出國報告（出國類別：開會）

2019年亞太網路資訊中心國際會議（APNIC48）

服務機關：國家通訊傳播委員會
姓名職稱：楊分析師啟仁
吳技士奕慶
劉科員楚慧
派赴國家：泰國
出國期間：**108**年**9**月**9**日至**108**年**9**月**13**日
報告日期：**108**年**12**月**5**日

摘要

亞太網路資訊中心（APNIC, Asia Pacific Network Information Centre）為掌管亞太地區網際網路位址分配之非政府國際組織機構（NGO），1993年於澳洲成立，亦是全球五大區域性網際網路註冊管理（RIR）機構之一。APNIC 主要負責網際網路資源（IP 位址和 AS 號碼）的管理、分配，以及網際網路 Whois 查詢資料庫之系統維護；亦積極參與亞太地區網際網路基礎設施發展，包括提供網際網路相關技術之培訓講習，支持 DNS 根伺服器部署等技術活動，並與其他地區和國際組織合作。其會員包括網際網路服務提供者（ISP, Internet Service Provider）、網路位址及網域名稱註冊管理機構、學界與政府研究單位等。

為廣納會員對於 IP 位址及 AS 號碼相關政策之意見，同時進行網路管理相關技術交流，APNIC 每年至少舉行 2 次國際會議，約每半年舉辦一次，並由各會員國輪流舉辦，年度第一次會議通常與亞太地區網際網路營運技術大會（APRICOT）合辦，第二次會議則由 APNIC 單獨舉辦。此次會議係第 48 屆，包括全球各地網際網路工作者、專家學者、政府代表、產業代表等超過 20 個經濟體及 422 名以上人員參與。本會本次參與為期 **3** 天的研討會，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。

本次會議研討內容主要包括亞太地區各 NIR 現況、網路管轄權、IPv6 發展、RPKI 推動、資訊安全以及其他網路安全相關議題，不僅將臺灣在 IP 位址發放、IPv6、RPKI 等推動情形讓其他國家瞭解，同時也藉由各場次演講，掌握目前 IP 位址與 AS 號碼相關技術發展趨勢以及亞太主要國家發展現況，皆有助於本會制定網際網路相關監理政策。

目錄

壹、前言 1
貳、行程安排 2
參、APNIC48會議 3
（一） 第一日（9月10日星期二） 4
（二） 第二日（9月11日星期三） 4
（三） 第三日（9月12日星期四） 5
肆、會議過程及摘要 6
一、 第一日會議摘要 6
（一） 合作論壇（Coperation SIG） 6
（二） 開幕式和全體會議（Opening Ceremony & Keynotes） 9
（三） 邊境閘道器協定 11
（四） 國家級網際網路位址註冊機構論壇（NIR SIG） 13
（五） 路由安全（Routing Security） 15
（六） APNIC產品與服務（APNIC Products & Services） 16
二、 第二日會議摘要 18
（一） APNIC-資安事件應變及安全小組論壇（APNIC-FIRST Security） 18
（二） IPv6部署（IPv6 Deployment） 23
（三） 專為5G設計之IP傳輸線路（Designing the IP transport network for 5G） 25
（四） 資源公鑰基礎設施（RPKI） 26
三、 第三日會議摘要 28
（一） APNIC開放政策會議（Policy SIG） 28
（二） 分段路由（Segment Routing） 29
（三） 網路地圖集（Atlas of the Internet - Creating geographical maps with RIPE Atlas data） 31
（四） APNIC年度全體成員會議（AMM） 34
伍、心得與建議 36

壹、前言

亞太網路資訊中心（APINC, Asia Pacific Network Information Centre）1993 年於澳洲成立，為亞太地區網際網路位址分配之非政府國際組織機構（NGO），與 RIPE（歐洲）、ARIN（美洲），LACNIC（拉丁美洲），AFRINIC（非洲）並列全球五大區域性網際網路註冊管理（RIR）機構。APNIC 主要負責網際網路資源（IP 位址和 AS 號碼）的管理、分配與網際網路域名及位址 Whois 查詢資料庫之系統維護，也積極參與亞太地區網際網路基礎設施發展，包括提供網際網路相關技術之培訓講習，支持 DNS 根伺服器部署等技術活動，並與其他地區和國際組織合作。其會員包括網際網路服務提供者（ISP, Internet Service Provider）、網路位址及網域名稱註冊管理機構、學界與政府研究單位等。

為廣納會員對於 IP 位址及 AS 號碼相關政策之意見，APNIC 每年至少舉行 2 次國際會議，約每半年舉辦一次，並由各會員國輪流舉辦，以供各界針對亞太地區 IP 位址及 AS 號碼資源相關技術及政策進行交流。同時也藉由相關管理政策提案的公開討論，讓與會會員對於 IP 位址及 AS 號碼資源管理政策達成共識，並進一步制訂相關政策。

此次會議係第 48 屆，包括全球各地網際網路工作者、專家學者、政府代表、產業代表等超過 20 個經濟體及 422 名以上人員參與。本會本次參與為期 **3** 天的研討會，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。

圖 1 大會 LOGO

貳、行程安排

一、 出國時間：108 年 9 月 9 日至 108 年 9 月 13 日

二、 地點：泰國清邁

三、 本會出席人員：

（一）楊分析師啟仁

（二）吳技士奕慶

（三）劉科員楚慧

四、 時程安排暨航班表

日 期	時程安排
9月9日(一)	長榮航空(BR257) 07:25 出發：臺灣桃園國際機場 10:25 抵達：清邁國際機場
9月10日(二) ~ 9月12日(四)	出席亞太網路資訊中心 48th 論壇活動
9月13日(五)	長榮航空(BR258) 11:30 出發：清邁國際機場 16:35 抵達：臺灣桃園國際機場

參、APNIC48 會議

一、會議時間：2019年9月10至12日

二、會議地點：泰國清邁艾美酒店（Le Meridien Chiang Mai）

圖2 會場

圖3 會議地點

三、 會議議程：

（一）第一日（9 月 10 日星期二）

時間	議程	
09:00	**Cooperation SIG** 09:00 to 10:30	**Newcomers session** 09:00 to 10:30
11:00	**Opening ceremony and keynotes** 11:00 to 12:30	
14:00	**Technical Session 1** 14:00 to 15:30	**NIR SIG** 14:00 to 15:30
16:00	**Technical Session 2** 16:00 to 17:30	**APNIC Products & Services** 16:00 to 17:30
17:30	**NextGen Careers BoF** 17:30 to 18:30	**APNIC Community Trainers BoF** 17:30 to 18:30
19:00	**Opening Reception** 19:00 to 21:00	

（二）第二日（9 月 11 日星期三）

時間	議程	
09:00	**APNIC - FIRST Security** 09:00 to 10:30	**IPv6 Deployment** 09:00 to 10:30
11:00	**APNIC - FIRST Security** 11:00 to 12:30	**Technical Session 3** 11:00 to 12:30
12:30	**Women in ICT Lunch** 12:30 to 14:00	**Lunch** 12:30 to 14:00
14:00	**APNIC - FIRST Security** 14:00 to 15:30	**RPKI - Industry Trends and Initiatives** 14:00 to 15:30
16:00	**APNIC - FIRST Security** 16:00 to 17:30	**Lessons learned from RPKI Deployments** 16:00 to 17:30
17:30	**RPKI BoF** 17:30 to 18:30	
18:30	**Meet the APNIC EC Cocktail** 18:30 to 19:00	
19:00	**ROA signing Social** 19:00 to 21:00	

（三）第三日（9 月 12 日星期四）

時間	議程	
09:00	**Policy SIG 1** 09:00 to 10:30	**Tutorial: Segment Routing** 09:00 to 10:30
11:00	**Policy SIG 2** 11:00 to 12:30	**Tutorial: Atlas of the Internet - Creating geographical maps with RIPE Atlas data** 11:00 to 12:30
12:30	**Lunch** 12:30 to 14:00	
14:00	**AMM 1** 14:00 to 15:30	
16:00	**AMM 2** 16:00 to 17:30	
18:30	**Closing Dinner** 18:30 to 21:00	

肆、會議過程及摘要

一、第一日會議摘要

（一）合作論壇（Coperation SIG）

此場次主持人為 TWNIC 副執行長丁綺萍、共同主持人為來自尼泊爾的 Bikram Shrestha，並邀請臺灣律師詹婷怡、緬甸學者 Mie Mie Su Thwin、韓國學者 Eun Chang Choi 就網路司法主題，討論網路管轄權及進行意見交流座談。

詹婷怡以「Internet Jurisdiction Emerging Issues and Way Forward」為主題談到，網際網路的過去重點在於硬體環境及技術創新，從現在起，政策、規範及治理將成為核心。如今的網路已跨國界，然而司法系統仍以領土為界。她提到未來將面對更加複雜極具爭議性的情況，包括來自全球數位經濟、網路人權及網路安全等層面。同時，她也提到國際網路犯罪及網路司法案例，像是瑞典 Pirate Bay 網站、twitter、太空人 Anne McClain、中國大陸網路長城網路犯罪或網路司法事件。

圖 4 跨國網路管轄架構

（資料來源：講者簡報）

她認為網路是跨國界媒介，非單一官方組織所能治理，每個國家的網路規管政策也各有不同，沒有放諸四海皆準的解決方案。同時，詹律師比較各個網路政策發展組織的特色，認為網路治理生態包括政府政策規範、ISP 協定、使用者的學習教育狀況、跨界協議、多方利益關係人的網路治理等。

characteristics	ICANN	ITU	IGF	APNIC	IETF	NATO
multistakeholder	x		x	x		
bottom-up model of governance	x		x	x	x	
standard setting	x	x		x	x	
operates based on contractual compliance	x			x		
governmental		x				x
sets internationally enforceable obligations for states		x				x

圖 5 各相關國際組織特色

（資料來源：講者簡報）

Eun Chang Choi 的講題為「IP Address and Cross-border Cooperation for Resolving the Cyber Attribution Challenge」，探討 IP 位址與網路司法的關係以及網路犯罪該如何歸責。在網路世界中，每個人都是一組號碼，也就是 IP 位址，但仍有人透過不同方式迴避 IP 位址追蹤，像是近年來常見的偽裝 IP 及偽裝所在地點這類的 IP 位址欺騙（IP spoofing），另外也有 DNS 欺騙（DNS spoofing）。

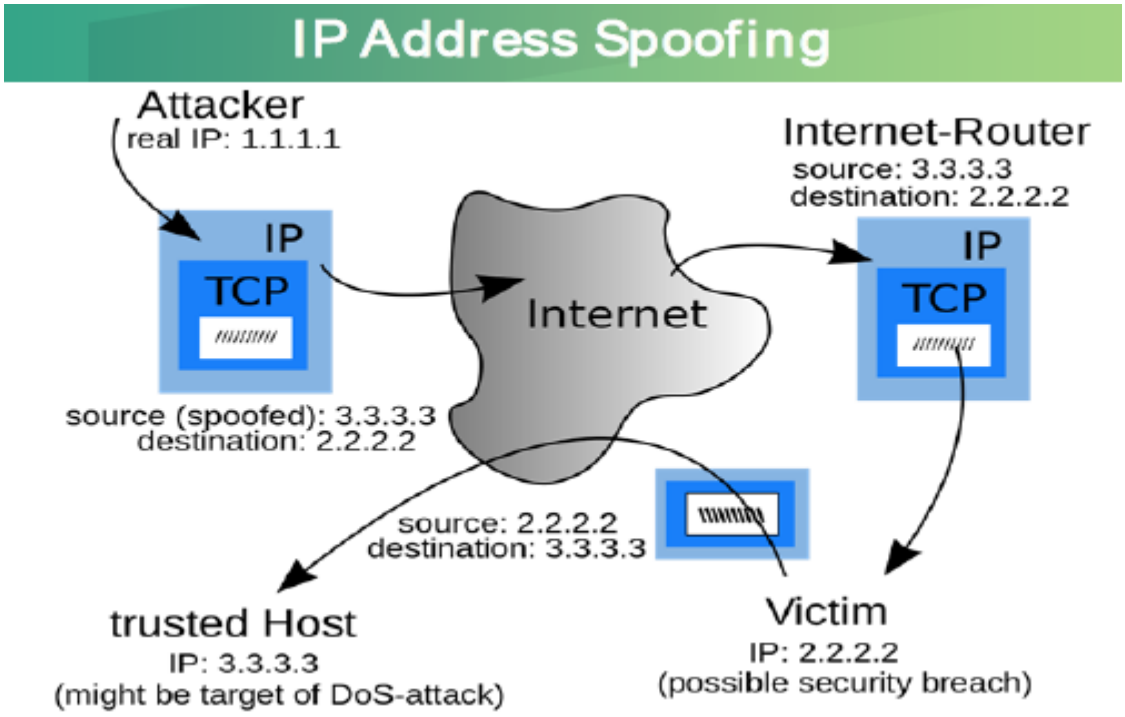

圖 6 IP 位址欺騙途徑說明

（資料來源：講者簡報）

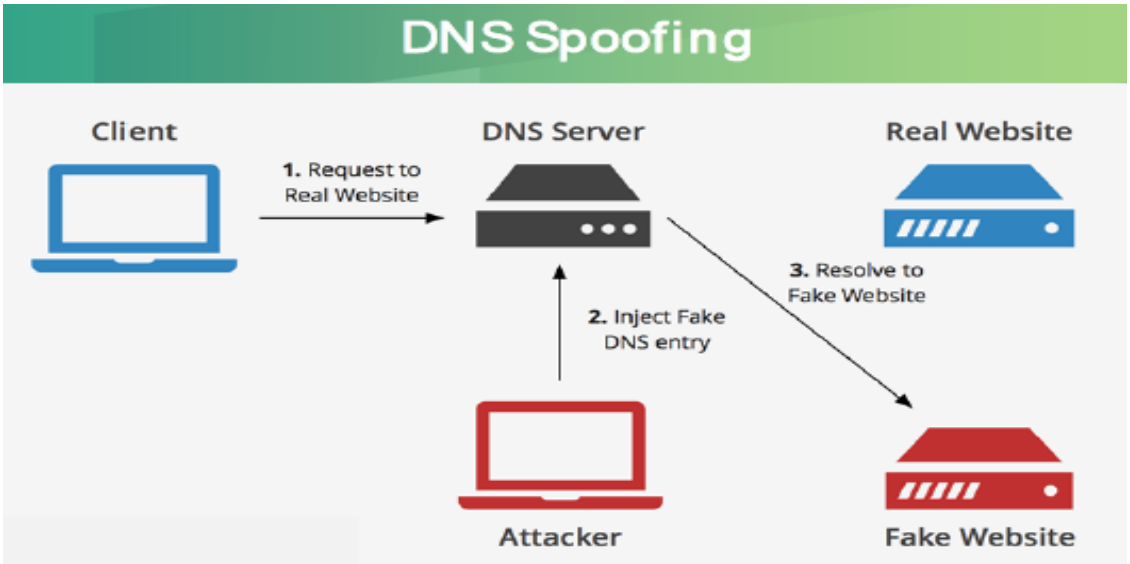

圖 7 DNS 位址欺騙途徑說明

（資料來源：講者簡報）

他談到網路歸責並非易事，原因包括無法追蹤的 IP 位址、缺乏司法調查權等，必須藉由多方利益關係人的合作才能達成，在亞太地區就透過各地 CERT(Computer Emergency Response Tam)，跨越國界進行合作。但 IP 位址無法和犯罪者或非法行動完全正確連結，仍是網路歸責的一大挑戰。

