出國報告（出國類別：開會）

2018年亞太網路資訊中心國際會議（APNIC45）

服務機關：國家通訊傳播委員會
姓名職稱：陳簡任技正俊安
林科長隆全
陳科長坤中
派赴國家：尼泊爾
出國期間：**107**年**2**月**24**日至**3**月**3**日
報告日期：**107**年**3**月**30**日

摘要

亞太網路資訊中心（Asia Pacific Network Information Centre，APNIC）1993 年成立於澳洲，為亞太地區網際網路位址分配之非營利國際組織機構（NGO），並為五大區域性網際網路註冊管理（RIR）機構之一，負責網際網路號碼資源（IP 位址和 AS 號碼）的管理、分配暨網際網路位址 Whois 查詢資料庫之系統維護。APNIC 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，支持根服務器部署等技術活動，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（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。APNIC 每年至少舉行 2 次國際會議，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運營技術大會（APRICOT）一起合辦。此次會議係第 45 屆，共匯集世界各地的網際網路工作者、專家學者、政府代表、產業代表等 1020 名參與。

為期 10 天的峰會，分為工作小組及研討會兩部分，工作小組係提供與會者網際網路技術學習平臺，並實際操作演練。研討會部分，則透過論壇討論、講習方式，將最新的網際網路發展趨勢與所有與會者分享；本會僅派員參加 4 天研討會。

此次會議相關議題計有 Peering、IPv6 量測等議題，另有多場技術研討會涉及 ISP 維運管理等，經由參與 ICANN GAC、Peering、IPv6、SDN、Security 等相關論壇或講習，瞭解網際網路未來監理策略與實務之最新發展趨勢，有助益於國家通訊傳播委員會制定網際網路相關監理政策。

目錄

圖目錄

壹、前言

亞太網路資訊中心（Asia Pacific Network Information Centre，APNIC）1993 年成立於澳洲，為亞太地區網際網路位址分配之非營利國際組織機構（NGO），與 RIPE（歐洲）、ARIN（美洲），LACNIC（拉丁美洲），AFRINIC（非洲）並列五大區域性網際網路註冊管理（RIR）機構，負責網際網路號碼資源（IP 位址和 AS 號碼）的管理、分配暨網際網路位址 Whois 查詢資料庫之系統維護。APNIC 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，支持根服務器部署等技術活動，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（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。APNIC 每年至少舉行 2 次國際會議，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運營技術大會（APRICOT）一起合辦，此次會議係第 45 屆，共匯集世界各地的網際網路工作者、專家學者、政府代表、產業代表等 1020 名。

圖 1 大會LOGO

為期 10 天的峰會，分為工作小組及研討會兩部分，工作小組係提供與會者一網際網路技術學習平臺，並實際操作演練。研討會部分，則透過論壇討論、講習方式，將最新的網際網路發展趨勢與所有與會者分享。此次會議相關議題計有 Peering、IPv6 量測等議題，另有多場技術研討涉及 ISP 維運管理等。讓與會者在開放的氛圍中進行討論與溝通，提供學習與經驗分享的機會。

貳、行程安排

一、 出國時間：2018 年 2 月 24 日至 3 月 3 日

二、 地點：尼泊爾加德滿都

三、 本會出席人員：

（一）射頻與資源管理處 陳簡任技正俊安

（二）平臺事業管理處 林科長隆全

（三）基礎設施事務處 陳科長坤中

四、 時程安排暨航班表

日 期	時程安排
2月24日(六)	國泰航空(CX421) 12:10 出發：臺灣桃園機場(TPE) 14:20 抵達：香港國際機場(HKG)
	國泰港龍航空(CX5104) 19:00 出發：香港國際機場(HKG) 22:05 抵達：加德滿都特瑞布文國際機場(KTM)
2月25日(日) ~ 2月28日(三)	出席亞太網路資訊中心 45th 論壇活動
3月2日(五)	國泰港龍航空(CX5103) 23:15 出發：加德滿都特瑞布文國際機場(KTM)
3月3日(六)	05:50 抵達: 香港國際機場(HKG)
	國泰港龍航空(CX5486) 08:05 出發：香港國際機場(HKG) 09:45 抵達：臺灣桃園機場(TPE)

參、APNIC45 會議（2018 APRICOT）

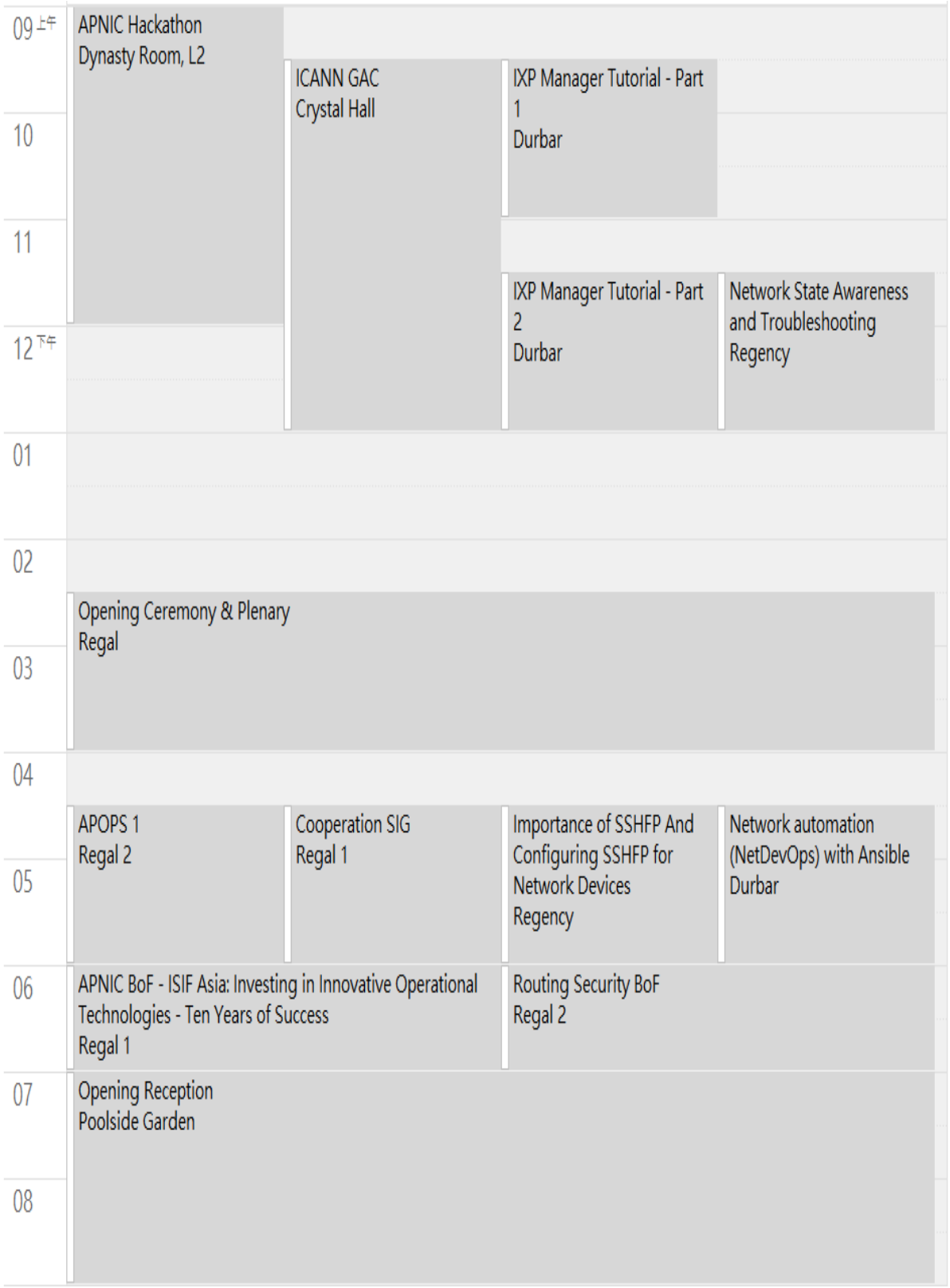
一、會議時間：2018年2月24日至2月28日

二、會議地點：尼泊爾加德滿都犛牛和雪人酒店（Hotel Yak & Yeti）

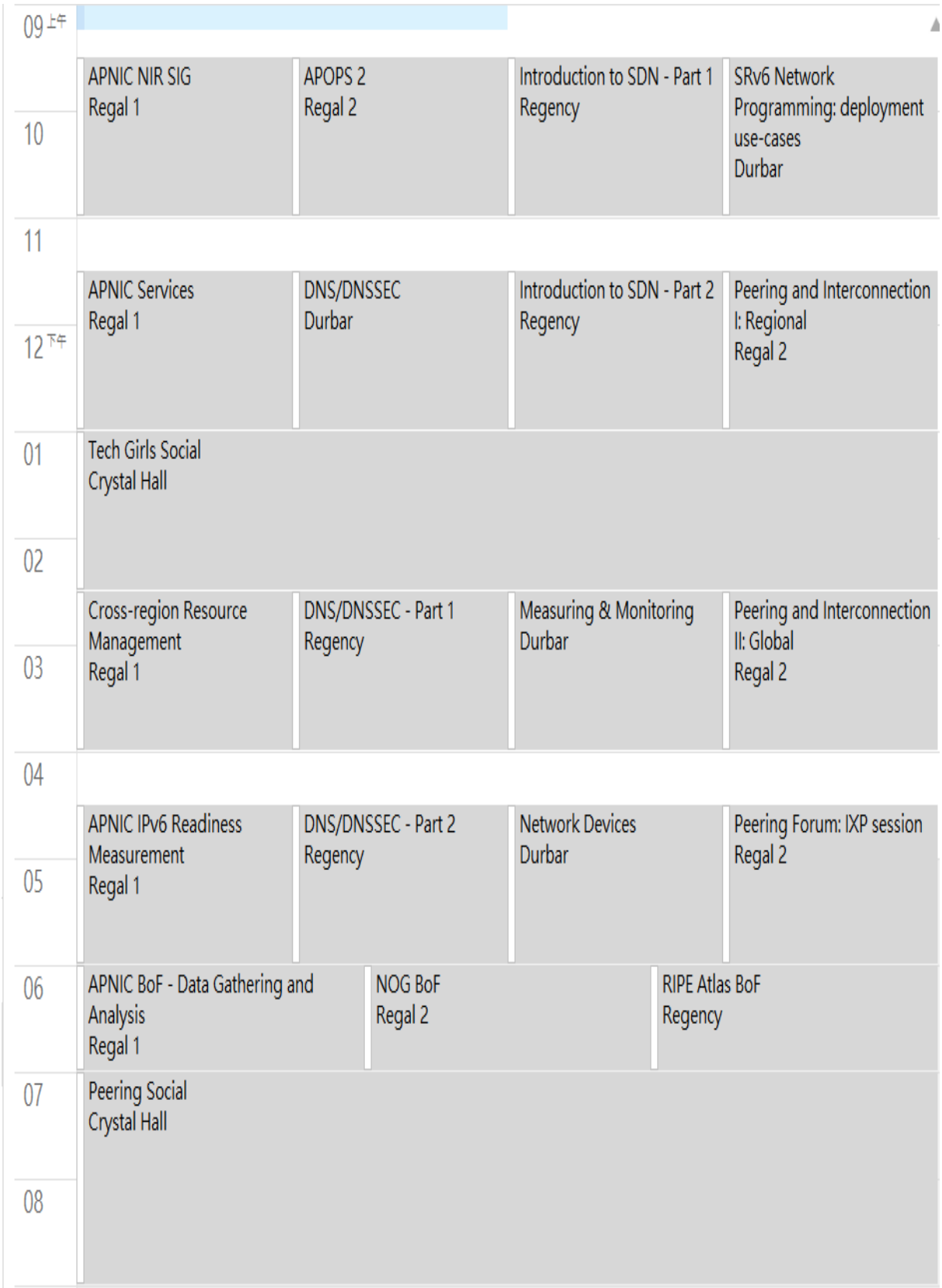
圖 2 會議地點 Hotel Yak and Yeti 地理位置

三、會議議程：

（一）第一日（2 月 25 日星期日）



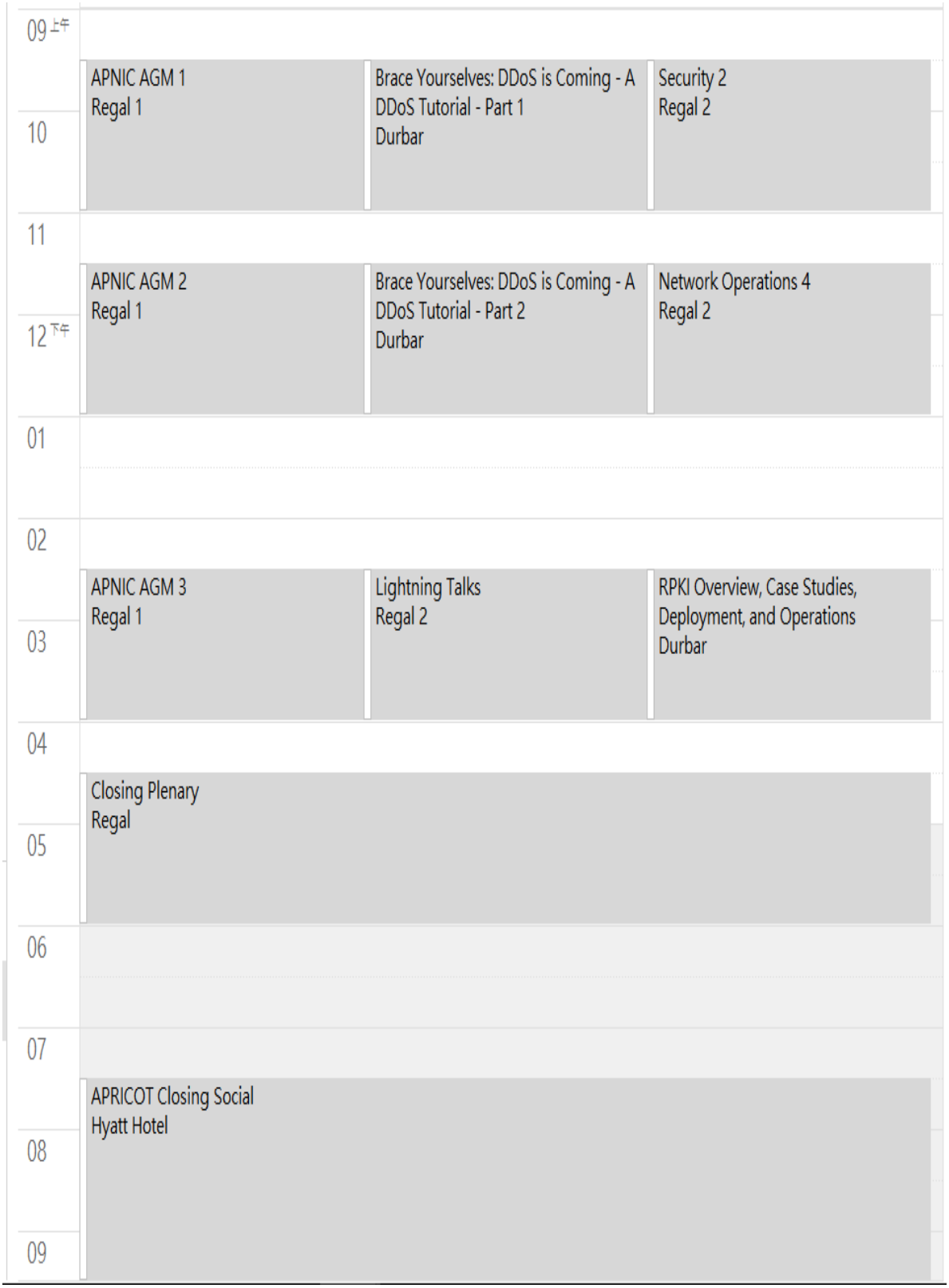
（二）第二日（2 月 26 日星期一）



（三）第三日（2 月 27 日星期二）

09 上午				
	ASO Review Consultation Regal 1	Network Function Virtualisation - Part 1 Durbar	Routing to SDN Era Regency	Security 1 Regal 2
10				
11				
	APNIC Policy SIG 1 Regal 1	IPv6 transition and deployment tutorial - Part 1 Regency	Network Function Virtualisation - Part 2 Durbar	Network Operations 1 Regal 2
12 下午				
01	Sponsors Lunch Crystal Hall			
02				
	APNIC Policy SIG 2 Regal 1	IPv6 transition and deployment tutorial - Part 2 Regency	Network Operations 2 Durbar	Secure SDN Regal 2
03				
04				
	Cross-Border Internet Relationships in Asia Regal 2	Global Reports Regal 1	IPv6 - A Real World Deployment for Mobiles Regency	Network Operations 3 Durbar
05				
06	Abuse Desk Operations and M3AAWG Durbar	APNIC BoF - Community Trainers Regal 1	BoF: NOG Reports Regal 2	ISOC@APRICOT Regency
07	Meet the APNIC EC Social Crystal Hall			

（四）第四日（2 月 28 日星期三）



肆、會議過程及摘要

一、第一日會議摘要

（一）ICANN GAC 會議

本次 ICANN GAC 系列會議係 ICANN 針對亞洲地區國家的政府代表所舉辦，用以提升 GAC 未提供服務地區的發展能力。此系列會議包括 2 月 23 日晚上的晚宴；2 月 24 日一整天的會議 (議程為開幕會議、了解 ICANN 生態系、了解網際網路：名稱、網址及協定參數、網路安全技術、DNS 安全與 DNS 濫用之處理)；以及 2 月 25 日上午的會議。由於 ICANN GAC 系列會議需受邀才能參加，此次本會透過 TWNIC 的居間協調，而能出席 2 月 25 日 ICANN GAC 系列會議中最後一天的會議。當天出席會議的政府代表有來自泰國、巴基斯坦、大陸及新加坡…等國。會議重點摘述如下：

會議一開始由 GAC 的 USR 工作小組共同主席 Pua Hunter 簡介 ICANN 政策制定流程。他首先說明 ICANN 的生態系是由社群、董事會、組織三部分組成，而 ICANN 多利益方社群分為兩大部分：一、負責政策制定；二、提供諮詢意見。ICANN 的社群有三個政策制定的支援組織(Supporting Organization; SO)：位址支援組織(ASO)、同屬性名稱支援組織(GNSO) 及國碼名稱支援組織(ccNSO)，分別負責針對 IP 位址、一般頂級網域名稱及國碼頂級網域名稱的政策制訂提供建議。

1、Introduction to gTLD/ccTLD Policy Development

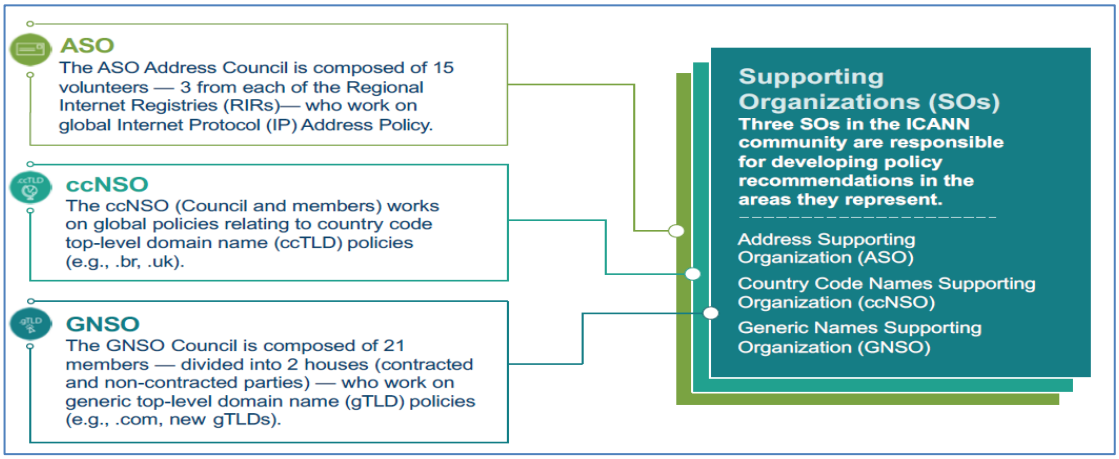


圖 3 ICANN 政策制定支援組織

[資料來源：講者簡報]

此外，ICANN 有四個諮詢委員會(Advisory Committees; ACs)，即：一般會員諮詢委員會(ALAC)、政府諮詢委員會(GAC)、根伺服器系統諮詢委員會(RSSAC)、網路安全及穩定諮詢委員會(SSAC)。諮詢委員會係針對 ICANN 的各項主題提供建議。其中 GAC 係由國家級政府(National Governments)、國際論壇承認之經濟體(Distinct Economies as recognized by International Fora)、多國政府組織(Multinational Governmental Organizations)及條約組織(Treaty Organizations)以會員代表或觀察員身分所組成之諮詢委員會，針對公共政策議題提供建議，特別是針對政策與國家法律或國際協議間的相互作用提供建議。

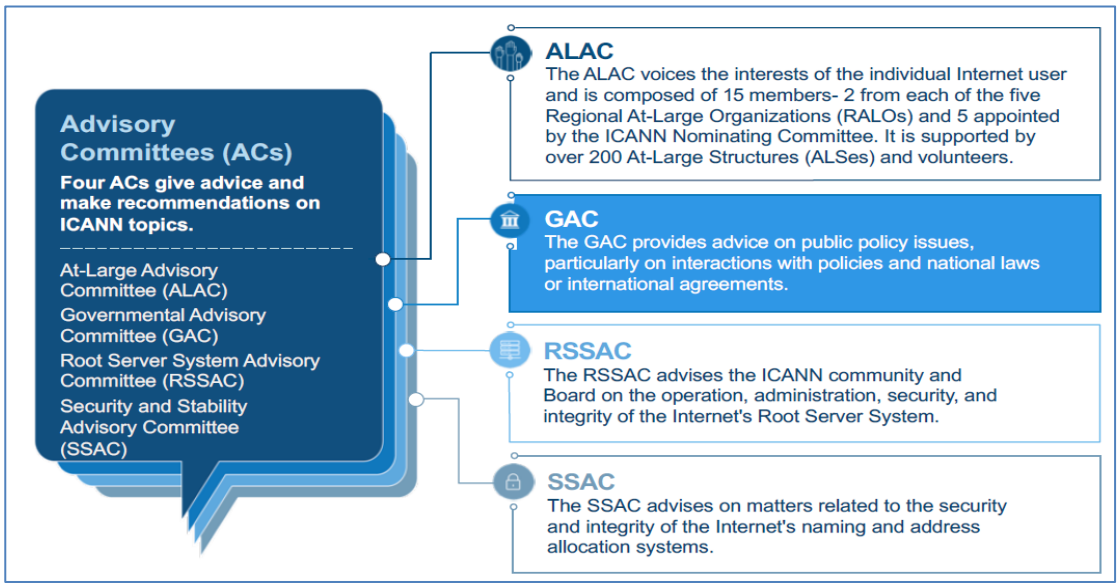


圖 4 ICANN諮詢委員會

[資料來源：講者簡報]

在簡單介紹了 ICANN 組織之後，Pua Hunter 接著表示，GNSO 係由 gTLD 登記註冊管理機構、智慧財產權團體、商業團體、學術機構及消費者團體所組成，主要負責向 ICANN 提出有關同屬性頂級域名之政策性建言。GNSO 政策制定程序(GNSO PDP)如下：

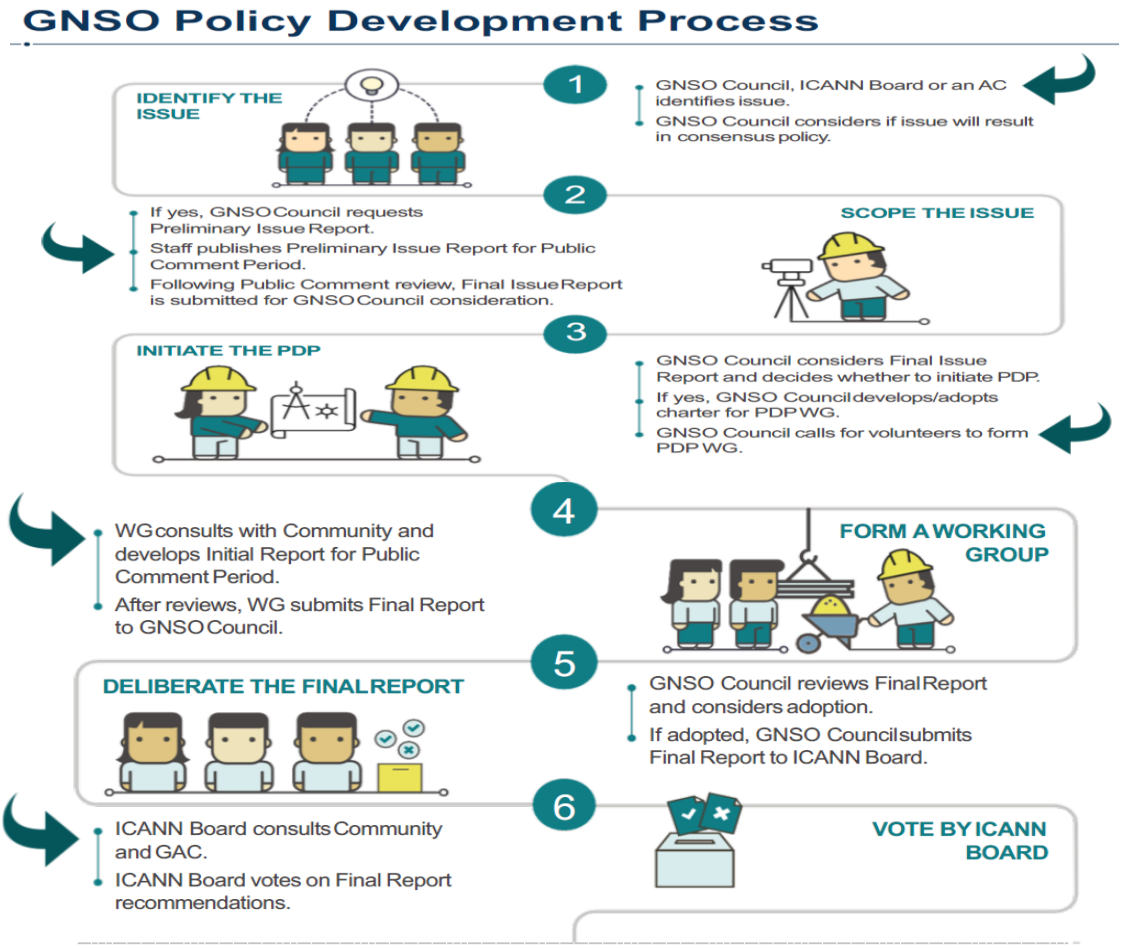


圖 5 GNSO政策制定程序

[資料來源：講者簡報]

