『推動 IPv4/IPv6 雙軌普行方案』

附錄五
出國報告

目錄

『IETF 104 Prague Meetings』出國報告

財團法人台灣網路資訊中心因公出國人員報告書 108 年 4 月 18 日

報告人 姓　名	丁綺萍 顧靜恆	服務單位及 職稱	副執行長 組長
出國期間	108/3/23-30	出國地點	Prague, Czech
出國事由	參加 IETF 104 Prague Meetings		

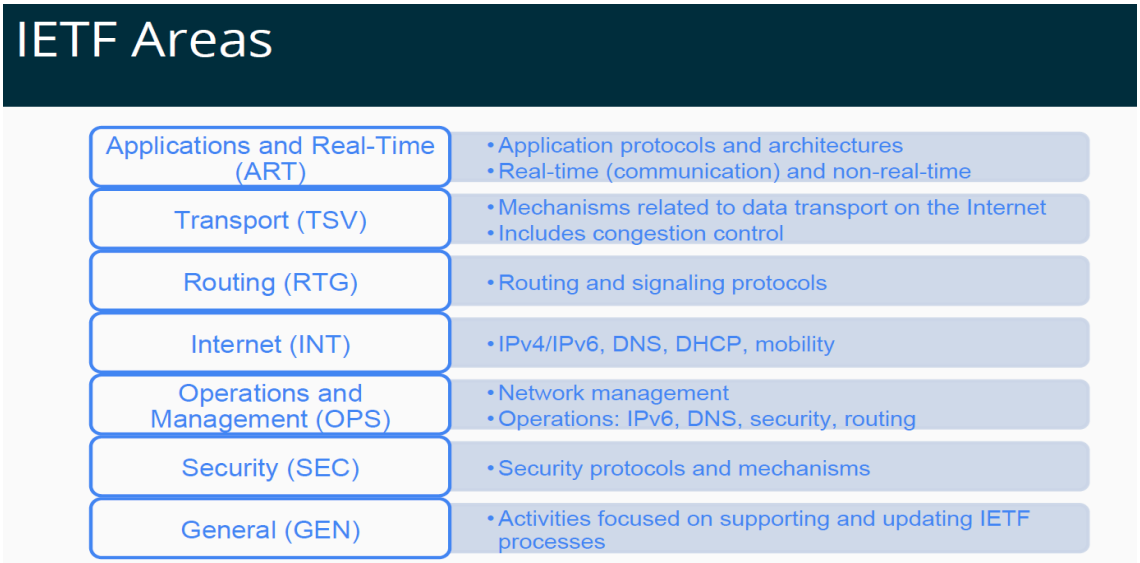
報告書內容包含：
一、 出國目的
二、 會議行程
三、 考察、訪問心得
四、 建議意見
五、 會議議程

授　權 聲 明 欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人： 丁綺萍 顧靜恆 (簽章)

註
二、請於授權聲明欄簽章，授權本中心重製發行公開利用。
附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

一、 出國目的：

參加 IETF 104 Prague 會議。網際網路工程任務小組（全名：Internet Engineering Task Force，縮寫為 IETF）負責網際網路標準的開發和推動。此次會議在捷克布拉格召開，會議日期 3 月 23 日至 29 日共為期 7 天，這是 IETF 所舉行的第 104 次會議。本次會議約有 1,213 人到場參與及 864 人遠端參與，由 Cisco（思科）及 CZ.NIC 共同主辦，會議主題共分為以下 7 大項目：



中心參加此次會議的主要目的為參與及了解各 WGs（Working Groups，工作小組）技術發展的趨勢及討論方向，包含 IPv6、Security、及 IoT 等相關議題。

Working Groups 是制定 IETF 技術規格和規範的主要機制，各小組負責不同技術規格的討論，並接收各方的意見加以修改，最終目的是要讓技術規格成為網際網路運作的標準或建議書，提供網際網路的技術開發團隊能有技術標準規格可做為依循，及保障全球網際網路能通行無礙。WGs 的運作方式是透過建立一個新的章程，該章程定義特定問題及成果（包含建議、標準規範等）。各 Working Group 會有一位主席追蹤小組的運作狀況，並在章程規定小組的工作範圍，

列出如何完成此項工作的目標和里程碑等資訊。通常會有超過 100 個正在進行中的 Working Group，每個 Working Group 都是由和其本身工作領域相關的技術人員參與。當完成目標後，Working Group 就會結束，但有些 Working Group 會隨著環境及應用的變化，不斷改進已建立的標準協議，則此 Working Group 就會持續維持運作狀態。所有進行中的 Working Group 可以在 IETF Datatracker 找到完整列表。

IETF Datatracker 查詢網站：https://datatracker.ietf.org/

圖：IETF 104 大會報到處

圖左至右：TWNIC 顧靜恆組長及 TWNIC 丁綺萍副執行長

二、 會議行程：

詳如會議網站 https://www.ietf.org/how/meetings/104/。
議程 https://datatracker.ietf.org/meeting/104/agenda.html。
IETF 網站 https://www.ietf.org/。

參與會議的行程安排如下表列：

日期	時間	議程
108/3/24 (日)	10:00	IETF Registration
	12:30-13:30	Tutorial: Newcomers' Overview
	13:45-14:45	Tutorial: GitHub Tools
	15:00-16:00	Newcomers' Quick Connections
	16:00-17:00	Newcomers' Meet and Greet
108/3/25 (一)	9:00-11:00	IPv6 Maintenance WG
	9:00-11:00	Privacy Enhancements and Assessments Proposed Research Group
	11:00-11:20	Beverage Break
	11:20-12:20	IPv6 over the TSCH mode of IEEE 802.15.4e WG
	11:20-12:20	Operational Security Capabilities for IP Network Infrastructure WG
	12:20-13:50	Break
	13:50-15:50	IPv6 over Networks of Resource-constrained Nodes WG
	15:50-16:10	Beverage and Snack Break
	16:10-18:10	Stopping Malware and Researching Threats
	16:10-18:10	Quantum Internet Proposed Research Group
108/3/26 (二)	9:00-11:00	SIDR Operations WG
	9:00-11:00	Home Networking WG
	11:00-11:20	Beverage Break
	11:20-12:20	Managed Incident Lightweight Exchange WG
	11:20-12:20	DNS Over HTTPS WG
	12:20-13:50	Break
	13:50-15:50	Interface to Network Security Functions WG
	15:50-16:10	Beverage and Snack Break
	16:10-18:10	IPv6 over Low Power Wide-Area Networks WG
	16:10-18:10	Thing-to-Thing
108/3/27	9:00-11:00	Security Events WG