緬甸學者 Mie Mie Su Thwin 以「Educating Netiquettes, Skill, Moral and Awareness Developments of Myanmar」為題，從網路倫理教育角度來談網路司法，她認為具有網路倫理與規範的認知，對於網路司法有所幫助，網路禮儀在網際網路空間也具有重要地位。

她首先談到網路議題來自於法律、環境、文化以及倫理各層面，近來較熱門的像是著作權保護、文本誤用、資訊誤導、網路騷擾等。並提到緬甸如何透過不同階段，以課程、研討會、論壇、等方式，對學生教導、大眾宣導，以導入網路禮儀認知與技巧教育，最後達到具備網路隱私權及資安概念。

圖 8 各階段所需具備的網路認知

（資料來源：講者簡報）

Bikram Shrestha 以「Internet and Jurisdiction: Nepali Perspective」為題，分享尼泊爾的網路司法經驗。他談到，尼泊爾在 2006 年實施電子交易法案，這也是尼泊爾第一個論及 ICT 犯罪境外司法的法律，他認為網路司法非常複雜，可能不是一個國家所能處理，而必須採取相互合作的方式，同時他也分享尼泊爾政府和澳洲、紐西蘭的相關合作經驗。

（二）開幕式和全體會議（Opening Ceremony & Keynotes）

APNIC 48 開幕式首先由 APNIC EC 主席 Gaurab Raj Upadhaya 致歡迎詞，之後再由泰國相關單位代表 Air Marshal Dr. Thanapant Raicharoen、Kanchana Kanchanasut、Morragot Kulatumyotin 以及 APNIC 董事會執行長 Paul Wilson 依序致詞。

在開幕式中，也邀請 2 位專家進行專題演講。第一位是 Narelle Wakely，目前是 Trustwave 首席安全顧問，第二位是 Job Snijders，目前在 NTT 擔任 IP 發展工程師。

- 專題演講 1：團隊合作完成不可能的任務

Narelle Wakely 以 2018 年在澳洲舉辦的大英國協運動會（Commonwealth Games 2018）為例，她認為，2018 年的大英國協運動會向全球 3,500 個媒體轉播 2,213 個小時 HD 賽事畫面，在 2 週內共傳輸 106TB 資料量，若以科技角度來看，堪稱是有史以來最「科技連結」的運動賽事。然而這樣的大型賽事也容易成為網路犯罪的目標，因此她針對賽事進行中資安所扮演的角色，以及遇到的挑戰、解決方式進行分享，她也提到，這必須有賴廣大安全合作體系才成功。

圖 9 GC2018 創下的里程碑

（資料來源：講者簡報）

她談到，網路安全不再只是 IT 基礎建設的一部份，而是整體企業運作的一部份，必須落實到組織運作。國際賽事的資安不單單只是技術，也牽涉到國際政治發展現況等因素。因此第一必須進行演練，最好以全球正發生的事件為情境，重要的是要納入資安團隊、政府團隊、運作團隊等，讓每個人瞭解各自的角色及任。第二是必須視覺化，將所有狀況圖示化畫出，這對於團隊溝通非常有幫助。最後，她也強調嚴重漏洞與風險管理，將網路資安視為企業風險層級，並藉由資安架構藍圖的繪製，能夠清楚串連每個層面，當某個漏洞或意外事件發生時，能夠立即知道影響環節，進一步迅速處理危機。

- 專題演講 2：朝更強健的網路發展

現今網際網路流量控制工程所遭遇到困境為在特定的地點傳遞網路流量的路徑選擇及頻寬為有限，以及該組織或企業無法聘僱網路專職人員。大部分的公司往往只能使用付費軟體去增進網路傳輸效能、降低營運成本並達成 24 小時監視網路狀態。這些軟體如 BGP 優化器（BGP optimizer）偵測現有的路徑的流量來決定傳輸路徑，以達成平衡負載流量（balance traffic）。藉著發布「假的」特定路由資訊以達成控制網路流量經由特定路徑的目的（如網路分流），這樣的手段看似相當合理，但「假的」特定路由資訊可能造成路由迴圈（routing loop），影響的層面不僅僅只存在於 BGP optimizer 的使用者，而是全球網際網路使用者。

Job Snijders 提出兩個建議來解決前述 BGP optimizer 所產生的問題：1.建立路由源授權（RPKI ROA states），用以宣告己身的在網路中的存在，以利他人判斷是否為合法的路由宣告。2.使用 BGP 路由來源驗證，可以降低接受錯誤路由資訊資之機會。為檢視使用路由來源驗證(origin validation)前後對於所在網域的流量上的影響，Job Snijders 建議可使用 pmacct 及 kentik 開源程式（open source code）來協助檢視。

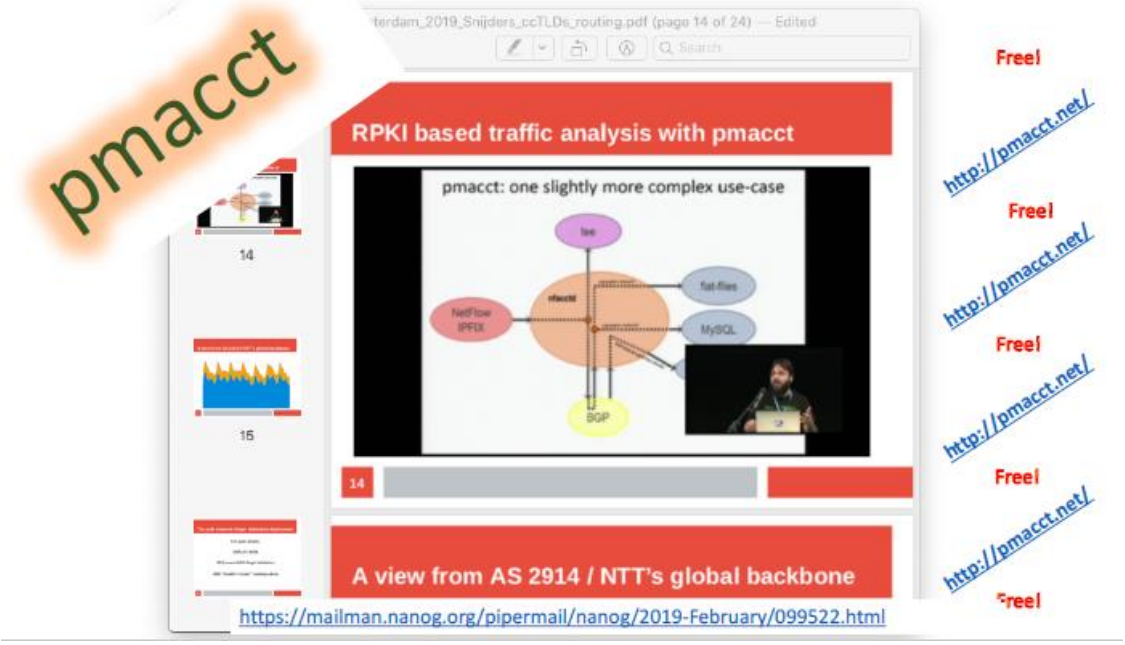

圖 10 pmacct 開源程式

（資料來源：講者簡報）

https://www.kentik.com/blog/bgp-and-rpki-a-path-made-clear-with-kentik/

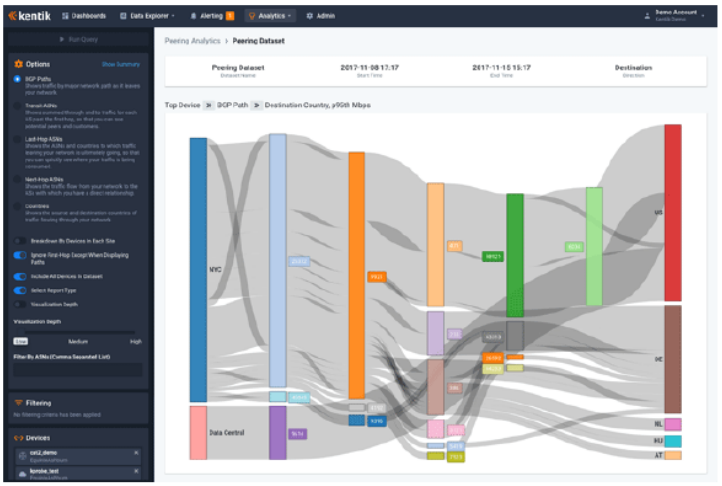

圖 11 kentik 開源程式

（資料來源：講者簡報）

（三）邊境閘道器協定

- 網際網路的背景雜訊

一個網路中的主機除了收到社群中想要的封包資訊，其他的封包資訊稱為網際網路的背景雜訊。從封包來源種類針對雜訊來源來加以分類：封包發起端（initiator）有掃描行為、病毒傳播、網路攻擊及其他錯誤設定等所造成的；另有反射端（reflector）將偽裝其他的 IP 封包送至目的裝置或錯誤設定所造成的。

為了進行本研究，由 AS2522 宣告其 Prefix 並開始接收封包，並對其進行觀察及丟棄，並將其觀察的結果加以分類，但僅能推測其傳送封包的意圖像是裝置掃描，反射端的傳送封包，錯誤的網路實現等等，上述成因並無法加以驗證。本次實驗於 24 小時內將針對其宣告的 prefix 所收到的封包共計約六億個，平均來說，相當於一個主機每天收到 2758 個封包。所收到的封包 95%為 TCP,4%為 UDP,1%為 ICMP,IPv6 低於 1%。其中上述 TCP 的封包 98%為了開始 TCP 服務所做的 TCP 同步（TCP SYN），2%為 TCP 服務確認（TCP ACK），該類可能包含被攻擊者所送的封包，其餘為少量的其他用途之封包。令人感興趣的是，大約有一百萬的發送者（sender）僅發送不到 10 個封包，但有非常少數的主機（host）卻送出數億個封包。

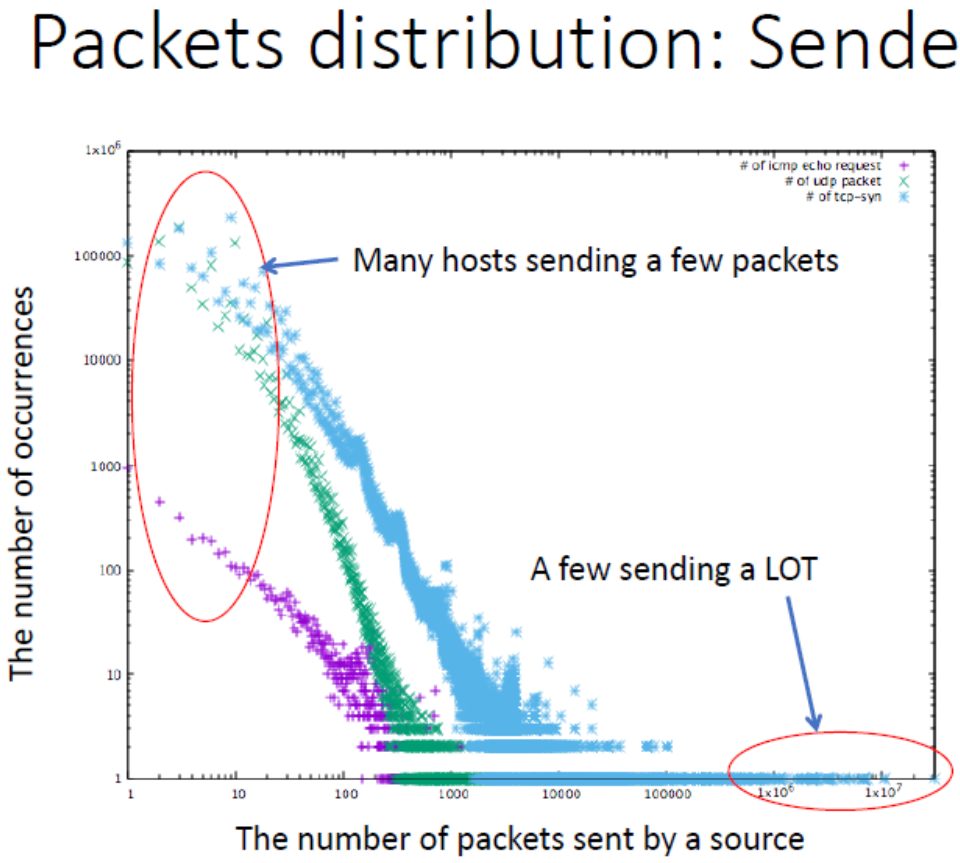

圖 12 發送者的封包分布

（資料來源：講者簡報）

網路安全服務業者（security service providers）透過設置於全世界的主機發送連接埠 23 的掃描封包並提供服務，換言之，我們使用越多的服務卻使得我們收到越來越多的垃圾封包。而少量封包發送者有些是為點對點（Peer-to-peer）軟體如 BitTorrent，為了連接點對點網路進而開啟所需的服務所送的封包，即便網路中並無使用其服務，推測可能網路節點設置錯誤或者遭受到網路攻擊所致。

透過分析這些發送大量發包者，是網路安全服務業者（security service providers），透過某些地區的 IP 在進行 TCP 掃描特定或是否一範圍內的連接埠，但掃描的連接埠並沒有包含道常用的 TCP23 連接埠（TCP Port 23）。

- BGP 異常偵測

講者提出的建構可能分析的方式有三種：

1. 建立分析系統規則；用所建立的規則下去偵測，但何者是正常和何者是異常活動規則難以建立，因為每一個人對於正常的定義不同。
2. 建立自我學習能力之機器系統：建立具有 n 維參數之機器自我學習系統，設定系統參數如 IP prefex 的長度（length），AS 的長度等等，並且使用集群分析（Cluster Analysis）工具，理論上來說即可區別出 BGP 的正常行為與異常行為區分出來；惟在 BGP 中異常行為往往是依附在其正常的運作而難以區分，使的自我學習能力之機器系統往往無法將其異常運作區分出來。

3. 試探式（HEURISTIC）分析法：將 BGP 更新資訊輸入分析程式，並使用臨界值（thresholds）去篩選出可能異常之情形。

BGP 是個耗費時間的協定，透過自治系統(AS)的 BGP 宣告，其資訊將從鄰近的 AS 慢慢傳遞擴散出去，系統進而收斂而建立整個路由路路徑，而非透過直接運算的方式來進行，因此在 BGP 中的暫態數量是相當多的，這暗示著欲從如此高度的 BGP 更新當中偵測出異常運作仍是極大的挑戰。

