出國報告 （出國類別：開會）

出席亞太網路資訊中心第 58 次（APNIC 58）會議報告書

Asia-Pacific Network Information Centre 58 Conference

服務機關	姓名 / 職稱
數位發展部	牛信仁 司長、吳宜倫 副處長、周湧裕 科長、吳瑄俞 專員
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：紐西蘭 威靈頓

出國期間：113 年 8 月 30 日至 9 月 6 日

報告日期：113 年 11 月 20 日

摘 要

亞太網路資訊中心（Asia Pacific Network Information Centre，APNIC）第 58 次會議於本（2024）年 8 月 30 日至 9 月 6 日以結合線上參與及實體會議的混合模式於紐西蘭威靈頓舉行，前 4 日 8 月 30 日至 9 月 2 日為 APNIC 工作坊（詳情請參閱附錄）。此為本年度第 2 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 4 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，前往紐西蘭威靈頓參加 APNIC 58（Asia-Pacific Network Information Centre 58 Conference）會議，並在會議中蒐集有關網路安全、亞太及國際 IP 政策進展、技術等最新發展訊息。

本次實際參與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，除開幕典禮暨專題演講（APNIC Opening Ceremony and Keynotes）外，還包括技術會議（Technical Session）、IPv6 布建（IPv6 Deployment）、座談（Panel Discussion）、國家級網路位址註管機構特別興趣小組會議（NIR SIG Session）、APNIC 會員大會（APNIC Member 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 58（Asia-Pacific Network Information Centre 58 Conference）會議於本年8月30日至9月6日於紐西蘭威靈頓舉行，前4日8月30日至9月2日為APNIC工作坊（詳情請參閱附錄）。此為本年度第2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 58會議所有場次議程，詳參APNIC58網站資訊。會議匯集了來自世界各地網際網路專家、政府代表、產業領袖和其他有興趣的各方，共同學習、分享想法和經驗、與同行建立聯繫並製定與網際網路運營相關的政策。

[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4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，前往紐西蘭威靈頓參加APNIC 58會議，在會議中蒐集有關網路安全、亞太及國際IP政策進展、技術等最新發展訊息。

（二）過程：

1. 會議時間：本年8月30日-9月6日
2. 參與場次：表1為參與APNIC 58會議之場次（APNIC 58 會議完整議程表，請詳參活動網站。）

表1. APNIC 58會議參與場次

日期	場次名稱
8/30-9/2	Network Security 網路安全
	Network Automation 網路自動化
9/4	Opening Ceremony and Keynotes 開幕典禮暨專題演講
	Technical Session 1 技術會議 場次1
	Technical Session 2 技術會議 場次2
9/5	IPv6 Deployment IPv6 布建
	Panel Discussion

日期	場次名稱
	大會座談
	NIR SIG Session 國家級網路位址註管機構特別興趣小組會議
	Technical Session 3 技術會議 場次3
9/6	Open Policy Meeting - Policy SIG 1 公開政策會議　場次1
	Open Policy Meeting - Policy SIG 2 公開政策會議　場次2
	APNIC Member Meeting 1 APNIC會員大會 場次1
	APNIC Member Meeting 2 APNIC會員大會 場次2

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（APNIC Opening Ceremony and Keynotes）

（二）時間：本年 9 月 4 日 11:30 - 13:00（UCT +12:00）

（三）講者：

1. Opening remarks：Kenny Huang（APNIC EC Chair）
2. Introductory remarks：Jia Rong Low（APNIC Incoming Director General）
3. Welcome remarks：
   (1)Vivien Maidaborn（InternetNZ Chief Executive）
   (2)Sarai Faleupolu Tevita（PacIGF 2024 Organiser）
4. Keynotes：
   (1)Robyn Kāmira（Paua Interface Ltd Managing Director）
   (2)Jonathan Brewer（Telco2 Limited Consulting Engineer）

（四）會議摘要：

場次開始，APNIC執行委員會（Executive Committee，EC）主席Kenny Huang（黃勝雄）、即將於10月上任的新APNIC執行長Jia Rong Low及當地主辦單位InternetNZ執行長Vivien Maidaborn發表開幕致詞。接續開幕專題演講分別請到兩位講者：首先由女性毛利科技創業家Robyn Kāmira分享在紐西蘭邊陲地帶架設電信網路的經驗，接續由目前定居威靈頓的資深網路工程師Jonathan Brewer分享長年來在紐西蘭偏鄉架設寬頻網路的經驗。

1. 前線的電子通訊：真正重要的東西（Telecommunications stories from the frontline: What matters.）

Robyn Kamira一直把支持毛利人利用科技來改善生活當作她的職

業目標。在開始之前，她強調今天介紹的專案都是紐西蘭在地，為紐西蘭毛利族群服務而生。希望透過分享專案內容，讓聽眾更了解當地偏鄉的困境，以及科技能帶來的益處。

第一個專案是2014年開始、以改善偏鄉地區連網普及度的「Mitimiti on the Grid」。Mitimiti因為地理位置偏遠且臨海，始終面臨諸如淹水、停電頻仍、人口外流等重重挑戰，其中更因電信基礎建設老舊，仍使用銅線電纜、通訊塔僅於退潮時運作等因素，網路品質不穩且速度極慢，當地民眾甚至無法使用都市人口熟悉的線上購物或電子銀行等服務。

研究顯示，網路「光纖化」能帶來具體、顯著且長期的改善：當地工作機會、商業活絡程度及產能都會大幅提升，且能帶動地區整體且持續的經濟成長。「Mitimiti on the Grid」也證實相關研究，網路基礎建設全面升級後，當地網路使用人口穩定成長，帶動經濟活絡，更因此能舉辦吸引觀光人口的大型活動。

其餘兩個專案「TuÊAtea」與「Cybersecurity 99」都以培養毛利技術人才為重心。雖然毛利佔紐西蘭整體人口兩成，但在科技產業的代表性卻極度不足。TuÊAtea透過如「未來毛利領袖」（Future Maori Leaders）等在地計畫，培養並支援毛利年輕人進入科技產業，並逐步爬升至領導地位。

「Cybersecurity 99」則聚焦於改善中小企業及非營利團體的網路安全。此類組織往往因資金不足，無法建置完備的網路安全框架。此專案有三大主軸，「可負擔」聯合中小企業，為他們爭取較低廉的網路安全團體價；「網路安全落差分析」則幫對方找到安全弱點，且不強迫銷售昂貴的因應方案；「羽翼之下」刻意招募並將服務不足地區的人才納入網路安全專案，養成實務操作經驗並提供工作機會。

最後，Kamira再次重申社群參與和支持，在解決網路連線、人才培

育及網路安全等挑戰中的重要。

2. 紐西蘭偏鄉的寬頻建設（Delivering Broadband to Rural Aotearoa）

Brewer首先強調紐西蘭城鄉差距極大，雖然有少數人口集中、高度都市化的城市，但有更多國土面積是地廣人稀。紐西蘭的電信基礎建設產業結構也反映此特殊的人口分布，與由少數主要業者壟斷市場的大多數其他國家不同，紐西蘭有無數中小型網路公司。

紐西蘭的網路服務供應業者（Internet Service Provider，ISP）包括3家主要行動通訊業者、11家光纖中盤商、8家基礎建設公司、94家零售ISP、55家無線ISP，以及7家同時提供無線及光纖服務的ISP。Brewer認為，紐西蘭ISP如此多元且眾多，乃由於以下關鍵歷史事件及管制政策變動：

(1) 1989年電信市場管制放鬆，ISP開業無需證照，促使網路服務興起。

(2) 2001年海底纜線的出現，改善過去僅能仰賴衛星網路的跨國連線。同年紐西蘭開放一般使用者申請頻譜，進一步鼓勵大量小型ISP進入市場。

(3) 2008年紐西蘭修法，在公有領地建設電信基礎建設的申請流程全國統一，無需再向地方政府另行申請。

(4) 2011年政府強制命令紐西蘭電信將基礎建設和零售實體分家，禁止實體建設供應業者直接提供終端服務，藉此鼓勵零售ISP競爭。

(5) 2012年紐西蘭政府推出針對光纖基礎建設，以及偏鄉地區寬頻網路建置等低額借貸鼓勵政策，完善紐國境內網路基礎建設。

Brewer列舉多項實例說明以上關鍵政策的實際影響，包括許多他實際參與的專案，如利用光纖及無線網路於偏鄉提供網路服務的Maori Net和Kiwi WiFi。

總結而言，紐西蘭之所以成功打造穩健、高競爭力的電信市場，主要歸功於早期開放管制、先進的頻譜政策、友善的基礎建設標準、政府介入防止壟斷，以及針對光纖及偏鄉連網建設的國家投資。多虧以上因素，紐西蘭境內雖然人口分佈極度不均，但即使在人口稀缺之偏鄉，也能達到一定程度的網路連線。

二、 技術會議 場次1

（一）議程：技術會議 場次1（Technical Session 1）

（二）時間：本年9月4日14:30 - 16:00（UTC +12:00）

（三）講者：

1. Moderator：Shane Hermoso（APNIC Training Delivery Manager）
2. Speakers：
   (1)Geoff Huston（APNIC Chief Scientist）
   (2)Michael Tadault（Red Hat Chief Technologist Telco）
   (3)Ulrich Speidel（University of Auckland Senior Lecturer）

（四）會議摘要：

會議由主持人Shane Hermoso開場致詞，歡迎所有與會者出席第一場次技術會議。

第一位講者為APNIC首席科學家Geoff Huston，演講的題目是「基礎設施安全是市場失靈嗎?（Is Infrastructure Security a Market Failure?）」。

為什麼域名系統安全擴充（Domain Name System Security

Extensions，DNSSEC）會花了三十年的時間仍在進行中？大家都知道，一個經過認證的名稱系統是多麼重要，理應應用普及，但實際情況並非如此。同樣地，為什麼路由安全工作只在部分地方得到採用，而完全的路由驗證卻沒有被採納？本次演講著眼於探討基礎設施安全所採用的指標，並指出一些經濟原因，解釋為什麼這會這麼困難。該演講也提出未來可能解決這些結構性障礙的工作。

