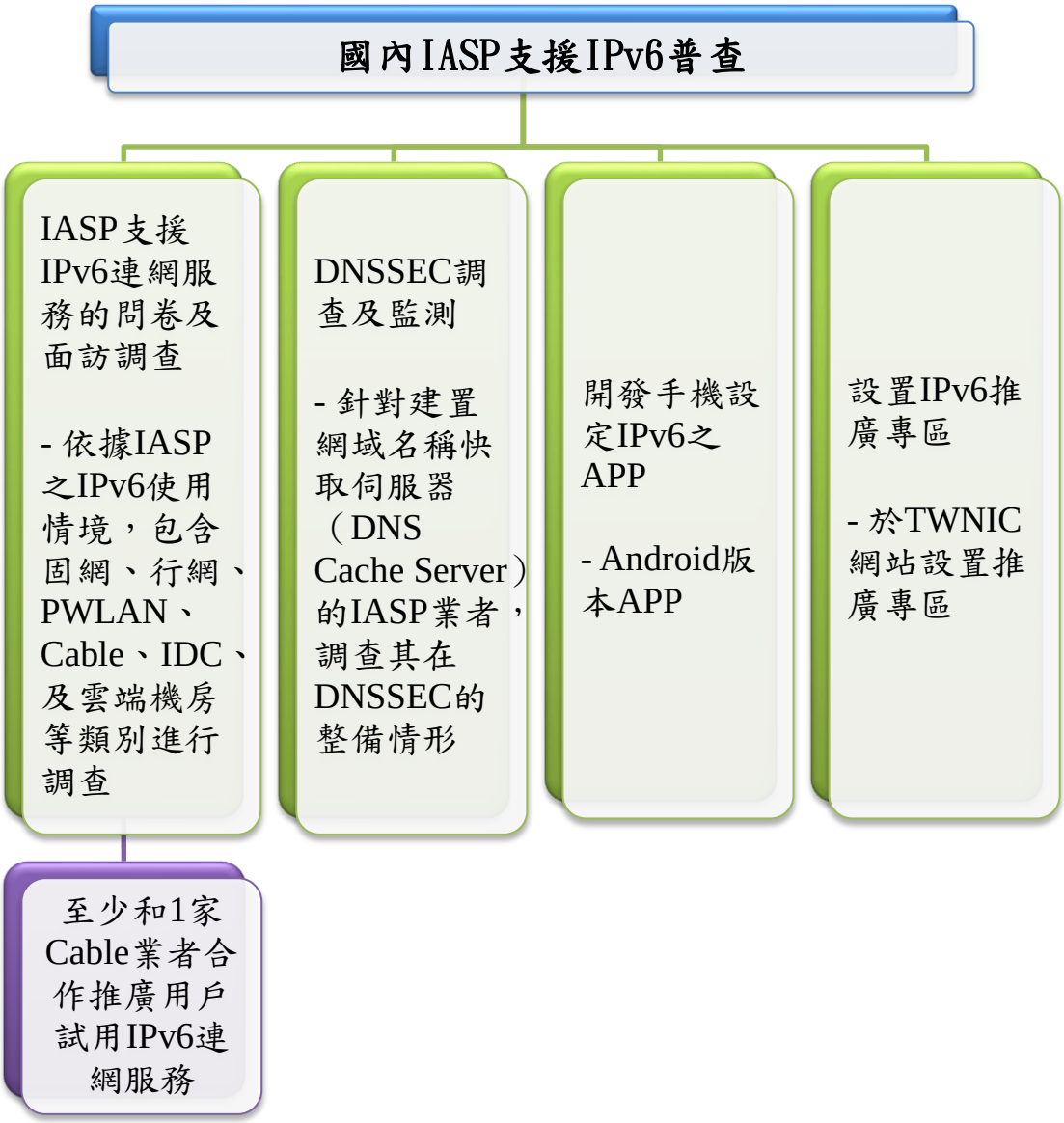

圖 4、國內 IASP 支援 IPv6 普查工作項目與執行程序

以下將就本工作項目下的各別子項目，其所採用的施行方法及步驟分項說明如下：

(1) 國內 IASP 支援 IPv6 問卷及面訪調查：

國內 IASP 支援 IPv4/IPv6 雙軌連網服務整備程度調查，將以問卷及面訪兩方向進行，調查 IASP 關於各種網路服務支援 IPv6 程度及時程，及該服務設備支援 IPv6 之程度。除問卷調查外，另輔以面訪方式以期能更了解業者的想法及規畫。

針對 Cable 業者的調查，本計畫預計調查的 Cable 業者對象為 TWNIC IP 會員共 20 家；根據 NCC 統計國內有線電視業者家數，共有 5 家 MSO，分別為凱擘寬頻（旗下 12 家有線電視）、中嘉寬頻（旗下 11 家有線電視）、台灣數位光訊（旗下 6 家有線電視）、台固媒體（旗下 5 家有線電視）及台灣寬頻（旗下 4 家有線電視）；及 27 家獨立系統業者。此次調查對象將包含 5 家 MSO 及 15 家獨立系統業者。針對行動電信業者的調查，去年（107 年）中華電信、遠傳電信及台灣大哥大都已經陸續推出 IPv6 網路服務，108 年的調查對象將納入國內另外 2 家行動通信業者亞太電信及台灣之星，以掌握國內所有行動電信業者在提供用戶 IPv6 網路服務的計畫。

下圖為國內 IASP 業者支援 IPv6 網路服務及開啟 DNSSEC 驗證調查流程：

圖 5、國內 IASP 業者支援 IPv6 及開啟 DNSSEC 驗證之調查流程

(2) DNSSEC 調查及監測：

因應 DNS Cache Poisoning(DNS 快取中毒)的安全漏洞，引發全球對於 DNS 安全問題的高度重視，並且加速 DNSSEC（DNS Security Extensions，DNS 安全協議）的發展推動，且近年來雲端服務的快速成長，DNS 安全威脅的風險程度也隨之升高，為掌握業者的連網環境安全性的佈建狀況，因此將調查內容擴大，對於有建置 DNS Cache Server 的 IASP 業者，將涵蓋業者在開啟 DNSSEC 驗證機制的支援狀況調查。執行方式將以問卷調查進行，執行步驟如上圖所示。

(3) 至少和 1 家 Cable 業者合作推廣用戶試用 IPv6 連網服務。

計畫將由訪查的 Cable 業者中，至少找出 1 家業者共同合作進行用戶 IPv6 網路服務試用測試，累積經驗作為後續推廣的基礎。

下圖所示為 Cable 業者推廣 IPv6 網路服務試用的流程及施行步驟：

圖 6、和 Cable 業者推廣 IPv6 試用流程

(4) 開發手機設定 IPv6 之 APP：

開發手機設定 IPv6 之 Android 版本 APP，讓使用者安裝於手機內可以簡易方式開啟 IPv6 連網設定。

(5) 設置 IPv6 推廣專區：

於中心網站增加專區網頁，放置終端設備支援 IPv6 資訊、終端設備改用 IPv6 之設定方法、IASP 之 IPv6 申請及設定方法、IASP 之 IPv6 支援情形、手機設定 APP 等資訊。

2. 寬頻分享器和 IASP 實際測試平台建置及研擬寬頻分享器支援 IPv6 之共同供應契約：

寬頻分享器符合 IASP 的網路服務支援 IPv6 規範及標準測試項目的制定，需透過向 IASP 收集相關規格的要求，並依照規格以訂定所需的標準測試項目。而實際測試平台之建置，需選定相

對應的測試設備，再輔以所制定測試項目，才能建置完備的寬頻分享器的驗證環境。

下圖為寬頻分享器和 IASP 實際測試平台之建置及研擬支援 IPv6 共同供應契約工作項目，及工作執行程序：

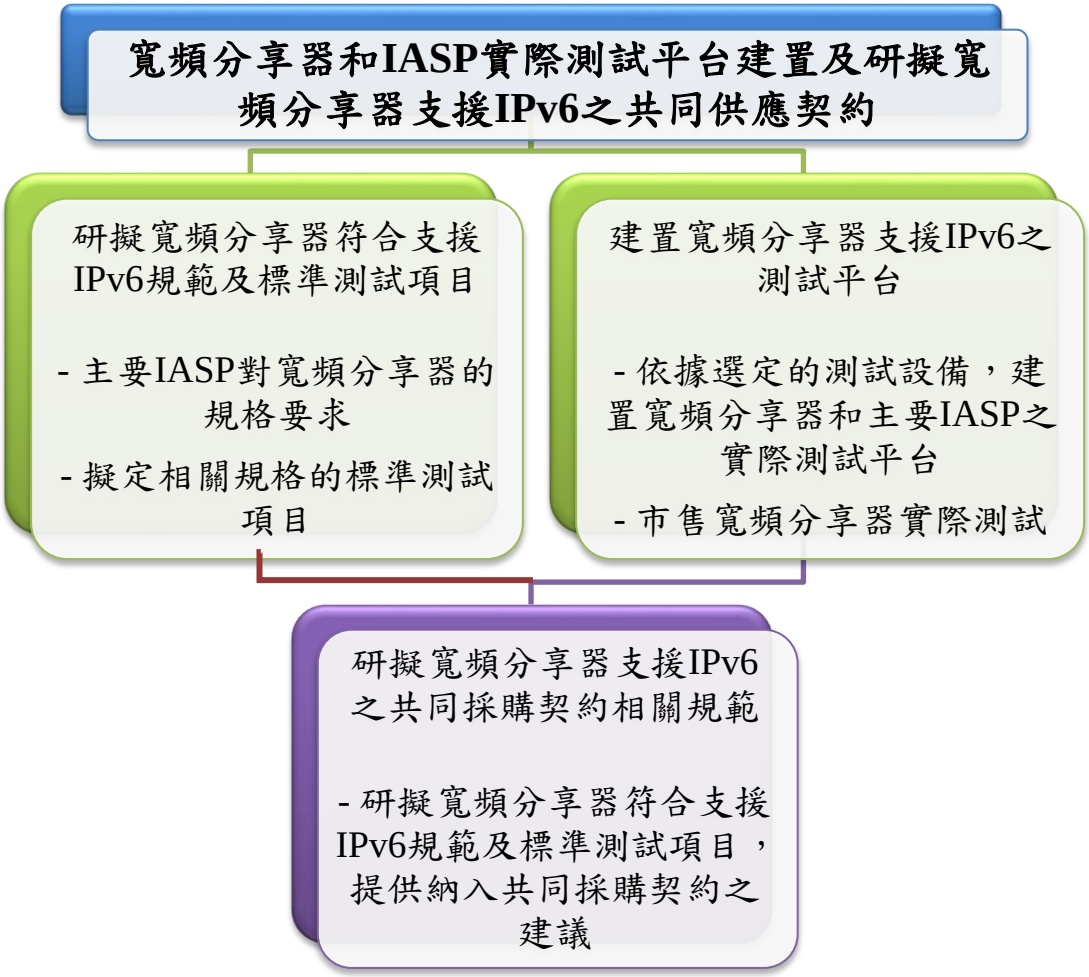

圖 7、寬頻分享器和 IASP 實際測試平台之建置及研擬支援 IPv6 共同供應契約工作項目與執行程序

針對寬頻分享器和 IASP 實際測試平台建置及研擬寬頻分享器支援 IPv6 之共同供應契約的工作項目說明如下：

(1) 研擬寬頻分享器符合支援 IPv6 規範及標準測試項目：

針對主要 IASP，收集其對用戶端所採用的寬頻分享器（WiFi Router）的規格要求，並擬定相關規格的測試項目，以製作寬頻分享器符合支援 IPv6 規範及標準測試項目。

(2) 建置寬頻分享器支援 IPv6 之測試平台：

調查主要 IASP 目前主力的家用數據機規格，並選定至少一項產品做為測試用標準設備，以做為測試平台的驗證基準。依據所選定的測試設備，建置寬頻分享器（WiFi Router）和主要 IASP 之實際測試平台，以建立寬頻分享器的驗證環境。

本計畫將針對中華電信固網支援 IPv6 PPPoE 連網環境做測試。實際測試產品將以製造日期為西元 2018 年（107 年）(含)後之 IPv6 寬頻分享器至少 10 款，須包含友訊、華碩、TP-Link、及 TOTOLINK 等至少 4 個品牌，所製造生產的寬頻分享器商品每家至少 2 款，並整理測試報告。針對通過測試的商品，將建議寬頻分享器品牌業者，未來所生產製造寬頻分享器，於國內銷售的商品都能預設開啟支援 IPv6，以逐步提升國內 IPv6 連網比例。

本計畫執行期間預計將協助至少 1 家 Cable 業者導入 IPv6 網路服務試用，若經測試升級穩定，預計將升級導入 IPv6 網路服務的 Cable 業者連網環境納入實際測試平台。

(3) 研擬寬頻分享器支援 IPv6 之共同採購契約相關規範：

根據以上二個分項工作所研擬的規範及標準測試項目，及支援 IPv6 之測試平台規格，彙整為商品符合支援 IPv6 規範

的技術要求及測試項目，提供詳細相關產品採購規格，建議政府將規範納入共同採購契約之規格項目，讓對於有意投入政府採購標案的業者，有清楚的規範可以依循。

3. 調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗：

透過研究及調查國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗，作為我國推動 IPv4/IPv6 雙軌普行政策的參考依據。

下圖為調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗工作項目，及工作執行程序：

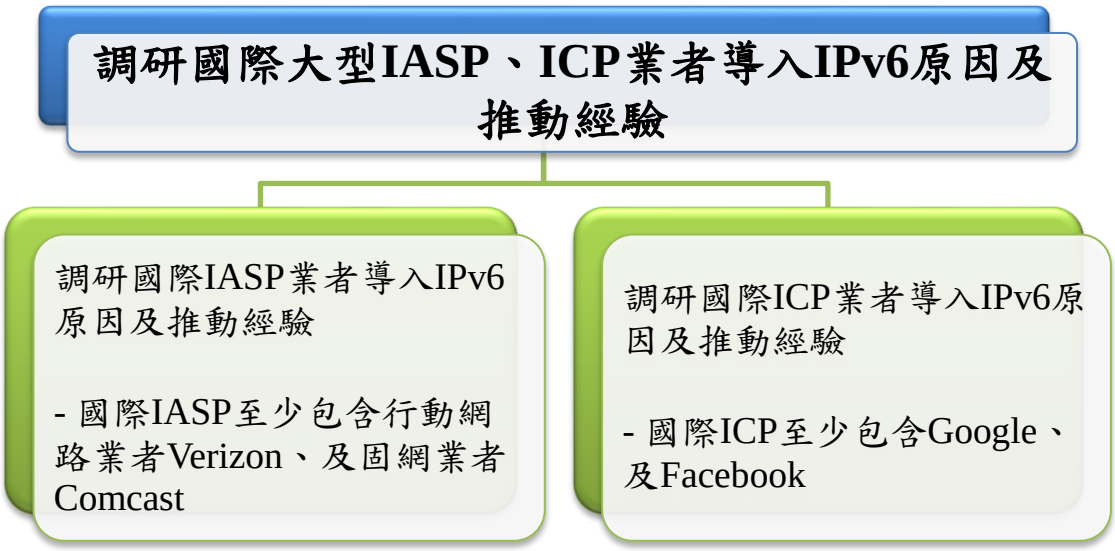

圖 8、調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗工作項目與執行程序

針對調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗的工作項目說明如下：

(1) 調研國際 IASP 業者導入 IPv6 原因及推動經驗：

國際 IASP 業者導入 IPv6 原因及推動經驗的調查，至少包含行動網路業者 Verizon 及固網業者 Comcast 等。

(2) 調研國際 ICP 業者導入 IPv6 原因及推動經驗：

國際 ICP 業者導入 IPv6 原因及推動經驗的調查，至少包含 Google 及 Facebook 等。

調研內容包含業者導入 IPv6 原因，將分為技術原因及商業原因二方面進行探討；及研究業者導入 IPv6 推動經驗。

除了調研國際推動 IPv6 原因及推動經驗外，計畫將融合國內推動 IPv6 網路服務的情況及發展，以提供政策全面導入 IPv6 必要性及時機判斷依據。

(二) 分項二：解析 ICP 網路安全防護平台架構

依照 107 年調查結果， ICP 對 IPv6 支援比例並不高，業者經營網站不論是內容服務商或電子商務業者，其最關切的是如何衝高使用者的來訪數量或交易量,及讓使用者到訪時網站穩定運作，業者在沒有大量新增或擴大業務的情況下，目前 ICP 對 IP 的需求並未大量增加，且在 107 年之前國內 IASP 並不支援 IPv6 連網服務，終端使用者尚未有真正的使用需求出現，因此對業者來說缺乏支援 IPv6 的誘因。但 107 年中華電信固網及國內 3 大行動電信業者陸續開通 IPv6 連網服務，真正的使用者需求已經出現，對於推動 ICP 業者支援 IPv6 的誘因也出現了一道曙光，如何幫助 ICP 業者加快支援 IPv6 連網服務，為本計畫延續 107 年調查結果的一

個重要推動方向。

由 107 年調查得知，ICP 業者所遭遇的問題點為缺乏具有 IPv6 技術能力與管理經驗的人員，因技術資源相對不足的情況下，造成業者裹足不前的情況，為業者排除技術資源不足的阻力，為本項工作的重點。因此本分項計畫，希望透過從 IPv4/IPv6 雙協定平台架構解析、及技術人才培訓等兩方面著手，幫助 ICP 業者縮短建置支援 IPv6 網路服務環境的技術門檻，減少業者的阻力，以期能達到增加支援 IPv4/IPv6 之應用網站的目標前進。

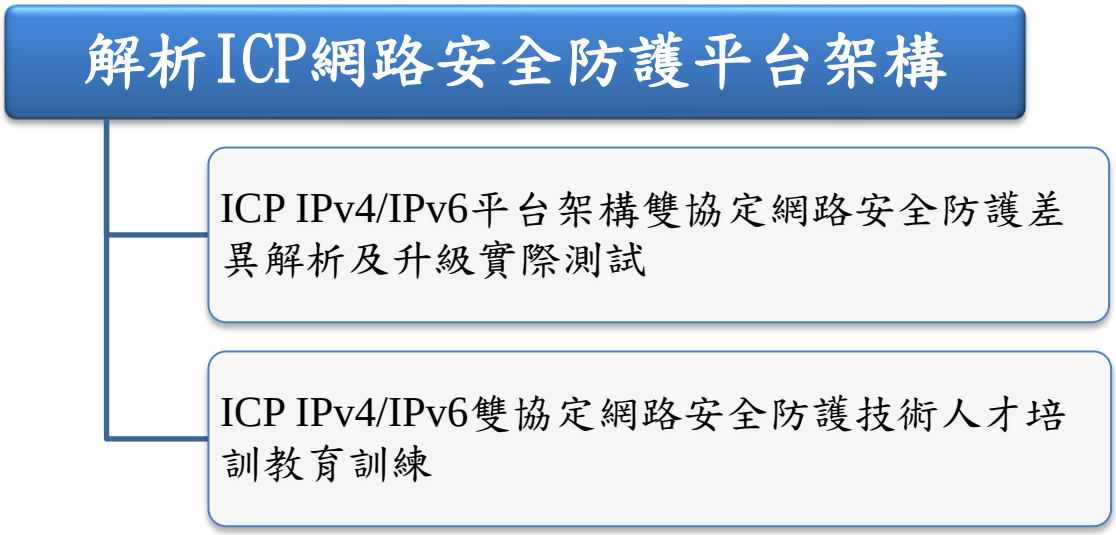

圖 9、解析 ICP 網路安全防護平台架構工作項目

上圖為解析 ICP 網路安全防護平台架構工作項目，以下將就分項工作說明：

1. ICP IPv4/IPv6 平台架構雙協定網路安全防護差異解析及升級實際測試：

由於 IPv4 和 IPv6 不只是位址長度及表示方式不同，其連線方式也可能有差異而產生影響使系統設計及網路架構不同，且

IPv4 和 IPv6 網路未經過轉換無法互相連結，所以現階段 IPv6 的連網應用要同時支援 IPv4 及 IPv6 雙軌並行，形成其複雜度更高，且 ICP 規劃網站升級轉換支援 IPv6 時，不能因為網站支援 IPv6 後，造成網站連線不通，網頁內容無法顯示，網站回應速度變慢..等現象，必須同時考慮到前台網站，後台資料及通訊設備和路由等相關因素。並且在升級過程中，必須有啟動上線的規劃及緊急復原機制，分階段導入升級，維持網站的穩定運作，才能成功完成升級。

本分項計畫希望幫助 ICP 業者建立 IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單，使業者能快速完成基礎檢測項目，降低 ICP 業者支援 IPv6 的阻力。除此之外將以實際案例，輔導業者進行升級規劃、實際測試和導入，並將記錄導入過程以及網站支援升級所遭遇的問題及解決方式，做成升級實例供業者參考。

下圖為 ICP IPv4/IPv6 平台架構雙協定網路安全防護差異解析及升級實際測試的工作項目，及工作執行程序：

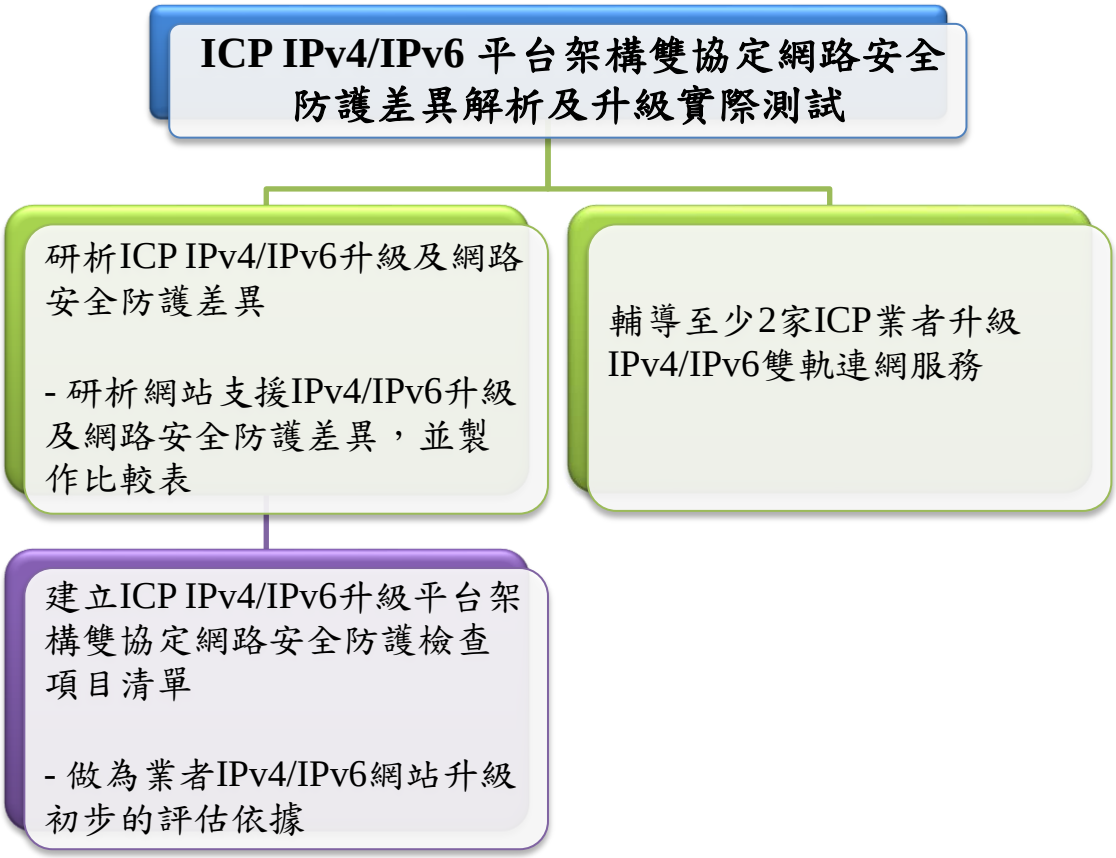

圖 10、ICP IPv4/IPv6 雙協定網路安全防護差異解析及升級實際測試工作項目與執行程序

針對 ICP IPv4/IPv6 平台架構雙協定網路安全防護差異解析及升級實際測試工作項目說明如下：

(1) 研析 ICP IPv4/IPv6 升級及網路安全防護差異：

蒐集及研析網站支援 IPv4/IPv6 升級及網路安全防護設定，並比較其差異性以製作比較表。內容如下所述：

- ICP IPv4/IPv6 雙軌網路環境升級。包含 ICP 升級 IPv6 網路架構、網路管理規劃、及軟硬體升級等相關資訊。
- ICP IPv4/IPv6 雙軌網路伺服器及服務升級。包含 ICP 升級 IPv6 網路伺服器、Web 網路程式及相關服務軟硬體升級等資訊。

◆ ICP IPv4/IPv6 雙軌網路資安設備升級。包含 ICP 升級 IPv6 資訊安全規劃、資訊安全設備軟硬體升級等相關資訊。

除了 IPv4/IPv6 升級及網路安全防護差異比較表外，亦將整合 IPv4/IPv6 升級資訊以製作成 ICP 網站服務升級 IPv6 技術手冊，介紹網站服務升級流程及步驟，以供相關業者參考。

(2) 建立 ICP IPv4/IPv6 升級平台架構雙協定網路安全防護檢查項目清單。

根據 IPv4/IPv6 升級及網路安全防護差異，製作 IPv4/IPv6 網站升級平台架構雙協定網路安全防護檢查項目清單，業者可以根據此檢查項目清單，作為初步的評估依據。

(3) 輔導至少 2 家 ICP 業者升級 IPv4/IPv6 雙軌連網服務

輔導 ICP 業者網站升級 IPv4/IPv6 雙軌連網服務的工作內容及流程如下所述：

◆ 規劃合作案例升級 IPv6 導入方案：

選定升級 IPv6 導入計畫合作對象，並分析案例的網路應用架構提出升級 IPv6 導入計畫，包含執行流程、導入的時程表、人力經費估算、及計畫書撰寫等。

◆ 執行合作案例升級 IPv6 導入方案：

根據合作案例升級 IPv6 導入計畫及時程表，執行導入方案，包括軟硬體設備採購、設備安裝及設定 IPv6 網路環境、調整設定防火牆、伺服器等網路設備、及進行測試驗證等。

◆ 撰寫合作案例升級 IPv6 建置報告：

根據合作計畫升級 IPv6 實際導入案例，撰寫建置報告，包含紀錄建置階段所使用的設定參數網路架構、問題排除..等內容；另外有關完工後，需紀錄完工報告作為後續系統維修參考資料；並根據案例執行過程，紀錄完整導入流程；以此做成升級 IPv6 實例供業者參考。

下圖所示為 ICP 實際升級 IPv6 導入方案流程：

圖 11、ICP 實際升級 IPv6 導入方案流程

2. ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練：

ICP IPv4 網站要升級支援 IPv4/IPv6 雙協定，有許多因雙協定產生的網路安全防護技術問題，本計畫將舉辦 IPv4/IPv6 雙協定網路安全防護技術教育訓練，以協助 ICP 培育雙協定網路安全防護技術人才。

下圖為 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練的工作項目，及工作執行程序：

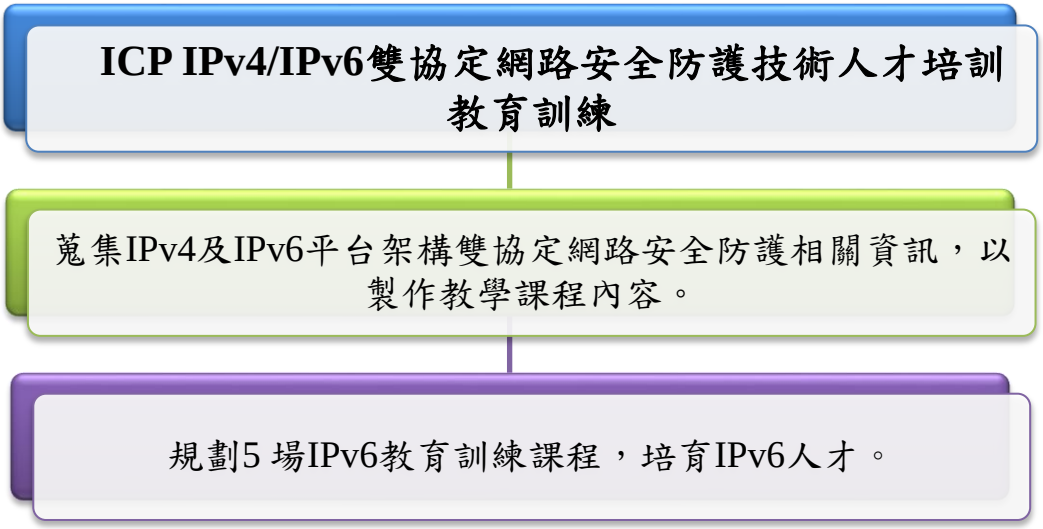

圖 12、ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練工作項目與執行程序

針對 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練工作項目說明如下：

(1) 蒐集 IPv4 及 IPv6 平台架構雙協定網路安全防護相關資訊，以製作教學課程內容。

課程內容將做 ICP IPv4/IPv6 雙協定升級基本介紹，並加強升級雙協定網路安全防護的架構及設定的議題。

(2) 規劃 5 場 IPv6 教育訓練課程，培育 IPv6 人才：

本計畫針對 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓課程，將提供國內網站經營業者、及其他民營業者的相關網路管理技術人員參與培訓計畫。預計於北、中、南部合

計辦理 5 場教育訓練，每場至少 20 人次，合計至少 100 人次參與。

(三) 分項三：研析物聯裝置標準及平台與應用

本分項計畫的目的為透過研析物聯網、5G 與 IPv6 相關的技術、及分析物聯網平台與應用等兩方面，以期能更了解新一代網路技術與應用的發展方向及市場脈動。

下圖為研析物聯裝置標準及平台與應用工作項目，以下將就分項工作說明：

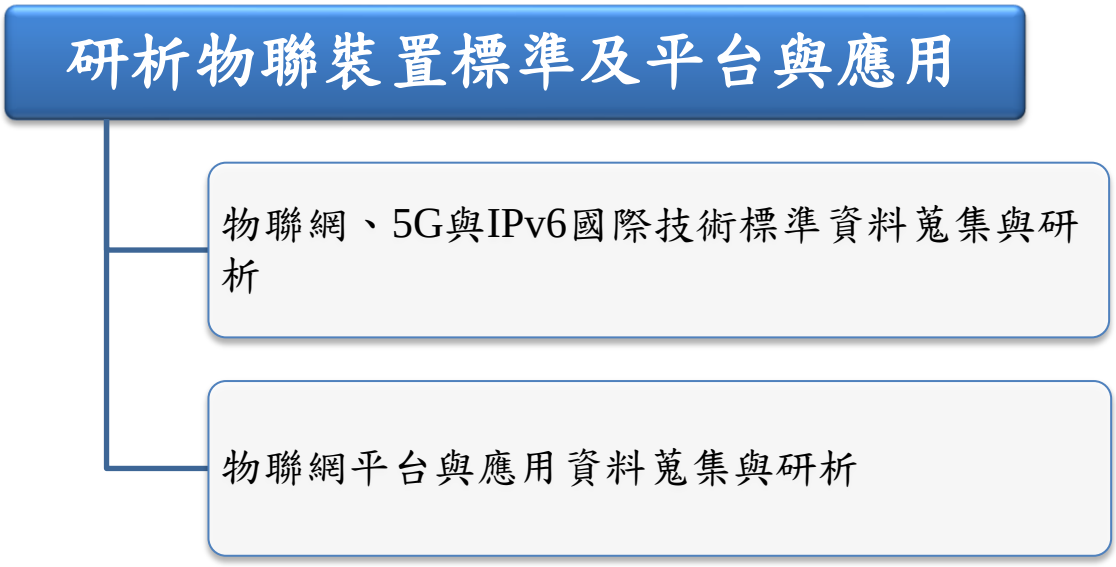

圖 13、物聯裝置標準及平台與應用研析工作項目

1. 物聯網、5G 與 IPv6 國際技術標準資料蒐集與研析

從西元 1990 年(79 年)開始，網際網路工程任務小組(IETF，Internet Engineering Task Force)[2]即開始規劃 IPv4 的下一代協定，除要解決即將遇到的 IP 位址短缺問題外，更希望能發展更多的

擴充功能及改善連網環境。IPv6 的發展已經歷經 20 個年頭，最近幾年 IPv6 的使用率終於呈現穩定的成長。

近年來因應物聯網的發展，就網際網路協議的需求，IETF 也成立相關技術工作小組，對物聯網在網路連網環境有關議題進行討論，且已經公布了第一波所制定的標準。其中 6lo、6tisch、lpwan、及 ipwave 等工作小組所研究的方向，都和物聯網裝置與網路 IPv6 技術相關，本計畫將持續蒐集與研析物聯網與 IPv6 相關的國際技術標準（RFC），解析其內容，以期對技術有更深入的了解，並掌握重點技術的發展動向，強化技術能量。

隨產業需求及網際網路的發展，新的研究議題不斷被提出，IETF 除有專門的工作小組在進行物聯網裝置與 IPv6 相關的技術研議之外。網際網路研究工作小組（IRTF，Internet Research Task Force），於西元 2015 年（104 年）成立了物聯網專門研究小組（T2TRG，Thing-to-Thing），以調查物聯網的開放性問題研究，重點在關注 IETF 所公布的標準協議可能潛在的問題。目前探討的主題包括物網聯的安全與挑戰，在物聯網場景中使用 REST 的方法以及語義等議題。並對於在物聯網領域其他組織的討論和進展，持續追蹤及了解其發展方向和推動跨組織之間相互合作。例如，W3C 中的 WoT 小組（Web of Things），兩個研究小組持續共同探討物聯網和網路技術的未來和挑戰。

本計畫除收集及研讀物聯網與 IPv6 相關的國際技術標準（RFC）之外，也將蒐集及研析 IETF 對於 5G 與 IPv6 技術的相關討論，整合物聯網、5G 與 IPv6 有關聯的技術資料，以提供給相關政府機關作為技術基礎文件，期能掌握產業技術的發展，強化技術能量，並做為決策的參考。

下圖為物聯網、5G 與 IPv6 國際技術標準資料蒐集與研析的工作項目，及工作執行程序：

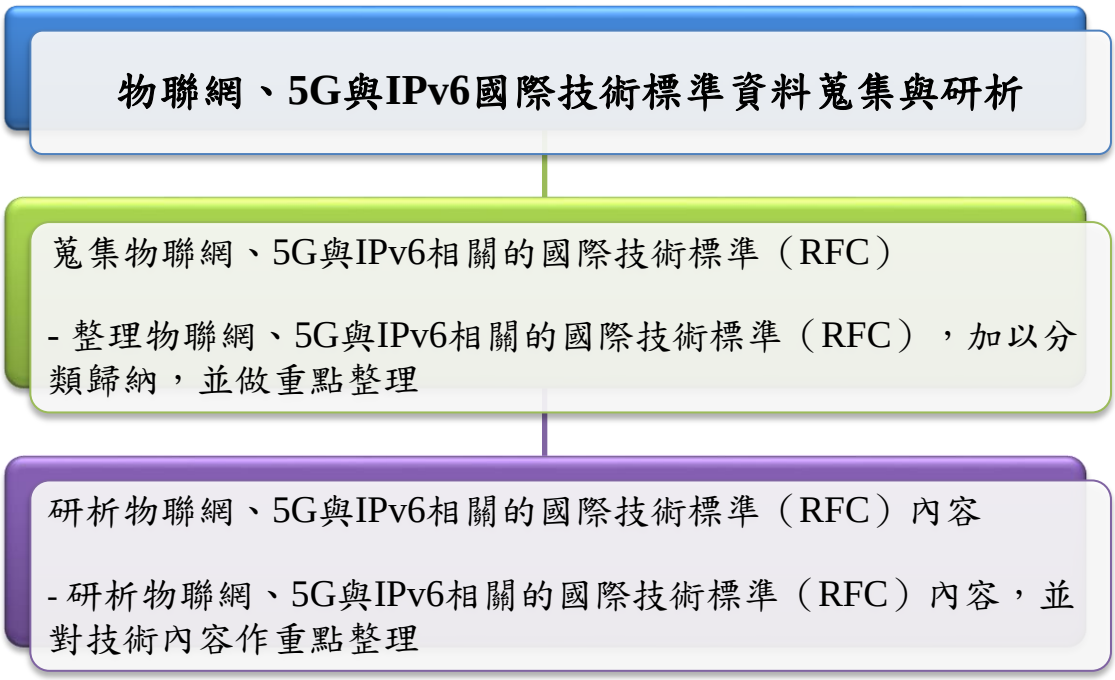

圖 14、物聯網、5G 與 IPv6 國際技術標準資料蒐集與研析工作項目與執行程序

本工作項目，進行方式說明如下：

(1) 蒐集物聯網、5G 與 IPv6 相關的國際技術標準（RFC）

整理物聯網、5G 與 IPv6 有關的網路國際技術標準(RFC)項目列表，將已通過技術標準加以分類歸納，並做技術標準摘要翻譯及重點整理。

(2) 研析物聯網、5G 與 IPv6 相關的國際技術標準（RFC）內容

研析物聯網、5G 與 IPv6 有關的網路國際技術標準(RFC)

內容，針對和 IPv6 有關的重要國際技術標準文件做翻譯，並對技術內容作重點整理。

2. 物聯網平台與應用資料蒐集與研析

物聯網概念的出現已經形成下一個科技產業的大事件，雖然物聯網近年來被廣泛討論,但整體產業還是處於初期發展階段，且參與在整個產業生態系的廠商為數眾多,因此也呈現百家爭鳴的狀況。

雖然物聯網平台相當多，但主要還是以知名國際大廠佔有優勢，主要的 3 大商用平台以 Amazon 的 AWS IoT、Mircosoft 的 Azure IoT Suite、及 Google 的 Google Cloud IoT。 本計畫將比較國際 3 大物聯網平台的設計,收集各家所使用的技術等相關資訊，解析物聯網平台的架構及可能應用分析,及對IPv6的支援狀況。並透過解析前 3 大物聯網平台架構，以掌握產業的發展動向，及應用面的可行方向,以做為擬定未來創新產業發展方針的參考依據。

下圖為物聯網平台與應用資料蒐集與研析的工作項目，及工作執行程序：

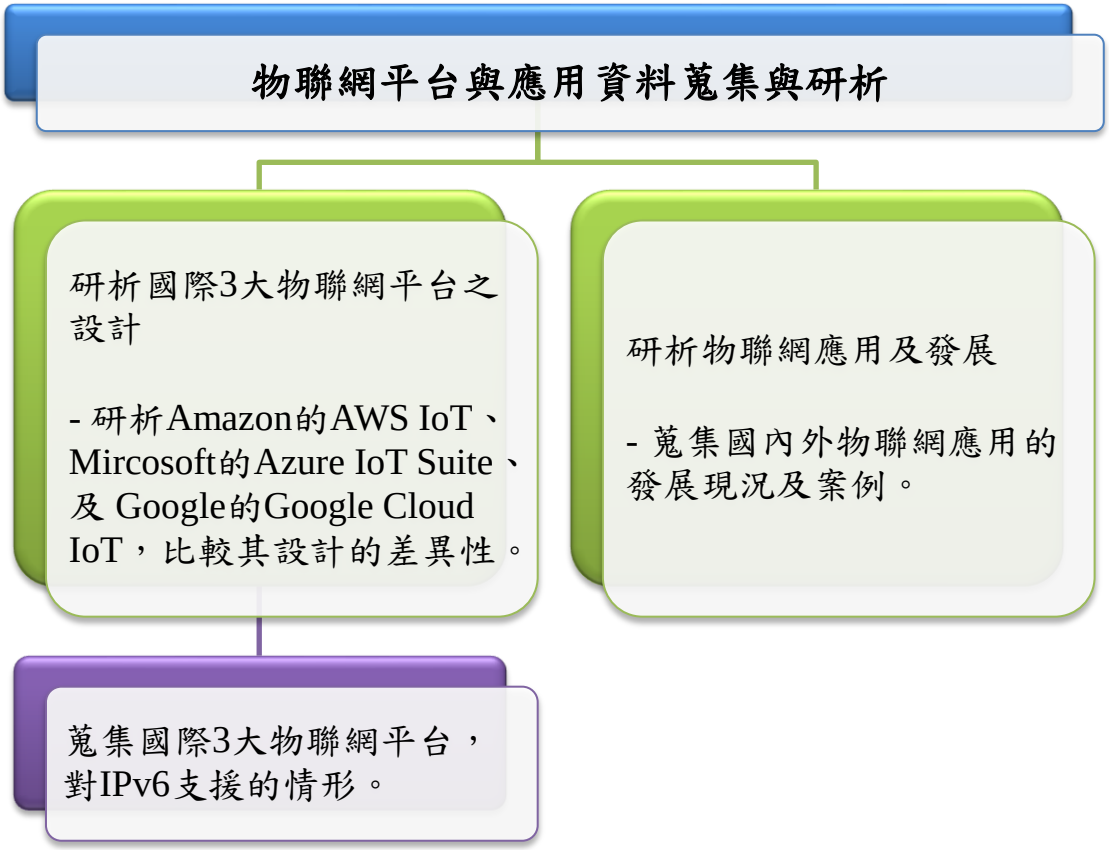

圖 15、物聯網平台與應用資料收集與研析工作項目與執行程序

本工作項目，分為三個子工作項目，各子項工作內容及進行方式說明如下：

(1) 研析國際 3 大物聯網平台之設計：

針對國際 3 大物聯網平台比較其設計的差異性。並根據平台的設計差異性，分析其對應用面的影響及優缺點。

(2) 蒐集國際 3 大物聯網平台，對 IPv6 支援的情形：

整理國際 3 大物聯網平台，對 IPv6 支援的相關資訊。

(3) 研析物聯網的應用及發展：

蒐集國內外物聯網應用的發展現況及案例，以了解產業的發展現況。

四、 預期成果

本計畫接續 107 年度「我國 IPv4/v6 雙軌普行關鍵問題調查與可行解決方案研究」，持續推動對使用者設備、IASP 網路、應用網站等 3 方面之問題推行解決方案，調查 IASP 業者支援 IPv4/v6 雙軌連網服務之整備程度，推動寬頻分享器和 IASP 實際測試，提出 ICP IPv4/IPv6 平台架構雙協定網路安全防護差異解析，以及物聯網、5G 與 IPv6 國際技術標準和平台與應用之資料蒐集與研析。預期產出的主要研究成果與效益如下。

(一) 推動商用網路雙軌普行

本計畫進行 IASP 整備程度支援 IPv6 調查，以掌握未來 IPv6 相關創新應用之服務基礎，所得成果將可作為我國推動 IPv4/IPv6 普及與建構適合創新應用發展所需生態體系之政策參考。並透過以實際案例輔導 Cable 業者升級支援 IPv6 連網服務，建立 Cable 業者導入 IPv6 實例。

針對推動市售寬頻分享器支援 IPv4/IPv6，訂定一套符合支援 IPv6 規範及標準測試項目，建立寬頻分享器和 IASP 實際測試平台，並建議將符合支援 IPv6 規範及標準測試項目納入政府共同供應契約，並持續推動增加支援 IPv4/IPv6 之 IASP 業者及應用網站，將我國 IPv6 使用率提升至 35% (以 APNIC 之統計數字為準)，建立我國 IPv6 完整生態系。

另透過調研國際大型 IASP、ICP 業者導入 IPv6 之原因及推動經驗，以做為我國推動 IPv4/IPv6 雙軌普行政策之參考。

除研究調查外將開發手機設定 IPv6 之 APP 及於 TWNIC 網站設定 IPv6 推廣專區，持續推動國內 IPv6 網路服務普行。

(二) 解析 ICP 網路安全防護平台架構

本計畫推動 ICP 支援 IPv4/IPv6，分析 IPv4 和 IPv6 網路安全防護雙協定平台架構的差異，彙整一份檢查項目清單，協助 ICP 業者能快速完成基礎檢測項目進行實際測試。此外，辦理 IPv4/IPv6 升級之網路安全防護教育訓練，協助 ICP 業者 培育 IPv4/IPv6 雙協定網路安全防護技術人才，幫助 ICP 業者快速培養技術能力，強化產業界 IPv6 技術能量。

並以實際案例輔導 ICP 業者做網站支援 IPv6 升級，建立 ICP 導入 IPv6 網路服務之實例、規劃升級指引及教育手冊。

(三) 研析物聯裝置標準及平台與應用

本計畫將協助主管機關研析有關物聯網、5G 與 IPv6 有關的國際標準（RFC）內容，以期對技術有更深入的了解，並掌握重點技術的發展動向，強化技術能量。並透過解析國際 3 大物聯網平台架構，以充分掌握產業的技術發展脈動，及應用面可行方向，以做為擬定未來創新產業發展方針的參考依據。

第二節　與計畫符合情形

一. 目標達成狀況

依照計畫內容將工作項目分為 7 個項目，各項目下另規劃數個執行細項，部分工作細項之間存在執行順序的依存性，目前計畫預計完成工作項目皆已執行完成，各項工作執行進度如下表所示：

表 1、各項工作執行進度

工作項目	一月	二月	三月	四月	五月	六月	七月	八月	九月	十月	十一月	十二月	已完成進度
國內 IASP 支援 IPv6 普查													
國內 IASP 支援 IPv6 問卷及面訪調查		■	■	■	■	■	■	■	■	■	■		100%
DNSSEC 調查及監		■	■	■	■	■	■	■	■	■	■		100%
至少和 1 家 Cable 業者合作推廣用戶試用 IPv6 連網服務					■	■	■	■	■	■	■		100%
開發手機設定 IPv6 之 APP					■	■	■	■	■	■	■		100%
設置 IPv6 推廣專區					■	■	■	■	■	■	■		100%
寬頻分享器和 IASP 實際測試平台建置及研擬寬頻分享器支援 IPv6 之共同供應契約													
研擬寬頻分享器符合支援 IPv6 規範及標準測試項目		■	■	■	■	■	■	■	■	■	■		100%
建置寬頻分享器支援 IPv6 之測試平台				■	■	■	■	■	■	■	■		100%

工作項目	一月	二月	三月	四月	五月	六月	七月	八月	九月	十月	十一月	十二月	已完成進度
研擬寬頻分享器支援 IPv6 之共同採購契約相關規範				■	■	■	■	■	■	■	■		100%
調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗													
調研國際 IASP 業者導入 IPv6 原因及推動經驗		■	■	■	■	■	■	■	■				100%
調研國際 ICP 業者導入 IPv6 原因及推動經驗		■	■	■	■	■	■	■	■				100%
ICP IPv4 / IPv6 平台架構雙協定網路安全防護差異解析及實際測試													
研析 ICP IPv4/IPv6 升級及網路安全防護差異		■	■	■	■	■	■	■	■	■			100%
建立 ICP IPv4/IPv6 升級平台架構雙協定網路安全防護檢查項目清單		■	■	■	■	■	■	■	■	■			100%
輔導至少 2 家 ICP 業者升級 IPv4/IPv6 雙軌連網服務				■	■	■	■	■	■	■			100%
ICP IPv4 / IPv6 雙協定網路安全防護技術人才培訓教育訓練													
蒐集 IPv4 及 IPv6 平台架構雙協定網路安全防護相關資訊，以製作教學課程內容		■	■	■	■	■	■	■	■				100%
規劃 5 場 IPv6 教育訓練課程，培育 IPv6 人才				■	■	■	■	■	■	■			100%

工作項目	一月	二月	三月	四月	五月	六月	七月	八月	九月	十月	十一月	十二月	已完成進度
物聯網、 5G 與 IPv6 國際技術標準資料蒐集與研析													
蒐集物聯網、5G 與 IPv6 相關的國際技術標準（RFC）													100%
研析物聯網、5G 與 IPv6 相關的國際技術標準（RFC）內容													100%
物聯網平台與應用資料蒐集與研析													
研析國際 3 大物聯網平台之設計													100%
蒐集國際 3 大物聯網平台，對 IPv6 支援的情形													100%
研析物聯網的應用及發展													100%

二. 進度符合情形

各項工作的查核點進度，符合原計畫申請書之規劃，完成期末預定應完成項目，詳細細目及工作進度，如下表所示：

表 2、各項查核進度表

分類	工作項目	執行進度			原因說明
		超前	符合	落後	
國內 IASP 支援 IPv6 普查	國內 IASP 支援 IPv6 問卷及面訪調查		✓		
	DNSSEC 調查及監測		✓		
	至少和 1 家 Cable 業者合作推廣用戶試用 IPv6 連網服務		✓		
	開發手機設定 IPv6 之 APP		✓		
	設置 IPv6 推廣專區		✓		
寬頻分享器和 IASP 實際測試平台建置及研擬寬頻分享器支援 IPv6 之共同供應契約	研擬寬頻分享器符合支援 IPv6 規範及標準測試項目		✓		
	建置寬頻分享器支援 IPv6 之測試平台		✓		
	研擬寬頻分享器支援 IPv6 之共同採購契約相關規範		✓		
調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗	調研國際 IASP 業者導入 IPv6 原因及推動經驗		✓		
	調研國際 ICP 業者導入 IPv6 原因及推動經驗		✓		

分類	工作項目	執行進度			原因說明
		超前	符合	落後	
ICP IPv4 / IPv6 平台架構雙協定網路安全防護差異解析及實際測試	研析 ICP IPv4/IPv6 升級及網路安全防護差異		✓		
	建立 ICP IPv4/IPv6 升級平台架構雙協定網路安全防護檢查項目清單		✓		
	輔導至少 2 家 ICP 業者升級 IPv4/IPv6 雙軌連網服務		✓		
ICP IPv4 / IPv6 雙協定網路安全防護技術人才培訓教育訓練	蒐集 IPv4 及 IPv6 平台架構雙協定網路安全防護相關資訊，以製作教學課程內容		✓		
	規劃 5 場 IPv6 教育訓練課程，培育 IPv6 人才		✓		
物聯網、5G 與 IPv6 國際技術標準資料蒐集與研	蒐集物聯網、5G 與 IPv6 相關的國際技術標準（RFC）		✓		
	研析物聯網、5G 與 IPv6 相關的國際技術標準（RFC）內容		✓		
物聯網平台與應用資料蒐集與研析	研析國際 3 大物聯網平台之設計		✓		
	蒐集國際 3 大物聯網平台，對 IPv6 支援的情形		✓		
	研析物聯網的應用及發展		✓		

各項工作於期末須完成的工作皆已如期完成，各項工作量化指標如下表所列：

表 3、期末報告量化指標

編號	計畫工作項目	期末報告產出
1	國內 IASP 支援 IPv6 普查	面訪 20 家 Cable 業者和 2 家行動業者並進行問卷調查報告。 輔導1家Cable業者進行IPv6使用者試用。
2	寬頻分享器和 IASP 實際測試平台建置及研擬寬頻分享器支援 IPv6 之共同供應契約	完成 1 份寬頻分享器支援 IPv6 規格報告。 完成寬頻分享器和IASP符合支援IPv6規範測試項目實測平台1套。 完成寬頻分享器技術符合支援IPv6規範及測試項目報告1篇，完成建議政府納入共同供應契約之項目1套。
3	調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗	完成各 2 家國際大型 IASP、ICP 導入 IPv6 原因及推動經驗報告。
4	ICP IPv4 / IPv6 平台架構雙協定網路安全防護差異解析及升級實際測試	ICP IPv4/IPv6 網路安全防護架構技術手冊 1 份。 ICP IPv4/IPv6 網路安全防護架構差異檢查項目清單及研析報告 1 份。 輔導2家ICP業者進行IPv6升級。
5	ICP IPv4 / IPv6 雙協定網路安全防護技術人才培訓教育訓練	舉辦 5 場 ICP 網路安全防護教育訓練。每場至少 20 人，至少共 100 人參與。
6	物聯網、 5G 與 IPv6 國際技術標準資料蒐集與研析	物聯網、5G 相關 RFC 整理報告 1 份。 參與至少 5 場國際會議出國報告。
7	物聯網平台與應用資料蒐集與研析	物聯網平台報告1份，介紹Amazon的AWS IoT、Mircosoft的Azure IoT Suite、及 Google的Google Cloud IoT共3個國際平台及應用。

第三節　資源運用檢討

一、　人力運用情形

本研究計畫共投入總執行人力 5 人，包含專職人員 1 人，及兼職人員 4 人，與原計畫申請書之規劃相符，各人力擔任之工作如下表所示：

表 4、執行人力表

類別	姓名	職位	最高學歷	在本計畫中擔任之工作
主持人	顧靜恆	組長	博士	計畫主持人，整體計畫控管與執行督導。
協同研究人員	蔡更達	工程師	學士	負責商用雙軌普行推動，問題研析及解決方案建議。
協同研究人員	王彥傑	工程師	碩士	負責 ICP 網安平台架構解析，問題研析及解決方案建議。
協同研究人員	陳玟羽	管理師	碩士	負責物聯裝置標準與平台及應用研析，問題研析及解決方案建議。
專任研究人員	許淑芳	專案經理	碩士	負責資料研析，資料整合建議及計畫報告撰寫。

二、　經費運用情形

依照目前本研究計畫進度，依據工作規畫執行各項經費，經費運用情形與進度相當，各項經費使用如下表所示：

表 5、合計總經費運用情形統計表

項　目	預算金額	使用金額	使用率	備　註
人事費用	$2,587,186	$2,587,186	100%	
業務費	$2,886,451	$2,886,451	100%	
差旅費	$840,000	$840,000	100%	
行政管理費	$631,363	$631,363	100%	
合　計	$6,945,000	$6,945,000	100%	

第二章　國內 IASP 支援 IPv6 普查

國內 IASP 支援 IPv6 普查工作項目，主要目的是透過調查，以掌握 Cable 業者、固網業者及行動通信業者等，根據所提供的各類網路連線服務所需 IP 使用情境的不同，對 IPv6 支援的整備程度，以了解國內 IPv6 的普及狀況及預估未來可能的發展。本項工作又可細分為 5 個工作分項，以下將就各分項工作成果說明：

第一節　國內 IASP 支援 IPv6 問卷及面訪調查

IASP 支援 IPv6 的調查，是以問卷及面訪方式進行，調查內容包含業者在各項網路服務支援 IPv6 的程度、預計商用服務上線時程、及該服務之設備支援 IPv6 的建置準備程度等方向。以期能掌握業者的佈建狀況及提供服務的時程計畫。

一.Cable 業者

目前我國 Cable（有線系統）業者分為多系統業者（Multi-System Operator，MSO）及獨立系統業者（System Operator，SO）；MSO 業者主要有〝中嘉〞、〝凱擘〞、〝台固媒體〞、〝台灣寬頻〞及〝台灣數位光訊〞等集團，其他為獨立系統業者。本次調查共完成 20 家 Cable 業者的問卷及面訪調查，包含 5 家 MSO 及 15 家獨立系統業者，其中台灣數位光訊由集團下台灣基礎開發科技接受面訪及問卷回覆，下表為完成面訪的業者名單及面訪時程表：

表 6、Cable 業者面訪時程表

序號	Cable業者	有線電視系統經營者	面訪日期
1	凱擘大寬頻（MSO）	凱擘金頻道、凱擘新台北、凱擘陽明山、凱擘大文安、全聯、新唐城、北桃園、新竹振道、豐盟、新頻道、南天、及觀昇有線電視(共12家)	2月22日
2	台固媒體股份有限公司（MSO）	永佳樂、觀天下、紅樹林、聯禾、及鳳信數位有線電視(共5家)	2月22日
3	台灣寬頻通訊（MSO）	南桃園、北視、信和、吉元、及群健有線電視(共5家)	3月4日
4	全國數位有線電視	DCTV全國數位有線電視(以新北市為主)	3月5日
5	天外天數位有線電視	TWT天外天數位有線電視(新北市三重、蘆洲、八里、新莊、泰山、五股、淡水)	3月7日
6	超宇寬頻	聯維有線電視、寶福有線電視	3月19日
7	大新店民主有線電視	大新店民主有線電視(新北市新店、深坑、石碇、坪林、烏來)	3月21日
8	台灣基礎開發科技 台灣數位光訊科技集團（MSO）	大屯有線電視、中投有線電視、佳光(台中市區、西海岸區)、大揚及佳聯有線電視；數位電視哈TV	3月25日
9	新永安有線電視	新永安有線電視(台南市十五個行政區)	4月3日
10	世新有線電視	世新有線電視(嘉義)	5月10日
11	國聲有線電視	國聲有線電視(嘉義)	5月10日
12	新彰數位有線電視	新彰數位有線電視(彰化)	7月22日
13	三大有線電視	三大有線電視(南彰化)	7月25日
14	南國有線電視	南國有線電視(高雄)	7月26日

序號	Cable業者	有線電視系統經營者	面訪日期
15	洄瀾有線電視	洄瀾有線電視(花蓮)	8月5日
16	東亞有線電視	東亞有線電視(花蓮)	8月5日
17	高雄大大新寬頻	新高雄有線電視(高雄市)	9月16日
18	北都數位有線電視	北都數位有線電視(台北)	9月19日
19	中嘉寬頻（MSO）	bb TV(吉隆-基隆市、長德-台北市、麗冠-台北市、萬象-台北市、新視波-新北市、家和-新北市、北健-桃園、三冠王-台南市、雙子星-台南市、慶聯-高雄市、港都-高雄市)	10月5日
20	大台中數位寬頻有線電視	大台中數位寬頻有線電視(台中市)	10月9日

Cable 業者共回收 20 份問卷，以下就回收問卷內容，彙整業者回覆的狀況資料：

(一) 貴公司 IPv4 位址會在何時面臨不足？

Cable 業者對於是否預期有 IPv4 位址面臨不足的問題，在回收的 20 份問卷中，其中凱擘寬頻最早在去年（107 年）即面臨 IPv4 位址不足；另外台固媒體、大新店有線電視及北都數位有線電視共 3 家業者預計今年（108 年）將面臨 IPv4 位址不足；天外天數位有線電視、世新有線電視、國聲有線電視及大台中數位有線電視共 4 家業者預期在明年（109 年）可能面臨 IPv4 位址不足的情況；台灣寬頻通訊、全國數位有線電視、三大有線電視及中嘉寬頻共 4 家業者，預期於西元 2022 年（111 年）將面臨 IPv4 位址不足的情況；而新永安有線電視預期於西元 2023 年（112 年）將面臨 IPv4 位址不足的情況；另有 7 家業者（超宇寬頻、台灣基礎開發、新彰數位有線電視、南國有線電視、洄瀾有線電視、東亞有線電視及高雄大大新寬頻）回覆沒有 IPv4 不足的情況，業者沒有

IP 不足的情況包含使用 NAT 解決、向其他 ISP 租用等方式因應使用者需求；面訪過程發現有線電視經營因有同業間經營競爭外，網路電視及 OTT（Over-The-Top）網路隨選串流影片服務競爭，行動裝置的興起等眾多因素，造成部分客戶流失，在無客戶成長或成長放緩的情況下，多家業者估計近期對 IPv4 位址需求並不會大量增加。

(二) 貴公司是否已在進行 IPv4 位址不足的相關策略？

下表針對有關 Cable 業者，目前是否已在進行 IPv4 位址不足相關策略統計表。由問卷回覆統計結果顯示，超宇寬頻、台灣基礎開發、南國有線電視及高雄大大新寬頻，4 家業者回覆沒有 IPv4 不足的情況，且公司尚未進行任何 IPv4 位址不足的相關策略；台灣基礎開發並提出說明主因為，因用戶數近年無成長，沒有增加 IP 的需求，因此尚未有任何計畫；而超宇寬頻使用 CGNAT 核發 IP 給用戶，因此 IP 數量仍足夠；另外 2 家獨立系統業者向其他 ISP 租用頻寬及 IP，目前都還有穩定的供給資源，因此未針對此項議題研擬解決方案。其他 16 家業者都已經開始針對 IPv4 位址不足進行相關策略，其中有 10 家業者以〝從其他 ISP 中取用 IPv4 位址〞比例為 50%最高；其次為〝回收用戶閒置 IPv4 位址〞比例為 40%；另有 4 家業者以〝減少各項服務 IPv4 核發數量或以價制量〞比例為 20%；而凱擘寬頻及台固媒體在 Cable 業者中相對 IPv4 資源較為吃緊，再加上全國數位有線電視共 3 家業者有〝使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶〞，比例為 15%；天外天數位有線電視在〝其他〞選項中也提列公司已經開始在研擬啟用 IPv6 服務的可能性；而中嘉寬頻則是以〝提供客戶端設備

含 NAT 功能〞來解決 IPv4 不足的問題；關於業者對 IPv4 不足的問題所採取的解決策略，問卷回覆統計結果請參考以下及統計圖表。

表 7、Cable 業者是否有 IPv4 位址面臨不足的問題統計表

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
貴公司 IPv4 位址會在何時面臨不足？																					
沒有 IPv4 位址不足的問題																					
						✓		✓				✓		✓	✓	✓	✓				7
預期在西元__?__年發生 IPv4 位址不足																					
	✓	✓	✓	✓	✓		✓		✓	✓	✓		✓					✓	✓	✓	13
貴公司是否已在進行 IPv4 位址不足的相關策略?																					
沒有進行 IPv4 位址不足相關策略，請問原因為何?																					
						✓		✓						✓			✓				4
已在進行 IPv4 位址不足相關策略，以下哪些是在進行的項目(複選)																					
	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	16
	使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶																				
	✓	✓		✓																	3
	減少各項服務 IPv4 核發數量或以價制量																				
			✓						✓				✓							✓	4
	回收用戶閒置 IPv4 位址																				
	✓	✓			✓		✓		✓	✓	✓		✓								8
	從其他 ISP 中取用 IPv4 位址																				
			✓		✓				✓	✓	✓	✓	✓		✓	✓		✓			10
	配發用戶 IPv6 位址提供用戶 Native IPv6 連線服務																				
																					0
	其他																				
					✓														✓		2

下表詳列 Cable 業者提列實際預期面臨 IPv4 不足時程的年份資料：

表 8、Cable 業者預期面臨 IPv4 不足時程表

預期面臨 IP 不足時程	Cable業者	總計
西元 2018 年（107 年）	凱擘寬頻	**1**
西元 2019 年（108 年）	台固媒體、大新店民主有線電視及北都數位有線電視	**3**
西元 2020 年（109 年）	天外天數位有線電視、世新有線電視、國聲有線電視及大台中數位有線電視	**4**
西元 2022 年（111 年）	台灣寬頻通訊、全國數位有線電視、三大有線電視及中嘉寬頻	**4**
西元 2023 年（112 年）	新永安有線電視	**1**
沒有 IPv4 位址不足	超宇寬頻、台灣基礎開發、新彰數位有線電視、南國有線電視、洄瀾有線電視、東亞有線電視及高雄大大新寬頻	**7**

下圖依據上表資料 Cable 業者提列預期面臨 IP 不足時程的比例統計圖：

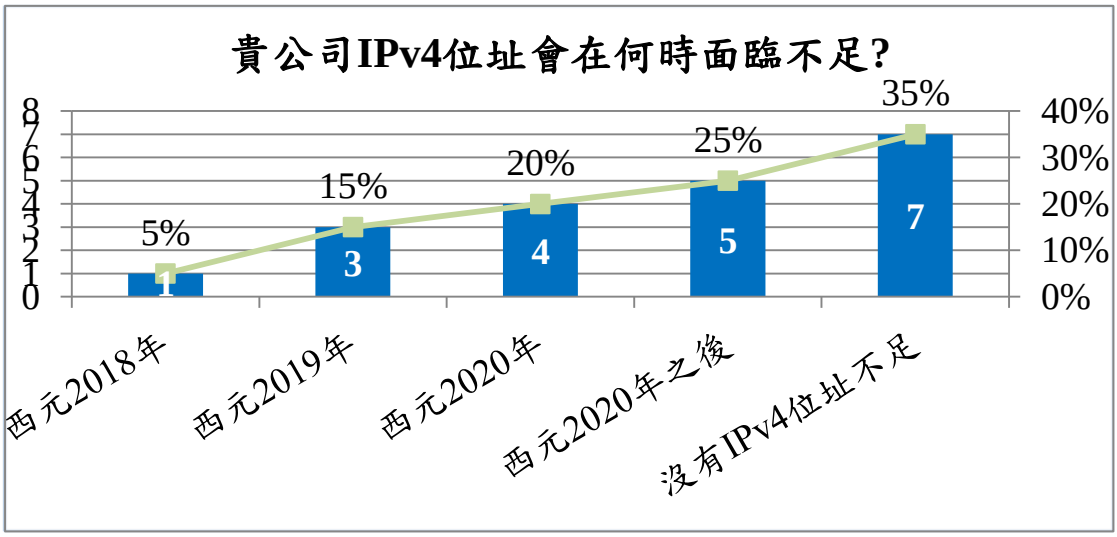

圖 16、Cable 業者面臨 IPv4 位址不足的時程統計圖

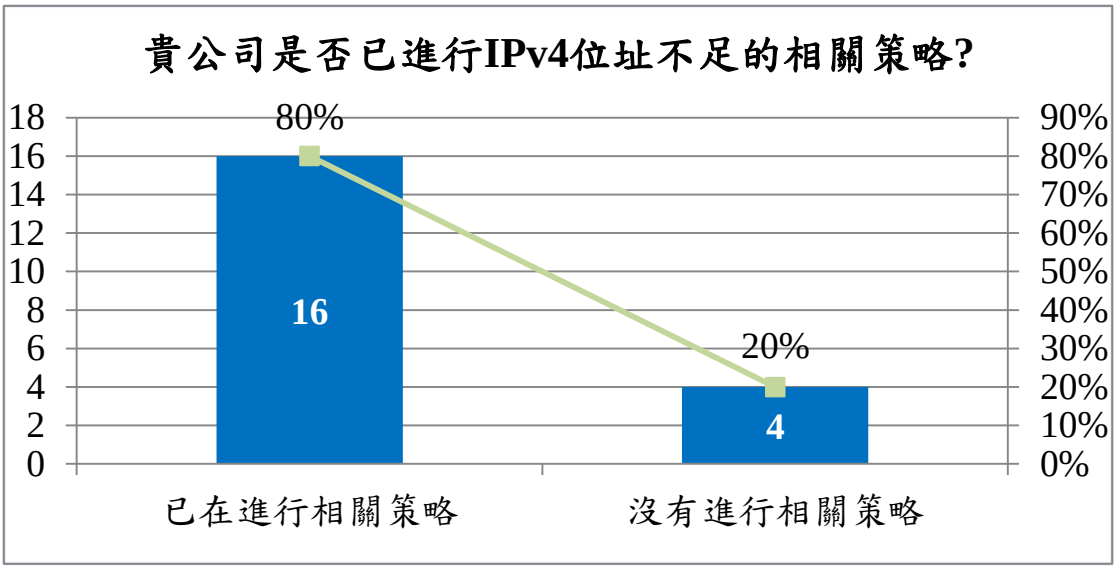

圖 17、Cable 業者是否已進行 IPv4 位址不足的相關策略統計圖

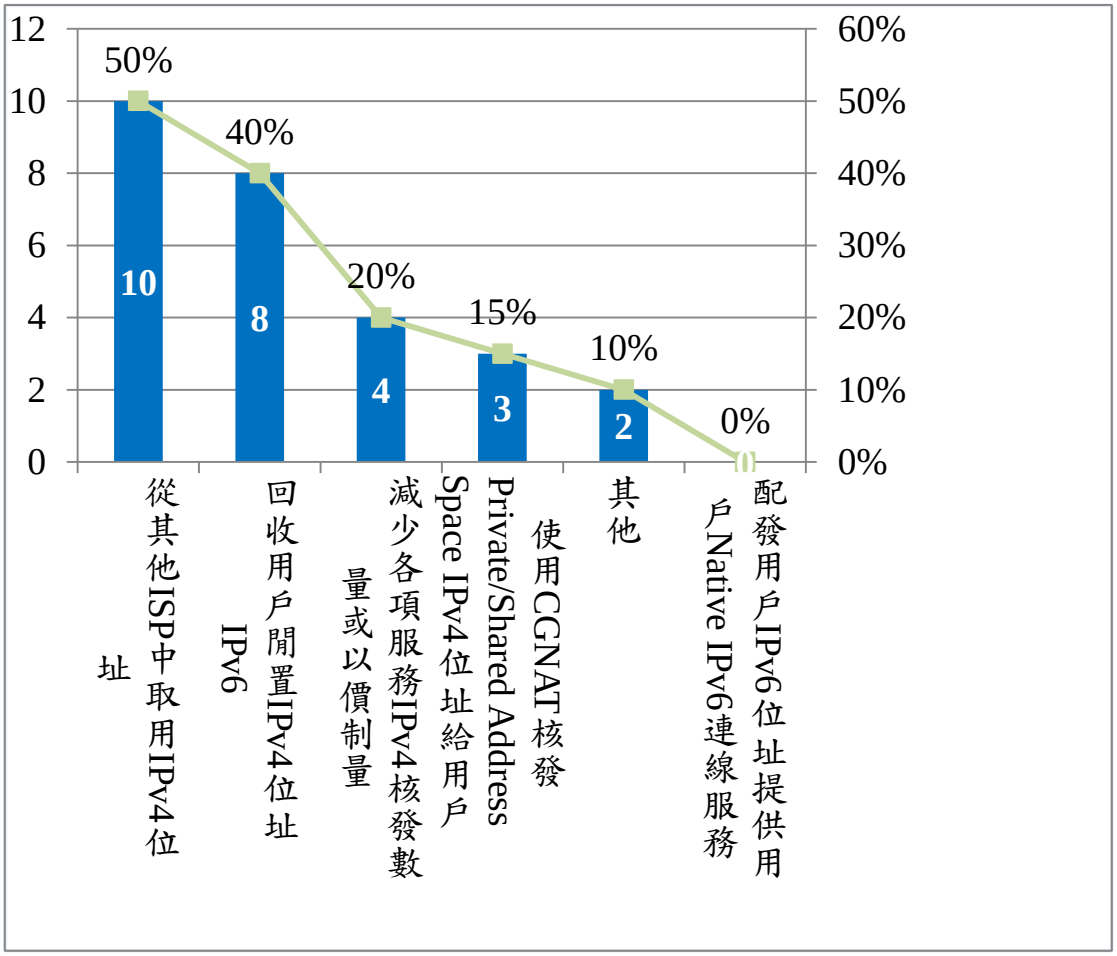

圖 18、Cable 業者對於 IPv4 位址不足所進行相關策略統計圖

(三) 若貴公司未提供 IPv6 服務考慮的原因為何呢？

下表根據 Cable 業者，對於未提供 IPv6 服務考慮的原因為何的問題項目回覆統計表，依照 Cable 業者回覆來看，可分成收入及支出 2 大方向，其中收入面多數業者勾選〝目前業務以 IPv4 為主〞的選項為最多，達到 95%比例，只有中嘉寬頻未選擇此項目，中嘉寬頻在訪談中提及和其他 ISP 網路互連（peering）或借道連外（transit）的需求，目前中嘉寬頻骨幹的部分已經支援 IPv6 網路服務，但使用者端因為還有人力、成本及技術性問題有待克服，目前尚未進行，可見商業利益及服務需求才是業者推動新服務的最大動力；對於一般網路使用者較在意的重點為網路連線的穩定度及速度，網站內容正確即可，目前國人常瀏覽的網站不是只有支援 IPv4，就是支援 IPv4/IPv6 雙軌服務，因此消費者對 Cable 業者尚未支援 IPv4/IPv6 雙軌服務，並不會產生任何不便，且現階段企業用戶對網路服務是否支援 IPv6 也沒有強烈需求，因此也降低業者積極投入的動力；這也反應到有 40%的業者勾選〝提供 IPv6 不會增加收入〞這個選項，這 2 項在收入面上的考量，為主要影響業者投入的意願。

而就支出面的考量，有 8 家業者勾選〝服務升級 IPv6 所需的成本大於使用 IPv4 的成本〞，因此也不會積極推動；另外有 5 家業者勾選〝目前公司大部分軟硬體設備不支援 IPv6〞比例為 25%，額外的建置成本也是業者不願意投入的原因。

除此之外有 5 家業者勾選〝目前公司政策並未推動 IPv6〞比例為 25%；新永安有線電視在〝其他〞選項上反映公司部分重要軟硬體不支援 IPv6，在公司沒有編列足夠的預算做軟硬體升級下無

法進行；而三大有線電視回覆用戶端設備不支援 IPv6，為考量到用戶自行購買寬頻分享器支援 IPv6 比例並不高，整體環境不完善也影響業者的投入意願。除此之外在訪談過程中多家業者反應，業者除需要增購新軟硬體設備以支援 IPv6 外，DHCP 伺服器廠商在配發 IPv4 及 IPv6 時會向業者收取個別位址配發授權費用，為了支援雙軌服務需同時配發 IPv4 及 IPv6 位址給同一用戶，業者須負擔雙重的授權費；近年來市場競爭壓力增大，不少業者面臨用戶數減少，這對業者而言形成更大的營運壓力，也是業者對於支援 IPv4/IPv6 雙軌服務裹足不前的重要原因之一。

在〝其他〞選項上，業者說明如下所述：

- ◆ 新永安有線電視提列原因為〝公司部分重要軟硬體不支援 IPv6〞。
- ◆ 三大有線電視提列原因為〝用戶端設備不支援 IPv6〞。

下圖根據 Cable 業者的問卷回覆表，整理出有關業者尚未提供 IPv6 服務考慮的原因統計圖。

表 9、Cable 業者問卷統計未提供 IPv6 服務考慮的原因

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
若貴公司未提供 IPv6 服務考慮的原因為何呢？(複選)																					
目前業務以 IPv4 為主																					
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	**19**
服務升級 IPv6 所需的成本大於使用 IPv4 的成本																					

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
	✓	✓		✓			✓							✓			✓		✓	✓	8
目前公司大部分軟硬體設備不支援 IPv6																					
				✓										✓	✓	✓	✓				5
目前公司政策並未推動 IPv6																					
	✓	✓					✓										✓	✓			5
提供 IPv6 不會增加收入																					
	✓	✓					✓	✓									✓	✓	✓	✓	8
上游 ISP 路由不支援 IPv6																					
																					0
其他，請說明_____																					
									✓				✓								2

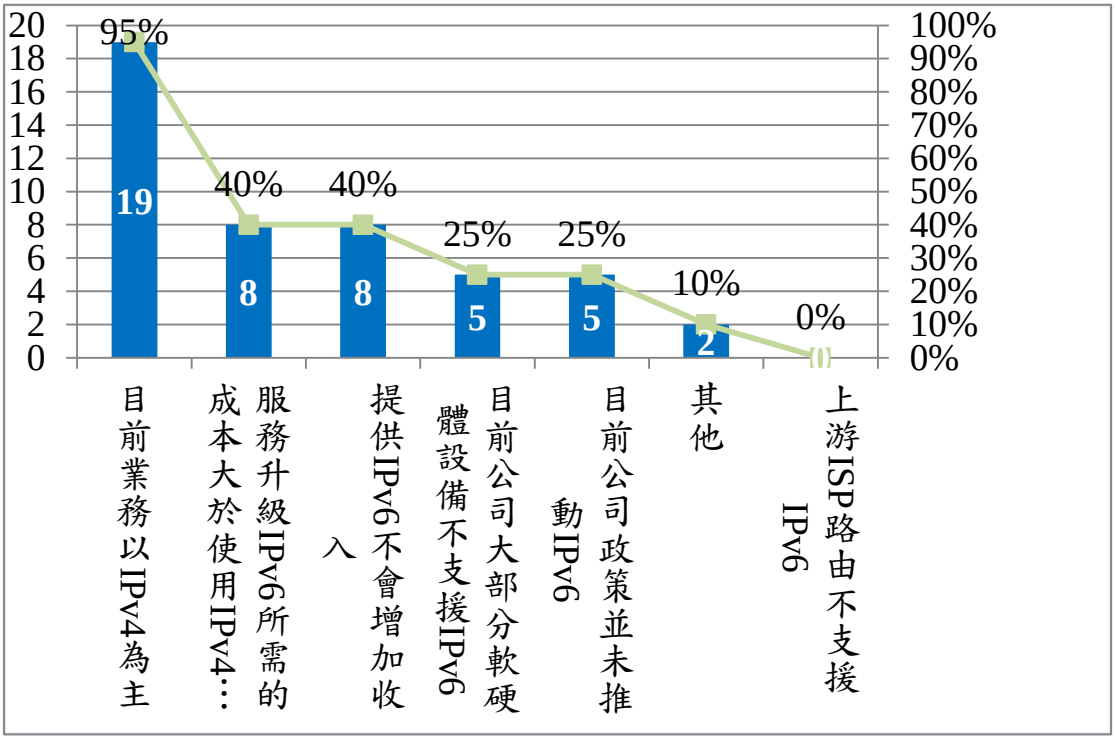

圖 19、Cable 業者問卷未提供 IPv6 服務考慮的原因統計圖

(四) 貴公司的 IPv6 位址申請及 IPv6 路由狀況為何？

下表根據 Cable 業者，對於 IPv6 位址申請及 IPv6 路由狀況的問卷回覆統計表，依照 Cable 業者回覆來看，其中共 12 家業者〝尚未申請 IPv6 位址〞，比例為 60%，超過半數以上的業者都還沒有準備；Cable 業者尚未申請 IPv6 位址者，預計申請詳細時程資料請參考表 11;目前新永安有線電視及北都數位有線電視 2 家業者，預計於今年（108 年）申請 IPv6 位址；超宇寬頻、世新有線電視、國聲有線電視及新彰數位有線電視 4 家業者，預計於明年(109 年）申請 IPv6 位址；全國數位有線電視及南國有線電視 2 家業者，預計於西元 2021 年（110 年）申請 IPv6 位址；三大有線電視，預期於西元 2022 年（111 年）申請 IPv6 位址；洄瀾有線電視、東亞有線電視及中嘉寬頻共 3 家業者未註明。

〝已申請 IPv6 位址，但尚未將 IPv6 放在全球路由〞的業者共有 6 家，比例達 30%；Cable 業者預計將 IPv6 放在全球路由，詳細時程資料請參考表 12；其中台固媒體、台灣寬頻通訊及大新店民主有線電視 3 家業者預計於今年（108 年）將 IPv6 放在全球路由；另外天外天數位有線電視及大台中數位有線電視 2 家業者，預計於西元 2020 年（109 年）將 IPv6 放在全球路由；而高雄大大新寬頻未註明其計畫時程。

而凱擘寬頻及台灣基礎開發 2 家業者回覆〝已申請 IPv6 位址且將 IPv6 放在全球路由〞，為目前進度較快的業者。台灣基礎開發客戶中有一家企業用戶要求其支援 IPv6，因此也是所有業者中唯一網路有支援 IPv6 及實際服務客戶的案例，業者是以專線連接到客戶公司的方式支援；但對一般家戶使用者目前尚未有計畫。下

圖根據Cable業者的問卷回覆表，整理出有關IPv6位址申請及IPv6路由狀況的統計圖。

表 10、Cable 業者問卷統計 IPv6 位址申請及 IPv6 路由狀況

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
貴公司的 IPv6 位址申請及 IPv6 路由狀況為何？																					
尚未申請 IPv6 位址，預計西元_____年申請 IPv6																					
				✓		✓			✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		**12**
已申請 IPv6 位址，但尚未將 IPv6 放在全球路由，預計西元_____年將 IPv6 放在全球路由																					
		✓	✓		✓		✓										✓			✓	**6**
已申請 IPv6 位址且將 IPv6 放在全球路由。																					
	✓							✓													**2**

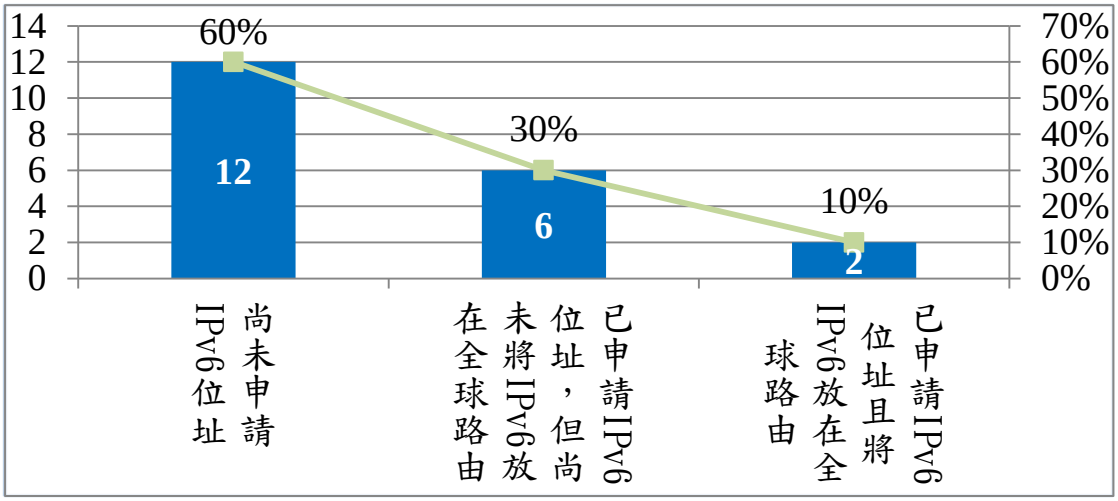

圖 20、Cable 業者問卷對 IPv6 位址申請及 IPv6 路由狀況的統計圖

目前〝尚未申請 IPv6 位址〞業者中，預計申請 IPv6 的時程計畫如下表所列：

表 11、Cable 業者尚未申請 IPv6 位址預計申請時程表

預計申請 IPv6 位址時程	Cable業者	總計
西元 2019 年（108 年）	新永安有線電視、北都數位有線電視	2
西元 2020 年（109 年）	超宇寬頻、世新有線電視、 國聲有線電視、新彰數位有線電視	4
西元 2021 年（110 年）	全國數位有線電視、南國有線電視	2
西元 2022 年（111 年）	三大有線電視	1
未註明	洄瀾有線電視、東亞有線電視、中嘉寬頻	3

針對〝已申請 IPv6 位址，但尚未將 IPv6 放在全球路由〞業者中，預計將 IPv6 放在全球路由的時程計畫如下表所列：

表 12、Cable 業者尚未將 IPv6 放在全球路由者預計執行時程表

預計將 IPv6 放在 全球路由時程	Cable業者	總計
西元 2019 年（108 年）	台固媒體、台灣寬頻通訊、 大新店民主有線電視	3
西元 2020 年（109 年）	天外天數位有線電視、 大台中數位有線電視	2
未註明	高雄大大新寬頻	1

(五) 請問貴公司骨幹及各項產品提供 IPv6 網路服務設備支援狀況、時程及相關規劃為何？

下表根據 Cable 業者，對於骨幹及各項產品提供 IPv6 網路服務設備支援狀況、時程及相關規劃的問題項目回覆統計表，依照 Cable 業者回覆來看，20 家業者中有針對骨幹支援 IPv6 部分回覆

共有 15 家業者，針對其骨幹所用路由設備之 IPv6 支援能力，其中有家 14 業者在這部分的整備狀態都已經達到完全可支援，比例為 70%;僅有中嘉寬頻回覆其骨幹設備並未達到 100%支援 IPv6，業者仍有少部分 Border Router 及 Edge Router 尚待更新,但支援率也有 90%以上。而有 5 家業者未對骨幹設備支援 IPv6 狀況回覆，比例為 25%。而關於骨幹提供 IPv6 的時程及規劃，目前已經提供 IPv6 服務的業者僅有台灣基礎開發、台灣寬頻通訊及中嘉寬頻共 3 家業者比例為 15%;台灣基礎開發因有企業客戶提出需求，因此其 IPv6 骨幹服務已經上線，台灣寬頻通訊今年（108 年）6 月推出家用客戶使用者可申請試用 IPv6 連網服務，正式成為國內第一家支援 IPv6 的 Cable/MSO 業者，而中嘉寬頻因為連結 Google 服務需支援 IPv6，客戶及業務需求是業者推動服務升級的動力；另外天外天數位有線電視業者預計今年（108 年）將啟動 IPv6 骨幹服務上線計畫；世新有線電視及國聲有線電視 2 家業者，預計西元 2020 年(109 年)將啟動 IPv6 骨幹服務上線計畫;而凱擘寬頻、台固媒體、全國數位有線電視、大新店民主有線電視、新永安有線電視、新彰數位有線電視、三大有線電視及大台中數位有線電視共 8 家業者預計西元 2020（109 年）之後，才會啟動 IPv6 骨幹服務上線計畫；但也有部分業者包含超宇寬頻、洄瀾有線電視、東亞有線電視、高雄大大新寬頻及北都數位有線電視共 5 家無導入計畫，各業者回覆理由整理如下：

- ◆ 超宇寬頻：IP 足夠，目前超宇寬頻採用 CGNAT 以 1:10 的比例配發給用戶使用，目前 IPv4 數量仍足夠，因此短期內沒有規劃進行 IPv6 網路服務升級計畫。
- ◆ 洄瀾有線電視：目前公司大部分軟硬體設備不支援 IPv6。

◆ 東亞有線電視：目前公司大部分軟硬體設備不支援 IPv6。

◆ 高雄大大新寬頻：經費、營運策略。尚無考慮推動 IPv6。

◆ 北都數位有線電視：相關人員技能不成熟。

詳細的問卷回覆請參考下表所列。

表 13、Cable 業者骨幹及提供 IPv6 網路服務時程規劃統計表

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
請問貴公司骨幹及各項產品提供 IPv6 網路服務設備支援狀況、時程及相關規劃為何？(複選)																					
(一). 骨幹所用路由設備之 IPv6 支援能力為何?																					
	100%	100%	100%	×	100%	100%	100%	100%	100%	100%	100%	100%	100%	×	×	×	×	100%	<100%	100%	
提供 IPv6 的時程及相關規劃?																					
已提供																					
			✓					✓											✓		3
2019 年（108 年）																					
					✓																1
2020 年（109 年）																					
										✓	✓										2
2020 年（109 年）之後																					
	✓	✓		✓			✓		✓			✓	✓							✓	8
若無計畫導入請說明原因																					
						✓									✓	✓	✓	✓			5
(二). 各項服務(請填寫貴公司有提供的服務項目)																					
Cable Modem 上網																					
1. 服務所用網路設備之 IPv6 支援能力為何？																					

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
	<100%	<100%	<100%	100%	<100%	100%	<100%	<100%	<100%	<100%	<100%	100%	100%	<100%	<100%	<100%	×	100%	100%	×	
2. 服務是否使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶?																					
	否																				
			✓		✓		✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓		**13**
	是 ，若回答是，此服務一個 Public IP 給客戶的比例____																				
	✓	✓		✓		✓															**4**
3. 提供 IPv6 服務的時程?																					
	已提供，請填寫此服務的 IPv6 帳號數/用戶數																				
			✓																		**1**
	2019 年（108 年）提供																				
																					0
	2020 年（109 年）提供																				
					✓					✓	✓										**3**
	2020 年（109 年）之後提供																				
	✓	✓		✓			✓		✓			✓	✓					✓	✓		**9**
	請說明目前進行的階段																				
	規劃中，預計?年完成																				
	✓	✓			✓		✓		✓	✓	✓	✓	✓					✓			**10**
	測試中，預計?年完成																				
													✓					✓			**2**
	若無計畫導入請說明原因																				
						✓		✓						✓	✓	✓					**5**
光纖(FTTx)上網																					
1. 服務所用網路設備之 IPv6 支援能力為何？																					
	<100%	<100%	100%	×	×	100%	<100%	100%	<100%	×	×	100%	100%	×	×	×	<100%	×	×	100%	

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
2. 服務是否使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶?																					
	否																				
	✓	✓	✓				✓					✓								✓	**6**
	是 ，若回答是，此服務一個 Public IP 給客戶的比例____																				
						✓		✓					✓								**3**
3. 提供 IPv6 服務的時程?																					
	已提供，請填寫此服務的 IPv6 帳號數/用戶數																				
			✓					✓													**2**
	2019 年（108 年）提供																				
																					0
	2020 年（109 年）提供																				
																					0
	2020 年（109 年）之後提供																				
									✓			✓	✓							✓	**4**
	請說明目前進行的階段																				
	規劃中，預計?年完成																				
									✓			✓	✓							✓	**4**
	測試中，預計?年完成																				
																					0
	若無計畫導入請說明原因																				
	✓	✓				✓	✓										✓				**5**

下圖根據 Cable 業者的問卷回覆表，整理出有關骨幹設備提供 IPv6 網路服務的時程規劃統計圖。

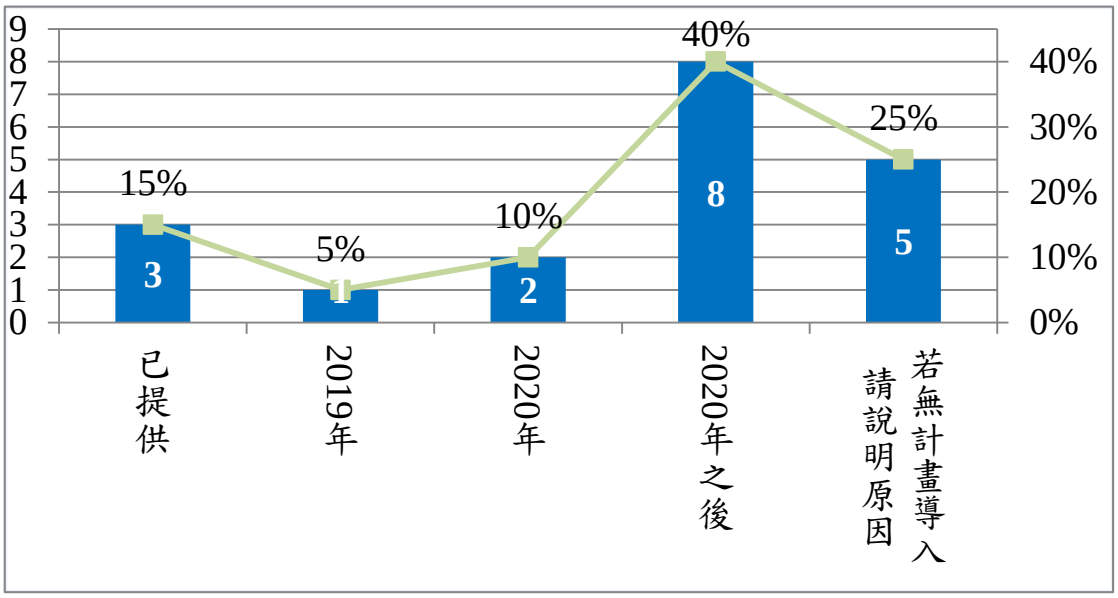

圖 21、Cable 業者問卷骨幹提供 IPv6 網路服務時程規劃統計圖

根據上表 Cable 業者的問卷回覆表，有關 Cable Modem 上網服務其網路設備之 IPv6 支援能力，調查的 20 家業者中共有 18 家業者提供相關資訊，而高雄大大新寬頻及大台中數位有線電視 2 家業者，並未提供 Cable Modem 上網服務；根據問卷統計結果目前有 6 家業者包含全國數位有線電視、超宇寬頻、新彰數位有線電視、三大有線電視、北都數位有線電視及中嘉寬頻，在設備已經達到 100%支援 IPv6；其他業者都還未完成全部的設備支援 IPv6 能力，其中以 DHCP server 及家用使用者的 Cable Modem 尚未更新為主；目前有凱擘寬頻、台固媒體、大新店民主有線電視、台灣基礎開發、新永安有線電視、南國有線電視、洄瀾有線電視及東亞有線電視共 8 家業者尚未完成 DHCP server 設備更新，因為此項設備費用較高昂，業者計畫逐年編列預算汰換舊設備，因此執行時間較長；另外台灣基礎開發及南國有線電視 2 家業者，除了 DHCP server 設備尚未完全更新外，其 CMTS 設備也未達 100%支援 IPv6；而台灣寬頻在 Cable Modem 上只有 50%支援 IPv6，世新

有線電視及國聲有線電視在 Cable Modem 上約有 60%支援 IPv6，洄瀾有線電視及東亞有線電視在 Cable Modem 上約有 70%支援 IPv6，而天外天數位有線電視，所有的 Cable Modem 都尚未支援 IPv6，Cable Modem 因舊有設備需更換數量龐大，無法在短期限內完成。有關 Cable Modem 上網服務提供 IPv6 時程規劃比例，請參考下圖統計業者回覆結果。

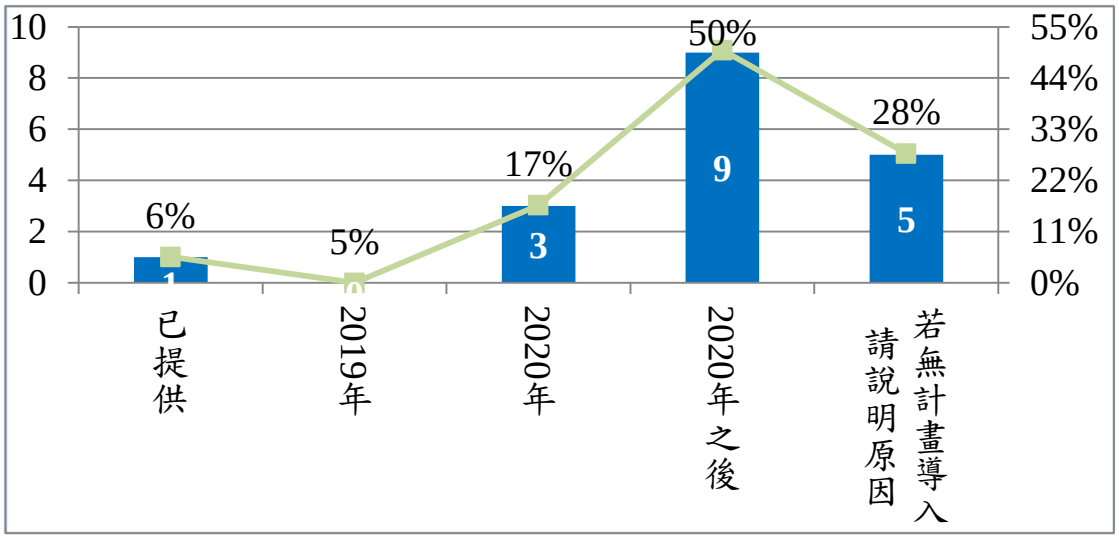

圖 22、Cable 業者問卷 Cable Modem 服務提供 IPv6 時程規劃統計圖

凱擘寬頻、台固媒體、全國數位有線電視及超宇寬頻共 4 家業者，其 Cable Modem 上網服務是使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶，服務一個 Public IP 給客戶的比例，其中凱擘寬頻、台固媒體及全國數位有線電視以 1:8 比例配發，而超宇寬頻以 1:10 比例配發。其他 14 家業者（包含台灣寬頻通訊、天外天數位有線電視、大新店民主有線電視、台灣基礎開發、新永安有線電視、世新有線電視、國聲有線電視、新彰數位有線電視、三大有線電視、南國有線電視、洄瀾有線電視、東亞有線電視、北都數位有線電視及中嘉寬頻）並未使用 CGNAT。

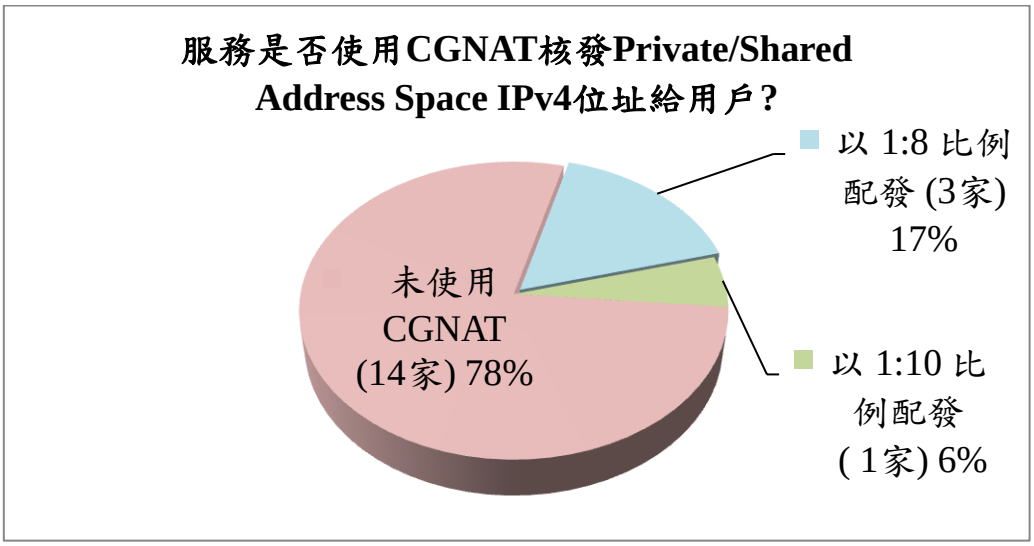

圖 23、Cable 業者問卷 Cable Modem 服務使用 CGNAT 核發 IPv4 比例

其中台灣寬頻通訊已於今年（108 年）導入支援 IPv6，為所有業者中最為積極；天外天數位有線電視、世新有線電視及國聲有線電視 3 家業者，規劃於明年（109 年），對 Cable Modem 上網服務提供支援 IPv6；全國數位有線電視、新彰數位有線電視、三大有線電視、北都數位有線電視及中嘉寬頻 5 家業者規劃於西元 2020 年（109 年）之後，而凱擘寬頻、台固媒體、大新店民主有線電視及新永安有線電視，4 家業者目前規劃將於西元 2023 年（112 年）為 Cable Modem 上網服務提供 IPv6 支援；另外有 5 家業者回覆〝無導入計畫〞，其理由整理如下：

◆ 無 IPv6 需求用戶。(台灣基礎開發)

台灣基礎開發雖然在骨幹設備已經可支援 IPv6，且也有企業客戶個別需求，為了服務該客戶而以專線支援該客戶 IPv6 連網服務，但對一般家庭用戶，因為要面對客戶數量較多，除技術能力是否到位，還需要考量包括維修及客服等相關支

援能力，目前該公司評估一般用戶並不一定重視連網服務是否支援 IPv6，因此還未考慮支援 IPv6。

◆ IP 足夠。(超宇寬頻)

◆ 設備不支援。(南國有線電視)

◆ 目前公司大部分軟硬體設備不支援 IPv6。(洄瀾有線電視、東亞有線電視)

部分有線電視業者如超宇寬頻雖然設備上已經具備可支援 IPv6 的能力，但公司政策並未積極推動，且有線電視的獨立系統業者在技術人員的配置上相對非常少，支援 IPv6 對業者而言需在技術人員、維修人員、及客服人員有相對應的能力支援，且目前國內尚未有有線電視支援 IPv6 的經驗可當參考，獨立系統業者大多採取觀望態度。