一般來說，BGP 是為了封包傳遞資訊以及特定路徑的封包傳遞（traffic engineering），而 BGP 更新是在此通訊協定下的產物以及為了新網段連接，因此了解日常 BGP 更新的成因有助於篩選異常事件的發生。透過分析每日的 BGP 更新數目發現，BGP 的更新資訊往往是重複之前舊有的資訊，僅有非常少數新的更新資訊。利用這些少量更新資料來當作篩選 BGP 異常運作的重要指標。除上述的指標外，對於每個 AS 來說，可分析每個 AS 與其相鄰的 AS 上下游關係，以及利用地理位置去對應每個 Prefix 及來源 AS，並配合 ROA(路由來源授權)狀態來處理 BGP 的更新資料，講者僅知道這些原則有助於分析此問題，但是要如何實行上有困難待克服。

BGP 更新資料處理後，講者預期令人感興趣的事件如下：

1. AS 路徑包含「山谷」（Valley），即 AS 路徑從本身的 AS 經過上游的 AS 再回到自己本身，這意味著路由洩漏（route leak）。
2. AS 路徑包含不尋常之處。
3. 之前未出現過的 Prefix。
4. 之前未出現過的 AS。
5. Prefix 的地理位置散佈在多個經濟體當中是不太合理的。
6. Prefix 的地理位置與其 AS 所在的地理位置不同亦不合理 。
7. 短時間（幾小時或者更短)的宣告資訊是可疑的,因為資訊更新後所造成的影響,會有人去修正他(例如路由路徑劫持）。

（四）國家級網際網路位址註冊機構論壇（NIR SIG）

NIG SIG 目的在於讓各國網際網路註冊機構能夠彼此分享營運、政策及相關技術佈建現況，藉此促進各註冊機構與 APNIC 秘書處間的緊密合作。本次先進行 Co-Chair 改選，由中國大陸 CNNIC 營運經理 Zhen Yu 當選。接著由由韓國 KISA 的 Billy MH Cheon 擔任主持人，陸續由中國大陸（CNNIC）、臺灣（TWNIC）、越南（VINNIC）、韓國（KISA）、日本（JPNIC）、印尼（APJII）、印度（IRINN），針對 IP 及 AS 資源核配、舉辦 IP 相關研討會及 IPv6 教育訓練等現況進行說明。

1. 中國大陸

2019 年，中國大陸網際網路用戶達 8 億 5,400 萬人，普及率為 61%；行動網際網路用戶達 8 億 4,700 萬人，占全體網際網路用戶 99%。截至 2019 年 8 月，CNNIC 的 IP 會員數為 1,399。CNNIC 的 IPv4 位址核發總數為 331,880 個/24、IPv6 位址核發總數為 16,126 個/32，ASN 核發總數為 1,013 個。

中國大陸在今年 6 月也舉辦 IP 聯合研討會，也在 7 月、11 月舉辦與 IPv6、RPKI 相關的 2 至 3 天訓練課程。在 IPv6 發展上，截至 2019 年 8 月，中國大陸擁有 47,544/32 個 IPv6 位址，占全球分配的 17%；同時，具有 244 個 IPv6 ASN。目前中國大陸在 30 個省分皆進行 LTE 網路的 IPv6 升級；在使用者方面，中國電信、中國移動、中國聯通等電信業者在行動 LTE 與固網寬頻上已提供超過 10 億個用戶 IPv6 地址服務。

2. 臺灣

目前 TWNIC IP 會員數為 282 個，其中服務型態以 Co-location/IDC 居多，為 64 個，其次為 Cable Modem，25 個。TWNIC 的 IPv4 位址核發總數為 132,578 個/24、IPv6 位址核發總數為 2,502 個/32，大多數 TWNIC 會員已經擁有 IPv6 位址。同時，截至 2019 年 9 月，臺灣 IPv6 使用者可用率達 39%。

TWNIC 在今年 6 月 20 舉辦第 32 屆 TWNIC IP 政策資源管理會議，在教育訓練上，以 IPv6 和 RPKI 為主題，包括 5 月舉辦 IPv6 教育訓練、4 場 RPKI 教育訓練（自 2018 年 12 月至 2019 年 7 月）。在 RPKI 服務推動上，若依路由比數統計，目前 IPv4 Valid Prefix 比例達 90.1%、IPv6 Valid Prefix 比例達 95.2%。

3. 越南

越南近年積極發展 IPv6，2009 年成立推動計畫 VNIPv6TF，2017 年越南 IPv6 採用率為 10%，2018 年底迅速成長至 25.58%，到了 2019 年 9 月已達 39%，排名全球第 8，IPv6 使用者約 2,100 萬人。同時，越南也透過教育訓練課程培養 IPv6 相關人才以及透過 RPKI 工作坊，推動 RPKI。在 IP 位址核發上，截 2019 年至 8 月底，VNNIC 的 IPv4 位址核發總數為 15.621 blocks/22， IPv6 位址核發總數為 72 block/32 及 108 blocks/48。

4. 韓國

目前 KRNIC IP 會員共 277 個、ASN 會員共 693 個。截至 2019 年 6 月 30 日，KRNIC 已經核發 IPv4 位址 112,404,224 個、IPv6 位址已核發 5,253/32 個，ASN 則核配 1,005 個。同時在 2019 年 8 月針對 APNIC 和 KISA 間的 API 進行測試，也預計在 2019 年第 4 季完成網路位址管理系統的轉換。

5. 日本

JPNIC 具有 449 個 IP 會員，其中以東京最多，截至 2019 年 8 月，IPv4 核發數為 391,819/24 個、IPv6 核發數為 7,268/32 個，其中有 65%IP 會員已經核發 IPv6 位址，而 JPNIC 的 ASN 數則為 615 個。。JPNIC 積極推動 IPv6，舉辦多場 IPv6 相關活動，包括針對初學者或非技術背景人士的研討會、針對技術人員的工作坊，同時也與其他組織合作，分享 IPv6 佈建現況。在 RPKI 推動上，IPv4 涵蓋率為 9.1%、IPv6 涵蓋率為 56.8%，同樣也透過舉辦訓練課程持續推廣 RPKI。此外，JPNIC 也舉辦資源管理會議，並形成提議於 APNIC 提出。

6. 印尼

目前 IDNIC-APJII 具有 1,720 個會員，IPv4 核發數超過 2 萬 2,000 個、IPv6 核發數超過 2,200 萬個 block/48、ASN 個數達 776 個。目前部分 IDNIC-APJII 會員已經開始導入 ROA 和 RPKI，同時 IDNIC-APJII 也建置 MyIDNIC 會員及資源管理系統，提供會員使用，包括會員專屬入口平臺、資源維護系統等功能。

7. 印度

IRINN 目前 IPv4 核發數為 10,883,584 個、IPv6 核發數為 6,073,440,256/56 個、ASN 個數則為 1,935。印度在 IPv6 的推動非常積極，大部分的電信業者已經開啟 IPv6，印度在全球國家中的 IPv6 採用率也名列前茅，IPv6 比例達 68.94%。

（五）路由安全（Routing Security）

網際網路是由許多個自治網路（autonomous network）所建構的，目前約有 65,000 個，並透過邊境閘道協定（BGP）來達成路由資訊傳遞，以確保整個網路的連接性。

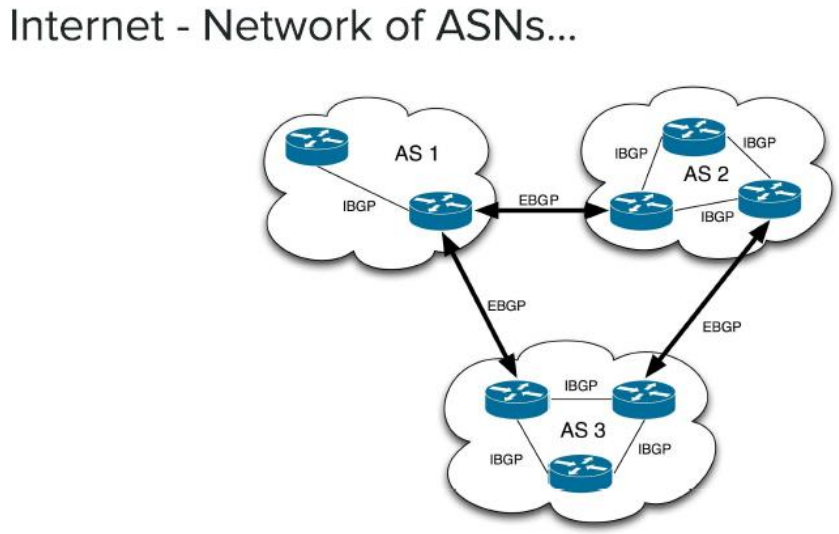

圖 13 自治網路系統構成的網際網路

（資料來源：講者簡報）

大約是 15 個自治系統 AS（autonomous system）所構成的 default free zone，使得這世界約 65k 的自治網路可以透過下游關係（downstream relationship）或者是他的 peer 的關係已達成整個網路的互聯（reachability），惟現今大部分的網路流量只經過有限個 AS。BGP 要如何信賴別人所發布的路由資訊呢?BGP 可以根據 IP 前綴（IP prefix）、AS 號碼（AS number）及 AS 路徑（AS path）等來選擇拒絕或者接受別人所發布的路由資訊。基本上 BGP 對於與其 AS 相連接的 AS 比較容易去判別其所發佈的路由資訊的正確性，離其越遠越（無直接連接），則越不容易判斷。因此為了幫助 BGP 篩選有用的資訊，網際網路路由登記（IRR, Internet routing registry）及資源公鑰基礎建設（RPKI, Resource Public Key Infrastructure）是個普遍良好的選擇。若欲宣告 IP 前綴，首先要建立路由物件及來源 AS（origin AS）及 AS 集合（AS set） 等相關描述，供後續 BGP 作為篩選路由資訊的依據，而常用的 IRR 的軟體工具經常利用到世界最大的路由資源資料庫（RADb, Routing Assets Database），除了本身的資料外亦包含 IRR 的鏡像資料庫，以供大眾使用。目前主要的 25 個 IRR 是由區域網際網路註冊管理機構（如 APNIC、RIPE NCC 等）所維護管理。根據 IRR 統計資料，現今全球計有 758313 Prefixes，其中的 79.54% 擁有有效的路由物件，7.73%擁有無效的路由物件，其餘的 12.73%Prefix 與路由物件無法匹配，因此根據 IRR 來篩選路由資訊約可達 20%。以網際網路路由登記為

基礎篩選路由物件需仰賴 IRR 的正確性，惟 IRR 資料老舊龐大更新與路由器不易整合，故維持 IRR 資料正確性將是未來的一大挑戰。

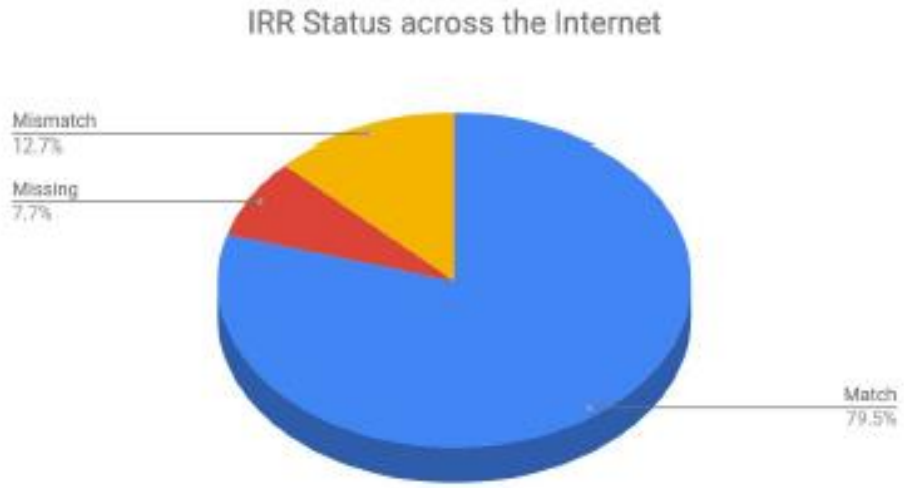

圖 14 IRR 統計資料

（資料來源：講者簡報）

（六）APNIC 產品與服務（APNIC Products & Services）

本場次主題為 Advanced Active Directory Attack & Defense Technique，由 Anton Strydom（APNIC Product Development Director）主持，介紹 APNIC 產品及服務，內容摘要如下：

- Internet Directory

提供基於 APNIC 每日產生的統計資訊作動態可視化的展示。它可以快速提供有關 IPv4，IPv6 和 ASN 配發和使用的資訊。圖表可以按子區域或經濟體查詢，並可以下載或嵌入於網頁中。

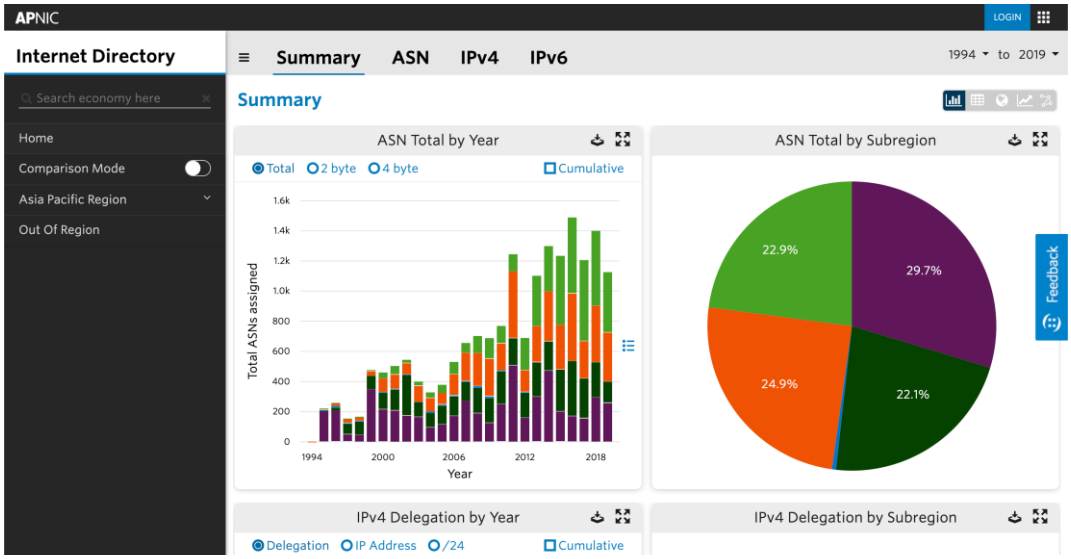

圖 15 Internet Directory

（資料來源：講者簡報）

- 自治系統健康儀表板（Dashboard for Autonomous System Health，DASH）

利用 APNIC 社群蜜網（Honeynet）計畫，允許用戶查看是否有任何惡意流量來自他們管理的前綴。這些訊息使他們能夠減輕攻擊並在將來阻止攻擊。目前，在 MVP（Minimum Viable Product，最小可行產品）階段，該工具可檢測 SSH 攻擊，並將在未來擴展到其他攻擊類型。

