出國報告 （出國類別：開會）

出席亞太網路資訊中心第 57 次（APNIC 57）會議報告書
Asia-Pacific Network Information Centre 57 Conference

服務機關	姓名 / 職稱
數位發展部	江世民 高級分析師 黃郁勝 科員
財團法人中華民國國家資訊基本建設產業發展協進會	陳曼茹 經理

派赴國家：泰國 曼谷

出國期間：113 年 2 月 26 日至 3 月 2 日

報告日期：113 年 4 月 16 日

摘 要

亞太網路資訊中心（Asia Pacific Network Information Centre，APNIC）第 57 次會議於本（2024）年 2 月 27 日至 3 月 1 日以結合線上參與及實體會議的混合模式於泰國曼谷舉行。此為 2024 年度第 1 次 APNIC 會議，會議中藉由講者演講、論壇討論等形式，將最新的網際網路發展趨勢與所有與會者分享。

我國政府由數位發展部指派 2 名人力，財團法人中華民國國家資訊基本建設產業發展協進會 1 名人力協同，前往泰國曼谷參加 APNIC 57（Asia-Pacific Network Information Centre 57 Conference）實體會議，蒐集有關網路安全、亞太及國際 IP 政策進展、技術等最新發展資訊。

本次實際參與的 11 場會議，主要是挑選內容以 IP 位址政策及網路安全相關議題為主之會議/研討會，除開幕暨專題演講（Opening Ceremony & Plenary）之外，還包括公開政策會議（Open Policy Meeting）、APNIC IPv6 布建（APNIC IPv6 Deployment）、APNIC 座談（APNIC Panel Discussion）、APNIC 路由安全特別興趣小組（APNIC Routing Security SIG）、APNIC 年度大會（APNIC Annual General Meeting）等場次。

IP 位址是網際網路基礎建設不可或缺的關鍵元素，因此制定亞太號碼資源政策、討論網際網路協定技術發展的 APNIC 具有重要的參與意義。我國社群自 APNIC 成立之始經年踴躍參與 APNIC 相關活動，我國應持續參與 APNIC，與其他國家地區進行交流，俾提高國際能見度。

目　錄

壹、 亞太網路資訊中心會議簡介

一、 會議概要

1993年於澳洲成立的亞太網路資訊中心（Asia Pacific Network Information Centre，APNIC），為掌管亞太地區網路號碼資源分配的區域型網際網路註冊管理機構（Regional Internet Registry，RIR）之一，主要負責IP位址及AS（Autonomous System）[1]號碼的管理與分配等，亦積極參與亞太地區網際網路基礎設施發展與網路技術培訓等工作。

APNIC每年至少舉行2次國際會議，匯集來自世界各地的網路技術專家、網路政策及治理代表、業界領袖，以及其他利害關係人，參加者可透過會議學習，分享經驗及觀點，並藉此建立人脈。

APNIC 57會議（Asia-Pacific Network Information Centre 57 Conference）於2024年2月27日至3月1日於泰國曼谷舉行，此為2024年度第1次APNIC會議，會議中藉由講者演講、論壇討論等形式，將最新的網際網路發展趨勢與所有與會者分享。

APNIC 57會議所有場次議程，詳參APNIC57網站資訊。本次會議係與亞太網路科技高峰會（Asia Pacific Regional Internet Conference on Operational Technology，APRICOT）合辦。

[1] AS為 Autonomous System的簡稱，即自治系統，指的是所有處於同樣的管理網域（Administrative Domain）下所有網路的集合；而管理網域指的是歸屬於相同管理系統下的主機、路由器與內部連接網路的集合。

二、 參與場次

（一）目的：

本部指派2名人力，財團法人中華民國國家資訊基本建設產業發展協進會1名人力協同，前往泰國曼谷參加APNIC 57實體會議，在會議中蒐集有關網路安全、亞太及國際IP政策進展、技術等最新發展資訊。

（二）過程：

1. 會議時間：2024年2月27日-3月1日
2. 參與場次：表1為參與APNIC 57會議之場次。（APNIC 57 會議完整議程表，請詳參活動網站。）

表1. APNIC 57會議參與場次

日期	場次名稱
2/27	Opening Ceremony and Plenary 開幕典禮暨專題演講
	Asia Pacific Operators Forum（APOPS）1 亞太網路業者論壇 第一場
2/28	Asia Pacific Operators Forum（APOPS）2 亞太網路業者論壇 第二場
	APNIC Panel Discussion APNIC 座談
	APNIC IPv6 Deployment APNIC IPv6布建。
2/29	Routing Security SIG Forum APNIC 路由安全特別興趣小組論壇
	Open Policy Meeting 1 公開政策會議 場次1

日期	場次名稱
	Open Policy Meeting 2 公開政策會議 場次2
3/1	APNIC Annual General Meeting （AGM） 1 APNIC 年度大會 場次1
	APNIC Annual General Meeting （AGM） 2 APNIC 年度大會 場次2
	APNIC Annual General Meeting （AGM） 3 APNIC 年度大會 場次3

貳、 會議摘要

一、 開幕典禮暨專題演講

（一）議程：開幕典禮暨專題演講（Opening Ceremony & Plenary）

（二）時間：2024 年 2 月 27 日 15:30 - 17:00（UCT +08:00）

（三）講者：

1. 主持人：Thawan Paruggamanont （Point）
2. 致詞嘉賓：
   (1)Ole Jacobsen（APNOG Board Secretary）
   (2)Kenny Huang（APNIC EC Chair）
   (3)Pensri Arunwatanamongkol（THNIC Foundation Executive Director）
   (4)Mona Jaber（Queen Mary University of London Senior Lecturer in IoT）
   (5)Randy Bush（Internet Initiative Japan Research Fellow）

（四）會議摘要：

本場次請到APNOG董事會秘書Ole Jacobsen、APNIC執行委員會（Executive Committee，EC）主席黃勝雄博士，以及主辦單位泰國網路資訊中心基金（THNIC Foundation）執行長Pensri Arunwatanamongkol發表開幕致詞。本次也請到網際網路之父Vint Cerf以影片祝賀並致詞。致詞完畢後，分別由倫敦瑪麗王后大學（Queen Mary University of London）物聯網資深講師Mona Jaber及Internet Initiative Japan資深研究員Randy Bush發表專題演講。

1. 應用物聯網達成永續目標(The Intelligent Internet of Things for Sustainable Development Goals)

聯合國在2015年發布2030年永續發展議程（2030 Agenda for Sustainable Development），列出17項希望於2030年達成的永續發展目標（Sustainable Development Goals，SDG）。然而，根據聯合國2023年發布的SDG報告（The Sustainable Development Goals Report 2023: Special edition），至少85%的目標都仍離實現遙遙無期，氣候暖化和空氣污染改善幅度尤為緩慢。

有鑑於此，Mona Jaber及其團隊希望探討利用數位科技，尤其是物聯網（Internet of Things，IoT）和機器學習（Machine Learning，ML），加速達成SDG的可能。

Jaber的團隊之所以希望應用物聯網，是看中物聯網部署便宜簡單且無所不在的特性。團隊以分散式感應裝置的方式應用物聯網，達成「整合感測及通訊」（integrated sensing and communication，ISAC），同時做到感測及回傳感測結果的兩種功能。

Jaber分享應用案例，團隊在倫敦的地下光纖網路設置智慧感測裝置，用以即時感測路面資訊並分析交通實況，透過整合資訊達成更安全、值得信賴且更環保的交通網路。

此應用實驗雖證明物聯網能有效協助改善地面交通網路，但也呈現多重挑戰。Jaber將挑戰分成兩種類型，技術上的挑戰如：如何有限的可用頻譜中選擇傳輸訊號的網路、物聯網裝置囿於尺寸難以確保高安全性、如何從蒐集到的大量無效資料中過濾汲取有效資料，以及物聯網裝置導致的碳足跡等。

非技術的挑戰則包括「新興技術僅能治標不治本」的批評、永續假象（雖然資料呈現空氣品質改善，但原因並非環保作為生效，而是因為人民負擔不起油價），以及部分民眾對永續目標的抗拒心理，認為強制要求環保是限制人民自由等。

針對上述挑戰，Jaber的團隊在瑪麗王后大學成立新的實驗室，以社會科學專業領軍，結合跨領域長才，希望從根本定義問題、積極與社群溝通後，再以科技輔助解決問題。

2. 區域網際網路註冊管理機構的社會契約(The RIR Social Contract)

社會契約（social contract）的概念起源於啟蒙時期，主張人民透過與國家政府簽訂社會契約，以認可政府統治的正當性、同意履行一定責任義務，交換國家保護。若應用於其他情境，則代表雙方對彼此社會或政治上關係達成協議的過程。

Randy Bush以歐洲網際網路註冊中心RIPE NCC((Réseaux IP Européens Network Coordination Centre)為例，說明RIPE NCC的工作不僅止於分派IP位址，更包括負責歐洲、中東及部分俄羅斯的網路營運。根據RIPE NCC的創始文件，RIPE NCC成立目的是確保歐洲網路營運的行政與技術協調，希望促進資訊交流、網路互連及協調合作。以日常運作而言，RIPE 大致分成自願者組成的社群，以及受薪職員組成的秘書處；前

者負責制定政策，後者則負責執行。

Bush強調，他不打算在此演講中討論RIR的行政體制。並非這不重要，僅因為這不是他今天希望探討的主題。他表示，行政體制必須建立於社會契約之上，所以此講著重研討「我們」對與RIR的社會契約的期待，以及誰是「我們」。

Bush認為，所謂的「我們」應包含網際網路營運社群、一般使用者、公民社會、政府及我們的下一代。過去RIR的社群通常以網路營運從業人士、工程師等為主，而且極度排外，抗拒如公民社會或政府的參與。Bush特別指出，隨著網路成為現代社會不可或缺、無處不在的一部份，此想法已經過時且不切實際，網路營運現在亟需其他利害關係方，尤其是公民社會及政府的積極參與。