表 14、Cable 業者 Cable Modem 上網提供 IPv6 時程表

Cable Modem 上網提供 IPv6 時程	Cable業者	總計	比例
已提供		0	0%
西元 2019 年（108 年）	台灣寬頻通訊	1	5%
西元 2020 年（109 年）	天外天數位有線電視、世新有線電視及國聲有線電視	3	17%
西元 2020 年（109 年）之後	凱擘寬頻、台固媒體、大新店民主有線電視、新永安有線電視、全國數位有線電視、新彰數位有線電視、三大有線電視、北都數位有線電視、中嘉寬頻	9	50%
無計畫	台灣基礎開發、超宇寬頻、南國有線電視、洄瀾有線電視、東亞有線電視	5	28%
總　計			**100%**

高雄大大新寬頻和大台中數位有線電視是採用光纖到府，並不使用 Cable Modem，因此對 Cable Modem 支援 IPv6 時程並未回覆。以上 Cable Modem 服務是根據 18 家有提供此項服務業者回覆統計結果。

對於 Cable 業者所提供光纖上網服務調查，20 家業者中有 11 家業者有提供光纖上網服務（凱擘寬頻、台固媒體、台灣寬頻通訊、大新店民主有線電視、台灣基礎開發、新永安有線電視、超宇寬頻、新彰數位有線電視、三大有線電視、高雄大大新寬頻及大台中數位有線電視），比例為 55%；全國數位有線電視、天外天數位有線電視、世新有線電視、國聲有線電視、南國有線電視、洄瀾有線電視、東亞有線電視、北都數位有線電視及中嘉寬頻共 9 家業者並未提供光纖上網，比例為 45%。

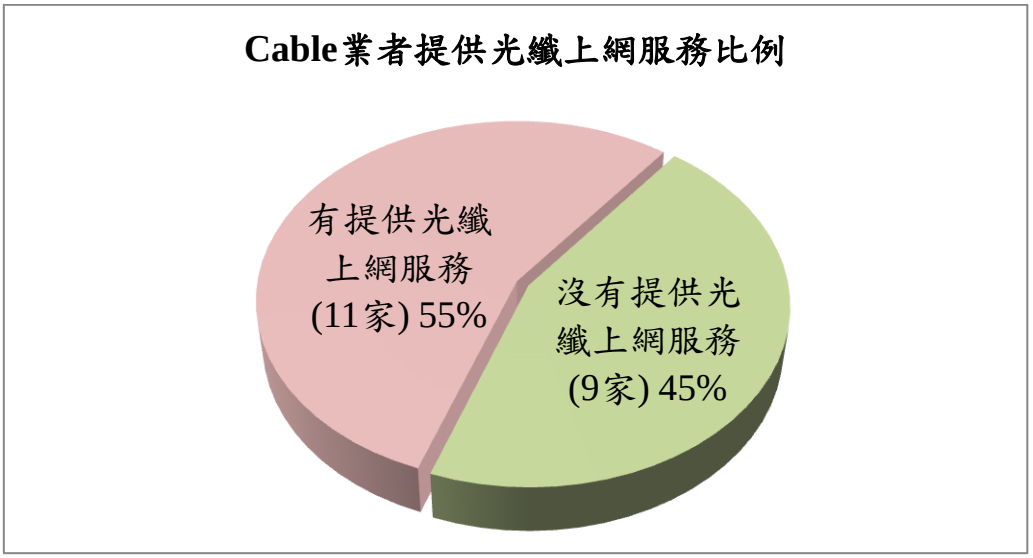

圖 24、Cable 業者提供光纖上網服務比例

台灣寬頻通訊、超宇寬頻、台灣基礎開發、新彰數位有線電視、三大有線電視及大台中數位有線電視 6 家業者回覆其網路設備之 IPv6 支援能力已經 100%整備完成，其他 4 家業者（凱擘寬頻、台固媒體、大新店民主有線電視及新永安有線電視）還未完成全部的設備支援能力，其中大部分以 VDSL 數據機（VDSL Modem，VTUR）設備尚未更新為主。高雄大大新寬頻未對設備支援程度進行回覆。

有關 IP 配發方式，超宇寬頻及台灣基礎開發 2 家業者採用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶，此服務一個 Public IP 配發給客戶的比例各為 1:10 及 1:8。

有關 Cable 業者光纖上網服務提供 IPv6 時程規劃，詳細資訊請參考表 15；下圖統計業者回覆結果。其中台灣基礎開發目前有能力提供 IPv6 網路服務，且有 1 家企業用戶已經申請啟用 IPv6 上網服務，但對一般家庭用戶服務尚無計畫；台灣寬頻通訊已於今年（108 年）導入支援 IPv6，目前正式進行用戶試用階段；新彰數位有線電視、三大有線電視及大台中數位有線電視共 3 家業者預計西元 2020 年（109 年）以後提供 IPv6 服務；新永安有線電視預計西元 2023 年（112 年）提供 IPv6 服務；另外有 5 家業者回覆〝無導入計畫〞比例最高約 46%，其理由整理如下：

- ◆ 陸續將用戶轉移成 Cable Modem 用戶。(凱擘寬頻、台固媒體及大新店民主有線電視)
- ◆ IP 足夠。(超宇寬頻)
- ◆ 經費、營運策略。(高雄大大新寬頻)

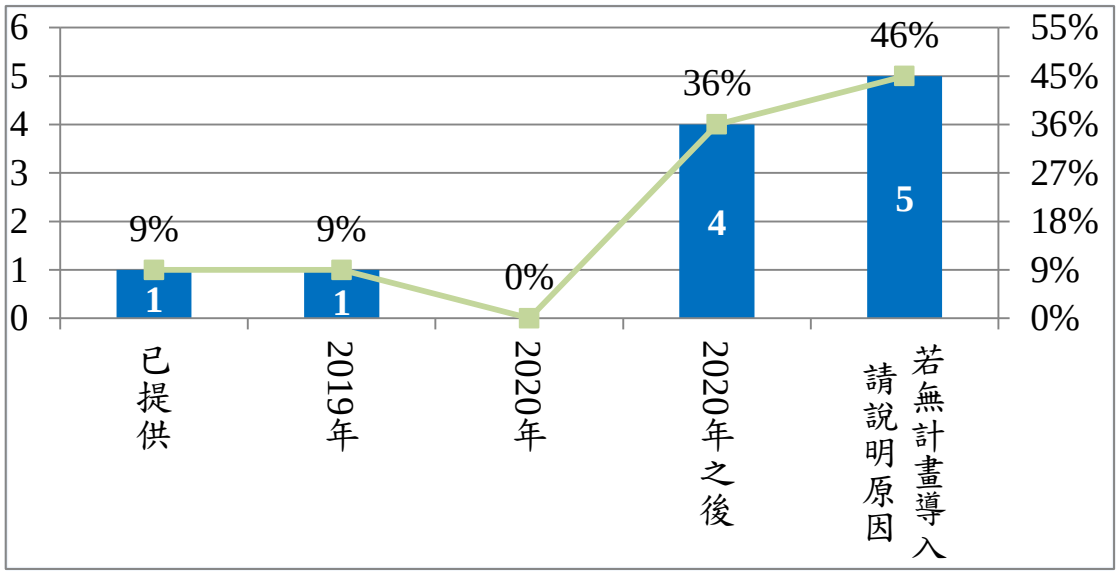

圖 25、Cable 業者問卷光纖服務提供 IPv6 時程規劃統計圖

表 15、Cable 業者光纖上網提供 IPv6 時程表

光纖上網提供 IPv6 時程	Cable業者	總計	比例
已提供	台灣基礎開發、台灣寬頻通訊	1	18%
西元 2019 年（108 年）		0	0%
西元 2020 年（109 年）		0	0%
西元 2020 年（109 年）之後	新永安有線電視、新彰數位有線電視、三大有線電視、大台中數位有線電視	4	36%
無計畫	凱擘寬頻、台固媒體、大新店民主有線電視、超宇寬頻、高雄大大新寬頻	5	46%
總　計			**100%**

Cable 業者主要上網服務以〝Cable Modem 上網〞及〝光纖上網服務〞為主，超宇寬頻除提供以上兩項服務外，另提供 PWLAN 無線上網服務，有關此服務所用網路設備之 IPv6 支援能力已經達 100%支援，業者並採用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶，此服務一個 Public IP 給客戶的比例為 1:10，業

者目前所擁有的 IPv4 數量足夠，因此還未有明確計畫導入支援 IPv6 上網服務。

(六) 貴公司提供 IPv6 服務時，預計增加支出主要用在哪些項目？

下表根據 Cable 業者，對於有關支援 IPv6 預計增加支出項目回覆統計表，依照 Cable 業者回覆來看，最多的預算支出為用在〝更新相關軟體系統〞業者勾選的比例為 85%，其次為〝更新硬體設備〞，有 75%比例的業者選擇此項目；其次為〝人員訓練〞上有 70%比例，為了支援 IPv6 連網服務，業者除了軟體及硬體投資外，技術人員、維修人員、及客服人員都需要相對應的能力支援，才能為用戶帶來良好的使用經驗，這些都需要時間準備及訓練；另外有關〝IPv6 連線費用〞，多家業者反應要支援 IPv4/IPv6 雙軌服務，業者同時配發 2 個 IP 位址給使用者時需付出雙倍費用，對業者形成不小的負擔，也大大降低業者主動積極投入的意願。

由業者所填排序計算出的權重加總來看，〝更新相關軟體系統〞及〝更新硬體設備〞平均權重相同，軟硬體的更新費用對業者而言是一筆可觀的投資；另外雖然勾選〝IPv6 連線費用〞的業者家數比〝人員訓練〞少，但權重卻比〝人員訓練〞多，尤其大型的 MSO 如凱擘寬頻和台固媒體，對這方面的考量更為重視。

下圖根據業者的問卷回覆，列出有關支援 IPv6 預計增加支出項目的統計圖。

表 16、Cable 業者問卷統計支援 IPv6 預計增加支出項目

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
貴公司提供 IPv6 服務時，預計增加支出主要用在哪些項目(複選，請於括號內以 1, 2, 3,...標示出該項目所需經費之比重排名，其中 1 最高，2 次高，以此類推)？																					
更新硬體設備																					
	3	3	1		1		3	2	2	1	1	3	1	1			1		1	1	
更新相關軟體系統(例如 DNS/Radius/DHCP/Web/E-mail 等)																					
	2	2	2		1	1	2	1	1	2	2	1	3	2			2	2	1	2	
人員教育訓練																					
	4	4	3		2		4	3	3			2	4	3			4	1	1	3	
IPv6 連線費用																					
	1	1	4			1	1		4			1	2				3				
其他，請說明_____																					
						1															

註：1, 2, 3,...標示出該項目所需經費之比重排名，其中 1 最高。業者未標註比重排名以 1 顯示。排名 1 換算成權重（weight）指數 5，排名 2 換算成權重指數 4，以此類推。下圖顯示〝w=x〞，代表該選項權重加總；〝a=x〞代表平均權重。

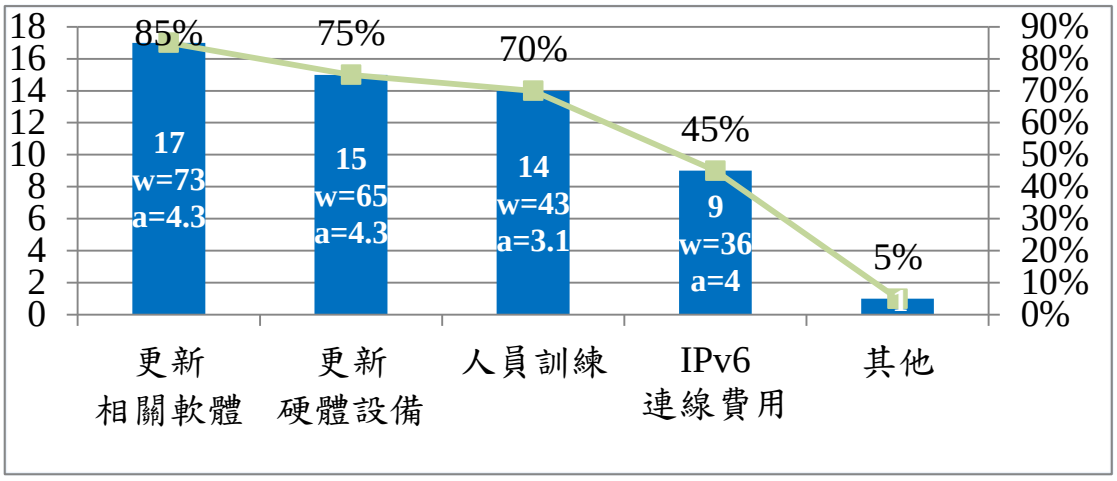

圖 26、Cable 業者問卷支援 IPv6 預計增加支出項目的統計圖

(七) 貴公司在 IPv6 可能面臨的問題有哪些？

下表根據 Cable 業者，對於有關支援 IPv6 可能面臨的問題項目回覆統計表，依照 Cable 業者回覆來看，業者最常遇到的問題是〝人員 IPv6 技術能力與管理經驗不足〞，其次為〝軟硬體支援度不足〞及〝投入成本高〞，再來是〝廠商 IPv6 技術能力不足〞為主要因素，其他選項比例較低。另外全國數位有線電視其機上盒採用 Android 系統，可提供使用者安裝各項服務，因此在管理上較複雜，業者需更改的應用也較多，業者回覆內容如下所述：

◆ IPv6 無法達成公司原有 IPv4 各服務的功能，針對機上盒管理、應用服務。(全國數位有線電視)

另外三大有線電視提到支援 IPv6 對目前管理無法支援原因如下所述：

◆ IPv6 無法達成公司原有 IPv4 各服務的功能，網路管理/監控系統未支援 IPv6。(三大有線電視)

詳細的問卷回覆請參考下表。下圖根據 Cable 業者的問卷回覆，列出有關支援 IPv6 可能面臨的問題項目的統計圖。

表 17、Cable 業者問卷統計支援 IPv6 可能面臨的問題

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
貴公司在 IPv6 可能面臨的問題有哪些(複選)？																					
投入成本高																					
	✓	✓		✓		✓	✓		✓	✓	✓			✓			✓		✓	✓	**12**
軟硬體支援度不足																					
	✓	✓		✓	✓		✓	✓	✓	✓	✓		✓	✓			✓		✓	✓	**14**
IPv6 無法達成公司原有 IPv4 各服務的功能(複選)																					
				✓									✓								**2**
	管理功能，例如_																				
													✓								**1**
	安全功能，例如_																				
																					0
	效能，例如_																				
																					0
	其他_																				
				✓																	**1**
人員 IPv6 技術能力與管理經驗不足																					
	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓	✓			✓	✓	✓	✓	**15**
廠商 IPv6 技術能力不足																					
	✓	✓	✓				✓												✓		**5**
上游國際 ISP 無提供 IPv6 路由互連																					
					✓																**1**
客戶使用 IPv6 服務會產生體驗(QoE)不佳之問題																					
												✓									**1**
其他 _																					
																					0
本公司目前並無上述問題																					
																					0

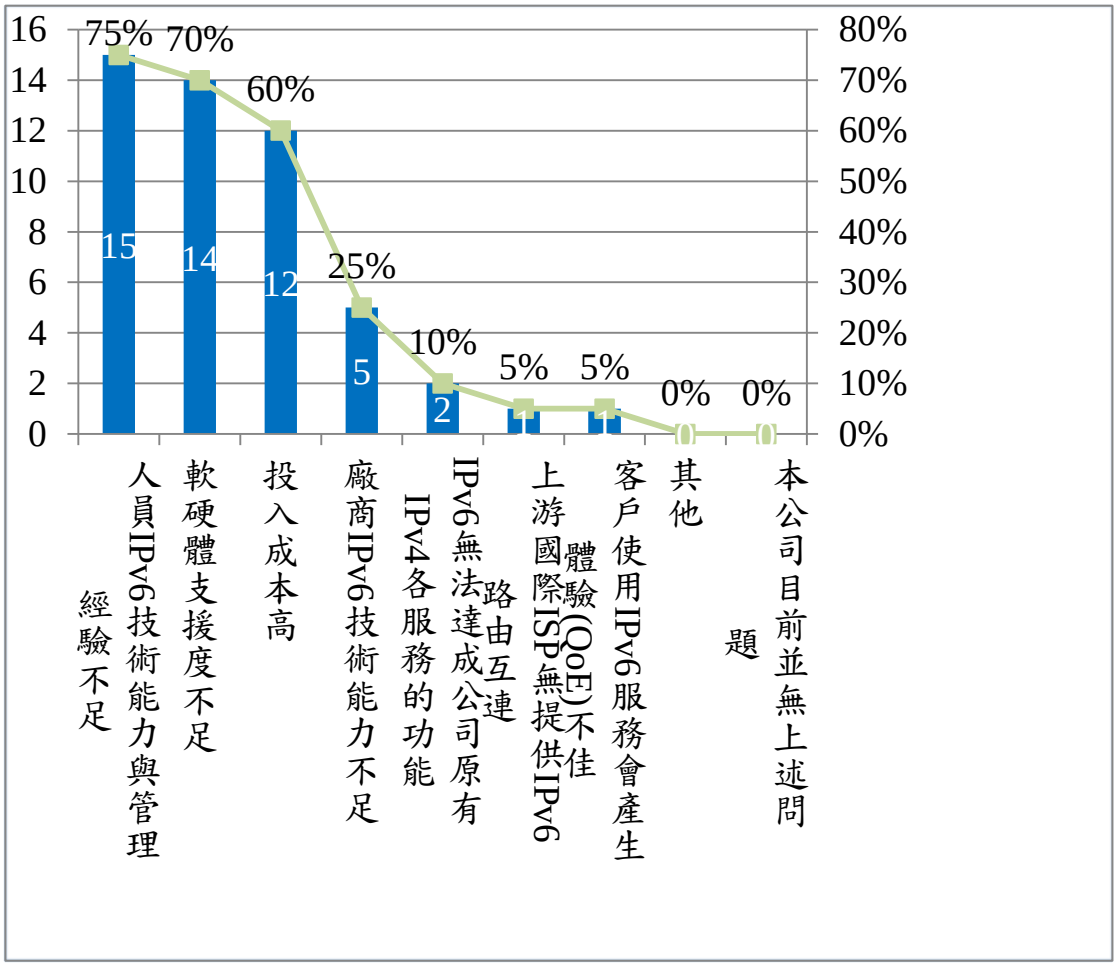

圖 27、Cable 業者問卷支援 IPv6 可能面臨的問題統計圖

(八) 貴公司是否認為在 IPv6 網路發展上有政府可以協助之項目？

下表根據 Cable 業者，對於有關支援 IPv6 網路發展上希望政府協助項目回覆統計表，依照 Cable 業者回覆來看，就政府可以協助之項目上，調查 20 家業者中，有 14 家業者都希望政府能夠〝提供獎勵補助措施〞，有 9 家業者希望政府能夠〝提供投資抵減優惠〞以減輕業者投資負擔，加速提高業者更新技術服務的腳步和意願。

業者回覆〝提供獎勵補助措施〞的意見整理如下：

◆ 相關設備補助措施。(天外天數位有線電視、三大有線電視和中嘉寬頻)

◆ 軟硬體建置獎勵補助措施。(台灣基礎開發)

◆ 小型實驗區補助措施。(世新有線電視、國聲有線電視)

◆ 提供人員教育訓練。(新彰數位有線電視)

◆ IPv6 用戶連網數(設定上限)。(高雄大大新寬頻)

業者回覆希望政府〝提供投資抵減優惠〞的意見整理如下：

◆ Router/Switch/DHCP 設備採購投資抵減優惠。(凱擘寬頻、台固媒體及大新店民主有線電視)

在訪談過程中多家業者反應面臨市場多方競爭壓力，如有線電視業者間的競爭、網路電視、及 OTT（Over-The-Top）網路隨選串流影片服務競爭及行動網路的興起等，造成部分客戶流失，業者同時需要投資高速傳輸以提升上網速度，對支援 IPv6 的支出上相對能投入的資源較少，多數業者認為支援 IPv6 的急迫性並不高，且不會影響到業者營運狀況，因此業者推動上多處於被動狀態，如果政府能提供獎勵補助措施或投資抵減優惠，對業者有正向的意義。

下圖根據 Cable 業者的問卷回覆，列出有關支援 IPv6 網路發展上希望政府協助項目的統計圖。

表 18、Cable 業者統計支援 IPv6 網路發展上希望政府協助項目

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
貴公司是否認為在 IPv6 網路發展上有政府可以協助之項目(複選)？																					
提供獎勵補助措施，例如_																					
			✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓			✓		✓	✓	**14**
提供投資抵減優惠，例如_																					
	✓	✓	✓	✓		✓	✓		✓										✓	✓	**9**
無需要政府協助																					
																		✓			**1**
其他 _																					
																			✓		**1**

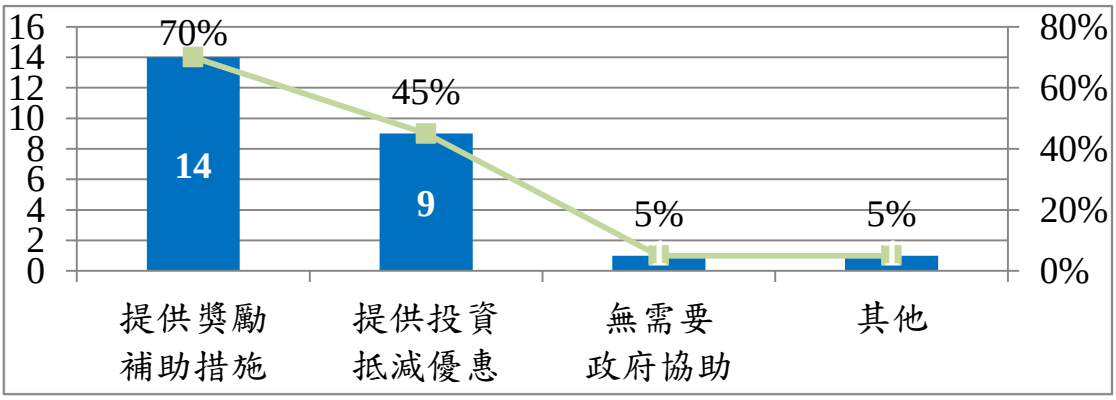

圖 28、Cable 業者支援 IPv6 網路發展上希望政府協助項目統計圖

(九) 貴公司若提供用戶 IPv6 網路連線服務，將會如何提供配發用戶 IPv6 位址？

下表根據 Cable 業者，對於有關支援 IPv6 連線服務位址配發方式項目回覆統計表，依照 Cable 業者回覆來看，20 家業者中，多

家業者如超宇寬頻、南國有線電視、洄瀾有線電視及東亞有線電視等目前還沒有明確支援 IPv6 計畫，因此對此問題並未回覆；其餘業者中有 4 家業者（凱擘寬頻、台固媒體、天外天數位有線電視及大新店民主有線電視）可以根據使用者需求，支援〝動態配發 IPv6 位址或網段(Prefix)〞及〝固定配發 IPv6 位址或網段(Prefix)〞兩種配發方式；台灣寬頻通訊、全國數位有線電視、新永安有線電視、世新有線電視、國聲有線電視、新彰數位有線電視、三大有線電視、高雄大大新寬頻、中嘉寬頻及大台中數位有線電視共 10 家業者，是採取〝動態配發 IPv6 位址或網段(Prefix)〞方式；而台灣基礎開發因應企業客戶需求支援 IPv6 連網服務，採用〝固定配發 IPv6 位址或網段(Prefix)〞方式配發,除既有單一客戶需求外，並未做其他規劃。北都數位有線電視屬於新進業者，目前主力在於業務擴張，對於 IPv6 網路服務的想法，公司內部尚未有明確的想法，對於如何提供配發用戶 IPv6 位址方式還沒有明確規劃，因此勾選〝其他〞選項。

表 19、Cable 業者統計支援 IPv6 連線服務位址配發方式

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
貴公司是否認為在 IPv6 網路發展上有政府可以協助之項目(複選)？																					
動態配發 IPv6 位址或網段(Prefix)																					
	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓				✓		✓	✓	**14**
固定配發 IPv6 位址或網段(Prefix)																					

Cable 問卷調查內容	凱擘寬頻	台固媒體	台灣寬頻通訊	全國數位有線電視	天外天數位有線電視	超宇寬頻	大新店民主有線電視	台灣基礎開發	新永安有線電視	世新有線電視	國聲有線電視	新彰數位有線電視	三大有線電視	南國有線電視	洄瀾有線電視	東亞有線電視	高雄大大新寬頻	北都數位有線電視	中嘉寬頻	大台中數位有線電視	總計
	✓	✓			✓		✓	✓													5
其他 _																					
																		✓			1

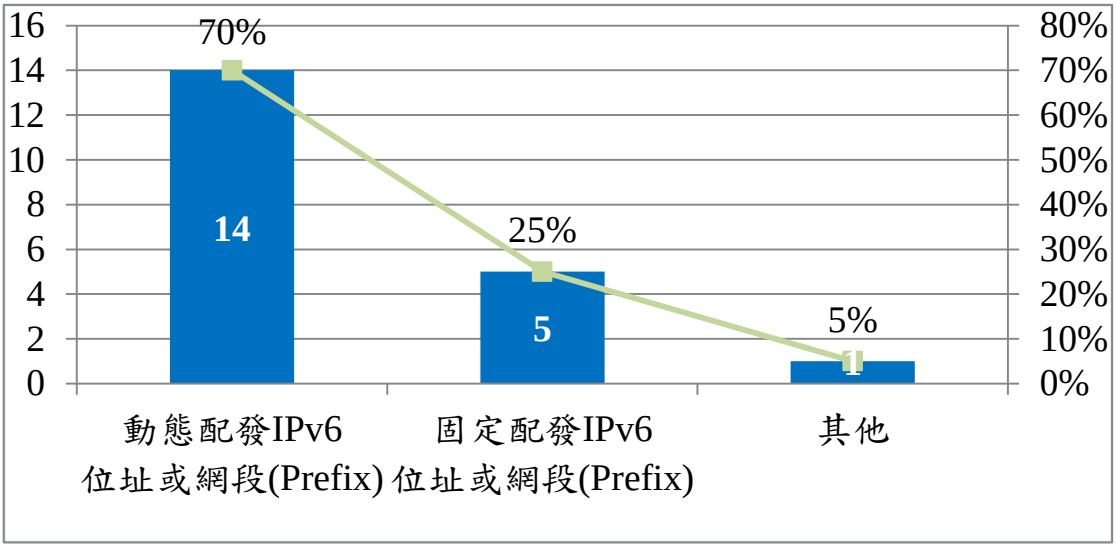

圖 29、Cable 業者支援 IPv6 連線服務位址配發方式統計圖

表 20、Cable 業者支援 IPv6 連線服務位址配發方式比例

位址或網段(Prefix)配發方式	IASP業者	總計	比例
只支援動態配發	台灣寬頻通訊、全國數位有線電視、新永安有線電視、世新有線電視、國聲有線電視、新彰數位有線電視、三大有線電視、高雄大大新寬頻、大台中數位有線電視及中嘉寬頻	10	50%

位址或網段(Prefix)配發方式	IASP業者	總計	比例
只支援固定配發	台灣基礎開發	1	5%
支援動態及固定兩種配發方式	凱擘寬頻、台固媒體、天外天數位有線電視及大新店民主有線電視	4	20%
其他	北都數位有線電視	1	5%
未回覆	超宇寬頻、南國有線電視、洄瀾有線電視、東亞有線電視	4	20%
總　計			**100%**

Cable 業者面訪紀錄表，詳細請參考附錄一；業者問卷調查表回覆內容，詳細請參考附錄二。

二. IASP 業者

台灣 5 家行動業者中，中華電信、遠傳電信及台灣大哥大 3 家行動業者在 107 年已經陸續支援 IPv6 連網服務，因此今年（108 年）度僅以問卷進行調查；為了解台灣主要 IASP 業者不同類型網路服務在 IPv6 的建置狀況，除行動業者外，並將固網業者新世紀資通及台灣固網納入問卷調查範圍，中華電信行動通信及固網服務也會納入調查範圍；而亞太電信及台灣之星將透過面訪及問卷並行的方式進行，以期能更了解這 2 家行動業者在 IPv6 的佈建計畫，下表為行動業者面訪時程表：

表 21、行動業者面訪時程表

序號	公司名稱	面訪日期
1	亞太電信	3月14日
2	台灣之星	4月10日

由固網及行動電信 IASP 業者共回收 7 份問卷，以下就問卷內容，彙整統計業者回覆的狀況：

下表為 IASP 業者是否有 IPv4 位址面臨不足的狀況，針對此問題統整業者回覆結果如下所示 ：

表 22、IASP 業者是否有 IPv4 位址面臨不足的問題統計表

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
貴公司 IPv4 位址會在何時面臨不足？								
沒有 IPv4 位址不足的問題							✓	**1**
預期在西元__？__年發生 IPv4 位址不足	✓	✓	✓	✓	✓	✓		**6**
貴公司是否已在進行 IPv4 位址不足的相關策略?								
沒有進行 IPv4 位址不足相關策略，請問原因為何?								**0**
已在進行 IPv4 位址不足相關策略，以下哪些是在進行的項目(複選)	✓	✓	✓	✓	✓	✓	✓	**7**
使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶	✓	✓		✓		✓	✓	**5**
減少各項服務 IPv4 核發數量或以價制量		✓	✓		✓	✓		**4**
回收用戶閒置 IPv4 位址	✓	✓	✓		✓	✓		**5**
從其他 ISP 中取用 IPv4 位址			✓					**1**
配發用戶 IPv6 位址提供用戶 Native IPv6 連線服務		✓				✓		**2**
其他	✓							**1**

(一) 貴公司 IPv4 位址會在何時面臨不足？

IASP 業者對於是否有 IPv4 位址面臨不足的問題，在回收的 7 份問卷中，台灣大哥大回覆在西元 2017 年(106 年)，即 2 年前就已經有 IPv4 位址不足的情況，是最早面臨 IPv4 資源不足的業者。行動業者亞太電信、及 2 家固網業者台灣固網及新世紀資通，預期於明年（109 年），將面臨 IPv4 位址不足的情況。而中華電信預期西元 2021 年（110 年），將發生 IPv4 位址不足的情況，相較去年（107 年）預估為西元 2020 年（109 年），目前 IPv4 資源使用需求預估趨勢沒有太大改變。而遠傳電信去年（107 年）回覆〝沒

有 IPv4 位址不足的問題〞，今年（108 年）預估於西元 2022 年（111 年）之後可能會產生 IPv4 位址不足，在行動電信業者中 IPv4 位址資源相對充足。而台灣之星回覆〝沒有 IPv4 位址不足的問題〞，主要原因是以 CGNAT 配發使用者共用 IP 資源為因應策略。

表 23、IASP 業者預期面臨 IPv4 不足時程表

預期面臨 IP 不足時程	IASP業者	總計	比例
西元 2017 年（106 年）	台灣大哥大	1	14%
西元 2020 年（109 年）	亞太電信、台灣固網及新世紀資通	3	44%
西元 2021 年（110 年）	中華電信	1	14%
西元 2022 年（111 年）	遠傳電信	1	14%
沒有 IPv4 位址不足	台灣之星	1	14%
總　計			**100%**

(二) 貴公司是否已在進行 IPv4 位址不足的相關策略?

下表針對有關 IASP 業者，目前是否已在進行 IPv4 位址不足相關策略統計表。由問卷回覆結果可看出，所有業者都在積極進行 IPv4 位址不足相關策略。其中業者主要採取的策略為〝使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶〞，及〝回收用戶閒置 IPv4 位址〞所佔比例為約 71%；其次為〝減少各項服務 IPv4 核發數量或以價制量〞所佔比例為約 57%；遠傳和亞太電信並回覆已經開始進行〝配發用戶 IPv6 位址提供用戶 Native IPv6 連線服務〞。此外中華電信在〝其他〞的選項回覆如下：

◆ 上網服務已導入 Dual stack（已支援 IPv4/IPv6 雙軌服務）。

下圖根據 IASP 業者的問卷回覆表，統整列出有關業者對於 IPv4 位址不足相關策略，已進行因應項目統計圖。

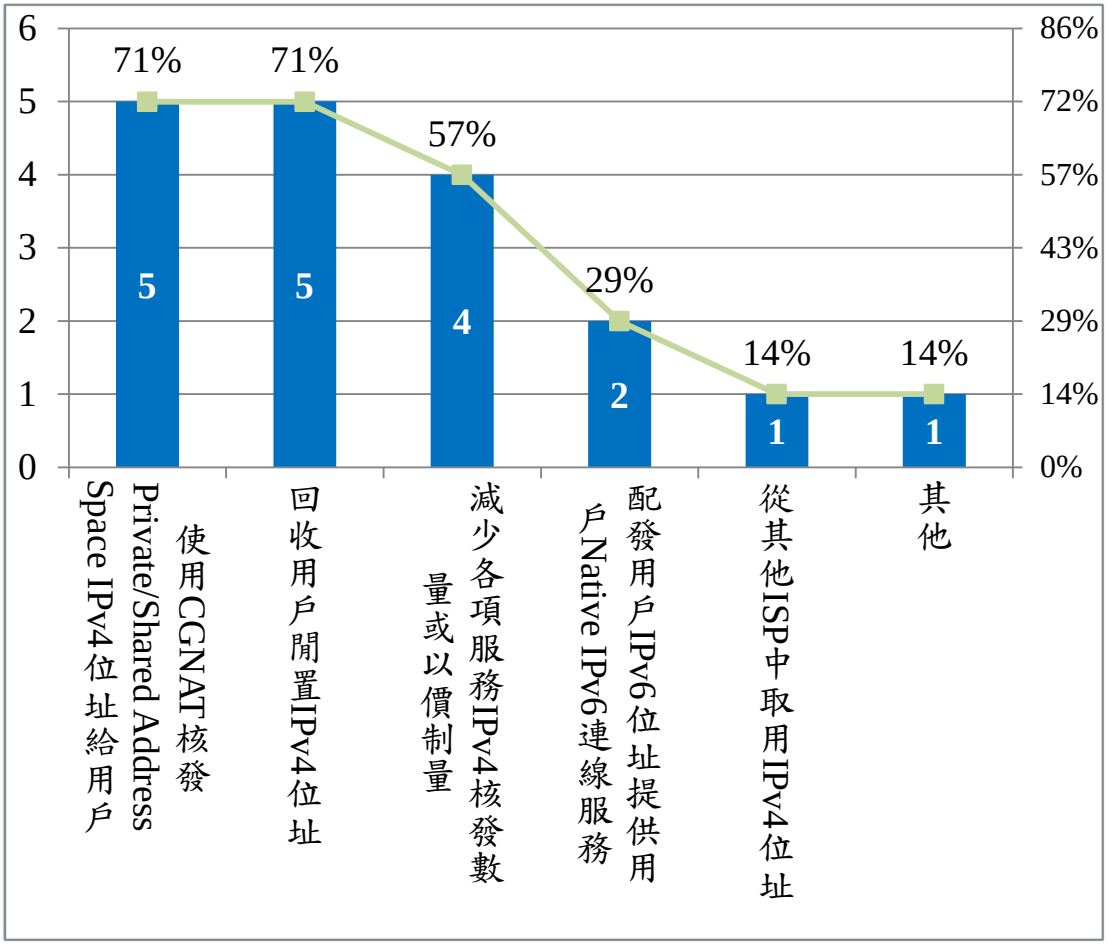

圖 30、IASP 業者對於 IPv4 位址不足所進行相關策略的統計圖

(三) 若貴公司未提供 IPv6 服務考慮的原因為何呢？

中華電信和遠傳電信都已經提供使用者 IPv6 的連線服務，並未對此問題回覆。下表根據業者有回覆對於如果未提供 IPv6 服務考慮的原因為何的問題項目回覆統計表，依照 IASP 業者回覆來看，其中業者以勾選〝目前業務以 IPv4 為主〞的選項為最多，有 5 家業者勾選比例為 71%；其次為〝提供 IPv6 不會增加收入〞，有 2 家業者勾選比例為 29%，問卷統計資訊請參考下表。由業者回覆的統計結果可看出，支援新服務業者最在意的因素是有沒有增加營收，或是來自於客戶或業務上的需求。下圖根據 IASP 業者的問卷回覆表，統整列出有關未提供 IPv6 服務考慮的原因的統計圖。

表 24、IASP 業者問卷統計未提供 IPv6 服務考慮的原因

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
若貴公司未提供 IPv6 服務考慮的原因為何呢？(複選)								
目前業務以 IPv4 為主			✓	✓	✓	✓	✓	**5**
服務升級 IPv6 所需的成本大於使用 IPv4 的成本			✓					**1**
目前公司大部分軟硬體設備不支援 IPv6								**0**
目前公司政策並未推動 IPv6								**0**
提供 IPv6 不會增加收入			✓			✓		**2**
上游 ISP 路由不支援 IPv6								**0**
其他，請說明_____								**0**

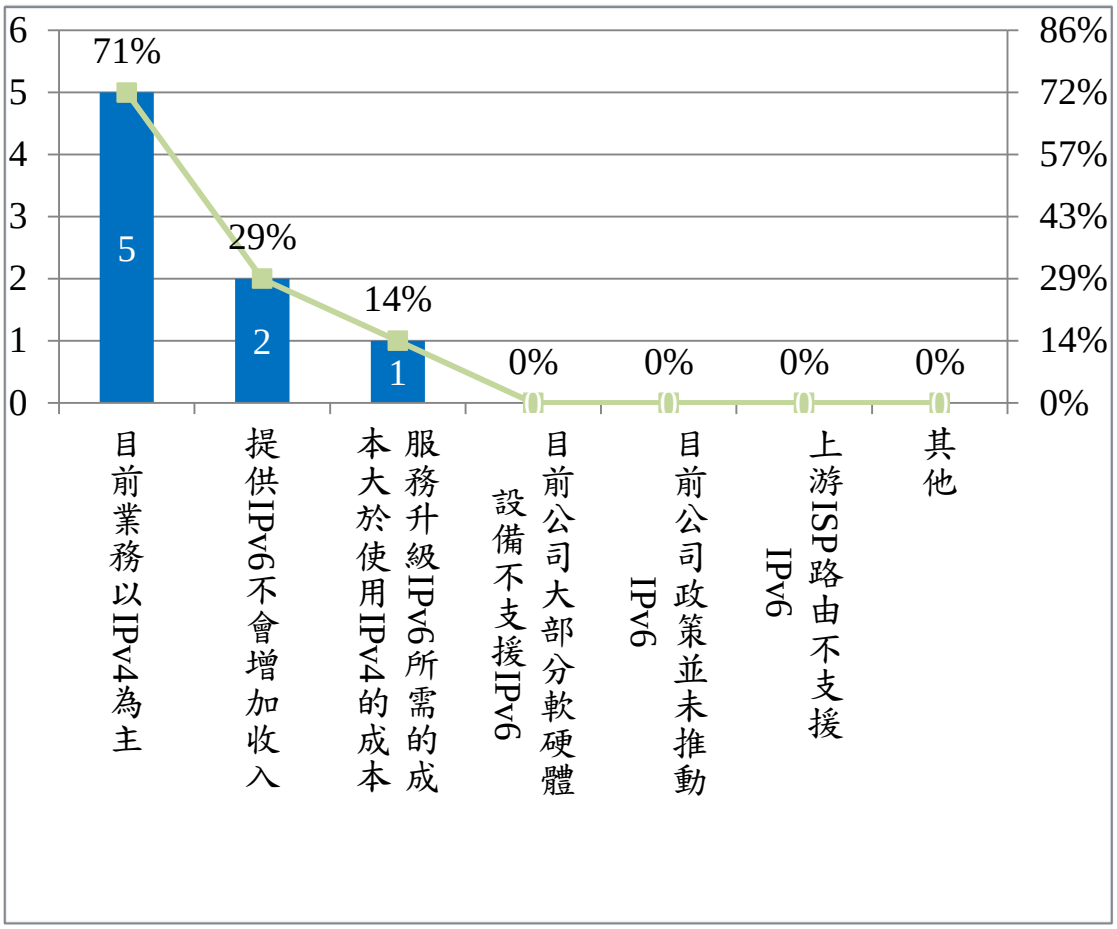

圖 31、IASP 業者問卷未提供 IPv6 服務考慮的原因統計圖

(四) 貴公司的 IPv6 位址申請及 IPv6 路由狀況為何？

下表根據 IASP 業者對於 IPv6 位址申請及 IPv6 路由狀況的問題回覆統計表，依照業者回覆來看，已經有 6 家業者〝已申請 IPv6 位址且將 IPv6 放在全球路由〞，整備的達成狀況已經到 86%比例，目前只有台灣之星已申請 IPv6 位址但尚未將 IPv6 放在全球路由，預計今年（108 年）底會將 IPv6 位址放在全球路由。問卷回覆統計資料請參考下表。

表 25、IASP 業者問卷統計 IPv6 位址申請及 IPv6 路由狀況

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
貴公司的 IPv6 位址申請及 IPv6 路由狀況為何？								
尚未申請 IPv6 位址，預計西元_____年申請 IPv6								**0**
已申請 IPv6 位址，但尚未將 IPv6 放在全球路由，預計西元_____年將 IPv6 放在全球路由							✓	**1**
已申請 IPv6 位址且將 IPv6 放在全球路由。	✓	✓	✓	✓	✓	✓		**6**

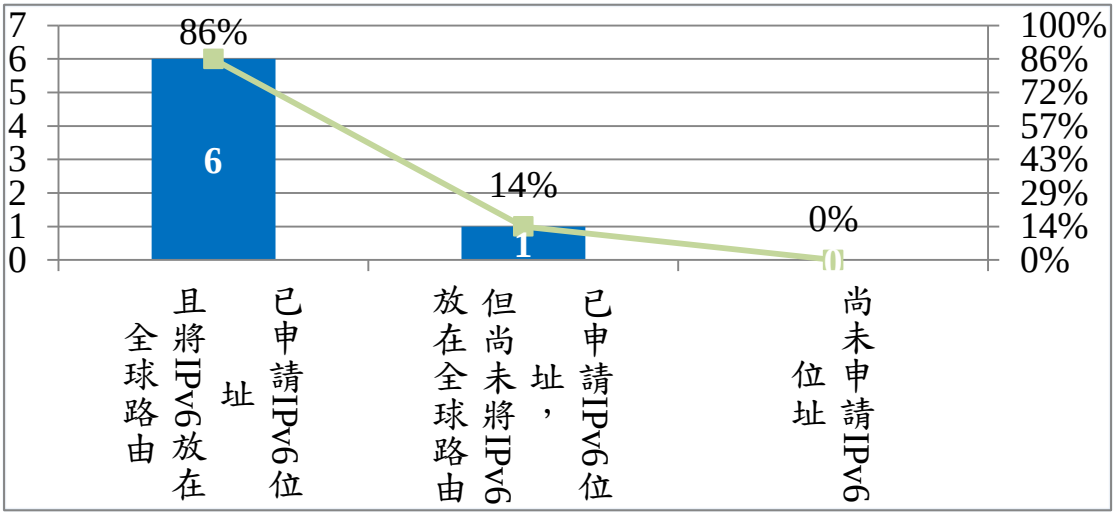

圖 32、IASP 業者問卷 IPv6 位址申請及 IPv6 路由狀況的統計圖

(五) 請問貴公司骨幹及各項產品提供 IPv6 網路服務設備支援狀況、時程及相關規劃為何？

下表根據 IASP 業者，對於骨幹及各項產品提供 IPv6 網路服務設備支援狀況、時程及相關規劃的問題項目回覆統計表，依照 IASP 業者回覆來看，其中業者針對其骨幹所用路由設備之 IPv6 支援能力，7 家 IASP 業者在這部分的整備狀態都已經達到全部設備都支

援 IPv6。而關於骨幹提供 IPv6 連網服務的時程及相關規劃，目前中華電信、遠傳電信、新世紀資通、台灣大哥大、台灣固網及亞太電信 6 家業者已經將服務上線，而台灣之星規劃於今年(108 年）底提供服務，目前已開始進行內部測試及試用，預計 109 年 3 月中會正式開放給一般用戶使用。

IASP 服務調查，分為光纖(FTTx)上網、Co-Location/IDC 服務、雲端（Cloud）服務、PWLAN 無線上網、及 4G 行動上網等服務類別，以下針對各項服務，統計 IASP 提供 IPv6 網路服務設備支援狀況、時程及相關規劃，描述如下：

1. 光纖(FTTx)上網

中華電信、新世紀資通、台灣固網及亞太電信 4 家業者有提供固網光纖上網服務，目前 4 家業者所用網路設備之 IPv6 支援能力，都還未達到全部設備都支援 IPv6。針對中華電信固網光纖(FTTx)上網的整備情形調查，其中主要是 L3 Switch（HiNet 接取設備專線路由器）及家庭閘道器（Home Gateway，HGW）尚未全部支援，目前約完成 60%的設備更新；新世紀資通主要是 Radius Server 尚未支援；而台灣固網和亞太電信主要是寬頻遠程接入伺服器(Broadband Remote Access Server，BRAS)設備尚未支援。中華電信及新世紀資通服務已經正式上線，亞太電信計畫於明年（109 年）提供服務，而台灣固網針對用戶光纖上網，目前沒有計畫提供用戶 IPv6 連網服務。

表 26、IASP 業者光纖上網提供 IPv6 時程表

光纖上網提供 IPv6 時程	IASP 業者	總計	比例
已提供	中華電信及新世紀資通	2	50%
西元 2020 年（109 年）	亞太電信	1	25%
無計畫	台灣固網	1	25%

2. Co-location/IDC 服務

根據業者問卷回覆中華電信、新世紀資通、台灣固網及亞太電信 4 家業者有提供 Co-location/IDC 網路服務，目前 4 家業者在 Co-location/IDC 服務所使用的網路設備 IPv6 支援能力，已經完成全部設備支援 IPv6，且 4 家業者都可提供給企業用戶使用支援 IPv6 網路服務。

表 27、IASP 業者 Co-location/IDC 服務提供 IPv6 時程表

Co-location/IDC 服務提供 IPv6 時程	IASP業者	總計	比例
已提供	中華電信、新世紀資通、台灣固網及亞太電信	4	100%

3. 雲端（Cloud）服務

針對雲端（Cloud）服務目前有中華電信及台灣固網 2 家業者經營此業務。中華電信此服務網路設備之 IPv6 支援能力，尚未完成 100%的設備支援能力，只有極少部分防火牆（Firewall）及伺服器負載平衡（Server Load Balance，SLB）尚未支援 IPv6，其比例低於 3%以下；目前此服務已經提供給企業用戶使用支援 IPv6 網路服務。台灣固網在設備建置上已經達到全部設備支援 IPv6 網路服務，該公司預計於西元 2020 年（109 年）支援 IPv6 網路服務。

表 28、IASP 業者雲端服務提供 IPv6 時程表

雲端服務提供 IPv6 時程	IASP業者	總計	比例
已提供	中華電信	1	50%
西元 2020 年（109 年）	台灣固網	1	50%

4. PWLAN 無線上網

目前中華電信及台灣固網 2 家業者有支援 PWLAN（Public Wireless Local AreaNetwork，公眾無線區域網路）無線上網服務。針對中華電信的 PWLAN 無線上網整備情形，目前服務網路設備之 IPv6 支援能力，只有 WiFi Gateway 尚未完成全部設備支援能力，但其設備容量支援 IPv6 比例已經達到 99% 以上，接近完全支援；此服務已經正式上線，可讓用戶使用 IPv6 連線上網。台灣固網也是 WiFi Gateway 尚未完成 100%的設備支援 IPv6 能力，目前支援比例達 83%，業者並沒有提供 IPv6 網路服務計畫，無導入計畫原因說明如下所述：

- ◆ PWLAN 已導入 CGNAT 服務，IPv4 位址充足。
- ◆ 目前共計有 6,800 多個 WiFi AP，每天僅 30,000 人次使用，使用人數偏低，因此無規劃提供 IPv6 服務。
- ◆ 依用戶使用觀察，目前並無成長之趨勢，即使用人次及流量的趨勢都是遞減。

表 29、IASP 業者 PWLAN 無線上網提供 IPv6 時程表

PWLAN 無線上網提供 IPv6 時程	IASP 業者	總計	比例
已提供	中華電信	1	50%
無計畫	台灣固網	1	50%

5. 4G 行動上網

5 家行動業者中華電信、遠傳電信、台灣大哥大、亞太電信及台灣之星，在 4G 行動上網服務的網路設備之 IPv6 支援能力，都已經達到全部的支援。目前所有行動業者服務都有使用

CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶，以因應行動業務量需求增加，中華電信、遠傳電信及台灣大哥大其核發比例為1:16。但台灣大哥大因IPv4位址不足情況較嚴重，部分 CGNAT 核發比例提高為 1:64。亞太電信和台灣之星 CGNAT 核發比例也達 1:64。顯示出行動業者能支配的 IPv4 位址，呈現資源不足的情況較明顯，業者必須提高使用者共用 IP 的比例，以因應需求。CGNAT 設備會將每個 IP 可使用的連接埠（Port）數量 65,535 個,平均分配給共用使用者，當核發比例為 1:64，每個用戶約可分配到 1 千個左右連接埠，當使用者同時開啟過多應用使用網路連結，可能影響連線的使用品質。IP 位址共用的比例並非無限制，5G 及物聯網發展對 IP 需求勢必會再增加，為因應未來環境支援 IPv6 有其必要性。

表 30、IASP 業者 4G 行動上網提供 IPv6 時程表

4G 行動上網提供 IPv6 時程	IASP業者	總計	比例
已提供	中華電信、遠傳電信、台灣大哥大及亞太電信	4	80%
西元 2019 年（108 年）	台灣之星	1	20%

表 31、IASP 業者 4G 行動上網 CGNAT IP 位址核發比例表

CGNAT IP 位址核發比例	IASP業者	總計	比例
1 : 16	中華電信、遠傳電信及台灣大哥大（部分）	2.5	50%
1 : 64	台灣大哥大（部分）、亞太電信及台灣之星	2.5	50%

表 32、IASP 業者提供 IPv6 支援時程統計表

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
請問貴公司骨幹及各項產品提供 IPv6 網路服務設備支援狀況、時程及相關規劃為何？(複選)								
(一). 骨幹所用路由設備之 IPv6 支援能力為何?	100%	100%	100%	100%	100%	100%	100%	
提供 IPv6 的時程及相關規劃?								
已提供	✓	✓	✓	✓	✓	✓		**6**
2019 年（108 年）							✓	**1**
2020 年（109 年）								**0**
2020 年（109 年）之後								**0**
若無計畫導入，請說明原因								**0**
(二). 各項服務(請填寫貴公司有提供的服務項目)								
光纖(FTTx)上網								
1. 服務所用網路設備之 IPv6 支援能力為何？	<100 %	×	<100 %	×	<100 %	<100%	×	
2. 服務是否使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶?								
否			✓		✓	✓		**3**
是，若回答是，此服務一個 Public IP 給客戶的比例								
3.提供 IPv6 服務的時程?								
已提供，請填寫此服務的 IPv6 帳號數/用戶數	✓		✓					**2**
2019 年（108 年）提供								**0**
2020 年（109 年）提供						✓		**1**
2020 年（109 年）之後提供								**0**
請說明目前進行的階段								
規劃中，預計西元_____年完成						✓		

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
測試中，預計西元_____年完成								
若無計畫導入，請說明原因					✓			**1**
Co-location /IDC 服務								
1. 服務所用網路設備之 IPv6 支援能力為何？	100%	×	100%	×	100%	100%	×	
2. 提供 IPv6 服務的時程?								
已提供，請填寫此服務的 IPv6 帳號數/用戶數	✓		✓		✓	✓		**4**
2019 年（108 年）提供								**0**
2020 年（109 年）提供								**0**
2020 年（109 年）之後提供								**0**
請說明目前進行的階段								
規劃中，預計西元_____年完成								
測試中，預計西元_____年完成								
若無計畫導入，請說明原因								**0**
雲端(Cloud)服務								
1. 服務所用網路設備之 IPv6 支援能力為何？	<100%	×	×	×	100%	×	×	
2. 提供 IPv6 服務的時程?								
已提供，請填寫此服務的 IPv6 帳號數/用戶數	✓							**1**
2019 年（108 年）提供								**0**
2020 年（109 年）提供					✓			**1**
2020 年（109 年）之後提供								**0**
請說明目前進行的階段								
規劃中，預計西元_____年完成					✓			**1**
測試中，預計西元_____年完成								
若無計畫導入，請說明原因								**0**

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
PWLAN 無線上網								
1. 服務所用網路設備之 IPv6 支援能力為何？	<100%	×	×	×	<100%	×	×	
2. 服務是否使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶?								
否								**0**
是，若回答是，此服務一個 Public IP 給客戶的比例	✓				✓			**2**
3.提供 IPv6 服務的時程?								
已提供，請填寫此服務的 IPv6 帳號數/用戶數	✓							**1**
2019 年（108 年）提供								**0**
2020 年（109 年）提供								**0**
2020 年（109 年）之後提供								**0**
請說明目前進行的階段								
規劃中，預計西元_____年完成								
測試中，預計西元_____年完成								
若無計畫導入，請說明原因					✓			**1**
4G 行動上網								
1. 服務所用網路設備之 IPv6 支援能力為何？	100%	100%	×	100%	×	100%	100%	
2. 服務是否使用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶?								
否								**0**
是，若回答是，此服務一個 Public IP 給客戶的比例	✓	✓		✓		✓	✓	**5**
3.提供 IPv6 服務的時程?								

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
已提供，請填寫此服務的 IPv6 帳號數/用戶數	✓	✓		✓		✓		**4**
2019 年（108 年）提供							✓	**1**
2020 年（109 年）提供								**0**
2020 年（109 年）之後提供								**0**
請說明目前進行的階段								
規劃中，預計西元_____年完成							✓	
測試中，預計西元_____年完成								
若無計畫導入，請說明原因								**0**

根據上表 IASP 業者問卷回覆，下圖針對業者所經營的不同業務，依業者現有之 IPv6 位址使用情境統計目前業者對各項服務是否已經提供 IPv6 連網服務佔比。

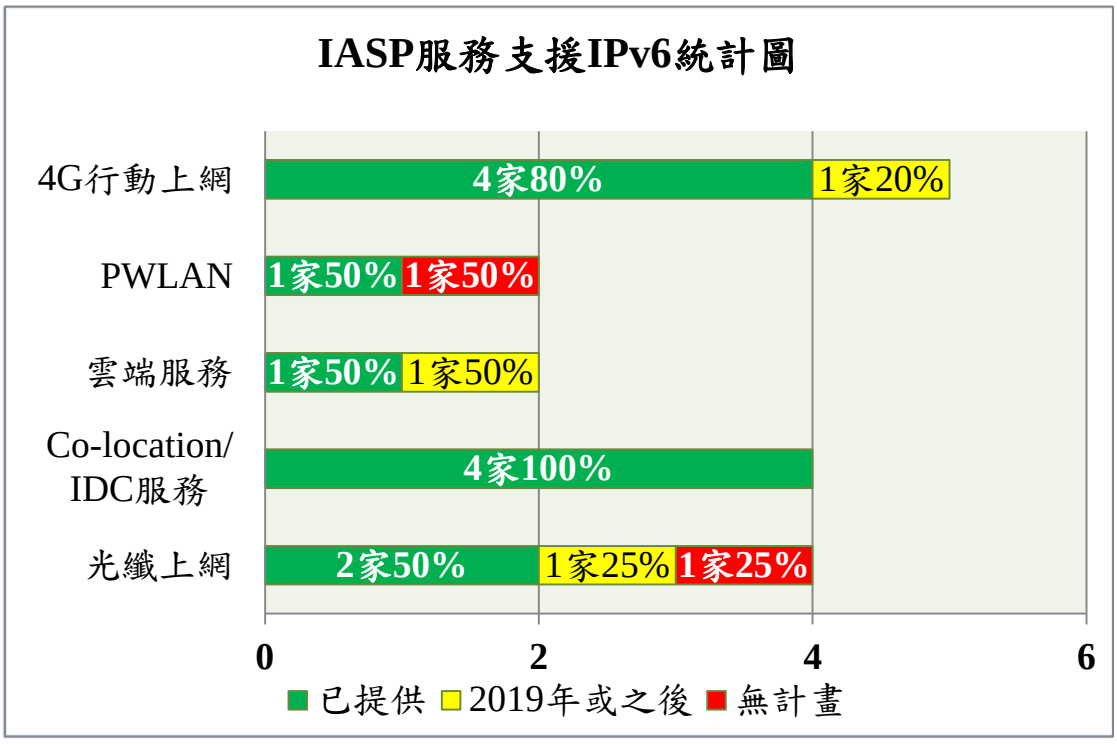

圖 33、IASP 業者各項服務支援 IPv6 佔比統計圖

從去年(108 年)中華電信行動網路和固網支援 IPv6 網路服務後，遠傳電信及台灣大哥大也陸續於去年(108 年)開啟支援 IPv6 網路服務，今年(108 年)亞太電信也加入支援 IPv6 網路服務，由年初以來使用率持續穩定成長，11 月初已經成長到約 45%，行動電信業者的支援對提高國內 IPv6 網路使用比例有相當重要的貢獻，下圖為 4 家行動電信業者 IPv6 連網比例圖[25]：

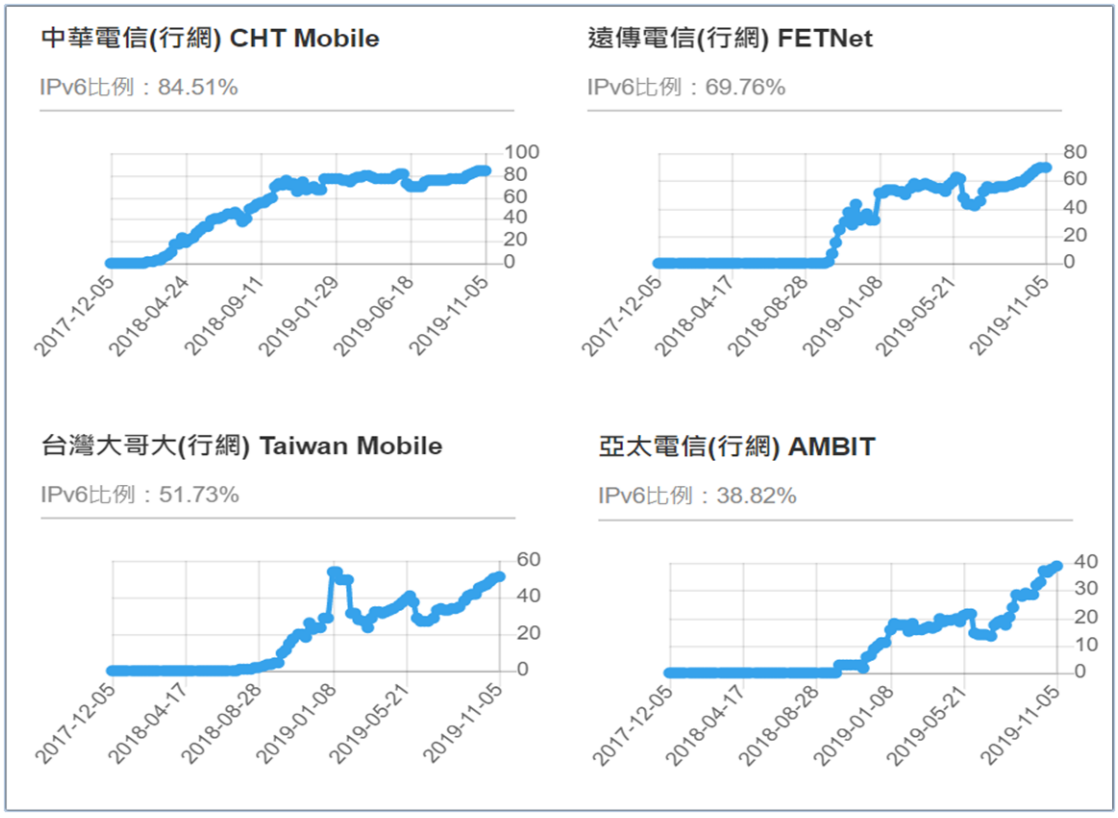

圖 34、IASP 業者行動電信業務使用者 IPv6 連網比例

但在固網的部分，目前除中華電信使用比例約 24%，相較年初約有 5%的成長，台灣固網、新世紀資通及亞太電信以企業客戶為主的網路服務進展較少。下圖為 4 家固網業者 IPv6 連網比例圖[25]：

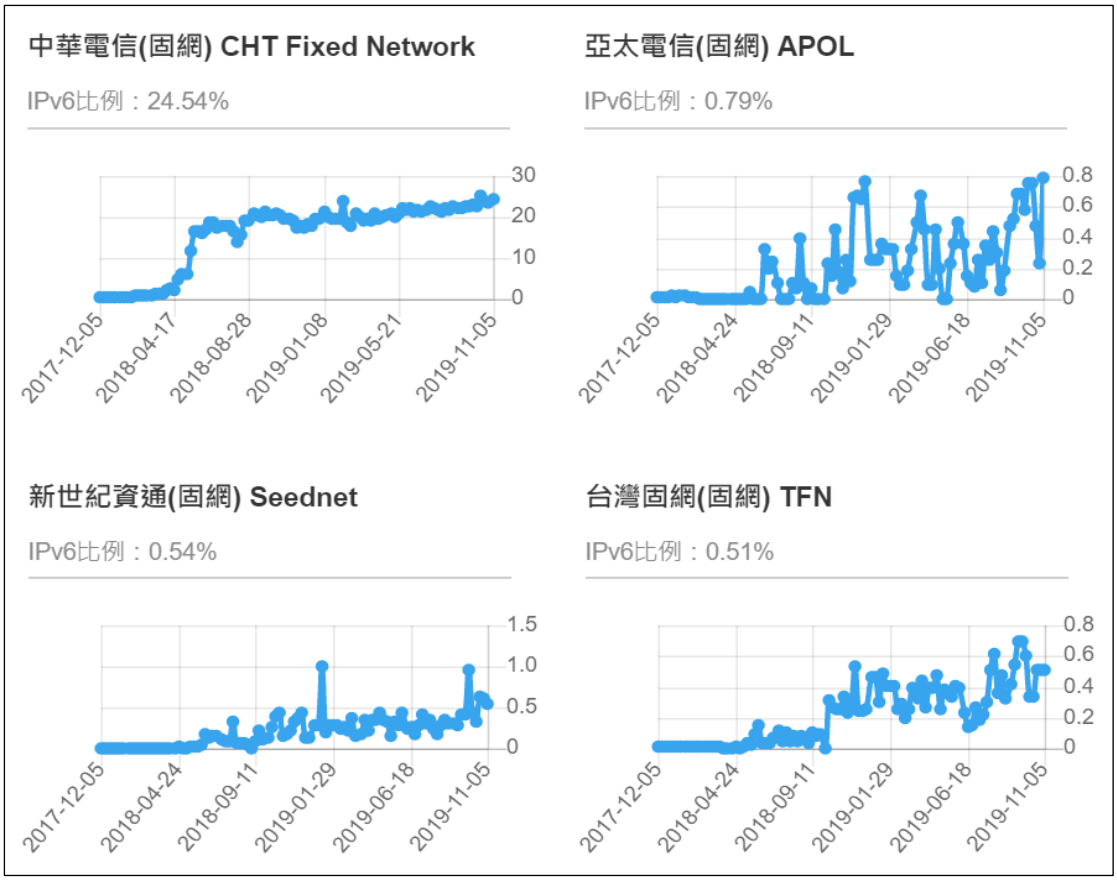

圖 35、IASP 業者固網業務使用者 IPv6 連網比例

(六) 貴公司提供 IPv6 服務時，預計增加支出主要用在哪些項目？

下表根據行動網路及固網共 7 家 IASP 業者，對於有關支援 IPv6 預計增加支出項目回覆統計表，依照 IASP 業者回覆來看，最多的預算支出為用在〝更新相關軟體〞，其次為〝更新硬體設備〞，此 2 個項目為支援 IPv6 需要支出預算最多的部分，第 3 為〝人員訓練〞。但若計算該項目的平均權重計算，排名第一為〝更新硬體設備〞，其次為〝更新相關軟體〞，第 3 名為〝IPv6 連線費用〞，排名順序略有不同。下圖根據業者的問卷回覆，列出有關支援 IPv6 預計增加支出項目的統計圖。

表 33、IASP 業者問卷統計支援 IPv6 預計增加支出項目

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
貴公司提供 IPv6 服務時，預計增加支出主要用在哪些項目(複選，請於括號內以 1, 2, 3,...標示出該項目所需經費之比重排名，其中 1 最高，2 次高，以此類推)？								
更新硬體設備	1	1	1	1	1	2		**6**
更新相關軟體系統(例如 DNS/Radius/DHCP/Web/E-mail 等)	2	2	2	2	2	1	1	**7**
人員教育訓練	3	3	3	3		3		**5**
IPv6 連線費用		4	4					**2**
其他，請說明_____								**0**

註：1, 2, 3,...標示出該項目所需經費之比重排名，其中 1 最高。排名 1 換算成權重（weight）指數 5，排名 2 換算成權重指數 4，以此類推。下圖顯示〝w=x〞，代表該選項權重加總；〝a=x〞代表平均權重。

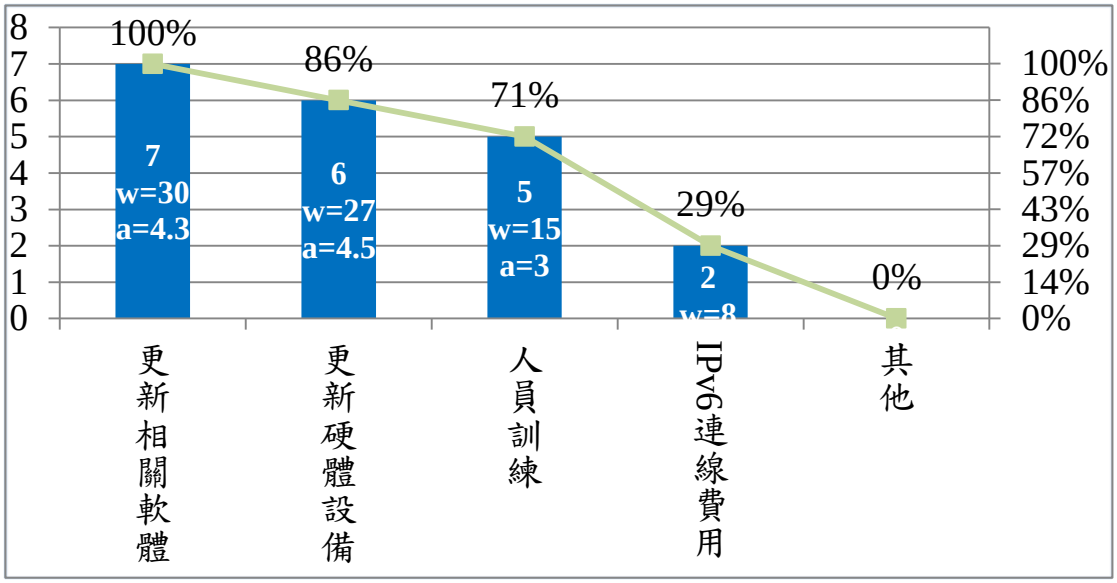

圖 36、IASP 業者問卷支援 IPv6 預計增加支出項目統計圖

(七) 貴公司在 IPv6 可能面臨的問題有哪些？

下表根據 IASP 業者，對於有關支援 IPv6 可能面臨的問題項目回覆統計表，依照 IASP 業者回覆來看，業者最常遇到的問題是〝人員 IPv6 技術能力與管理經驗不足〞的問題比例達 86%，其次是〝軟硬體支援度不足〞比例為 57%，另外〝廠商 IPv6 技術能力不足〞也會影響服務品質，另有部分業者反應〝IPv6 無法達成公司原有 IPv4 各服務的功能〞，對各業者服務造成的影響整理如下所述：

- 〝管理功能〞上，IPv6 位址資源配發管理問題和 IPv4 不同。（遠傳電信）
- 〝管理功能〞上，無法達成公司原有 IPv4 各服務的功能。（亞太電信）
- 〝安全功能〞上，需新購防火牆才能達到 IPv4 NAT 的阻擋外部主動連線功能。（台灣大哥大）
- 〝安全功能〞上，無法達成公司原有 IPv4 各服務的功能。（亞太電信）

各家電信業者因為新的服務上線，就技術的掌握度可能隱藏一些未知因素，因此業者除了負擔本身的技術設備的掌握度外，也會擔心外部使用其服務的設備等相關的問題。此外中華電信及新世紀資通，反映支援 IPv6〝投入成本高〞。中華電信及台灣之星在〝其他〞項目提列意見，詳細內容如下所述：

- IPv6 缺乏關鍵應用以及吸引用戶之誘因。（中華電信）
- 國際及國內互連之 ISP 部分業者無提供 IPv6 路由互連。（中華電信）
- 內容業者 IPv6 支援能力有待加強。（中華電信）
- 用戶端設備不支援 IPv6。（中華電信）

◆ 如未藉由新建或汰舊換新機會順勢將 IPv6 導入，將增加額外導入成本。(中華電信)

◆ 網際網路並未全面提供 IPv6 網路，甚至多數自治網路(AS)亦未全面 IPv6，使得提供用戶上網服務實際使用 IPv6 或是 IPv4 連線不易辨認。(台灣之星)

下圖根據 IASP 業者的問卷回覆，列出有關支援 IPv6 可能面臨的問題項目的統計圖。

表 34、IASP 業者問卷統計支援 IPv6 可能面臨的問題

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
貴公司在 IPv6 可能面臨的問題有哪些(複選)？								
投入成本高	✓		✓					2
軟硬體支援度不足	✓		✓	✓	✓			4
IPv6 無法達成公司原有 IPv4 各服務的功能(複選)		✓		✓		✓		3
管理功能，例如_		✓				✓		2
安全功能，例如_				✓		✓		2
效能，例如_								0
其他_								0
人員 IPv6 技術能力與管理經驗不足		✓	✓	✓	✓	✓	✓	6
廠商 IPv6 技術能力不足			✓		✓	✓		3
上游國際 ISP 無提供 IPv6 路由互連								0
客戶使用 IPv6 服務會產生體驗(QoE)不佳之問題								0
其他 _	✓						✓	2
本公司目前並無上述問題								0

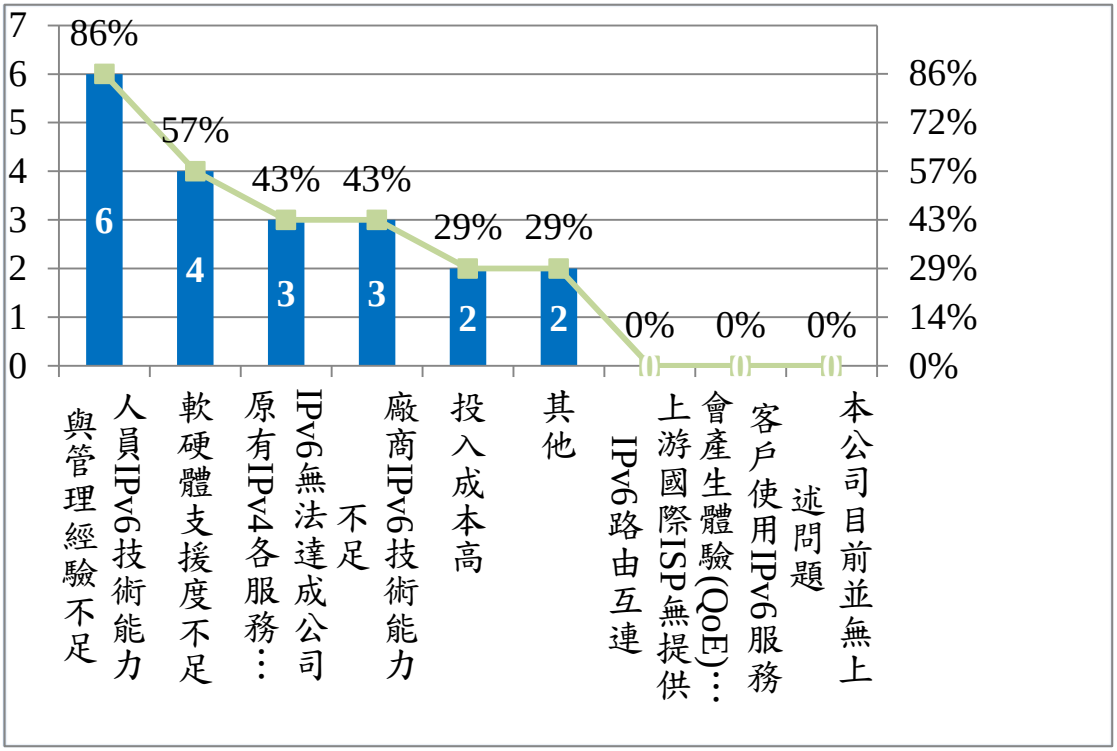

圖 37、IASP 業者問卷支援 IPv6 可能面臨的問題統計圖

(八) 貴公司是否認為在 IPv6 網路發展上有政府可以協助之項目？

下表根據 IASP 業者，對於有關支援 IPv6 網路發展上希望政府協助項目回覆統計表，依照 IASP 業者回覆來看，就政府可以協助之項目上，大多數業者都希望政府能夠〝提供獎勵補助措施〞或〝提供投資抵減優惠〞，以提高業者的投資意願，加速提高業者更新技術服務的腳步。業者所提建議如下：

- ◆ 提供獎勵補助措施，例如 IPv6 設備採購稅金減免(韓國或日本案例減免業者 3~5%可做為參考)、補助固網寬頻升級 IPv6 實施計畫、降低營所稅稅率鼓勵服務創新等獎勵補助措施。(中華電信)
- ◆ 提供獎勵補助措施，例如獎勵服務升級。(台灣之星)

◆ 提供投資抵減優惠，例如 IPv6 相關研究與發展計畫研發補助、設備加速折舊以及人才培訓等投資抵減項目。(中華電信)

◆ 提供投資抵減優惠，例如更新軟硬體投資可抵減稅賦或列為一定額度的獎勵投資等。(遠傳電信)

此外在問卷〝其他〞的選項中，業者提到多項意見，希望政府能提供協助項目，詳細如下所列：

◆ 協助本公司推動主要相關網通業者市售設備預設支援IPv6功能。(中華電信)

◆ 協助本公司推廣企業用戶、內容業者導入IPv6。(中華電信)

◆ 協助尋找IPv6創新應用服務發展商機，增加業者導入IPv6的動能，有助於帶動國內IPv6發展與普及。(中華電信)

◆ 協助產、官、學、研之資源整合，建立IPv6產業價值鏈，創造新客戶及新市場。(中華電信)

◆ 促進跨業合作，將有關物聯網產業之產品及技術加以整合至IPv6以創造更大的產業效益。(中華電信)

◆ 警政單位通信監察支援。(台灣大哥大及台灣固網)

表 35、IASP 業者問卷統計支援 IPv6 網路發展上希望政府協助項目

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	**總計**
貴公司是否認為在 IPv6 網路發展上有政府可以協助之項目(複選)？								
提供獎勵補助措施，例如_	✓		✓	✓	✓	✓	✓	**6**
提供投資抵減優惠，例如_	✓	✓	✓	✓	✓	✓		**6**
無需要政府協助								**0**
其他 _	✓			✓	✓			**3**

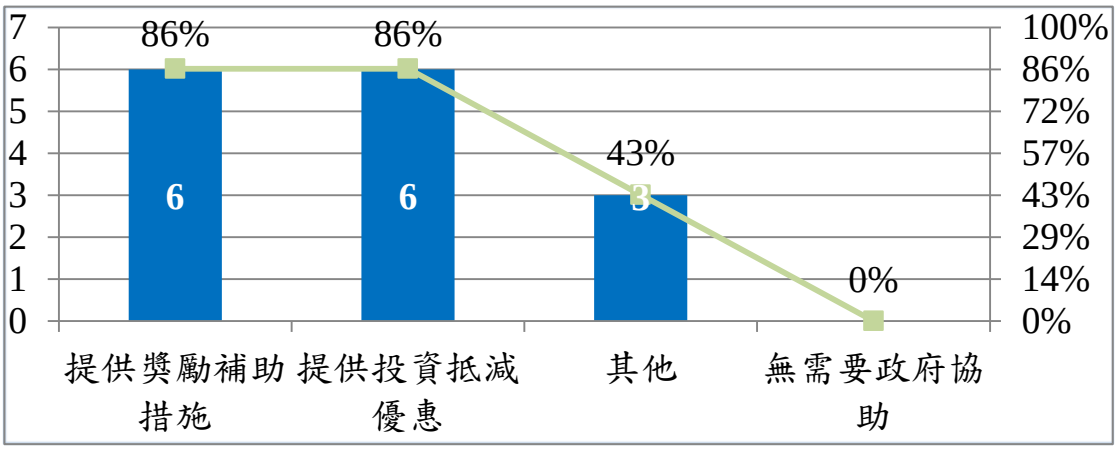

圖 38、IASP 業者問卷支援 IPv6 網路發展上希望政府協助項目

(九) 貴公司若提供用戶 IPv6 網路連線服務，將會如何提供配發用戶 IPv6 位址？

下表根據 IASP 業者，對於有關支援 IPv6 連線服務位址配發方式項目回覆統計表，依照業者回覆來看，7 家業者中，主要支援〝動態配發 IPv6 位址或網段(Prefix)〞，但中華電信及新世紀資通可根據客戶需求選擇〝固定配發 IPv6 位址或網段(Prefix)〞。

表 36、IASP 業者統計支援 IPv6 連線服務位址配發方式

IASP 問卷調查內容	中華電信	遠傳電信	新世紀資通	台灣大哥大	台灣固網	亞太電信	台灣之星	總計
貴公司若提供用戶 IPv6 網路連線服務，將會如何提供配發用戶 IPv6 位址？								
動態配發 IPv6 位址或網段(Prefix)	✓	✓	✓	✓	✓	✓	✓	**7**
固定配發 IPv6 位址或網段(Prefix)	✓		✓					**2**
其他 _								**0**

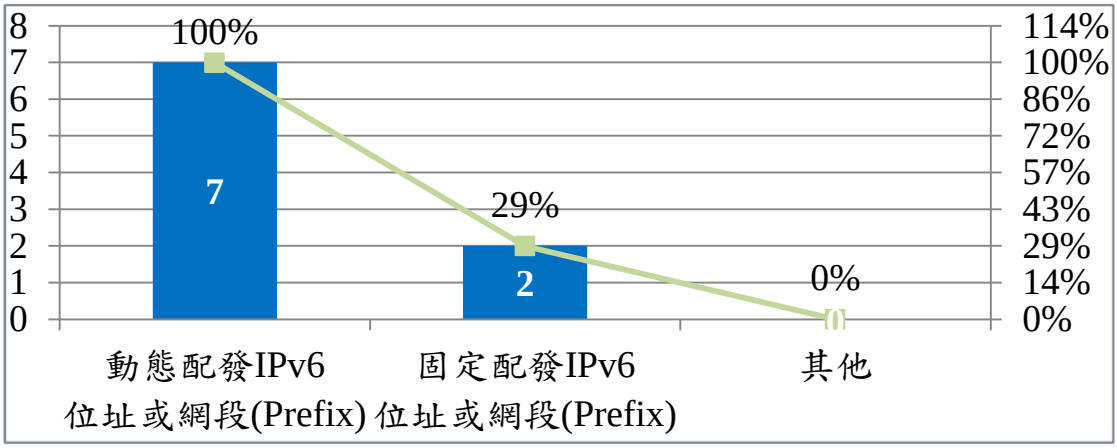

圖 39、IASP 業者支援 IPv6 連線服務位址配發方式統計圖

IASP 業者面訪紀錄表，詳細請參考附錄一；業者問卷調查表回覆內容，詳細請參考附錄二。

下圖為 11 月初台灣 IPv6 使用量測數據，IPv6 使用比例約 45%全球排名第 5 名。[26~27]

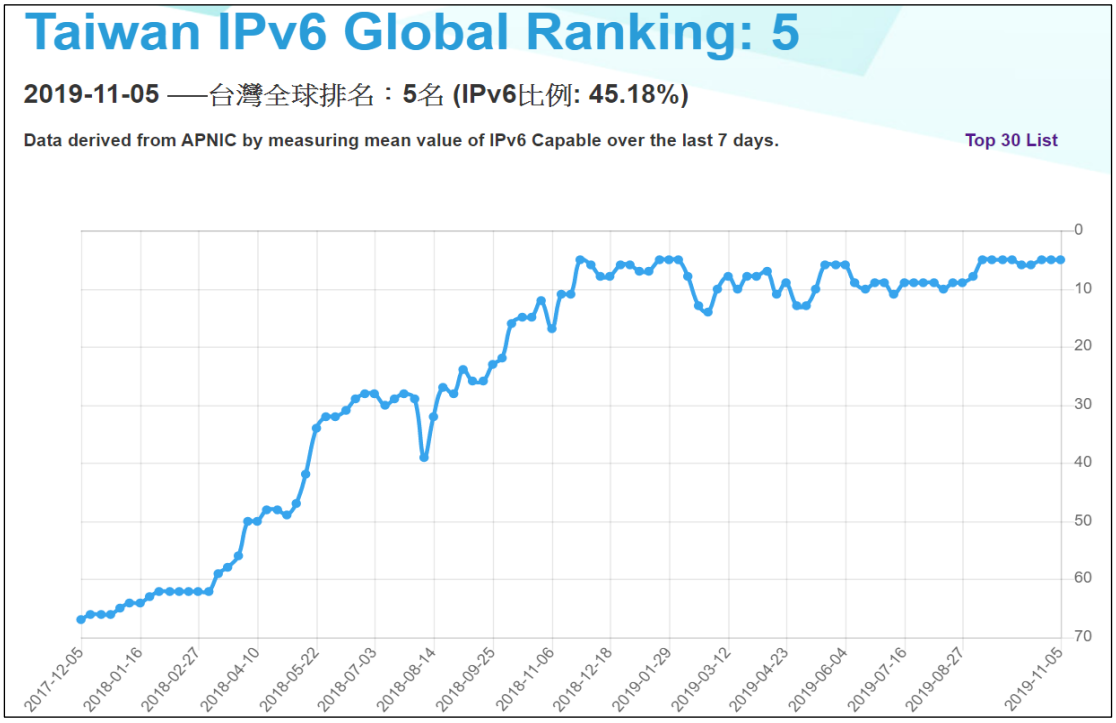

圖 40、台灣 IPv6 使用量測數據圖

表 37、全球 IPv6 使用率排名前 30 國家列表

Top 30 List

SN	CC	Display Name	IPv6 %
1	YT	Mayotte	68.93
2	IN	India	63.78
3	BE	Belgium	59.07
4	US	United States of America	54.32
5	TW	Taiwan	45.18
6	MY	Malaysia	44.55
7	GR	Greece	44.19
8	MF	Saint Martin	43.85
9	DE	Germany	41.11
10	FR	France	38.74
11	LU	Luxembourg	38.66
12	VN	Vietnam	37.66
13	GF	French Guiana	36.72
14	JP	Japan	35.79
15	CH	Switzerland	34.65
16	NO	Norway	34.26
17	PT	Portugal	32.65
18	UY	Uruguay	31.71
19	FI	Finland	31.32
20	MX	Mexico	31.31
21	GB	United Kingdom of Great Britain and Northern Ireland	31.02
22	BR	Brazil	30.67
23	TH	Thailand	28.02
24	EE	Estonia	25.89
25	LK	Sri Lanka	25.66
26	CA	Canada	25.31
27	HU	Hungary	24.99
28	AE	United Arab Emirates	24.34
29	NZ	New Zealand	23.42
30	TT	Trinidad and Tobago	22.99

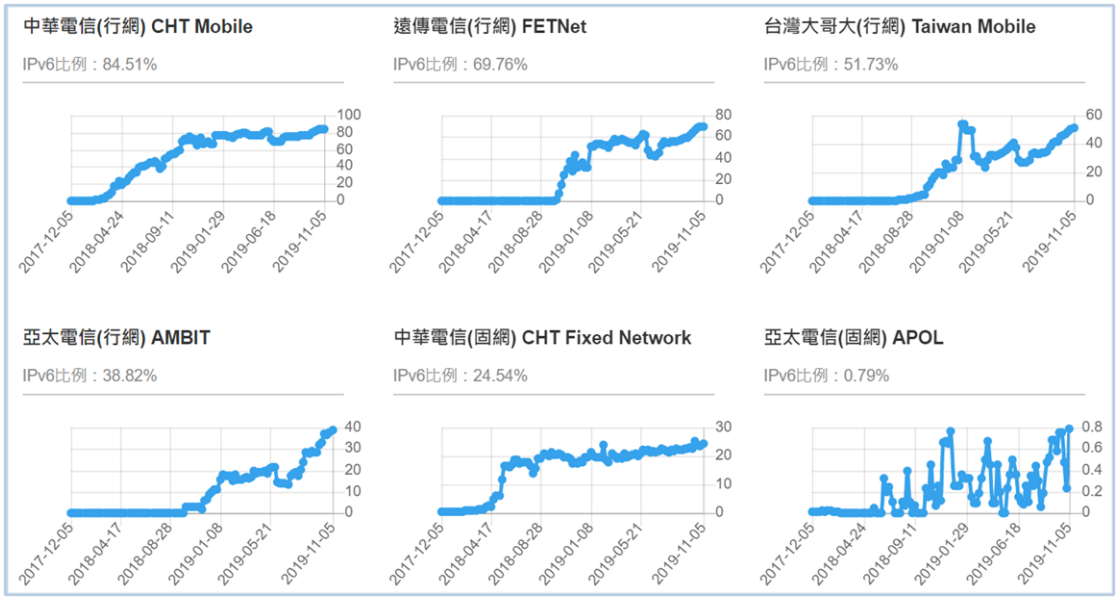

圖 41、台灣商用網路 IASP 業者 IPv6 連網比例

第二節 DNSSEC 調查及監測

針對業者 Cache DNS 是否支援 DNSSEC 調查工作項目，調查主要對象是以向 NCC 申報支援 Cache DNS 的對象為主，以下為業者回覆問卷統計表：

表 38、業者 Cache DNS DNSSEC 支援調查統計表

IASP 問卷調查內容	中華電信	新世紀資通	台灣固網	亞太電信	台灣之星	台灣碩網	凱擘寬頻	中嘉寬頻	中嘉和網	總計
貴公司是否有提供 Cache DNS 伺服器？										
否							✓	✓		2
是，若回答是，請接續回答以下問題：	✓	✓	✓	✓	✓	✓			✓	7
1.貴公司 Cache DNS 伺服器是否有支援 DNSSEC?										
否	✓	✓			✓	✓				4
是			✓	✓					✓	3
2.貴公司 Cache DNS 伺服器預計啟用 DNSSEC 驗證的時程？										
已提供			✓	✓					✓	3
2019 年（108 年）	✓									1
2020 年（109 年）										0
2020 年（109 年）之後		✓			✓	✓				3
3. 貴公司 Cache DNS 伺服器是否開放網外用戶使用？										
否		✓	✓	✓	✓	✓				5
是，若回答是，請提供 IP 資訊：	✓								✓	2

目前調查的 9 家中，凱擘寬頻及中嘉寬頻 2 家業者並未提供 Cache DNS 服務，其他 7 家有提供 Cache DNS 伺服器的業者中，只有中華

電信及中嘉和網有開放網外用戶使用，中華電信所使用的 IP 為 168.95.1.1 及 168.95.192.1，其預計於今年（108 年）啟用 DNSSEC 驗證；而中嘉和網所使用的 IP 為 203.133.1.1，目前已經啟用 DNSSEC 驗證；其他 5 家業者所提供 Cache DNS 伺服器並沒有對外開放，其中有 2 家業者（台灣固網及亞太電信）回覆已經啟用 DNSSEC 驗證；另外 3 家業者（新世紀資通、台灣之星及台灣碩網）回覆預計於西元 2020 後才有啟用 DNSSEC 驗證計畫。

下圖根據業者回覆狀況針對 Cache DNS 伺服器預計啟用 DNSSEC 驗證的時程統計圖，已經啟用有 3 家佔比為 43%，預計今年（108 年）啟用有 1 家佔比為 14%，另有 3 家預計要西元 2020 年（109 年）以後才會啟用佔比為 43%。

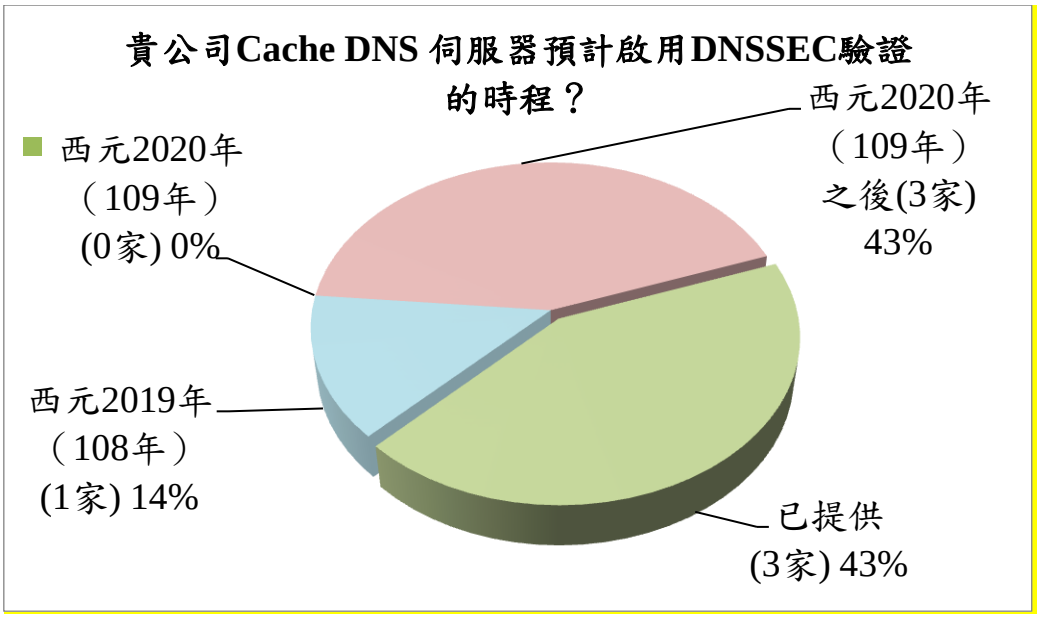

圖 42、Cache DNS 伺服器預計啟用 DNSSEC 驗證的時程統計圖

業者 Cache DNS DNSSEC 支援問卷調查，包含在 IASP 問卷調查內容中，詳細請參考附錄二。

第三節 Cable 業者合作推廣用戶試用 IPv6 連網服務

目前調查的 Cable 業者中，較積極於建置 IPv6 上網服務多屬於具規模的網路服務業者包括凱擘寬頻、台固媒體、台灣寬頻通訊及中嘉寬頻，4 家業者都有在進行實驗測試，凱擘寬頻及台固媒體在後端設備上其 DHCP server 尚未完全支援，因公司政策及投資預算等因素，其網路服務支援 IPv6 的計畫目前以實驗室小型測試階段，為先期設備及服務支援的前期作業準備，距離能提供使用者測試仍有一段距離；中嘉寬頻在後端準備狀況相當不錯，且因為商業考量與需求其骨幹網路已經支援 IPv6，但消費端的部分還未有明確的時程計畫；台灣寬頻通訊在後端設備上支援 IPv6 上網服務已經建置完成，因此在提供小規模的先期試用的可行性相對提高，但使用者端的 Cable Modem 在支援 IPv6 上只達到 50%，為業者要進行商用計畫上的一大挑戰；獨立系統業者以天外天數位有線電視在規劃上相對較為積極，其他獨立系統業者在此議題上的態度相對較保守，計畫時程相對較不明確。

各家業者大多還未完成支援 IPv6 的準備，目前 Cable 試用 IPv6 連網服務的推動，還處於相當前期階段。根據上半年調查結果以台灣寬頻通訊在今年（108 年）進行用戶試用 IPv6 網路服務的準備度及意願最高，在和業者的討論會議中也就技術、設備、客服、維護等多方面進行交流，此外也將中心所提供的各項資源如教育訓練課程等相關訊息，提供業者參考。中心於 5 月份和 APNIC 共同舉辦〝TWNIC - APNIC Joint Training – IPv6 Workshop〞為期 3 天的教育訓練課程，主要目的在幫助業者網路維運相關人員，了解 IPv4/IPv6 雙協定並行技術介紹，

並透過實作加強業者對雙協定運作的瞭解及掌握，此次課程有多家 Cable 業者參與其中，並就在 Cable 上支援 IPv6 的技術及實務和講師進行交流。

今年（108 年）Cable 業者合作推廣用戶試用 IPv6 連網服務，為國內 Cable 業者第一次進行 IPv6 連網服務試用，將以小型試用並結合使用者環境測試做為推動方向，合作對象為台灣寬頻通訊，計畫執行內容說明如下：

一. 測試 IPv6 連網環境

結合今年（108 年）計畫中的寬頻分享器支援 IPv6 之測試平台的建置及測試計畫，進行試用並測試台灣寬頻通訊的 IPv6 連網環境和市售寬頻分享器連網情況。台灣寬頻通訊其有線電視品牌經營區域包含桃園、新竹及苗栗等區域，計畫協調台灣寬頻通訊旗下的有線電視品牌南桃園有線電視，申請試用專線的形式提供 IPv6 連網測試環境，整合原先規劃 IPv6 寬頻分享器測試機種作為測試標的，並依照規劃的測試項目進行，測試項目主要以使用者行為設計，目的為了解業者在 IPv6 網路服務建置的整合情況，及掌握在使用端 IPv6 連網狀況。詳細的測試內容及結果請參閱下一節說明，或附錄六將有更完整說明。

二. 推廣寬頻分享器業者加入試用行列

關於測試 IPv6 連網環境，主要以模擬使用者連網情境進行，就技術面來看，實際連網傳輸的資料傳送情形，業者的測試會有更完整的判別能力，因此在進行今年（108 年）計畫中的寬頻分享器支援 IPv6 之測試平台的建置及測試計畫時，在計畫執行中曾拜訪華碩和友訊兩

家寬頻分享器製造商，除和業者共同討論設備測試規範需求之外，因華碩此類商品的研發辦公室位於竹北市，為台灣寬頻通訊所經營有線電視品牌所涵蓋區域，訪談過程也將相關訊息傳達給業者，希望透過不同面向的測試，讓網路服務商和設備商的服務能有更好的整合。

三. 發文推廣用戶申請試用 IPv4/IPv6 雙協定服務

今年（108 年）TWNIC 在台網中心電子報分別在 8 月時以〝台灣寬頻 TBC 全國第一家 MSO 通訊協定採用 IPv6〞為題，及 10 月時以〝TBC 台灣寬頻開放用戶申請 IPv4/IPv6 雙協定服務〞，透過電子報宣傳台灣寬頻 IPv4/IPv6 雙協定服務，以期能吸引更多使用者加入試用行列。根據 TBC 台灣寬頻內部統計到 11 月底經過約有 700 個使用者申請 IPv6 網路服務。

四. 推廣 Cable 業者加入支援 IPv6 網路服務

今年（108 年）計畫中針對 20 家 Cable 業者進行訪談過程中，推廣台灣寬頻通訊支援 IPv6 網路服務訊息給業者知悉，透過業者彼此競爭及仿效的動能，增加業者支援 IPv6 網路服務的意願。

五. 討論未來合作推動 IPv6 網路服務計畫

在計畫執行初期於 3 月 4 日和台灣寬頻進行第一次訪談，推動業者啟用支援 IPv6 網路服務試用的決定，業者於 6 月 1 日正式推出讓用戶可透過主動申請試用方式，取得 IPv6 網路服務，經過一個季度於 9 月 18 日再次和業者訪談，以了解目前用戶申請試用狀況及業者未來推動計畫，並討論未來相互合作進行推廣活動的可行性。

第四節 開發手機設定 IPv6 之 APP

目前智慧型手機作業系統分為兩大主流，分別為iPhone所採用的作業系統iOS及Android手機作業系統，iPhone並未開放任何設定給使用者控制開啟或關閉IPv6網路連線設定，而是由行動電信業者和APPLE做測試程序後，由APPLE出貨給行動電信業者時即已經設定完成；但Android手機作業系統版本眾多且生產業者眾多，目前國內5家行動電信業者，並非所有業者都已經支援IPv6連網服務，因此部分手機業者作業系統預設不開啟IPv6，造成IPv6在Android手機上推廣的障礙。不同業者生產的Android手機設定IPv6的方式雖大同小異，但卻沒有一致的標準步驟及畫面，對使用者仍造成一定的阻礙。

此項工作目的為開發一個Android手機專用控制IPv6設定之APP，功能須符合以下需求：

一. 可供Android手機使用者快速切換IPv6的功能

二. 支援Android5.x, 6.x, 7.x, 8.x, 9.x手機作業系統

三. 支援直式跟橫式操作

四. APP上架到Google Play供使用者下載

五. APP Icon設計

六. Google Play的APP宣傳圖設計

使用者到Google Play下載並安裝此APP後，執行程式將出現如下圖手機設定IPv4/IPv6之APP執行畫面。啟動畫面有兩個功能按鈕，分別為：

◆ 關於：〝關於〞按鍵會出現一個簡單介紹此APP功能的畫面。

◆ 繼續：〝繼續〞按鍵會出現下圖說明畫面，列出步驟引導使用者完成啟動IPv4/IPv6通訊協定啟用設定。設定步驟為：

- ■ 步驟一：點選「存取點名稱(APN)
- ■ 步驟二：點選目前正在使用的電信業者項目
- ■ 步驟三：點選「APN協定」或「APN通訊協定」
- ■ 步驟四：點選「IPv4/IPv6」

圖 43、手機設定 IPv4/IPv6 之 APP 執行畫面

下圖為手機設定 IPv4/IPv6 之 APP 在 Google Play 上架畫面：

圖 44、手機設定 IPv4/IPv6 之 APP 上架 Google Play 畫面

今年度（108年）本計畫並將在中心網站設立〝IPv6推廣專區〞，因此在IPv6推廣專區的網頁上也將放置手機設定IPv4/IPv6之APP的QR Code及下載連結，方便使用者更容易找到此APP在Google Play上的下載區，下圖為手機設定IPv4/IPv6之APP在推廣專區的截圖：

圖 45、手機設定 IPv4/IPv6 之 APP 的 QR Code 畫面

第五節　設置 IPv6 推廣專區

為持續推廣 IPv6 普及並提高 IPv6 使用率，本工作項目將透過收集和終端用戶相關資訊，於 TWNIC 網站增設 IPv6 推廣專區網頁，網頁主畫面如下圖所示。IPv6 推廣專區網頁內容主要分為三大主題，分別為：

