出國報告（出國類別：開會）

2019年亞太網路資訊中心國際會議（APNIC47）

服務機關：國家通訊傳播委員會
姓名職稱：林科長隆全
姜技正政男
派赴國家：韓國
出國期間：108年2月24日至3月1日
報告日期：108年4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政府國際組織機構（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。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 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（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營運技術大會（APRICOT）一起合辦。此次會議係第 47 屆，共匯集世界各地的網際網路工作者、專家學者、政府代表、產業代表等超過 63 個經濟體及 714 名以上人員參與。為期 10 天的峰會，分為工作坊及研討會兩部分，工作坊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 108 年 2 月 25 日至 28 日 4 天研討會。

此次會議相關議題計有 IPv6 網路發展、Peering、內容封鎖、路由安全等議題，另有多場技術研討會涉及 ISP 維運管理等，經由參與 DNSSEC、Peering、IPv6、SDN、Security 等相關論壇或講習，可汲取各網際網路專家分享之網路維運新知及網際網路發展所面臨問題與各方見解，強化同仁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

壹、前言 2
貳、行程安排 3
參、APNIC47會議（2018 APRICOT） 4
（一） 第一日（2月25日星期一） 5
（二） 第二日（2月26日星期二） 6
（三） 第三日（2月27日星期三） 7
（四） 第四日（2月28日星期四） 8
肆、會議過程及摘要 9
一、 第一日會議摘要 9
（一） DNS安全協議驗證機制（DNSSEC Validation） 9
（二） 利用DNS64 / NAT64 / 464XLAT構建純IPv6網路 （The IPv6-Only Network: Building Networks with DNS64/NAT64/464XLAT） 9
（三） 開幕式和全體會議（Opening Ceremony & Plenary） 11
（四） APNIC合作論壇（APNIC Cooperation SIG） 12
（五） 亞太地區電信商論壇（APOPS 1） 17
二、 第二日會議摘要 18
（一） APNIC國家互聯網註冊管理機構論壇（APNIC NIR SIG） 18
（二） DNS運作（DNS Operations） 23
（三） 網路互連I：區域化（Peering and Interconnection I：Regional） 23
（四） 技術研析會議（Technology） 24
（五）APNIC：合作遏制安全威脅（APNIC: Cooperating To Contain Security Threats） 27
（六） 工具（Tools） 27
三、 第三日會議摘要 28
（一） 事件驅動的網絡自動化和編排（Event-driven Network Automation and Orchestration） 28
（二） APNIC政策討論論壇1（APNIC Policy SIG 1） 29
（三） 5G技術-教學（5G technology: a tutorial） 31
（四） 路由安全2（Routing Security 2） 32
（五） APNIC政策討論論壇3（APNIC Policy SIG 3） 34
（六） 資訊中心（Data Centre） 35
（七） 網路營運1（Network Operations 1） 37
四、 第四日會議摘要 38
（一） 訪談南韓電信業者SK 38
（二） APNIC年度全體會議1~3（APNIC AGM 1~3） 38
（三） IPv4aaS教程和實踐（IPv4aaS tutorial and hands-on - Part 1） 39
（四） 網路營運2（Network Operations 2） 40
（五） ONOS SDN-IP：SDX的教程和使用案例（SDN-IP: Tutorial and Use Case for SDX） 41
（六） 參訪韓國電子通信研究院 42
（七） 閉幕大會（Closing Plenary） 43

伍、心得與建議..... 44

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）並列五大區域性網際網路註冊管理（RIR）機構，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。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 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（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，各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）一起合辦，此次會議係第 47 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 714 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、路由安全等議題，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：2019 年 2 月 24 日至 3 月 1 日

二、 地點：韓國大田

三、 本會出席人員：

（一）平臺事業管理處 林科長隆全

（二）射頻與資源管理處 姜技正政男

四、 時程安排暨航班表

日 期	時程安排
2月24日(日)	中華航空(CI260) 09:20 出發：臺北松山機場 14:20 抵達：金浦國際機場
2月25日(一) ~ 2月28日(四)	出席亞太網路資訊中心 47th 論壇活動
3月1日(五)	中華航空(CI163) 20:55 出發：仁川國際機場 22:45 抵達：臺灣桃園機場(TPE)

參、APNIC47 會議（2018 APRICOT）

一、會議時間：2019年2月25日至2月28日

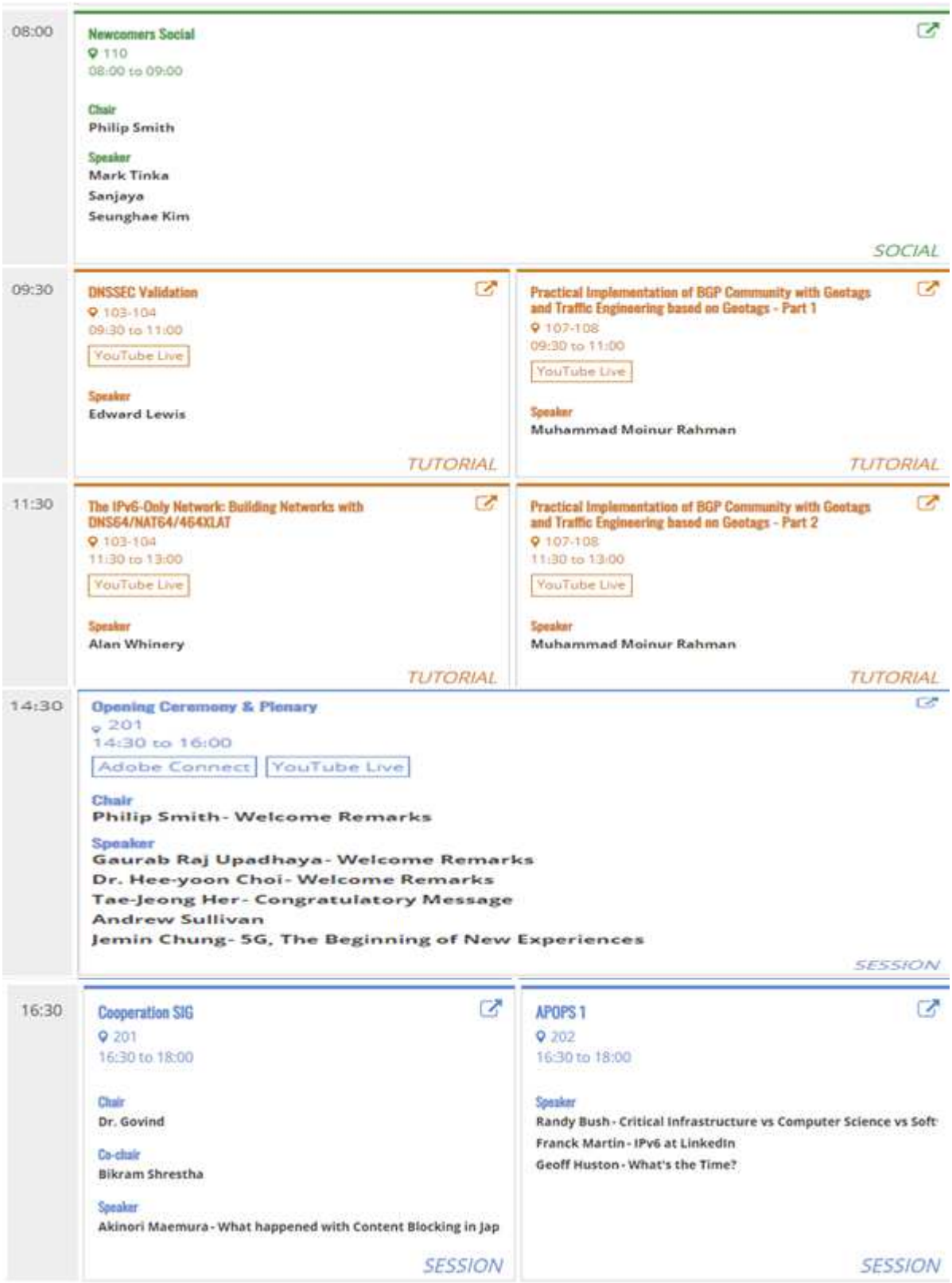
二、會議地點：大田廣域市國際會議中心DCC（Daejeon Convention Center）