(三)	9:00-11:00	Software Updates for Internet of Things WG
	11:00-11:20	Beverage and Snack Break
	11:20-12:20	Security Automation and Continuous Monitoring WG
	15:00-17:00	Technology Deep Dive - Modern Router Architecture BOF
	16:50-17:10	Beverage and Snack Break
	17:10-19:40	IETF Plenary
108/3/28 (四)	9:00-10:30	Web Authorization Protocol WG
	10:30-10:50	Beverage Break
	10:50-12:20	IP Security Maintenance and Extensions WG
	12:20-13:50	Break
	13:50-15:50	IPv6 Operations WG
	15:50-16:10	Beverage and Snack Break
	16:10-18:10	Human Rights Protocol Considerations
108/3/29 (五)	9:00-10:30	IPv6 Maintenance WG
	10:30-10:50	Beverage Break
	10:50-12:50	IP Wireless Access in Vehicular Environments WG

三、 考察、訪問心得：

（一）IETF 104 Prague 會議

圖：IETF 104 會場

在此次 IETF 104 Prague 會議中主要參與的會議主題包含 IPv6、Security、及 IoT 領域的相關議題，以下將分別對此 3 大議題之報告彙

整如下：

IPv6 相關技術討論

本次參與有關 IPv6 技術討論會議，包括下列幾個工作小組：

1. v6ops Working Group - IPv6 Operations
2. 6MAN Working Group - IPv6 Maintenance，
3. dhc Working Group - Dynamic Host Configuration，
4. 6lo Working Group - IPv6 over Networks of Resource-constrained Nodes，

會中進行的主題包含以下內容：

1. 464XLAT Optimization for CDNs/Caches

本文發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，描述了 IP / ICMP 轉換算法（IP/ICMP Translation Algorithm，SIIT）在用作 NAT46 時，以及 IPv4-only 設備或應用啟動到雙協定內容傳遞網路（Content Delivery Networks，CDNs）或快取（Caches）伺服器，造成通過 NAT64 被強制轉譯回 IPv4 的缺點。該文件提出了可避免的解決方案。

詳細草案請參考：draft-palet-v6ops-464xlat-opt-cdn-caches-01 (https://tools.ietf.org/html/draft-palet-v6ops-464xlat-opt-cdn-caches-01)

2. Pros and Cons of IPv6 Transition Technologies for IPv4aaS

目前已經有幾種 IPv6 移轉技術被發展出來，以便讓 ISP 在 IPv6-only 的接取或核心網路提供用戶 IPv4 即服務（IPv4-as-a-Service，IPv4aaS）。不同的技術各有其優點和缺點，取決於其網路拓撲架構，技術，策略和其他偏好。這些技術之一可能是某個網路維運商最合適的解決方案。

本文發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，考慮了五種最著名的 IPv4aaS 技術，考慮了許多不同面向，為網路維運者提供了易於使用的參考，以幫助他們選擇最符合需求的技術參考。

詳細草案請參考：draft-lmhp-v6ops-transition-comparison-02 (https://tools.ietf.org/html/draft-lmhp-v6ops-transition-comparison-02)

3. Reaction of Stateless Address Autoconfiguration (SLAAC) to Renumbering Events

在與IPv6前綴相關的網路組態資訊變為無效而沒有任何該狀況的明確訊號狀況下（例如，當CPE在不知道先前使用的前綴的情況下崩潰並重新啟動時），本地網路上的節點於不可接受的長時間繼續使用過時的前綴，從而導致連接問題。 本文分析了這些問題場景，並提出了改進網路穩健性的解決方法。

本文發表於IPv6維運（IPv6 Operations，v6ops）工作小組，更新了RFC4861和RFC4862，以便對網路組態更改做出穩健的反應。

詳細草案請參考：draft-gont-6man-slaac-renum-01
(https://tools.ietf.org/html/draft-gont-6man-slaac-renum-01)

4. NAT64/DNS64 detection via SRV Records

本文發表於IPv6維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

本文發現使用NAT64池搭配DNS伺服器，向本地客戶提供DNS64服務的方法。該發現是通過SRV記錄完成的，SRV記錄還允許為NAT64池和DNS64伺服器分配優先權。它還允許客戶端擁有與NAT64提供商不同的DNS提供商，同時通過提供SRV記錄的DNSSEC驗證以提供安全連線的方式。 這樣，即使在使用基於HTTPS的DNS狀況下，它仍可提供DNS64服務。

詳細草案請參考：draft-ietf-v6ops-nat64-srv-00
(https://tools.ietf.org/html/draft-ietf-v6ops-nat64-srv-00)

5. IPv6 Router Advertisement IPv6-Only Flag

本文發表於IPv6維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document specifies a Router Advertisement Flag to indicate to hosts that the administrator has configured the router to advertise that the link is IPv6-Only. This document updates RFC4861 and RFC5175.

詳細草案請參考：draft-ietf-6man-ipv6only-flag-05
(https://tools.ietf.org/html/draft-ietf-6man-ipv6only-flag-05)

6. Privacy Extensions for Stateless Address Autoconfiguration in IPv6

本文發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Nodes use IPv6 stateless address autoconfiguration to generate addresses using a combination of locally available information and information advertised by routers. Addresses are formed by combining network prefixes with an interface identifier. This document describes an extension that causes nodes to generate global scope addresses from interface identifiers that change over time. Changing the interface identifier (and the global scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node.

詳細草案請參考：draft-ietf-6man-rfc4941bis-01
(https://tools.ietf.org/html/draft-ietf-6man-rfc4941bis-01)

7. Discovering PREF64 in Router Advertisements

本文發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，提出一個 Router Advertisement 選項，用於將 NAT64 前綴傳遞給客戶端。

詳細草案請參考：draft-pref64folks-6man-ra-pref64-02
(https://tools.ietf.org/html/draft-pref64folks-6man-ra-pref64-02)

8. IPv6 Segment Routing Header (SRH)

本文發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Segment Routing can be applied to the IPv6 data plane using a new type of Routing Extension Header. This document describes the Segment Routing Extension Header and how it is used by Segment Routing capable nodes.

詳細草案請參考：draft-ietf-6man-segment-routing-header-18

(https://tools.ietf.org/html/draft-ietf-6man-segment-routing-header-18)

9. Link-Layer Addresses Assignment Mechanism for DHCPv6

本文發表於動態主機設定（Dynamic Host Configuration，dhc）工作小組，草案摘要如下：

In certain environments, e.g. large scale virtualization deployments, new devices are created in an automated manner. Such devices typically have their link-layer (MAC) addresses randomized. With sufficient scale, the likelihood of collision is not acceptable.

Therefore an allocation mechanism is required. This draft proposes an extension to DHCPv6 that allows a scalable approach to link-layer address assignments.