Pua Hunter 接著說明，ccNSO 的評議會(Council)及成員致力於與全球有關的全球政策國家代碼頂級域名（ccTLD）政策（例如.br，.uk）， ccNSO 政策制定程序(ccNSO PDP) 如下：

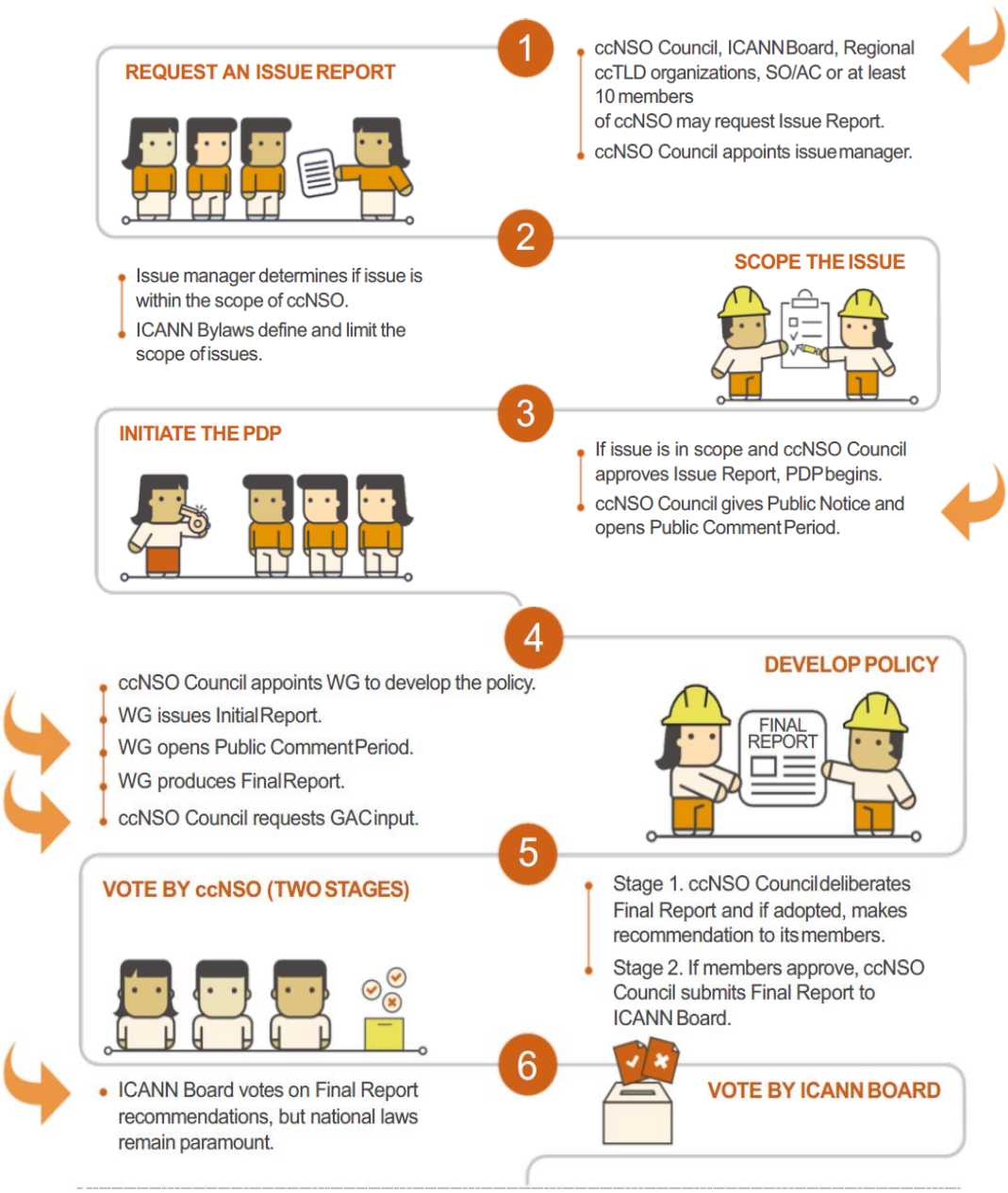


圖 6 ccNSO政策制定程序

[資料來源：講者簡報]

有與會者提問，如果當地法律規定與 ICANN 的政策規定不一致時，該如何因應。ICANN 亞洲地區副總裁 Low Jia Rong 則回答：應先遵守當地法律。

Pua Hunter 接著指出，ASO 係由 15 位志願者組成，每個區域的網際網路註冊管理機構（RIR）選出 3 位，即五大洲各推選 3 位。ASO 負責向 ICANN 提出有關 IP 位址運作、指配、及管理之政策性建言。ASO 政策制定程序(ASO PDP)如下：

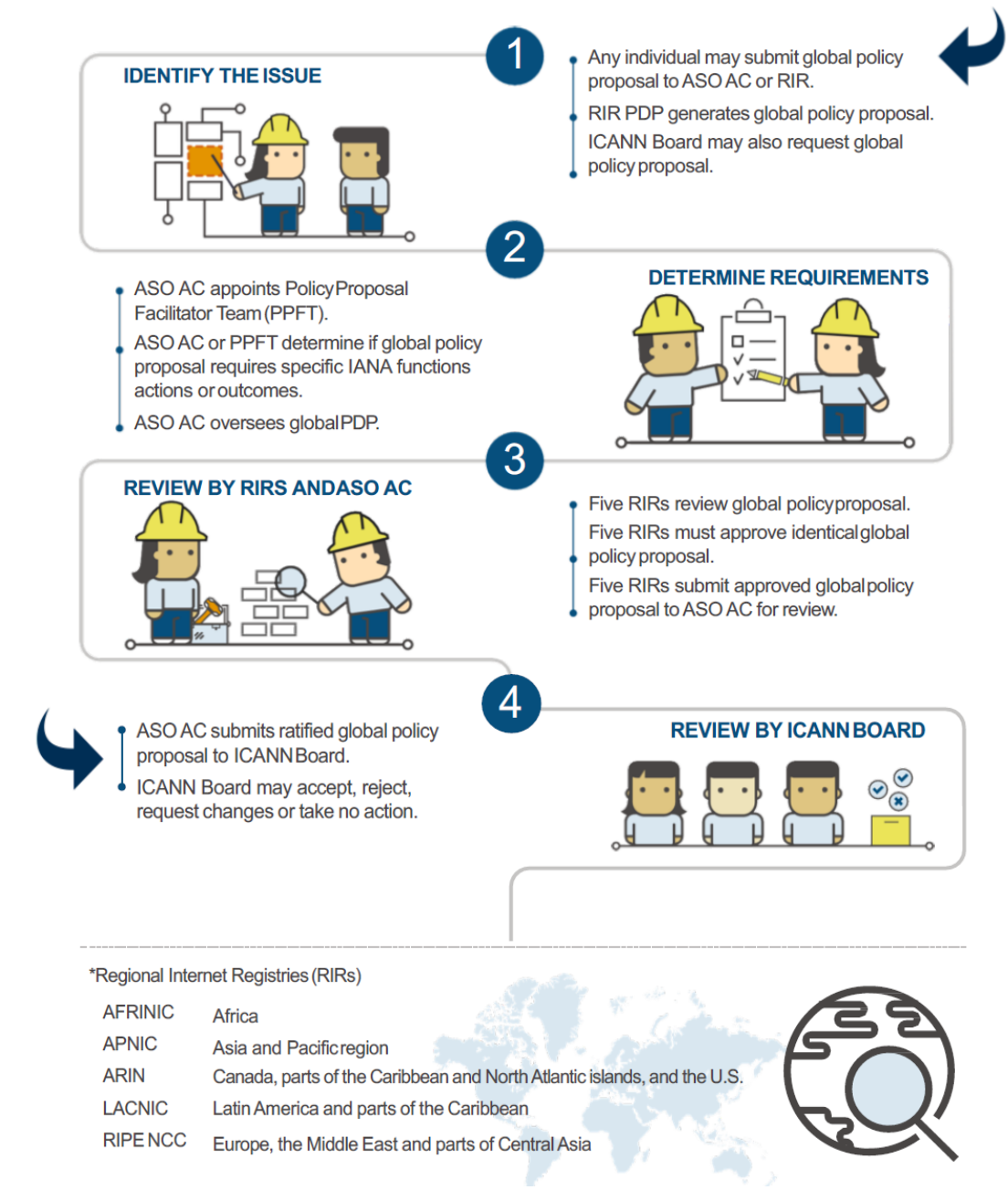


圖 7 ASO政策制定程序

[資料來源：講者簡報]

Pua Hunter 最後補充說明，參與政策制定的方式有三種：一、加入一個開放的社群或工作組；二、透過加入信件串或電話，參與觀察；三、提出公眾評論。

2、Introduction to ongoing PDPs in relation to GAC

由 GAC 副主席 Guo Feng(郭丰)首先透過 ICANN 網站，介紹 ICANN 政策可分

為三大部分：NDS Policy、Operational Policy、General Practices。接著介紹 ICANN 政策的制定的三個支援組織(Supporting Organization; SO)：GNSO、ccNSO、ASO。ICANN 的諮詢委員會(Advisory Committees; ACs)有 ALAC、SSAC、RSSAC、GAC。

接者 Guo Feng 表示，ICANN 61 將於今(107)年 3 月 10 日至同年 3 月 15 日在波多黎各的聖胡安舉行。https://meetings.icann.org/en/sanjuan61。他接著介紹 ICANN 61 GAC 目前擬定的最新會議議程，並向與會者逐一簡介 GAC 會議議程中各場次討論的主題。最新會議議程網址：https://gac.icann.org/agendas/icann61-gac-agenda#10March2018

Guo Feng 同時告訴與會者，ICANN 的社群會議除了 GAC 限定由政府監理機關參加外，其餘均開放各界參與，Guo Feng 邀請現場聽眾亦能出席 ICANN 其他群組的會議。

3、ICANN Meeting Readout Sessions in Japan

JPNIC 網際網路開發處經理 Maemura Akinori(前村 昌紀)先生首先簡介 JPNIC，他說 JPNIC 並非 ccTLD 的管理者，而是日本的網際網路促進單位。設立宗旨是致力於促進網際網路的持續營運。JPNIC 是非政府、非營利的組織，負責網際網路的合作、教育訓練、技術與政策的研究。自 2001 年起，JPNIC 會定期舉辦會議，由日本出席 ICANN 會議的人員向域名網址註冊機構、ISP 業者及產業界報告 ICANN 會議所討論的內容，以及對日本社群的影響。接著以 ICANN 60 在阿布達比的討論內容為例，介紹定期會議的典型議程，包括：簡介 ICANN APAC、ccNSO 報告、GAC 報告、董事會報告、GNSO NCSG 報告、RDS 政策制定程序工作小組進度報告、有關註冊管理機構的主題報告、New gTLD 後續程序的政策制定工作小組進度更新。此外，在資料保存方面，JPNIC 將 ICANN 第 1 次至第 50 次會議的資料均翻譯為日文，置於網站供日本國人參閱。網址是：https://www.nic.ad.jp/ja/materials/icann-report/

圖 8 JPNIC網站保存ICANN文件

[資料來源：講者簡報]

這樣做的好處是：1、能讓未參與 ICANN 會議的日本人能有機會了解 ICANN 各社群會議討論了些甚麼議題；2、能讓經常參與 ICANN 特定社群會議的人能有機會知道 ICANN 其他社群會議討論了甚麼議題；3、能讓日本的多利益方能有機會討論 ICANN 的政策；4、使用日本語，日本國人容易理解；5、屬於地區性社群。

ICANN 亞洲地區副總裁 Low Jia Rong 總結說道，若其他國家有意成立類似日本 JPNIC 的組織，ICANN 能夠提供相關協助。

4、We would like to invite you all to APrIGF Vanuatu

APrIGF 的主席 Rajnesh Singh 先生上台邀請大家參加 2018 年 8 月 13 日至 16 日於瓦努阿圖舉行的 APrIGF 會議。

5、Open Forum and Next Steps

首先講者 Guo Feng(郭丰)說明 GAC 主席與副主席係透過電子投票方式產生，任期兩年。目前 GAC 主席是來自埃及的 Manal Ismail 女士。GAC 副主席有五位，即五大洲各有一位，分別是來自法國的 Ghislain de Salins 先生、來自大陸的 Guo

Feng 先生、來自秘魯的 Milagros Castañón Seoane 女士、來自塞內加爾的 Cherif Diallo 先生，以及來自紐埃的 Pär Brumar 先生。

GAC 是 ICANN 的一個諮詢委員會，根據 ICANN 章程建立。 它就 ICANN 有關網際網路域名系統（ “DNS” ）責任的公共政策方面向 ICANN 提供建議。GAC 不是一個決策機構，它僅就 ICANN 範圍內的問題向 ICANN 董事會提供建議。GAC 的建議在 ICANN 章程下具有特殊的地位，ICANN 董事會必須充分考慮 ICANN 所提建議。如果董事會建議採行的行動與 GAC 建議的不一致，則董事會必須說明理由並嘗試達成雙方均可接受的解決方案。

接著 Pua Hunter 將現場與會人員分成四組，以分組討論的方式討論亞洲 GAC 代表主要面對的挑戰與限制，以及如何達成更加密切合作的建議與溝通的管道。

討論過程中本組成員認為 GAC 代表所面對的挑戰是，不同時區的 GAC 代表要透過電話會議進行會談時，有時所選定的時間是睡覺時間。因此覺得見面會議是較好的方式，但是須耗費旅行的成本，對於開發中國家的財務是一項重要考量。因此建議 GAC 會議可分為 A、B、C 三類，一年只召開一次全球 GAC 代表面對面會議即可，否則財務的負擔很重。可先針對區域內 GAC 代表召開會議，得出結論，再於全球 GAC 會議中討論。此外，本組成員巴基斯坦 GAC 代表建議針對 GAC 會員至少一年召開一次區域型的工作小組會議，以增加亞洲地區 GAC 代表出席的機會。另外，為增加溝通的管道，本組建議 ICANN 能發展 GAC 會議行動 APP，讓 GAC 代表能透過行動電話進行會議。

6、Post workshop servey

簡介 GAC 工作小組針對本次 ICANN GAC 系列會議的滿意度所進行的問卷調查，希望與會者都能針對這次兩天的會議提供滿意度的意見。網址：https://go.icann.org/asiagacpostworkshop

（二）IXP Manager Tutorial

此課程係由INEX（ Ireland's Internet exchange point）的技術長Nick Hilliard擔任講師，課程規劃為二個段落，第一段進行IXP Manager應用程式的簡介，第二段則進行上機演練。

Nick首先介紹，INEX是一個位於愛爾蘭島都柏林（Dublin）的網際網路交換點，該機構自創立之初就致力於回饋全球IXP（Internet eXchange Point）社群並作出貢獻，並支持在全球各地開發新的IXP。IXP Manager軟體是由ISOC等機構贊助INEX所開發，自2007迄今已近10年。IXP Manager代表了INEX至今對社區做出的最大貢獻，並且讓INEX得到了來自世界各地的高度尊重和認可。

Nick表示，INEX軟體可幫助IXP更有效率的經營，達到經營IXP必需具備的3個關鍵要求：安全性，一致性和可靠性。IXP Manager讓INEX有效率的運作，同時降低營運成本，目前全球已有54個IXP已採用IXP Manager；IXP Manager是免費軟體，使用者可以根據自由軟體基金會發布的GNU通用公共許可證條款對其進行重新分配和/或修改

Nick進一步指出，IXP Manager軟體有3個主要目標：減少人為錯誤、少成本多做事、提供會員良好的服務。功能上，在用戶面能提供：埠訊務圖示、點對點的圖示、互連管理、路由伺服器前置碼（Prefix）分析工具、用戶管理等功能。在管理及自動化面向上，則具備路由收集器、路由伺服務器、圖示化配置、監控及告警等特色，同時亦有豐富、實用的IXP工具和實用程序，儀表板和管理功能。

於課程第2階段，Nick則提供現場人員在虛擬主機上進行軟體安裝、設定等實作演練，期讓與會者透過按步就班的操作，學習如何安裝軟體，並進行參數設定、建立用戶埠資料及路由器組態設定。

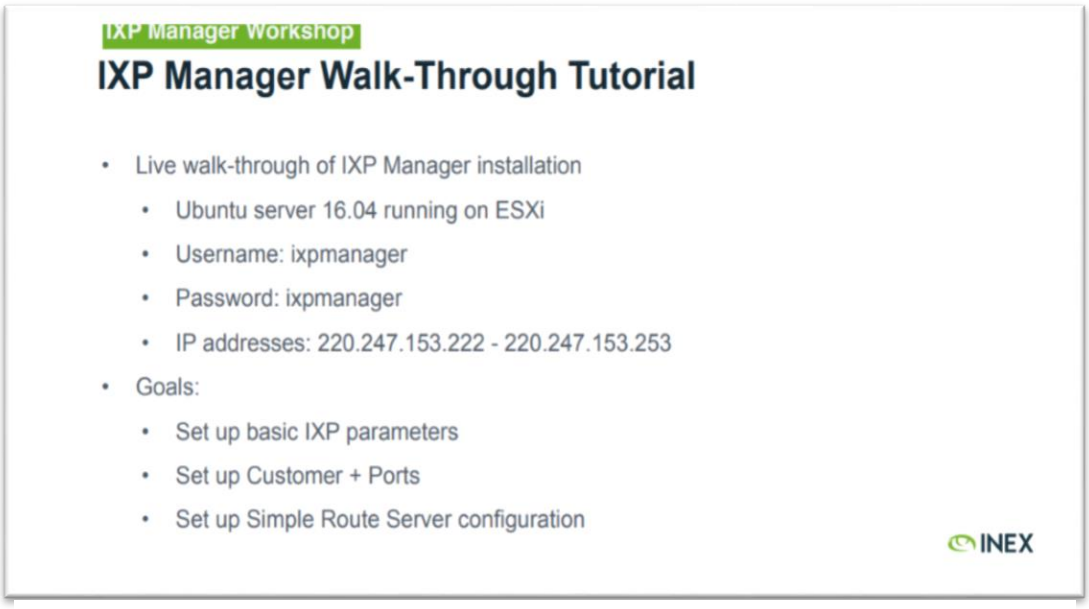


圖 9 IXP Manager軟體實作課程目標

[資料來源：講者簡報]

總結來說，IXP Manager是一套應用程式，供網際網路交換中心管理其用戶、連線和服務，並且記錄交換流量、維護骨幹路由器連接與路由處理器設定檔。該軟體亦設有入口網站，供每一位交換中心成員查詢流量。未來IXP Manager平台也會與PeeringDB、whois等平台同步，以達訊息一致化。

（三）Network State Awareness and Troubleshooting

網路狀態識別可以儘早預防更大的網路問題發生，以確保消費者權益及業者商譽，其重點在於觀察網路所為何事，與之前的網路狀態比較則是最簡單且有用的方式，這也是人工智慧及機器學習的基礎，在SDN盛行時代，控制層資安防護更顯重要。一個成功的網路守護者，首先須具備足夠的專業知識，經由相關工具及知識來識別網路狀態的是是非非，抓出相關可疑之處，再進行詳細識別後，排除可能發生的風險，並將網路進行必要之升級或調整，以避免類似情形再次發生。講者並分享NetFlow, Netdisco, Netdot, ICMP/traceroute等數款故障排除工具，包括商用、開源軟體予與會來賓。

- Netflow：是一個分析引擎，只要讀取其他設備或程式送出格式支援的資料，便可提供用以分析的 IP 流量資料。
- Netdisco：是一款適用於小型到超大型網路的基於網路的管理工具。

使用 SNMP，CLI 或設備 API 將 IP 和 MAC 位址數據收集到 PostgreSQL 數據庫中。

- Netdot：是一款開源工具，旨在幫助網路管理員收集，組織和維護網路文檔。功能包括：通過 SNMP 發現設備、第 2 層拓撲發現使用、IPv4 和 IPv6 位址空間管理（IPAM）、位址空間可視化、DNS 區域文件生成（BIND）、ISC DHCPD 配置生成、IP 和 MAC 位址跟踪、BGP 對等體和自治系統跟踪等。
- Traceroute，現代 Linux 系統稱為 tracepath，Windows 系統稱為 tracert，是一種電腦網路工具。它可顯示封包在 IP 網路經過的路由器的 IP 位址。

（四）Opening Ceremony & Plenary

除APRICOT主席Philip Smith、APNIC 總裁 Paul Wilson、NpIX主席Gaurab Raj Upadahaya外，加德滿都市長Bidya Sundar Shakya先生亦到場致歡迎詞，他表示臉書、推特等社群軟體深深影響人們的生活，身為市長他將致力使加德滿都成為一個智慧城市，讓市民能輕鬆接取政府的公共服務，提升政府施政能力，相信通信技術能解決這些問題，並計劃建立地鐵、寬頻網路，在主要城市地區提供免費WiFi，使所有公立學校和學院能連上網際網路。

圖 10 加德滿都市長致歡迎詞

（五）APOPS-1

主持人（Philip Smith ,APRICOT chair） 首先說明，APOPS是指亞太地區營運者論壇（Asia Pacific Operations forum），共有2場次，此為第1場次。相關簡報重點如下：

1、The Self-Driving Network

由Juniper Network的CTO Kireeti Kompella主講。Kireeti以1885年「現代自動車」的誕生，但當時所謂自動車是連啟動引擎都得用人工來轉動曲軸，演進至今，自駕車則追求能自動剎車、轉向及停車，一切創新都是為了讓駕駛更容易，主要目標則是「方便」及「安全」來比喻並為其「SDN（Self-Driving Network）」開場。而建構自我驅動網路的目標在於能自我復原、自我建立組態、自我監控、自我修正、自動檢測等，且對消費者能自動提供、自我優化、自我報告等。

其結果能讓人們工作更便利，例如更有利於新服務設計、創造新服務更快速、更能智慧的回應安全等。

他指出必需面對邊緣網路（edge network）大量增加更多的服務及維護品質質的改善、必須學習使用者的行為、預測使用者需求的改變等挑戰，而這些都將產生包括建立新技能、新設計、AI政策…等衝擊。

講者提到SDN必需具備「DECLARATIVE INTENT」、「TELEMETRY」、「CORRELATION」、「AUTOMATION 」、「DECISION MAKING」5種技術，以及將有「HIGH-LEVEL, INTENT-BASED SERVICE DESCRIPTION」、「END-TO-END, DEVICE INDEPENDENT SERVICE MGMT」、「OPTIMAL, TELEMETRY-BASED SERVICE PLACEMENT」、「AUTOMATIC MGMT OF UNDERLAY TO MATCH SERVICES」及「REAL-TIME SERVICE OPTIMIZATION via SERVICE MOTION」等5個好處。

講者最後並期許大家該有一個強大的網路視野，認知SDN是真的值得追求，業者該去克服對大膽創意既存的恐懼，來滿足服務敏捷性及主動服務管理的需求，並將此視為經濟上迫在眉睫的問題及安全上的必要條件，體認利用相關技術組合來達成是勢在必行的。

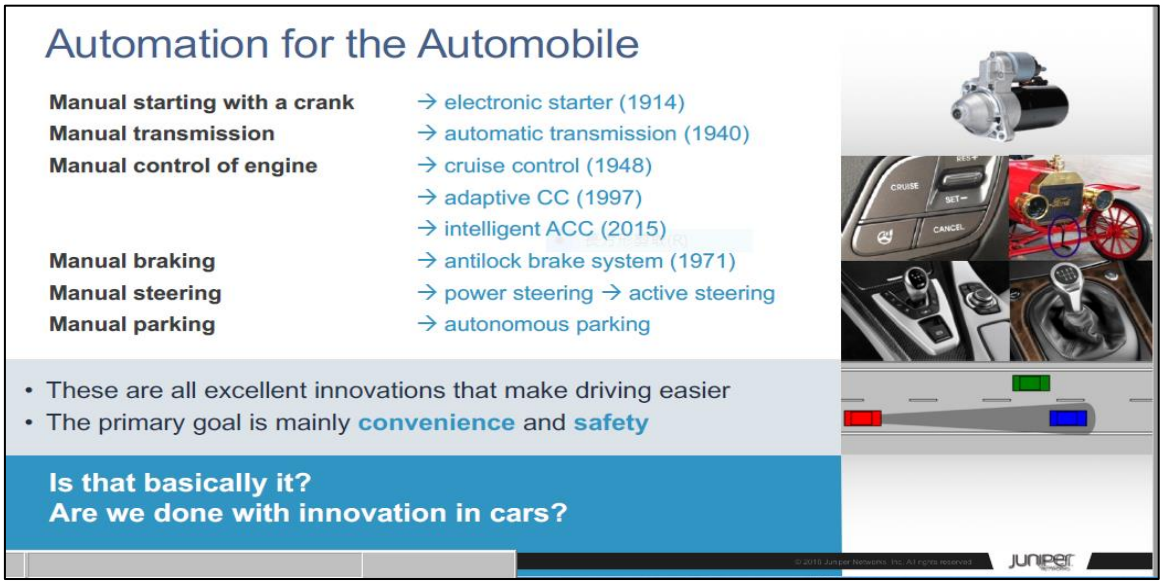


圖 11 以汽車自動化引喻網路自動化的目的

[資料來源：講者簡報]

2、IPv6 in the Wireless Telco Cloud and 5G

電信雲正在演變成電信業者的基礎設施。本演講介紹了將雲的基礎架構引入行動通信核心網路環境（包括採用 IPv6 的 5G，IOT）的一些挑戰。

來自 Telstra 的講者 Jeff Schmidt 表示，隨著 IPv4 位址的耗竭，要擴展 IPv4 資源所需費用將更加昂貴，雙堆疊是一種有效的轉換技術，但並不能解決 IPv4 耗竭的問題。唯有引進 IPv6，才能減少對 NAT 的依賴、降低區域化的需求、並且推動應用程式轉移到 IPv6。IPv6 的行動通信話務流示意圖如下：