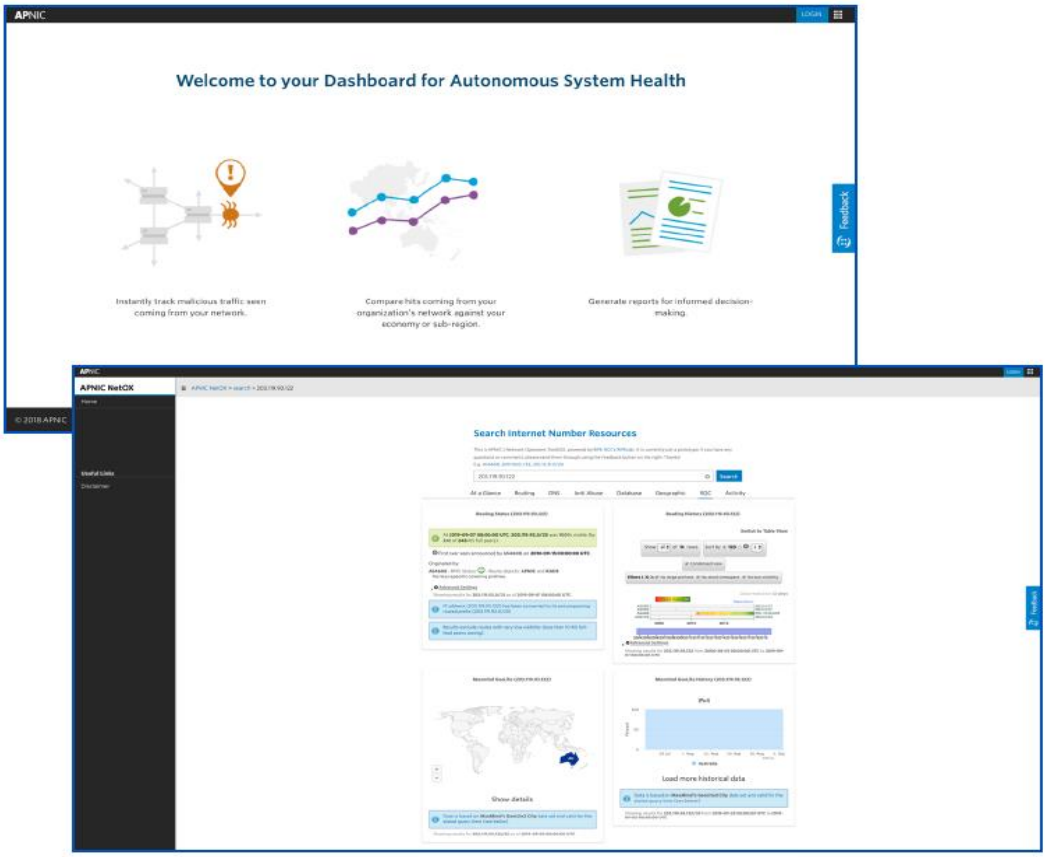

圖 16 DASH – Dashboard for AS Health

（資料來源：講者簡報）

- NetOX（Network Operators tool boX）

NetOX 與 RIPE NCC 合作開發，可通過單一 Web 介面向用戶提供 whois、路由狀態和歷史記錄以及反向 DNS 信息。

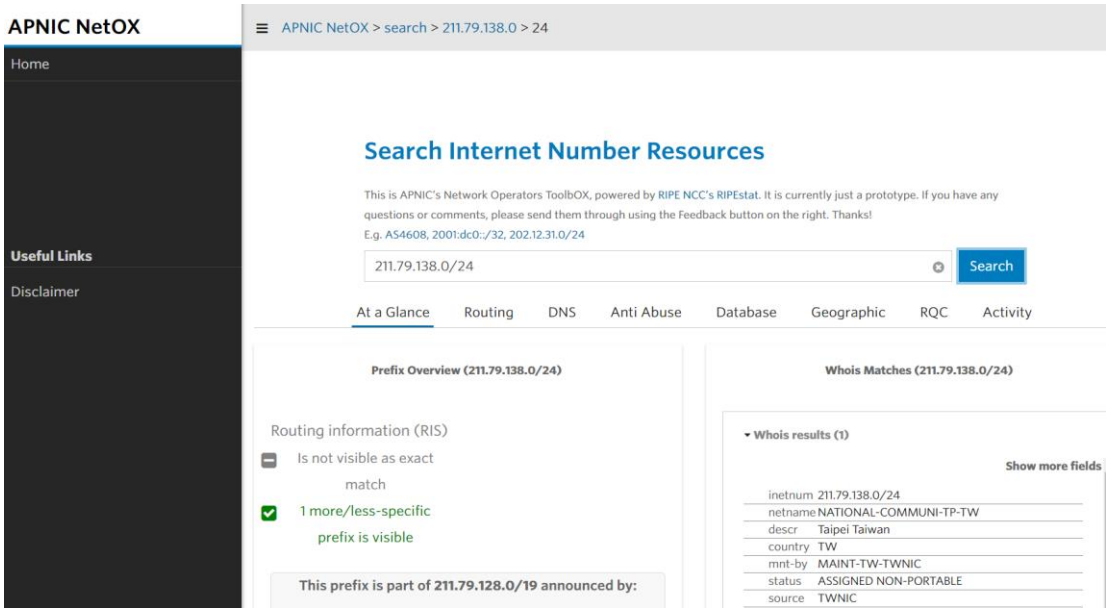

圖 17 ToolbOX（NetOX）

（資料來源：講者簡報）

二、第二日會議摘要

（一）APNIC-資安事件應變及安全小組論壇（APNIC-FIRST Security）

本日安全論壇介紹了多個有關資訊安全相關議題，各主題說明如下：

- Advanced Active Directory Attack & Defense Technique

本主題由 ALSID 公司技術總監 Kenneth Teo 進行微軟 Active Directory Attack & Defense Technique 說明，內容摘要如下：

Kenneth Teo 指出， Active Directory（AD）是微軟作業系統內建的目錄服務，微軟作業系統為市場上最多人使用的系統，因此為成為最多人使用者的目錄服務，而目錄服務存放許多駭客有興趣的資訊，如帳號、密碼，故也成為駭客最喜歡攻擊得首要標的物，但是大多使用者的安全戰略卻是不夠的，多數沒有透過工具來保護以及監控 AD。調查顯示 100%有資訊系統安全的策略，但是卻只有 45%有透過工具來保護 AD。

圖 18 多數使用者的安全策略是不足夠

（資料來源：講者簡報）

ALSID 公司的工具，透過即時威脅分析、不須安裝代理程式、50 個以上的檢查點、具有圖形導向的智慧型分析等方式來保護 AD。

圖 19 ALSID 工具優勢

（資料來源：講者簡報）

- Developments made by Thai Banks in Cyber Security

本主題由 TB-CERT 經理 Kitisak Jirawannakul 進行泰國銀行網路安全發展說明，內容摘要如下：

TB-CERT（Thailand Banking Sector/Computer Emergency Response Team, TB-CERT）創立過程：

- 2016 起始於 Information Sharing Group
- 2017 建立 TB-CERT
- 2018 成為 FIRST（Forum of Incident Response and Security Teams）會員

- 2019 成為 FS-ISAC（Financial Services Information Sharing and Analysis Center）會員

TB-CERT 發展內容：

- 有關人員部分：會員、客戶、新進銀行業者教育訓練
- 有關程序部分：處理意外回應以及資訊分享
- 有關技術部分：實作資訊分享平臺及其他協同合作

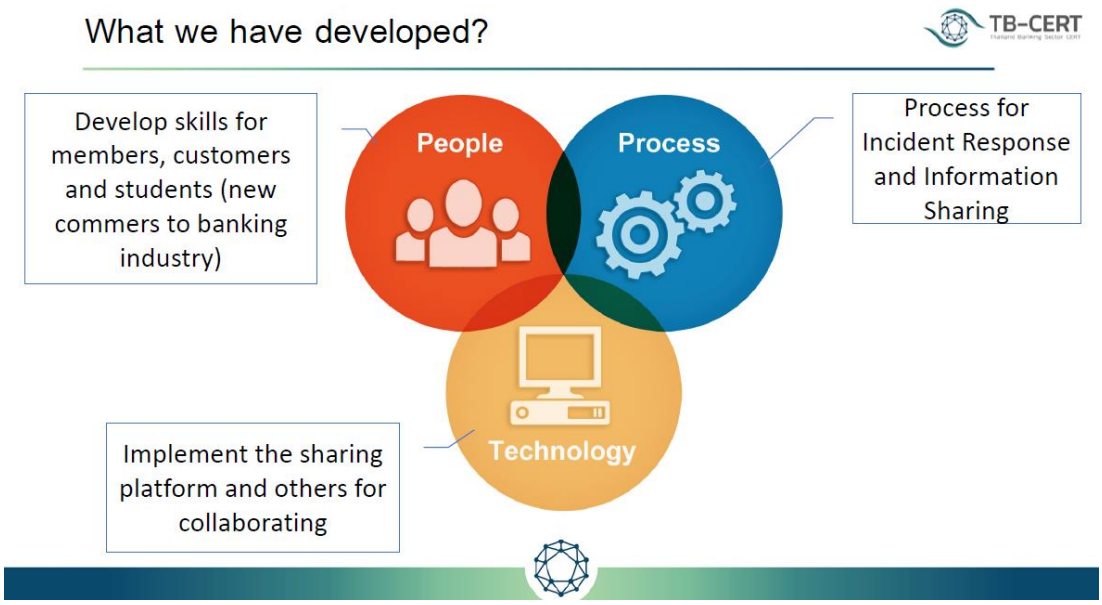

圖 20 TB-CERT 發展內容

（資料來源：講者簡報）

講者強調發展一個 CERT 分支成功關鍵因素為「信任」以及「合作」；「信任」指的是分享意外事件資訊，並透過 TLP（Traffic Light Protocol）控制所有資訊；「合作」指的是在意外事件處理、網路專研及探索、訓練及演練上互相合作。

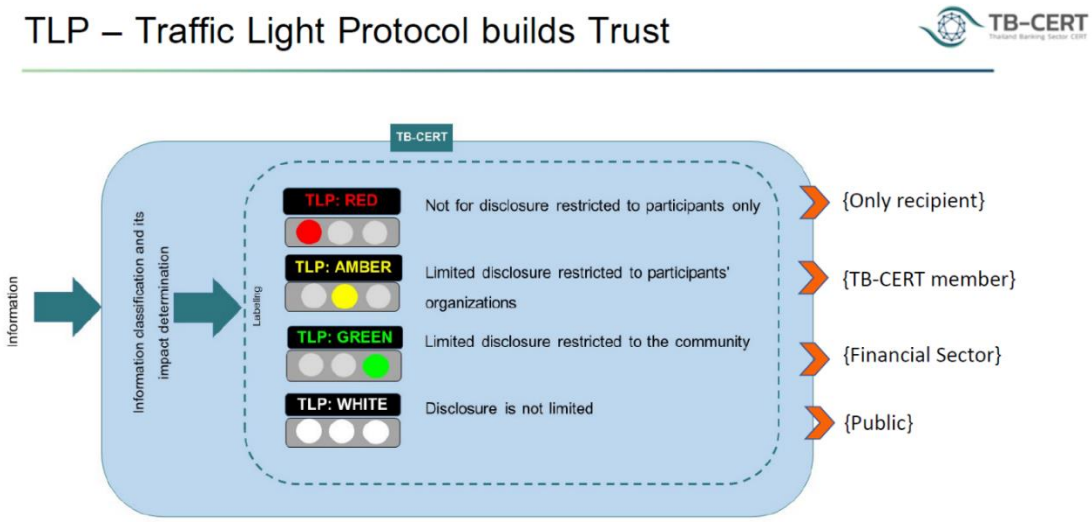

圖 21 TLP – Traffic Light Protocol builds Trust

（資料來源：講者簡報）

同時，講者也提到「資訊分享」的重要性，資訊分享指的是，可建立資安事件回應能力，透過主動分享威脅（事件）來蒐集合作夥伴間知識、經驗和能力，並保護事件相關資料。其優點為共享情境意識、改善安全狀況，讓知識更成熟，以具備更高的防禦敏捷能力；其困難通常不在技術問題，而是彼此間互動的問題（例如：信任）、擔心訊息洩漏的風險，同時自己覺得沒有可分享的信息、無權分享、沒有時間來處理或貢獻訊息、模型不適合，以及可用於共享信息的工具、特定的格式等。

因此，講者鼓勵彼此要超越分享，而訊息分享的藝術是分享更多，透過更多的分享，來帶動其他人的分享，以創造更多人的分享，但是需要特別注意的是隱私的問題。最後他也指出「分享」的挑戰在於，如何建立相互間的信任、實現相互資訊系統之操作性和自動化、保護敏感訊息、資訊發布、瀏覽外部訊息，以及評估收到的信息的品質等挑戰。

- Enabling a Mobile SOC to Protect Security Conferences Worldwide

本主題由 Kiran S Narayan（Cisco’ s SOC manager）說明，內容摘要如下：

安全討論會議已經成為資安業界同行聚會、交流和分享新的網絡威脅和安全解決方案最新訊息的方式，但同時這對於駭客來說也是一個很吸引地的場所。本場次演講者說明他們參加了許多會議，包括 FIRST（Forum of Incident Response and Security Teams）年度會議以及許多其他會議，這些會議的邏輯安全與保護任何組織的網絡一樣重要。鑑於這些會議是利用酒店/會議中心和公共互聯網等公共環境舉行，同時因為是公開的網路，以及所有與會人也帶來自己的連網設備，這些設備上可能的資安漏洞，都有可能造成國際會議上資安風險。因此對會議網絡上惡意攻擊變得非常重要。講者介紹如何使用他們的解決方式來實施安全監控工具、檢測策略以及幾乎即時回應安全事件，以保護會議上所有用戶，本次簡報介紹 Mobile SOC 如何運行。

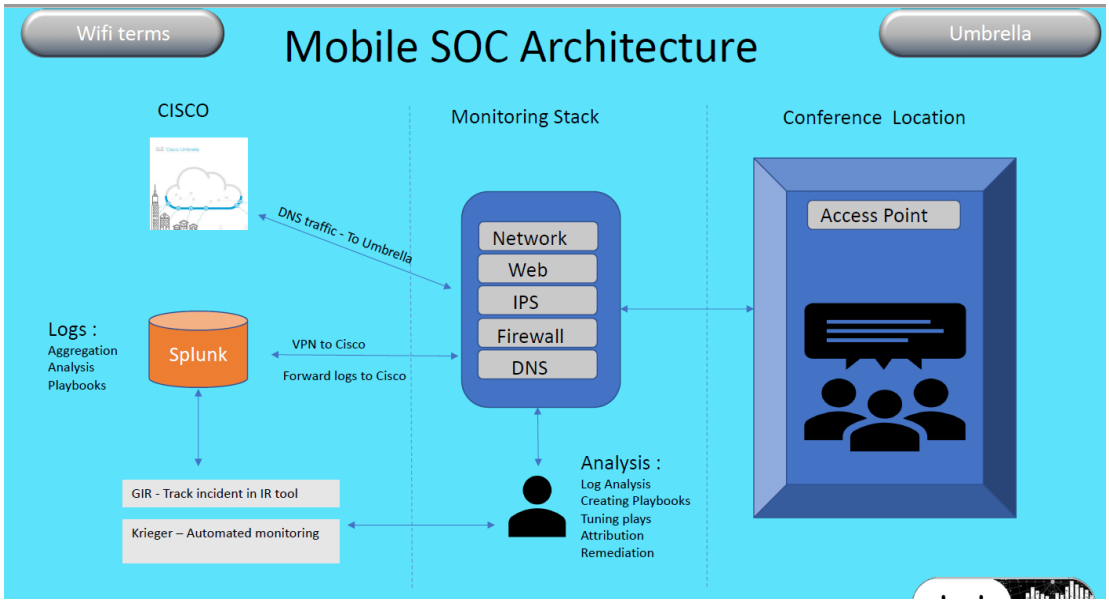

圖 22 思科公司 Mobile SOC Architecture

（資料來源：講者簡報）

透過結合思科公司資安防護傘，當接收 DNS 要求時，會使用該公司之智慧

情報來判斷此要求是安全、惡意或具風險性，安全與惡意的請求和平常一樣經路由處理，分別允許通過或遭到封鎖。具風險的請求會經路由處理至思科公司的雲端代理服務，以進行深度檢測。該公司資安防護傘代理會使用網路信譽和其他第三方摘要，來判斷該 URL 是否為惡意軟體，同時也使用防毒軟體 (AV)引擎和思科進階惡意程式防護 (AMP) 解決方案，檢查試圖從這些危險網站下載而來的檔案，接著會根據此檢查的結果，決定是否允許或封鎖該連線。