演講者討論了基礎設施安全所面臨的實際挑戰，特別是在市場上推廣的困難。儘管有許多安全技術可用，比如DNSSEC和邊界閘道器協定（Border Gateway Protocol，BGP）的安全增強措施，但因為實施成本高、管理麻煩，很多企業並沒有廣泛採用這些技術。這種情況被稱為「市場失靈」，主要是因為缺乏經濟誘因，許多企業在看不到明確的成本效益的情況下，選擇忽視這些安全措施。

演講中介紹DNSSEC與BGP安全的挑戰，DNSSEC能有效防範域名系統（Domain Name System，DNS）欺詐，但其複雜的部署過程使得很多企業不願投資，尤其是中小企業。此外，DNSSEC的管理和維護也需要專業人員的投入。BGP安全性增強技術同樣面臨採用困難，雖然它能防止路由攻擊，但其技術實施要求的營運商協作程度較高，這在現實中難以推動。

最後強調政策建議與協作的重要性，Geoff認為，政府應該加強對基礎設施安全的政策支持，透過激勵機制以促使企業更多地投入到安全技術的採用和實施中。他還強調了產業協會和政府應攜手合作，提供資金或減免政策以支持企業進行網路安全投資，最終才能提升全球網際網路的整體安全性。

第二位講者為Red Hat電信技術專家Michael Tadault，演講的題目

是「從虛擬網路功能到雲端原生網路功能（VNF[2] to CNF[3]）」。

電信服務供應商面臨嚴峻的挑戰，包括：收入成長緩慢，有時甚至停滯，而對網路（例如 5G）的投資需求卻沒有減弱。為了應對這項挑戰，他們開始了一段旅程，透過最終採用一些在IT領域非常成功的雲端原生技術，使他們的網路更加自動化、更加靈活，例如：雲端運算首先以虛擬機器的形式出現，現在以容器的形式出現。雖然這技術始於網路核心，但現在正擴展到包括無線電存取網路（Radio Access Network，RAN）[4]在內的邊緣網路。本演講討論影響電信網路的一些根本性變化，以及在此過程中如何使用雲端原生技術和自動化。

雲端原生網路的功能，是利用容器（container）技術實現網路功能的運行，具有更高的靈活性、可擴展性和敏捷性。相比傳統的虛擬網路功能，雲端原生網路功能能夠更快速應對市場變化，並降低維護成本。容器的輕量級設計使得系統可以更加靈活應對不同工作負載。

過去企業主要依賴虛擬機技術來運行應用，但隨著容器技術的成熟，許多公司開始逐步轉向使用容器，從而在單一硬體平臺上運行更多的應用。容器化技術使得開發者能夠加快部署速度，提高運行效率，並且更好地利用基礎設施資源。

現今，企業不僅使用單一雲端服務，還需要在多個雲端環境中進行應用部署。多雲端架構允許公司利用不同雲端服務的優勢，從而實現成本優化、性能提升以及業務靈活性。不過，設計多雲端架構時，需考量各雲端服務提供商的差異，包括兼容性、管理複雜度及營運成本。

此外，企業在推進雲端原生網路功能時，必須高度重視安全問題。

---

[2] 虛擬網路功能（Virtual Network Functions，VNF）是一種將傳統網路硬體任務轉移到軟體層的技術。這種轉變使得網路管理和服務的部署變得更加靈活和高效。常見的 VNF 包括虛擬化路由器、防火牆、廣域網路最佳化和網路位址轉換服務。

[3] 雲端原生網路功能（Cloud Native Network Functions，CNF）是一種以軟體形式實現的網路功能，傳統上這些功能是由專用硬體設備執行的。CNF 的設計理念是充分利用雲計算的彈性和可擴展性，以便更有效地管理和運行網路服務。

[4] 無線電存取網路（Radio Access Network，RAN）是行動通訊系統中一個重要的組成部分，負責連接用戶設備（如手機、電腦等）與核心網路。

由於多雲端架構的複雜性，安全威脅的來源更加多樣，因此必須建立自動化的監控和防禦系統來即時應對潛在威脅。

第三位講者為奧克蘭大學高級講師Ulrich Speidel，演講的題目是「星鏈到底有多快？（How fast can Starlink[5] really be?）」。本演講基於星鏈向聯邦通訊委員會（Federal Communications Commission，FCC）提交的監管文件以及一些鏈路預算和資訊理論，探討對星鏈性能限制的了解。

Starlink是由低軌衛星營運商SpaceX所推出的全球衛星網際網路服務，它通過低軌道衛星網路向全球提供網際網路連接服務。這些低軌衛星與地面站進行連接，能夠提供相對傳統衛星網際網路更低延遲、更高速度的網路服務。Starlink的技術重點在於其使用數千顆小型衛星組成的網路，這些衛星以較低軌道運行，從而減少了信號傳輸延遲。

Starlink最大的市場優勢是能夠為傳統網際網路覆蓋不到的地區提供服務，尤其是偏遠地區的用戶，因此在全球的市場潛力巨大。

儘管Starlink在技術上具有領先優勢，但面對不斷增加的市場競爭，Starlink需持續創新，並且努力降低用戶的使用成本，以保持其競爭優勢。隨著其他企業和技術發展，Starlink必須在技術研發和商業模式上進一步提升，以應對未來的市場挑戰。

三、 技術會議 場次 2

（一）議程：技術會議 場次 2（Technical Session 2）

（二）時間：本年 9 月 4 日 16:30 - 18:00（UTC +12:00）

（三）講者：

1. Moderator：Terry Sweetser（APNIC Training Delivery Manager）

[5] 星鏈（Starlink）是由低軌衛星營運商 SpaceX 所開發的一個衛星網路，旨在通過低軌道衛星提供全球高速網際網路接入服務。相關介紹可參閱：https://zh.wikipedia.org/zh-tw/%E6%98%9F%E9%93%BE

2. Speakers：

(1)Christoff Visser（Internet Initiative of Japan’s research lab Network researcher）

(2)Duncan Cameron（Victoria University of Wellington PhD Candidate）

(3)Miho Moriyama（NTT Communications Staff）

(4)Pasan Nishantha（Sri Lanka Telecom General Manager）

（四）會議摘要：

第一位講者為日本IIJ研究實驗室網路研究員Christoff Visser，演講的題目為「蘋果的無線連接：蘋果的網路魔法還是痛苦（Apple Wireless Direct Link : Apple’s Network Magic or Misery.）」。

蘋果公司在全球擁有超過15億部的iPhone，對行動領域的影響是毋庸置疑的。這種廣泛採用的關鍵原因之一是「Apple生態系統」，具有AirDrop、AirPlay等功能。

Apple Wireless Direct Link（AWDL）是蘋果專有的一項技術，讓蘋果設備之間可以輕鬆傳輸資料。但這項技術也有可能導致蘋果設備的Wi-Fi連接不穩定，出現延遲或所謂網路抖動（Network Jitter）[6]的情況。在這次演講中，將解釋AWDL是如何影響蘋果設備的網路連接，並討論一些非傳統的網路設定，如何反而能提升蘋果設備的使用體驗。

AWDL的優點在於其低延遲和高傳輸效率，尤其適用於需要快速設備互相連接的應用場景。然而，隨著設備數量的增加和數據需求的增長，AWDL的性能也受到挑戰，特別是在Wi-Fi頻道擁擠的環境。

當多個設備同時連接到Wi-Fi時，頻道干擾成為主要瓶頸之一。這種干擾會導致網路連接速度變慢、封包丟失和延遲增大。通過智能路由

[6] 網路抖動（Network Jitter）是指在封包到達目的地的時間間隔中出現的隨機變化，這種變化會導致延遲的不一致性。這是因為封包的到達順序可能會被打亂，接收端需要重新排列封包，增加了延遲和處理負擔。

技術，企業可以優化頻寬分配，避免流量過於集中於單一區域。即時監控網路中所有設備的狀態，對異常情況作出快速反應，可確保資源的高效利用。

Apple的AWDL技術在提升設備間無線連接方面具有重要意義，但在高密度的Wi-Fi使用環境下，企業需採取有效措施應對可能出現的性能挑戰。通過頻道管理、集中化網路資源管理和專業的網路監控工具，企業可以在高流量環境中保持Wi-Fi的穩定與高效。

第二位講者為威靈頓維多利亞大學博士候選人Duncan Cameron，演講的題目是「每個ISP都需要在其網路上使用QoE中介盒[7]（Every ISP needs to use a QoE middle-box on their network）」。

每個網路服務供應商都需要在其網路上使用體驗品質中介盒。中介盒可以讓使用者了解網路像是延遲、抖動和緩衝膨脹（Bufferbloat）[8]等問題，只有在查看時才會變得明顯，中介盒能協助使用者發現網路各個層級的擁塞和延遲峰值。中介盒提供主動監控，在客戶打電話反應之前先識別出問題。

透過主動管理緩衝區膨脹、增強感知延遲和主動調整資料封包速度，可以立即提高客戶的體驗品質。根據經驗，這大大減少了客服電話的數量以及服務成本。

LibreQoS是一個針對網路服務供應商的開源體驗品質平臺。LibreQoS使用串流佇列和主動佇列管理演算法減少互動式應用程式的延遲，從而改善ISP客戶的日常體驗，並作為網路邊緣和核心之間的橋樑。其主要能力是用於可擴展的網路效能和延遲監控。

單一LibreQos設備上的吞吐量約為50-100 Gbps，區域光纖服務提

[7]體驗品質（Quality of Experience，QoE）中介盒是一種網路設備，旨在改善用戶的網路體驗，特別是在服務提供商的網路中。QoE 中介盒能夠監控和評估用戶在使用網路服務時的實際體驗。
[8]緩衝膨脹（Bufferbloat）是一種因封包過度緩衝而引起的封包交換網路高延遲。這種現象在網路設備如交換器、路由器等處理過量數據時發生。緩衝膨脹會引起延遲變化，並可能產生抖動。