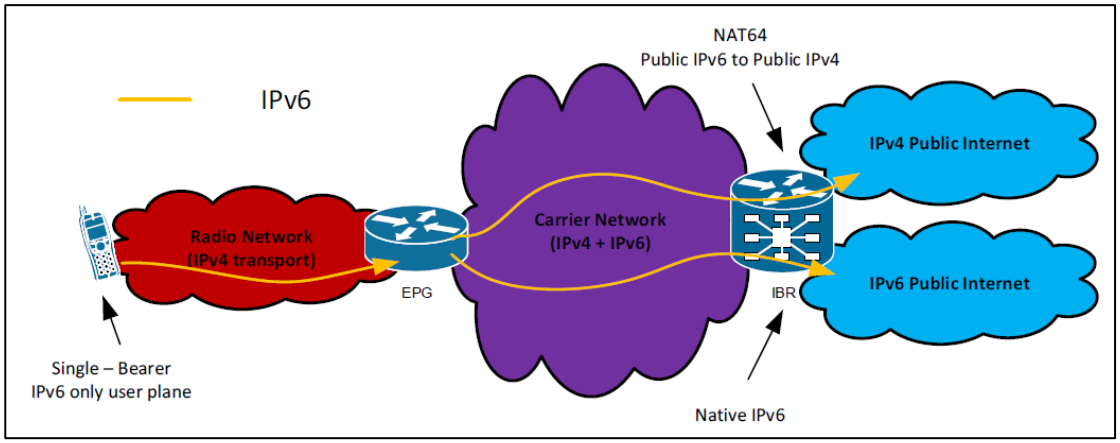


圖 12 IPv6的行動通信話務流示意圖

[資料來源：講者簡報]

目前已獲致的成果是：大多數主要的內容供應商都在提供 IPv6 可達性、某些提供商已經在其應用商店中強制要求支援 IPv6，並且所有新應用都必須支援本地 IPv6、網路正在發展以支持新的 IPv6 連接--SS 或 DS、設備開始支援 IPv6、由於更多應用程式和設備支援 IPv6，因此降低對 464xlat 的依賴性。未來尚待克服的是網路的複雜性。加值服務或數據封包處理目前仍需要手動的步驟。每條路徑可能需要一個唯一的 VPN 或 PBR 來定義其路徑。隨著加值服務的增加，網路複雜度呈指數增長。其次是網路功能的虛擬化可能會降低網路功能的成本，但不一定會降低網路的複雜性。每條路徑可能需要一個唯一的 VPN 或 PBR 來定義其路徑。服務越多，將變得越複雜。

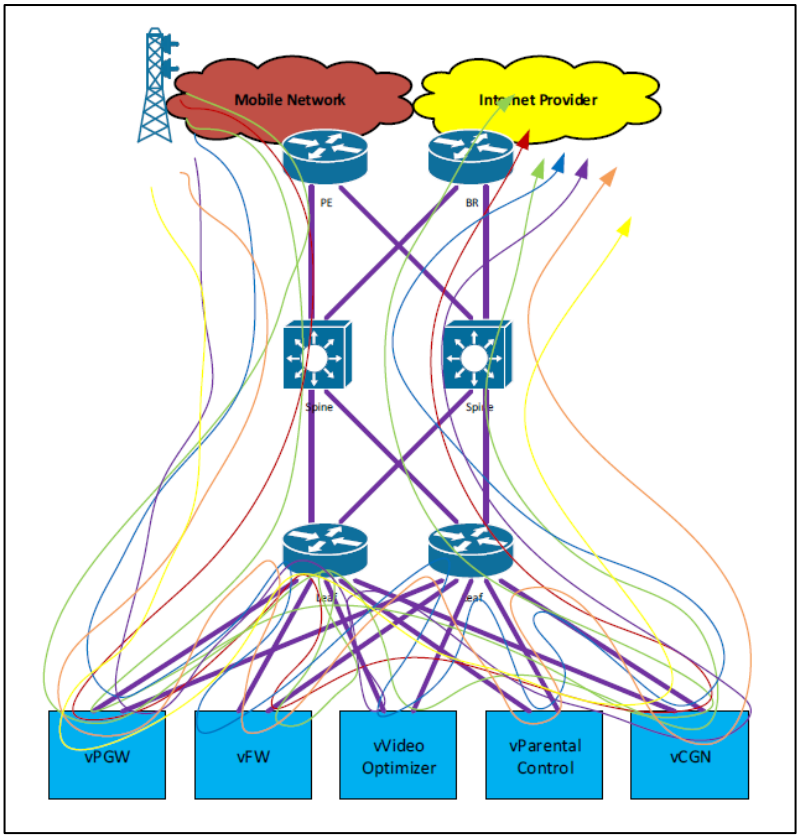


圖 13 網路功能虛擬化的複雜性

[資料來源：講者簡報]

軟體定義網路(SDN)只解決許多問題中的一個問題。軟體定義網路對許多人而言意味著許多不同的事情。SDN 是簡化網路服務鏈的一種方式，可用來 1.識別用戶；2.根據用戶的訂閱為用戶分配一個服務鏈；3.編輯網路，將該用戶的數據封包導向相應的 VNF。

5G 需要超低延遲，具體取決於所需的網路分片及其背後的應用。在某些時候，我們必須將電信雲移得更靠近用戶，以提供 1. VNF 中的服務功能；2.虛擬化分組核心節點；3.媒體暫存；4.加值服務。與當前的行動接取技術類似，IPv6 的部署應關注用戶終端，因為這是對位址空間存在壓力的地方。O&M 網路可以跟著使用雙堆疊，而最終移除 IPv4，成為純 IPv6。物聯網將需要大規模的企業網路解決方案。此外，將網路切片將增加基礎設施定址的壓力。

遙測技術正在推動具有非常大的電池壽命和低成本設備的專用無線設備的開發。系統允許客戶控制自己的 SIM 卡。傳統的企業解決方案允許重用位址空間，因此可能不會成為轉向 IPv6 的關注焦點，但隨著 IOT 的出現，解決方案的規模將會增加，並且

一些客戶可能會要求 IPv6 提出要求。核心將需要支持一套解決方案來滿足客戶的需求，其中一些解決方案並不是新方案。

我們的目標是將 IPv4 私有和公共位址全面從整個網路中刪除，只啟用必要的 NAT 轉換 IPv4aaS。因此，對於 IPv6 我們還有很長的路要走，而這只是起點。

（六）Route Security **BOF**

網路上愈來愈多的網路連結在一起，且彼此透過 BGP 協定進行訊務交換，業者間並以 TRUST 為基礎來運作，但此特質卻被不法分子利用，近來 Google、Facebook 等大型網站被劫持的事件層出不窮，因此路由安全的議題甚被重視。

今天除與談人與聽眾對於究竟是內容提供者、平臺提供者或由誰來承擔更多路由正確性責任分站不同觀點外，主持人也趁著這次難得的機會，對所有與會者進行一場線上調查活動，調查內容及結果摘要如下：

- 超過 9 成與會者認為：路由安全很重要。
- 近 1/3 與會者：難以啟齒曾經經歷與路由安全相關的網路不尋常事件。
- 近半數與會者認為：路由安全無法落實的主要原因為不具誘因。
- 近 3/4 與會者認為：由群組自發性落實路由安全才是驅使路由安全的關鍵。

圖 14 Route Security座談

二、第二日會議摘要

（一）APNIC NIR SIG

NIR SIG 會議旨在透過分享各國網際網路註冊機構之營運、政策及程序，以促進各機構境內、各註冊機構間及與 APNIC 秘書處間更緊密合作。本次會議首先由主席 Shyam Nair 先歡迎大家參加會議，並說明 2018 年將進行 APNIC 每 2 年 1 次的調查作業，網路調查將從 6 月份開始，以蒐集會員及其他主要利益關係者對 APNIC 的回饋意見，請大家參與，調查結果將在 Noumea 的 APNIC 46 上發布。

接著依序由大陸(CNNIC)、越南（VNNIC）、我國（TWNIC）、印尼（IDNIC）、印度（IRINN）、日本（JPNIC）等報告更新其會員成長及 IPv4、IPv6、ASN 等資源核配最新資訊，以及其對於會員之相關培訓情形及最新規畫。

1、CNNIC update

在 CNNIC 簡報中，值得注意的，中國大陸在 106 年 11 月發布大規模部署 IPv6 的國家行動計畫（2018-2025），預計於 2025 年全部的網路、應用及終端設備均將完全轉換到 IPv6。

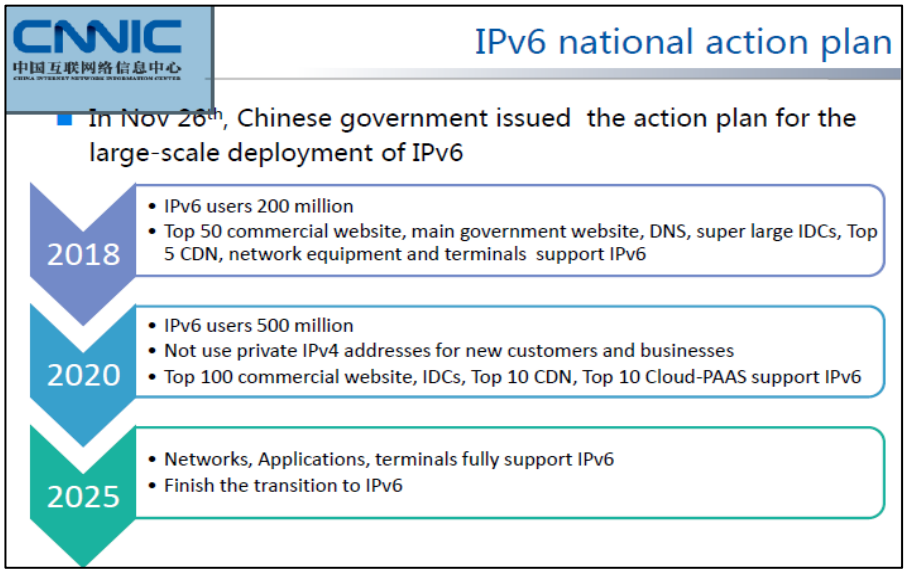


圖 15 中國大陸IPv6行動計畫

[資料來源：講者簡報]

2、VNNIC update

VNNIC 簡報強調與 APNIC、JPNIC 等機構的緊密合作，並說明該國為提升 IPv6 推展，VNNIC 不但舉辦多場研討會，並於 2017 年成立專案小組，在資訊通信部副部長帶領下，目前 IPv6 雖僅約占 10%，但在政府部門帶頭及主要電信業者已陸續加入推動下，預計 2019 年起將有很好的成效。

圖 16 VNNIC教育訓練規畫

[資料來源：講者簡報]

3、TWNIC update

我國 TWNIC 係由王彥傑工程師進行簡報分享，除更新 TWNIC 會員、IPv6、IPv6 位址核配最新統計外，並說明 2017 年 12 月 12 至 15 日舉辦的「2017 Taiwan Internet Forum and 29th TWNIC IP Open Policy Meeting」會議，歡迎有興趣者可到官網查看。另指出我國在 IPv6 推動上，於 2017 年下半年由 3 大行動業者進行試驗計畫，獲致良好的成果。針對 TWNIC 的簡報，JPNIC 與會者詢問，TWNIC 如何成功吸引電信業者參與網際網路論壇，王工程師回應表示，邀請不同領域專家參加並提供豐富資訊應該是關鍵。另來自 IRINN 的與會者則詢問，為何我國 IPv6 的核配能在 2005 年、2006 年間極快速的成長？TWNIC 黃執行長勝雄說明，TWNIC 從 2005 年開始核予大部分會員很多的 IPv6 區塊，所以有很大的成長，但因為沒有實際大量使用，以致 2006 至 2018 年間 IPv6 的核配幾無成長。

圖 17 我國4G IPv6試驗計畫

[資料來源：講者簡報]

4、IDNIC update

IDNIC 說明該國網際網路進展狀況，指出該國有 Open-IX（Open-Internet Exchange Point）及 IIX（Indonesia Internet Exchange）2 個訊務交換中心，Open-IX 的訊務量達 380G，IIX 則有 50.6G。因為訊務分散，所以 IIX 目前有 11 個交換點，且持續依訊務需求增建中。另為強化技術人員 IPv6 的知識，IDNIC 已規劃在各地舉辦相關教育訓練。

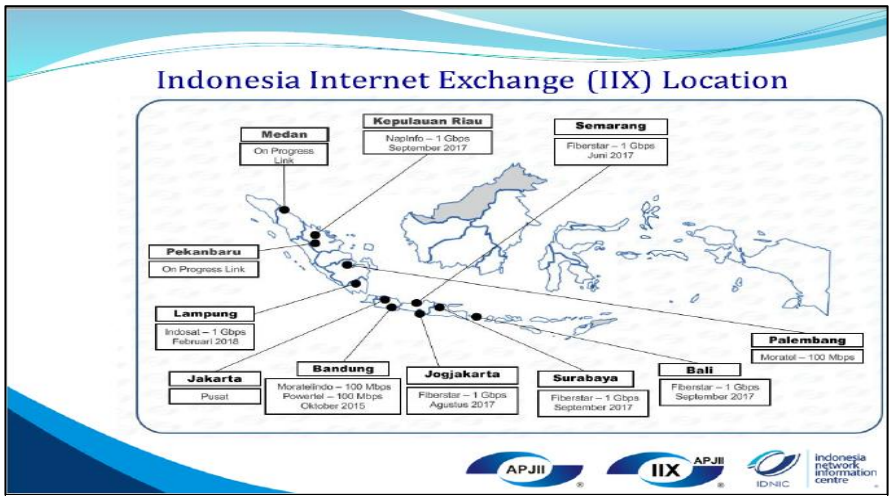


圖 18 印尼IIX配置

[資料來源：講者簡報]

圖 19 APJII教育訓練規畫

[資料來源：講者簡報]

5、IRINN update

IRINN（Indian Registry for Internet Names and Numbers）代表簡報指出，該國無論 IPv4、IPv6 或 ASN 的核配數均呈現逐年上升的趨勢，在 IPv6 的部署上，更是名列全球前 15 名。該組織亦經營訊務交換中心（Internet eXchange Point），目前全國有 8 個交換點，儘可能使訊務在地交換，避免國際路由交換。

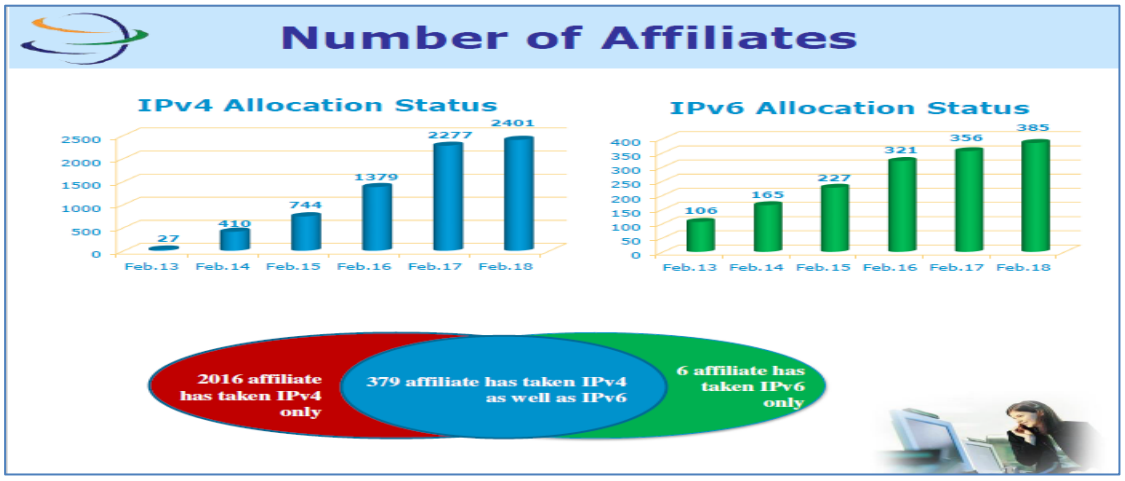


圖 20 IRINN IP位址配置情形

[資料來源：講者簡報]

6、JPNIC update

JPNIC 代表說明該機構為了促進 IPv6 部署，基於「IPv4 耗竭專案小組」提供許多知識予技術營運者，除舉辦技術研習營，讓學員進行實作。目前也開始針對非技術人員（例如行銷及客戶支援部門）研討會，希望這些部門人員開始支持 IPv6。同時辦理 RPKI 研習、Open Policy Meeting 等活動。

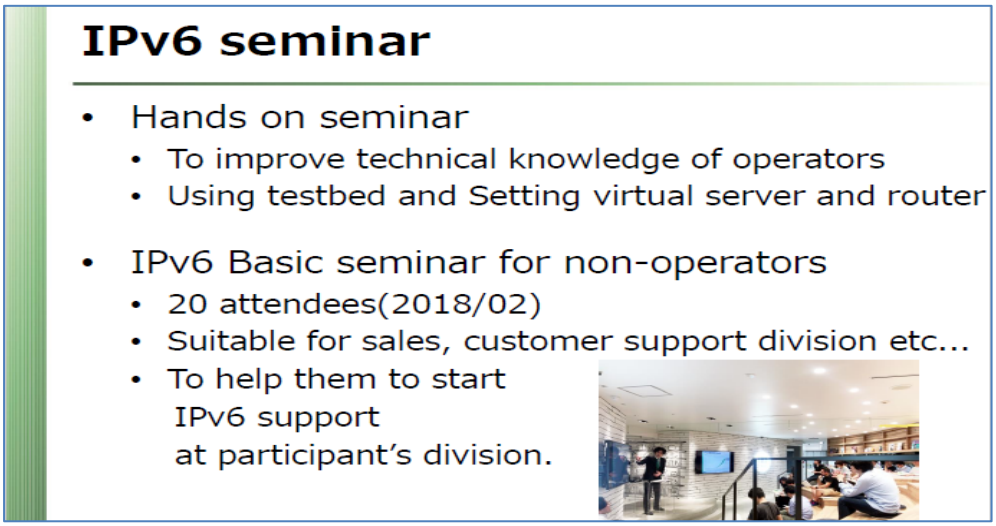


圖 21 JPNIC IPv6 研習活動

[資料來源：講者簡報]

會中主席詢問各 NIRs 會員成長趨勢形，印尼及越南代表均表示，愈來愈多獨立 IP 位址的釋出，許多企業為網路連結備援考慮而加入會員，故會員數仍會持續成長。TWNIC 黃執行長則說明，以往 TWNIC 會員以 ISP 為基礎，擬加入會員必須先取得政府許可執照，目前該中心已修改其會員政策，未來會員數應可有所成長。

圖 22 TWNIC執行長發表意見

圖 23 NIRs報告人合影

（二）Introduction to SDN

軟體定義網路（Software-Defined Network，SDN）是近幾年快速新興的網路架構，主要的概念是將傳統的網路區分為Application 、Control及Infrastructure Layer（或稱Data Layer）三層，其中Application Layer 是指應用及服務的部分；Control Layer，一般又稱SDN Controller，是網路控制的核心，包含許多控制模組（Control Program/Bundle）；底層Infrastructure Layer的部分，即硬體交換機（Switch）設備。

在SDN架構中，所有底層設備（Switch）皆交由SDN Controller集中控制；SDN Controller負責維護所有網路架構，並利用軟體來定義網路中所有資料傳輸路徑。因為SDN可程式化（Programmable）特性，開放式API的概念也因應而生。透過開放式API，不同廠商開發之SDN Controller，即可連接控制同廠牌或不同廠牌的SDN Switch，大幅提升網路資源的控制彈性與使用效率，以因應未來網路的快速成長與多元化。

儘管外界炒作，但SDN仍是當前網路技術的一種重要演變，不過目前並無一個SDN定義為大家所認同，只知SDN是一種新的資料網路架構框架，只要是所採的協議或技術，可以將控制層集中化、抽象網路和拓撲、及強化標準介面的可程式化，就可視為SDN技術框架的一部分。

很多人認為SDN與NFV是類似技術，實際上，SDN處理的是開放式系統互聯通信參考模型（OSI）中的2-3層（即Network、Data link Layer），NFV處理的是4-7層（即Application、Presentation、Session及Transportation Layer）。簡言之，SDN主要是優化網路基礎設施架構，比如乙太網路交換機，路由器和無線網路等。NFV主要是優化網路的功能，比如負載均衡，防火牆，WAN網優化控制器等。

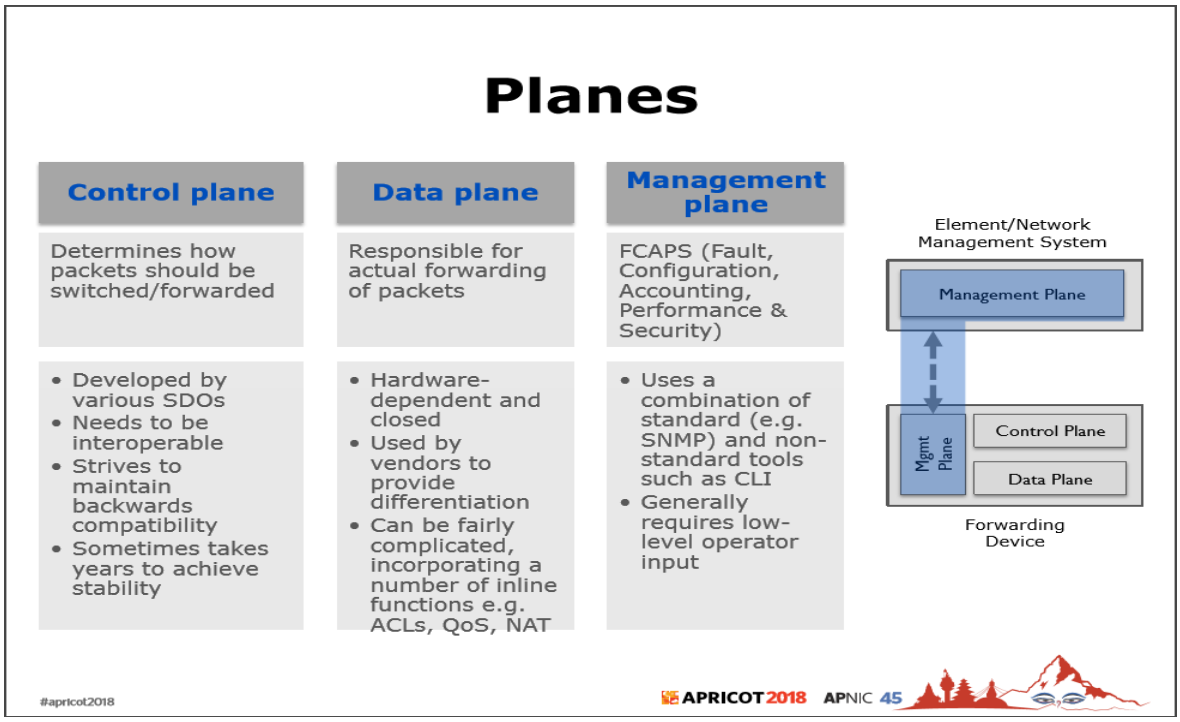


圖 24 SDN各層介紹

[資料來源：講者簡報]

（三）DNS/DNSSEC

網域名稱系統（Domain Name System, DNS）是一個缺乏安全性設計的分散式架構，各種轉稼（Pharming）、偽裝（Spoofing）、快取下毒（Cache Poison）與阻絕服務（Denial of Service）等攻擊手法，均涵蓋著DNS區域傳送的安全性、動態更新的安全性，偽裝資料和快取記錄污染等問題。

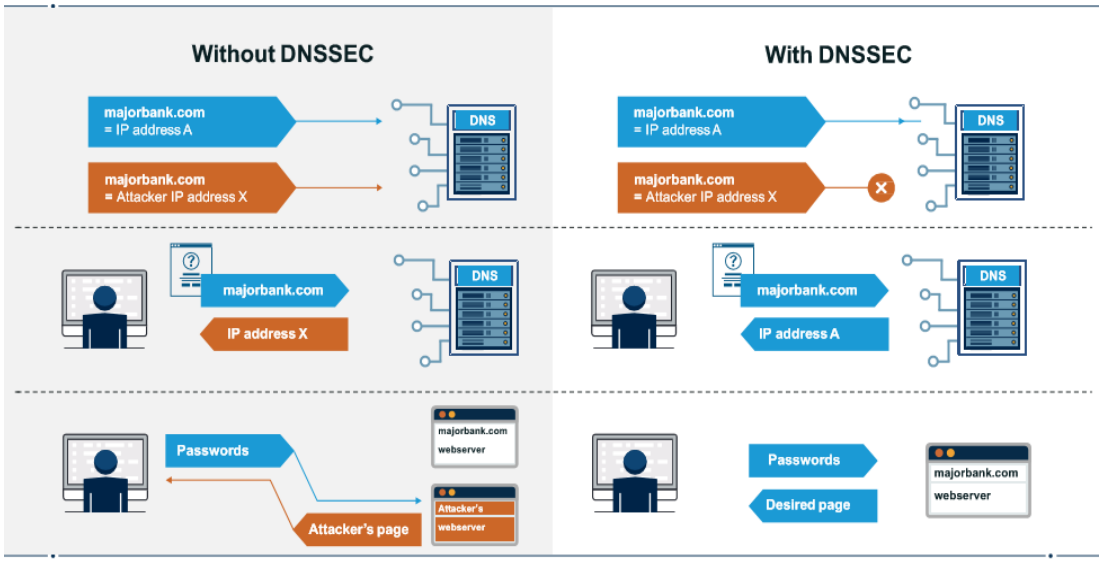


圖 25 DNSSEC 運作概要

[資料來源：講者簡報]

DNSSEC是DNS資料的安全認證機制，利用非對稱金鑰的技術對DNS資料進行簽章，並未改變任何DNS的查詢/回覆/錯誤/流程，向下相容現有DNS協定的方式。另增加DNSKEY、RRSIG、NSEC/NSEC、NSEC3PARAM及DS等欄位，並進行資料驗證。DNSSEC之引用雖然造成部分網路資源損耗，但依然瑕不掩瑜，相關優點如下：

- 消費者：更有自信的使用網際網路
- 網際網路位址或網域名稱註冊人：減少欺詐和更好的品牌保護
- 受理網際網路位址或網域名稱註冊機構：遵守業界標準及符合網際網路位址或網域名稱註冊人對於安全性的要求
- 網際網路位址或網域名稱註冊管理機構- 符合業界最佳實踐方案及受理網際網路位址或網域名稱註冊機構對於域名安全的要求。
- 保護查尋目錄（Lookup Directory）
- 補充其他技術（https）
- 為其他安全改進作為提供平台