- Anonymizing Cyber Security Events Data

本主題由 TWNIC 組長林志鴻說明，內容摘要如下；

網絡安全資料非常很多，但由於其性質，它們很多時候卻都是敏感的，即使進行初步分析，也很難將網路上安全資料處理並與能與其他機構共享。本次的演講者分享有關如何通過匿名化（去識別化）資料，將網路上安全資料轉換為可使用資料。考量最大化資料之可用性，演講者團隊研究了 DID（Directed Identifiers）、QID（Quasi-identifiers）和 Unstructured Data 等三類資料進行去標識，用以在保護資料和資料完整性兩方面取得最佳平衡，並從去識別化資料中獲得更多用途，以用於不同的應用和研究。

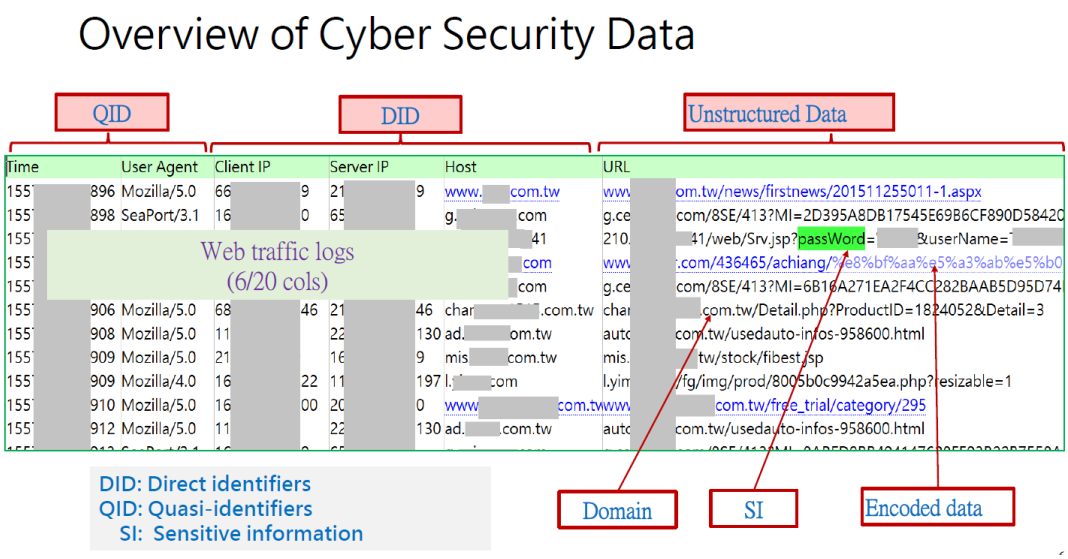

圖 23 網路安全資料範例

（資料來源：講者簡報）

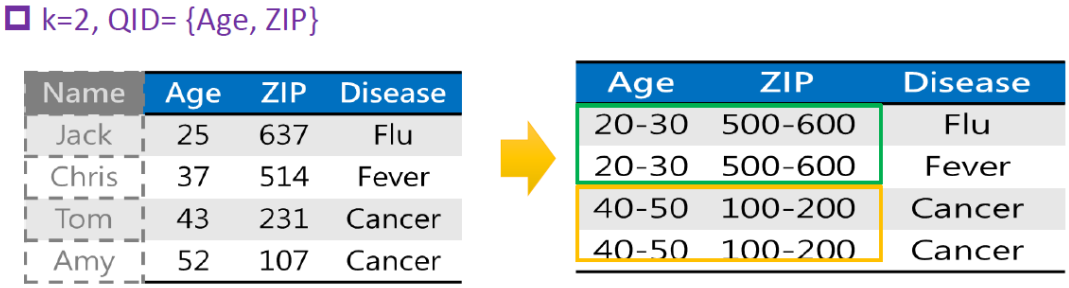

圖 24 Privary Method

（資料來源：講者簡報）

不同的領域的資料具有不同類型的隱私和實用程序問題，以現有的去識別化很難應用，而非結構化資料更複雜，更難以完全去識別化。因此建議限制對非結構化資料的存取，演講者團隊他們目前仍處於測試階段•未來他們將再繼續評估去識別化資料的工具。

（二）IPv6 部署（IPv6 Deployment）

本場次由 TWNIC 執行長黃勝雄主持，邀請 Tanapon Chandavasu、Geoff Huston、Koji Yasukagawa 、Nguyen Hong Thang–IPv6 Deployment in Vietnam 及 Maile Halatuituia 等專家與會，分享泰國、日本、越南等不同國家 IPv6 部署經驗。

Tanapon Chandavasu 分享泰國經驗，True 集團為該國匯流及數位生活的領導品牌，其服務經營可分為 True online、Ture move、True digital、Ture visions4 大部分。True online 是泰國最大的寬頻業者，服務項目以 Games、stream、internet 為主，亦提供 IPv6 服務。Ture move 是泰國第二大行動業者，預計明（2020）年開始 5G 服務。True digital 提供音樂、電影等數位內容，亦有 IoT 服務，Ture visions 則為有線電視服務。泰國由於內部 IPv4 枯竭、為減少 CG 擴充，再加上外在的全球連結以及應用趨勢，自 2012 年便開始發展 IPv6，2018 年達到雙軌並行，2019 年繼續朝純 IPv6 網路邁進。

Geoff Huston 提到，雖然大家都預測 IPv4 還能存活很久，但 IPv4 和 IPv6 雙軌並行並非目標，最終目標應該是要使整體運作能夠自動轉換到 IPv6 網路，而要達到這個目標，就是在用戶系統端盡量採用 IPv6。他提出在應用端，尤其是瀏覽器，必須採取「快樂眼球（Happy Eyeballs）」策略。

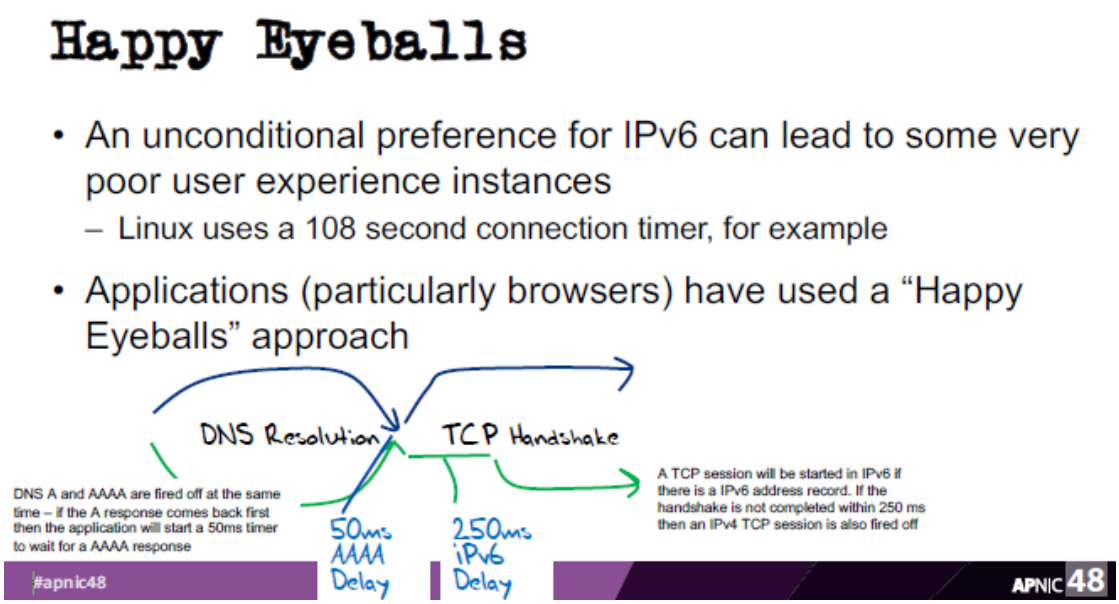

圖 25 Happy Eyeballs 概念

（資料來源：講者簡報）

日本於 2015 年在國際事務與傳播部下的 IP 網路委員會成立 IPv6 研究單位，由委員會成員和三大電信公司每月召開會議，討論相關議題、IPv6 推動等事宜。Softbank 率先在 2016 年 6 月開始提供 IPv6 服務，NTT docomo、KDDI au 則分別

在 2017 年 3 月、2017 年 9 月提供，因此三大電信業者已具備 IPv6 網路，IPv6 滲透率達 28.9%，下一步會將 IPv6 推廣至內容業者。

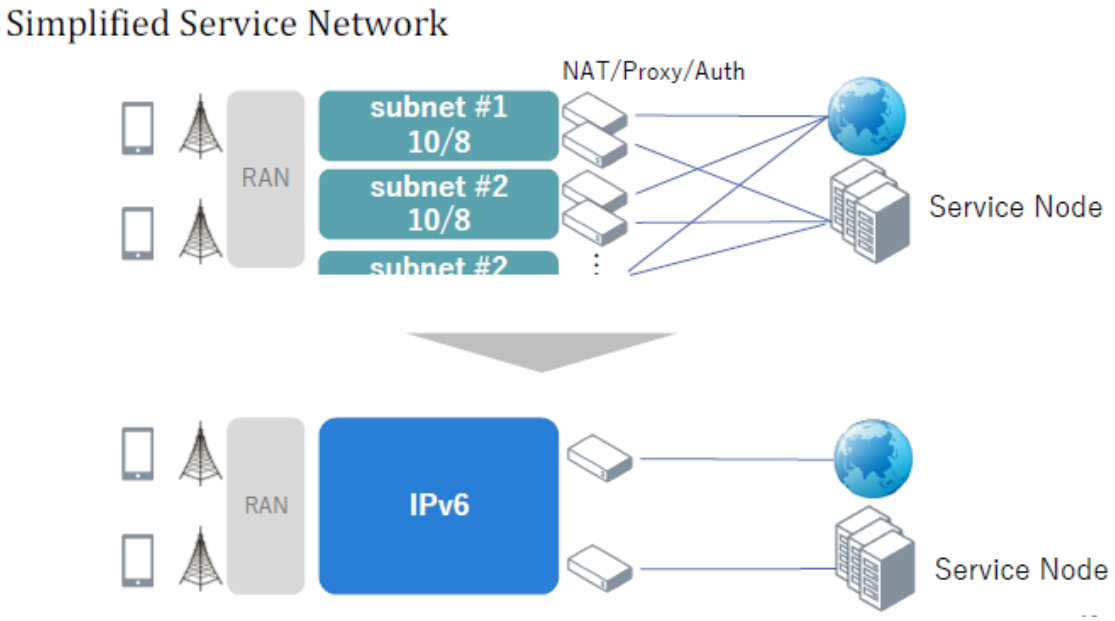

圖 26 IPv6 簡化服務網絡

（資料來源：講者簡報）

有鑑於 IPv6 具有巨大位址空間、自動配置、點對點以及安全等優點，因此越南積極發展 IPv6，而越南的 IPv6 發展工作計畫透過政策支持、教育訓練、傳播推廣、業者訪談及諮詢四方面著手推動，以時間劃分，可分準備期（2011-2012 年）、導入期（2013-2015 年）及實現期（2016-2019 年），截至 2019 年 8 月，越南 IPv6 比率達 39.63%。上述計畫將於 2019 年結束，越南，接下來繼續藉由內容業者推廣、政府推動，再加上 5G、IoT 等驅動因素，持續發展 IPv6。

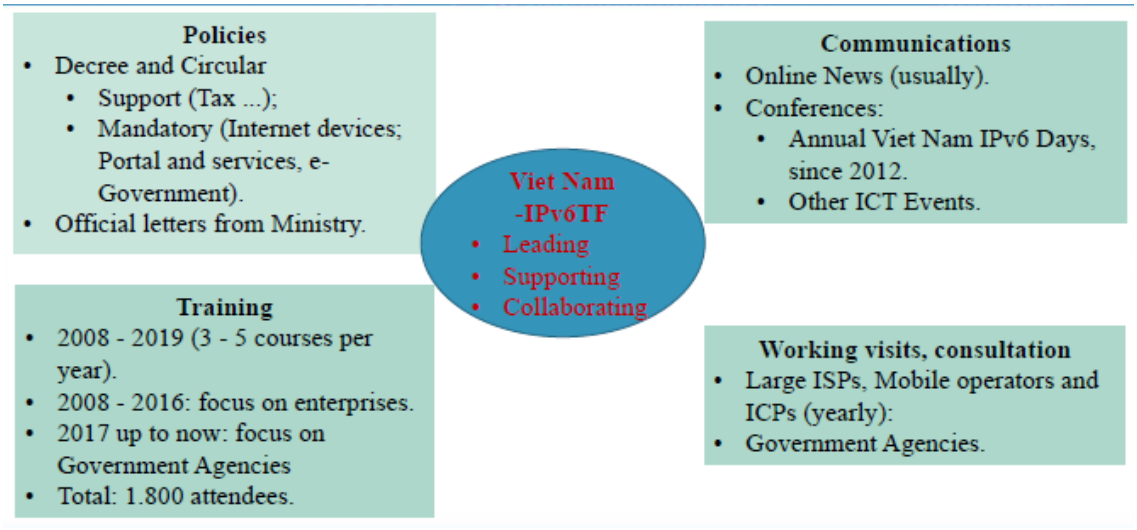

圖 27 越南 IPv6 發展

（資料來源：講者簡報）

（三）專為 5G 設計之 IP 傳輸線路（Designing the IP transport network for 5G）

在本場次中，針對 5G 來臨後的 IP 網路設計進行討論，Paresh Khatri 談到 5G 對於 IP、傳輸網絡的影響以及 5G 傳輸網路的設計。他談到，5G 帶來更多的傳輸容量、數據流量、更多的終端設備，因此未來不再只是多元輸入輸出（MIMO, Multiple Input, Multiple Output），更是大量的多元輸入輸出（mMIMO, massive Multiple Input, Multiple Output）。他也提到，隨著 5G 來臨，在網路服務上預計也會產生新的營運及營收模式。