他也分享他心目中網路營運社群應具備的特質，包括開放、公平、透明、文明、具多元代表性並且謹慎行事。他強調，所謂的多元不只性別、種族或文化背景上的多元，更包含看法或理想目標的多元。

五大RIR自成立至今，已順利運轉數十年，雖然各RIR有各自的問題，AFRINIC目前也正因過去主事者貪腐而遭受苦果中，但Bush認為社群理當為RIR至今的成功自豪，也應正視須改善修正之處。他最後強調，此改善進化之路不能由網路工程師獨行，必須強力招徠社經工程師（social engineerers），也就是公民社會與政府代表的加入。

二、 亞太網路業者論壇 場次1

（一）議程：亞太網路業者論壇場次 1（Asia Pacific Operators Forum 1，APOPS 1）

（二）時間：2024 年 2 月 27 日 16:30 - 18:00（UTC +08:00）

（三）講者：

1. 主持人：Yoshinobu Matsuzaki（IIJ Senior Engineer／APNIC EC Treasurer）
2. 專題演講：

(1)Geoff Huston（APNIC Chief Scientist）

(2)Massimo Candela（NTT Principal Engineer）

(3)Lia Hestina（RIPE NCC Senior Project Coordinator）

（四）會議摘要：

會議一開始，由主持人Yoshinobu Matsuzaki開場致詞，歡迎所有與會者出席亞太網路業者論壇。

第一位講者為APNIC首席科學家Geoff Huston，演講的題目是「外側陰影中的網路（Networking in the Penumbra）」。

過去十年，網路傳輸服務供應商和網路應用服務之間的相互不信任程度急劇上升。應用服務逐步將用戶流量轉變為加密通訊模式。本演講探討了這個主題，並探討了當今的應用程式環境如何試圖向底層網路隱藏用戶交易，以及其對於網路營運商所代表的意義。

值得信賴的網路是指網路享有特權地位，能夠觀察誰在與誰通信，以及他們互相說的話。用戶期望在通訊中隱私被保護，這種期望往往是以限制公共網路業者揭露透過網路營運所獲得的知識等監管措施來加強。然而，信任已被侵入性中介軟體所侵蝕，這些中介軟體收集有關使用者行為的資料。其普遍採用廣告收入作為服務平臺的獲利手段，也是收集個人使用者詳細資料的主要動力，而且個人資料越詳細，使用者對廣告商的價值越高。

那我們該如何應對？IETF 2014年RFC 7258[2]「遍布的監控是對隱私的攻擊（Pervasive Monitoring is an attack on privacy）」提到：「IETF社群的技術評

[2] RFC 7258：Pervasive Monitoring Is an Attack，https://datatracker.ietf.org/doc/html/rfc7258

估指出遍布的監控(Pervasive Monitoring,PM)是對網路使用者和組織隱私的攻擊。」該社群已表示強烈同意，遍布的監控是一種攻擊，需要透過設計協定使遍布的監控顯著更昂貴或不可行來減輕這種攻擊。

這代表應用程式的改變，朝向隱藏網路流量，轉向對所有網路交易使用傳輸層安全標準（Transport Layer Security，TLS[3]），即超文本傳輸安全協定（Hyper Text Transfer Protocol Secure，HTTPS[4]）向客戶端驗證伺服器的身份，並且讓服務交易被加密。依據Cloudflare統計目前用戶連線其網站，使用安全協定HTTPS約佔98.3%，HTTP約佔1.7%。

另一個應用是隱藏DNS，隱藏來自網路中DNS解析的查詢和回應，工作集中在透過加密交換的DNS資料來隱藏DNS查詢名稱。由APNIC統計查詢Cloudflare公開DNS進行解析的資料顯示，使用透過HTTPS保護DNS用戶端域名系統的安全協定(DNS over HTTPS，DoH[5]）約佔12.5%，通過傳輸層安全協定來加密並存取域名系統的安全協定（DNS over TLS，DoT[6]）約佔8.5%。

我們可以更進一步嗎？我們能否將兩端彼此隱藏，以便在網路中的任何點上都無法同時看到傳輸的兩端？我們是否也可以選擇性地隱藏交易內容，使得端點和交易內容不能同時被發現。

誰關心隱私？主要是花費大量資金收集詳細使用者檔案的單位都不想將這些資料外洩給競爭對手，因此，隱私是為了保護從以下來源收集使用者個人資料的核心資產，包括：其他服務，通用主機平臺，通用基礎設施服務，以及網路等。

我們希望允許應用程式以隱藏其行為的模式運行。作法上可透過從公共服務管理的協定堆疊中的較低層級盡可能地提取並在應用程式中執行它。

因此在傳輸層隱私上，正在研究如何將傳輸控制協定（Transmission Control Protocol，TCP）[7]從主機平臺的公共部分中提升出來，並將其轉移到應用程式中，我們

[3] TLS：傳輸層安全性協定（Transport Layer Security，縮寫：TLS），目的是為網際網路通訊提供安全及資料完整性保障。
[4] HTTPS：超文本傳輸安全協定（Hyper Text Transfer Protocol Secure，縮寫 HTTPS；常稱為 HTTP over TLS、HTTP over SSL 或 HTTP Secure）是一種透過計算機網路進行安全通訊的傳輸協定。HTTPS 經由 HTTP 進行通訊，但利用 SSL/TLS 來加密封包。HTTPS 開發的主要目的，是提供對網站伺服器的身分認證，保護交換資料的隱私與完整性。
[5] DoH：DNS over HTTPS（縮寫：DoH）是域名系統的安全協定，以 HTTPS 協定完成 DNS 解析來保護網路主機的隱私，能避免傳統 DNS 協定中使用者的 DNS 解析請求被竊聽或者修改的情況。DoH 由 IETF RFC 8484 支援。
[6] DoT：DNS over TLS（縮寫：DoT）是通過傳輸層安全協定（TLS）來加密並打包域名系統（DNS）的安全協定。此協定旨在防止中間人攻擊與控制 DNS 資料以保護使用者隱私。RFC 7858 及 RFC 8310 定義了 DNS over TLS。
[7] 傳輸控制協定（Transmission Control Protocol，TCP）是一種連接導向的、可靠的、基於位元組流的傳輸層通訊協定，由 IETF 的 RFC

需要更改TCP。至於如何更改TCP？2021年5月IETF公布RFC9000[8]，QUIC:A UDP-Based Multiplexed and Secure Transport（一種基於UDP的安全多工傳輸協議），QUIC[9]規範推出了標準化版本，可以使用通用的傳輸層網路協定QUIC來改變TCP。

QUIC是新的TCP，QUIC是傳輸服務的邏輯演進，提供更大的彈性、更快的連線設定和更多的傳輸服務，這是我們對強大的現代傳輸協定的期望。依據Cloudflare針對使用者透過安全協議保護流量統計報告，QUIC的使用率約占28.8%，TLS 1.3約佔64.3%。

QUIC很重要的原因是，因為QUIC更快，QUIC可將一切加密，而且QUIC具有應用層能力，QUIC可以透過UDP[10] API與平臺溝通，因此QUIC的所有內容都可以在應用程式內實現。這使應用程式能夠更好地控制其服務結果並減少外部依賴。

TCP的前景看起來不太好，QUIC的優點在於不僅啟動速度更快，而且以順暢的方式支援多通道，QUIC阻止網路營運商透過直接操縱TCP控制參數來執行流量管制，以及QUIC允許應用程式服務提供者可控制其網路工作的擁塞行為。

QUIC正在將網路傳輸和主機平臺推向網路中的商品角色，並允許應用程式有效地自訂它們想要提供服務的方式並主導整個網路環境，這讓QUIC成為應用程式對傳輸的期待。

這對網路意味著應用程式、主機和網路之間的關係已惡化為相互不信任和懷疑，應用程式現在透過加密和間接封裝盡可能做更多的服務事務來保護其完整性，QUIC成為加密和重定向傳輸流量過程的部分，對於網路業者來說，幾乎就沒有什麼可看或可做的。

預期未來新的網路空間，首先，垂直整合服務提供者退出歷史舞臺，使得放鬆管制的競爭性服務業在各個層面繼續專業化；其次，傳輸不再是不可避免的壟斷，大量複製的內容可以取代許多傳輸服務單元；最後，對平臺的控制不再是對使用者的控制。作業系統被推回基本的任務排程角色，其功能則被吸收到應用程式空間中。

---

793 定義。在簡化的電腦網路 OSI 模型中，它完成第四層傳輸層所指定的功能。

[8] RFC 9000 QUIC: A UDP-Based Multiplexed and Secure Transport，https://datatracker.ietf.org/doc/html/rfc9000。

[9] QUIC：QUIC 最初是「快速 UDP 網際網路連接」（Quick UDP Internet Connection）的首字母縮寫，但在 IETF 標準中，QUIC 不是任何內容的縮寫。QUIC 提高了目前使用 TCP 的連接的網路應用的效能。QUIC 透過 UDP 協定在兩個端點之間建立若干個多路連接，以達到在網路層淘汰 TCP 的目標。因為其設計目標在於取代 TCP 協定，該協定偶爾也被暱稱為「TCP/2」。2021 年 5 月 IETF 公布 RFC9000，QUIC 規範推出了標準化版本。

[10] UDP：使用者資料包協定（User Datagram Protocol）是一個簡單的資料包的通訊協定，位於 OSI 模型的傳輸層。該協定在 1980 年設計且在 RFC 768 中被規範。

未來的網路，每個服務都能夠定義自己的操作行為，這些行為是該服務固有的；此外，未來將成功地最小化和商品化網際網路的公共部分，並將有價值的功能和服務置入每個應用程式中。