瑞典網際網路位址或網域名稱註冊管理機構（registry）是最早採用DNSSEC的註冊管理機構，於2005啟用，後來跟進的包含NL、BR、CZ及PR等。現行已超過90%的頂級網域名稱註冊管理機構及約50%的國家級網域名

稱註冊管理機構已簽屬將採用DNSSEC。其中49% .NL的域名防護已採用DNSSEC，50%以上 .CZ、58%以上 .NO都已簽屬將採用DNSSEC。

DNSSEC機制中，使用兩種非對稱金鑰，分別為KSK（Key Signing Key）和ZSK（Zone Signing Key）。這兩種KEY的目的不同，ZSK是用來針對zone file內容進行簽章，KSK僅用來對ZSK簽章，這樣區分的方式有很大的好處，因為DNSSEC是由root DNS一層一層往下驗證下來的，所以任一層KEY的更換都要通知上一層進行指向調整，分成KSK和ZSK之後，只有KSK更換需要調整上一層DNS的DS（Delegation Signer），ZSK的更換只要KSK對ZSK重新作一次簽章就可以了。

KSK密鑰與任何密碼一樣，從一而終或是和鑽石一樣亙久不變是極度危險的，Root Zone的KSK公鑰和私鑰亦同，所以更換KSK是一個非常重要的安全措施。但更換Root Zone的KSK，採用DNSSEC驗證的解析器都會受到影響，直接更換可能造成驗證錯誤問題，因為解析器以暫存的舊KEY驗證新KEY簽章的資料。

ICANN原訂2017年10月11日進行Root Zone KSK更換，但同年9月19日發現，更換標準ZSK造成DNSKEY回饋量超出預期，爰於9月27日緊急喊卡，直到蒐集到足夠資訊，確定情況轉好，並與網路社群討論相關重要過程（2018年2月1日至4月1日對外意見徵詢）後，方進行Root Zone KSK更換。

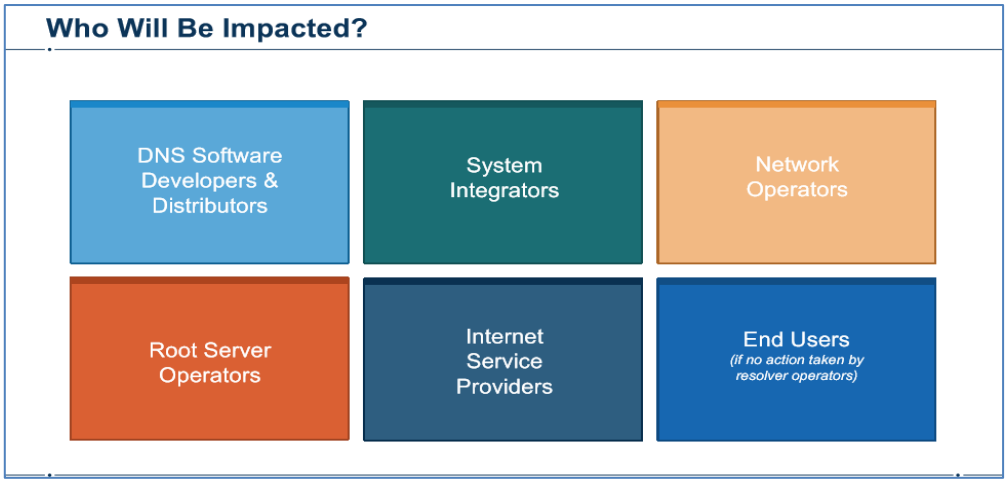


圖 26 Root Zone KSK更換涉及相關利害關係人

[資料來源：講者簡報]

簡言之， DNSSEC係著重於由用戶端驗證DNS回應資料的正確性（含資料來源正確性及不存在的驗證）及完整性，並透過數位簽章來進行驗證，而非為了防禦DDoS攻擊、處理隱私權、使用開放金鑰架構及防禦IP偽裝等。

雖然DNSSEC強化及延伸DNS服務安全性，但仍無法解決所有DNS服務所面臨的所有安全性問題，且無法提供私密性及可用性之安全性服務。

（四）Peering and Interconnection

（第1場次）

會議由Equinix的 Raphael Ho擔任主持人，首先介紹今日3場Peering Forum的議程，並預告後續相關活動規劃，包括將於8月14-16日在Combodia舉辦的Asia Peering Forum，及於10月23-25日在香港舉辦的APIX Peering Asia活動。此一系列論壇活動，除了提供相關產業專業分析及經驗分享外，亦是提供業者尋求商業合作的媒合活動，相關簡報重點如後。

1、Interconnectivity within South Asia

Hurricane Electric公司的Anurag Bhatia分析南亞地區包括阿富汗、孟加拉、不丹、印度、馬爾地夫、尼泊爾、巴基斯坦及斯里蘭卡等國的網路互連不足的情形，他指出南亞地區除孟買有12條海纜登陸外，其餘地區都很少（約1~3條）。由於目前南亞多個國家間並沒有直達陸纜或海纜，以尼泊爾和孟買為例，尼泊爾路由必須由海纜繞到英國倫敦交換中心，再由海纜到達孟買，造成高延遲與路由品質不佳。

他分析業者不願直接互連的理由包括商業考量（例如電路成本：海纜電路成本比直接互連的成本還低，ISP 寧願繞到新加坡等地互連；區域營運商希望較高的頻寬售價，Gobal的transit價格比國內互連便宜，導致其他ISP成本考量選擇頻寬較差的路由）；技術問題之路由規劃（部分南亞地區ISP尚未提供v6路由）、法規問題（例如印度對連接至國外有嚴格的特別規定，所以，像孟加拉及印泊爾要在印度設置互連節點及機房，就比在香港、新加坡困難）；其他因素（例如政治關係緊張）。

圖 27 路由不良的成因

[資料來源：講者簡報]

2、The Story of NPIX

NPIX的Indiver Badal則向大家介紹NPIX（NEPAL IX）的創設及發展歷程，該中心是非營利的公司，每月只收會員費100美元。Indiver說明尼泊爾受地理環境限制，早期擬與外界的連接始終是一個挑戰，必須依賴昂貴的衛星鏈路連接香港、印尼、新加坡等，不但網際網路服務非常貴且也阻礙了本地內容的發展。2002年在APRICIC執行委員會現任主席Gaurab Raj Upadhaya從APRICOT 2002返回之後，由幾名業者網管工程師在網路專家的幫助下聯合起來建立了尼泊爾的第一個網際網路交換中心NPIX，當時的設立宗旨是在此交換本地流量、降低成本、提高質量和性能。

Indiver說明，當時成立了委員會並在2002年8月30日啟動了NPIX的第一個交換點，最初連接了三個成員，當時大部分流量都來自美國、歐洲等地，且因為大多數連接都是無線連接，流量有限。經過6個月的運營，委員會決定在其中一個成員的機房中增加第二台交換機，其中大多數ISP已經使用銅線租用線路連接。儘管提高了連接速度，但直到2008年將第二台交換機從成員的場所搬到位於加德滿都Putalisadak的中立數據中心，提供光纖連接，讓更多的人可以使用網際網路並讓本地內容更易於發展，目前本地的內容託管迅速增長，這對IXP的經營也非常有幫助。

Indiver認為NPIX是一個由不同網路營運商進行團隊合作而改善整個經濟發展的例子，從NPIX的成功中學到三個重要經驗：

- **採取由下而上的方法**：它可以讓操作人員分享他們的想法並建立供應商參與的興趣。
- **培訓非常重要**：NPIX 需要動態路由和 BGP 培訓才能成功，提供培訓課程來幫助 ISP 配置他們的路由器。
- **形成 IX 社群**： NPIX 的持續成功歸功於本地業者的網管工程師們結合成一個本地網際網路社群，樂意在互惠項目上進行合作，公開討論、分享營運經驗。

3、Dissecting the African Internet: An Intra-Continental Study

來自AFRINIC的Amreesh Phokeer則簡報「Insights into Africa's country-level latencies」，其表示經過3個月對國家間進行的封包延遲（RTT）測速，平均延遲為非洲地區約78ms、拉丁美洲及加勒比海地區約76ms、北美地區約40ms、歐洲地區約30ms，非洲地區封包延遲嚴重主要為高度仰賴向上游購買轉訊，且訊務多流向海外（例如衣索比亞是100%，往歐洲的延遲354ms、往北美的144ms），因此Google、Facebook等媒體業者多使用CDN來降低封包延遲。

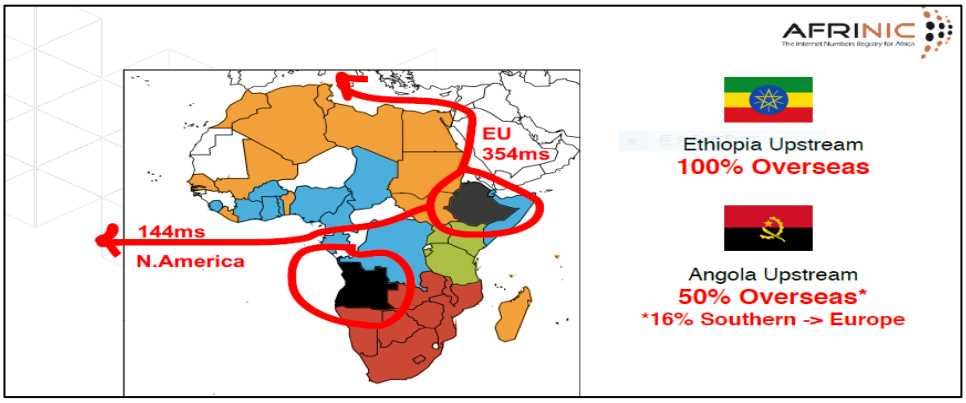


圖 28 境外封包延遲

[資料來源：講者簡報]

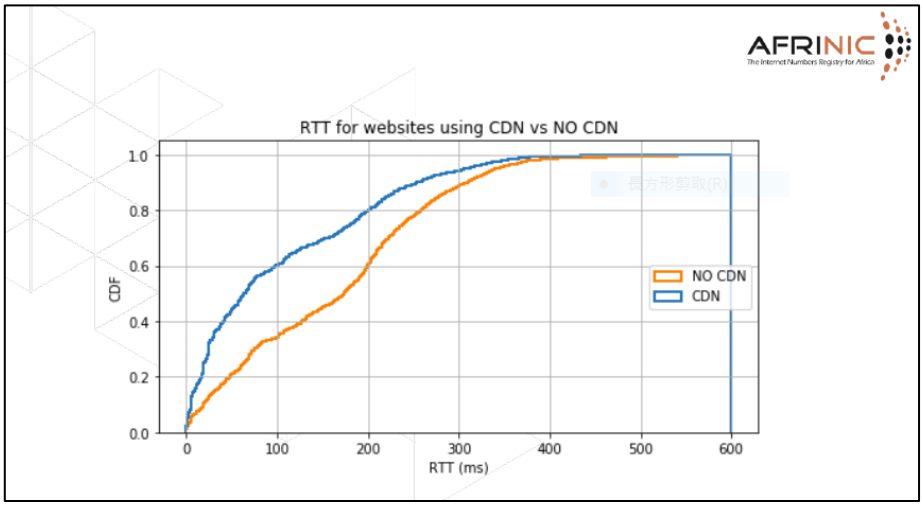


圖 29 CDN改善延遲

[資料來源：講者簡報]

4、Peering Personals

本場次Peering Personals活動，共有twitch、Limelight、Akamai、facebook、ChineCache、Globe Telecom、Amazon等7家與會業者上臺，簡報其相關互連政策及聯絡資料等資訊，期能進行相關互連合作機會。

（第2場次）

5、Market Launch Guide

Hurricane Electric公司的Walt Wollny則簡報菲律賓2家主要電信業者PLDT 與Globe Telecoms於2015至2018年間，無論其網際網路訊務量、路由表路由、互連及轉訊均快速成長，早期2公司間並未互連，訊務均透過國際Tier 1、Tier 2業者遞送，為改善境內網際網路訊務品質，資通訊龍頭PLDT自2016年6月16日開始與Globe Telecoms建立雙邊互連（bilateral IP peering）協議，但結果2公司間本地訊務卻低於2%且封包延遲仍非常高；Globe到PLDT有66%以上封包超過200ms，PLDT到Globe則有40%以上封包超過200ms。大量的訊務是遠從香港、新加坡等境外而來，從用戶需求、服務效能、成本等諸多需求來看，仍有基礎網路建設、CDN、IXP等許多問題待克服。

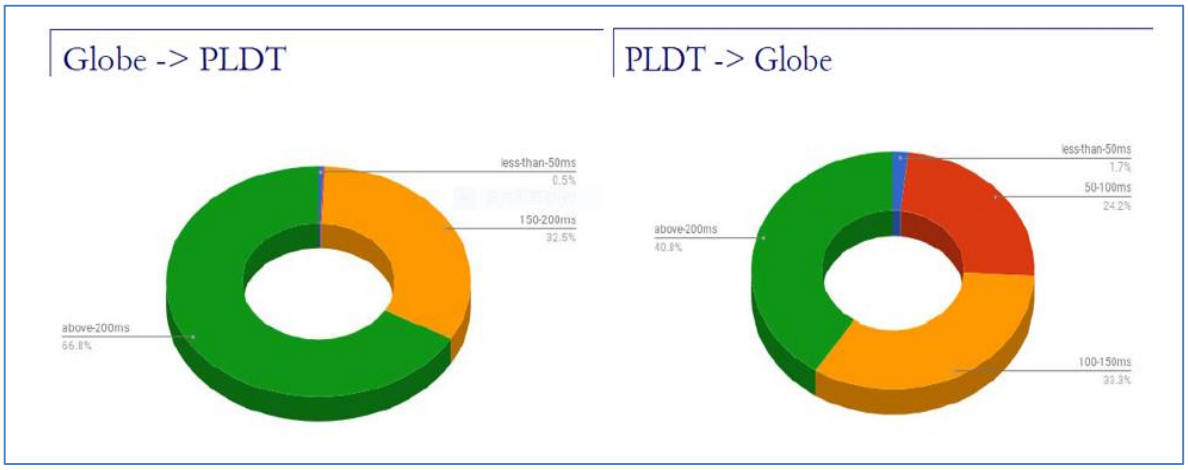


圖 30 菲律賓境內封包延遲情形

[資料來源：講者簡報]

6、Introduction to PeeringDB

PeeringDB公司的Arnold Nipper則向與會者說明PeeringDB是一家非盈利的會員制組織，主要用於方便用戶維護互連所需資訊。同時說明會員條件、組織運作原則、運作方針並展示如何使用PeeringDB。

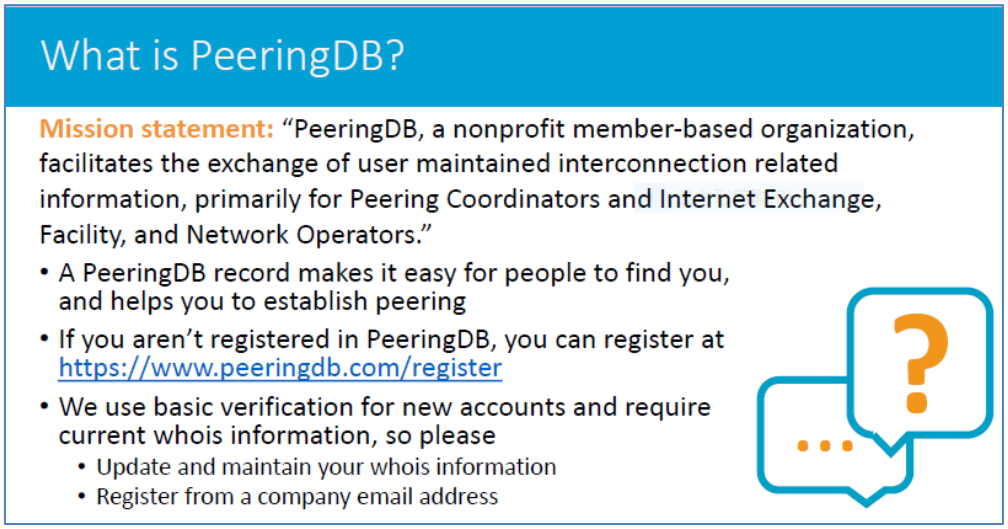


圖 31 PeeringDB 使命

[
資料來源：講者簡報]

7、Peering in Japan from JPNAP Perspective

JPNAP營運長Katsuyasu Toyama首先介紹JPNAP的營運概況，包括目前在東京及大阪各有1個獨立的IXP節點，2節點間並無連接；2018年2月訊務

交換量達1.29T（東京1T，大阪292G），在2017年2月約0.8T，成長快速。他並說明日本政府從2003開始鼓勵3大電信公司、電力公司及有線電視業者建設光纖到戶（FTTH），因投資金額龐大僅NTT及電力公司參與建置。目前FTTH已涵蓋日本99%地區，使用率為53.6%，其政府試圖提升偏鄉的使用率寬頻發展情形，並說明日本的IXP發展情形：主要有JPNAP、JPIX、BBIX、EIE，內容業者接入每個IXP，而小型EYE BALL則接入1或2個。

Katsuyasu提及日本OTT業者基於商業及備援等考量，當東京訊務成長後，會分散訊務到大阪，所以JPNAP大阪節點成長快速。

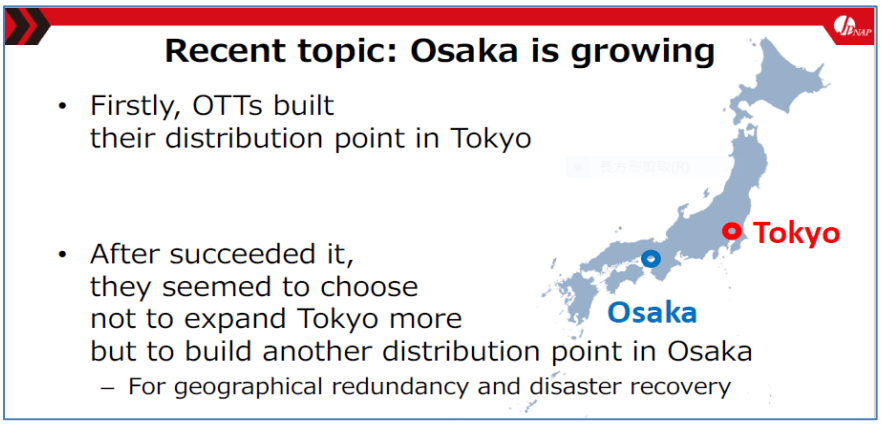


圖 32 JPNAP 節點分布

[資料來源：講者簡報]

Katsuyasu表示，日本Peering市場狀況與各國相同，規模較小的網路業者及內容業者多持開放政策，但上游Tier-1、Tier-2業者及大的網路業者則持限制或選擇性的政策。

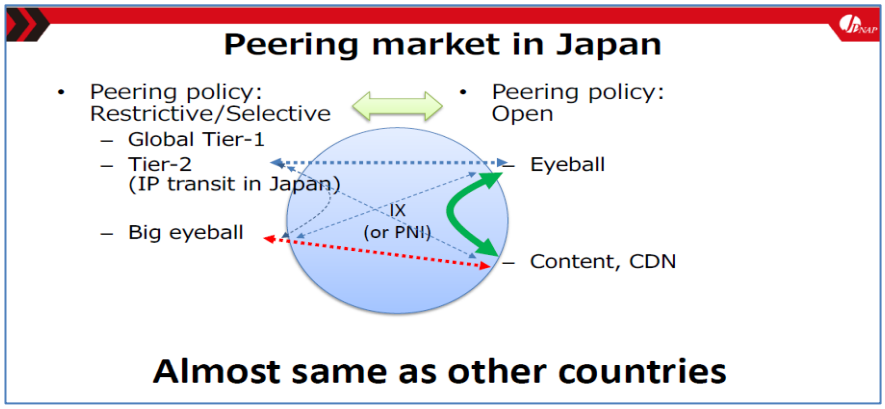


圖 33 日本PEERING市場情形

[資料來源：講者簡報]

Katsuyasu強調日本IXP市場非常競爭，JPNAP雖為NTT投資成立，但屬「中立的」交換中心，不強迫使用NTT電路，會員可選擇不同業者電路。

我國是方電訊公司魯堯協理詢問講者，為促進Peering市場競爭，由政府投資設立IXP的可行性？Katsuyasu回應，日本政府也曾考慮過此方案，但大型ISP沒有加入的意願，是不會成功的，所以就作罷了。

8、Peering Personals

本場次Peering Personals活動，共有我國是方電訊、Yahoo !BB、CAT、PCH、Cloudflare等業者上臺簡介。

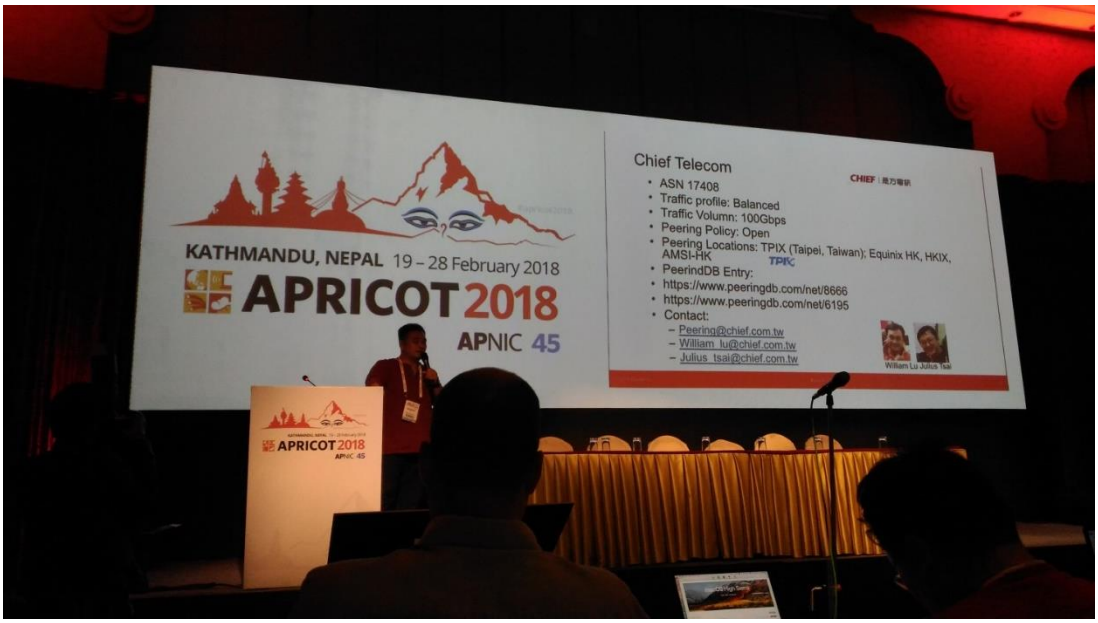


圖 34 是方電訊進行簡介

（五）Peering Forum：IXP Session

1、APIX update

APIX協會（Asia-Pacific Internet Exchange）主席Katsuyasu TOYAMA表示，該協會2010年創立，是由亞太地區IXP組成，主要提供會員分享資訊、經驗及共同討論所面臨問題的解決方案。目前係由17個地區及國家的25個IXP組成，我國的是方電訊已是成員之一。

圖 35 APIX會員組成

[資料來源：講者簡報]

Katsuyasu指出，APIX於2017年11月在日本京都舉辦Peering Asia 1.0論壇，這是一個開放且中立的活動，可以共同促進亞太地區的Peering發展。本次論壇共有來自亞太地區、北美及歐洲的239位與會者，9成與會者均表示將再參加第2次論壇，經與會者投票表決，Peering Asia 2.0將於香港舉行，目前已規劃於2018年10月24、25日辦理並由HKIX及HKNOG主辦。

圖 36 Peering Asia 2.0論壇規畫

[資料來源：講者簡報]

2、Security Project FENIX

NIX.CZ執行長Martin Semrad則介紹捷克的FENIX資安專案，該專案源自2013年3月長達4天的DDOS攻擊後，於2014年1月由6個會員發起，目前已有19個成員，共同進行相關組織運作及技術規定，致力建立「值得信任」的關係。

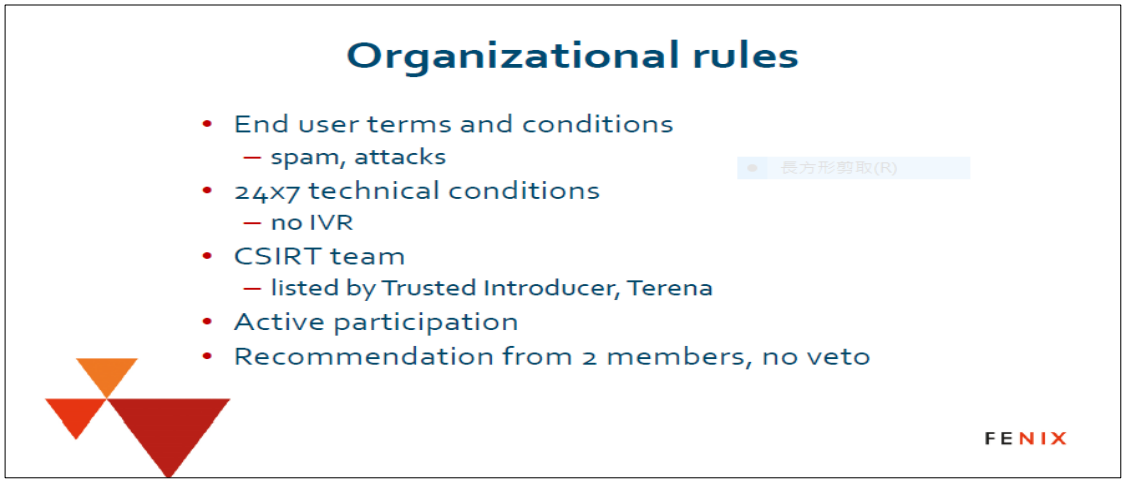


圖 37 FENIX資安專案組織規定

[資料來源：講者簡報]