圖 2 DCC會場

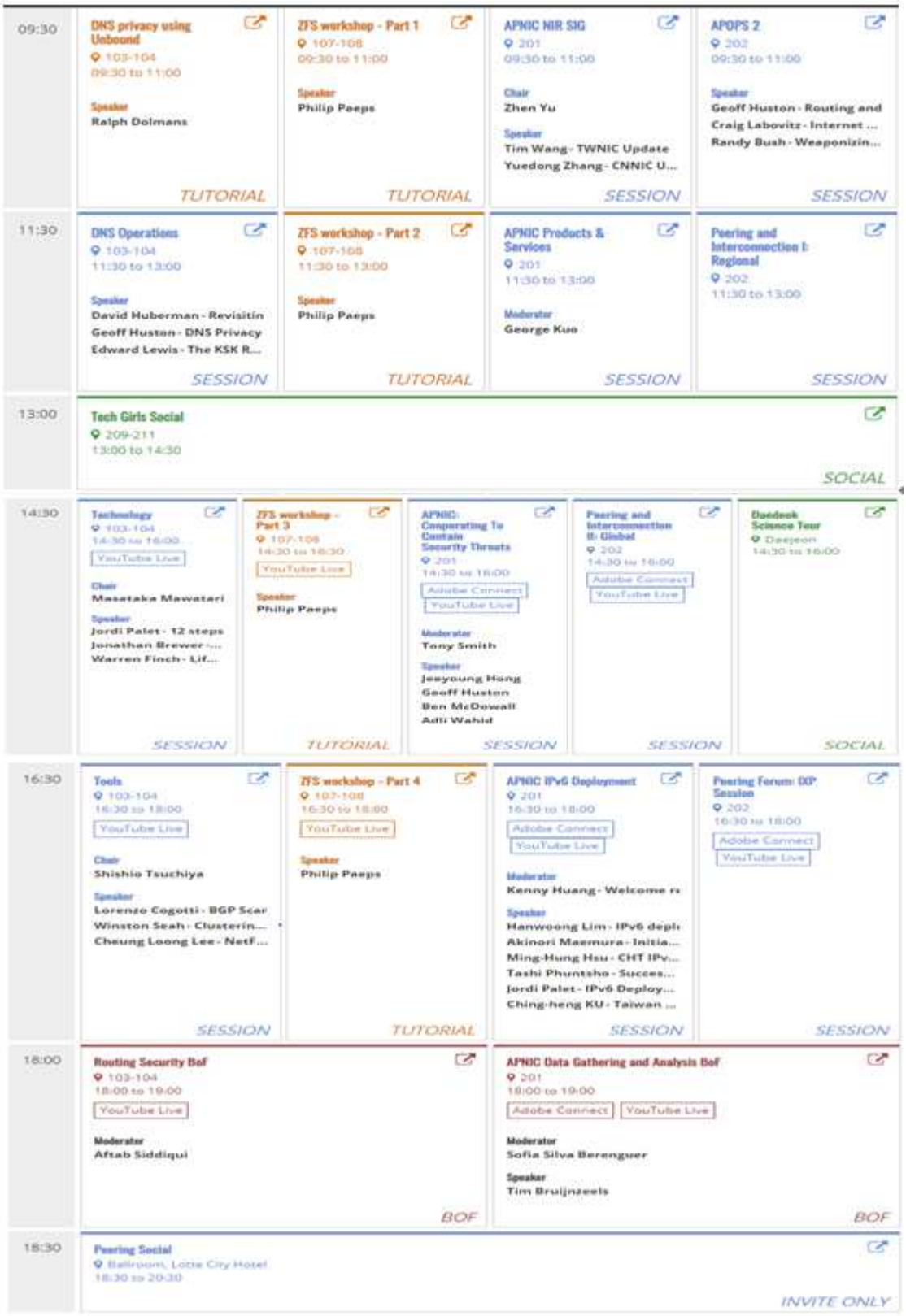
圖3 會議地點 DCC 地理位置

三、會議議程：

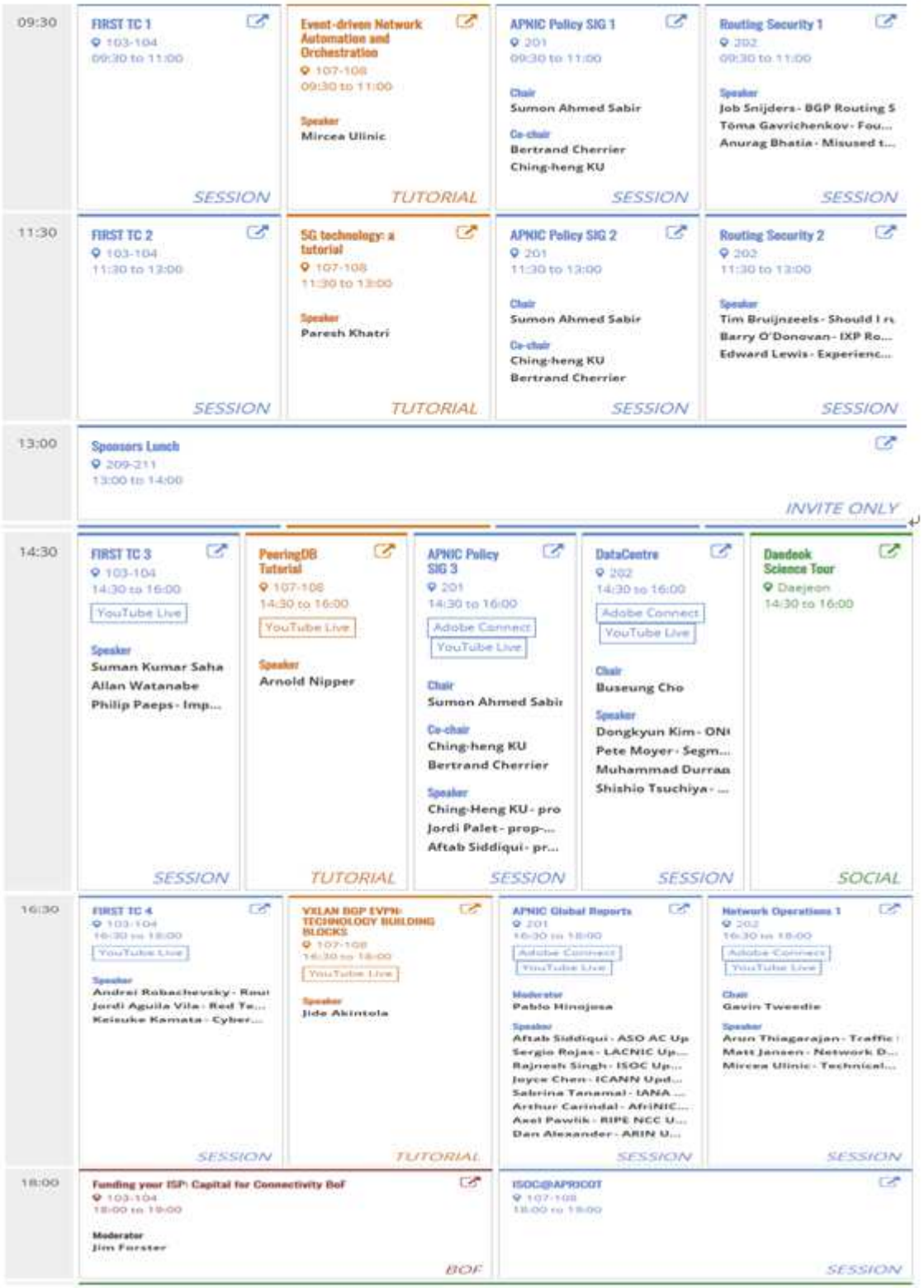
（一）第一日（2 月 25 日星期一）



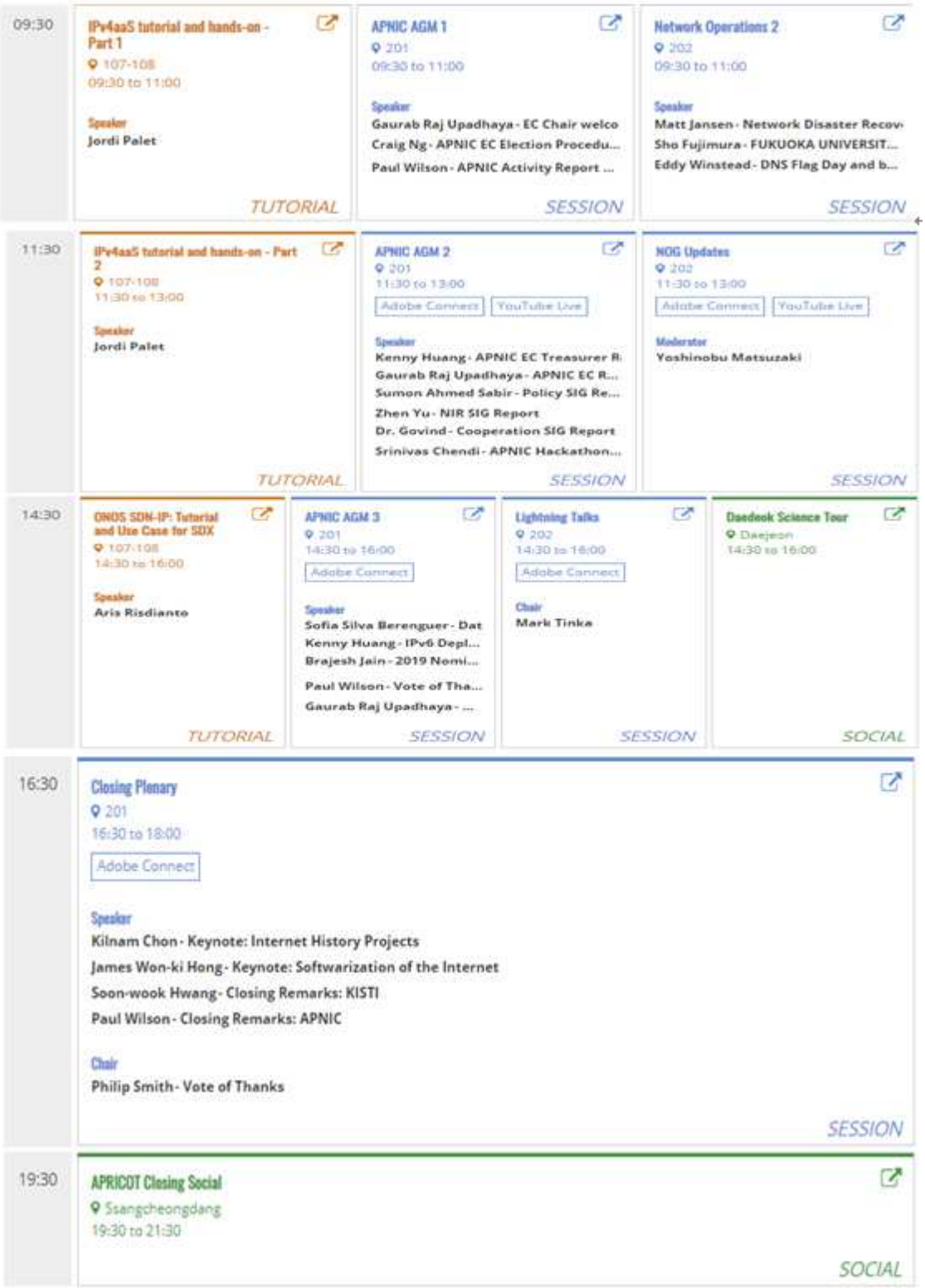
（二）第二日（2 月 26 日星期二）



（三）第三日（2 月 27 日星期三）



（四）第四日（2 月 28 日星期四）



肆、會議過程及摘要

一、第一日會議摘要

（一）DNS 安全協議驗證機制（DNSSEC Validation）

本場次由ICANN高級工程師 Edward Lewis進行DNSSEC驗證機制之教學，內容摘要如下：

Edward Lewis 說明， DNSSEC (DNS Security Extensions standard)是 DNS 資料的安全認證機制，主要目的是驗證資料來源，透過數位簽章以確保 DNS 查詢的紀錄沒有被竄改，而非將資料加密。有關數位簽章之運作方式，係一方利用雜湊函式(Hash Function) 將欲傳送之資料產生一組驗證值(Hash Value)，並用私有鑰匙(Private Key)對該驗證值加密後，產生一組數位簽章交給另一方，另一方收到後，若能順利使用公眾鑰匙(Public Key)將數位簽章解開，即可確定該資料之來源，接著因為雜湊函式是多對一的映射，無法由輸出回推原本的輸入訊息，爰使用相同的雜湊函式計算該資料的驗證值，若發現與先前公眾鑰匙解開的數位簽章內附的值是相符，即可表示該資料之內容未遭竄改。 DNSSEC 的優點在於可完全兼容於現行的 DNS，更額外提供三項資訊安全：

- 資料完整性 (data integrity)。
- 來源可驗證性 (origin authentication of DNS data)。
- 可驗證之不存在性 (authenticated denial of existence)。

但 DNSSEC 並無法提供下列二項安全性服務：

- 隱密性 (Confidentiality)：DNS 請求與回應的資料無法避免被竊聽。
- 有效性 (Availability)：阻斷服務(Denial of Service)的攻擊仍可能有效。

另講者增加 DNSKEY、RRSIG、NSEC/NSEC、NSEC3PARAM 及 DS 等欄位，並進行資料驗證，渠說明在 DNSSEC 機制中，有兩種非對稱金鑰分別為 KSK（Key Signing Key）和 ZSK（Zone Signing Key）。這兩種 KEY 之差異在於， 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好處，因為 DNSSEC 是由 root DNS 一層一層往下驗證，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 重新作一次簽章即可。最後渠說明 DNSSEC 可歸納如下優點：

- 消費者端：可安全的使用網際網路。
- 網際網路位址或網域名稱註冊人：減少欺詐及更好的品牌保護。
- 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）。
- 為其他安全改進作為提供平臺。

（二）利用 DNS64 / NAT64 / 464XLAT 構建純 IPv6 網路 （The IPv6-Only Network: Building Networks with DNS64/NAT64/464XLAT）

講者(Alan Whinery)說明鑒於 IPv4 數量不足、IPv4 成本高、用戶及設備數量

快速增加，特殊應用程式(如 VM)、IOT、長期經營策略等理由，直接建置 IPv6 仍為可能選項，此時需要解決用戶與 IPv4 網站連接的問題，爰講者以其長達 15 年 IPv6 經驗，向參與會議者表示，維護純 IPv6，比維護 IPv4/IPv6 雙堆疊（Dual stack），更可降低大量維護成本，但在目前仍有許多用戶是 IPv4 情況下，IPv4 訊務仍有其需求，爰須透過網路位址轉換（NAT），以解決 IPv6 與 IPv4 主機間通訊的 IPv6 轉換機制，其方式包含：NAT64、NAT64 與 DNS64、464XLAT 等方法。

有關 DNS64 與 NAT64 運作原理如下：

- NAT64 是為了讓純 IPv4 與純 IPv6 的網路位址互相轉換格式，讓 IPv4 與 IPv6 互相連線。
- NAT64 需透過 DNS64，始知道要轉換的 IP。
- IPv4 用戶查詢 DNS 的請求，會產生兩個 DNS 封包，分別查詢 IPv6 與 IPv4 位址，若查詢結果為 IPv6 位址，則直接回傳，若查詢結果是 IPv4，則會進行轉換。

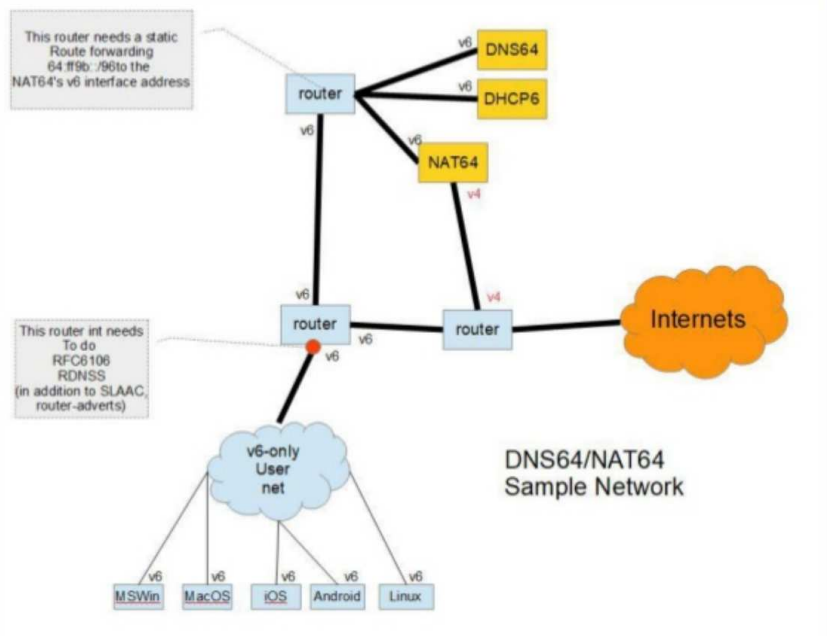


圖4 DNS64與NAT64網路運作方式 [資料來源：講者簡報]

有關 464XLAT 是用於 IPv4 與 IPv6 之間通信，464XLAT 採用翻譯方式進行 IPv4 轉換 IPv6，在 IPv4-IPv6 網路邊界利用 CLAT 進行 NAT 翻譯，在 IPv6 網路中以 IPv6 報文進行轉發和處理。

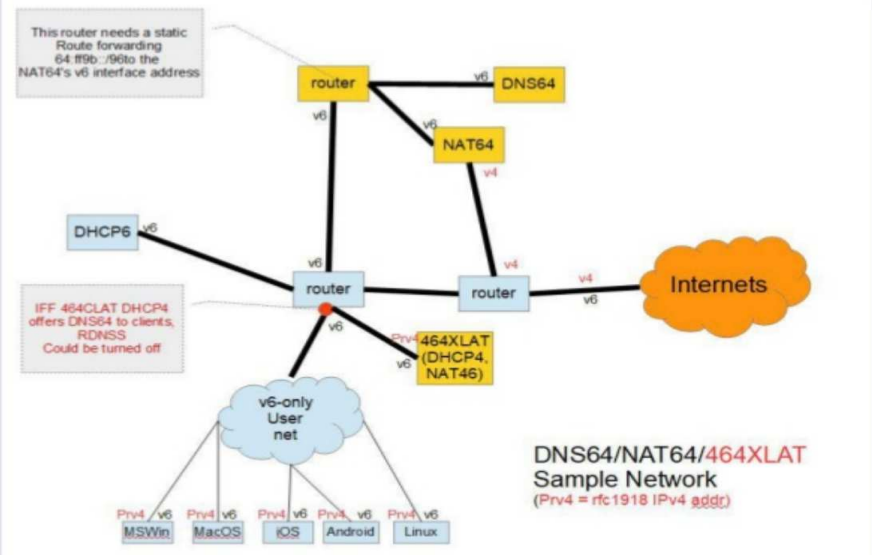


圖 5 DNS64 與 NAT64 與 464XLAT 網路運作方式 [資料來源：講者簡報]

（三）開幕式和全體會議（Opening Ceremony & Plenary）

由APRICOT主席Philip Smith、APNIC 總裁 Paul Wilsona及 KISTI Dr. Hee-yoon Choi 博士開場致詞，歡迎超過63個經濟體及714名以上人員參與會議，並於大略說明接下來為期4天的議程後，由韓國大田廣域市長 Tae-Jeong Her歡迎與會人員參加本次會議，接續由韓國電信(KT)首席工程師 Jemin Chung進行「開始新的實驗-5G」專題演講，介紹5G的基本概念，摘要如下：

韓國電信 Jemin Chung說明，自MWC於2015年3月發表下一代行動通信服務5G的版本以來，韓國電信就開始研究、開發，至今約4年的時間，並於2019年1月正式商轉，該技術被認為可以提高行動數據速度並將能減少延遲，預計5G的來臨將以新方式改變目前用戶對無線通信服務體驗。在本次演講中，主要討論5G的重要性，在這資訊、數據爆炸的時代，虛擬、擴增實境與全像投影都仰賴大量訊息交換，而5G網路具有峰值速率20Gbps、網路實際連接速率100Mbps、3倍頻譜效率、網路延遲1ms、移動速度500km/h、網路能源效率為4G LTE的100倍、連網密度每平方公里100萬個裝置及區域聯網能力每平方公尺10Mbps等主要優勢，可帶動產業發展增進便利性，講者並說明在不久的將來，5G進入行動通信市場，應用於汽車、智慧工廠、無人機時可能發生的挑戰和機遇，如：韓國電信在3.5GHz取得100MHz的頻寬，DL為3.08Gbps、UL為300Mbps，而在28GHz取得800MHz的頻寬，需多少下載和上傳量才足夠應付20G bps峰值流量(peak throughput)、E2E (End to End)13ms (空氣延遲1ms+傳輸延遲<<1ms+晶片延遲1ms+App與伺服器延遲10ms)之延遲率是否可接受、面臨大規模的連線是否可以應付等。

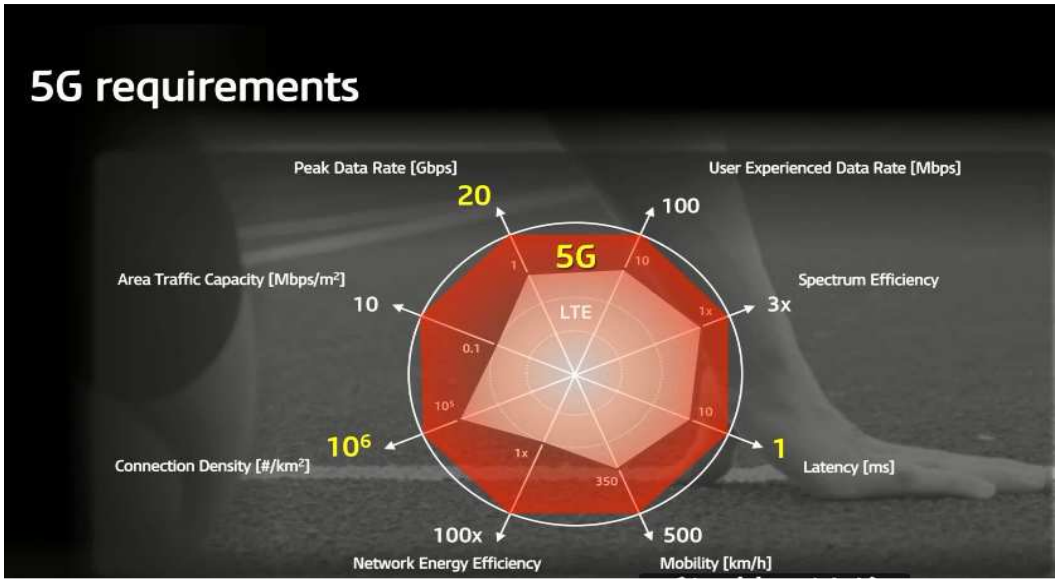


圖 6 下一代移動通信服務 5G 與 4G LTE 之特性比較 [資料來源：講者簡報]

（四）APNIC 合作論壇（APNIC Cooperation SIG）

Cooperation SIG（Special Interest Groups）是一個提供廣泛討論網際網路問題的論壇，如公共政策和網際網路治理，這些問題與APNIC社群利益有關，也涉及政府和其他相關組織、團體或社群。

本場次會議由Dr. Govind擔任主席，首先是辦理下一屆的主席（chair）選舉，共有4名候選人，包括我國TWNIC丁副執行長綺萍(Joy Chan)；經全體與會者舉手投票，由我國TWNIC丁副執行長獲選為Cooperation SIG 下屆主席。

會議緊接著進行內容阻斷之相關座談，並由主席Dr. Govind作開場引言，渠說明隨著全球越來越多的人連接到網際網路，創造產生了多元的且大量的人類活動內容，如社會，政治，經濟和娛樂……等。網際網路建立在全球技術基礎設施下，以開放性、全球互連為原則，可自由且不受限進行通訊，並創造出創新的應用服務及內容，但也帶來更多假新聞、激發仇恨演講、惡意且侮辱性內容。

主席進一步說明，媒介機構如網際網路供應商ISP、社交媒體和搜索引擎是促進內容業者與最終用戶溝通的平臺。雖然這些平臺是以全球為基礎，但內容卻通常是以當地為主。在這背景下產出衝突矛盾。一方面，言論自由和隱私問題對終端用戶來說非常重要。另一方面，政府和執法機構則關注越來越多擾亂社會公共秩序並威脅民主規範的非法內容。到底這些平臺中需要什麼樣的內容？哪些內容需要被封鎖、過濾？有哪些規範、政策需要遵循？這必須在各種不同利害相關者間取得平衡。內容封鎖和過濾會影響到不同需求的用戶、服務供應商、技術、網路社群及政策制定者在成本、風險的觀點。技術專長是關鍵問題。此外，更進一步的方向可能是進行各利害團體的對話、協力、合作，目前已越來越多的國家開始對內容進行審查。

接著，主席分別邀請Sanima Bank Ltd公司Bikram Shrestha、JPNIC Japan Network Information Center Akinori Maemura（前村 昌紀）、Fiber@Home 公

司Chief Strategic Officer Mr Sumon Ahmed Sabir、ICANN APRALO主席Satish Babu就本主題設定相關子議題，並做進一步之經驗或觀點分享：

1、2018 年日本對內容封鎖做了哪些措施？（What happened with Content Blocking in Japan in 2018?）

本場次由JPNIC Japan Network Information Center Akinori Maemura(前村昌紀)擔任講者，渠說明漫畫Manga在日本一直以來很受歡迎，即使是成年人、老年人也喜歡將漫畫當作自己的休閒娛樂。在2017年，一個知名盜版網站大幅崛起–"漫畫村 Manga-Mura"。這網站實際上對於卡通漫畫的知識產權造成相當大的損失。這個漫畫盜版網站，是以收集了大量的頁面瀏覽量而聞名，但是卻侵犯了合法的內容業者之適當利潤。 隨著盜版網站的問題日趨嚴重，去年，2018年 4月13日，日本內閣政府決定對內容封鎖立法，並成立一個特定的專責小組Task force，對盜版行為進行為期四個月的反制措施討論。然而在討論的幾個月後，專責小組並未作出具體的結論。以下是這段期間主要的事項里程:

- 2018 年 4 月 13 日

日本時報網站Japan Times website報導 日本政府以緊急措施呼籲封鎖非法漫畫及動畫網站(Japan calls for 'emergency measure' blocking access to websites that pirate manga and anime) ：https://www.japantimes.co.jp/news/2018/04/13/national/japan-calls-emergency-measure-blocking-access-websites-pirate-manga-anime/#.XH3nxSIzacM 。 內閣當日舉行了打擊犯罪措施會議並決定了三件事，如下：

(1) 針對盜版漫畫、動漫……等網站必需採取反制措施。
(2) 對三個為害最大的盜版網站，目前網路接取業主動對這些網站封鎖是適當的作法。
(3) 雖然 ISP 因應內閣要求對盜版網站作有效的封鎖，內閣知識產權戰略本部應針對立法事項和其他措施，與專家和業者作適當的考量。即暫時要求 ISP 對盜版網站內容封鎖，再想到未來相關的立法。

- 2018 年 6 月 22 日

在內閣知識產權戰略本部驗證・評估・企劃委員會下成立新的「盜版網站反制措施專責小組」(Task force on the counter-measures for piracy sites on the internet)，成員包括由兩位聯合主席：慶應義塾大學的Nakamura教授和Jun Murai教授，及其他6位來自電信及網際網路業者(包括演講者)；5位來自出版業及出版協會；1位來自消保協會和6位專長分別是知識產權，憲法，電信政策的法學專家成。專責小組在四個月內共舉辦9次會議及1次研討會，這是非常密集且忙碌的會議。這九次會議和一次研討會都非常公開透明，所有的會議記錄都公開在以下網站：http://www.kantei.go.jp/jp/singi/titeki2/。