第二位講者為NTT首席工程師Massimo Candela，演講的題目是「BGP和RPKI監控（BGP and RPKI Monitoring）」。

提供易於使用的工具來監控邊界閘道器協定（Border Gateway Protocol，BGP[11]）和資源公鑰基礎設施（Resource Public Key Infrastructure，RPKI[12]）的正確性是提高全球網路穩定性的關鍵操作。儘管RPKI的採用持續增加，但許多業者仍然缺乏基本的監控。相當大比例的AS每天都會宣布無效RPKI，但卻很慢才發現。在本次簡報中，展示了BGPalerter，這是一款受到全球許多ISP信賴的開源監控工具。能夠監控劫持、可見性遺失、洩漏、無效RPKI公告以及錯誤RPKI配置等。此外，本簡報也展示過去4年來，由RPKI監控所偵測到影響RPKI信任錨故障的案例清單。

BGPalerter是一個NTT所開發用於BGP和RPKI監控的工具，開發的動機是為了監控NTT宣告的位址前綴（prefix），以偵測劫持、可見性遺失、或是不預期的設定改變，NTT將其程式碼開源，特性是能即時回應，易於使用，可自動組態配置，以及無需收集資料。

BGPalerter BGP監控若出現以下情況，您將收到警報，如您的任何前綴不見了、您的任何前綴被劫持、您的AS正在宣布一個新的前綴，以及會出現一個新的下游或上游AS。

BGPalerter RPKI監控若出現以下情況，您將收到警報：您的AS正在宣告RPKI無效前綴，您的AS正在宣告未涵蓋在路由來源授權（Route Origin Authorization，ROA[13]）的前綴，涵蓋您任何前綴或AS的ROA被刪除/新增/修改，信任錨TA（Trust Anchor，TA）[14]故障，以及ROA即將到期。

[11] 邊界閘道器協定（Border Gateway Protocol，BGP）是網際網路上一個核心的去中心化自治路由協定。它通過維護 IP 路由表來實現自治系統（AS）之間的可達性，屬於向量路由協定。BGP 使用基於路徑、網路策略或規則集來決定路由。

[12] 資源公鑰基礎設施（Resource Public Key Infrastructure，RPKI），也稱資源認證（Resource Certification），是一項旨在使網際網路路由基礎設施更安全的公開金鑰基礎建設（PKI）框架。

[13] 路由來源授權（Route Origination Authorizations，ROA），他讓 IP 位址持有者將本身擁有的 IP 位址前綴綁定到特定的自治系統，用以證明 BGP 路由的正確性，避免被有心人士偽造路由資訊，而發生 BGP 路由劫持情況。

[14] 信任錨（Trust Anchor，TA），信任錨這一概念出自信任模型，即信任的起點，是指在信任模型中，當可以確定一個實體身份或者有一個足夠可信的身份簽發者證明該實體的身份時，才能做出信任那個身份的決定。這個可信的身份簽發者成為信任錨。

第三位講者為RIPE NCC高級專案協調員Lia Hestina，演講的題目是「使用RIPE Atlas和RIS將事件發生時的影響降至最低（Minimising Impact When Incident Occur with RIPE Atlas and RIS）」。演講內容是概述網路營運商如何利用RIPE Atlas[15]和路由資訊服務RIS（Routing Information Service，RIS[16]）數據，透過策略準備和快速回應，最大限度地減少事件的影響。

第一個重點是在事件發生之前做好準備，其中RIPE Atlas和RIS資料發揮著重要作用。這些工具可協助營運商分析網路行為、識別漏洞並優化基礎設施。透過特定的案例和最佳實踐，操作員可以將這些資源整合到事件發生前的準備工作中。

下一步的重要性是在事件發生期間採取迅速的通報行動。簡報中介紹了即時測量、結果顯示和數據收集的功能和方法。透過利用RIPE Atlas和RIS的分析，營運商可以找出事件發生、了解其範圍並立即採取行動進行偵錯或向客戶透明地傳達網路效能。

這種整合方法將有助於增強網路韌性，並使營運商能夠維持最佳效能標準，即使面對不可預見的事件也能確保穩健且反應迅速的網路效能。

[15] RIPE Atlas 是一個全球探測器網路，用於測量網際網路連接性和可及性，提供對網際網路狀態的即時了解。
[16] 路由資訊服務（Routing Information Service，RIS），RIS 是一個路由資料收集平臺。它收集 BGP 上的數據，透過收集這些數據，RIS 提高了我們對全球網際網路路由系統的理解和解決安全風險。

三、 亞太網路業者論壇 場次2

（一）議程：亞太網路業者論壇場次 2（Asia Pacific Operators Forum 2，APOPS 2）

（二）時間：2024 年 2 月 28 日 10:30 - 12:00（UTC +08:00）

（三）講者：

1. 主持人：Yoshinobu Matsuzaki（IIJ Senior Engineer／APNIC EC Treasurer）
2. 專題演講：

(1)Geoff Huston（APNIC Chief Scientist）

(2)Doug Madory（Kentik Director of Internet Analysis）

(3)Thomas Holterbach（University of Strasbourg Postdoctoral researcher）

（四）會議摘要：

會議一開始，由主持人Yoshinobu Matsuzaki開場致詞，歡迎所有與會者出席第二場次亞太網路業者論壇。

第一位講者為APNIC首席科學家Geoff Huston，演講的題目是「2023年的邊界閘道器協定（BGP in 2023）」。

BGP路由表可以告訴我們很多關於網路動態的資訊。這不僅與儲存路由表所需的記憶體大小有關，而且其成長率可以告訴我們網路成長的動態以及IPv6與IPv4網路成長的相對比較。網路融合的動態還可以告訴我們BGP路由基礎設施如何應對擴展壓力。在本演講中，展示所研究的2023年BGP路由表，並對其未來五年的可能規模和動態特性做出預測。

由IPv4路由表統計顯示，2023年IPv4位址總共1,800萬個位址從宣告的網路中撤銷，轉移為未使用，未宣告的IPv4位址淨增加了1,800萬個。從路由成長圖來看，IPv4網路規模成長正在放緩，路由表的成長速度也略低於近5年平均，2022年新增36,000筆，2023年新增20,000筆。此外，AS數量也略降低，2023年宣告了1,100個新的ASN（2021年為1,400個），經過2023年，觀察到整體IPv4路由成長趨勢將放緩甚至可能逆轉。

反觀2023年IPv6 BGP路由表數量方面仍在增加，目前每年約增加30,000筆路由，

約17%。其中主要使用/48，另外新增2,000筆ASN宣告IPv6前綴，增加了2,500筆 /32 IPv6位址，只是2023年成長率低於2018－2020年的成長率。

IPv4路由表數量的預測方面，依過去4年資料採用最佳預測模型的多項式函數，該函數將在2024年達到尖峰值，路由數量略低於100萬筆。

至於IPv6的成長模型到目前仍高度不確定，看起來線性成長模型與最近24個月的數據相匹配，但基礎網路成長較緩，該模型中超過一半的成長是由於/48持續密集使用。從路由表的數量增長來看，IPv6路由表成長速度仍比IPv4路由表快得多。

第二位講者為Kentik網際網路分析總監Doug Madory，演講的題目是「網際網路史上最大的BGP事件(A Brief History of the Internet's Biggest BGP Incidents)」。

追溯1997年的AS7007洩漏事件，本次演講介紹了網際網路歷史上最引人注目、最重大的BGP事件，從干擾流量的洩漏到最近的加密竊取劫持。從歷史的角度探討了「已經取得了哪些進展以及甚麼是最終保護BGP的方法？」的問題

回顧BGP事件的歷史，這些事件主要發生的原因，首先是合法流量被中斷，其次是通訊被錯誤導向。

由於路由洩漏而造成的網路中斷方面，路由洩漏是指路由宣告的傳播超出其預期範圍。也就是說，從一個AS向另一個AS發布所學習到的BGP路由違反了AS路徑的預期策略。詳細內容可從IETF RFC7908[17]了解BGP路由洩漏的問題定義與分類。1997年4月AS7007的洩漏事件，就是路由源洩漏的案例。此為第一次因路由洩漏造成重大中斷的事件，發生原因是軟體錯誤導致路由器宣告大部分全球路由表成為路由源。

另外由於鄰接點洩漏而造成的中斷案例，例如2018年11月MainOne AS37282的洩漏，將互連路由傳遞給轉傳提供者，造成Google、Cloudflare等網路中斷。2019年6月Allegheny Technologies AS396531的洩漏，約有29,000筆路由從一個提供者發送到另一個提供者，造成Cloudflare經歷了最大的中斷。

近年來，路由洩漏的防範隨著國際第一級網路服務提供商同意過濾掉未經授權的RPKI，取得了巨大進展，例如NTT、GTT、Arelion (Telia)、Cogent、Telstra、PCCW、

[17] RFC7908: Problem Definition and Classification of BGP Route Leaks，BGP路由洩漏的問題定義與分類，https://datatracker.ietf.org/doc/html/rfc7908

Lumen等等公司，可由NIST RPKI Monitor[18]的趨勢線觀察正朝著正確的方向發展。

如果只有少數網路拒絕無效路由，則單獨存在ROA仍是無用的。但從最近的分析顯示，RPKI無效路由的傳播是其他類型的一半或更少。因此，希望成為常識的是，大部分流量都是由有效的RPKI路由所引導，而當RPKI無效時，路由傳播要減半。

至於仍然存在誤導通訊的路由劫持，需要BGPsec[19]來消除AS的冒充，保護透過連續BGPsec感知的AS延展，主要雲端供應商和網路服務供應商採用的話可以嚴格限制AS冒充的功效，而且部分部署也仍然會有好處，期待此來消除AS來源冒充。

第三位講者為法國Strasbourg史特拉斯堡大學博士後研究員Thomas Holterbach，演講的題目是「偵測偽造來源劫持的系統（A System to Detect Forged-Origin Hijacks）」。

儘管全球都在努力保護網路路由的安全，但攻擊者仍然成功地利用了BGP缺乏強大安全機制的漏洞。講者重點介紹一種經常使用的攻擊媒介：偽造來源劫持，這是一種BGP劫持，其中攻擊者操縱AS路徑，使其不受RPKI-ROV過濾器的影響，並從BGP監控的角度來看，使其顯示為合法的路由更新。檢測偽造來源劫持（Detect Forged-Origin Hijacks，DFOH）系統，這是一個能夠快速、一致地檢測整個網際網路中偽造來源劫持的系統。歸結偵測偽造來源劫持為推斷BGP路由中的AS路徑是否合法或已被操縱。經證明，目前檢測BGP異常的最先進方法不足以應對偽造來源劫持。我們確定了讓偽造AS路徑具有挑戰性的關鍵屬性，並將DFOH設計成對現實因素具有穩健性。我們的推理管道包括兩個關鍵要素：（i）提供一組策略選擇的特徵，以及（ii）偵測違反由業務關係模式的虛假AS路徑。DFOH僅在5分鐘內即可偵測到90.9%的偽造來源劫持。此外，它每天向整個網路報告約17.5起可疑案件，這個數量可以讓業者依據調查報告的案件採取對策。DFOH已啟動並運行，詳細內容請參考連結 https://dfoh.uclouvain.be/。

[18] NIST RPKI Monitor，美國國家標準暨技術研究院 RPKI 觀測網，https://rpki-monitor.antd.nist.gov/

[19] 邊界閘道協定安全性: （Border Gateway Protocol Security，BGPsec）是 2017 年 9 月發布的 RFC 8205 中定義的邊界閘道協定的安全性擴充。

四、 APNIC 座談

（一）議程：APNIC 座談 - 內容傳遞網路的崛起與對網際網路及位址政策的意義

APNIC Panel - The rise and rise of CDNs; what that means for the Internet and address policy.