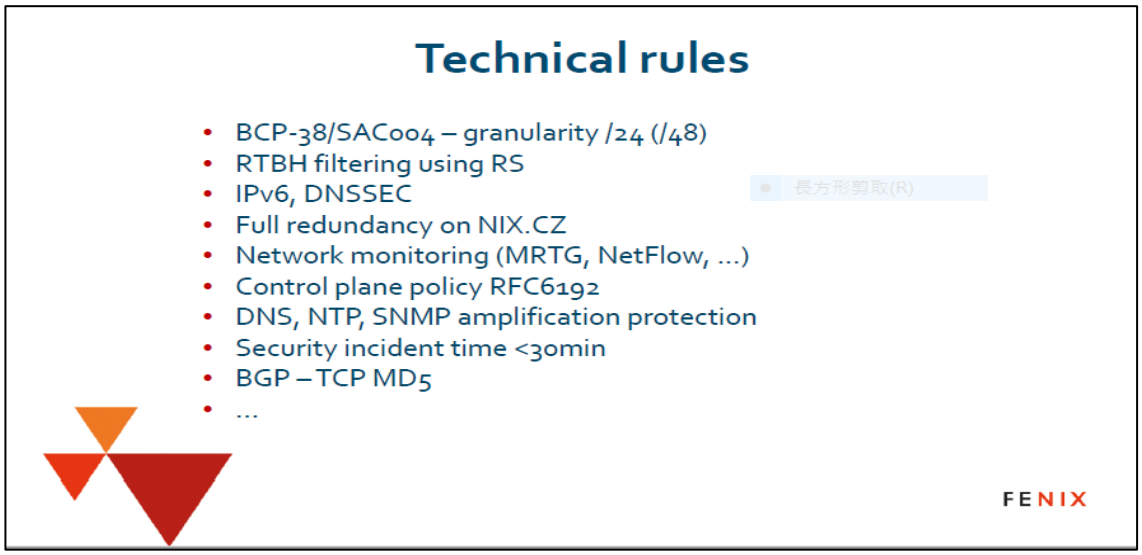


圖 38 FENIX資安專案技術規定

[資料來源：講者簡報]

3、IXP Database and tools

EURO-IX秘書長Bijal Sanghani說明，因為網際網路交換中心（IXP）是能夠讓三個或更多網路達到互連的網路設施，能夠促進網際網路互連流量，因此IXP被認為是網路互連基礎設施的核心，其訊務交換量占全世界網際網路流量占比越來越高。

她闡述網際網路交換聯盟（IX-F, Internet eXchange Federation) 開發的IXPDB（Internet eXchange Point Database）平臺的目的，是要自動化的將在IXP所產生的數據進行擷取、彙整及分析，產出可視覺化、有價值的報告，可提供網路經營者、研究人員在全球網際網路互連生態中做出明智決策。她不但向與會者說明該資料庫所蒐集的重要資料，並說明如何利用該資料庫。

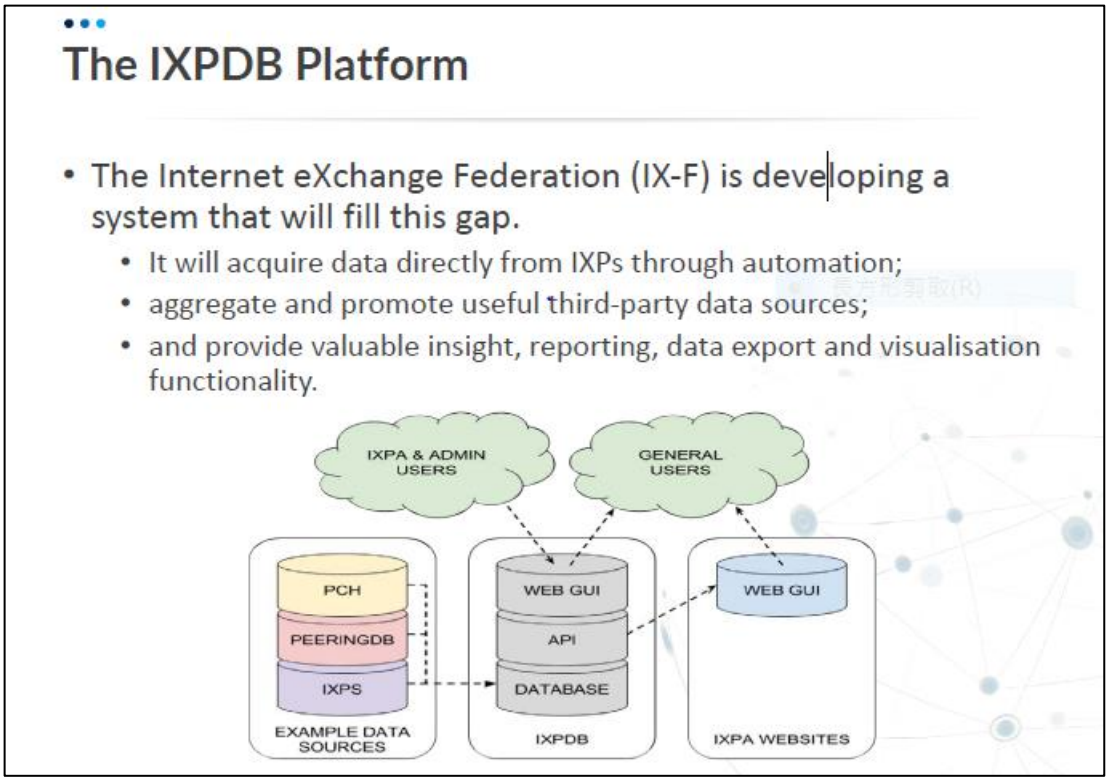


圖 39 IXPDB的目標

[資料來源：講者簡報]

4、IXP Automation with SaltStack and NAPALM

INEX的CTO Nick Hilliard強調，對於確保一致性的設備組態配置管理以及降低錯誤的發生率，網路堆疊組態配置自動化至關重要。他簡報分享INEX改善IXP Manager軟體自動化功能的歷程及經驗。

他說明早期開發的IXP Manager軟體雖能儲存會員交換器組態配置資訊，但因欠缺相關網路設備介面之支援工具，想利用所擁有資訊進行組態配置的改善及部署，結果卻是成本效益不佳。經過了許多的努力，INEX已將REST API功能構建到IXP Manager中，讓IXP經營者在其網路設備上提供完整的設備組態配置。

Nick說明如何將NAPALM和SaltStack整合到IXP Manager軟體功能中，以便在IXP環境中實現完整的自動化進行端到端、核心和路由協議組態配置；在簡報中，Nick非常完整分享其開發經驗給與會者，包括詳細說明Openflow、YANG、Vendor API等方法的特性差異，及其選擇NAPALM的理由，也說明從Ansible及 SaltStack中採用SaltStack的原因。對網管有興趣的讀者可參考其簡報：https://2018.apricot.net/assets/files/APNT806/inex-apricot-ixp-automation-2018.pdf

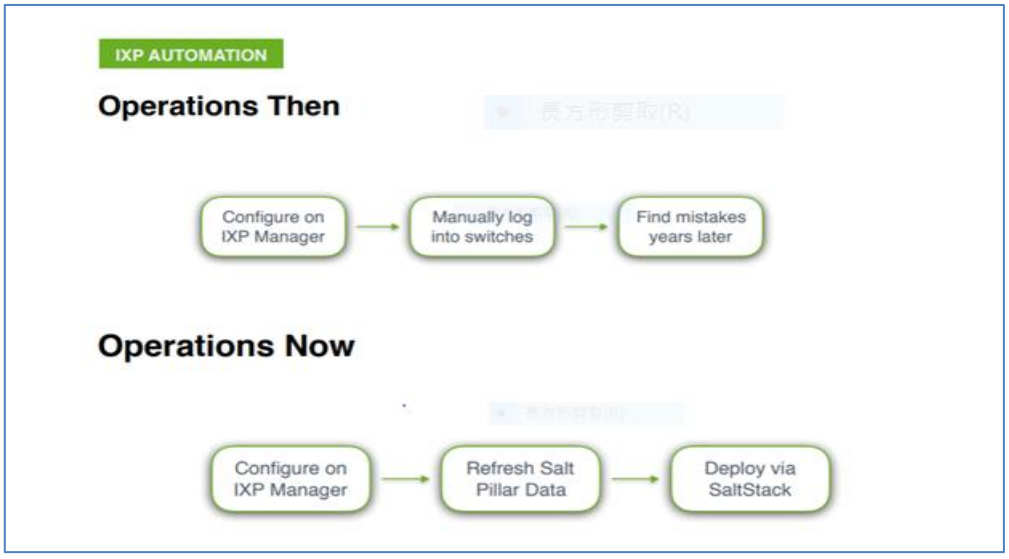


圖 40 IXP自動化的優點

[資料來源：講者簡報]

5、IXP Personals

本場次共有28個IXP向與會者進行1分鐘的自我簡介，期能有更多的合作機會；其中TPIX為我國是方電訊所經營，其他IXP包括AMS-IX、BBIX、BKNIX、CHNIX、Equinix-IX、Extreme-IX、HKIX、JPIX、JPNAP、MegaIX、MMIX、MumbaiIX、MyIX、NZIX、PhOpenIX、SGIX、Asteroid international、IX.br、DE-CIX、InterLAN、JINX、CINX、DINX、LINX、LONAP、 NIX.CZ、NIX.SK等。

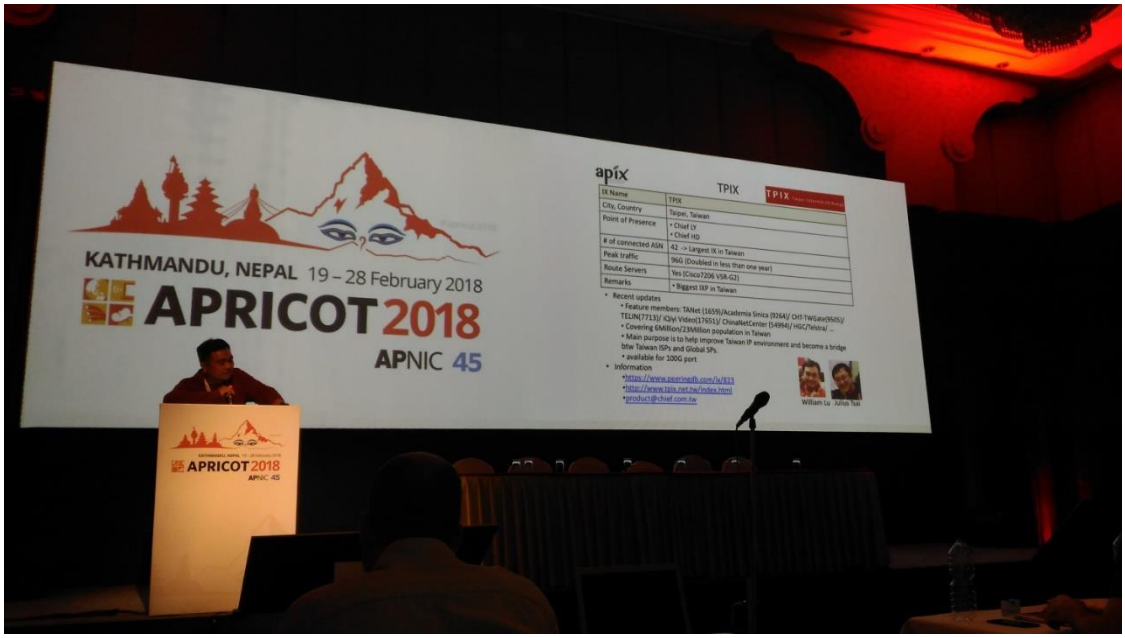


圖 41 TPIX上臺簡介

（六）APNIC IPv6 Readiness Measurement

IPv6 整備度度量會議係 TWNIC 於 2013 年在 APNIC 36 會議中倡議下形成。其目標是鼓勵一直致力於 IPv6 部署的組織，分享其 IPv6 整備度度量方法和結果。本場會議係由亞洲大學的曾憲雄教授主持，他表示，IPv6 整備度 BoF 專注於 IPv6整備測量和有幾種不同的類型準備就緒度量。 每個測量都可以提供某些方面具體的洞察力，所以不同的測量會導致不同的結果和不同的解釋。BoF 的目標不僅是提供分享資訊與交換 IPv6 環境知識的平台，同時也建立共同衡量標準。接著他分別邀請由來自澳洲 Telstra 公司的 Jeff Schmidt 先生、來自日本的 Hiroki Kawabata 先生、來自印度的 Ajai Kumar 先

生及來自台灣 TWNIC 的 Tim Wang 先生上台報告。

1、澳洲的 IPv6 整備度

Jeff Schmidt 先生表示，他是一名技術團隊經理，任職於 Telstra，負責管理一個建立 IP 的網路工程師團隊，以提供無線運輸服務。澳洲採行集中化 CGN，CGN 可執行 NAT / PAT 44 和 NAT / PAT 64，可大大減少公共和私有 IPv4 位址的需求，但並無法避免 IPv4 位址的耗竭。

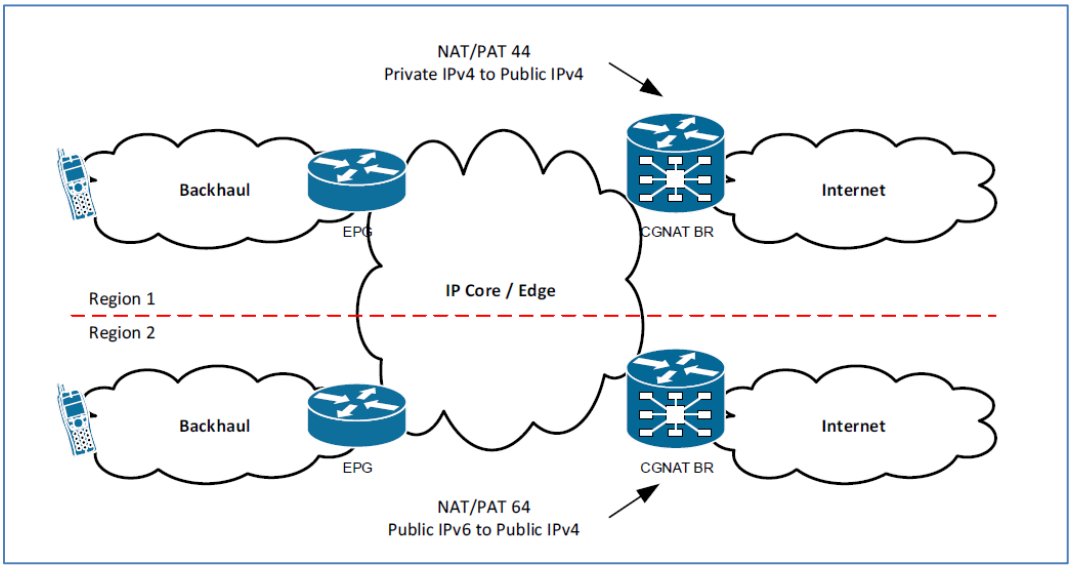


圖 42 IPv6採行集中化CGN示意圖

[資料來源：講者簡報]

Jeff Schmidt 接著分享澳洲的經驗。澳洲自從 iPad 進行雙堆疊(Dual-Stack)設定之後，澳洲的 IPv6 用量才開始明顯增加。目前澳洲政府擬定各項策略，以期由雙堆疊(Dual-Stack)過渡到單一堆疊(Single Stack)。由於係透過 iSO 修補程式進行更新，用戶不會立即覺察到他們的 iPad 可以使用 IPv6，進而達到透明移轉的效果。當 iPad 軟體更新到最新版本時，就能使用 IPv6。澳洲計畫在今年稍晚的時候部署單堆疊(Single Stack)。澳洲採用 DNS64 作為從雙堆疊(Dual-Stack)過渡到單堆疊的方式。DNS64 會同時查 IPv6 和 IPv4 的位置, 有 IPv6 就用 IPv6, 若沒有就將 IPv4 轉換為 IPv6。由於應用程式將繼續使用 IPv4，所以沒有 DNS64 的雙堆疊設備在由雙堆疊轉換為單堆疊所受到的影響最小。當啟用 DNS64 將增加設備使用 IPv6 的情形，並且可以在用戶的應用程式受到影響時很容易禁用。應用程式及協定的數量，以及採行特定措施能持續對轉移到 IPv6

單堆疊提出挑戰。隨著設備像 iPad 一樣改採 IPv6，例如雙堆疊模式，能增加 IPv6 位址使用量。且有越來越多設備內建支援 VoLTE，也提升了 IPv6 位址的使用量。澳洲過渡到 IPv6 單一堆疊所採行的策略是：透過運營商組態設定將設備逐一過渡、進行內部 APN 測試、單一設備改採雙堆疊模式、啟動 DNS64，以及針對不太常見的設備推動單一堆疊(Single Stack)。而在客戶支援方面，應儘早讓社群民眾參與，讓他們知道即將發生的事情，他們會感激你在發展階段就讓他們有機會參與。透過聯絡點收到表達支持的電子郵件要儘快回覆，不要讓用戶等待。讓用戶直接和工程師接觸。隨時向大眾報告頻寬使用情形。

2、日本的 IPv6 整備度

來自 JPNIC 的 Hiroki Kawabata 表示，JPNIC 就像 APNIC 一樣，將 IP 和 ASN 號碼作為亞太地區的國家互聯網註冊機構。在日本有許多業者在網際網路上提供各種服務，包括：內容及應用服務提供者、數據中心及雲端服務業者、ISP 業者、有線電視業者、固網接取網路(光纖到戶)業者、行動網路業者，而 IPv6 的部署與每個業者都有關聯。日本的 IPv6 整備情形，目前內容及應用服務提供者尚未部署，少數的數據中心及雲端服務業者有部署，主要的 ISP 業者透過 PPPoE 或是 IPoE 提供 IPv6 連網服務、有線電視業者則有部分業者已部署、行動業者將於 2016 年中或 2017 年開始部署、固網用戶約有 40%能透過 IPv6 上網、數據中心及雲端服務業者 IIJ 和 Sakura 明確宣佈將在 2017 年 4 月 19 日的“IPv6 雲端服務研討會”上提供 IPv6 服務。合計日本約有 23.24%是以 IPv6 上網。日本 IPv6 促進評議會致力於與政府、產業界、學術界及其他網際網路團體合作，以推廣 IPv6，同時有許多工作小組在運作，自 2012 年起針對 IPv6 的部署情況進行評量。IAjapan 則致力於農村推廣 IPv6。IPv6 部署委員會自 2003 年以來每年舉行一次區域 IPv6 高峰會。JPNIC 在日本負責 IPv6 位址的發放，就像 NIR，且與 IPv4 Exhaustion Task Force、IPv6 Promotion Council、IPv6 deployment committee、及 MIC 等組織團體合作，以推廣 IPv6。JPNIC 一共發放了 7,224 */32 個 IP 位址，其中 60%的 IP 號碼已能收到 IPv6 位址分配。JPNIC 經常舉辦研討會，以增進業者技術知識，並與 ISP、NGO、區域社群進行合作。日本 MIC(總務省)於 2007 年成立促進 IPv6 研究小組，並分別於 2008 年、2010 年及 2012 年發布研究報告，最新研究報告於 2016 年 1 月 26 日發

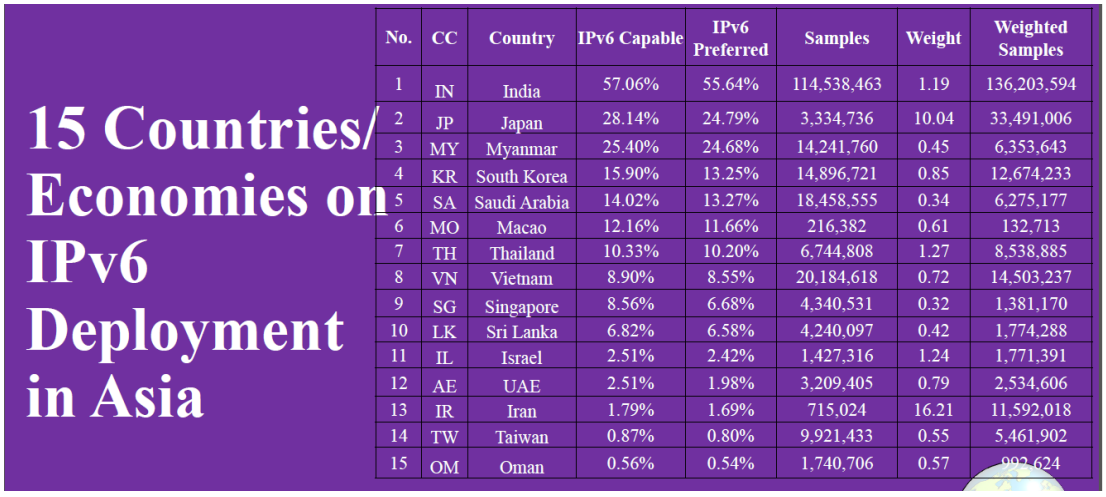
布。該報告提到了 IPv6 對物聯網時代的重要性。 而且還描述了行動業者和 MVNO 將在 2017 年之前啟動內定的 IPv6 服務。

3、印度的 IPv6 整備度

Ajai Kumar 表示他任職於孟買網際網路交換中心，由於與 NIXI 合作的緣故，而有機會從事 IPv6 的推廣。他說明，為提高印度國內 IPv6 的意識，印度第一家網際網路交換中心 NIXI 在 APNIC 的協助下，提供 IPv6 線上訓練課程。此外，印度的 ccTLD 採取雙堆疊(Dual-Stack)方式完成 IPv6 的連接，WHOIS 服務亦能以雙堆疊(Dual-Stack)方式連接。印度政府的通訊部電信處正推動 NTP2012 計畫以部署 IPv6，使印度的所有網路均採用 IPv6。

印度 Sify 公司是一家民間的網際網路服務公司，自 2005 年即開始布建 IPv6 服務。在 2005 年，ERNET India 與 IIT，Kanpur 在 IT 部門的協助下完成了 IPv6 計畫項目。IRINN 幾乎免費委託 IPv6 資源。Reliance Jio 從第一天營運開始即採行 IPv6，擁有 1 億個 LTE 用戶使用 IPv6。

印度的 IPv6 整備情形，根據 APNIC 實驗室的資料統計，印度 IPv6 部署已達 46.97%，在亞洲 15 個國家中排名第一。其次是日本、緬甸、南韓。



No.	CC	Country	IPv6 Capable	IPv6 Preferred	Samples	Weight	Weighted Samples
1	IN	India	57.06%	55.64%	114,538,463	1.19	136,203,594
2	JP	Japan	28.14%	24.79%	3,334,736	10.04	33,491,006
3	MY	Myanmar	25.40%	24.68%	14,241,760	0.45	6,353,643
4	KR	South Korea	15.90%	13.25%	14,896,721	0.85	12,674,233
5	SA	Saudi Arabia	14.02%	13.27%	18,458,555	0.34	6,275,177
6	MO	Macao	12.16%	11.66%	216,382	0.61	132,713
7	TH	Thailand	10.33%	10.20%	6,744,808	1.27	8,538,885
8	VN	Vietnam	8.90%	8.55%	20,184,618	0.72	14,503,237
9	SG	Singapore	8.56%	6.68%	4,340,531	0.32	1,381,170
10	LK	Sri Lanka	6.82%	6.58%	4,240,097	0.42	1,774,288
11	IL	Israel	2.51%	2.42%	1,427,316	1.24	1,771,391
12	AE	UAE	2.51%	1.98%	3,209,405	0.79	2,534,606
13	IR	Iran	1.79%	1.69%	715,024	16.21	11,592,018
14	TW	Taiwan	0.87%	0.80%	9,921,433	0.55	5,461,902
15	OM	Oman	0.56%	0.54%	1,740,706	0.57	992,624

圖 43 亞洲15個國家/經濟體部署IPv6的情況

[資料來源：講者簡報]

有關網際網路數據交換點採行 IPv6 的情況，印度第一家網際網路數據交換中心 NIXI 採行一些措施以鼓勵該國的 IPv6，包括：NIXI 的所有路由器採行雙堆疊模式(Dual-

Stack)、孟買的 IX 網站啟用了 IPv6，透過孟買 IX 交換的訊務有 50%是 IPv6 的訊務、計劃在不久的將來舉辦 IPv6 研討會。

在印度不僅政府部門，還有很多組織，像 ERNET，BSNL，每個人都在盡力推廣 IPv6。ERNET 在 IT 部門的支持下，已針對 3000 名政府工作人員經進行 IPv6 的培訓。

4、台灣的 IPv6 整備度

來自 TWNIC 的 Tim Wang 表示，他將介紹台灣的政府網路及教育學術網路 IPv6 的整備情況。其次介紹中華電信 IPv6 部署情況，包括專業IPv6 里程碑以及 IPv6 部署路線圖和測試。最後介紹 IPv6 整備度的評量指標。

圖 44 TWNIC簡報台灣的IPv6整備度

台灣的政府網路 AS 號碼為 4782，於 2018 年2 月 24 日 IPv6 用戶可用性已達 3.84%，台灣教育學術網路 TANet 中的 IPv6 用戶可用性已達19.49%，且持續成長，TANet 的 IPv6 流量達到 3.8Gbps，約佔 IPv4 流量的 18%。

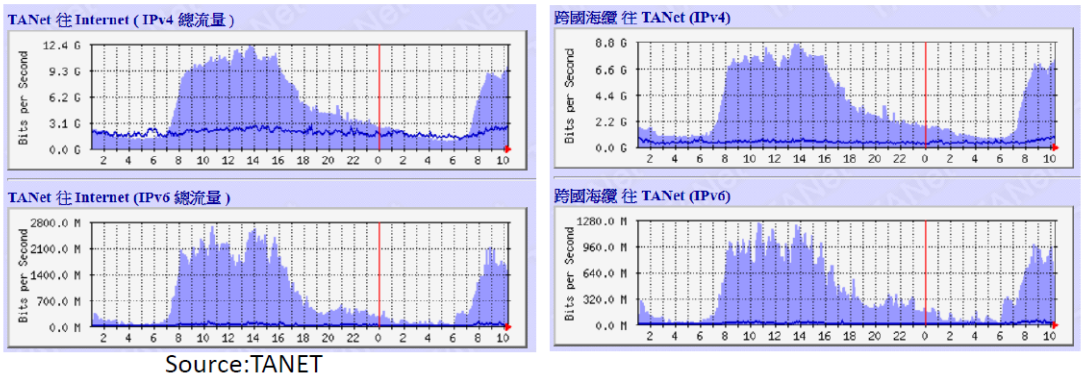


圖 45 台灣教育學術網路部署IPv6的情況

[資料來源：講者簡報]