- ◆ 關於 IPv6：包含網通商品、IDC 支援 IPv6 調查報告及各國 IPv6 普及度等資訊。
- ◆ 民眾升級 IPv6：包含終端設備寬頻分享器、手機設定 IPv6 及 IASP 支援 IPv6 等資訊。
- ◆ 企業升級 IPv6：包含網站及企業內部升級、IPv6 資訊安全及技術手冊下載等資訊。

圖 46、IPv6 推廣專區-首頁

以下就 IPv6 推廣專區的網頁內容，將就各分項所包含項目提列並做簡要介紹：

一. 關於 IPv6

關於 IPv6 的內容共分為 4 個項目，各項目內容介紹如下所述：

(一) IPv6 基本介紹：以簡要方式介紹 IPv6 基本概念

(二) 網通商品支援 IPv6 調查報告：本項目將包含 107 年「我國 IPv4/v6 雙軌普行關鍵問題調查與可行解決研究」計畫報告內容中，關於網通商品支援 IPv6 調查報告資訊。

(三) IDC 支援 IPv6 調查報告：本項目將包含 107 年「我國 IPv4/IPv6 雙軌普行關鍵問題調查與可行解決方案研究」計畫報告內容中，關於 6 家 IDC 支援 IPv6 調查報告資訊。

(四) 世界各國 IPv6 普及度：本項目將連結到 APNIC 的世界各國 IPv6 普及度調查頁面。

圖 47、IPv6 推廣專區首頁-關於 IPv6

二. 民眾升級 IPv6

民眾 IPv6 升級的內容共分為 6 個項目，各項目內容介紹如下所述：

(一) 終端設備支援 IPv6 資訊：

一般使用者較常接觸的終端設備分家用及行動用，家用設備除固網業者配置的連線設備，使用者主機也可透過購置寬頻分享器以無線網路連結上網，寬頻分享器支援 IPv6 資訊將結合寬頻分享器支援 IPv6 之測試平台工作項目所測試品牌及商品，提供使用者參考，以鼓勵消費者購進支援 IPv6 網路通訊產品。行動設備以手機及平板為主，手機及平板主要以 iOS 及 Android 區分，本項內容將包含手機作業系統資源 IPv6 相關訊息及主要品牌手機及平板支援 IPv6 資訊。

(二) 寬頻分享器啟用 IPv6：

依據去年（107 年）市場調查結果，家用設備終端和連網 IP 相關產品以市售寬頻分享器為大宗，主要品牌包含 D-Link（友訊）、ASUS（華碩）、TP-Link 及 TOTOLINK，雖然各家所生產的商品型號眾多，但目前每家業者朝向以相同設計及流程提供同類型商品共同使用，因此市售寬頻分享 IPv6 之設定方法，將依主要品牌介紹各家業者目前主要採用的版本做介紹以利使用者獲得相關資訊。

除此之外並提供 108 年計畫執行成果，關於寬頻分享器支援 IPv6 測試報告內容，提供消費者參考。

(三) 手機啟動 IPv4/IPv6 設定 APP：

推廣頁面將提供包含上個工作項目所開發手機設定IPv6之APP連結，供 Android 手機使用者下載使用。除下載連結外，並介紹手機設定 IPv4/IPv6 流程資訊，方便使用者操作。

(四) Cable 之 IPv6 申請及設定方法：

此部分將介紹國內第一家提供 IPv6 網路服務的 MSO 業者台灣寬頻通訊(TBC)的簡介；及台灣寬頻通訊用戶之 IPv6 申請及設定方法，主要內容將參考台灣寬頻通訊所提供相關訊息，做重點介紹及提供連結，讓用戶容易取得相關訊息，以利推廣更多用戶加入試用行列。

(五) 國內 IASP 支援 IPv6 調查：

本項目將提供已支援 IPv6 網路服務的行動電信業者及固網業者相關訊息，及各家 IASP IPv6 連網使用比例連結等資訊。

(六) 一般民眾升級 IPv6 資訊：

包含 IPv6 連線檢測、IPv6 支援手機型號及設定說明及手機啟動 IPv4/IPv6 設定 APP 的連結。

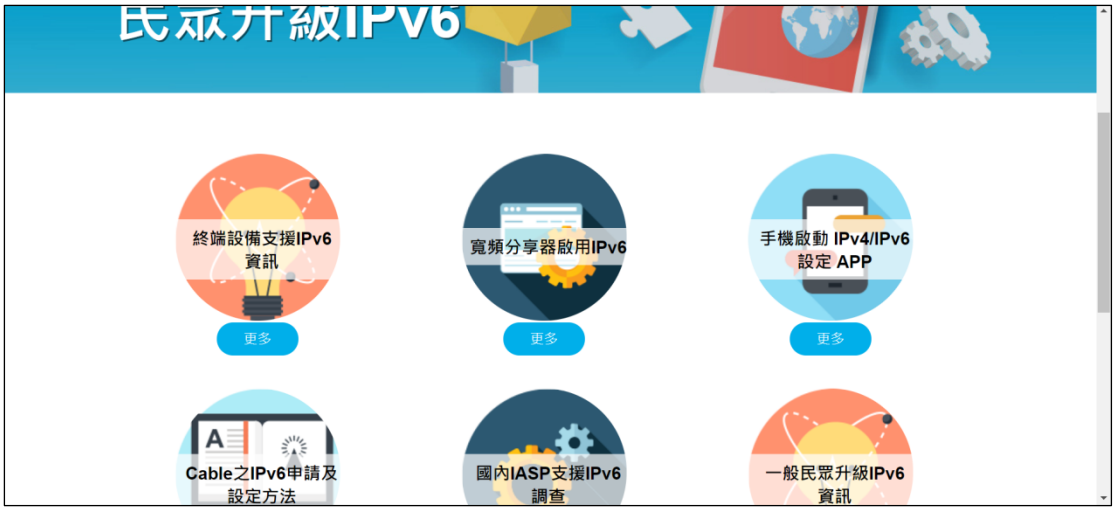

圖 48、IPv6 推廣專區首頁-民眾升級 IPv6

三. 企業升級 IPv6

企業 IPv6 升級的內容共分為 5 個項目，各項目內容介紹如下所述：

(一) ICP IPv4/IPv6 網路安全防護

本項目包含計畫報告內容中，關於 ICP IPv4/IPv6 網路安全防護架構技術手冊報告資訊，並提供手冊下載連結。及關於 ICP IPv4/IPv6 升級平台架構商協定網路安全防護檢查項目清單報告資訊，並提供手冊下載連結。

(二) ICP IPv4/IPv6 平台架構雙協定升級

本項目包含計畫報告內容中，關於 ICP IPv4/IPv6 平台架構雙協定升級內容，及 ICP 升級支援 IPv4/IPv6 雙協定輔導手冊，並提供手冊下載連結。

(三) 企業內部 IPv6 升級資訊

提供企業升級 IPv6 指南，及歷年來 TWNIC 所整理撰寫 IPv6 升級技術手冊下載連結。

(四) IPv6 資訊安全防護

收集歷年來討論和 IPv6 資訊安全防護相關議題的參考資料。

(五) 技術手冊資料下載

包含歷年來 TWNIC 所撰寫出版及整理 IPv6 升級技術手冊下載連結。

圖 49、IPv6 推廣專區首頁-企業升級 IPv6

IPv6 推廣網站網址為 https://ipv6.twnic.tw/

第三章 寬頻分享器和 IASP 實際測試平台建置及研擬寬頻分享器支援 IPv6 之共同供應契約

第一節 研擬寬頻分享器符合支援 IPv6 規範及標準測試項目

一. 寬頻分享器製造商開發規範

IPv4/IPv6 固網寬頻通訊架構及相關 RFC 關係，如下圖所示：

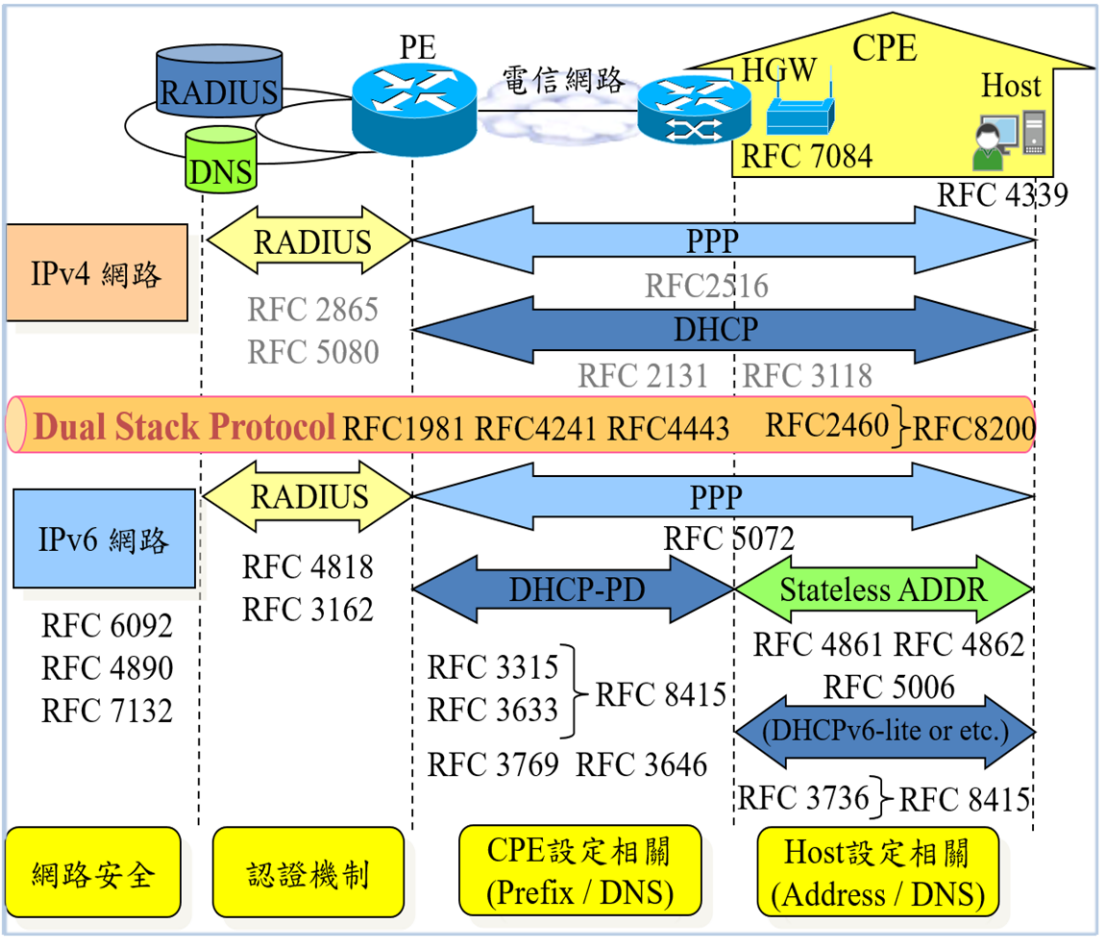

圖 50、IPv4/IPv6 固網寬頻相關 RFC 參考標準

針對 IPv6 寬頻分享器製造商開發規範部分，主要參考下圖之 RFC 相關標準：

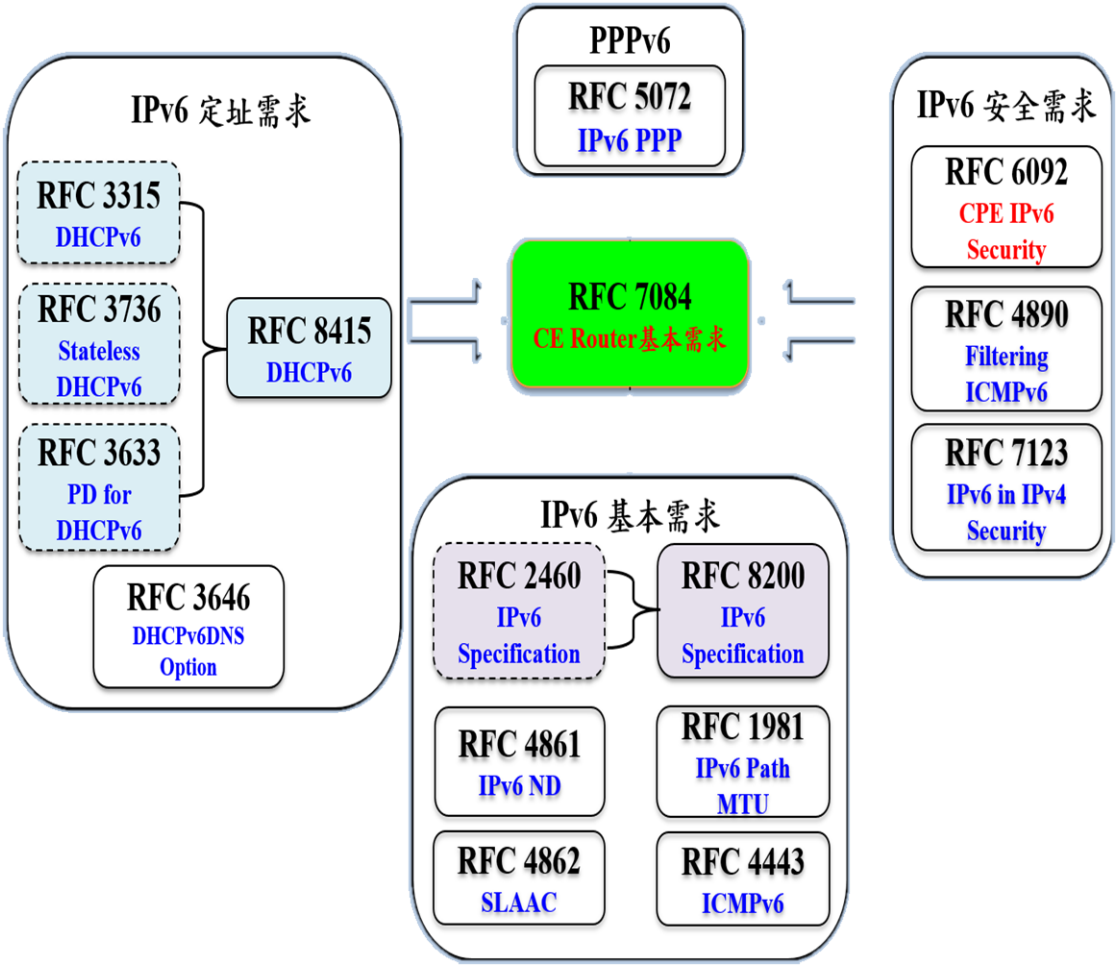

圖 51、寬頻分享開發規範 IPv6 RFC 關連圖

整理適合台灣上網環境連線中華電信 IPv6 PPPoE 及有線電視 Cable 業者之 IPv6 連線功能項目，主要 RFC 分為核心通訊功能的基本需求、位址配置的定址需求、PPP 通訊協定需求、及防護功能的安全需求 4 方面，如下表所示：

表 39、適合國內固網及 Cable 環境連線支援 IPv6 的 RFC 列表

類別	RFC No.	功能
核心通訊功能的基本需求 核心通訊功能的基本需求	RFC 7084	Basic Requirements for IPv6 Customer Edge Routers
	RFC 2460	Internet Protocol, Version 6 (IPv6) Specification
	RFC 8200	Internet Protocol, Version 6 (IPv6) Specification
	RFC 4861	Neighbor Discovery for IP version 6 (IPv6)
	RFC 4862	IPv6 Stateless Address Autoconfiguration
	RFC 1981	Path MTU Discovery for IP version 6
	RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
位址配置的定址需求	RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
	RFC 3736	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
	RFC 3646	DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
	RFC 8415	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
	RFC 3633	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
PPP 通訊協定需求	RFC 5072	IP Version 6 over PPP
防護功能的安全需求	RFC 6092	Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service
	RFC 4890	Recommendations for Filtering ICMPv6 Messages in Firewalls
	RFC 7123	Security Implications of IPv6 on IPv4 Networks

關於 IPv6 寬頻分享器的基本需求，針對核心通訊功能部份，以 RFC 7084 為主又分為 WAN 端及 LAN 端需求，另外 RFC 8200 為 IPv6 基本規範，RFC 4861 為 ND 相關規範，RFC 1981 為 MTU 相關規範，RFC 4862 為 SLAAC 相關規範，RFC 4443 為 ICMPv6 相關規範，這些都屬於基本需求，其中規範重點如下表所示：

表 40、IPv6 寬頻分享器基本需求必須規範建議

寬頻分享器之 IPv6 基本需求必須規範建議	
RFC 7084 WAN 介面	1. IPv6 CE router 必須實作 ICMPv6。 2. IPv6 CE router 必須實作 stateless 或 stateful 位址分配機制。 3. IPv6 CE router 必須產生 link-local 位址，並於其網路介面完成 DAD 以及發送 RS。 4. IPv6 CE Router 必須支援 DHCPv6 prefix delegation。 5. IPv6 CE Router 必須支援 DHCPv6 規範之客戶端行為。 6. IPv6 CE Router 必須支援 Ethernet 以及 PPP encapsulation。 7. CE Router 必須支援 SOL_MAX_RT Option。 8. IPv6 CE Router 必須支援 DHCPv6 options： ➢ Identity Association for Non-temporary Address (IA_NA)。 ➢ Reconfigure Accept。 ➢ DNS_SERVERS。 9. 如 WAN 端連線中斷，必須透過 RA 機制通告 LAN 端用戶。 10. 如收到的 RA 訊息中的 M or O flags 設置為 1 時，IPv6 CE Router 必須啟動 DHCPv6 prefix delegation。 11. 如 IPv6 CE Router 沒有從 SLAAC 或 DHCPv6 獲取 Global IPv6 位址，則必須從其 delegated prefix 創建一個 Global IPv6 位址。 12. IPv6 CE Router DHCPv6 同時請求 IA_NA 和 IA_PD 選項，其必須接受 DHCPv6 Advertise/Reply 訊息中的 IA_PD 選項，即使該訊息不包含任何位址。
RFC	1. IPv6 CE Router 必須作為 site border router ，並可依 IPv6

寬頻分享器之 IPv6 基本需求必須規範建議	
7084 LAN 介面 RFC 7084 LAN 介面	來源或目的位址過濾 IPv6 封包。 2. IPv6 CE Router 必須支援 Neighbor Discovery for IPv6。 3. IPv6 CE Router 必須為其每個 LAN Interface 分配一個單獨的/ 64 (由其被委託的 delegated prefix(es)) 。 4. IPv6 CE Router 必須透過 Route Information Option 通告其為 delegated prefix 配置的 Router。 5. IPv6 CE Router 的每個 LAN Interface 都必須發送 RA。 6. IPv6 CE Router 必須支援 IPv6 位址分配的 DHCPv6 server 或 stateless DHCPv6 server 功能。 7. IPv6 CE Router 必須支援在 DHCPv6 DNS_SERVERS 以及和 DOMAIN_LIST options 中提供 DNS 資訊。 8. IPv6 CE Router 必須支援可在 RA 中提供 DNS 資訊（Recursive DNS Server RDNSS 和 DNS Search List options）。 9. 如 delegated prefix 發生變化，則 IPv6 CE Router 必須立即通告舊的 prefix 其 Preferred Lifetime 為零。
RFC 8200 (取代 RFC 2460)	1. Extension 標頭必須依序處理。 2. 所有 node 必須檢驗和處理 Hop-by-Hop Options header。 3. 如果 Segments Left 為零，則節點必須忽略 Routing 標頭並繼續處理封包中的下一個標頭，其類型由 Routing 標頭中的 Next Header 欄位標識。 4. 如果 Segments Left 不為零，則節點必須丟棄該封包並向封包的來源地址發送 ICMP Parameter Problem, Code 0 訊息。 5. 如在接收到封包的第一個到達分段的 60 秒內收到不足的分段，則必須放棄該封包的重組，並且必須丟棄已經為該封包接收的所有分段。 6. 必須適當選擇分段的長度，使得分段封包適合到達封包目的地的路徑上的 MTU。 7. 在任何無法傳輸 1280 字節封包的鏈路上，必須在低於 IPv6 網路層提供特定於鏈路的分段和重組。 8. 具有可配置 MTU 的鏈路（例如，PPP 鏈路[RFC-1661]）必須配置為具有至少 1280 個八位字節的 MTU。 9. 節點必須能夠接受分段的封包，在重組後，該封包的大小為 1500 個八位字節。
RFC	1. 當節點收到 Packet Too Big 消息時，它必須根據消息中

寬頻分享器之 IPv6 基本需求必須規範建議	
1981	MTU 欄位的值減少其對相關路徑的 PMTU 的估計。 2. 節點不能將路徑 MTU 的估計值降低到 IPv6 最小鏈結 MTU 以下。
RFC 4443	1. IPv6 網路節點必須支援 ICMPv6。 2. 如收到未知類型的 ICMPv6 訊息，則必須以靜默方式丟棄。
RFC 4861 RFC 4861	1. RA/NA 來源 address 必須是傳送該訊息 interface 上的 link-local address。 2. MTU option 用於 RA，且其他 ND 訊息必須將其忽略。 3. Host 必須丟棄任何收到的 RS 訊息，且任何時候都不能傳送 RA。 4. Router 必須丟棄任何不完全符合以下檢驗的的 RS 訊息: ➢ IP Hop Limit 欄位為 255，意即封包沒辦法讓 router 傳送。 ➢ ICMP Checksum 是合法的。 ➢ ICMP Code 是 0。 ➢ ICMP length 是 8，或更多 octet。 ➢ 所有 option 都有大於 0 的 length。 ➢ 若來源 IP 位址為 unspecified address，則訊息中沒有 source link-layer option。 5. RS/RA/NS/NA Reserved 欄位和任何無法辨認的 option，都必須被忽略。 6. Router 必須丟棄任何沒有滿足以下所有檢驗的 RA 訊息: ➢ 來源 IP address 是 link-local address。 ➢ IP Hop Limit 欄位為 255，意即封包沒辦法讓 router 傳送。 ➢ ICMP Checksum 是合法的。 ➢ ICMP Code 是 0。 ➢ ICMP length 是 16，或更多 octet。 ➢ 所有 option 都有大於 0 的 length。 7. 一個 node 必須丟棄任何沒有滿足以下全部正當性檢查的 NS： ➢ Hop Limit 欄位的值為 255，也就是說該封包沒辦法透過 router forward。 ➢ ICMP Checksum 是合法的。

寬頻分享器之 IPv6 基本需求必須規範建議	
RFC 4861	➢ICMP Code 是 0。 ➢ICMP 長度大於 24 個 octets。 ➢目標 Address 不是 multicast address。 ➢其中所有 option 的長度都大於 0。 ➢若來源 IP address 沒有被標註，則目標 IP address 就是一個 solicited-node multicast address。 ➢若來源 IP address 是未被標註的，則訊息中不會有 link-layer address option。 8. 一個 node 必須丟棄任何沒有滿足以下全部正當性檢查的 NA： ➢Hop Limit 欄位的值為 255，也就是說該封包沒辦法透過 router forward。 ➢ICMP Checksum 是正當的。 ➢ICMP Code 是 0。 ➢ICMP 長度大於 24 個 octets。 ➢目標 Address 不是 multicast address。 ➢若目標 address 是一個 multicast address，則 Solicited flag 為 0。 ➢其中所有 option 的長度都大於 0。
RFC 4862	1. 在將所有單播位址分配給 Interface 之前，必須對所有單播地址執行重複位址檢測。 2. 節點必須以靜默方式丟棄任何未通過[RFC4861]中指定的有效性檢查的 NS 或 NA。 3. 無效位址不得用作傳出通信中的來源位址，不得將其識別為接收 Interface 上的目標。

除上表所提必須規範外，下表列出 IPv6 寬頻分享器基本需求選項規範建議：

表 41、IPv6 寬頻分享器基本需求選項規範建議

寬頻分享器之 IPv6 基本需求選項規範建議	
RFC 7084 WAN	1. IPv6 CE Router 應支援 DNS Search List (DNSSL)。 2. IPv6 CE Router 應實作 Network Time Protocol (NTP)。 3. IPv6 CE Router 應實作 Information Refresh Time option 相

寬頻分享器之 IPv6 基本需求選項規範建議	
介面	關客戶端行為。 4. 如 delegated prefix 太小無法配置其所有 Interface 時，IPv6 CE Router 應該記錄系統管理錯誤。 5. 如 IPv6 CE Router 收到的任何封包目的為 CE Router delegated prefix(es)但不屬於 CE Router LAN 端 prefix 包含的子集時，必須丟棄該封包。 6. IPv6 CE Router 應支援 Prefix Exclude option。
RFC 7084 RFC 7084 LAN 介面	1. IPv6 CE Router 應可產生 ULA prefix 且該 ULA Prefix 的值是可配置的，重新啟動後仍維持此 Prefix。 2. A and L flags 應可由用戶自行配置(預設情況皆應設定為 1) 。 3. RA 通告訊息應將 M flag 設置為 0 並將 O flag 設置為 1。 4. IPv6 CE Router 應可於 WAN Interface 上的 DHCPv6 客戶端接收到其配置給 LAN 端的 DHCPv6 options。
RFC 7084 其他	1. IPv6 CE Router 應支援 6rd 與 DS-Lite 轉移技術。 2. IPv6 CE Router 應支援 RFC6092 針對 CPE 設備訂定之安全能力。 3. IPv6 CE Router 應支援 BCP 38 ingress filtering 的規範建議。 4. 如 IPv6 CE Router 防火牆配置為可過濾 tunnel 技術封裝之資料，則防火牆應提供過濾來自 tunnel 解封裝封包的功能。

關於寬頻分享器之 IPv6 安全需求必須規範，其中 RFC 6092 定義了 CPE 的 IPv6 安全規範，另外 RFC 4890 及 RFC 7123 制定 ICMPv6 過濾原則及 IPv6 在 IPv4 的安全規範，有關安全需求必須規範建議如下表所示：

表 42、寬頻分享器之 IPv6 安全需求必須規範建議

寬頻分享器之 IPv6 安全需求必須規範建議	
RFC 6092	1. 當封包從內部轉送到外部時，必須刷新 flows 的狀態記錄，並且當封包以反向方向轉送時，可以更新狀態記錄。 2. 在預設的情況下，Gateway 必須回應 ICMPv6 Destination

寬頻分享器之 IPv6 安全需求必須規範建議	
RFC 6092	Unreachable 錯誤代碼 1 給以下封包（等待至少 6 秒）： ➢ unsolicited inbound SYN packet。 ➢ Destination Unreachable。 3. 如果 Gateway 無法確定 TCP flow 或 DCCP 端點是否處於活動狀態，則其可放棄該狀態記錄。在這種情況下： ➢ established flow idle-timeout 的值不得少於兩小時四分鐘。 ➢ transitory flow idle- timeout 的值不得少於四分鐘。 ➢ idle-timeouts 的值可以由網路管理員配置。 4. IPv6 簡化安全功能的 Internet gateways 必須提供一個易於選擇的配置選項 transparent mode(可預先配置) 。 5. IPv4/IPv6 共存且採用 IPv4/IPv6 協定轉換(Translation)架構，位址轉換設備應提供 IPv4 與 IPv6 轉換日誌紀錄資訊並傳送給日誌伺服器。
RFC 4890、RFC 7123	1. 網路管理不允許 IPv6 隧道時，需可阻擋 IPv4 header 中 Type 欄位值為 41 的 IPv4 封包。 2. 可過濾 ICMPv6 封包，並制定封包過濾規則。 3. 可過濾內含 Extension Header 的 IPv6 封包，並制定封包過濾規則。

關於寬頻分享器之 IPv6 定址需求必須規範，其中 RFC 3646 定義了 DHCPv6 DSN 規範，另外 RFC 3315、RFC 3736 及 RFC 633 制定 DHCPv6 定址規範，有關定址需求必須規範建議如下表所列：

表 43、寬頻分享器之 IPv6 定址需求必須規範建議

寬頻分享器之 IPv6 定址需求必須規範建議	
RFC 3646	1. DNS Recursive Name Server option 不能出現在以下訊息中：Solicit，Advertise，Request，Renew，Rebind，Information-Request 和 Reply。 2. Domain Search List option 不能出現在以下消息中：Solicit，Advertise，Request，Renew，Rebind，Information-Request 和 Reply。

寬頻分享器之 IPv6 定址需求必須規範建議	
RFC 8415 (取代 RFC 3315、3736、3633)	1. 每個 DHCP client 或 DHCP server 都要必須有一個固定且唯一的 DUID。 2. Client 配置請求 delegated prefixes 應該要生成至少一個不同的 IA_PD。 3. Client 的每個網路 interface 必須至少關聯一個 IA。 4. 如 DHCP client 從 server 沒有接收到應該要收到的回應，client 必須重送請求。 5. Client 在重送的訊息中必須讓 transaction ID 維持不變。 6. Client 或 server 必須丟棄任何收到含有未知訊息形式的 DHCP 訊息。 7. Client 必須使用該 interface 上的 link-local address 作為 IP 封包 header 中的 source address。 8. Client 必須丟棄任何以下接收到的訊息：: request, confirm, renew, rebind, decline, release, information request, relay-forward, relay-reply。 9. Server 必須丟棄以下接收到的訊息： ➢任何接收到的訊息: advertise, reply, reconfigure, relay-reply。 ➢任何目標位址是 unicast address 的 solicit、confirm、rebind 或 Information-request。 ➢沒有包含 client 和 Server Identifier option 的 solicit, confirm, rebind。 10.Relay agent 必須丟棄任何以下接收到的訊息，任何接收到的訊息: advertise, reply, reconfigure。 11.Servers 必須丟棄任何符合以下任一條件的 request message： ➢ 沒有包含 Server Identifier option。 ➢ Server Identifier option 中的內容跟 server 的 DUID 不匹配。 ➢ 不包含 Client Identifier option。 12.Server 必須丟棄任何符合以下任一條件的 renew message： ➢ 不包含 Server Identifier option。 ➢ Server Identifier option 中的內容和 server 識別碼不匹配。 ➢ 不包含 Client Identifier option。

寬頻分享器之 IPv6 定址需求必須規範建議	
RFC 8415 (取代 RFC 3315、3736、3633)	13.Servers 必須丟棄符合以下任一條件的 decline message： ➢ 不包含 server 識別選項。 ➢ 在 Server Identifier option 中的內容與 server 的識別碼不匹配。 ➢ 不包含 Client Identifier option。 14.Server 必須丟棄任何符合以下任一條件的 release message： ➢ 不包含 Server Identifier option。 ➢ Server Identifier option 中的內容和 server 識別碼不匹配。 ➢ 不包含 Client Identifier option。 15.Servers 必須丟棄任何符合以下條件的 Information-request message： ➢ Server Identifier option 中的 DUID 和 server 的 DUID 不匹配。 ➢ 包含 IA 選項。 16.Client 必須丟棄任何符合以下任一條件的 advertise message： ➢ 沒有包含 Server Identifier option。 ➢ 沒有包含 Client Identifier option。 ➢ Client 的識別碼選項跟 client 的 DUID 不匹配。 ➢ Transaction-id 欄位的值和 client 在 solicit message 所用的值不匹配。 17.Clients 必須丟棄任何符合以下任一條件的 reply message： ➢ 不包含 Server Identifier option。 ➢ “transaction-id”欄位中的值和原來訊息中的值不匹配。 18.Clients 必須丟棄任何符合以下任一條件 的 Reconfigure message： ➢ 不是以 unicast 傳給 client。 ➢ 沒有包含 Server Identifier option。 ➢ 沒有包含 client 的 DUID 在 Client Identifier option 中。 ➢ 沒有包含 Reconfigure Message 選項且 msg-type 要是正確的。 ➢ 包含 IA 選項和 msg-type 是 INFORMATION-REQUSET ➢ 沒有包含 DHCP 驗證。

另外為了符合中華電信固網所採用 PPPoE 連線規格，寬頻分享器之 IPv6 需支援 RFC 5072 所定義的 PPPv6 規範，此項目必須規範建議如下表所列：

表 44、寬頻分享器之 PPPv6 需求必須規範建議

寬頻分享器之 PPPv6 需求必須規範建議	
RFC 5072	1. PPP 連結的本地端需使用協商的介面識別碼來自動配置 PPP 介面的 IPv6 連結本地單播地址。

以上所列為寬頻分享器和 IPv6 有關的 RFC 規範，詳細資訊請參閱附錄六說明。

二. 寬頻分享器製造商測試規範

針對 IPv6 寬頻分享器製造商測試規範，分為兩大部分分別為:

◆ 主要建議測試項目規範

- IPv4/IPv6 PPPoE（Point-to-Point Protocol over Ethernet）連線功能測試
- IPoE（Internet Protocol over Ethernet）連線功能測試
- 寬頻分享器 IPv6 位址配置模式測試
- IPv6 PPPoE 斷線重撥測試
- MTU（Maximum Transmission Unit，最大傳輸單位）測試
- 寬頻分享器 IPv6 防火牆功能測試

◆ IPv6 ready logo 建議測試項目規範

- WAN（Wide Area Network，廣域網路）測試
- LAN（Local Area Network，區域網路）測試
- 一般（General Requirement）測試
- ULA（Unique Local Address，唯一區域地址）測試

(一) 主要建議測試項目規範

1. IPv4/IPv6 PPPoE 連線功能測試

IPv6 Ready Logo 針對 CE Router 的測試項項目中，只針對 IPoE 連線功能有相關測試項目，並未提列 PPPoE 連線功能測試項目，因應國內一般家用使用者所使用的主要固網 ISP 中華電信，其所採用網路連線通訊協定為 PPPoE，因此將此功能列為建議測試項目。

PPP 通常用在兩個網路節點間建立直接的通訊管道。主要是用於利用點對點的通道（Tunnel）來連接兩台網路設備，也適

合用在寬頻網路設備的通訊連接。PPP 模式主要是提供一種資料鏈結層網路認證連線的機制，ISP 端的網路設備 BRAS 必須向 RADIUS 伺服器轉發用戶訊息，由 RADIUS 伺服器進行用戶身份認證，如果認證通過，用戶才可以繼續進行配置 IP 位址程序。PPPoE 測試架構如下圖所示：

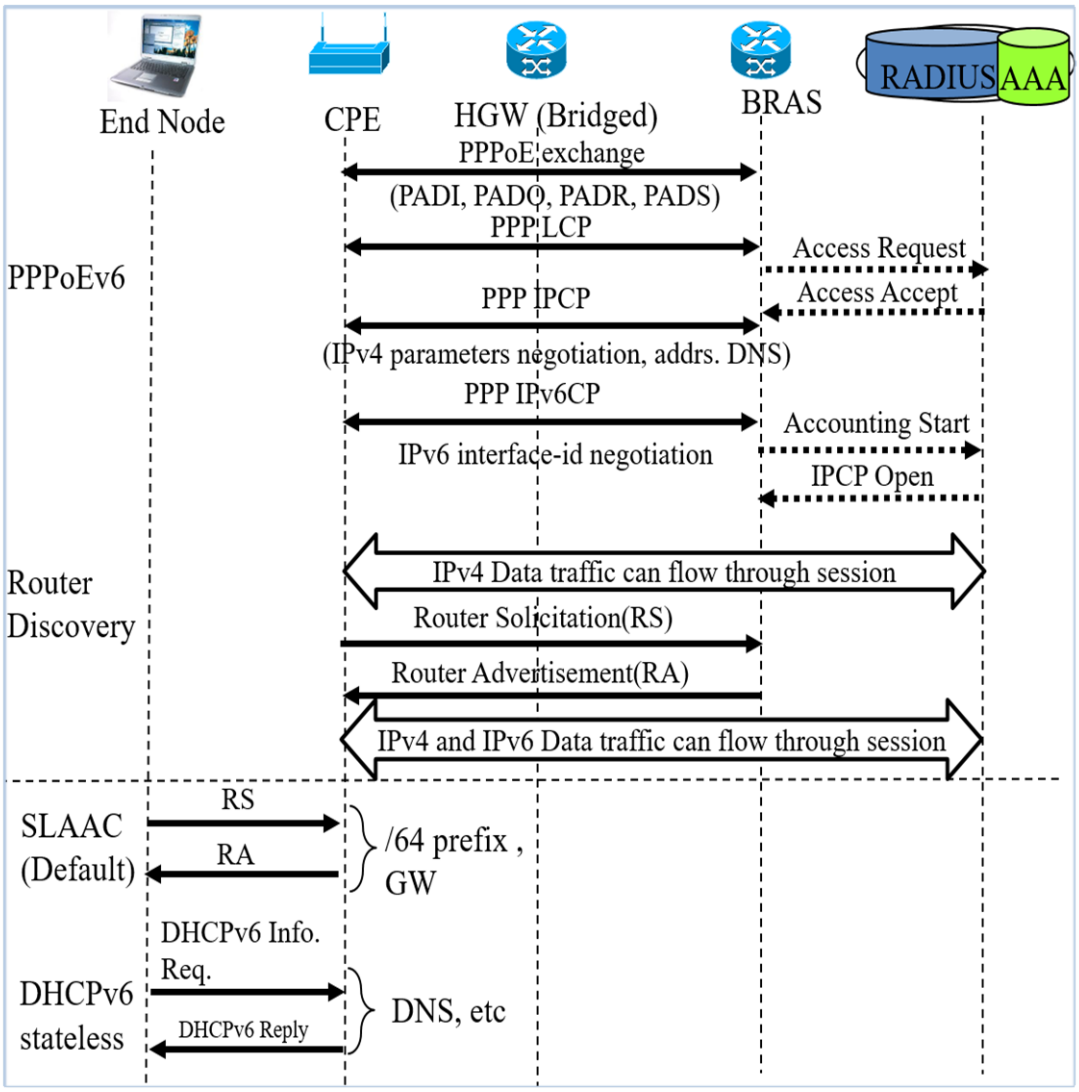

圖 52、IPv6 PPPoE 連線測試架構

PPPoE 測試規範建議步驟及測試內容如下表所示:

表 45、PPPoE 測試規範建議流程

步驟	測試內容
1	動作：發起 PPPoE exchange 進行 PADI、PADO、PADR 及 PADS。 檢驗：是否收到對方的 MAC address 及此對話的 session ID。
2	動作：發起 PPP LCP。 檢驗：收到每部裝置檢視的資料大小、壓縮及認證。
3	動作：發起 PPP IPCP。 檢驗：是否順利完成 IPCP 訊息交換。
4	動作：發起 PPP IPv6CP。 檢驗：是否順利完成 IPv6CP 訊息交換。
5	動作：同時以 IPv4 及 IPv6 進行連線測試，檢查是否在同一 PPP session ID 裡。 檢驗：是否同一 PPP session ID 的連線同時包含 IPv4 與 IPv6 連線成功收到 RA 封包。
6	動作：寬頻分享器向使用者終端裝置配置連網參數。 檢驗：用戶終端設備是否能成功連線 IPv4 與 IPv6 網際網路。

2. IPoE 連線功能測試

IPoE 通常用在區域網路內，用戶端設備本身無需建立點對點的網路連線，而是由業者端網路設備直接配發連網參數給終端裝置的方式進行。國內 Cable 業者多採用此種連線規範。IPoE 連線測試架構如下圖所示：

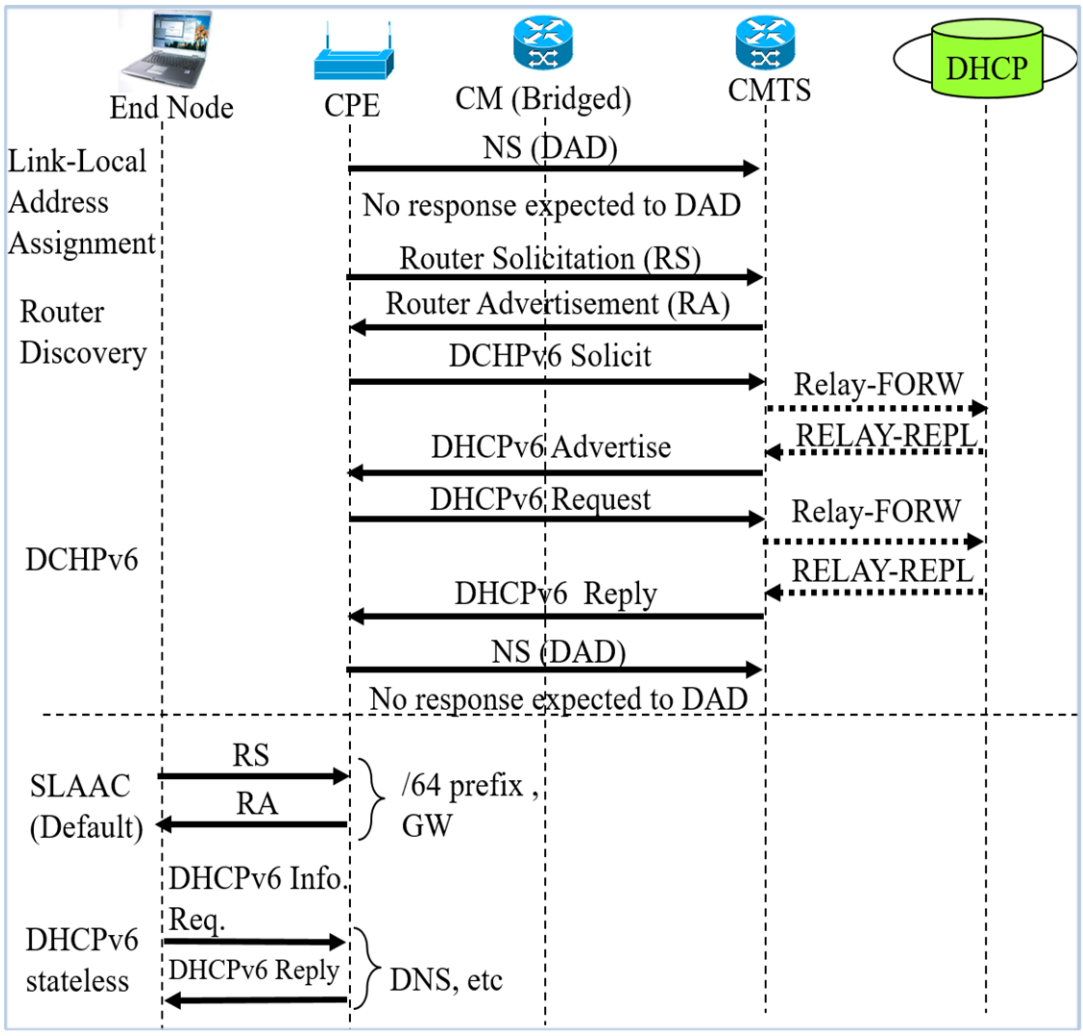

圖 53、IPv6 IPoE 連線測試架構

IPoE 測試規範建議步驟及測試內容如下表所示:

表 46、IPoE 測試規範建議流程

步驟	測試內容
1	動作：CE-Router WAN 端 interface 傳送 Neighbor Solicitation (即進行 DAD)。 檢驗：不會收到相對應的 Solicited Neighbor Advertisement。
2	動作：CE Router 向 FF02::2 (所有 router 的 multicast address)發送 Router Solicitation。 檢驗：CE Router 收到 M bit 和 O bit 皆為 1 的 Solicited Router Advertisement，內容告知 CE Router 需要透過 DHCP 取得資訊。

步驟	測試內容
3	動作：CE Router 向 ff02::1:2 (所有 DHCP server 和 relay agent 的 multicast address) 傳送 DHCP Solicit 訊息。 檢驗：CE Router 收到 DHCP Advertisement，並從這個封包中的來源 IP address 得知 DHCP server 的 link-local address。
4	動作：CE Router 向在步驟 3 所得知的 DHCP server 的 link-local address 傳送 DHCP Request 訊息。 檢驗：CE Router 收到 DHCP Reply 訊息，取得 prefix 和 DNS Server 等資訊。
5	動作：使用者終端設備向 CE Router 發送 Router Solicitation (即進行 SLAAC)。 檢驗：CE Router 向終端設備回傳 Router Advertisement，告知終端設備 prefix 和 gateway 位址資訊。
6	動作：使用者終端設備向 CE Router 發送 DHCP Request。 檢驗：CE Router 向終端設備發送 DHCP Reply，讓終端設備取得 DNS Server 等資訊。
7	動作：寬頻分享器向使用者終端裝置配置連網參數。 檢驗：用戶終端設備是否能成功連線 IPv4 與 IPv6 網際網路。

3. 寬頻分享器 IPv6 位址配置模式測試

在實際生活中，行動裝置經常需要在無線網路中切換，因此需要分配動態地址。而 DHCP（Dynamic Host Configuration Protocol）動態主機配置協議，用於網路內自動分配地址的網路協議，也是網路管理的重要組成部分，而 DHCPv6 是網路協議 DHCP 為 IPv6 制定的升級版本。但是主流行動裝置的作業系統 Android，並不支援 IPv6 的 DHCPv6 動態主機配置協議。但是 Windows、OS X、iOS 以及大部分 Linux 系統，都支援 DHCPv6 協議。為符合支援大多數裝置的規格，寬頻分享器須具備不同的位址配置模式。

此測試項目的目的即是在測試寬頻分享器是否具備 SLAAC、RDNSS、DHCPv6 三種位址配置模式功能，可供使用者選擇不同 LAN 端位址配置方法。

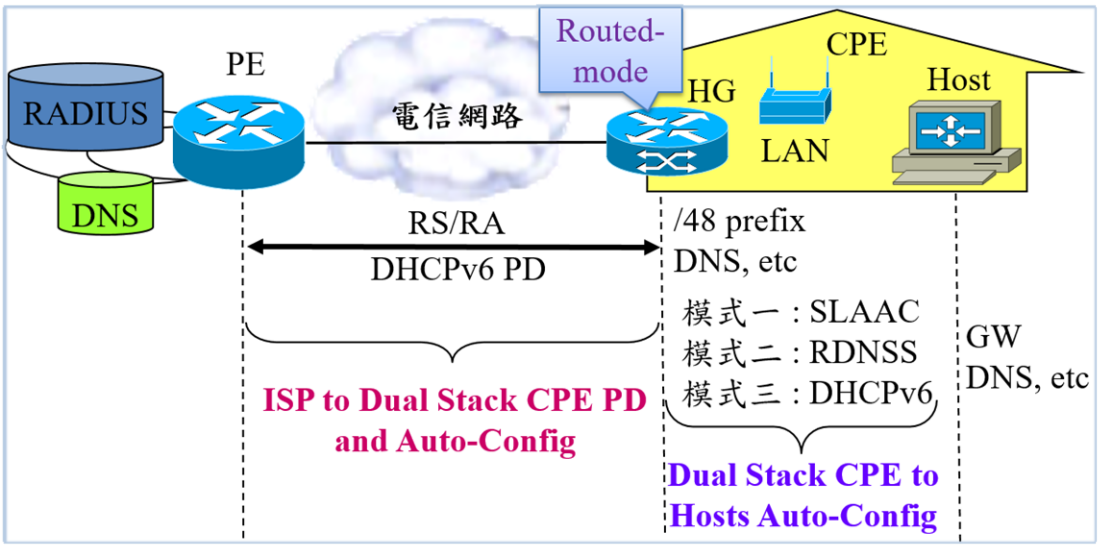

圖 54、寬頻分享器 IPv6 位址配置模式測試

寬頻分享器 IPv6 位址配置模式測試規範建議分為〝SLAAC + stateless DHCPv6 搭配 RDNSS 配置〞及〝SLAAC + stateful DHCPv6 配置〞模式，其測試步驟及內容如下表所示:

表 47、SLAAC + stateless DHCPv6 搭配 RDNSS 配置測試規範建議

步驟	測試內容
1	動作：CE-Router 從 WAN 端取得 Prefix 和 DNS Server 位址資訊。
2	動作：CE-Router 設定啟動 SLAAC 和 RDNSS 功能。
3	動作：CE-Router 啟動 LAN 介面。 檢驗：CE-Router 會定期發送 RA 訊息，其中 M、O 旗標都設定為 0，RA 訊息中 Option 欄位帶有 DNS Server 位址資訊。
4	動作：Host 介面設定為自動指派 IPv6 位址。
5	動作：Host 啟動介面並連線至 CE-Router 的 LAN 介面。 檢驗：Host 發送 RS 訊息到網域中，CE-Router 收到後會立刻

步驟	測試內容
	發送 RA 訊息。Host 收到 RA 訊息後，根據其 Prefix 使用 EUI-64 或是 Privacy Extension 組成位址，此外 Host 會解析 RA 的 Option 欄位得到 DNS Server 資訊。

表 48、SLAAC + stateful DHCPv6 配置測試規範建議

步驟	測試內容
1	動作：CE-Router 從 WAN 端取得 Prefix 和 DNS Server 位址資訊。
2	動作：CE-Router 設定啟動 SLAAC 和 DHCPv6 功能。
3	動作：CE-Router 啟動 LAN 介面。 檢驗：CE-Router 需定期發送 RA 訊息，其中 M 旗標設定為 0 而 O 旗標設定為 1。
4	動作：Host 介面設定為自動指派 IPv6 位址。
5	動作：Host 啟動介面並連線至 CE-Router 的 LAN 介面。 檢驗：Host 發送 RS，CE-Router 收到後會立刻發送 RA。Host 收到 RA 訊息後，根據其 Prefix 使用 EUI-64 或是 Privacy Extension 組成位址。Host 向 DHCPv6 伺服器請求 DNS 伺服器位址，CE-Router 收到請求後傳送回覆訊息給 Host，Host 解析回覆訊息得到 DNS 資訊。

4. IPv6 PPPoE 斷線重撥測試

中華電信 Hinet 是以非固定制 IP 配發位址，系統為保持營運的彈性會固定一段時間後回收 IP 一次，回收 IP 時用戶會產生斷線的情形，因此一般寬頻分享器多會設計斷線自動重撥的機制，才能讓 IP 在回收後再重新連結上網路。

本項測試主要目的在測試當網路產生斷線後，寬頻分享器是否會自動重撥，自動重撥的過程是否符合規範。

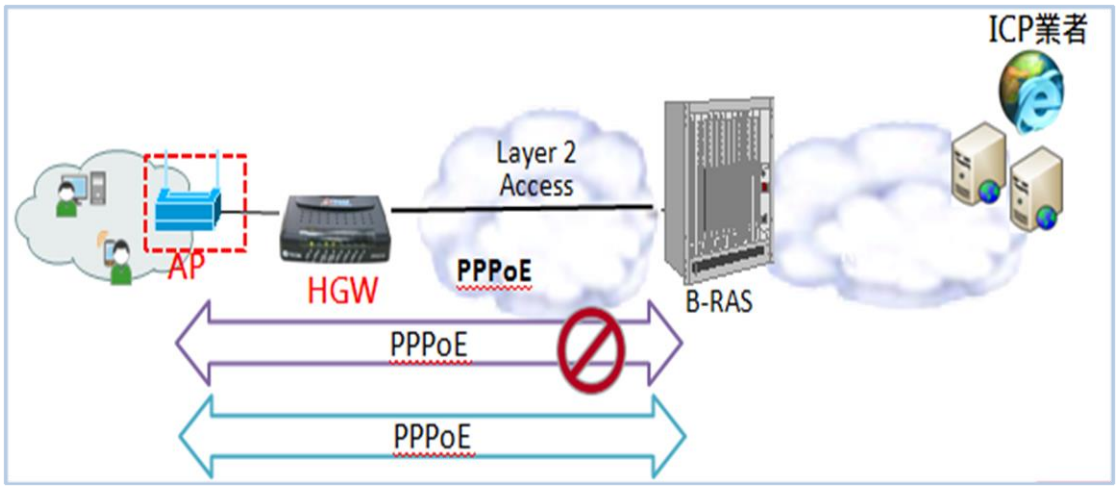

圖 55、IPv6 PPPoE 斷線重撥測試

寬頻分享器 IPv6 PPPoE 斷線重播測試規範建議如下表所示:

表 49、寬頻分享器 IPv6 PPPoE 斷線重播測試規範建議流程

步驟	測試內容
1	動作：第一次撥接成功後，將 WAN 端斷線。 檢驗：如果沒有其他路由資訊，IPv6 CE Router 必須使用 [RFC4861]中規定的 Router Discovery 來尋找 default router(s)，將發現的 Router 位址作為 next hop，並更新路由表預設路由。

5. MTU（Maximum Transmission Unit，最大傳輸單位）測試

MTU 代表傳送一個數據封包時可以使用的最大長度，以位元組（byte）為單位。在電腦主機上指的是第三層封包（如 IP Packet）的大小，在路由器上則是指網路第二層的訊號框(如 Ethernet Frame)。不同的網路通訊協定會有不同的 MTU。LAN port 預設的 MTU 為 1500 位元組，但當撥接上網時，PPPoE 介面會因為 PPP header（包含 6 位元組 PPPoE header 及 2 位元組

PPP ID)，造成 IPv6 MTU 降低為 1492 位元組，而可能引發後續問題。

- ◆ 若由用戶主機直接撥接，因為 PPP 協定會協調 MTU，應該不會有 MTU 及封包切割問題
- ◆ 若是由路由器撥接，就容易引發 MTU 議題

本測試項目的目的在於測試寬頻分享器 IPv6 MTU 是否符合規定，在封包過大時訊息傳遞是否正確。

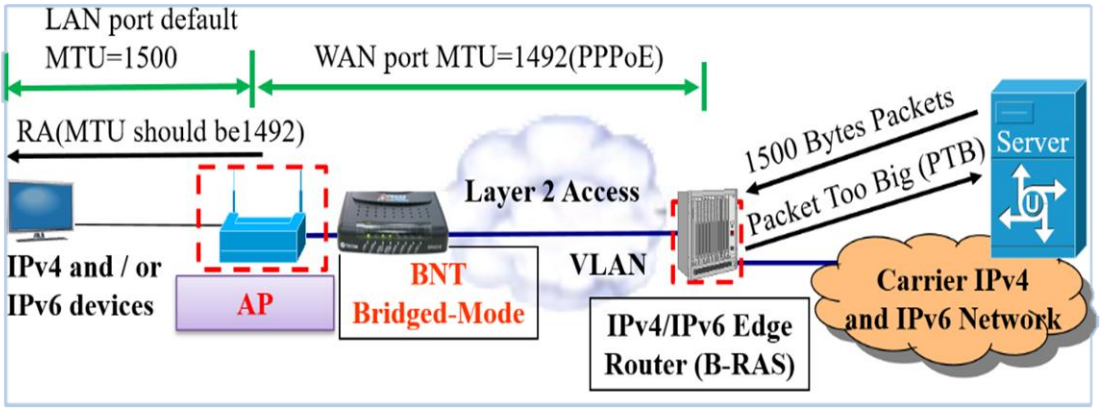

圖 56、寬頻分享器 IPv6 MTU 測試架構

寬頻分享器 IPv6 MTU 測試規範建議如下表所示:

表 50、寬頻分享器 IPv6 MTU 測試規範建議流程

步驟	測試內容
1	動作：將 CE-Router WAN 端 interface 的 MTU 設為 1492。
2	動作：LAN 端使用者設備向 2001:4860:4860::8888 (Google Public DNS for IPv6)發送 payload 為 1444 bytes 的 ICMPv6 Echo Request (ICMPv6 的 header 長度為 48，加上 payload 剛好為 1492) 。 檢驗：2001:4860:4860::8888 回傳 ICMPv6 Echo Reply 給使用

步驟	測試內容
	者設備。
3	動作：LAN 端使用者設備向 2001:4860:4860::8888 發送 payload 為 1445 bytes 的 ICMPv6 Echo Request (ICMPv6 的 header 長度為 48，加上 payload 為 1493) 。 檢驗:CE-Router 要向 LAN 端使用者設備發出 ICMPv6 Packet Too Big。

6. 寬頻分享器 IPv6 防火牆功能測試

以位址配發方式來說，IPv6 具備隨插即用(Plug & Play)的特性，也就是用戶設備主機具備自動配置能力。因為 IPv6 配發的位址都是公用位址（Public IP），網路安全防護更顯重要，目前 IPv6 Ready Logo 有關 CE-Router 的部分，並不包含安全（Security）測項，CE-Router Logo 是根據 RFC 7084 制定測試項目，但有關 Security 的部分，目前並非為必須功能。

本測試項目主要的目的為：

◆ 阻擋不必要的 incoming 連線：

■ 可過濾 ICMPv6 封包，並制定封包過濾規則。

■ 可過濾內含 Extension Header 的 IPv6 封包，並制定封包過濾規則。

◆ 透通 ICMPv6 Destination Unreachable 和 Packet Too Big 訊息。

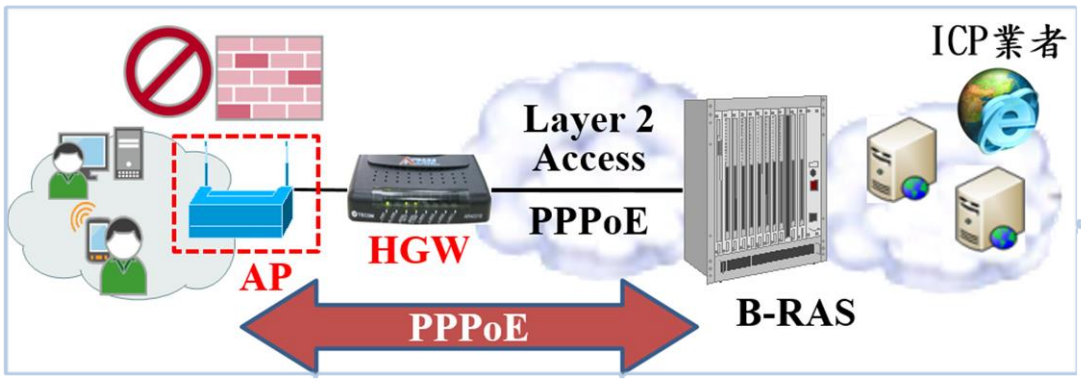

圖 57、寬頻分享器 IPv6 防火牆功能測試

寬頻分享器 IPv6 防火牆功能測試規範建議分為 ICMPv6 封包過濾〝Destination Unreseachable〞及〝Packet Too Big〞，測試步驟及內容如下表所列:

表 51、ICMPv6 封包過濾測試規範建議–Destination Unreseachable

步驟	測試內容
1	動作：勾選開啟防火牆功能。
2	動作：加入防火牆規則，allow ingress ICMPv6 Unreachable。
3	動作：加入防火牆規則，deny Ingress ICMPv6。
4	動作：內部客戶端對外 ping 不存在的 ip 位址。 檢驗：內部客戶端會接收到 ICMPv6 Unreachable 的訊息。
5	動作：內部客戶端對外 ping 存在的 ip 位址。 檢驗：內部客戶端不會接收到 ICMP Echo Rely 的訊息。

表 52、ICMPv6 封包過濾測試規範建議 – Packet Too Big

步驟	測試內容
1	動作：勾選開啟防火牆功能。
2	動作：加入防火牆規則，allow Ingress ICMPv6 Packet Too Big。
3	動作：加入防火牆規則，deny Ingress Extension Header
4	動作：外部客戶端對內部客戶端傳送加入 Extension Header 的封包(例如設定帶有 fragment Header)。 檢驗：內部客戶端不會接收到外部客戶端傳送的封包。

5	動作：內部客戶端對外傳送超過支援 MTU 大小的封包，並不加入 fragment Header。 檢驗：內部客戶端會接收到 ICMPv6 Packet Too Big 訊息。

(二) IPv6 ready logo 建議測試項目規範

IPv6 CE ready logo 的測試可區分為 WAN、LAN、一般測試及 ULA 四類，共 23 項測試項目，如下表所示。WAN 與 LAN 兩類為建議測試項目，一般測試以及 ULA 部分測試項目，則建議可視廠商實際需求評估是否納入建議測試項目。

表 53、IPv6 ready logo 建議測試項目規範

WAN Side Test:
1. DUPLICATE ADDRESS DETECTION
2. ROUTER DISCOVERY
3. ADDRESS LIFETIME
4. DHCPV6
5. DHCPV6 PREFIX DELEGATION
6. UNNUMBERED WAN
7. DHCPV6 SOL_MAX_RT
8. L FLAG PROCESSING

General Requirement Test:
1. ICMPV6
2. IPV6 FORWARDING BEFORE ADDRESS ACQUISITION
3. NO DEFAULT ROUTE
4. FORWARDING LOOPS

LAN Side Test:
1. DUPLICATE ADDRESS DETECTION AND NEIGHBOR DISCOVERY
2. ASSIGNING PREFIXES TO LAN INTERFACES
3. ROUTER ADVERTISEMENT
4. STATELESS DHCP SERVER
5. DHCP SERVER
6. PREFIX CHANGE
7. LINK MTU
8. DNS INFORMATION IN ROUTER ADVERTISEMENT
9. INGRESS FILTERING

Unique Local Address Test:
1. ULA PREFIX GENERATION
2. ULA SITE BORDER

各類測試項目中，經過整理及訪談友訊及華碩業者建議，又以下表所提列為主要重點測試項目。針對各項測試方法及流程詳細內容介紹，請參考附錄六。

表 54、IPv6 ready logo 建議主要重點測試項目

類別	測試項目
WAN 測試項目	◆ ROUTER DISCOVERY ◆ ADDRESS LIFETIME ◆ DHCPV6 ◆ DHCPv6 PREFIX DETECTION ◆ DHCPv6 SOL_MAX_RT
LAN 測試項目	◆ DUPLICATE ADDRESS DETECTION AND NEIGHBOR DISCOVERY ◆ ASSIGNING PREFIXES TO LAN INTERFACES ◆ ROUTER ADVERTISEMENT ◆ STATELESS DHCP SERVER ◆ DHCP SERVER ◆ LINK MTU ◆ DNS INFORMATIONATION IN ROUTER ADVERTISEMENT ◆ INGRESS FILTERING
一般測試項目	◆ ICMPV6 ◆ NO DEFAULT ROUTE

以上寬頻分享器所提建議開發規範及測試項目，分別和國內前兩大品牌業者友訊及華碩進行訪談溝通，以聽取業者意見修訂後內容，期能更符合業者的期待及需求。業者訪談時程及訪談內容及記錄，詳細資訊請參閱附錄六說明。

以上所列為寬頻分享器和 IPv6 有關的測試項目，詳細資訊請參閱附錄六說明。

第二節　建置寬頻分享器支援 IPv6 之測試平台

關於寬頻分享器支援 IPv6 之測試平台，規畫連線測試系統將包含中華電信 HiNET 非固定制電路及南桃園大寬頻 Cable 電路所組成。實測平台架構如下圖所示：

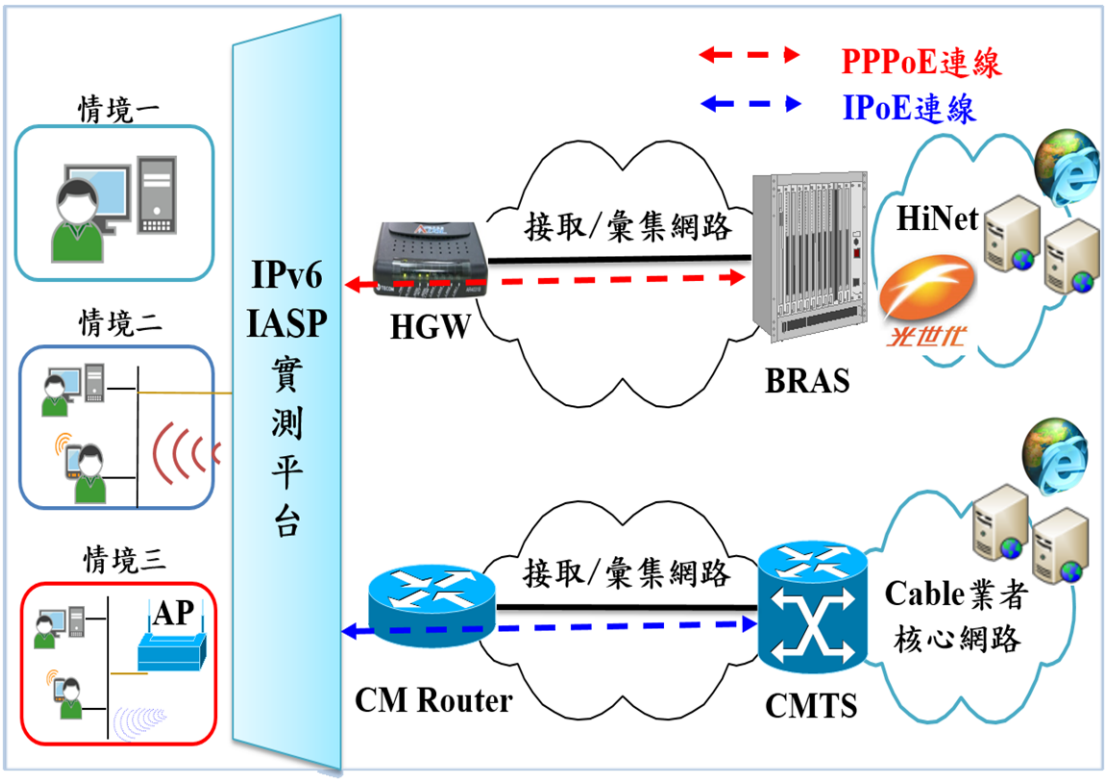

圖 58、寬頻分享器支援 IPv6 之測試平台架構

測試項目將以使用者情境為主，測試條件為：

◆ 中華電信 IPv6 PPPoE 及 TBC IPv6 Cable Modem 之連線實際測試，以測試製造日期為西元 2018 年（107 年）（含）之後之 IPv6 寬頻分享器 10 款，包含友訊、華碩、TP-Link 以及 TOTOLINK 等 4 家寬頻分享器製造商，每家至少二款。

下表所列為本次測試寬頻分享器廠牌及型號：

表 55、寬頻分享器測試廠牌及型號列表

廠牌	D-Link	ASUS	TP-Link	TOTOLINK
型號	◆ DIR-85 ◆ DIR-2608 ◆ DIR-1960 ◆ DIR1760	◆ RT-AC66U ◆ RT-AC 1300UHP	◆ Archer C1200 ◆ Archer A9	◆ A7000R ◆ A950RG
款式數量	4	2	2	2

一. 市售 IPv6 寬頻分享器之 PPPoE 測試項目成果

本次市售 IPv6 寬頻分享器和中華電信一般家用非固定制固網所支援的 IPv6 PPPoE 的連線測試，包含以下所列測試項目：

表 56、市售 IPv6 寬頻分享器和 PPPoE 連線測試項目

編號	測試項目	測試方法
1	驗證分享器 PPPoE 撥接是否正常?	連結至分享器 Web 介面，確認 PPPoE 已連線
2	驗證分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?	連結至分享器 Web 介面，確認取得 IPv6、IPv6 PD、DNSv6
3	驗證用戶 IPv6、DNSv6 取得是否正常?	使用 ipconfig 指令，確認取得用戶 IPv6、DNSv6
4	驗證用戶至 HiNet 路由是否正常?	使用 Ping 與 trace route 指令確認用戶路由正常
5	驗證用戶 IPv6 上網是否正常?	連結至 IPv6 測試網頁，確認 IPv6 上網正常 網址：http://test-ipv6.com/ 網址：http://ipv6-test.com/
6	驗證用戶熱門網頁開啟是否正常?	連結至 Google、Youtube、HiNet、Microsoft、Yahoo 等網站，確認開啟正常
7	驗證用戶上網速率是否正常?	使用 Dr. Speed 確認上下行速率正常
8	驗證分享器重撥，用戶 IPv6 更新是否正常?	用戶終端取得 IPv6 後，分享器重新撥接 PPPoE，驗證用戶終端是否

編號	測試項目	測試方法
		正常更新 IPv6
9	驗證用戶使用 IPv6 之 MTU 是否正常?	使用 netsh 指令確認用戶電腦的網路介面(區域連線)MTU 是否為 1492
10	驗證用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?	用戶終端使用 Wi-Fi 連接分享器，確認用戶取得之 IPv6、DNSv6 與上網是否正常
11	驗證用戶連接 Wi-Fi IPv6 上網是否正常?	連結至 IPv6 測試網頁，確認 IPv6 上網正常 網址：http://test-ipv6.com/ 網址：http://ipv6-test.com/
12	IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用?	測試 IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用，且正常連線
13	IPv6 PPPoE (或是 PPPoEv6)連線之 PPPoE Session 是「Share with IPv4」或是「Create a new Session」?	測試 IPv6 PPPoE (或是 PPPoEv6)連線之 PPPoE Session 是「Share with IPv4」或是「Create a new Session」
14	IPv6 寬頻分享器 IPv6 ACL 功能是否正常?	測試寬頻分享器 IPv6 ACL 功能是否能限制用戶終端 IPv6 連線

根據以上測項所得測試結果如下表所示：

表 57、市售 IPv6 寬頻分享器和 PPPoE 連線測試結果

廠牌型號	D-Link				ASUS		TP-Link		TOTOLINK	
	DIR-853	**DIR-2680**	**DIR-1960**	**DIR-1760**	**RT-AC66U**	**RT-AC1300UHP**	**Archer C1200**	**Archer A9**	**A7000R**	**A950RG**
1	分享器 PPPoE 撥接是否正常?									
	O	O	O	O	O	O	O	O	O	O
2	分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?									
	O	O	O	O	O	O	O	O	O	O

廠牌型號	D-Link				ASUS		TP-Link		TOTOLINK	
	DIR-853	DIR-2680	DIR-1960	DIR-1760	RT-AC66U	RT-AC1300UHP	Archer C1200	Archer A9	A7000R	A950RG
3	用戶 IPv6、DNSv6 取得是否正常?									
	O	O	O	O	O	O	O	O	O	O
4	用戶至 HiNet 路由是否正常?									
	O	O	O	O	O	O	O	O	O	O
5	用戶 IPv6 上網是否正常?									
	O	O	O	O	O	O	O	O	O	O
6	用戶熱門網頁開啟是否正常?									
	O	O	O	O	O	O	O	O	O	O
7	用戶上網速率是否正常?									
	O	O	O	O	O	O	O	O	O	O
8	分享器重撥，用戶 IPv6 更新是否正常?									
	O	O	O	O	O	O	O	O	O	O
9	用戶使用 IPv6 之 MTU 是否正常?									
	1500	1492	1500	1500	1492	1492	1492	1492	1484	1500
10	用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?									
	O	O	O	O	O	O	O	O	O	O
11	用戶連接 Wi-Fi IPv6 上網是否正常?									
	O	O	O	O	O	O	O	O	O	O
12	IPv6 PPPoE (或是 PPPoEv6)是否隨著 IPv4 PPPoE 啟用而自動啟用?									
	O	O	O	X	X	X	X	X	O	X
13	IPv6 PPPoE (或是 PPPoEv6)連線之 PPPoE Session 是『Share with IPv4』或是『Create a new Session』?									
	可設定兩種模式『New Session』WAN 端為斷線	可設定兩種模式	可設定兩種模式『New Session』WAN 端為斷線	可設定兩種模式『New Session』WAN 端為斷線	無提供此項設定	無提供此項設定	可設定兩種模式	可設定兩種模式	無提供此項設定	無提供此項設定

廠牌型號	D-Link				ASUS		TP-Link		TOTOLINK	
	DIR-853	DIR-2680	DIR-1960	DIR-1760	RT-AC66U	RT-AC1300UHP	Archer C1200	Archer A9	A7000R	A950RG
14	IPv6 ACL 功能是否正常？									
	O	O	O	O	O	O	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能

由以上測試結果可以看出，測試的產品中 D-Link 有 3 個型號和 TOTOLINK 有 1 個型號的產品有預設開啟支援 IPv6，其他品牌還未預設開啟支援 IPv6。

除以上所述之測試項目外，為驗證一般使用者以寬頻分享器設備長時間使用 IPv6 連網狀況，另外測試 PPPoE 以連續連網 84 小時進行測試，測試方法如下：

以自行撰寫的 windows batch 檔，每一小時下載一個檔案大小為 72 KB 的 html 檔及一個檔案大小為 49 MB 的 MP4 檔，並強制透過 IPv6 下載測試連續連網 84 小時。詳細 batch 腳本如圖下所示：

(一) 以開源專案 youtube-dl 下載 49MB 的 MP4 影片

(二) 以開源軟體 wget 下載 72KB 的 RFC 7084 網頁

(三) 以上指令皆以「-6」的參數強制透過 IPv6 下載

(四) 下載取得之檔案將以下載時間命名，如 date.mp4、date.html

完成長時間連網的寬頻分享器型號有 D-Link DIR-853、D-Link DIR-2680、D-Link DIR-1760、ASUS RT-AC66U、TP-Link Archer C1200 及 TP-Link Archer A9 等。

```
@ECHO OFF
set INTERVAL=3600

:DOWNLOADINTERVAL
echo. >> log.txt
echo %date%%time% >> log.txt
echo ----------------------------------------^
----------------------------------------^
----------------------------------------^
---------------------------------------- >> log.txt

For /f "tokens=1-4 delims=/ " %%a ^
in ('date /t') do (set mydate=%%a-%%b-%%c)
For /f "tokens=1-2 delims=/:" %%a ^
in ("%TIME%") do (set mytime=%%a%%b)

echo. >> log.txt
echo "[Youtube Download]" >> log.txt
youtube-dl.exe "https://www.youtube.com/watch?v=YbJOTdZBX1g" ^
-6 --verbose -o "[%mydate%_%mytime%] Rewind.mp4" >> log.txt 2>&1

echo. >> log.txt
echo "[RFC7084 Download]" >> log.txt
wget.exe -6 -v --no-check-certificate ^
https://tools.ietf.org/html/rfc7084 ^
-O "[%mydate%_%mytime%] RFC7084.html" >> log.txt 2>&1 || del ^
"[%mydate%_%mytime%] RFC7084.html"

timeout %INTERVAL%
GOTO DOWNLOADINTERVAL
```

將輸出檔名設為目前的時間

限制youtube-dl.exe透過IPv6方式下載

限制wget.exe透過IPv6方式下載

間隔3600秒後再次執行

圖 59、寬頻分享器測試長時間以 IPv6 連網 batch 腳本

二. 市售 IPv6 寬頻分享器之 IPoE 測試項目成果

本次市售 IPv6 寬頻分享器和 TBC 寬頻網路所支援的 IPv6 IPoE 的連線測試，其中測試項目，以及根據測項所得測試結果如下述 2 個表格內容所示：

表 58、市售 IPv6 寬頻分享器和 IPoE 連線測試項目

編號	測試項目	測試方法
1	驗證分享器連接 Cable Modem 是否正常?	連結至分享器 Web 介面，確認 IPv6 Cable Modem 已連線
2	驗證分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?	連結至分享器 Web 介面，確認取得 IPv6、IPv6 PD、DNSv6
3	驗證用戶 IPv6、DNSv6 取得是否正常?	使用 ipconfig 指令，確認取得用戶 IPv6、DNSv6
4	驗證用戶至 Cable 業者路由是否正常?	使用 Ping 與 trace route 指令確認用戶路由正常
5	驗證用戶 IPv6 上網是否正常?	連結至 IPv6 測試網頁，確認 IPv6 上網正常 網址：http://test-ipv6.com/ 網址：http://ipv6-test.com/
6	驗證用戶熱門網頁開啟是否正常?	連結至 Google、Youtube、HiNet、Microsoft、Yahoo 等網站，確認開啟正常
7	驗證用戶上網速率是否正常?	使用 Dr. Speed 確認上下行速率正常
8	驗證分享器重撥 Cable Modem，用戶 IPv6 更新是否正常?	用戶終端取得 IPv6 後，分享器重新連接 Cable Modem，驗證用戶終端是否正常更新 IPv6
9	驗證用戶使用 IPv6 之 MTU 是否正常?	使用 netsh 指令確認用戶電腦的網路介面(區域連線)MTU 是否為 1492
10	驗證用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?	用戶終端使用 Wi-Fi 連接分享器，確認用戶取得之 IPv6、DNSv6 與上網是否正常

編號	測試項目	測試方法
11	驗證用戶連接 Wi-Fi IPv6 上網是否正常?	連結至 IPv6 測試網頁，確認 IPv6 上網正常 網址：http://test-ipv6.com/ 網址：http://ipv6-test.com/
12	IPv6 連線功能是否隨著 IPv4 啟用而自動啟用?	測試 IPv6 連線功能是否隨著 IPv4 啟用而自動啟用，且正常連線
13	IPv6 寬頻分享器 IPv6 ACL 功能是否正常?	測試寬頻分享器 IPv6 ACL 功能是否能限制用戶終端 IPv6 連線

表 59、市售 IPv6 寬頻分享器和 IPoE 連線測試結果

廠牌型號	D-Link				ASUS		TP-Link		TOTOLINK	
	DIR-853	DIR-2680	DIR-1960	DIR-1760	RT-AC66U	RT-AC1300UHP	Archer C1200	Archer A9	A7000R	A950RG
1	分享器連接 Cable Modem 是否正常?									
	O	O	O	O	O	O	O	O	O	O
2	分享器 IPv6、IPv6 PD、DNSv6 取得是否正常?									
	O	O	O	O	O	O	O	O	O	O
3	用戶 IPv6、DNSv6 取得是否正常?									
	O	O	O	O	O	O	O	O	O	O
4	用戶至 Cable 業者路由是否正常?									
	O	O	O	O	O	O	O	O	O	O
5	用戶 IPv6 上網是否正常?									
	O	O	O	O	O	O	O	O	O	O
6	用戶熱門網頁開啟是否正常?									
	O	O	O	O	O	O	O	O	O	O
7	用戶上網速率是否正常?									
	O	O	O	O	O	O	O	O	O	O
8	分享器重撥 Cable Modem，用戶 IPv6 更新是否正常?									
	O	O	O	O	O	O	O	O	O	O
9	用戶使用 IPv6 之 MTU 是否正常?									
	1500	1500	1500	1500	1500	1500	1492	1500	1480	1500
10	用戶連接 Wi-Fi 上網 IPv6、DNSv6 是否正常?									

	O	O	O	O	O	O	O	O	O	O
11	用戶連接 Wi-Fi IPv6 上網是否正常?									
	O	O	O	O	O	O	O	O	O	O
12	IPv6 連線功能是否隨著 IPv4 啟用而自動啟用?									
	O	O	O	X	X	X	X	X	X	X
13	IPv6 ACL 功能是否正常？									
	O	O	O	O	O	O	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能	無支援 IPv6 ACL 功能

由以上測試結果可以看出，測試的產品中 D-Link 有 3 個型號的產品有預設開啟支援 IPv6，其他品牌還未預設開啟支援 IPv6。

除以上所述之測試項目外，為驗證一般使用者以寬頻分享器設備長時間使用 IPv6 連網狀況，另外測試 IPoE 以連續連網 18 小時進行測試，測試方法如下：

以自行撰寫的 windows batch 檔，每一小時下載一個檔案大小為 72 KB 的 html 檔及一個檔案大小為 49 MB 的 MP4 檔，並強制透過 IPv6 下載測試連續連網 18 小時。完成長時間連網的寬頻分享器型號有 D-Link DIR-853、D-Link DIR-2680、D-Link DIR-1760、D-Link DIR-1960、ASUS RT-AC66U、TP-Link Archer C1200、TP-Link Archer A9 及 TOTOLINK A7000R 等。

以上所列為寬頻分享器和中華電信 PPPoE 及 TBC IPoE 的 IPv6 連網測試，詳細資訊請參閱附錄六說明。

以上所列測試結果，已經和我國主要寬頻分享器製造銷售業者 D-Link 及 ASUS 分享和討論，業者訪談時程、訪談內容及記錄，詳細資訊請參閱附錄六說明。

第三節 研擬寬頻分享器支援 IPv6 之共同採購契約相關規範

由以上寬頻分享器製造商開發規範及寬頻分享器製造商測試規範內容，並參考包含：美國政府 IPv6 技術規畫-USG IPv6 Profile、國際 IPv6 測試計畫-Ready Logo Program、歐洲網路資訊中心-RIPE 554 Requirements for IPv6 in ICT Equipment 及中華民國交通部-IPv6 資通認證設備與軟體採購規範建議書。提出家用寬頻分享器之共同供應契約之建議規範書以供參考，其中的規範囊括 IPv6 的基本規格、路由、位址、安全性與管理。

下圖為寬頻分享器共同供應契約之設備參考規範架構，將分主機、伺服器、路由器、及網路保護裝置採購規範需求說明。針對設備對 IPv6 之功能需求規範，其中主機的規範內容包含大部分的 IPv6 基本功能，而其他設備則基於主機之規範，再加上針對該類設備額外的功能需求。針對共同採購契約 IPv6 規範驗收可操作性部分需求，請參考本節分項一.研擬寬頻分享器符合支援 IPv6 規範及標準測試項目敘述，及附錄六有詳細說明寬頻分享器測試規範建議進行 IPv6 基礎與必須功能驗證。

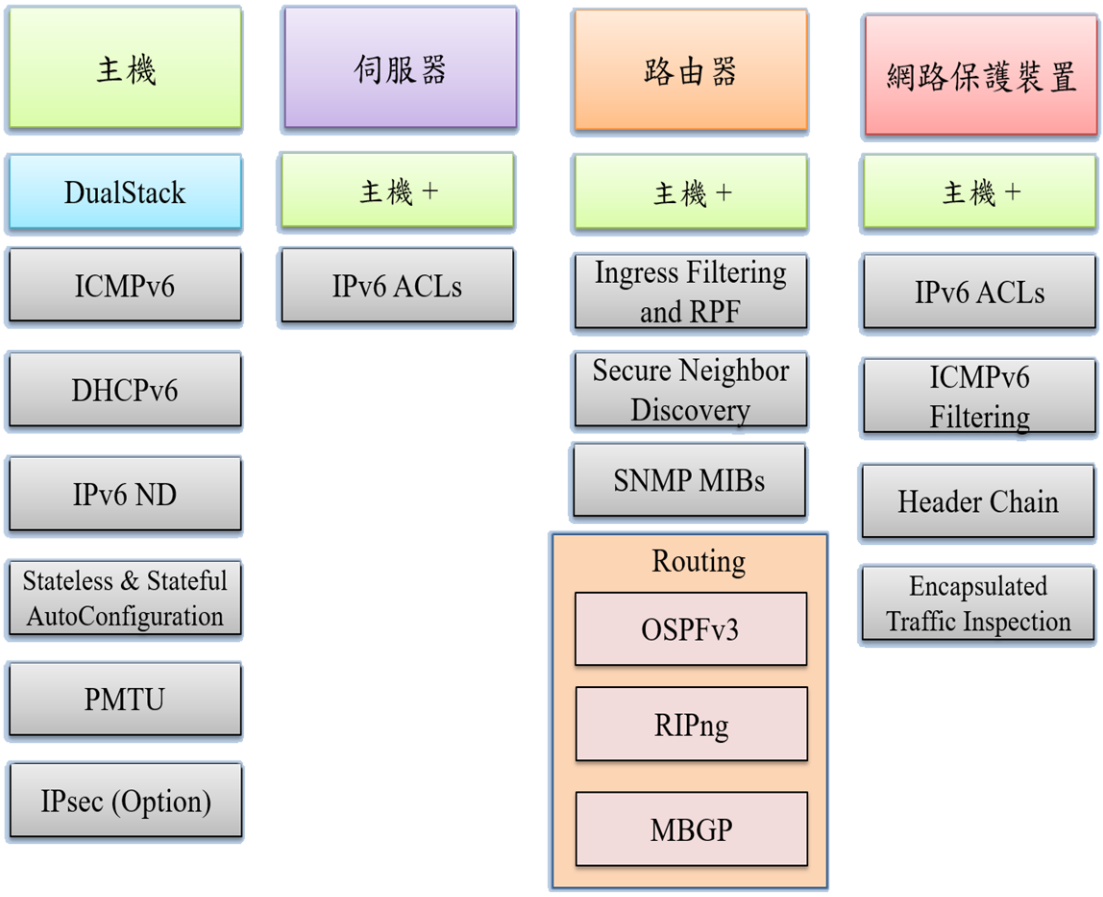

圖 60、寬頻分享器之共同供應契約之設備參考規範架構

下表為主機設備共同供應契約規範建議：

表 60、主機設備共同供應契約規範建議

項目	主機設備建議規範
1	必須支援 IPv6 Addressing Architecture 定義之位址格式規範
2	必須支援 IPv6 Default Address Selection 功能
3	必須支援 Unique Local IPv6 Unicast Addresses (ULA)位址格式
4	必須支援 ICMPv6 通訊協定
5	必須支援 DHCPv6 規範之 Client 行為
6	必須支援 Stateless 或 Stateful 位址分配機制
7	必須支援 Path MTU Discovery 功能
8	必須支援 Neighbor Discovery 功能
9	必須支援 IPv6 DNS 資源記錄以及 Extension DNS 功能

項目	主機設備建議規範
10	如須支援 Tunneling 以及 DualStack 環境，則主機必須支援基本 IPv6 轉移機制
11	如須支援 Mobile IPv6 環境，則主機必須支援 MIPv6 機制
12	必須棄用 IPv6 Type 0 Routing Headers

下表為伺服器設備共同供應契約規範建議：

表 61、伺服器設備共同供應契約規範建議

項目	伺服器設備建議規範
1	必須支援 IPv6 Addressing Architecture 定義之位址格式規範
2	必須支援 IPv6 Default Address Selection 功能
3	必須支援 Unique Local IPv6 Unicast Addresses (ULA)位址格式
4	必須支援 ICMPv6 通訊協定
5	必須支援 DHCPv6 規範之 Client 行為
6	必須支援 Stateless 或 Stateful 位址分配機制
7	必須支援 Path MTU Discovery 功能
8	必須支援 Neighbor Discovery 功能
9	必須支援 IPv6 DNS 資源記錄以及 Extension DNS 功能
10	如須支援 Tunneling 以及 DualStack 環境，則主機必須支援基本 IPv6 轉移機制
11	如須支援 Mobile IPv6 環境，則主機必須支援 MIPv6 機制
12	必須棄用 IPv6 Type 0 Routing Headers

下表為路由器設備共同供應契約規範建議：

表 62、路由器設備共同供應契約規範建議

項目	路由器設備建議規範
1	必須支援 IPv6 Addressing Architecture 定義之位址格式規範
2	必須支援 IPv6 Default Address Selection 功能
3	必須支援 Unique Local IPv6 Unicast Addresses (ULA)位址格式

4	必須支援 ICMPv6 通訊協定
5	必須支援 SLAAC 功能
6	應支援 Multicast Listener Discovery version 2 (MLDv2)以及 MLDv2 snooping 功能
7	必須支援 Router-Alert option 功能
8	必須支援 Path MTU Discovery 功能
9	必須支援 Neighbor Discovery 功能
10	必須支援 IPv6 QoS 功能
11	必須棄用 IPv6 Type 0 Routing Headers
12	如須支援 Interior Gateway Protocol (IGP) ，則 Router 路由器必須支援 RIPng 以及 OSPFv3
13	如須使用 OSPFv3，則 Router 路由器必須支援 Authentication/Confidentiality for OSPFv3
14	如須支援 Exterior Gateway Protocol (EGP)，則 Router 路由器必須支援 MBGP 功能
15	如須支援 Tunneling 以及 DualStack，則 Router 路由器必須支援基本 IPv6 轉移機制
16	如須支援 Mobile IPv6 ，則 Router 路由器必須支援 MIPv6 機制以及 Mobile IPv6 Operation With IKEv2 的行為模式
17	如須支援 MPLS，則 Router 路由器必須支援 MPLS Traffic Engineer(TE)以及 MPLS Fast Reroute(FRR)功能
18	如須支援 L3 VPN，則 Router 路由器必須支援 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN

下表為網路保護裝置設備共同供應契約規範建議：

表 63、網路保護裝置設備共同供應契約規範建議

項目	網路保護裝置設備建議規範
1	必須支援 IPv6 Addressing Architecture 定義之位址格式規範
2	必須支援 IPv6 Default Address Selection 功能
3	必須支援 ICMPv6 功能
4	必須支援 IPv6 StateLess Address AutoConfiguration 功能 (FW, IPS)
5	必須支援 Router-Alert option 功能 (FW, IPS)
6	必須支援 Path MTU Discovery 功能

7	必須支援 Neighbor Discovery 功能
8	必須支援 IPv6 QoS 功能(FW, APFW)
9	如須支援 Interior Gateway Protocol (IGP) ，則裝置必須支援 RIPng 以及 OSPFv3
10	如須支援 Exterior Gateway Protocol (EGP)，則裝置必須支援 MBGP
11	如須使用 OSPFv3，則裝置必須支援 Authentication/ Confidentiality for OSPFv3
12	如須支援 Tunneling，則裝置必須支援基本 IPv6 轉移機制 (FW)
13	必須棄用 IPv6 Type 0 Routing Headers
14	網路管理不允許 IPv6 隧道時，需可檢查/阻擋 IPv4 header 中 Type 欄位值為 41 的 IPv4 封包(IPS/FW)
15	可過濾 ICMPv6 封包，並制定封包過濾規則(FW)
16	可過濾內含 Extension Header 的 IPv6 封包，並制定封包過濾規則(FW)

原有主機、伺服器、路由器、及網路保護裝置共同採購供應契約規範項目說明，詳細資訊請參閱附錄六說明。

以上所列共同供應契約規範建議項目，已和國內主要寬頻分享器製造銷售業者 D-Link 及 ASUS 分享和討論，業者訪談時程、訪談內容及記錄，詳細資訊請參閱附錄六說明。

第四章 調研國際大型 IASP、ICP 業者導入 IPv6 原因及推動經驗

第一節 調研國際 IASP 業者導入 IPv6 原因及推動經驗

一. 行動業者 Verizon：

Verizon 身為美國前兩大行動通訊電信業者之一，原本在 3G 時代是採用 CDMA 網路系統，西元 2009 年（98 年）Verizon 到 4G 的時代並未繼續支持超行動寬頻（Ultra Mobile Broadband, UMB），卻轉而投入支持 LTE 陣營，Verizon 之所以投入 LTE 的懷抱，主要的考量因素在於經營 4G 業務所需投入建置的成本。相對於 UMB 來說，LTE 在 3GPP 已經獲得廣泛採用，其經濟規模具有足夠的影響力，因此需投入的成本相對較低。而 Verizon 採取主動佈署 IPv6 網路的計畫，主要是行動業務持續增長及支援新的網路系統 LTE 佈建的需求。

根據報告 Verizon 為維護及運作龐大的複雜網路，需要耗費大量的人力和成本來處理，而 IPv6 佈署是一種簡化網路並降低營運成本的解決方案，尤其是在建置新系統早期的投入，可避免以後系統轉換所需付出的設備及人力成本。到西元 2018 年（107 年）從 Verizon 連結到主要線上內容供應商，所產生的網路流量有 80％以上都是使用 IPv6。[3]

西元 2013 年（102 年）APNIC 34 會議上，Verizon 分享在 IPv6 網路建置之想法和經驗，要同時支援營運 LTE 及 CDMA 二種網路系統，且服務超過 9 千 4 百萬的用戶，對於 Verizon 業務發展及希望提供給用戶優質的網路連線服務，導入 IPv6 有其必要性而不只是可選項目之一，以商業考量來說，其導入支援 IPv6 的原因如下：[4~5]

(一) 全球 IPv4 地址耗盡，網路服務需要適合的解決方案：

因智慧手機的快速及蓬勃發展，且網路連線服務需要〝Always-on〞之特性，為因應大量使用者的行動網路需求，公司內部早就意識 IPv4 地址耗盡的危機必須找到解決方案，雖然 CGNAT 可以暫時解決問題，但卻有發展上的限制，而採用 IPv6 才能根本解決以持續為廣大用戶提供優質的網路服務。[4~5]

(二) IPv6 可擴充性才適合做為大型網路建置的標準：

當西元 2007 年（96 年）第一代 iPhone 及西元 2008 年（97 年）第一代 Android 手機在市場上銷售時，正式開啟智慧型手機的成長期，IPv4 地址需求快速增加，而 CGNAT 的佈建在當時 Verizon CDMA 網路系統中確實也提供快速有效的解決方案，但當 Verizon 在西元 2009 年（98 年）開始建置一個大型的網路系統以支援 4G LTE 時，Verizon 的網路工程師非常清楚根本沒有足夠的 IPv4 地址，即使採用 CGNAT 也不足以撐起一個龐大且須具備擴充性的網路系統，因此 Verizon 決定採用 IPv6 做為發展 4G LTE 網路的標準。[4~5]

(三) 採用 IPv6 才能提供全域路由地址，提供用戶高品質的網路連結服務：

採用 IPv6 才能為所有的用戶提供足夠公用 IP 地址，而不需要使用到私有 IP 再透過 NAT 轉換，也才能為所有用戶提供全域路由地址，維持高效率的網路服務，提供用戶高品質的網路連結服務。[4~5]

(四) 支援 IPv6 網路才能支撐手機連網業務的快速成長：

隨著智慧型手機的成熟發展所產生的行動用戶業務增加，依 Verizon 所擁有的 IPv4 數量，很快就會耗盡，雖然 CGNAT 得以延緩 IPv4 不足的問題，但卻帶來其他技術限制及提高維護營運成本等問題的浮現，為回應客戶的需求 Versioz 需要更積極的往下一代網際網路 IPv6 遷移，以提供更好的連網服務。[4~5]

(五) 支援 IPv6 以保持市場競爭力：

Verizon 除了經營行動網路，在固網也擁有廣大的使用者，西元 2010 年（99 年）1 月 Comcast 開始在美國進行家戶使用者 IPv6 試用計畫，同年（99 年）4 月 Verizon 也宣布由員工開始試用測試，提早為未來網路世界做好準備以提供使用者更好的網路服務，避免未來只有支援 IPv6 的內容網站出現，因為 IASP 不支援而讓用戶無法到訪該網站的情形發生，所以支援 IPv6 以提供用戶好的使用經驗也是美國大型 IASP 保持市場競爭力的基本條件。[6]

(六) 避免仰賴 CGNAT 而延遲轉換到 IPv6 計畫：

CGNAT 雖然可快速解決部分 IPv4 位址不足問題，但長遠還是需要根本的解決方案，Verizon 希望能加快轉換到 IPv6 網路，減少對 CGNAT 的仰賴及投資。[4~5]

(七) IPv6 佈署是一種簡化網路並降低營運成本的解決方案：

Verizon 為維護及運作龐大的複雜網路，需要耗費大量的人力和成本來處理，而 IPv6 佈署是一種簡化網路並降低營運成本的解決方案。[4~5]

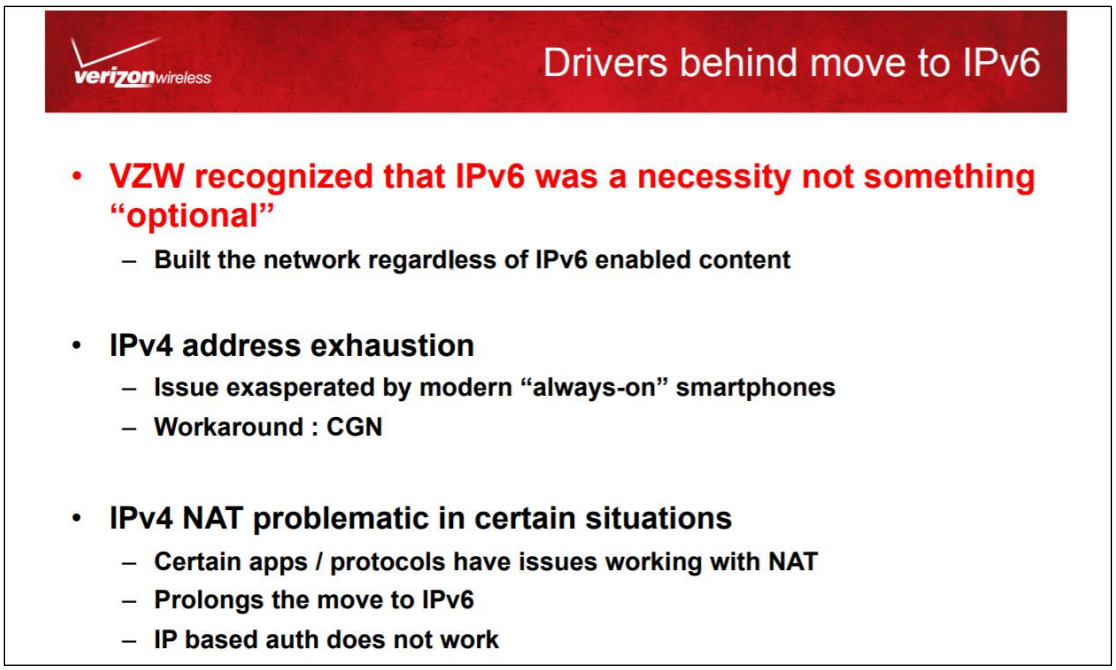

圖 61、Verizon 在 APNIC 34 會議上分享對 IPv6 網路建置想法和經驗

而以技術面評估採用 IPv6 對其企業發展也具有實質的效益，就技術面而言其導入 IPv6 的原因可歸納如下：[4~5]

(一) 解決採用 NAT 對應用發展之限制：

有些特定的應用或協議在 NAT 的環境下無法正常運作，因此限制網路服務商在提供終端用戶創新應用服務發展可能性，而採用 IPv6 比較少有這方面的問題存在。[4~5]

(二) 採用 NAT 將無法以 IP-based 做為認證授權機制：

NAT 機制將形成多個用戶共享同一個 IPv4 地址的情形，部分應用服務若希望以 IP-based 做為單一識別的認證機制，將形成認證障礙。[4~5]

(三) 採用 IPv6 協議佈建 LTE 網路是對的技術方向可以幫助企業的發展：

IPv6 標準於西元 1998 年（87 年）公布到西元 2009 年（98 年）Verizon 要由 CDMA 轉進支援 LTE 網路系統時，已經過 10 年的演進時間，雖然全球在 IPv6 佈建上的進展很緩慢，但 Versizon 經過 3G CDMA 系統逐步實驗支援 IPv4/IPv6 雙軌網路的經驗，最終經過技術的評估後認為在 LTE 系統以 IPv6 做為網路協議標準是較佳的選擇，其計畫利用演進高速分組網路（Evolved High Rate Packet Data，eHRPD）技術提供新 LTE 到舊 CDMA 無線接取網路（Radio Access Network，RAN）之間的轉換，同時可增加 3G CDMA 網路對 IPv6 的支援。[4~5]

(四) 降低網路系統維護難度：

CGNAT 讓網路架構更為複雜，因此也增加維護網路營運所需的人力，採用 IPv6 網路架構可以降低網路複雜度及維護的人力需求。[4~5]

(五) 增加網路連網效率：

減少 CGNAT 做地址轉換可以增加連網效率，為使用者提供更好的網路服務。[4~5]

就公司的立場要推動一項新政策或新的解決方案，考量不外乎人力成本、資本投資、公司的競爭力及使用者經驗等四大面向，下圖將 Verizon 推動 IPv6 的商業原因及技術原因，分別歸類於此四大面向，就可看出推動 IPv6 對 Verizon 的發展具有相當重要的實質意義。

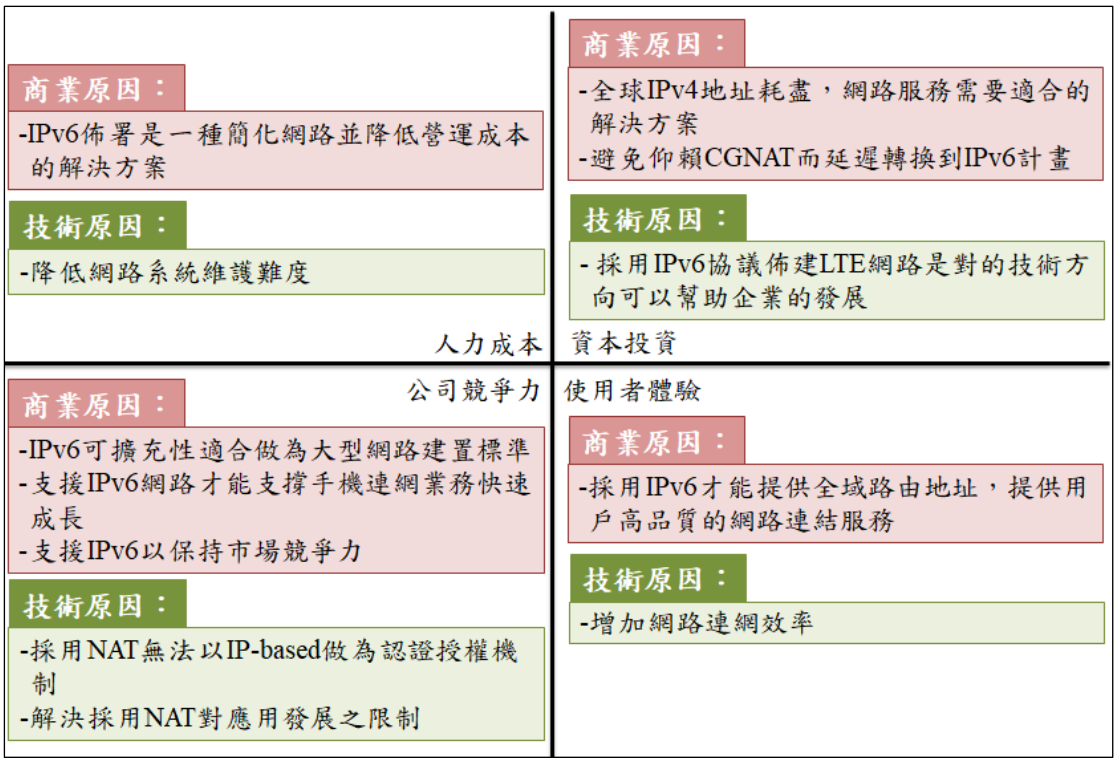

圖 62、Verizon 推動 IPv6 的原因

以上的分析說明 Verizon 採用 IPv6 做為網路技術標準的原因可看出 IPv6 對 Verizon 的業務發展具有重要的影響力，以下就 Verizon 在 IPv6 的推展經驗及過程做簡要說明：

(一) 西元 2009 年（98 年）採用 IPv6 網路架構建置 4G LTE 系統

Verizon 4G 行動網路系統在西元 2009 年（98 年）開始建置時決定採用支援 IPv6 網路架構，以因應未來手機及其他創新應用業務成長的需求。

(二) 西元 2010 年（99 年）第四季 LTE 網路系統上線

Verizon 4G LTE 行動網路系統在西元 2010 年（99 年）第四季上線，為當時全球最大支援 IPv6 網路系統。

(三) 參與西元 2011 年（100 年）6 月世界 IPv6 日（World IPv6 Day）以了解 IPv6 網路營運問題：

在缺乏 IPv6 內容網站的實際測試下，雖然 Verizon 意識到 IPv6 網路服務建置可能有許多潛在的問題，但沒有實際環境的驗證，本身很難發現網路運作的問題並做修正，因此 Verizon 決定參與世界 IPv6 日，這是 Verizon 第一次開放使用者對 IPv6 網路進行實際測試，由 Google 將 Verizon DNS 解析器（Resolvers）列表加入白名單，由此次的測試過程使用者透過 Google 的服務連結 Verizon 的網路，在實驗過程中發現相當多的 IPv6 網路潛在的問題包含網路互連問題（Peering issuzes）、網路問題（Network issuzes）及終端設備問題（Device issuzes）等，這些資訊幫助 Verizon 能有效的修正 IPv6 網路設計問題及缺失。

(四) 進行 IPv6 網路問題分析及障礙排除：

在世界 IPv6 日之後只有少數的內容網站有開啟 IPv4/IPv6 雙軌支援，因此 IPv6 相關的問題對多數使用者所造成的影響相當小，而 Verizon 也要求 Google 將其 DNS 解析器由白名單中刪除，並進

行問題分析及障礙排除，由 Verizon 自身投入並要求網路設備商及終端設備商共同投入心力，總共歷時 8 個月的時間修正完成在世界 IPv6 日所發現的相關問題。

(五) 和 Google 合作進行充分 IPv6 網路運行實驗及除錯：

Google 針對 IPv6 的支援相當的積極，因此 Verizon 在 IPv6 網路運行實驗及除錯的過程中和 Google 進行密切的合作，Verizon 將公司的創新中心實驗室和 Google DNS 解析器相連結，讓 Google 所提供的 IPv4/IPv6 雙軌網路服務可以在 Verizon 的實驗室運行，幫助 Verizon 在服務上線前可以修復更多終端設備的問題，確保服務上線能更順利。

(六) 在 IPv6 試營轉期間成立專門服務中心解決相關問題：

在世界 IPv6 啟動日前持續和主要具有雙軌服務的內容網站業者合作，提供關於 IPv6 的統計數據 並建立網路追踪機制以修正 IPv6 所引發的問題。並成立專責電話服務中心，負責回答及解決使用者的問題，並收集相關技術漏洞，回報技術單位以進行修補。

(七) 在西元 2012 年（101 年）6 月世界 IPv6 啟動日（World IPv6 Launch）讓 LTE 支援 IPv6 網路商轉：

Verizon 是否參與世界 IPv6 啟動日開啟 LTE 支援 IPv6 網路商轉的考量點，在於是否能在世界 IPv6 啟動日前將先期測試 IPv6 網路問題障礙排除，Verizon 技術團隊順利在期限前完成任務，讓 IPv6 網路如期上線進行商業運轉。

(八) 成立 War Room 以支援世界 IPv6 啟動日可能產生網路運作問題：

為了讓 IPv6 網路正式商用能順利，Verizon 成立 War Room 以支援世界 IPv6 啟動日可能產生網路運作問題，在正式商用前所投入一整年的努力，正式商用啟動後數週雖然還有發現部分問題，但都可以很快修正完成，整體的啟用過程相當順利。從 6 月正式上線時 IPv6 使用率為 7.36%經過二個月時間到 8 月時使用率上升到 10.64%，根據 Akamai 統計當時全球的 IPv6 使用率有 38%是由 Verizon 所貢獻。

二. 固網業者 Comcast：

Comcast 作為美國最大的有線電視公司、及最大的網際網路服務供應商，其業務包含有線電視、寬頻網路接取服務、IP 電話服務、行動網路、及其他加值服務等多元性的商業營運；每天幾乎提供包含超過 140 億次的網頁瀏覽量，1.67 億次的電話使用量、及 1500 萬次的隨選（On Demand）視訊服務需求。

且 Comast 也是 CableLabs consortium [32]的主要成員之一，這個組織正是有線電視產業標準的制定者，其中多項標準，與 IP 的發展息息相關，像是纜線數據服務介面規格（Data Over Cable Service Interface Specification，DOCSIS）等。Comcast 不僅經營橫跨有線電視、網際網路服務、內容製作及媒體等多項事業版圖，在 DOCSIS 及 Internet Engineering Task Force（IETF）相關標準的制定上，也有相當多的貢獻。[36]

美國政府在西元 2005 年相繼由國防部與商業部發布的兩份 IPv6 政策文件，訂定導入 IPv6 規格。由於軍事採購與政府採購的利基點，廠商為避免被排除於政府購案之外，就必須實現相關的規格需求，並驗證其產品符合國防資訊系統局（Defense Information Systems Agency）所制定的 IPv6 特別相容認證 (IPv6 Special Interoperability Certification)，因此推動網路設備供應商開始積極發展支援 IPv6 的系統，或改寫舊有的系統以提供 IPv6 支援；Comcast 身為網際網路規格的制定者，在設備逐漸成熟，加上自身的需求與商業競爭上的考量，配合政府政策的鼓勵，也開始對建構 IPv6 網路投入心力。以商業考量方面分析，其推動導入 IPv6 原因如下：

(一) 提供足夠的位址空間：

由西元 2006 年(95 年)Comcast 技術長辦公室協理 Alain Durand 在 NANOG（North American Network Operation's Group）37 會議演說中談到，Comcast 單就現有的數位機上盒客戶數就有 2 千萬，每個客戶平均有 2.5 個機上盒，每個機上盒需要使用 2 個 IP，光要提供此業務所需的 IP 數量就達到 1 億個，如果全部換算成實體的 IPv4 位址，就需要 6 個 Class A 的區段，佔掉全球 IPv4 實體位址的 2.7%。況且 Comcast 當時還有網路電話及寬頻網路服務，未來還有其他新服務上線的需求，或透過收購、企業合併等方式拓展 Comcast 的業務範圍所產生的 IP 需求。

除了客戶需要使用 IP，公司內部要管理如此龐大的客戶設備及提供網路服務，也需要相當多的 IP，供應網路系統設備使用。

由以上數字就可了解到 Comcast 所經營的業務對 IP 需求相當高，且 IPv4 地址短缺加劇，及 IPv6 商用腳步加速的背景下，加強 Comcast 導入 IPv6 的動機。[32][34]

(二) IPv6 是解決 IPv4 位址不足的較佳選擇：

在導入 IPv6 之前，Comcast 曾試圖使用多種方式，來充分管理其所持有的 IPv4 位址，以延長 IPv4 的使用壽命。一開始，Comcast 使用位址生命週期管理的規劃方式，在大部分的終端設備(包含纜線數據機、數位機上盒、網路電話設備等)，使用動態分配的 IPv4 位址；而網路連接設備則採用固定 IP 的方式配置。實施幾年後由於業務量快速的成長，不得不改採混和的位址型態，將網路連接設備改用私有網路 IP 連接，以便能挪出更多的實體 IP 供客戶端使用。然而，這種方式在西元 2005 年 7 月以後，也達到了極限，

單就設備端需要的 IP 數量，已經超出了 RFC 1918 所定義的所有私有網路 IP 位址空間。因此，Comcast 不得不再將實體 IP 也用在設備管理上，而由於網路的使用者快速激增，也使得 Comcast 必須經常重新向 ARIN（American Registry for Internet Numbers）提出新的 IPv4 位址申請。

對 Comcast 而言 IPv4 位址不足的問題，對網路管理營運所需造成極大的衝擊，也限制公司的成長，而 IPv6 可以解決 IPv4 不足的問題。[33]

(三) 使各區域網路能相互連結且集中管理讓營運更有效率：

Comcast 自西元 2003 年開始進行導入 IPv6 可行性評估，當時其網路分成 21 個收斂區域網路(Converged Regional Area Networks，CRAN），包含網路通訊與管理所需的設備及程式等，所需的 IP 數量相當多。以往每個 CRAN 是獨立的網路環境，各自獨立管理。設備之間的通訊，藉由 RFC 1918 所定義的私有網路位置，進行設備的網路管理。隨著營運項目的日益複雜與業務的快速成長，Comcast 面臨到要將全國既有網路、及新建構起的高速網路等，整合到一個中央管控中心的問題。在這個環境上，由於管控中心必須能直接連線到各個 CRAN 下的設備，如要將所有設備都透過 RFC 1918 定義的私有網路位址做控管，首先將面對的問題是 Comcast 並沒有足夠的 IP 分配給所有的設備；若將網路切割，因為必須建立起路由，讓管理系統得以連接，私有網路位址也無從用起。

此外 IPv4 和 IPv6 的不同點，除了 IPv6 提供更多的位址空間之外，IPv6 更有多項的改進功能，其中提升路由的效率，以維持良好的網路連結效率，對網路服務供應商而言是相當重要的因素。[34]

(四) 網路設備相互連結降低營運成本：

讓原本分散區域網路設備互相連結集中管理，可以增加設備的使用性及提高使用率，可以減少設備所需的投資，對大型網路服務商 Comcast 而言，具有實質的意義。[34]

(五) 提供創新服務的發展空間：

根據 Comcast 在西元 2006 年（95 年）的預測，因應新型態的業務發展，未來幾年對 IP 數量的需求，至少還會呈現倍數以上的成長，對 Comcast 創新服務的發展空間，足夠的 IP 資源是基本需要被滿足的要求。

同時 IPv6 也能為網路服務供應商在新服務的佈建及創新上，提供新的潛在市場與加值應用的利基。例如 IPv6 所提供的無狀態位址自動設定（StateLess Address AutoConfiguration），可自動為裝置配置 IP，達到物聯網裝置隨插即用（Plug&Play）的需求，IPv6 不但能幫網路服務供應商解決即將面對的 IP 位址不足的問題，更可以為網路服務供應商擴展新的潛力市場。[34]

(六) 爭取足夠的建置時間：

IPv4 在西元 2005 已經耗盡，但新的應用及用戶需求不斷的增加，經過幾個階段調整網路架構，仍然無法解決 IP 不足的問題，而 IPv6 的部署並非可以短時間快速完成，及早準備才能爭取充足

的時間規劃及建置，可以更完整的測試和驗證 IPv6 網路佈建狀況，提供用戶無縫轉換，讓遷移的過程更為平順且不影響既有的網路服務。[34]

(七) 保持市場的競爭力：

隨著客戶量的成長，IPv6 不但可以解決 IP 位址不足的問題，也能幫網路服務供應商解決即將面對為新營業項目及擴展市場版圖所產生的 IP 需求，隨著提供 IPv6 服務的業者愈來愈多，為了保持市場的競爭力，導入 IPv6 建置對於網路服務供應商來說只是早晚的事，愈早規劃與導入，當 IPv6 網路被廣泛使用時，能順利銜接新一世代網際網路，而不至於被市場淘汰。[34]

Contingency Plans: Buying Time to Deploy IPv6

or how to Get 100 Million IPv4 Addresses (and more)?