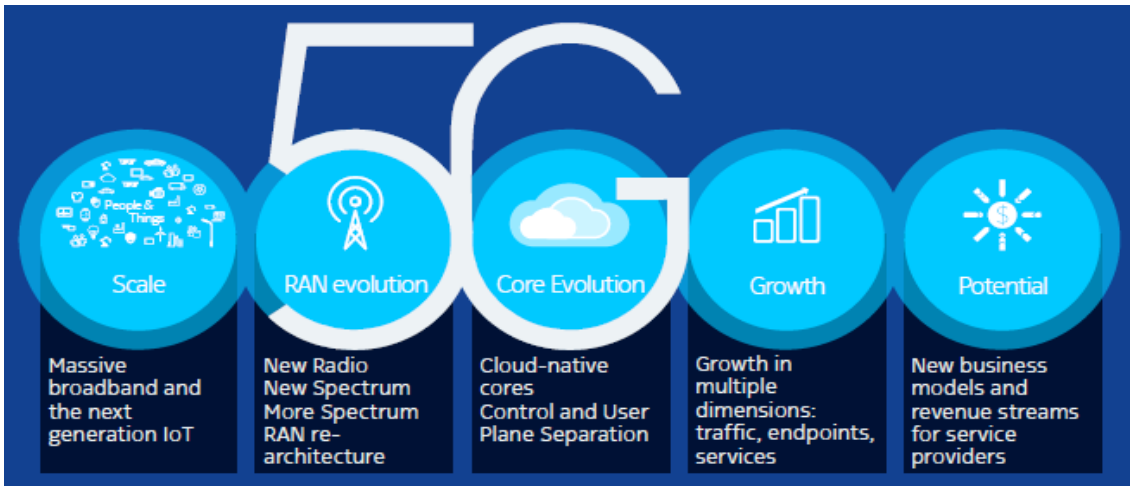

圖 28 5G 帶來的改變

（資料來源：講者簡報）

來自 NTT 澳洲的 Bihn Lam 談到路由安全的幾項重要議題，包括 BGP 優化產品造成路線劫持、末端自治系統（stub-AS）有傳輸漏洞、Tier-1 的 ISP 接受漏洞且傳送給消費者及其他國際合作同儕（Global Peers）甚至將錯誤的路線漏洞傳至消費者等。他也談到阻止上述狀況發生的方法，包括極大化 IP 字首（Prefix）；嚴格執行 Prefix 的過濾認證；不要使用 BGP 優化產引；在收、傳訊息時進行過濾，像是拒絕來自消費者會國際合作同儕的大量傳送漏洞（Transit Leaks）等。

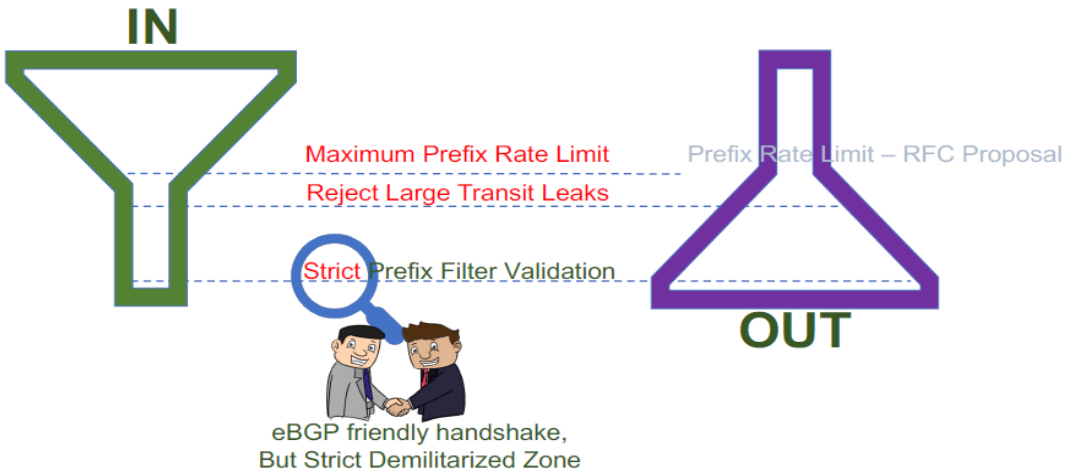

圖 29 提升路由安全的作法

（資料來源：講者簡報）

（四）資源公鑰基礎設施（RPKI）

- 偵測路由洩漏

現今網路的發展並非當初 1977 年 3 月所設計的樣貌，原先設計的網路的目的是以交換資訊為主要目的，並沒有將網路安全納入考量，例如 1991 年 BGP3 通訊協定為其中一例。然而隨著網際網路的普遍，人們越來越重視網路安全相關議題。

最典型的 BGP 路由洩漏為 2008 年巴基斯坦電信為了不讓其國內使用者存取 YouTube 而劫持其路由路徑，不僅影響巴基斯坦國內的使用者，亦使全球的使用者無法存取 YouTube。

自治系統（AS）中對於任何一個下游客戶的前綴（prefix）宣告應該直接傳遞至另一個網路而非透過第三方來傳遞，亦即一個網路若具有直接連接到其他網路的能力，將不需要透過第三方連接到目的網路，換言之所有的第一層級(tier one)網路連接可視為獨立的一對一關係（one-to-one relationship）。因此 Peerlock 可以視為一種簡單的 AS 路徑過濾器，而 CLOUDFLARE 公司於 2019 年 6 月 24 日捲入與 Verizon 電信的斷線事件正與 Peerlock 有關。因為 BGP 並不是一個完美的通訊協定，BGP 優化器在先天上就有造成路由洩漏的缺陷，僅使用 BGP 優化器但沒有聘用相關的專門人員亦無法確保 BGP 網路社群的安全。"假的"路由資訊（more specific prefixes）不應洩漏到整個網路，僅可由上游的網路提供者透過 RPKI 將其資訊過濾掉，但仍有賴網路提供者的通力合作，例如 AT&T 已於 2019 年 2 月利用 RPKI 開始過濾經由互聯網路所收到無效的 BGP 路由宣告。下圖為有過濾與沒過濾路由資訊對網路頻寬的影響。

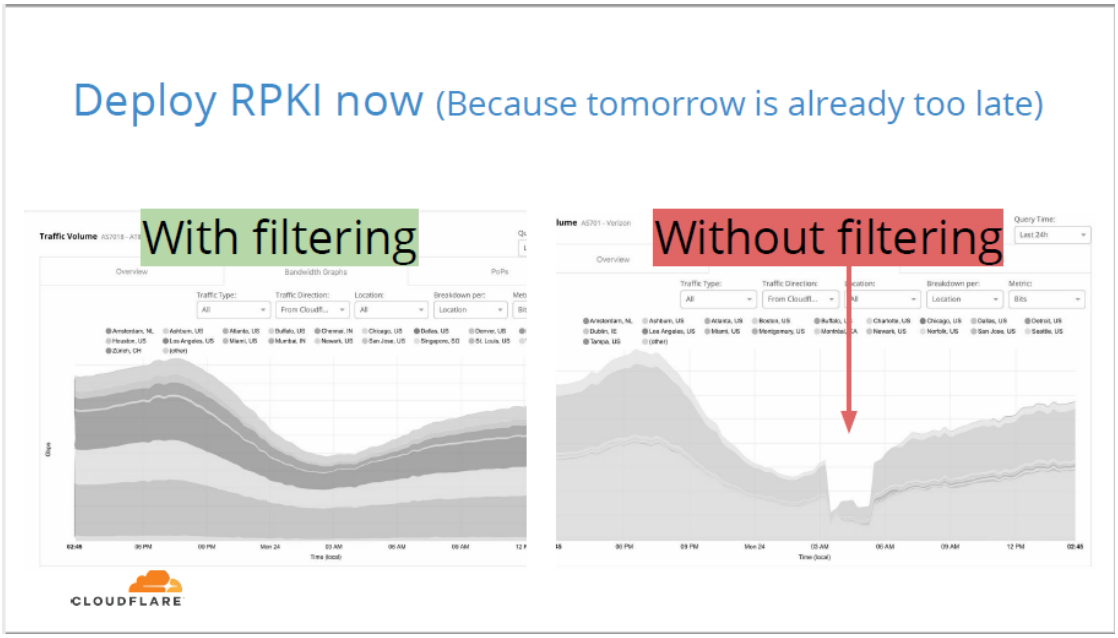

圖 30 有過濾與沒過濾路由資訊對網路頻寬之影響

（資料來源：講者簡報）

- JPNIC 如何推展資源公鑰基礎建設（RPKI）

講者認為 JPNIC 在推行 RPKI 為一種具實驗性質的服務，透過簡單的使用者網頁介面，以當地語言（日文）顯示路由源授權（ROA）等相關回饋訊息。

一般而言，對 IP 位址擁有者（(IP address holder）來說，建立 ROA 的流程須向 PRKI 驗證機構申請建立 ROA，供其驗證取得 ROV 後才得以宣告其 IP 前綴（IP prefix），總計作業處理時間約為數天。講者強烈建議 ROA 須由 IP 網址擁有者親自處理物假他人之手。

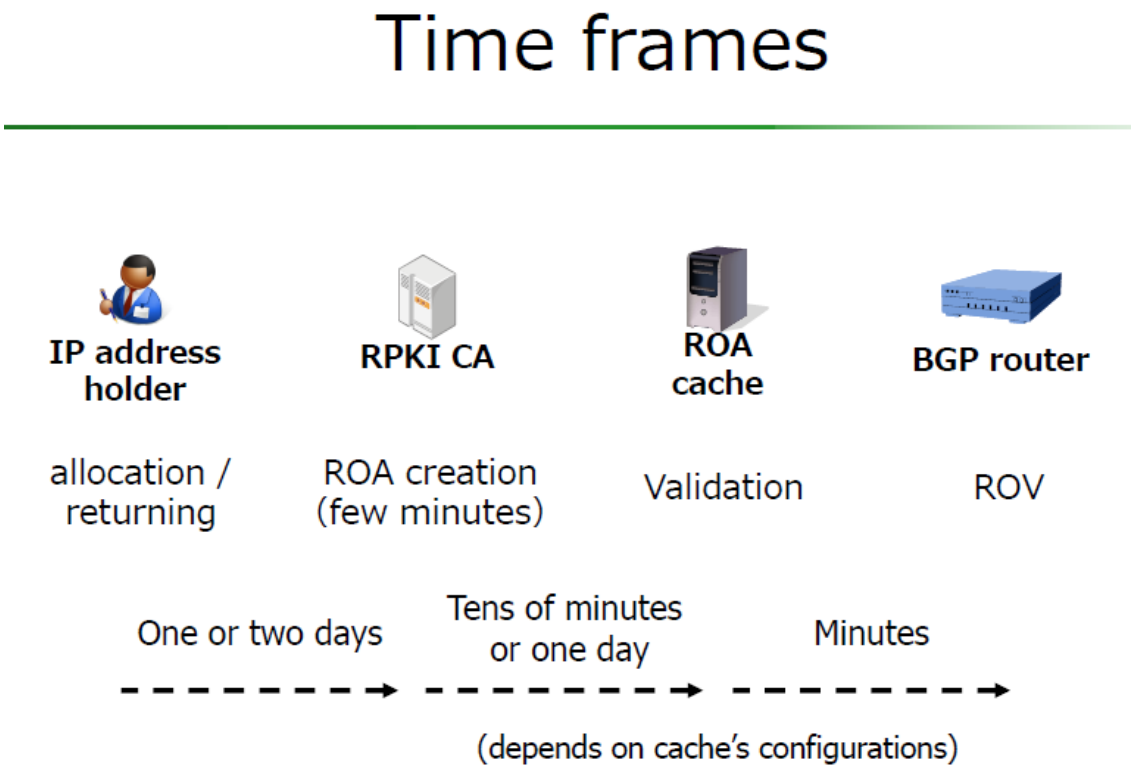

圖 31 申請 ROA 相關流程及預計作業處理時間

（資料來源：講者簡報）

從 RPKI 的使用者角度來看，申請流程依序為了解 RPKI、創建 ROA、觀看結果、建立快取、測試並發布。

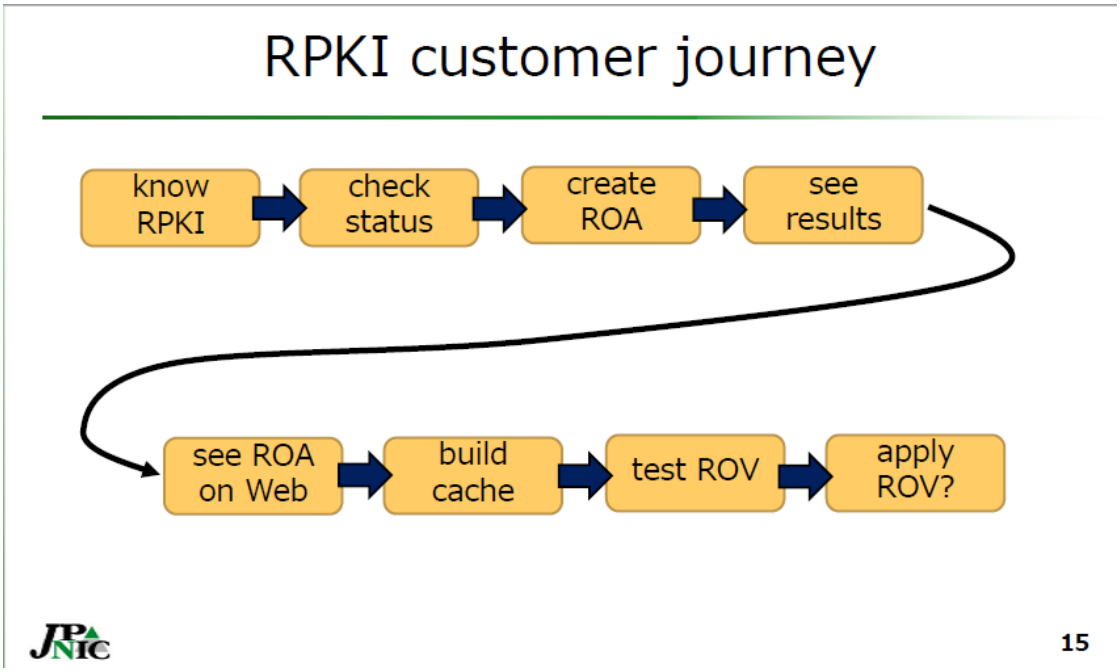

圖 32 申請 ROA 相關流程及預計作業處理時間

（資料來源：講者簡報）

完成 ROA 及 ROV 後，使用者若更改其 IP 前綴宣告，應更新路由物件(route change)，必要時透過 JPNIC 的協助加以修正，修正 ROA。JPNIC 未來將邀請相關人員及單位加入 RPKI 推展的行列，以確保 BGP 之安全。