中華電信在 2011 年參加了世界 IPv6 日，於 2013 年 IDC 數據中心開始支援 IPv6，同時支援政府的 IPv6 GSN 網路計畫。在去年進行 FTTx 的 IPv6 擴大試營運，並計劃在明年提供商用 FTTx IPv6 服務。部署 IPv6 的重要里程碑如下：

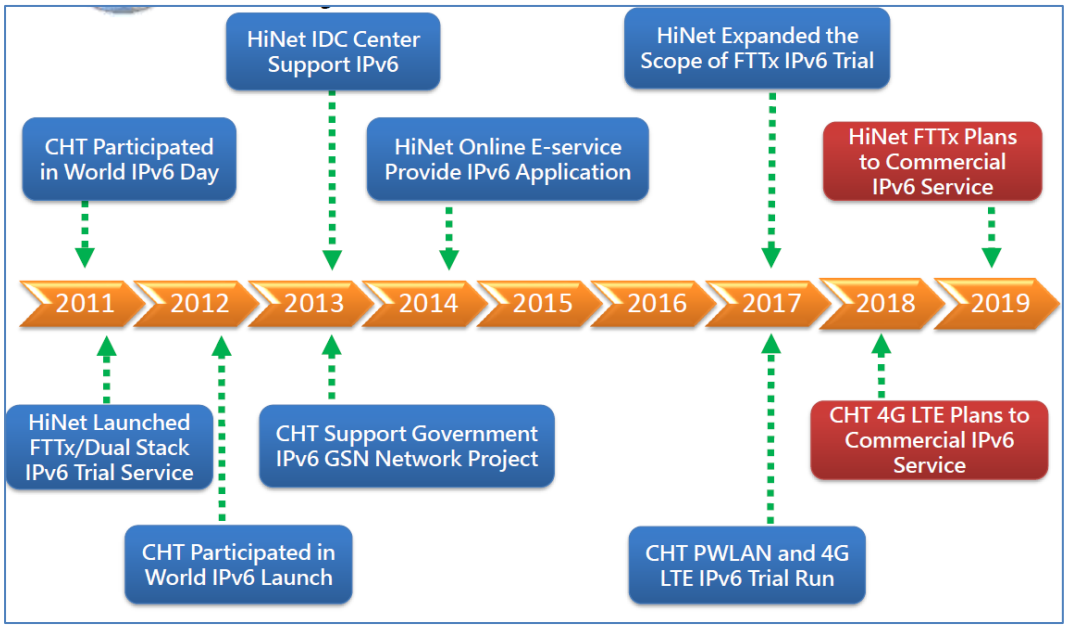


圖 46 部署IPv6的重要里程碑

[資料來源：講者簡報]

中華電信在 2017 年已針對員工和部分客戶提供 4G LTE 行動網路的 IPv6 試用服務，並計劃在今年提供 4G LTE 商用 IPv6 服務。

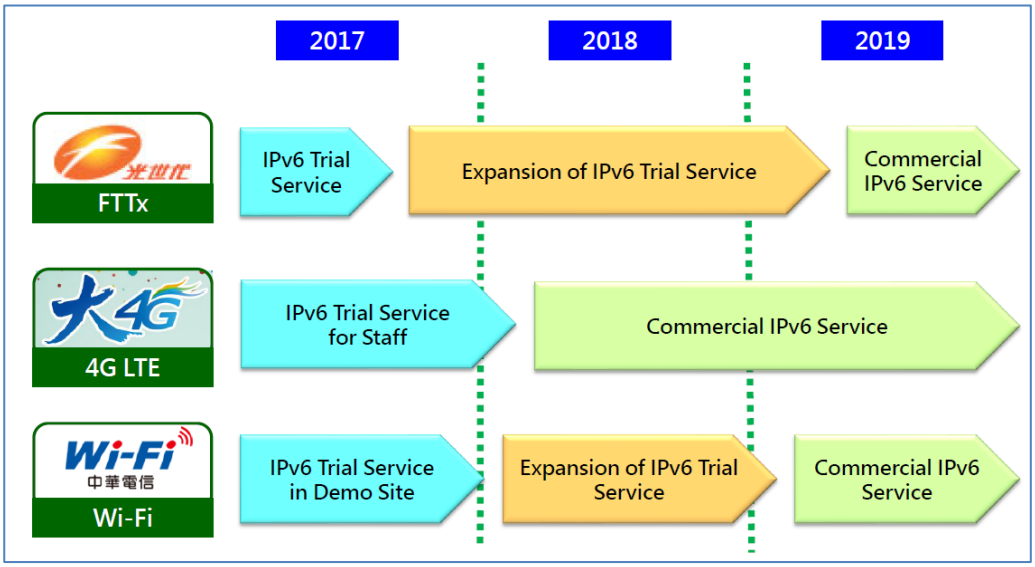


圖 47 中華電信部署IPv6的路徑圖

[資料來源：講者簡報]

同時為使電信終端設備能支援 IPv6，中華電信的電信研究院於 2003 年在台灣成立 IPv6 認證標章實驗室，負責認證 IPv6 Core、IPSec、DHCPv6、SNMPv2C 及 CE Router。

迄今認證全世界可支援 IPv6 設備共 1,693 種產品，其中台灣廠商通過認證的設備有 320 種產品，約佔 18.9%，排名世界第二。

最後講者介紹三個常見的評量指標，第一個是 IPv6 BGP 廣告比率，於 2017 年 12 月已達到 40.77%。第二個指標是 IPv6 服務可用性比率，根據來自 Alexa 的前 100 萬個網站的數據資料顯示，於 2018 年 1 月達到 15.39%。第三個指標是 IPv6 用戶可用性比率，於 2018 年 2 月達到 0.8%。此三項指標在台灣仍持續成長。另一方面，中華電信已於 2017 年進行 IPv6 的實驗，並預計於今年提供 4G LTE 商用 IPv6 服務，將進一步推升 IPv6 比率。

圖 48本會同仁與曾教授及TWNIC同仁合影

三、第三日會議摘要

（一）Security 1

1、Worldwide Infrastructure Security Report Highlights

Arber Networks每年十月都會向ISP或大型企業進行有關網路安全的調查，2017年，DDoS攻擊流量從2016年的800 Gbps 降至 600 Gbps，但其複雜度及數量卻有增無減。以發生區域來看，歐洲遭受DDoS攻擊的數量較其他國家為高，但以平均規模來看北美較高。

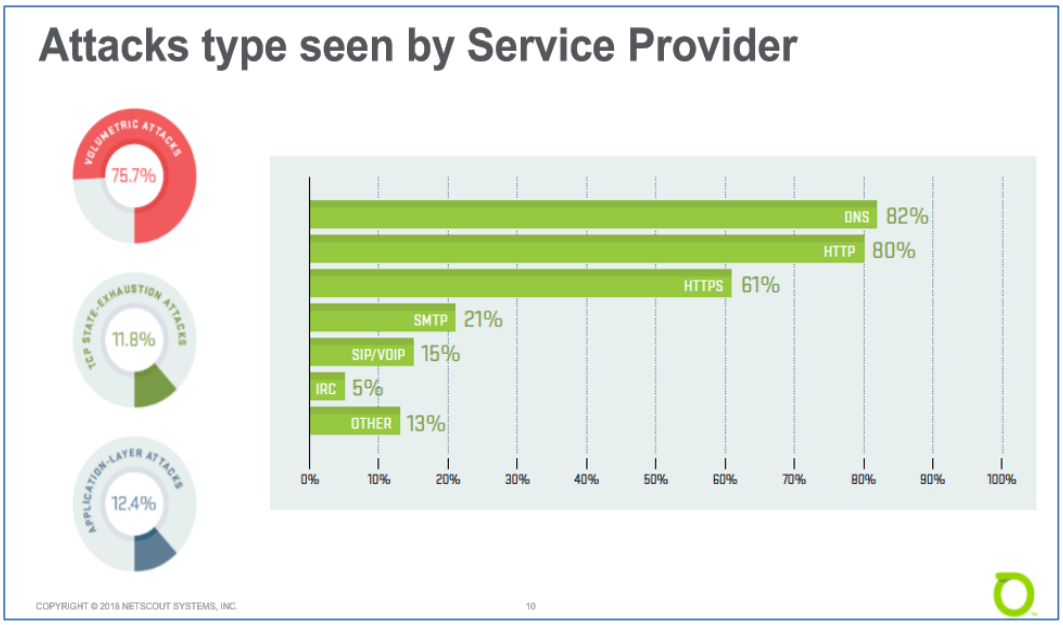


圖 49 2017年ISP遭受之網路攻擊統計

[資料來源：講者簡報]

DNS及NTP反射/放大攻擊仍為主流、C-LDAP攻擊在過去半年有持續增加趨勢，平均每周可達5464次。另混合應用層攻擊、TCP狀態耗盡等攻擊組合的多向DDoS攻擊逐漸成形，更增加了ISP或企業防禦、緩解網路攻擊的複雜度。2017年遭遇應用層攻擊的企業增加30%、應用層攻擊仍以Web服務和DNS為主流。每年遭受100次以上DDoS攻擊的企業較以往增加一倍，78%的IDC遭受1~20次服務影響（service-affecting）攻擊，影響所及到各個行業。

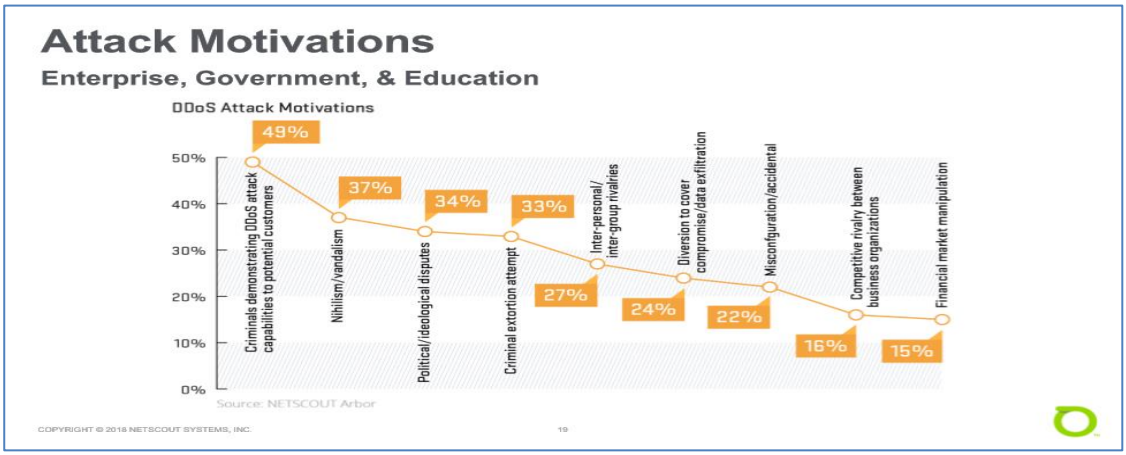


圖 50 ISP認為網路攻擊者之動機統計

[資料來源：講者簡報]

勒索軟體（Ransomware）是企業、政府及學術單位最關心的議題及主要威脅，DDoS次之。但ISP卻視DDoS為主要威脅，考慮物聯網殭屍網路持續增長及攻擊者可以輕鬆獲得先進的攻擊技術和功能，這結果並不令人訝異。另外從攻擊動機視之，企業、政府及學術單位認為自我能力之實現為主因，但ISP卻認為是因為與線上遊戲相關。

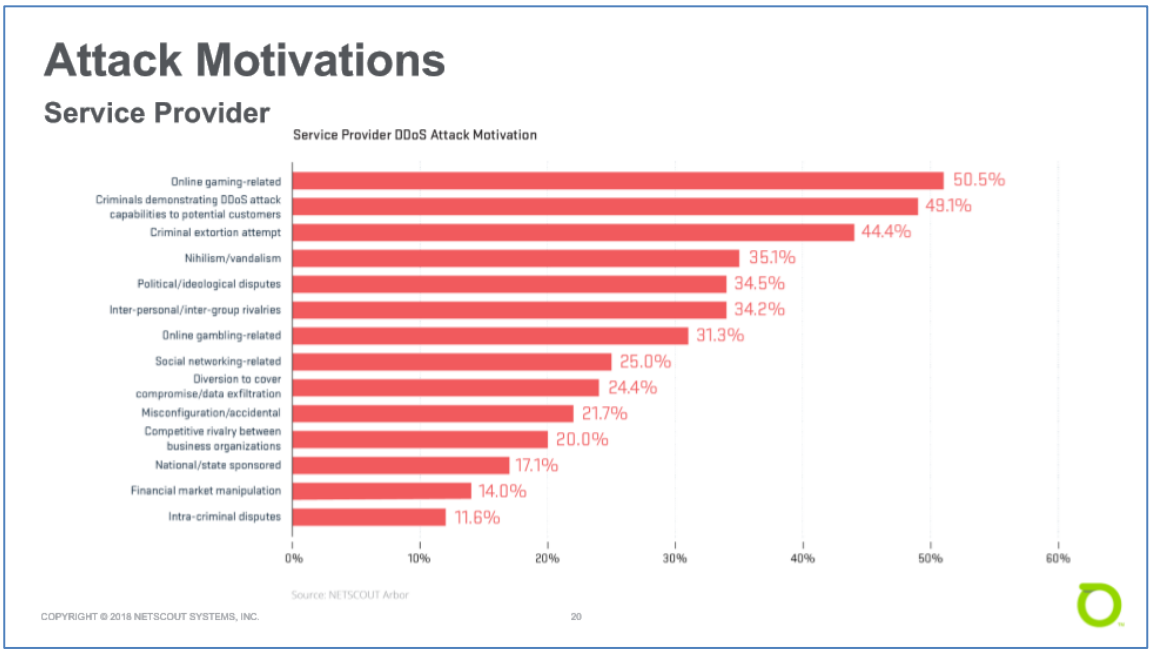


圖 51 企業、政府及學術單位認為網路攻擊者之動機統計

[資料來源：講者簡報]

DDoS首選威脅檢測工具仍是NetFlow，但SNMP工具之使用將再度增長，超過了防火牆日誌的普及率。在線DDoS檢測/緩解系統結合NetFlow分析工具將視為檢測威脅最有效方法。安全分析師和事件響應者在世界範圍內的短缺仍然是一個關鍵問題。 缺乏資源，再加上招聘和留住技術人員的困難，再次成為建立有效的運營安全團隊的兩個主要關注點。

2、BGP Flexibility and its Consequences

去年八月Google操作失誤，造成日本網路大規模斷線、同年12月亦有其他公司造成的網路斷線事件，全球路由事件已成常態，但其錯誤卻源自工程

師操作失當。究其原因係IRR 過濾器不執行原生驗證、AS-SET物件沒有授權、AS-SET疏於維護造成失效、ISP業者並未使用任何IRR過濾器。經調查結果，目前前十大ISP，其過濾器不論IPv4、IPv6都會接收來自第一層傳來的路由洩漏（Leaks），讓DoS攻擊、中間人攻擊有機可趁，而且增加網路延遲時間。建議Transit端，於客戶連接端設置IRR過濾器、與客戶端一起合作、私人互連使用IRR過濾器、使用Ad-hoc過濾及持續監控BGP。IX業者建議在所有連接設置IRR過濾器、與客戶端一起合作、移除過時的過濾器及使用RS內的RPKI暫存器。多宿主則建議路由物件、AS-SETS都要及時更新、建立ROA紀錄及持續監控BGP。

3、Routing Security in 2017: We can do better!

2017年發生在網際網路的路由狀態統計數據：

- 總共 13,935 起事件（停機或攻擊如路線洩漏和劫持）：其中 62％被列為中斷，38％被認為是路由攻擊，例如路由洩漏和劫持。
- 網際網路上超過 10％的自治系統受到影響：停電事故，其中幾乎一半發生在巴西
- 3,106 個自治系統是至少一個路由事件的受害者：絕大多數事件受害的網路都位於美國
- 1546 個網路至少導致一起事件：美國、巴西、俄羅斯和中國是網路引發事件之首，含括 75%以上事件。

【事件】是路由系統狀態的一個可疑變化，可以歸因於中斷或路由攻擊，如路由洩漏或劫持（無論是故意的還是由於配置錯誤）。講者闡述，路由安全的相互約定準則（Mutually Agreed Norms for Routing Security，MANRS）建議了最低限度的低成本和低風險行動，包括【過濾】、【反欺騙】、【協調】及【全局驗證】等。這些行動合起來可以幫助提高路由基礎設施的彈性和安全性。越多的服務提供商採用這些最低限度的行動，就會發生的事件越少，損失越小。

圖 52 MANRS的使命

[資料來源：講者簡報]

- 過濾：確保您自己的公告和客戶通過前綴和 AS 路徑粒度到鄰近網路的公告的正確性。
- 反欺騙：至少為單宿主客戶網路，您自己的最終用戶和基礎架構啟用源位址驗證。
- 協調：保持全球可訪問的最新聯繫信息。
- 全局驗證：發布您的數據，以便其他人可以在全球範圍內驗證路由信息。

4、Secure SDN

SDN 是近幾年快速新興的網路架構， 它的設計理念是將網路的控制層（Control Layer）和資料層（Data Layer）分離，由控制層集中控管網路， 實現網路的可編輯化（ Programmable），以大幅提升網路資源的控制彈性與使用效率，同時也提高了駭客攻擊機會。SDN Control Layer為網路控制的核心，更是攻擊者覬覦的目標。已知SDN主要漏洞為控制層與資料層間之通訊中斷，應用層與控制層間之北橋介面（Northbound API）則為潛在漏洞。此外，工程師如果將經入侵的應用程序安裝在控制層，網路控制權將遭嚴重挑戰。來自Telstra的講者建議採授權管制、落實系統修補或強化、使用高可用性控制器體系結構來防止DDoS攻擊、北橋介面通信應採TLS或SSH加密、南橋介面則建議採TLS對端點進行身份驗證，並且控制信號流與主資料

流隔離。另來自Juniper的講者則建議，單個SDN部署可在多個環境中提供連通性和安全性、發現應用層內/層之間的拓撲和活動（底層覆蓋相關）、集中式安全策略與多個分佈式執行點（L2-L4、L7使用基於主機的防火牆）、策略定義（即配置）和SIEM（即報告，故障排除，應用程序流發現等）的可視化、控制層和資料層跨多雲環境均予以加密等策略。

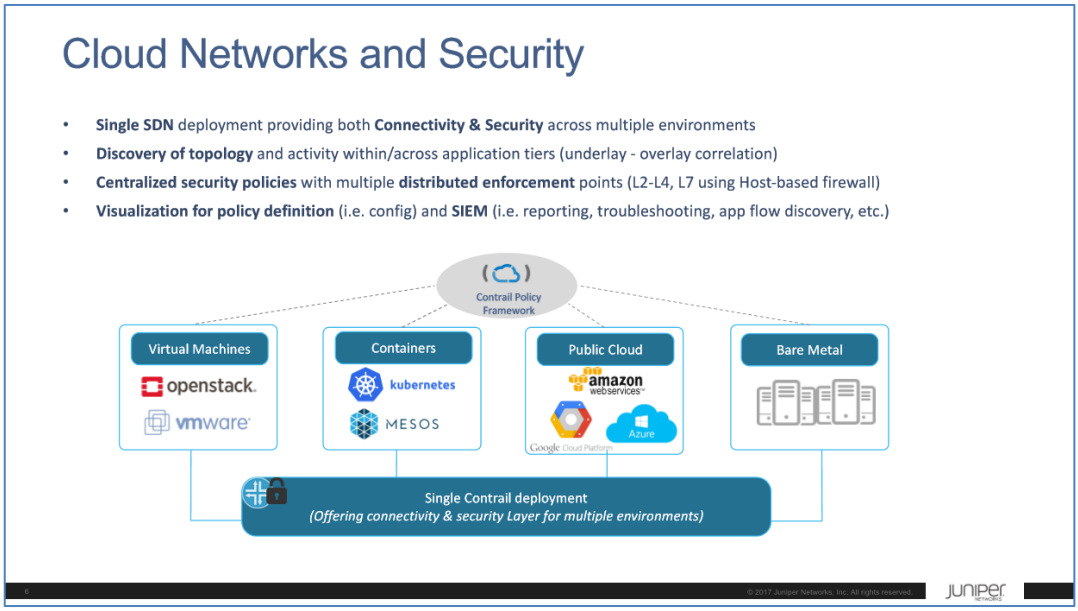


圖 53 雲端網路及安全

[資料來源：講者簡報]

（二）Network Functions Virtualization

本研習課程分 2 場次，每場次各 90 分鐘。Nokia 的 E2E 平台架構戰略總監 Paresh Khatri，首先說明設備長期來就在專用化與通用化間交替循環演進，而 NFV 會是最新的循環階段，同時說明目前專用化設備存在新產品推出緩慢、擴充性不佳、新設備需增加成本、設備週期短等諸多問題需要解決，因此由 AT&T、BT 等 13 個主要電信業者發起並於 2012 年 10 月誕生了 NFV（Network Functions Virtualization）。

Paresh 指出，網路功能虛擬化（Network Functions Virtualization，NFV）是將網路功能從網路設備中抽離，並以軟體來實現，藉此以打破過去網路功能必須存在硬體設備中的必然關係，著重的是網路設備功能的虛擬化。與 SDN 將網路的管理層從硬體中分離，將網路管理的集中化與可程式化有別。Paresh 同時針對許多術語進行解說，

及說明如何衡量與強化 performance 之方法。

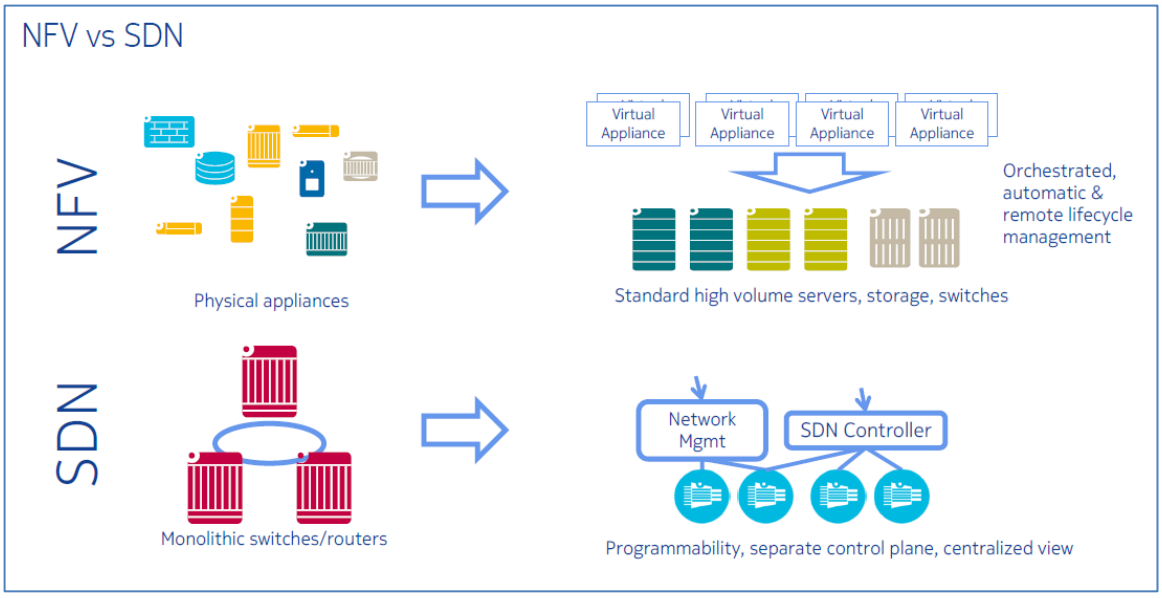


圖 54 NFV vs SDN

[資料來源：講者簡報]

Paresh 表示，指出目前產業進展是：尚未很多 NFV 都沒有真正實現雲優化（cloud-optimised），而是簡單的 PNF 埠（NFV washing），然而，這是開始獲得經驗的必要步驟；實現高性能（用於數據平面功能）仍然是一項挑戰；所有 NFV 都使用通用硬體的能力還沒有實現；NFV 的擴充是更動態的，所以 license 難以訂價; 管理 NFV（通過 MANO 基礎設施）與管理網路硬體有很大不同， 業者需要更新的技能。

圖 55 NFV參考資料

[資料來源：講者簡報]

（三）IPv6 Transition and Deployment

本議題共分兩場，每場各 90 分鐘，由 IPv6 公司的 Jordi Palet 主講。第一場是研究 IPv6 轉換機制並描述所有可能的“邏輯”選項，包括：Dual stack、Tunnel 及 Translation。此外，介紹運營商在網路中部署 IPv6 所需的步驟，包括轉址方式。第二部分則集中探討行動網路部署 IPv6 實例，但可將相同的概念應用於非行動網路。

1、IPv6 轉換或與 IPv4 共存的技術

Jordi Palet 表示，IPv6 已設計為能與 IPv4 共存或容易自 IPv4 轉換。目前有三種策略：Dual stack、Tunnel 及 Translation。所謂 Dual stack 是同時支援 IPv6 及 IPv4 兩種堆疊。

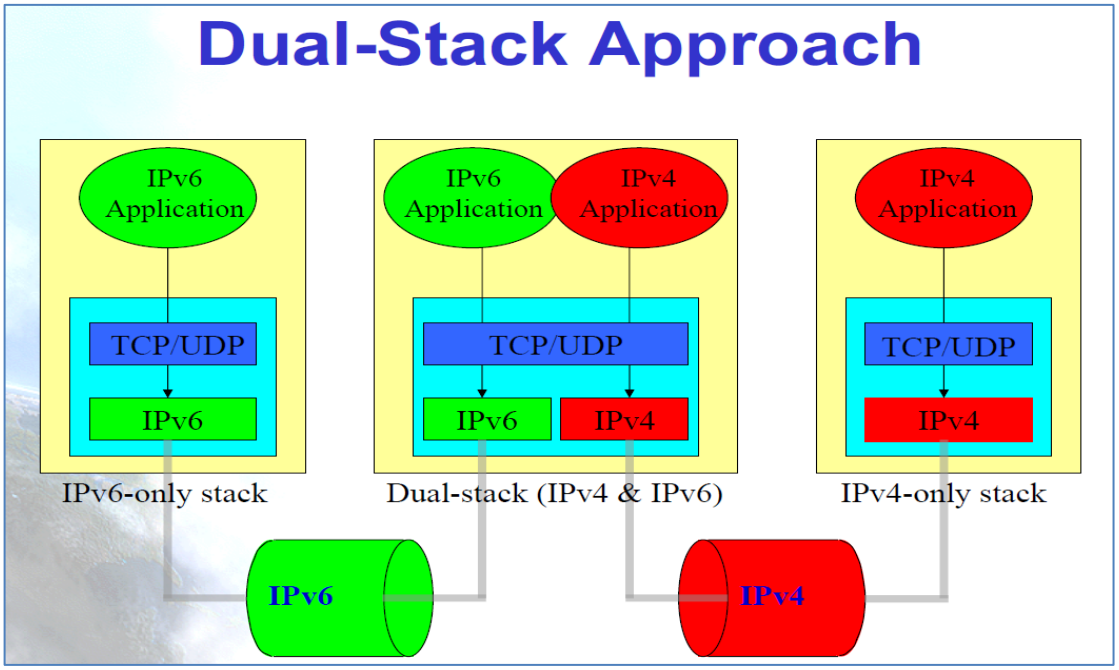


圖 56 雙堆疊模式

[資料來源：講者簡報]