（二）時間：2024 年 2 月 28 日 15:30 - 17:00（UTC +08:00）

（三）講者：

1. 主持人：George Michaelson（Asia Pacific Network Information Centre Senior Research Scientist）
2. 專題演講：

(1)Geoff Huston（APNIC Chief Scientist）

(2)Bart Van de Velde（Cisco Sr. Director Engineering）

(3)Joanne Liew（Cloudflare Interconnection Manager）

(4)Kam Sze Yeung（Akamai Principal Network Architect）

（四）會議摘要：

本場次由APNIC產品經理George Michaelson擔任主持人，邀請到APNIC首席科學家Geoff Huston、Cisco資深工程主任Bart Van de Velde、Cloudflare互聯經理Joanne Liew，以及Akamai首席網路架構師兼APNIC執委會成員Kam Sze Yeung與談，探討內容傳遞網路（Content Delivery Network，CDN）的崛起，及其對網際網路，尤其位址政策代表的意義。

首先由Geoff Huston介紹CDN為何崛起。Huston回顧通訊技術歷史，從電話談起，解釋網路技術代表的革新意義，包括取消同時性需求、去集中化、將複雜功能推向邊緣裝置；以封包交換為主的網路技術之所以迅速取代電路交換的電話技術，「便宜」是最大主因。

內容的出現，動搖了網路的「伺服器與客戶端」架構。以網路服務供應業者的角度而言，內容供應業者和存取內容的一般使用者一樣，都是「客戶端」。但對內容供應業者而言，網路服務供應業者之所以有顧客，是因為顧客希望透過他們存取內容。網路服務業者與內容業者彼此之間因此產生齟齬，雙方都認為對方應該為自己的服務

付費。

內容業者試圖利用OTT（over the top）服務，將使用者直接帶到自己的伺服器，以解決此爭端。但此做法的問題在於全球網路分布不均，網路技術的演進連帶提升使用者對速度的要求；使用者位置離內容越遠，不只使用體驗下滑，內容業者的成本也提高。

CDN將內容快取並存放於網路邊緣，不只降低延遲，也透過繞道網路傳輸避開網路中立爭議，儲存和傳輸至本地網路的成本大幅降低，也因此彌補CDN的營運成本。對內容業者而言，CDN的優點包括規模化、降低服務成本、降低對中介服務的依賴及不確定性，更能強化服務韌性。換句話說，簡直無可挑剔。

Bart Van de Velde則從網路角度分享對網際網路和CDN的觀察，他分享Cisco的量測資料，特別點出幾個目前網路樣態的基本重點，包括已經不存在未加密的網路訊務、七成以上流量都傳至雲端、至少一半的流量是DNS。換句話說，DNS擔任整個網際網路中所有內容的負載平衡器。隨著QUIC使用率穩定成長，Van de Velde也預測QUIC將成為未來主流傳輸協定。

雖然加密成為趨勢，但為了仍想監測轄下網路的業者，Van de Velde提醒有些資訊無論如何加密都不會消失。諸如IP表頭、訊務負載尺寸和封包之間的時間間隔等資訊，都仍能在網路線路上觀測到。

觀測網路有其意義。對網路樣態的了解有助於我們發現問題、解決痛點，以及觀察趨勢。有鑑於此，Van de Velde認為網路營運業者應開始發掘新的觀測資料點，以了解轄下網路狀況。

根據Van de Velde分享的觀測資料，當代網路流量的目的地幾乎被十大雲端網站[20]獨佔。主持人因此詢問所有與談人，尤其3位主流雲端網路業者代表，公共政策對他們的意義為何？畢竟對這些業者而言，他們必須遵守的義務僅限於合約，包含與內容業者及終端使用者的合約，不像過去電信業者和網路服務供應商，一定程度上仍受政府規管。

Kam Sze Yeung回應表示，以業者角度而言，最終考慮的都是如何改善技術以更

[20] Apple、Amazon、Meta （Facebook & Instagram）、Netflix、Disney、Microsoft、Alphabet （Google & YouTube）、Akamai。

有效地提供服務。他認為只要CDN的商業模式和位址使用方式正當，其治理方式與位址管理政策應大同小異。

主持人再提問，鑑於當代網路生態已沒有單一節點專用單一IP位址的需求，究竟IP位址還算是當年眾人以為的稀缺資源嗎？IP位址的價值到底為何？

Joanne Liew認為，對雲端服務供應業者，如其代表的Cloudflare來說，IP位址和邊界閘道協定（Border Gateway Protocol，BGP）仍很重要，在日常運作中他們仍需要這些資源，以將使用者導向最近的資料中心。

Geoff Huston則主張，單一節點使用單一IP位址的想法不符經濟效益，加上各種新興技術，早已並非必須。他大膽宣言，現在有了CDN，我們已經進入「後IP位址」的時代。

五、 APNIC IPv6 布建

（一）議程：APNIC IPv6 布建（APNIC IPv6 Deployment）

（二）時間：2024 年 2 月 28 日 17:30 - 19:00（UTC +08:00）

（三）講者：

1. 主持人：Kenny Huang（TWNIC Chairman of Board）
2. 專題演講：
   (1)Geoff Huston（APNIC Chief Scientist）
   (2)Mukhammad Andri Setiawan（IDNIC Head of Training and People Productivity / Universitas Islam Indonesia Chief Information Officer）
   (3)Yan,Gao（CERNET CORPORATION General Manager of the Marketing Department）
   (4)Mohit P. Tahiliani（National Institute of Technology Karnataka, Surathkal, India Associate Professor）

（四）會議摘要：

會議一開始，由主持人TWNIC Kenny Huang黃勝雄董事長致詞，歡迎所有與會者出席IPv6布建場次，並說明本場次主要著重於IPv6布建的進展，以及營運商的最佳實踐。

第一位講者為APNIC首席科學家Geoff Huston，演講的題目是「IPv6部署：30年後（IPv6 Deployment: 30 Years Later）」。介紹IPv6過去30年的位址分配、路由和部署等資料。

早期IPv6部署，是使用IPv6-over-IPv4[21]封裝的覆蓋網路[22]來進行的，網際網路協定版本6的測試平臺，是IETF專案的產物，1996年3月建立了6Bone[23]，使用IPv6試用位

[21] IPv6-over-IPv4 是一種 IPv6 轉換傳輸機制，是將 IPv6 的封包直接封裝在 IPv4 的封包中，並通過內嵌於 IPv6 位址的 IPv4 位址資訊直接在 IPv4 網路上傳輸。

[22] 覆蓋網路：Overlay network，是一種建立在另一網路之上的電腦網路。覆蓋網路中的節點可以被認為是通過虛擬或邏輯連結相連，其中每個連結對應一條路徑（Path）。節點之間也可能通過下層網路中的多個物理連接實現相連。網際網路自身最初也是作為一個電話網路之上的覆蓋網路構建，而當今（藉由 VoIP 的引入），電話網路正越來越變成一個建立在網際網路之上的覆蓋網路。

[23] 6bone 是網際網路協定版本 6 的測試平臺，它是 IETF IPng 專案的產物，該專案創建了 IPv6 協定，旨在最終取代目前的網際網路網路層協定（即 IPv4）。

址，3FFE::/16（RFC 2471[24]），該6Bone網路於2004年1月開始逐步淘汰，並於2006年6月完全退役。早期的IPv6位址分配，1999年1月1日，IANA記錄了以下IPv6地址分配：2001:200::/23至APNIC，2001:400::/23至 ARIN，2001:600::/23至RIPE NCC。

由統計圖展示20年來IPv6位址宣告使用的成長趨勢，也可以看到IPv6部署的演進。總結IPv6全球的進展，仍然是一張零散的圖片：在印度、法國、德國、馬來西亞、沙烏地阿拉伯、美國、烏拉圭和越南已經成熟，在非洲、中東、東歐和南歐的部署很少；此外，推動IPv6部署的緊迫感並不存在：整體成長率似乎已經放緩，這意味著現有的IPv4 NAT[25]網路沒有立即面臨改變的壓力，而2024年的IPv6部署進展似乎會遵循一般網路設備的生命週期。

此外，IPv4/IPv6雙協定不意味著終點，網路從IPv4過渡到IPv4/IPv6雙協定的整個目標並不是要看到普遍存在的IPv4/IPv6雙協定環境，一旦達到雙協定部署的「群聚效應」[26]，就可以放棄支援IPv4，我們可能需要一段時間才能達到這種「群聚效應」部署場景，但一旦達到這個臨界值，那麼下一步放棄支援IPv4的速度可能會快得多。