三、第三日會議摘要

（一）APNIC 開放政策會議（Policy SIG）

這次首先針對上述 APNIC 開放政策會議目的之定義進行文字修正，「The Policy SIG charter is to develop policies and procedures which relate to the management and use of Internet address resources by APNIC, NIRs, and ISPs within the Asia Pacific region.」（APNIC 政策討論論壇目的在於針對亞太地區有關 APNIC、NIR、ISP 的 IP 資源使用及管理形成政策），尤其是「internet address resource」的用字，最後決議採用「internet number resources」。其次報告 APNIC46 形成共識的 Prop-125、APNIC47 形成共識的 Prop-127 及 128 的落實進度。

本次討論提案共 5 案，其中 2 案為先前在 APNIC 47 未獲通過之舊提案，其他 3 案則為新提案。各項提案分述如下：

- 提案 124：釐清二度指定的定義（Clarification on Sub-Assignments）

這項提案釐清《APNIC 網際網路號碼資源政策》第 2.2.3 節對 IPv4/IPv6 指派的指定位址空間之定義。之前草擬這項政策時，指定/二度指定的概念並未考慮到，IPv4 被複製到 IPv6 時，IP 位址用於點對點連結或 VPN 的狀況會被放大。這項提案釐清這種情況，同時也將概念更妥善地定義，特別對 IPv6 (RFC 8273) 的新用途加以考量。

結果：未獲共識。

- 提案 126：更新政策制定程序（PDP Update）

這項提案建議更新 APNIC 政策制定程序第 4 節，目的是擴大社群成員的參與，將通訊名單（mail list）的意見也納入考量，以確定共識。因此，藉由平衡通訊名單和開放政策會議的討論，來衡量達成共識的程度。同時引入「最後呼籲」（last call），讓社群成員在開放政策會議和會員大會上，有最後機會透過通訊名單對達成共識的提案發表意見。

本提案同時建議，廢除 Policy SIG 和 APNIC 會員大會的「雙重」共識，並提議將共識定義從「普遍共識（general consensus）」改成「粗略共識（rough general consensus）」，並包括「粗略共識」的完整定義。最後，也在變更政策制定程序中，增加上訴程序，以解決過程中的分歧。

結果：未獲共識。

- 提案 130：修改移轉政策（Modification of transfer policies）

目前 RIR 間的移轉僅允許移轉 IPv4 位址和 AS 號碼，這項提案目的在於改變現有的移轉政策，當企業發生部分或完整業務合併、收購、重組或重新安置的狀況時，允許在 RIR 內部和 RIR 間移轉，並將 IPv6 位址包含在內。

結果：未獲共識。

- 提案 131：編輯變更 IPv6 政策（Editorial changes in IPv6 Policy）

這項提案建議針對 IPv6 政策進行多重編輯變更，目的在於刪除不必要的文字並將政策簡化。

結果：達成共識。

- 提案 132：授權 APNIC 建立未核發或指定位址之 RPKI ROA（RPKI ROAs for unallocated and un-assigned APNIC address space）

這項提案授權 APNIC 為其未核發的位址空間建立 AS0 路由來源授權（ROA），以解決 Bogon 公告問題。在 APNIC 的管理下，為未核發的位址空間建立 AS0 ROA 時，相同位址空間如果有人試圖宣告（advertise），則會被標記為「無效」。

目前，在無任何 ROA 的情況下，這些 Bogon 會被標記為「無法找到」。但若有業者已部署路由來源驗證（ROV）且已經或規劃放棄「無效的」ROA， APNIC 為其管理的未核發位址空間所建立的所有 AS0 ROA，也將被捨棄。

結果：達成共識。

（二）分段路由（Segment Routing）

現今於 IP 網路中實現路由的方式是在封包內加入目的 IP 網址，以讓傳遞路徑中的收到封包的路由能夠去決定下一個路由、節點或介面。然而對分段路由(segment routing)而言，封包在網路中之傳遞路徑已由封包內的資訊決定，傳遞路徑的相關資訊由送出封包的來源於傳送時將該資訊放入封包中，這樣的概念與一般的路由方式是截然不同的。

分段路由源自於多協議標籤交換（Multi-Protocol Label Switching），多協議標籤交換協定使的網路中的節點可以針對封包內的標籤執行加入、刪除以及置換

三種運作。透過標籤分配協定（LDP, Label Distribution Protocol)讓路由器知道節點與標籤的對應關係(Incoming Label map）。當收到封包時，路由器知道何種標籤並對標籤執行相關的運作。LDP 根據最短路徑來傳遞封包，不做流量控制（traffic engineering）。不像封包往往由上游往下游路由器傳遞，LDP 中所用的標籤是被下游的路由器所指派的，（即上游的路由器所使用的標籤是由下游路由器所指定的）標籤在每一個節點皆不盡相同，標籤只對該節點的意義，封包以最短路徑之傳遞如下圖所示。

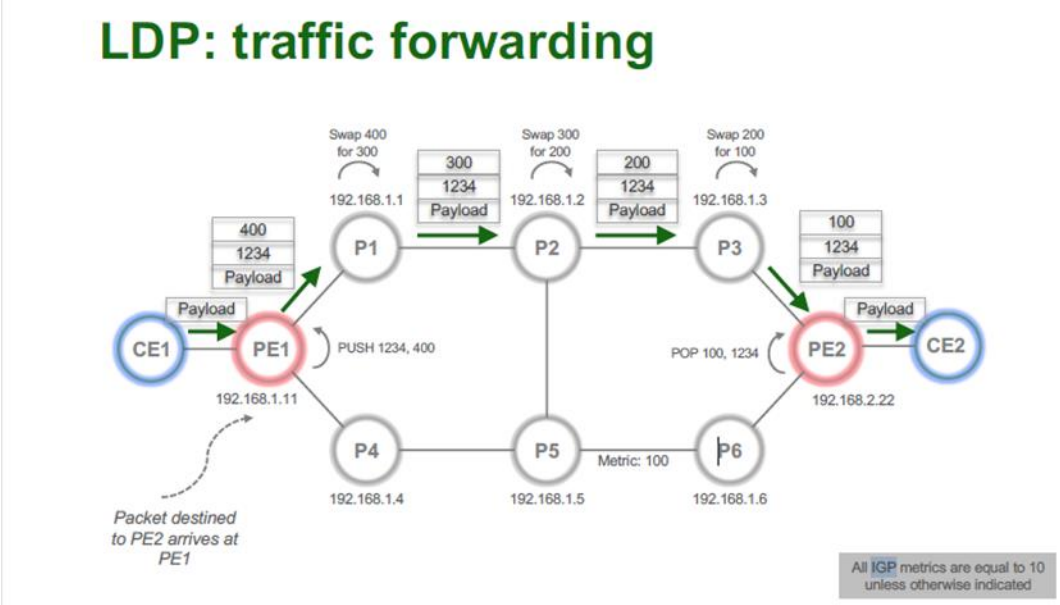

圖 33 使用標籤分配協定來傳遞封包

（資料來源：講者簡報）

另一個 MPLS 所使用具有網路流量控制功能的通訊協調為資源預定協定（RSVP-TE, Resource Reservation Protocol - Traffic Engineering），由起點至終點沿著標籤更換路徑（LSP, label switched path）傳遞路徑訊息至目的節點，其傳遞路徑不須為最短路徑。接著沿著傳遞路徑的相反方向送出預留資源訊息（reservation message）分配節點標籤，建立每個節點的狀態，封包之傳遞方式如下圖所示。

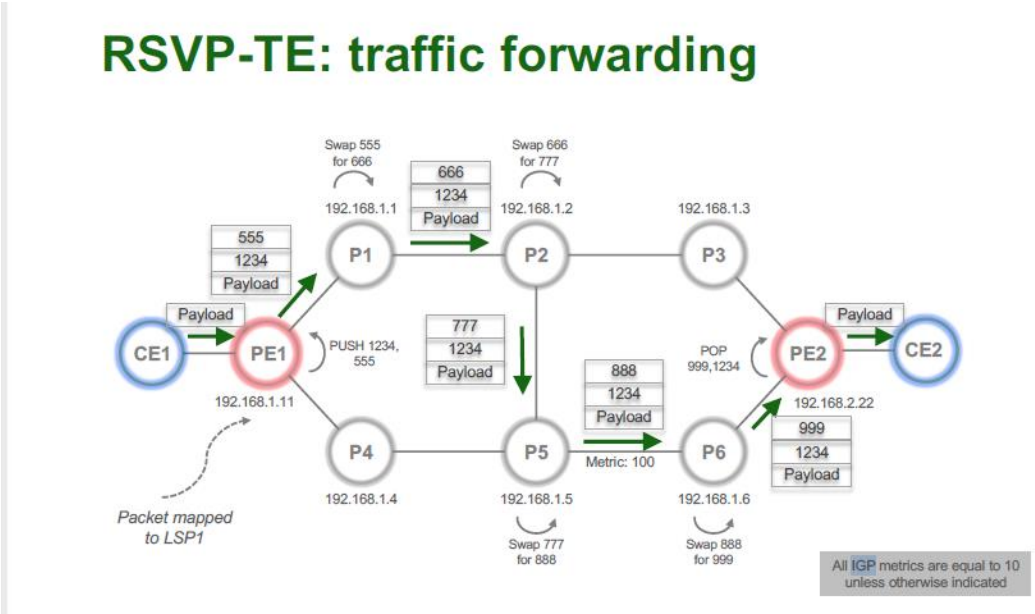

圖 34 使用資源預定協定來傳遞封包

（資料來源：講者簡報）

分段路由使用來源路由（sourcing routing）的概念，封包的來源除了包括封包本身的路由信息亦決定了封包該走的路徑以及封包內的所包含的一串的分段資訊（segments）。分段資訊包含最短路徑的節點標籤及通過指定的鄰近區域的連結相關資訊，以供中繼點來轉送發包。分段路由一開始在來源與目的之間建立傳輸路徑時可額外多建立一個傳輸路徑備用，當網路遇到節點（node）或者聯結（link）有問題時，可以透過快速的切換至備用路徑來發送封包，以避免損失大量的網路流量。分段路由透過內部閘道協定(iGP)來實現標籤分配，故無需使用前述之 LDP 或 RSVP-TE 來實現。

分段路由使用來源路由（sourcing routing）的概念，封包的來源除了包括封包本身的路由信息亦決定了封包該走的路徑以及封包內的所包含的一串的分段資訊（segments）。分段資訊包含最短路徑的節點標籤及通過指定的鄰近區域的連結（link）相關資訊，以供中繼點來轉送發包。分段路由一開始在來源與目的之間建立傳輸路徑時可額外多建立一個傳輸路徑備用，當網路遇到節點（node）或者聯結（link）有問題時，可以透過快速的切換至備用路徑來發送封包，以避免損失大量的網路流量。分段路由透過內部閘道協定（iGP）來實現標籤分配，故無需使用前述之 LDP 或 RSVP-TE 來實現。分段路由的實現可以減少網路的狀態數及允許路徑集中化的（centralized）運算，以利網路路由最佳化。

（三）網路地圖集（Atlas of the Internet - Creating geographical maps with RIPE Atlas data）

RIPE Atlas 是探測網路連接和可達性（reachability）的全球網絡，用以提供及時的網絡狀態。RIPE Atlas 網路中有成千上萬的探針，並且還在不斷增長。

RIPE Atlas 探針（Probe）為小型、USB 供電並驅動的硬體設備，主機通過網絡電纜連接到路由器的乙太網路，以進行不同的測量，並將此數據中繼到 RIPE NCC，並與 RIPE Atlas 網路其餘部分的數據進行彙整。探針使用的頻寬非常小，

且無法決定有關傳遞到其主機（host）或從其主機傳出的內容的任何信息。探針執行 ping，traceroute，SSL / TLS，DNS 等量測。

另一種量測裝置稱為定錨器（Anchor），定錨器內含許多的探針，可以進行多樣且客製化的量測，並提供本地和區域性有關連接性和可達性之寶貴的信息。其使用的軟體與探針（Probe）一致。

圖 35 RIPE NCC 所使用量測的探針與定錨器

（資料來源：講者簡報）

RIPE NCC 提供一般使用者的功能如下：

1. 持續監控全球數千個網路之可達性（reachability）。

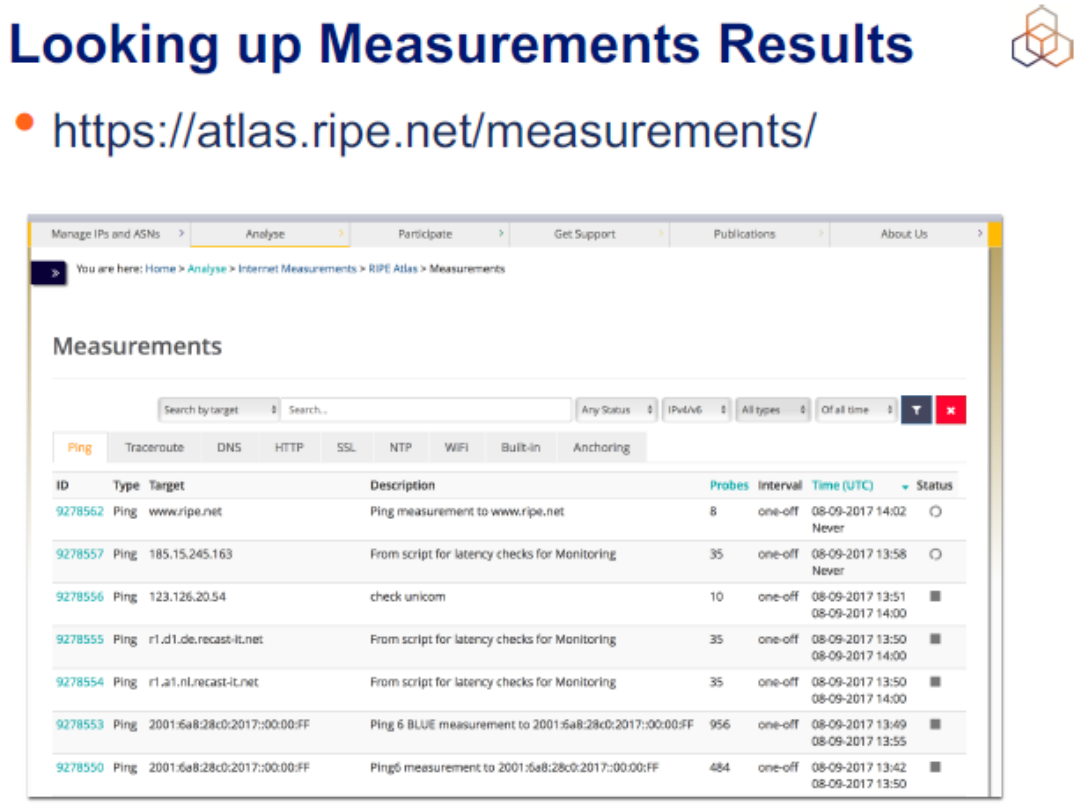

圖 36 RIPE Atlas 相關量測結果

（資料來源：講者簡報）

2. 透過快速，靈活的連接檢查來調查網路問題並進行故障排除

3. 使用 RIPE Atlas 狀態檢查來建立警報訊息，該警報可與併同監視工具一起使用。

4. 檢查 DNS 基礎設施的響應能力。

圖 37 DNS 之視覺化量測結果

（資料來源：講者簡報）

5. 測試 IPv6 連接。

RIPE NCC 從該網路收集數據，並彙整結果以提供網際網路地圖、數據工具和視覺化效果。提供探針設置的 RIPE Atlas 用戶可以使用整個 RIPE Atlas 網絡進行客製化的測量，這些測量可提供有關其自身網絡的有價值的數據。