供商使用的LibreQoS盒，已在高效能多CPU伺服器上實現了100 Gbps的聚合吞吐量。LibreQoS目前已在46個國家和美國24個州使用。使用LibreQoS的ISP數量最多的國家是菲律賓，其次是美國、加拿大、南非、香港、捷克、多明尼加、波蘭和肯亞。

第三位講者為NTT通訊人員Miho Moriyama，演講的題目是「網路資源管理在業務中的必要性（The Necessity of Network Resource Management in Business）」。

在本次演講中，討論網路資源管理對公司的重要性。2020年，NTT建立了ComNIC，以推動資源（AS號碼、IP位址、網域）的管理。在ComNIC成立之前，組織內發生了重大的入侵資安事件。事件發生時，每位管理員獨立管理網路資源，很難辨識事件對不同系統的影響。ComNIC的建立是為了應對這項挑戰，現在作為網路資源管理的集中平臺。本演講展示ComNIC的工作原理以及未來為確保各種網路資源安全而開展的工作。

ComNIC有三個主要作用，第一是制定管理政策、操作指南等及內部宣導，第二是作為APNIC和JPNIC等外部組織以及內部使用者的聯絡點，第三是集中管理和更新每個擁有資源的使用狀態和使用者資訊。

ComNIC為網路資源集中管理，規劃三項步驟，其一是軟體開發，制定集中管理辦法，進行資訊化平臺開發，其二是資訊收集，訪談資源經理，收集有關資源的外部訊息，其三是有效利用，落實各項安全措施，檢查和分析不再使用的網域。

第四位講者為斯里蘭卡電信總經理Pasan Nishantha，演講的題目是「GIS[9]如何激發電信數位化之旅（How GIS Inspires in the Telecom Digitization Journey）」。

近年來，地理資訊系統（Geographic information system，GIS）

[9] 地理資訊系統（Geographic information system，GIS）是一門綜合性學科，結合地理學與地圖學，已經廣泛的應用在不同的領域，是用於輸入、儲存、查詢、分析和顯示地理資料的電腦系統。

在電信業的必要性主要在固網運作中增加，因為網路資訊的可視化非常重要。GIS透過地點資料、資源的有效利用、銷售和行銷活動、故障修復、服務交付和網路規劃等來增強客戶服務。GIS還讓使用行動應用程式的員工能夠有效地利用GIS解決方案。本演講說明斯里蘭卡電信如何在內部建立自己的GIS系統以支援固定和無線服務運作。

四、 IPv6 布建

（一）議程：IPv6 布建（IPv6 Deployment）

（二）時間：本年 9 月 5 日 09:30 - 11:00（UTC +12:00）

（三）講者：

1. Moderator：Kenny Huang（APNIC EC Chair & TWNIC Chairman of Board）
2. Speaker：
   (1)Maile Halatuituia（Tonga Communications Corporation Engineer Cyber Security）
   (2)Alexandra Huides（Amazon Web Services Principal Network Specialist Solutions Architect）
   (3)Guoliang Yang（Xiongan Digital Office, China Technical Expert）
   (4)Wei Zhang（Tsinghua University）

（四）會議摘要：

會議一開始，由主持人TWNIC Kenny Huang（黃勝雄）致詞，歡迎所有與會者出席，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。

第一位講者為東加通訊公司網路安全工程師Maile Halatuituia，演講的題目是「東加通訊公司IPv6專案進展（TCC IPv6 Project Updates）」。

本演講討論行動網路營運商在部署IPv6時所面臨的挑戰，強調雖然網路部署是可行的，但真正的挑戰在於獲得用戶和供應商的支援。講者回顧自身的經驗，介紹了IPv6部署從最初步驟到當前狀態的過程，並分享了經驗教訓。透過分享過程，目標是協助該地區的其他小型電信營運商更有效地在其行動網路上部署IPv6。

Maile指出，管理階層的支持和資金投入是成功推動IPv6部署的關鍵。此外，對於像東加通訊公司這樣的小型營運商，講者建議必須從上游供應商開始，逐步向客戶端推行，因為大多數中間基礎設施已經多年支援IPv6。

他們面臨的挑戰之一是其舊的LTE用戶設備不支援IPv6，但通過更新設備和獲取基金會的資金支持，他們解決了這一問題。此外，IPv6連結移除網路防火牆後，他們的小型網路可以由一個小型技術團隊來進行管理，大大簡化了網路營運負擔。

第二位講者為AWS首席網路專家解決方案架構師Alexandra Huides，演講的題目是「在AWS上建置IPv6網路、用例、經驗教訓和參考架構（Build IPv6 networks on AWS, Use cases, lessons learned, and reference architectures）」。

本演講中回顧了AWS的IPv6部署過程、功能、以及加速採用IPv6的最佳實務。也深入探討了推動客戶採用IPv6的參考架構，以及協助加速採用IPv6過程的經驗教訓。

來自AWS的演講者介紹在雲端環境中部署IPv6的成功案例和其好處。他強調，IPv6可以幫助企業擴展網路連接、優化成本，並減少管理重疊IP位址的需求。AWS還提供了支持雙協定（IPv4和IPv6）的彈性負載平衡器，允許內部和外部連接。這樣的支持在容器和EC2部署中極具價值，特別是隨著雲端原生應用程式的增加。

AWS還指出，IPv6的應用能改善客戶體驗，擴大用戶基礎，同時減少對公共IPv4位址的需求，這對全球性企業尤為重要。

第三位講者為中國雄安數位辦公室技術專家Guoliang Yang，演講的題目是「純IPv6城市的實作方法（The Implementation Method of IPv6-Only City）」。

講者分享了在城市中全力部署IPv6的經驗。他們在建設和維護應用程式和終端設備時選擇了IPv6-only（僅使用IPv6）架構，這大大簡化了網路結構和開發工作，儘管需要較高的初期投資。這一做法有效地解決了應用兼容性問題，但仍然需要持續監測和調整來應對實際營運中的挑戰。

雄安新區IPv6部署有幾個方面的規劃，其一是IPv6數位道路，部署感測通訊設備，包括多功能資訊桿、數位攝影機、車路協同攝影機。數位公路總里程達153公里，建設規模涵蓋12.7平方公里。其二是網路實驗室，包含內部IPv6-Only電腦/終端機可以正常存取內部和外部IPv6資源，以及內部僅支援IPv6的電腦透過網路互通系統轉譯存取外部IPv4資源。其三是公寓及社區方面，雄安新區已有2,500多戶公寓安裝了家電，公寓內的家電可以透過內建的IPv6網路模組快速連接網路。當裝置連接到公寓網路時，會自動搜尋並連接，從而簡化了網路配置流程，並支援家庭物聯網接頭和設備。

第四位講者為清華大學Wei Zhang，演講的題目是「目前IPv6部署中IPv6位址介面識別碼模式的綜合測量（Comprehensive measurement of IPv6 address interface identifier pattern in current IPv6 deployment）」。

介面識別碼（Interface Identifier，IID）是IPv6位址的重要組成部分，極大地影響用戶隱私和掃描效率。儘管有像RFC7707這樣的早期綜合研究，但最近仍缺乏IID模式測量。此外，用於分析IID模式的現有

工具在識別隨機IID方面的準確性較低。在本演講中，提出了一種基於種子的新穎方法來識別隨機IID，將伺服器資料集上的誤報減少至少69%。也首次嘗試使用公共郵件清單收集IPv6位址，產生高品質的資料集並揭示了長達十年的IID模式演變趨勢。

測量結果表明，與RFC7707相比，IID模式發生了顯著變化。伺服器中低位元組模式從93%減少到39%，加上隨機模式顯著增加，使得IPv6位址掃描更具挑戰性。儘管伺服器位址掃描難度呈上升趨勢，但由於傳統方法識別隨機 IID的準確性較低，此難度被明顯高估。客戶端中基於IEEE的模式從8.87%下降到1.51%，進一步降低了隱私風險。但用戶端邊緣路由器具有更高的基於IEEE的模式，約為18%，這對透過這些裝置連接的用戶構成了巨大的隱私風險。研究結果提供了對IPv6隱私和掃描難度的當前評估，並為IPv6位址測量研究提供了新的方法。

五、 大會座談

（一）議程：天災下的韌性——穩健基礎建設及災後緩解計畫對太平洋島國的必要

Panel Discussion on Disaster Resilience: Pacific Islands and the need for robust infrastructure and mitigation plans

（二）時間：本年 9 月 5 日 11:30 - 13:00 （UTC +12:00）

（三）講者：

1. Moderator：Whitiaua Ropitini（Internet NZ）
2. Speaker：
   (1)Tenanoia Simona（Tuvalu Telecommunications Corporation, Government of Tuvalu CEO）
   (2)Sonia Edward（PNG DataCo IP Core Engineer）
   (3)'Esau Tupou（CERT Tonga Director）
   (4)Ashutosh Maharaj（Fiji National University Senior Instructor in IT）

（四）會議摘要：

火山爆發及颶風等天災，嚴重者可能導致這些島國與全世界斷聯。隨著氣候變遷，天災的頻率與破壞力逐年打破紀錄，其中太平洋島國的網路基礎建設在這些災害下尤其脆弱。本場次聚焦於太平洋島國的基礎建設韌性，請到數個太平洋島國代表，分享親身經驗及慘痛教訓。

來自巴布亞紐幾內亞的Sonia Edward任職於國立電信服務公司PNG Dataco。PNG Datoca負責管理的網路建設包括長達12,000公里的光纖海纜、Tier III資料中心[10]、51座衛星基礎建設，以及位於雪梨、關島及印尼查亞普拉的跨國網路服務提供點（points of presence，POP）。

巴布亞紐幾內亞2022年經歷重大震災，導致國內部分地區網路斷線。PNG Datoca當下透過備援衛星網路緊急恢復連線，災後改善計畫則包括建立新資料中心、網際網路閘道等，強化網路之餘，並購買地震保險。

來自斐濟的Ashutosh Maharaj介紹，斐濟常見的天災包括颱風、水災及地震。資料不足及系統老化是斐濟資通訊基礎建設的主要挑戰。Maharaj認為，強化網路韌性的關鍵策略應著重於建立穩健的資料中心、強化通訊網路，並積極善用如低軌衛星網路及雲端等技術。目前斐濟正透過在離島興建基礎建設，以及鼓勵公私部門合夥建設等方式，希望多元化國內網路基礎建設。Maharaj也強調，平時充分演習和訓練，非常有助於實際天災發生時的及時完善應變。