Plan	Description	Impact (to us…)
Public Address Space	Go to ARIN and ask for address space every time we can justify it in accordance to policies.	Minimal.
"Dark" Space	Use already allocated, non-globally routed, public IPv4 address space.	Operationally minimal unless a conflict arises.
Federalization	Subdivide the network into several independently managed domains (e.g. division boundaries).	Loss of global visibility in the network. Need to redesign the network & provisioning systems.

8 *Comcast – Nanog37: Managing 100+ million IP addresses*

圖 63、Comcast 在 NANOG 37 會議分享對 IPv6 網路建置經驗

以技術面評估採用 IPv6 對 Comcast 的整體性發展，有實質上的幫助，有關其推動 IPv6 在技術方面的原因可歸納如下:

(一) 提供足夠的位址空間：

Comcast 身為全美最大的複合式系統商，也是最大的寬頻網路服務供應商，除寬頻網路服務外，亦提供多項加值服務，這也造成 IP 地址需求加劇，而顯示出 IPv4 短缺的嚴重問題，需要對應的解決方法，才能維持正常的營運及擴大加值服務。[34]

(二) 保持 Comcast 技術領先地位：

作為大型網路服務供應商，本身在標準制定上又佔有一席之地，可見 Comcast 對技術領導者地位的重視，因此對採用新技術上保持開放的心態，並且不斷求進步，以提升既有的服務，來滿足廣大客戶的不同需求。[34]

(三) NAT 無法解決 IPv6 位址不足的問題：

在採用 IPv6 之前，Comcast 也試圖延長 IPv4 使用的可能性，將網路連接設備改用私有網路 IP 連接，以便能挪出更多的實體 IP 供客戶端使用。但網際網路的蓬勃發展所帶出的需求，遠遠超出其所能提供的極限，終究是需要有更長期的解決方法。

在 Comcast 的網路架構中，所有的設備需要能由遠端管理，要能達到此目的就需有足夠的 IP 供設備使用，NAT 無法滿足 Comcast 的設備管理上的需求。[34]

(四) 增加網路管理的彈性：

更充足的位址空間，可以讓服務商在管理層面上，有更充裕的

規劃空間，不再受限於全球沒有足夠的IPv4位址影響，或必須使用RFC 1918定義的私有網路位址，來管理內部的相關設備。成功導入IPv6後，也強化了公司的網路架構、維運政策、以及未來發展方向的信心。[34]

(五) 減少網路管理者的負擔：

因網路使用者不斷增加，及新服務上對 IP 需求不斷擴張所引發的 IP 缺口持續增加，因此技術人員需因應需求而調整網路架構，增加網路管理者的負擔。且持續使用 IPv4 並無法找到適當的長期可行解決方法，而 IPv6 可以提供網路服務商更好的解決方案。[34]

(六) 使網路營運更有效率：

IPv4實體位址與私有網路位址，皆不足以因應現今需要管理巨大網路架構的營運商需求。IPv6可以提供大量的IP，提供網路營運商更彈性也更有效率的集中管理網路設備。[34]

(七) 增加提供新加值應用服務的彈性：

新的網路服務及應用不斷被創造出來，IP 的新需求也不斷被提出，IPv6 可解決 IP 短缺的問題，提供更彈性及更有發展潛力的網路架構，讓網路服務供應商有更大空間發展新服務及應用 。[34]

下圖將 Comcast 推動 IPv6 的原因，依人力成本、資本投資、公司的競爭力及使用者經驗等四大面向分析，以了解推動 IPv6 對 Comcast 營運的影響。

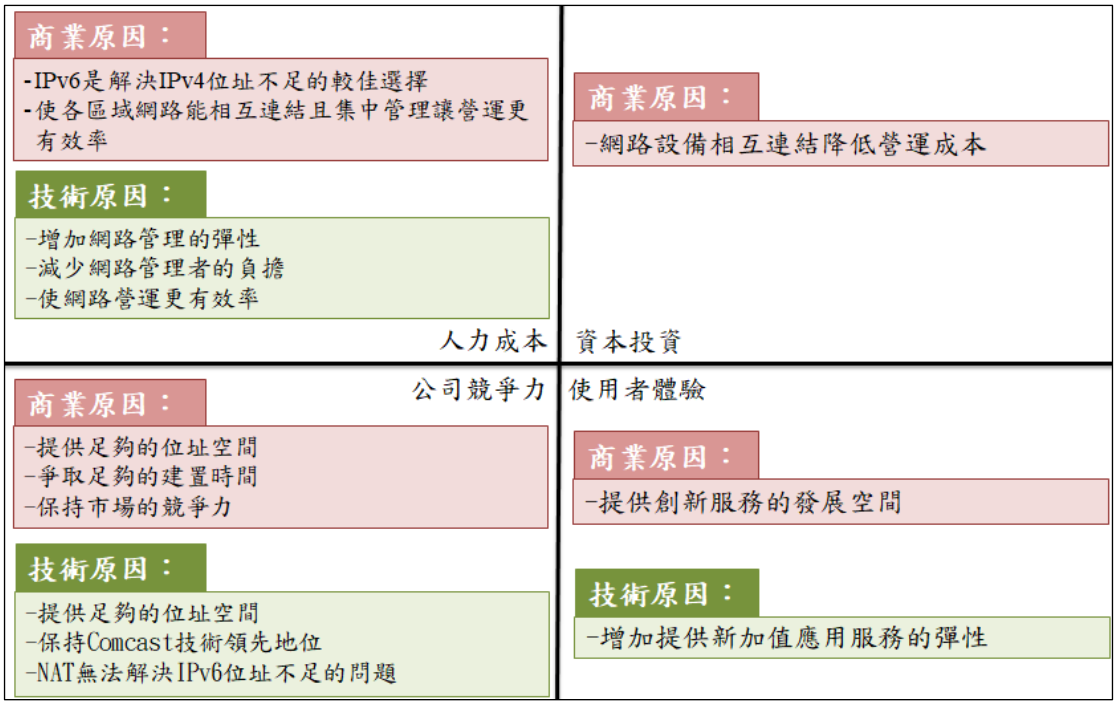

圖 64、Comcast 推動 IPv6 的原因

Comcast 的技術團隊，在 IPv4 資源吃緊的早期階段，即進行支援 IPv6 的評估，於西元 2005 年私有網路 IP 位址於內部網路耗盡後，更加快導入 IPv6 的腳步。關於 Comcast 推動 IPv6 的經驗，該公司推動 IPv6 的演進過程如下：

(一) 基礎核心網路建置：

此階段於西元 2003-2006 年（92-95 年）間進行，主要致力於推動 DOCSIS 3.0 標準的制定，並促使該標準中含蓋 IPv6 協定；與網路設備供應商密切合作，透過清查網路架構，將 IPv6 整合到所有的網路設備中，以確保 IPv6 在基礎網路建設準備就緒；Comcast 於西元 2003 年（92 年）1 月自 ARIN 取得 2001:558::/32 IPv6 網段獲取 IPv6 位址後，開始測試 IPv6 在核心網路佈建，安全性問題評估，並完成 IPv6 核心網路的建置。

(二) 管理系統及設備整合測試

西元 2007-2008 年（96-97 年）間，Comcast 開始與後台系統開發商合作，將 IPv6 整合到網路管理系統中，與網路設備商合作，將 IPv6 整合到纜線設備及數位機上盒中，執行互相連結測試，以評估邊緣網路的設計是否恰當，啟動網路上的 IPv6 連線服務，並開始使用 IPv6 來管理網路相關設備。

(三) 推動內容服務支援 IPv6

當網路設備做好準備，進入第三階段於西元 2009 年（98 年）開始，結合內容供應商提供新服務支援 IPv6 連網服務，初期合作夥伴包括網頁主機服務商 The Planet、線上電影出租服務商 Netflix、與視訊串流服務商 Limelight 等。

Comcast 在西元 2010 年（99 年）開始規劃推動 IPv6 商用計劃，並於當年度第二季開始開放用戶申請試用 IPv6 連網服務，主要分四種支援 IPv6 網路類型架構進行試驗，此四種類型分別為：

(一) 採用〝6RD〞技術：

6RD 是 IPv6 快速部署（IPv6 Rapid Deployment）的簡稱，其對應標準為 RFC5569，6RD 是在 6to4 基礎上發展起來的一種 IPv6 網路過渡技術。通過現有 IPv4 網路中增加 6RD-BR，對使用 IPv6 的用戶提供 IPv6 接入；在 IPv6 用戶的家庭閘道器和 6RD 閘道器之間建立 6in4 隧道，以實現在 IPv4 網路提供 IPv6 服務的能力。6RD 因為容易實施，擴展性強而且可靠。6RD 是 6to4 自動隧道的擴展技術，部署更加靈活。讓網路服務商透過已經部署完畢的 IPv4 網路提供 IPv6 服務，也是通過最常用的把 IPv6 封裝在 IPv4 中實

現。6RD 和 6to4 自動隧道的區別是 6RD 不需要特定的使用 2002::/16，而可以使用網路服務商自己的地址區塊，增加了實施的便利性。[33]

(二) 評估本機 IPv4/IPv6 雙軌網路服務：

IPv4/IPv6 雙協定技術，是每一台能連網的設備上都具備 IPv4 與 IPv6 的處理能力，通常這類設備能同時搭載 IPv4 與 IPv6 的 IP 位址。譬如微軟 Windows 7 作業系統的網路就有雙協定，它內建 IPv4 與 IPv6 位址，只要 ISP 業者有提供 IPv6 服務，使用者就能夠連線至 IPv6 網站。

雙協定技術的優點為設置簡單，並同時提供 IPv4 與 IPv6 的功能。使用者透過雙協定技術，可以連線至雙協定堆疊主機、純 IPv4 主機與純 IPv6 主機。缺點為，用戶端到伺服器端中間的節點，都必須支援雙協定。否則連線至 IPv6 網站時，假設傳輸過程經過的節點為純 IPv4，就不能連線。也因為這樣，導致每個節點都必須同時消耗 1 個 IPv4 及 IPv6 位址，並增加系統複雜度及管理上困難。[35]

(三) 採用〝精簡雙軌〞技術（又名為 DS-Lite）：

DS-Lite 是具備 IPv6 為主的傳遞網路與 IPv6 用戶管理。在 CPE 設備與 CGNAT 之間建立 4-in-6 Tunnel，換言之，就是在 CGNAT 上面 完成 IPv4 與 IPv6 的轉換，採用此方案的客戶，將不需要面臨『第二次』升級的困擾，由於 DS-Lite 內部已經是完全的 IPv6 架構，故首次投資成本較為高昂，一次性的汰換將面臨內部 CPE

是否支援 DS-Lite 的問題，以及核心端設備是否支援超大量 LSN 的能力。

(四) 為用戶提供真正商用的 IPv4/IPv6 雙軌網路服務：

經過不同階段的網路類型架構試驗，最終還是以提供用戶真正商用的 IPv4/IPv6 雙軌網路服務為目標。

為了完成真正 IPv6 商用部署，Comcast 採取分型態及分階段試驗方式逐步推行，逐漸達成 IPv6 商用目標。在部署 IPv6 的過程，Comcast 並對內部執行團隊訂定以下原則，作為遷移到下一代網際網路建置準則：

(一) 部署 IPv6 不能影響現有 IPv4 設備和對網路服務的營運造成影響：

IPv6 的佈建是一項長期工程，技術人員先規劃好架構，由核心到邊緣的網路設備，逐步升級支援 IPv6，以不影響原有 IPv4 網路營運為原則，進行網路服務升級的建置計畫。

(二) 下一代網路設備及終端採購，必須包含 IPv6 的規格需求：

Comcast 早期在佈建 IPv6 時，當時網路設備跟使用者終端對 IPv6 的支援尚未成熟，為保障所採購設備能真正支援 IPv6，因此採購的要求比 IPv4 商品要求更為嚴格，必須要能通過 IPv6 的認證產品，才能列在採購清單。

(三) Comcast 的營運、基礎設施和系統必須準備好支援 IPv6 的終端設備：

透過 IPv6 逐步升級計畫，在支援 IPv6 的終端設備準備好時，Comcast 也已經準備好為使用者提供 IPv6 服務。

(四) IPv6 將慢慢滲透到成為公司的 DNA：

Comcast 預期在公司早期導入 IPv6 的過程當中，技術人員對於 IPv6 並不熟悉，因此必須克服對工程技術陌生而產生的恐懼及排斥現象，才能讓 IPv6 的佈建計畫有穩定的進展，因此公司提倡持續的對技術人員進行教育訓練，透過教育訓練、網站課程及實際操作，讓 IPv6 技術深化到成為公司的 DNA。

Comcast 於 2010 年（99 年）初即開始展開 IPv6 的商用計畫，其互聯網系統執行董事 Jason Livingood 認為，〝我們在 2010 年(99 年）展開商用計畫,將有助於全面發現和解決各領域內 IPv6 過渡的困難，提前確定有效的解決方案，作為向客戶提供 IPv6 服務的無縫體驗做好充分準備。Comcast 將持續與業界分享所得經驗，特別是與 IETF 的合作，為網際網路用戶創造利益〞。西元 2015 年（104 年）Comcast 成為美國第一個採用 IPv4/IPv6 雙軌並行（Dual-stack）的主要有線電視業者及寬頻服務商[7~9]。

第二節　調研國際 ICP 業者導入 IPv6 原因及推動經驗

一. Google：

從西元 2008 年(97 年)起，Google 就致力於推動「Google over IPv6」網路升級計畫，除已推出對外服務「Google Search」的 IPv6 版本之外，並在內部推動各項 IPv6 內網示範計畫。Google 表示，透過這些示範計畫讓內部工程師預先測試對外服務的升級情況，升級過程先從單一主機環境的測試著手，採用雙協定（Dual Stack）轉換技術，來建立 IPv4 和 IPv6 都可共通的網路環境。接著再以 GRE 通道連接可同步支援 IPv4 和 IPv6 的實體主機，不管是 IPv4 或 IPv6 的網路封包都可經由通道完成傳送與接收的動作。待單一主機網路環境測試完成後，Google 再進一步將雙協定轉換技術擴充至 Google 實驗室、分公司等更為複雜的網路架構中。到西元 2011 年(100 年)底為止，Google 內部網路環境已有 5 成設備升級到 IPv6，且朝完整 IPv6 網路環境持續努力。Google 從西元 2008 年（97 年）內網展開升級計畫後，所面臨的最大困難是支援 IPv6 協定的相關產品不足，還有待市場機制成熟，企業升級 IPv6 網路環境才能更為順利。[15]

為了能集結網際網路業者的力量，持續往支援下一代網際網路協定標準 IPv6 推進，Google 從西元 2008 年（97 年）開始，連續數年舉辦 IPv6 開發者大會，廣邀網路產業的業者包含 ISP、網路系統商、及 ICP 等參與，邀請業界做 IPv6 的佈建經驗、及新技術的分享，經由業界的相互交流及合作，以加快向新一代網際網路協定標準遷移的速度。Goolge 也在會中就本身佈建 IPv6 的經驗及原因做分享。[16]

Google 身為全球第一大網路搜尋引擎業者，對於提供全球廣大使用者優良的連網服務及品質，一直是 Google 相當重視的技術能力，對於 Google 而言導入 IPv6 的理由非常簡單，以商業面而言，其導入支援 IPv6 的原因如下：[17~21]

(一) 保持 Google 在網際網路的世界屹立不搖：

早在西元 2011 年（100 年）Google 就觀察到越來越多的終端設備支援 IPv6，如美國電信商也是最大有線電視業者 Comcast 的機上盒（Set-top Boxes）、法國電信業者 free.fr 的機上盒、及 NTT 的網路電視及網路電話（Voice over Internet Protocol, VoIP）都支援 IPv6 連結等，顯示 IPv6 越來越被市場所接納，當網際網路進入 IPv6 連網的世代，使用者以 IPv6 連網，Google 要在網路的世界屹立不搖，對 Google 而言提供使用者 IPv6 連網服務是最基本的要求。

身為大型全球網際網路服務的提供者，不斷優化網路服務才能持續維持領先的地位，當 IPv4 位址資源耗盡，在下一世代技術轉折點上，Google 採取的是以積極的態度來面對市場的需求，以確保其在全球網際網路服務上擁有一席之地。[17~21]

(二) 全球 IPv4 地址耗盡，IPv6 是合理可行的解決方案：

網際網路號碼分配局（Internet Assigned Number Authority，IANA）在西元 2011 年（100 年）2 月將最後的 IPv4 網段，分配給 5 大區域網際網路註冊管理機構（Regional Internet Registry, RIP）後，正式宣告 IPv4 地址資源已經耗盡，在此同時全球行動通訊及物聯網的發展也進入擴展高峰期，為了支援下一代網際網路的發展，尋找可行的替代方案，已經是無可避免的事情。Google 認為 IPv6 是合理可行的解決方案，也支持 IPv6 的發展。[17~21]

(三) 面臨 IPv4 位址不足的狀況：

美國雖然擁有大量的 IPv4 位址資源，但相對也是網路科技的重鎮，大型跨國企業的大本營，網路位址資源消耗量大，且 Google 本身不斷擴展其企業版圖增加不同的營運項目，早在西元 2011 年（100 年）Google 就已經面臨 IPv4 位址不足的情況。[17~21]

(四) 導入 IPv6 可節省投資成本：

IPv4 位址已經成為網際網路服務的珍貴資源，資源越來越稀少即反映到價格相對會提高，也代表網際網路服務經營者若要取得更多的 IPv4 地址，將需要付出越來越高昂的代價。這對 Google 除發展網際網路技術相關應用外，持續發展多角化經營如手機作業系統及平台、自動車、車聯網、穿戴式裝置、及物聯網等相關技術，導入 IPv6 服務對 Google 持續開發新技術以擴展其事業版圖有其重要的意義。[17~21]

(五) 為所有的客戶提供優質的服務是 Google 的商業營運模式：

無論終端使用者或企業用戶，對於 Google 所提供的所有服務，從網路搜尋引擎（Search Engine）、智慧手機（Smart Phones）、網路電視（Internet Protocol TV, IPTV）、雲端計算（Cloud Computing）、點對點（Peer to peer, P2P）應用程式、及其他的服務等，所有 Google 提供的服務都需要支援 IPv6，以維持高品質的網路服務。[17~21]

(六) 確保網際網路可以持續成長及保持開化性：

網際網路經過 30 年，原本所設計的網路架構，因行動通訊的加入，讓網際網路發展的規模，早已超越當初所能想像的範圍；隨

著物聯網（Internet of Thing）、人工智慧（Artifical Intelligence, AI）等創新技術的加入，網路的世界又進入另一個快速發展的世代。為確保網際網路可以持續成長及保持開化性，移轉到下一世代的網際網路協定（Internet Protocol）已經是不可擋的浪潮。IPv6 除了解決位址不足的問題，也改善許多 IPv4 的缺點如擁有可擴充性的網路通訊協定、整合認證及安全機制、減輕路由器（Router）負擔以提高路由效率、支援隨插即用（Plug and Play, PnP）、及強化支援移動性等的特性，都更適合於新一代的網際網路發展。[17~21]

(七) NAT 無法支援網際網路持續擴張及發展：

重疊性網路位址轉譯(Network Address Translation, NAT)需增加記憶體、網路頻寬等設備投資成本，而 NAT 設計增加網路架構的複雜性，同時讓網路的運作效率降低，因此而增加了營運維護的人力成本，並且產生的網路運作安全的疑慮。時間及人力成本的增加，卻換得效率不佳的網際網路系統，對所有的網路營運業者都不是一項聰明的選擇。[17~21]

(八) 支援 IPv6 連網服務已經不是假設性的議題，而是何時該導入支援 IPv6 連網服務：

IPv4 位址資源不足、NAT 無法持續支撐網際網路的蓬勃發展，且增加投資成本卻無法帶來足以支撐的效益、影響網路服務品質、及限制應用發展的可能性等，多項因素造成下一代網際網路遷移的必要性，而 IPv6 獲得市場的支持及共識，因此我們該思考的是支援 IPv6 連網服務已經不是假設性的議題，而是何時該導入支援 IPv6 連網服務。[17~21]

(九) 維持網際網路的開放性就是 IPv6 的殺手級應用：

最初網際網路的創建以維持平等、及開放的精神而誕生，當 IPv4 的發展到達極限，該如何讓網路能持續發展，且維持原本的精神及有效率的運作?很多人一直在問，甚麼是 IPv6 的殺手級應用?而 Google 認為能繼續支持網際網路未來的蓬勃發展，且維持網路平等、及開放的精神，就是 IPv6 的殺手級應用， 下一代網際網路協定的標準 IPv6 就是答案。[17~21]

(十) Google 公司創新文化使然，為未來發展提早做好準備：

Google 公司本身的企業文化強力支持創新，並為未來發展提前做好準備，早一步布局未來市場，一直是 Google 迎接全球市場激烈競爭，維持不墜的力量。[17~21]

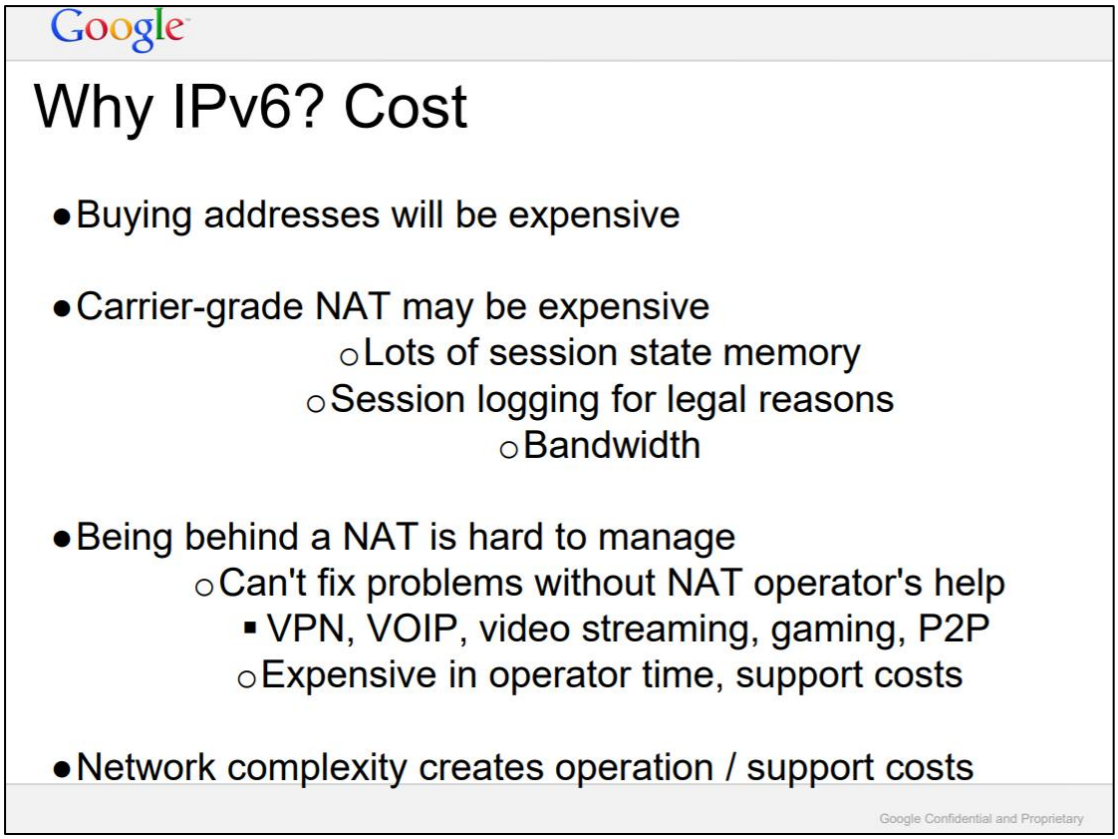

圖 65、Google 分享對 IPv6 網路建置想法

除考量商業因素之外，以技術面而言，Google 導入支援 IPv6 的原因如下：

(一) 採用 NAT 技術只是暫時緩解 IPv4 地址短缺的問題，並非正確的解決方案：

NAT 技術雖然可以暫時緩解 IPv4 地址短缺的問題，但卻讓網路架構變的相對複雜化，因此也對新應用的開發形成無形的障礙，同時 NAT 的使用也違背網際網路開放的原則，無法達到點對點的連結。就應用程式開發商、網際網路服務者、及使用者的角度而言，採用 NAT 技術不會是解決 IPv4 位址短缺的最終解決方案。而採用 IPv6 的網路架構可以支撐網際網路持續的成長，並給新的應用程式更寬廣的開發空間。[17~21]

(二) 先期導入支援 IPv6 網路服務，對於未來所能提供給使用者的網路服務品質非常關鍵：

技術先期導入，技術人員可以有較長的時間開發、測試、及修正，並能透過先期試用，經由使用者的回饋，以尋求更佳的解決方案。[17~21]

(三) 導入支援 IPv6 並非需要高深的技術，但需要時間來完成建置計畫：

網際網路通訊協定的轉移很難一步到位，因此需要開發人員分階段進行規畫、執行、測試、及調整，且不能影響現有網際網路的運作，需要足夠的人力及時間才有辦法順利完成技術的轉移。[17~21]

(四) 提供使用者更好的網路服務、及較佳的使用者經驗：

採用 IPv6 可以提供給使用者更好的網路服務品質，這是 Google 一直以來不斷努力的方向。根據使用者回報的使用經驗，IPv6 具有更低的延遲性、及較少有資料封包（Data Packet）遺失的狀況產生。因此資料的傳輸更快更好。IPv6 提供新的定址方式，且擁有可擴充新的通訊協定、減輕路由器(Router)負擔、即插即用、強化移動性及安全性等好處。[17~21]

(五) 減少應用程式開發及維護的人力資源浪費：

因為過度使用網路位址轉譯（Network Address Translation，NAT）常造成 AJAX 應用程序中斷的狀況，起因在於過多的連結造成公用 IP 接口空間被消耗殆盡。有些應用程式如 Google Talk 因為使用 NAT 穿越（NAT Traversal）技術，而變得非常複雜，因此浪費過多的技術開發人力資源。[17~21]

(六) 增加使用者地理位置資訊識別的準確度：

由網路營運商採用 NAT 分配 IPv4 地址給用戶，產生多個用戶共享同一個 IPv4 地址的情形，部分的網路應用將受到影響，例如無法取得使用者精確的地理位置資訊，若有犯罪釐清需求時容易產生問題、或救援需求時無法及時得知使用者位置，同時也影響以使用者地理位置資訊為依據的相關應用，如廣告發送、地震及海嘯警報等服務的運作。而採用 IPv6 能有足夠的 IP 位址，分配給終端使用者，避免需要用戶共享 IP 位址的情形發生，降低使用者地理位置資訊識別的難度。[17~21]

(七) 降低垃圾信件或是駭客攻擊來源查證難度：

當多個用戶共享同一個 IPv4 地址，如果此 IPv4 位址是發送垃圾信件或是駭客攻擊的來源，哪一個使用者才是真正的元兇，將增加查證的難度。如果採用 IPv6 位址分配，即可避免此種情形發生。[17~21]

(八) 採用 NAT 機制將無法採用以 IP-based 做授權：

NAT 機制將形成多個用戶共享同一個 IPv4 地址的情形，因此無法以 IP-based 做為單一識別的認證機制。[17~21]

(九) 開發新應用需要大量的新 IP 位址：

Google 內部不斷開發新的應用程式產出新的網路服務，而新的服務往往需要大量新的 IP 地址，IPv4 位址短缺，形成 Google 的創新發展的一大障礙。[17~21]

(十) 開發 IPv6-ready 相關創新產品：

西元 2011 年（100 年）當時 Google 即已面臨 IPv4 地址不足的情況，因此 Google 內部也決議新服務、及新產品的構想，可以以 IPv6-ready 的方向發展，迎接未來網路的趨勢，這也展示 Google 擁抱 IPv6 向下一代網際網路通訊協定遷移的決定。[17~21]

下圖將 Google 推動 IPv6 的原因，依人力成本、資本投資、公司的競爭力及使用者經驗等四大面向分析，以了解推動 IPv6 對 Google 營運的影響。

圖 66、Google 推動 IPv6 的原因

Google 從一開始推展 IPv6 時就理解到，要讓所有的網路設備及服務一次到位支援 IPv6 是不可能、且不可行的計畫，因此採取分階段推行的方式，逐步由實驗室測試，分區域或國家測試，到真正商用化逐漸一步步進行，下表所列為 Google 在推動 IPv6 的歷程紀錄中，重要的里程碑。[22]

表 64、Google 推動 IPv6 的歷程紀錄

序號	時程	事件
1	2005/3/14	向美國網際網路號碼註冊中心(American Registry for Internet Numbers, ARIN）申請 IPv6 位址 — 2001:4860::/32
2	2007/8	開始進行網路架構更新及軟體開發工程，先期以更新20%的服務專案如Gmail、Google新聞等為目

序號	時程	事件
		標。
3	2007/12/5	Mark Townsley公開建議Google在IETF 73的會議上提供AAAAs IPv6位址服務（Google為IETF 73的贊助商）。
4	2008/1/11	公開第一個商用 IPv6 路由。
5	2008/1/29	首次公開展示Google的服務可以透過IPv6連結。
6	2008/3/12	Google在IETF 71公開展示搜尋服務在 ipv6.google.com 上線。
7	2008/7	公開中國測試Google IPv6搜尋網站ipv6.google.cn
8	2008/10	公開日本測試Google IPv6搜尋網站 ipv6.google.co.jp
9	2008/10 ~ 2008/11	Google 首次在 RIPE 及 IETF 開放外部測試人員試用以 IPv6 連結 Google 搜尋服務。
10	2008/11/16	Google在IETF 73會議上為Google的服務提供AAAAs。
11	2009/1/7	正式讓 Google 搜尋服務上線支援 IPv6 連結。
12	2009/3	Google 的 IPv6 的流量增加為 3 倍。
13	2009/8	Android 平台支援 IPv6 的網路連結程式碼。
14	2010/2	Youtube 支援 IPv6 連網，IPv6 的流量增加為 10 倍以上。
15	2010/3	Google 網路骨幹(Backbone)全面支援 IPv4/IPv6 雙軌服務。

Google 採取的策略是先以實驗室測試環境開始，先期開發 IPv6 網路測試環境，透過內部討論驗證並改善 IPv6 實驗網路架構，當實驗網路環境發展到可行階段，即開始應用服務的網路升級開發計畫，因為 Google 的應用服務項目眾多，進行第一階段服務支援 IPv6 的應用程式計畫，只選出約20%的服務如Gmail、Google新聞等為執行目標，經過內部實驗測試結果能順利運行，再執行其他應用服務的升級計畫，逐步推進。[19]

當小型支援 IPv6 的網路架構及應用程式在實驗室環境下，能運行無礙且達成預期的效果，再將試驗連結網站開放給經過驗證的使用者，

做擴大規模的實驗，剛開始的實驗結果並不理想，部分使用狀況會產生網頁應用破碎、及較高的延遲時間等問題，幾經修正才讓 IPv6 網路連結效率和 IPv4 一樣或較佳表現，才會進到下一階段做擴大試驗網路架構規模，並依以下 3 個方向執行：

(一) 透過試用方式及監控管理網路運作狀況，以做為修正網路架構的依據。

(二) 將升級執行紀錄完整文件化做為改善或其他服務的參考資料。

(三) 跨部門的支援以改善 IPv6 網路架構。

終極目標以朝向 IPv6 網路商用化前進。對 Google 而言進行實驗性質的網路並不需要付出高昂的代價，且小型的試點網路可以降低計畫參與者執行的門檻，增加開發人員的成就感，也可激起參與者的熱情，確保專案執行的成功率。更重要的是網路經營者在計畫支援 IPv6 上，必須要消除 IPv6 是〝實驗性〞的概念，且堅定往支援 IPv6 商用化的方向前進，以設計出和 IPv4 具有相同或更好的連網品質為目標。從西元 2005 年（94 年）Google 向 ARIN 申請 IPv6 位址，到西元 2008 年歷經 3 年時間，才讓 Google 搜尋網站支援 IPv6 的實驗連結〝ipv6.google.com〞在 IETF 71 釋出，供與會者測試，再歷經將近 1 年的時間，於西元 2009 年（98 年）1 月正式讓 Google 搜尋網站〝www.google.com〞支援 IPv6。

在往 IPv6 網際網路遷移的過程，不可能一夕之間就擁有和 IPv4 網路一樣的能力，是 Google 一開始就有的體認，因此 Google 採取的策略是緩慢且穩定的方式推展、及保持謹慎的態度經營網路的營運，在轉換的過程中一步步反覆的驗證，且不間斷的監控整體應用服務的運作狀況，並及時修正直到在 IPv6 的網路環境下能運作無礙。

二. Facebook：

網路的發展速度遠超出當年剛開始所能預測的情況，早在西元 1990 年（79 年）IP 資源不足的問題就已經浮上檯面，因此有 IPv6 的發展，但發展到西元 2006 年（95 年）前，都還沒有正式的商用 IPv6 網路實際運行，但隨時間演進，IPv4 不足的問題已經越來越難被忽略。

Facebook 為全球第一大社群網站，擁有各國眾多的使用者，如何提供全球更多的用戶可以連上 Facebook 網站，需考慮到不同國家使用者的網路基礎建設及連網設備狀況，尤其在社群網路發展的年代也是行動上網急速成長的時代，對於 Facebook 導入 IPv6 有其必要性，依商業面向來看，其導入 IPv6 的理由說明如下：[37~46]

(一) 解決 IPv4 不足的問題：

Facebook 在西元 2003 年（92 年）由創辦人從哈佛大學校園內開始發展，於西元 2005 年（94 年）對外開放並逐漸發展成為全球第一大社群網站，在 Facebook 蓬勃發展的年代，IPv4 資源不足已經是網站經營者需面對的問題。公司認為解決 IPv4 不足的問題是遲早的事，盡早解決對公司發展更有利。[42]

(二) 讓更多使用者可以連接上 Facebook 網站：

對於社群網站經營業者而言，更多的使用者上線，代表能為公司帶來更大的商機，Facebook 需考慮到使用者的網路環境，行動通訊的發達帶進更大量的上網人口，但部分行動電信業者一開始就因為缺少 IPv4 而採用 IPv6 網路協定，例如美國的行動電信業者

T-Mobile、新興市場印度的 Reliance Jio 等，為滿足不同使用者的需求，支援 IPv6 是必然的趨勢。[42]

(三) 提供更好的連網體驗：

Facebook 經營社群網站的使命和目標就是希望連結全世界，讓使用者可以分享各種生活體驗和想法，並建立線上相互連結關係，因此提供支援 IPv6，完全符合 Facebook 所追求的使命和目標。[42]

(四) 減少使用 NAT 可能引發的潛在性問題：

NAT 的作用是將 IP 地址作私有和公有位址轉址動作，目的讓設備共用 IP 以減緩因 IP 數量不敷使用的問題，但層層轉址所產生的網路連結效率問題，多個設備共用 IP 所產生的安全性及可靠性的疑慮，都顯示 NAT 並不足以真正解決日益蓬勃的網路所面臨的 IP 不足的問題，而 IPv6 才能提供長遠且更為可靠的解決方案。[42]

(五) 減少網路管理的負擔：

Facebook 認為網際網路轉換到 IPv6 的世界是遲早的事，因此投入心力進行網路支援 IPv6 的改造計畫，經過陸續完成部分設備支援 IPv6 實際連結測試後，顯示網路效率更好，更進一步將資料中心架構改造為 IPv6-Only 系統後，簡化網路系統，也減少網路管理的負擔。[42]

(六) 節省硬體投資成本：

當內部網路資料中心連結轉為 IPv6-Only 系統後，只有外部使用者連結部分才需要 NAT 設備或應用層閘道器（Application Layer

Gateway，ALG），不只網路系統管理更為簡化，也減少硬體投資所需的成本。[42]

Facebook 導入 IPv6 除商業面的考量外，經過實際驗證也證實 IPv6 具有多方面技術優勢，其導入 IPv6 的技術原因說明如下：

(一) 支援 IPv6 可以節省應用程式開發成本：

IPv4 位址不足的限制終究需要被解決，如果開發人員持續撰寫僅支援 IPv4 的應用程式，當 IPv6 連網環境越來越成熟，技術人員終究需要面對修改程式以支援 IPv6 的問題，若能提早面對可避免日後修改所需的人力成本。[42]

(二) 簡化網路管理負擔：

IPv6 的設計除解決全球 IPv4 枯竭的問題之外，另外針對 IPv4 當初設計時未預想到的需求，提出相對應的解決方案，其中之一就是 IPv6 網路提供位址自動配置功能，讓網路設備的管理更簡單。[42]

(三) 維持網路點對點連接完整性：

網際網路最初的設計是為點對點的直接連結而創建，但隨著網路的持續增長，並為了解決隨之而來的問題，因此增加了許多技術來幫助減緩 IPv4 的消耗，而讓網路發展偏離原本的開放性及點對點直接連結設計。由於 IPv6 擁有大量地址空間，因此可以進行直接找尋地址，消除對網路 NAT 的需求。借助 IPv6，讓重返點對點連接的開放性網路，變成可能。[42]

(四) 擁有更好的服務品質和移動性功能：

IPv6 除擁有較長的地址外，也改進 IPv4 許多問題，如 IPv6 設計包含控制訊息 QoS，可以改善網路服務品質，對於語音和視訊流量調度有更好的支援，此類型的應用需要及時性和高服務品質，對時間靈敏度高，在 IPv6 網路中實現要比在 IPv4 更容易。

關於移動性，顧名思義可以讓設備在網路之間漫遊，而不會中斷連接。IPv4 也支援移動性，允許用戶在網路內移動，只不過效率很低。IPv6 對移動性的支援借用了 IPv4 的許多概念，移動 IPv4 要求每個可能的外區網路都要有外區代理，如果沒有外區代理，每個移動節點就需要由外區網路上獲得全球可路由地址，由於 IPv4 地址的匱乏，因此很難實現，但 IPv6 可以為用戶保留永久的 IP 位址，無論用戶如何接入網路，或移動到哪裡可以一直保留此 IP 位址，就可以維持連線。[42]

(五) 提升網路連結效率：

初期 Facebook 進行遷移到 IPv6 測試時就觀察到，以 IPv6 連結 Facebook 網站的速度比 IPv4 快 10-15%。在西元 2014 年（103 年）時，Facebook 甚至提及以支援 IPv6 的行動裝置連結 Facebook News 的數據下載效率快上 20%~40%。開發人員分析認為 IPv6 網路的連結比傳統 IPv4 網路上的服務快，因為 IPv4 服務必須經過中間轉換，例如 NAT 設備或 ALG 等，且 IPv6 分組表頭包含的欄位減少了一半，且所有欄位都與 64 位元邊界對齊，相對提高查找速度，讓 IPv6 連網效率提高。下圖 Facebook 測試 IPv6 連網效率比較資訊。[42]

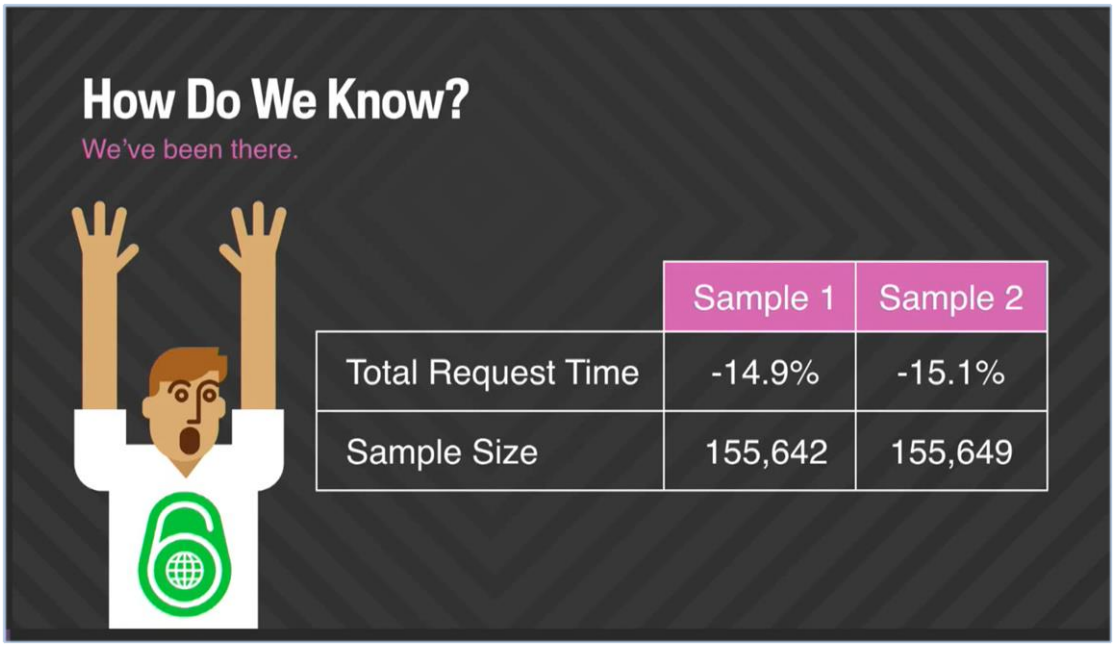

圖 67、Facebook 測試 IPv6 連網效率比較圖

下圖將 Facebook 推動 IPv6 的原因，依人力成本、資本投資、公司的競爭力及使用者經驗等四大面向分析，以了解推動 IPv6 對 Facebook 營運的影響。

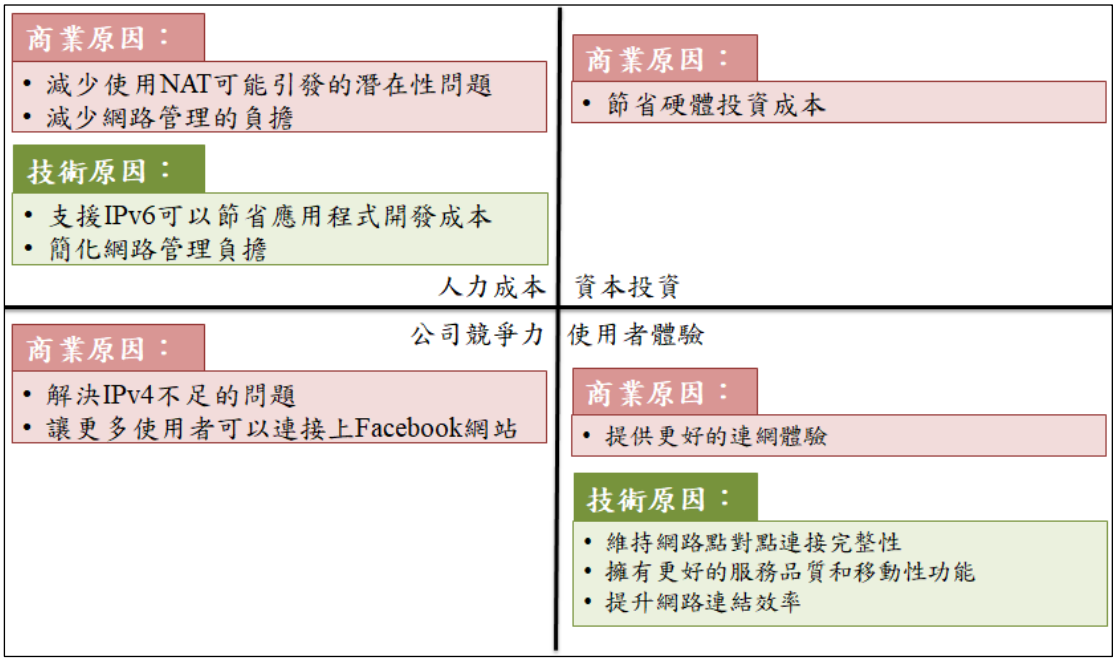

圖 68、Facebook 推動 IPv6 原因

Facebook 導入支援 IPv6 的發展過程，以分階段逐步完成的方式進行，以下就各階段進展說明：

(一) 開發測試網站支援 IPv4/IPv6 雙軌網路服務：

參與西元 2011 年（100 年）世界 IPv6 日測試，測試過程除一開始有極少數使用者反映網站速度慢之外，整體測試結果相當不錯，因此 Facebook 開發團隊決定讓支援 IPv4/IPv6 測試網站仍保留在公開網路上，並持續開放網友進行測試及推展後續開發作業。

(二) 支援商用 IPv4/IPv6 雙軌服務網路服務：

經過世界 IPv6 日測試，Facebook 開發團隊對測試結果抱持正面樂觀態度，積極準備隔年 6 月世界 IPv6 啟動日要正式支援商用 IPv4/IPv6 雙軌網路服務，在西元 2012 年（101 年）5 月中 Facebook 如期完成 IPv4/IPv6 雙軌服務網路建置，正式啟動商用計畫。開始支援商用 IPv4/IPv6 雙軌網路服務後，使用者以 IPv6 連結 Facebook 網站的成長率前幾年的成長率並不高，到西元 2015 年（104 年）才超過 10%，但到西元 2017 年（106 年）就達到 20%使用比率，顯示 IPv6 使用成長比率近年來有加快趨勢，美國的行動用戶成長率更是快，尤其 T-Moible 的行動用戶在 Facebook 的統計資料顯示西元 2018 年（107 年）達到 95%使用比率。

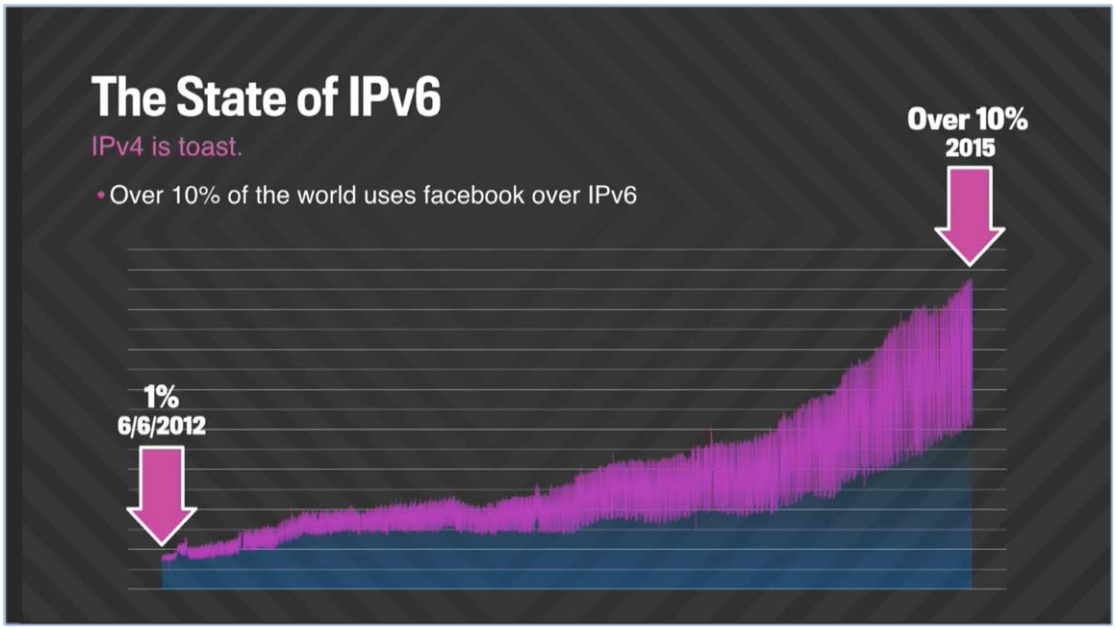

圖 69、Facebook 顯示世界 IPv6 啟動日後 IPv6 使用成長率

(三) 內部網路全部支援 IPv4/IPv6 雙軌服務：

內部網路進行 IPv4/IPv6 雙軌服務升級，所有 IPv4 網路基礎架構增加支援 IPv6。

(四) 進行 IPv6-only 內部網路架構開發測試：

Facebook 將新建立的數據中心集合成群，改用 IPv6-only 進行連結。嘗試將在數據中心處理及運作的所有應用程序和服務，使用 IPv6-only 架構運作。在西元 2014 年（103 年）9 月完成初步開發，並開放 IPv6-only 測試網站提供社群進行測試。

(五) 發布在 iOS 上支援 IPv6-only 應用程式：

除內部網路轉向採用 IPv6-only 架構外，Facebook 也持續進行軟體服務的改造，在西元 2014 年（103 年）12 月即釋出在 iOS 上

可支援 IPv6-only 的應用程式，包含 Facebook 及 FB Messenger 在 iOS 上都有支援 IPv6-only 的版本。

(六) 內部網路數據中心轉為支援 IPv6-only：

根據 Facebook 觀察，使用 IPv6 提供服務可以有效改善用戶下載所需時間，且 IPv6-only 的數據中心可以降低服務營運及管理的複雜性。因此將整個數據中心設備轉移到支援 IPv-only6，並逐步讓 IPv4 數據中心群組退役。西元 2018 年（107 年）根據 Facebook 所發布訊息提到，該公司已經計畫將 IPv4 從數據中心內關閉。

(七) 外部支援 IPv4/IPv6 雙軌網路服務：

下圖根據 Facebook 統計，全球連上 Facebook 應用程式的使用者，只有約 25%是以 IPv6 連網。即使數據中心內可以支援 IPv6-only 的架構，仍需要考慮約 75%使用者只能以 IPv4 連網。因此外部連結部分，使用者連上數據中心前會透過負載平衡器進入，此部分的設備將維持支援 IPv4/IPv6 雙軌服務。這樣就可以讓所有數據中心維持在 IPv6-only 的環境運作中，同時仍然可以為 IPv4 流量提供服務。

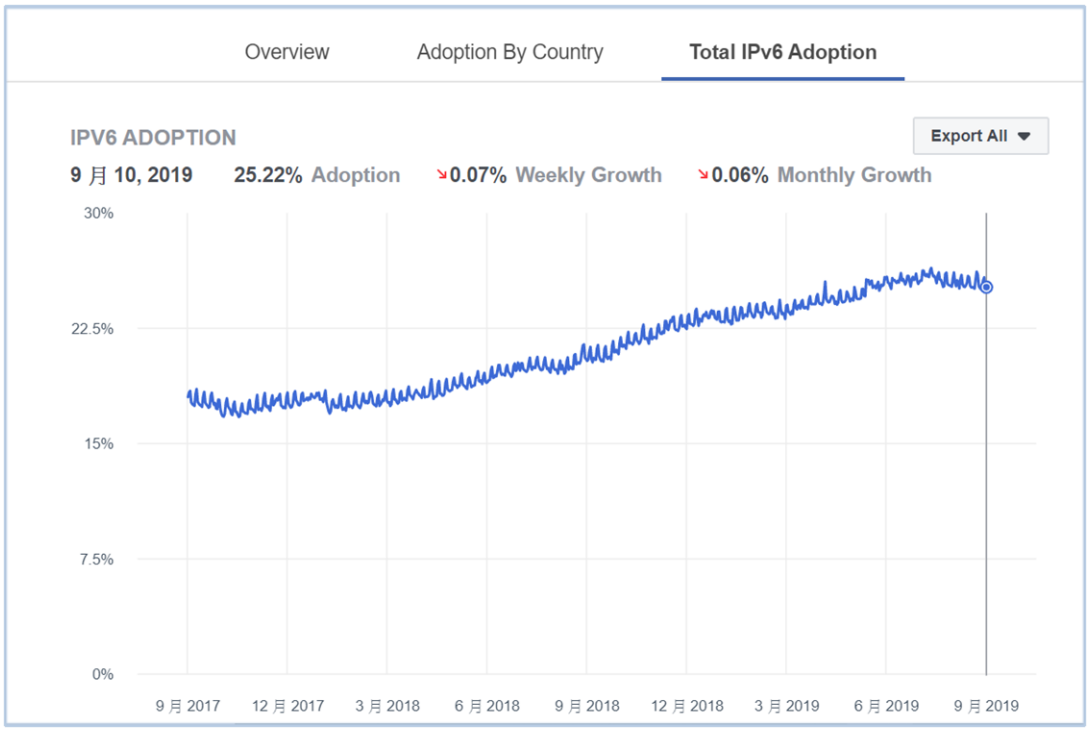

圖 70、Facebook 全球 IPv6 使用率統計資料

(八) 持續統計各國 IPv6 使用狀況：

IPv6 在全球的使用率穩定成長，且成長速度越來越快，顯示全球對 IPv6 發展的信心，Facebook 除積極布局支援 IPv6 外，並透過持續統計及觀察各國 IPv6 發展狀況，以掌握世界發展趨勢，西元 2017 年(106 年)9 月後 Facebook 也將統計資料公開在網路上，供使用者參考。

第三節 調研東南亞國家 IPv6 推動狀況

觀察今年（108 年）在東南亞國家中馬來西亞、越南和泰國 3 個國家，其 IPv6 的使用率成長也相當的快，根據下圖今年（108 年）10 月中全球 IPv6 使用率排名前 20 名，顯示馬來西亞的 IPv6 使用率來到約 45%，越南將近 38%，名列全球前 10 名，而泰國的 IPv6 使用率也來到將近 30%，今年（108 年）以來 3 個國家的 IPv6 成長速度驚人，以下將就此 3 個國家主要電信業者在 IPv6 連網服務的發展狀況逐一探討。

Top 30 List

SN	CC	Display Name	IPv6 %
1	YT	Mayotte	68.93
2	IN	India	63.78
3	BE	Belgium	59.07
4	US	United States of America	54.32
5	TW	Taiwan	45.18
6	MY	Malaysia	44.55
7	GR	Greece	44.19
8	MF	Saint Martin	43.85
9	DE	Germany	41.11
10	FR	France	38.74
11	LU	Luxembourg	38.66
12	VN	Vietnam	37.66
13	GF	French Guiana	36.72
14	JP	Japan	35.79
15	CH	Switzerland	34.65
16	NO	Norway	34.26
17	PT	Portugal	32.65
18	UY	Uruguay	31.71
19	FI	Finland	31.32
20	MX	Mexico	31.31
21	GB	United Kingdom of Great Britain and Northern Ireland	31.02
22	BR	Brazil	30.67
23	TH	Thailand	28.02
24	EE	Estonia	25.89
25	LK	Sri Lanka	25.66
26	CA	Canada	25.31
27	HU	Hungary	24.99
28	AE	United Arab Emirates	24.34
29	NZ	New Zealand	23.42
30	TT	Trinidad and Tobago	22.99

圖 71、全球 IPv6 使用率排名

一. 馬來西亞

從西元 2004 年(93 年)起,馬來西亞政府先後成立推動與發展 IPv6 相關機構,首先由政府單位的能源、水務及通訊部(Ministry of Energy, Water and Communications，KTAK）成立國家 IPv6 委員會（National IPv6 Council)，開始主導馬來西亞的 IPv6 推動計畫，隔年西元 2005 年（94 年）在馬來西亞理科大學（University of Science Malaysia）成立國家先進 IPv6 卓越中心（National Advanced IPv6 Centre of Excellence， NAv6)，這中心成為現在馬來西亞國內 IPv6 頂尖人才培訓、網路專家諮詢及馬來西亞 IPv6 的領導先驅。

馬來西亞政府除了先後成立兩個推動與發展 IPv6 的相關機構外，西元 2006 年（95 年）1 月份馬來西亞政府的能源、水務及通訊部與通訊與多媒體委員會（Malaysian Communications and Multimedia Commission，MCMC）公布「MyICMS 886」政策，從西元 2006 年（95 年）開始至西元 2010 年（99 年）止，每 2 年檢視工作進度，其著眼於改善民眾生活品質及在馬來西亞產業及全球競爭力提升上,扮演整體環境的催化劑角色，並支援既有的 ICT（Information and Communication Technology）基礎建設及服務。在 MyICMS 886 中主要規劃推動 8 項創新服務、8 項基礎建設及 6 項成長領域，期望藉由 8 項創新服務的刺激，加速各界投入 8 項基礎建設（硬體及軟體）的構建，進而發展 6 大成長領域，替馬來西亞民眾與企業帶來最大的綜效。在「MyICMS 886」政策中更是將 IPv6 定為 8 項基礎建設其中之一的項目，由此可看出馬來西亞對於 IPv6 發展的重視。

在馬來西亞政府先後成立了相關推動 ipv6 的部門與政策後，馬來西亞政府推動一個 IPv6 先導計畫（Pilot Project)，該計畫將 IPv6 的相關部門整合進同一個工作團隊中，其主要目標是完成國家 IPv6 委

員會的願景，即於西元 2010 年（99 年）完成 IPv6-enabled（後來修訂到西元 2015 年（104 年））、於西元 2008 年（97 年）完成政府部門的網路 IPv6-Ready（後來修訂到西元 2011 年（100 年）），並由國家先進 IPv6 卓越中心擔任 IPv6 團隊顧問，帶領其他成員一同執行這項 IPv6 先導計畫，另外也選定兩個政府單位一同參與此計畫，分別是能源、水務及通訊部與馬來西亞行政現代化和管理規劃單位（Malaysian Administrative Modernisation and Management Planning Unit, MAMPU）作為政府部門的網路 IPv6-Ready 示範建置對象。此 IPv6 先導計畫亦成為馬來西亞佈署 IPv6 網路環境的先驅，對打算建置 IPv6 網路環境感興趣的對象而言是一個極具參考價值與指導方針的指南，此外 IPv6 網路環境建置示範建置對象是以兩個政府部門為例，針對政府部門的單位而言更是極具參考意義。

馬來西亞政府為了發展國內新一代的網路技術 IPv6，推動了一個 IPv6 先導計畫，在這項 IPv6 先導計畫中，最主要的目標為建立一個具有基本 IPv6 連線能力的網路環境。而在此計畫中所定義的「基本 IPv6 連線能力」指的是讓所有設備可在雙軌（dual-stack，IPv4 and IPv6）模式底下進行資料傳輸與路由（transport and route），並且可同時進行 IPv4 與 IPv6 這兩種協定的運作。在 IPv6 先導計畫報告中主要分為 8 大重點領域，包含：

- ◆ 網路基礎建設（Networking Infrastructure）
- ◆ 位址規劃（Address Planning）
- ◆ 信息安全（Information Security）
- ◆ 過度機制（Transition Mechanisms）
- ◆ 標準（Standards）
- ◆ 訓練（Training）

◆ 測試（Testing）

◆ 過度成本（Cost of Transition）

IPv6 先導計畫執行團隊在執行能源、水務及通訊部的網路更換的過程中，為了讓所有設備皆可在雙軌模式下運作並確保所有網路設定從純 IPv4 轉換成雙軌模式不會出現任何技術故障或安全問題，他們將整個IPv4轉換到雙軌過程分成四階段逐步執行，此四步驟分別為：

◆ 隔離佈署（Isolated deployment）

◆ 拓展基礎設備（Expanding the infrastructure）

◆ 產品安裝啟用（Production Implementation）

◆ 商業服務（Commercial Services（Web & DNS））

以確保網路移轉到雙軌模式後可以正常運作。此外，在 IPv6 先導計畫中還整理規畫設計出 6 個機關內部進行 IPv4 轉換到雙軌主要的實施步驟。首先要先定義出該機關的骨幹網路與區域網路的設備架構，而其中最具挑戰性的地方為中心區域骨幹網路的部分。接著確認每一組設備對 IPv6 連線能力的等級，再來制定出雙軌模式和 IPv4 轉換到 IPv6 的風險評估，然後根據需求決定升級或是購買新的網路設備，務必使每一台設備都具有基本的 IPv6 運作能力，再將這些設備分別在機關的骨幹網路與區域網路內進行 IPv6 路由、IPv6 傳輸及 IPv4 與 IPv6 雙協定同時運作等實際操作測試，最後評估 IPv4 轉換到 IPv6 的有效性、IPv4 轉換到 IPv6 的要求以及 IPv4 轉換到 IPv6 的議題。

IPv6 先導計畫分別從西元 2007 年（96 年）9 月在 KTAK 及西元 2008 年(97 年)4 月在 MAMPU 由 NAv6 派遣工程師進行佈署 IPv6，於西元 2008 年（97 年）9 月完成此案，並在西元 2010 年（99 年）1 月 4 日將馬來西亞 IPv6 實作情況與 IPv6 介紹及兩個單位的 IPv6 佈

署經驗、管理架構及推薦給機構的 IPv6 實施階段等資訊撰寫成冊放置於網路上。

對於國家先進 IPv6 卓越中心而言，他們除了執行 IPv6 先導計畫，並在該項計畫中協助 2 個政府機關網路從 IPv4 升級到支援 IPv6，另外他們還有協助馬來西亞境內的 ISP 業者完成 IPv6 的網路佈署，首先輔導各 ISP 業者讓他們可做到基本的 IPv6 連線，再來讓 ISP 業者們可以做到彼此IPv6相互連通，最後實際佈署到客戶使用的環境中，提供具有商業服務的 IPv6，例如在 Wi-Fi、3G 網路等。另外，還協助兩個政府部門制定國家 IPv6 策略指標（the National Strategic IPv6 Roadmap）與國家 IPv6 研發指標（the National IPv6 R&D Roadmap）兩份文件。

國家先進IPv6卓越中心協助兩個政府部門制定國家IPv6策略指標與國家 IPv6 研發指標兩份文件。首先，NAv6 於西元 2008 年（97 年）6 月製作完成馬來西亞的通訊與多媒體委員會委託的國家 IPv6 策略指標，在這本策略指標中檢查了當時馬來西亞在 IPv6 的實行狀況並繪製出一個未來採用 IPv6 的整體網路搬遷規畫路徑，並蒐集了各個國家 IPv6 的推動小組與其國家的 IPv6 發展情況並闡述馬來西亞政府當時為了推動 IPv6 所制定的相關政策與計畫，還說明了使用 IPv6 對人民以及國家的好處與介紹幾個馬來西亞國內成功建置 IPv6 網路環境的案例，包含先導計畫中的兩個政府機構示範對象-能源、水務及通訊部與馬來西亞行政現代化和管理規劃單位的建置經驗。之後也在西元 2008 年（97 年）12 月完成馬來西亞的科學技術與創新部（the Ministry of Science, Technology and Innovation, MOSTI）所委託編制的國家 IPv6 研發指標，規劃了科技創新部、高等教育部(Ministry of Higher Education, MOHE)、通信和多媒體委員會、國際貿易和工業部

(Ministry of International Trade and Industry)等四個部門分別從學術、研發、ISP、工業等領域推動 IPv6 的研究發展。

為了能更有效的推動 IPv6 使用與普及，馬來西亞政府在先導計畫中也規劃並開辦培訓具備 IPv6 相關專業技能的工程師證照班，負責開班授課的機構為國家先進 IPv6 卓越中心。因為 NAv6 在協助馬來西亞網路轉換至 IPv6 架設上有豐富的經驗與各種專業的知識，而且也是馬來西亞國內 IPv6 研究發展重要的領導先驅，由 NAv6 開設相關證照訓練課程具有公信力，且能夠培訓出 IPv6 專業技能熟練的工程師，有助於馬來西亞推動 IPv6 使用與普及。NAv6 提供四種 IPv6 相關證照訓練課程，分別為

- ◆ Certified IPv6 Network Engineer（CNE6）Level 1：1 級 IPv6 網路工程師（CNE6 Level 1）主要是教導網路工程師如何在實際環境中啟動 IPv6 的技能。
- ◆ Certified IPv6 Network Engineer（CNE6） Level 2：2 級 IPv6 網路工程師（CNE6 Level 2）講授更為深入的 IPv6 轉換到 IPv4 知識內容，並且含括 IPv6 網路系統的安全和管理等內容。
- ◆ Certified IPv6 Network Programmer（CNP6）：IPv6 網路程式設計師（CNP6）為進階的培訓課程，適用於需要深入了解 IPv6 網路程式設計並開發 IPv6 應用程式、移植現有應用程式或是審核與測試 IPv6 應用程式的人員，需擁有 IPv6 基礎知識、基礎的程式撰寫能力。
- ◆ Certified IPv6 Network Security（CSE6）：IPv6 網路安全工程師（CSE6）教導如何提高 IPv6 網路安全設定。

此外，CNE6 Level 1 獲得全球 IPv6 論壇(IPv6 Forum Global)認證的銀級證照課程，CNE6 Level 2 與 CSE6 為黃金級證照課程，並且有來

自新加坡、澳大利亞、印度等國的 IPv6 工程師在馬來西亞或是其他地方取得證照。

馬來西亞 IPv6 的推動,由西元 2013 年(102 年)下半年當時 APNIC IPv6 量測數據已慢慢在發展中，到西元 2019 年（108 年）7 月 IPv6 連網比率約 36%，其 IPv6 使用比率統計圖如下圖所示：

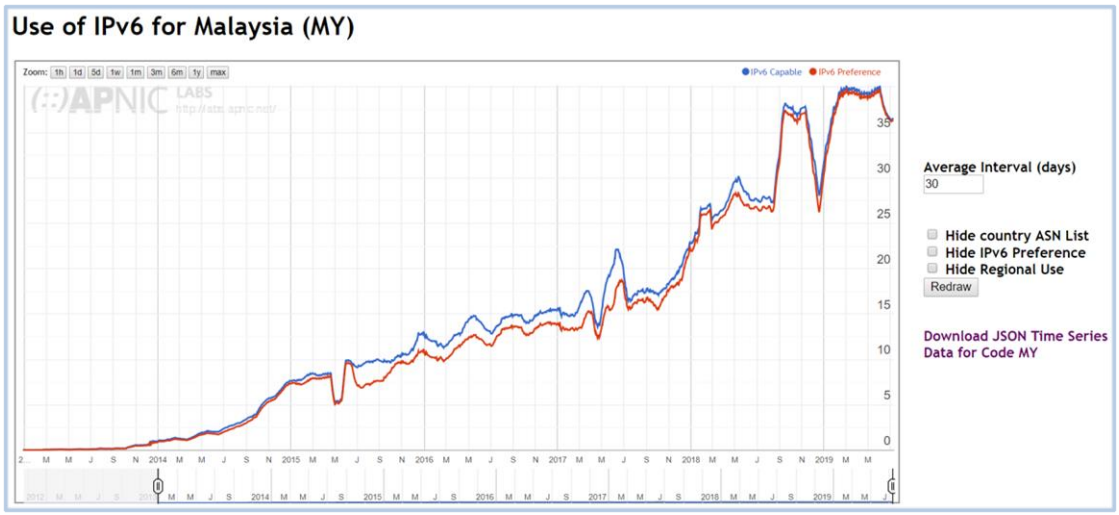

圖 72、馬來西亞 IPv6 使用比率統計圖

下表根據 APNIC IPv6 統計數據顯示，主要 IPv6 網路服務供應商包含 TM Net、MAXIS、DIGIIX、 UMOBILE、CelcomNet、TNet、YTLCOMMS 及 WEBE。

ASN	AS Name	IPv6 Capable	IPv6 Preferred	Samples
AS4788	TMNET-AS-AP TM Net, Internet Service Provider	40.23%	39.98%	863,022
AS9534	MAXIS-AS1-AP Binariang Berhad	32.58%	32.25%	646,997
AS4818	DIGIIX-AP DiGi Telecommunications Sdn. Bhd.	55.29%	55.03%	609,075
AS38466	UMOBILE-AS-AP U Mobile Sdn Bhd	23.41%	23.36%	586,647
AS10030	CELCOMNET-AP Celcom Internet Service Provider	31.26%	31.15%	488,873
AS9930	TTNET-MY TIME dotCom Berhad	20.57%	20.22%	77,019
AS45960	YTLCOMMS-AS-AP YTL COMMUNICATIONS SDN BHD	60.40%	60.21%	51,473
AS38322	WEBE-MY-AS-AP WEBE DIGITAL SDN. BHD.	39.96%	39.85%	40,273

圖 73、馬來西亞 IPv6 主要連結 IASP 統計資料

馬來西亞電訊公司（Telekom Malaysia，TM），簡稱馬電訊，為馬來西亞最大的固網電信（家用電話）和光纖通訊電信公司。由原先的

固定電話，廣播電視廣播業務的國家電信公司，現已發展為最大的寬頻業務提供業者。主要提供數據，固定電話，付費電視和網路服務。TM 的 IPv6 使用比率統計圖如下圖所示，由圖中統計數據顯示，TM 由西元 2013 年（102 年）底開始提供 IPv6 網路服務，IPv6 連網比例逐年緩步上升，到 7 月時 IPv6 使用率已經來到約 40%。

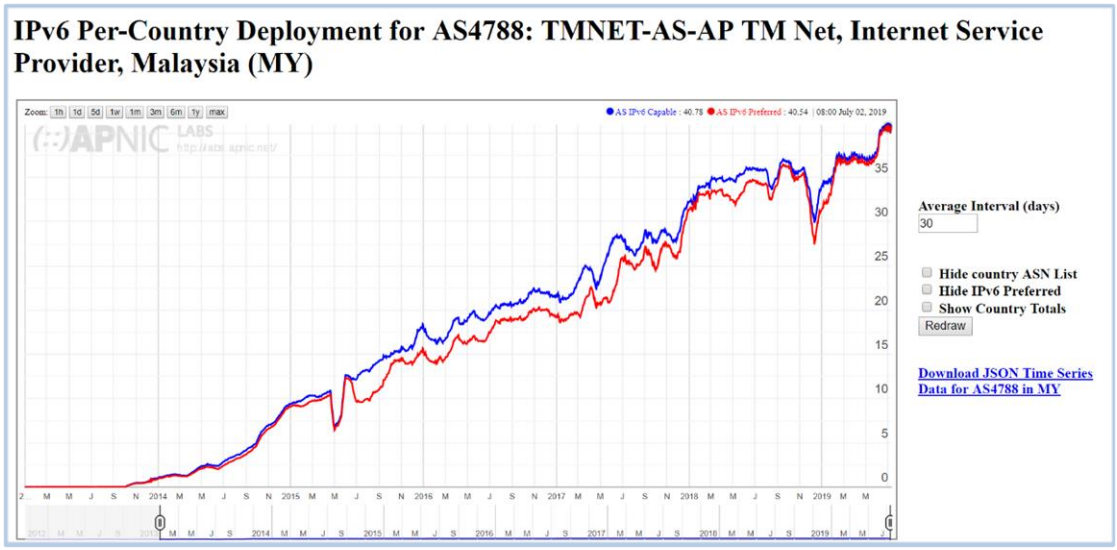

圖 74、馬來西亞 TM Net 的 IPv6 使用比率統計圖

TM Net 旗下的數位服務品牌為 Webe Digital，作為該集團的數位服務供應商，為 TM 的行動、數位和設計中心。前身為 Packet One Networks，該公司於西元 2014 年（103 年）10 月被 TM 集團收購。

Webe Digital 的 IPv6 使用比率統計圖如下圖所示，由圖中統計數據顯示，該公司由西元 2017 年（106 年）初開始提供 IPv6 網路服務，其用戶連網 IPv6 使用比率到 7 月已經超過 40%。

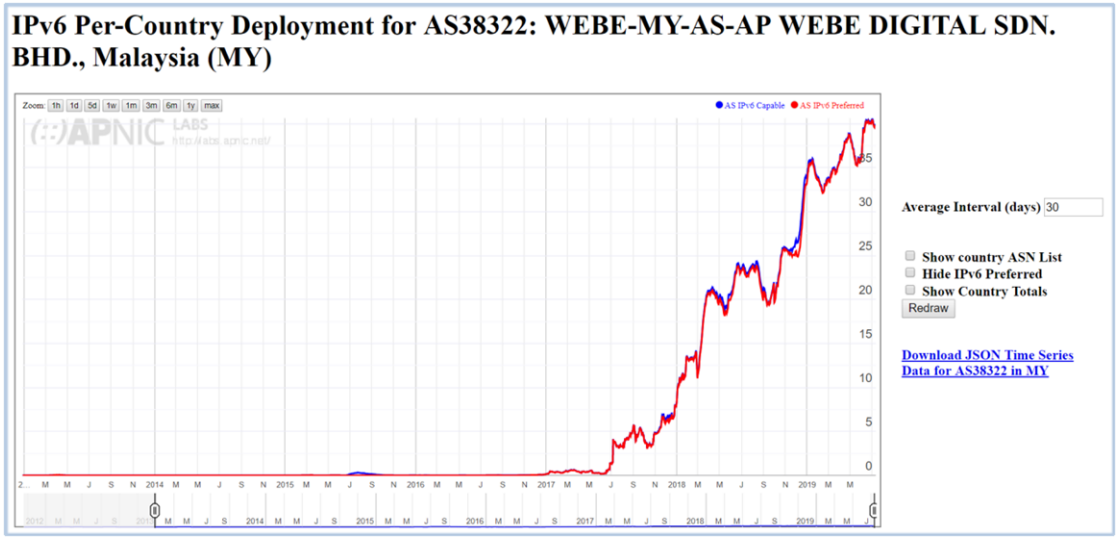

圖 75、馬來西亞 Webe Digital 的 IPv6 使用比率統計圖

馬來西亞行動電信業三大巨頭為 Maxis、Celcom 和 Digi，各大行動電信服務商都有各自的優勢。到目前為止，Maxis 是馬來西亞預付費和後付費用戶群的市場領導者。而 Celcom 和 Digi 則在整體用戶群和預付費用戶群方面占有優勢。

Maxis 的 IPv6 使用比率統計圖如下圖所示，根據圖中統計數據顯示，Maxis 由西元 2016 年（105 年）下半年開始提供 IPv6 網路服務，到西元 2017 年（106 年）底經過一年半的時間，其 IPv6 連網比率還低於 15%，但西元 2018 年（107 年）初開始，Maxis 的用戶在 IPv6 連網比例有大幅的成長，今年（108 年）的使用率在 30%到 50%之間仍有大幅度的變動。

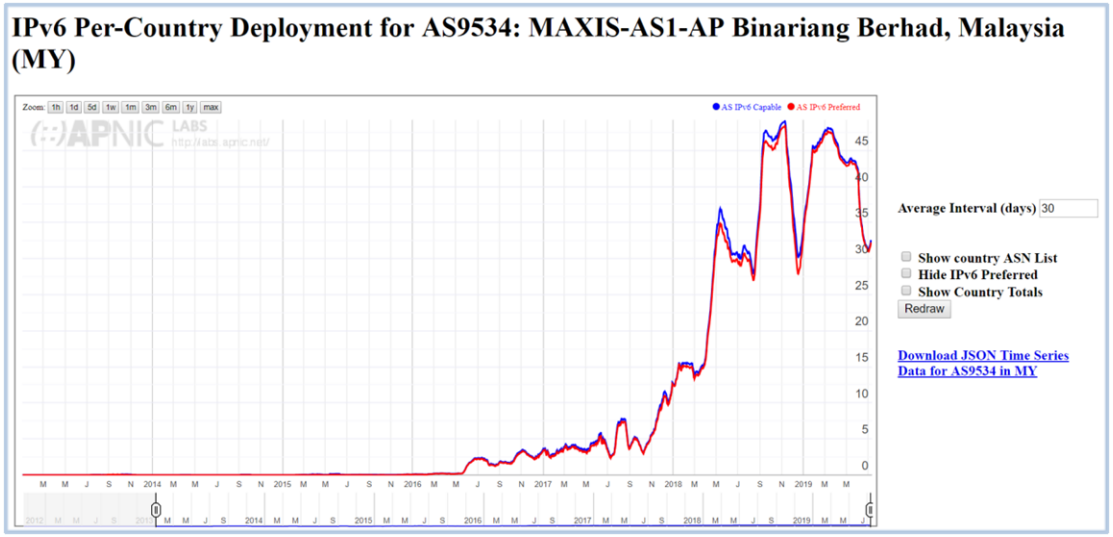

圖 76、馬來西亞 Maxis 的 IPv6 使用比率統計圖

Celcom 用戶在 IPv6 使用比例發展上和 Maxis 的情形類似，Celcom 用戶 IPv6 使用比率統計圖如下圖所示，根據圖中統計數據顯示，Celcom 由西元 2016 年（105 年）下半年開始提供 IPv6 網路服務，到西元 2017 年（106 年）底經過一年半的時間，其 IPv6 連網比率還不到 5%，但西元 2018 年（107 年）初開始，Celcom 的用戶在 IPv6 連網比例有大幅的成長，今年(108 年)使用率在 30%到 40%之間擺盪。

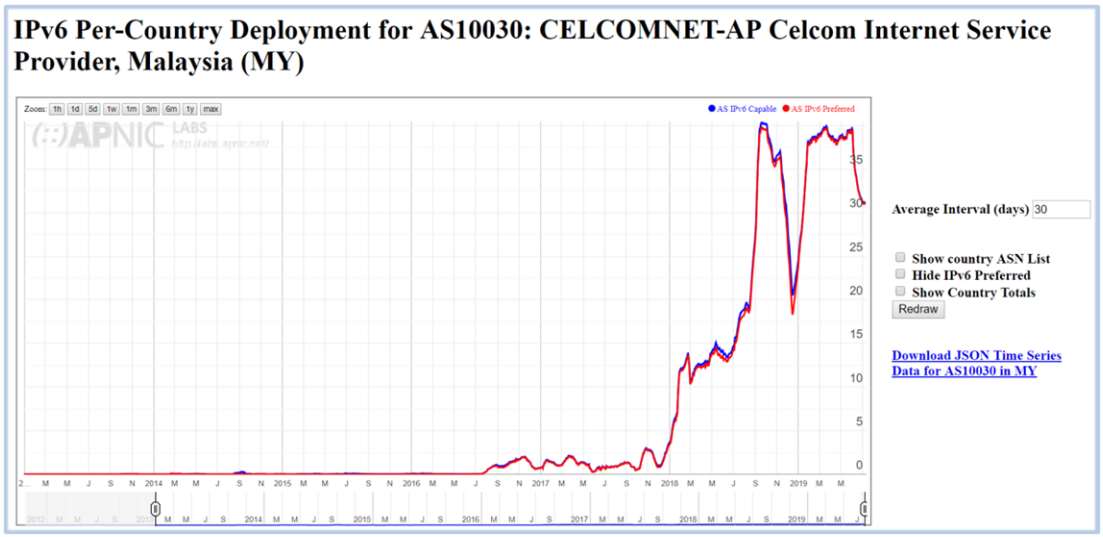

圖 77、馬來西亞 Celcom 的 IPv6 使用比率統計圖

DiGi 的 IPv6 使用比率統計圖如下圖所示，根據圖中統計數據顯示，可以看出馬來西亞的三大行動通信服務商用戶在 IPv6 使用比例在時間軸的發展上相當類似， DiGi 一樣在接近西元 2016 年（105 年）下半年開始提供 IPv6 網路服務，到西元 2017 年（106 年）底經過一年半的時間，其 IPv6 連網比率超過 20%，是馬來西亞的三大行動通信服務商在同時間點 IPv6 使用比例最高的行動通信服務商，西元 2018 年（107 年）初開始，用戶在 IPv6 連網比例又有大幅的成長，到今年（108 年）7 月使用率已經超過 50%。

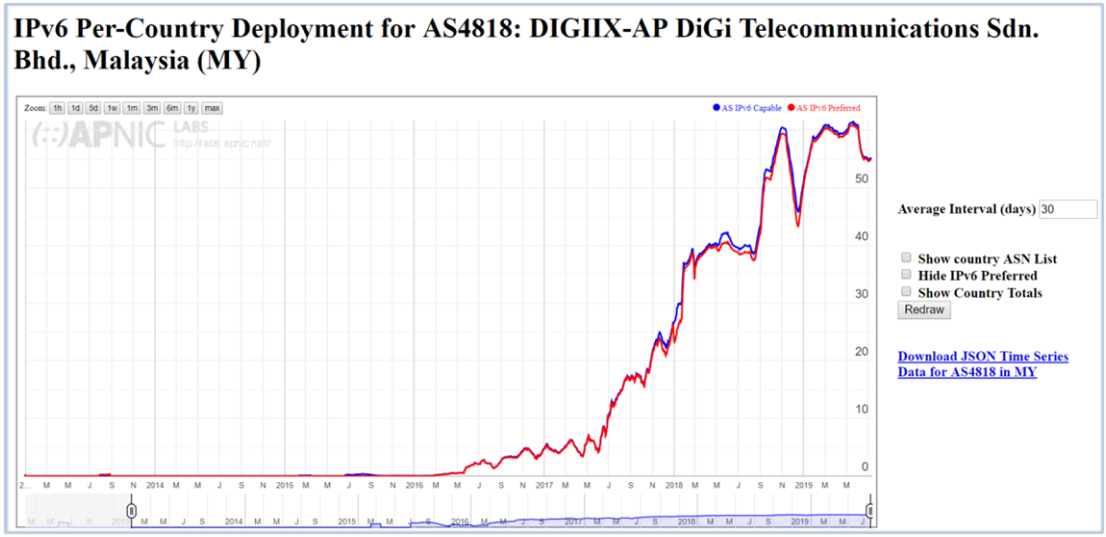

圖 78、馬來西亞 DiGi 的 IPv6 使用比率統計圖

馬來西亞除了三大電信商都有提供 IPv6 連網服務之外，另外楊忠禮行動電信商（YTL Communications）也有提供 IPv6，其 IPv6 使用比率統計圖如下圖所示，該公司 IPv6 連網服務在時間軸的發展上和三大電信商都很類似， YTLComm 一樣在接近西元 2016 年(105 年）下半年開始提供 IPv6 網路服務，到西元 2017 年（106 年）底經過一年半的時間，其 IPv6 連網比率約 10%，西元 2018 年（107 年）再成

長到約 20%，今年（108 年）用戶在 IPv6 連網比例又更大幅的成長，目前使用率已經接近 60%。

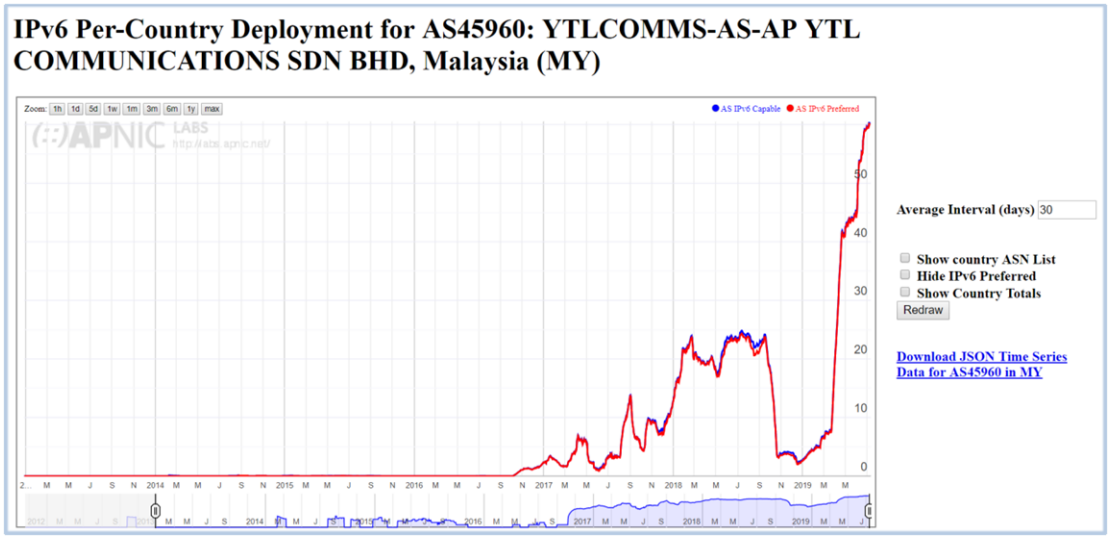

圖 79、馬來西亞 YTL Communications 的 IPv6 使用比率統計圖

馬來西亞在西元 2018 年（107 年）之後，各大行動通信業者在 IPv6 連網比例都有大幅度的成長，因此推升了馬來西亞總體的 IPv6 連網比例，也讓其 IPv6 使用率擠進全球排名 10 名內。

二. 越南

西元2017年(106年)7月26-27日,越南互聯網路信息中心(VNNIC)與中央郵政局(BDTW)共同主辦了一個新世代網際網路協定的培訓會議，討論了對黨中央、政府辦公室與國民議會辦公室的有關IPv6的部署。其中包括專門從事資訊技術人員。這是依據西元2017年(106年)國家計劃發展與推動IPv6全國委員會的決定，所進行的IPv6部署大規模的活動之一。