詳細草案請參考：draft-bvtm-dhc-mac-assign-02
(https://tools.ietf.org/html/draft-bvtm-dhc-mac-assign-02)

10. SLAP quadrant selection options for DHCPv6

本文發表於動態主機設定（Dynamic Host Configuration，dhc）工作小組，草案摘要如下：

The IEEE originally structured the 48-bit MAC address space in such a way that half of it was reserved for local use. Recently, the IEEE has been working on a new specification (IEEE 802c) which defines a new "optional Structured Local Address Plan" (SLAP) that specifies different assignment approaches in four specified regions of the local MAC address space.

The IEEE is working on mechanisms to allocate addresses in the one of these quadrants (IEEE 802.1CQ). There is work also in the IETF on specifying a new mechanism that extends DHCPv6 operation to handle the local MAC address assignments. In this document, we complement this ongoing IETF work by defining a mechanism to allow choosing the SLAP quadrant to use in the allocation of the MAC address to the requesting device/client.

This document proposes extensions to DHCPv6 protocols to enable a DHCPv6 client or a DHCPv6 relay to indicate a preferred SLAP quadrant to the server, so that the server allocates the MAC address to the given client out of the quadrant requested by relay or client.

詳細草案請參考：draft-bernardos-dhc-slap-quadrant-01

(https://tools.ietf.org/html/draft-bernardos-dhc-slap-quadrant-01)

11. Problem Statement of Multirequirement Extensions for DHCPv6

本文發表於動態主機設定（Dynamic Host Configuration，dhc）工作小組，草案摘要如下：

The manageability, security, privacy protection, and traceability of networks can be supported by extending DHCPv6 protocol. This document analyzes current extension practices and typical DHCP server software on extensions, defines a DHCP general model, discusses some extension points, and present extension cases.

詳細草案請參考：
draft-ren-dhc-problem-statement-of-mredhcpv6-01(https://tools.ietf.org/html/draft-ren-dhc-problem-statement-of-mredhcpv6-01)

12. IPv6 Backbone Router

本文發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document updates RFC 4861 and RFC 8505 in order to enable proxy services for IPv6 Neighbor Discovery by Routing Registrars called Backbone Routers. Backbone Routers are placed along the wireless edge of a Backbone, and federate multiple wireless links to form a single MultiLink Subnet.

詳細草案請參考：draft-ietf-6lo-backbone-router-11
(https://tools.ietf.org/html/draft-ietf-6lo-backbone-router-11)

13. IPv6 over Constrained Node Networks (6lo) Applicability & Use cases

本文發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document describes the applicability of IPv6 over constrained node networks (6lo) and provides practical deployment examples. In addition to IEEE 802.15.4, various link layer technologies such as ITU-T G.9959 (Z-Wave), BLE, DECT-ULE, MS/TP, NFC, PLC (IEEE 1901.2), and IEEE

802.15.4e (6tisch) are used as examples. The document targets an audience who like to understand and evaluate running end-to-end IPv6 over the constrained node networks connecting devices to each other or to other devices on the Internet (e.g. cloud infrastructure).

詳細草案請參考：draft-ietf-6lo-use-cases-06
(https://tools.ietf.org/html/draft-ietf-6lo-use-cases-06)

14. IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP

本文發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

RFC 7668 describes the adaptation of 6LoWPAN techniques to enable IPv6 over Bluetooth low energy networks that follow the star topology. However, recent Bluetooth specifications allow the formation of extended topologies as well. This document specifies mechanisms that are needed to enable IPv6 mesh over Bluetooth Low Energy links established by using the Bluetooth Internet Protocol Support Profile. This document does not specify the routing protocol to be used in an IPv6 mesh over Bluetooth LE links.

詳細草案請參考：draft-ietf-6lo-blemesh-05
(https://tools.ietf.org/html/draft-ietf-6lo-blemesh-05)

15. Transmission of IPv6 Packets over PLC Networks

本文發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

Power Line Communication (PLC), namely using the electric-power lines for indoor and outdoor communications, has been widely applied to support Advanced Metering Infrastructure (AMI), especially smart meters for electricity. The inherent advantage of existing electricity infrastructure facilitates the expansion of PLC deployments, and moreover, a wide variety of accessible devices raises the potential demand of IPv6 for future applications. This document describes how IPv6 packets are transported over constrained PLC networks, such as ITU-T G.9903, IEEE 1901.1 and IEEE 1901.2.

詳細草案請參考：draft-ietf-6lo-plc-00
(https://tools.ietf.org/html/draft-ietf-6lo-plc-00)

Security 相關技術討論

本次參與有關 Security 技術討論會議，包括下列幾個工作小組：

1. mile Working Group - Managed Incident Lightweight Exchange；
2. sacm Working Group - Security Automation and Continuous Monitoring；
3. secevent Working Group - Security Events；
4. smart Working Group - Stopping Malware and Researching Threats。

會中進行的主題包含以下內容：

1. Using XMPP for Security Information Exchange

本文發表於託管事件輕量級交換（Managed Incident Lightweight Exchange，mile）工作小組，草案摘要如下：

This document describes how to use the Extensible Messaging and Presence Protocol (XMPP) to collect and distribute security incident reports and other security-relevant information between network-connected devices, primarily for the purpose of communication among Computer Security Incident Response Teams and associated entities.

To illustrate the principles involved, this document describes such a usage for the Incident Object Description Exchange Format (IODEF).

詳細草案請參考：draft-ietf-mile-xmpp-grid-10
(https://tools.ietf.org/html/draft-ietf-mile-xmpp-grid-10)

2. CBOR/JSON binding of IODEF

本文發表於託管事件輕量級交換（Managed Incident Lightweight Exchange，mile）工作小組，草案摘要如下：

RFC7970 specified an information model and a corresponding XML data model for exchanging incident and indicator information. This draft provides an alternative data model implementation in CBOR/JSON.

詳細草案請參考：draft-ietf-mile-jsoniodef-08
(https://www.ietf.org/id/draft-ietf-mile-jsoniodef-08.txt)

3. Definition of ROLIE CSIRT Extension

本文發表於託管事件輕量級交換（Managed Incident Lightweight Exchange，mile）工作小組，草案摘要如下：

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type categories and related requirements needed to support Computer Security Incident Response Team (CSIRT) use cases. The indicator and incident information types are defined as ROLIE extensions. Additional supporting requirements are also defined that describe the use of specific formats and link relations pertaining to the new information types.