惟當內閣決定成立專責小組時即已有定見，內閣似乎有意在2018國會正常會期內提交立法規範內容封鎖，但由於成員來自不同背景下，專責小組對於贊同與反對內容封鎖出現兩極化爭論，爰會議上並未達到合適、理性及公平的討論。 最後，在第八次會議上，有九名成員反對立法，拒絕產出專案報告。而為何進行了討論，不進行討論報告？因為反對成員名明白

即使報告涵蓋贊同與反對內容封鎖，內閣也只會擷取贊同內容封鎖論點提交立法，這就反對內容封鎖成員拒絕產出報告的理由。

最後，講者說明針對網站內容封鎖，有以下二點值得探討：

- 通信保密 secrecy of communications：在日本已有法規保護通信秘密，其中之一是日本的憲法第 21 條、另一項是電信企業法第 4 條 Telecommunications Business Act, article 4。 通信秘密是一項複雜的概念，但一位著名的日本的博主 Akimichi 在 APNIC blog 上發表了自己的觀點，通信秘密的基本觀點是，截取用戶端在網路上發送的任何內容即違反通信秘密，即使是 IP 數據封包標頭。雖然這是一個基本概念，但是有四點例外仍可將違規視為正當的理由，如下：
  (1) 為達成正當的商業行為。
  (2) 急於處理當前風險的迫切性。
  (3) 沒有任何其他方法可以避免類此情況發生。
  (4) 本作法之獲益將遠超越違法行所造成的損失。 例如，路由本身就是從數據包中獲取 IP 地址信息。這雖違反了通信的秘密，但它絕對是商業行為所需，將數據封包送至正確目的地。所以它是合法，即使違反和侵犯了通信的秘密。

  其次，對於兒童色情問題child porn case，目前在日本的網際網路上已經對兒童色情網站進行內容封鎖。近幾年也進行了大量的探討，在這種情況下，兒童色情問題的緊急風險處理就變得的非常重要。透過封鎖，雖然會侵犯一些權利，但是保護受虐孩子的人權之獲益將彌補這種權利受損的損失。所以封鎖行為就有其正當性。
- 除了封鎖外，其他解決盜版的方法：通信保密在去年由法學家和業內人士進行了大量討論，針對支持與反對的不同觀點下作探討，例如：加強數據權利保護機制(data right protection mechanism)、推廣合法內容的傳播、道德教育、禁止下載內容、過濾搜尋結果、處理水蛭網站 leech sites、過濾廣告內容、刪除要求、刪除 CDN 內容、識別和強制執行此類盜版網站、過濾客戶、由 ISP 作封鎖等。

Multiple approaches

Measure	For-blocking argument	Anti-blocking argument
Reinforce DRM	Longer term solution	
Promote the distribution of legitimate content		
Moral education		
Outlaw downloading	Not yet	Now on the way (another problem)
Suppress search result	not enough to be effective	Getting more effective
Address Leech sites	Difficult to define the leech	On the way to define
Suppress ads	Not enough to be effective	action being taken
Removal request	CDN doesn't disclose the content origin	CDN does
Takedown at CDN	CDN doesn't take it down	Should be done at the origin
Identify and enforce	Difficult to enforce on those who are abroad	
Filtering at the client	Not enough to be effective	Already enforceable
Blocking at ISP	The only effective means	many other ways

圖7 正、反二方對解決盜版方法的看法 [資料來源：講者簡報]

2、內容阻斷：解決社會/政治問題的技術方法？（Content blocking and filtering: A Technical approach to solve Socio/Political Issue?）

本場次由Fiber@Home公司Chief Strategic Officer Mr Sumon Ahmed Sabir擔任講者，講者說明，網際網路成為多元且強大的溝通工具，很容易製造一些正確或錯誤的訊息，因此各國政府皆急於想管控，也形成一項艱鉅的挑戰。原因如兒少保護或某些國家對不同宗教信仰之過濾，許多國家基於政治動機對內容封鎖，及最近的假新聞，都是每個國家及人民所關注。內容封鎖也可能是商業公司避免員工在上班時間上社交網站或政府以法令要求電信業者對特定內容作封鎖。一些國家以filtering mechanism去過濾進出該國的訊務量。欣慰的是，統計數據顯示一些國家直接要求內容來源的供應商過濾特定內容，而非透過媒介的中間商。

接續講者提供2017年要求Facebook阻斷內容次數統計分析，前3名國家依序為土耳其、墨西哥及印度，並說明2016年至2018年要求關閉網站次數最多之國家為印度，另在講者提供Google 2018年的公開報告中，說明大多數政府基於國家安全要求，請求Google過濾特定內容。渠說明在技術及運作上對的挑戰如下：

- 不破壞網際網路的情況下獲得理想的結果(講者認為本項影響最大)。
- 網際網路服務供應商對應遵守政府命令阻止特定內容成承受巨大壓力。
- 限制 IP 位置、APP ID、URL 等使用網際網路/內容的資源，是不公平的。
- 向攻擊者開放個人數據和用戶權利，目前尚不合法。
- 阻止特定內容到特定用戶群，很容易就變成阻止整個國家的整個服務。
- 如何區分假新聞、恐怖主義、誹謗、金融犯罪和許多其他反國家/社會的活動，哪個需要政府對其進行強有力的控制，進而從阻斷內容阻止和過濾。

最後，講者說明內容封鎖是可用各種不同技術、ISP依政府要求用字首prefixes過濾或URL、DPI(Deep packet inspection) filtering等其他方式。其中DPI會造成其他問題，因為封鎖一個內容可能連帶影響到與該內容無關的整個網站，且DPI也會侵犯到隱私及人權。另網際網路的過濾成為箝制言論自由也成為關注的焦點，在南亞國家ISP機房成排的DPI設備遠大於提供上網的設備，對特定族群封鎖特定內容也可能變成封鎖整個區域或國家，因此，在科技不斷在進步下，今日鎖特或許有效，但不保證未來依然有效。

Content Blocking Request to Facebook [H2 - 2017]

Country	Count
Turkey	3,832
Mexico	2,280
India	1,914
Germany	1,893
Brazil	1,137
Italy	535
Israel	487
France	354
Pakistan	301

Source :
https://transparency.facebook.com/

圖8 2017年要求Facebook阻斷內容次數統計　[資料來源：講者簡報]

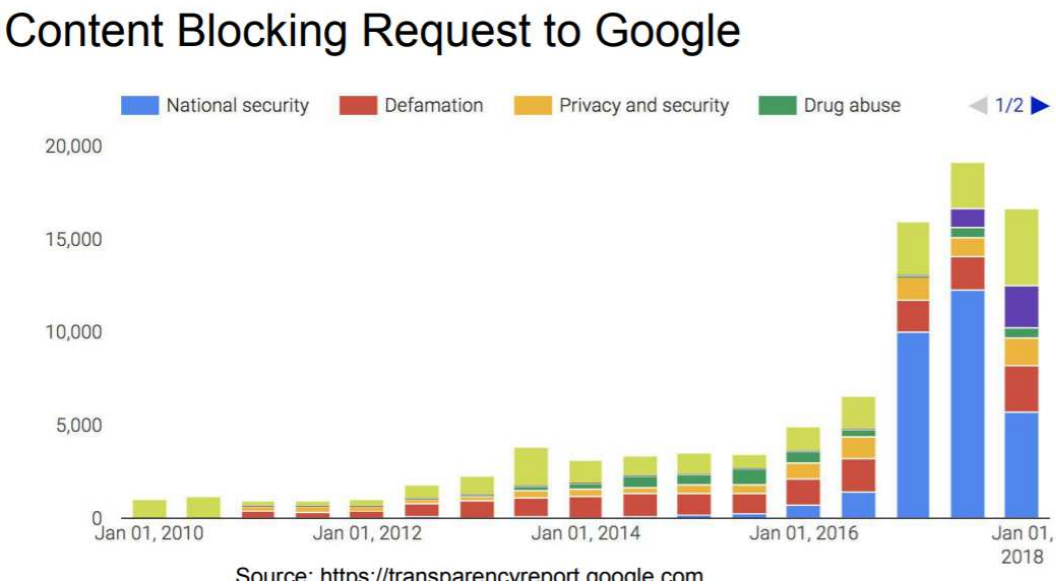


圖9 Google分析2018年阻斷內容之主要原因　[資料來源：講者簡報]

3、內容阻斷：用戶觀點（Content Blocking: End-user Perspectives）

本場次由ICANN APRALO主席Satish Babu擔任講者，渠說明說明阻斷內容可能需要克服事項，包括：成本、效能、與執法部門的衝突、需要安裝第三方軟體等。

接續與談人及現場與會者熱烈討論，大致為網際網路提供人類生活各方面需求（社會，政治，經濟，娛樂等），但所創造大量內容卻未全相容於法規，其間似未能完全相互取得平衡。至今網際網路充斥越來越多假新聞、仇恨言論、惡意和侮辱性內容，雖網際網路已被設計為開放性的全球技術基礎設施，可於全球相互連結。對於最終用戶來說，言論自由和隱私問題相對重要，而政府機構關注的可能是擾亂公共秩序和威脅社會民主規範的有害/非法內容。因此，如何要求平臺業者提供哪種內容、如何過濾不

影響用戶、哪種類型需要阻止或過濾以及應遵循哪些規範/政策，尚需從各利益關係團體、符合政府機關、成本、風險和技術專業知識的角度間取得平衡，並對阻斷內容有以下結論：

- 阻斷內容在世界許多地方都是困難的。
- 作為一種概念，阻斷內容違背了網際網路的精神。
- 實際上它會提高性能和安全/穩定性問題，並給網際網路服務供應商帶來負擔。
- 對於最終用戶而言，人權與生產力之間存在複雜的問題。
- 各國政府於協商阻斷內容政策時，應先讓人民對政策之制定充滿信心。

（五）亞太地區電信商論壇（APOPS 1）

APOPS（Asia Pacific Operators Forum）是一個在所有APNIC會議上舉行，提供亞太地區全體網路營運者及技術人員參加的論壇。每次會議主題各不相同，但者是當前社群普遍關注、感興趣的重大營運問題。本場次為此屆大會之第1場次，各講者重點摘述如下：

1、LinkedIn 對 IPv6 政策（IPv6 at LinkedIn）

本場次由美國社群網站LinkedIn公司Franck Martin擔任講者，渠說明該公司自2012年以來，一直致力於支持IPv6之發展，首先係從電子郵件開始，然後是網站，並說明該公司在各地區都發現巨大的成長，尤其是印度和中國，渠並說明該公司支持IPv6平順的移轉，不僅限於外部網路服務，目前已經開始轉變為內部網路，如：辦公室，數據中心……，目標是在任何地方都佈建IPv6，但因更重要的是，要如何刪除IPv4，爰渠提出目前該公司面臨的挑戰，及應對之解決方案如下：

- 儘早知道所有的知識。
- 立即與電信商合作。
- 不要忘記自己還有 IPv6。
- 聘請頂級管理人員。
- 需要軟體工程師而不是網路工程師。
- 建立 AAAA 團隊。

2、網際網路時間同步化（What ‘s the time？）

本場次由APNIC 首席科學家Geoff Huston擔任講者，本議題主要表達每臺電腦都內建有某種內部振盪器（稱為'時鐘'），當時鐘'滴答'後會被送到該電腦內建的數字計數器，以維持當前時間，而須維持正確的時鐘有下列挑戰：

- 電腦的時鐘係基於內部石英晶體振盪 - 只有在溫度和激勵電壓保持穩定的情況下，石英晶體振盪才會穩定。
- 電腦的時鐘計時器需依賴於計數器中的計數滴答 - 如果處理器在更高的中斷級別延長運行的時間，則時鐘滴答可能會延遲。

為確保時鐘之準確性，渠快速說明時間和網路時間協議（NTP），該協議原理透過網路讀取 NTP 時間伺服器之標準時間後，於電腦螢幕上顯示標準時間，並可立即更新系統時鐘，以執行時間同步之功能。通常NTP

可以在伺服器之標準時間的百分之幾秒內維護客戶端時鐘。接續講者快速簡介測量整個網際網路時間準確性之練習。

二、第二日會議摘要

（一）APNIC 國家互聯網註冊管理機構論壇（APNIC NIR SIG）

NIR（National Internet Registries） 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。

本會議由CNNIC 營運經理 Zhen Yu擔任主席，首先歡迎大家參加會議，接著依序由我國（TWNIC）、中國大陸(CNNIC) 、越南（VNNIC）、印度（IRINN）、日本（JPNIC）、韓國（KRNIC）及印尼（IDNIC）等國家網際網路註冊機構報告更新其國內網際網路發展，主要包括其會員成長情形、IP / AS分配情形、相關培訓計畫及其IPv6推動情形，以及其對於會員之相關培訓情形及最新規畫。摘述如下：

1、我國（TWNIC）

我國TWNIC係由王彥傑工程師代表發表，渠說明TWNIC目前IP會員有246家，經統計2018年IPv4位置分配快速成長至132,190 /24s，IPv6位置分配到達2,455 /32s，而TWNIC大多數的會員都已獲得都獲得IPv6地址，在2018年TWNIC已啟用RPKI服務，並舉辦2次教育訓練，目前IPv6用戶已由2017年底為0.46%，上升至31.89%，世界排名第9（在2019年2月13日的統計），未來亦將持續辦理IPv6等訓練，及邀請與會者參加下午場次的IPv6會議；APNIC之與會人亦在會中讚揚我國能推出RPKI服務，為網際網路安全共同做出努力。

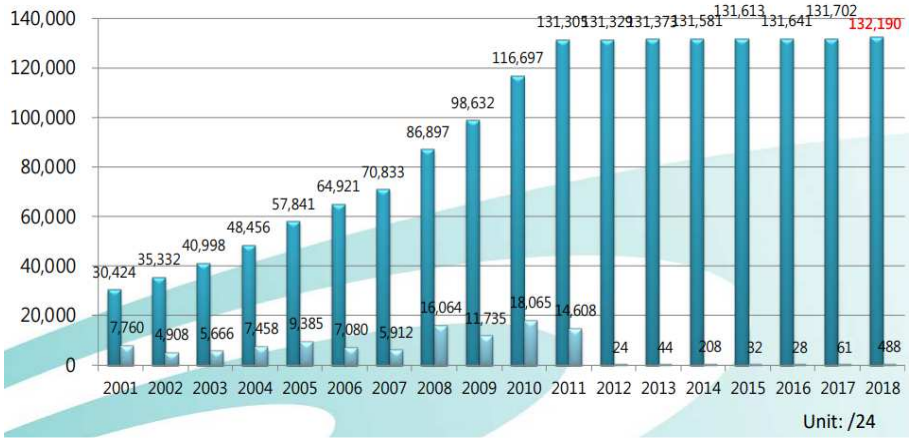


圖10 2018年我國IPv4位置分配情形 [資料來源：講者簡報]

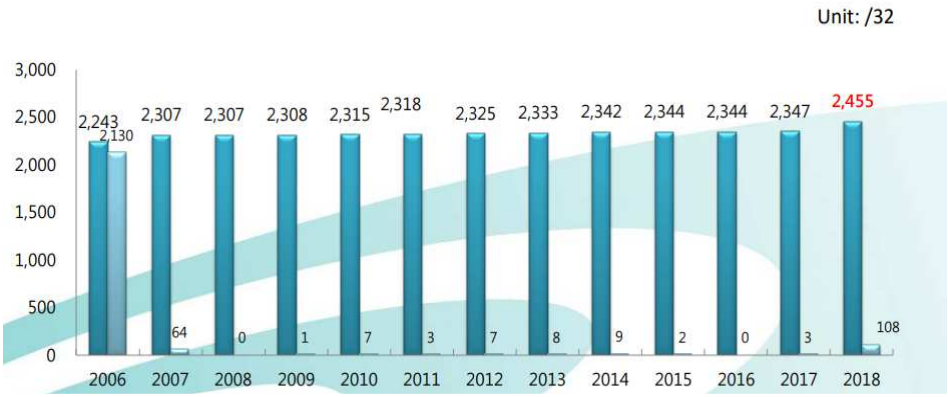


圖11 2018年我國IPv6位置分配情形　[資料來源：講者簡報]

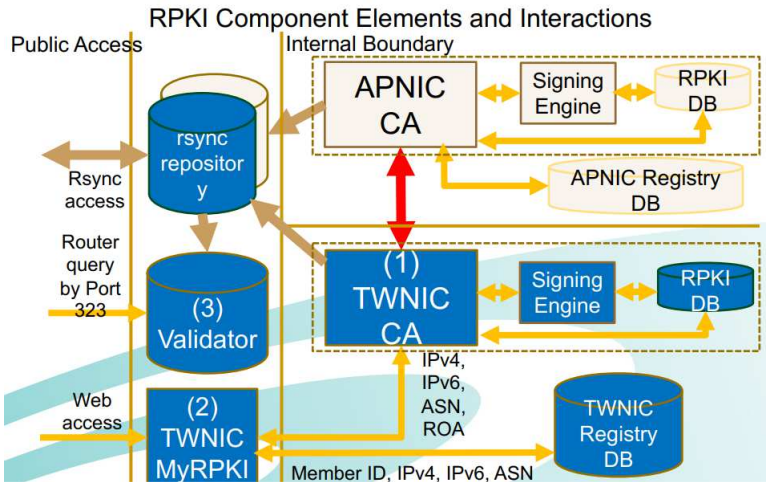


圖12 TWNIC之RPKI服務架構　[資料來源：講者簡報]

2、 中國大陸(CNNIC)

中國大陸 CNNIC 係由 Yuedong Zhang 代表發表，渠說明中國大陸網路用戶為 80,200 萬、滲透率為 57.7%，而行動網路用戶 7.88 億，佔網路用戶總數的 98.3%，經統計至 2018 年 12 月，CNNIC IP 會員有 1,395 家、IPv4 位置分配為 331,090 /24s，IPv6 位置分配為 16,048 /32s，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。