近幾年來，透過各式各樣的培訓會議，持續推動IPv6的國家的發展和企業的合作，越南的IPv6推動部署有顯著提升。隨著政府支持IPv6網路服務，訓練計劃的內容包含IPv6的部署，政府調控在IPv6部署政策，在網路和服務部署IPv6的詳細說明等。另外，創造條件，交流和探討，提出計劃中較佳的網路服務部署計畫，包含電子郵件、網路線上服務等也是計畫重點。根據IPv6國家行動計劃的目標，落實培訓IPv6連接計劃，透過政府所支持的工作與政策，加緊腳步完成政府辦公室、議會特別的辦公室、中央辦公廳、以及其他政府單位之間IPv6網路架設與提供相關服務。

其中越南IPv6網路信息中心的越南IPv6工作組常務委員會（VNIPv6TF）為紀念越南IPv6第2018天日，舉辦了一系列會議和研討會，以推動IPv6在4GLTE中的部署，內容服務和政府機構的網路。會議由MIC越南副部長就其IPv6行動和內容服務的IPv6部署解決方案和計劃發表了演講。及分享ISP之間關於戰略，轉換問題和IPv6技術問題的信息。

越南IPv6的發展由西元2016年（105年）5月當時APNIC IPv6量測數據仍不到0.1%，到西元2019年(108年)7月已經超過38%，其IPv6使用比率統計圖如下圖所示：

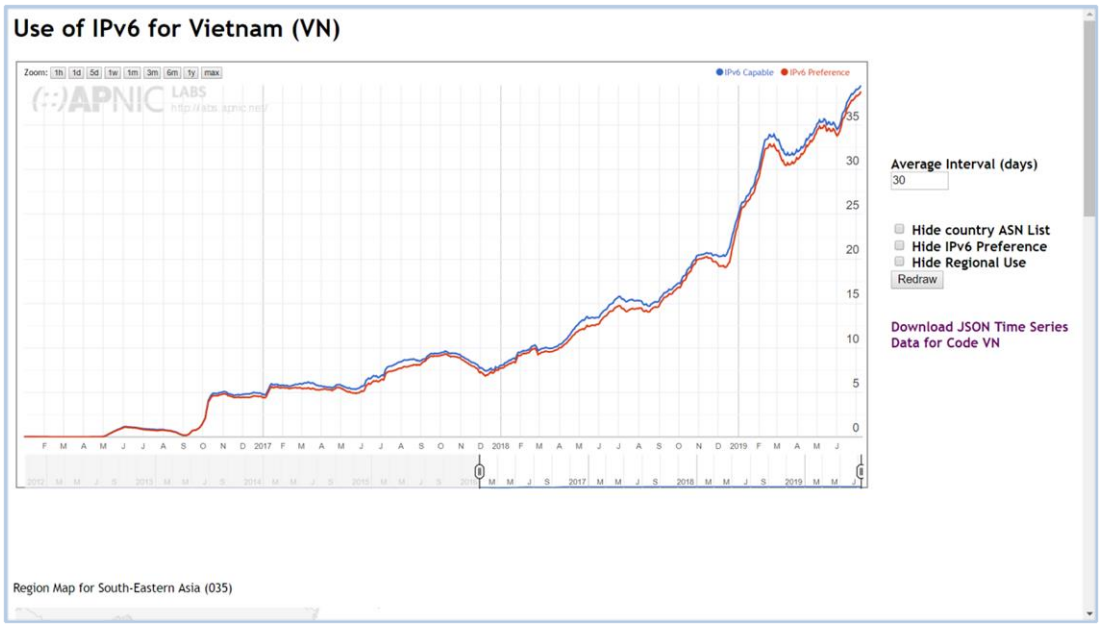

圖 80、越南 IPv6 使用比率統計圖

下表根據 APNIC IPv6 統計數據顯示，主要 IPv6 網路服務供應商包含 VNPT、FPT、Viettel 及 Mobifone。

ASN	AS Name	IPv6 Capable	IPv6 Preferred	Samples
AS45899	VNPT-AS-VN VNPT Corp	39.70%	39.27%	1,684,365
AS7552	VIETEL-AS-AP Viettel Group	45.08%	44.72%	1,474,713
AS18403	FPT-AS-AP The Corporation for Financing Promoting Technology	30.44%	30.05%	726,607
AS24086	VIETTEL-AS-VN Viettel Corporation	62.35%	61.87%	380,807
AS131429	MOBIFONE-AS-VN MOBIFONE Corporation	37.73%	28.62%	175,630

圖 81、越南 IPv6 主要連結 IASP 統計資料

固網業者中以越南郵政電信集團 VNPT（Vietnam Posts and Telecommunications Group）貢獻度最大，其隸屬於越南政府以及越南郵政部。底下擁有 VinaPhone、MobiFone 越南前三大電信公司之二。VNPT 除提供固網服務外，行動通訊服務是由 VinaPhone 提供，VNPT 的 IPv6 使用比率統計圖如下圖所示，由圖中統計數據顯示，VNPT 由西元 2017 年（106 年）初開始提供 IPv6 網路服務，其用戶連網 IPv6

使用比率約和越南全國使用比率發展趨勢接近，目前 IPv6 使用率超過 39%。

FPTTelecom 和 VNPT 是越南固網服務的兩大主要 ISP，而且 FPTTelecom 比 VNPT 更早開始部署 IPv6，兩大固網服務 ISP 提供 IPv6 服務，對越南整體 IPv6 使用率提升具有一定的影響力。

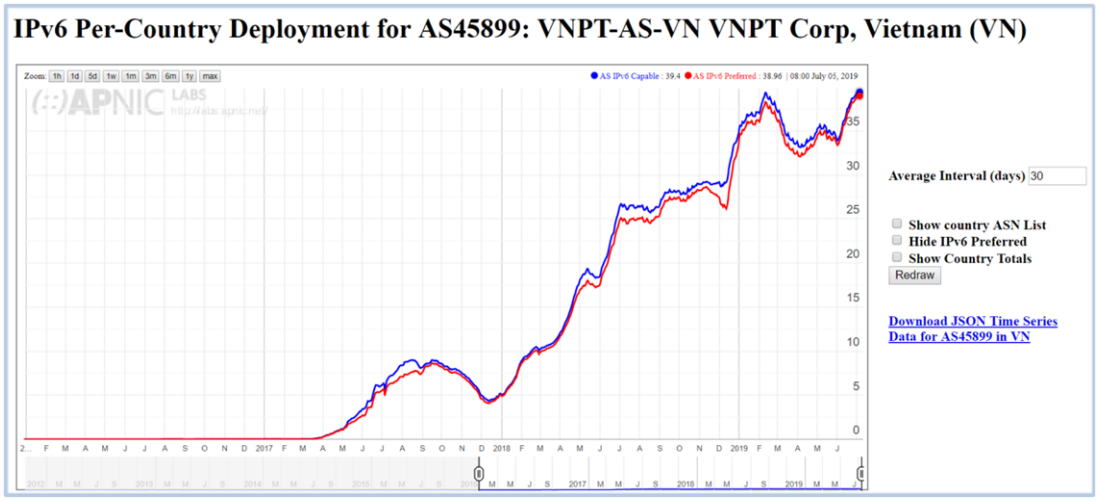

圖 82、越南 VNPT 的 IPv6 使用比率統計圖

根據越南公布的《越南 2017 年（106 年）訊息技術與傳播媒體白皮書》，西元 2016 年（105 年）Viettel 在越南 2G 及 3G 服務市場擁有領先地位，市佔率達 46.7%（包括語音流量、數據流量和簡訊）；其次是 MobiFone，占 26.1%；VNPT (VinaPhone)占 22.2%，排在第三；其他運營商比如 Vietnamobile 和 Gtel (Gmobile)則占較小份額，分別為 2.9%和 2.1%。

Viettel 的 IPv6 使用比率統計圖如下圖所示，由圖中統計數據顯示，Viettel 由西元 2018 年（107 年）下半年開始提供 IPv6 網路服務，其用戶連網 IPv6 使用比率成長相當快速，今年（108 年）7 月已經超過 44%，且 Viettel 為越南的第一大行動通信服務商，其市佔率將近一半，

因此 Viettel 提供 IPv6 網路服務，對越南整體的 IPv6 連網比例有很大的推升作用。

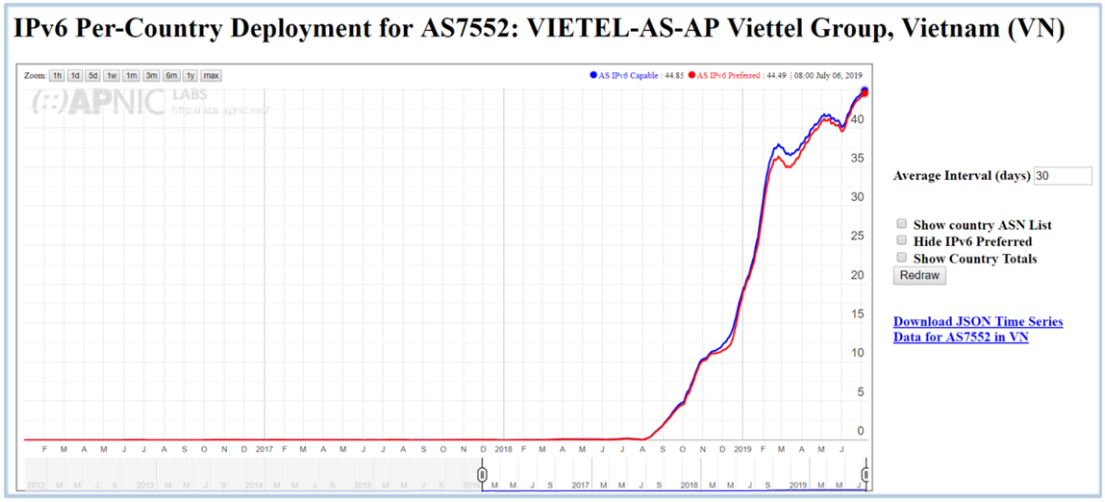

圖 83、越南 Viettel 的 IPv6 使用比率統計圖

MobiFone 的 IPv6 使用比率統計圖如下圖所示，由圖中統計數據顯示，MobiFone 由今年（108 年）初開始提供 IPv6 網路服務，其用戶連網 IPv6 使用比率成長驚人，目前已經超過 37%。且 MobiFone 為越南的第二大行動通信服務商，也就是越南前三大行動通信業者都已經提供 IPv6 網路服務，因此越南整體的 IPv6 連網比例在亞洲相當高僅次於印度、馬來西亞及台灣等少數國家，全球排名已經推升到前 10 名。

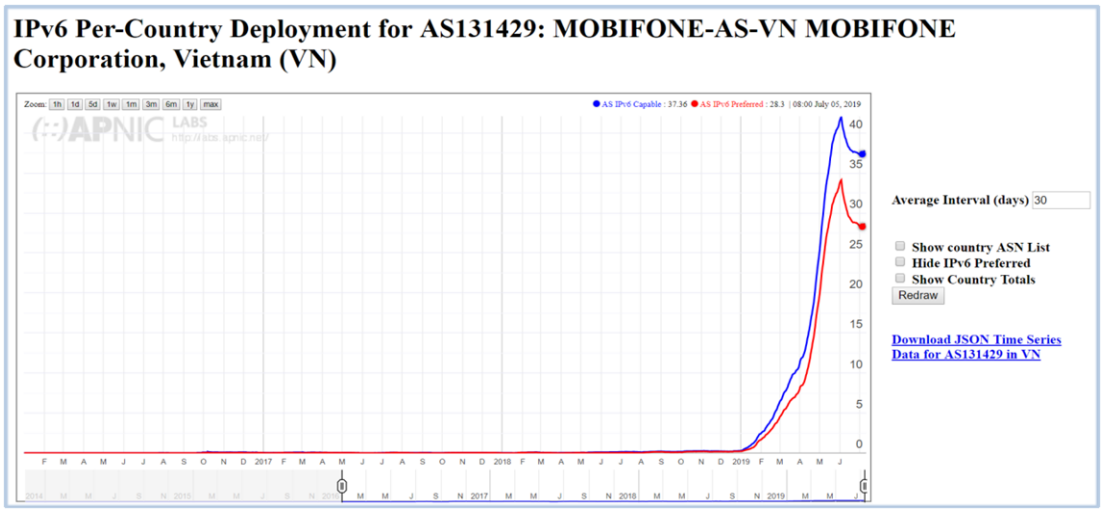

圖 84、越南 MobiFone 的 IPv6 使用比率統計圖

三. 泰國

在泰國負責 IPv6 推廣的部門為數位經濟和社會發展部(Ministry of Digital Economy and Society，MDES)，前身為信息和通信技術部門（MICT)， 西元 2016 年（105 年）9 月，MICT 解散，並被數位經濟和社會部取代。新部會承擔了 MICT 的職責。其下設有專門推動 IPv6 的部門與計畫，並且發行過 IPv6 推廣的專書，對於 IPv6 的推廣不遺餘力。泰國在民間推廣 IPv6 最積極的就是 AIS，是泰國最大行動通訊服務商，集團旗下也投資固網服務。

整體而言， 泰國的 IPv6 隨著泰國申請上網服務人口的成長， 越來越多的上網需求,也帶動了政府部門、ISP 業者以及學術界的升級，在產、官、學三方面的發展亦持續不斷推升著 IPv6 的普及。

泰國 IPv6 的推動，由西元 2016 年（105 年）中當時 APNIC IPv6 量測數據已慢慢在發展中，到西元 2019 年（108 年）7 月 IPv6 連網比率約 30%，其 IPv6 使用比率統計圖如下圖所示：

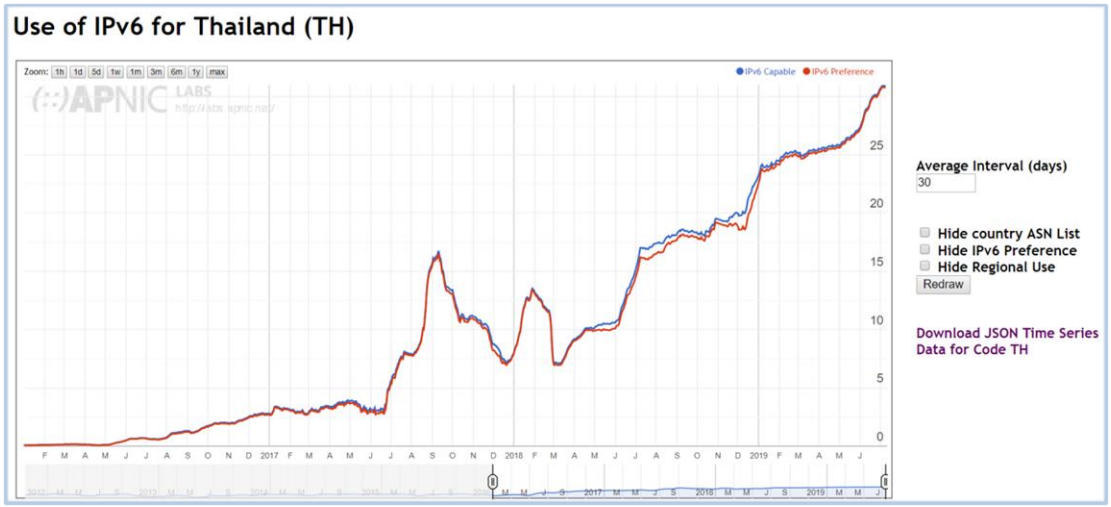

圖 85、泰國 IPv6 使用比率統計圖

下表根據 APNIC IPv6 統計數據顯示，主要 IPv6 網路服務供應商包含 AIS（Advance Wireless Network）、TripleTNet、及 AIS Fibre。

ASN	AS Name	IPv6 Capable	IPv6 Preferred	Samples
AS131445	AIS3G-2100-AS-AP Advance Wireless Network	83.74%	83.59%	710,636
AS45758	TRIPLETNET-AS-AP Triple T InternetTriple T Broadband	50.02%	49.54%	392,949
AS133481	AIS-FIBRE-AS-AP AIS Fibre	59.51%	59.26%	148,968

圖 86、泰國 IPv6 主要連結 IASP 統計資料

AIS 通信（Advanced Info Service）成立於西元 1986 年（75 年），是泰國第一大行動通信服務業。提供泰國國內的 2G、3G 及 4G 行動電話服務。根據西元 2013 年（102 年）的統計，AIS 用戶數達 3500 萬戶，隨著行動網路在泰國的發展，西元 2016 年（105 年）的統計，其用戶數達 6500 萬戶以上。

AIS 行動通信服務的 IPv6 使用比率統計圖如下圖所示，由圖中統計數據顯示，AIS 由西元 2017 年（106 年）下半年開始提供 IPv6 網路服務，IPv6 連網比例上升速度相當快，今年（108 年）7 月 IPv6 使用率已經超過 40%並維持穩定成長。

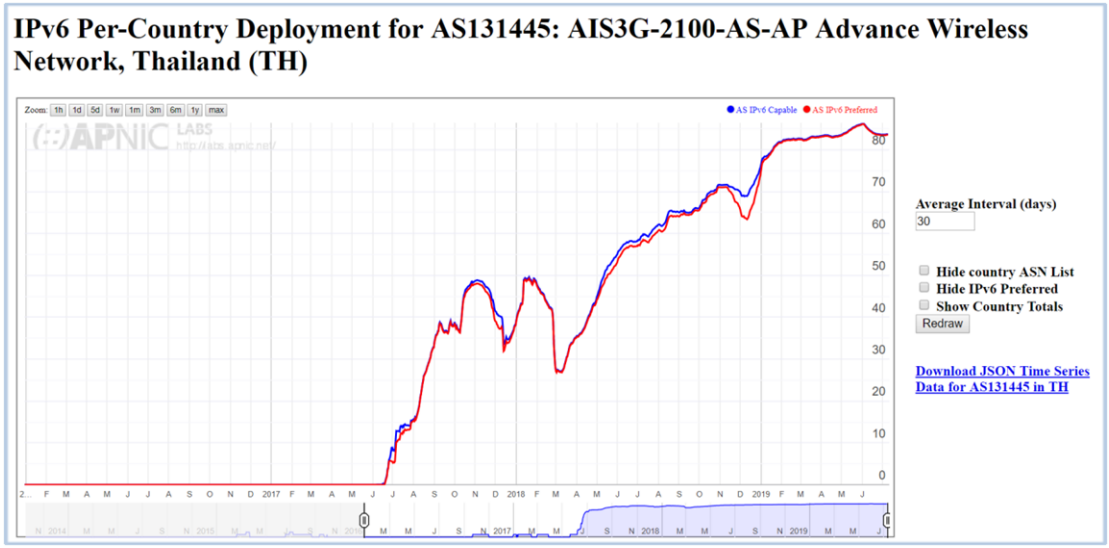

圖 87、泰國 AIS 的 IPv6 使用比率統計圖

AIS 是泰國第一大行動通信服務商。泰國電信市場競爭激烈，行動通信市場競爭更是白熱化。為了繼續保持領先優勢，AIS 於西元 2014 年（103 年）開始進軍固網寬頻市場，積極向全業務通信服務商轉型。AIS 希望經由進軍固網寬頻市場，提升自身在泰國電信市場格局中的競爭力。

泰國 AIS 電信公司，從西元 2016 年（105 年）4 月 1 日起，所有新加入的光纖客戶預設服務直接開通 IPv6 雙協定，發送 Public IPv6 address 給用戶，並且其他光纖用戶也能經過申請取得該項服務不需要額外收費。AIS 將針對光纖用戶提供 Private IPv4 與 Public IPv6 的定址服務。使用者將不再需要經過 NAT 轉換可以直接存取支援 IPv6 的網路服務。這是泰國第一個完成 IPv4/IPv6 雙軌服務的寬頻業者，用戶可以使用家中的路由器直接利用 IPv6 通訊協定與全球網際網路連接。

AIS 的光纖上網服務 IPv6 使用比率統計圖如下圖所示，由圖中統計數據顯示，該公司由西元 2016 年（105 年）上半年開始對新用戶預設開啟 IPv6，經過約一年的時間，西元 2017 年（106 年）上半年其 IPv6 使用比例已經提升到約 50%，成長速度相當快，今年（108 年）7 月用戶連網 IPv6 使用比率來到約 60%。

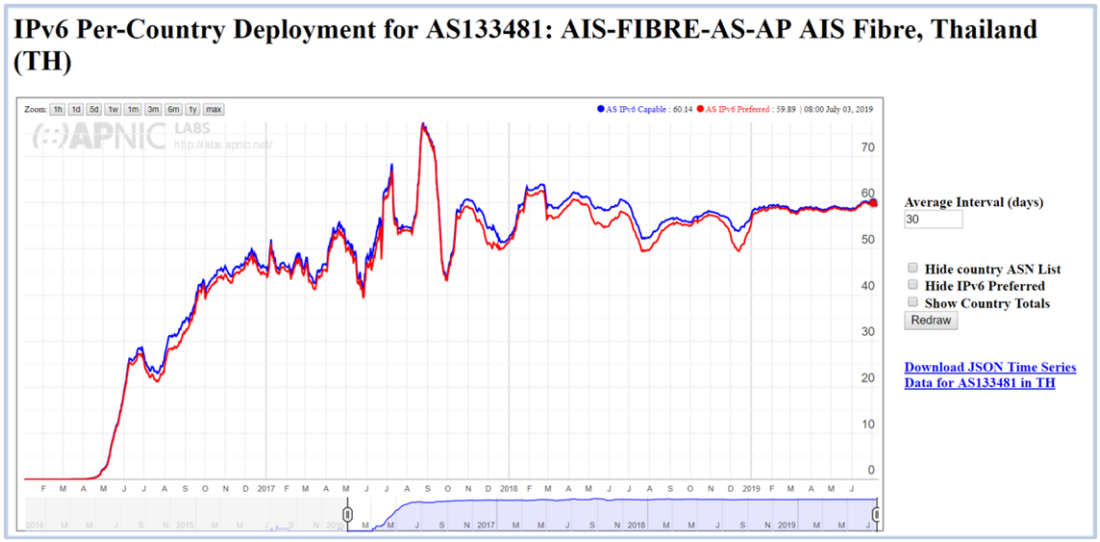

圖 88、泰國 AIS Fibre 的 IPv6 使用比率統計圖

另一家寬頻服務業者 TeipleTNet 的 IPv6 使用比率統計圖如下圖所示，根據圖中統計數據顯示，TeipleTNet 在西元 2018 年（107 年）下半年 IPv6 網路連網比例逐步攀升，目前使用率約達 50%。

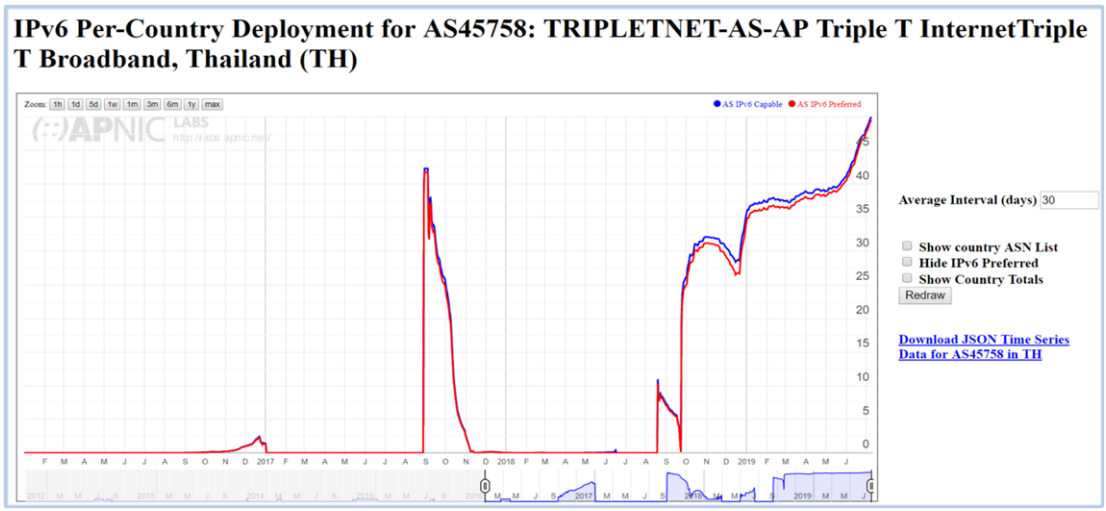

圖 89、泰國 TeipleTNet 的 IPv6 使用比率統計圖

泰國行動通信業者主要有 3 家，分別為 AIS、truemove 及 dtac，西元 2017 年(106 年)Bangkok Post 調查結果各家市佔率如下圖所示[47]

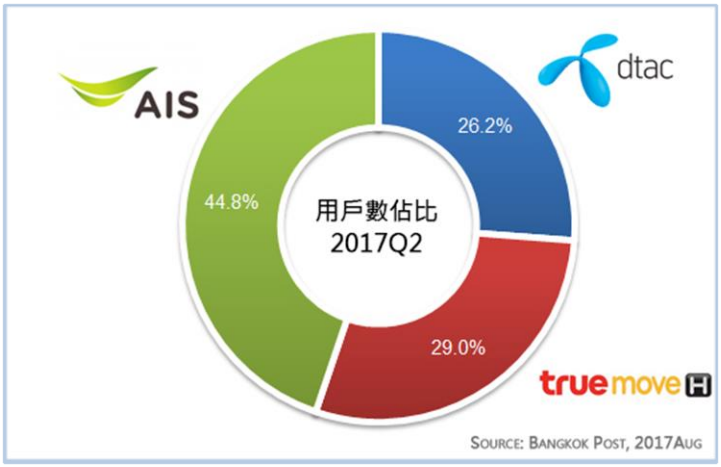

圖 90、泰國主要行動通信業者市佔率

目前泰國行動通信業者，只有 AIS 有提供 IPv6 網路服務，根據 APNIC 的統計資料顯示，其他 2 家業者的 IPv6 流量都極少，目前都尚未正式商業運轉 IPv6 連網服務。

第四節　調研中國 IPv6 推動狀況

中國雖然在早期也由政府及學術網站加入 IPv6 網路佈建試驗及研究的行列，即使其所擁有的 IPv4 數量和人口比例，相對歐美國家而言比例相對低，但因為有 CGNAT 解決方案，暫時推遲 IPv6 的發展腳步，因此到西元 2017 年（106 年）前中國網際網路環境在支援 IPv6 服務的進展並不多；近年隨著物聯裝置越來越盛行及 5G 的推展讓實現萬物連網的理想離實際更近一步，也讓各國推展 IPv6 的熱潮更為明顯，中國也不例外。[48~ 51]

西元 2017 年（106 年）11 月中共中央辦公廳、國務院辦公廳發行《推進網際網路協議第六版（IPv6）規模部署行動計劃》，訂立主要目標要〝用 5 到 10 年時間，形成下一代網際網路自主技術體系和產業生態，建成全球最大規模的 IPv6 商業應用網路，實現下一代網際網路在經濟社會各領域深度融合應用，成為全球下一代網際網路發展的重要主導力量〞，並發出通知，要求各地區各部門實際認真貫徹落實。隔年 5 月工業和信息化部門針對此項計畫，就其所主管事項訂立具體的工作項目，主要分為 6 大工作方向包含：

一. 推動行動網路支援 IPv6

(一) 行動電信業者於西元 2018 年（107 年）底，完成全國 LTE 核心網、接入網、承載網、業務營運系統等支援 IPv6 並實現商業運轉。

(二) 行動電信業者西元 2018 年（107 年）前，需完成企業入口網站支援 IPv6，業者自營流量排名前 10 名的 APP 需支援 IPv6 網路服務，並引導用戶完成支援 IPv6 APP 更新。西元 2018 年（107 年）底前完成 IPv6 行動用戶至少達到 5,000 萬戶，其中，中國電信用戶至少 1,000 萬戶，中國移動用戶至少 3,000 萬戶，中國聯通信用戶至少 1,000 萬戶。

(三) 要求國內行動裝置製造商，新推出的行動裝置出廠需預設支援 IPv6，舊有裝置需透過軟體更新。行動電信業者採購設備需支援 IPv6。

(四) 行動電信業者間網路與手機應用可以 IPv6 互相連結。

二. 加快固定網路基礎設施支援 IPv6

(一) 西元 2018 年（107 年）底完成北京、上海、廣州、鄭州、成都的骨幹網路 IPv6 互相連結。

(二) 西元 2018 年（107 年）底，固網電信業者完成都會網路和接入網支援 IPv6 商業運轉，為寬頻用戶配置 IPv6 地址，提供政府企業客戶 IPv6 專線。

(三) 推動新生產的家庭閘道器、企業閘道器、路由器等固定終端設備出廠預設支援 IPv4/IPv6，固網電信業者訂製和採購的固定終端設備應全面支援 IPv6。

(四) 西元 2018 年（107 年）第三季要達成固網電信業者營運系統支援 IPv6，並具備管理、維護、開通及統計用戶使用 IPv6 能力。

三. 推動應用基礎設施支援 IPv6

(一) 數據中心支援 IPv6。要求三大電信業者西元 2018 年(107 年）底前完成數據中心支援 IPv6；IDC 業者支援 IPv6 等。

(二) 內容傳遞網路（Content Delivery Network，CDN）支援 IPv6。要求阿里雲、騰訊雲等 CDN 業者，在西元 2018 年（107 年）底前完成支援 IPv6。

(三) 雲端服務平台支援 IPv6。要求三大電信業者及阿里雲、騰訊雲等主要雲端服務業者於西元 2018 年(107 年)底完成 50%，到西元 2020 年（109 年）底須全部完成支援 IPv6。並鼓勵雲端服務業者向客戶提供 IPv6 技術諮詢、網站升級等服務。

(四) 域名系統支援 IPv6。要求三大電信業者、政府及主要企業提供域名註冊、解析等服務業者支援 IP6。

四. 開展政府網站支援 IPv 6 與工業物聯網 IPv6 應用

(一) 推動政府各部門服務網站支援 IPv6。

(二) 推動工業物聯網應用支援 IPv6。鼓勵主要企業針對工業物聯網進行網路升級支援 IPv6。

五. 強化 IPv6 網路安全保障

(一) 加強 IPv6 網路安全管理。將 IPv6 相關網路及應用基礎設施安全防護納入電信和網路安全防護體系，健全 IPv6 環境下網路安全相關管理和技術要求，推動 IPv6 的網路安全等級保護、風險評估、通報預警等工作。

(二) 做好 IPv6 網路安全保障措施升級。電信業、IDC、CDN、雲端服務等業者要同步做好現有網路安全保障系統在由 IPv4 升級轉換到 IPv6 過程，須確保具備 IPv6 的安全保障能力。

(三) 強化 IPv6 網路安全能力建設。加強 IPv6 固定網路和應用基礎設施的網路安全防護建設，推動 IPv6 網路環境下的工業物聯網、物聯網應用、人工智慧等新興領域網路安全技術和管理機制研究。鼓勵企業、研究機構等加強合作，加快 IPv6 安全技術研發、應用和創新。

六. 落實配套保障措施

(一) 加強組織領導。各地通信管理局、工業和信息化主管部門須加強與有關部門的溝通協調，建立共同工作機制。

(二) 落實主體責任。要求各企業投入人力及資金，確保各項目標任務如期完成。

(三) 強化規範管理。完善相關電信業務管理要求，要求數據中心（含雲端服務）、內容傳遞網路（CDN）等企業提交年報時，

提供支援 IPv6 相關情況;修訂電信設備網路檢測的相關規定,明確規定網路及終端設備有關 IPv6 的檢測要求。加強公部門電子化系統、資訊化系統及服務平台等項目，應將支援 Pv6 作為必要條件，並負責考核落實等制度。

(四) 加強督查考核。工業和信息化部門將成立 IPv6 督查工作專家組織，研究制定推動 IPv6 規模部署相關任務完成情況的考核標準，並定期督查。建置 IPv6 發展監測平台，對網路、應用、終端、用戶、流量等關鍵發展指標做監測和分析。

由以上敘述可看出在西元 2018 年（107 年）主要是以推動連網基礎的建置，包括行動網路及固定網路雙向並行，訂立明確的 KPI 要求行動電信業者須於期限內完成目標用戶數升級 IPv6;要求電信業者不管是企業設備採購或配置給用戶設備都須支援 IPv6,並做應用軟體升級,IDC 及雲端服務支援 IPv6,政府部門及主要大型企業一起做總體性的推動 IPv6 升級，才能有效改善 IPv6 的連網環境。除推動 IPv6 升級，並加強推動 IPv6 網路安全，確保網路轉換過程安全議題不會被忽視；再輔以強化管理及考核制度，確保發布命令能確實執行。

西元 2019 年（108 年）4 月工業和信息化部門，再發布通知擴大 IPv6 推展工作，今年（108 年）訂立的重點任務，也是分為 6 大工作包含：

一. 網路基礎設施 IPv6 能力

到西元 2019 年（108 年）底，武漢、西安、瀋陽、南京、重慶、杭州、貴陽、貴安、福州 8 個網際網路骨幹完成支援 IPv6，並支援網際網路間 IPv6 流量交換。

二. 應用基礎設施提升 IPv6 業務能力

電信業者數據中心全面完成支援 IPv 6。西元 2019 年（108 年）底完成 CDN 的 IPv 6 支援能力達到 IPv 4 涵蓋區域能力的 85 %以上。阿里雲、天翼雲等雲端服務業者到西元 2019 年（108 年）底，完成包含 IPv 6 雲端主機、負載均衡、內容分發、域名解析、雲端桌面、存儲、雲端資料庫、 Web 應用防火牆等在內的 70 %公有雲端產品支援 IPv6。

三. 終端設備加強 IPv6 支援能力

華為、蘋果及三星等國內外手機品牌新生產的行動終端出廠預設支援 IPv4 /IPv6 雙軌模式；並應加快系統軟體升級，推動庫存量行動終端設備支援 IPv6。

新生產家庭閘道器設備應全部支援 IPv6，並預設支援 IPv4/IPv6 雙軌模式；到西元 2019 年（108 年）底，完成 70 %的原有智慧家庭閘道器的 IPv6 升級。

TP-LINK、D-LINK、華碩等企業新生產的家庭路由器應支援 IPv6，並向原有用戶家庭路由器設備發送支援 IPv6 的軟韌體版本更新。

四. 網站及網路應用生態加快 IPv6 升級

政府相關單位新建網站及外部系統應全面支援 IPv6 連結。對於行動應用軟體新上架的 APP 按照統一的方法及檢測工具推動 IPv6 支持度檢測與標識；西元 2 019 年（108 年）6 月起，各應用商店需在醒目位置為支援 IPv6 的 APP 設置專區並推薦用戶使用；到西元 2019 年（108 年）底，各應用商店新上架的 APP 均應支援在 IPv6 網路環境正常運作。

五. IPv6 網路及服務效能持續提升

西元 2019 年（108 年）9 月底前，IPv6 基礎網路設施、應用基礎設施須達到與 IPv4 接近同樣品質的服務，平均封包遺失率、延遲等指標與 IPv4 效能相比不超過 10%。

六. IPv6 網路安全保障進一步加強

各企業須進一步完整支援網路安全管理制度體系，包涵 IPv6 安全防護和管理相關要求。

今年（108 年）的主要目標為：

一. 支援 IPv6 的行動終端設備比例達到 90 %，支援 IPv6 的固網寬頻終端設備比例達到 40 %。

二. 行動網路 IPv6 用戶數達到 8 億。其中，中國電信達到 1.6 億，中國移動達到 4.8 億，中國聯通達到 1.6 億。

三. 完成全部 13 個網際網路骨幹以 IPv6 相互連結。

工業與訊息部門依照計畫發布年度目標，透過通知及會議加強和業者的溝通，並訂立考核制度，要求在網際網路整體生態系的業者包含硬體製造商、軟體應用商及連網服務業者等共同配合，一起推升 IPv6 的建置及使用率。不只其本國的業者須配合政策推行，國際手機品牌蘋果及三星，我國家用路由器品牌商 D-Link 及華碩也被要求需配合。

在今年（108 年）可以看到明確的成效，下圖為中國 IPv6 使用率的成長圖，到今年（108 年）10 月其 IPv6 的連網比例來到約 14.8%：

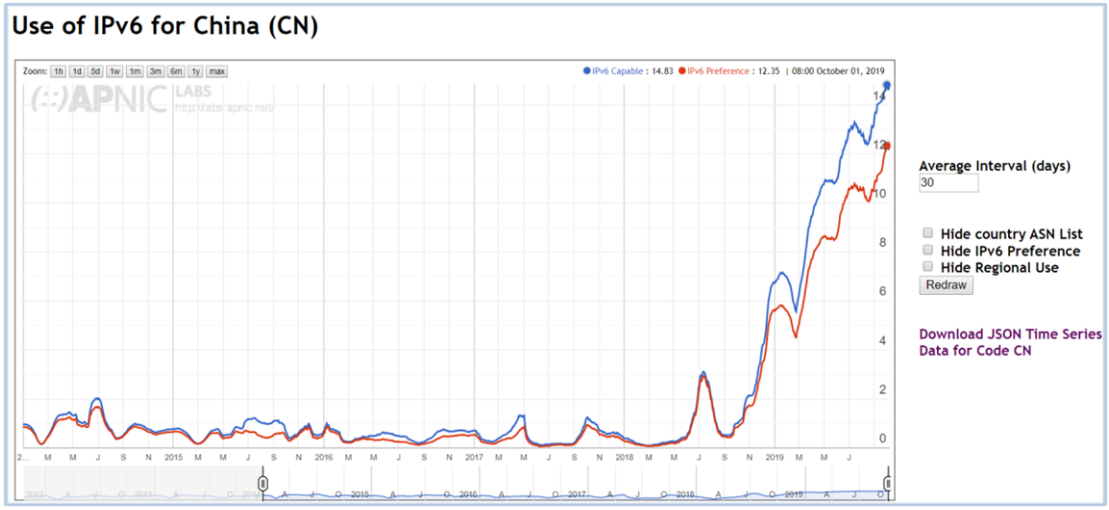

圖 91、中國的 IPv6 使用比率統計圖

三大電信業者中國移動（China Mobile）、中國電信（China Telecom）及中國聯通（China Unicom），在十幾年前就已經陸續在進行 IPv6 實驗。如中國電信為重大活動提供 IPv6 能力，包括上海世博會、博鰲亞洲論壇等都有提供 IPv6 服務能力的經驗。西元 2008 年（97 年）中國聯通進行北京奧運 IPv6 影像服務，讓奧運場館提供現場即時轉播和溫度環境監控。中國移動在西元 2015 年（104 年），將 IPv6 引進 VoLTE 商用化，隔年達到 3,000 萬用戶成為純 IPv6 VoLTE 連網系

統，現在中國移動不再分配 IPv4 地址給 VoLTE 用戶，而是單純使用 IPv6，西元 2018 年（107 年），中國移動 VoLTE 用戶達到 2 億，全都使用純 IPv6 進行語音通話。

中國三大電信業者 IPv6 支援在西元 2018 年（107 年）已經陸續商用化，下圖由 APNIC 所提供的資料，可看出各電信業者在 IPv6 的連網比例：

ASN	AS Name	IPv6 Capable	IPv6 Preferred	Samples
AS4134	CHINANET-BACKBONE No.31,Jin-rong Street	7.60%	5.78%	2,192,678
AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone	7.49%	5.78%	907,985
AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd.	21.42%	19.16%	481,248
AS4812	CHINANET-SH-AP China Telecom (Group)	7.74%	5.85%	295,640
AS4808	CHINA169-BJ China Unicom Beijing Province Network	12.57%	9.92%	214,893
AS56040	CMNET-GUANGDONG-AP China Mobile communications corporation	21.76%	19.54%	213,237
AS56046	CMNET-JIANGSU-AP China Mobile communications corporation	16.68%	14.91%	152,472
AS24400	CMNET-V4SHANGHAI-AS-AP Shanghai Mobile Communications Co.,Ltd.	30.98%	28.32%	88,410
AS24444	CMNET-V4SHANDONG-AS-AP Shandong Mobile Communication Company Limited	19.63%	16.84%	79,263
AS56048	CMNET-BEIJING-AP China Mobile Communicaitons Corporation	35.87%	33.20%	75,409
AS56041	CMNET-ZHEJIANG-AP China Mobile communications corporation	45.68%	42.40%	69,696
AS4847	CNIX-AP China Networks Inter-Exchange	12.50%	9.99%	63,386
AS17816	CHINA169-GZ China Unicom IP network China169 Guangdong province	10.08%	7.71%	59,507
AS24445	CMNET-V4HENAN-AS-AP Henan Mobile Communications Co.,Ltd	16.56%	15.43%	56,330
AS56044	CMNET-AS-LIAONING China Mobile communications corporation	27.05%	25.36%	43,490
AS17621	CNCGROUP-SH China Unicom Shanghai network	13.65%	9.35%	43,485
AS17622	CNCGROUP-GZ China Unicom Guangzhou network	17.85%	13.46%	40,608
AS56047	CMNET-HUNAN-AP China Mobile communications corporation	17.81%	16.57%	39,398
AS24547	CMNET-V4HEBEI-AS-AP Hebei Mobile Communication Company Limited	15.68%	14.47%	36,821

圖 92、中國 IPv6 主要連結 IASP 統計資料

第五節　其他

白俄羅斯成首個強制 ISP 提供 IPv6 服務的國家，今年（108 年）9 月白俄羅斯總統發布行政命令，要求 ISP 業者自明年（109 年）起完整支援 IPv6 裝置，此外，所有用戶都會配給 IPv4 和 IPv6 兩種 IP 位址。白俄羅斯總統魯卡申柯（Alexander Lukashenko）發佈一份名為「關於國家網路區段功能」的行政命令，在網路服務供應商（ISP）部份，該命令除了要求 ISP 應提供充足網路儲存服務、保障用戶資訊安全及隱私外，並規定為回應網路用戶之需求，提供網路資訊系統及資源的 ISP，應從西元 2020 年（109 年）1 月 1 日起完整支援 IPv6 裝置，所有連線都可以 IPv6 連結。此外，所有用戶都會配給 IPv4 和 IPv6 兩種 IP 位址。成為首位將 IPv6 納入強制政策的國家元首。[52]

以前 IPv6 的推動主要以歐美開發國家為主，但 IP 不足的問題越來越嚴重，尤其行動通訊發展，手機用戶不斷增長，全球推動 IPv6 的態勢越來越明顯，由上述各國的努力可以看出，IPv6 在全球已被多個國家所採納，讓網際網路漸漸遷移到 IPv6 已經獲得不少國家的支持。今年（108 年）5G 發展的狀況也比市場預期來的快，預期未來更多裝置連網的需求不會改變，全球對 IP 需求不斷增加，讓更多國家支持 IPv6 的態勢及信心也越來越強。為維護網際網路健康及永續的發展，IPv6 可以帶來更好的選擇。

第五章 ICP IPv4/IPv6 平台架構雙協定網路安全防護差異解析及實際測試

第一節 研析 ICP IPv4/IPv6 升級及網路安全防護差異

IPv6 的設計不只是 IP 位址的擴充，早期網際網路設計不完善的部分，在 IPv6 也做了多項修正，以更符合現在網際網路的現況，並為未來預留發展空間。以下就 ICP IPv4/IPv6 升級及網路安全防護差異分項做簡要介紹。

一. IPv6 的封包

IPv6 為了增加網路傳輸效率，對檔頭(header)結構進行簡化工作，刪除部分 IPv4 檔頭，讓 IPv6 檔頭更精簡且變成固定長度，以減少檔頭在網路傳輸過程中消耗的頻寬。下圖為 IPv4 及 IPv6 檔頭比較圖：

圖 93、IPv4/IPv6 檔頭欄位比較

由上圖可以歸納出 IPv6 移除 5 個 IPv4 的檔頭欄位，下表說明移除欄位為：

表 65、IPv6 移除 IPv4 的檔頭欄位說明

編號	欄位	說明
1	首部長度 （Internet Header Length）	IPv6 檔頭為固定長度因此不需要此欄位
2	片段共用的唯一識別碼 （Identification，簡稱識別碼）	封包過大在傳送端會進行切割，目的端可透過識別碼重組
3	片段標誌（Flags）	控制及辨識封包切割片段
4	片段位移 （Fragment Offset）	每一個封包切割片段相對於原始封包開頭的偏移量
5	header 檢查碼 （Header Checksum）	長度為 16 位元，對檔頭進行驗證及檢查錯誤用，但不包括資料（Payload）錯誤檢查

上表中的 2~4 分項都是封包片段相關資訊，IPv6 已經不需要封包切割訊息因此此 3 個欄位都不需要而移除，後續會對 IPv6 封包傳送部分進行說明。

IPv6 除刪除以上的欄位外，在檔頭增加了〝流量標籤〞的欄位，一般 IPv4 網路上，封包每經過中途路由器，路由器只負責將封包轉送到適當的路徑上，並未做任何的紀錄。在 IPv6 網路上，每一個封包提供一個流量標籤，同一筆資料串列給予相同的標籤號碼，因此可以做流量控制及統計。

以下就 IPv4 與 IPv6 在封包檔頭（header）的差異比較，內容說明如下表所述：

表 66、IPv4/IPv6 封包檔頭比較說明

IPv4	IPv6
欄位：首部長度（Internet Header Length）	
◆ 用來說明檔頭長度（此欄位 佔用 32 位元）。 ◆ 確認資料偏移量（offset）。 ◆ 欄位最小值為 5（5x32 位元即 20 位元組），最大值是 15。	◆ IPv6 移除此欄位。 ◆ 因為 IPv6 的檔頭長度為固 40 位元組。 ◆ 優點增加處理效率。
欄位：片段共用的唯一識別碼（Identification，簡稱識別碼）、片段標誌（Flags）及片段位移（Fragment Offset）	
◆ 片段共用的唯一識別碼，（此欄位佔用 16 位元）。 ◆ 傳送封包過大時將被切割，所有被切割封包擁有同一個識別碼（Identification）。 ◆ 因被切割封包不會依照順序到達，所以在重組時使用片段共用的唯一識別碼資訊以辨別所屬的封包。	◆ IPv6 移除此 3 個欄位。 ◆ IPv6 是由主機詢問傳送路徑上的路由器最大傳送單位（Path Maximum Transmission Unit，Path MTU）大小。 ◆ 如果路由器因為封包太大，會透過 ICMP 回傳一個〝Packet Too Big〞訊息給來源主機。 ◆ 來源主機收到〝Packet Too Big〞時，會決定是否利用 IPv6 的

IPv4	IPv6
	Extension header 來處理，
欄位：header 檢查碼（Header Checksum）	
◆ 利用 header 檢查碼對檔頭進行檢查，若不一致封包就會被丟棄。 ◆ 因為傳遞過程中，可能發生 TTL (Time To Live)、Flag、Offset 變更的情況，為避免檔頭錯誤需重新計算。 ◆ 資料（payload）錯誤，則交給 TCP/UDP 層來處理。	◆ IPv6 移除此欄位。 ◆ 現在網路架構，上一層會確保資料的正確性，因此 IPv6 網路不需要做檔頭檢查。 ◆ 可以大幅提升傳遞速度，減少路由器檢查封包的時間。
欄位：流量標籤（Flow Label）	
◆ IPv4 在資料（payload）內做 QoS（Quality of Service）判斷，但檔頭沒有此欄位。 ◆ QoS 表示網路環境中送出封包的品質，品質越好，表示有越低的延遲、較少掉包和抖動等情形，並搭配更高的吞吐量和可靠性。 ◆ 實際作法是利用封包內容的特定欄位的高低，告訴交換器/路由器等如何處理封包。	◆ IPv6 新增欄位。 ◆ 用來當從來源傳送到一個或者多個目的地時，對一串或者一組 IPv6 封包資料(payload)訂標籤。 ◆ 標籤化的封包經過 IPv6 路由器時，可以被特別處理，例如高優先權傳送。

在 MTU (Maximum transmission unit，最大傳輸單位)部分，IPv4 最小值是 576 個位元組，而 IPv6 最小值是 1280 個位元組。IPv4 網路中，若傳出的封包大於接收路由裝置的 MTU 限制時，一般會進行封包分段成小於 MTU 的封包;在 IPv6 網路中,則是透過 IPv6 Path MTU Discovery（PMD）機制得到封包傳送路徑上的 MTU（PMTU），將封包在網路源頭即進行分段，因此 IPv6 不需要 Identification、Flags 及 Fragment Offset 欄位，IPv6 檔頭可以更小也避免重送封包，增加傳輸效率。

二. IPv4/IPv6 的位址格式

下表說明 IPv4/IPv6 的位址格式的差異：

表 67、IPv4/IPv6 的位址格式的差異

IPv4	IPv6
位址格式	
◆ 32 位元長（4 個位元組）。 ◆ IPv4 位址總數為 4 294 967 296。 ◆ IPv4 位址的文字形式為 nnn.nnn.nnn.nnn，其中 0<=nnn<=255，每一個 n 是一個十進位數。	◆ 128 位元長（16 個位元組）。 ◆ 基本架構是以 64 位元代表網路號碼，另以 64 位元代表主電腦號碼。 ◆ 通常 IPv6 位址的主電腦部分衍生自 MAC address 或其他介面 ID。 ◆ IPv6 位址的文字形式為 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx，其中的每一個 x 是一個十六進位數字，代表 4 個位元。例如 2001:b011:6a00:18ff:d87a:8712:dh8b 就是一個 IPv6 的位址。
Private and public addresses（專用與公用位址）	
◆ IETF RFC 1918 指定 10.0.0.0/8、172.16.0.0/12 及 192.168.0.0/16 作為 Private IP 使用。	◆ 專屬於 IPv6 專用的私有位址位址為 fc00::/7。 ◆ IPv6 將位址分為公用或者私有位址。 ◆ 在 RFC 3041 內有定義 IPv6 對於暫時 IP 的規範，暫時 IP 可以做全域遞送，IPv6 的暫時位址生命週期有限，且不包括 MAC 位址的介面 ID。

三. IPv6 位址的分配方式

現有的 IPv6 位址發放方式為階層式架構，可參考下圖的 IPv6 配置規則架構圖，以一個 IPv6 地址位址來說明 2001:0db8:130f:0000:0000:7000:0000:140b，以 16 位元為一組，每組以冒號「:」隔開，可以分為 8 組，每一個 16 位組都代表一個 IPv6 的發放規則，例如第一個 16 位元組是 Allocation Global Address，這樣的架構可以確保 IPv6 位址的發放有公平性，另外在網路安全的控管上也會有其對應的好處，以下會有更詳盡說明。

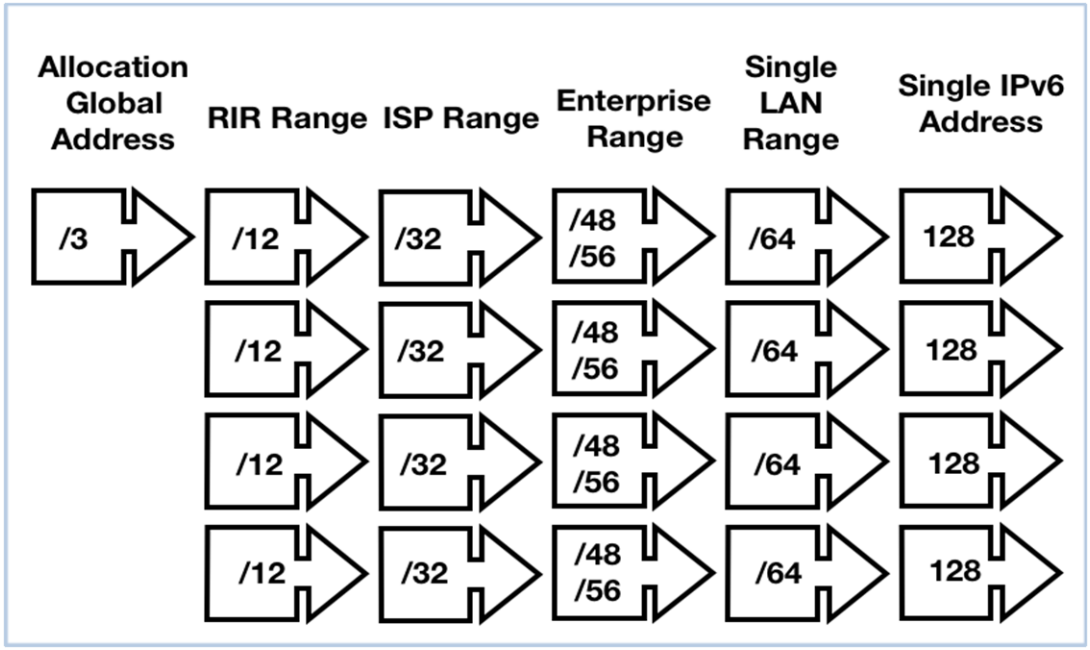

圖 94、IPv6 配置規則

四. IPv6 對 Multicast（群播）協定的調整

IPv6 的位址類型分為 Unicast（單播）、Multicast（群播）和 Anycast（任播）三種。不再使用 IPv4 的廣播（Broadcast）方式來通信，而是使用 Multicast（群播）來取代 IPv4 的 Broadcast（廣播），而 IPv6 新

增的 Anycast（任播）則可以視為群播的一種變形。群播是將訊息傳遞給同一個群組內的設備或主機，而任播則是將訊息傳遞給群組內的單一設備或主機。同時在 IPv6 保留了 ff00::/8 給 Multicast 使用。 IPv6 的位址類型說明及比較如下表所示：

表 68、IPv6 unicast, multicast 與 broadcast 比較

傳遞方式	說明
Unicast（單播）	唯一區域位址（unique local address，簡稱 ULA，保留區塊為 fc00::/7）類似 IPv4 的私有 IP 位址（Private IP address）的可用位址空間，即同一路由內的區域網路（或稱內網）可用位址的集合。 連結本地位址（link local address，保留區塊為 fe80::/64）類似 IPv4 啟用時本機自動產生的本地位址，而此本地位址只存在本機中無法跨過路由器。
Multicast（群播）	IPv4 使用 224.0.0.0/4 作為 multicast 封包使用，而 IPv6 則使用 FF00:::/8。在 IPv6 中以 multicast 取代 IPv4 的 broadcast。在 IPv4 使用 Internet Group Management Protocol（IGMP）協定來管理 multicast group membership，而 IPv6 則不使用 IGMP，改以 Multicast Listener Discovery（MLD） messages。簡單來說，MLDv1 跟 IGMPv2 很接近，MLDv2 跟 IGMPv3 很接近。 scope 欄位是用在 multicast 時，決定哪些路由器可以轉送這些 multicast 封包。 scope 欄位共有 4-bit，其值可以是 0 - reserved 1 - Interface-Local scope 2 - Link-Local scope 3 - Reserved 4 - Admin-Local scope 5 - Site-Local scope 6 - Unassigned 7 - Unassigned 8 - Organization-Local scope 9 - Thru D Unassigned E - Global scope F - Reserved

傳遞方式	說明
	在 scope 欄位之後有 112 bits 用來表示 multicast group ID。
Anycast（任播）	任播用來送給一群主機中的任何一台。 所謂的 anycast 是指該 IPv6 位址可以被指定到多個介面上（通常是多台不同設備）。換句話說，多台機器可以共用同一個 IPv6 位址。當有一個封包被要求傳送到一個 anycast IPv6 位址時，路由器會依據 routing table 決定送給最近的一台設備。

五. IPv4/IPv6 對 IP 設定組態的差異

IPv4 利用 DHCP 做為動態配置 IP 的協定，DHCP 可以使用在辦公室、家裡或工廠等場合。因為 IPv4 的數量有限及費用考量，無法為所有電腦及主機配置獨有 IP，因此會使用 NAT 搭配 DHCP 為設備動態配置 IP，也就是假 IP，此 IP 無法透過 Internet 傳遞，也稱為 Private IP(私有 IP)，在 RFC 1918 內有完整的定義。

IPv6 使用 DHCPv6 協定達成類似的效果，又稱為 Stateful Address Auto-configuration（全狀態位址自動配置）。DHCPv6 協定使用 UDP port 546(用戶端使用)跟 547(伺服器端使用)作為溝通用的連接埠。

在 IPv6 中，除了 DHCPv6 之外，IP 配置還有 Stateless Address Auto-configuration（無狀態位址自動設定，SLAAC）方式，定義在 RFC 2462 及 RFC 4862。SLAAC 運作機制是當一部主機啟動 IPv6 送出多點傳送的路由請求時，路由器回應以路由器公告訊息（Router Advertisement，RA）讓主機從路由器取得 prefix 再加上自己的介面識別碼，來自動配置 IPv6 位址。

使用 SLAAC 在管理上有其便利性，當更換上網的 ISP 後，設備會從新的 ISP 得到全球性位址首碼，ISP 的路由器會將這個位址首碼傳

給企業的路由器，企業內主機即可透過路由器的公告訊息，自動取得新的 IP 位址並覆蓋掉舊的 IPv6 位址即可完成替換。

IPv6 的自動定址機制包括了以下兩種：

(一) 全狀態位址自動配置（Stateful Address Auto-configuration）

透過 DHCPv6 伺服器自動取得 128 位元的 IP 位址及相關組態。

(二) 無狀態位址自動配置（Stateless Address Auto-configuration）

依據 RFC 2462 及 RFC 4862 定義，可以依據自己可用資訊（介面識別碼）和路由器公告取得的訊息（首碼）產生自己的位址。SLAAC 作法上由主機先送出多點傳送路由器請求（Router Solicitation），路由器則透過回應路由器公告訊息來完成。

IPv6 雖然是透過芳鄰探索來執行自動組態配置，但因為路由器公告訊息內的 M 及 O 旗標值不同，會組成四種不同的設定方式。

(一) M 旗標是 Managed Address Configuration，如果 M=1 代表要向 DHCPv6 取得 IPv6 prefix。

(二) O 旗標是 Other Configuration，如果 O=1，代表主機需要向 DNS 取得其他組態資料。

因為路由公告內的 M 及 O 可以分別為 1 或者 0，故 IPv6 的位址自動組態配置有四種選項：

表 69、IPv6 的位址自動組態配置選項

	M=0	M=1
O=0	Stateless Auto-configuration ◆ 適用沒有 DHCPv6 伺服器環境。 ◆ 主機利用路由器 RA 封包首碼自動產生 IP 位址。 ◆ DNS 手動輸入。	Stateless DHCPv6 ◆ 路由器 RA 封包取得首碼自動產生 IP 位址。 ◆ DNS 由 DHCPv6 伺服器取得。
O=1	Stateful DHCPv6 ◆ 適用 DHCPv6 環境 ◆ 主機由 DHCPv6 伺服器取得 IP 位址。 ◆ 其他參數如 DNS 位址也由主機向 DHCPv6 伺服器取得。	其他 ◆ DHCPv6 提供 IP 位址。 ◆ DNS 或者其他參數卻不跟 DHCP 伺服器索取。

IPv6 位址配置根據不同應用場合及使用情境，適合位址配置方法建議如以下表所述：

表 70、IPv6 位址配置建議

編號	位址配置方式	適合場景
1	人工配置位址	適合網路設備及網頁伺服器
	1. 建議關閉 RA（Router Advertisement）的發送。 2. 每一台主機都手動設定 IP（包括 gateway、DNS、防火牆）。 適合網站使用。	
2	SLAAC+RDNSS	適合物聯網設備
	1. 物聯網設備通常不需要主動連網，因此網路環境越單純越好，SLAAC 有助於物聯網的發展。 2. 作法是定期經由 Multicast 發出 Router Advertisement（RA）的封包，從 RA 封包取得 IPv6 Prefix 及 Default Gateway 的資訊。 3. 主機利用收到 Prefix 跟自動產生的 Host ID（主機識別碼）即可變成主機的 IPv6 位址，位址發放之後就不再管理。 4. SLAAC 不支援發送 DNS 伺服器位址，不過新增訂 SLAAC RDNSS 已經解決此問題，只是作業系統不見得有支援。	
3	SLAAC+Stateless DHCPv6	不需嚴格資安查核管理場所

	1. 利用 SLAAC 及 DHCPv6 進行位址配置。 2. RA 負責 IPv6 位址及 Default Gateway 的指派，DHCPv6 則提供 DNS 伺服器位址。SLAAC 機制不會進行 IPv6 位址的更新跟維護。 3. 適合家裡使用。
4	Stateful DHCPv6　　需要嚴格資安查核管理場所 1. RA（Router Advertisement）負責提供 Default Gateway 2. DHCPv6 伺服器負責 IPv6 位址分配（包括 Prefix、Host ID）及 DNS 伺服器位址。 3. DHCPv6 會記錄 IPv6 位址與 MAC 位址的對應表，並經由定期位址更新維護記錄。 4. DHCPv6 不提供 Default Gateway 資訊，因此 DHCPv6 需要跟 RA 配合。 5. 適合企業內部使用。

和 IPv4 比較，IPv6 具有多項優點，詳細說明如下表所示：

表 71、IPv6 優點

編號	分類	說明
1	增加 IP 位址的擴充性	◆ IPv6 位址由 32 bits 變為 128 bits，支援更多 IP。 ◆ 支援位址自動設定。 ◆ 「scope」欄位讓 Multicast（群播）路由延伸性增加。 ◆ 新增支援 Anycast（任播）。
2	封包檔頭簡化	捨棄部分 IPv4 檔頭欄位，減少封包處理頻寬消耗。
3	增加擴充性及更多選項	Extension header 允許更有效率的轉送、更有彈性的選項長度及新增選項。
4	流量標籤	◆ 流量標籤機制可幫封包貼上標籤，讓封包屬於某個特定的「flows」，可用於即時服務。 ◆ 每個封包提供一個流量標籤，同一筆資料串列給予相同的標籤號碼，可以做流量控制及統計。 ◆ 用於支援像視訊、語音類即時服務的需求，以提高 QoS 的品質。
5	授權及隱私的擴充性	在 IPv6 內增加認證、資料完整性、資料保密的能力。

六. IPv4/IPv6（Dual Stack）雙軌服務說明

所謂的雙軌服務，是指 ICP 網站可以讓訪客以 IPv4 或 IPv6 連線，代表網站須同時支援兩種不同 IP 位址的連線方式。IPv6 的推廣在世界各國都正積極進行中，提供 IPv4 與 IPv6 同時支援是因應現實網路的使用狀況，原因是目前網路上仍舊以 IPv4 為主要的連線方式，但支援 IPv6 是一種趨勢，且 IPv6 連網比例全球持續成長。

網站要支援 IPv4/IPv6 雙軌運作，需先從網路基礎開始。對所有網路設備而言，封包傳輸過程是以網路卡為起始出發點，再分為 IPv4 或 IPv6 封包，接著以 TCP（保證傳遞）或 UDP（不保證傳遞）協定往應用程式端傳遞，最後完成任務。

在以太類型（Ether Type）中定義多種協定，與 IPv4 及 IPv6 有關的項目整理於下表：

表 72、Ether Type 定義

編號	以太類型編號	代表協定
1	0x0800	Internet Protocol version 4 (IPv4)
2	0x86DD	Internet Protocol version 6 (IPv6)

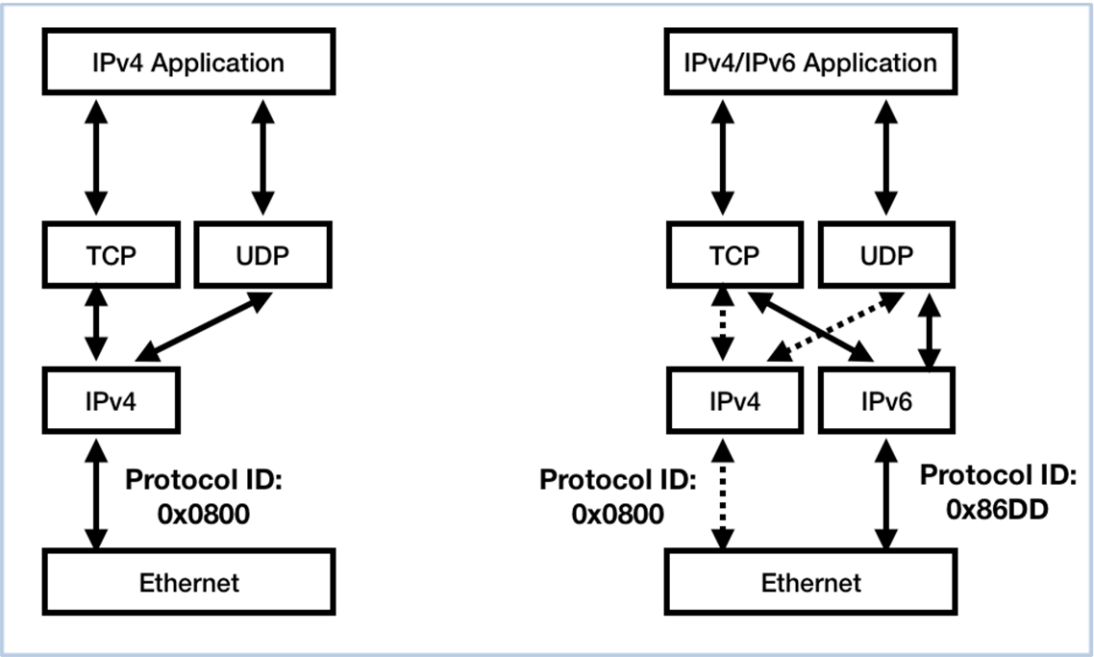

圖 95、IPv4/IPv6 傳輸差異

從上圖可以看出，IPv4 的 Ethernet frame 的 Ethernet Type 為 0x0800，而 IPv6 為 0x86DD。雖然在 Ethernet frame 內，IPv4 跟 IPv6 在 Ethernet Type 帶的值不同，但 Ethernet 是 Layer 2，因此對於 Layer 2 的設備如 Switch（交換器），並不需要去判斷 Ethernet Type，所以並沒有所謂的不支援 IPv6 的 Switch 交換器，對於所有的 IPv6 封包，仍舊可以順利的從現有的 Switch 傳遞到下一個節點。

對於 IPv6 的支援，在作業系統層面，包括 Windows、Mac OS 跟 Linux（例如 Ubuntu、Centos、Fedora、SUSE 等都是 Linux 作業系統），早就已經支援。而硬體設備如 Cisco，也早在西元 2000 年（89 年）宣布在 Cisco IOS Release 12.2(2)T 版本中開始支援 IPv6。

下圖 IPv4/IPv6 連線範例，說明一個同時具備 IPv4 與 IPv6 的設備（如電腦、手機或平板等）連到一個同時支援 IPv4 跟 IPv6 的網站連線的示意圖。

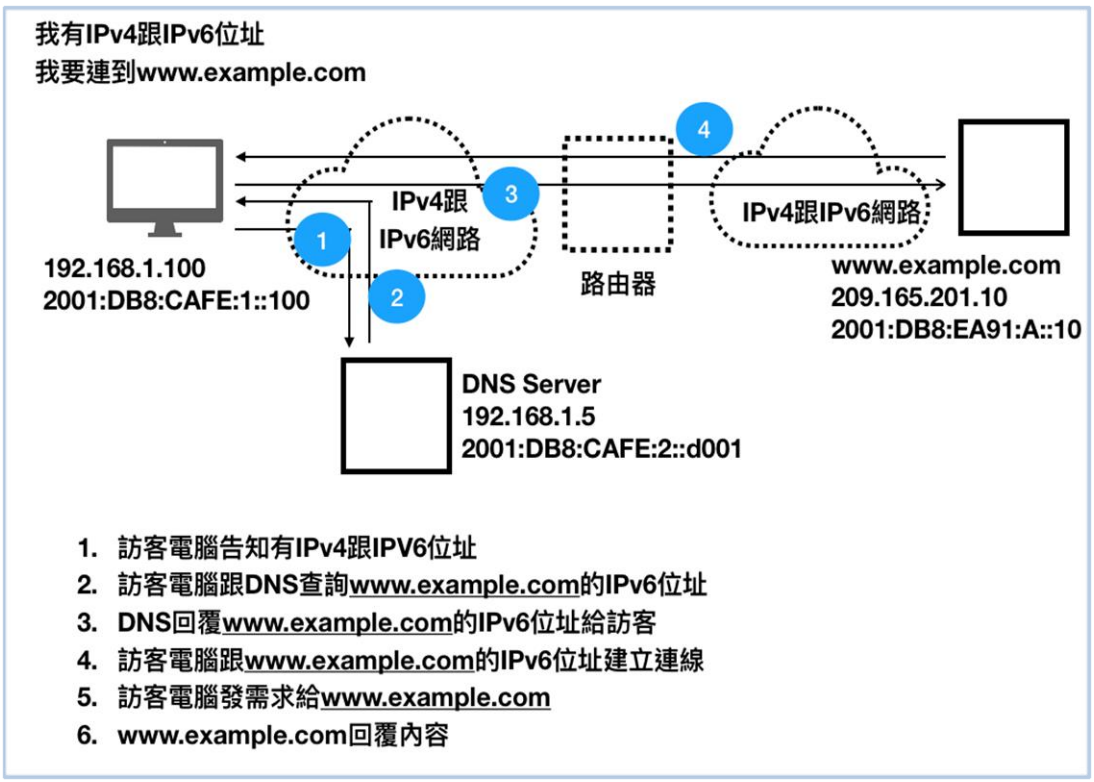

圖 96、IPv4/IPv6 連線範例

七. ICP 機房環境比較

早期網站大都依靠業者自行建立，當網路服務越趨成熟，雲端平台服務可以讓早期網站建置變得更容易，因此 ICP 業者的選擇更多元，以下表列就 ICP 業者的機房設施建置環境整理說明：(資料調查日期 108 年 8 月)

表 73、ICP 業者機房選擇方案

編號	作法	描述	提供業者
1	自建	所有設備都由 ICP 業者自行採購、安裝、維護及部署。	依據需求，跟硬體廠商購買
2	租賃	設備由設備廠商提供給 ICP 業者租賃，有固定租期，在租用期滿之後，可以用低價購買。	遠振資訊 探集數位科技

編號	作法	描述	提供業者
3	IaaS	基礎設施即服務（Infrastructure as a Service，IaaS）是提供消費者處理、儲存、網路以及各種基礎運算資源，以部署與執行作業系統或應用程式等各種軟體。	中華電信 台灣固網 遠傳電信 Amazon Web Services Google Cloud Platform Microsoft Azure IBM Cloud Linode DigitalOcean
4	PaaS	平台即服務（platform as a service，PaaS）是一種雲端運算服務，提供運算平台與解決方案服務。在雲端運算的典型層級中，PaaS 層介於軟體即服務與基礎設施即服務之間。 PaaS 提供使用者將雲端基礎設施部署與建立至用戶端，或者藉此獲得使用程式語言、程式庫與服務。	Amazon Web Services Google Cloud Platform Microsoft Azure Heroku DreamHost Oracle Cloud IBM App Connect Salesforce Platform LiquidWeb rackspace cloud Cloudways

將以上四種網站建置方法歸納成自建/租用機房設備、IaaS 及 PaaS 三種類別，下表就此三種類別的優缺點進行比較及說明：

表 74、ICP 選擇網路架構優缺點比較

編號	類別	優點	缺點
1	自建/租用機房設備	◆ 自行架構及部署所需設備，網路拓墣及設備等級。 ◆ 完全自主掌控，可隨時增加或減少硬體設備。	◆ 人員數量倍增，須 24 小時支援。 ◆ 投資成本高，硬體定期淘汰及升級成本。 ◆ 技術人員能力要求高，人員不好找。
2	IaaS	◆ 依據需求選擇 CPU 數量及等級、記憶體大小、硬碟種類及空間大小、IP 數	◆ 對機房建置而言，不需要採購機房所需硬體。 ◆ 技術人員需熟悉 IaaS 管

編號	類別	優點	缺點
		量，作業系統型態跟版本、資料庫種類及版本。 ◆ 無須管理硬體設備。 ◆ 不需 24 小時有人員定期維護設備。	理及設定方式。 ◆ 作業系統須自行安裝及管理。
3	PaaS	◆ 只需專注於軟體應用部署即可。 ◆ 無須管理作業系統、資料庫的安裝。	◆ 如果遇到系統效能瓶頸時，相對於 IaaS 可以藉由優化作業系統或者資料庫設定就可以提升效能，但 PaaS 只能藉由租用更高級服務達成。

以下就市場主要網路服務商 IPv6 支援度的調查，以了解 ICP 業者是否可以現有網路服務商進行升級支援 IPv4/IPv6 雙軌服務：（資料調查日期 108 年 8 月）

表 75、網路服務商支援 IPv6 表

編號	服務類型	支援 IPv6	不支援 IPv6
1	IDC 機房	中華電信 台灣固網 速博 sparq 亞太線上 數位聯合 台灣電訊	
2	IaaS 服務	中華電信 遠傳電信 Amazon Web Services Google Cloud Platform Microsoft Azure Linode DigitalOcean	台灣固網 IBM Cloud
3	PaaS 服務	Amazon Web Services Google Cloud Platform Microsoft Azure DreamHost	Heroku Oracle Cloud IBM App Connect Salesforce Platform

編號	服務類型	支援 IPv6	不支援 IPv6
		LiquidWeb rackspace cloud	Cloudways

八. IPv4/IPv6 對 ICP 作業系統、網頁伺服器的網路安全防護差異

對 ICP 業者建置網站所常採用的作業系統，最早從 1996 年（85 年）開始，就有部分作業系統開始支援 IPv6，只是早期的 IPv6 功能屬於實驗及測試性質，在目前市面上商用化主流系統大都已經支援 IPv6。

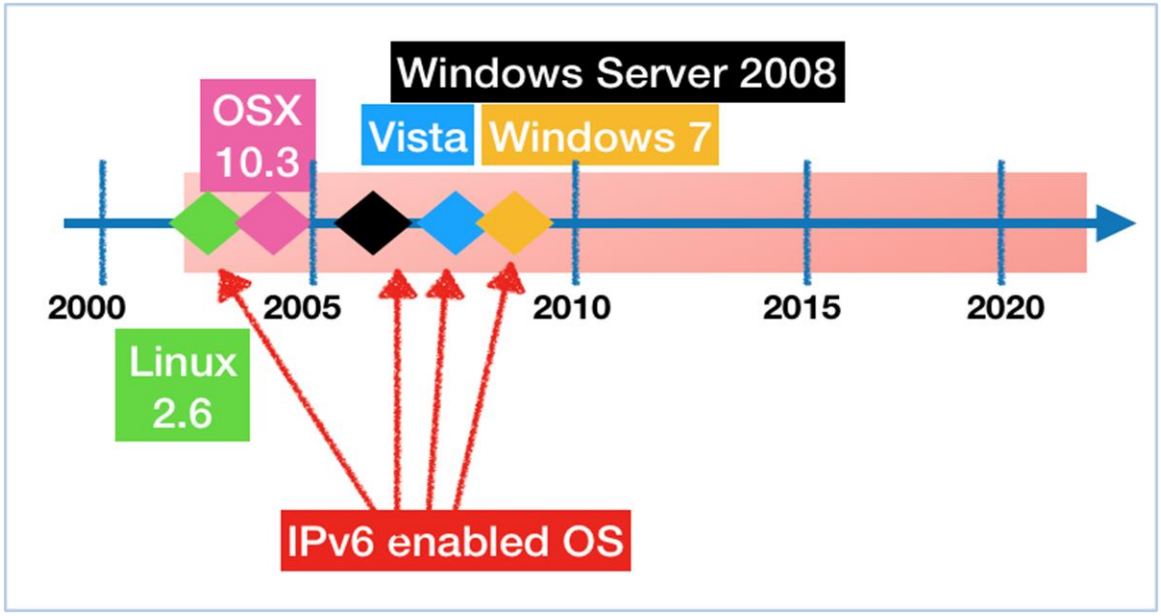

圖 97、網站建置作業系統支援 IPv6 歷程

表 76、網站建置作業系統支援 IPv6 時程

編號	時程	作業系統	支援 IPv6 狀況
1	1996	Linux Kernel	2.1.8 開始支援 IPv6
2	1997	IBM AIX	4.3 開始支援 IPv6
3	2000	FreeBSD 、 openBSD 、	已支援 IPv6

編號	時程	作業系統	支援 IPv6 狀況
		NetBSD	
4	2000	Windows 2000	開始支援 IPv6
5	2000	Sun Solaris	開始支援 IPv6
6	2001	Compaq OpenVMS	開始支援 IPv6
7	2001	Cisco IOS 路由器及 L3 交換機	開始支援 IPv6
8	2001	HP HP-UX 11i	v1 開始支援 IPv6
9	2002	Microsoft Windows NT	4.0 開始支援 IPv6
10	2003	Apple Mac OS	v10.3 開始支援 IPv6
11	2007	Microsoft Windows Vista	開始支援 IPv6

網頁伺服器(Web Server)是指可以提供網站服務軟體。在早期，以 IIS 跟 Apache 兩套為主，使用者多，且文件豐富。近幾年，Nginx 的高效能讓它變成許多大流量網站的首選。跟 Apache 相比較，Nginx 優異的處理速度，讓許多技術人員放棄 Apache 改用 Nginx 的原因。以下就 3 個網頁伺服器服務軟體支援 IPv6 做簡要說明。

IIS 內建支援 IPv6，在 Windows 主機建立 IPv6 連線後，網站即可設定 IPv6 位址以提供 IPv6 服務。只要開啟 Windows Server 主機 Server Manager 的畫面後，選擇 Internet Information Services（IIS）Manager 選項進行 IIS 的設定。

Apache 是 Linux 系統上最廣泛用來架設網站的軟體，Apache 在 2.0 版本之後都有支援 IPv6，在作業系統啟用 IPv6 後，Apache 只要在設定檔加入 IPv6 的位址，並允許外部連線可以連到 IPv6 位址，即可服務 IPv6 客戶。

Nginx 從 0.7.36 的版本後開始支援 IPv6，如果要驗證現行的 Nginx 版本是否已經啟用 ipv6，可以執行 nginx -V 的指令，如結果有出現「--with-ipv6」即表示有支援 IPv6。

詳細網頁伺服器服務軟體支援 IPv6 設定方式，請參閱附錄九〝ICP IPv4/IPv6 平台架構雙協定升級輔導手冊〞第六章有詳細說明。

除作業系統及網頁伺服器支援 IPv6 升級之外，以下將就作業系統及網頁伺服器對於網路攻擊的防禦方式進行比較：

表 77、作業系統跟網頁伺服器對於網路攻擊的防禦方式比較

編號	IPv4 防禦方式	IPv6 防禦方式
1	防禦項目：連線及封包控制	
	Linux 預設使用 iptables 控制。	Linux 預設使用 ip6tables 控制。
2	防禦項目：主機跟主機之間的安全連線	
	安裝 IPSec 軟體，建立端點到端點的連線加密。	啟用 IPv6 的 IPsec 機制，建立端點到端點的安全加密。
3	防禦項目：黑名單與白名單主機連線控制	
	在/etc/hosts.deny 設定。	和 IPv4 相同，在/etc/hosts.deny 設定。
4	防禦項目：Brute Force Attacks(暴力式攻擊)	
	DenyHosts 僅對使用 IPv4 連接有效，在 IPv6 不會起任何作用。	在 IPv6 改用 Fail2ban 軟體，跟 iptables（IPv4 使用）及 ip6tables（IPv6 使用）搭配，直接將 IP 阻擋下來。
5	防禦項目：封包過濾規則	
	若網路不接受 multicast，直接設定過濾阻擋 multicast 封包即可。	若支援在 IPv4 網路上傳送 IPv6 封包（包括以 tunnel 方式在 IPv4 網路上傳遞 IPv6 封包），則建議以特定網卡服務此類封包，並套用過濾規則，阻擋所有的 IPv4 封包（protocol 欄位=41 的封包）且目的地為 239.0.0.0/8 的封包。
6	防禦項目：阻擋保留位址	
	在作業系統或者網站伺服器上禁止保留位址進入，因為這些位址不應該從外部連線到主機。例如 192.88.99.0/24 是 6to4 Anycast	在作業系統或者網站伺服器上禁止保留位址進入，因為這些位址不應該從外部連線到主機。如果是在純 IPv6 環境，應該阻擋

編號	IPv4 防禦方式	IPv6 防禦方式
	（任播）保留網址。	64:ff9b::/96。
7	防禦項目：Teredo 隧道	
	◆ Teredo 是一個 IPv6 轉換機制，可為執行在 IPv4 網際網路但沒有 IPv6 網路原生連接支援 IPv6 的主機提供完全連通性。與其他的類似協定不同，它可以在網路位址轉換（NAT）裝置（例如家庭路由器）後完成功能。 ◆ Windows 作業系統預設會啟用。 ◆ 在純 IPv4 環境中，需要濾掉 UDP port 3544 避免有未授權的 Teredo 連線。	◆ Teredo 是一種臨時措施。在長遠的未來，所有 IPv6 主機都應該使用原生的 IPv6 連接。Teredo 應在原生 IPv6 連接可用時被停用。 ◆ Teredo 伺服器監聽 UDP 埠 3544。 ◆ 在純 IPv6 環境下，應該濾掉 Teredo 封包。
8	防禦項目：禁止爬蟲	
	◆ 透過 nginx 或 apache 模組可以設定訪客連線的速度，避免爬蟲大量抓取資料，造成主機負荷過高，無法正常運作。 ◆ Nginx 限制速率是透過 limit_req_zone 模組，可支援 IPv4 及 IPv6。 ◆ Apache 限制速率是透過 mod_ratelimit 模組。 ◆ IIS 是透過 denyByRequestRate、requestLimits 或 limits 方式來達成限制速率效果。	◆ Nginx 限制速率是透過 limit_req_zone 模組，可支援 IPv4 及 IPv6。 ◆ Apache 限制速率模組可透過 mod_limitipconn，此模組支援 IPv6。 ◆ IIS 則是使用 Dynamic IP Restrictions（DIPR）模組來做限制速率。

九. IPv4/IPv6 對 ICP 防火牆、入侵偵測系統的網路安全防護差異

(一) IPSec 在 IPv4/IPv6 上的比較

IPSec（Internet Protocol Security）協定框架，是透過對 IP 協定的封包進行加密和認證以保護 IP 協定的網路傳輸協定，但 IPSec 並未定義加密和金鑰交換等機制。

IPSec 是 IPv4 組成的一部分，但是 IPSec 是網路層協定，只負責其下層網路安全， 但不負責其上層網路安全部分。也就是說，像網頁傳遞仍舊需要 SSL，檔案傳輸需要 SFTP，郵件傳遞需要 TLS，連線傳輸需要 SSH 進行加密及網路安全認證。IPSec 協定組成說明如下表所述：

表 78、IPSec 組成說明

編號	IPv4	IPv6
1	協定：Authentication Header (AH)	
	1. 利用 hash 及一個安全共享金鑰確保連線的完整性。 2. 對來源封包認證。 3. 利用一個序號來防止 replay 攻擊 4. 防止 options 欄位被注入攻擊。 5. 保護 IP payload 跟所有的 header 欄位。 ◆ 定義在 RFC 2402。	1. 防止 header 注入攻擊。 2. 防止 option 注入攻擊。 3. 保護 IPv6 基本 header、AH 欄位、AH 之後固定的欄位、IP Payload。 ◆ 定義在 RFC 2402。
2	協定：Encapsulating Security Payload (ESP)	
	1. 提供來源認證。 2. 利用 hash 確保資料完整性。 3. 對封包加密確保資料安全。 4. Transport mode(傳送模式)ESP 不提供整個封包的完整性跟驗	1. 在 Transport mode，ESP 預留原本的 IPv6 header，但是新增一個 ESP extension header 及一個 optional ESP trailer。 2. 增加一個 optional ESP

編號	IPv4	IPv6
	證。 5. Tunnel mode(隧道模式)是對整個封包加密後封裝，並添加一個新的 header。 ◆ 定義在 RFC 2406。	authentication trailer，利用 HMAC(Keyed-Hash Message Authentication Code;又稱為 keyed hash)驗證封包。 ◆ 定義在 RFC 2406。
3	協定：Security Associations (SA)	
	1. 用來交換建立安全連線之間所需的資訊，包括演算法、金鑰用來加密封包。 2. 用途包括連線、驗證。 3. IPv4 使用 IKEv1 作為金鑰管理。	1. 使用 IKEv2 作為金鑰管理的方式。 ◆ 定義於 RFC 4301。

IPv6 的 IPSec 架構跟 IPv4 很類似，只是在 IPv4，AH 跟 ESP 是 IP protocol headers，而 IPv6 則是使用 extension header 的作法。而 IPv6 這樣作法優點是將 IPSec 作為 IPv6 protocol 的基本，而不是像 IPv4 需要額外考量的。

IPSec 是 Internet Layer 的安全通道，提供設備或者網段之間的安全連線。在 RFC 規範的早期版本，IPv6 實作 IPSec 是建議使用 IKE (Internet Key Exchange，IKE Internet Key Exchange)的金鑰管理，並要求所有的 IPv6 設備都需要支援 IPSec 架構，並同時支援手動及自動設定。現在，新版的規範是建議自動設定改用 IKEv2(第二版)，此需求定義在 RFC 5996。

IPSec 有兩種模式，分別為 Transport Mode (host-to-host)跟 Tunnel Mode (gateway-to-gateway or gateway-to-host)，以下說明 IPSec 兩種模式下對於封包的欄位變更、加密範圍及驗證範圍。

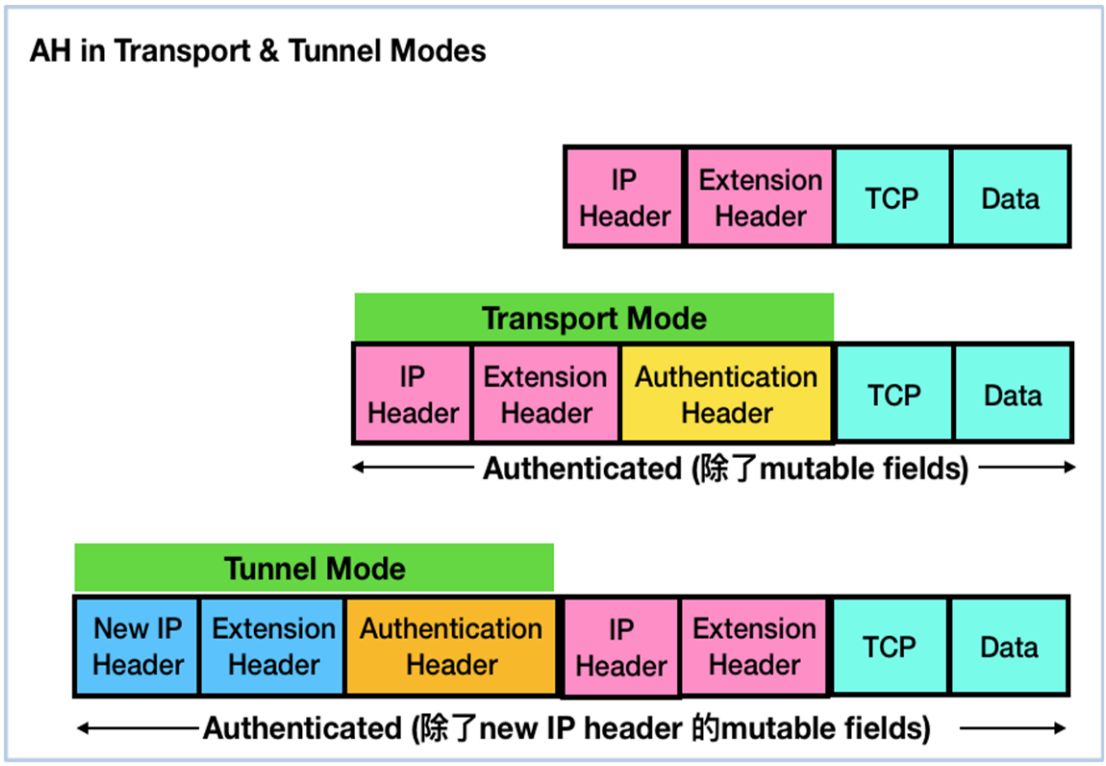

圖 98、AH in Transport & Tunnel Modes

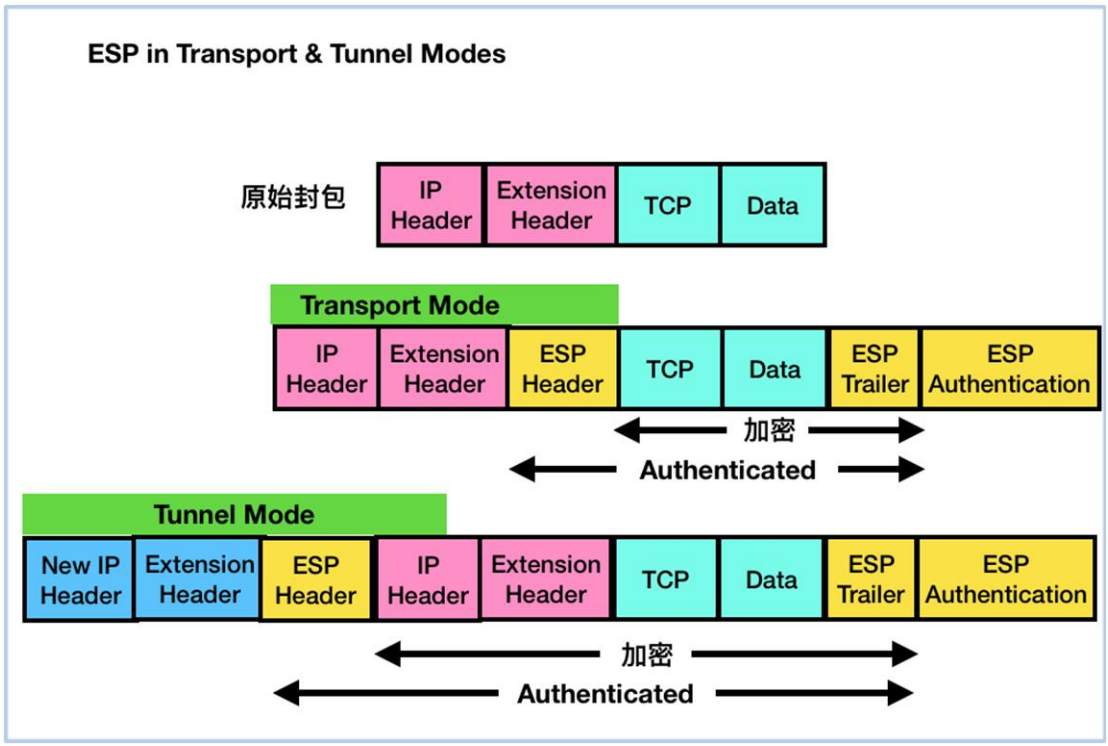

圖 99、ESP in Transport & Tunnel Modes

關於 IPv6 的安全設計，可以參考 RFC 2401。在 IPv4 中最重要的端點到端點的加密 IPSec 已經直接加到 IPv6 內，關於 IPv6 IPsec 有關的討論，可以參考 RFC 4301 及 RFC 5996。

(二) NAT 在 IPv4 與 IPv6 上的探討

在 IPv4，如果不需要幫每一個設備都配置一個公開實體 IP 時，此時會使用 NAT 去配置私有 IP。在 IPv6 網路環境下，由於 IPv6 數量夠多，因此不需要使用 NAT 機制來解決 IP 不足的問題。

網際網路架構委員會(Internet Architecture Board，簡稱 IAB)在 RFC 5902 描述關於 IPv6 環境下使用 NAT 機制的情境。會有 IPv6 是否需要 NAT 的討論起因於原本在 IPv4 下使用 NAT 的廠商，他們覺得也需要類似的機制可以在 IPv6 下使用。不過依據 IETF(Internet Engineering Task Force，網際網路工程任務組)討論結果，不需要在 IPv6 提供 NAT 機制。更多關於 IPv6 是否需要 NAT 的討論可以參考 RFC 4864。

IPv6 NAT 的討論主要可以整理如下：

表 79、NAT 問題討論

編號	討論	IPv6 解決方式
1	問題：Avoid Renumbering(避免重新編號)	
	在 RFC 4864 第 2.5 節討論的，許多業者希望能夠盡量減少網路維運的負責度跟工作量。對家庭用戶而言，重新編號不是一個嚴重的問題，但對企業用戶卻是。影響範圍包括需要重新配置 IP 跟 prefix 的設備，包括 DNS、DHCP、防火牆、IPSec 策略、入	RFC 2462 提供 IPv6 Stateless Address Autoconfiguration(無狀態地址自動配置)，提供自動配置跟重新編號。IPv6 的 Stateless Autoconfiguration 是 IPv6 的新功能，包括 link-local 位址、multicasting(群播)、the Neighbor Discovery(ND)通訊協定、從底層

編號	討論	IPv6 解決方式
	侵偵測系統、庫存管理系統、程式碼修正管理系統內部系統。許多大企業使用提供商無關地址空間（Provider-independent address space，又稱 PI 地址空間）是由區域網際網路註冊管理機構（RIR）直接分配給最終用戶的一段 IP 位址，主要優點是方便設定路由(Wiki 維基百科說明)。	數據鏈路層地址生成地址的接口標識符的能力。
2	問題：Site Multihoming(網站多宿主)	
	站點多宿主提供了網際網路所需的可靠性跟負載平衡。內送流量備援容錯機制(Multihoming)，亦作多重主目錄，是網際網路連線的一種容錯機制，用以提高 IP 網路上對網際網路連線的可靠度。這個機制一般只用在客戶端，而不會用在網際網路供應商(ISP)，透過為客戶端提供多於一條網際網路連線，使當中其中一條連線中斷時，系統可以自動切換使用另一條連線。(Wiki 維基百科說明)	在 RFC 3852 此篇 RFC 描繪了新的 IPv6 site-multihoming 架構下所欲達成的理想目標，這些理想包括提供有高效率的備援功能(redundancy)、優質的負載分享(load sharing)、高效能(performance)、支援客戶所要求的管理政策需求(policy)等優於 IPv4 目前 site-multihoming 所能提供的功能。 如何在不影響目前 site-multihoming 運作環境下(包括對營運者的維運、路由器、用戶主機等)，仍然可以優於 IPv4 目前 site-multihoming 所能提供的功能。(參考中華電信研究所 NICI IPv6 標準測試分組電子報)
3	問題：Homogenous Edge Network Configurations (同質邊緣網路配置)	
	對家庭用戶而言，這是電信業者最常提供給家庭用戶的方案。一個家庭內即使有多台機器，對外也是只使用同一個 IP 位址。	參考 RFC 5902，在 IPv6，link-local 位址可以被用來確保所有的家用 gateway 使用相同的 IP 位址，並提供 homogenous addresses 供支援的設備使用。
4	問題：Network Obfuscation(網路混淆)	

編號	討論	IPv6 解決方式
	大多數的網路管理人員都希望隱藏主機的詳細資訊，包括網路架構跟通訊內容。這樣的考量是基於這些主機都是其公司的私有資產，由於某些主機可能需要較高機密性，特別是很重要的主機更是希望能夠完全保密，因此網路管理在考量網路安全時，總是認為以 NAT 來保護這些設備是最恰當的方式。	可以參考 RFC 4941，利用專用介面識別元搭配亂數產生一個全球都可以識別的位址，並不定時更新資料，避免資料被收集，降低被主機資訊洩漏的風險。
5	問題：Hiding Hosts(隱藏主機)	
	對於網路管理人員來說，隱藏跟保護內部網路內的主機資訊是重要的。這些主機可能包括工作站、筆記型電腦、伺服器、特定的終端設備(印表機、掃瞄器、IP 電話、POS 系統、門禁系統)等。由於這些設備不需要對外服務，因此希望外部無法探知這些設備及資訊。 對駭客而言，對於要攻擊 NAT 內的主機，難度較高。而且駭客要知道一個 NAT 內有多少主機也較困難，即使可以藉由收集不同的封包內容去猜測跟收集不同主機的指紋資訊，但透過這些資訊要組合成可被攻擊的目標，仍舊是一件困難的事情。	對於駭客而言，他們已經設計出透過特洛伊木馬病毒來穿透 NAT 的攻擊方式。另外有一點是 NAT 不是防火牆，不少管理者把 NAT 作為一種安全防護手段，這樣已經把防火牆跟 NAT 搞混了。安全防護應該透過防火牆來執行，而非以為 NAT 可以做到防火牆相同的效果。參考 RFC 3041 的作法隨機在 IPv6 中將主機隱私資訊依據需要產生，而且僅限於有限期間內才有效。由於 IPv6 位址很多，因此有許多自由隨機化子網分配，透過這種方式，讓意圖記錄跟追蹤主機資訊的人，無法推敲出真正的主機資訊。
6	問題：Topology Hiding(隱藏拓撲)	
	隱藏網路架構圖(拓撲圖)對於網路管理人員也是很重要的，包括隱藏內部路由器及內部連接狀況。	參考 RFC 4864，作法在 RFC 3014 內有描述，主要是透過有期限限制的 IPv6 資訊，避免網路拓撲被收集跟窺探。
7	問題：Simple Security(簡單安全)	
	因為外部主機無法直接連接到 NAT 內的主機，因為 NAT 通常	透過防火牆過濾跟阻擋不安全的連線是主要解決方案，而不是

編號	討論	IPv6 解決方式
	是為一種安全機制。 但是不應該將 NAT 跟防火牆混淆，兩者是不同的。NAT 是幫忙建立內部機器與外部連線，而防火牆才是控管網路安全。	誤以為用了 NAT 就可以做到簡單安全。

(三) Intrusion Detection Systems（IDS）入侵偵測系統

針對三個開源入侵檢測系統 Snort，Suricata 和 Bro 介紹對 IPv6 的支援概況。

1. Snort

於西元 2014 年（103 年）發布的 Snort 1.6 版本後就支援檢測 IPv6 的功能，總共有 64 種與 IPv6 相關的 VRT+ET 規則，VRT rules 為 snort.org 的官方 rules，由 Sourcefire Vulnerability Research Team (VRT) 提供，每一條 rules 均經過 VRT 嚴格測試，ET rules 則為 Emerging Threats rule。

表 80、Snort 規則 IPv6 特徵值統整

編號	特徵值說明	規則數量
1	ICMPv6 protocol alerts	24
2	IPv6 protocol decode messages	24
3	Metasploit meterpreter binding	8
4	Other	8

2. Suricata

這是一套開源的入侵偵測跟入侵防禦系統。跟 Snort 使用相同規則庫，一樣有 64 種，另有一項 decoder-events.rules 檔案又提供 32 種規則，因此 Suricata 總共提供 96 種關於 IPv6 的規則。

3. Bro(Zeek)

是一套免費的開源軟體網路分析軟體。它可以用在網路入侵偵測系統，也可以對網路事件進行額外的即時分析。於西元 2012 年（101 年）發布的 0.17-8 開始支援檢測 IPv6 的功能。