第二位講者為IDNIC人員培訓和生產力主任暨印尼伊斯蘭大學首席資訊長Mukhammad Andri Setiawan，演講的題目為「透過策略採用、治理和自動化加速企業IPv6布建（Accelerating IPv6 Deployment in Enterprises through Strategic Adoption,Governance,and Automation）。

演講介紹由印尼伊斯蘭大學Mukhammad Andri Setiawan博士領導的一個計畫項目，該計畫是ISIF.ASIA專案的一部分。該計畫旨在提高印尼企業、教育和政府部門對IPv6的採用。利用設計思維啟發的技術採用方式來解決技能短缺和技術知識不足等挑戰。這種方法強調以人為本的設計和實施IPv6時的同理心，提倡原型、圖表和自動化的結合。也強調IPv4/IPv6雙協定基礎架構從IPv4無縫過渡到IPv6的必要性。

有哪些不同的方法可以幫助IPv6被採用，從2024年開始，我們將引入自動化來幫助企業重新配置他們的設備，我們甚至會使用生成式人工智慧[27]，人工智慧將幫助我們

[24] RFC 2471: IPv6 Testing Address Allocation，https://datatracker.ietf.org/doc/html/rfc2471。
[25] 網路位址轉譯（Network Address Translation，NAT），又稱 IP 動態偽裝（IP Masquerade），是一種在 IP 封包通過路由器或防火牆時重寫來源或目的 IP 位址或埠的技術。這種技術普遍應用於有多臺主機，但只通過一個公有 IP 位址訪問網際網路的私有網路中。
[26] 群聚效應（Critical mass）是一個社會動力學的名詞，用來描述在一個社會系統裡，某件事情的存在已達至一個足夠的動量，使它能夠自我維持，並為往後的成長提供動力。又叫作「臨界量」或「轉捩點」。
[27] 生成式人工智慧（Generative artificial intelligence，或稱 Generative AI、生成式 AI、產生式 AI）是一種人工智慧系統，能夠產生文字、圖像或其他媒體以回應提示工程。產生模型學習輸入數據的模式和結構，然後產生與訓練數據相似但具有一定程度新穎性的新內容，而不僅僅是分類或預測數據。

識別所有設備的當前配置參數，並根據提供的情境，人工智慧將重新配置所有設備，使其支援IPv6。

第三位講者為CERNET行銷部總經理Gao Yan，演講的題目是「基於CERNET2（IPv6）的超級電腦網際網路專案進度報告（The Progress Report of Supercomputing Internet Project based on CERNET2（IPv6））」。

本演講介紹以純IPv6骨幹的中國教育與研究網路（CERNET2）為基礎的大型超級運算中心間之高速網路互連專案。本計畫由CERNET網路中心和CERNET CORPORATION組成的CERNET HPC6團隊共同負責。該計畫的目的在於將大規模專業超級運算資源、大學超級運算資源和其他相關社會資源部署在CERNET2（純IPv6基礎設施）上，同時保持與IPv4網路的兼容性。這將有助於廣泛連接高效能運算領域的供需雙方，促進不同超級運算中心之間的異質整合。

CERNET2是目前全球規模最大的採用純IPv6技術的下一代網際網路骨幹網路，有41個核心節點，骨幹頻寬為100G（Gbit/s或Gbps），總頻寬大於4.18T（Tbit/s或Tbps），超過1,500萬用戶。

CERNET2的連線單位超過2,000多個，基本上涵蓋了所有大學，他們也是高效能運算的主要使用者。CERNET2參與高效能運算環境下的核心資源網路專案，目標是網路聚合運算處理能力大於2 Eflops[28]，儲存量大於1 EB[29]，並採用IVI[30]轉換技術，支援IPv4到IPv6、IPv6到IPv4、以及IPv6到IPv6之間的傳輸。目前專案中，有4個超級運算中心接取10-100G頻寬到CERNET2網路。

目前專案進度是2個超級運算中心以頻寬10Gbps-100Gbps連接至CERNET2（IPv6）網路並投入運作，其他2個超級運算中心已完成網路接取至CERNET2，其餘超級運算中心的談判正在進行中。

後續工作為，繼續部署超級運算中心互聯、平臺開發，以及平臺測試運行。部署方面的目標是盡快完成6個大型超級運算中心的網路存取，以及41所大學節點全部連接，並進一步測試。平臺開發的初步框架設計已完成，後續將重點放在軟體升級，以

[28] EFLOPS：一個 EFLOPS（exaFLOPS）等於每秒一百京/一百億億（=10^{18}）次的浮點運算。FLOPS（Floating-point operations per second，FLOPS）是指每秒浮點運算次數，亦稱每秒峰值速度，而 E 代表的是一百京，所以 EFLOPS 為每秒一百京次（=10^{18}）浮點運算。

[29] 艾位元組（Exabyte，EB）又稱百京位元組，是資訊計量單位位元組的多倍形式，通常在標示網路硬碟總容量，或具有大容量的儲存媒介時使用。國際單位制（SI）以 10^{18}來定義字首艾，故 1 艾位元組表示 10^{18}位元組。

[30] IVI Translation 是指無狀態 IPv4/IPv6 轉換技術。它允許不同位址（IPv4 和 IPv6）中的主機相互通訊並保持端對端位址透明度。

及支援中英文雙語使用。平臺運行測試方面，在前期互聯部署的基礎上，選擇一些大學用戶參與平臺試運行，以監控資料傳輸並持續優化效能。

第四位講者為印度Surathkal卡納塔克邦國家理工學院（National Institute of Technology Karnataka，NITK）副教授Mohit P. Tahiliani，演講的題目是「由學生和教職員帶領將NITK Surathkal校園網路升級到 IPv6（Migrating NITK Surathkal Campus Network to IPv6: Led by Students and Faculty Members）」。

本演講概述印度蘇拉特卡爾卡納塔克邦國家理工學院的學生和教職員工實施的IPv6部署計畫，以深入了解將NITK校園網路過渡到IPv6系統性的方法，包括從本地網際網路註冊表保護IPv6位址、建立實驗性IPv6測試臺以及將關鍵應用程式服務遷移到IPv6等流程。並介紹在此過程中遇到的挑戰以及相應解決方案。此外，演講中深入探討該專案更廣泛的影響，並強調IPv6部署的重要性以及學生參與推動的努力及其關鍵作用。

目前網路現狀有超過45,000臺終端機接上網，並將在40公里的範圍內擴建校園，網路基礎設施約有超過350臺交換器以及1,200個室內/室外WiFi存取點。NITK Surathkal擁有從IRINN申請取得自己的IPv6位址區塊，2400:4F20::/32，NITK的網路服務供應商是：Bharat Sanchar Nigam Limited（BSNL），為進行支援IPv6，首先請BSNL使用他們的ASN發布我們的IPv6網段，其次請IRINN新增ROA，最後向BSNL提供ROA詳細資訊以宣告IPv6位址區塊。

應用程式遷移到IPv6方面，主要進行的是在NITK中使用最廣泛的綜合資源和資訊共享（Integrated Resource and Information Sharing，IRIS）應用系統，約有7,000多名學生和600多名員工每天使用它。目前IRIS已啟用對IPv6的支援！IRIS上IPv6的總點擊數已達12,584,565，大多數IPv6請求來自行動設備，正在進行的工作是延遲和彈性方面的效能評估和測試（IPv4與IPv6的比較）。後續進行工作包括，測試平臺實驗，將IRIS的所有整合服務移轉到IPv6，以及準備完整的移轉流程文件。

六、 APNIC 路由安全特別興趣小組

（一）議程：APNIC路由安全特別興趣小組（APNIC Routing Security SIG）

（二）時間：2024年2月29日10:30 - 12:00（UTC +08:00）

（三）講者：

1. 主持人：Jocelyn Bateman（Amazon Global Interconnection Strategy）
2. 共同主持人：Di Ma（ZDNS Principal Research Fellow）
3. 專題演講：

(1)Priya Shrinivasan（Cable Labs Director, Technology Policy）

(2)Phil Mawson（Vocus Senior IP Network Engineer）

(3)Terry Sweetser（APNIC Training Delivery Manager for South Asia and Oceania）

(4)Christopher Hawker（Internet Society Network Policy）

（四）會議摘要：

會議一開始，由主持人Jocelyn Bateman開場致詞，歡迎所有與會者出席APNIC路由安全特別興趣小組，並介紹共同主持人Di Ma。

第一位講者為美國CableLabs技術政策總監Priya Shrinivasan，演講的題目是「提高網際網路路由安全的框架（A Framework for Improving Internet Routing Security）」。

本演講介紹CableLabs及其成員、和國家有線與電信通訊協會（National Cable & Telecommunications Association，NCTA）開發了網際網路路由的網路安全框架（Cybersecurity Framework，CSF）輪廓，稱為路由安全輪廓（Routing Security Profile，RSP）。

RSP是有線電視行業專業知識的彙編，與美國國家標準暨技術研究院（National Institute of Standards and Technology，NIST）CSF v1.1 保持一致，為任何組織提供了推動更安全的網路路由的路線圖。

有線電視產業早已認識到網路路由面臨的威脅，並積極尋求在內部和透過產業技術論壇解決這些威脅。下一步是將RSP更廣泛地推廣到網路社群，以提高人們的意識並

進一步推進這項工作。

RSP是一個用於提高網路路由安全性和管理風險的框架，也是關鍵基礎設施中網路安全難題的關鍵部分。它從整體風險管理的角度探討，適用於任何自治系統營運商使用以增強路由安全性。

RSP是參與網路安全風險管理的網路工程師、IT經理、網路安全專業人員和決策者的基本工具，用於評估、實施和管理強大的路由安全策略。它的目標是具有適應性和可擴展性，不僅可以幫助營運商強化自己的網路環境，而且還有助於實現創建更安全、更有彈性的全球網際網路基礎設施的目標。