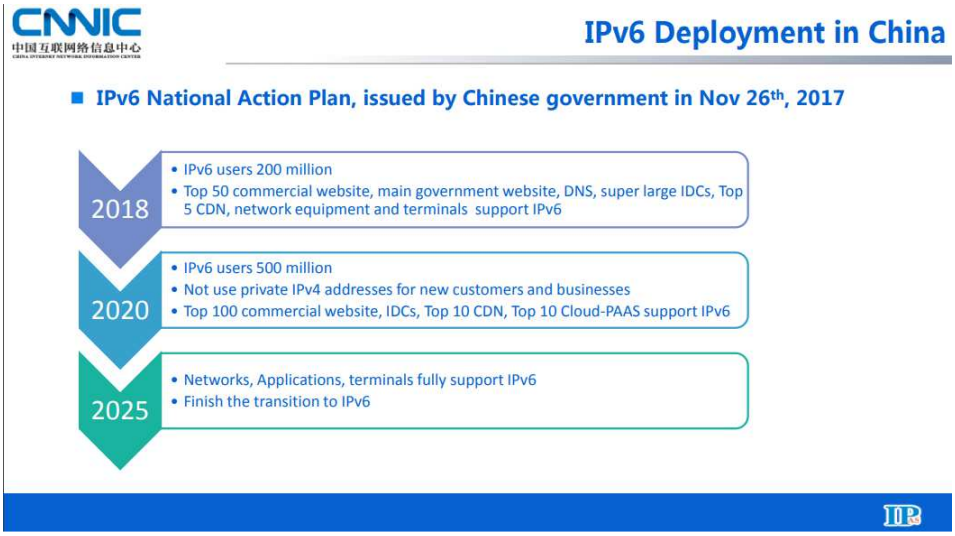


圖 13 中國大陸部署 IPv6 的國家行動計畫 [資料來源：講者簡報]

3、越南（VNNIC）

越南 VNNIC 係由 Oanh Nguyen 簡報，渠強調與 APNIC、JPNIC、KISA 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。經統計至 2019 年 2 月 20 日，VNNIC IP 會員有 382 家、ASN 核配成長至 306 家。目前使用 IPv6 用戶占 33.74%，在東南亞國家排名第二，在 APNIC 地區排名第 3，在世界排名第 8。

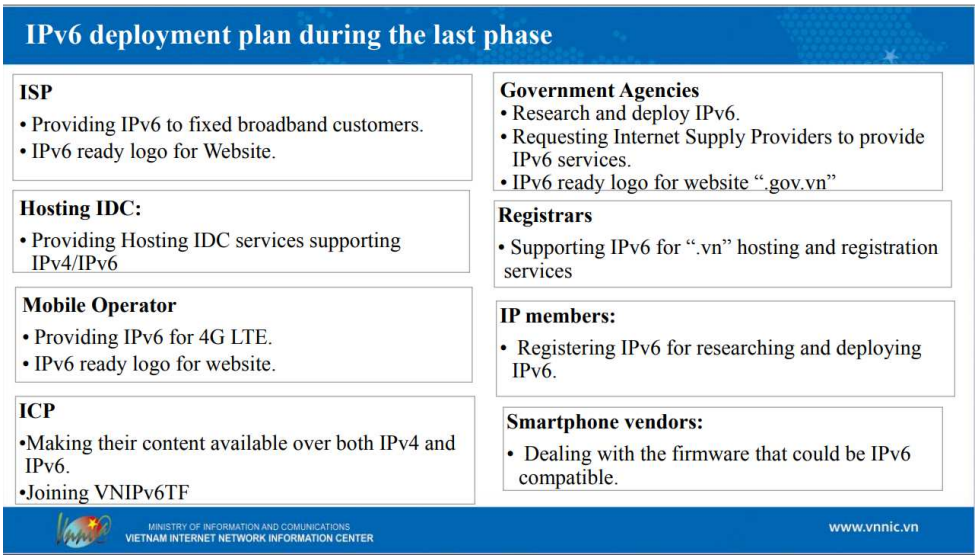


圖 14 越南下一階段部署 IPv6 計畫 [資料來源：講者簡報]

4、印度（IRINN）

印度 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，目前 IPv4 位置分配 10,839,040、IPv6 位置分配 5.3 億/ 56、ASN 核配 1713，在 IRINN 會員中，2189 家會員僅採取 IPv4、IPv4 與 IPv6 共存有 481 家、採取 IPv6 僅 2 家。

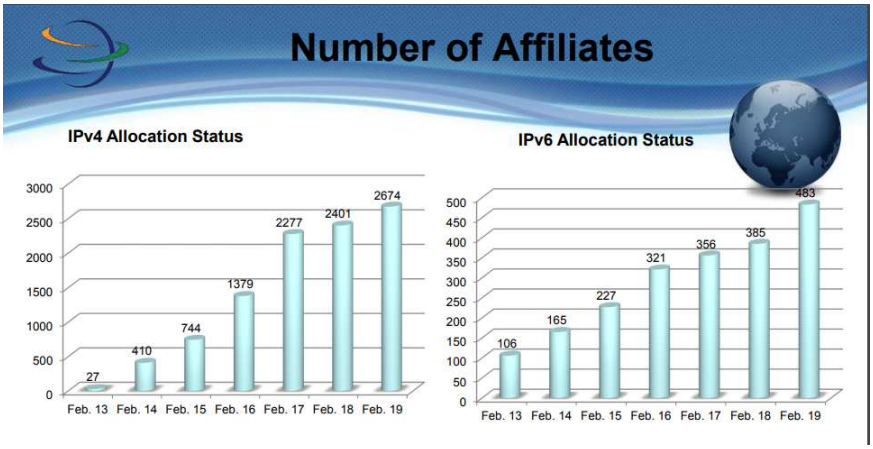


圖 15 IRINN IP 位址配置情形　[資料來源：講者簡報]

5、日本（JPNIC）

日本 JPNIC 係由 Hiroki Kawabata 簡報，講者說明基於「IPv4 耗竭專案小組」提供許多知識予技術營運者，JPNIC 於 2018/9/16 至 2019/2/15 間針對非技術人員（例如行銷及客戶支援部門）研討會、RPKI 研習、Open Policy Meeting 等活動計 7 場技術研習營，讓學員進行實作。截至目前為止，JPNIC IP 會員有 439 家、發布 69 個資源認證證書和 257 個 ROA，而使用 IPv6 用戶占 38.1%、使用 IPv4 用戶占 3.7%，已有 63%的 IP 成員收到 IPv6 分配及有 351 件 IPv4 轉換案例及 7 件 ASN 轉換案例，IPv4 剩餘空間為 25%。

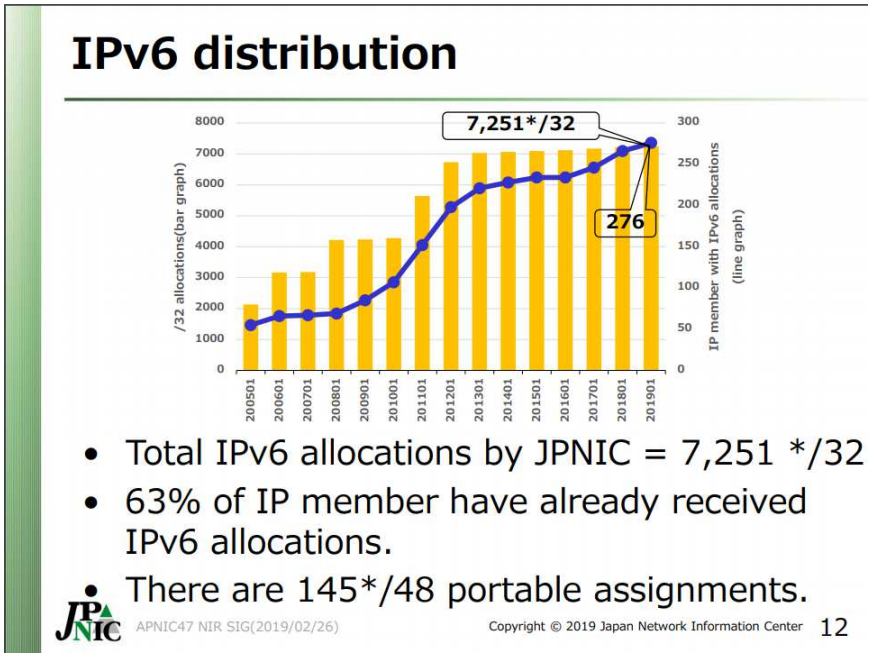


圖 16 JPNIC IPv6 分配之情形　[資料來源：講者簡報]

6、韓國（KRNIC）

韓國 KRNIC 代表簡報指出，目前 KRNIC IP 會員有 271 家、ASN 會員有 680 家，至 2018 年 KRNIC 已分配 IPv4 位置 112,397,056 個、IPv6 位置分配到達 5,253 /32s、

ASN 核配 1,005，過去及未來將對持續辦理 WHOIS 資訊更新、準備 RDPA 佈建、網際網路位址管理系統之轉換作業、公、私部門參予 IPv6 佈建計畫等事宜。

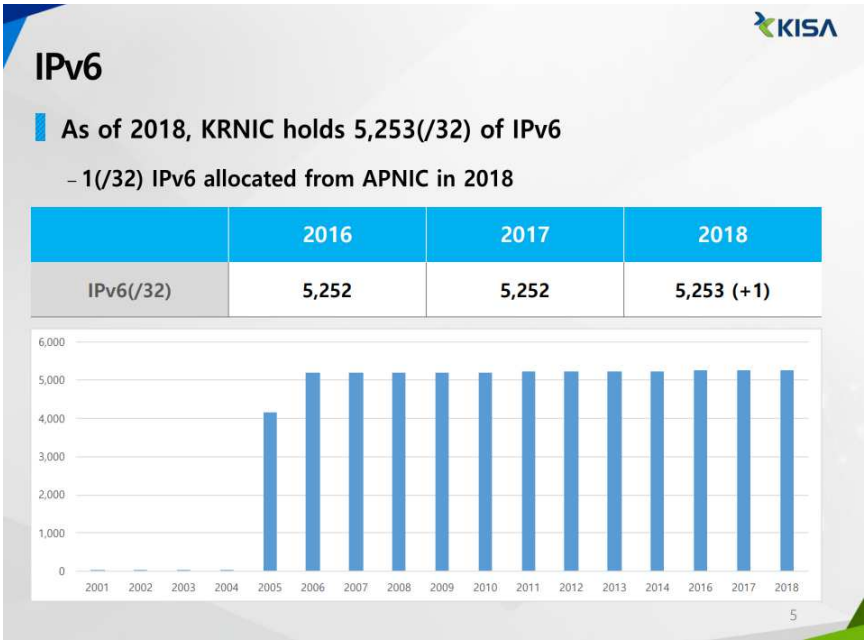


圖 17 KRNIC IPv6 分配之情形　[資料來源：講者簡報]

7、印尼（IDNIC）

IDNIC 代表說明該國網際網路進展狀況，經統計至 2019 年 2 月 IDNIC IP 會員有 1,590 家，其中大部分係企業或協會比率約占 52%，近期辦理過 2 場研討會，講者並指出該國有 Open-IX(Open-Internet Exchange Point)及 IIX(Indonesia Internet Exchange) 2 個訊務交換中心。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。

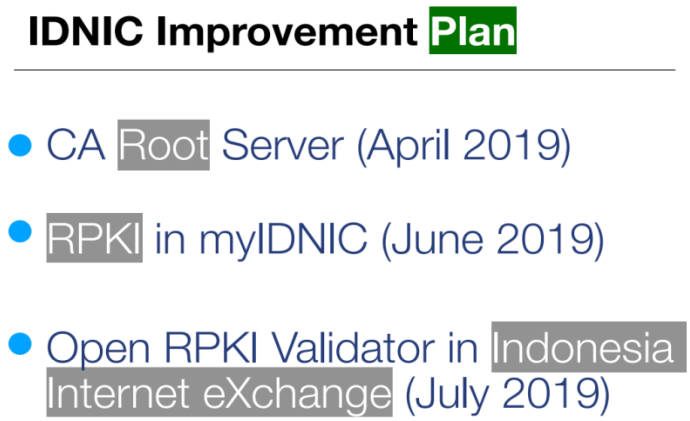


圖 18 IDNIC 未來計畫　[資料來源：講者簡報]

（二）DNS 運作（DNS Operations）

本場次會議由 DZCRD Networks Ltd 技術主管 Muhammad Moinur Rahman 擔任主席，首先渠說明描 DNS 根域名伺服器（英語：root name server）之的歷史和目前發展，並說明該系統在 1997 年（現在差不多 22 年前）停止演變之方式和原因後，渠討論了讓 DNS 根域名伺服器逐步發展之重大努力，包含一個新的根服務管理模式，接下來，渠討論了根域名伺服器潛在的威脅，概述了技術、經濟和政治挑戰，並在過程中介紹 ICANN 提出根服務的新態樣：hyperlocal，為這些威脅提供了緩解選項。

另 APNIC 首席科學家 Geoff Huston 說明目前大多數的在線資料經過整理、分析與貨幣化， DNS 結構是開放和混雜的，在這個時代似乎非常異常，但對 DNS 描述正在發生改變，並刻正採取相關措施來改進名稱解析的隱私保護，渠說明目前為改善 DNS 隱私所做的努力。最後，由 ICANN 高級工程師 Edward Lewis 結尾，分享隨著 DNS 資料的安全認證機制 DNSSEC 更換 Root Zone 的非對稱金鑰 (Key Signing Key，KSK) 即將結束，快速回顧到目前為止，所發現的經驗教訓。

（三）網路互連 I：區域化（Peering and Interconnection I：Regional）

本場次會議由 Equinix 公司的 Raphael Ho 擔任主席，並介紹 Asia Peering Forum 等 peering 社群活動規畫後，即進行 4 位專家依序進行相關專題簡報，最後並提供與會者上臺進行宣傳活動，摘述如下：

1、在印度營運 IX 的挑戰（Challenges in Operating IX in India）

講者是來自印度 Extreme 集團的 Raunak Maheshwari，他開宗明義的說，IX 終其一生都得面臨挑戰，包括 ASN 資源不足、BGP 知識不足（例如於 IX 介接業者竟不知要將其 Prefix 提供給互連業者）、基礎網路不足、對 IX 中立性不信任；但其亦強調，Extreme IX 雖面臨無窮盡的挑戰，但仍持續成長中。

2、AS15169 外部路由過濾（AS15169 changes to route filtering）

講者是來自 Google 的互連經理 Seiichi Kawamura 表示 ，包括路由劫持(hijack)、錯誤組態等造成的資安問題日益嚴重，Google 將自 2019 年開始對進入 peering 網路採取嚴格的 BGP announcements 過濾措施，並請與其 peering 業者應配合其規劃。

3、IXP introduction（IXP 介紹）

講者是 APIX 主席 Katsuyasu Toyama，其簡報是著重在介紹 APIX 成員資料包括 IX 名稱、公司所在地、介接點所在、ASN 數、尖峰訊務量、有無路由服務 、最新營運資料更新 、窗口資料等，我國中華電信的 TWIX 及是方電訊的 TPIX 均為其會員，亦在簡報資料中。

4、無法預測的訊務暴增-以 NPIX 為例（Unpredictable Traffic Bursts at npIX）

講者是來自尼泊爾 NPIX 的 Rupesh Shrestha，其簡報介紹 NPIX 有 2 個 sites，目前平時最大訊務為 5GBites/sec，但在 2018 年 6 月份時則僅為 3G。該中心曾預期世界盃足球賽期間可達 2 倍訊務量。2018 年 6 月 14 日開幕日交換訊務就達到預期的 6G，該中心很高興達到預測，但隨著賽事激烈化，6 月 22 日即達到超乎預測的 15G，因此

該中心趕緊協調採取包括負載分流等相關措施。講者表示，賽事期間，交換訊務隨著賽事上下巨幅震盪，最大交換量高達 32G，是平時訊務的 10 倍。他分享 NPIX 於世足賽之實際經驗，並提醒與會者，重大賽事可造成難以預估的訊務需求量，尤其 OTT 業者提供消費者更高的畫質時，將嚴重連鎖影響相關業者之電路寬頻及設備容量的需求。

5、網路互連人員活動（Operators introducing their network and peering policy）

此係提供各與會業者得藉此機會進行公司行銷，共有 6 家公司上臺行銷，包括我國是方電訊，由其魯堯經理上臺介紹該公司。

（四）技術研析會議（Technology）

本場次由 JPIX Masataka Mawatari 擔任主席，並分別由 IPv6 公司 Jordi Palet 說明「政府和企業網路在網路中部署 IPv6 所需的 12 個步驟」、NSRC 公司 Jonathan Brewer 介紹「用於物聯網的低功率廣域網路-LoRaWAN」及 APNIC 高級網路分析師 Warren Finch 以「QR 碼的生命-要掃描還是不掃描」為議題進行分享，摘述如下：

1、政府和企業網路在網路中部署 IPv6 所需的 12 個步驟 （12 steps for IPv6 deployment in governments and enterprises）

IPv6 公司 Jordi Palet 說明，政府和企業網路需考慮的主要典型問題，目前 IPv6 與 IPv4 過渡及共存方式有三種，Dual Stack、Tunnels 及 Translation，並描述政府和企業網路在網路中部署 IPv6 所需的 12 個步驟，如下：

- 取得訓練(Get Training)
- 建立部署策略(Create a Deployment Strategy)
- 取得 DNS 控制(Get Control of the DNS)
- 考慮使用 BGP(Consider Using BGP)
- 制定尋址計劃(Develop an Addressing Plan)
- 獲取自己的網路資源(Obtain your own Internet Resources)
- 使用 IP 位址管理(Use an IPAM)
- 分配和審查地址(Assign and Audit Addresses)
- 確認 IPv6 支援(Verify IPv6 Support)
- 測試 Apps/Services 的影響(Test Impact on Apps/Services)
- 建立長期網路(Create a Long-Term Network)
- 由第 3 方(業務合作夥伴、客戶或提供者)確認合約(Check Contracts with 3rd parties)