詳細草案請參考：draft-ietf-mile-rolie-csirt-02
(https://tools.ietf.org/html/draft-ietf-mile-rolie-csirt-02)

4. Definition of the ROLIE Software Descriptor Extension

本文發表於安全自動化和持續監控（Security Automation and Continuous Monitoring，sacm）工作小組，草案摘要如下：

This document uses the "information-type" extension point as defined in the Resource-Oriented Lightweight Information Exchange (ROLIE) [RFC8322] Section 7.1.2 to better support Software Record and Software Inventory use cases. This specification registers a new ROLIE information-type, "software-descriptor", that allows for the categorization of information relevant to software description activities and formats. In particular, the usage of the ISO 19770-2:2015 (SWID Tag) and the Concise SWID (COSWID) formats in ROLIE are standardized. Additionally, this document discusses requirements and usage of other ROLIE elements in order to best syndicate software description information.

詳細草案請參考：draft-ietf-sacm-rolie-softwaredescriptor-06
(https://tools.ietf.org/html/draft-ietf-sacm-rolie-softwaredescriptor-06)

5. Security Automation and Continuous Monitoring (SACM) Architecture

本文發表於安全自動化和持續監控（Security Automation and Continuous Monitoring，sacm）工作小組，草案摘要如下：

This memo documents an exploration of a possible Security Automation and Continuous Monitoring (SACM) architecture. This work is built upon [I-D.ietf-mile-xmpp-grid], and is predicated upon information gleaned from SACM Use Cases and Requirements ([RFC7632] and [RFC8248] respectively), and terminology as found in [I-D.ietf-sacm-terminology].

詳細草案請參考：draft-mandm-sacm-architecture-01 (https://tools.ietf.org/html/draft-mandm-sacm-architecture-01)

6. Security Automation and Continuous Monitoring (SACM) Terminology

本文發表於安全自動化和持續監控（Security Automation and Continuous Monitoring，sacm）工作小組，本備忘錄記錄了 SACM 產出的文件中使用的術語。

詳細草案請參考：draft-ietf-sacm-terminology-16 (https://tools.ietf.org/html/draft-ietf-sacm-terminology-16)

7. Concise Software Identifiers

本文發表於安全自動化和持續監控（Security Automation and Continuous Monitoring，sacm）工作小組，草案摘要如下：

This document defines a concise representation of ISO/IEC 19770-2:2015 Software Identification (SWID) tags that are interoperable with the XML schema definition of ISO/IEC 19770-2:2015 and augmented for application in Constrained-Node Networks. Next to the inherent capability of SWID tags to express arbitrary context information, Concise SWID (CoSWID) tags support the definition of additional semantics via well-defined data definitions incorporated by extension points.

詳細草案請參考：draft-ietf-sacm-coswid-08 (https://tools.ietf.org/html/draft-ietf-sacm-coswid-08)

8. Endpoint Posture Collection Profile

本文發表於安全自動化和持續監控（Security Automation

and Continuous Monitoring，sacm）工作小組，草案摘要如下：

This document specifies the Endpoint Posture Collection Profile, which describes the best practices for the application of IETF, TNC, and ISO/IEC data models, protocols, and interfaces to support the on-going collection and communication of endpoint posture to a centralized server where it can be stored and made available to other tools. This document is an extension of the Trusted Computing Group's Endpoint Compliance Profile Version 1.0 specification [ECP].

詳細草案請參考：draft-ietf-sacm-ecp-04
(https://tools.ietf.org/html/draft-ietf-sacm-ecp-04)

9. Push-Based Security Event Token (SET) Delivery Using HTTP

本文發表於安全事件（Security Events，secevent）工作小組，草案摘要如下：

This specification defines how a Security Event Token (SET) may be delivered to an intended recipient using HTTP POST. The SET is transmitted in the body of an HTTP POST request to an endpoint operated by the recipient, and the recipient indicates successful or failed transmission via the HTTP response.

詳細草案請參考：draft-ietf-secevent-http-push-05
(https://tools.ietf.org/html/draft-ietf-secevent-http-push-05)

10. Subject Identifiers for Security Event Tokens

本文發表於安全事件（Security Events，secevent）工作小組，草案摘要如下：

Security events communicated within Security Event Tokens may support a variety of identifiers to identify the subject and/or other principals related to the event. This specification formalizes the notion of subject identifiers as named sets of well-defined claims describing the subject, a mechanism for representing subject identifiers within a [JSON] object such as a JSON Web Token [JWT] or Security Event Token [SET], and a registry for defining and allocating names for these claim sets.

詳細草案請參考：draft-ietf-secevent-subject-identifiers-03
(https://tools.ietf.org/html/draft-ietf-secevent-subject-identifiers-03)

11.Poll-Based Security Event Token (SET) Delivery Using HTTP

本文發表於安全事件（Security Events，secevent）工作小組，草案摘要如下：

This specification defines how a series of Security Event Tokens (SETs) may be delivered to an intended recipient using HTTP POST over TLS initiated as a poll by the recipient. The specification also defines how delivery can be assured, subject to the SET Recipient's need for assurance.

詳細草案請參考：draft-ietf-secevent-http-poll-02 (https://tools.ietf.org/html/draft-ietf-secevent-http-poll-02)

12.Capabilities and Limitations of an Endpoint-only Security Solution(CLESS)

本文發表於惡意軟體阻止和威脅研究（Stopping Malware and Researching Threats，smart）工作小組，草案摘要如下：

In the context of existing, proposed and newly published protocols, this draft RFC is to establish the capabilities and limitations of endpoint-only security solutions and explore benefits and alternatives to mitigate those limits with the support of real case studies.

詳細草案請參考：draft-taddei-smart-cless-introduction-00 (https://tools.ietf.org/html/draft-taddei-smart-cless-introduction-00)

Capabilities and Limitations of an Endpoint-only Security Solution(CLESS)簡報投影片請參閱：https://datatracker.ietf.org/meeting/104/materials/slides-104-smart-slides-for-cless-draft-taddei-smart-cless-introduction-00

13.惡意軟體阻止和威脅研究（Stopping Malware and Researching Threats，smart）工作小組相關報告。

惡意軟體阻止和威脅研究（Stopping Malware and Researching Threats，smart）工作小組邀請相關單位進行了威脅研究相關報告，包含：

(1) Threat Landscape Update

由賽門鐵克（Symantec）公司報告，簡報投影片請參閱：https://datatracker.ietf.org/meeting/104/materials/slides-104-smart-threat-landscape-slides-00 ，

2019 Internet Security Threat Report 請參閱：

https://go.symantec.com/istr

(2) Malicious Uses of Evasive Communications and Threats to Privacy
由思科（CISCO）公司報告，簡報投影片請參閱：
https://datatracker.ietf.org/meeting/104/materials/slides-104-smart-malicious-uses-of-evasive-communications-and-threats-to-privacy-00

(3) Threat Testing for the Good of the Internet
由英國 SE Labs 公司（公司網址：https://selabs.uk/）報告，簡報投影片請參閱：
https://datatracker.ietf.org/meeting/104/materials/slides-104-smart-testing-for-the-good-of-the-internet-se-01