未來將更廣泛地與網際網路生態系統利害關係人合作，以提高認識並進一步改進和推進所有營運商在這方面的工作，包括ISP、雲端服務提供商、政府機構、大學和其他組織等。此外，將根據利害關係人的回饋，更新RSP第一版，並回應NIST CSF 2.0中的變更。

第二位講者為澳洲Vocus資深IP網路工程師Phil Mawson，演講的題目是「營運商對於RPKI實施、成果和發現的問題（Carrier RPKI Implementation, the results and issues found）」。

為了RPKI實施的設計決策，涵蓋多個層面，包括網路設備來自多供應商(如:Cisco, Juniper, Arista, Nokia），國際傳輸架構（如：澳洲、紐西蘭、美國和亞洲），安全問題，集中管理和監控，以及使用什麼驗證器軟體。驗證器軟體的選擇，包括NLNet Labs Routinator，Fort，OctoRPKI，以及open-rpki。

從時間軸來看，2020年2月最初啟動，2020年4至6月Vocus集團擁有的所有路由均透過APNIC簽署了有效ROA，2020年4至7月我們實驗室針對驗證器軟體進行內部測試，2020年8月AS9443及AS38285開始阻止無效路由，2021年3月16日AS4826開始阻止無效的ROA。

在路由聚合和路由註冊表（Internet Routing Registry，IRR）清理方面，AS9443路由被盡可能地聚合，我們在全球路由表中刪除了大約60% 已發佈的路由。現在，任何Vocus擁有的路由都會有 APNIC登記的WHOIS物件，並從許多第三方資料中刪除，保持單一事實來源。截至2023年底，Vocus已退出所有路由資產資料庫。

第三位講者為APNIC南亞和大洋洲培訓經理Terry Sweetser，演講的題目是「亞太地區RPKI資料成果（RPKI Data Results for APAC）」。

本報告所有數據為2024年2月7日取得，資料來源是由俄勒岡大學RouteViews計畫項目。從APNIC路由來源授權ROA[31]統計資料，可看到已經有大部分地區的ROA比例都很高，至於亞太地區路由來源驗證ROV[32]的比例，臺灣和澳洲的表現比較好，但大部分亞洲地區的比例仍有待加強。

國際標準組織IETF RFC7115[33]（基於資源公鑰基礎設施RPKI的來源驗證操作）加上RFC9319[34]（maxLength在資源公鑰基礎設施RPKI中的使用）成為BCP 185[35]，是RPKI目前最佳實踐，以作為RPKI實作的最佳參考準則，建議對路由進行簽署時，僅限於向全球路由表公佈的內容，不要使用公共資料來源進行奇怪且無意義的實驗。

第四位講者為網際網路協會網路政策Christopher Hawker，演講的題目是「路由驗證和RPKI作為授權書替代方案之研究（Research into Route Validation and RPKI as an alternative to Letters of Authority）」。

授權書（Letter of Authority，LOA[36]）是用於證明知識產權的權利文件，自從網路營運商彼此認識並且存在固有的信任程度以來，該技術至少在過去20年一直被使用。路由來源授權ROA是RPKI下的加密簽章對象，讓網路決定允許哪些AS號碼宣告哪些IP前綴，使用ROA的好處是網路營運商可以使用路由物件驗證和BGP前綴過濾機制來自動執行前綴過濾。

LOA的問題是LOA接受的是依賴基於信任的資訊，非常容易偽造，且需要額外的工作來驗證內容，沒有自動驗證的方法，當授權被撤銷時，還需要透過後續信函手動撤銷。

本演講於2023年11月至2024年1月中旬，調查了代表61個不同網路的個人，這61

[31] 路由來源授權（Route Origination Authorizations，縮寫：ROA），他讓 IP 位址持有者將本身擁有的 IP 位址前綴綁定到特定的自治系統，用以證明 BGP 路由的正確性，避免被有心人士偽造路由資訊，而發生 BGP 路由劫持情況。
[32] 路由來源驗證（Route Origin Validation，ROV）是一種依賴資源公鑰基礎設施 RPKI 的安全機制，可讓您驗證 BGP 公告的真實性和準確性。
[33] RFC7115: Origin Validation Operation Based on the Resource Public Key Infrastructure （RPKI），基於資源公鑰基礎設施 RPKI 的來源驗證操作，https://datatracker.ietf.org/doc/html/rfc7115。
[34] RFC9319: The Use of maxLength in the Resource Public Key Infrastructure （RPKI），maxLength 在資源公鑰基礎設施 RPKI 中的使用，https://datatracker.ietf.org/doc/html/rfc9319。
[35] BCP 185: 第 185 號 RPKI 目前最佳實踐（Best Current Practices，BCP），https://datatracker.ietf.org/doc/bcp185/。
[36] 授權書（Letter of Authority，LOA）是用於在三方或多方之間達成協議的文件。它本質上是您向經紀人提供的特殊許可單，允許他們在商定的範圍內代表您與其他企業交談。

個網路共使用了51個不同的上游供應商。其提供LOA的原因，有28位受訪者提供了LOA來確認所有權/授權，10位表示是為了驗證下游資源，8位表示是要遵守監理要求和業界標準，5位是出於其他原因。

對於所需的LOA格式，24個上游要求以PDF格式的官方信箋提供LOA，並以電子郵件附件的形式發送給他們。6個需要來自公司電子郵件信箱的電子郵件。1個接受資源擁有者所發送儲存為PDF的電子郵件，作為允許公佈其資源的授權。

對於LOA資料內容的安全性，網路營運商是否放心，LOA中包含的資訊僅被用於預期目的，證明前綴公告的授權。30位表示非常放心，5位有點放心，6位感到中等，7位一點也不放心。

其使用LOA的一些擔憂包括：無論是否提供LOA；ISP仍要求採用替代授權方法；LOA可以相對容易且快速地偽造；由於下游不提供LOA，網路無法向上游提供其下游對等點通告的前綴；以及將授權路由新增至路由過濾器以及隨後取消前綴會造成延遲。

ROA可以取代LOA嗎？29位受訪者表示可以，3人說不能，10位相信他們可以若通過額外的驗證步驟，以及6人不確定。

ROA可以用於法律驗證嗎？25位同意ROA可用於合法驗證，以確認給定的來源AS，3位不相信他們可以，10位同意他們可以採取額外的驗證方法，6位不確定他們是否可以，17位沒有回答。

依據IETF RFC9255[37]，RPKI中的「I」並不代表身份，ROAs不得用於驗證真實世界的文件或交易。ROA的目的是驗證INR的來源AS。使用ROA並不是為了驗證實體。實體驗證是此過程的外部。

此外，從傳輸提供者租賃IP空間的新進網路將無法為這些前綴創建ROA，因為它們不是RIR成員且無法存取RIR的RPKI基礎設施。另外也可能需要自治系統提供者授權（Autonomous System Provider Authorization，ASPA）才能完全取代LOA。如果給定的前綴存在ROA，則表示經過驗證的資源持有者已同意指定ASN使用該前綴。整體而言，這仍將減少錯誤、路由劫持和實施時間。

[37] RFC9255: The 'I' in RPKI Does Not Stand for Identity，RPKI 中的「I」並不代表身份，https://datatracker.ietf.org/doc/html/rfc9255。

七、 公開政策會議 場次1

（一）議程：公共政策會議 場次 1 （Open Policy Meeting 1）

（二）時間：2024 年 2 月 29 日 12:30 - 14:30 （UTC +08:00）

（三）講者：

1. 主持人：Bertrand Cherrier（Micro Logic Systems）
2. 共同主持人：
   (1)Shaila Sharmin（Prime Bank Limited Cyber Security Architect, Information Security）
   (2)Anupam Agrawal（Tata Consultancy Services Limited Lead Corporate Industry Forums and Standards Cell）
3. 專題演講：Geoff Huston（APNIC Chief Scientist）

（四）會議摘要：

本議程為公開政策會議，由APNIC政策特別興趣小組（Policy SIG）主持，討論社群成員向Policy SIG提出的政策提案。提案人說明提案內容後，會在SIG主席主持下現場舉手投票，同時利用Zoom內的投票功能線上投票；投票結果會直接公布，主席和副主席綜合評估投票結果及Policy SIG mailing List中的相關討論後，會決定該提案是否獲得共識支持。若是，則提案將交由APNIC秘書處負責後續執行；若否，則不成案，但可將提案帶回mailing list討論，於下次APNIC會議再次提出修正版本，再次投票。

場次正式開始前，APNIC營運資深主任Tony Smith報告政策提案（prop-155）的最新進度。

Prop-155建議協同會員[38]（Associate Member）即使未曾獲發配IPv4位址資源，也可單獨申請取得IPv6資源。本提案於APNIC 56京都會議經公開政策會議及會員大會表決通過，並於2023年11月由APNIC執行委員會（EC）決議通過。EC決議通過公告中，原本敘明協同會員或發配/48的「無供應商」（Provider independent，PI）[39]IPv6資

[38] 協同會員 （Associate Member），指有會員資格但未持有號碼資源的會員。
[39] 無供應商（Provider independent，PI），指直接由 RIR 發派予個人或組織的 IP 位址。獲發派 PI 位址的使用者必須自行透過網路服務供應商（Internet Service Provider，ISP）與本地網際網路註冊管理機構（local Internet registry，LIR）簽約，以取得此 PI 位址區段在網際網路中的路由。

源後12個月內可豁免註冊費用，12個月後才需開始繳費。

然而，自公告後，EC收到大量來自社群的反對意見。積極考量社群意見後，EC決定改變原先決策，取消「12月後收費」規定，將/48的PI IPv6位址列入「不收費」資源管理。

接續由APNIC首席科學家Geoff Huston說明2023年IP位址發展趨勢(What happened with Addresses in 2023)，詳細內容請參考完整簡報：https://2024.apricot.net/assets/files/APIC378/2024-02-29-addresses_1708997237.pdf。

本場次討論的政策提案如下：

(1) prop-156: Assignment of Temporary IP Resources

提案人：

- Christopher Hawker

提案內容：

保留/21 的 IPv4 前綴、/29 的 IPv6 前綴和 8 筆自治系統號碼（Autonomous System number，ASN），以便未來必要情境（如會議網路需求）作為臨時發放位址使用。