Tunnel 是將 IPv6 封包以 IPv4 的形式包裝，這是最常採用的策略，現在則期待將 IPv4 封包以 IPv6 的形式包裝，以促進純 IPv6 網路的早日實現。

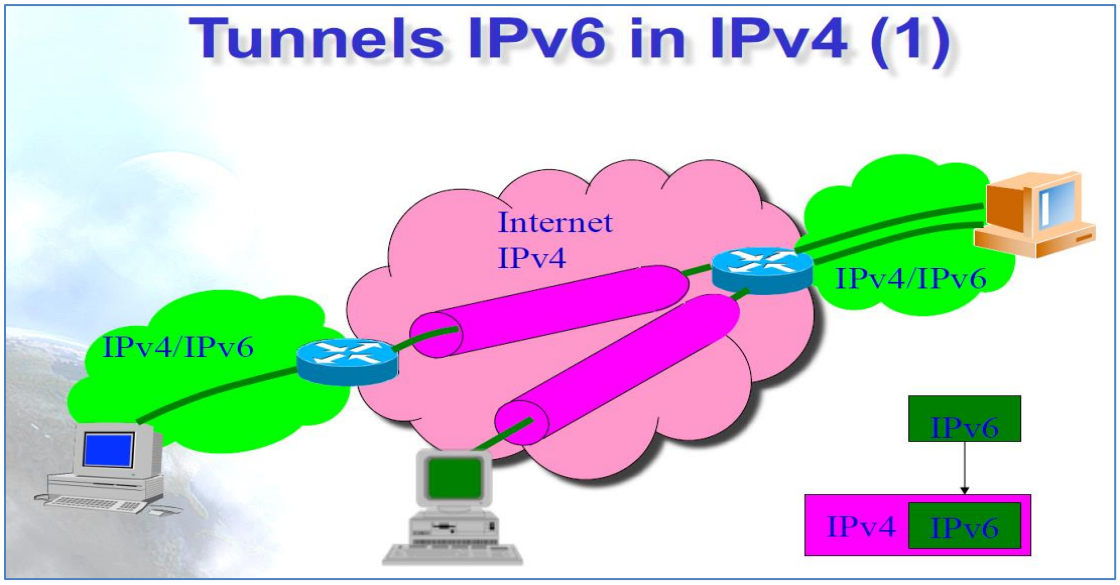


圖 57 隧道模式

[資料來源：講者簡報]

轉址(Translation)則是使僅 IPv4 的網路與僅 IPv6 的網路彼此溝通。目前有數種解決方案，均是將 IPv4 的封包轉成 IPv6 的封包，反之亦然。最常見的作法是 NAT-PT，以路由器連接僅 IPv4 的網路與僅 IPv6 的網路，由此路由器負責將 IPv4 的封包頭轉換成 IPv6 的封包頭。

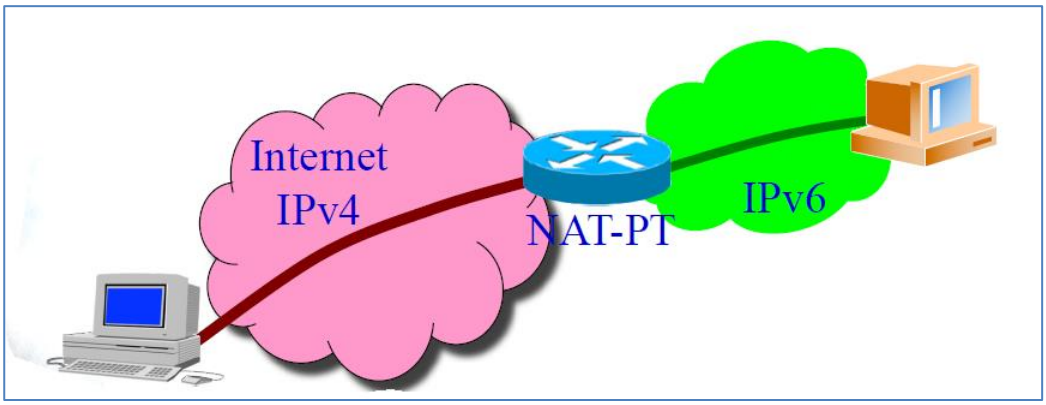


圖 58 IPv4與IPv6間轉址

[資料來源：講者簡報]

轉址(Translation)的處理過程是複雜且不完美的，需要 ALG 的支援，因此是最差的一種解決方案。在初期並不建議採用，只要在無其他選擇時才採用。目前則期望能組合採用前述三種策略。

由於 IPv4 位址已耗盡，所以應避免將 IPv4 分配給終端用戶及公眾網路，只用來與僅 IPv4 的網路相互溝通使用。後續則要建置僅 IPv6 的網路。

2、轉址技術

當 ISP 僅提供 IPv6 的連接，或是設備僅具 IPv6 功能(例如行動電話)，但網際網路上仍有僅 IPv4 的黑箱存在，則需要類似 NAT-PT 功能的存在，也就是 NAT64。NTA64 允許多個僅 IPv6 的網路點共用一個 IPv4 位址，來接取 IPv4 網路：

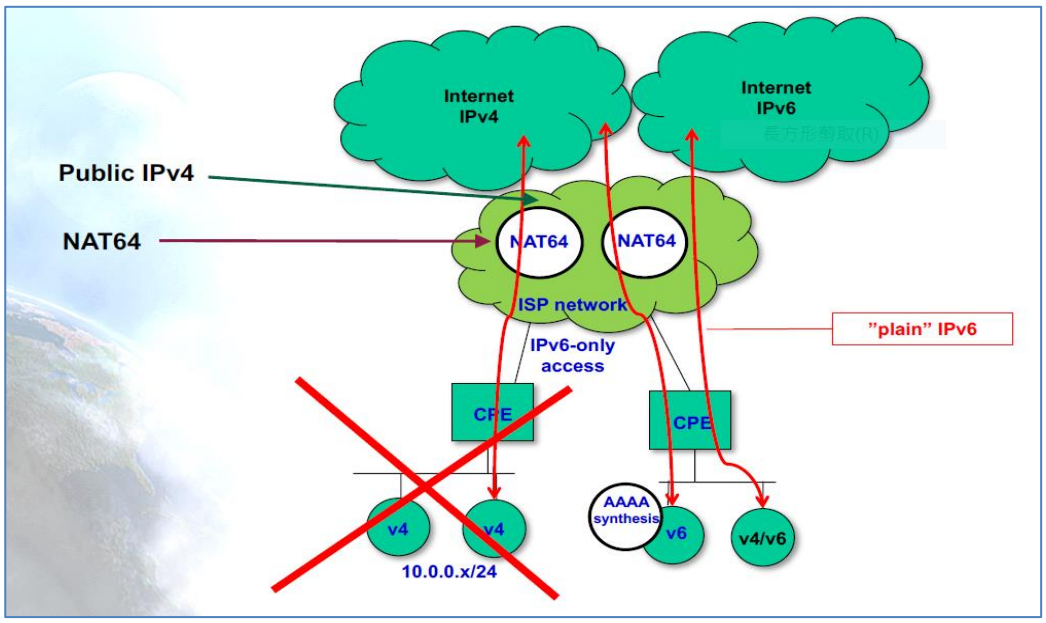


圖 59 NTA64示意圖

[資料來源：講者簡報]

由於採用 NTA64 技術會造成某些 APP 無法正常運作(例如 Skype、Netflix)，因此發展出 464XLAT。464XLAT 運作方式如下：

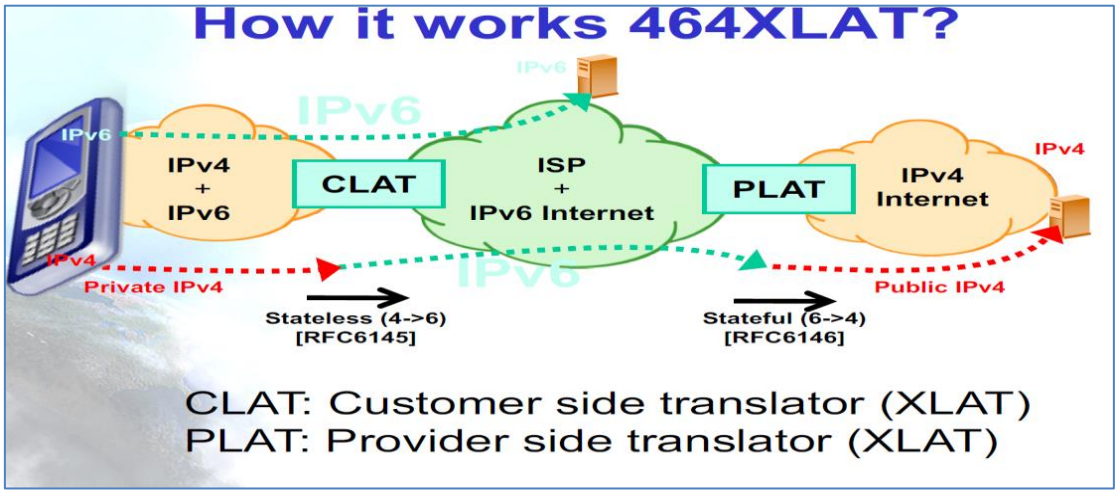


圖 60 464XLAT的運作方式

[資料來源：講者簡報]

464XLAT 定址方式如下：

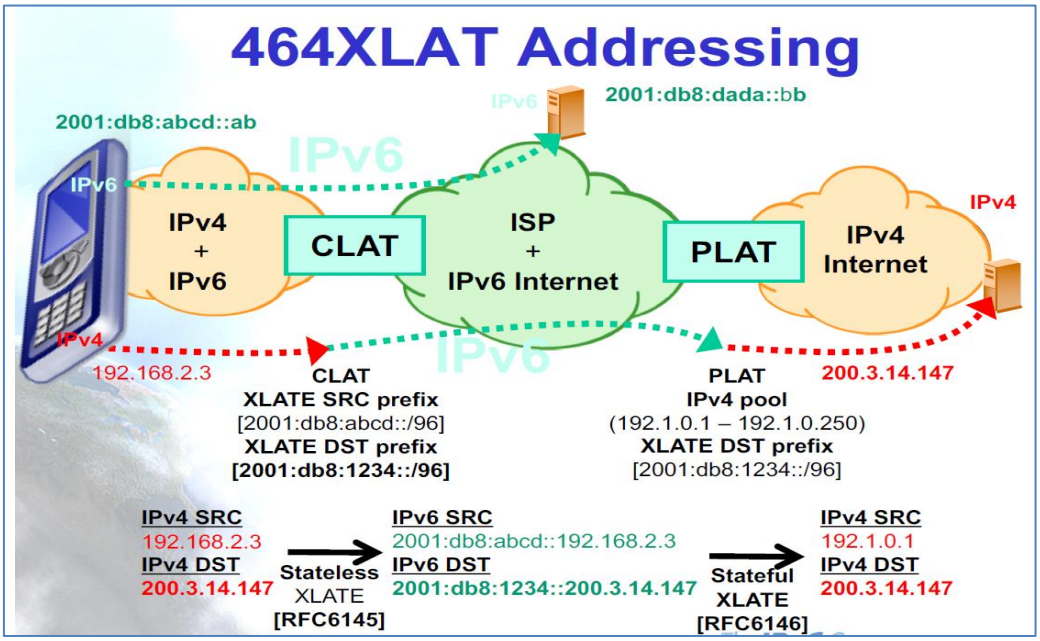


圖 61 464XLAT的定址方式

[資料來源：講者簡報]

3、行動網路部署 IPv6 實例

IPv6 公司的 Jordi Palet 介紹在行動網路裡部署 IPv6。由於 IPv4 已耗竭，而共享 IPv4 位址仍不足以解決耗竭的問題，以及使用者數量不斷增加、每個使用者所擁有的設備數不斷增加、每個設備所需位址數不斷增加、VoLTE、IoT、長期策略…等因素，需要支持 IPv6，而最佳的解決方案是 Dual stack。

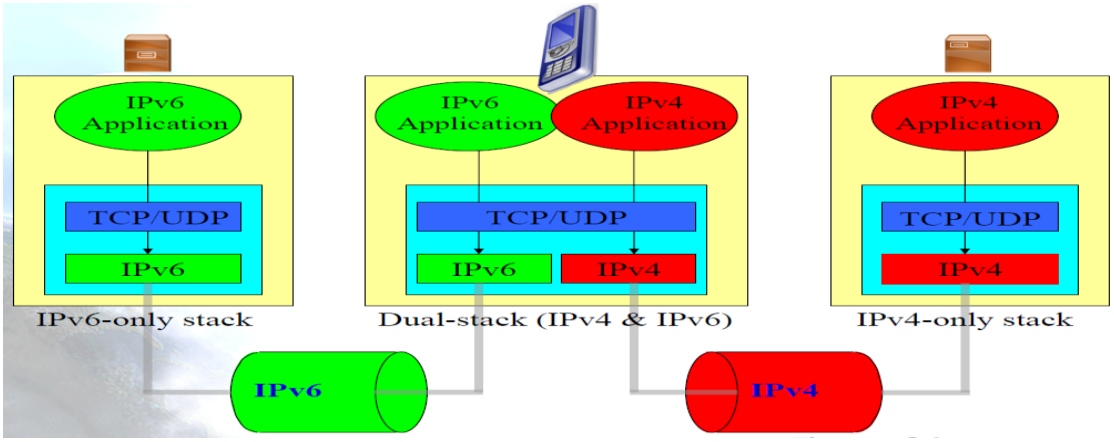


圖 62 最佳解決方案--雙堆疊

[資料來源：講者簡報]

首先要先確定，是否擁有足夠的 IPv4 位址？Q&M 的成本為何？對 Call center 的

影響為何？性能如何？是否需要執照？認證 2 個位址的問題如何？

除了採行 Dual stack 外，可採行的替代方案有：建置僅 IPv6 的網路、建置僅 IPv6 的網路並採行 NAT64、建置僅 IPv6 的網路並採行 NAT64 及 DNS64、採行 464XLAT、採行其他轉址技術。而所謂其他轉址技術指的是 6RD、DS-Lite、MAP-E 或 MAP-T。

行動網路採用僅建置 IPv6 網路，並非現今可採行的選項，因為會讓使用戶只能接取僅 IPv6 的內容及 APP，而無法接取僅 IPv4 的內容及 APP，且手機若為僅 IPv4，將無法使用。此外，其他轉址技術在行動網路並不可行，因為智慧手機並不具備這些轉址技術，且這些轉址技術需使用許多 IPv4 位址，而設定的負擔很重且會增加網路額外負擔。

（四）IPv6 - A Real World Deployment for Mobiles

Telstra 的 Jeff Schmidt 表示，IPv6 在行動通信的行業中正在獲得牽引力。本場次介紹了 IPv6 部署的好處，以及 Mobiles Telco 環境中 IPv6 部署的挑戰和進展。內容包括：部署 IPv6 的理由、營運及技術考量、行動網路架構、網路安全、定址及劃分子網路、部署 IPv6 的模式等。

1、部署 IPv6 的理由

- 行動網路話務的不斷成長以及每個人擁有的裝置數不斷增
- 網路對新技術(物聯網、VoLTE、ViLTE、管理及 Backhaul) 已準備就緒
- IPv4 公眾及私有位址的耗竭
- 提升網路效能

2、營運及技術考量

- 公眾及私有 IPv4 位址的耗竭
- 在不同網域內公共及私有 IPv4 位址重複且無法互通。
- 須持續投資以擴充 IPv4 可用資源，卻無法像 IPv6 可滿足未來物聯網對位址的需求。

- 隨著 IPv4 位址的耗盡，擴展 IPv4 資源將會更加昂貴。雙堆疊是一種有效的位址轉換技術，但無法解決 IPv4 耗盡的問題。
- 引進 IPv6 可降低對 NAT 的依賴、消除對區域化的需求，並促進應用程式轉移到 IPv6。

3、行動網路架構

IPv6 可實施集中式 CGN。CGN 執行 NAT / PAT 44 和 NAT / PAT 64，PAT 大大減少了公共和私有 IPv4 位址的需求，但無法阻止 IPv4 位址的耗竭。實施 IPv6 的話務流如下：

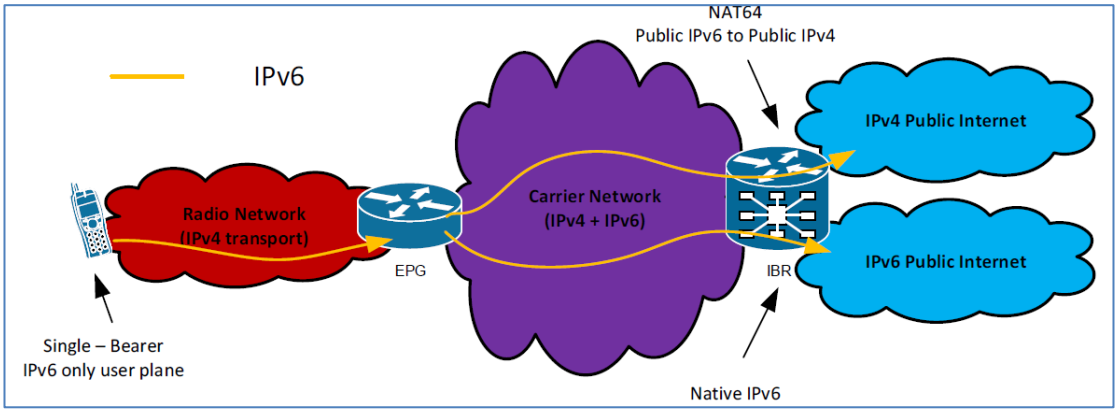


圖 63 實施IPv6的話務流示意圖

[資料來源：講者簡報]

為使網路能夠執行多重 APN，需創建多個真實 APN 以支援 IPv4，IPv6 和個別 IPv4v6。

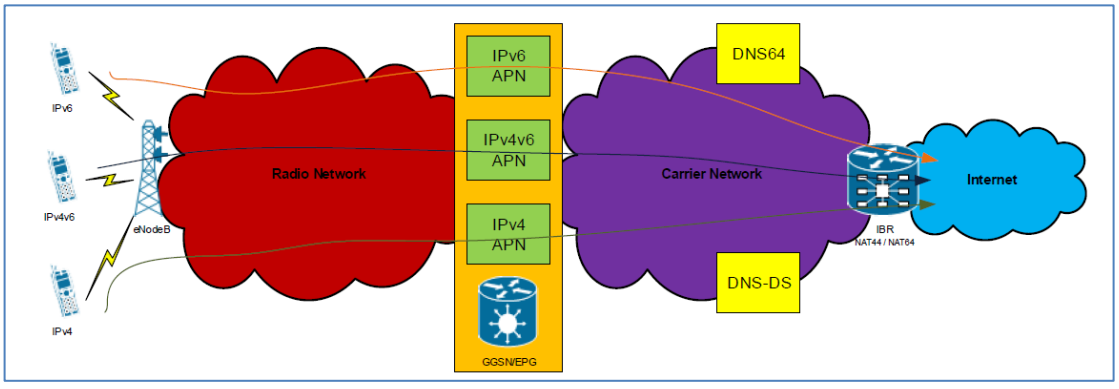


圖 64 執行多重APN示意圖

[資料來源：講者簡報]

若網路只須執行單一 APN，則只需創建單一真實 APN 以支持一個 DS 和 SS。

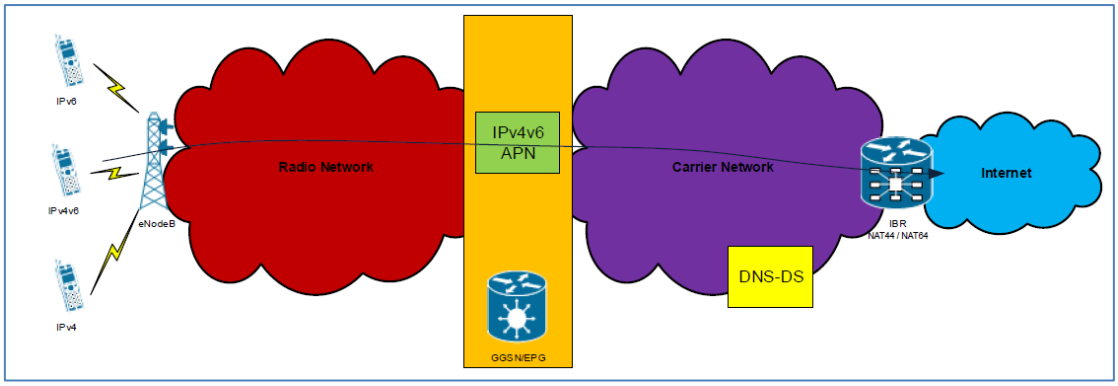


圖 65 執行單一APN示意圖

[資料來源：講者簡報]

4、網路安全

隨著 CGNAT 服務從網路中移除，無線設備將暴露於來自網際網路未經請求的流量。由於未經請求的流量，將導致無線用戶對於計費異常更加敏感，因此有必要設置一個簡單的防火牆服務，來阻止未經請求的流量。同時防火牆也能確保無線核心網路不被透過網際網路接取。

5、定址及劃分子網路

3GPP 目前規定每個 UE 可接收一個/ 64 的位址，未來版本可能需要使用 DHCP-PD 的/ 60 用於單個 APN 共享。

6、部署 IPv6 的模式

每個行動業者都有一套獨特的環境，因此並沒有一套由 IPv4 過渡到 IPv6 的標準模式，必須由各行動業者自行評估，以確定本身的網路適合哪種方法。不論採行哪種方法，應同時擬定最終部署本地 Single Stack IPv6 的長期策略。

四、第四日會議摘要

（一）Brace Yourselves: DDoS is Coming

最近的研究顯示，近 75%的組織在過去 12 個月中至少遭受過一次攻擊，而且曾遭受攻擊者，再次受到攻擊的機率越高。任何組織都是 DDoS 攻擊的潛在目標，DDoS 攻擊越來越頻繁，且攻擊規模越來越大，除加重 ISP 網路負載，更造成客戶端的困擾，尤其是現行很多企業都提供線上服務，因此網路中斷對其商譽及財務均有重大影響。

相較於實體攻擊（如投石器、飛彈）所需費用（從數百到數百萬美元不等，視使用之武器而定），DDoS 攻擊所需費用相對實惠許多，只需 19.99 美元，甚至更少就可以買通駭客協助攻擊特定網站 1 個月，還可以選擇攻擊類型。攻擊者成本很低，但防禦或緩解 DDoS 攻擊所需費用，及後續網路中斷損及之商譽及財務，卻所費不貲，而這些攻擊的目的卻有可能只是好玩、自我能力表現、企業競爭等。

為讓與會者瞭解 DDoS 攻擊前後，對於路由器、防火牆、網站及資料庫之頻寬、封包處理能力等所生影響，講者直接演練 DDoS 攻擊特定網站，並監控其產生之效應。

講者同時說明體積型的攻擊（Volumetric Attacks）及應用層的攻擊（Application-Layer Attacks）等 DDoS 攻擊類型，並演示如何以 WireShark、HPING3 及 Scapy @ Python、Burp 等開源軟體觀察網路是否遭受 DDoS 攻擊，透過知己知彼，讓與會者更有信心面對 DDoS 攻擊。

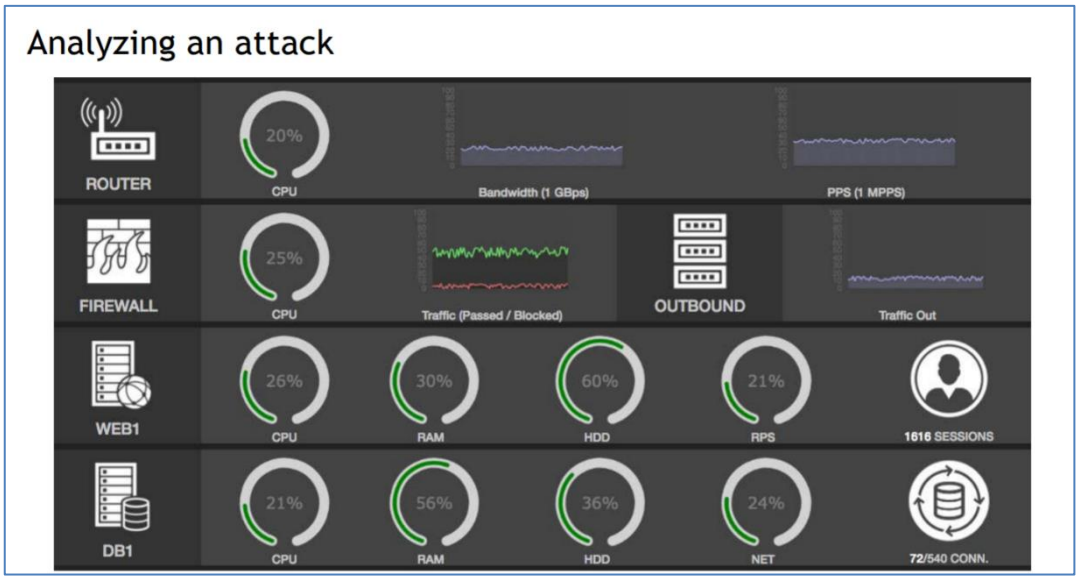


圖 66 DDoS攻擊分析

[資料來源：講者簡報]

- DNS 放大 - 在反射類型的攻擊中，犯罪者首先使用預期受害者的欺騙性 IP 位址進行小型查詢。利用可公開訪問的域名系統（DNS）服務器上的漏洞，這些響應會膨脹到更大的 UDP 數據包負載中，並壓倒目標服務器。
- SYN Flood - 每個 TCP 會話都需要兩個系統之間的三次握手。 使用