(4) BGP hijacking
由捷克 Qrator Labs 公司（公司網址：https://qrator.net/）報告，簡報投影片請參閱：
https://datatracker.ietf.org/meeting/104/materials/slides-104-smart-bgp-hijacking-01

(5) One Snake
由英國國家網路安全中心（NCSC: National Cyber Security Centre，https://www.ncsc.gov.uk/ ）報告，簡報名稱為 For sale : One snake. Good oil producer. No longer required，簡報投影片請參閱：
https://datatracker.ietf.org/meeting/104/materials/slides-104-smart-one-snake-slides-00

IoT 相關技術討論

本次參與有關 IoT 技術討論會議，包括下列幾個工作小組：

1. suit Working Group - Software Updates for Internet of Things；
2. 6TiSCH Working Group - IPv6 over the TSCH mode of IEEE 802.15.4e；(TSCH is the abbreviation of Time Slotted Channel Hopping)
3. lpwan Working Group - IPv6 over Low Power Wide-Area Networks；
4. t2trg Working Group - Thing-to-Thing。

會中進行的主題包含以下內容：

1. A Firmware Update Architecture for Internet of Things Devices

本文發表於物聯網軟體更新（Software Updates for Internet

of Things，suit）工作小組，草案摘要如下：

Vulnerabilities with Internet of Things (IoT) devices have raised the need for a solid and secure firmware update mechanism that is also suitable for constrained devices. Incorporating such update mechanism to fix vulnerabilities, to update configuration settings as well as adding new functionality is recommended by security experts.

This document lists requirements and describes an architecture for a firmware update mechanism suitable for IoT devices. The architecture is agnostic to the transport of the firmware images and associated meta-data.

This version of the document assumes asymmetric cryptography and a public key infrastructure. Future versions may also describe a symmetric key approach for very constrained devices.

詳細草案請參考：draft-ietf-suit-architecture-05
(https://www.ietf.org/id/draft-ietf-suit-architecture-05.txt)

2. Firmware Updates for Internet of Things Devices - An Information Model for Manifests

本文發表於物聯網軟體更新（Software Updates for Internet of Things，suit）工作小組，草案摘要如下：

Vulnerabilities with Internet of Things (IoT) devices have raised the need for a solid and secure firmware update mechanism that is also suitable for constrained devices. Incorporating such update mechanism to fix vulnerabilities, to update configuration settings as well as adding new functionality is recommended by security experts.

One component of such a firmware update is the meta-data, or manifest, that describes the firmware image(s) and offers appropriate protection. This document describes all the information that must be present in the manifest.

詳細草案請參考：draft-ietf-suit-information-model-02
(https://tools.ietf.org/html/draft-ietf-suit-information-model-02)

3. SUIT CBOR manifest serialisation format

本文發表於物聯網軟體更新（Software Updates for Internet of Things，suit）工作小組，草案摘要如下：

This specification describes the format of a manifest. A manifest is a bundle of metadata about the firmware for an IoT device, where to find the firmware, the devices to which it applies, and cryptographic information protecting the manifest.

詳細草案請參考：draft-moran-suit-manifest-04
(https://www.ietf.org/id/draft-moran-suit-manifest-04.txt)

4. An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4

本文發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，

This document describes a network architecture that provides low-latency, low-jitter and high-reliability packet delivery. It combines a high-speed powered backbone and subnetworks using IEEE 802.15.4 time-slotted channel hopping (TSCH) to meet the requirements of LowPower wireless deterministic applications.

詳細草案請參考：draft-ietf-6tisch-architecture-20
(https://www.ietf.org/id/draft-ietf-6tisch-architecture-20.txt)

5. Minimal Security Framework for 6TiSCH

本文發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document describes the minimal framework required for a new device, called "pledge", to securely join a 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e) network. The framework requires that the pledge and the JRC (join registrar/coordinator, a central entity), share a symmetric key. How this key is provisioned is out of scope of this document. Through a single CoAP (Constrained Application Protocol) request-response exchange secured by OSCORE (Object Security for Constrained RESTful Environments), the pledge requests admission into the network and the JRC configures it with link-layer keying material and other parameters. The JRC may at any time update the parameters through another request-response exchange secured by OSCORE. This specification defines the Constrained Join Protocol and its CBOR (Concise Binary Object Representation) data structures, and configures the rest of the 6TiSCH communication stack for this join process to occur in a

secure manner. Additional security mechanisms may be added on top of this minimal framework.

詳細草案請參考：draft-ietf-6tisch-minimal-security-10
(https://www.ietf.org/id/draft-ietf-6tisch-minimal-security-10.txt)

6. 6TiSCH Minimal Scheduling Function (MSF)

本文發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This specification defines the 6TiSCH Minimal Scheduling Function (MSF). This Scheduling Function describes both the behavior of a node when joining the network, and how the communication schedule is managed in a distributed fashion. MSF builds upon the 6TiSCH Operation Sublayer Protocol (6P) and the Minimal Security Framework for 6TiSCH.

詳細草案請參考：draft-ietf-6tisch-msf-03
(https://www.ietf.org/id/draft-ietf-6tisch-msf-03.txt)

7. LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP

本文發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This document defines the Static Context Header Compression (SCHC) framework, which provides both header compression and fragmentation functionalities. SCHC has been designed for Low Power Wide Area Networks (LPWAN).

SCHC compression is based on a common static context stored in both the LPWAN device and the network side. This document defines a header compression mechanism and its application to compress IPv6/UDP headers.

This document also specifies a fragmentation and reassembly mechanism that is used to support the IPv6 MTU requirement over the LPWAN technologies. Fragmentation is needed for IPv6 datagrams that, after SCHC compression or when such compression was not possible, still exceed the layer-2 maximum payload size.

The SCHC header compression and fragmentation mechanisms are independent of the specific LPWAN technology

over which they are used. This document defines generic functionalities and offers flexibility with regard to parameter settings and mechanism choices.

This document standardizes the exchange over the LPWAN between two SCHC entities. Settings and choices specific to a technology or a product are expected to be grouped into profiles, which are specified in other documents. Data models for the context and profiles are out of scope.

詳細草案請參考：draft-ietf-lpwan-ipv6-static-context-hc-18
(https://tools.ietf.org/html/draft-ietf-lpwan-ipv6-static-context-hc-18)

8. SCHC over Sigfox LPWAN

本文發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

The Static Context Header Compression (SCHC) specification describes a header compression scheme and fragmentation functionality for Low Power Wide Area Network (LPWAN) technologies. SCHC offers a great level of flexibility that can be tailored for different LPWAN technologies.

The present document provides the optimal parameters and modes of operation when SCHC is implemented over a Sigfox LPWAN.