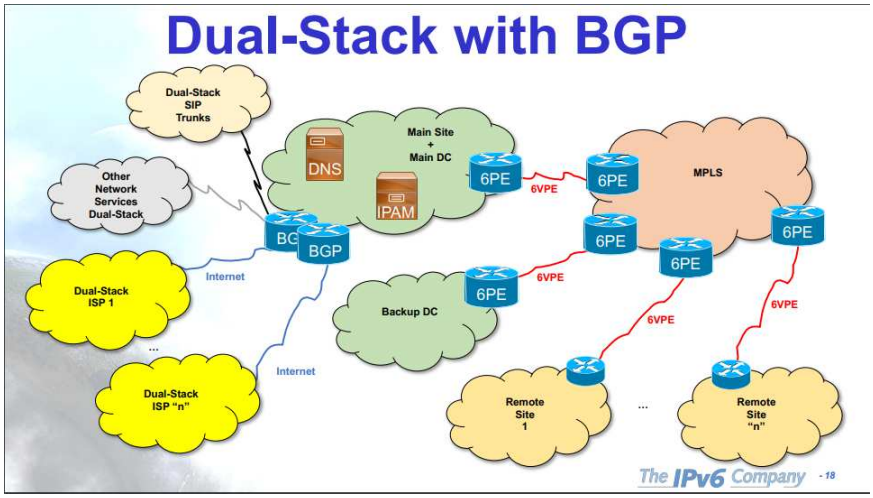


圖 19 BGP 使用雙堆疊之架構 [資料來源：講者簡報]

2、 用於物聯網的低功率廣域網路-LoRaWAN（LoRaWAN, a Low Power Wide Area Network for the Internet of Things）

NSRC 公司 Jonathan Brewer 針對網路運營商提供技術介紹一種用於物聯網的低功率廣域網路-LoRaWAN，並說明 LoRa 是低功率、廣域網路中少數新的物聯網無線電協議之一，其特性為屬於物聯網實體層、專為長距離、低功耗而設計、使用星形拓撲（非網狀或 p2p）及每秒傳送 1bit~kbit 及屬一套開放的協議，無特定標準，而 LoRaWAN 網路架構中包含了終端、基地臺、NS(網路伺服器)、應用伺服器等四個部分，其網路架構以星形拓撲為基礎，閘道器在終端裝置及後端的中央網路伺服器間。其以極快的速度進行傳輸，數據傳輸率介於 0.3 kbps 至 50 kbps，使用 LoRa 可建立具有多層加密和移動性的 IoT 網路。另渠說明 LoRaWAN 使用之頻率在歐洲是 433MHz 及 863-870MHz、中國 470-510MHz 及 779-787MHz、紐西蘭 865-867MHz、美國 902-928MHz。

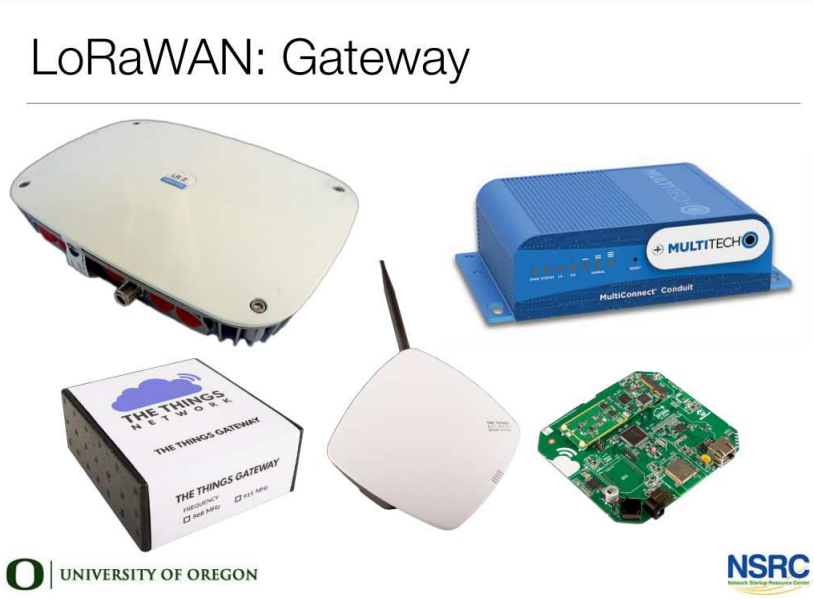


圖 20 市面上使用 LoRaWAN 技術之閘道器(Gateway) [資料來源：講者簡報]

圖 21 市面上使用 LoRaWAN 之產品 [資料來源：講者簡報]

3、 QR Codes 的生命-要掃描還是不掃描？(Life of a QR code. To scan or not to scan, that is the question?)

APNIC 高級網路分析師 Warren Finch 說明 QR Codes 是一個快速反應代碼的縮寫，QR Codes 的使用及可以惡意使用的地方，包括對 Kali Linux 和 Social Engineering Toolkit 發送網路釣魚電子郵件，並通過它們的審核，然後利用 QRLJacking 工具包，劫持 whatsApp 登錄。最後，渠說明 MalQR 是惡意 QR 碼和條形碼的集合，可用於測試掃描儀和應用程式的安全性，而防止惡意的 QR Codes 之方法如下：使用前觀察、繼續之前查看 URL、要懷疑、切勿提供個人訊息或登錄訊息及使用具有安全功能的 QR Codes 掃描器等。

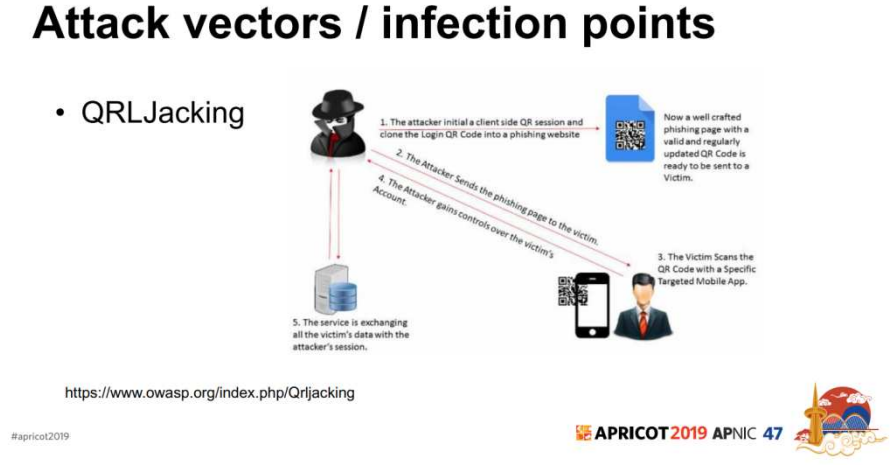


圖 22 QRLJacking 工具包攻擊流程 [資料來源：講者簡報]

（五）APNIC：合作遏制安全威脅（APNIC: Cooperating To Contain Security Threats）

本場次由 KISA 公司 Jeeyoung Hong、APNIC 首席科學家 Geoff Huston、Spark 集團 Ben McDowall 及 APNIC 安全專員 Adli Wahid 主講，主要說明最近的 APNIC 調查中，網路安全再次成為網路運營商面臨的頭號問題，包含：惡意軟件，DDoS 攻擊和路由安全，渠等說明因應目前威脅趨勢所面臨強大安全性和專業安全人員之需求，及網路運營商刻正執行保護網路和路由之方式，與 APNIC 為了控制網路運營商、政府機構和技術組織所面臨之安全威脅，採取之措施，並期未來透過合作來保護網際網路基礎設施。

（六）工具（Tools）

本場次由 Arista Network Japan 公司 Shishio Tsuchiya 擔任主席，並介紹「BGP 掃描程序 - Isolario BGP-MRT 數據讀取器：C 函式庫及工具」，接續分別由 Alpha Cogs 公司 Lorenzo Cogotti 簡介「叢集-利用 heavy-hitter 檢測分析流量」、威靈頓維多利亞大學 Winston Seah 教授簡報「利用 ELK Stack 進行 NetFlow 數據分析」，摘述如下：

1、BGP 掃描程序 - Isolario BGP-MRT 數據讀取器：C 函式庫及工具（BGP Scanner - Isolario BGP-MRT Data Reader: C library & tool）

Arista Network Japan 公司 Shishio Tsuchiyat 說明，自 20 世紀 90 年代末以來，RIPE NCC RIS 和 Route Views 等項目正在收集邊界閘道通訊協定 (Border Gateway Protocol，BGP)數據以監控網際網路之網域間的發展，在過去幾年中，收集的數據量急遽增加，主要是由於引入了新的路由收集器（例如，PCH、Isolario）、新的 BGP 饋線，新的 BGP 擴充功能（例如多重協定 RFC4760，ADDPATH RFC7911），當然，由於網際網路的自然增長，大多數 MRT-BGP 數據讀取器是在可用數據量較小時設計的，因此無法有效地使用當前數據集。此外，其中一些不支援即時引入大多數的 BGP 擴充功能，通常是因為它們沒有得到適當的維護和更新。爰渠向 APRICOT 提出了一個 BGP 掃描器，新的 MRT-BGP 數據讀取器和在 IIT-CNR 上實現的 C 函式庫，在 Isolario 項目中被有效使用，並說明 BGP 掃描程序在速度和消耗內存方面優於即時免費提供的所有 MRT-BGP 數據讀取器。

2、叢集-利用 heavy-hitter 檢測分析流量（Clustering-based Analysis for Heavy-Hitter Flow Detection）

Alpha Cogs 公司 Lorenzo Cogotti 說明，Heavy Hitter 是一種數量少但佔據絕大部分頻寬的流量，這種流量通常會造成網路壅塞，它的發生可能和攻擊行為有關。因此，對於適當的偵測 HH 和管理對於維持網路性能至關重要，且是嚴峻的網路挑戰。然而，HH 偵測已減少到使用臨界值，即如果流量超過先前設定的臨界值，則檢測器確定流量是 HH，目前臨界值尚無統一的定義，渠概述利用機器學習（ML）之工具，進行數據分析的方法，將流分類為流量叢集(Cluster)，其中每個叢集具有不同的流量特徵，相關屬性統計訊息為視覺化，有助於判斷叢集(Cluster)類型，並概述該方案可以在真實網路中實現。

3、利用 ELK Stack 進行 NetFlow 數據分析（NetFlow Data Analytic with ELK Stack）

本場次威靈頓維多利亞大學 Winston Seah 教授，利用 ELK Stack 進行 NetFlow 數據分析，NetFlow 是一種網路監測功能，可以收集進入及離開網路界面的 IP 封包的數量及資訊，應用於路由器及交換器等產品上，為網路管理員提供了一種讓管理員確定通過網路方向的方法。而 ELK 是由 Elasticsearch、Logstash 及 Kibana 三個系統所組成的 Log 蒐集、分析、查詢系統。在不變更原系統架構的情況下，架設 ELK 蒐集、分析、查詢 Log，可有效簡化過去繁鎖又沒效率的查 Log 工作。將 NetFlow 放入 ELK，可以通過可視化工具、成本計算和使用模式為工程師提供有關網路數據封包之原始目的地詳細訊息，亦可 即時處理與異常偵測網路大量攻擊。

三、第三日會議摘要

（一）事件驅動的網絡自動化和編排（Event-driven Network Automation and Orchestration）

本場次由 Cloudflare 網路工程師 Mircea Ulinic 主講，講者說明網路化的主要挑戰之一是不同的供應商利用不同之數據呈現，原因包括：供應商應用程式介面（Application Programming Interface，API）不一致且不完整、某些主流平臺已關閉、客戶的裝置不允許使用定製軟體，且要自動化，必須學習 Python 或其他編程語言非常困難，爰講者介紹一種用於網路之工具「Salt」，該工具具有可擴展、易於配置、網路自動化等特性，並可透過 Salt Proxy Minios 與第三方函式庫組合，如 NAPALM 等。講者說明 NAPALM 是一種供應商中立的跨平臺開源項目，能夠在網路中開發與維運之方法，其除為網路設備提供統一的 API，並可呈現與供應商無關的資料數據。NAPALM 目前官方已支援整合至 Salt 版本，除了提供跨供應商之配置管理外，對內部和外部網路事件的反應亦變得簡單容易，且無編排之限制。

在本會議中，渠介紹如何利用 Salt 實現事件驅動的自動化，利用該軟體，可呈現網路狀態的變化、配置之更改，對警報或不同類型的通知（電子郵件，SMS， Webhooks 等）做出反應。另雖然 Salt 足夠靈活，可以擴展任何業務邏輯並從任何資源中提取事件，但在本次演講中，渠主要專注於利用從第三方開放程式 daemon 、napalm-logs，從中獲取網路設備收到系統之日誌訊息。

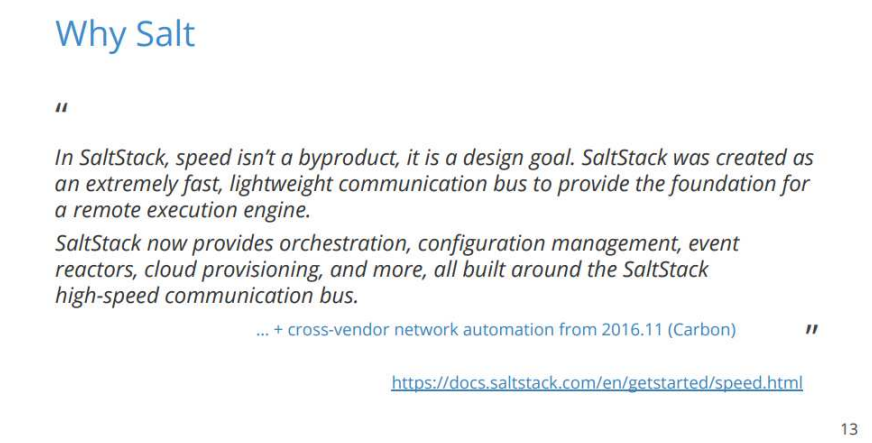


圖 23「Salt」工具之優點 [資料來源：講者簡報]

（二）APNIC 政策討論論壇 1（APNIC Policy SIG 1）

本場次首先進行主席選舉，因僅有既有主席 Sumon 獲提名，故由其連任之；本會議我國 TWNIC 顧組長靜恆為副主席。

接續由 Fiber@Home 策略長 Sumon Ahmed Sabir 擔任主席，並介紹 APNIC 任何政策的形成程序，包括須經過提案提交(包括遠端)，並由關注者（包括會員及非會員）以郵件群組或 YouTube 或 confer.apnic.net 等多元工具討論、政策 SIG 的共識、會員協商一致、評論期、執行委員會認可、修正後評論期及實施等階段。其並說明該政策 SIG 如何做成共識決定，其中最重要的包括在郵件群組或公開政策會議中討論，並評估異議、解決爭議。主講人並列出本次會議，經過郵件群組討論，決定排入政策 SIG 而待確定共識的議題。

第 47 屆 APNIC「政策開放會議」有五項政策提案供大家討論，摘述如下：

1、 第 46 屆 APNIC 討論過的提案

- 提案-124-v005 - 明確 IPv6 位址二度指定的定義

明確在《APNIC 網際網路號資源政策》一文第 2.2.3 節中對 IPv6 指派時指定位址空間的定義。之前在草擬這項政策的時，指定/二度指定的概念並無考慮到熱點的 IP 位址使用、或「自帶設備」(BYOD)的客人或僱員的 IP 位址使用、以及諸多其他類似情況下的使用。本提案在這方面明確了這種情形，更好地定義了概念，尤其是通過對一項指定的定義時加入額外語言，對新的 IPv6 (RFC 8273) 使用做了特別的考慮。

- 提案-126-v003: - 政策制定程序**(PDP)**更新

建議更新 APNIC 政策制定程序第四節，本提案將有助擴大成員的參與，計劃是在通過共識決定時將會同時考慮來自名單上的發言。因此，共識的達成將由通訊名單和論壇討論的兩者平衡來決定，從而擴大成員的參與。提案同時建議廢除須要「政策特別興趣小組」(Policy SIG)和 APNIC 成員會議決定的'雙重'共識要求，如下：

- ✓ 修改共識定義，從「全面共識」改成「粗略共識」。
- ✓ 假如提案在開放政策會議(OPM)達成共識的話就轉發到 SIG 通訊名單上去。
- ✓ 施行在無提交新版的情況下舊版提案自動失效的做法。
- ✓ 推出一個「上訴」程序，即假如提案人認爲 SIG 主席違反了 PDP 原則時可向 APNIC 行政局「上訴」。

2、 新提案

- 提案-127 - 把 103/8 IPv4 位址池的最高指派額改成至/23

APNIC IPv4 位址塊以及 103/8 位址池目前的最高指派額是/22。本提案旨在把這個最高指派額降至/23。目的是把 IPv4 位址保留一些給新加入者，延長 103/8 位址空間的枯竭時間，鼓勵派用 IPv6。而指派最低額沒有變動，仍爲/24。

- 提案-128 - 自治系統編號(ASN)無需多宿主

在 ASN 指定政策最開始提出時，網路的可靠性是沒有目前這樣好的。在那時，ASN 持有者是多宿主的這個做法不無道理。隨著網路互通的最新發展，多宿主已經不

需要了。本提案是對未來的多宿主作修改，考慮到與其他自治系統互通的需要。

- 提案-129 - 廢除無法滿足 IPv4 請求的輪候名單

目前的 APNIC IPv4 政策允許每一位 APNIC 登記用戶在收到來自最後/8 位址池(103/8)的/22 數目之後可收到來自 IPv4 回籠位址的可至/22 的數目。然而，「回籠池」不總是有足夠的資源來進行指派，於是就建立了一份輪候名單。本提案建議廢除目前的輪候名單。逢 APNIC 從 IANA 或閉包或回交之類收到回籠的 IPv4 位址空間時，應該予以與最後/8 位址池(103/8)同樣的政策對待。提案並建議在 APNIC 最後/8 資源完結時就建立一份輪候名單，以/8 分配政策同樣對待這份新的輪候名單。