'Esau Tupou是東加王國電腦網路危機處理中心（Computer Emergency Response Team，CERT）主任，他首先播放影片，回顧2022年東加王國鄰近海域的海底火山爆發，導致全國斷網將近一個月的慘痛事件。Tupou分享此事件後的改善工作，包括規劃建設第二條聯外海纜，以及強化衛星網路建設與海纜互補。他也建議，政府應考慮招徠科技巨頭

[10] 根據全球權威國際機房認證機構Uptime Institute的機房分級認證，依機電設備、供電策略、管線分布及維修、容錯能力等將機房分成4級。

如Google建設海纜，並要求本地ISP建立急難應變計畫。

最後開放現場提問。一名與會者問道，太平洋島國是否有可能聯合發展區域網路能力計畫，如共同建設、鋪設海纜，或建立地面網路接取點的太平洋境內跨國通用標準等？

與談人同意此想法，表示這也是太平洋資通科技社群努力推動的目標。但斐濟代表也誠實指出，此類計畫理想上很棒，但現實是他們缺乏資金付諸實行。

六、 國家級網路位址註管機構特別興趣小組會議

（一）議程：國家級網路位址註管機構特別興趣小組會議（NIR SIG Session）

（二）時間：本年 9 月 5 日 14:30 - 16:00（UTC +12:00）

（三）講者：

1. Chair：Oanh Nguyen（VNNIC）
2. Co-Chair：Gaurav Kansal（ASO AC member / National Informatics Centre Joint Director （IT））
3. Speaker：
   (1)Koki Nakagawa（JPNIC）
   (2)Sanghyun Kang（KISA / Researcher of Korea Network Information Center （KRNIC）
   (3)Wen Yu Chen（TWNIC）
   (4)Zhen Yu（CNNIC Operations Manager）
   (5)Tom Harrison（Asia Pacific Network Information Centre Product and Delivery Manager）
   (6)Trần Cảnh Toàn（VNNIC Deputy Director of Technical Division）
   (7)Mukhammad Andri Setiawan（IDNIC Head of Training and

People Productivity）

（四）會議摘要：

NIR SIG場次目的是為，透過各個國家級網路位址註管機構（National Internet Registry，NIR）分享有關組織營運、政策等相關資訊，促進NIR之間，以及NIR與APNIC秘書處間的合作。本場次計有包括日本、越南、韓國、臺灣及中國等5個NIR提出報告，最後一個報告則是APNIC提出有關註冊資料的安全與永續之說明。接續為以「安全、永續網路基礎設施及NIR角色」為題的座談討論。

日本的JPNIC由Koki Nakagawa分享其最新的IP資源分配及技術活動成果。目前JPNIC的IP會員有來自12個機構計521位，和上一次APNIC會議時比較，會員數有增加；而JPNIC成立前的legacy資源持有者的數量則減少了11個。目前JPNIC已分配出40萬個/24 IPv4位址區塊，以及5,678個/32 IPv6位址區塊。其也概述了JPNIC在自治系統號碼（Autonomous System number，ASN）、資源公鑰基礎建設（Resource Public Key Infrastructure，RPKI）、以及採用路由來源授權（ROA）等的統計。活動部分，JPNIC 於今年7月在福岡舉辦一場網際網路週展示活動，主題是電子競技。此外，JPNIC 還舉辦了多場技術培訓課程，主題包括DNSSEC和RPKI實作等；其也擔任於奈良舉辦的JANOG54活動的金牌贊助者。今年的JPNIC公開政策會議（JPOPM）於6月21日舉行，討論主題包括WHOIS用戶研究、JPNIC與APNIC政策現況、獎學金計畫等。

接續是KRNIC/KISA 代表Snghyun Kang和Billy Mooho Cheon向大家說明韓國相關進展。Kang首先說明，KRNIC截至本年7月為止的會員總數為1,074名，雖然分配出的IPv4地址總量較去年略有減少，目前仍管理了超過1.12億個IPv4地址；IPv6位址的分配量則是5,259個/32s。在活動部分，KRNIC在本年上半年舉辦了3場線上及1場實體的技術研討會，並參加韓國最大網路會議KRnet 2024活動擔任講者，該場會議主要聚焦於

DNS/BGP、區塊鏈及加強隱私技術等議題。KRNIC還參加了韓國網路治理論壇，討論了路由安全議題。Cheon則介紹了今年在釜山舉行的亞太網路治理學院（Asia Pacific Internet Governance Academy，APIGA）辦理情形，計有39名學員參與，KRNIC希望通過全球化該活動，與其他國家級網路位址註管機構（NIR）合作，推廣網路治理相關議題。他也介紹了目前KRNIC與其他國家NIR合作情形，像是辦理聯合工作坊等；另也提及目前與JPNIC簽署新的合作備忘錄之規劃。

TWNIC則由Wen Yu Chen (陳玟羽)說明工作進展。他提到目前TWNIC的會員總數為332個，TWNIC目前已分配出1.3萬個/24s IPv4位址和2,581個/32s IPv6位址。台灣在本年8月底的IPv6 User Availability比率已達60.34%，和2017年的0.46%比較已有長足進步，目前全球排名第十。接續講者繼續介紹TWNIC在RPKI、ROA等方面推動之統計數據。在活動方面，TWNIC於本年4月舉辦了ICANN APAC-TWNIC Enagegement Forum 和TWNIC IP公共政策會議，並於8月主辦了APSIG及APrIGF會議，吸引超過1,000名參加者。最後講者也總結TWNIC未來將繼續推動IPv6培訓，並協助ISP管理ROA，以提升ROA覆蓋範圍，並持續域名濫用聯絡人驗證工作，進一步強化臺灣的網路安全與管理。

中國的CNNIC由Zhen Yu(禹楨)代表說明中國網路發展的相關數據與規劃。他首先提到截至本年8月，中國網路使用者達10.99億，普及率為78%，其中行動網路用戶規模為10.96億。目前CNNIC會員為1,300家，涵蓋製造、金融、教育等領域。CNNIC目前已經分配出332,553個/24s IPv4位址、28,784/32s，以及1,211個AS號碼。活動方面，本年4月，CNNIC組織了線上培訓活動，並計劃於11月舉辦IPv6與DNS主題的實體培訓課程。最後講者更新中國的IPv6發展，截至本年5月，中國的IPv6用戶達7.94億，占網路用戶總數的72.7%；其中行動網路訊務量超過六成，而固網的訊務量超過20%。主要入口網站與前200大應用程式都已支援IPv6。

VNNIC代表Oanh Nguyen則更新了越南的IPv6部署進展。越南目前已有超過60%的IPv6採用率，並計畫在未來進一步提升該數字。該國專注於ISP和行動業者的IPv6部署，同時也在推廣RPKI加強網路安全。VNNIC也與政府密切合作，推動資通訊基礎設施政策，包括透過各種會議和培訓提高社群對RPKI和IPv6的認識。VNNIC也在今年舉辦了多場工作坊和會議活動，其中包括在峴港市舉辦的APTLD會議活動。未來也規劃在物聯網（Internet of Things，IoT）和雲端服務等領域進一步應用IPv6。

最後一場報告是由APNIC的Tom Harrison介紹註冊資料存取協議（Registration Data Access Protocol，RDAP）的安全性和可持續性。特別是與NIR有關的部分。他接續介紹，RDAP基於HTTP協定，使用JSON和TLS來加強安全性和資料傳輸保護，與WHOIS協議比較，RDAP解決了其格式和擴張性不佳等問題。RDAP通過統一的格式和編碼來簡化查詢過程，提高了查詢的準確性和可持續性。APNIC正在逐步實施RDAP擴展功能，並計畫在未來12個月內實施一些改進，如多語言支援。儘管部分數據無法傳遞到APNIC，APNIC正與NIRs合作解決這些挑戰。RDAP已被ICANN投資和推廣，因此RDAP將在未來長期存在並持續改進。

與會者提問，若RDAP有這麼多優點，為什麼人們仍在使用WHOIS，RDAP何時完成，或取代WHOIS系統，APNIC是否會部署RDAP取代WHOIS？Harrison回應，類似情況在歷史上經常發生，需要強制措施才能推動轉變。儘管RDAP有多項優勢，但目前對於那些既有的WHOIS使用者來說，重新編寫系統的動力不強。未來隨著更多功能實現，可能會更有利於推動轉換。又有與會者詢問APNIC逐步淘汰WHOIS服務的計畫，Harrison則尷尬地回答轉換是棘手的工作，目前APNIC尚未考慮要積極逐步淘汰WHOIS。

接續的座談主要講者除Harrison外，還有越南、印尼的NIR代表，就網路基礎設施、網路安全與永續發展等議題展開對話。VNNIC代表Trần Cảnh Toàn首先說明，越南網際網路基礎設施之發展已納入2021至2030年

的國家資通訊計畫中，並且還會延伸至2050年。該計畫包括數位基礎設施、IT基礎設施、數位轉型平臺及網絡安全系統等。目標是建設數位政府、數位經濟和數位社會，確保人人都能連接到網際網路。到2025年，計劃每個家庭都可連接光纖網路,每位年滿18歲的學生將擁有智能手機,並提高寬頻和移動網路速度，確保高速連接。此外，越南將加強國際光纖連接，包括海底光纖，並推動IPv6和物聯網（IoT）的應用，確保關鍵基礎設施如電力、交通和供水系統能夠使用IoT技術。

主持人接續邀請Tom Harrison從網路安全的觀點發表看法。Tom強調，網路資源因為具有排他性，故網路安全和可持續性更為重要，尤其是對於IP位址和ASN號碼等網路資源來說。若出現多方爭奪資源情況，能明確判定誰應該擁有該資源是非常重要的。此外，能聯繫到這些資源的管理者也同樣重要，事關系統運作的正常與否。