詳細草案請參考：draft-zuniga-lpwan-schc-over-sigfox-03
(https://tools.ietf.org/html/draft-zuniga-lpwan-schc-over-sigfox-03)

9. Static Context Header Compression (SCHC) over LoRaWAN

本文發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

The Static Context Header Compression (SCHC) specification describes generic header compression and fragmentation techniques for LPWAN (Low Power Wide Area Networks) technologies. SCHC is a generic mechanism designed for great flexibility, so that it can be adapted for any of the LPWAN technologies.

This document provides the adaptation of SCHC for use in LoRaWAN networks, and provides elements such as efficient parameterization and modes of operation.

詳細草案請參考：draft-petrov-lpwan-ipv6-schc-over-lorawan-03 (https://www.ietf.org/id/draft-petrov-lpwan-ipv6-schc-over-lorawan-03.txt)

10.LPWAN Static Context Header Compression (SCHC) over NB-IoT

本文發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

The Static Context Header Compression (SCHC) specification describes a header compression and fragmentation functionalities for LPWAN (Low Power Wide Area Networks) technologies. SCHC was designed to be adapted over any of the LPWAN technologies.

This document describes the use of SCHC over the NB-IoT wireless access, and provides elements for an efficient parameterization.

詳細草案請參考：draft-minaburo-lpwan-nbiot-hc-02 (https://www.ietf.org/id/draft-minaburo-lpwan-nbiot-hc-02.txt)

11.Data Model for Static Context Header Compression (SCHC)

本文發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This document describes a YANG data model for the SCHC (Static Context Header Compression). A generic module is defined, that can be applied for any headers and also a specific model for the IPv6 UDP protocol stack is also proposed. Note that this draft is a first attempt to define a YANG data module for SCHC, more work is needed to use all the YANG facilities.

詳細草案請參考：draft-toutain-lpwan-schc-yang-data-model-00 (https://tools.ietf.org/html/draft-toutain-lpwan-schc-yang-data-model-00)

12.LPWAN Static Context Header Compression (SCHC) for CoAP

本文發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This draft defines the way SCHC header compression can be applied to CoAP headers. CoAP header structure differs from IPv6 and UDP protocols since the CoAP use a flexible header with a variable number of options themself of a variable length. Another important difference is the asymmetry in the header

format used in request and response messages. Most of the compression mechanisms have been introduced in [I-D.ietf-lpwan-ipv6-static-context-hc], this document explains how to use the SCHC compression for CoAP.

詳細草案請參考：draft-ietf-lpwan-coap-static-context-hc-04 (https://tools.ietf.org/html/draft-ietf-lpwan-coap-static-context-hc-04)

13. OAM for LPWAN using Static Context Header Compression (SCHC)

本文發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

With IP protocols now generalizing to constrained networks, users expect to be able to Operate, Administer and Maintain them with the familiar tools and protocols they already use on less constrained networks.

OAM uses specific messages sent into the data plane to measure some parameters of a network. Most of the time, no explicit values are sent is these messages. Network parameters are obtained from the analysis of these specific messages.

This can be used:

- To detect if a host is up or down.
- To measure the RTT and its variation over time.
- To learn the path used by packets to reach a destination.

-AM in LPWAN is a little bit trickier since the bandwidth is limited and extra traffic added by OAM can introduce perturbation on regular transmission.

Two scenarios can be investigated:

- OAM coming from internet. In that case, the NGW should act as a proxy and handle specifically the OAM traffic.
- OAM coming from LPWAN devices: This can be included into regular devices but some specific devices may be installed in the LPWAN network to measure its quality.

The primitive functionalities of OAM are achieved with the ICMPv6 protocol.

ICMPv6 defines messages that inform the source of IPv6 packets of errors during packet delivery. It also defines the Echo Request/Reply messages that are used for basic network troubleshooting (ping command). ICMPv6 messages are transported on IPv6.

This document describes how basic OAM is performed on Low Power Wide Area Networks (LPWANs) by compressing

ICMPv6/IPv6 headers and by protecting the LPWAN network and the Device from undesirable ICMPv6 traffic.

詳細草案請參考：draft-barthel-lpwan-oam-schc-00
(https://tools.ietf.org/html/draft-barthel-lpwan-oam-schc-00)

14.RESTful Design for Internet of Things Systems

本文發表於物到物（Thing-to-Thing，t2trg）工作小組，草案摘要如下：

This document gives guidance for designing Internet of Things (IoT) systems that follow the principles of the Representational State Transfer (REST) architectural style. This document is a product of the IRTF Thing-to-Thing Research Group (T2TRG).

詳細草案請參考：draft-irtf-t2trg-rest-iot-02
(https://tools.ietf.org/html/draft-irtf-t2trg-rest-iot-02)

15.State-of-the-Art and Challenges for the Internet of Things Security

本文發表於物到物（Thing-to-Thing，t2trg）工作小組，草案摘要如下：

The Internet of Things (IoT) concept refers to the usage of standard Internet protocols to allow for human-to-thing and thing-to-thing communication. The security needs for IoT systems are well-recognized and many standardization steps to provide security have been taken, for example, the specification of Constrained Application Protocol (CoAP) secured with Datagram Transport Layer Security (DTLS). However, security challenges still exist, not only because there are some use cases that lack a suitable solution, but also because many IoT devices and systems have been designed and deployed with very limited security capabilities. In this document, we first discuss the various stages in the lifecycle of a thing. Next, we document the security threats to a thing and the challenges that one might face to protect against these threats. Lastly, we discuss the next steps needed to facilitate the deployment of secure IoT systems.

This document can be used by implementors and authors of IoT specifications as a reference for details about security considerations while documenting their specific security challenges, threat models, and mitigations.

This document is a product of the IRTF Thing-to-Thing

Research Group (T2TRG).

詳細草案請參考：draft-irtf-t2trg-iot-seccons-16
(https://tools.ietf.org/html/draft-irtf-t2trg-iot-seccons-16)

16.The Constrained RESTful Application Language (CoRAL)

本文發表於物到物（Thing-to-Thing，t2trg）工作小組，草案摘要如下：

The Constrained RESTful Application Language (CoRAL) defines a data model and interaction model as well as two specialized serialization formats for the description of typed connections between resources on the Web ("links"), possible operations on such resources ("forms"), as well as simple resource metadata.