接續由多位講者針對上開議題進行簡報，APNIC 的 George Odagi 說明先前之提案-125 驗證"濫用郵箱"和其他 IRT 電子郵件之最新執行情形，並請 APNIC 會員知道註冊 MyAPNIC 的訪問權限、閱讀政策並了解即將發生的變化、確認 IRT 連絡人資料是最新且可聯絡到、定期監控網路濫發信件並適時採取行動。Jordi Palet 則說明，APNIC 會承認因內部 RIR 或 RIR 間因合併、收購或組織重整所造成 ASN 轉移。另 Geof Huston 則簡報其一份觀察資料，其指出 IPv4 已耗竭，但仍有大量已核配的 IP 卻未見於 BGP 通告中，其中大陸最多，則臺灣排名第 8，多位與會者對講者的統計提出疑問，包括中華電信董事吳國維提問，是否部分 IP 因被使用於私網故未 BGP 通告。講者同意「可能有已使用，但相關因素而未通告」之看法。隨後則由我國 TWNIC 王彥傑工程師上臺說明提案-127，簡要說明該政策內容。

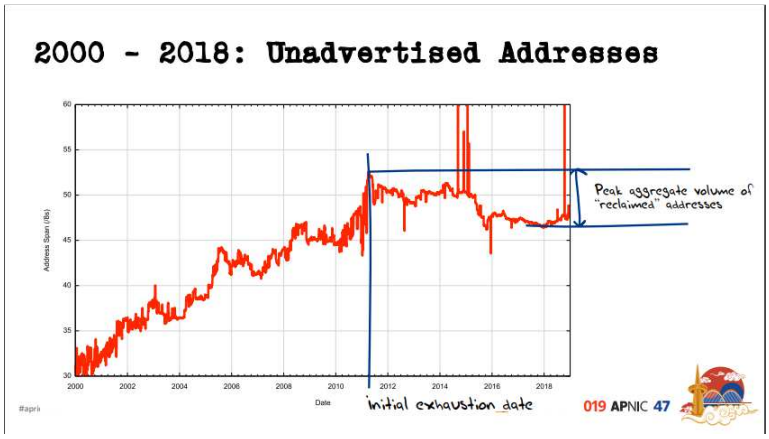


圖 24 2000 至 2018 未通告位址之統計 [資料來源：講者簡報]

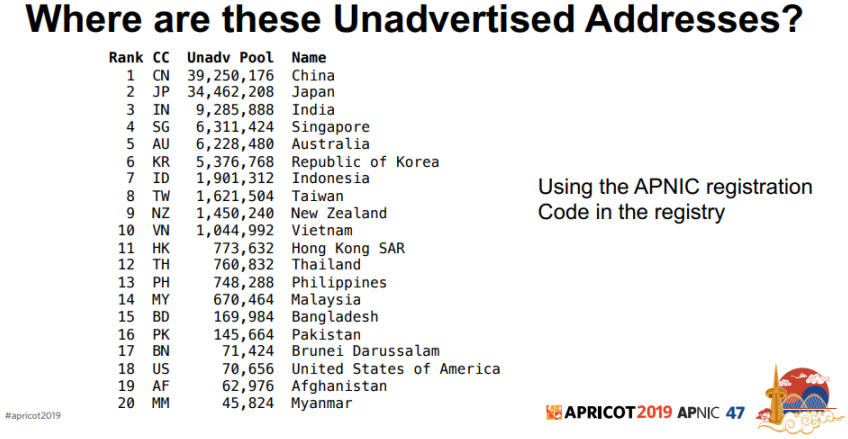


圖 25 已核配的 IP 卻未見於 BGP 通告中之經濟體排名 [資料來源：講者簡報]

（三）5G 技術-教學（5G technology: a tutorial）

本場次由 NOIKA IP 中心、E2E 平臺策略長 Paresh Khatri 擔任講者，渠說明 5G 的第一個商業版本將在 2019 年發生，一些亞太地區的運營商將領先，5G 帶來了對頻譜、無線接取架構、移動核心和各種用戶使用上巨大的變化。隨著技術的演進，5G 網路的平均下載速度最有可能達到 1Gbps，並可能達到 10Gbps，若以此無線傳輸速率傳輸影像，甚至已比目前的光纖還要快，爰在本演講中，渠說明更高效率的網路，需有下列特點：

- 支持更多用戶。
- 提供更高傳輸速率。
- 更一致的用戶體驗。
- 更高的連接密度。
- 更廣泛的網路覆蓋。
- 更有效的訊號。
- 延長設備電池壽命。
- 更多分佈式的用戶介面。

因此，5G 將改變行動網路的世界 - 結合低延遲、非常短的傳輸、高可用性、高可靠性和高安全性等優點，接續講者概述說明更有效率過渡 5G 之關鍵及為了連接不同行動網路元件需要之 IP /光纖網路所產生之影響。

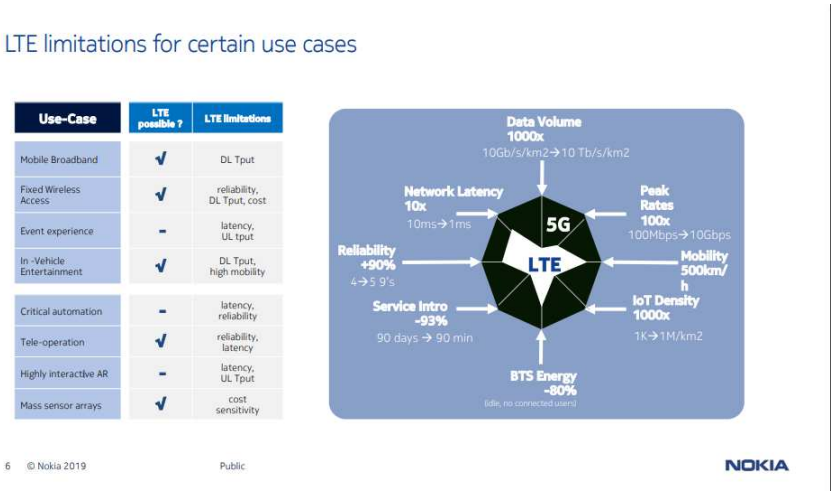


圖 26 5G 與 LTE 之特性比較 [資料來源：講者簡報]

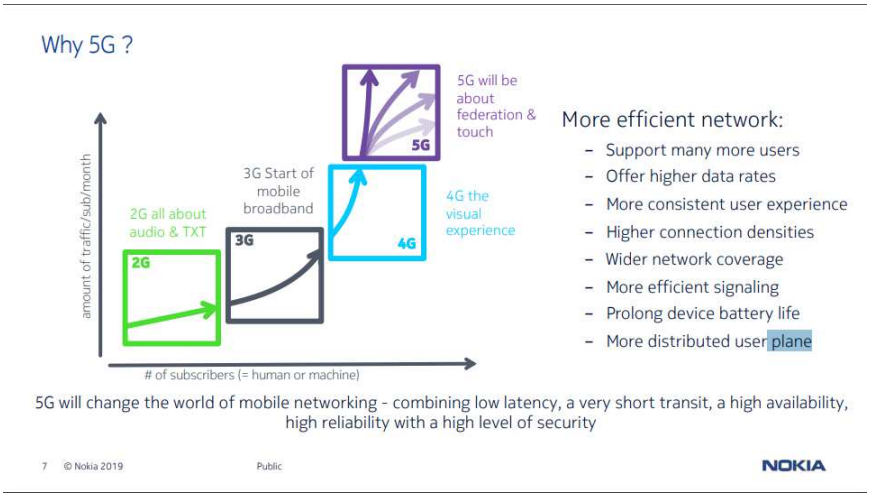


圖 27 各代行動通訊網路之比較 [資料來源：講者簡報]

（四）路由安全 2（Routing Security 2）

本場次由 APNIC 高級網路分析師 Tashi Phuntsho 擔任主席，並分別由 NLnet Labs 公司高級軟體開發師 Tim Bruijnzeels 說明「我應該進行自己的 RPKI 證書認證體系嗎」、INEX 公司 Barry O'Donovan 說明「具有 RPKI 和 IXP Manager 的 IXP 路由伺服器」及 ICANN 高級工程師 Edward Lewis 說明「使用 RIR WhoIs 的經驗」，摘述如下：

1、我應該進行自己的 RPKI 證書認證體系嗎？（Should I run my own RPKI Certificate Authority? ）

NLnet Labs 公司高級軟體開發師 Tim Bruijnzeels 說明，自 2011 年以來，五個區域網際網路註冊管理機構管理機構（RIR）一直在提供資源公鑰基礎建設（Resource Public Key Infrastructure，RPKI），RPKI 是一個基於公共密鑰基礎建設框架，用於保護網際網路路由基礎建設，特別是在邊界閘道器協定（Border Gateway Protocol，BGP）劫持的風險上，RPKI 是網路位址資源的加密認證技術，使用 RPKI 加密認證，管理者可以瞭解網路 IP 位址資源使用者是否為合法 IP 位址所有者，讓號碼資源的合法持有者能夠掌握網際網路路由協定的運作，以防止路由劫持和其他攻擊。RPKI 允許單位發布路由來源授權（Route Origin Authorization，ROA）驗證，證明 IP 位址和自治系統（Autonomous System，AS）號碼在 BGP 路由表資訊中是對應的組合。

目前五大 RIR 中，有四大管理機構 RPKI 證書認證體系，僅 LACNIC 尚未提供，惟 LACNIC 致力於在 2019 年底之前提供此功能，雖然前揭託管設置可以很好地服務許多小型 ISP 業者，但營運商可能有很好的理由來運行自己的基礎架構：

- 需要更簡單的 RPKI 管理的運營商，以更簡化的方式整合他們自己的系統。
- 具有安全意識的運營商，要求他們只擁有他們自己使用的系統私鑰。
- 希望在運營上獨立於 parentRIR 的運營商，例如國家網際網路註冊機構（NIR）或企業。
- 全球網路的運營商，其可能希望只運行單個系統，而不是在多達五個 Web 界面中維護 ROA。

最後，講者提供可能的緩解策略，並使感興趣的用戶了解哪種選擇最適合他們。

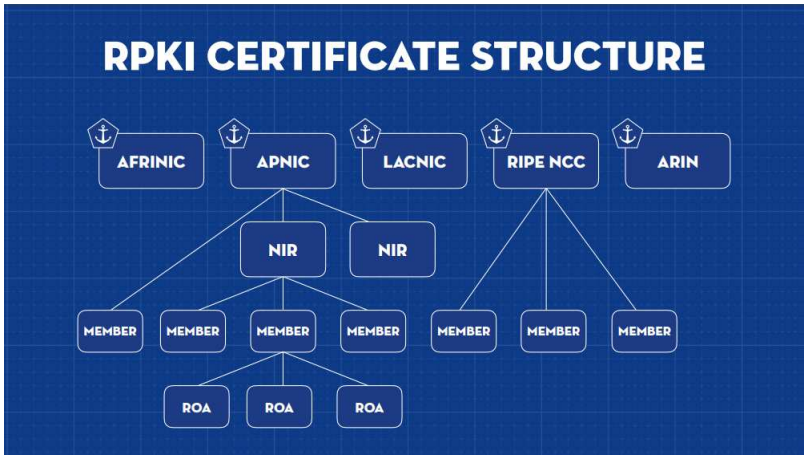


圖 28 RPKI 證書認證體系 [資料來源：講者簡報]

2、具有 RPKI 和 IXP Manager 的 IXP 路由伺服器（IXP Route Servers with RPKI and IXP Manager? ）

INEX 公司 Barry O'Donovan 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網際網路交換中心（Internet eXchange Point，IXP）社群並作出貢獻，並支援全球各地開發新的 IXP。IXP 通常會提供兩種連結的選擇，分別為公用互連(Public Peering)與專用互連(Private Peering)，現實上，大多數 IXP 上的路由伺服器存在 IRRDB 物件資料品質老舊、常發生遺失問題及重複過時、錯誤訊息等問題，由於物件集解耦 (decoupled)與 RIR 資源指配分離，資源擁有者通常難以糾正該訊息，目前雖可透過一種基於公共密鑰基礎建設框架 RPKI，取代 IRR 的方式保護網際網路的路由基礎設施，惟仍存在一些問題，如：無法實現對 AS-SET 等功能的支援。爰講者介紹一「IXP Manager」，以解決類此問題。

圖 29 IXP Manager 簡介 [資料來源：講者簡報]

3、使用 RIR WhoIs 的經驗（Experience using RIR WhoIs）

ICANN 高級工程師 Edward Lewis 說明，WHOIS 是一種查詢網域名稱或 IP 位址的方法，當通知網路運營商即將發生的變化時，可能會影響許多人，此時，可至 RIR 註冊數據庫會查詢，以獲取相關資訊。最後講者簡要分析目前 RIR“WhoIs”常見問題如下：

- 需要許多領域特定的知識-必須知道 RIR 是誰和 NIR 結構。
- 缺乏常見的查詢 - 語言或服務點。
- 缺乏通用的反應格式。
- 缺少特定的聯繫字段-使用備註或註釋字段提供資訊。
- 使用“虛擬值”表示誰是“推薦”。
- 資料探勘的防護（速率限制）。

（五）APNIC 政策討論論壇 3（APNIC Policy SIG 3）

本場次延續 **APNIC Policy SIG 1 議題**，進行「提案-127 」、「提案-128 」「提案-129」等 3 提案之詳細說明、討論及投票。

首先由 TWNIC 王彥傑工程師就所提案「提案-127」案進行簡報說明提案目的、優缺點及衝擊，本提案旨在考量 IPv4 即將耗竭，故建議 103/8 池的最高核配大小由/22 調整延長/23，以利更多新進業者有機會取得，並鼓勵核派 IPv6。本案雖有與會者表達不同意見（例如中華電信董事吳國維發話提醒此新作法或有 IPv6 部署意願之負面影響，另部分與會者建議調為/24 更具效益），但多數發言是支持此提案的（例如 TWNIC 黃執行長及丁副執行長表示此案已有時效急迫性，此案可降低新進者進入門檻及提供其機會。本案最後經主席進行現場與會者之投票並檢視 Confer 網站及 email list 統計結果，宣布此案獲致「共識」（我國與會人員均到場投票支持本提案）。另「提案-128 (ASN 無需多宿主)」、「提案-129（廢除無法滿足 IPv4 請求的輪候名單）」此 2 政策提案亦接續由提案者簡報並進行與會者之提問、回應及討論，此 2 案亦獲得「共識」。

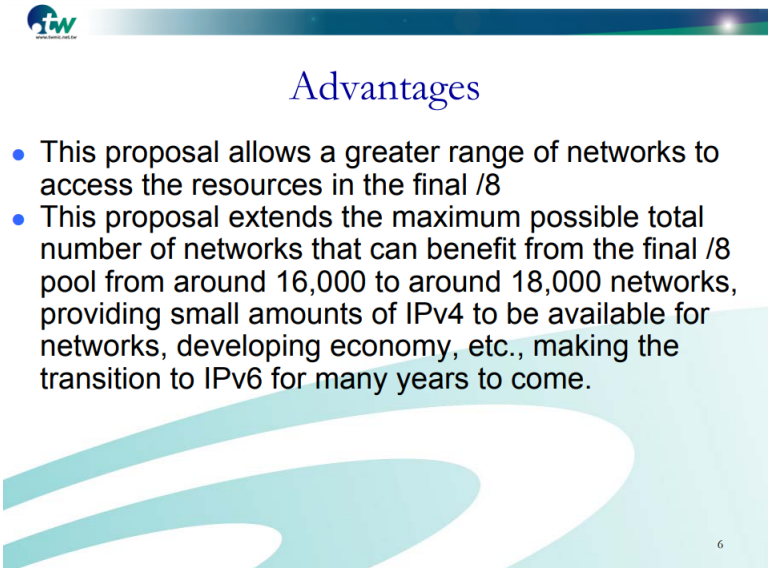


圖 30 我國 TWNIC 說明「提案-127 」之優點 [資料來源：講者簡報]

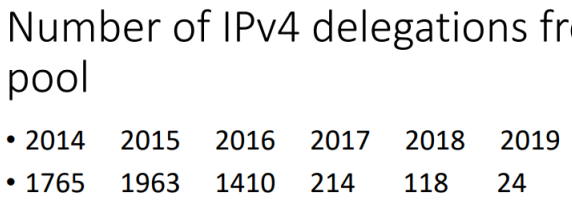


圖 31「提案-129」近年 IPv4 回籠池核配數量統計 [資料來源：講者簡報]

（六）資訊中心（Data Centre）

本場次由韓國政府科技部與韓國電子通訊研究所(Korea Institute of Science and Technology Information，KISI) Buseung Cho 教授擔任主席，並分別由 KISI Dongkyun Kim 簡介以基於 ONOS 位址及透過 KREONET-S 加載感知虛擬專用容器網路、由 LINE 公司 Ikao Nakajima 簡介 LINE 公司使用 eBGP 實現 CLOS 自動化及由 Arista Network Japan 公司 Shishio Tsuchiya 簡介密集拓撲中的路由，摘述如下：

1、 基於 ONOS 位址及透過 KREONET-S 加載於感知虛擬專用容器網路（ONOS-based Location and Load aware Virtually Dedicated Container Networking over KREONET-S）

KISI Dongkyun Kim 介紹 SDN / ONOS 的計算、儲存、網路編排架構及其基於位置和於系統上實現加載之感知虛擬專用容器(Container)網路，渠透過實施新的容器網路接口（VDN-CNI）使用 Kubernetes 和廣域虛擬網路資源收集容器化之服務資源，並運用 KREONET-S 上的虛擬專用網路（VDN）應用程序，使 KREONET-S 用戶能夠動態、快速地管理其嚴格的容器化計算、儲存資源及高速觸發高性能虛擬網路（VDN），渠說明 KREONET-S 主要是用於 ONOS 平臺上，以 SDN 控制並管理其他網路功能，同時採開放的技術，整合 OVS、OPNFV 等協定，並在 KREONET-S 上的分佈式 k8s 測試平臺展示及模擬實現系統編排組件和功能，其中包括幾個關鍵組件，如協調器、容器管理器（Kubernetes）、虛擬網路管理器（VDN 應用程序）、SDN 控制器（ONOS）及韓國部署八個網路交換中心的 OpenFlow 網路設備和服務資源，包括韓國（5）、美國（2）和中國（1）。在前揭架構中，協調器通過判斷從容器管理器和虛擬網路管理器獲取負載（例如，CPU，內存和儲存使用）和 VDN 狀態訊息，在接收到其服務請求之後，可聰明的確定用戶最近的服務位置。