來自印尼的IDNIC代表Mukhammad Andri Setiawan 則分享其組織營運的成功經驗，他提到IDNIC每個月會收到60份會員的新申請案，每年約新增700名會員，印尼的規模龐大，因此基礎設施對營運非常重要。自2019年開始，IDNNIC便非常關注會員服務，並計畫在印尼各地建立多個備援，目前已有15個以上的交換中心。他也直言，會員數量的增長以及RPKI的實施對基礎設施也帶來壓力，因此增加備援和提升容量將會是未來發展的關鍵。

七、 技術會議 場次 3

（一）議程：技術會議 場次 3（Technical Session 3）

（二）時間：本年 9 月 5 日 16:30 - 18:00（UTC +12:00）

（三）講者：

1. Moderator：Christoff Visser（Internet Initiative of Japan’s research lab Network researcher）
2. Speaker：

(1)Sophie Hamel（University Paris 8 PhD Candidate）

(2)Amber McEwan（REANNZ CEO）

(3)Richard Nelson（Searchlight NZ OpenLI manager）

(4)Anh Nguyen（Viettel DevOps Engineer）

（四）會議摘要：

會議一開始，由主持人Christoff Visser開場致詞，歡迎所有與會者出席本場次的技術會議。第一位講者為巴黎第八大學博士候選人Sophie Hamel，演講的題目是「資料路由作為地緣政治工具：來自太平洋島國網路的見解（Data Routing as a Geopolitical tool: Insights from Pacific Island Countries' Networks）」。

本研究探討了太平洋島國（Pacific Island Countries，PICs）的數據路由，從地緣政治的角度分析數據傳輸如何反映地區間的權力和經濟依賴。研究採用RIPE Atlas移動探針收集的2023年數據，並進行了與斐濟、瓦努阿圖及澳洲的電信營運商、通訊監管機構的訪談。數據顯示，PICs高度依賴澳洲的區域營運商和美國的國際頻寬提供商，尤其是在數據流向的集中方面。即便部分島國間有直連海底電纜，地區間的數據互聯性依然有限。

研究也特別分析了斐濟在數據路由中的戰略角色，該國作為南太平洋地區的轉運樞紐，負責中轉多數島國的數據通信，這進一步加強了該地區對澳洲的依賴。這種依賴不僅是技術上的，也有重要的經濟和地緣政治影響，反映了各國之間的權力不對稱關係。

此外，研究還對比了斐濟和瓦努阿圖的國內互連政策，指出斐濟的數據路由政策更具戰略性，擔任區域數據交換中心的角色，而瓦努阿圖等國的內部數據路由仍有改善空間。通過分析BGP的數據流動，這項研究揭示了數據路由如何成為一個地緣政治對象，並強調了太平洋島國之間的依賴關係和國際營運商的影響力。

本演講說明太平洋島嶼的網路架構在很大程度上依賴於美國和澳洲的基礎設施，這種依賴性來自歷史上鋪設的海底電纜與兩國的政治聯繫。太平洋島國的數據流量多數要通過這些國家，而這樣的現象在地緣政治上有著深遠影響，特別是在澳洲和中國在太平洋地區競爭的背景下，這些國家在技術上與地緣政治上的競爭影響到了該地區的網際網路發展。

講者進一步說明了透過分析自治系統的BGP路由策略來理解地緣政治的關聯性，指出BGP路由政策是由政治和經濟利益驅動的，並具有人為控制的特徵。她的研究集中在太平洋島嶼與外部網路的連接性，發現太平洋地區的數據流動與物理基礎設施的建設有很大關聯，而這些基礎設施多數由美國和澳洲控制。

這種情況使得太平洋島嶼的網路像「半島」一樣，必須通過外部網路連接到世界其他地區。這使得當地的網路建設極度集中在外部利益上，並且缺乏內部的自給自足性。她還討論了由聯合國發起的「Pacific IX」項目，旨在提升當地營運商之間的網路互聯性，但由於商業利益的驅動，當地營運商並沒有強烈的意願彼此互連。

第二位講者為REANNZ總經理Amber McEwan，演講的題目是「透過教育創建基礎設施以支持數位平權（Creating infrastructure to support digital equity across education）」。

REANNZ與紐西蘭教育部合作，旨在建立一個覆蓋全紐西蘭的互連學習空間網路，讓學生能夠在最適合學習的環境中工作、學習和協作。這項計畫的目的是通過靈活的學習方式，提升學生的學習體驗，打破傳統空間限制。

其中一個關鍵技術是全球Wi-Fi解決方案eduroam[11]，這是一個全球教育機構廣泛使用的安全網路系統。2023年，全球範圍內的學生、研究

[11] eduroam 是一個國際無線區域網路漫遊系統，允許學術界用戶在全球多個地點透過單一帳號安全連線。相關內容請參閱：https://eduroam.org/。

人員和教職員工使用eduroam超過70億次。它讓學生能夠在不同的校區和國際合作機構中無縫連接網路，提供便捷且安全的網路接取。

此次會議更新該計畫的進展，並提供關於eduroam技術的詳細介紹，強調其在支持互連學習空間網路中不可或缺的作用。

紐西蘭國家研究與教育網路分享了他們如何利用技術手段來改善紐西蘭的數位平權問題，尤其是在COVID-19疫情期間，當學生需要居家學習時，該問題變得尤為突出。根據DIGITAL EQUITY COALITION AOTEAROA（DECA）[12]的報告，許多學生因貧困、無法接入網路或家庭環境不安全等原因，無法參與數位學習。

其通過一項名為「edome」的全球性工具來解決這一問題，這是一種聯邦Wi-Fi解決方案，旨在打破連接可用性和實際可接入性之間的障礙。這個工具不僅能夠讓學生們自動連接到網路，還幫助提供Wi-Fi的機構向其資助者展示使用統計數據。該工具具有成本效益高且易於擴展的特點，使得其成為解決紐西蘭數位落差的重要手段。

此外，Amber還提到，研究與教育網路與幾家紐西蘭本地的電信公司以及無線ISP進行合作，以擴展這個聯邦Wi-Fi網路，並且正在計劃將這個項目擴展至醫院等公共場所，進一步提升紐西蘭教育領域的數位平權。

第三位講者為Searchlight NZ OpenLI 經理Richard Nelson，演講的題目是「Experiences delivering Open Source software to Network Operators Worldwide（向全球網路營運商提供開源軟體的經驗）」。

OpenLI是一個開發開源軟件的項目，專門用於合法攔截（Lawful Interception，LI）。最初，它是為了應對紐西蘭的新法規需求而設計的。然而，由於全球大部分地區採用相同的技術標準，該項目吸引了來

[12] https://www.digitalequity.nz/

自世界各地的關注和查詢。

此次演講介紹與來自不同國家的網路營運商進行交流和合作的經驗，討論了各國如何在不同的司法管轄區內監管和實施合法攔截。從這些交流中學到了各種實施方式和挑戰，這有助於適應更廣泛的國際需求並提升其兼容性和實用性。

Richard Nelson介紹了他們在世界各地部署開源合法攔截（Lawful Interception）軟體的經驗。他們的開源項目OpenLI主要旨在幫助網路營運商滿足法律要求，提供給執法機構符合規範的服務。這項技術雖然在全球範圍內推廣，但面臨著不同國家的法律和技術挑戰。

在紐西蘭，網路營運商需要遵守法律規定，向執法部門提供攔截服務。該項目從2013年開始，通過與當地執法機構合作，成功部署了OpenLI軟體。Richard提到，由於不同國家的規範和流程差異，項目的實施存在複雜性，例如德國擁有完善的法律框架，而在澳洲和孟加拉，規範的實施仍在發展中。

Richard還提到了在網路技術轉型時的挑戰，這使得他們在應用OpenLI系統時需要調整操作流程。這些技術在幫助各國應對國家安全問題和嚴重犯罪方面發揮了積極作用。

第四位講者為Viettel開發營運工程師Anh Nguyen，演講的題目是「探究黑盒子:使用基本工具和技術調試kubernetes[13]網路(Probing the blackbox : Debugging kubernetes networking with basic tools and techniques）」。

Kubernetes 網路常常讓人覺得複雜且充滿抽象概念，像是一個「黑盒子」。這場演講的目的是回歸基礎，幫助開發者解決 Kubernetes 常

[13] K8s 全名為 Kubernetes，之所以被稱作 K8s，是因為名稱的 k 與 s 之間有 8 個英文字母而得其名。K8s 是一種可用來自動化部屬、擴展及管理多個容器的系統，適用於當容器數量增加，需要穩定容器環境，以及管理資源或權限分配的狀況。Kubernetes 網路提供網路基礎架構，用於實現容器化應用程式的通訊、可擴展性、安全性和外部存取。網路錯綜複雜，包括 Kubernetes 叢集內部（例如 Pod、節點、容器、服務）和外部（例如外部流量）的所有主要元件之間的通訊。

見的網路問題，讓複雜的網路概念變得簡單易懂。

Kubernetes使用了各種網路元件（如服務發現和負載均衡），這些抽象層次雖然能自動化許多網路工作，但同時也讓問題排查變得困難。本次分享聚焦於如何解構這些關鍵概念，例如內部通訊、服務之間的互動以及網路策略的運作。

本演講主要的內容是提供實用的故障排除技巧，讓Kubernetes網路變得更加透明且易於管理。學習如何追蹤如DNS解析問題、網路延遲或通訊錯誤等常見問題。目標是幫助開發者從「為什麼不工作？」的挫敗感中解脫，並能自信地解決Kubernetes網路問題。

藉由解密這些挑戰，這場演講使Kubernetes的網路更加親近，開發者也能迅速掌握日常問題的解決技巧，提升系統穩定性。

Kubernetes網路技術是一種為現代應用提供靈活且可擴展網路環境的解決方案。講者深入探討了Kubernetes的網路架構，包括容器網路介面的設置、負載平衡技術、DNS解析等關鍵技術環節。

特別值得注意的是，講者介紹了如何解決在Kubernetes網路環境中常見的通信問題，還展示了實際案例，說明如何通過檢查網路政策、更新防火牆規則、檢測服務和端點配置來解決負載平衡的問題。