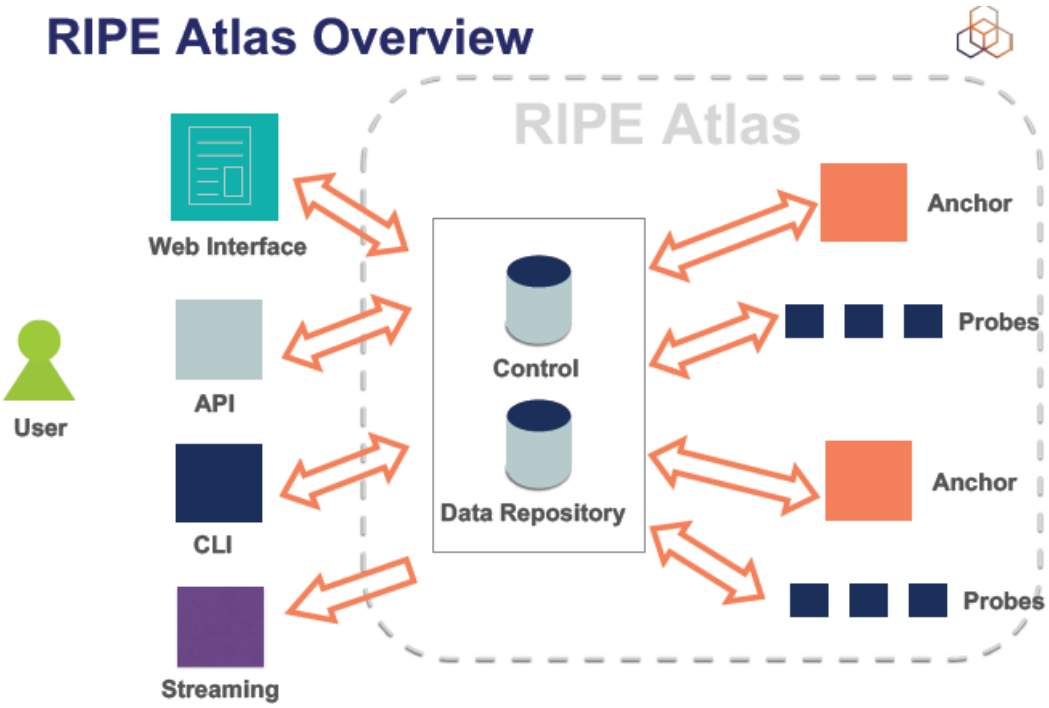

圖 38 RIPE Atlas 架構示意圖

（資料來源：講者簡報）

（四）APNIC 年度全體成員會議（AMM）

AMM 是 APNIC 的全體成員會議，除了由 APNIC 執行理事會（EC, Executive Council）報告目前 APNIC 營運現況，也由本次會議各場次主持人做出該場次總結，同時也針對當日稍早通過的政策提案，再次尋求參與會員共識。另外，本次 AAM 亦完成 NRO NC（Number Council）選舉，包括線上及現場皆可投票。AMM 相關重點說明如下：

- AMM1

APNIC 執行理事會首先邀請所有 APNIC 成員和社群中有興趣的成員，在現場親自或透過遠端視訊參加 APNIC 全體成員會議。在主席等人致詞後，EC 開始進行報告，包括行政、財務等事務，同時也鼓勵在場或線上成員向 EC 和 APNIC 秘書處提出問題和回饋。

秘書處針對其成員、IPv4、IPv6 與 ASN 等相關數量統計資料進行報告，同時也提及 APNIC 提供的各項服務與設備、目前正討論的各項政策議題，另外也說明目前 APNIC 正進行的各項工作進度、與其合作的相關國際組織等，讓與會成員能夠瞭解目前 APNIC 在業務上的發展現況。

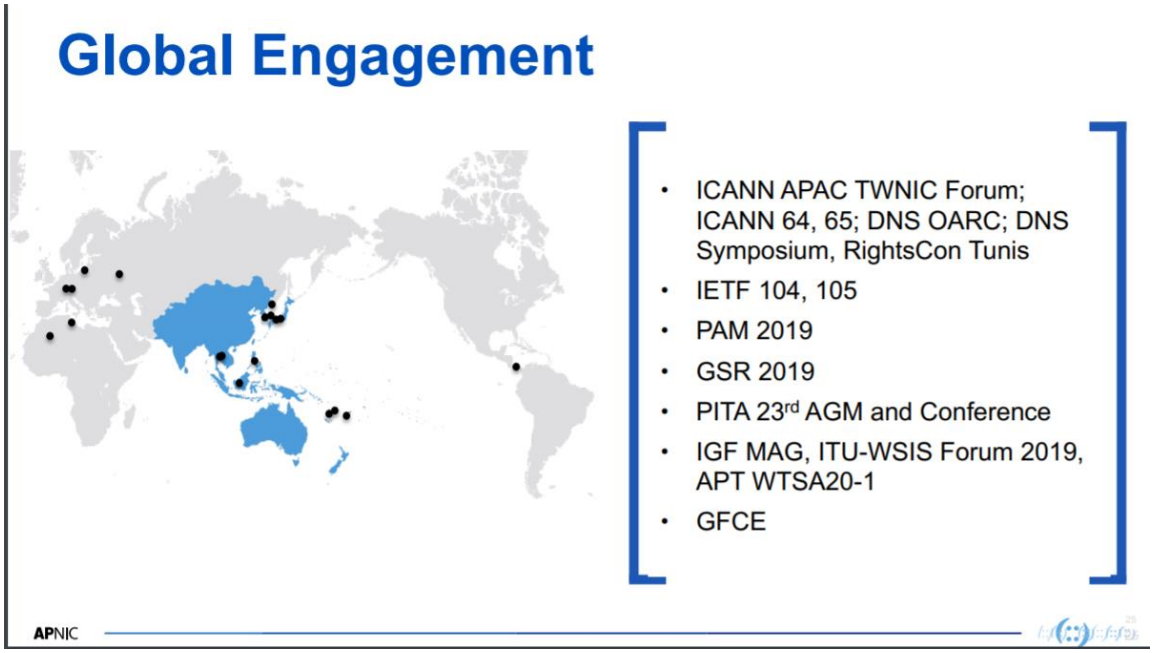

圖 39 全球與 APNIC 有合作關係的相關組織

（資料來源：講者簡報）

我國 TWNIC 董事長兼執行長黃勝雄亦為 APNIC EC 成員，在本次會議負責報告 APNIC 截至 2019 年 6 月底止的財務報表與活動紀錄，相關財務報告關鍵指標如下圖。

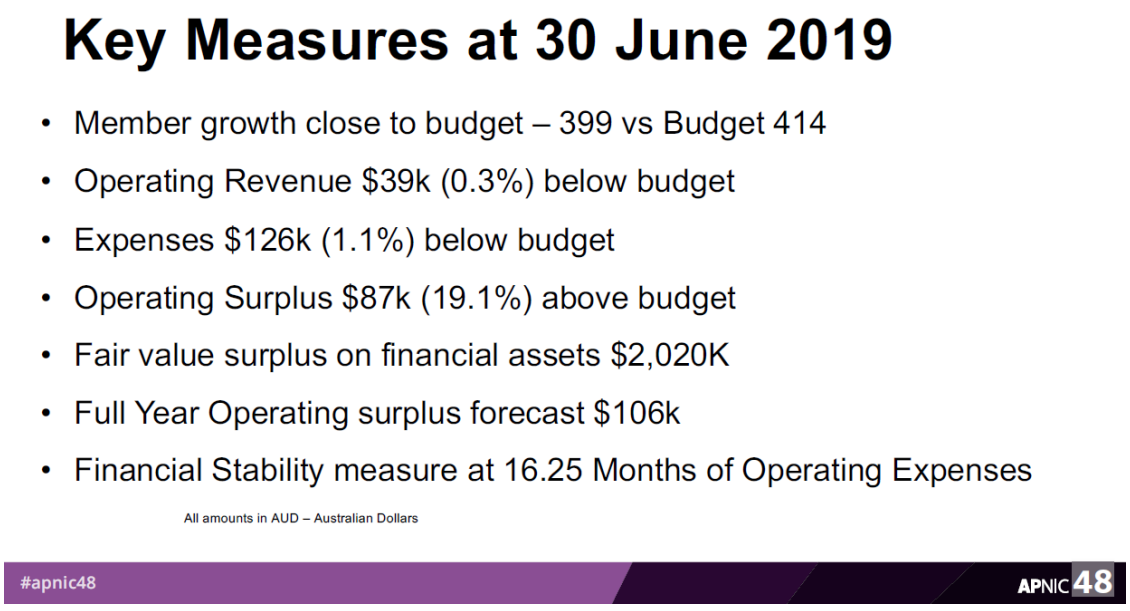

圖 40 2019 年 6 月底止財務報告關鍵指標

（資料來源：講者簡報）

同時，NRO 執行委員會也在會中進行報告，包括執行委員會的結構、定期報告、財務收支及相關技術計畫等，讓與會成員瞭解目前發展現況。

- AMM2

在 AMM2 中，由多位場次主持人總結該場次的重點摘要，像是 Cooperation SIG 各議題的演講摘要、IPv6 整備度量測會議的各個演講摘要及 IPv6 目前的整備程度等場次。接著也報告 APIX（Asia-Pacific Internet Exchange）情形，最後亦公布 APNIC 50 將於孟加拉舉辦，歡迎大家屆時前往參加。並以影片介紹孟加拉達卡當地的風光。

伍、心得與建議

一、本次會議研討內容主要包括亞太地區各NIR現況、網路管轄權、IPv6發展、RPKI推動、資訊安全以及其他網路安全相關議題，不僅將臺灣在IP位址發放、IPv6、RPKI等推動情形讓其他國家瞭解，同時也藉由各場次演講，掌握目前網際網路發展趨勢以及各國發展現況，皆有助於本會制定網際網路相關監理政策。

二、在本次APNIC 48會議，臺灣參與度也逐漸提升，除了我國TWNIC董事長兼執行長黃勝雄擔任APNIC執行委員會委員（EC, Executive Council）並主持IPv6 Deployment場次；TWNIC副執行長丁綺萍也擔任Cooperation SIG主持人，討論網路管轄權；TWNIC IP組長顧靜恆亦擔任Policy場次的共同主持人，該場次為每屆APNIC會議的重要場次，針對APNIC相關政策進行討論，這些參與皆有助增加我國在亞太地區網路資源管理、網路治理的重要性，也顯示臺灣在此領域的努力獲得認同。

三、這次在開幕典禮之前先進行Cooperation SIG，並以網路管轄權為主題進行交流，顯見此議題在亞太地區的重要性。目前網路已成為人們不可或缺的生活面向，網路管理亦日趨複雜，尤其面對網路詐欺、網路盜版等事件頻傳，如何界定網路司法管轄也成為各國討論焦點。在這次會議中，講者們透過案例討論網路管轄歸屬，亦皆指出網路管轄無法由單一國家為之，必須透過各國政府或組織合作才可能完成。因此，透過瞭解國際判例及作法，累積網路管轄處理能量，亦可提供我國做為參考。

四、IPv6在近幾次APNIC會議的重要性逐漸提升，從一開始的概念推廣，到今年亞太各國分享該國推動及部署IPv6作法。整體看來，不少國家將IPv6列為國家級計畫積極推動，並以ISP業者預設啟用IPv6著手，但目前仍以IPv4、IPv6雙軌並行為主，甚至在近期也會呈現雙軌並行。不過，最終目標仍應該要使整體運作自動轉換到IPv6網路環境，因此，如何儲備我國IPv6發展能量，讓整體網路環境能夠無縫也無痛接軌從IPv4至IPv6，亦是我國必須持續進行的工作，以利屆時環境成熟，能夠讓相關產業一起進入單軌IPv6網路環境。

五、隨著網路的發展日益蓬勃及普及，現今的網路已經不是當初1977年所規劃的樣貌，以往網路只著重在於如何可靠地傳遞訊息，現今資訊安全越來越受到重視。其所使用的傳輸技術，有部分已考量加密、解密等網路安全議題，但有些部分仍繼續使用以往的技術。目前除了最基本的安全性要求外，隨著往戶攻擊的事件增多，攻擊的手法不斷日新月異，資訊安全更顯重要。在本次APNIC 48會議中，網路資安亦具有吃重角色，場次亦多，透過參與網路安全議題以及瞭解相關單位所提出的適合建議方案，亦可提供本會或我國參考。

六、就網路的路由安全而言，邊境閘道器協定（BGP）是很重要的議題。BGP是自治網路系統傳遞路由資訊的重要通訊協定，若因該協定的運作方式及網路流量控制工程，進而導致路由洩漏、路由劫持等安全性問題，輕者無法傳遞資訊封包，重者危害國家安全。為了防止以上問題，資源公鑰基礎設施（RPKI）就顯得重要，因此在本次APNIC 48會議場次比例亦提高。而我國透過TWNIC積極推展佈建，並定期針對其會

員辦理教育訓練，日本JPNIC亦已推展之，建議未來臺灣仍應持續推動RPKI並提升ROA覆蓋率、ROV valid比例，並持續關注各國RPKI發展。

七、資訊、資安技術在一直進步，除防禦方擴充許多資安設備、導入資安管理機制以加強防禦外，同時攻擊方也持續演變中，以各種新科技、新技術、新漏洞進行攻擊行為。在本次多場研討會中，吸收資安新知，同時也感覺自身技術能力的不足，需要持續吸收新資訊、學習新技術，多參加研討會議，最後導入實務作業環境，以提升本會資訊及資安能力。

八、資訊安全愈來愈受重視，以往系統發展主要著重功能面需求，現在則是除原本功能面需求外，再額外增加資安需求，以及後續一連串資安相關規定及要求。本次會議有多場資安研討會，除了提高本身單位防禦、偵測能力外，也藉由TB-CERT經理Kitisak Jirawannakul進行泰國銀行網路安全發展說明，強調透過「信任」以及「合作」資安資訊分享及分析，以提早因應資安事件與提升資安預警的效果，達到各領域間的情資整合、分享與應變，提升資安防護與應變能力，這點亦值得我國各單位借鏡。

九、APNIC素以平等、開放為宗旨，資通訊產業人士常以男性為主，本次APNIC 48會議特別舉辦資通訊產業女性午餐聚會，透過各圓桌小組討論，針對在資通訊產業女性職涯發展、其在資通訊領域所遭遇到的困難進行分享與交流，藉此凝聚女性在資通訊領域產、官、學界的力量，使領域中兩性平等，亦符合性別主流化趨勢。這項活動也是本次會議中的小亮點，若未來持續辦理，或將成為APNIC會議另一特色。