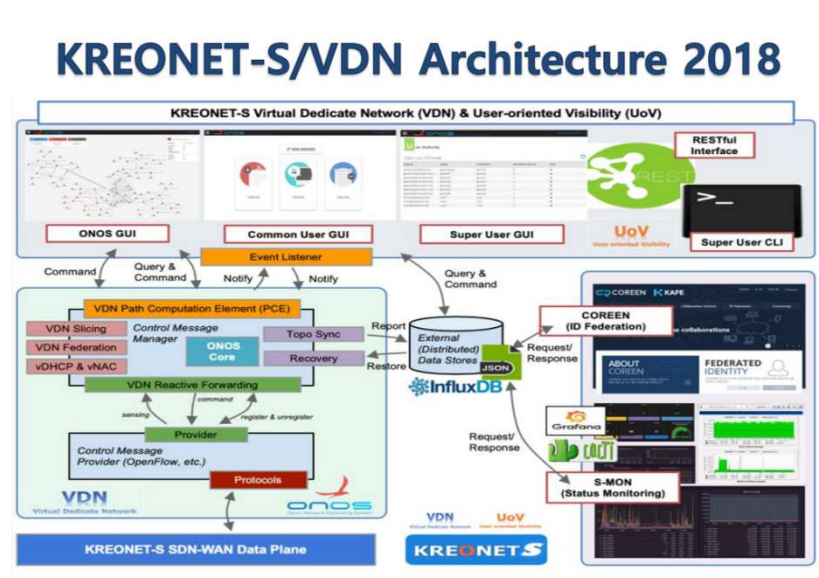


圖 32 KREONET-S/VDN 架構 [資料來源：講者簡報]

2、 LINE 公司使用 eBGP 實現 CLOS 自動化（Automation of CLOS with eBGP at LINE）

LINE 公司 Ikao Nakajima 首先說明，該公司業務以拓展至日本、臺灣、泰國及越南等國家，並致力挑戰高品質之網路，而非以多級方式超額使用傳統網路，爰渠介紹 LINE 公司如何利用自動化佈署資料中心 CLOS 網路架構之方法，依序為初始化設定、Cable 連線檢查及於資料中心作業系統「Cumulus」配置 BGP。最後，講者說明 LINE 公司未來工作如下：

- 將簡化暫存檔案變複雜，以處理某些功能像 MLAG 和 ACL。
- 建立友善的用戶 GUI，以編輯 DB 中的值。
- 加強監控工具-檢查 eBGP 對等、路由資訊和流量延遲的整體狀態。
- 在 Clos 網路上建構多租戶

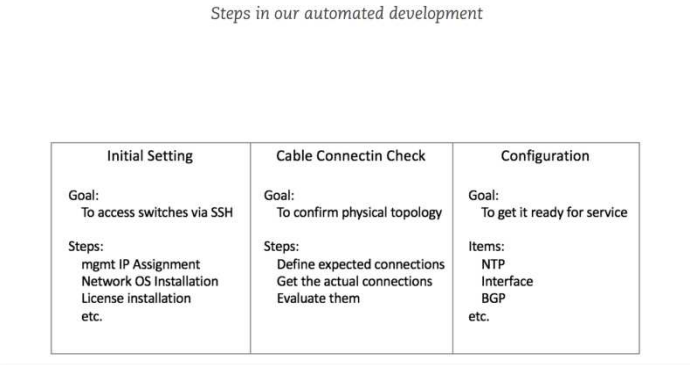


圖 33 LINE 公司自動化開發步驟 [資料來源：講者簡報]

3、 密集拓撲中的路由（Routing in Dense Topologies - What's all the Fuss? ）

Arista Network Japan 公司 Shishio Tsuchiya 說明，所有的路由器都是預先配置基

本介面與根據開放式最短路徑優先（Open Shortest Path First，OSPF）配置拓撲圖，而最近對數據中心路由的興趣大幅增加，引發了 IETF 和其他標準組織以及團體大幅討論，渠表示數據中心一直在利用 BGP 進行底層路由，主要是由於鏈路狀態 IGP 廣泛擴展的問題，為了更好地控制策略，爰渠概述各種方法及其目標，雖然仍存在部分缺點，但主要目的是告知與會人員，這個令人振奮的訊息。

（七）網路營運 1（Network Operations 1）

本場次由 Megaport 公司 Gavin Tweedie 擔任主席，並分別由 LinkedIn 公司 Arun Thiagarajan 介紹 LinkedIn 骨幹網路之流量工程、Facebook 公司互連經理 Matt Jansen 介紹網路災難之恢復及 Cloudflare 公司網路工程師 Mircea Ulinic 分享技術負債-Anycast 的故事，摘述如下：

1、LinkedIn 骨幹網路之流量工程（Traffic Engineering in LinkedIn Backbone）

LinkedIn 公司 Arun Thiagarajan 介紹如何在 LinkedIn 骨幹網路（Backbone）中完成流量工程，包括在一段時間內完成的學習和改進，並介紹該公司使用動態標籤路由器(LSP)，即藉由通過路由自動產生交換路徑，有以下優點：

- 提高頻寬使用率（Gbps）（少數鏈接超過 20%）。
- 節省 Opex - 縮減營運成本、減少手動更改及節省大量工時。
- 明顯降低 MTTR-減少服務影響之最大限度。
- 設置新的網路節點較為簡單等。

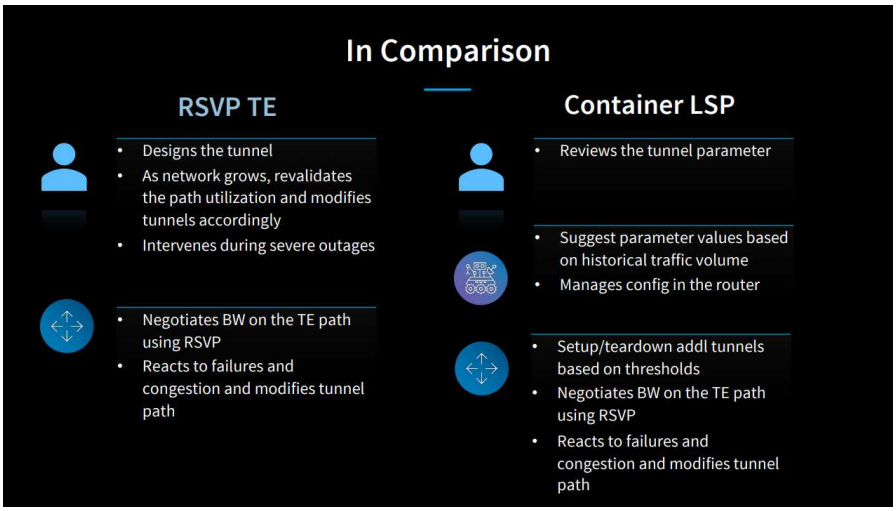


圖 34 RSVP TE 與動態標籤路由器(LSP)之比較 [資料來源：講者簡報]

2、網路災難之恢復（Network Disaster Recovery）

Facebook 公司 Matt Jansen 說明，過去幾年渠任職之公司一直致力於全球拓展之腳步，該公司利用建構 POPs 並部署快取（Caches）連接到世界各地的多個 ISP 業者，以便用戶可以安全的訪問內容並獲得最佳性能，而提供最佳性能的重要一部分是面對網路攻擊時，仍能繼續提供 Facebook 應用系列程式的運作，而對用戶無任何影響，渠說明 Facebook 隨時為網路周邊發生重大災難做準備，避免天災發生造成網路數據中心損壞，使民眾無法使用，進而影響公司營收，最後渠介紹「暫存」（caching）的

軟體技術，即係將常用的資訊存在網路各處，俾利用戶存取時，可於最近之周邊暫存器取用，大幅減少伺服器之負荷，並提升使用效率。

3、 技術負債-Anycast 的故事（Technical Debt: an Anycast Story）

Cloudflare 公司網路工程師 Mircea Ulinic 說明，Anycast 是一種網路定址和路由的方法，使資料可根據路由拓撲來決定送到最佳的目的地，渠說明渠任職之公司 Cloudflare 運轉一個大型的 Anycast 網路，並於全球範圍內部署了約 150 多個，這個網路越大，提供的效能與安全性就越好，而這種規模的部署也帶來了各自獨立的困難和挑戰，其中一個更大的挑戰是全球對 Anycast 路由的變化，發生輕微的錯誤或延遲可能會產生巨大的影響。過去，Cloudflare 的網路團隊決定在我們的路由伺服器前置碼（Prefix）通知中加入 prepend，當時，這是一個合理的決定，實際上使 Anycast 網路按預期工作。這些 prepends 當時有用，但不再是必需的配置，因改變這一配置可能會導致大量問題，例如超載單個位置或超載單個傳輸管道等。 最後，講者介紹 Anycast 網路之特性如下：

- 客戶影響微不足道。
- 路由的波動在±2 分鐘。
- 可花 1 小時更改完成。
- 即時檢測並解決小問題。
- 嚴重依賴開放程式。

四、第四日會議摘要

（一）訪談南韓電信業者 SK

與南韓 SK broadband Young shin Kim 就網際網路訊務監理機制進行短暫會談，依其說明，南韓政府每 2 年會重新檢討 peering 上限費率，供業者進行費率協商。但渠認為 Internet 是雙邊市場模式，電信業者之兩端分別為內容業者及終端用戶，在已經無法從終端用戶端增加收入下，基於內容業者係利用電信業者之網路提供服務給在網路另一端的訂戶，此商業模式造成業者必須不斷擴充網路頻寬及更新高效能設備，所以政府應該開放讓業者間自行協商 peering 費用，才是有利於電信業者未來之發展，例如建設 5G 網路。

（二）APNIC 年度全體會議 1~3（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 ）執行理事選舉。首先由 APNIC EC 主席 Gaurab Raj Upadhaya 進行致詞，接著由 APNIC 法務長說明 APNIC EC 選舉流程，並由 6 位候選人(應選 4 位)各進行 2 分鐘的政見發表，隨後展開現場投票至 14:30 後，續由 APNIC 執行長 Paul Wilson 就 APNIC 2018 年之會員、對區域網際網路發展及全球社群合作所進行活動，以及所提供相關服務等年度績效報告。緊接由 APNIC 執行理事黃勝雄進行財務報告，總結與會者對 APNIC 2018 年財務之建議是希望非營利組織 APNIC 能充分善用預算，針對更多國家提供相關教育訓練等服務。

接續由 Policy SIG 主席報告本屆會議 5 個政策提案的討論結果(3 個達成共識，2 個未達成)，爰由 EC 主席向與會者說明 3 個共識提案後續發展程序，並再次向與會者

確認有無反對者，結果均無反對者。開放與會者發言時，針對是否增設 SIG 及提供更多元的討論工具進行熱烈討論，EC 表示將持續努力如何促進相關政策更多參與者及更有效的討論。

最後，APNIC AGM 會議辦理 APNIC 執行理事選舉，我國 TWNIC 執行長黃勝雄順利連任 APNIC 理事。

（三）IPv4aaS 教程和實踐（IPv4aaS tutorial and hands-on - Part 1）

本場次由 IPv6 公司 Jordi Palet 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，渠說明網路環境要從 IPv4 轉換到 IPv6，可能因為一些因素(如 IPv4 網路設備無法完全汰換掉)需要花費非常久的時間，並討論在 ISP /企業業者網路中使用 IPv4-as-a-service（IPv4aaS）技術過渡 IPv6 所需的方法有三種，如下：

- 堆疊（Dual Stack）：即網路裝置同時支援 IPv4 和 IPv6 協定。
- 穿隧（Tunnels）：將 IPv6 封包以 IPv4 的形式包裝，係目前最常採用的方法，目前有轉換技術如：6RD、DS-Lite、lw4o6 及 MAP-E 等。
- 轉換（Translation）：是讓只有 IPv4 的網路與只有 IPv6 的網路彼此能夠互相溝通，因 IPv4 與 IPv6 封包格式完全不同，所以不能互相連線，若以 NAT-PT(Network Address Translator - Protocol Translator)充當兩者間的翻譯後，就能夠讓 IPv4 與 IPv6 相互轉換格式，目前有數種轉換技術，如：MAP-T，464XLAT，NAT64。

最後，渠簡要說明 NAT64 與 DNS64 和 464XLAT 及 DNSSEC 之運作流程，並說明 464XLAT 係類似 NAT64，但主要差異在於手機上需要安裝 CLAT 服務，始能運作。

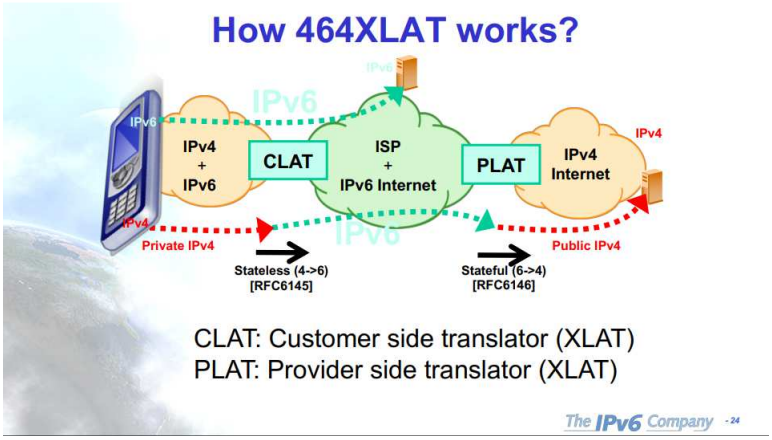


圖35 464XLAT運作方式 [資料來源：講者簡報]

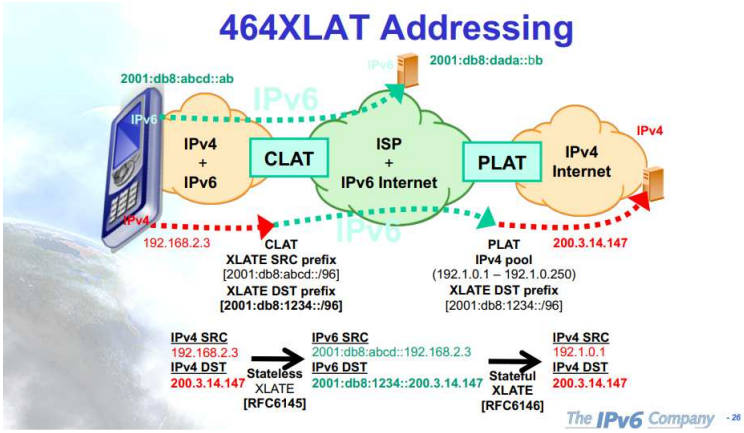


圖36 464XLAT定址方法 [資料來源：講者簡報]

（四）網路營運 2（Network Operations 2）

本場次由 LEARN 公司 Thilina Pathirana 擔任主席，並分別由 ADVA Optical Networking 公司 Rocky Zhou 介紹捷運網路轉型及 ISC 公司 BIND 及 DHCP 顧問 Eddy Winstead 分享 DNS Flag Day 後之影響。摘述如下：

1、捷運網路之轉型（Metro Network Transformation）

ADVA Optical Networking 公司 Rocky Zhou 說明，目前於地鐵建置網路有下列決條件，包含空間有限、較低成本、須簡化營運方式提升效率及須惟開放性的設計，以利未來升級，爰講者說明新的光學技術正推動捷運網路之轉型，開放式系統可實現最佳的設備部署，而優化的 ROADM 解決方案可讓部署變得簡單，且具有空間和功率效率及低成本之優勢，並說明下一代 Metro OLS 同步解決方案正在徹底改變捷運運涵蓋率，進而顯著節省成本並提高服務靈活性。

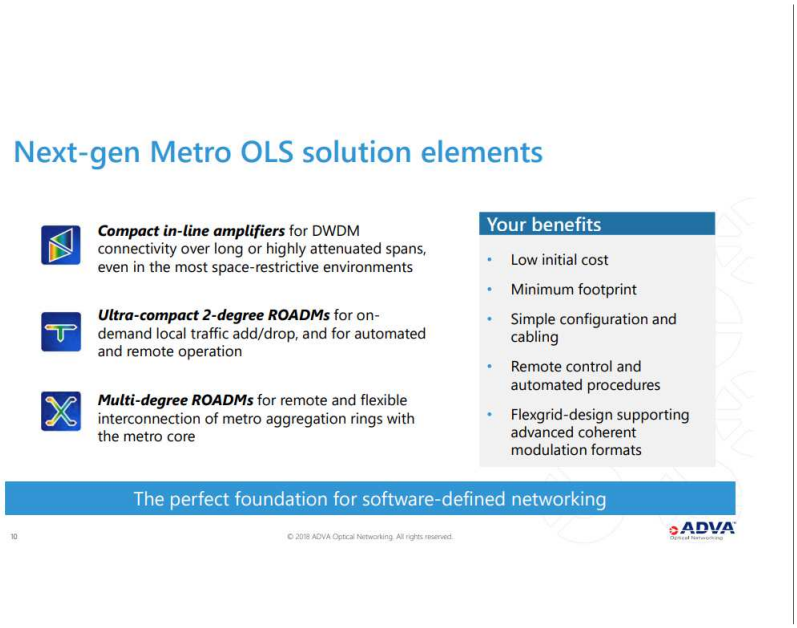


圖37 講者說明下一代Metro OLS解決方案要素 [資料來源：講者簡報]

2、DNS Flag Day 之後將如何影響你？（DNS Flag Day and beyond - how will it affect you? ）

ISC 公司 Eddy Winstead 說明，礙於從前制定的 DNS 系統標準過於老舊，造成現行的 DNS 解析速度緩慢，且過去的 DNS 系統尚無法安裝部署新的功能，因此許多 DNS 服務供應商已宣布將在 2019 年 2 月 1 日更改某些 DNS 實施的標準，正式導入 EDNS (Extension Mechanisms for DNS)協定，以提升整體 DNS 解析速度與加強 DDoS 攻擊的防禦功能，如下：