SYN 氾濫，攻擊者會通過太多的連接請求迅速擊中目標，導致網路飽和。

- UDP Flood - 作案者在這攻擊中，使用包含 UDP 數據的封包來淹沒目標網路上的隨機端口。 受害系統嘗試將每個數據包與應用程序進行匹配，但失敗。 當它嘗試處理 UDP 數據包回復量時，系統很快就會變得不堪負荷。
- DNS 洪水 - 類似於 UDP 洪水，這種攻擊實施者涉及使用大量 UDP 數據封包耗盡服務器端資源。 然而，在這裡，目標是 DNS 服務器及其緩存機制，其目標是防止傳入合法請求重定向到 DNS 區域資源。
- HTTP Flood - 此攻擊使用非常大量的 HTTP GET 或 POST 請求（看起來合法）來定位應用程序或 Web 服務器。 這些請求通常是為了避免犯罪者在攻擊之前獲得關於目標的有用信息而發現的。
- IP 碎片攻擊 - 這種攻擊涉及利用 IP 數據包的最大傳輸單元（MTU）使系統過載的犯罪者。 這可以通過發送超過網路 MTU 的虛假 ICMP 和 UDP 數據包到資源消耗迅速並且系統在數據包重建期間變得不可用的點來完成。 犯罪者也可以執行淚滴攻擊，通過防止 TCP / IP 數據包重建來工作。
- NTP 放大 - 互聯網連接的設備使用網路時間協議（NTP）服務器進行時鐘同步。 與 DNS 放大攻擊類似，此處犯罪者使用多個 NTP 服務器以用戶數據協議（UDP）流量超負荷目標。
- Ping Flood - 另一種常見的泛洪類型的攻擊，它使用任意數量的 ICMP 回應請求或 ping 來超載受害者的網路。 對於每次發送的 ping，應該返回一個包含相同數量的數據包的倒數。 目標系統試圖響應無數的請求，最終堵塞自己的網路頻寬。
- SNMP 反射 - 簡單網路管理協議（SNMP）使系統管理員可以遠程配置並從連接的網路設備擷取數據。 偽造使用受害者的 IP 位址，犯罪

者可以將很多 SNMP 請求發送給設備，每個設備都應該輪流回復。 連接設備的數量會上升，網路最終會受到 SNMP 響應數量的限制。

- SYN Flood - 每個 TCP 會話都需要兩個系統之間的三次握手。 使用 SYN 氾濫，攻擊者會通過多個連接請求迅速擊中目標，導致網路飽和。
- Smurf 攻擊 - 就像 ping 洪水一樣，smurf 攻擊依賴於大量的 ICMP 回顯請求數據包。 但相似之處就在此停止，因為 smurf 攻擊使用放大矢量來增加它們在廣播網路上的有效負載。 Smurf 惡意軟件被用來觸發這種攻擊類型。
- Ping of Death - PoD 是駭客通過發送異常或虛假數據封包（通過 ping）凍結，破壞目標系統或服務的方法。 當它試圖重建過大的數據包時，會發生內存溢出。 不要單獨使用 ping 命令，攻擊者可以使用任何 IP 數據類型發起攻擊，包括 ICMP 回應，UDP，IDX 和 TCP。
- 叉炸彈 -此 DoS 攻擊源自目標服務器內部。 在基於 Unix 的環境中，fork 系統調用將現有的“父”進程複製到“子進程”進程。 然後這兩個進程可以獨立處理系統內核中的同時任務。 使用叉子炸彈（又名“兔子病毒”），犯罪者會發出如此多的遞歸分支，導致目標系統內部不堪重負。

（二）APNIC AGM 1~3

今日APNIC Annual General Meeting（AGM）會議共有3場次，每場次90分鐘。此會議的重頭戲是進行3名任期屆滿的APNIC Executive Council （EC ）委員選舉。會議先由APNIC EC主席 Gaurab Raj Upadhaya致開場歡迎詞，接著由選舉主席 Craig Ng說明選舉規則，續由候選人上臺發表2分鐘自我介紹，介紹內容多集中於候選人之INTERNET產業專業能力及曾參與APNIC運作的經驗、擬對APNIC社群做更多付出之抱負，以及對APNIC核心

價值及如何持續強化之願景。接著由選舉主席宣布開始會場投票活動，並訂於下午2點30分截止投票（另有線上投票，在本次會議前即已開始）。

接著由APNIC秘書長Paul Wilson報告APNIC在2017年的工作績效，重點包括APNIC雖會員仍持續成長，但已趨緩。中心努力推展下IPv6 呈健康成長。該中心亦致力於Whois、Whowas、RPKI、ROA等服務，另針對SDN 等新技術提供訓練課程，對於NOG、IXP等產業也提供協助。近來資安議題相當重要，因此也提供CERT相關服務，以本次大會為例SECURITY的課程時數是最多的。

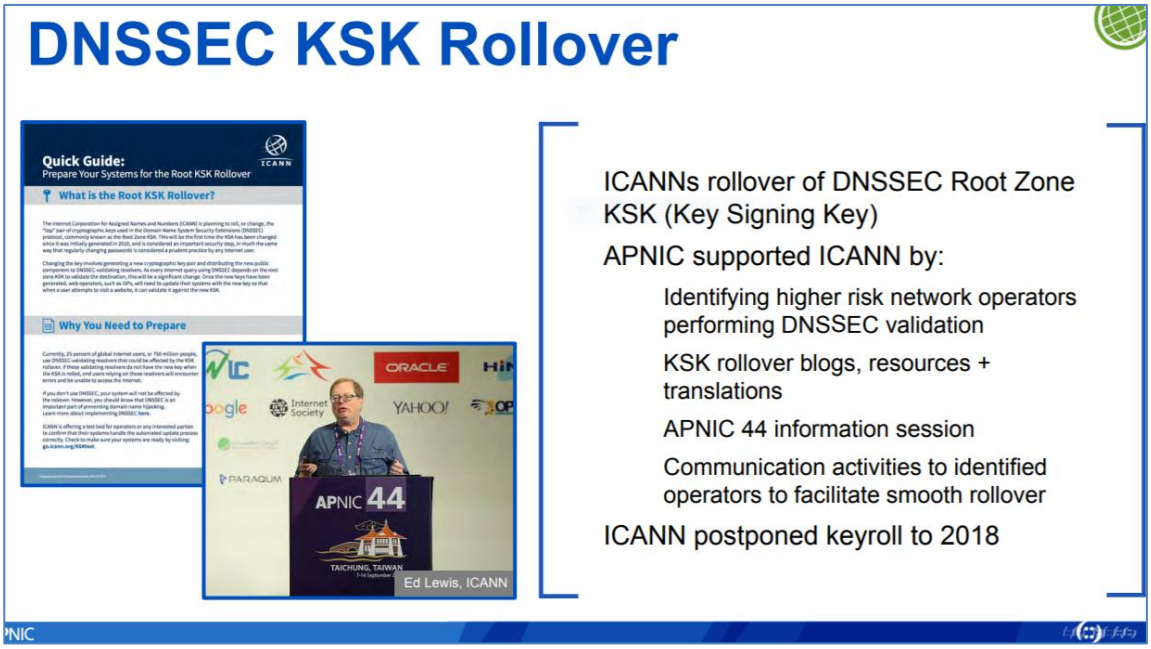


圖 67 APNIC致力推動資安

[資料來源：講者簡報]

另我國TWNIC黃執行長勝雄亦是現任APNIC EC並擔任出納委員職務，他則報告APNIC在2017年的財務出支詳細說明及2018年的財務規劃，他也指出該中心財務係委由PWC稽核，詳細資料可到APNIC網站下載。

緊接由EC主席報告EC工作事項、會議運作方式及2018年會議規劃，並說明今年6月將辦理2年1次的調查作業，以蒐集會員意見供作委員會優先議題及服務之決策參考。他指出，因為中心營收下降，因此將對財務規劃進行討論。同時介紹該中心新成立的Review Committee 將在APNIC 46進行委員

選舉， 並預告2017年開始運作的APNIC 基金會將在今年5月於香港召開會議。

另由Policy SIG主席報告今年會議成果，首先完成副主席選舉，由我國TWNIC的顧組長敬恆當選，另今年4個提案均沒有獲致完全共識。

我國亞洲大學曾憲雄教授則進行IPv6 Readiness Measurement BoF 報告指出，亞太各國2017年在v6用戶都有成長， IPv6 BGP年成長率約 0.6%、IPv6 服務可用年成長率為1.07%

接著進行Cooperation SIG、NIR SIG會議報告，另APIX亦進行2017年成果報告，除說明會員情形外，亦說明由日本在京都舉辦第1次Peering Asia 1.0 Forum非常成功，2018年將辦理第2次論壇，將由香港主辦。

下午會議先進行選舉結果報告，接著進行HACKATHON競賽獲勝者頒獎，本次主題是IPv6，共有5隊參加，參與者中18位男性、6位女性。現場3位學員發言，均表示參與競賽是很好的經驗，藉此學習到很多。

接著由APNIC 46主辦國NEW CALEDONIA向與會者說明其舉辦規畫並介紹該國漂亮、豐富的觀光資源及入境與交通資訊。

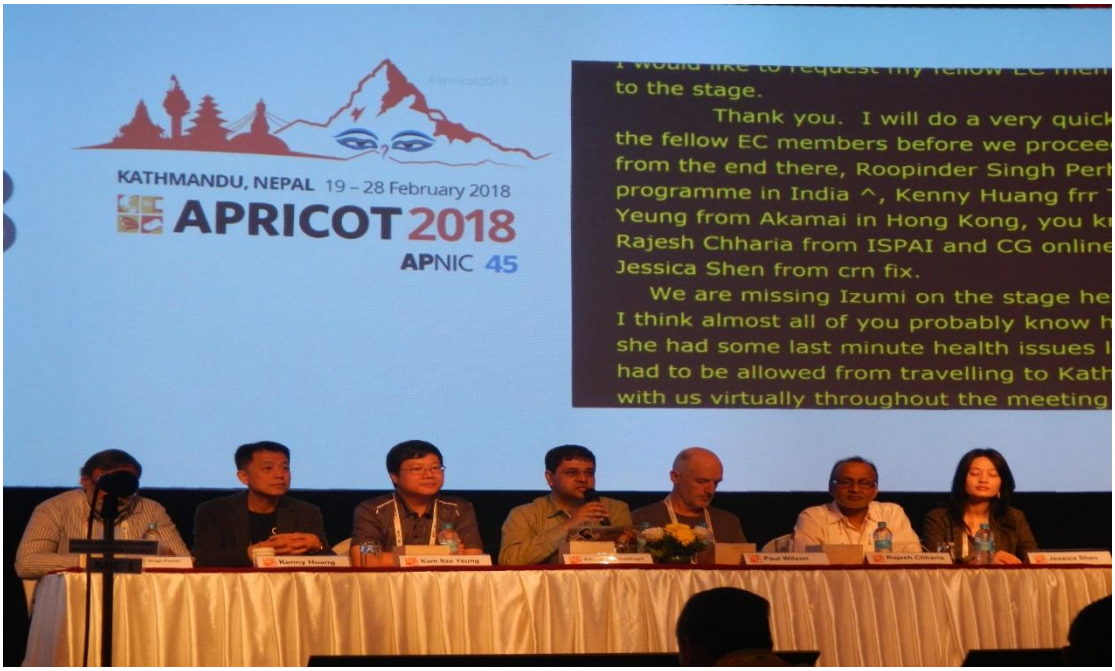


圖 68 APNIC 年度股東會議

伍、心得與建議

一、有關需受邀方能出席ICANN GAC會議一節，經利用會議中場休息時間向ICANN的人員詢問，始知本會已是GAC會員，因此只要透過事先報名，即可參加完整的ICANN GAC會議。惟此次針對亞洲地區所舉辦的ICANN GAC會議，並不像一般每年三次的ICANN GAC會議針對各議題進行討論，而是較偏重於經驗的分享。其目的似乎是針對尚未成為GAC會員的國家宣傳GAC的政策制定，以吸引發展中國家加入成為GAC會員。

二、為加強網路治理、促進我國國內業界對於ICANN各小組所討論之議題的熟悉度與參與程度，似可要求TWNIC仿照JPNIC的作法，將ICANN歷次會議討論議題譯成中文，置於網站供大家閱覽，並適時就ICANN討論之議題舉辦研討會，以凝聚國內共識後，於ICANN相關會議中提出建言，爭取我國之網際網路話語權。

三、我國推動IPv6的普行，在策略上除採用雙堆疊(Dual stack)模式外，亦應思考並擬定最終部署Single Stack IPv6的長期策略。而澳洲由雙堆疊(Dual-Stack)過渡到IPv6單一堆疊所採行的策略，是值得參考的策略。

四、IPv6 Transition and Deployment會議除了邏輯概念的介紹外，涉及許多技術細節，在沒有相關背景知識的情況下，並不容易理解。

五、APNIC的會議內容較不涉及政治意涵，有利於我國爭取話語權。因此建議應持續關注會議中所討論之特定議題，深入研究，並透過在國內舉辦研討論之形式，邀集國內產業界討論以形成共識，俾利積極在會議中表達我國之看法，對全球網際網路發展做出貢獻。

六、期TWNIC未來可持續辦理相關國際資通訊會議，有助提升國內產業技術並行銷台灣：以尼泊爾爭取主辦本次會議，除提供該國更多技術人員研習機會、降低出國研習成本外，亦能帶動、行銷該國觀光及人文產業。此與日本及韓國近年爭取舉辦奧運目的是相近的，除可帶動該國產業技術升級（例如5G、4K/8K）外，主要仍是達到國際行銷所帶來的後續觀光及經濟效果。我國TWNIC於2017年舉辦APNIC第44次國際會議，除便利我國業者參與經、吸引亞太地區相關專家齊聚台中經驗交流外，本次會議期間諸多簡報亦有提及該次活動，對行銷台灣實有助益。

七、舉辦國際會議宜提供優質設施及環境：此次大會，針對APNIC組織運作及政策研商之會議均有提供即時英文字幕的服務，主要是協助與會者克服各國腔調不同的問題，充分瞭解發言內涵才能做出正確判斷及決策。利用AI技術提供語音辨識，應該是相關產業提供此類服務的方向，技術成熟後更可利用到老人居家照護及聽障服務等利用。鑑於尼泊爾相關民生公共建設尚在進步中，本次會議雖經常發生電力中斷的情形，但總是很快就能恢復，可看出大會及主辦單位的努力。

八、持續加強普及服務及前瞻基礎建設計畫的推動：在開幕會議中，加德滿都市長等多位講者均共識數位落差的嚴重影響，並表示尼泊爾正努力追趕中，期望提升偏鄉無線寬頻，以提供遠距醫療及遠距教學等利用，也期望各界能提供資源協助。我國普及服務推動多年，透過電信事業分攤虧損的方式辦理，目前2Mbps寬頻服務已達全部偏鄉村里，12Mbps亦已有96.7%的涵蓋，確實有效降低了數位落差的問題。為更積極促進城鄉均衡發展及各種數位創新服務於偏鄉的可及性，政府亦投入預算推動前瞻基礎建設計畫，相信成果應能更為豐碩。

六、因應資訊跨境傳輸趨勢，積極參與相關國際組織、論壇或會議，以利相關管理措施能與國際主流一致：鑑於網際網路帶動跨境電子商務、OTT與IoT服務，然數據跨境傳輸所涉個資、隱私及侵權等問題層出不窮。目前全世界對Cross-Border Data Flow的管理尚無一致的法規及執法標準，歐盟、美國等經濟強權及相關組織（例如APNIC）已展開相關倡議及研議，為確保我國企業及民眾權益，除應及早進行國內法規研訂外，亦應與國際接軌，有完整的瞭解及因應措施（例如針對歐盟的GDPR）以利跨境服務貿易的推展。

七、應督責、鼓勵業者持續加強網路建設，以優化服務品質

從Peering Forum及IXP Forum相關會議中幾位專家研究、分析南亞地區及非洲地區的網際網路封包延遲現象，主因在於「基礎設施不足」、「境外內容需求度高」，所建議未來努力方向亦可供作我國參考：

（一）提升海纜及陸纜骨幹網路建設：所研究地區國家之骨幹網路普遍不足，欠缺直達之陸纜電路，訊務交換多採購買轉訊服務，繞至歐、美、日、香港、新加坡等節點交換，不利於服務品質及成本。同時，許多國家對外路由僅1至3條，路由備

援相當不足。我國雖不致於有上述情形，但因應民眾寬頻需求及天然災害日益增加下，電信業者亦應提早規劃擴充足適的國內外電路容量及備援路由。

（二）因應AR、VR等服務需求，積極提升FTTH接取網路的普及：從講者資料發現，撥接及ADSL等服務在南亞地區仍大量使用，確實不符合目前網際網路訊務以vedio為主的潮流。另一方面，雖然日本FTTH涵蓋率已達99%，使用率僅53.6%，但因投資金額龐大，需有相當長的建設期，或許目前國內業者對於FTTH的市場需求仍持保留態度，惟基礎建設非一蹴可及，仍需思考未來市場需求，提早進行規劃及建設，俾保持市場競爭力。

（三）鼓勵電信業者與國內外相關產業緊密合作，提供優質服務：雖長久以來全球普遍存在以來電信業者與內容業者間存有搭便車（free rider）爭議，但鑑於國內民眾對Google、Facebook、Amazon等國際級網際網路公司服務高度依賴，相關產業間確實需要更多對話，共同和諧解決消費者需求。我國為海島型國家，為滿足消費者接取境外內容時仍有低延遲的優良品質需求，除應持續投資、採購更多海纜頻寬外，與CDN（Content Delivery Network）協商達成雙贏之合作，應該是值得努力的方案。

（四）鼓勵、營造合理的互連市場，本地訊務本地交換：基於營運策略及成本考量，網際網路產業，無論電信事業、內容產業、CDN等業者於進行互連協議時均有商業的判斷基準及打算，政府確實較難且不便介入，惟如可能妨礙國內整體經濟發展的爭議發生時，政府亦會採取相關措施；例如持續透過X值機制引導固網市場主導者的網際網路互連頻寬費用，兼顧設施競爭及服務競爭的發展。以印尼IIX於全國廣設11個交換節點為例，主要是考量其「萬島之國」及各主要人口聚集島嶼自成訊務交換需求的特質，廣設IXP交換節點可降低集中訊務所需骨幹成本及品質上的減損。目前我國資訊產業聚落集中於北部地區，故主要IDC及IXP均設置於北部，倘未來中、南部也有形成聚落跡象時，亦期望相關業者能於當地投資IXP可提升訊務品質，甚或加速聚落的形成。

八、鼓勵、支持TWNIC強化與APNIC等組織合作，對網際網路社會做出貢獻：因應網際網路演進迅速，雖帶來許多好處，但隱藏在後的犯罪問題也不容忽視。Whois等資

料庫的正確性，除提供業者商業發展外，對於防制犯罪亦有其功效。目前APNIC等組織刻正積極推展Whoi、Whowas等註冊資料庫及RPKI (Resource Public Key Infrastructure，亦稱為RC，Resource Certification)之資源驗證機制，這些努力要真正獲得成果是必需全員合作的。

九、網路資安做得好，用戶上網沒煩惱

（一）資安可謂國安

政府、社群網站及多數企業均經由網際網路提供相關服務或電子商務，然而根據bgpstream.com提供的統計資訊顯示，網路攻擊每天都在發生。單一網站遭受網路攻擊造成服務中斷，其影響尚為有限；但如果是ISP或提供網域名稱解析服務的公司遭受網路攻擊而服務停擺，對國家、社會、經濟等所產生之影響將更為深遠。2016年10月，美國知名網域名稱服務公司Dyn攻擊遭受大規模DDoS攻擊，造成Amazon、Twitter、Netflix、CNN、eBay、App Store、Pinterest、Box、PayPal、Shopify、Github、Etsy等大型網站服務中斷，其影響之深遠可見一斑。

我蔡英文總統105年12月1日出席「第12屆台灣駭客年會HITCON Pacific 2016」，即表態政府強化資安管理制度的努力與決心，並提及執政半年以來，積極將「資安就是國安」的觀念帶入政府的組織文化。

隨著物聯網裝置應用漸廣，又具備上網特性，爰吸引駭客青睞。近年來IPCAM、CCTV、DVR、路由器等有嵌入Linux作業系統之物聯網裝置，變成殭屍網路之一員時有所聞。前述DYN及同時期發生的雲端服務與主機代管供應商OVH、KrebsOnSecurity網站攻擊事件，經資安專家審視結果，其攻擊來源都遙指Mirai殭屍網路（OVH計14萬臺物聯網設備、KrebsOnSecurity計2.4萬臺物聯網設備），且攻擊等級都遠遠超越了2015年底英國BBC遭遇的602Gbps攻擊流量。

根據市調機構Gartner的報告顯示，全球物聯網裝置數量至2020年將高達204億台。在這亮麗的數字背後，也潛藏著極大的風險。Gartner預估，2020年企業所遭受的資安攻擊，25%以上將與物聯網裝置相關。物聯網裝置沒有資安設計、未設密碼或使用弱密碼即可接取，或資料傳輸沒有加密等都是資安防護的大忌，但這些只要製造商或使用者花點心思，就可以避免多數駭客入侵。

但網路攻擊就止於物聯網裝置嗎？其實不然，這點從APRIOT 2017 暨 APNIC 43 資安議題著重在物聯網裝置，此次會議資安議題則圍繞在網路傳輸平臺部分就可看出端倪。

此次會議，Worldwide Infrastructure Security Report Highlights場次，講者提及2017年DDoS攻擊流量峰值較2016年雖有下降趨勢，但網路攻擊的複雜度及次數卻有增無減，要大家不可掉以輕心，同時指出多數ISP認定之最大網路攻擊威脅仍為DDoS。果不其然，APNIC45會議結束次日，3月1日凌晨，知名程序開發網站「GitHub」即遭受了歷史上最嚴重的DDoS攻擊，攻擊流量峰值更高達1.3Tbps，所幸GitHub緊急向Akamai求助，將流量轉至Akamai 方解除一場驚險之旅。3月5日，該名講者服務的NETSCOUT Arbor公司又發出聲明，已確認針對某美國ISP客戶遭受攻擊流量達1.7Tbps的DDoS攻擊。短短數日，DDoS攻擊流量峰值又破紀錄，但這兩次的網路攻擊來源非殭屍網路，而是業者端的Memcached伺服器。Memcache是一個開源的分佈式內存緩存系統，用於幫助提高網站的速度。據Shodan網站稱，全球有超過80,000台Memcached服務器正在使用默認的不安全配置，並且正被濫用來發起反射、放大DDoS攻擊。

俗諺「殺頭的生意有人做，賠錢的生意沒人做」！提高網路頻寬、提升網路速度，引入新的通訊技術對營收可帶來正面助益。網路納入資安，雖可以提升網路可靠度、獲得良好商譽，但也提高網路複雜度、降低一定之網路效能，而且在網路攻擊技術不斷創新，所需投入之資源亦須與時俱進才能有效防護。對於事事將本求利的業者而言，網路投入大量資安資源實在誘因有限。此次會議亦有針對類似議題進行線上投票，多數投票者仍認為只有業者自發性落實才能真正確保路由安全。

（二）資安防護應從大處著眼、小處著手

為營造一安全的連網環境，從終端、傳輸平臺到雲端都應注入心力。在終端部分，為推動物聯網等終端設備資安防護，本會已於106年3月發布「智慧型手機系統內建軟體資通安全檢測技術規範」，今年更與經濟部工業局一起合作，各就所屬主管領域發布物聯網終端檢測規範。本會擬發布資安檢測技術規範包括無線IP CAM、WiFi AP及有線廣播電視數位機上盒；經濟部工業局為網路儲存設備NAS、

數位視訊錄影機DVR，並修訂IP CAM 資安檢測技術規範。

網路傳輸平臺部分，本會自106年起，即積極推動年度電信事業網路域名伺服器(DNS)防護演練，除驗證電信事業DNS伺服器之安全防護機制及應變處置程序，發掘風險管理潛在問題外，更期藉由演練精進應變指揮協調要領，提升電信事業DNS設施安全防護能量，確保服務提供及持續營運。演練項目分為情境演練及實兵演練兩種，並以DNS主機伺服器及DNS Cache伺服器設置合計5部以上之事業為演練對象。107年亦規劃研訂或修正增波器、網頁防火牆WAF、網路防火牆Firewall、入侵偵測系統IDS、入侵防護系統IPS、APT檢測沙箱等電信業者系統或網路所使用資通設備之資安檢測技術規範，俾據以加強網路傳輸平臺之資安防護能量。

至於雲端部分，經濟部工業局已於105年制訂「行動應用App基本資安規範」，提供第三方機構針對行動應用程式，進行資訊安全檢測及評估其安全水準之依據。藉由行動應用程式符合檢測基準要求，建立國人對行動應用程式使用之安全信賴感。

行動應用App基本資安規範與其他資安檢測技術規範般，均非強制規定，屬自主推動性質，雖其檢測對於隱私權保護、網路安全等有正面助益，但為符合其規定，在商品或程式設計規劃上，即須將資安議題納入考量，同時增加其成本及上市時程，爰部分業者對於資安檢測多採保留態度。。推動政府機關使用之終端設備或雲端服務應通過資安檢測尚有可為，但民間單位僅能多加宣導，以奏其效。崙此，資安檢測之推廣，仍需相關目的事業主管機關將其納入強制規定之一部。此外，目前本會積極推動年度電信事業網路域名伺服器(DNS)防護演練，亦應參考如Arber Networks單位所發布的Worldwide Infrastructure Security Report，以瞭解國際間網路傳輸平臺業者普遍認同之最大資安威脅，與時俱進調整演練標的，始得真正落實網路資安。

（三）資安防護深入人心才能營造一安全連網環境

身處資訊爆炸、萬物聯網的世代，除了從終端、傳輸平臺到雲端，布建一一安全的連網環境，最重要的還是使用者的習慣。根據 Worldwide Infrastructure Security Report Highlights場次講者提供之資料顯示，勒索軟體（Ransomware）是企

業、政府及學術單位最關心的議題及主要威脅。勒索軟體與DDoS攻擊不同，通常都是使用者瀏覽了不當網站或點了不當連結所造成，因此唯有資安防護深入人心，從小紮根，才能營造一安全連網環境。

陸、附件：會場照片

圖 69 本會同仁與APNIC總裁Paul Wilson合影