討論：

現場無特別討論。

表決結果：

共識通過。

(2) prop-158: IPv6 auto-allocation for each IPv4 request

提案人：

- David Aditya Yoga Pratama
- M. Andri Setiawan

提案內容：針對每筆 IPv4 資源請求，在發放時自動附贈發放同等 IPv6 位

址，以加速 IPv6 使用率。

討論：

現場許多強烈反對意見，理由包括買 IPv4 送 Ipv6 只是製造 IPv6 發配數量增加的假象，強制贈送將導致或發配方的額外支出，必須負擔這些不需要的 IPv6 位址的註冊費用，對中小規模的企業或組織無疑平添財務負荷。

另有來自 RIPE NCC 的現場與會者分享，過去 RIPE NCC 也曾通過類似政策，實行效果不佳，會員多抱怨此政策不必要地將位址發配過程複雜化，最後 RIPE 社群在 2015 年共識同意撤銷該政策。

表決結果：

反對多於同意，政策未通過。退回予提案人決定是否修改後重遞，或撤銷提案。

八、 公開政策會議 場次2

（一）議程：公共政策會議 場次 2 （Open Policy Meeting 2）

（二）時間：2024 年 2 月 29 日 15:30 - 17:00 （UTC +08:00）

（三）講者：

1. 主持人：Bertrand Cherrier（Micro Logic Systems）
2. 共同主持人：
   (1)Anupam Agrawal（Tata Consultancy Services Limited Lead Corporate Industry Forums and Standards Cell）
   (2)Shaila Sharmin（Prime Bank Limited）
3. 專題演講：Geoff Huston（APNIC Chief Scientist）

（四）會議摘要：

首先由Geoff Huston針對「當代網際網路中位址的角色(The Role of Addresses in Today's Internet)」發表簡短演講。

Huston指出，IPv6的出現是為了實現當初理想中的網路，確保所有連網裝置都享有專屬IP位址，不需要利用網路位址轉換（Network Address Translation，NAT）等技術轉譯或共享位址。但現在我們應該面對現實，這樣的理想已不切實際，「每個裝置都擁有專屬位址」已不再是IPv6的賣點，無法以此說服或吸引業者轉換至IPv6。

觀察當代網路運作生態，一個雲端平臺大致僅需要一筆IP位址，連伺服器都不需要專用位址。過去IP位址有3種功能：識別（辨別終端裝置的身分）、定位（確定裝置在網路中的位置），以及聯絡方式（決定將封包傳送至該裝置的路線）。但如今位址只剩下定位及聯絡方式2種功能，識別身分的功能已完全轉嫁至域名上。

換句話說，當代網路並非以位址為基礎，而是以域名為基礎。位址已失去「識別碼」的功能，這在網路發展上是根本架構的一大變革。

有鑑於此，Huston認為我們應開始思考：在這個識別功能已從位址轉至域名的網路架構中，IPv6的價值為何？如果連網裝置不再需要永久專屬的IP位址，我們究竟需要多少筆IP位址？IP位址還能算是稀缺資源嗎？

簡短演講結束後，接續討論政策提案。

(1) prop-157: Temporary IPv4 Transfers

提案人：

- Jordi Palet Martinez

提案內容：

目前政策僅容許永久 IPv4 位址移轉。建議修改政策以容許 IPv4 位址臨時移轉。

討論：

提案中建議臨時移轉 IPv4 位址的接收人必須符合「具運作中 IPv6 位址」的條件，此但書遭許多現場與會者強烈反彈，表示許多小型公司僅有 IPv4 資源，仍會遇到急需臨時接收 IPv4 位址移轉的緊急狀況。若因此條件限制而無法接收臨時移轉位址，對成本資源較低的小型單位不公平。

另亦有反對意見認為提案中提出的解決方案，在當今政策下本可實現。此意見認為提案仍缺乏具體細節，難以看出修訂政策後能達到什麼實質改善。

表決結果：

反對多於同意，政策未通過。退回予提案人決定是否修改後重遞，或撤銷提案。

(2) prop-154: Resizing of IPv4 assignment for the IXPs

提案人：

- Simon Sohel Baroi
- Aftab Siddiqui

提案內容：

本提案建議發配給網路交換中心（Internet Exchange Point，IXP）的 IPv4 位址空間從預設/23 縮小至預設/26，但若 IXP 歸還過去獲發配的位址，則能獲發配/22 的位址空間。

討論：

本提案為 APNIC 56 未達成共識退回後修正重遞。提案初版建議「若 IXP 提出合理事由，可獲發配/22 位址空間」，此但書遭社群反對，因此本修正提案中刪除相關文字。

RIPE NCC 約 5 個月前開始實行類似政策，RIPE NCC 註冊服務副理 Marco Schmidt 分享經驗，表示自政策上路開始至今已發配予 10 家 IXP /26 的 IPv4 位址。他認為雖時間尚短，難以斷定此政策實質功效，但就目前來看算是成功。

表決結果：

共識通過。

九、 APNIC 年度大會 場次1

（一）議程：APNIC 年度大會 場次 1 （APNIC Annual General Meeting 1）

（二）時間：2024 年 3 月 1 日 10:30 - 12:00 （UTC +08:00）

（三）講者：

1. 主持人：Kenny Huang（APNIC Executive Council）
2. 專題演講

(1)Jeremy Harrison（APNIC General Counsel）

(2)Kanchana Kanchanasut（intERLab/AIT）

(3)Paul Wilson（APNIC Director General）

(4)Yoshinobu Matsuzaki（APNIC EC Treasurer）

（四）會議摘要：

本場次為APNIC年度大會，分成3場舉行。第一場由秘書處報告APNIC 2023年活動、EC財務主管進行財務報告；第二場由APNIC執行長報告2024年計畫、EC主席報告，合作及國家網際網路註冊機構（National Internet Registry，NIR）SIG主席續簡報會議期間討論精華；其餘SIG則於第三場分享，並由選委會主席公告選舉結果。

EC主席黃勝雄博士開場致詞並簡介本場次內容後，由APNIC法務長Jeremy Harrison介紹本屆選舉流程，選委會主席Kanchana Kanchanasut介紹本屆EC候選人。

APNIC執行長Paul Wilson簡報2023年APNIC活動。2023年APNIC活動報告已公告，報告全文可參考：https://blog.apnic.net/2024/02/26/2023-annual-report-now-available/。報告中總覽APNIC在2023年的表現，並根據2023年APNIC執行計畫暨預算比對秘書處於2022年的實際工作成果。報告中亦涵蓋APNIC的財務表現。

EC財務主管Yoshinobu Matsuzaki接續進行財務報告，詳情請參考簡報：https://2024.apricot.net/assets/files/APIC378/february2024treasure_1709260740.pdf。

最後開放問答時間，供秘書處與EC聆取社群意見。

許多針對APNIC的財務和稽核問題，包括海外稅務處理、APNIC基金會收支和資金

運用，以及匯差導致會員費用金額差異的處理方式等。現場會員詢問APNIC歷史資源回收計畫進度，APNIC註冊管理服務資深主任Karla Skarda說明，目前此計畫已正式結束，目前正陸續清點並重新分配回收資源的路由。

由於APNIC年度大會是免費參與，但與其合辦的APRICOT必須付費報名。由於公開政策會議與APRICOT最後一天（2月29日）重疊，部分29日抵達的會員因此無法參與公開政策會議。現場會員因此建議，應開放未報名APRICOT的會員參加公開政策會議。

十、 APNIC 年度大會 場次2

（一）議程：APNIC 年度大會 場次 2 （APNIC Annual General Meeting 2）

（二）時間：2024 年 3 月 1 日 12:30 - 14:00 （UTC +08:00）

（三）講者：

1. 主持人：Kenny Huang（APNIC Executive Council）
2. 專題演講

(1)Paul Wilson（APNIC Director General）

(2)Kenny Huang（APNIC Executive Council）

(3)Joy Chan（TWNIC Cooperation SIG Chair）

(4)Oanh Nguyen（VNNICNIR SIG Chair）

(5)Srinivas Chendi（APNIC Senior Advisor, Membership and Policy）

（四）會議摘要：

APNIC執行長Paul Wilson報告2024年APNIC執行計畫。APNIC主要透過問卷調查募集社群意見以制定執行計畫，並定期向會員會報計畫執行狀況。除每年執行計畫外，APNIC亦以每四年為單位規劃長期戰略計畫，2024年是新四年戰略計畫的第一年。

2024 年 執 行 計 畫 暨 預 算 完 整 內 容 可 點 選 以 下 連 結 參 考 ：https://www.apnic.net/wp-content/uploads/2024/02/APNIC_AP_2024.pdf。

EC主席報告EC相關活動。依慣例，EC每年召開4次實體會議。自上屆年度大會（APNIC55）以來，已召開7場EC會議，下一次將於6月3、4日在馬來西亞吉隆坡舉行。APNIC EC去年11月在羅馬與RIPE NCC董事會舉行聯合會議，今年2月26日於曼谷與APNIC基金會董事會舉行聯合會議。EC會議記錄可前往https://www.apnic.net/about-apnic/organization/structure/apnic-executive-council/ec-minutes/ 查看。

APNIC每兩年執行一次社群滿意度調查，邀請外部獨立單位進行匿名調查。2024年度調查已經展開，利用APRICOT期間進行焦點訪談，並將於6月開放線上問卷調查，歡迎社群踴躍填答。

財務方面，2023年會員數量成長超乎預期，至2023年12月31日止，APNIC會員共

達9,944名，來自53個國家。2023年營運赤字為59萬澳幣，預算赤字為110萬澳幣。

過去APNIC選舉僅指派一名選委會主席。自2023年9月APNIC 56京都會議通過新組織章程後，今年EC成立由5名委員組成的選舉委員會，負責檢視EC候選人資格並監督選舉過程。