其中一個範例示範了在集群環境中，如何解決前端應用與後端API服務之間的網路連接問題，並展示了使用封包分析工具找出問題的過程。最終通過調整DNS部署的內存資源，並清除阻止UDP通信的防火牆規則，成功解決了連接問題。

這些內容強調了在Kubernetes集群中穩定保持網路連接的重要性，並展示了診斷和解決網路問題的有效工具與技術。

八、 公開政策會議 場次1

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

（二）時間：本年9月6日09:30 - 11:00 （UTC +12:00）

（三）講者：

1. Chair：Bertrand Cherrier（Micro Logic Systems Policy SIG）
2. Co-chair：
   (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. Speaker：Srinivas Chendi（Asia Pacific Network Information Centre Senior Regional Advisor - Membership and Policy）

（四）會議摘要：

本議程為公開政策會議（Open Policy Meeting，OPM），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；投票結果會直接公佈，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。

首先由APNIC政策及社群部門資深顧問Srinivas（Sunny）Chendi報告政策實施進度。於APNIC 57通過的政策提案「縮小發派予網際網路交

換點（IXP）的IPv4位址空間」[14]（prop-154）及「臨時發放位址」[15]（prop-156），因為政策實施涉及改變APNIC的核心系統模組，所以目前仍在逐步實行中，預計於本年Q4期間完成實施。

本場次原訂討論兩項政策提案，但prop-159提案作者未報名出席APNIC 58，也沒有線上或實體參與本場次，因此主席判定prop-159提案視同撤銷，未予討論。

本場次僅討論prop-157。

(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：

本提案曾於 APNIC57 提出，並未獲共識支持。目前為第四版。

秘書處分享政策衝擊評估。首先說明，由於提案作者在會前突然修改提出第四版，衝擊評估乃針對第三版。評估認為此提案未考慮諸如資源臨時移轉雙方協議破局、其中一方未遵守協議規定、其中一方遭收購等情況，將為 APNIC 組織帶來過多法律風險。

現場討論大多同意秘書處評估。亦有與會者直指此提案企圖合法化位址租賃，不應通過。作者回應強調此提案內容並非

[14] 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。

[15] 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。

位址租賃，且強調訂定規則勝過缺乏明令禁止而導致私下交易，但此解釋並未獲接受，整體風向仍堅決反對位址租賃。

表決結果：

未獲共識通過，主席建議作者棄案。

九、 公開政策會議 場次 2

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

（二）時間：本年 9 月 6 日 11:30 - 13:00 （UTC +12:00）

（三）講者：

1. Chair：Bertrand Cherrier（Micro Logic Systems Policy SIG）
2. Co-chair：
   (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）

（四）會議摘要：

本場次繼續討論其餘政策提案如下：

(1) prop-160: Change IPv6 Initial assignment to /44 for Organizations Eligible for multihoming

提案人：

- Md. Rafeeun Noby Babir
- Muhammad Redwanul Karim

提案內容：

已獲發派 IPv4 的帳戶持有人若同時具有多連接（multi-homed）網路基礎建設，則可自動獲發派/44 的 IPv6 位址，並

可將多連接網路的最小發派空間大小改成/44。

討論：

與會者指出此提案在 8 月初提出第一版後，突然在 8 月底撤銷並於 9 月 1 日提出第二版，改變過於臨時，沒有充分時間研議並商討第二版，因此難以支持。雖主席解釋兩個版本之間僅有些微用詞差異，但也了解社群立場。

其他與會者指出，此提案與目前 APNIC 政策沒有顯著差異，雖政策中未講明，但既有帳戶持有人若有需求，本來就可輕易申請並取得大於/48 的 IPv6 位址。此提案雖立意良善，但似乎過度干涉而適得其反，略嫌可惜。

表決結果：

未獲共識通過，退回 mailing list 重新討論。

本次會議本來有4項政策提案，但prop-159因作者未到場而撤銷，另一項提案則由作者於會前撤銷，改成簡報介紹，內容為IPv6有助於物聯網。結論而言，APNIC58總共僅討論2項政策提案。

十、 APNIC 會員大會 場次 1

（一）議程：APNIC 會員大會 場次 1 （APNIC Member Meeting 1）

（二）時間：本年 9 月 6 日 14:30 - 16:00 （UTC +08:00）

（三）講者：

1. Chair：Kenny Huang（APNIC Executive Council）
2. Speaker：
   (1)Karla Skarda（APNIC Senior Director Registry）
   (2)Che-Hoo Cheng（Asia Pacific Network Information Centre Senior Director, Development）
   (3)Pablo Hinojosa（APNIC Senior Director, Engagement）
   (4)Tony Smith（Asia Pacific Network Information Centre

Senior Director, Operations）

(5)Yoshinobu Matsuzaki（IIJ APNIC EC Treasurer）

(6)Brenda Mainland（Survey Matters Co-Founder）

（四）會議摘要：

本場次為APNIC會員大會，分成上下半場舉行。上半場由執行委員會（EC）和秘書處報告APNIC營運情形，並宣布本屆年度選舉結果。下半場邀請所有SIG主席簡報會議期間SIG場次的討論精華。

EC主席黃勝雄介紹所有EC成員後，APNIC四大部門的資深協理Karla Skarda(註冊管理/ Registry)、Che-Hoo Cheng(發展 / Development)、Pablo Hinojosa(交流 / Engagement)及Tony Smith(營運 / Operations)依序報告本年APNIC秘書處執行成果。APNIC自今年起組織重整，並開始新一回合的四年戰略計畫。新APNIC組織架構如圖1：

圖1.　新 APNIC 組織架構圖

從圖中可看出，新的組織架構以「能力」（capability）為基礎，「註冊管理」（registry）及「發展」（development）奠基其上，最上方則是「交流」（engagement）。「註冊管理」與「發展」是APNIC作為亞太地區的區域網際網路註冊管理機構(Regional Internet Registry,

RIR）應發揮並提供的價值（value），「能力」及「交流」則是「賦能因素」（enabler），確保APNIC具有能力，一方面提供RIR的充分價值，一方面作為秘書處，協助社群發揮能量。

1.註冊管理（Registry）

因為2023年IP位址市場交易活絡，APNIC本年的IPv4和IPv6發派數量皆下降。在此同時，APNIC透過歷史資源回收專案回收不少IPv4位址，也仍是少數尚具可發派IPv4位址的RIR。會員數量成長雖減緩，但根據會員滿意度調查，整體滿意度仍高達81%。APNIC產品服務的具體改善包括：整體安全性提升（利用OKTA進行多重驗證）、重建APNIC聯絡管理系統並新增API。APNIC的網路健康監測服務「DASH」今年新增的「顯示可疑訊息細節」也受社群好評。

2.發展（Development）

今年APNIC Academy與亞太地區境內不同當地網際網路註冊機構（National Internet Registry，NIR）、網路維運小組（Network Operating Groups，NOG）等合作，共舉辦104場由講師親自帶領的訓練課程（包括線上與實體）。線上課程的「虛擬實驗室」相關課程新增「共享實驗室」功能，讓使用者可線上協作練習。

APNIC參與支援的社群蜜罐計畫(Community Honeypot Project)[16]本年新增100個蜜罐偵測器。APNIC持續在DNS基礎建設和技術上與社群合作並協助會員，本年協助設立7個網路交換點，大幅改善當地訊息效能。

3.交流（Engagement）

APNIC的交流工作聚焦於賦能予組織本身與社群。比起參與活動，

[16] 社群蜜罐計畫（Community Honeypot Project）請參閱：https://blog.apnic.net/2019/09/17/the-apnic-community-honeynet-project/

APNIC更重視如何支援主辦單位及與會者，透過會議、mailing list和政府交流等，居中協調、促進社群互動交流。本年1月至7月期間，APNIC完成297項交流相關工作，其中半數以上以實體方式進行，35%以上為安全相關的教育訓練。APNIC今年支援參與22場網路維運小組（Network Operating Group，NOG）活動，包括新創如巴基斯坦、阿富汗，以及今年重啟的臺灣。

政府交流方面，APNIC持續追蹤相關討論並派員參與會議，包括聯合國的全球數位契約（Global Digital Compact，GDC），目前也正在準備參與ITU世界電信標準大會（World Telecommunications Standardization Assembly，WTSA）。

全球協作方面，APNIC在號碼資源組織（Numbers Resource Organization，NRO）架構下與其他RIR合作，聚焦於RPKI計畫。本年8月方於台灣落幕的亞太網路治理論壇，APNIC也是關鍵支援及參與方。

4. 營運（Operations）

APNIC本年依序通過ISO27001（資訊安全管理）、ISO9001（品質管理）稽核及財務稽核。APNIC目前正在公開招標徵求新的投資經理，同時進行組織內差旅管理規劃重整，目的為降低開銷並增加效率。根據最新員工調查（9成以上填答率），APNIC員工滿意度為82%，超越全球基準7%，人員流動率僅3.2%。

在治理方面，APNIC成功滿足社群要求，提前發布年度報告及活動報告。目前所有EC成員都依法同時作為APNIC Pty Limited及APNIC EC Limited董事；EC新成立，負責監督選舉期間違規行為的選舉委員會，並未在剛結束的EC選舉發現任何異常。

整體而言，APNIC在營運和治理目標上穩定進步，並確保於成本限度內完成所有營運標的。

EC財務Yoshinobu Matsuzaki（松崎吉伸）報告2023年財務情形，相關細節可參考簡報內容[17]。

EC主席黃勝雄報告EC去年工作。自本年3月APNIC 57結束至今，EC共舉行3場實體會議，下一場預計於本年11月於布里斯本進行。

APNIC前總經理Paul Wilson於APNIC 57期間宣布卸任，EC本年上半年的首要任務之一便是尋找下一任總經理。EC於本年7月公告選任Jia Rong Low，後者將於同年10月就任APNIC總經理。

APRICOT 2025暨APNIC59原訂於孟加拉首都達卡舉行，但因全球旅遊警示，APRICOT已宣布將更改APRICOT 2025暨APNIC59會議地點，新地點預計在未來幾個月內公佈。APNIC 60將於越南峴港舉行。