詳細草案請參考：draft-hartke-t2trg-coral-08
(https://tools.ietf.org/html/draft-hartke-t2trg-coral-08)

量子網路（Quantum Internet）

本次會議 IRTF（Internet Research Task Force）的量子網路研究團隊（Quantum Internet Proposed Research Group，qirg）舉辦了講座，介紹了量子網路（Quantum Internet）的概念，架構以及實作技術，簡報內容可由下列網址下載：
https://datatracker.ietf.org/meeting/104/materials/slides-104-qirg-sessa-tutorial-on-quantum-repeaters-pdf-00

研究團隊並規劃在 108 年 9 月 5-6 日於日本舉辦 Workshop for Quantum Repeaters and Networks，歡迎有興趣者報名參加。

有關量子網路聯盟（Quantum Internet Alliance）相關資訊請參考網站：http://quantum-internet.team/

（二）參訪主辦單位 CZ.NIC

本次會議由 Cisco（思科）及 CZ.NIC 共同主辦，TWNIC 利用此次機會安排前往 CZ.NIC 參訪，並與 CZ.NIC CEO Ondrej Filip，CTO Zdenek Bruna，以及 Technical Fellow Jaromir Talir 進行交流，介紹台灣 TWNIC 及 TWCERT/CC 的運作狀況，並針對捷克在網域名稱註冊管理及資安防護運作等相關系統與主題交換意見。

CZ.NIC 財團法人是捷克.cz ccTLD 管理者，其主要活動是管理.cz 域名，確保.cz 頂級域名操作和域名的教育。該組織還運行 0.2.4.e164.arpa（ENUM）網域。

該協會的員工致力於推動 DNSSEC 技術項目，並開發網域管理系統和 mojeID 服務，推廣有利於捷克網路基礎設施的新技術。自 2011 年 1 月起，CZ.NIC 還負責維運國家安全團隊 National CSIRT (Cyber Security Response Team) Team，CSIRT.CZ。CSIRT.CZ 團隊也是 Trusted Introducer 和 FIRST 的會員。

CZ.NIC 成立一個學習中心 CZ.NIC 學院，並以 CZ.NIC Laboratories 品牌開展自己的研究。在實驗室中，它開發了用於開發網路基礎設施的原始工具，並分析了線上安全相關問題。 CZ.NIC 是 EURid 的成員，EURid 是管理歐洲 .EU 域名的組織，以及具有類似專業的其他國際公司（CENTR，ccNSO 等）的成員。

圖左至右：
Zdenek Bruna, CTO of CZ.NIC，Ondrej Filip, CEO of CZ.NIC，
TWNIC 丁綺萍副執行長，TWNIC 顧靜恆組長，以及
Jaromir Talir, Technical Fellow of CZ.NIC

（三）與中華民國駐捷克代表處科技組交流

科技部中華民國駐捷克代表處科技組推動中東歐八國雙邊與多邊科技研究合作相關事務，包括：捷克、斯洛伐克、匈牙利、波蘭、保加利亞、烏克蘭、羅馬尼亞及斯洛維尼亞。TWNIC 利用此次機會安排與中華民國駐捷克代表處科技組組長廖思善博士進行交流，介紹台灣 TWNIC 及 TWCERT/CC 的運作狀況，並針對捷克以及中東歐等國在網路基礎環境以及資安防護能量等相關議題進行交流討論。TWNIC 也很樂意提供相關經驗與歐洲各國分享。

圖左至右：TWNIC 顧靜恆組長，TWNIC 丁綺萍副執行長，科技部中華民國駐捷克代表處科技組組長廖思善博士

四、 建議意見：

<u>建議事項</u>

- ☐ 建議持續關注相關各 WGs 動態及相關訊息。
- ☐ IPv6 技術規範已有 IPv6-only 以及因應物聯網需求的草案提出，建議持續關注 IPv6 的相關技術規範發展，強化新一代網路基礎建設。
- ☐ 網路安全除了威脅研究外，在事件通報的技術規範上已有相關草案提出，建議持續關注 Security 的相關技術規範發展，以掌握資訊安全相關技術，並強化網路資訊安全的防護機制。
- ☐ 物聯網相關技術規範，廣泛地從架構，軟體，安全，應用，格式等

各方面都有草案提出，建議持續關注 IoT 的相關技術規範發展，以取得新一代網路應用技術，作為創新產業的基礎。

- ☐ 建議國內 ISP 持續積極投入 IPv6 的佈建，並加強與國際上其他 ISP 討論及分享佈建經驗。
- ☐ 建議與國外相關單位進行更密切及多元的交流及經驗分享。
- ☐ 建議持續參與 IETF 以掌握相關技術規範的演進及狀態。
- ☐ CZ.NIC 歡迎 TWNIC 共同參與開放原始碼的技術交流，並希望有機會推動人員互訪交流，增進彼此的技術能量。
- ☐ 中華民國駐捷克代表處科技組歡迎 TWNIC 在網路資訊及網路安全方面的專業，與捷克或中東歐各國有機會互相交流。

IETF 下一次會議將於 2019 年 7 月 20-26 日於加拿大蒙特婁 舉行，相關資訊請參考 https://www.ietf.org/how/meetings/105/。

五、 會議議程：

以下為 IETF 104 Prague 的完整議程表：

Saturday, March 23, 2019 (CET)	
時間	議程
8:30-22:00	IETF Hackathon
9:30-18:00	Code Sprint

Sunday, March 24, 2019 (CET)	
時間	議程
8:30-16:00	IETF Hackathon
10:00-12:00	IEPG Meeting
10:00-19:00	IETF Registration
12:30-13:30	Tutorial: How to Create an Internet-Draft Using XML or Markdown
12:30-13:30	Tutorial: Newcomers' Overview
13:45-14:45	Tutorial: GitHub Tools
14:00-16:00	RTG AD Office Hours
14:30-15:30	TSV AD Office Hours
15:00-16:00	Newcomers' Quick Connections (Open to Newcomers. Note that pre-registration is required)
16:00-17:00	Newcomers' Meet and Greet (Open to Newcomers, WG chairs and Mentors only)
17:00-19:00	Welcome Reception
18:00-20:00	Hot RFC Lightning Talks

Monday, March 25, 2019 (CET)	
時間	議程
8:00-9:00	Systers Networking Event
8:00-18:00	IETF Registration
9:00-11:00	
	Dispatch Joint with ARTAREA
	IPv6 Maintenance
	Privacy Enhancements and Assessments Proposed Research Group
	Network Configuration 09:00 - 10:00
	Network Modeling 10:00 - 11:00
	Bit Indexed Explicit Replication
	Common Control and Measurement Plane
	EAP Method Update
	IP Performance Measurement
11:00-11:20	Beverage Break
11:20-12:20	
	Calendaring Extensions
	IPv6 over the TSCH mode of IEEE 802.15.4e
	Network Management
	Operational Security Capabilities for IP Network Infrastructure
	Bit Indexed Explicit Replication
	Transport Layer Security
	RTP Media Congestion Avoidance Techniques
12:20-13:50	Break
13:50-15:50	
	Email mailstore and eXtensions To Revise or Amend 13:50 - 14:50
	JSON Mail Access Protocol 14:50 - 15:50
	Registration Protocols Extensions
	IPv6 over Networks of Resource-constrained Nodes
	IRTF Open Meeting
	Network Modeling
	Security Dispatch
	TCP Maintenance and Minor Extensions
15:50-16:10	Beverage and Snack Break
16:10-18:10	
	Stopping Malware and Researching Threats