Cooperation SIG主席、台灣網路資訊中心副執行長丁綺萍報告本屆會議討論重點。Cooperation SIG作為平臺，供社群討論關乎APNIC利益但範疇較廣，同時涉及其他如政府、其他組織或社群等多方利害關係團體的公共政策或網路治理議題。透過合作SIG的討論，社群成員也可就公共政策議題，研議並確立APNIC社群的正式立場。

APNIC 57的Cooperation SIG場次探討人才培育的重要，邀請產官學界人才與談，分享人才培育經驗，強調發掘、培養並支援專業人才成長，以確保亞太地區網際網路永續發展的重要。

國家網際網路註冊機構（National Internet Registry，NIR）SIG主席報告本屆討論重點。本屆NIR SIG場次邀請到包括CNNIC（中國）、IDNIC（印尼）、VNNIC（越南）、JPNIC（日本）、TWNIC（臺灣）、KISA/KRNIC（韓國）和IRINN（印度）分享各國現況，大部分報告著重於該國的IPv6部署情形、RPKI教育訓練工作。各NIR在分享中也不約而同提到希望獲得更多來自APNIC的支援，尤其希望APNIC在可能影響NIR的新政策推廣和教育上更積極用心。

十一、 APNIC 年度大會 場次3

（一）議程：APNIC 年度大會 場次 3 （APNIC Annual General Meeting 3）

（二）時間：2024 年 3 月 1 日 15:30 - 17:00 （UTC +08:00）

（三）講者：

1. 主持人：Kenny Huang（APNIC Executive Council）
2. 專題演講：

(1)Srinivas Chendi（APNIC Senior Advisor, Membership and Policy）

(2)Bertrand Cherrier（Micro Logic Systems）

(3)Di Ma（ZDNS Principal Research Fellow）

(4)Richard Brown（APIDT Chief Financial Officer）

(5)Katsuyasu Toyama（APIX Chair）

(6)Jon Brewer（Telco2 Limited Consulting Engineer）

(7)Kanchana Kanchanasut（intERLab/AIT）

(8)Paul Wilson（APNIC Director General）

（四）會議摘要：

Policy SIG主席Bertrand Cherrier報告本屆於政策會議討論的政策提案（詳情請參考本報告Policy SIG場次會議紀錄），並再次就政策會議中通過共識決的提案付諸全體會員共識決。提案154及156皆通過共識決，下一步將於Policy SIG mailing list徵求最後一輪社群意見。

路由安全SIG共同主席Di Ma簡報本屆討論重點，APNIC 57場次共邀請4位講者，分享議題包括：透過標準化特定技術與實踐並制定社群守則以強化網路路由安全；方格子（Vocus）的RPKI部署經驗分享；亞太地區的RPKI部署成長趨勢及路由來源驗證（Route Origin Validation，ROV）情形；授權書（Letters of Authority，LOA）及ROA是否可取代LOA。

亞太網際網路發展信託（Asia Pacific Internet Development Trust，APIDT）乃日本WIDE計畫與APNIC共同成立，為資助亞太地區的網際網路發展專案，諸如技術技能發展與能力建構、改善關鍵網際網路基礎建設及研究與發展支援等，以期協助社群

建立開放、穩定及安全的全球網際網路。APIDT財務長針對APIDT的投資情形、地產及財務活動提出簡報。詳細內容請參考：https://2024.apricot.net/assets/files/APIC378/apidtpresentationapn_1709259825.pdf。

亞太網路交換協會（Asia Pacific Internet Exchange Association, APIX）每年都會在APRICOT期間舉辦會員大會。APIX主席Katsuyasu Toyama分享本屆會議重點，APIX會員數成長至42名，共來自包括臺灣、澳洲、泰國、柬埔寨等20個國家。本次新增的會員之一來自婆羅洲，進一步豐富APIX會員的地理多元性。我國福爾摩沙開放網際網路交換中心（Formosa Open Exchange，FOX）也是新進會員之一。

APNIC 58將於2024年8月30日至9月6日在紐西蘭威靈頓舉行，主辦國.nz註冊管理機構InternetNZ介紹會議地點，歡迎大家今年9月造訪紐西蘭。

最後由選委會主席Kanchana Kanchanasut宣布本屆EC選舉結果。Kam Sze Yeung、Sumon Ahmed Sabir、Vincent Atienza 連任當選成為EC成員，將展開2年任期。

參、 心得與建議

根據本次所參與的會議，提出以下心得觀察與建議事項：

一、網路合作特別興趣小組探討「網際網路發展技術能力建構」主題，邀請學界、政府代表及網路技術社群組織分享發展網路技術能力的經驗，希望促進利害關係人的協作，並對於未來的網路技術能力的要求提出建議。與會各界代表分享了不同的發展經驗，從由下而上的私部門、學界合作推廣與人才培育，到公部門政策制定補助推動等方式，其中泰國與澳洲通訊傳播部門的代表分享以政府主導模式建構網路能力，包含舉辦網路技術發展教育訓練、座談會交流論壇、專家學者人才培育、公私部門協力資訊通訊技術(ICT)及網際網路服務提供者(ISP)之網路技術發展等。網路人才培育需要長期間的人力及經費的投入，且具有外部公共效益，由政府主導投入資源較能達到網路技術建設之成效，可做為未來政策制定的參考。

二、國家網際網路註冊機構(NIR)特別興趣小組及 IPv6 佈署等主題，分享亞太地區等國家 2023 年 IP 註冊業務情形、人才培育社群交流活動及 2024 年規劃人才培育社群交流計畫。討論包含 IPv4 註冊使用量、推動 IPv6 佈署使用率、資源公鑰基礎建設（RPKI）與路由來源授權（ROA）的簽署率等議題。在 IPv4 數量方面，各國普遍即將使用耗盡，但於 IPv6 的佈署發展則存在明顯差異。例如中國 IPv6 的佈署率有 70%，印度亦高達的 80%，皆為 IPv6 佈署程度相當高的國家，究其主因，應為印度在 IPv6 早期發展階段即已全面推動佈署，而中國則是透過由政府主導以推動公私部門的佈署，藉此方式，使中國在行動網路、固定通信網路、網路平臺、APP 等方面的平均佈署率均相當高。而未以政府主導佈署 IPv6 之國家，其佈署率則普遍較低。臺灣在 IPv6 佈署率將近 60%，全球排名第 12 位，相對名列前茅，但要如何進一步提高佈署率達到普及，牽涉網路業者佈署成本與使用者需求等問題，參考他國經驗，由政策主導亦是提高 IPv6 採用率的選項之一。

三、每次的公開政策會議之政策提案討論及年度大會 APNIC 執行委員會(EC)的選舉，一直是 APNIC 社群成員重視且積極參與的事項，本次政策提案共有 4 案，其中 2 案共識決通過提案，另 2 案未成案，社群成員可在會議現場舉手表決，同時也能在線上進行表決，表決結果並立即在現場公布。另本次 EC 選舉將選出 3 名成員，候選人共有 5 位，投票為期兩週至活動結束當日，選舉資訊均已事先公布於網路上，經由社群成員進行線上投票，順利選出 3 名 EC 成員。兩項活動充分體現網路治理的民主與效率。關心 APNIC 的網路治理的社

群成員，只要完成 MY APNIC 註冊，不論有無親臨現場參加會議，皆都可參與表決與投票，充分展現 APNIC 積極推動網路社群多方利害關係人的共同參與，並體現網際網路無遠弗屆的通訊及作業效率。

四、QUIC 是新的 TCP，是傳輸服務的邏輯演進，其傳輸速率更快，並可將一切加密，而且 QUIC 具有應用層能力，QUIC 可以透過 UDP API 與平臺溝通，因此 QUIC 的所有內容都可以在應用程式內實現。這使應用程式能夠更好地控制其服務結果並減少外部依賴，建議可持續關注 QUIC 的發展。

五、預期未來新的網路空間，垂直整合服務提供者退出歷史舞臺，傳輸不再是不可避免的壟斷；對平臺的控制也不再是對使用者的控制，作業系統被推回其基本的排程角色任務，也被吸收到應用程式空間中，建議持續關注網路應用層的發展。

六、監控邊界閘道器協定（Border Gateway Protocol，BGP）和資源公鑰基礎設施（Resource Public Key Infrastructure，RPKI）的正確性是提高全球網路穩定性的關鍵操作，包括監控劫持、可見性遺失、洩漏、無效 RPKI 公告以及錯誤 RPKI 配置等，建議可多利用易於使用的工具來監控。

七、路由洩漏的防範隨著國際第一級網路服務提供商同意過濾掉未經授權的 RPKI，取得了巨大進展，希望大部分流量都是由有效的 RPKI 路由所引導，而當 RPKI 無效時，路由傳播應要減半。至於誤導通訊的路由劫持，需要邊界閘道協定安全性（Border Gateway Protocol Security，BGPsec）來消除 AS 的冒充，以保護透過 BGPsec 感知的連續 AS 延展，而且部分部署也仍然會有好處，期待以此來消除 AS 來源冒充，建議持續關注 BGPsec 的發展。

八、2024 年的 IPv6 部署進展似乎會遵循一般網路設備的生命週期。此外，IPv4/IPv6 雙協定不意味著終點。網路從 IPv4 過渡到 IPv4/IPv6 雙協定的整個目標並不是要看到普遍存在的 IPv4/IPv6 雙協定環境，一旦達到雙協定部署的「群聚效應」，就可以放棄支援 IPv4，我們可能需要一段時間才能達到這種「群聚效應」部署場景，但一旦達到這個臨界值，那麼下一步放棄支援 IPv4 的速度可能會快得多，建議持續關注全球 IPv6 部署的進展。

九、從 APNIC ROA 統計資料，可看到大部分地區的路由來源授權 ROA 比例都很高，至於亞太地區路由來源驗證 ROV 的比例，臺灣和澳洲的表現較好，但大部分亞洲地區的比例仍有待加強，IETF 已有提出 RPKI 實作的最佳參考準則，建議持續關注全球 RPKI ROV 的進展。