開放問答期間，與會者指出過去曾建議EC應至少一名成員透過其他流程，以獨立方式選任。此提議主要希望解決APNIC EC始終性別比例極度不均的問題。主席表示EC認同此提議，也同意應試圖解決性別比例不均的問題，將積極與社群交流，探討下一步。

問卷調查顧問公司Survey Matters代表Brenda Mainland報告問卷調查結果。APNIC每兩年舉行問卷調查，募集會員及社群對APNIC表現及未來目標的回饋意見。本次調查首先以訪談及焦點小組等方式搜集質化資料，訪問對象總計48人。接續的問卷調查達到1,100份填答數，大部分填答者為APNIC會員或NIR，其餘利害關係方僅佔14%。

APNIC在關鍵效能指標上整體保持高分，超過95%的受訪者評價服務品質高於平均、良好或優秀，而這其中有54%評為優秀。然而，不同地區的給分差距值得注意。相較於南亞的平均高分，大洋區填答者的滿意度下降，推測可能與歷史資源回收計畫有關。針對APNIC治理的公開透明性，填答者一率給出高分。APNIC新組織章程的相關問題也取得正面評價，除

[17] https://conference.apnic.net/58/assets/files/APNZ606/apnic-ec-treasurer-r_1725566071.pdf

資源發放外，填答者也讚許APNIC在能力建構、協作及支援改善網際網路基礎建設上的付出。

填答者普遍認為網際網路安全是APNIC面對的最大挑戰，營運上的挑戰則包括成本控管及人才短缺。在APNIC教育訓練方面，訓練主題、費用高低和是否能提供訓練結業證書，是填答者最在意的因素。

十一、 APNIC 會員大會 場次 2

（一）議程：APNIC 會員大會 場次 2 （APNIC Member Meeting 2）

（二）時間：本年 9 月 6 日 16:30 - 18:00 （UTC +08:00）

（三）講者：

1. Chair：Kenny Huang（APNIC Executive Council）
2. Speaker：
   (1)Cherie Lagakali（Netsafe New Zealand APNIC Election Chair）
   (2)Kim Davies（Internet Corporation for Assigned Names and Numbers VP, IANA Services and President, PTI）
   (3)Nicole T. I. Chan（ASO Vice Chair /Digital Transformation Association Taiwan APNIC NRO NC Member）
   (4)Bertrand Cherrier（Micro Logic Systems Policy SIG）
   (5)Joy Chan（TWNIC Deputy CEO）
   (6)Oanh Nguyen（VNNIC）
   (7)Di Ma（ASO AC member / ZDNS Principal Research Fellow）

（四）會議摘要

選委會主席Cherie Lagakali分享本屆選舉結果。Nicole T. I. Chan（詹婷怡）選上APNIC派任號碼資源組織（NRO）號碼委員會（NC）暨ICANN位址支援組織（Address Supporting Organization，ASO）位址理事會(Address Council，AC)理事，財團法人台灣網路資訊中心(Taiwan

Network Information Center，TWNIC）顧靜恆組長選上Policy SIG聯席主席。

ICANN附屬單位「公共技術識別碼」（Public Technical Identifier，PTI）主席報告網際網路號碼指配機構（Internet Assigned Numbers Authority，IANA）近況。Davies首先介紹「建立新地區網際網路註冊管理機構準則（Criteria for Establishment of New Regional Internet Registries，ICP-2）」。此文件完成於2001年，目的為提供IANA認證區域網際網路註冊管理機構（RIR）的指導原則；拉丁美洲網路資訊中心（LACNIC）與非洲網路資訊中心（AFRINIC）皆依據此指導原則而成立並獲得IANA認可。目前ICP-2正經歷審核修訂，預計近期內發布修訂提案，屆時將廣募社群意見。

維護DNS的安全是IANA重要職責之一。自2018年首次置換DNSSEC的根區簽署金鑰（key signing key，KSK）後，目前IANA正在籌備下次KSK置換。預計於本年生成新KSK，並於2026年全面完成置換。最後，Davies提醒IANA的五年戰略計畫正開放募集社群意見中，鼓勵社群踴躍參與並發表意見。

ASO AC副主席Nicole T. I. Chan（詹婷怡）報告ASO AC近況。AC主要職責包括監督全球位址政策制定（上次出現全球位址政策為2012年）、推派2名ICANN董事，以及派任一名代表參與ICANN提名委員會。ASO AC今年重點工作為遴選出ICANN董事，以及ICP-2文件修訂原則提案。

Policy SIG主席Bertrand Cherrier報告本屆OPM討論結果。本屆OPM沒有通過任何政策提案。

合作特別興趣小組（Cooperation SIG）主席Joyce Chan（丁綺萍）報告本屆合作SIG會議討論。本屆合作SIG場次的主題是「ICP-2的重要性」。場次中請到多方利害關係代表，回顧ICP-2誕生的歷史，並檢視、重申此文件的重要性。

NIR SIG主席Oanh Nguyen報告NIR SIG討論重點。本次請到JPNIC、KRNIC、TWNIC、CNNIC、VNNIC分享各國近況，分享內容皆聚焦於國內IPv4與IPv6部署率及RPKI普及率。APNIC產品經理Tom Harrison則介紹註冊資料存取協定（Registration Data Access Protocol，RDAP）。

路由安全特別興趣小組（Routing Security SIG）主席Di Ma（馬迪）報告本屆討論重點。這次共邀請到4位講者，分享議題包括：路由安全、路由來源授權(ROA)及驗證ROA負載(validated ROA payload，VRP)的安全不穩定問題、遠端觸發黑洞路由(Remote Triggered Black Hole，RTBH）如何適用RPKI、多來源自治系統組成簽署群組後如何適用RPKI。同時亦請到APNIC資深網路分析師Dave Phelan 報告亞太地區RPKI近況。

亞太網際網路交換協會（Asia Pacific Internet Exchange Association，APIX）由亞太地區的網路交換中心組成，提供成員經驗交流的平臺。本屆工作坊總參與人數為46人，討論聚焦於網路交換中心的經營經驗分享。

參、 觀察與建議

一、 觀察事項

（一） 網路安全的重要性日益增加，隨著網路攻擊事件的頻繁發生，企業和個人對於網路安全的重視程度顯著提升。會議中強調了加強防護措施和即時響應的必要性，顯示出安全性已成為網絡技術發展的核心議題。

（二） 技術創新與應用的快速變化，隨著 5G 和物聯網技術的推廣，網路的效能和應用場景正在快速擴展。這不僅改變了用戶的需求，也促使技術提供者必須不斷創新，以適應市場的變化。

（三） 企業對串流媒體需求增加的挑戰，隨著串流媒體應用需求的增加，企業網路需要支持大量設備同時在線，並保證高品質的視訊和音頻傳輸。這對 Wi-Fi 的頻寬、延遲控制和資源管理有更高要求，特別是在對應多設備、多品牌的連接需求時，網路負載管理成為主要挑戰。

（四） 太平洋地區網路地緣政治的脆弱性與依賴性，會議中強調了太平洋島國在網路基礎設施上高度依賴美國和澳洲，這種依賴暴露了地緣政治上的脆弱性。外部控制的基礎設施讓這些國家缺乏自主性，進而影響了當地的網路發展和安全。

（五） 強化 IPv6 培訓與技術支持，IPv6 的部署涉及大量新技術和架構的學習，因此，提供專業的培訓課程和技術支持是推動 IPv6 廣泛應用的關鍵。企業和政府應建立持續的培訓計劃，縮小知識差距，確保網路工程師和開發團隊掌握 IPv6 的基礎和高級應用，從而降低部署過程中的錯誤率。

（六） 逐步過渡到 IPv6 單一環境為未來發展趨勢，為減少 IPv4 和 IPv6 共存環境的管理複雜性，企業可以考慮逐步轉向 IPv6 單一環境。這不僅能簡化網路架構，減少重疊位址的問題，還有助於未來技

術的擴展和創新，特別是在物聯網（IoT）和 5G 技術的應用中。

二、 建議事項

（一） **定期舉辦網路安全教育訓練：**企業應定期舉辦網路安全培訓，提升員工對於潛在威脅的認識和應對能力。這不僅能降低內部安全風險，還能增強整體的安全防護意識。

（二） 提升網路安全技術應用的激勵方案：政府和產業應考慮引入更多的激勵措施，以促使企業投入到 DNSSEC 和 BGP 等安全技術的實施上。此外，通過產業協會推廣安全技術的標準化和工具化，也有助於降低技術實施的門檻，鼓勵中小企業參與，從而提升整體網路基礎設施的安全性。

（三） **關注技術趨勢，增強競爭力：**企業應持續關注技術趨勢，建立持續監測和評估新技術的機制，特別是在 5G 和物聯網領域。這樣可以及時調整策略，利用新技術提升業務效率和競爭力。

（四） **集中網路管理資源並優化頻寬體驗：**企業應優先部署集中化的網路管理系統，以合理分配網路資源。並且透過配置 QoS 來優化頻寬分配，確保串流媒體應用在高流量的環境下穩定運作，提升整體網路的使用效率和用戶體驗。

（五） 強化區域合作，提升網路自主性：太平洋地區的網路高度依賴美國和澳大利亞，應考慮引入更多區域性合作和投資，推動本地網路基礎設施的建設，促進本地營運商的參與，減少對其他國家和網路的依賴，提升該地區的網路自主性和安全性。

附錄、工作坊

此次工作方為期 4 天，開設 2 主題，分別是網路安全 Network Security 及網路自動化 Network Automation。在這 4 天的課程，結合理論及虛擬實驗室環境的方式，透過實際動手操作的方式，使參與者更能理解在實際環境中的應用。

一、 網路安全Network Security

網路安全是一個廣泛的主題，涉及終端用戶、應用程式和基礎設施等各方面。本次工作坊的目標是探討關於網路安全的關鍵概念、協定、政策和實踐，以保護資料和資產免受潛在攻擊或濫用，內容涵蓋網路基礎設施安全，如網路安全基礎、設備與基礎設施安全、封包分析、入侵偵測、DDoS 攻擊與對策、安全的網際網路路由、安全運作與監控等，特別是建立穩健的安全路由網路，同時也探討關於網路安全運作、常見的安全事件及漏洞，與對應的對策和緩解工具，並透過 Linux 虛擬實驗室進行操作演練。