十. ICP IPv4/IPv6 管理策略及安全政策

RFC 4890 主要建議在防火牆中過濾 ICMPv6 消息，為 IPv6 安全提供了最基本的防護。在設有防火牆的 IPv4 網路中，通常會阻斷大多數 ICMP 訊息的傳送，最主要原因是駭客可利用 ICMP 協定獲取網路異常原因等相關訊息，調整網路探測及攻擊方式。但在 IPv6 的環境，Neighbor Discovery(ND)協定須依據 ICMPv6 回應訊息，判斷路由器或主機是否存在，因此防火牆須允許 ICMPv6 封包通過。為防止 ICMPv6 訊息洩漏可能造成的影響，RFC 4980 針對防火牆可能需要開放的規則提出建議，這個建議就是在實際設定時，應秉持最小化原則，針對防火牆規則的來源與目的端設定限制，盡可能設定明確的 IP 範圍，不應貪圖方便而設定為 Any，介接網際網路的防火牆如有 Echo Request 及 Echo Reply 連線需求，則須進一步確認其必要性，以下是依據 RFC 4890 整理的表格。

表 81、RFC 4890 防火牆對 ICMPv6 建議設定

編號	ICMP 類型	建議處理
1	1,2,3,4,12,129,130,131,123,143,148,149,151,152,153,133,134,135,136,141,142	必須開放
2	3-Code 1,4-Code 0	通常開放
3	138,144,145,146,147	必須過濾丟棄
4	137,139,140,5-99,102,126	視需要制定是否過濾丟棄

RFC 7359 討論了雙協定下第 3 層 Virtual Private Network （VPN）tunnel 流量洩漏，並討論了可能的解決措施。由於此問題是基於路由第 3 層流量的 VPN 解決方案，因此它適用於基於 IPsec 的 VPN 隧道及 SSL / TLS VPN 隧道的解決方案。當一台主機是雙協定主機(同時啟用 IPv4 及 IPv6)，並在這台主機上安裝的 VPN 軟體不支援 IPv6 的 VPN 隧道，並且該主機連接到雙協定網路時，如果客戶端上的某些應用程序打算與目標進行通信，則客戶端通常將查詢 A 和 AAAA DNS 資源記錄(A 是對應到 IPv4 位址，AAAA 是對應到 IPv6 位址)。由於主機同時具有 IPv4 和 IPv6 連接能力，並且預期的目的地將同時具有 A 和 AAAA DNS 資源記錄，因此可能發生主機使用 IPv6 與預期的目的地進行通信。如果此時 VPN 軟體不支援 IPv6，因此 IPv6 流量將不會使用 VPN 隧道；因此，從來源主機到目的主機，它既沒有完整性也沒有機密性保護，因此有以下兩個注意事項：

(一) 如果 VPN 軟體不支援 IPv6，請在所有網路接口中禁用支援 IPv6。

(二) 如果 VPN 軟體支援 IPv6，請確保所有 IPv6 流量也通過 VPN 發送。

第二節 建立 ICP IPv4/IPv6 升級平台架構雙協定網路安全防護檢查項目清單

以下根據 ICP 業者的 IPv6 設定檢測及 ICP 業者的網路安全檢查兩個項目，分別提列網站 IPv4/IPv6 升級檢查項目清單。

一. ICP 業者的 IPv6 設定檢測

表 82、ICP 業者的 IPv6 設定檢測表

編號	測試說明	測試方法	通過條件
測試類別：主機			
CT-1	網站的 IPv6 位址可以連上(http 或 https)	◆工具：curl ◆指令： curl -v 網址 –head	Trying 顯示 IPv6 位址、出現 TCP_NODELAY set、Connected to 網址(IPv6 位址) port 443 、並顯示 successfully set certificate verify locations 出現 HTTP/2 200
測試類別：路由器			
CT-2	測試路徑上所有路由器都有 IPv6 位址	◆工具：traceroute6 ◆指令： traceroute6 根網域	顯示路徑上所有路由器 IPv6 位址
測試類別：DNS			
CT-3	網站是否正確設定 IPv6 位址	◆工具：dig ◆指令： dig aaaa 根網域 @8.8.8.8 +short	顯示測試網站 IPv6 位址
CT-4	網站使用的	◆工具：dig	顯示 DNS Server

編號	測試說明	測試方法	通過條件
	所有 DNS Server 本身要有 IPv6 位址	◆指令： for i in `dig @8.8.8.8 +short NS 根網域`; do echo -n "$i => [ipv6] "; dig aaaa $i @8.8.8.8 +short; done;	IPv6 位址
CT-5	網站使用的 DNS 其 IPv6 都可以 PING 通過	◆工具：ping6 ◆指令： ping6 根網域	成功顯示 PING 到的 IPv6 位址
CT-6	網站使用的 DNS 要設定網站根網域的 IPv6 位址	◆工具：dig ◆指令： for i in `dig @8.8.8.8 +short NS 根網域`; do echo -n "$i => [ipv6] "; dig aaaa 根網域 @$i +short; done;	顯示網站使用的 DNS 網站根網域的 IPv6 位址
測試類別：Mail Server			
CT-7	網站使用的 Mail Server 都要有 IPv6 位址，且可以連得上	◆工具：curl ◆指令： for i in `dig @8.8.8.8 +short MX 根網域`; do echo -n "$i => [ipv6] "; dig aaaa $i @8.8.8.8 +short; done;	顯示 IPv6 位址

二. ICP 業者的網路安全檢查

ICP 業者的網路安全檢查項目又可分為外網測試項目、內網測試項目及專為 IPv4 測試使用項目共三類，以下表格將對不同類別提列對應測試項目及說明。

下表為 ICP 業者的網路安全檢查表關於外網測試項目：

表 83、ICP 業者的網路安全檢查表-外網測試項目

編號	測試項目	測試工具	測試方法
測試類別：路由器			
ST-1	未經驗證或者偽照的裝置	thcsyn6	thcsyn6 [-AcDrRS] [-p port] [-s sourceip6] interface target port
ST-2	未經驗證或者偽照的裝置	exploit6	exploit6 interface destination [test-case-number]
ST-3	DDoS 攻擊（ICMPv6）	fuzz_ip6	fuzz_ip6 [-x] [-t number | -T number] [-p number] [-IFSDHRJ] [-X|-1|-2|-3|-4|-5|-6|-7|-8|-9|-0 port] interface unicast-or-multicast-address [address-in-data-pkt]
ST-4	Ping of Death（PoD）	frag6	frag6 -i [interface] --frag-id-policy -d [destination]
ST-5	網路掃描	flow6	flow6 -i [interface] --flow-label-policy -d [destination] -v
測試類別：網站主機			
ST-6	DDoS 攻擊（Smurf 攻擊）	implementation6	implementation6 [-p] [-s sourceip6] interface destination [test-case-number]
ST-7	DDos 攻擊（Duplicate Address Detection）	flood_mld6	flood_mld6 interface
ST-8	Upper Layer Header 的攻擊	flood_mld26	flood_mld26 interface
ST-9	Atomic Fragment 攻擊	denial6	denial6 interface destination test-case-number

以下為 ICP 業者的網路安全檢查表關於內網測試項目：

表 84、ICP 業者的網路安全檢查表-內網測試項目

編號	測試項目	測試工具	測試方法
測試類別：路由器			
ST-10	DDoS 攻擊（Router Advertisement）	alive6	inject_alive6 [-ap] interface
ST-11	DDoS 攻擊（neighbor advertisements）	alive6	inject_alive6 [-ap] interface
ST-12	DDoS 攻擊（MLD reports）	redir6	redir6 interface victim-ip target-ip original-router new-router [new-router-mac] [hop-limit]
ST-13	DDoS 攻擊（MLDv2 reports）	dos-new-ip6	dos-new-ip6 interface
ST-14	中間人攻擊	fake_mipv6	fake_mipv6 interface home-address home-agent-address care-of-address
ST-15	DDoS 攻擊（unknown options）	fake_advertiser6	fake_advertise6 [-DHF] [-Ors] [-n count] [-w seconds] interface ip-address-advertised [target-address [mac-address-advertised [source-ip-address]]]
測試類別：網站主機			
ST-16	DDoS 攻擊（Smurf 攻擊）	implementation6d	implementation6d interface
ST-17	滲透測試	flood_dhcpc6	flood_dhcpc6 [-n|-N] [-1] [-d] interface [domain-name]
ST-18	未經驗證或者偽照的裝置	toobig6	toobig6 [-u] interface target-ip existing-ip mtu [hop-limit]
ST-19	未經驗證或者偽照的裝置	fake_dns6d	fake_dns6d interface ipv6-address [fake-ipv6-address [fake-mac]]
ST-20	未經驗證或者偽照的裝置	fake_dnsupdate6	fake_dnsupdate6 dns-server full-qualified-host-dns-name ipv6address

編號	測試項目	測試工具	測試方法
測試類別：作業系統			
ST-21	CVE-2003-0429 Ethereal OSI 解析緩衝區溢位漏洞	mitm6	mitm6.py [-h] [-i INTERFACE] [-l LOCALDOMAIN] [-4 ADDRESS] [-6 ADDRESS] [-m ADDRESS] [-a] [-v] [--debug] [-d DOMAIN] [-b DOMAIN] [-hw DOMAIN] [-hb DOMAIN] [--ignore-nofqdn]
ST-22	CVE-2004-0257 OpenBSD ICMPv6 處理遠程 DDoS 攻擊漏洞	fake_mld6	fake_mld6 [-l] interface add|delete|query [multicast-address [target-address [ttl [own-ip [own-mac-address [destination-mac-address]]]]]]
測試類別：防火牆			
ST-23	DDoS 攻擊（TCP-SYN）	fake_mld26	fake_mld26 [-l] interface add|delete|query [multicast-address [target-address [ttl [own-ip [own-mac-address [destination-mac-address]]]]]]
ST-24	網路掃描	fake_mldrouter6	fake_mldrouter6 [-l] interface advertise|solicitate|terminate [own-ip [own-mac-address]]
ST-25	基本設定	fake_router6	fake_router6 [-HFD] interface network-address/prefix-length [dns-server [router-ip-link-local [mtu [mac-address]]]]
ST-26	基本設定	flood_router6	flood_router6 [-HFD] interface
測試類別：其他			
ST-27	DDoS 攻擊	flood_advertise6	flood_advertise6 [-k | -m mac] interface [target]
ST-28	未經驗證或者偽照的裝置	ndpexhaust26	ndpexhaust26 [-acpPTUrR] [-s sourceip6] interface target-network
ST-29	未經驗證或者偽照的裝置	parasite6	parasite6 [-lRFHD] interface [fake-mac]
ST-30	安全評估工具（ flow label）	smurf6	smurf6 interface victim-ip [multicast-network-address]
ST-31	掃描工具	rsmurf6	rsmurf6 interface victim-ip

以下為 ICP 業者的網路安全檢查表關於 IPv4 測試項目：

表 85、ICP 業者的網路安全檢查表-IPv4 測試項目

編號	測試項目	測試工具	測試方法
測試類別：路由器			
ST-32	中間人攻擊	Arpspoof	arpspoof -i [Network Interface Name] -t [Victim IP] [Router IP]
測試類別：防火牆			
ST-33	DDoS 攻擊	hping3	hping3 --traceroute -V -1 網站
ST-34	中間人攻擊	ettercap	圖形化介面操作
ST-35	DDoS 攻擊, 中間人攻擊	Evil FOCA	圖形化介面操作

第三節　輔導至少 2 家 ICP 業者升級 IPv4/IPv6 雙軌連網服務

本項工作將針對 ICP 業者如何升級支援 IPv4/IPv6 雙軌連網服務，主要軟硬體升級及設定方法，集結成輔導手冊，並以實際輔導 2 家 ICP 業者升級作為佐證。本次計畫成功輔導的 ICP 業者為〝旅遊咖〞及〝寵物迷〞。以下將就各項工作成果說明：

一. 輔導手冊

有關 ICP 業者升級 IPv4/IPv6 雙軌連網服務輔導手冊，詳細內容請參閱附錄九。

二. ICP 業者升級 IPv4/IPv6 雙軌連網服務

ICP 業者升級 IPv4/IPv6 雙軌連網服務，工作內容將分以下項目進行：

(一) 整理網站業者環境架構(包括網路環境、設備、主機、系統、，資料庫及程式碼等)

(二) 網路環境調整(Firewall、Router、Load Balance、DNS)

(三) 網站環境調整(作業系統、資料庫及程式碼)

(四) 安全策略跟規範調整

(五) 官網通過 IPv4/IPv6 檢查清單

三. 旅遊咖升級 IPv4/IPv6 雙軌連網服務

旅遊咖網站升級 IPv4/IPv6 雙軌連網服務的頁面包含如下表所示：

表 86、旅遊咖網站升級 IPv4/IPv6 雙軌連網服務的頁面

編號	網站頁面	支援 IPv6
1	首頁	是
2	搜尋首面	是
3	註冊頁面	是
4	登入頁面	是
5	會員頁面	是
6	加入訂單頁面	是
7	最新消息頁面	是
8	旅行社評價頁面	是

以下 2 個圖例提列旅遊咖網站〝首頁〞及〝搜尋首面〞頁面，驗證旅遊咖網站升級 IPv4/IPv6 雙軌連網服務的測試畫面，其餘畫面及旅遊咖網站升級輔導相關資訊，請參閱附錄七。

圖 100、驗證旅遊咖網站首頁支援 IPv6

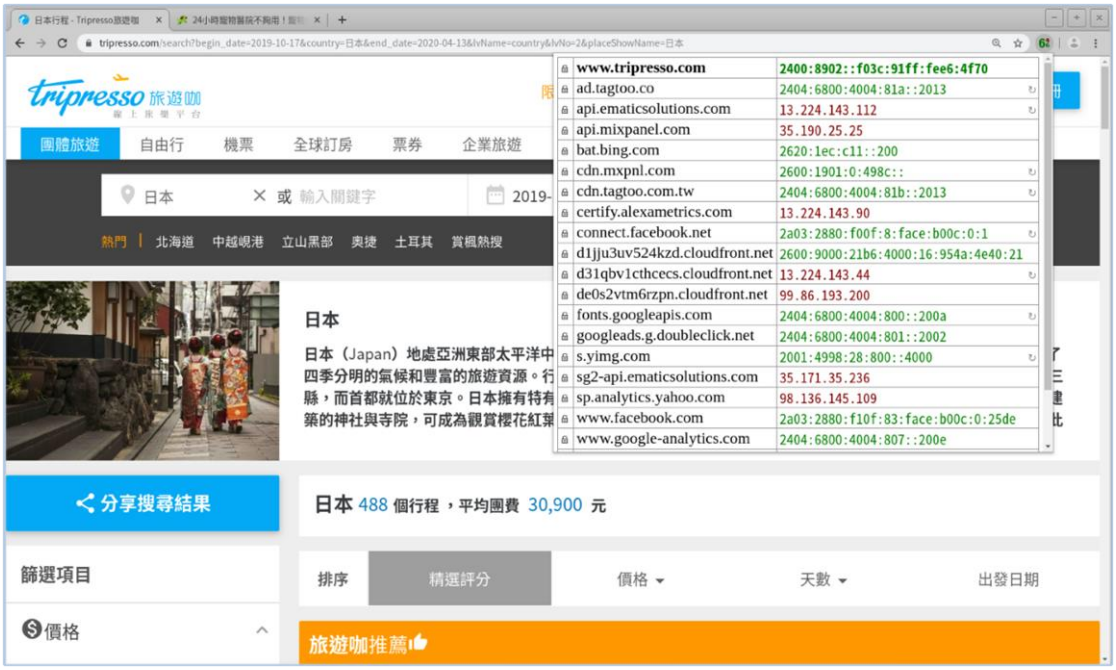

圖 101、旅遊咖搜尋頁面

本次計畫執行除輔導旅遊咖網站業者進行升級支援 IPv4/IPv6 雙軌服務之外，並對網站升級後進行外網安全檢查測試，測試項目依照上一項目關於 ICP 業者的網路安全檢查表-外網測試項目做檢測，測試結果如下表所列：

表 87、旅遊咖 IPv6 網路安全檢查表

編號	測試工具	輸入指令	測試結果
ST-1	thcsyn6	thcsyn6 eth0 2400:8902::f03c:91ff:fea2:a133 443	通過
		thcsyn6 eth0 2400:8902::f03c:91ff:fea2:a133 80	通過
ST-2	exploit6	exploit6 eth0 2400:8902::f03c:91ff:fea2:a133	通過
ST-3	fuzz_ip6	fuzz_ip6 -xIFSDHRJ eth0 2400:8902::f03c:91ff:fea2:a133	通過
ST-4	frag6	frag6 --frag-type atomic -d 2400:8902::f03c:91ff:fea2:a133 -v	通過
		frag6 --frag-reass-policy -d	通過

編號	測試工具	輸入指令	測試結果
		2400:8902::f03c:91ff:fea2:a133 -v	
ST-5	flow6	flow6 -d 2400:8902::f03c:91ff:fea2:a133 -i eth0 -W	通過
ST-6	implementation6	implementation6 eth0 -s sourceip6 2400:8902::f03c:91ff:fea2:a133	通過
ST-7	flood_mld6	flood_mld6 eth0 2400:8902::f03c:91ff:fea2:a133	通過
ST-8	flood_mld26	flood_mld26 eth0 2400:8902::f03c:91ff:fea2:a133	通過
ST-9	denial6	denial6 eth0 2400:8902::f03c:91ff:fea2:a133 1	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 2	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 3	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 4	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 5	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 6	通過
		denial6 eth0 2400:8902::f03c:91ff:fea2:a133 7	通過

由上表的測試結果可以發現，旅遊咖的資訊安全檢查項目，在外網測試部分皆有通過。關於 ICP 業者的網路安全檢查表-內網測試項目及 IPv4 測試項目，因測試內容牽涉到公司營業機密及安全考量而沒有進行測試。

四. 寵物迷升級 IPv4/IPv6 雙軌連網服務

寵物迷網站升級 IPv4/IPv6 雙軌連網服務的頁面包含下表所示內容：

表 88、寵物迷網站升級 IPv4/IPv6 雙軌連網服務的頁面

編號	網站頁面	支援 IPv6
1	首頁	是
2	搜尋首面	是
3	文章頁面	是

以下 2 個圖例提列寵物迷網站〝首頁〞及〝文章頁面〞內容，驗證寵物迷網站升級 IPv4/IPv6 雙軌連網服務的測試畫面，其餘畫面及寵物迷網站升級輔導相關資訊，請參閱附錄七。

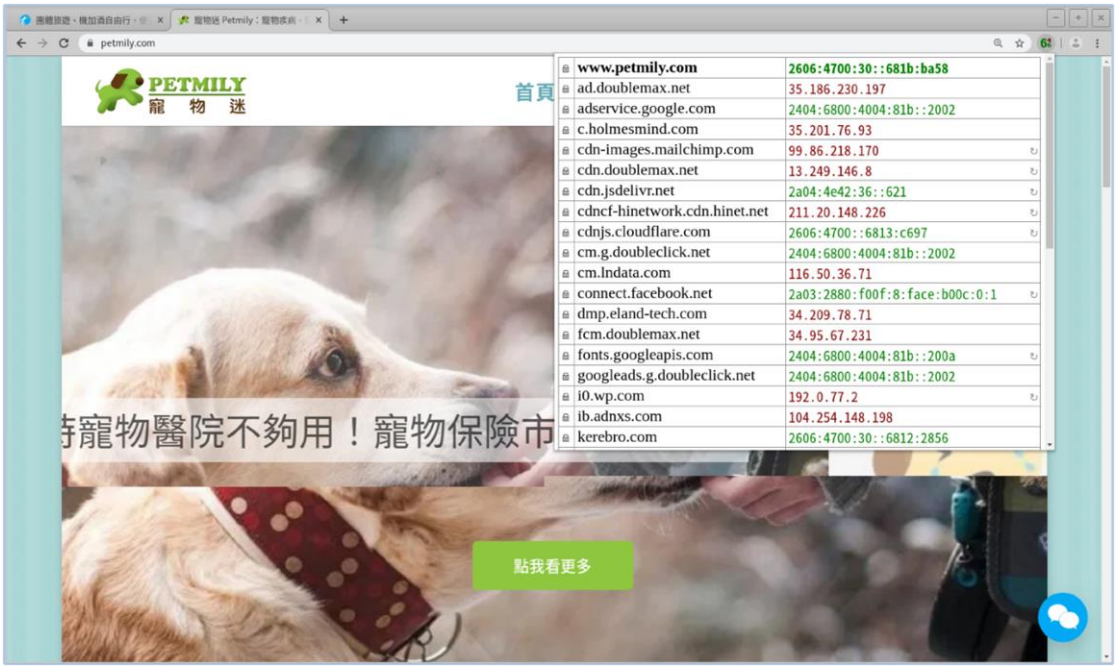

圖 102、驗證寵物迷網站首頁支援 IPv6

圖 103、寵物迷文章頁面

下表為輔導寵物迷網站業者進行升級支援 IPv4/IPv6 雙軌服務，針對網站升級後所進行外網安全檢查測試，測試結果如下所示：

表 89、寵物迷 IPv6 網路安全檢查表

編號	測試工具	輸入指令	測試結果
ST-1	thcsyn6	thcsyn6 eth0 2606:4700:30::681b:ba58 80	通過
		thcsyn6 eth0 2606:4700:30::681b:bb58 80	通過
		thcsyn6 eth0 2606:4700:30::681b:ba58 443	通過
		thcsyn6 eth0 2606:4700:30::681b:bb58 443	通過
ST-2	exploit6	exploit6 eth0 2606:4700:30::681b:ba58	通過
		exploit6 eth0 2606:4700:30::681b:bb58	通過
ST-3	fuzz_ip6	fuzz_ip6 -xIFSDHRJ eth0 2606:4700:30::681b:ba58	通過
		fuzz_ip6 -xIFSDHRJ eth0 2606:4700:30::681b:bb58	通過
ST-4	frag6	frag6 --frag-type atomic -d	通過

編號	測試工具	輸入指令	測試結果
		2606:4700:30::681b:ba58 -v	
		frag6 --frag-type atomic -d 2606:4700:30::681b:bb58 -v	通過
ST-5	flow6	flow6 -d 2606:4700:30::681b:ba58 -i eth0 -W	通過
		flow6 -d 2606:4700:30::681b:bb58 -i eth0 -W	通過
ST-6	implementation6	implementation6 eth0 -s sourceip6 2606:4700:30::681b:ba58	通過
		implementation6 eth0 -s sourceip6 2606:4700:30::681b:bb58	通過
ST-7	flood_mld6	flood_mld6 eth0 2606:4700:30::681b:ba58	通過
		flood_mld6 eth0 2606:4700:30::681b:bb58	通過
ST-8	flood_mld26	flood_mld26 eth0 2606:4700:30::681b:bb58	通過
		flood_mld26 eth0 2606:4700:30::681b:ba58	通過
ST-9	denial6	denial6 eth0 2606:4700:30::681b:ba58 1	通過
		denial6 eth0 2606:4700:30::681b:ba58 2	通過
		denial6 eth0 2606:4700:30::681b:ba58 3	通過
		denial6 eth0 2606:4700:30::681b:ba58 4	通過
		denial6 eth0 2606:4700:30::681b:ba58 5	通過
		denial6 eth0 2606:4700:30::681b:ba58 6	通過
		denial6 eth0 2606:4700:30::681b:ba58 7	通過
		denial6 eth0 2606:4700:30::681b:bb58 1	通過
		denial6 eth0 2606:4700:30::681b:bb58 2	通過
		denial6 eth0 2606:4700:30::681b:bb58 3	通過
		denial6 eth0 2606:4700:30::681b:bb58 4	通過
		denial6 eth0 2606:4700:30::681b:bb58 5	通過
		denial6 eth0 2606:4700:30::681b:bb58 6	通過
		denial6 eth0 2606:4700:30::681b:bb58 7	通過

由上表的測試結果可以發現，寵物迷的資訊安全檢查項目，在外網測試部分皆有通過。關於 ICP 業者的網路安全檢查表-內網測試項目及 IPv4 測試項目，因測試內容牽涉到公司營業機密及安全考量而沒有進行測試。

第六章 ICP IPv4/IPv6 雙協定網路安全防護技術人才培育教育訓練

第一節 蒐集 IPv4 及 IPv6 平台架構雙協定網路安全防護相關資訊製作教學內容

一. IPv4/IPv6 雙軌運作概念介紹

IP（Internet protocol）是電腦在網際網路上用來辨認作為彼此溝通的方法， IP 位址就像是每家都有的門牌地址，網際網路經過三十多年的發展，原本的網際網路協定 IPv4 已經面臨挑戰及資源不足的問題，因為沒有足夠的 IPv4 位址來提供新型態網路服務，而影響既有網路服務無法擴展。而 IPv6 的制定是為解決 IPv4 所產生的問題。

下表為針對 IPv4 位址枯竭所提出因應建議策略分析表：

表 90、IPv4 位址枯竭因應建議策略

因應措施	開源(回收、移轉)	節流（使用 NAT）	部署 IPv6
優勢 (Strengths)	無技術門檻與實施費用。	屬於現有成熟技術，可大量節省 IP 位址的使用，花費比部署 IPv6 相對便宜。	擁有大量的位址，可根本解決位址不足問題。
劣勢 (Weaknesses)	無確實可行的方法(回收或移轉均無好的實行經驗)，也非長期可	NAT 本身對一些應用的連線有所限制，每一個網路使用者	對於大量實施在一些技術上仍有顧慮（如設備能力不

因應措施	開源(回收、移轉)	節流 (使用 NAT)	部署 IPv6
	行政策。	需要的連線數正快速增加中，減少可共享一個 IP 的使用者數。	足、安全性尚未完整考量)且部署費用相對較高。
機會 (Opportunities)	有不少可回收位址(約有 50 個/8 未出現在 BGP routing table 中、36 個/8 是歷史或特殊用途位址)。	短期內有可能是唯一便宜可行的技術。	唯一長期的解決方案，極有可能是未來會被全面採用的協定。
威脅 (Threats)	合法擁有的 IP 位址要回收不容易，需擁有者願意配合。	非長期解決方案且對於大量的使用者、電信等級的 NAT 均仍有待市場考驗。	尚無明顯看到 IPv6 使用者市場，讓大部份的公司採觀望態度。

相對於 IPv4，IPv6 發展之優勢如下：

◆ 足夠的位址空間：IPv4 位址長度 32 為位元，而 IPv6 位址長度 128 為位元，可提供更多位址空間。

◆ 彈性的連網機制(Plug & Play)：支援隨插即用的特性，更適合物聯網設備發展及使用。

◆ 安全機制：IPv4 無法在基本網路層提供安全的加密通訊。IPSec 直接可以鑲嵌在 IPv6 的封包中，在 IPv6 中實作 IPsec 有其必要性。大多數的 IPv6 相容設備都可加密通訊內容。

◆ QoS 功能增強：IPv6 提供順暢、有秩序的網路傳輸將網路資源分級與分類，通過流量控管保持網路傳輸的順暢。

◆ 強化的 Mobility 與 Multicast 能力等。

下表為針對 IPv4 及 IPv6 的特性比較：

表 91、IPv4 及 IPv6 的比較表

版本	IPv4	IPv6
位址空間	2^32 ＝4,294,967,296	2^128 ≒3.4*10^38
ICMP 發放方式	以廣播（Broadcast）方式	以群播（Multicast）方式
QoS 策略	推測遺失資料與暫存器	資源保留與優先等級
協定的可擴充性	沒有彈性（最多提供 1 個 Option 欄位的擴充）	較有彈性（具有延伸標頭）
IPSec 的支援	本身沒有支援，需額外設定	將 IPSec 納入本身協定中
Plug and Play	需透過 DHCP 分配 IP	具有 Statefull（透過 DHCPv6）與 Stateless（自動組態）分配 IP
繞回位址	127.0.0.1	::1
表示方式	十進位表示，以點分隔	十六進位表示，以冒號分隔

二. IPv4/IPv6 雙軌環境建置概述

IPv6 的實現必須透過既有 IPv4 設備升級，來達成提供 IPv6 網路服務的方法，慢慢過渡至 IPv6，才能以最少的代價實現 IPv6 網路升級。以下為三種 IPv4 與 IPv6 轉換技術，分別是：

- ◆ 雙軌協定架構（Dual-Stack）
- ◆ 隧道技術（Tunneling）
- ◆ 網路位址與協定轉換（NAT-PT，Network Address Translation - Protocol Translation）

IPv4 與 IPv6 雙軌協定架構（Dual-Stack），即是在同一條線路上同時提供 IPv6 及 IPv4 的通訊協定，這是目前最為推薦的方案。下圖為 IPv4/IPv6 雙軌模式示意圖：

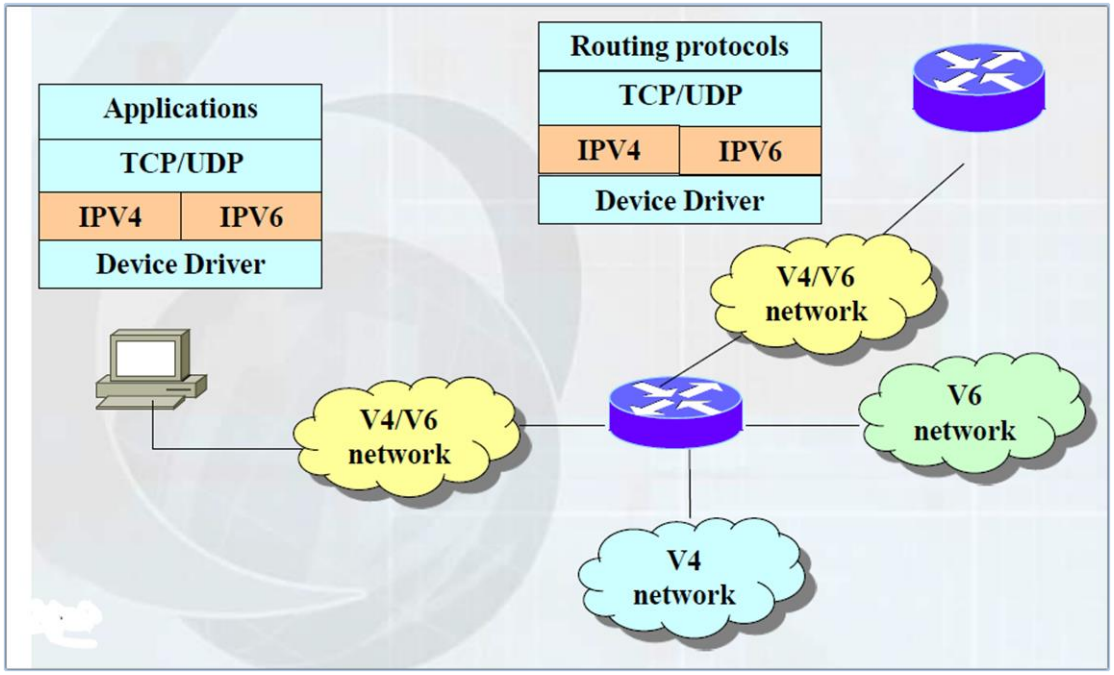

圖 104、IPv4/IPv6 雙軌模式示意圖

三. IPv4/IPv6 雙軌網路環境建置（Router、Firewall、Load Balance）

IPv4 網路位址核發方式主要有固定位址配置及動態位址配置兩種。固定位址配置需要手動設定，主要應用於伺服器主機及網路設備，動態位址配置大多透過 DHCP 協定（Dynamic Host Configuration Protocol），由 DHCP 伺服器進行位址核發。

IPv6 網路除保留手動設定固定位址的機制外，另提出無狀態定址自動配置（Stateless Address Autoconfiguration，SLAAC）的全新技術，可直接由路由器直接核發 Prefix 給用戶端主機，不需要再透過 DHCP 伺服器，主機得到 Prefix 後將結合自動產生的 Host ID 而組成 IPv6 位址。

透過 SLAAC 技術核發 IPv6 Prefix 時不會同時提供 DNS 伺服器位址，雖然後來修訂的 SLAAC RDNSS 技術已解決這個問題，但系統支援程度尚未普及。變通的方案是結合 DHCPv6 伺服器來提供 DNS 資訊，稱為 Stateless DHCPv6。還有一種方式是將位址配置及 DNS 伺服器位址的提供，都由 DHCP 負責，稱為 Stateful DHCPv6，這個方式與傳統 IPv4 的 DHCP 相近，但仍有部分差異。

IPv6 位址自動核發技術在 DNS 伺服器位址提供方面較為複雜，甚至部分作法可能無法提供 DNS 資訊給用戶端主機。在雙協定網路架構下，主機透過 IPv4 DNS 就可以查詢解析網址的 IPv6 位址，沒有 IPv6 DNS 伺服器也不會造成問題。下表為針對 IPv4 及 IPv6 的位址配發方式比較：

表 92、IPv4 及 IPv6 的位址配發方式比較表

派址方式	預設閘道	Prefix 指派	Host ID 指派	DNS 位址指派	說明	適用環境
人工配置位址	手動設定	手動設定	手動設定	手動設定	穩定可靠、較無資安疑慮，但無彈性、設定麻煩	伺服器及網路設備
SLAAC + RDNSS	RA 指派	RA 指派	EUI-64 或亂數法自動產生	RA 指派	簡單方便，但無法管理位址指派原則及使用紀錄，但大部分作業系統尚未支援 RDNSS	物件連網應用服務
Stateless DHCPv6	RA 指派	RA 指派	EUI-64 或亂數法自動產生	DHCP 指派	簡單方便，但無法管理位址指派原則及使用紀錄，另外，Windows XP 不支援 DHCPv6(可外掛)	家用網路環境
Stateful DHCPv6	RA 指派	DHCP 指派	DHCP 指派	DHCP 指派	可管理位址指派原則及使用紀錄，但 Prefix 與 Gateway 分由 DHCP 及 RA 指派，增加偵錯難度，另外，Windows XP 不支援 DHCPv6(可外掛)	辦公室網路環境

防火牆的設置可分為二種模式分別為：

(一) 透通模式（Transparent Mode）

機關 IPv4 防火牆位置如設置於 ISP 路由器與內部 NAT 路由器之間，並採用 Transparent 透通模式進行運作，內部路由器最少有三個介面，一個與防火牆介接，一個與內部一般使用者連接，一個與伺服器區塊連接。

採用本架構可以限制外來的訪客對於內部網路的存取，並且在不改變內部原有的設備設定，以提供內部使用者安全的 IPv4/IPv6 對外存取服務。內部使用者若採用 IPv6 Public IP address，不再經

由 NAT 或 PAT 位址轉換，可直接提供 IPv6 接取服務。防火牆可抵擋外部 IPv4/IPv6 對於內部使用者的所有連線訪問。

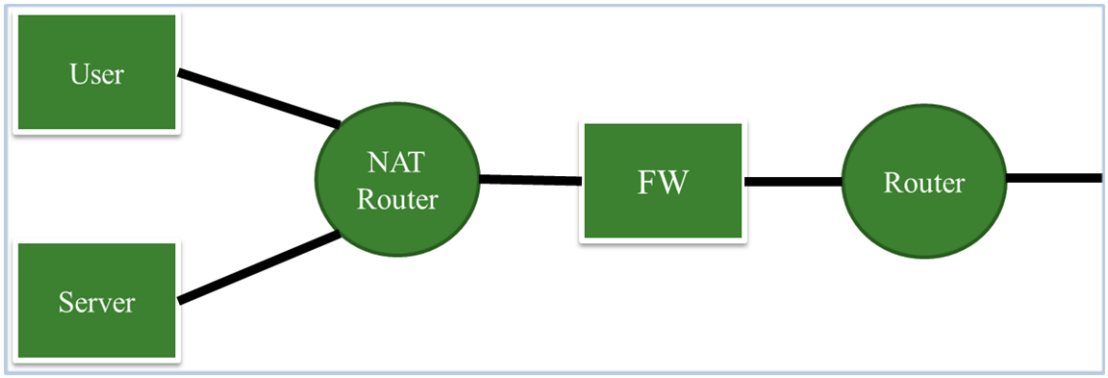

圖 105、防火牆透通模式示意圖

(二) 路由模式（Route Mode）

機關 IPv4 防火牆位置如設置於 ISP 路由器與內部路由器之間，並採用 Route Mode 路由模式進行運作，防火牆最少有三個介面，一個與外部 ISP 業者介接，一個與內部路由連接，一個與 DMZ 伺服器區塊連接。採用本架構可以限制外來的訪客對於內部網路的存取，並且限制 DMZ 區對於內部使用者的存取，可以提供內部使用者安全的 IPv4/IPv6 對外存取服務。內部使用者若採用 IPv6 Public IP address，不再經由 NAT 或 PAT 位址轉換，可直接提供 IPv6 接取服務。防火牆可抵擋外部 IPv4/IPv6 對於內部使用者的所有連線訪問。

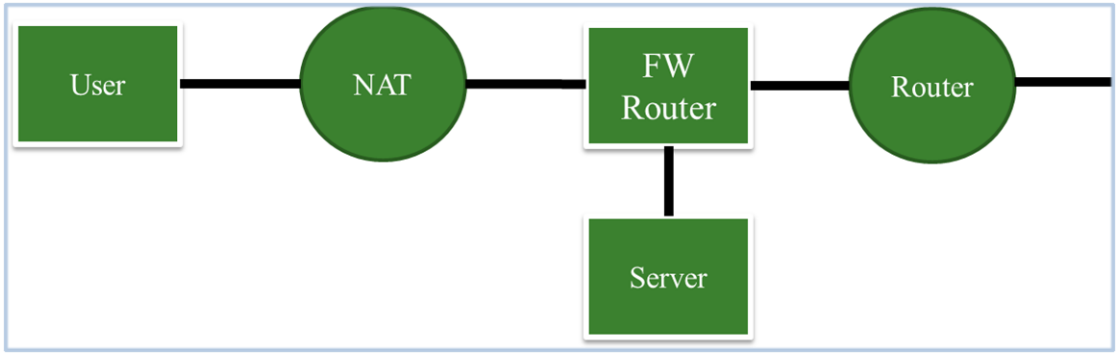

圖 106、防火牆路由模式示意圖

四. 網路升級流程步驟和檢查項目清單

升級清查作業須從服務系統角度出發，逐一填寫對外提供服務的應用服務系統，其次應依據各服務系統逐一清查相關之軟硬體設備，包括伺服器、服務系統或軟體、基礎網路設備及其他相關設備等，參考步驟如下：

◆ 評估現有網路環境：

網路設備種類甚多，唯有釐清設備功能，才能規劃 IPv6 升級優先順序，其中需調查項目包含： 技術人員 IPv6 相關能力調查、資訊應用服務系統（包含自行開發、委外設計或購買套裝軟體）、網路架構圖（包含區域網路、DMZ、連外網路、接取網路、核心網路、機房等）、硬體設備（包含設備使用年限與 IPv6 支援程度）及評估現有網路設備之屬性等。

◆ 規劃 IPv6 升級策略：

根據上述調查結果，可大致掌握現有網路設備特性與屬性。接著需制定 IPv6 導入之網路範疇與時程，三個升級重要參考指標為：降低導入成本、規劃重要網路應用服務升級及規劃升級時程與順序。

◆ 評估依據：

建議以 IPv4/IPv6 雙協定（Dual Stack，同時支援 IPv4 與 IPv6）為首要目標，IPv6 部署先由骨幹單一網路節點下手，逐步擴增支援 IPv6 功能的網路節點，最後連接成 IPv4/IPv6 網路，並達到全面性的 IPv6 網路佈建。

◆ 網路升級檢測：

完成升級後可使用 https://www.gsnv6.tw/inventory/checkservicepub.cgi 或 http://test-ipv6.com/ 做為升級檢測工具。

圖 107、行政院網際網路通訊協定升級推動方案 IPv6 檢測畫面

五. 網站升級 IPv6 設定

有關作業系統IPv6建置示範(Centos7, Ubuntu18, Windows 2016)、資料庫 IPv6 調整示範（MySQL5, Windows SQL server 2017）、網站伺服器 IPv6 調整示範(IIS8, Apache2, Nginx)及程式檢查(PHP, ASP.NET)等資訊，詳細請參考附錄三教材內容。

六. IPv4/IPv6 雙軌環境下資訊安全規劃概述

常見網路安全管理機制有三類：

◆ 防火牆：

防火牆以提供網路封包篩選過濾為主要功能，其做法是依據預設好的規 則，對流入或流出的 IP 封包是否放行進行管制，以決定是否允許或阻止網路連線存取的行為。封包過濾通常只檢查封包的表頭（Header），不會檢查資料段的內容，可以檢查的項目包括來源 IP 位址、目的 IP 位址、協定種類（TCP、UDP 等）、TCP 或 UDP 的來源埠（Source Port）、TCP 或 UDP 的目的埠（Destination Port）、以及 ICMP 的訊息代碼等。

◆ NetFlow 流量監測：

Netflow（Network Flow）是一套網路流量監測方式，一個 Flow 代表一個來源 IP 位址和目的 IP 位址之間傳輸的單向流量，且所有封包具有相同傳輸層的來源及目的通訊埠編號（Port Number）。Netflow 以網路介面為單位呈現分析的結果，包含各服務流量的資訊、各 IP 位址的流量資訊，甚至各種傳輸協議之流量高低排序…等，並可以列出疑似受病毒感染或被植入惡意程式的電腦所使用的 IP 列表。

◆ DPI 資安防禦系統：

DPI 資安防禦系統可以判斷封包所屬的服務類型，例如是否屬於 YouTube 等常見的服務流量。也可以偵測出典型的殭屍病毒，例如網路聊天感染（Internet Relay Chat Bot，IRC Bot）等安全相關的病毒程式，並可以將相關資訊儲存於資料庫中，再藉由網頁介面呈現統計資料。

大部分 IPv4 常見的攻擊已可藉由成熟的防禦機制過濾出可疑封包，或是經由一些網路技術而避免。IPv6 則從網路的設計上，提供比 IPv4 更完整的網路安全機制，說明如下：

◆ 預設啟動 IP 安全性協定（Internet Protocol Security，IPSec）：

雖然 IPv4 也支援 IPsec，但為選擇性使用，而在 IPv6 由 RFC4301 指定所有網路節點都必須使用 IPsec。

◆ Psec 包含 Authentication Header（AH）和 Encapsulating Security Payload （ESP），以及 Internet Key Exchange（IKE）等技術：

這些技術在 IPv6 都提供更好的設計，可以防止封包欺騙、偽造、修改及重播等攻擊。

◆ 使用鄰居探索（Neighbor Discovery，ND）進行位址自動設定：

不同於 IPv4 於資料鏈結（Link-Layer）層以 ARP-RARP 找出主機位址，ND 於網路層 (Network-layer)操作減少欺騙主機的可能。

◆ 更多的位址空間（Large address space）：

不同於 IPv4 掃描一個 Class C 僅需 4 分鐘，由於 IPv6 一個子網是由 64 位元組成，整個掃描則需耗時達 584,942,417,35 年。

IPv4/IPv6 雙協定共存的安全議題：

◆ 雙堆疊相關安全性問題：

例如不適當的防火牆攔截、不穩定的 DNS 區 域記錄等，因此在網路建立前就須審慎規劃。

◆ ICMPv6 安全性問題：

IPv6 網路存在封包被攔截的可能，由於採用開放式路由廣播訊息（Router Advertisement，RA），以協調網域中主機自動獲取位址，可能發生節點假扮為路由設備並發出錯誤的 RA 廣播訊息。

◆ 標頭操作相關議題：

由延伸性標頭（Extension header）及 IPSec 的使用可以抵擋掉大部分攻擊種類，然而，由於 EH 須被整個網路堆疊進行處理，很長的延伸性表頭及大封包可能被利用來癱瘓某些特定節點（例如防火牆），或是假扮為攻擊，因此，最好的方式是過濾掉不支援的服務流量。

◆ Spoofing 議題：

欺騙技術仍然可能發生在 IPv6 網路中，但由於 Neighbor Discovery，Spoofing 欺騙的位址範圍僅侷限在內部網域。

◆ Flooding 議題：

IPv6 位址不使用廣播位址已大幅減少攻擊的可能性，但多點位址傳送的位址仍然是問題，最主要的防範方式仍為過濾不存在服務之流量。

◆ 移動性 Mobility：

移動性為 IPv6 的新特色，該協定是一複雜方程式，利用兩種類別的位址─真實位址（Real address）和移動位址（Mobile address），由於此種網路的特性加上暫時性的移動位址可能暴露而成為 欺騙攻擊，這需要特別安全性量測，並且網路管理者須全面了解設定。

七. IPv4/IPv6 雙軌環境之資訊安全軟體與硬體設定

◆ 防火牆：

防火牆支援 IPv6 後可參考 IPv4 既有規則設定 IPv6 的過濾方式，再依據監控蒐集的 IPv6 流量資訊進行觀察，逐步補足 IPv6 的防禦

規則。ICMPv6 在 IPv6 網路扮演很重要的角色，在 IPv4 網路裡大部分的 ICMP 都會被關掉，需選擇適當的項目開放。

◆ NetFlow 流量監測：

升級路由器的 iOS 至支援 NetFlow version 9，以提供 IPv6 的流量統計資料，Netflow 分析軟體（如 Netflow Analyzer）也要升級到支援 IPv6。建議以不同時間排程將 IPv6 與 IPv4 流量資訊的抓取與分析時間錯開，以降低設備負載度。每天依據服務類別統計流量資訊，例如依據 Inbound、Outbound、SSH 連線、FTP 連線、網路芳鄰、遠端桌面連線、遠端程序呼叫、Proxy、Mail、ICMP 等進行統計。

◆ DPI 資安防禦系統：

DPI 主要目的為觀察封包 Payload 並比對出可疑流量，IPv6 流量 Payload 的比對方式與 IPv4 並無不同，目前持續累積足夠的 IPv6 可疑流量特徵（Signature），建議可配合 Netflow 的統計，針對異常流量進行 Payload 的觀察，以蒐集建立異常流量的特徵值數據庫。

IPv6 用戶端位址的自動核發機制主要為 SLAAC（包含 SLAAC RDNSS 及 SLAAC+Stateless DHCPv6）以 Stateful DHCPv6，建議優先選用 Stateful DHCPv6 的位址核發機制，可以如同 IPv4 DHCP 的管理方式，記錄 IPv6 位址的核發記錄，並控管位址的核發原則，例如依據 MAC 位址綁定 IPv6 位址，或依據 MAC 位址管制是否核發 IPv6 位址。

如果選用 SLAAC 機制，則只能依據 Prefix 追蹤到相關的區域網路，雖然藉由 EUI-64 運算法可從 IPv6 位址反算出 MAC 位址，但用戶端

可設定不使用 EUI-64，MAC 位址也可以手動變造，並不能保證能找出特定 IPv6 位址的使用者。所以在 SLAAC 的機制下，要責成每個區域網路的連線單位自行負擔/64 網段的資安管理責任。

八. IPv4/IPv6 雙軌環境下資訊安全檢查項目清單（網路環境、作業系統、網站、資安設備）

在進行 IPv4/IPv6 雙軌環境網路架構規劃時，建議網路進行升級的執行順序為：

(一) 核心層（Core Layer）：

1. 環境：骨幹網路（Core Network, Backbone）。
2. 用途：負責運輸大量的網路訊務，並且達到快速與可靠的服務。
3. 設備：對外 ISP 連接之路由器，如 ATM Switch、MPLS Switch、Core Router…等。

(二) 分配層（Distribution layer）：

1. 環境：接取網路（Edge Network）。
2. 用途：負責做額外判斷網路訊務封包，提供 Routing、Network Policy （如 Security、Filter、QoS…等）服務。
3. 設備：Layer 3 Switch、Firewall…等。

(三) 接取層（Access Layer）：

1. 環境：DMZ（外部 WWW/DNS/E-mail 伺服器）、Server Farm（內部使用伺服器）、辦公室區域網路。

2. 功能：負責提供可靠的網路接取給終端設備或重要的 Content 和網路應用服務，提供 Switching、Access Control（VLAN Tagging…等）。
3. 設備：Layer 3 Switch（VLAN）、Layer 2 Switch（VLAN）、Wireless Router、PCs、Servers、Printers…等。

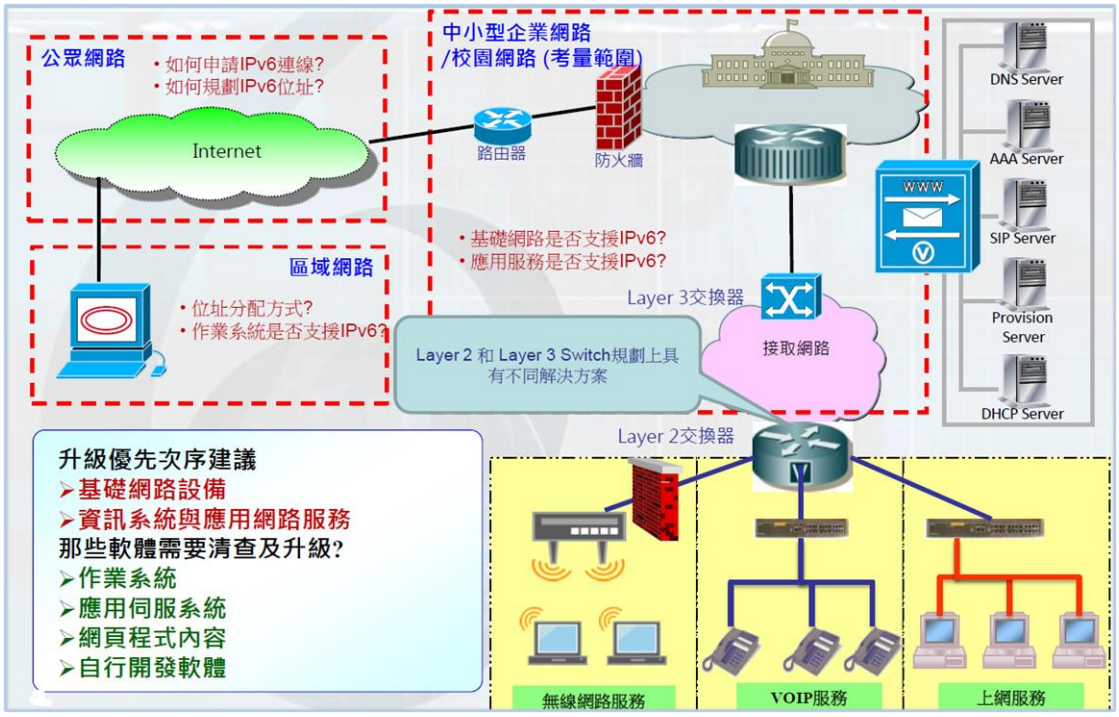

圖 108、IPv6 網路升級考量架構

ICP IPv4/IPv6 雙協定網路安全防護技術人才培育教育訓練課程教材，詳細請參考附錄三。

第二節 規劃 5 場 IPv6 教育訓練課程培育 IPv6 人才

有關 IPv6 教育訓練課程的教材內容簡介如上所述，課程大綱如下表所列：

表 93、「ICP IPv4IPv6 雙協定網路安全防護技術人才培訓教育訓練」課程大綱

時間	課程內容
08:30-09:00	報到
09:00-10:20	● IPv4/IPv6 雙軌運作概念介紹 ● IPv4/IPv6 雙軌環境建置概述 ● IPv4/IPv6 雙軌網路環境建置（Router, Firewall, Load Balance）- 第一部分
10:20-10:40	休息
10:40-12:00	● IPv4/IPv6 雙軌網路環境建置（Router, Firewall, Load Balance）- 第二部分 ● 網路升級流程步驟和檢查項目清單
12:00-13:30	用餐及休息
13:30-14:50	● 作業系統 IPv6 建置示範（Centos7, Ubuntu18, Windows 2016） ● 資料庫 IPv6 調整示範（MySQL5, Windows SQL server 2017） ● 網站伺服器 IPv6 調整示範(IIS8, Apache2, Nginx） ● 程式檢查（PHP, ASP.NET） ● 作業系統與網站升級流程步驟和檢查項目清單
14:50-15:10	休息
15:10-16:30	● IPv4/IPv6 雙軌環境下資訊安全規劃概述 ● IPv4/IPv6 雙軌環境之資訊安全軟體與硬體設定（IPtables, Firewall） ● IPv4/IPv6 雙軌環境下資訊安全檢查項目清單（網路環境、作業系統、網站、資安設備）
16:30-17:00	Q&A

今年（108 年）度共完成 5 場教育訓練課程，於台北舉辦 2 場，高雄完成 2 場，及台中舉辦 1 場，各場教育訓練課程活動紀錄如下所述。

一. 第一場教育訓練課程

課程於 108 年 5 月 29 日舉行，會場地點為 TWNIC 辦公室會議中心，由張瑛杰先生擔任講師，參與人數共 36 人，回收 28 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 78%，本次教育訓練課程活動整體問卷分數為 4.59 分，高於品質目標分數 3.8，詳細的統計結果請參考下列圖示。

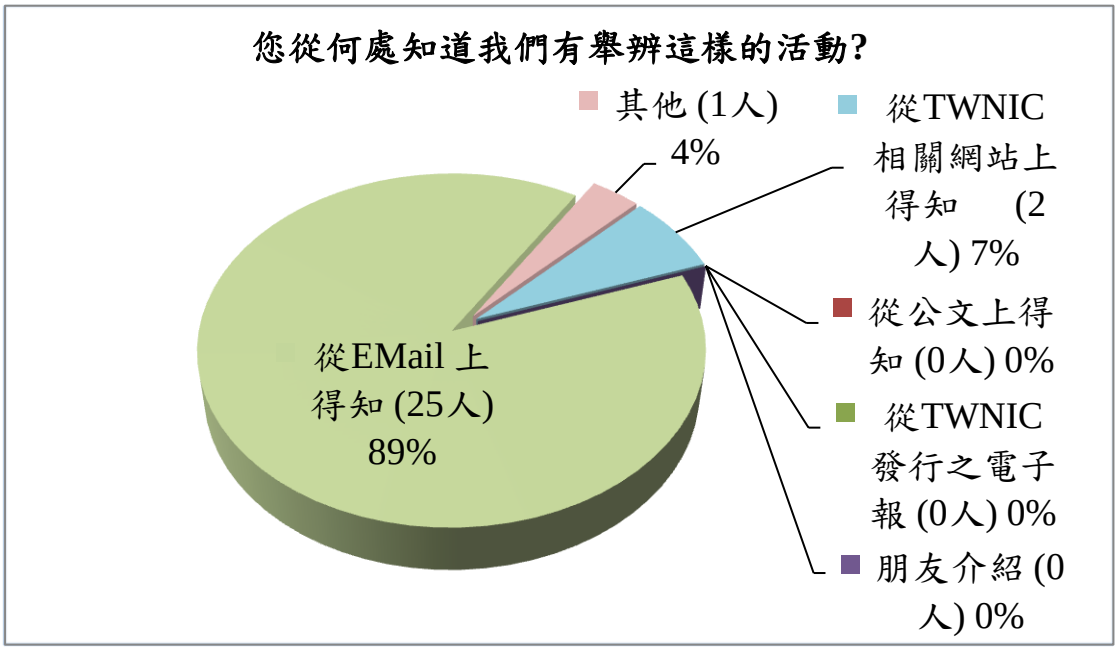

圖 109、5/29 台北場 ICP IPv4/IPv6 教育訓練活動資訊來源調查

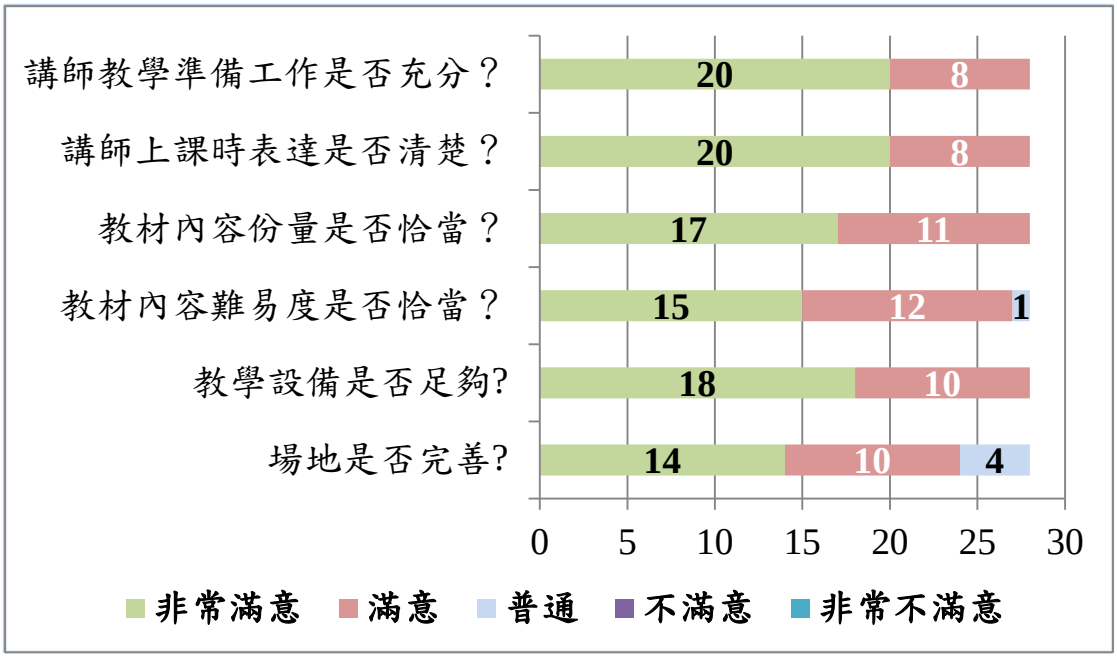

圖 110、5/29 台北場 ICP IPv4/IPv6 教育訓練滿意度統計

參與本次教育訓練課程人數 36 人，依據與會者行業別統計資料如下圖所示：

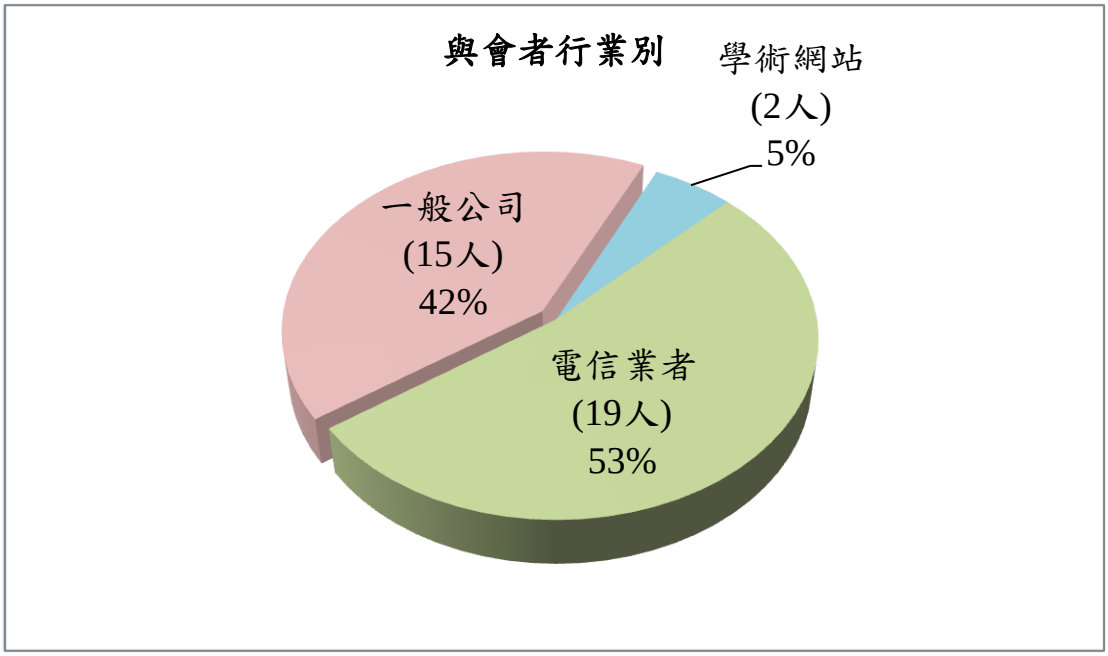

圖 111、5/29 台北場 ICP IPv4/IPv6 教育訓練與會者行業別統計

參與本次教育訓練課程其中一般公司人數 15 人，依據與會者公司類別統計資料如下圖所示：

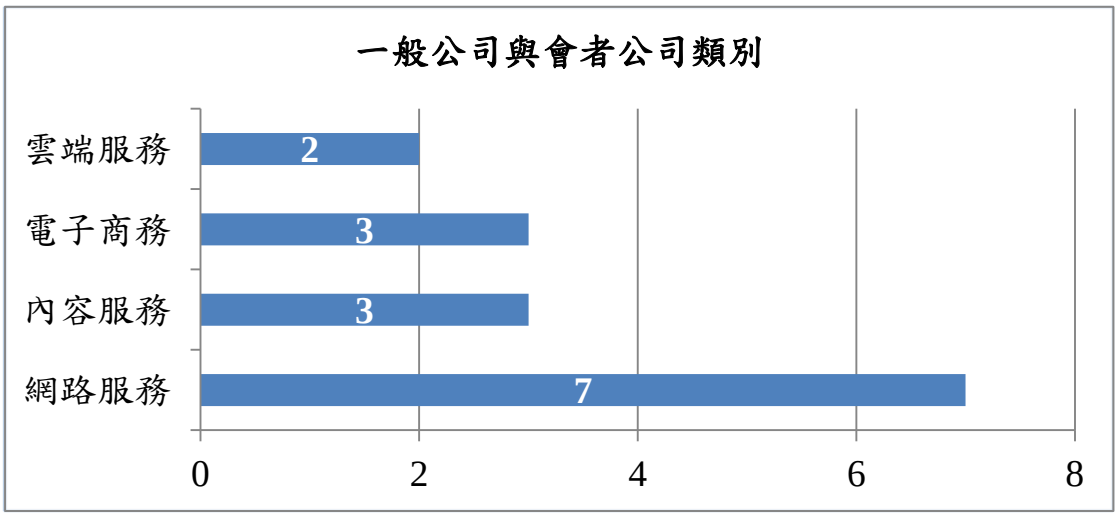

圖 112、5/29 台北 ICP IPv4/IPv6 教育訓練與會者屬一般公司類別統計圖

參與本次教育訓練課程其中一般公司人數 15 人，依據與會職級統計資料如下圖所示：

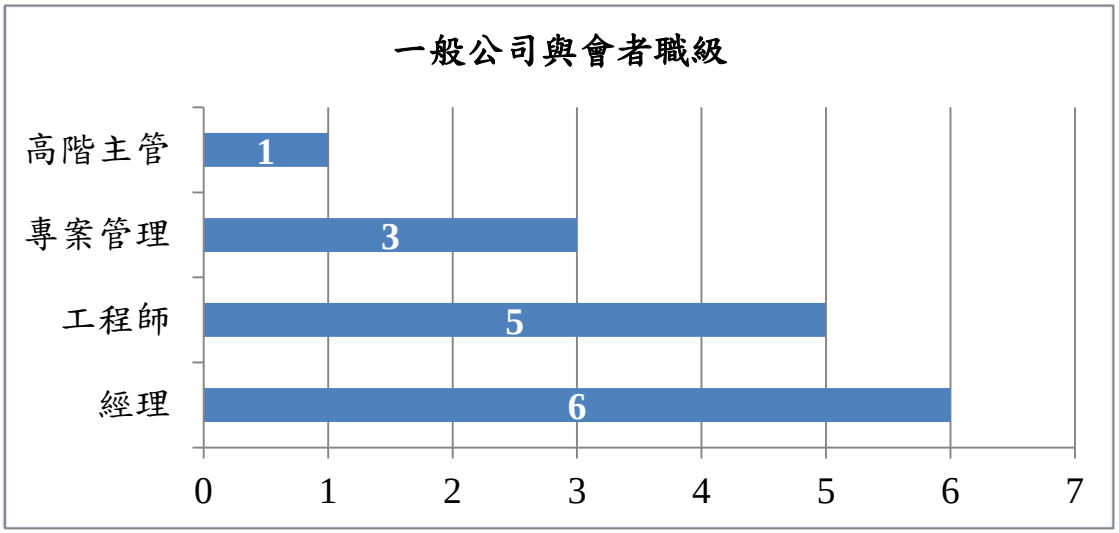

圖 113、5/29 台北 ICP IPv4/IPv6 教育訓練一般公司與會者職級統計圖

圖 114、5/29 台北場 ICP IPv4/IPv6 教育訓練會場

二. 第二場教育訓練課程

於 108 年 6 月 6 日舉行,會場地點為國立高雄科技大學管理學院，由張瑛杰先生擔任講師，參與人數共 35 人，回收 24 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 69%，本次教育訓練課程活動整體問卷分數為 4.62 分，高於品質目標分數 3.8，詳細的統計結果請參考下列圖示。

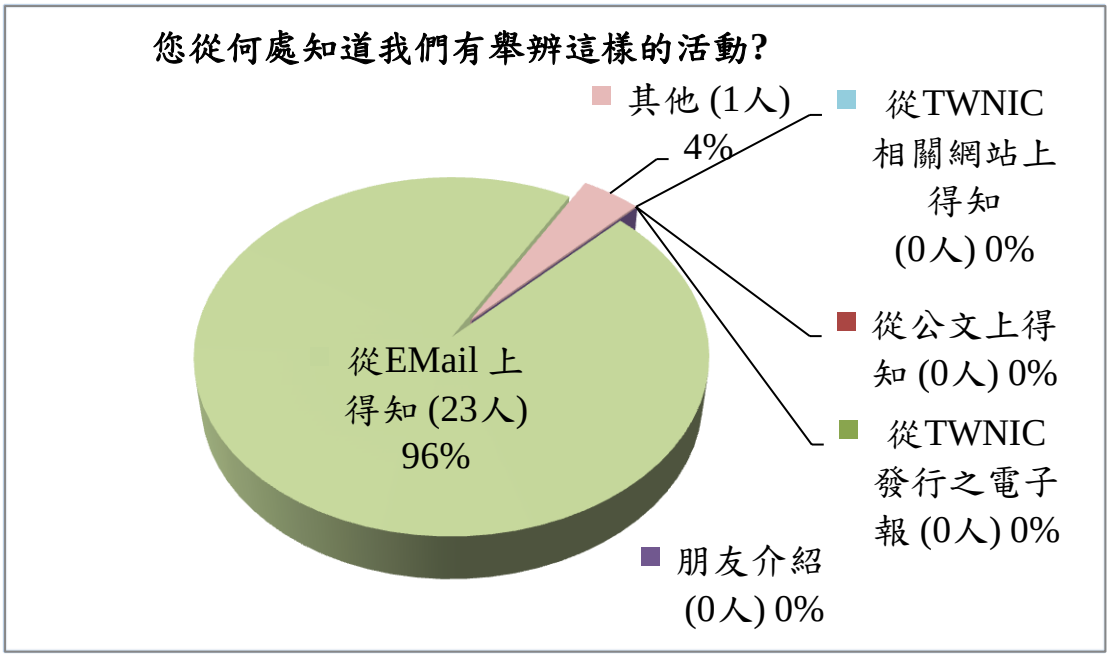

圖 115、6/6 高雄場 ICP IPv4/IPv6 教育訓練活動資訊來源調查

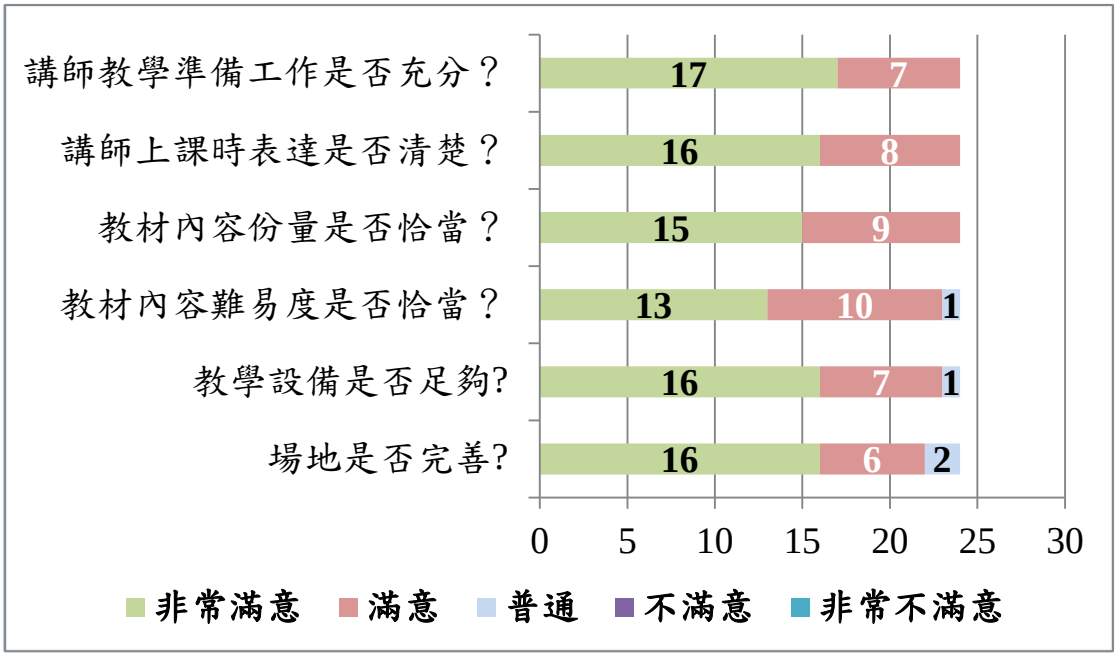

圖 116、6/6 高雄場 ICP IPv4/IPv6 教育訓練滿意度統計

參與本次教育訓練課程人數 35 人，依據與會者行業別統計資料如下圖所示：

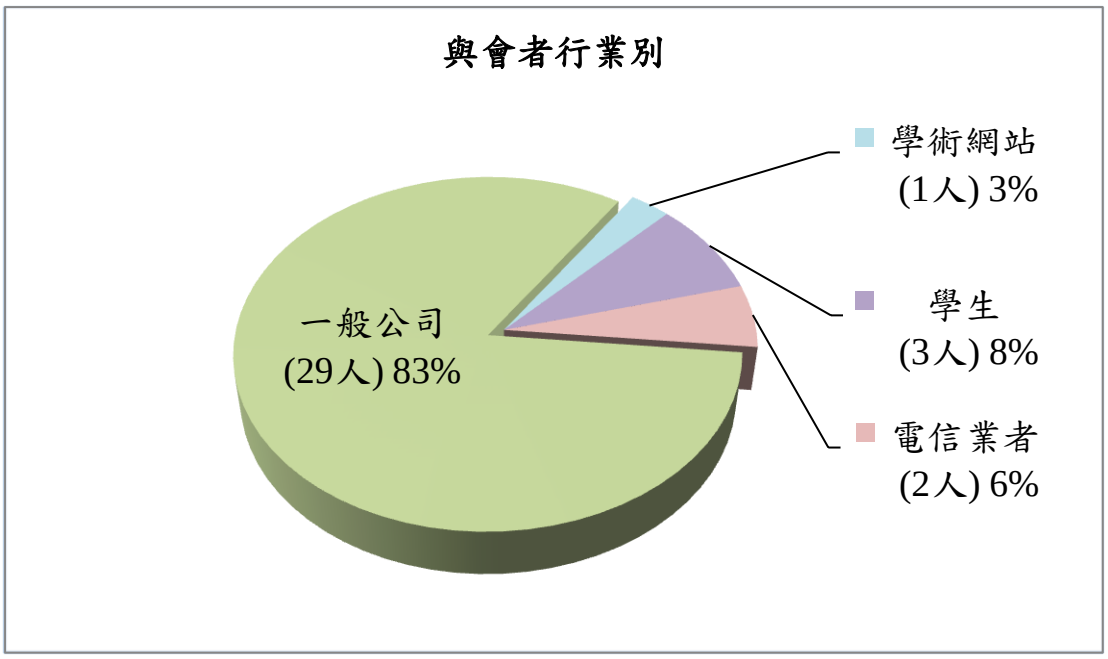

圖 117、6/6 高雄場 ICP IPv4/IPv6 教育訓練與會者行業別統計

參與本次教育訓練課程其中一般公司人數 29 人，依據與會者公司類別統計資料如下圖所示：

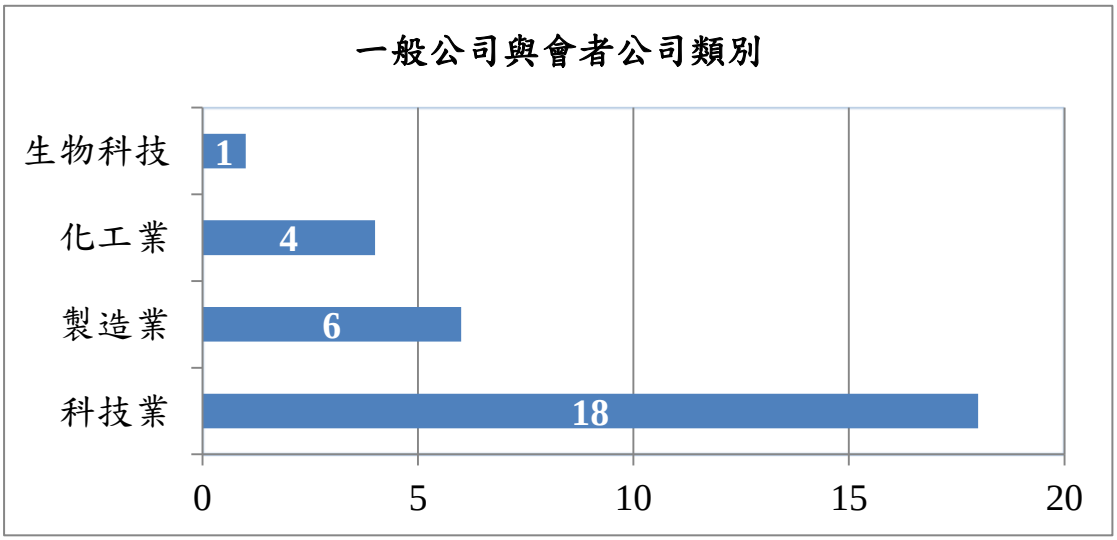

圖 118、6/6 高雄 ICP IPv4/IPv6 教育訓練與會者屬一般公司別統計圖

參與本次教育訓練課程其中一般公司人數 29 人，依據與會職級統計資料如下圖所示：

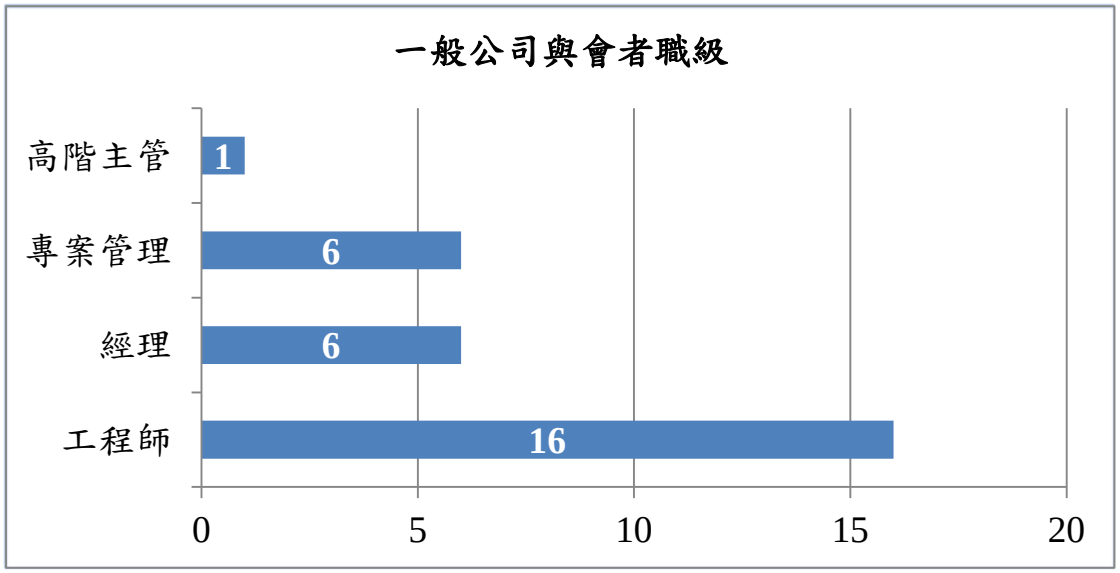

圖 119、6/6 高雄 ICP IPv4/IPv6 教育訓練一般公司與會者職級統計圖

圖 120、6/6 高雄場 ICP IPv4/IPv6 教育訓練會場

三. 第三場教育訓練課程

於 108 年 7 月 24 日舉行，會場地點為國立中興大學計算機及資訊網路中心，由張瑛杰先生擔任講師，參與人數共 39 人，回收 33 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 85%，本次教育訓練課程活動整體問卷分數為 4.48 分，高於品質目標分數 3.8，詳細的統計結果請參考下列圖示。

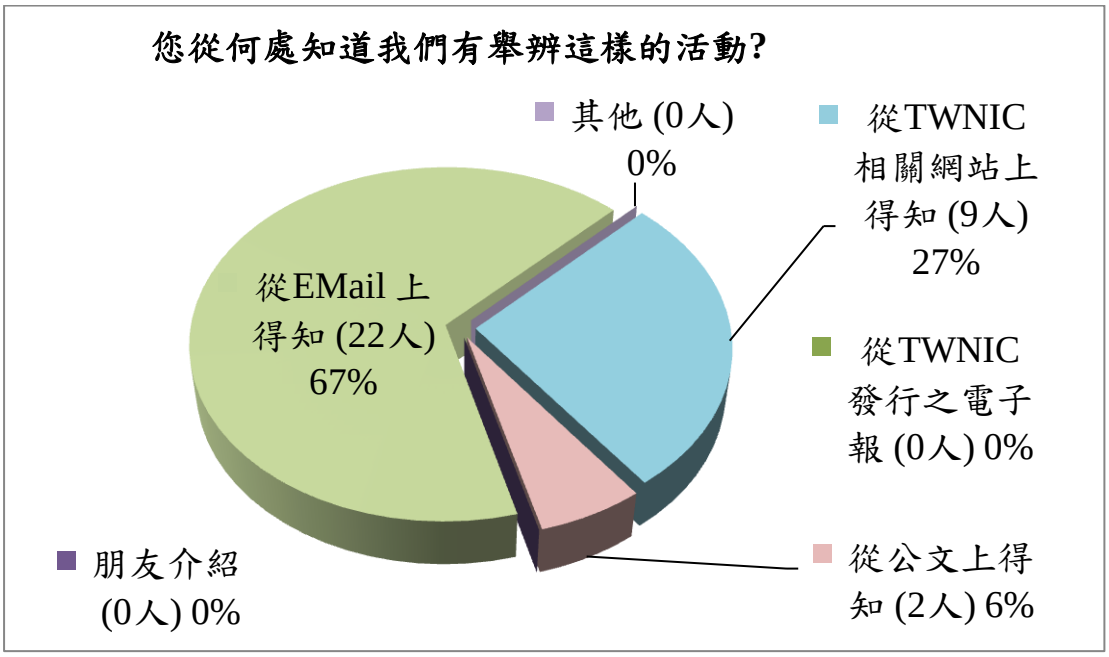

圖 121、7/24 台中場 ICP IPv4/IPv6 教育訓練活動資訊來源調查

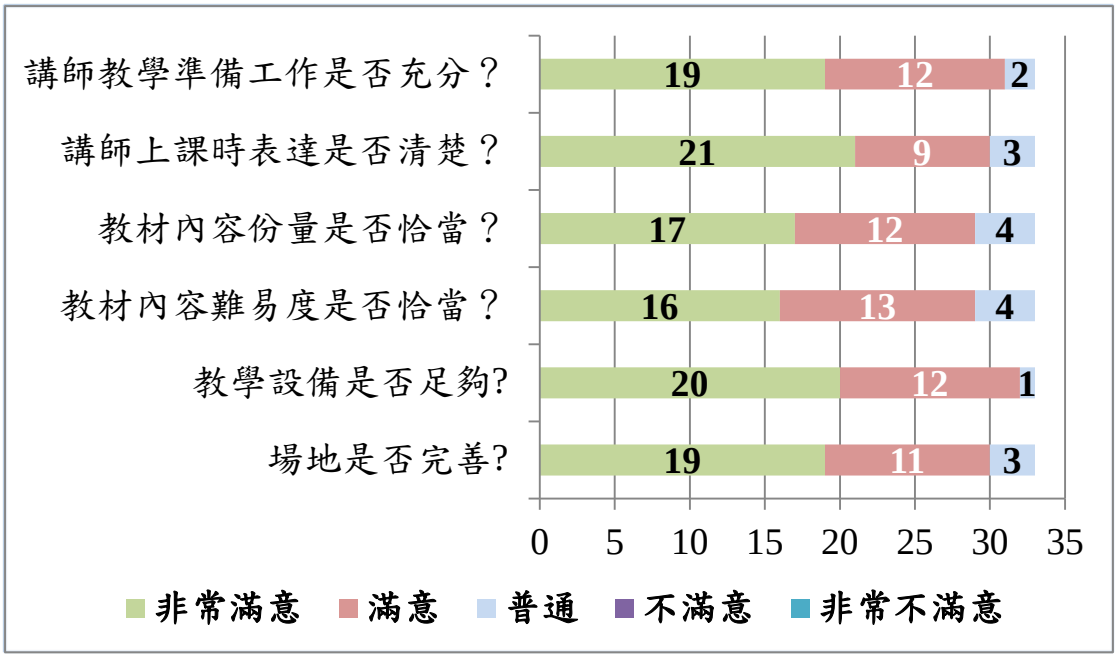

圖 122、7/24 台中場 ICP IPv4/IPv6 教育訓練滿意度統計

參與本次教育訓練課程人數 39 人，依據與會者行業別統計資料如下圖所示：

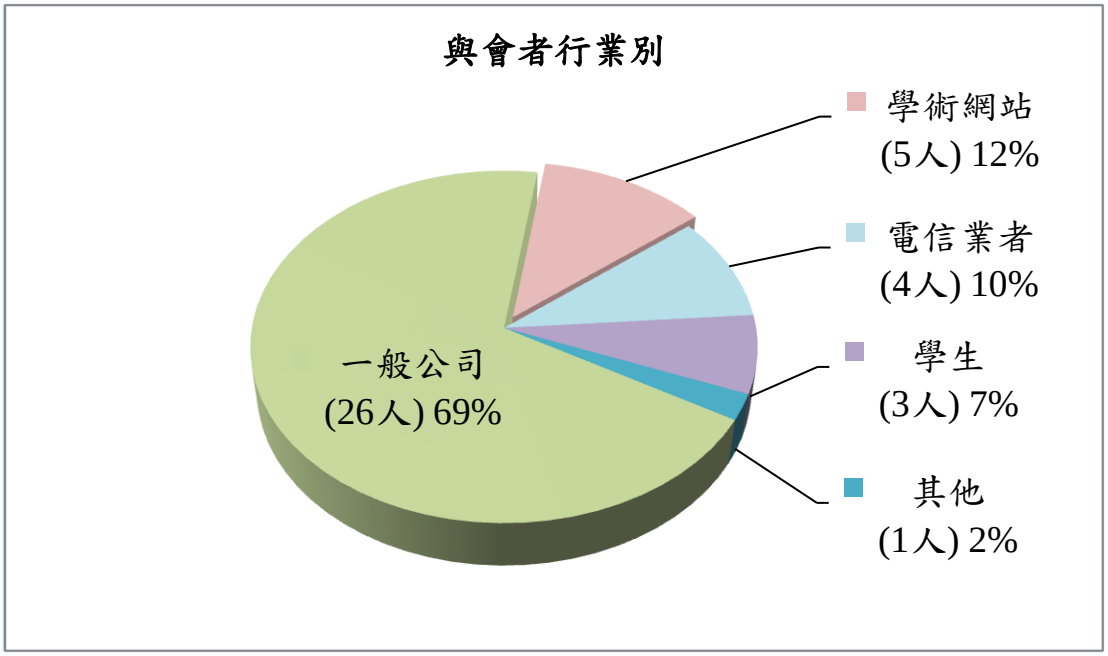

圖 123、7/24 台中場 ICP IPv4/IPv6 教育訓練與會者行業別統計

參與本次教育訓練課程其中一般公司人數 26 人，依據與會者公司類別統計資料如下圖所示：

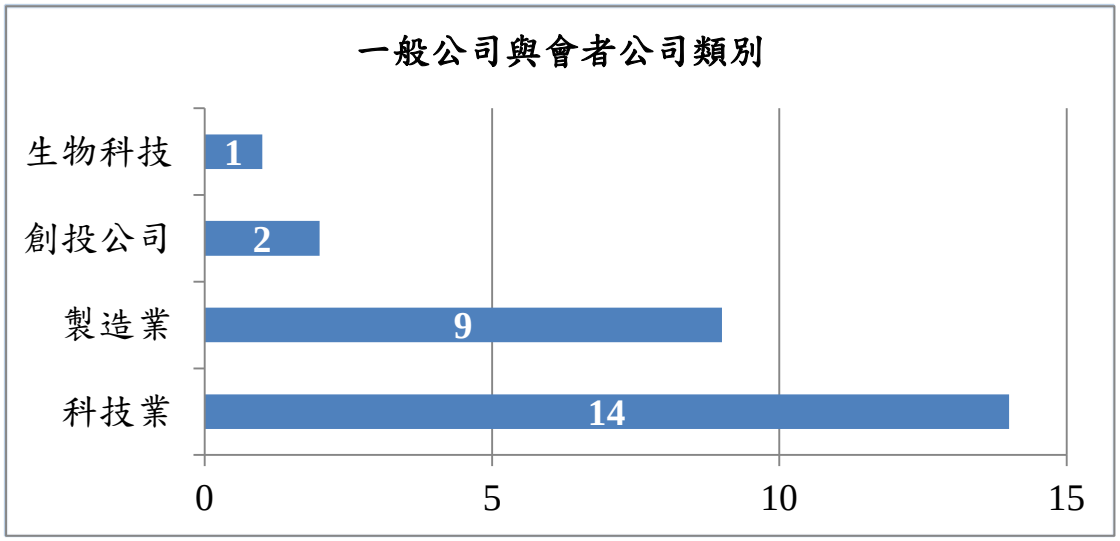

圖 124、7/24 台中 ICP IPv4/IPv6 教育訓練與會者屬一般公司別統計圖

參與本次教育訓練課程其中一般公司人數 26 人，依據與會職級統計資料如下圖所示：

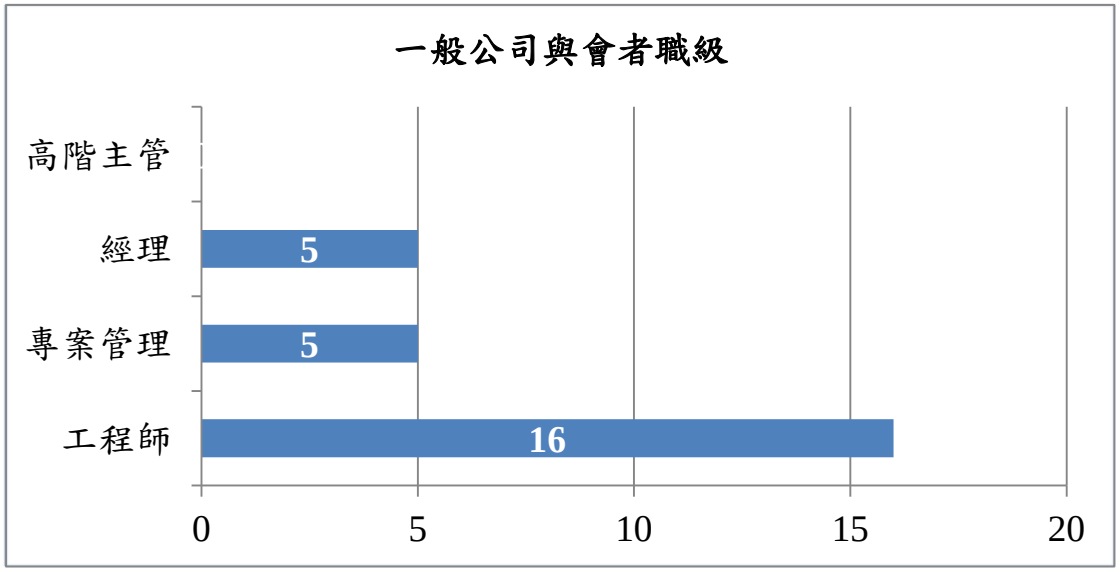

圖 125、7/24 台中 ICP IPv4/IPv6 教育訓練一般公司與會者職級統計圖

圖 126、7/24 台中場 ICP IPv4/IPv6 教育訓練會場

四. 第四場教育訓練課程

於 108 年 8 月 23 日舉行，會場地點為台灣網路資訊中心，由張瑛杰先生擔任講師，參與人數共 37 人，回收 25 份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為 68%，本次教育訓練課程活動整體問卷分數為 4.65 分，高於品質目標分數 3.8，詳細的統計結果請參考下列圖示。

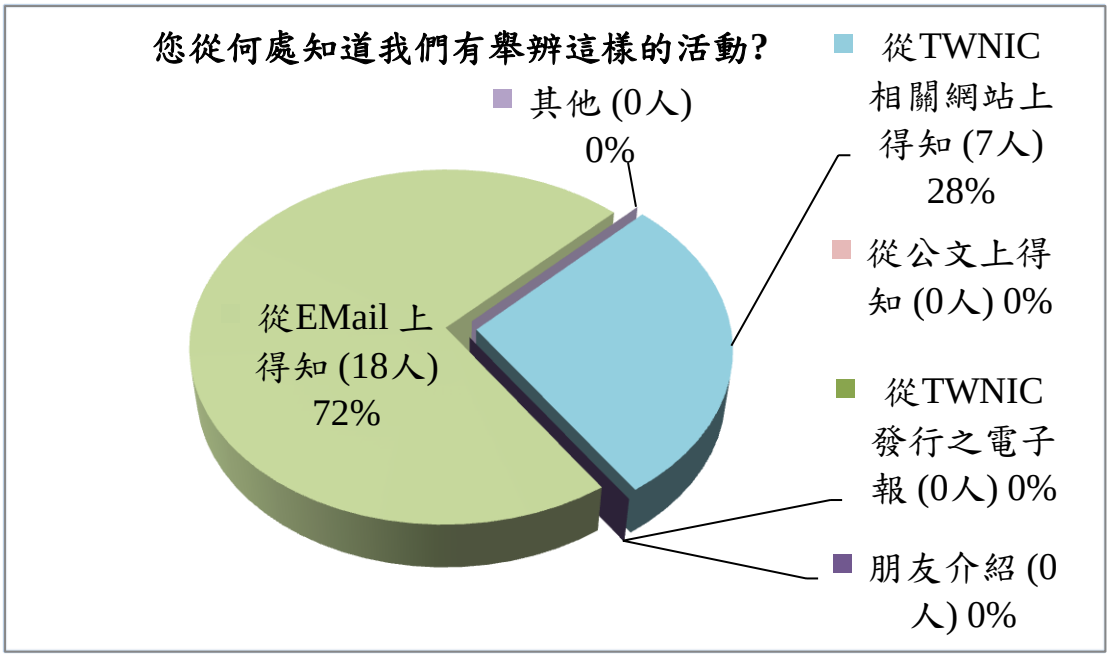

圖 127、8/23 台北場 ICP IPv4/IPv6 教育訓練活動資訊來源調查

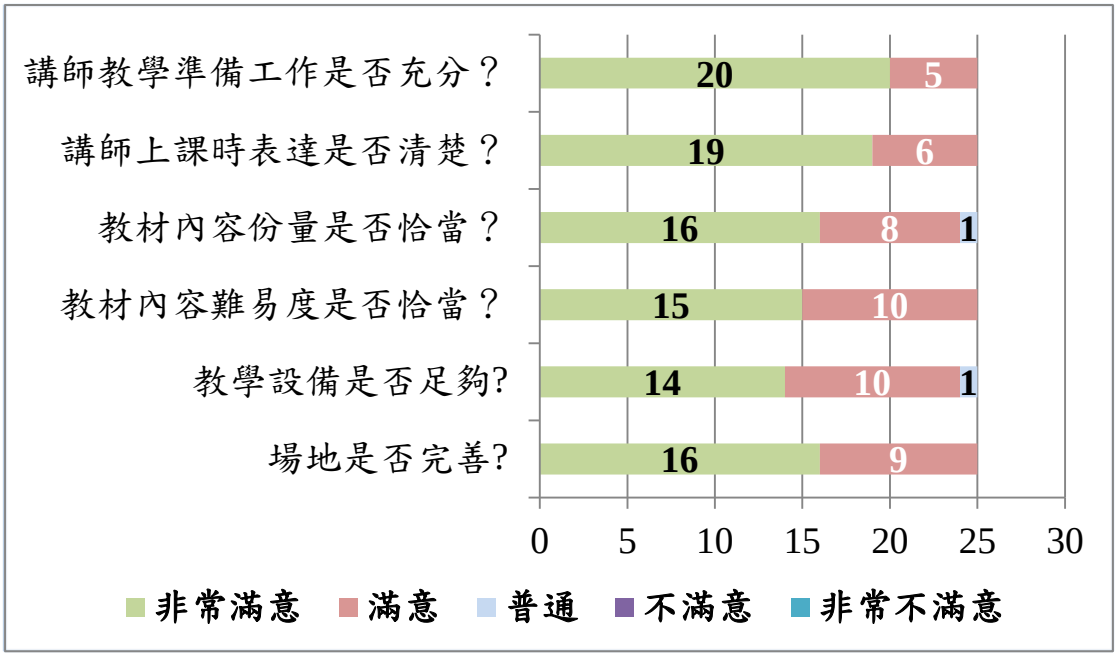

圖 128、8/23 台北場 ICP IPv4/IPv6 教育訓練滿意度統計

參與本次教育訓練課程人數 37 人，依據與會者行業別統計資料如下圖所示：

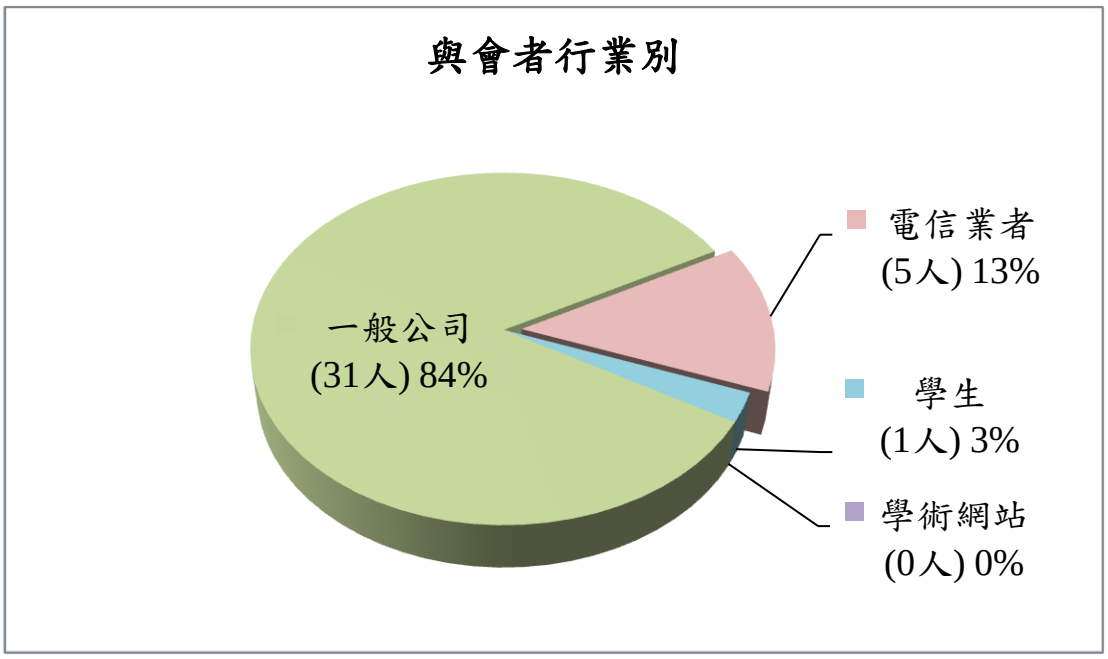

圖 129、8/23 台北場 ICP IPv4/IPv6 教育訓練與會者行業別統計

參與本次教育訓練課程其中一般公司人數 31 人，依據與會者公司類別統計資料如下圖所示：

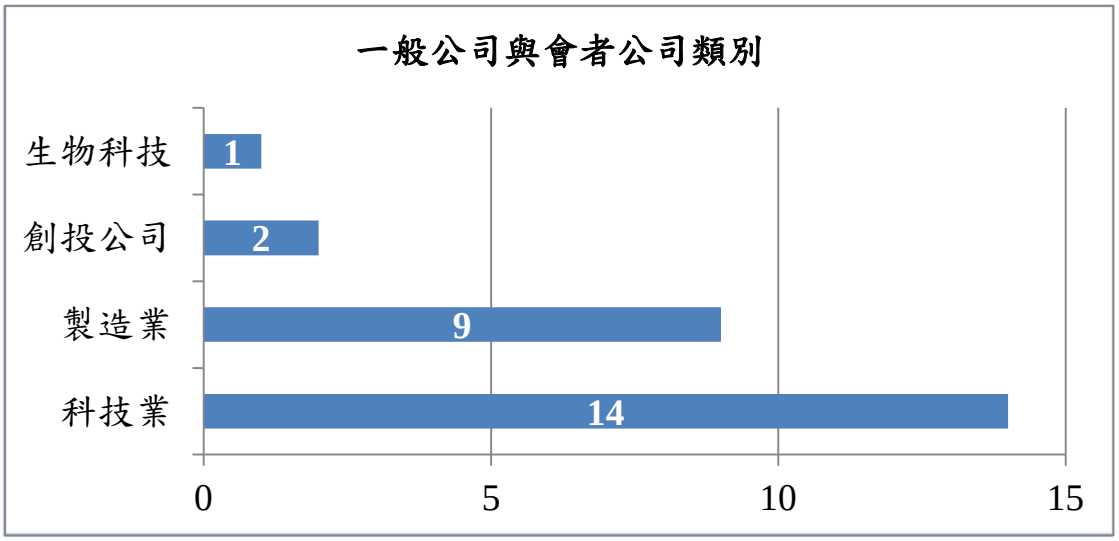

圖 130、8/23 台北 ICP IPv4/IPv6 教育訓練與會者屬一般公司別統計圖

參與本次教育訓練課程其中一般公司人數 26 人，依據與會職級統計資料如下圖所示：

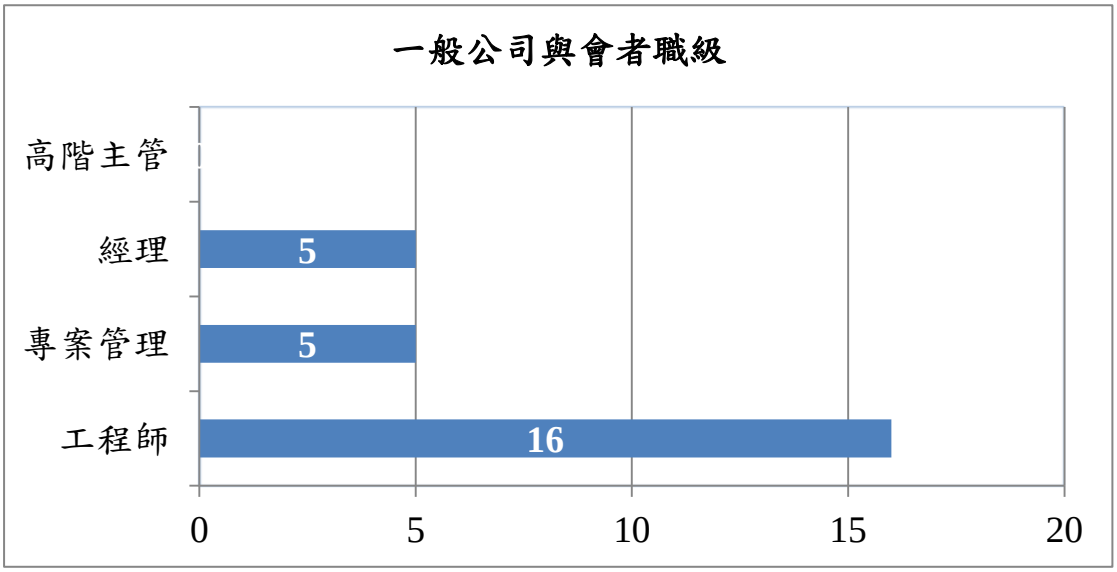

圖 131、8/23 台北 ICP IPv4/IPv6 教育訓練一般公司與會者職級統計圖

圖 132、8/23 台北場 ICP IPv4/IPv6 教育訓練會場

五. 第五場教育訓練課程

於108年9月12日舉行,會場地點為國立高雄科技大學管理學院，由張瑛杰先生擔任講師，參與人數共39人，回收28份問卷，有關教育訓練課程活動資訊來源及滿意度調查，問卷回收率約為72%，本次教育訓練課程活動整體問卷分數為4.62分，高於品質目標分數3.8，詳細的統計結果請參考下列圖示。