- BIND 9.13.3 (development) 和 9.14.0 (production)。
- Knot-Resolver。
- Power DNS Recursor 4.2.0。
- Unbound 1.9.0。

講者說明 DNS 內有一個延伸安全協定 EDNS，其功能主要是提供 DNS 的安全性功能，包括 DNSSEC 與延展 DNS 封包，並可讓 DNS 的查詢更加安全，爰若公司的 DNS zones 由不符合規定的供應商提供服務，則當 ISP 和其他組織更新其 Resolver 時，連線狀態將逐漸降低或消失，且當公司內部的 DNS Resolver 更新為無法實現之解決方案的版本時，公司的某些站點和電子郵件服務器可能無法運作，最後，講者介紹「DNS flag day」（https://dnsflagday.net/）網站及其應用之方法，只要輸入域名，即可檢測出網站是否有受到影響，方便讓網際網路用戶/供應商查詢自己的網站是否受影響，以尋求更安全的上網環境。

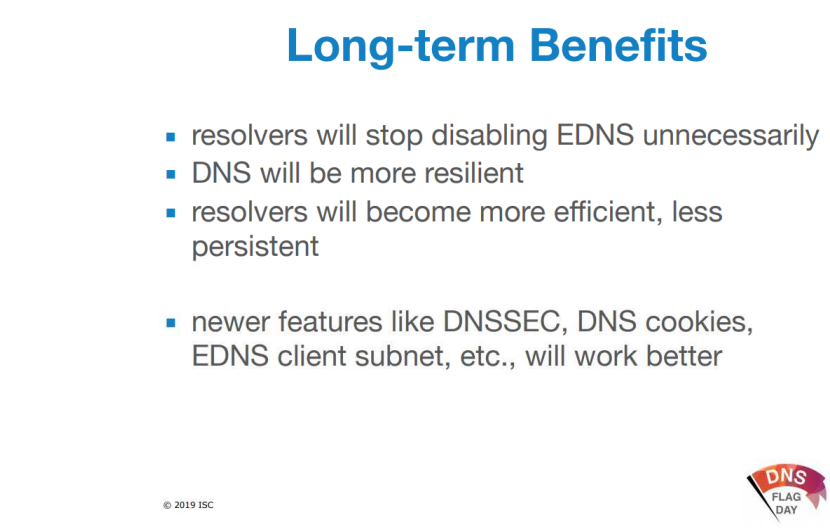


圖 38 講者介紹提早檢測網站之長期效益 [資料來源：講者簡報]

（五）ONOS SDN-IP：SDX 的教程和使用案例（SDN-IP: Tutorial and Use Case for SDX）

本場次由 ITB 系統工程師 Aris Risdianto 擔任講者，渠說明 SDN-IP 是一種 ONOS（Open Networking Operating System）應用程式，它允許軟體定義網路使用標準 Border Gateway 協議（BGP）與 Internet 上的外部網路連接。從 BGP 的角度來看，SDN 網路顯示為單個自治系統（AS），其行為與任何傳統 AS 相同；在 AS 內，SDN-IP 應用程序提供 BGP 和 ONOS 之間的整合機制。渠介紹了 SDN-IP 運行方式的實際案例，並

透過啟動一個簡單的模擬網路，看到 SDN-IP 如何控制此網路，將數據從一個地方移動到另一個地方。最後，渠討論 SDX / SD-IX 的 SDN-IP 案例，實現 BGP 的安全性，如利用 RPKI serve 之 BGP ROA。

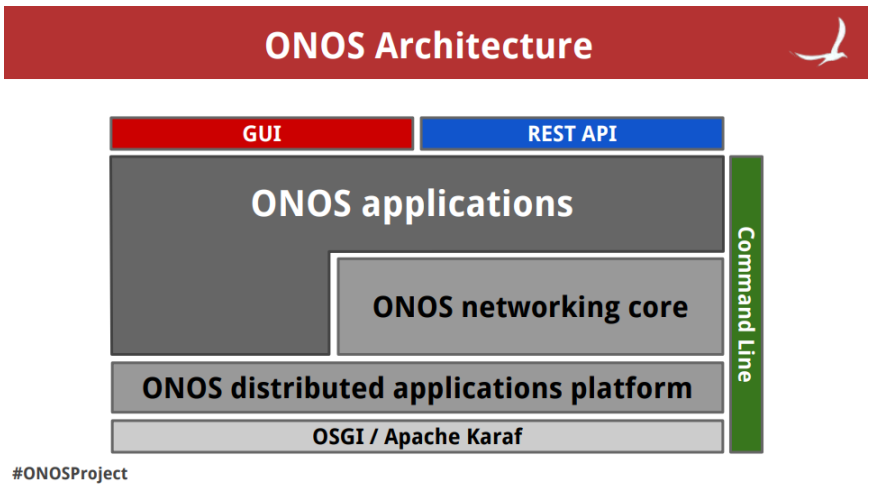


圖 39 ONOS 應用程式架構 [資料來源：講者簡報]

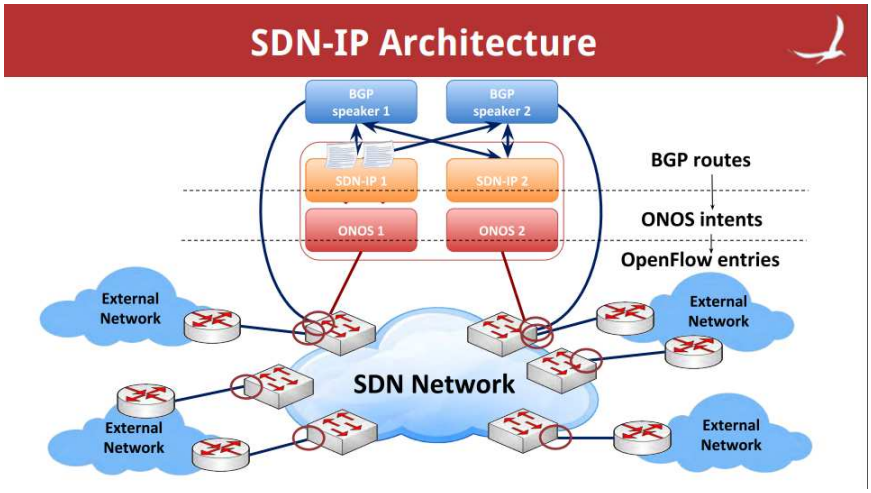


圖 40 SDN-IP 應用程式架構 [資料來源：講者簡報]

（六）參訪韓國電子通信研究院

本活動係由大會所安排之參訪行程，韓國電子通信研究院(Electronic and Telecommunications Research Institute, ETRI)；ETRI 是一個致力於研發資訊、通信、電子、廣播及匯流產業核心技術，以促進國家經濟、社會發展的非營利政府資助科研機構。此次係參訪 ETRI 之媒體研究實驗室相關成果。導覽人員為與會者介紹其體驗館內的相關展示，包括：擴增實境(AR)應用、虛擬實境(VR)應用於 4D 虛擬滑翔翼、4D 虛擬吉普車之技術，讓自願者親身體驗，接續簡介 GenieTalk 語音翻譯 app、骨傳導話機、數位油畫、2D 轉 3D 立體顯像、4K 3D 影像技術，最後，導覽人員說明 ETRI 媒體研究實驗室研發電影動畫已 10~20 年，期間已獲頒 2 次國際獎項，可有效降低拍片成本、減少演員演出之危險，並展示該技術應用於中國、韓國電影上之成果，讓與會人員非常驚艷。

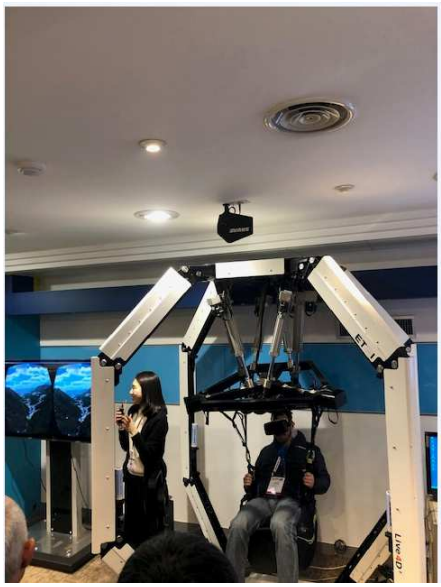


圖 41 與會人員體驗 4D 虛擬滑翔翼情形

（七）閉幕大會（Closing Plenary）

本場次由韓國 Keio 大學教授 Kilnam Chon 擔任主席，渠以網際網路歷史為題主題演講，接續由韓國 Pohang University of Science and Technology 教授 James Won-ki Hong 簡介軟體化的網際網路後，由 APNIC 董事長 Paul Wilson 及 APRICOT 主席 Philip Smith 進行結語，感謝主辦單位 KISTS 及各贊助單位（我國 TWNIC 為股東年度大會贊助者）並說明本次註冊與會者高達 714 人，人數排名前 10 者為韓國 127 人，日本 81 人、美國 70 人、澳洲 67 人、香港 66 人、菲律賓 55 人、新加坡 45 人、孟加拉 32 人、Nigh sha28 人、中國 25 人等，最後，渠等感謝本次的贊助廠商，並歡迎與會人員參與下一次於泰國清邁舉辦之 APNIC 48 會議。有關專題演講部分，摘述如下：

1、 主題：網際網路歷史（Keynote: Internet History Projects）

韓國 KAIST 大學教授 Kilnam Chon 說明，講者根據對亞洲網際網路歷史的研究，回顧了 20 世紀 60 年代到 90 年代的網際網路發展歷史，渠介紹網際網路於 1969 年開始發展，迄今已有 4.2 億人口使用，並於 1970 年代開始亞太地區的一些國家開始研究計算機通信，至 1980 年成立 AsiaNet（與 UUCP 連接）、太平洋計算機通訊研討會（Pacific Computer ommunications Symposium）、網際網路年會（IANW-AP） 亞太地區網際網路社區年會（IANW-AP）啟動、ARPANET 取代網際網路及在亞太地區多個國家/地區提供網際網路服務。1990 年成立亞太網路集團（APNG）、20 世紀 90 年代的許多 APNG 分拆，如：APNIC、APTLD、APCERT、APIA、APAN、AP *、等……，並於 1996 年創立 APRICOT 及更多組織。爰自 2011 年以來講者與 100 多位作者共同努力，出版了 80 年代、90 年代和 2000 年代三本書，廣泛的參考 1000 多份資料及電視訪問，其主題涵蓋網際網路的許多方面發展，最後講者建議各國記錄每個國家國內之網際網路發展，俾利外界參考。

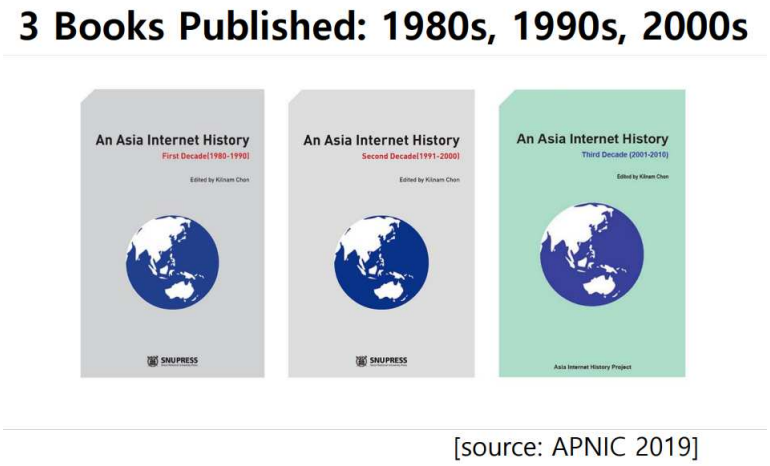


圖 41 Kilnam Chon 教授出版回顧網際網路發展歷史 3 本書 [資料來源：講者簡報]

2、 主題：軟體化的網際網路（Keynote: Softwarization of the Internet）

韓國Pohang University of Science and Technology教授 James Won-ki Hong說明，網際網路是世界各地網路和數據中心的相互聯通，並在過去 50 年中不斷發展，網際網路包括電信網路、企業網路、公共網路和研究網路。其數據中心包括來自電信公司、雲端服務供應商、企業和政府組織的數據中心。最近，其中一些網路和數據中心正在“軟體化”，爰講者說明如何營運管理這些軟體化的網際網路基礎設施及 AI 和機器學習幫助管理軟體化之基礎架構。

伍、心得與建議

一、此次會議相關議題包含各會員成長情形、Peering、IP / AS分配情形、相關培訓計畫及其IPv6推動情形，路由安全等，並經由參與APNIC Policy SIG 、Peering、IPv6、Routing 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，有助益於本會制定網際網路相關監理政策。

二、持續參與國際組織及會議，為國際社會做出努力：APNIC負責亞太地區網際網路資源管理，並在促進網際網路治理及發展上與其他地區國際組織合作上不斷努力並獲致豐碩成果，因此，我國如能積極參與此組織活動，將有更多機會可對國際社會及環境發展提供持續的貢獻。本次會議舉行其中4個席次的執行委員會委員（Executive Council）選舉，共有我國TWNIC黃執行長勝雄等7名候選人，黃執行長不負眾望連任成功，未來2年將繼續參與APNIC預算、功能及活動計畫等重要事務之決定做出貢獻。另TWNIC丁副執行長綺萍亦於本次會議參加Cooperation SIG小組主席選舉並獲多數與會者支持、當選，本小組是一個提供網際網路問題廣泛討論的論壇，如公共政策和網路治理，透過該小組的資訊共享、外展、能力建置和其他活動，可使我國於健全網際網路發展上共同出力。在Policy SIG中，我國TWNIC提案將IPv4 103/8池的最大核配額度由/22降至/23以協助更多新進者能取得IPv4，該提案除於APNIC Policy SIG階段獲致共識，並於APNIC AMG通過。以上我國於此次大會的努力，均能增加我國對國際社會的努力並獲得肯定。

三、持續觀察國際上對於網際網路資源管理趨勢並適當採取措施：透過參與本次會議之

NIR SIG會議，瞭解各國對於發展數位經濟發展所面臨大量IP位址需求，除針對IPv4進行相關回收及交易機制之探討外，各國主要仍以推動IPv6為主，例如越南及中國大陸均以國家級專案計畫進行推動。另網際網路路由安全亦是本次會議之重點，早期基於「信任」的路由交換機制，於近來不斷發生惡意的網路劫持或意外組態設定錯誤之情境下，DNSSEC、RPKI等相關簽章、加密及驗證程序已應運而生，並亟需共同推廣。我國在過去一年IPv6 之部署推廣已有很好的成績，TWNIC亦於2018年推出RPKI服務，可以幫助解決路由IP位址前綴錯誤的安全問題，使用RPKI號碼資源的合法持有者能夠掌握網際網路路由協定的運作，以防止路由劫持和其他攻擊，值得持續推廣。

四、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。

五、APNIC的會議內容較不涉及政治意涵，爰值得建議相關單位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、為持續推動完善的下一代網際網路連網環境的建立，未來的工作方向可以以下3大策略目標來進行：

- 落實 IPv6 連網環境：持續推動商用網路雙軌普行計畫，包含 ISP 網路、使用者設備及應用網站推行 IP4/IPv6 雙軌普行解決方案。
- 強化 IPv6 連網安全：目標透過網路安全架構研析，及技術人才培育的方法，幫助 ICP 業者能快速掌握 IPv4 和 IPv6 網路安全架構的差異。
- 探索 IPv6 連網應用：目標物聯裝置標準研析，包含 IoT、5G 和 IPv6 相關 RFC 標準資料研析，累積相關技術能量，加強創新產業連結。

七、持續與相關利益團體溝通對話，尋找平衡、合宜的網際網路內容阻止和過濾政策契機：政府推動網際網路內容阻斷和過濾之政策，在符合法令，且不破壞網際網路開放、全球連結的情況下，想獲得最理想的結果係相當困難的，爰建議可持續朝向如何阻斷和過濾而不影響用戶、哪種類型需要阻止或過濾及應遵循哪些規範/政策等多角度思考，並與各利益關係團體、符合政府機關、成本、風險和技術專業知識間取得平衡，讓人民對政策之制定充滿信心，找到共同前進的方向。

八、研訂部署IPv6長期解決方案，積極執行回收及實施移轉政策：鑒於IPv4已耗竭，但仍有大量已核配發的IP因被使用於私網，未見於BGP訊息公告中，且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，但不論採行哪種方法，建議可藉由獎勵行動業者自主研發，節省 IPv4 位址的使用，同時由政府擬定最終部署IPv6的長期策略，以提升產業效益，增進民眾福祉。

九、與時俱進，持續關注資安議題：網際網路安全包括對應其應用層之系統安全與資訊安全、網路層的數據傳輸加密、終端感知及終端應用層的安全等問題，對於資安防護挑戰，除須重視安全風險，如何評估朝向具防護性、靈活性、避免不必要成本的解決方案外，更重要是提升資訊安全關鍵技術，採取可行相應作法，建立可於任何環境運行保護應用程序及其數據的應用程序，以營造一安全的連網環境。

十、韓國電信公司雖自MWC於2015年3月發表下一代移動通信服務5G網路的版本以來，已於2019年1月正式商轉，高頻5G技術已逐漸從實驗室進入商業化，並朝向更高速更大頻寬發展，但有關5G網路之標準迄今仍尚未完全制訂完成，且相關檢測、應用設備仍昂貴，在目前無殺手級應用的情況下，預計仍要等到3、4年後，相關產業才會有較明顯的成長。

十一、Google、Cloudflare等公共DNS服務商已將108年2月1日訂為「DNS Flag Day」，開始正式導入 EDNS 符合性驗證，以解決DNS的安全性問題，有些網站因不支援EDNS（ Extension Mechanisms for DNS）協定之域名，將造成公共DNS無法順利解析，或解析反應變慢，影響到正常上網，爰網際網路用戶/供應商應儘快至DNS Flag Day網站（https://dnsflagday.net/）查詢自身網站是否受影響，若經檢測有影響之虞，可儘速更改的DNS設定，以尋求更安全的上網環境。