（一）第 1 天主要研討「網絡安全基礎」、「密碼學」、「設備與基礎架構安全」及「BGP 劫持、洩漏偵測及預防」等 4 項主題之主要概念知識及相關應用。

1. 網絡安全基礎討論網絡安全的目的和目標，包含機密性、完整性和可用性，亦說明各種類型的安全威脅及風險，例如機會性攻擊、針對性攻擊、高級持續性威脅，及針對不同類型攻擊的具體防禦機制及措施，例如縱深防禦策略、風險評估矩陣。最後，針對網絡層攻擊詳細說明在不同 OSI 層上的各種攻擊方法，包括 L2 層的攻擊如 ARP 欺騙、DHCP 攻擊和 MAC 洪水攻擊，L3 層的攻擊如 ICMP 洪水攻擊，及應用層攻擊如 DNS 中毒和 SQL 注入。
2. 密碼學說明加密的定義、歷史發展及其不同形式，如對稱加密與非對稱加密及兩者的工作原理、優缺點及常用的加密算法，如

AES 和 RSA。另透過哈希函數和數位簽名講述加密哈希的作用、如何保護數據完整性，及使用數位簽名驗證數據來源的真實性；同時介紹針對加密的攻擊方法，例如彩虹表攻擊、暴力破解和哈希碰撞等，並討論對這些攻擊的防禦措施。

3. 設備與基礎架構安全教導設備存取控制，涵蓋實體層面接觸安全措施，例如鎖定伺服器機房、設置監控、保護便攜設備等，並針對基礎設備保護討論邏輯存取控制，包括密碼保護、關閉不需要的服務、SNMP 安全性和準確的 logging 日誌記錄，並透過提供保護管理功能（如 SSH、TFTP 和 NTP）存取的建議，限制接取與明確的權限設置來加強安全。最後針對封包過濾著重於說明封鎖惡意封包的過濾建議，包括阻止群播、廣播和偽造的封包，並建議使用多層安全防護、設置防火牆策略及根據 BCP38 進行入口過濾，以防止 IP 偽造。

4. BGP 劫持、洩漏偵測及預防說明對網路路由系統的基本認識、BGP 在路由決策中的功用、BGP 劫持之通常目的及重大或知名的 BGP 洩漏事件。

（二） 第 2 天主要研討「封包分析」、「Suricata 入侵偵測系統」、「日誌管理」等 3 項主題之主要概念知識及相關應用。

1. 封包分析先介紹網路協定概述，包含 OSI 和 TCP/IP，並說明 OSI 各層常見的協定，如 Ethernet、TCP、HTTP 等；並說明封包截取工具，如 tcpdump、Wireshark 和 TShark 的使用並提供使用範例和指令，及封包分析技術如使用特徵值分析偵測已知威脅模式，例如 IP 地址、標頭資訊，工作階段分析則用於理解通訊行為並識別異常。最後於虛擬實驗室環境練習多個協定檢查及分析，如分析 Telnet session、FTP 活動和秘密通道，及藉由真實範例和封包截取檔案作為實際操作。

2. Suricata 入侵偵測系統是由非營利組織管理的入侵偵測系統，

具備即時入侵偵測、網路安全監控及封包分析等功能，支援 JSON 格式輸出，且易於整合至各類安全工具。另於虛擬實驗室環境做各項分析練習，教導如何撰寫 Suricata 規則、使用不同協定的篩選條件如特定字串匹配、TLS 指紋檢測等，及建立基本警報規則的實作範例與進階簽名演練，同時透過 MISP 威脅情報共享平台的應用，示範如何將 MISP 事件轉換為 Suricata 規則，以進行威脅偵測。

3. 日誌管理介紹日誌、日誌管理的流程，及集中式日誌管理的重要性，並說明 Syslog 使用的常見埠、各等級的日誌嚴重性及日誌系統來源分類以識別 syslog 事件建立的過程（如核心訊息、郵件系統、NTP 子系統等）。另介紹常見的日誌伺服器工具，如 syslog-ng、Rsyslog、Graylog、Logstash、lnav 及每個工具的特點，及說明 ELK 堆疊與 Grafana Loki 等日誌分析及蒐集管理系統。

（三）第 3 天主要研討「流量監控」、「分散式阻斷服務攻擊（DDoS）及其防範措施」、「IPv6 安全基礎和相應的防護措施」、「IPv6 安全工具」及「IPv6 路由安全的關鍵技術與防護措施」等 5 項主題之主要概念知識及相關應用。

1. 流量監控主要內容包括網路流量分析的關鍵概念和工具、流量分析及封包分析，及 Cisco 開發用於收集 IP 流量數據，實現網路監控的協定 NetFlow 與進階流量監控工具 Flexible NetFlow，用戶可以自定義流量，以滿足特定的網路分析需求。另說明一款用於處理 NetFlow/sFlow 數據，支援過濾、IPv4/IPv6 和時間聚合的命令列工具 nfdump 和其圖形化前端且可提供流量視覺化、歷史數據分析、警示及外掛支援的 NfSen，及以 NetFlow/sFlow 數據紀錄產出流量圖，有助於網路營運商做出對等連接和容量規劃決策 AS-Stats 等工具。

2. 分散式阻斷服務攻擊及其防範措施說明 DoS 和 DDoS 的定義與影響、DDoS 攻擊的類型、DDoS 趨勢、反射與放大攻擊，及防禦策略包括網路配置調整 TCP/IP 設定、速率限制，並使用 SYN cookies、硬體解決方案如部署針對 DDoS 的過濾設備、服務保護使用負載平衡器、Web 應用防火牆(WAF)及基於雲端(Cloud-based)的 DDoS 過濾，以緩解攻擊影響及 Anycast 地理分佈式伺服器來分散影響等。
3. IPv6 安全基礎和相應的防護措施說明 IPv6 安全的重要性、常見的誤解、延伸標頭問題及威脅、ICMPv6 的重要性、NDP 攻擊及防禦工具、路由標頭及 IPv6 地址攻擊等。
4. IPv6 安全工具概述 IPv6 網路掃描工具如 Nmap、Masscan、Fi6s、Scan6 等，及 IPv6 攻擊工具套件、攻擊類型與測試，並於虛擬實驗室環境練習工具的實際操作，利用 THC-IPv6 進行防火牆測試、使用 Chiron 發送路由廣告消息、實施中間人攻擊（Man-in-the-Middle attacks），及使用 Scapy 自行構建 IPv6 封包以進行精確的協議測試。
5. IPv6 路由安全的關鍵技術與防護措施說明 ICMPv6 過濾、過濾過渡技術、BGP 路由過濾、Bogons 過濾、IPv6 DDoS 緩解、RTBH（Remote Triggered Black Hole）過濾、uRPF（Unicast Reverse Path Forwarding)及 ROV 過濾。

（四） 第 4 天主要研討「資源公鑰基礎架構」、「DNS 安全」、「DNSSEC」、「漏洞評估和滲透測試」及「蜜罐和蜜網」等 5 項主題之主要概念知識及相關應用。

1. 資源公鑰基礎架構（RPKI）列舉多個 BGP 路由劫持和洩漏事件，展示了不正確的路由配置可能造成的影響，及說明路由安全挑戰、RPKI 的信任鏈、ROA 和 ROV 驗證、RPKI 操作模式、RPKI 驗證的路由器配置及 RPKI 發展與改進。

2. DNS 安全簡要介紹對稱加密 AES、3DES 和非對稱加密 RSA、DSA 的基礎、DNS 協議的安全漏洞、DNS Spoofing 與快取污染、基於 DNS 的惡意軟體活動、DNS DDoS 攻擊與放大攻擊、加密的 DNS 傳輸協議及基本的 DNS 安全實踐包括定期更新 DNS 軟體、限制查詢、隨機化來源端口、啟用交易簽名(Transaction Signature,TSIG)和 DNSSEC 以防止未授權的區域轉移和資料偽造，與 DNS 交易安全；並於虛擬實驗室環境練習操作 DNS 的基本安全措施，包括對 TLD、SLD 區域和公共/私人解析器的管理，並引入多層冗餘和地理分佈，以確保 DNS 韌性和服務可用性。

3. DNSSEC 概述了 DNSSEC 的目的，即透過數位簽名 DNS 資料來保護數據的完整性，及其工作原理技術與資源記錄、DNSSEC 密鑰類型（ZSK 和 KSK）、其角色、密鑰生成、存儲以及密鑰輪替過程與 DNSSEC 驗證、佈署和工具。

4. 漏洞評估和滲透測試介紹滲透測試的目的、滲透測試範疇和法律問題、滲透測試報告、定期測試及多種安全工具和措施如 NMAP、SPARTA、OpenVAS、Nikto、Metasploit 等，並於虛擬實驗室環境練習操作提供每個工具的命令行操作步驟和範例，包括使用 NMAP 的 TCP 和 UDP 掃描、版本偵測、輸出格式，如何在 Metasploit 中搜索漏洞模組並利用等操作指引。

5. 蜜罐（Honeypots）和蜜網（Honeynet）主要概述歷史背景、蜜罐的目的、蜜罐和蜜網的類型、蜜罐技術的核心主題－檢測及欺騙、蜜令（Honeytokens）及常用的蜜罐軟體，並透過虛擬實驗室環境練習操作設置蜜罐和蜜網時需考慮的位置、目標和相應輔助工具及 APNIC 社區蜜網專案的應用情況。

二、 網路自動化 Network Automation

網路自動化是希望設計能自動修復的網路，或至少收集資料進行調查、嘗試修復及報告問題的網路，使工程師能將時間花在打造

更穩定的網路或計算機無法解決的問題上。本次工作坊是實作學習 Salt 的開放原始碼遠端執行架構，內容包括主節點及部屬節點的配置管理、如何利用主節點發出執行指令、建立主節點及部屬節點之事件程序通訊系統等。