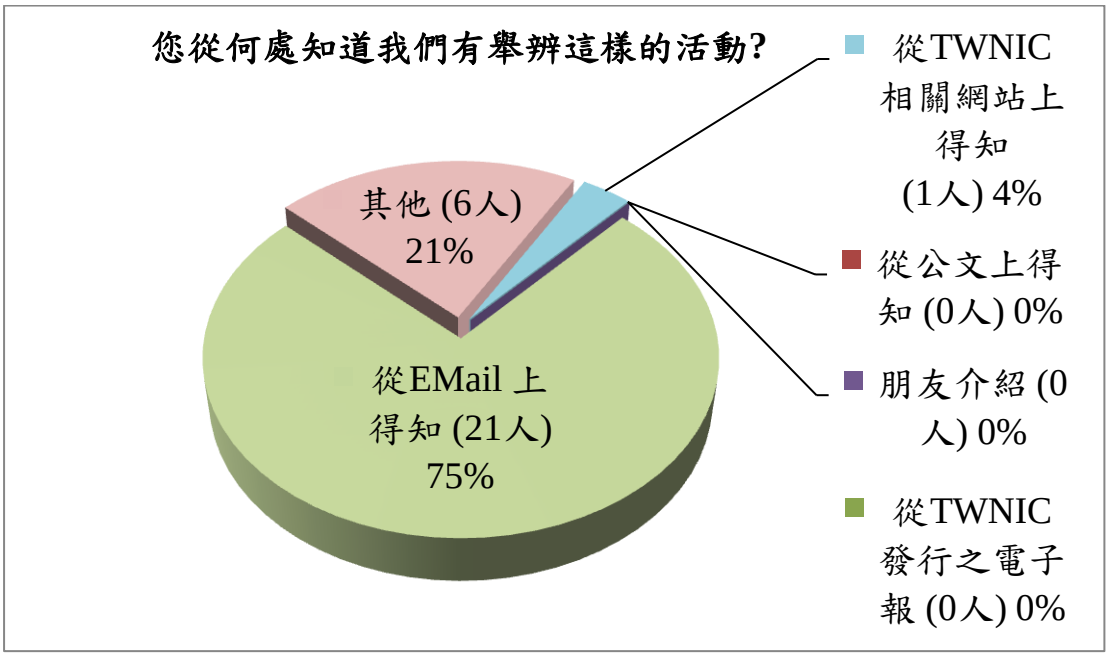

圖 133、9/12 高雄場 ICP IPv4/IPv6 教育訓練活動資訊來源調查

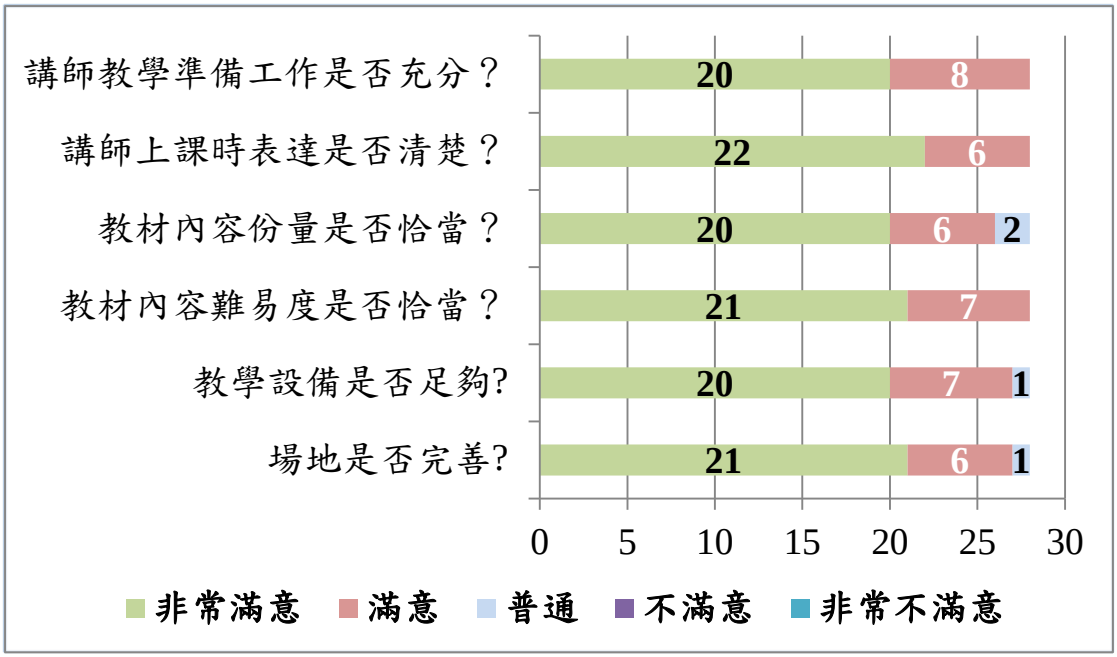

圖 134、9/12 高雄場 ICP IPv4/IPv6 教育訓練滿意度統計

參與本次教育訓練課程人數 39 人，依據與會者行業別統計資料如下圖所示：

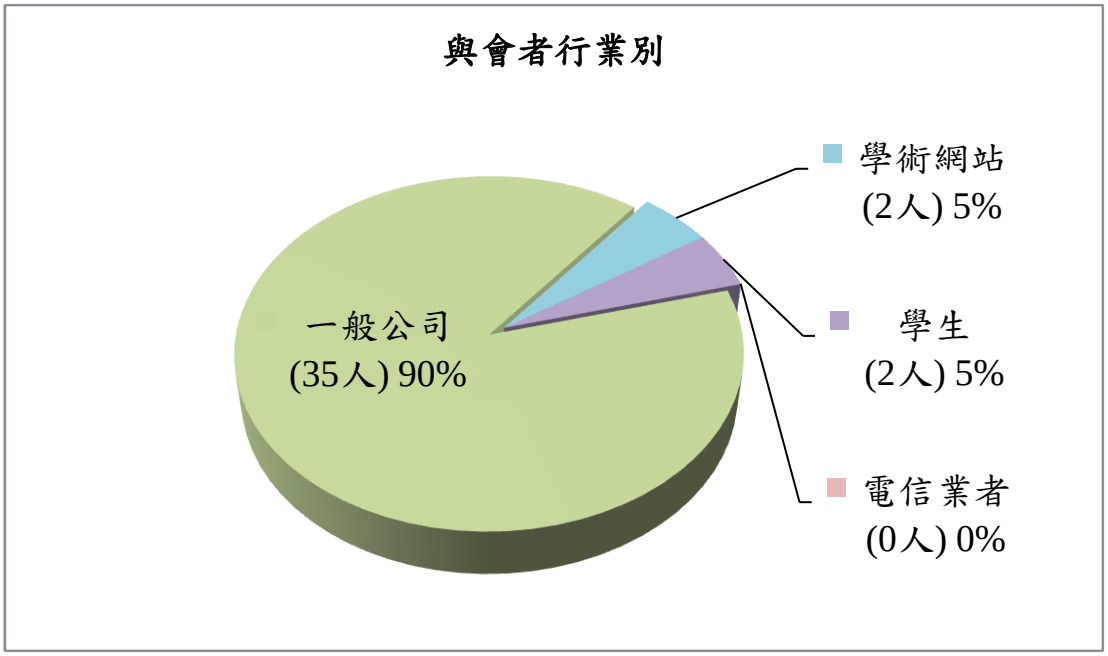

圖 135、9/12 高雄場 ICP IPv4/IPv6 教育訓練與會者行業別統計

參與本次教育訓練課程其中一般公司人數 35 人，依據與會者公司類別統計資料如下圖所示：

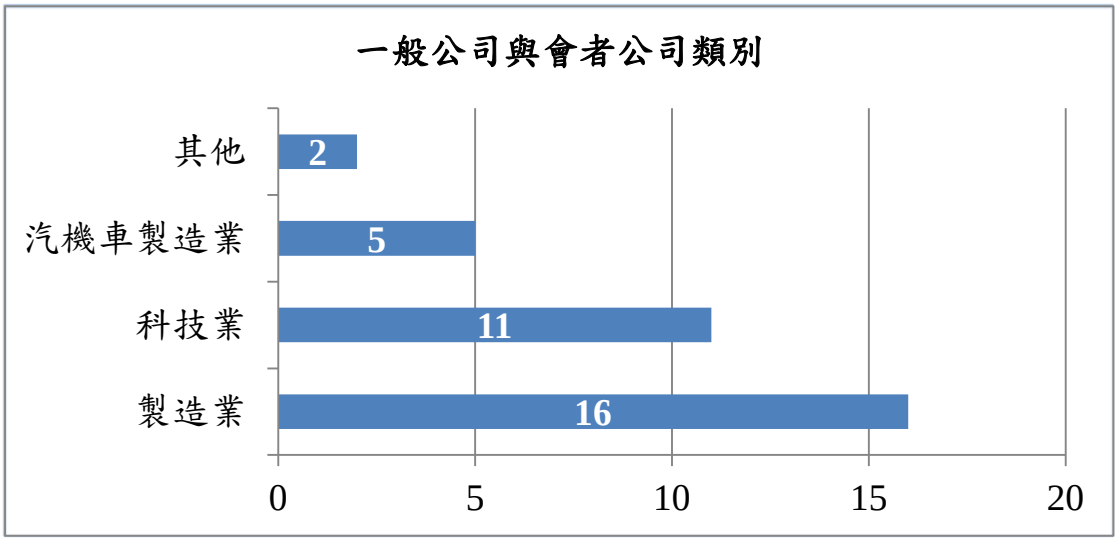

圖 136、9/12 高雄 ICP IPv4/IPv6 教育訓練與會者屬一般公司別統計圖

參與本次教育訓練課程其中一般公司人數 35 人，依據與會職級統計資料如下圖所示：

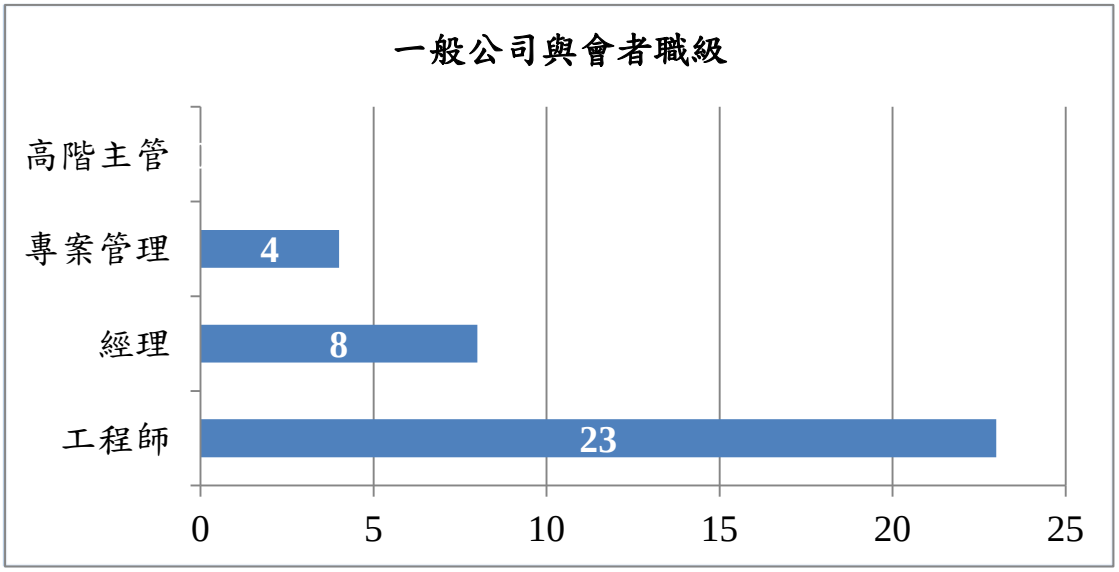

圖 137、9/12 高雄場 ICP IPv4/IPv6 教育訓練一般公司與會者職級統計圖

圖 138、9/12 高雄場 ICP IPv4/IPv6 教育訓練會場

今年（108 年）5 場 ICP IPv4/IPv6 教育訓練，目的為持續推廣國內網站升級支援 IPv6。同時今年（108 年）計畫中進行〝ICP IPv4/IPv6 網路安全防護架構技術手冊〞的撰寫，在下半年所舉辦的 3 場教育訓練課程內容，也將技術手冊內容增加到教育訓練課程內，以豐富課程內容及增加實用性。今年（108 年）計畫於 TWNIC 網站設置 IPv6 推廣專區，也將 IPv6 升級技術手冊放到 IPv6 推廣專區網頁上，提供業者參考，以加速推動國內 IPv4/IPv6 雙軌普及。以下為參與今年（108 年）度 5 場教育訓練課程參與人數統計表：

表 94、5 場教育訓練課程參與人數統計表

場次	日期	地點	總參與人數	一般公司參與人數
1	108 年 5 月 29 日	台北	36	15
2	108 年 6 月 06 日	高雄	35	29
3	108 年 7 月 24 日	台中	39	26
4	108 年 8 月 23 日	台北	37	31
5	108 年 9 月 12 日	高雄	39	35
總計			**186**	**136**

下圖為參與今年（108 年）度 5 場 ICP IPv4/IPv6 教育訓練一般公司與會者職級統計圖，以工程師參與的人數最多，另有部分專案管理或經理參與，少部分為公司高階主管：

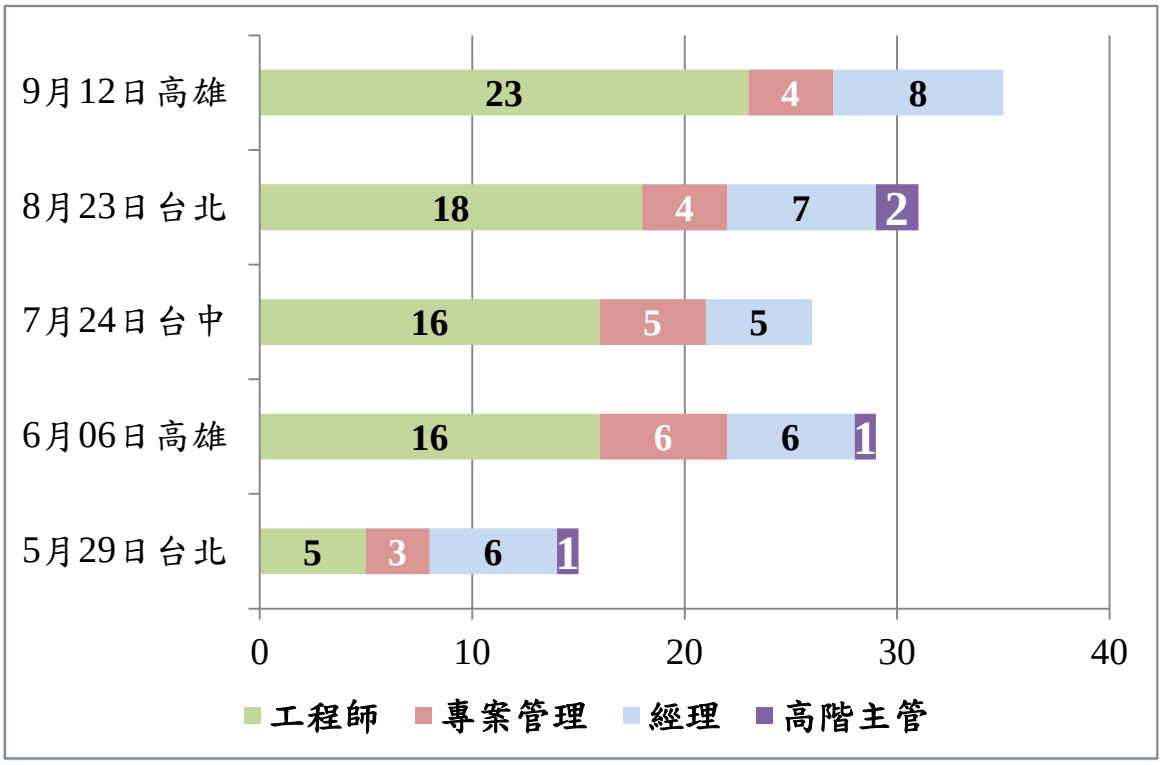

圖 139、5 場 ICP IPv4/IPv6 教育訓練一般公司與會者職級統計圖

第七章 物聯網、5G 與 IPv6 國際技術標準資料蒐集及研析

第一節 蒐集物聯網、5G 與 IPv6 相關的國際技術標準（RFC）

IPv6 已經成為 5G、IoT、SDN/NFV、雲計算以及邊緣計算等新興技術的基礎。大量的終端設備聯網產生了大量的地址需求，使用傳統 NAT 的方式無法支持新的 5G 及物聯網應用。

關於IETF工作小組，依不同類型的網際網路相關技術分為7大類，下表列出個別工作小組的相關資訊，包含每個工作小組的全名、任務、及相關連結等資訊。

表 95、IETF 工作小組分類

工作小組類別	工作小組類別全名	任務	相關連結
ART	Applications and Real-Time Area	-Application protocols and architecture -Real-time (communication) and non-real-time	https://trac.ietf.org/trac/art/wiki
INT	Internet Area	-IPv4/IPv6, DNS, DHCP, mobility	https://trac.ietf.org/trac/int/wiki
OPS	Operations and Management Area	-Network management -Operations: IPv6, DNS, security, routing	https://trac.ietf.org/trac/ops/wiki

工作小組類別	工作小組類別全名	任務	相關連結
RTG	Routing Area	-Routing and signaling protocols	https://trac.ietf.org/trac/rtg/wiki
SEC	Security Area	-Security protocols and mechanisms	https://trac.ietf.org/trac/sec/wiki
TSV	Transport Area	-Mechanisms related to data transport on the Internet -Includes congestion control	https://trac.ietf.org/trac/tsv/wiki
GEN	General Area	-Activities focused on supporting and updating IETF processes	https://trac.ietf.org/trac/gen/wiki

因應物聯網的發展，就網際網路相關協定的需求，IETF 也成立了相關的工作小組，對物聯網在網路連網環境相關議題進行討論，且已經公布了第一波所制定的標準。除此之外，網際網路研究工作小組（IRTF，Internet Research Task Force）於西元 2015 年（104 年）成立了物聯網專門研究小組（T2TRG，Thing-to-Thing），以調查物聯網的開放性研究問題。物聯網相關的工作小組資料，如下表所列：

表 96、物聯網相關的工作小組列表

編號	工作小組	工作小組全名及簡介	領域
1	6lo/ 6LoWPAN	IPv6 over Networks of Resource-constrained Nodes ● 使用 6LoWPAN 的 IPv6-over-foo 適配層規範鏈路層技術，適用於受限制網路與節點的規範。	網路
2	6tisch	IPv6 over the TSCH mode of IEEE 802.15.4e ● 專注於通過 TSCH 模式啟用 IPv6。	網路
3	ipwave	IP Wireless Access in Vehicular Environments	網

編號	工作小組	工作小組全名及簡介	領域
		● 致力於 V2V (Vehicle-to-vehicle)和 V2I (Vehicle-to-Internet)的網路使用情境，並將開發基於 IPv6 的直接和安全網路連接，以解決車輛與其他車輛或固定系統之間的網路連接問題。這些車載網路的特點是動態變化的網路拓撲和連通性。	路
4	lpwan	IPv6 over Low Power Wide-Area Networks ● 產生介紹性文件，描述 LPWAN 低功耗廣域網路技術 ● 生成標準以啟用壓縮和 LPWAN 網路上的 CoAP / UDP / IPv6 資料封包。	網路
5	lwig	Light-Weight Implementation Guidance ● 收集受限制設備中 IP protocal stack 的實現經驗。僅專注於實際使用的技術實施，並且不影響與其他設備的互操作性。	網路
6	homenet	Home Networking ● 該小組的任務是產生一個架構文件，概述如何建構涉及多個路由器的家庭網路，以及子網。	網路
7	roll	Routing Over Low power and Lossy networks ● 致力於家庭、建築物、都會網路中感測裝置的路由問題。這些裝置的能源、記憶體和計算資源都相當的受限，使用不同的實體網路技術。	路由
8	ace	Authentication and Authorization for Constrained Environments ● 目標在產生標準的認證與授權方法，可以在受限制網路中存取一個由 URI 指定的資源。伺服器與客戶端都可能是受限制的，預設使用 CoAP 與 DTLS。	安全
9	cose	CBOR Object Signing and Encryption ● COSE (RFC 8152)描述如何將 CBOR (RFC 7049)物件進行簽章與加密。	安全
10	suit	Software Updates for Internet of Things ● 專注於 IoT 裝置中如何安全的進行韌體更新的解決方案。	安全
11	dice	DTLS In Constrained Environments ● 致力於在受限制環境中支援 DTLS	安全

編號	工作小組	工作小組全名及簡介	領域
		Transport-Layer Security 的解決方案，以支援 CoAP。 ● 此工作小組已關閉	
12	cbor	Concise Binary Object Representation Maintenance and Extensions ● Concise Binary Object Representation (COBR)延伸 JavaScript Object Notation (JSON)資料交換格式，以支援可擴充的二進制資料表示格式。	應用
13	core	Constrained RESTful Environments ● 建立一個能在受限制環境中執行的資源導向應用軟體框架 CoAP。	應用
14	t2trg	Thing-to-Thing research group ● 探索開放的研究議題，以期能真正的實現物聯網，特別是讓資源受限的受限制節點可以彼此互連或與 Internet 相連。 ● 隸屬於網際網路研究工作小組（IRTF，Internet Research Task Force）	

和物聯網相關 RFC 共有 81 篇，依據其內容可以分為 5 大類別，分別為研討會概述 4 篇、概念型 17 篇、應用層 14 篇、資訊安全 9 篇及網路層與傳輸層 37 篇。下表為此計畫研究物聯網相關 RFC 分類統計資訊：

表 97、物聯網相關 RFC 分類

序號	類別	RFC 編號	篇數
1	研討會概述	RFC 6574、RFC 7397、RFC 8240、RFC 8477	4
2	概念型	RFC 4919、RFC 5548、RFC 5673、RFC 5867、RFC 5826、RFC 6568、RFC 7102、RFC 7228、RFC 7548、RFC 7368、RFC 7788、RFC 7388、RFC 7452、RFC 7547、RFC 8376、RFC 8352、RFC 7733	17

序號	類別	RFC 編號	篇數
3	應用層	RFC 7049、RFC 7252、RFC 7641、RFC 7959、RFC 7967、RFC 8132、RFC 8323、RFC 8075、RFC 7390、RFC 7650、RFC 6690、RFC 7744、RFC 8148、RFC 8428	14
4	資訊安全	RFC 8065、RFC 8387、RFC 8576、RFC 7416、RFC 7925、RFC 8152、RFC 8230、RFC 8392、RFC 7815	9
5	網路層與傳輸層	RFC 4944、RFC 6282、RFC 7400、RFC 7973、RFC 8025、RFC 8066、RFC 6606、RFC 6550、RFC 6551、RFC 6687、RFC 6552、RFC 6553、RFC 6554、RFC 8585、RFC 6719、RFC 6997、RFC 6998、RFC 8036、RFC 6206、RFC 7787、RFC 8138、RFC 6775、RFC 8505、RFC 7428、RFC 7554、RFC 8180、RFC 8480、RFC 7668、RFC 8105、RFC 8163、RFC 8272、RFC 8375、RFC 7695、RFC 8539、RFC 7731、RFC 7774、RFC 7732	37
合計			81

關於研討會概述 4 篇的彙整資訊如下表所述：

表 98、研討會概類別的彙整資訊

編號	RFC 編號	狀態	時間	類別	工作小組
1	6574	Informational	2012/04	Smart Objects	iab
		Report from the Smart Object Workshop 概述網際網路架構委員會(IAB)舉辦的關於將智慧對象與網際網路連接研討會的結論和建議。			
2	7397	Informational	2014/12	Smart Objects	iab
		Report from the Smart Object Security Workshop 總結西元 2012 年（101 年）3 月 23 日在巴黎舉行的智慧對象安全研討會的討論情況，並列出了網際網路工程任務組(IETF)社群的結論和建議。			
3	8240	Informational	2017/09	Ops & Mgmt IoTSU	IoTSU
		Report from the Internet of Things Software Update (IoTSU) Workshop 2016			

編號	RFC 編號	狀態	時間	類別	工作小組
		概述西元 2016 年（105 年）6 月 13 日和 14 日在愛爾蘭都柏林聖三一學院舉辦的物聯網軟體更新(IoTSU)研討會。研討會的主要目標是促進對需求的討論，挑戰以及為物聯網設備帶來軟體和韌體更新的解決方案。			
4	8477	Informational	2018/10	Ops & Mgmt IoTSU	IoTSU
		Report from the Internet of Things (IoT) Semantic Interoperability (IOTSI) Workshop 2016 概述了物聯網(IoT)語義互操作性(IOTSI)研討會，研討會的主要目標是促進討論公司和標準開發組織(SDO)用於在應用層實現互操作性的不同方法。			

關於概念型 17 篇的彙整資訊如下表所述：

表 99、概念型類別的彙整資訊

編號	RFC 號	狀態	時間	類別	工作小組
1	4919	Informational	2007 /04	Internet 6loWPAN	6lo 6lowpan
		IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals 詳述了在 IEEE 802.15.4 網路上傳輸 IP 的假設，問題陳述和目標。本文列舉的目標集僅屬於初始集。			
2	5548	Informational	2009/05	Routing RPL	roll
		Routing Requirements for Urban Low-Power and Lossy Networks 設定一組 IPv6 路由需求，以反映和其他都會低功耗有損網路(U-LLN)的特定特徵。			
3	5673	Informational	2009/10	Routing RPL	roll
		Industrial Routing Requirements in Low-Power and Lossy Networks 分析工業用低功耗有損網路(LLN)場域設備使用的路由協定的功能需求。如廣泛部署的低成本無線設備將顯著提高工業			

編號	RFC號	狀態	時間	類別	工作小組
		設備的生產和安全性。			
4	5867	Informational	2010/06	Routing RPL	roll
		Building Automation Routing Requirements in Low-Power and Lossy Networks 根據低功耗有損網路(LLN)的路由解決方案，定義大樓自動化的 IPv6 路由要求。			
5	5826	Informational	2010/04	Routing RPL	roll
		Home Automation Routing Requirements in Low-Power and Lossy Networks 介紹低功耗有損網路路由(ROLL)於家庭控制和自動化應用的特定需求。			
6	6568	Informational	2012/04	Internet 6loWPAN	6lo 6lowpan
		Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) 研究低功耗無線個人網路(LoWPAN)的潛在應用場景和案例。			
7	7102	Informational	2014/01	Routing	roll
		Terms Used in Routing for Low-Power and Lossy Networks LLN 通常由許多嵌入式設備組成，這些嵌入式設備具有通過各種連結互連的有限功率、記憶體和處理資源，本文提供路由要求和術語解決方案中使用的術語表。			
8	7228	Informational	2014/05	Internet	lwig
		Terminology for Constrained-Node Networks 針對受限制節點和受限制網路進行各種術語的定義與說明，包含 LLN 與(6)LoWPAN，用以協助標準化。也說明了受限制裝置的分級，電力術語，能源限制分級，電力策略等。			
9	7548	Informational	2015/05	Ops & Mgmt	opsawg
		Management of Networks with Constrained Devices: Use Cases 討論涉及受限制設備的網路管理的案例。			
10	7368	Informational	2014/10	Internet HomeNet	homenet
		IPv6 Home Networking Architecture Principles 定義基於 IPv6 家庭網路的通用架構，描述相關的原則，注意事項和要求。			
11	7788	Standards Track	2016/04	InternetHome Net HNCP	homenet
		Home Networking Control Protocol			

編號	RFC號	狀態	時間	類別	工作小組
		介紹家庭網路控制協定(HNCP)，一個可擴充的配置協定，以及一組家庭網路設備的要求。			
12	7388	Standards Track	2012/07	Internet 6loWPAN	6lo
		Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) 定義部分管理資訊庫(MIB)，用於網際網路社群中的網路管理協定。			
13	7452	Informational	2015/03	Smart Objects	iab
		Architectural Considerations in Smart Object Networking 提供工程師設計連接網際網路的智慧對象指導原則。			
14	7547	Informational	2015/05	Ops & Mgmt	opsawg
		Management of Networks with Constrained Devices: Problem Statement and Requirements 提供了問題說明，部署和管理拓撲選項，以及針對涉及受限制設備網路管理的不同使用案例的要求。			
15	8376	Informational	2018/05	Internet LPWAN	lpwan
		Low-Power Wide Area Network (LPWAN) Overview 概述LPWAN技術集訊息，這些技術的需求與在LPWAN中運行IP的目標之間存在的差異。介紹LPWAN技術(LoRaWAN、NB-IoT、Sigfox、Wi-SUN)。			
16	8352	Informational	2018/04	Internet IoT	lwig
		Energy-Efficient Features of Internet of Things Protocols 總結用於節能網路的主要連結層技術，並強調這些技術對上層協定的影響，以便能夠共同實現節能行為。			
17	7733	Standards Track	2016/02	Routing RPL	roll
		Applicability Statement: The Use of the Routing Protocol for Low-Power and Lossy Networks (RPL) Protocol Suite in Home Automation and Building Control 為選擇和使用低功耗有損網路路由協定(RPL)套件中的協定提供指導原則，以實現建築和家庭環境中控制所需的功能。			

關於應用層 14 篇的彙整資訊如下表所述：

表 100、應用層類別的彙整資訊

編號	RFC號	狀態	時間	類別	工作小組
1	7049	Standards Track	2013/10	Applications and Real-Time CoRE CBOR	cbor
		Concise Binary Object Representation (CBOR) 許多物聯網應用 JSON 來傳輸資料，CBOR 定義如何將 JSON 這種純文字的資料轉為二進制的方式來儲存。			
2	7252	Standards Track	2014/06	Applications and Real-Time CoAP	core
		The Constrained Application Protocol (CoAP) CoAP 是一種專門的 web 傳輸協定，用於受限制節點和受限制網路，包含應用模型(訊息傳遞、請求/響應等)、訊息格式，資料傳輸(可靠、不可靠等等)。			
3	7641	Standards Track	2015/09	Applications and Real-Time CoAP	core
		Observing Resources in the Constrained Application Protocol (CoAP) 規定了 CoAP 的簡單協定擴充，使 CoAP 客戶端能夠“觀察”資源，即檢索資源的表示並在一段時間內保持服務器更新該表示。			
4	7959	Standards Track Updates 7252	2016/08	Applications and Real-Time CoAP	core
		Block-Wise Transfers in the Constrained Application Protocol (CoAP) 此規範更新了 RFC 7252。不支援這些選項的 CoAP 實現通常受限於可交換的表示的大小，因此期望塊選項將在 CoAP 實現中廣泛使用。			
5	7967	Informational	2016/08	Applications and Real-Time CoAP	core
		Constrained Application Protocol (CoAP) Option for No Server Response 該規範引入了一個名為“無響應”的 CoAP 選項。本文還討			

編號	RFC號	狀態	時間	類別	工作小組
		論了一些受益於此選項的應用程序範例。			
6	8132	Standards Track	2017/04	Applications and Real-Time CoAP	core
		PATCH and FETCH Methods for the Constrained Application Protocol (CoAP) 該規範定義了新的 CoAP 方法，FETCH，PATCH 和 iPATCH，用於訪問和更新資源的一部分。			
7	8323	Standards Track Updates RFC 7641, RFC 7959	2018/02	Applications and Real-Time CoAP	core
		CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets 概述在 TCP、TLS 和 WebSockets 傳輸上使用 CoAP 所需的更改。且更新了 RFC 7641 以使用這些傳輸，和 RFC7959，以便在可靠傳輸上能使用的更長訊息。			
8	8075	Standards Track	2017/02	Applications and Real-Time CoAP	core
		Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP) 提供了實現跨協定網路代理的參考資訊，該代理執行從 HTTP 協定到受限制應用協定(CoAP)的轉換。			
9	7390	Experimental	2014/10	Applications and Real-Time CoAP	core
		Group Communication for the Constrained Application Protocol (CoAP) 詳述了在 IP 群播上使用 CoAP 的方法。另外也提供了多種案例和對應的協定流程來說明重要概念，以及在各種網路拓撲中部署的指導原則。			
10	7650	Standards Track	2015/09	Applications and Real-Time CoAP	core
		A Constrained Application Protocol (CoAP) Usage for REsource LOcation And Discovery (RELOAD)			

編號	RFC號	狀態	時間	類別	工作小組
		定義 REsource LOcation And Discovery(RELOAD)的限制應用程序協定(CoAP)用法。			
11	6690	Standards Track	2012/08	Applications and Real-Time CoRE	core
		Constrained RESTful Environments (CoRE) Link Format 基於 RFC 5988 中定義的 HTTP 鏈接標頭字段，限制 RESTful 環境(CoRE)鏈接格式作為有效負載攜帶，並被分配網際網路媒體類型。			
12	7744	Informational	2016/01	Security ACE	ace
		Use Cases for Authentication and Authorization in Constrained Environments 討論受限制的設備是具有有限處理能力，存儲空間和傳輸容量的節點。在許多情況下，這些設備不提供用戶界面，並且通常用於在沒有人為干預的情況下進行訊息交互作用。			
13	8148	Standards Track	2017/05	Applications and Real-Time Vehicle	ecrit
		Next-Generation Vehicle-Initiated Emergency Calls 描述了如何使用基於 IP 的緊急服務機制來支援車輛發出的下一代緊急呼叫。			
14	8428	Standards Track	2018/08	Applications and Real-Time CoAP	core
		Sensor Measurement Lists (SenML) 定義一種格式，用於表示傳感器測量列表(SenML)中的簡單傳感器測量和設備參數。			

關於資訊安全 9 篇的彙整資訊如下表所述：

表 101、資訊安全類別的彙整資訊

編號	RFC號	狀態	時間	類別	工作小組
1	8065	Informational	2017/02	Internet	6lo

編號	RFC 號	狀態	時間	類別	工作小組
				6lo	
		Privacy Considerations for IPv6 Adaptation-Layer Mechanisms 討論了許多隱私威脅如何應用於各種 IPv6 連結層協定，並為協定設計者提供了有關如何通過此類連結解決 IPv6 適配層規範中的此類威脅的建議。			
2	8387	Informational	2018/05	Internet	lwig
		Practical Considerations and Implementation Experiences in Securing Smart Object Networks 關於資源受限制智慧物件上的安全挑戰，描述可能的佈署模式，資源受限制對訊息物件簽章，討論加密函數庫的可用性，和展示前導實驗。			
3	8576	Informational	2019/04	Security	t2trg
		Internet of Things (IoT) Security: State of the Art and Challenges 討論事物生命週期中的各個階段，並記錄事物的安全威脅以及人們可能面臨防範這些威脅的挑戰。最後討論促進安全物聯網系統部署所需的後續步驟。			
4	7416	Informational	2015/01	Routing RPL	roll
		A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs) 針對低功耗有損網路(RPL)的路由協定的安全威脅分析。			
5	7925	Standards Track	2016/07	Security TLD DTLS	dice
		Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things 針對既有的安全性協定 Transport Layer Security (TLS) 與 Datagram Transport Layer Security (DTLS)的進行修正，以滿足物聯網的特性。			
6	8152	Standards Track Possible Obsolete soon	2017/07	Security COSE CBOR	cose
		CBOR Object Signing and Encryption (COSE) 將用 RFC 7049 (CBOR)產生的 JSON 資料進行加密和簽章。			
7	8230	Standards Track	2017/09	Security COSE CBOR	cose

編號	RFC號	狀態	時間	類別	工作小組
		Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages 補充 COSE 物件進行加密和簽章時，可以使用 RSA 演算法，及相關的參數。			
8	8392	Standards Track	2018/05	Security CBOR	ace
		CBOR Web Token (CWT) 討論在一個 CWT 中的宣言，使用 CBOR 編碼，CBOR 物件簽章與加密(COSE)用於增加應用層的安全保護。			
9	7815	Informational	2016/03	Internet IKEv2	lwig
		Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation 描述在一個受限制節點上，最小的網際網路金鑰交換協定(IKEv2)。IKEv2 歸屬於 IPsec 協定之下，用於身份驗證以及建立與維持安全關聯(Security Associations，SAs)。			

關於網路層與傳輸層 37 篇的彙整資訊如下表所述：

表 102、網路層與傳輸層類別的彙整資訊

編號	RFC號	狀態	時間	類別	工作小組
1	4944	Standards Track	2007/09	Internet 6loWPAN	6lo 6lowpan
		Transmission of IPv6 Packets over IEEE 802.15.4 Networks 詳述在 IEEE 802.15.4 網路上傳輸 IPv6 封包的訊號框格式，以及形成 IPv6 本地連結位址和無狀態自動配置地址的方法。並說明一種標頭壓縮方法。			
2	6282	Standards Track	2011/09	Internet 6loWPAN	6lo 6lowpan
		Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks 更新 RFC 4944。規範了在 6LoWPAN 上傳遞 IPv6 封包時的 IPv6 標頭壓縮格式。同時使用這個框架規範 UDP 的標頭壓縮。			
3	7400	Standards	2014/12	Internet	6lo

編號	RFC 號	狀態	時間	類別	工作小組
		Track		6loWPAN	
		6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) 規定了一種簡單的附加，它能夠壓縮通用標頭和類似標頭的有效載荷，而無需為每個新標頭或類似標頭的有效負載定義新的標頭壓縮方案。			
4	7973	Informational	2016/11	Internet 6loWPAN	6lo
		Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation 當通過以太網等第 2 層技術承載時，必須識別使用 RFC 4944 中定義的低功耗無線個人網路(LoWPAN)封裝的 IPv6 封包，以便接收器能夠正確解釋編碼的 IPv6 封包。			
5	8025	Standards Track Update RFC 4944	2016/11	Internet 6loWPAN	6lo
		IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch 更新 RFC4944。引入新的文本切換機制，以支援 6LoWPAN 壓縮。以頁(Page)的型式，並通過 Paging Dispatch 來指派。			
6	8066	Standards Track Updates RFC 4944, RFC 6282	2017/02	Internet 6loWPAN	6lo
		IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines 更新 RFC 4944 和 RFC 6282，定義 ESC 擴充碼的碼點和列舉已知使用案例的註冊條目。			
7	6606	Informational	2012/05	Internet 6loWPAN	6lo 6lowpan
		Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing 6LoWPAN 由與 IEEE 802.15.4 標準兼容的設備構成，但是 IEEE 802.15.4 標準和 6LoWPAN 格式規範都沒有定義如何獲得網狀拓撲，本文提供了 6LoWPAN 路由的問題陳述和設計空間。			
8	6550	Standards	2012/03	Routing	roll

編號	RFC號	狀態	時間	類別	工作小組
		Track		RPL	
		RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks 詳述低功耗有損網路(Low-Power and Lossy Network，LLN)上的IPv6 路由協定(RPL)。			
9	6551	Standards Track	2012/03	Routing RPL	roll
		Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks 規定一組連結和節點路由度量和限制，適用於低功耗有損網路路由協定(RPL)使用的 LLN。			
10	6687	Informational	2012/10	Routing RPL	roll
		Performance Evaluation of the Routing Protocol for Low-Power and Lossy Networks (RPL) 介紹了低功耗有損網路路由協定(RPL)的性能評估，用於小型室外部署傳感器節點和大規模智慧電錶網路。			
11	6552	Standards Track	2012/03	Routing RPL	roll
		Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL) 設定一個基本的目標函數，該函數僅依賴於低功耗有損網路路由協定(RPL)中定義的對象，並且不使用任何協定擴充。			
12	6553	Standards Track	2012/03	Routing RPL	roll
		The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams 詳述 RPL 路由器中使用的 RPL 選項，以包括此類路由資訊。			
13	6554	Standards Track	2012/03	Routing RPL	roll
		An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL) 指定了一種新的 IPv6 路由標頭類型，用於在 RPL 路由域內傳遞資料封包。			
14	8585	Informational	2019/05	Internet	v6ops
		Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service 規定 IPv6 客戶邊緣(CE)路由器的 IPv4 服務連續性要求，這些要求由服務供應者或透過零售市場銷售的供應商提供。			

編號	RFC號	狀態	時間	類別	工作小組
15	6719	Standards Track	2012/09	Routing RPL	roll
		The Minimum Rank with Hysteresis Objective Function 描述具有最小秩遲滯目標函數(Minimum Rank with Hysteresis Objective Function, MRHOF)，該目標函數選擇最小化度量的路由，同時使用滯後來減少度量變化的流失。			
16	6997	Experimental	2013/08	Routing RPL	roll
		Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks 規定一種點對點路由發現機制，是對低功耗有損網路路由協定(RPL)核心功能的補充。			
17	6998	Experimental	2013/08	Routing RPL	roll
		A Mechanism to Measure the Routing Metrics along a Point-to-Point Route in a Low-Power and Lossy Network 規定了一種機制，得以讓低功耗有損網路路由協定(RPL)路由器可以延著已經存在的一條到另外一個RPL路由器的路由測量指定度量的聚合值，從而讓該路由器決定是否要啟動路由發現機制去尋找一條更好的路由。			
18	8036	Standards Track	2017/01	Routing RPL	roll
		Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks 討論低功耗有損網路(RPL)路由協定在高級計量基礎設施(AMI)網路中的適用性。			
19	6206	Informational	2011/03	Routing	roll
		The Trickle Algorithm 詳述了 Trickle 演算法及其使用的注意事項。Trickle 演算法允許有損共享媒體(例如：低功耗有損網路)中的節點能以高強度，節能，簡單和可擴充的方式交換資訊。			
20	7787	Standards Track	2016/04	Internet HomeNet DNCP	homenet
		Distributed Node Consensus Protocol 描述分佈式節點共識協定(DNCP)，這是一種使用 Trickle 演算			

編號	RFC號	狀態	時間	類別	工作小組
		法和雜湊樹的通用狀態同步協定。			
21	8138	Standards Track	2017/04	Routing RPL 6LoWPAN	roll
		IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header 引入一種用於 6LoWPAN 路由的新調度類型，涵蓋了低功耗有損網路路由協定(RPL)的需求。			
22	6775	Standards Track Update 4944	2012/11	Internet 6loWPAN	6lo 6lowpan
		Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) 描述一個對於 6LoWPAN 的 IPv6 鄰居發現機制的簡單優化，定址機制，重覆位址偵測。			
23	8505	Standards Track Updates RFC 6775	2018/09	Internet 6LoWPAN	6lo
		Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery 更新 RFC 6775 低功耗無線個人網路(6LoWPAN)鄰居發現規範，以闡明協定作為註冊技術的作用，簡化 6LoWPAN 路由器中的註冊操作，同時提供增強功能。			
24	7428	Standards Track	2015/02	Internet 6lo	6lo
		Transmission of IPv6 Packets over ITU-T G.9959 Networks 詳述在 ITU-T G.9959 網路上傳輸 IPv6 封包的訊號框格式，以及形成 IPv6 本地連結位址和無狀態自動配置地址的方法。			
25	7554	Informational	2015/09	Internet 6tisch	6tisch
		Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement 描述在低功耗有損網路(Low-Power and Lossy Network，LLN)的情境下，使用 IEEE 802.15.4e TSCH 媒體存取控制(MAC)協定的環境、問題陳述、與目的。			
26	8180	Best Current Practice	2017/05	Internet 6tisch	6tisch

編號	RFC 號	狀態	時間	類別	工作小組
		BCP 210			
		Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration 描述在 IEEE 802.15.4e TSCH 上支援 IPv6 的最小操作模式。			
27	8480	Standards Track	2018/11	Internet 6tisch	6tisch
		6TiSCH Operation Sublayer (6top) Protocol (6P) 描述 IEEE 802.15.4e TSCH 操作子層協定(6P)。是 6TiSCH 操作子層(6top)的一部份，允許在 6TiSCH 網路上啟用分散式排程。			
28	7668	Standards Track	2015/10	Internet 6lo	6lo
		IPv6 over BLUETOOTH(R) Low Energy 詳述如何通過低功耗無線個人網路 (6LoWPAN) 技術在低功耗藍牙上傳輸 IPv6 封包。			
29	8105	Standards Track	2017/05	Internet 6lo	6lo
		Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE) 描述如何通過低功耗無線個人網路 (6LoWPAN) 技術在 DECT ULE 上傳輸 IPv6 封包。			
30	8163	Standards Track	2017/05	Internet 6lo	6lo
		Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks 本規範通過最大程度地利用現有標準，直接在建築自動化和控制網路中的有線終端設備上啟用 IPv6，並與傳統的 MS/TP 實現共存。MS/TP 設備通常類似於 6LoWPAN 網路中面臨的限制			
31	8272	Informational	2017/11	Internet 6LoWPAN	6lo 6lowpan ipfix
		TinyIPFIX for Smart Meters in Constrained Networks 規定 TinyIPFIX 協定，如何在限制網路(如 6LoWPAN)中傳輸 TinyIPFIX 資料和模板記錄，以及如何將 TinyIPFIX 資料轉換為代理設備中不是 TinyIPFIX 的資料。			
32	8375	Standards Track	2018/05	Internet HomeNet DNS	homenet
		Special-Use Domain 'home.arpa.'			

編號	RFC號	狀態	時間	類別	工作小組
		指定了域名系統對於以“.home.arpa”結尾的名稱的 DNS 查詢所期望的行為。			
33	7695	Standards Track	2015/11	Internet HomeNet	homenet
		Distributed Prefix Assignment Algorithm 指定了一種分佈式演算法，用於以允許自動分配唯一且不重疊的子前綴的方式劃分一組前綴。			
34	8539	Standards Track	2019/03	DHCP	dhc
		Softwire Provisioning Using DHCPv4 over DHCPv6 定義一個 DHCPv6 選項，用於傳達建立 Softwires 通道的 IPv6 參數和一個 DHCPv4 選項(僅用於 DHCP 4o6)，以在 DHCP 4o6 客戶端和伺服器之間傳送資源通道的 IPv6 位址。			
35	7731	Standards Track	2016/02	Routing RPL MPL	roll
		Multicast Protocol for Low-Power and Lossy Networks (MPL) 描述在低功率有損耗網路上群播協定，提供在受限制網路上 IPv6 群播轉送。			
36	7744	Informational	2016/01	Security ACE	ace
		Use Cases for Authentication and Authorization in Constrained Environments 定義了一種通過 DHCPv6 選項為 MPL(低功耗有損網路的群播協定)配置參數集的方法。			
37	7732	Informational	2016/02	Routing RPL MPL	roll
		Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL) 描述了用於低功耗有損網路多播協定(Multicast Protocol for Low-Power and Lossy Networks，MPL) (RFC 7731)的自動化策略			

大致上，我們可以看到 IETF 從連結層、網路層、傳輸層到應用層幾個面個都有相關的 RFC 說明標準實施方向。在應用層，有輕量級

的 CoAP 系列 RFC 來替代 HTTP，用二進制的 CBOR 訊息來替代純文字的 JSON 訊息，CBOR 訊息的加密與簽章來確保訊息的安全。在傳輸層與網路層，同樣有輕量級的 6LoWPAN 來替代完整的 IPv6 協定堆疊，並制 RPL 相關路由協定來協助物聯網環境裡可能遇到的情形。同時，在低功耗有損網路 LLN 的概念下，針對不同的實體網路制定相關的協定，以協助受限制裝置在受限制網路裡完成資料傳輸。

此 81 篇 RFC 的資訊詳細資訊，各篇的摘要內容及中文翻譯資訊請參考附錄十及附錄十一。

隨產業需求及網際網路的發展，新的研究議題不斷被提出，IETF 除有專門的工作小組在進行物聯網與 IPv6 相關的技術研議之外。網際網路研究工作小組（IRTF，Internet Research Task Force），於西元 2015 年(104 年)成立了物聯網專門研究小組(T2TRG，Thing-to-Thing)，以調查物聯網的開放性研究問題，重點在關注 IETF 所公布的標準協議可能潛在問題的研究。正在探討的主題包括物網聯的安全與挑戰，在物聯網場景中使用 REST 的方法以及語義等相關議題。並對於在物聯網領域的其他組織的討論和進展，持續追蹤及了解其發展方向和相互合作。例如，W3C 中的 WoT 小組（Web of Things），兩個小組持續共同探討物聯網和網路技術的未來和挑戰。

第二節　研析物聯網、5G 與 IPv6 相關的國際技術標準（RFC）內容

從上述 81 篇 RFC 中，我們選出 23 篇相對重要的 RFC 進行全文翻譯，列表如下：

表 103、全文翻譯的 23 篇 RFC 列表

序號	RFC編號	RFC標題
1	RFC4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks
2	RFC6282	Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks
3	RFC6550	RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks
4	RFC6775	Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)
5	RFC7049	Concise Binary Object Representation (CBOR)
6	RFC7228	Terminology for Constrained-Node Networks
7	RFC7252	The Constrained Application Protocol (CoAP)
8	RFC7368	IPv6 Home Networking Architecture Principles
9	RFC7428	Transmission of IPv6 Packets over ITU-T G.9959 Networks
10	RFC7554	Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement
11	RFC7668	IPv6 over BLUETOOTH(R) Low Energy
12	RFC7732	Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL)
13	RFC7815	Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation
14	RFC7925	Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things
15	RFC8025	IPv6 over Low-Power Wireless Personal Area Network

序號	RFC編號	RFC標題
		(6LoWPAN) Paging Dispatch
16	RFC8066	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines
17	RFC8105	Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)
18	RFC8138	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header
19	RFC8152	CBOR Object Signing and Encryption (COSE)
20	RFC8163	Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks
21	RFC8180	Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration
22	RFC8230	Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages
23	RFC8376	Low-Power Wide Area Network (LPWAN) Overview

以下列出這 23 篇 RFC 的重點整理。

以上 23 篇，依據其內容可以分為 4 大類別，分別為概念型 3 篇、應用層 2 篇、資訊安全 4 篇及網路層與傳輸層 14 篇。下表為此計畫研究物聯網全文翻譯 RFC 分類統計資訊：

表 104、物聯網相關 RFC 全文翻譯分類

序號	類別	RFC 編號	篇數
1	概念型	RFC 7228、RFC 7368、RFC 8376	3
2	應用層	RFC 7252、RFC 7049	2
3	資訊安全	RFC 7925、RFC 7815、RFC 8152、RFC 8230	4
4	網路層與傳輸層	RFC 6550、RFC7732、RFC 4944、RFC 7428、RFC 8163、RFC 8105、RFC 7668、RFC 7554、RFC 8180、RFC 6282、RFC 8025、RFC 8066、RFC 6775、RFC 8138	14
合計			23

關於概念型 3 篇的內容重點如下表所述：

表 105、概念型 3 篇的內容重點

序號	RFC 編號	內容重點
1	7228	擁有受到限制的 CPU，記憶體，以及能源的小型設備被稱為“受限制性設備”的裝置數量正在日益增加，而這些“受限制設備”可以構成“受限制網路”，可以在物聯網中產生作用，為了應對未來可能會遇到大面積使用此類設備與網路的狀況，該文對這類文件進行了規範化處理，設定了一些規範來定義，規劃此類設備與網路。 對此類設備依照處理能力，功耗等各個方面來進行劃分等級，對其進行分類。設備的受限制等級（如其運算能力，功耗等）分為 0 類，1 類，2 類三種。 按照設備的可用能源的限制來劃分，不受限制的為 E9，一次性電池耗盡時被丟棄的設備為 E1，可充電的設備可以劃為 E2，可能存在可用於特定事件的有限量的能量，例如，用於能量收集燈開關中的按鈕按壓; 這些設備被歸類為 E0。
2	7368	本文描述了住宅家庭網路中不斷發展的網路技術，其中設備數量越來越多，內部路由越來越多。本文的目標是定義基於 IPv6 的家庭網路的通用架構，描述相關的原則，注意事項和要求。本文簡要強調了 IPv6 引入家庭網路的具體含義，討論了該架構的各個要素，並建議如何在家庭網路中採用標準的 IPv6 機制和定址。該體系結構描述了對特定附加功能的特定協定擴充的需求。假設 IPv6 家庭網路不是主動管理的，並且作為僅 IPv6 或 IPv4/IPv6 雙堆疊網路運行。本文中沒有針對 IPv4 部分的建議。 本文中主要關注於在引入 IPv6 時要解決的問題，著眼於比今天使用 IPv4 更好的結果，以及提供更一致的解決方案，以盡可能滿足已確定的要求。本文旨在為家庭網路中如何使用標準 IPv6 機制和定址提供基礎和指導原則，同時與現有的 IPv4 機制共存。在新興的雙堆疊家庭網路中，引入 IPv6 對 IPv4 操作沒有不利影響至關重要。我們假設家庭網路中的 IPv4 網路架構就是這樣，並且不能通過新建議進

序號	RFC 編號	內容重點
		行修改。本文未討論 IPv4 家庭網路如何提供對多個子網的支援。不應該假設任何未來使用 IPv6 創建的新功能將向後相容，以支援 IPv4。 此外，未來的部署或在其他 IPv4/IPv6 雙堆疊家庭網路內的特定子網可能僅是純 IPv6 環境，在這種情況下，考慮 IPv4 的影響將不適用。 本文提出了一種基本家庭網路體系結構，盡可能使用經過驗證和可靠的協定和實現。本文的範圍主要是網路層技術，提供了實現定址、連接、路由、命名和服務發現的基本功能。 例如，雖然家庭網路組件應該易於部署和使用，但本文不討論特定的用戶界面，也不討論特定的物理、無線或數據鏈路層考慮因素。同樣，也沒有從上到下指定整個家庭網路路由器的設計; 相反，專注於第 3 層方面。這表示第 2 層在很大程度上超出了本文範圍。假設存在支援 IPv6 的資料鏈路層，並且會做出相應的反應。
3	8376	低功率廣域網路（LPWAN）是具有諸如大覆蓋區域、低頻寬、可能非常小的封包以及使用電池等特性的無線技術。本文提供 IETF IPv6 低功耗廣域網路工作小組正在考慮的技術概述和背景資料，以及這些技術需求與在 LPWAN 中運行時的差距。本文還提供了這些技術需求與當前可用的 IETF 規範之間的分析。 本文不是網際網路標準規範，以提供資訊為目的。 該領域的大多數技術旨在實現類似的目標，即以極低的功耗支援大量極低成本、低吞吐量的設備，具有長距離傳輸能力以覆蓋大面積，即使是電池供電的設備也可以部署多年。 本文介紹 LPWAN 技術：LoRaWAN、窄頻物聯網(NB-IoT)、Sigfox、Wi-SUN 聯盟用戶端場域網路(FAN)。本文介紹使用 LPWAN 的一些應用可能會引起的隱私考慮。另一個挑戰是如何處理密鑰管理和相關協定。

關於應用層 2 篇的內容重點如下表所述：

表 106、應用層 2 篇的內容重點

序號	RFC 編號	內容重點
1	7252	受限制的應用協定(CoAP)是一種專門的 web 傳輸協定，用於受限節點和受限制的網路。節點通常具有 8 位元的微控制器，具有少量 ROM 和 RAM，而低功耗無線的 IPv6 等則受限制網路個人區域網路(6LoWPAN)常常有高封包錯誤率和典型的 10 kbit/s 的網路輸送量。該協定專為機器對機器(M2M)應用而設計，如智慧能源和建築自動化。 特點如下： • Web 協定在受限環境中可滿足 M2M 需求 • 基於 UDP，擁有可選的可靠性保障，支援單播和多播請求 • 非同步訊息交換 • 低標頭 overhead 且解析複雜度 • 支援 URI 與 HTTP 內容類型 • 簡單的代理和緩衝區功能 • 無狀態 HTTP 映射時，允許構建代理，以統一的方式通過 HTTP 訪問 CoAP 資源，或者通過 CoAP 實現 HTTP 的簡單介面 • 安全綁定到 DTLS 資料封包傳輸層安全(DTLS) 訊息傳輸特點： • 對於可確認的訊息，具有指數級回退的簡單停等重傳可靠性。 確認和非確認訊息的重複檢測。
2	7049	簡明二進制對象表示（CBOR）是一種數據格式，其設計目標包括極小的代碼大小，相當小的訊息大小和可擴充性，而無需版本協商。這些設計目標使它不同於早期的二進位序列化，如 ASN.1 和 MessagePack CBOR 的目標為： • 這種表示必須能夠明確地編碼網際網路標準中使用的最常見的資料格式。它必須使用二進位編碼表示一組合理的基底資料型別和結構。這裡的“合理”，在很大程度上受 JSON 功能的影響，主要是二進位位元組字串的添加。所支援的結構僅限於陣列和樹；循環圖表和點陣圖不被移

序號	RFC 編號	內容重點
		植。沒有要求所有資料格式都是唯一編碼的；也就是說，用多種不同的方式編碼數字“7”是可以接受的。 • 編碼器或解碼器的代碼必須緊湊，以支援記憶體、處理器電源和指令集非常有限的系統。編碼器和解碼器需要在非常少量的代碼中實現。該格式應使用現代機器表示的資料（例如，不需要二進位到十進位轉換）。 • 資料必須能夠在沒有模式描述的情況下解碼。與 JSON 類似，編碼資料應該是自描述的，這樣就可以編寫通用的解碼器。 • 序列化必須合理地緊湊。這裡的“合理”是指與 JSON 比較，實現序列化的複雜度來限定的。使用一般的壓縮方案或大量的位元處理都會違反複雜度目標。 • 該格式必須同時適用於受約束的節點和大容量應用程式。這意味著在編碼和解碼方面，CPU 的使用必須相當節儉。這既適用於受約束的節點，也適用於資料量非常大的應用程式中的潛在用途。 • 該格式必須支援所有 JSON 資料類型，以便在 JSON 之間進行轉換。只要表示的資料在 JSON 的能力範圍內，它就必須支援合理的轉換級別。必須能夠為所有類型的資料定義指向 JSON 的單向映射。 格式必須是可擴充的，並且擴充資料必須可以被早期的解碼器解碼。這種格式是為幾十年的使用而設計的。格式必須支援一種允許回退的擴充形式，以便不理解擴充的解碼器仍然可以對訊息進行解碼。

關於資訊安全 4 篇的內容重點如下表所述：

表 107、資訊安全 4 篇的內容重點

序號	RFC 編號	內容重點
1	7925	物聯網（IoT）部署中的常見設計模式是使用受限制設備，該設備通過傳感器收集數據，以用於家庭自動化，工業控制系統，智慧城市和其他物聯網部署。

序號	RFC 編號	內容重點
		本文定義了傳輸層安全協定（TLS）和資料封包傳輸層安全協定（DTLS）配置文件，為數據交換提供安全，以防止竊聽，篡改和訊息偽造。缺乏安全是物聯網產品中的常見漏洞，可以通過使用這些經過充分研究和廣泛部署的網際網路安全協定解決。 IoT 設備能夠交換數據通常需要對兩個端點進行身份驗證，並且能夠為交換的數據提供完整性和機密性保護。雖然可以在協定堆疊的不同層提供這些安全服務，但是使用傳輸層安全協定(TLS)/資料封包傳輸層安全協定(DTLS)已經受到許多應用程序協定的歡迎，對物聯網很有用。 將網際網路協定安裝到受限制設備中可能很困難，但由於標準化工作，可以使用新的配置文件和協定，例如受限制的應用協定（CoAP）[RFC7252]。CoAP 訊息主要通過 UDP/DTLS 傳輸，但也可以使用其他傳輸，例如 SMS（如附錄 A 中所述）或 TCP（由[COAP-TCP-TLS]提出）。 本文的主要目的是使用 DTLS 1.2 [RFC6347]保護 CoAP 訊息，但各節中包含的訊息不僅限於 CoAP，也不限於 DTLS 本身。 本文定義了 DTLS 1.2 [RFC6347]和 TLS 1.2 [RFC5246]的配置文件，為物聯網應用程序提供通信安全服務，並且可在許多受限制設備上實現。因此，配置文件意味著利用可用的配置選項和協定來擴充以支援 IoT 環境。本文不會改變 TLS/DTLS 規範，也不會引入任何新的 TLS/DTLS 擴充。本文的主要目標讀者是配置和使用 TLS/DTLS 堆疊的嵌入式系統開發人員。但是，該文也可以幫助那些為物聯網產品開發或選擇合適的 TLS/DTLS 堆疊的人。
2	7815	這份文件描述在一個受限制節點上，最小及初始版本的網際網路金鑰交換協定(IKEv2)。IKEv2 歸屬於 IPsec 協定之下，用於身份驗證以及建立與維持安全關聯(Security Associations，SAs)的運作。IKEv2 包含數個可選功能，在最小限度運行的要求中是不需要的。本文描述了對最小限度運行的要求，以及多種可被運行的最佳化成果。此處描述的協定可與使用共享密鑰身份驗證的完整 IKEv2 方法相互操作(IKEv2 無需使用身份驗證)。這個最小的啟動器只能與扮演回應者的完整 IKEv2 進行溝通。因此，兩個最小

序號	RFC 編號	內容重點
		的啟動器無法彼此通信。 此文件並非一個網路標準的規範，只是用於提供訊息。 網際網路協定越來越多地用於對電源、內存和處理資源有嚴格限制的小型設備上。本文描述了最小的 IKEv2 運行，設計用於可與網際網路密鑰交換協定版本 2（IKEv2）相互操作的受限制節點。主要描述如何在 IKEv2 中使用共享密鑰進行身份驗證，因為它最容易運行，也描述了如何使用原始公鑰而不是共享密鑰身份驗證。
3	8152	本文定義了 CBOR 物件簽章和加密（COSE）協定。簽章方面，它支援兩種不同的結構，及不同的情況下的參數。本文定義了如何計算簽章和驗證簽章的步驟，描述如何使用 CBOR 序列化來建立和處理簽章，訊息鑑別碼和加密。文件中提到加密物件內容密鑰的分配方法，和如何進行加密與解密，MAC 物件的內容如何計算及驗證。 文中介紹兩種簽章演算法，ECDSA 和 Edwards 曲線數位簽章演算法，訊息鑑別碼演算法可使用雜湊訊息鑑別碼和 AES 訊息驗證碼，內容加密演算法有 AES GCM, AES CCM, ChaCha20 和 Poly1305，及密鑰函數及密鑰分配方法，附錄中並提列數個 CBOR 編碼的範例。 在正常情況下，資料可以使用 JSON 格式去做傳輸，而物聯網（IoT）小型受限制設備會有傳輸上的限制。簡明二進制物件表示法（CBOR）是一種專為小程式和小訊息設計的數據格式。為提供 IoT 訊息安全服務，本文為 CBOR 格式定義基本安全服務，進行簽章及加密的動作。
4	8230	補充 COSE 物件進行加密和簽章時，可以使用 RSA 演算法，及相關的參數。

關於網路層與傳輸層 14 篇的內容重點如下表所述：

表 108、網路層與傳輸層 14 篇的內容重點

序號	RFC 編號	內容重點
1	6550	本文規定了 IPv6 的 LLN 路由協定，詳述了低功耗有損網

序號	RFC 編號	內容重點
		路(RPL)的 IPv6 路由協定。 網路可以同時運行多個 RPL 實例，而本文定義了單個實例的運行方式。RPL 實例可以提供路由給已訂定的前綴目的地，能通過 DODAG 根或 DODAG 中的備用路徑到達。這些根為獨立運作，可通過網路進行協調，不像 LLN 一樣受限。RPL 實例有兩種類型：本地和全局，且任何給定的 RPL 實例都是儲存或非儲存模式。本文介紹了可能形成的基本 RPL 拓撲，以及構建、識別、維護這些拓撲結構的規則及方法。也提到了 RPL 發現和上/下行路由的維護、目的地公告及安全機制。上行路由使用 DIS 用於引發傳送 DIO 訊息以進行發現及維護；下行路由以 RPL 通過目的地公告對象（DAO）訊息來構造和維護，主要分為兩種模式：儲存模式和非儲存模式。由目標函數（OF）定義了 RPL 節點如何選擇和優化路由。RPL 支援訊息的機密性和完整性，有三種自己的基本安全模式：不安全、欲安裝、已鑑別。而最後則是相關資訊的新註冊表內容。 低功耗有損網路(LLN)由幾十個到幾千個路由器(受限節點)組成，是一種路由及互連都受到約束的網路。LLN 路由器通常在處理能力，記憶體和能量(電池電量)端面受到限制。它們的互連具有高損耗率，低數據速率和不穩定性的特點。支援包括點對點、點對多點，以及多點對點的通信流。 目的： • 最小化能量 • 最小化延遲 • 滿足約束目標 • 最小化路徑(路由) • 最小化監控未使用的連接成本 上/下行路由的維護
2	7732	本文用於完善其他文件的定義。本文描述了用於低功耗有損網路多播協定（MPL Multicast Protocol for Low-Power and Lossy Networks）[RFC7731]的自動化策略（automated policy automated policy），該策略在位於運行 MPL 的網路和其他網路之間的邊界路由器內使用 Admin-Local 範圍轉發多播訊息。

序號	RFC 編號	內容重點
		MPL 的自動化策略需要通過 Admin-Local 範圍來配置。多播範圍在 RFC 4291 中被定義。RFC 7346 使用以下文本擴充定義範圍：Interface-Local，Link-Local 和 Realm-Local 範圍邊界，自動從物理連接或其他非多播相關配置派生。全域範圍（Global Scope）是沒有邊界的。Admin-Local 或更大的所有其他非保留範圍的邊界，由管理方式配置。 該文設定了相關的 MPL4 術語，界面參數等等。MPL4 路由器擁有相關的演算法用來確定 MPL 訊息可以傳播的網路層。該文定義了什麼是合法的多播訊息與 MPL 選項，以及 MPL 訊息在介面上的轉發方式等等。
3	4944	IPv6 封包並非先天適合 IEEE 802.15.4 網路。由於低吞吐量、緩衝有限、封包只有 IPv6 MTU 下限的十分之一，故必須壓縮標頭，進行資料分割，其次，由於 IEEE 802.15.4 特點為低功率、低吞吐量、使用射頻為媒介，較容易出現雜訊干擾、連結故障、不對稱連結(A 能聽見 B，但 B 無法聽見 A)，因此網路層必須具備彈性及迅速反應，同時維持低功率與高效能，本篇文章的目標為解決以上問題。 本文主要針對低功率無線個人區域網路。定義了 IPv6 [RFC2460]封包傳輸的訊號框格式，以及在 IEEE 802.15.4 網路之上形成 IPv6 連結本地位址和無狀態自動配置地址。由於 IPv6 需要支援比 IEEE 802.15.4 最大訊號框大小大得多的封包，因此定義了適應層，透過適應層以符合最低 MTU 的 IPv6 要求。本文也定義了使用 IPv6 在 IEEE 802.15.4 網路上實用所需的標頭壓縮機制，以及 IEEE 802.15.4 網格中封包傳送所需的規定。 為了讓不同設備製造商的設備之間能夠互連，需要製定統一的網路層標準。早期的無線感測網路缺乏一個共通的通訊協定標準，為了讓這些不同的感測網路裝置能夠互通，IPv6 over LR-WPAN (簡稱 6LoWPAN) 工作組，制定專屬於這些低功率、低可靠度、網路規模，極大網路裝置的互連通訊協定，即 IPv6 over IEEE802.15.4。因為 IP 對內存和頻寬要求較高，要降低它的運行環境要求以適應微控制器及低功率無線連接是比較難的。而 6LoWPAN 協定的制定提供了可能性。
4	7428	本文描述了用於傳輸 IPv6 封包裡的乙太網路訊號框以及

序號	RFC 編號	內容重點
		在 ITU-T G.9959 網路上形成 IPv6 鏈路本地地址和無狀態自動配置的 IPv6 地址的方法。 本文定義了 IPv6 資料封包傳輸的乙太網路訊號框，以及在 G.9959 網路上形成 IPv6 鏈路本地地址和無狀態自動配置的 IPv6 地址。一般方法是使 RFC4944 的元素適應 G.9959 網路。G.9959 提供分段和重組（SAR）層，用於傳輸大於 G.9959 媒體訪問控制協定數據單元（MAC PDU）的資料封包。RFC 6775 通過為 IPv6 鄰居搜索（ND）（最初由 RFC 4861 定義）的低功耗無線個人區域網路（6LoWPAN）優化指定 IPv6 來更新 RFC 4944。本文限制使用 RFC 6775 前綴和上下文頁面分配。介面標識符（IID）可以由 G.9959 鏈路層地址構成，從而產生“鏈路層導出的 IPv6 地址”。使用該方法，則不需要重複地址檢測（DAD）。可以透過 DHCP 集中分配 IPv6 地址，從而產生“非鏈路層導出的 IPv6 地址”。僅在某些情況下才需要地址註冊。除了 IPv6 應用程序通信之外，本文中定義的訊號框可以由 IPv6 路由協定使用，例如低功耗有損網路路由協定（RPL）[RFC6550]或點對點路由的反向發現。低功耗有損網路（P2P-RPL）[RFC6997]通過 G.9959 網路實現 IPv6 路由。由本文定義的封裝框架可以選擇透過 6LoWPAN 層下方的網格佈線來傳輸。網狀網路和其路由協定規範超出本文的範圍。 概述了適用於 G.9959 的 PHY 和 MAC 層的屬性以及如何將這些屬性用於 IPv6 傳輸。G.9959 定義了網路控制器如何分配唯一的 32 位 HomeID 網路標識符以及如何為每個節點分配 8 位 NodeID 主機標識符。 NodeID 在 HomeID 標識的網路中是唯一的。 G.9959 HomeID 表示由一個或多個 IPv6 前綴標識的 IPv6 子網。
5	8163	MS/TP 設備通常為具有有限處理能力和記憶體的低成本微控制器。這些限制以及低資料速率和小 MAC 位址空間，類似於 6LoWPAN 網路中面臨的限制。 該規範的主要目標是：(1)透過最大程度地利用現有標準，直接在建築自動化和控制網路中的有線終端設備上啟用 IPv6，以及(2)與傳統的 MS/TP 共存。共存允許 MS/TP 網路逐步升級以支援 IPv6。 為了與傳統設備共存，不允許對 BACnet 標準中規定的

序號	RFC 編號	內容重點
		MS/TP 定址模式，訊號框標頭格式，控制訊號框或主節點狀態進行任何更改。
6	8105	本文描述如何使用通過低功耗無線個人區域網路（6LoWPAN）技術在 DECT ULE 上傳輸 IPv6。 DECT 技術已在全球通信設備中使用了 20 多年。主要用於承載無線電話語音，但也用於以數據為中心的服務。DECT ULE 是 DECT 介面的最新成員，主要用於低頻寬，低功耗應用，如傳感器設備，智慧電錶，家庭自動化等。由於 DECT ULE 介面繼承了 DECT 的許多功能，因此受益於具有遠程和無干擾的全球保留頻段，低價格和成熟的操作。DECT ULE 的 IPv6 通信能力具有附加價值，例如物聯網應用程序。 DECT 是 ETSI 規定的標準系列，CAT-iq 是一套產品認證和互操作性配置文件，由 DECT 論壇定義。DECT ULE 是一種無線介面技術，建立在傳統 DECT/CAT-iq 的關鍵基礎之上，以犧牲資料流量為代價來降低功耗。 本文描述如何在 DECT ULE 鏈路上使用 IPv6 來優化功率，同時保持 IPv6 傳輸的多項優勢。RFC 4944，RFC 6282 和 RFC 6775 指定透過 IEEE 802.15.4 傳輸 IPv6。DECT ULE 具有許多類似於 IEEE 802.15.4 的特性，但也有差異。定義透過 IEEE 802.15.4 傳輸 IPv6 的機制子集，於 DECT ULE 鏈路上傳輸 IPv6。
7	7668	本文描述如何使用 IPv6 通過低功耗無線個人區域網路（6LoWPAN）技術使用低功耗藍牙傳輸 IPv6 訊息。 藍牙智慧型是藍牙技術聯盟定義的藍牙規範中藍牙低功耗特性（以下稱為“低功耗藍牙”）的品牌名稱。低功耗藍牙是一種無線電技術，適用於使用極低容量（例如鈕扣電池）電池或簡約電源工作的設備，低功耗藍牙設計用於以適度的數據速率不頻繁地傳輸少量數據，每位元的能量消耗非常小。這意味著低功耗、少量數據的特點非常適合於物聯網的使用。而物聯網的大量傳感設備也就需要非常大量的地址空間，所以才引入使用 IPv6。 考慮到傳感器和網際網路連接設備數量呈指數增長的可能性，IPv6 用於與這些設備進行通信是一種理想的協定，因為它提供了較大的地址空間。此外，IPv6 還提供了無狀

序號	RFC 編號	內容重點
		態地址自動配置工具，尤其適用於處理能力非常有限或缺乏完整操作系統或用戶界面的傳感器網路應用和節點。藍牙技術聯盟還發布了網際網路協定支援配置文件（IPSP），其中包括網際網路協定支援服務。IPSP 允許發現啟用 IP 的設備並建立用於傳輸 IPv6 資料封包的鏈路層連接。 為了描述如何使用 IPv6 通過低功耗藍牙傳輸訊息，本文首先講述了低功耗藍牙的原理與特性。包括堆疊與拓撲，每個低功耗藍牙設備都有一個 48 位元設備地址。通過低功耗藍牙為 L2CAP 固定通道定義的最佳 MTU 是 27 個位元組，包括 4 個八位元組的 L2CAP 標頭。之後講述了 IPv6 在低功耗藍牙上的工作原理，說明 IPv6 堆疊如何與低功耗藍牙 L2CAP 層之上的 GATT 堆疊並行工作。 低功耗藍牙協定(如 L2CAP)使用小端位元組排序，但 IPv6 資料封包必須以大端順序（網路位元組順序）傳輸。後面帶出了 IPv6 的標頭壓縮。
8	7554	本文描述了在低功耗有損網路（LLN）環境中使用 IEEE 802.14.4e 的時隙通道跳頻（TSCH）媒體存取控制（MAC）協定的環境，問題陳述和目標。 本文描述了在 LLN 背景下採用 TSCH 所產生的主要問題。附錄 A 進一步概述了 IEEE 802.15.4e 的 TSCH 修正案的主要特徵。TSCH 旨在使 IEEE 802.15.4 設備能夠支援廣泛的應用，包括但不限於工業應用。其核心是一種媒體存取技術，它使用時間同步來實現低功耗操作和通道跳躍，以實現高可靠性。同步精度會影響功耗，並且可能會在幾微秒到幾毫秒之間變化，具體取決於解決方案。這與傳統的 IEEE 802.15.4 MAC 協定非常不同，可說是重新設計。TSCH 不修改物理層，可以在符合 IEEE 802.15.4 的任何硬體上操作。 IEEE 802.15.4e 是針對 LLN 的最新一代超低功耗和可靠的網路解決方案。RFC 5673 討論了工業應用，並強調了 LLN 在工業環境中運行的操作條件以及可靠性，可用性和安全性要求。在這些環境中，具有大型（金屬）設備的大量部署環境會導致多徑衰落和干擾，從而阻礙單通道解決方案的嘗試；TSCH 的通道靈活性是其超高可靠性的關鍵。商

序號	RFC 編號	內容重點
		用網路解決方案現已上市，其中節點平均消耗 10 個微安，端到端資料封包傳輸率超過 99.999%。 TSCH 僅關注 MAC 層。這種乾淨的分層允許 TSCH 適合支援 IPv6 的 LLN 協定，通過低功耗無線個人區域網路（6LoWPAN）運行 IPv6 [RFC6282]，低功耗有損網路的 IPv6 路由協定（RPL）[RFC6550]和約束應用協定（CoAP）[RFC7252]。缺少的是負責調度要發送的訊號框的 TSCH 時隙的功能實體。在本文中，將此實體稱為“邏輯鏈路控制”（LLC），該實體的實現可以是不同類型的，包括分佈式協定或負責調度的集中式服務器。 雖然 IEEE.802.15.4e 定義了 TSCH 節點進行通信的機制，但它沒有定義構建和維護通信調度的策略，將該調度與 RPL 維護的多跳路徑相匹配，調整之間分配的資源。鄰居節點到數據業務流，對應用層生成的數據實施差異化處理，並對 6LoWPAN 和 RPL 發現鄰居，對拓撲變化作出反應，自行配置 IP 地址或管理密鑰資料所需的信號訊息進行處理。
9	8180	本文描述 6TiSCH (IEEE 802.15.4e 網路 TSCH 模式 IPv6) 的最小操作模式。這個最小操作模式指定了必需支援的協定基準集合，以及足以啟用 6TiSCH 功能網路的設定和操作模式的推薦。 在 IEEE 802.15.4 TSCH (Time-Slotted Channel Hopping)網路連結組成的 TSCH 網格之上，6TiSCH 提供 IPv6 連接能力。此最小模式使用具有相應配置的協定集合，包括 IPv6 6LoWPAN 框架，通過 IEEE 802.15.4 TSCH 實現可相互合作的 IPv6 連接。此最小配置提供了網路必要頻寬和安全導引，並為 IETF 協定與 IEEE 802.15.4 TSCH 之間的介面定義了適當的連結。所有符合 6TiSCH 標準的設備都應實現這個最小操作模式。
10	6282	這份文件指定了一個 IPv6 標頭壓縮格式，使得在低功耗個人區域網路路(6LoWPANs)中遞送 IPv6 封包。這種壓縮格式依賴於共享上下文，以允許壓縮任意前綴。而如何在共享上下文中保持訊息的完整性，超出本文範圍。這份文件指定了群播地址的壓縮方式，以及壓縮後續標頭的框架。在這個框架中也指定了 UDP 標頭的壓縮。

序號	RFC 編號	內容重點
		IEEE802.15.4 標準規定了 127 位元組的最大傳輸單元，在鏈路吞吐量為 250 kbps 或更低的無線鏈路上，在啟用安全性的情況下產生大約 80 個八位元組的實際媒體訪問控制（MAC）有效載荷。6LoWPAN 適應格式被指定用於在這種受約束的鏈路上承載 IPv6 資料封包，同時考慮到在無線傳感器網路的應用中預期的有限頻寬，儲存器或能量資源。RFC4944 定義了一個支援子 IP 轉發的網格尋址標頭，一個支援 IPv6 最小 MTU 需求的碎片標頭，以及針對 IPv6 數據(LOWPAN_HC1 和 LOWPAN_HC2)的無狀態標頭壓縮，以將相對較大的 IPv6 和 UDP 標頭減少(在最佳情況下)幾個位元組。 對於 6LoWPANs 中 IPv6 的大多數實際應用來說，LOWPAN_HC1 和 LOWPAN_HC2 是不夠的。本文定義了一種編碼格式，即 LOWPAN_IPHC，用於根據上下文中的共享狀態，有效壓縮唯一的本地、全局和群播 IPv6 地址。此外，本文還介紹了對 RFC4944 中定義的標頭壓縮格式的一些額外的改進。 本文還定義了 LOWPAN_HC1，一種任意後續標頭的編碼格式。LOWPAN_IPHC 指示是否使用 LOWPAN_IPHC 對以下標頭進行編碼。本文使用 LOWPAN_NHC 來定義了 UDP 的壓縮機制。雖然 RFC4944 為 UDP 定義了一種壓縮機制，但如果上層機制提供了可能性，如上層訊息完整性檢查(MIC)，則該機制不會啟動校驗和壓縮。此規範添加了在 6LoWPAN 上刪除 UDP 校驗總和的功能，從而可以保存另外兩個八字位元組。 此外，在使用 LOWPAN_NHC 時，本文定義了 IPv6-in-IPv6 封裝以及 IPv6 擴充標頭的編碼格式。
11	8025	低功耗有損網路（LLN）的設計通常側重於節約能源，這通常是一種非常受限制的資源。 控制資料傳輸量是節約能源的一種可能的方法。在許多 LLN 標準中，訊號框大小被限制為比 1280 位元組的 IPv6 最大傳輸單元（MTU）小得多的值。比較特別的是，依賴於 IEEE 802.15.4 實體層（PHY）的 LLN 會被限制在每個訊號框為 127 位元組。對於 IEEE 802.15.4 壓縮 IPv6 封包的需求促成了 6LoWPAN 標頭壓縮（6LoWPAN-HC）

序號	RFC 編號	內容重點
		[RFC6282]的工作。 為了減少在 IPV6 上傳遞訊息時相關的資源耗損，可以使用標頭壓縮的方法來減少工作量。該文建立在 RFC4944 的基礎上。 RFC4944 在 6LoWPAN 解析器中引入“解析上下文”的概念來適應 6LoWPAN，同時透過 IEEE 802.15.4 [RFC4944]保持與 IPv6 的向後相容性，該解析上下文由頁面標識。該規範定義了 16 個頁面。頁面在 6LoWPAN 資料封包中透過 Paging Dispatch 值分隔，該值指示下一個當前頁面。
12	8066	RFC 4944 的 5.1 節定義了調度(Dispatch)標頭和類型。ESC 類型被定義為在 6LoWPAN 標頭中使用附加的調度位元組。RFC 6282 修改了 ESC 調度類型的值，該值記錄在 IANA 註冊表中。但是，ESC 調度類型之後的位元組和用法未在 RFC 4944 或 RFC 6282 中定義。近年來，6LoWPAN 的部署、實施和標準組織已開始使用 ESC 擴充位元組。這顯示了更新 IANA 註冊政策的必要性。 本文定義了新的 ESC 擴充類型註冊表和 ESC 擴充位元組，以供將來的應用程式使用。此外，將 ITU-T 規範的 ESC 調度位元組碼點記錄為已知。 預期 RFC 4944 的現有措施不能處理本文中定義的 ESC 擴充資料位元組。為了互操作性，新的調度類型（EET）絕不能修改現有調度類型的行為。
13	6775	IETF 在低功耗無線個人區域網上的 IPv6 工作（6LoWPAN）定義了 6LoWPANs，如 IEEE 802.15.4。這個和其他類似的連結科技限制或不使用多播節能訊號。此外，無線網路可能不嚴格遵循傳統的 IP 子網概念和 IP 連結。 IPv6 鄰居發現不是為非傳遞無線鏈結所設計，因為其依賴於傳統的 IPv6 鏈結理念，並且大量的使用了多播，這使得其在低功耗有損網路中效率低並且有時候不切實際。因此，本文更新了 RFC4944,以便規範定義在這裡的優化的使用。考慮低功耗網路的特點，以及 IPv6 鄰居發現[RFC 4861]協定設計，一些對鄰居發現的優化和擴充對於在低功耗有損網路（例如：個人區域無限網路標準和其他同類低功耗網路）上廣泛部署 IPv6 非常有用）。

序號	RFC 編號	內容重點
		鄰居發現是一種專用於 IPv6 的新協定，由於 6LoWPAN 網路應用的特點，鄰居發現協定必須優化。為了更好地降低功耗，提出了限制多播路由請求和路由公告，避免重複位址檢測、多播鄰居請求和鄰居不可達檢測資訊等一系列 6LoWPAN 鄰居發現優化策略。 本規範介紹了針對低功耗有損網路如（底層網路）的 IPv6 鄰居發現[RFC4861]的以下優化： • 主機啟動的互動允許休眠主機。 • 消除主機基於多播的位址解析。 • 在單播鄰居請求（NS）和鄰居公告（NA）訊息中使用新選項的主機位址註冊功能。 • 一個新的鄰居發現選項，用於將低速無限個人網路標準標頭壓縮上下文分發給主機。 • 首碼和低速無限個人網路標準標頭壓縮上下文的多跳分佈。 多跳重複位址檢測（DAD），它使用兩種新的 ICMPv6 訊息類型。
14	8138	本文引入一種新的 IPv6 低功率無線個人區域網路（6LoWPAN）調度類型，用於 6LoWPAN 路由拓撲，最初涵蓋了低功耗有損網路（RPL）封包壓縮路由協定的需求。使用此調度類型，此規範定義了一種壓縮 RPL 選項和路由標頭類型 3 的方法，是一種高效的 IP-in-IP 技術，並且可擴充用於更多應用程序。 低功耗有損網路（LLNs）的設計通常以節約能源為主要考量，在大多數情況下，能源是非常有限的資源。其他限制，包含有損網路設備的儲存器容量和工作環境。 控制數據傳輸量是節省能源的一個可能方法。在許多有損網路標準中，訊號框大小被限制比 IPv6 最大傳輸單元（MTU）1280 位元組小得多。特別是依賴於 IEEE 802.15.4 物理層（PHY）的有損網路，限制每個訊號框最大為 127 位元組。透過 IEEE 802.15.4 壓縮 IPv6 資料封包的需求促成了基於 IEEE 802.15.4 網路上的 IPv6 封包壓縮格式。 出於安全性和將 ICMPv6 錯誤訊息發送回源頭的原因，原始封包不得被篡改，在 IPv6 封包中插入或刪除的任何訊息都必須放在額外的 IP-in-IP 封裝中。

序號	RFC 編號	內容重點
		使用頁面調度。該規範引入了一個新的 6LoWPAN 路由標頭（6LoRH）來承載 IPv6 路由訊息。6LoRH 可以包含來源路由訊息，例如 SRH 的壓縮形式，以及其他種類的路由訊息，例如 RPI 和 IP-in-IP 封裝。

此 23 篇 RFC 的資訊詳細資訊，各篇的內容重點及中文翻譯資訊請參考附錄十及附錄十二。

第八章 物聯網平台與應用資料蒐集與研析

雲端運算，是基於網際網路的資源使用方式，使用共享的軟硬體資源和按需求提供給不同終端電腦和其他裝置與服務的使用權利。能快速的搭建好企業級的資料庫或是電腦主機，無須透過傳統的硬體採購、安裝、網路配置、作業系統與服務開通的過程。可大幅度的降低資源操控的門檻，加速開發時程與有效的控制資源。雲端運算與物聯網被視為未來重要的產業趨勢與發展商機，物聯網主要是將物品透過有線或無線的聯網技術或感測設備與網際網路做連接，提供智慧化的辨識與資訊的管理及分享。物聯網的關鍵架構分為私有物聯網、公有物聯網、混合物聯網及社區物聯網，與雲端的私有雲、公有雲、混合雲概念不謀而合。更說明了雲端運算與物聯網結合將是未來發展趨勢。

根據 Gartner 的雲端基礎架構式服務 (Infrastructure-as-a-Service，IaaS) 領導品牌市場調查報告，西元 2019 年（108 年）雲端服務市場排名如下圖所示:

圖 140、西元 2019 年（108 年）雲端服務市場排名

由上圖可以看出，3 大領導品牌第一名為 Amazon Web Service，其次為 Microsoft Azure，而 Google Cloud Platform 緊追在後。

第一節 研析國際物聯網平台之設計

一.AWS（Amazon Web Services）IoT 平台

AWS IoT 可讓已與網際網路連線的 IoT 裝置連線至 AWS 雲端，並讓雲端中的 IoT 應用系統與其互動。IoT 應用系統收集並處理由來自各地 IoT 裝置的感測資料，必要時，也能遠端控制裝置。物件可以對不同的 MQTT 主題發佈訊息，以回報其狀態。每個 MQTT 主題都有一個階層式名稱，可識別正在更新狀態的裝置。當訊息以 MQTT 主題發佈時，此訊息會傳送至 AWS IoT MQTT 訊息中介裝置，再由訊息中介裝置將所有以 MQTT 主題發佈的訊息傳送至所有訂閱該主題的用戶端。

AWS IoT Core 能夠將裝置連接至 AWS 服務和其他裝置、保護資料和互動安全、處理裝置資料並採取行動，以及即使離線也能讓應用程式與裝置互動的平台。讓裝置透過 MQTT、HTTP 或 WebSocket 協定，與 AWS IoT Core 進行連線、驗證和交換訊息。支援 C、JavaScript 和 Arduino，而且內含用戶端程式庫、開發人員指南和製造商的移植指南。

AWS IoT 可在已與網際網路連線的裝置 (例如感測器、傳動器、嵌入式微控制器或智慧型設備) 和 AWS 雲端。AWS IoT 包含以下元件：裝置閘道、訊息中介裝置、規則引擎、安全與身分服務、裝置影子、裝置佈建服務、任務服務。

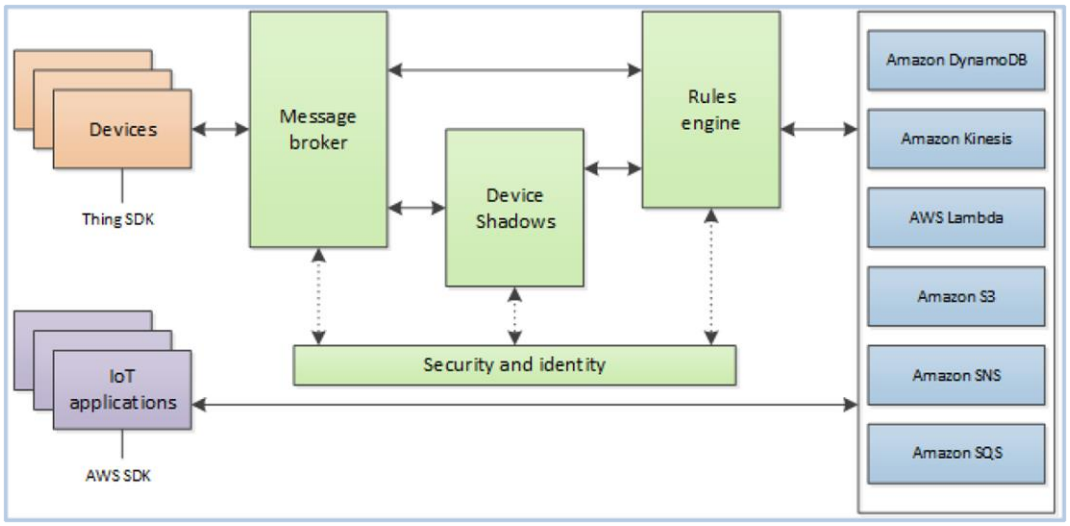

圖 141、AWS IoT 運作方式

AWS IoT 可讓已與網際網路連線的裝置連線至 AWS 雲端，並讓雲端中的應用程式與其互動。所有連線至 AWS IoT 的裝置，在登錄檔中都要有一個項目。登錄檔會存放裝置與該裝置使用之憑證(如 X.509)的相關資訊，以保護與 AWS IoT 之間的通訊。當裝置與 AWS IoT 通訊時，裝置會向 AWS IoT 提供憑證做為登入資料。

裝置以 JSON 格式對 MQTT 主題發佈訊息，用來回報其狀態。每個 MQTT 主題都有一個階層式名稱，可識別正在更新狀態的裝置。當訊息以 MQTT 主題發佈時，訊息會傳送至 AWS IoT MQTT 訊息中介裝置，再由訊息中介裝置將所有以 MQTT 主題發佈的訊息傳送至所有訂閱該主題的用戶端。

用戶端可以建立規則，定義根據訊息之內容執行的一個或多個動作。例如，插入、更新或查詢 DynamoDB 表格，或是呼叫 Lambda 函數。必要時，規則應包含 IAM 角色，授與 AWS IoT 權限使用相關的 AWS 資源。

每個裝置都有一個可存放及擷取狀態資訊的裝置影子。應用程式可以請求裝置目前狀態的資訊。裝置影子會回應請求，提供具有狀態資訊、中繼資料和版本編號的 JSON 文件。應用程式可要求變更裝置狀態，來控制裝置。裝置影子會接收狀態變更請求，更新其狀態資訊，並且傳送訊息指示狀態資訊已經更新。

相關 AWS IoT 包含以下元件描述如下：

- ◆ 裝置閘道讓裝置以安全有效的方式與 AWS IoT 通訊。
- ◆ 訊息中介裝置提供安全的機制，讓裝置和 AWS IoT 應用程式能夠互相發佈與接收訊息，可以直接使用 MQTT 通訊協定，或是經 WebSocket 的 MQTT 來發佈和訂閱，或是使用 HTTP REST 介面發佈。使用 MQTT 和 HTTPS 這兩種通訊協定均可透過 IPv4 及 IPv6 支援。
- ◆ 規則引擎可處理訊息並與其他 AWS 服務整合。以 SQL 為基礎的語言選擇資料，處理資料，然後傳送至其他服務，例如 Amazon S3 (Object Storage)、Amazon DynamoDB (NoSQL 資料庫)和 AWS Lambda (無伺服器運算)，或是使用訊息中介裝置重新發佈訊息給其他訂閱者。
- ◆ 安全與身分服務在 AWS 雲端對於雲端安全提供共同的責任。訊息中介裝置和規則引擎使用 AWS 安全功能，將資料安全傳送至裝置或其他 AWS 服務。登錄或群組登錄整理 AWS 雲端中與每項裝置相關聯的資源。自訂身分驗證服務可以定義自訂授權方，使用自訂身分驗證服務和 Lambda 函數，管理自己的身分驗證和授權策略。
- ◆ 裝置影子用於存放及擷取裝置目前狀態資訊的 JSON 文件。裝置影子服務提供裝置在 AWS 雲端中不變的表示方式，可以對

裝置影子發佈更新的資訊，裝置會在連線時同步其狀態，裝置也可以對裝置影子發佈其目前的狀態，供應用程式或其他裝置使用。

- ◆ 裝置佈建服務使用描述裝置所需資源的範本，來佈建裝置。
- ◆ 任務服務定義一組遠端操作，這組操作會傳送到連接 AWS IoT 的一個或多個裝置並且執行。

AWS IoT 整合了下列 AWS 服務: Amazon S3 (Simple Storage Service)，Amazon DynamoDB (NoSQL 資料庫)，Amazon Kinesis (大規模串流資料即時處理)，AWS Lambda (無伺服器運算)，Amazon SNS (Simple Notification Service)，Amazon SQS (Simple Queue Service)。AWS IoT API 使用 HTTP 或 HTTPS 請求來建置 IoT 應用程式。

在物聯網的情境中，裝置與 AWS 的網路連線基本上是以 AWS IoT Core 為進入點。在之後，則可以串接不同的服務，如 AWS IoT Analytics、Amazon QuickSight、AWS IoT Events、Amazon SNS、AWS Lambda 等等，這些後續的串接服務並不直接面向 IoT 裝置或一般使用者，屬於 management service，可以透過命令列工具(cli tool)或 web console 來管理或操作，不需要指定 domain name 或 IP address。

AWS 官網提供數個 IoT 的參考架構，根據 IoT 的應用情境，可以使用不同的 AWS 服務來建立許多不同類型的服務。裝置與 AWS 的網路連線基本上均是以 AWS IoT Core 為進入點，支援 IPv4 與 IPv6 兩種連接方式。

下圖展示一個工業預防性維護-機器學習建模與異常偵測的 AWS IoT 參考架構。在工廠端，使用了 AWS IoT Greengrass，提供邊緣運算服務，負責將 IoT 裝置感測到的資料進行預處理，並後送到 AWS IoT

Core。AWS IoT Core 收集到資料後，分兩路進行處理，一路是使用 Amazon Kinesis Data Firehose 串流服務將資料放到 Amazon S3 (物件儲存服務)，提供後續的 Amazon Athena 進行資料視覺化 Amazon QuickSight，以及 Amazon SegaMaker 進行機器學習建模，工廠端的 AWS IoT Greengrass 可以下載這個模型進行異常事件偵測。另一路，則可以透過 Amazon Kinesis Data Streams、Amazon Kinesis Data Analytics，進行不同類型的處理，並透過 Amazon SNS 發送訊息給相關人事。

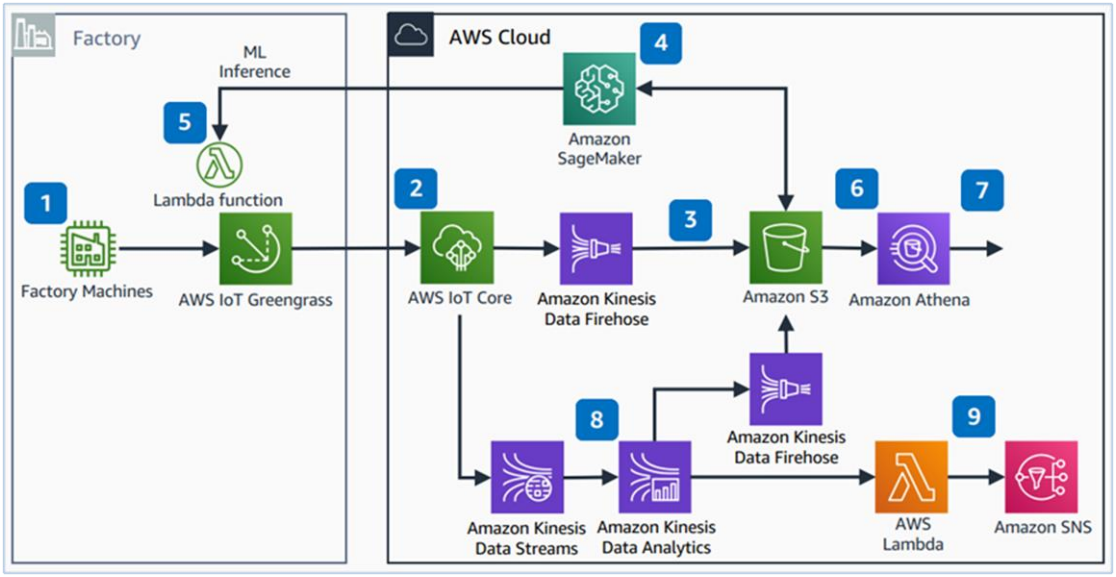

圖 142、AWS IoT 工業預防性維護參考架構

以下簡介幾個 AWS IoT 的應用情境：

(一) LG ThinQ

西元 2017 年（106 年），知名家電品牌 LG 已在全球銷售超過 7 千萬台的 Smart TV 和 5 百萬個 Home Applicans，為其內建 Wi-Fi 的 ThinQ 系列產品，LG 使用 AWS IoT 平台建立了自己的 IoT 平台，來聯結其 ThinQ 系列的 Smart 裝置與 LG 伺服器。LG 使用了

AWS IoT 與無服務器(serverless)架構，支援其空氣品質監控服務、客服機器人、和能源方案。

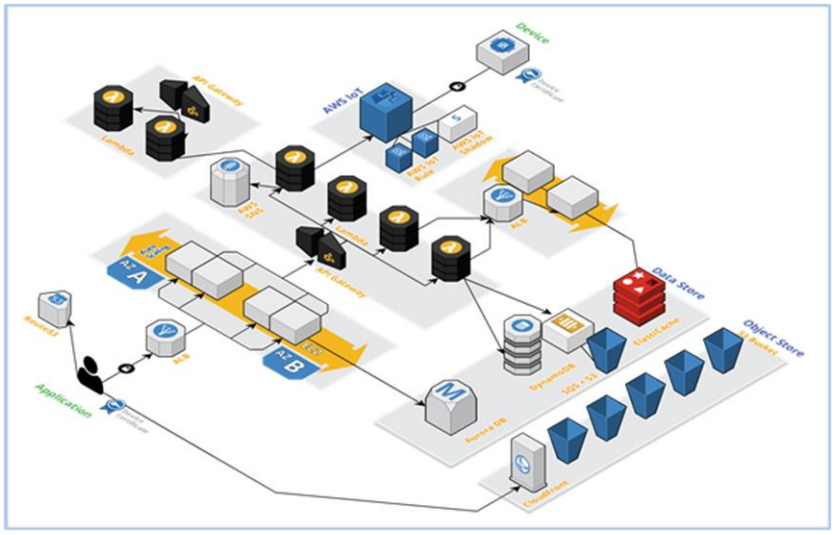

圖 143、LG ThinQ 採用 AWS IoT 解決方案架構

(二) 英國威爾斯 Newport 市

英國威爾斯 Newport 市在 AWS 上面實現了三個 Proof-of-Concept 的計畫，分別是空氣品質、洪水控制和垃圾管理。

原本，該市有 85 個空氣品質監測站，只有月平均值可以粗估空氣品質。在排水系統上，只能人工手動撿查，只有被洪水破壞後才會知道。而垃圾筒經常滿出來，造成污染和影響市容。為改善這些問題，因此增加許多空氣品質感應裝置、在排水系統上加裝水位監控裝置，在垃圾筒上放了感應器，透過 AWS IoT 與 AWS 的 Elastic (彈性)服務，少量的試點，再逐步擴大到更多的區域。因此，可以即時監控區域空氣品質；即時監控排水系統的水位，能更早發現問題，避免洪水造成災害；對於清潔人員的安排，可

以更有效的巡訪較多垃圾的區域，及早清運滿出來的垃圾筒，美化市容。

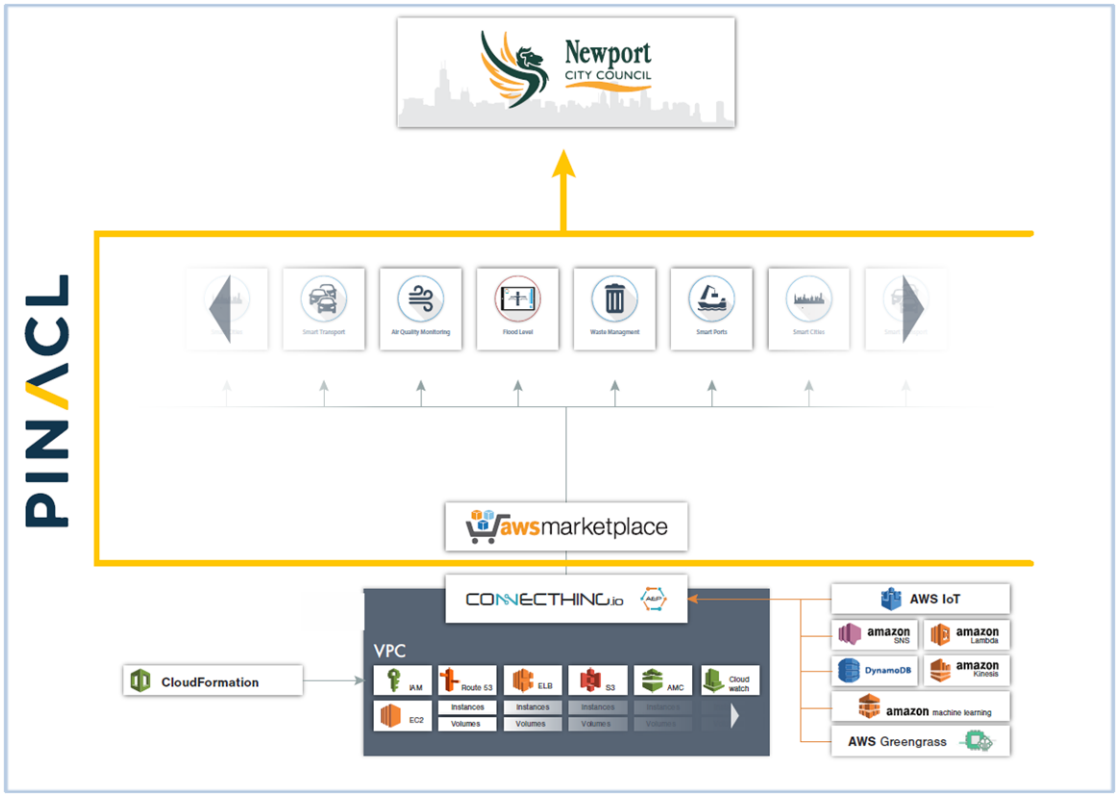

圖 144、英國威爾斯 Newport 市採用 AWS IoT 解決方案架構

(三) 美國 Rachio

Rachio 是一家在美國科羅拉多州生產製造灌溉用灑水控制器的廠商，採用 AWS IoT 做為其 Wi-Fi 智慧灑水控制器的管理平台。這些智慧灑水控制器可以透過網路查詢天氣(下雨)預報，配合使用者指示的灑水情境(時間長短、水量大小、灑水時間、灑水區域、植物種類、鹽份)來決定灑水排程。

二. Microsoft Azure 平台

Micorsoft Azure IoT 產品組合提供兩種途徑讓您建立自己的解決方案：

(一) 平台即服務 (PaaS)：

使用下列任何服務建置您的應用程式。

1. Azure IoT 解決方案加速器：

   預先設定的企業級解決方案集合，可讓用戶加快自訂 IoT 解決方案的開發速度。

2. Azure Digital Twins 服務：

   可讓用戶建立實體環境的模型，以使用空間智慧圖形和特定網域物件模型建立內容感知的 IoT 解決方案。

(二) 軟體即服務 (SaaS)：

可讓用戶快速開始使用 Azure IoT 中心這個 SaaS 解決方案，來開發 IoT 應用程式,而無須接觸到複雜的 IoT 解決方案。Azure IoT 中心是一種無程式碼的 IoT 解決方案，可以在數分鐘內建立裝置型號、儀表板和規則

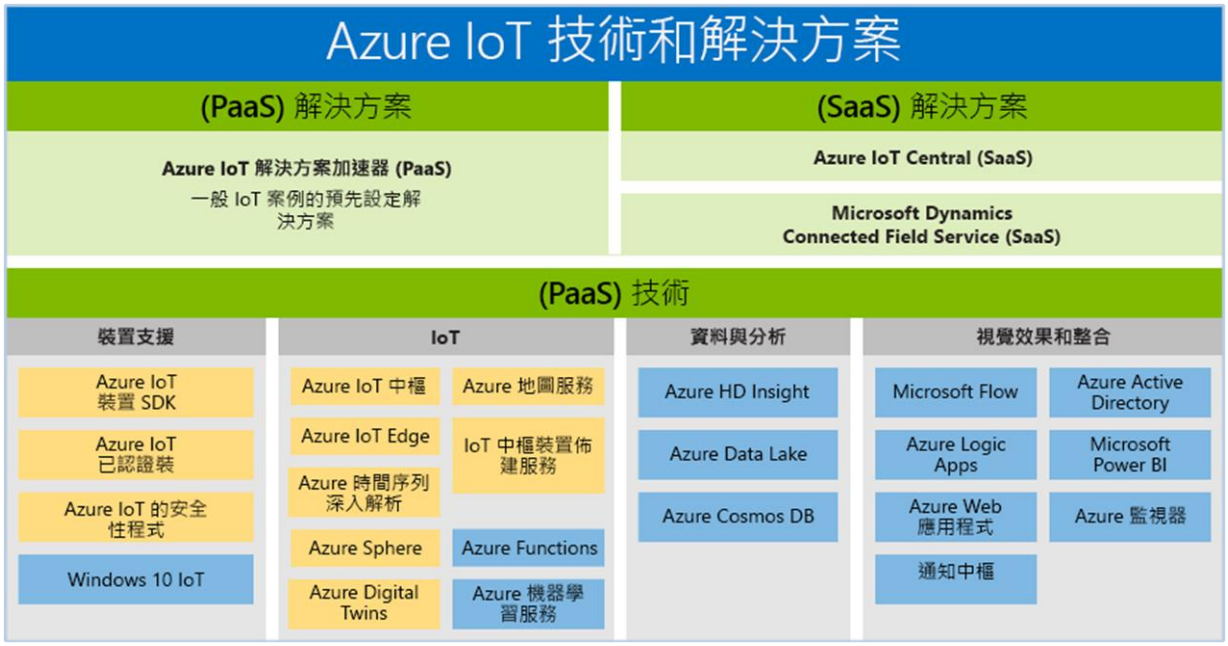

圖 145、Azure IoT 技術和解決方案

Azure 中有數個與 IoT 相關的服務。列舉如下：

◆ IoT Central：

這是 SaaS (Software as a Service) 解決方案，可協助連接、監視及管理 IoT 裝置。透過選取適用裝置類型的範本，然後建立及測試基本 IoT Central 應用程式，讓裝置操作員佈建新的裝置、監視裝置。此一服務適用於簡單而不需要深入自訂的解決方案。

◆ IoT solution accelerators (解決方案加速器)：

這是 PaaS 解決方案的集合，可用來加速開發 IoT 解決方案。從所提供的 IoT 解決方案著手，然後再根據需求來完整自訂此解決方案。需要 Java 或 .NET 技能來自訂後端，並需要 JavaScript 技能來自訂視覺效果。

◆ IoT Hub (中樞)：

此服務可讓裝置連線到 IoT 中樞，並監視及控制數十億個 IoT 裝置。如果需要讓 IoT 裝置與後端進行雙向通訊，特別實用。這是 IoT Central 和 IoT 解決方案加速器的基礎服務。

◆ IoT Hub Device Provisioning Service (中樞裝置佈建服務)：

這是 IoT 中樞的協助服務，可用來安全地將裝置佈建到 IoT 中樞。使用此服務，可以輕鬆且快速地佈建數百萬個裝置，而非一個一個逐一佈建。

◆ IoT Edge：

建立在 IoT 中樞之上，此服務可用來分析 IoT 裝置上的資料，而並非雲端中的資料。藉由將部分工作負載移到邊緣裝置，可以減少傳送至雲端的訊息量。

◆ Azure Digital Twins：

此服務可以讓用戶建立完整的實體環境模型。可以為人員、空間和裝置之間的關聯性和互動方式建立模型。例如，用戶可以預測工廠的維修需求、分析輸電網路的即時能源需求，或最佳化辦公室的可用空間。

◆ Time Series Insights (時間序列深入解析)：

此服務可讓用戶儲存、視覺化及查詢 IoT 裝置所產生的大量時間序列資料。可以搭配 IoT 中樞來使用。

◆ Azure Maps (地圖服務)：

此服務提供地理資訊給 Web 和行動應用程式。它有一組完整的 REST API 和 Web-based JavaScript 控制項，可用來建立有彈性的應用程式，並且適用於 Apple 和 Windows 裝置的桌面或行動應用程式。

有些服務，例如 IoT Central 和 IoT 解決方案加速器，會提供範本，以協助建立解決方案，快速上手。也可以使用其他可用服務來完整開發新的解決方案，取決於開發者需要多少協助和多大的控制權。

Azure IoT Hub 支援的通訊協定共有四種，分別是 HTTPS、AMQP、AMQP over WebSockets、MQTT。傳入的訊息目前支援 JSON 格式的字串。

以下簡介幾個基於 Micorsoft Azure IoT 的應用情境。

(一) Costa Farms：使用 IoT 自動化控制 pH 值

1. 客戶問題：

Costa Farms 近年開始創新並引進了新的室內植物，出售給 Walmart、Home Depot 和 Lowe's 等大型商店。pH 值是植物健康的關鍵因素之一，為了提高養分吸收使植物健康，進而提高產量，需要更加密切地監測和即時調節水和流質肥料中的 pH 值。然而，對他們來說，在整個植物生命週期內不斷測量和調節 pH 值是耗時、沒效益且困難的。

2. 解法方案：

將帶有 pH 感測器設備連上 Azure IoT Hub，在水力系統上測量精確的 pH 值。這個方案使用了 Adafruit Feather M0 Wi-Fi 和 pH 感測器，Microsoft Azure、Azure IoT Hub、Azure Stream Analytics、Azure Event Hubs、Azure Functions、Azure SQL 數據庫以及透過 Twilio 發送的訊息，以此構建了一個客戶可以在其解決方案中使用的概念驗證。其系統架構如下圖所示。包含測量數據發送到 Azure IoT Hub，然後傳入 Azure SQL 數據庫，並儲存於 Power BI。數據透過 AzureSQL 中的 Stream Analytics 發送，事件中心接收進入的數據。事件中心配置為 pH 警報和

pH 數據，然後觸發 pH 警報發送。使用 Azure Functions，通過 Twilio 發送訊息。使用 Azure Functions，根據最小和最大 pH 值，向 Twilio 發送訊息。最終將 pH 警報訊息發送到種植者的行動電話。

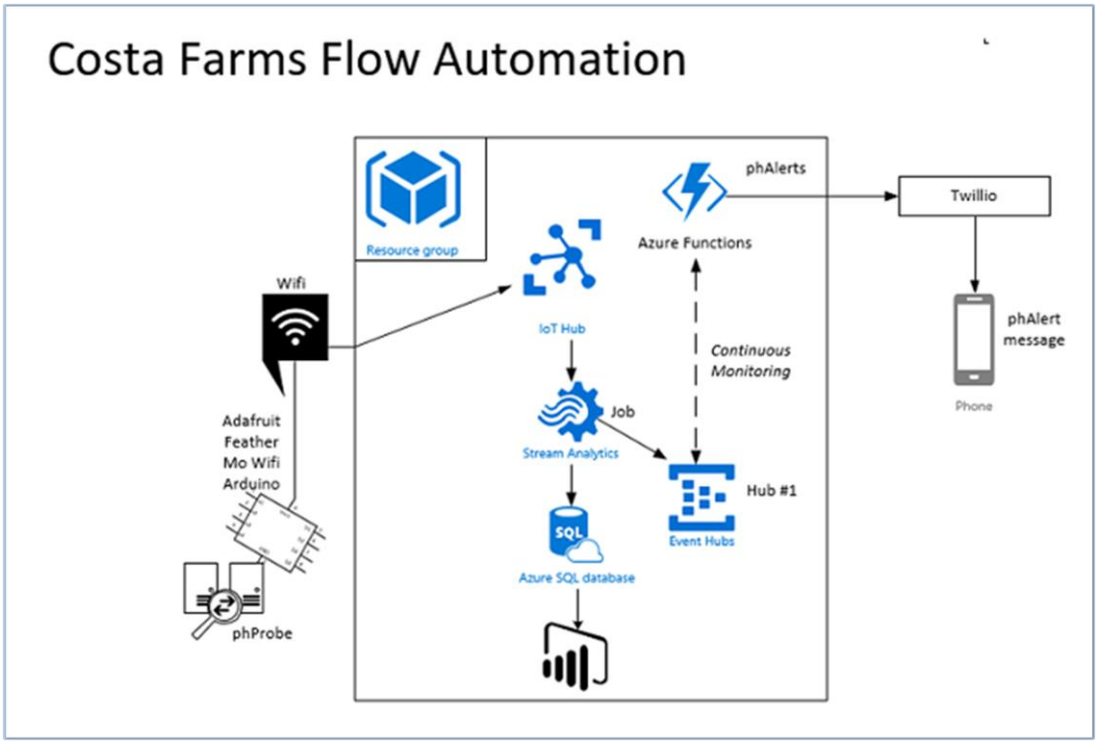

圖 146、Costa Farms 使用 Azure IoT 解決方案自動化控制 pH 值

(二) Powel：使用 IoT 檢測漏水情況

1. 客戶問題：

Powel 公司的配水系統面臨兩項挑戰，一是基礎設施中各種組件的使用年限，二是水壓的設定會保持一定的等級，因此若有破洞將增加流出的水量。在發生火災時，壓力會設定得更高，消防員需要為他們的水管施加額外的壓力。以下為 Powel 的目標：尋找一種安全的，可擴充的方式來傳送和存儲遙測數據。了解如何為機器學習準備遙測數據。配置 Azure 機器學習以對

數據執行異常檢測。將異常檢測結果連接到 SmartWater application。

2. 數據蒐集準備：

定位漏水是個實質的問題，利用特殊的麥克風連接到水管，然後用聲波對洩水處的大致位置進行三角測量。另外，收集盡可能越多的數據並查看它們和不同方法之間的關聯，如交通狀況、天氣或其他外部數據來源是否可以幫助確定漏水情況，並找到相關的第三方數據來源。

3. 解決方案：

該解決方案的關鍵部分是使用 Azure 機器學習，SmartWater 會比較監測到的數值與學習模型的分析結果，若有異常，操作員將在其應用程式中看到警報，並立即採取適當的操作。目標是儘早阻止漏水，未來安裝更多感測器和智慧水錶時，該解決方案將有可能提供更多效益。

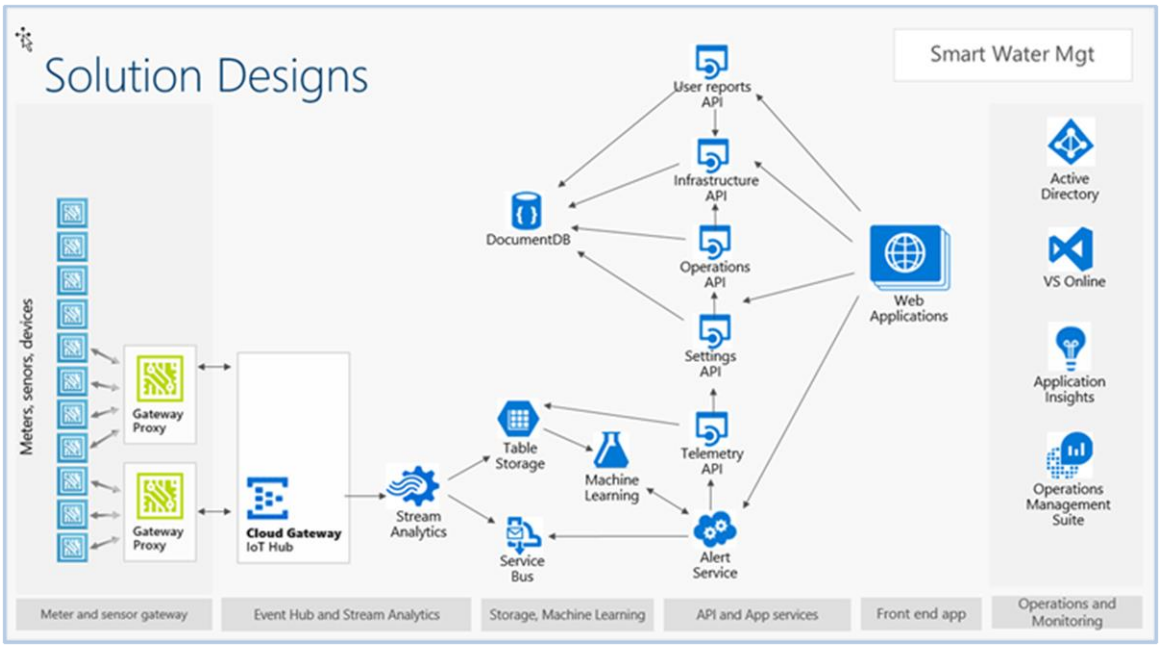

圖 147、Powel 使用 Azure IoT 解決方案檢測漏水情況

(三) GCBA：使用 IoT 無人機解決方案清理河流

1. 客戶問題：

Matanza-Riachuelo 河被河邊眾多工廠產生的大量工業廢物污染，尤其是製革廠。最危險的污染物是重金屬（砷，鉻，銅，鋅和鉛）和盆地飽和層的廢水。例如，鉻在土壤中的平均值為 1,141 ppm，顯著高於建議的 220 ppm 標準。西元 2013 年（102 年）發表在 Salud Colectiva 上的一篇文章發現，從 Matanza-Riachuelo 河流域附近井中取出的水，80％因污染而不能安全飲用。

2. 解決方案：

無人機將從同一個點降落並起飛，讀取感測器並將數據儲存在本身記憶體中。之後，設備將數據同步到 Azure IoT Hub 和開發的後端。感測器將測量以下內容：GPS、GSM、pH 值、溫度、流向、氯、鈣、Iodes、硝酸鹽、亞硝酸鹽、溶氧量、混濁度、導電率。無人機運行 Windows 10 IoT 的 Raspberry Pi 3。連接到 Raspberry Pi 3 的是感測器和 GSM 模塊，用於將數據發送到 Azure IoT Hub，再將感測器數據發送到 Azure Service Bus Queue，包含緯度，經度，設備 ID 和時間標記(Timestamp)。Azure Service Fabric 部署三位工作者，Worker1 將原始數據作為文件發送到 Azure Blob 儲存，然後將感測器數據發送到另一個佇列；Worker2 從佇列中獲取感測器數據，驗證其數據並將其發送到 Azure 表儲存，然後再將更新訊息發送到另一個佇列；更新訊息到達時會觸發 Worker3，在地圖上顯示的數據。

三. Google Cloud Platform IoT 平台

Google Cloud Platform for IoT 的中心是 Cloud IoT Core。

Cloud IoT Core 是一套全代管的 IoT 服務，可讓客戶以簡便又安全的方式來連結及管理散佈在全球各地的數百萬部感測裝置，擷取、儲存、分析這些感測裝置中的資料。結合 GCP 平台上的其他服務，Cloud IoT Core 可以提供企業一應俱全的解決方案，方便即時收集、處理、分析並視覺化 IoT 資料，以利提高作業效率。

Cloud IoT Core 有兩項主要元件：裝置管理員和通訊協定橋接器。裝置管理員可讓客戶安全地設定及管理各個裝置。裝置管理員會建立裝置的身分，並且在連線時提供裝置驗證機制。此外，裝置管理員還會保存每個裝置的邏輯設定，並可用於從雲端控制裝置。針對所有裝置連線，通訊協定橋接器會採用自動負載平衡技術為通訊協定提供連接端點。通訊協定橋接器支援透過業界標準通訊協定，如 MQTT 和 HTTP 建立安全連線。此外，通訊協定橋接器也會將所有裝置遙測事件發布至 Cloud Pub/Sub，以便下游分析系統接手處理。

Cloud IoT Core 是一個 GCP 中的一個無服務器元件，能夠支援任意數量的裝置連結到 Cloud IoT Core 裡，無需考量服務器的提供、設定、調校等等需要 IT 人員進行的管理作業。

Cloud IoT Edge 是一個基於 Linux 的裝置，結合一組軟體與服務，是供完整的 IoT 邊緣運算，可以在資料來源端執行與應用機器學習模型。在硬體架構上，Cloud IoT Edge 裝置可以配置一個或多個 Edeg TPU (Tensor Processing Unit)。Edeg TPU 是由 Google 為 TensorFlow 深度學習框架開發的小型 ASIC 硬體加速器。由 Google 開源的深度學習框架 TensorFlow 是一套知名的深度神經網路，在機器學習領域

中有很大的成果，並已應用在許多的實際案例中。Cloud IoT Edge 包含 TensorFlow Lite 和 Edge IoT Core。TensorFlow Lite 是一個為了行動裝置和內嵌式裝置設計的 TensorFlow 框架實現，內建 Edge ML，可執行在 GCP 上面建立且優化過後的 TensorFlow 模型。Cloud ML Engine 是 GCP 裡的一個無服務器、全代管的元件，是 Google 機器學習的核心，提供 TensorFlow 深度學習服務，建立深度神經模型。參考架構如下圖所示。

(一) 場域中的感測裝置將感測資料傳送到 Cloud IoT Core。使用 MQTT 協定，無論感測裝置的來源位置為何，全球使用一個端點 mqtt.googleapis.com。這個設計讓 Cloud IoT Core 解決方案無需考慮 GCP 端的 region 位置，也無需考慮跨 regions 的 GCP 服務裡的設定。

(二) Cloud IoT Core 收到資料後，後傳到 Cloud Pub/Sub 服務。Cloud Pub/Sub 是 GCP 中的一個無服務器、全代管的訊息佇列服務與事件轉發。Cloud Pub/Sub 會將資料以不同的通知主題送到佇列中。主題會被儲存 7 天，並可以被場景需要的其他後續服務立即存取。

(三) 由 Cloud IoT Core 或 Cloud Pub/Sub 起，資料處理可以經過任意數量的不同路徑。比如，感測資料可以被 Cloud Dataflow 轉換，並儲存在 Google Cloud Storage、Google BigQuery 或 Google Bigtable 中。

(四) 研究人員可以嚐試發展智慧系統，比如說，事件偵測與通知警告。他們可以使用儲存在 Google Cloud Storage 中的資料，透過 Cloud Machine Learning (ML) Engine 來訓練與修正模型。

(五) 在這個參考架構中，使用 Cloud Functions 訂閱 Cloud Pub/Sub 轉發的不同主題資料。Cloud Functions 也是 GCP 中的一個無伺服器、全代管服務，它是一個執行環境可以運行單一目標的特定函數，用以響應事件。同時使用數個函數可以快速的評估真實的狀況。若滿足某些預先設定的臨界值，可以立即觸發警告通知。

(六) 控制資料可以由 Cloud IoT Core 傳送回 IoT 裝置，必要時，可透過 Cloud IoT Edge 傳送。如，可將一個經 Cloud ML Engine 訓練好的深度神經網路模型下載到 Cloud IoT Edge，由 Edge TPU 在本地就近執行。

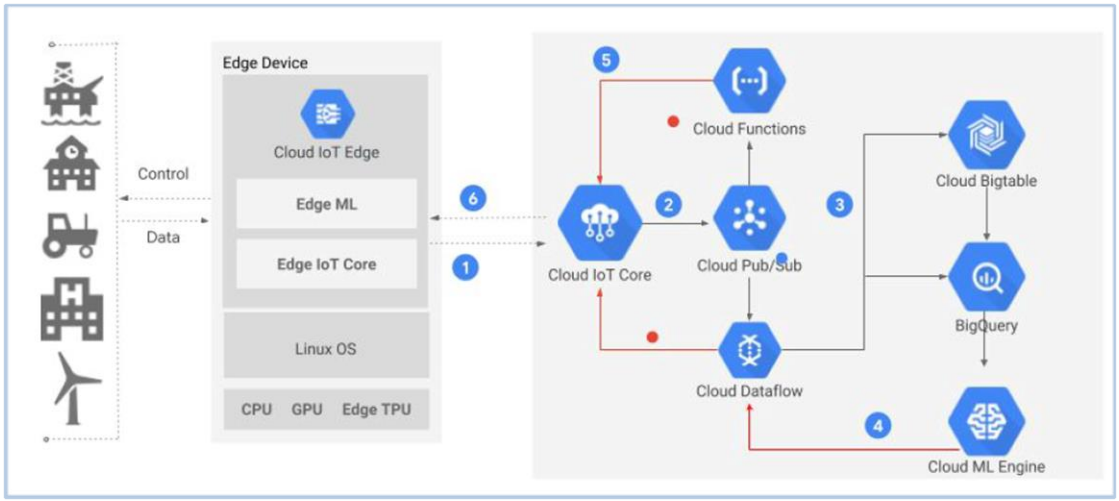

圖 148、Google Cloud Platform 的 IoT 參考架構

以下簡介幾個基於 GCP IoT 的應用情境。

(一) Smart Parking

1. 關於 Smart Parking：在紐西蘭、澳大利亞和英國營運，為全球城市和企業提供點到點的智慧停車管理/智慧城市解決方案。

2. 應用原理：核心產品是一個名為 Smart Park 的傳感器系統，包括地面傳感器，該傳感器使用紅外線和電磁技術記錄車輛的停靠，並與停車場出入口進行通訊。這使管理員可以及時了解停車場的使用情況並管理容量。提供自動導引和指示牌，告訴客戶在一個停車結構或城市街道區域的不同位置上有多少可用車位。超時功能，使停車場管理員能夠識別在限時停車格的車輛是否已經超時。經營者可以通知檢查人員採取強制行動，例如發出超時通知。

   應用範圍：可用於購物中心、商業停車場、機場、大學和市政街道等環境。Smart Parking 已在全球部署了 50,000 多個傳感器來支援停車系統。

(二) Oden Technologies

1. 關於 Oden Technologies：將工業硬體，無線連接和大數據架構整合到一個雲端基礎的平台中，製造商可以透過他們選擇的任何設備來分析和優化其生產。
2. 背景與目標：使用物聯網改進當今的工廠。透過網際網路相互連接的龐大的物(人)，減少浪費、提高效率與各行各業的安全性。透過無線連接，大數據和雲端計算相結合，引領製造業的物聯網創新。

   使用數據來改善製造業實際上與製造業本身一樣古老。但是，製造業的電腦化已導致對數據收集和處理方式以及可用數據量的巨大而迅速的改變。Oden 的目標是幫助製造商利用這些數據快速趨勢分析，甚至警告機器故障。視覺化可以改善製造和維護流程的機會，從而減少浪費並提高利潤。

解決方案： Oden 設計並開發了數據收集設備，該設備可以插入任何類型的機器中，並且可以以最小的複雜性和設置時間來進行無線傳輸數據。設備安裝後，Oden 技術平台將處理數據，以為製造商提供易於理解的分析。該平台產生的分析為工廠工程師提供了數據，例如詳細的根本原因分析，即時工廠範圍內的性能以及趨勢分析。Oden 運行 GCP，包括 Google Compute Engine、Google Cloud Pub/Sub、Google Cloud Bigtable、Google Stackdriver，和 Google Kubernetes Engine。從廠房，Oden 無線設備獲取數據。然後，Google Cloud Pub/Sub 及時將數據發送到 Google Cloud Bigtable，在其中使用 Oden 專有的分析工具處理數據。Google Stackdriver 支援 Google Cloud Platform 監視，日誌記錄和診斷，有助於 Oden 交付其雲端平台。Oden 建立了由 Kubernetes Engine 驅動的儀表板，該儀表板從 Google Cloud Bigtable 中提取了分析數據，為客戶提供其生產線的及時可見性。Oden 可以幫助每間工廠平均每天在一條生產線上獲取並存儲大約 1000 萬個指標性資料。度量標準可能包含極其詳細的細節，例如機器的電量、消耗的原材料量以及生產的物料量。傳感器還可以獲取並傳輸環境訊息，例如溫度和濕度，以便製造商可以識別與天氣有關的季節變化和季節性影響。

(三) Vagabond

1. 關於 Vagabond：Vagabond 是自動售貨行業的技術平台，將即時商務智慧傳遞到操作員的手掌上。

2. 背景與目標：該公司啟動了一個物聯網網路，將操作員即時連接到他們的每台自動售貨機，使他們可以從辦公室或道路上獲取有關每台機器的營運和銷售數據。為了補強其 Mobile Web 和 ERP 工具，該公司需要一個映射平台，使操作員能夠獲得機器的精確位置並有效地擬定運輸路線。
3. 解決方法：使用 Maps JavaScript API 構建了一個 Web 應用程式，將每位操作員的自動售貨機的位置顯示在地圖上。有關機器的重要訊息(例如庫存水準和收取的現金量)會覆蓋在地圖上，以便系統可以根據每台機器的需求和地理位置進行過濾。操作員使用此訊息來確定何時需要補充庫存，並建立有效的運輸路線。安裝機器後，操作員使用部署了 Places API 和 Geocoding API 的行動應用程式來確定其在建築物中的位置。

第二節　蒐集國際物聯網平台，對 IPv6 支援的情形

一. AWS（Amazon Web Services）IoT

AWS IoT 目前在 IPv6 的支援上包含了 15 個區域，亞太地區僅包含東京、新加坡、首爾、雪梨、孟買等地，台灣還未納入。在連接設備數量相當龐大的狀況之下，IPv4 的位址已不敷使用，因此 IPv6 的支援不僅能免去網路位址轉譯(NAT)的需要，亦可滿足終端設備對於 IP 位址的需求，這顯示出 IPv6 已在物聯網當中扮演一個相當重要的角色。根據官網的說明，目前支援 IPv6 的 AWS 服務包括 Elastic Load Balancing、AWS Direct Connect、Amazon Route 53、Amazon CloudFront、AWS WAF、S3 Transfer Acceleration 與 EC2 instances in Virtual Private Clouds，以及 AWS IoT。AWS IoT 訊息中介裝置支援使用 MQTT 通訊協定發佈與訂閱，也支援使用 HTTPS 發佈。使用這兩種通訊協定均可透過 IPv4 及 IPv6 支援。訊息中介裝置也支援透過 WebSocket 通訊協定的 MQTT。

二. Microsoft Azure IoT

目前 Microsfot Azure preview 階段的 IPv6 支援是在 IaaS (infrastructure) level。因為 Azure IoT Hub 是屬於 PaaS (platform)服務架構。Azure 目前有積極在規劃 VNET 及 IPv6 支援，但時間還不確定。

官方的建議是，若是現在當下要設計 IPv6 架構，可以先用 IaaS 部分服務，或是先採用 IPv4 在 Azure IoT Hub 等參考架構上開發，

待 Azure IoT 支援 IPv6 後，再將相關服務移植到支援 IPv6 的新服務上。

三. Google Cloud Platform IoT 平台

GCP 目前支援的 IPv6 位址只限通用位址，且只適用於 HTTP(S)、SSL Proxy 和 TCP Proxy 負載平衡器。

關於 3 大國際物聯網平台詳細資訊請參考附錄十。

第三節　研析物聯網的應用及發展

物聯網的發展促使了生活模式的創新與轉型，除了為人類的生活帶來全新的體驗外，物聯網的應用也得以有效率的方式解決目前生活上或社會上所帶來的問題，其應用的範圍與種類相當的廣泛，包括智慧運輸、智慧節能、智慧製造、智慧生活等各種面向，如下表所示。

表 109、物聯網之應用及其案例

類別	物聯網應用案例
智慧製造	遠端監控機器運作狀況，以確保穩定生產流程、故障預警、機器運作之最佳化、RFID 感測器等推動自動化流程
車聯網	提供影音娛樂系統(infotainment)，包括多媒體、SNS、定位系統等、運用車載感測裝置(雷達、加速器等)、GPS 等提升車輛操控性(無人駕駛等)
醫療照護	利用穿戴式裝置搜集人體資訊(血壓、脈搏、活動量、睡眠時間等)、疾病與診斷，並搭配個人遺傳因子等資訊，可推動預防醫療等
金融保險	利用 NFC、行動電話進行支付、依車聯網之駕駛傾向，計算汽車保險等
零售	利用 RFID 進行銷售與庫存管理、利用銷售資訊，進行促銷活動、透過人流分析調整賣場動線與商品陳列
物流	利用各式的 sensors 追蹤配送狀態、及早預知收件與配送壅塞狀況，提升效率、運用車輛運行資訊與駕駛者開車傾向，預防事故與防止故障發生
能源	分散電源的電力供應調整、依據 demand-response 控制電力消費量、最佳化家庭、工廠、大樓的電力消費量
農畜牧業	根據氣象、土壤、農作物等收成有關的數據來預測與最適化種植監控、搜集家畜的體溫、活動等數據，掌握家畜的體適能與繁殖期等
智慧居家	照明、空調、音響等設備的遠端操控、確保高齡者與

類別	物聯網應用案例
	小孩的使用安全性來自動調理設備
公共設施(道路下水道等)	遠端監控道路、橋梁、隧道等，預防崩塌與異常檢點、遠端監控水管線路，檢測與防治漏水
智慧校園	監控校園與宿舍安全、了解教室與設備的使用情形
智慧交通	如火車、公車、捷運、高鐵的大眾運輸公具的即時監控、行車資訊、紅綠燈等號誌的自動控制、道路使用情形監控與事故偵測、行車流量的估計等

為了使物聯網的應用能夠擁有更多功能以及更快的運算能力，多種技術之間的連結整合是必須的，在這種趨勢之下，人工智慧與物聯網的結合成為了智慧物聯(AIoT)。在 AIoT 的帶動下，自駕車的發展成為了熱門的焦點，這讓原本具有感測能力的汽車能透過蒐集的資料來加以學習，來達到更精確的判斷與操控。

第九章　會議及報告

第一節 每月月報

每月工作進度報告，於每月底完成彙總報告內容，並於隔月月初召開工作進度報告會議，向 NCC 報告，內容包含目前工作進度、已完成項目、及完成項目所得結果等。

詳細的月報內容，請參考附錄四；已完成工作項目，如下表所示：

表 110、已完成工作項目列表

序號	工作項目	完成日期
1	完成補助案審查會議，審查結果為修正後通過。	108/2/15
2	完成修改計畫書內容並回覆審查委員意見表。	108/2/22
3	完成計畫書內容確認通過。	108/2/26
4	完成 3 件委外執行案需求規格書。 1. IPv6 寬頻分享器互通測試項目研究及 IASP 實際測試平台建置。 2. ICP IPv4IPv6 平台架構雙協定升級之網路安全防護差異解析及升級實際測試。 3. 物聯網、5G 與 IPv6 國際技術標準及物聯網平台與應用之研析。	108/2/27
5	完成補助案確認通過。	108/3/28
6	完成參與 IETF104 國際會議。	108/3/29
7	完成凱擘寬頻、台固媒體、台灣寬頻通訊、全國數位有線通訊、天外天數位有線電視、天外天網路科技、天外天興業、超宇寬頻、大新店民主有線電視、台灣基礎開發科技、新永安有線電視，11 家 Cable 業者面訪。	108/4/3
8	完成補助案簽約。	108/4/8
9	完成亞太電信及台灣之星，2 家行動業者面訪。	108/4/10

序號	工作項目	完成日期
10	完成政府研究計畫基本資料表(GRB)填報。	108/4/11
11	完成 3 件委外執行案招標作業。	108/4/12
12	完成 IASP Verizon 及 ICP Google 導入 IPv6 原因及推動經驗調查。	108/4/12
13	完成 2 件委外執行案評審會議。 1. IPv6 寬頻分享器互通測試項目研究及 IASP 實際測試平台建置。 2. ICP IPv4IPv6 平台架構雙協定升級之網路安全防護差異解析及升級實際測試。	108/4/18
14	完成委外執行案評審會議。 1. 物聯網、5G 與 IPv6 國際技術標準及物聯網平台與應用之研析。	108/4/19
15	完成 IETF104 國際會議報告。	108/4/19
16	完成 4 月份工作月報會議。	108/5/2
17	完成參加 Internet of Things World 會議及展覽。	108/5/16
18	完成面訪 ASUS（華碩）討論寬頻分享器規範及測試項目。	108/5/27
19	完成邀請睿科網路科技介紹 CGNAT 設備及討論會議。	108/5/28
20	完成第一場在台北舉行 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練。	108/5/29
21	面訪 D-Link（友訊）討論寬頻分享器規範及測試項目。	108/5/31
22	完成第二場在高雄舉行 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練。	108/6/6
23	完成 5 月份工作月報會議。	108/6/11
24	完成期中報告初稿繳交。	108/6/28
25	完成 6 月份工作月報會議暨期中進度報告。	108/7/9
26	完成期中審查會議	108/7/15
27	完成第 3 場在台中舉行 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練。	108/7/24
28	完成 MWC19 Shanghai 出國報告	108/7/31
39	完成 Cable 業者新彰數位有線電視、三大有線電視、南國有線電視、洄瀾有線電視及東亞有線電視面訪。	108/8/5
30	完成 7 月份工作月報會議。	108/8/6

序號	工作項目	完成日期
31	完成 IETF 105 出國報告。	108/8/7
32	完成第 4 場在台北舉行 ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練。	108/8/23
33	完成 8 月份工作月報會議。	108/9/5
34	完成 IASP Comcast 及 ICP Facebook 導入 IPv6 原因及推動經驗調查。	108/9/12
35	完成第五場在高雄舉行ICP IPv4/IPv6 雙協定網路安全防護技術人才培訓教育訓練。	108/9/12
36	完成 Cable 業者高雄大大新寬頻面訪。	108/9/16
37	面訪 Cable 業者台灣寬頻討論 IPv6 試用推廣狀況。	108/9/18
38	完成 Cable 業者北都數位有線電視面訪。	108/9/19
39	完成 IPv4/IPv6 網路設定 APP 開發及 Google Play 上架。	108/9/30
40	完成 APNIC 48 出國報告	108/10/4
41	完成 Cable 業者中嘉寬頻面訪。	108/10/5
42	完成 9 月份工作月報會議。	108/10/8
43	完成 Cable 業者大台中數位有線電視面訪。	108/10/9

有關睿科網路科技介紹 CGNAT 設備簡報內容請參閱附錄四。

第二節　參與國際網際網路技術標準及應用會議

一. IETF 104

網際網路工程任務小組（全名：Internet Engineering Task Force，縮寫為 IETF）負責網際網路標準的開發和推動。此次會議在捷克布拉格召開，會議日期 3 月 23 日至 29 日共為期 7 天，這是 IETF 所舉行的第 104 次會議。本次會議約有 1,213 人到場參與及 864 人遠端參與。中心參加此次會議的主要目的為參與及了解各 WGs（Working Groups，工作小組）技術發展的趨勢及討論方向，包含 IPv6、Security、及 IoT 等相關議題。

本次會議由 Cisco（思科）及 CZ.NIC 共同主辦，TWNIC 利用此次機會安排前往 CZ.NIC 參訪，並與 CZ.NIC CEO Ondrej Filip，CTO Zdenek Bruna，以及 Technical Fellow Jaromir Talir 進行交流，介紹台灣 TWNIC 及 TWCERT/CC 的運作狀況，並針對捷克在網域名稱註冊管理及資安防護運作等相關系統與主題交換意見。

CZ.NIC 財團法人是捷克.cz ccTLD 管理者，其主要活動是管理.cz 域名，確保.cz 頂級域名操作和域名的教育。該組織還運行 0.2.4.e164.arpa（ENUM）網域。該協會的員工致力於推動 DNSSEC 技術項目，並開發網域管理系統和 mojeID 服務，推廣有利於捷克網路基礎設施的新技術。自西元 2011 年（100 年）1 月起，CZ.NIC 還負責維運國家安全團隊 National CSIRT (Cyber Security Response Team) Team，CSIRT.CZ。CSIRT.CZ 團隊也是 Trusted Introducer 和 FIRST 的會員。

圖 149、IETF 104 期間 TWNIC 參觀訪問 CZ.NIC

科技部中華民國駐捷克代表處科技組推動中東歐八國雙邊與多邊科技研究合作相關事務，包括：捷克、斯洛伐克、匈牙利、波蘭、保加利亞、烏克蘭、羅馬尼亞及斯洛維尼亞。TWNIC 利用此次機會安排與中華民國駐捷克代表處科技組組長廖思善博士進行交流，介紹台灣 TWNIC 及 TWCERT/CC 的運作狀況，並針對捷克以及中東歐等國在網路基礎環境以及資安防護能量等相關議題進行交流討論。TWNIC 也很樂意提供相關經驗與歐洲各國分享。

圖 150、IETF 104 期間 TWNIC 參觀訪問科技部中華民國駐捷克代表

以下為對於參與 IETF 104 技術研討會建議事項：

(一)建議持續關注相關各 WGs 動態及相關訊息。

(二)IPv6 技術規範已有 IPv6-only 以及因應物聯網需求的草案提出，建議持續關注 IPv6 的相關技術規範發展，強化新一代網路基礎建設。

(三)網路安全除了威脅研究外，在事件通報的技術規範上已有相關草案提出，建議持續關注 Security 的相關技術規範發展，以掌握資訊安全相關技術，並強化網路資訊安全的防護機制。

(四)物聯網相關技術規範，廣泛地從架構，軟體，安全，應用，格式等各方面都有草案提出，建議持續關注 IoT 的相關技術規範發展，以取得新一代網路應用技術，作為創新產業的基礎。

(五)建議國內 ISP 持續積極投入 IPv6 的佈建，並加強與國際上其

他 ISP 討論及分享佈建經驗。

(六)建議與國外相關單位進行更密切及多元的交流及經驗分享。

(七)建議持續參與 IETF 以掌握相關技術規範的演進及狀態。

(八)CZ.NIC 歡迎 TWNIC 共同參與開放原始碼的技術交流，並希望有機會推動人員互訪交流，增進彼此的技術能量。

(九)中華民國駐捷克代表處科技組歡迎 TWNIC 在網路資訊及網路安全方面的專業，與捷克或中東歐各國有機會互相交流。

其他詳細內容，請參閱附錄五，〝IETF 104〞出國報告。

二. 2019 Internet of Things World

Internet of Things World 世界物聯網會議從西元 2014 年（103 年）開始舉辦論壇 Forum，到今年（108 年）已經是第 6 屆，今年（108 年）的會議在美國加州聖克拉拉會議中心舉辦，會議日期 5 月 13 日至 16 日共為期 4 天，由 Informa Telecoms & Media 主辦，DELL Technologies 冠名贊助，是全球物聯網（IoT）技術創新與產業界交流的重要平台。本次國際研討會議與展覽會，連結了在各業界從事物聯網實用化策略規劃、技術開發、實際佈建的專家，也是未來商機的起點。

今年（108 年）的主題是 The Intersection of Industries and IoT Innovation，有 1 萬多位參與者，將政策專家，技術專家，開發人員和實際佈建者聯繫在一起，讓物聯網推向產業垂直生態鏈，使來自垂直產業生態系統和物聯網技術解決方案廠商聯合起來，通過物聯網實現產業的未來。

本次 2019 IoT World 有多項活動，除了 IoT World 研討會之外，還包括 IoT World 展覽會（Exhibition），新創公司後起之秀（Startup Elevate）展覽會，IoT World 開發者會議（Developers Conference），IoT World 黑客松（Hackathon），並且結合 Connected & Autonomous Vehicles 研討會一同舉行。

本次展覽會中特別規劃新創公司後起之秀區（Startup Elevate），本區域是獨特的新興企業輔助計畫與社群，以橋接特定投資人及相關業界與最具潛力的創新後起之秀。本次 Startup Elevate 特別由台灣科技部的國際科技創業基地（Taiwan Tech Arena，TTA）所贊助。

5 月 15 日至 16 日舉辦 IoT World 開發者會議 (Developer Conference)，重點在技術面，是以從事 IoT 解決方案開發的開發者、

硬體技術人員、設計人員為對象的活動，在 2 天會期中舉行，包括世界主要企業的主管或開放原始碼專案負責人演講，可以收集到要成功開發 IoT 相關技術時的相關資訊。

圖 151、(左至右)TWNIC 顧靜恆組長與 IoT World 開發者大會主席 Joe Maglitta, Principal at Maglitta Communications 合影

本次世界物聯網研討會議場次共有 12 個分項，分別為

(一) 製造業（Manufacturing）

(二) 智慧建築與能源管理（Smart Buildings & Energy Management）

(三) 能源與資源生產（Energy and Resource Production）

(四) 智慧城市（Smart Cities）

(五) 連網消費品（Connected Consumer）

(六) 連網與自動駕駛汽車（Connected & Autonomous Vehicles）

(七) 物聯網連接（IoT Connectivity）

(八) 人工智能與機器學習（AI & Machine Learning）

(九) 開發人員會議：建構與佈署（Developers Conference: Build & Deploy）

(十) 供應鏈與物流（Supply Chain & Logistics）

(十一) 物聯網安全（IoT Security）

(十二) 邊緣計算（Edge Computing）

以下為對於參與 2019 Internet of Things World 技術研討會建議事項：

(一) 本次會議的各家廠商都強調物聯網服務的成功，需要倚靠建立整個產業的生態系統（Ecosystem），包括從物聯網感測晶片設計，傳感系統，數據傳輸，分析，管理的物聯網雲平台，以及特定應用的智慧樣態和洞察分析，這些都需要有專業公司來提供服務，非常值得台灣在未來物聯網產業垂直整合發展上參考。

(二) 物聯網的應用層面可以很廣泛，本次會議已經有許多公司展示成功案例，也有許多新創公司展現其創新的應用構想，台灣的新創公司也積極的參與了此次盛會，台灣未來在物聯網的應用上，仍有很大的空間可以發揮，可多鼓勵新創構想以發展物聯網應用。

(三) 美國主要 ISP 如：Verizon，T-Mobile，AT&T 等，在物聯網無線傳輸環境的基礎建設上都已可提供 5G，NB-IoT，CAT-1，及 4G LTE 等不同傳輸標準，以因應不同物聯網的應用，並且積極整合特定應用的合作夥伴，提出整合的物聯網解決方案，值得台灣 ISP 未來提供物聯網無線傳輸的基礎建設以及探索

相關應用的參考。

(四) AWS IoT 的運作分三個層次，分別為 Edge，Cloud，以及 Enterprise，從物聯網應用的資料流架構上，這三個層次確實環環相扣，台灣在雲端服務的成熟度上及在邊緣運算的佈建上都是一大挑戰，此架構可以做為未來台灣物聯網服務提供及系統整合廠商的參考。

(五) 本次會議舉辦的物聯網 Hackathon，各隊為了要完成一個 IoT Hackathon 專案，必須結合問題探討，資料分析，以及感測硬體元件，軟體開發，訊號傳輸，視覺介面設計等系統整合等，才能完成一個雛形系統進行專案報告和展示。尤其物聯網的應用需要依據問題和目標，整合多種技術，在短時間內結合多人的技術專長，發揮團隊分工與合作，很值得在台灣推廣試驗。

(六) 許多國際業者會舉辦物聯網的技術研討和實作工作坊，也陸續舉辦多場展覽會，建議可多參與，並與國外相關單位及業者進行更密切及多元的交流及經驗分享，作為台灣發展的參考。

其他詳細內容，請參閱附錄五，〝2019 Internet of Things World〞出國報告。

三. MWC19 Shanghai

此次是全球行動通訊大會（Mobile World Congress，MWC）-上海的第八屆會議及展覽，也是亞洲行動通訊的年度大型會議及展覽之一，會議日期為 6 月 26 日至 28 日共 3 天。會議和展覽期間共有來自 100 以上國家，超過 7.5 萬人到場參與，今年（108 年）主題〝智聯萬物〞，描繪了高速靈活的 5G 網路、物聯網、人工智慧、大數據及邊緣計算等新科技的結合，達到連結萬物，共建美好未來。中國工信部於今年（108 年）6 月 6 日，也就是展期前 3 週，正式向中國電信、中國移動、中國聯通及中國廣電 4 家電信營運商發放了 5G 商用執照，象徵中國進入 5G 元年，這比原本預期的時間提早了一年，可以強烈感受到全球對 5G 的熱烈程度及競爭態勢。因此此次會展期間舉辦了相當多場 5G 技術研討會，並可看到參展業者對 5G 技術商品及應用著墨甚多，各個展廳都有 5G 相關的展示和體驗，此次整個展覽會場也布建 5G 連網環境，讓與會者可以體驗 5G 行動連網的真實感受。

會展期間活動包含主題演講、產業高峰會、合作夥伴活動、導覽以及研討會等。會展的八個核心主題如下：

(一) 人工智慧：探討各產業該如何運用人工智慧，及此革命性技術對人類生活的影響。

(二) 連接：5G 具有高速性、靈活性及敏捷性，能夠提供遠比現在更加可靠的服務與性能。

(三) 資訊安全：資訊安全須肩負分析實現消費者、政府和監管機構間良好平衡所需的重要責任。

(四) 數位健康：探討智慧手機普及，讓人對科技的依賴性，所引發對心理健康問題的影響。

(五) 顛覆性創新：企業需要保持警覺與具備靈活性，才能積極應對產業及市場的快速變化，新創系列活動讓與會者能接觸最新技術與應用。

(六) 沉浸式內容：探討產業所面臨的挑戰、獲利模式及消費增長與網路容量之間的關係。

(七) 工業 4.0：工業 4.0 由物聯網、虛實整合系統、雲端和認知計算所構成，主要在分析這些構成要素的實施方法與為產業帶來的影響。

(八) 美好未來：探討未來 10 年的技術發展，將如何塑造西元 2028 年（117 年）及之後的世界面貌。

圖 152、TWNIC 許淑芳於 MWC19 上海展覽會場入口

MWC19 上海展覽會場上，參與的業者相當多，針對 5G 和物聯網的相關應用展示相當多元，以下類別為此次展覽的重點包含：

(一) 4K/8K 直播：應用包含電視台的實況直播、結合影像畫面數據分析 AI 人工智慧、5G 賽事直播及 4K/8K 顯示器等領域。

(二) 機器人：應用包含 5G 醫院物流機器人、5G 無人配送及智慧工廠大規模機器人及機器手臂替代人力等領域。

(三) AR/VR：應用包含 AR/VR 互動體驗、AR 遊戲、結合物體辨識及人臉辨識做為社區安全防護及工廠檢修輔助等領域。

(四) 5G 設備：包含 5G 連網設備、5G 小型基地台、5G 手機及 5G 室內路由器等。

(五) 智慧城市：應用包含智慧垃圾回收站、智慧路燈、水資源管理、檢測及智慧交通等領域。

以下為對於參與 MWC19 Shanghai 會議及展覽建議事項：

(一) 本次會議過程中，以往同業之間大多以競爭者的姿態發表演說，但進入 5G 時代，一方面業者希望能更快為消費者提供服務，另一方面 5G 雖然有龐大的商機，但同時也需要龐大的投資，因此有些業者也希望透過合作聯盟的方式，以減少風險共創商機的想法，拋出同業合作的可能性，例如日本 KDDI、NTT Docomo 及 Softbank 合作富通信訊息應用，中國的電信業者也暢談合作議題，值得國內產業參考。

(二) 在 5G 之前時代，電信業者所扮演的角色大多停留在連網服務提供者上，但到了 5G 時代電信業者已經有明顯的角色轉變，業者談的是如何提供開放式的平台，攜手商業合作夥伴提供更好的應用服務，這種產業思維的轉變，值得國內 ISP 深入思考。

(三) 5G 的佈建需要龐大的投資，尤其中國幅員廣大，要能提供大量覆蓋 5G 服務，對中國 ISP 業者是一大挑戰，因此業者為了能快速進入商用化市場，採取分階段執行由 NSA（Non-

standalone）先實行，再到 SA（Standalone）佈建，及網路切片技術的應用等，值得國內業者參考，但也要考慮到分階段實行如何能滿足不同時期使用者，及使用者所使用的終端設備能力的需求。

(四) 5G 正式進入商用化年代，全球預測物聯網裝置將以飛快的速度成長，物聯網裝置的安全也成了產業界關注的焦點，因此英國、美國及歐盟等，為物聯網裝置的安全性，訂定了安全規範及認證機制，為因應國內物聯網產業發展，政府相關單位也應該重視此議題，訂立規範為產業發展鋪路。

(五) 5G 和物聯網是新一代數位科技發展的重點，近年相關國際技術研討和展覽活動非常頻繁，透過參與國際技術研討和展覽活動，吸取國際經驗，並與國際進行交流及經驗分享，有助國內產業政策制定，及作為國內產業發展方向的參考。

其他詳細內容，請參閱附錄五，〝MWC19 Shanghai〞出國報告。

四. IETF 105

這是 IETF(網際網路工程任務小組, Internet Engineering Task Force)所舉辦的第 105 次會議，於西元 2019 年(108 年)07 月 20 日(星期六)至西元 2019 年(108 年)07 月 26 日(星期五)在加拿大蒙特婁召開，總共為期七天的會議，是由 COMCAST 與 NBCUniversal 共同主辦。本次參與會議人數高達 1,961 人，其中有 859 人是利用遠端會議系統的方式參與。會議主題共分為以下 7 大項目：

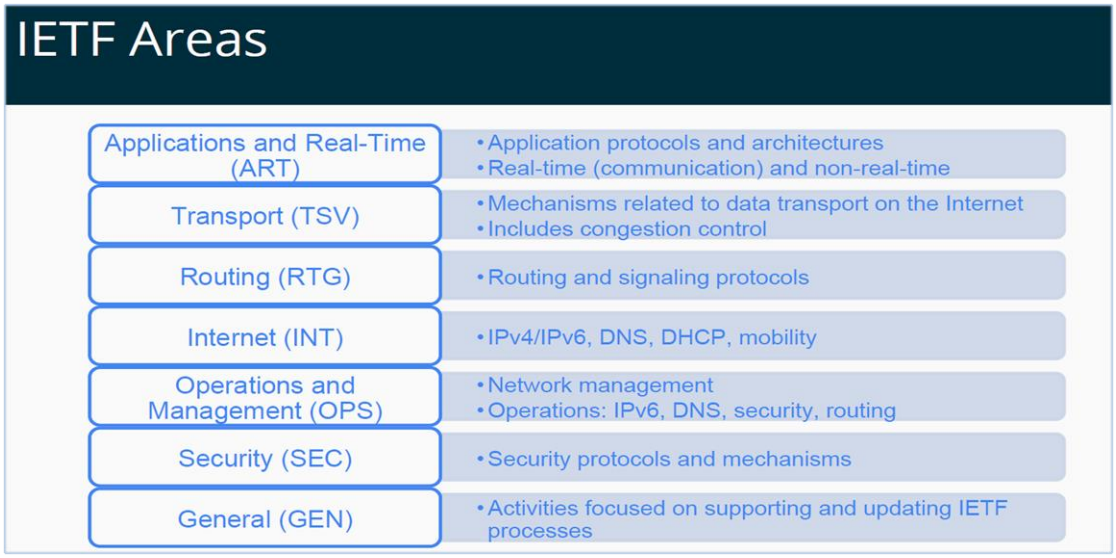

圖 153、IETF 105 會議主題項目

參加此次會議的主要目的為參與及了解各 WGs(Working Groups，工作小組)技術發展的趨勢及討論方向，包含 DNS、Security、EPP、IPv6 及 IoT 等相關議題。

於本次會議中，主要參與的主題包含 Hackathon、ANRW (Applied Networking Research Workshop)、DNS、路由安全維運、IPv6 及 IoT 等領域的相關議題，分別整理如下：

(一) Hackathon：本次 Hackathon 活動參與人數約有 384 名，分成 30 個不同的主題分組討論，並於第二天下午由各組進行 3 分鐘的簡短報告（下載連結）。

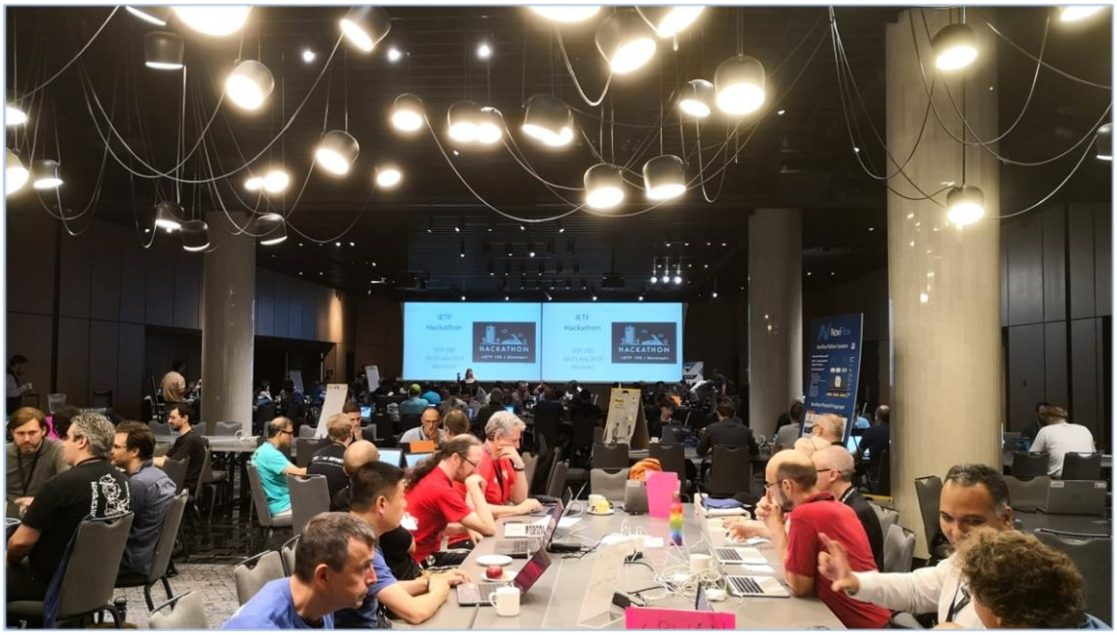

圖 154、IETF 105 Hackathon 活動分組討論現況

(二) ANRW (Applied Networking Research Workshop) ：ANRW 2019 是一個學術研討會，為研究人員、供應商、網路營運商和網際網路標準社群提供一個展示和討論研究新成果的論壇。

(三) DNS 主題：內容包含 DNS privacy、DNS support for specific network environments 及 DNS provisioning。

(四) 路由安全維運：本次參與有關路由安全維運技術的討論會議，的工作小組為 sidrops：SIDR 營運工作組（SIDR Operations，sidrops）為 SIDR 感知網路的營運制定指南，並提供有關如何在現有網路和新網路中部署和運行 SIDR 技術。會中進行和 SIDR 有關的主題如下表所列：

表 111、IETF 105 有關路由安全維運討論主題

編號	路由安全維運主題
1	A Profile for Autonomous System Provider Authorization
2	Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization
3	Signaling Prefix Origin Validation Results from an RPKI Origin Validating BGP Speaker to BGP Peers
4	RPKI Signed Object for Trust Anchor Keys

(五) IPv6：本次參與有關 IPv6 技術討論會議，包括下列幾個工作小組：

1. v6ops：營運工作組（IPv6 Operations，v6ops）為新的和現有的 IPv6 網路的佈署和操作制定指南。
2. 6MAN：維護工作組（IPv6 Maintenance，6man）負責維護和推進 IPv6 協議規範和尋址架構。
3. 6lo：約束節點於 IPv6 網路工作組（IPv6 over Networks of Resource-constrained Nodes，6lo）專注於通過約束節點網路促進 IPv6 連接的工作。

會中進行和 IPv6 技術有關的主題如下表所列：

表 112、IETF 105 有關 IPv6 技術討論主題

編號	IPv6 主題
v6ops Working Group（營運工作組）	
1	464XLAT Optimization
2	Neighbor Cache Entries on First-Hop Routers: Operational Considerations
3	Operational Security Considerations for IPv6 Networks
4	IS-IS Multi Topology Deployment Considerations
5	IPv6 Point-to-Point Links
6	IPv6-Only Terminology Definition

編號	IPv6 主題
6MAN Working Group（維護工作組）	
7	IPv6 Segment Routing Header (SRH)
8	ICMPv6 errors for discarding packets due to processing limits
9	IPv6 Minimum Path MTU Hop-by-Hop Option
10	IPv6 Neighbor Discovery on Wireless Networks
11	IPv6 Neighbor Discovery Unicast Lookup
12	Discovering PREF64 in Router Advertisements
13	IPv6 Support for Segment Routing: SRv6+
14	The IPv6 Compressed Routing Header (CRH)
15	The Per-Path Service Instruction (PPSI) Option
16	The Per-Segment Service Instruction (PSSI) Option
17	Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)
18	Service-aware IPv6 Network
19	Consideration of IPv6 Encapsulation for SFC and IFIT
20	Encapsulation of Path Segment in SRv6
21	Segment Routing Header encapsulation for In-situ OAM Data
22	DetNet SRv6 Data Plane Encapsulation
6lo Working Group（約束節點於 IPv6 網路工作組）	
23	Transmission of IPv6 Packets over Near Field Communication
24	Packet Delivery Deadline time in 6LoWPAN Routing Header
25	6LoWPAN Fragment Forwarding
26	6LoWPAN Selective Fragment Recovery
27	IPv6 over Constrained Node Networks (6lo) Applicability & Use cases
28	IPv6 Neighbor Discovery Unicast Lookup
29	Asymmetric IPv6 for IoT Networks

(六) IoT：本次參與有關 IoT 技術討論會議，包括下列幾個工作小組：

1. suit：IoT 軟韌體更新工作組（Software Updates for Internet of Things，suit），負責物聯網（IoT）設備中的漏洞引發對安全軟韌體更新機制的需求，該機制也適用於受約束設備。
2. 6TiSCH：IPv6 over the TSCH（Time Slotted Channel Hopping）mode of IEEE 802.15.4e 工作組，負責制定低功耗設備在 IPv6

網路的運作機制。IEEE 802.15.4e 主要為短距離、低功率及低速特性設備所提出的無線通訊標準。

3. lpwan：IPv6 於低功耗廣域網路工作組（IPv6 over Low Power Wide-Area Networks，lpwan）負責 SIGFOX，LoRa，WI-SUN 和 NB-IOT 等低功耗廣域技術實現 IPv6 連接。
4. t2trg：物聯網工作組（Working Group - Thing-to-Thing，t2trg）研究物聯網低資源節點設備連結相關問題。

會中進行和 IoT 技術有關的主題如下表所列：

表 113、IETF 105 有關 IoT 技術討論主題

編號	IoT 主題
suit Working Group（IoT 軟韌體更新工作組）	
1	A Firmware Update Architecture for Internet of Things Devices
2	Firmware Updates for Internet of Things Devices - An Information Model for Manifests
3	SUIT CBOR manifest serialisation format
6TiSCH Working Group	
4	An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4
5	Minimal Security Framework for 6TiSCH
6	6tisch Zero-Touch Secure Join protocol
7	IEEE802.15.4 Informational Element encapsulation of 6tisch Join and Enrollment Information
8	6TiSCH Minimal Scheduling Function (MSF)
9	Robust Scheduling against Selective Jamming in 6TiSCH Networks
lpwan Working Group（低功耗廣域網路工作組）	
10	LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP
11	SCHC over Sigfox LPWAN
12	Static Context Header Compression (SCHC) over LoRaWAN
13	Data Model for Static Context Header Compression (SCHC)
14	LPWAN Static Context Header Compression (SCHC) for CoAP

編號	IoT 主題
15	OAM for LPWAN using Static Context Header Compression (SCHC)
16	RTO considerations in LPWAN
t2trg Working Group（物聯網工作組）	
17	RESTful Design for Internet of Things Systems
18	YANG Object Universal Parsing Interface
19	Problem Statement of IoT integrated with Edge Computing

以下為對於參與 IETF 105 技術研討會建議事項：

(一) 建議持續關注相關各 WGs 動態及相關訊息。

(二) IPv6 技術規範已有 IPv6-only 以及因應物聯網需求的草案提出，建議持續關注 IPv6 的相關技術規範發展，強化新一代網路基礎建設。

(三) 物聯網相關技術規範，廣泛地從架構，軟體，安全，應用，格式等各方面都有草案提出，建議持續關注 IoT 的相關技術規範發展，以取得新一代網路應用技術，作為創新產業的基礎。

(四) 建議持續關注 DNS 的相關技術發展，以掌握最新的發展趨勢。

(五) 建議持續了解 EPP 的政策規範，以配合修改相關作業流程。

(六) 建議與國外相關單位進行更密切及多元的交流及經驗分享。

(七) 建議持續參與 IETF 以掌握相關技術規範的演進及狀態。

其他詳細內容，請參閱附錄五，〝IETF 105〞出國報告。

五. APNIC 48

APNIC 48 會議於西元 2019 年（108 年）9 月 5 日至 12 日在泰國清邁(CHIANG MAI, THAILAND)舉行，本次會議共有 422 人參與，會議內容涵蓋了網際網路維運、技術及發展等。本次會議有許多 NIR 代表、網路技術專家、政府代表、網路業者代表、Internet 工程師等共同參加。

此次參加會議之目的為參與相關議題及進行台灣最新發展現況報告，瞭解亞太地區各國網際網路發展狀況與網路運作之政策。另外，本中心參與此會議中，負責主持 APNIC IPv6 Deployment 場次，Cooperation SIG 場次，並共同主持 Policy SIG 場次，IPv6 Deployment 場次中包含 5 個 IPv6 佈建相關專題報告與經驗分享，以促進亞太地區 IPv6 發展；Cooperation SIG 場次邀請了 5 位講者針對 Internet Jurisdiction 主題進行座談；Policy SIG 場次共討論了 5 個 Policy Proposals 政策提案。

圖 155、顧靜恆組長共同主持 Policy SIG 場次

以下為對於參與 APNIC 48 會議建議事項：

(一) 目前國際上各國家都積極在推動 IPv6，愈來愈多國家的 ISP 業者都預設啟用 IPv6，建議國內 ISP 參考此方式推動使用 IPv6，也建議持續對國際 IPv6 發展持續關注。

(二) Policy 是推動網路發展的重要依據，在 Policy 形成之前，需先進行 Proposal 的提案及討論，由於 proposal 的討論需尊重整個社群的意見，建議國內 ISP 及相關單位能了解並參與相關的討論，以便能與國際接軌及健全國內網路的持續發展。

(三) RPKI 在 APNIC 48 會議場次比例提高許多，可見 APNIC 對於 RPKI 的重視，未來台灣仍應持續推動 RPKI 並提升 ROA 覆蓋率以及 ROV valid 比例。

其他詳細內容，請參閱附錄五，〝APNIC 48〞出國報告。

第十章　結論與建議

第一節　結論說明

一、 Cable 業者對 IPv6 網路服務支援仍處於初步階段

目前針對 Cable 業者所做支援 IPv6 網路服務調查，完成的 20 家業者訪談結果，以台灣寬頻通訊最為積極，後端網路設備支援 IPv6 建置已經完成，已經具備可供試用階段，但終端用戶設備只有 50%支援 IPv6，且目前國內尚無 Cable 業者有營運支援 IPv6 網路服務的經驗，對業者要進入商用階段仍有挑戰。另外凱擘寬頻及台固媒體雖然持續在進行網路支援 IPv6 建置上，但業者評估在設備投資、技術升級、客戶服務、維運成本、自動檢測系統及維修人員 SOP 等，還有相當多準備工作，因此對支援 IPv6 預估仍要一段時間。中嘉寬頻因商業考量完成骨幹支援 IPv6，但使用者端還有技術性問題尚未克服，目前還沒有明確計畫。台灣基礎開發，因應企業客戶需求已經有實際提供企業客戶 IPv6 網路服務，但對家用服務仍有設備待更新，目前也沒有明確計畫。其他獨立系統業者在尚未有 Cable 業者支援 IPv6 的情況下，雖然在設備上有陸續更新計畫，但大多還是持觀望的態度。

二、 行動電信業者對 IPv6 網路服務支援度高

去年國內前 3 大行動電信業者包括中華電信、台灣大哥大及遠傳電信，都已經支援 IPv6 連網服務，今年（108 年）初亞太電信也開啟支援 IPv6，到 10 月中 IPv6 的使用率已經約 37.5%，而台灣之星將於明年（109 年）初支援 IPv6 網路服務，目前已經開啟 IPv6 供內部進

行測試使用，預計於 109 年 3 月中採用預設開啟的方式開放給用戶使用，也預告國內 5 家電信業者將在明年（109 年）初完成 IPv6 網路服務啟用計畫，完成行動通信網路全面升級。

三、 行動電信業者對 IP 的需求持續增加

根據NCC 西元2018年(107年)第4季行動通訊市場統計資訊[30]，國內 5 家行動業者客戶數逼近 3 千萬，而全球各國 IPv4 位址分配列表[31]，顯示台灣分配到約 3 千 5 百萬 IPv4 地址，行動電信業者龐大的 IPv4 位址需求很難被滿足。針對 IASP 的調查結果來看，5 家行動電信業者都採用 CGNAT 核發 Private/Shared Address Space IPv4 位址給用戶，以因應 IPv4 不足的問題，其中中華電信、遠傳電信及台灣大哥大(部分)3 家業者所採用的比例為 1:16；而台灣大哥大(部分)、亞太電信及台灣之星 3 家業者所採用的比例達 1:64，顯示國內行動電信業者 IP 缺口逐漸擴大，共用的比例越來越高。

四、 家用固網 IPv6 連網比例仍待提升

目前一般使用者家用網路使用中華電信固網服務，已經於去年（107 年）支援 IPv6 網路服務，且家用電腦系統大多數已經支援 IPv6 且預設開啟支援，但到今年（108 年）10 月中華電信固網 IPv6 使用率約為 25.2%，相較於中華電信行動網路 IPv6 的使用率已經超過 80%，顯示固網 IPv6 網路服務的使用比例仍有相當大的進步空間。其中可能的原因為家用設備的使用年限相對較長且更換頻率低，目前中華電信配發給家庭用戶的 Home Gateway，支援 IPv6 的比例約為 60%，使用者大部分不會在意以 IPv4 或 IPv6 連線，且目前市售寬頻分享器對 IPv6 支援程度也不佳，都是影響固網 IPv6 網路使用比例的因素。

五、 企業固網 IPv6 連網比例很低

目前國內 IPv6 網路流量主要來自於一般使用者，在台灣固網、新世紀資通及亞太電信企業用戶的固網 IPv6 使用率都在 1%以下，比例非常的低，顯示在企業網路支援 IPv6 的進展相當少，仍有待改善。目前中華電信和新世紀資通都已經提供用戶 IPv6 網路服務，中華電信光纖上網服務的 IPv6 使用率約 25.2%，主要流量是來自於終端使用者而非企業用戶，而新世紀資通服務對象為企業用戶，目前其 IPv6 的使用率約 0.4%，比例相當的低，一方面因為其服務上線時間不長，另一方面也顯示國內企業網站在 IPv6 的支援上仍相當少。亞太電信的光纖網路，預計明年（109 年）才會支援 IPv6；而台灣固網的光纖網路服務，目前並未計畫支援 IPv6。在網路服務業者對 IPv6 並未完全支援，要推動企業網站支援 IPv6 的難度也相對提高。在推動企業網站支援 IPv6 的方式上，若能結合政府和電信業者的力量共同推動，由政府提供減稅或投資抵減優惠等獎勵措施，攜手電信業者和其企業用戶或內容網站業者推廣導入支援 IPv6。

六、 IASP 對 IPv6 的支援狀況對 ICP 支援 IPv6 推動至為關鍵

本次 IASP 服務調查，分為針對 IASP 所提供的使用情境調查，包含光纖(FTTx)上網、Co-Location/IDC 服務、雲端（Cloud）服務、PWLAN 無線上網、及 4G 行動上網等類別。各家 IASP 所提供的網路服務類別眾多，要能完全支援 IPv6 網路服務需要相當的時間及預算執行，因此到目前為止國內大部分 IASP 還無法達到所有網路服務完全支援

IPv6，因此要推動國內企業網站支援 IPv6，常形成相當阻力。在進行推動 ICP 業者網站升級 IPv4/IPv6 雙軌連網服務工作時，除要說服 ICP 業者本身願意投入外，在計畫進行過程中其中一個案例所要進行輔導的 ICP 業者為採用台灣固網所提供的雲端服務，但雲端服務供應商預計於明年（109 年）才會支援 IPv6，因此此案的升級計畫無法繼續推展。網路服務供應商對 IPv6 支援準備狀況，將影響後端服務推動可行性。

七、 支援 IPv6 屬於基礎建置早期規劃及投入能減少推動的阻力

由國際大型 IASP Verizon 推動 IPv6 的經驗調查發現，在建置新系統時選擇導入 IPv6，減少後續更新的資金及人力成本支出；中華電信在推行支援 IPv6 的經驗中，也提出相似的看法表示，如未藉由新建或汰舊換新機會順勢將 IPv6 導入，將增加額外導入成本，這也是業者在推動 IPv6 常遇到的阻力。

第二節 建議事項

政府相關單位經過多年努力推行 IPv6 的普及化，去年（107 年）開始在行動通信及中華電信對家用固網提供 IPv6 網路服務後，國內 IPv6 連網比例擁有豐碩的成果。而觀察國際 IPv6 發展趨勢，在去年（107 年）之前 IPv6 使用率較高的國家以歐洲及北美為主，亞洲除了日本較積極，及印度新進 IASP 一開始投入就須面對沒有足夠 IPv4 資源的問題，因此積極投入支援 IPv6 外，其他國家發展相對較慢。但從去年（107 年）開始亞洲區除了我國之外，越南、馬來西亞及泰國等國家也積極推動 IPv6，可見支援 IPv6 已經是國際共識。國內經過多年的努力才有去年(107 年)的大幅成長，以此基礎持續推動 IPv6 普及以提供對新一代網路標準完善支援相當重要，根據目前計畫執行狀況所提建議如下：

一. 推動 IASP 各項服務支援 IPv6

根據 IASP 普查結果得知，IASP 除行動網路及固網的網路連線外，業者還經營各項服務如 PWLAN、IDC/Co-Location、雲端服務等，業者提供的服務是否支援 IPv6，也和 IPv6 是否能普及息息相關，持續積極推動業者各項服務支援 IPv6，對提升國內 IPv6 使用率有相當助益。

二. 手機預設開啟支援 IPv6

國內 5 家行動通信業者目前已經有 4 家支援 IPv6，預計於明年(109 年）初將完成 5 家業者全部支援 IPv6 網路服務，在後端網路完成全部支援後，即能在此基礎上希望手機業者能開啟預設支援 IPv6，不論

使用者是經由向電信業者購買電信綁約手機或是經由零售市場購入，新手機都能預設支援 IPv6，以提高網路連線 IPv6 使用率。

三. 推動寬頻分享器預設開啟支援 IPv6

網通商品需支援 IPv6 必要規格及測試項目，並建議政府納入共同供應契約，確保新採購之設備均能支援 IPv6。

建置支援 IPv6 合規的網通商品型錄資料庫及建置推廣網站，提供消費者採購相關商品的參考依據。

四. ICP IPv4/IPv6 升級及網路安全防護差異

台灣缺乏 IPv6 推廣文章，可以邀請部落客撰寫 IPv6 推廣及介紹文章，從概念、實作、創意、安全等各種角度切入，提供更多的網路用戶參考，有助於日後 IPv6 的應用普與發展。

建議可以在 IPv6 推廣網站，將國外授權的 IPv6 文章翻譯成中文之後推廣。

五. 建立 ICP IPv4/IPv6 平台架構雙協定網路安全防護檢查項目清單

建議將檢查清單放置在網站上，例如整合於 IPv6 推廣專區網頁，若有增添修改檢查清單的項目，並能更新以保持資料的正確性。

六. 提升 ICP 支援 IPv4/IPv6 雙軌服務

ICP 業者願意配合輔導做網站 IPv6 升級，除提供 IPv4/IPv6 雙軌服務外，業者也希望能有其他的收穫如增加網站曝光度，如果能有媒體曝光機會或許能吸引更多業者加入。

第三節 未來研究方向

推動我國 IPv4/IPv6 雙軌普行，經過多年的努力在 107 年到 108 年有了豐碩成果。全球 IPv4 位址不足的情況已經相當明顯，新進業者很難再取得 IPv4，為延續既有成果並持續拓展國內 IPv6 使用比率，未來計畫可延續今年方針，在落實 IPv6 連網環境、強化 IPv6 連網安全及探索 IPv6 連網應用等各方面持續推動。

為整合推動 IPv4/IPv6 雙軌普行，研究方向亦可延續今年三項分項工作進行，包括落實 IPv6 連網環境推動商用網路雙軌普行、強化 IPv6 連網安全進行用戶連網環境安全研析，以及探索 IPv6 連網應用研析物聯網平台與應用。藉此確保我國數位通訊傳播基礎建設發展及國人數位資訊流通或晉用，皆與世界先進國家同步，促進國內數位經濟發展。執行工作項目建議包含：

一. 市售寬頻分享器產品 IPv6 支援調查：

107 年對市售寬頻分享器支援 IPv6 狀況進行調查，108 年研究市售寬頻分享器支援 IPv6 規格及測試項目建議，並實際進行市售產品和中華電信 Hinet PPPoEv6 及台灣寬頻 IPoEv6 線路測試結果，未來可延續之前推動結果，進行市售寬頻分享器在 IPv6 支援狀況調查，以掌握業者近年來對產品支援 IPv6 的狀況是否有所改變，及了解推動寬頻分享器支援 IPv6 的成果。

二. Native IPv6 連網試驗環境建置

在推動 IPv4/IPv6 雙軌普行多年後，108 年底我國 IPv6 使用率已經接近 45%，驗證了相關機關努力推動的成果，108 年 11 月底歐洲 RIPE

正式發布 IPv4 已經全數發放完畢，未來其他各大洲很快會面臨相同情形。在過渡時期網路仍會以 IPv4/IPv6 雙軌並行，但未來隨著物聯裝置成長，Native IPv6 環境可能需求將會出現，為因應未來環境需求提前作準備，可建置實驗型 Native IPv6 環境，進行前期研究為未來鋪路。

三. IASP 及 ICP IPv6 升級推廣

(一) IASP IPv6 升級推廣

1. 今年台灣寬頻推出 IPoEv6 網路服務試用，目前還處於初步少量試用階段，未來可延續推廣更多用戶進行試用，一方面為未來商用進行更多測試；另一方面讓累積的經驗形成成功案例，可供同業做為參考，並鼓勵其他 Cable 業者能升級支援 IPv4/IPv6 雙軌服務。
2. 108 年計畫完成手機簡易設定 APN 啟用 IPv4/IPv6 雙軌服務 APP 開發，未來可持續推廣使用者下載此 APP，開啟手機支援 IPv4/IPv6 網路連結，持續推升我國 IPv6 連網使用率。

(二) ICP IPv6 升級推廣

為持續推動 ICP 業者網站升級支援 IPv4/IPv6 雙軌服務，可進行跨單位合作例如透過公協會會議，進行會員推廣等方式，合作推廣網站升級 IPv4/IPv6 雙軌服務。

四. IPv6 用戶資通安全防護研析

(一) IPv6 家用及企業用戶資通安全防護研究

持續進行 IPv6 家用及企業用戶資通安全防護研究，以確保 IPv6 連網環境安全。

(二) IPv6 網路安全技術人才培訓教育訓練

未來可以持續規劃進行 IPv6 網路安全教育訓練課程，培養更多技術人才，增強業者推動升級支援 IPv4/IPv6 雙軌服務技術能力及意願。

第十一章　參考資料來源

[1] 「中華電信 IPv6 推動現況及未來發展」簡報：
http://www.seminar2017.twnic.tw/lec/0330-2-2.pdf

[2] 網際網路工程任務小組（IETF，Internet Engineering Task Force）
https://www.ietf.org/about/mission/

[3] State of IPv6 Deployment 2018, 6 June 2018,
https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

[4] IPv6 transition stories,
https://www.apnic.net/community/ipv6-program/ipv6-stories/

[5] IPv6 at Verizon Wireless, APNIC 34, 2012,
https://www.apnic.net/wp-content/uploads/2017/01/vzw_apnic_13462152832-2.pdf

[6] Verizon follows Comcast lead on IPv6, 06 April 2010,
https://www.networkworld.com/article/2206336/verizon-follows-comcast-lead-on-ipv6.html

[7] Comcast’s IPv6 Trials, by John Jason Brzozwski, 10 June 2010,
https://sites.google.com/site/ipv6implementors/2010/agenda

[8] World IPv6 Launch Four Years Later: Taking Stock and Looking Forward, by John Brzozowski, 8 June 2016,
https://labs.comcast.com/world-ipv6-launch-four-years-later

[9] IPv4 Depletion Not the Beginning of the End, It’s Just the End of the Beginning, by John Brzozowski, 24 Sep. 2015,
https://labs.comcast.com/ipv4-depletion

[10] One Mission :Making a Powerful Network Smarter, by John Schanz, 23 Feb. 2016,

http://labs.comcast.com/mission-making-a-powerful-network-smarter

[11] Calling All Researchers :Comcast Innovation Fund Seeking Projects, by Jason Livingood, 6 April 2016, https://labs.comcast.com/comcast-innovation-fund-seeking-projects

[12] Innovation Fund Spotlight : Drexel University IPv6 Segment Routing, by Jason Livingood, 10 August 2017, http://labs.comcast.com/innovation-fund-spotlight-drexel-university-ipv6-segment-routing

[13] Drexel :IPv6 Video Architecture; Clarkson University :IPv6 Advancements, by Jason Livingood, 12 Feb. 2018, https://labs.comcast.com/february-innovation-fund-grant-roundup

[14] 美國最大有線電視營運商 Comcast 宣布 IPv6 商用, 19 Jan. 2010, http://www.cctime.com/html/2010-1-29/20101291536521 71.htm

[15] Google 內網 5 成升級 IPv6, 30 Dec. 2011, https://www.ithome.com.tw/node/71524

[16] Google IPv6 Implementors Conference, https://sites.google.com/site/ipv6implementors/Home

[17] Looking towards IPv6, 13 May 2008, by Lorenzo Colitti and Erik Kline, https://googleblog.blogspot.com/2008/05/looking-towards-ipv6.html

[18] Google's IPv6 Deployment, 8 July 2009, by Lorenzo Colitti, https://www.youtube.com/watch?v=vFwStbTpr6E

[19] Google at IPv6, by Lorenzo Colitti, 5 May 2016, https://www.youtube.com/watch?v=Hh7ckfQUzHA

[20] IPv6 deployment at Googl, 29 July 2008, by Lorenzo Colitti, https://datatracker.ietf.org/meeting/72/materials/slides-72-ietf-4-ietf-operations-and-administration-plenary

[21] Google Enterprise IPv6 deployment, 5 Dec. 2011, by Irena Nikolova, https://www.usenix.org/legacy/events/lisa11/tech/slides/babiker.pdf

[22] Google and IPv6, July 2015, by Khaled Koubaa, http://ipv6.sa/wp-content/uploads/2015/07/Google_Strategy_for_IPv6-Google.pdf

[23] IPv6, the Internet, and Google, by Erik Kline, http://www.uuasc.org/google_uuasc_la.pdf

[24] Google IPv6 Statistics, https://www.google.com/intl/en/ipv6/statistics.html

[25] 台灣商用網路 IPv6 使用率統計圖, https://ipv6now.twnic.net.tw/ipv6/info.html

[26] 台灣 IPv6 全球排名, https://ipv6now.twnic.net.tw/ipv6/index.html

[27] 全球 IPv6 使用率排名前 30 國家列表, https://ipv6now.twnic.net.tw/ipv6/apnic_lab_7day_top.html

[28] 中華電信 4G LTE IPv6 支援手機型號與終端設備設定, https://www.emome.net/files/fckeditor/%E7%B5%82%E7%AB%AF%E8%A8%AD%E5%82%99%E8%A8%AD%E5%AE%9A_v4_20180131.pdf

[29] 中華電信公司 HiNet IPv6 用戶連線參考手冊, https://www.ipv6.hinet.net/form/HiNet_IPv6_fixed_setting.pdf

[30] NCC 西元 2018 年（107 年）第 4 季行動通訊市場統計資訊, https://www.ncc.gov.tw/chinese/files/19040/3773_41243_190402_1.pdf

[31] 各國 IPv4 位址分配列表, https://zh.wikipedia.org/wiki/%E5%90%84%E5%9C%8BIPv4%E4%BD%8D%E5%9D%80%E5%88%86%E9%85%8D%E5%88%97%E8%A1%A8

[32] CableLabs 相關訊息, https://www.cablelabs.com/

[33] 思科 6RD-從 IPv4 快速過渡到 IPv6 部署從理論到實現講解, https://www.cablelabs.com/

[34] Managing 100+ million IP addresses, June. 2006, by Alain Durand, Comcast, https://archive.nanog.org/meetings/nanog37/agenda ; https://archive.nanog.org/meetings/nanog37/presentations/alain-durand.pdf

[35] 如何在 IPv4 與 IPv6 共存下連線. 2011, https://www.ithome.com.tw/tech/92048

[36] 先進國家業者 IPv4/IPv6 位址經驗分析報告, 2008, 黃仁竑, http://www.ipv6.org.tw/docu/elearning8_2009/1009804292b-08.pdf

[37] World IPv6 Day: Sloving the IP Address Chicken-and-Egg Challenge, Jan. 2011, https://www.facebook.com/notes/facebook-engineering/world-ipv6-day-solving-the-ip-address-chicken-and-egg-challenge/484445583919/

[38] Facebook Now Available Over IPv6, May 2012, by Dan York, https://www.internetsociety.org/blog/2012/05/facebook-now-available-over-ipv6-two-weeks-early/

[39] Case Study: Facebook Moving To An IPv6-Only Internal Network, Jun. 2014, by Paul Saab, Facebook, https://www.internetsociety.org/resources/deploy360/2014/case-study-facebook-moving-to-an-ipv6-only-internal-network/

[40] Facebook News Feeds Load 20-40% Faster Over IPv6, Apr. 2015, by Dan York, https://www.internetsociety.org/blog/2015/04/facebook-news-feeds-load-20-40-faster-over-ipv6/

[41] IPv6: It's time to get on board, Sep. 2015, by Paul Saab, Facebook, https://engineering.fb.com/networking-traffic/ipv6-it-s-time-to-get-on-board/

[42] Embracing IPv6 for Optimal Performance, Sep. 2015, by Paul Saab, Facebook, https://www.youtube.com/watch?v=_7rcAIbvzVY

[43] Legacy support on IPv6-only infra, Jan. 2017, by Glenn Rivkees, Facebook, https://engineering.fb.com/networking-traffic/legacy-support-on-ipv6-only-infra/

[44] State of IPv6 Deployment 2018, Jun. 2018, https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

[45] 2018 Networking @Scale recap, Jun. 2018, https://engineering.fb.com/core-data/networking-scale-2018-recap/

[46] Facebook IPv6 使用率統計資料, Jun. 2018, https://www.facebook.com/ipv6/?tab=ipv6_country

[47] 泰國三大電信, Jan. 2019, https://www.beurlife.com/2018/04/Prepaid-Data-SIM-AIS-true-dtac.html

[48] 國務院辦公廳〝推進互聯網協議第六版(IPv6)規模部署行動計畫〞, Nov. 2017, http://www.miit.gov.cn/newweb/n1146290/n1146392/c5928494/content.html

[49] 工信部發布落實〝推進互聯網協議第六版(IPv6)規模部署行動計畫〞, Apr. 2018, http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c6154756/content.html

[50] 三大運營商 IPv6 建設如何了?, May 2018, https://fiber.ofweek.com/2018-05/ART-210021-8420-30234452.html

[51] 關於開展西元 2019 年（108 年）IPv6 網路就緒專項行動的通知, Apr 2019, http://www.miit.gov.cn/n1146295/n1146592/n3917132/n4062109/c6791072/content.html

[52] 白俄羅斯成為首個強制 ISP 提供 IPv6 的國家, Sep. 2019, https://ithome.com.tw/news/133230

中英專有名詞對照

3G 第三代行動電話
(3rd-Generation, 3G)
4G 第四代行動電話
(4rd-Generation, 4G)
5G 第五代行動電話
(5rd-Generation, 5G)
6RD IPv6 快速部署(IPv6 Rapid Deployment, 6RD)

A

ADSL 非對稱式數位用戶迴路
(Asymmetric digital subscriber line, ADSL)
ALG 應用層閘道器（Application Layer Gateway，ALG）
AI 人工智慧(Artifical Intelligence, AI)
Akamai 阿卡邁 (Akamai Technologies)
Always-on 隨時在線(Always-on)
AP 無線接入點(Access Point, AP)
APNIC 亞太網路資訊中心
(Asia-Pacific Network Information Centre, APNIC)
ARIN 美國網際網路號碼註冊中心(American Registry for Internet Numbers, ARIN)

B

Backbone 網路骨幹 (Backbone)
BRAS 寬頻遠程接入伺服器
(Broadband Remote Access Server, BRAS)

C

CDN 內容傳遞網路（Content Delivery Network，CDN）
CGN/CGNAT 電信級
NAT(Garrier Grade NAT, CGN/CGN)
Cloud Computing 雲端計算
(Cloud Computing)
Co-Location 主機代管(Co-Location)
CRAN 收斂區域網路
(Converged Regional Area Networks, CRAN)

D

DHCP 動態主機組態協定
(Dynamic Host Configuration Protocol)
DNS 網域名稱伺服器(Domain Name System, DNS)
Dual Stack IPv4/ IPv6 雙協定
(Dual Stack)
Data Packet 資料封包(Data Packet)

DOCSIS 纜線數據服務介面規格(Data Over Cable Service Interface Specification, DOCSIS)

DPI 深度封包檢測(Deep Packet Inspection, DPI)

E

eHRPD 演進高速分組網路(Evolved High Rate Packet Data, eHRPD)

Email 電子郵件(Electronic mail, Email)

F

FTTx 光世代網(Fiber To The x, FTTx)

Firmware 韌體(Firmware)

G

Gateway 閘道器(Gateway)

GOLD Logo 金質標章(GOLD Logo)

Google 谷歌(Google)

GRB 政府研究資訊系統(Government Research Bulletin, GRB)

GSN 政府網際服務網(Government Service Network , GSN)

H

Hot Spot 熱點(Hot Spot)

HGW 家庭閘道器(Home Gateway, HGW)

HGW-O 家庭閘道器(Home Gateway-Optiocal, HGW-O)

I

IaaS 基礎設施即服務 (Infrastructure as a Service, IaaS)

ICP 網際網路內容提供者(Internet Content Provider, ICP)

ICMP 網際網路控制訊息協定(Internet Control Message Protocol, ICMP)

IDC 資訊機房(Internet Data Center, IDC)

IETF 網際網路工程任務組(Internet Engineering Task Force, IETF)

Information Security 資訊安全(Information Security)

Internet APN 網際網路接入點名稱(Internet Access Point Name, Internet APN)

IoT 物聯網(Internet of Things, IoT)

IP 網際網路協議(Internet Protocol, IP)

IPsec 網際網路安全機制(Internet Protocol Security, IPsec)

IPSecv6 IPv6 網際網路安全機制(Internet Protocol Security of IPv6, IPSecv6)

IPSO IP 智慧物件(Internet Protocol Smart Objects, IPSO)

IPTV 網路電視(Internet Protocol Television, IPTV)

IPv4 網際網路通訊協定第四版(Internet Protocol version 4, IPv4)

IPv6 網際網路通訊協定第六版(Internet Protocol version 6, IPv6)

IPv4/v6 Dual Stack 網際網路通訊協定第四版及第六版雙軌並行(IPv4/v6 Dual Stack)

IPv6 Ready Logo 網際網路通訊協定第六版認證獎章(IPv6 Ready Logo)

ISP 網際網路服務提供者(Internet Service Provider, ISP)

IASP 網際網路服務提供者(Internet Access Service Provider, IASP)

IT 資訊技術(Information Technology, IT)

L

L3 Switch 第三層交換器(Layer 3 Switch)

Load Balancers 負載平衡器(Load Balance)

LSN 大規模 NAT(Large-Scale NAT, LSN)

LTE 長期演進技術(Long Term Evolution, LTE)

M

Mobile Internet 行動上網(Mobile Internet)

N

NAT 網路位址轉譯(Network Address Translation, NAT)

NAT Traversal NAT 穿越(NAT Traversal)

NCC 國家通訊傳播委員會(National Communications Commission, NCC)

Network Layer 網路層(Network Layer)

NRO 號碼資源組織(Number Resource Organization, NRO)

O

OTT 網路隨選串流影片服務(Over- The-Top, OTT)

P

P2P 點對點對等網路架構(Peer to Peer , P2P)

PnP 隨插即用(Plug and Play , PnP)

PPPoE 網路對等協定(Point-to-Point Protocol Over Ethernet, PPPoE)

Profile 設定檔(Profile)

PWLAN 公眾無線區域網路(Public Wireless Local Area Networks, PWLAN)

R

RAN 無線接取網路(Radio Access Network, RAN)

RIR 區域網路註冊管理機構(Regional Internet registry, RIR)

Router 路由器(Router)

RFC 網際網路協定規範(Reuest For Comments, RFC)

S

Smarter Meter 智慧量表(Smarter Meter)

STB 數位機上盒(Set-Top Box, STB)

SOP 標準作業程序(Standatd Operating Procedure, SOP)

T

TANet 臺灣學術網路(Taiwan Academic Network, TANet)

TCP 傳輸控制協定(Transmission Control Protocol, TCP)

Tunnel Broker 通道代理伺服器(Tunnel Broker)

TWNIC 財團法人台灣網路資訊中心(Taiwan Network Information Center, TWNIC)

U

UDP 用戶資料包協定(User Datagram Protocol, UDP)

USGv6 美國聯邦政府 IPv6 網通設備支援標準(United States Government IPv6 Profile, USGv6)

UMB 超行動寬頻 (Ultra Mobile Broadband, UMB)

V

VDSL 超高速數位用戶迴路(Very-High-Bit-Rate Digital Subscriber Line, VDSL)

VOD 隨選視訊(Video on Demand, VOD)

VoIP 網路電話(Voice over Internet Protocol, VoIP)

VTUR VDSL 數據機(VDSL Modem, VTUR)

W

WiFi Router 寬頻分享器(WiFi Router)