	Hypertext Transfer Protocol
	Extensions for Scalable DNS Service Discovery
	Quantum Internet Proposed Research Group
	Inter-Domain Routing
	Routing Over Low power and Lossy networks
	Web Authorization Protocol
	Transport Area Working Group
18:30-20:00	Newcomers' Dinner
18:30-20:00	Hackdemo Happy Hour

Tuesday, March 26, 2019 (CET)	
時間	**議程**
8:00-18:00	IETF Registration
9:00-11:00	
	Email mailstore and eXtensions To Revise or Amend 09:00 - 10:00
	Using TLS in Applications 10:00 - 11:00
	Distributed Mobility Management
	Home Networking
	SIDR Operations
	Routing Area Working Group
	CBOR Object Signing and Encryption
	Trusted Execution Environment Provisioning
	QUIC
11:00-11:20	Beverage Break
11:20-12:20	
	DNS Over HTTPS
	Light-Weight Implementation Guidance
	Quantum Internet Proposed Research Group
	BNG Control-plane And User-plane SEparation BOF×
	Traffic Engineering Architecture and Signaling
	Limited Additional Mechanisms for PKIX and SMIME
	Managed Incident Lightweight Exchange
	Transport Area Working Group
12:20-13:50	Break
12:35-13:35	WG Chairs Forum (For WG Chairs Only)
13:50-15:50	
	Constrained RESTful Environments

	Network Time Protocol Joint with TICTOC
	Timing over IP Connection and Transfer of Clock Joint with NTP
	Autonomic Networking Integrated Model and Approach
	Domain Name System Operations
	Traffic Engineering Architecture and Signaling
	Interface to Network Security Functions
	Messaging Layer Security
	Transport Area Open Meeting
15:50-16:10	Beverage and Snack Break
16:10-18:10	
	Audio/Video Transport Core Maintenance
	IPv6 over Low Power Wide-Area Networks
	Thing-to-Thing
	Global Routing Operations
	BGP Enabled ServiceS
	Transport Layer Security
	Application-Layer Traffic Optimization
	Delay/Disruption Tolerant Networking

Wednesday, March 27, 2019 (CET)	
時間	**議程**
8:00-17:10	IETF Registration
9:00-11:00	
	Dynamic Host Configuration
	Decentralized Internet Infrastructure
	Bidirectional Forwarding Detection
	Deterministic Networking
	Routing In Fat Trees
	Security Events
	Software Updates for Internet of Things
	QUIC
11:00-11:20	Beverage and Snack Break
11:20-13:20	
	Captive Portal Interaction 11:20 - 12:20
	Multiparty Multimedia Session Control 12:20 - 13:20
	Crypto Forum 12:20 - 13:20
	Benchmarking Methodology

	Link State Routing
	Multiprotocol Label Switching
	Automated Certificate Management Environment 11:20 - 12:20
	Security Automation and Continuous Monitoring
	Multipath TCP
15:00-17:00	
	Technology Deep Dive - Modern Router Architecture
16:40-17:00	IETF Executive Director Office Hours
16:50-17:10	Beverage and Snack Break
17:10-19:40	IETF Plenary

Thursday, March 28, 2019 (CET)	
時間	**議程**
8:00-17:50	IETF Registration
9:00-10:30	
	Concise Binary Object Representation Maintenance and Extensions
	Path Aware Networking RG
	KSK Futures
	Babel routing protocol
	Link State Vector Routing
	Path Computation Element
	Messaging Layer Security
	Web Authorization Protocol
10:30-10:50	Beverage Break
10:50-12:20	
	GitHub Integration and Tooling
	Computing in the Network Proposed Research Group
	Measurement and Analysis for Protocols
	MBONE Deployment
	Inter-Domain Routing
	Network Virtualization Overlays
	DDoS Open Threat Signaling
	IP Security Maintenance and Extensions
12:20-13:50	Break
12:30-13:30	Systers Lunch
12:30-13:15	Host Speaker Series
13:50-15:50	

	Hypertext Transfer Protocol
	Predictable and Available Wireless
	Network Management
	Coding for efficient NetWork Communications Research Group
	IPv6 Operations
	Protocols for IP Multicast
	Source Packet Routing in Networking
	Security Area Open Meeting
15:50-16:10	Beverage and Snack Break
16:10-18:10	
	Brand Indicators for Message Identification
	Internet Area Working Group
	Human Rights Protocol Considerations
	Internet Congestion Control
	Operations and Management Area Working Group
	Link State Routing
	Service Function Chaining
	Remote ATtestation ProcedureS

Friday, March 29, 2019 (CET)	
時間	**議程**
8:00-12:00	IETF Registration
9:00-10:30	
	Constrained RESTful Environments
	Secure Telephone Identity Revisited
	IPv6 Maintenance
	Global Access to the Internet for All
	Domain Name System Operations
	Locator/ID Separation Protocol
	Collaborative Automated Course of Action Operations for Cyber Security
10:30-10:50	Beverage Break
10:50-12:50	
	DNS PRIVate Exchange
	IP Wireless Access in Vehicular Environments
	Information-Centric Networking
	Routing Area Working Group

	Authentication and Authorization for Constrained Environments
	Transport Services

『2019 Internet of Things World』出國報告

財團法人台灣網路資訊中心因公出國人員報告書 108年 5月31 日

報告人 姓　名	顧靜恆	服務單位及職稱	組長
出國期間	108/5/12-18	出國地點	Santa Clara, USA
出國事由	參加 2019 Internet of Things World		
報告書內容包含： 一、 出國目的 二、 會議行程 三、 考察、訪問心得 四、 建議意見 五、 會議議程			
授　權 聲 明 欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人： 顧靜恆 (簽章)		

註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。
附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

一、　出國目的：

Internet of Things World 世界物聯網會議從 2014 年開始舉辦論壇 Forum，到今（2019）年已經是第 6 屆，今年的會議在美國加州聖克拉拉會議中心舉辦，會議日期 5 月 13 日至 16 日共為期 4 天，由 Informa Telecoms & Media 主辦，DELL Technologies 冠名贊助，是全球物聯網（IoT）技術創新與產業界交流的重要平台。本次國際研討會議與展覽會，連結了在各業界從事物聯網實用化策略規劃、技術開發、實際佈建的專家，也是未來商機的起點。

今年的主題是 The Intersection of Industries and IoT Innovation，有 1 萬多位參與者，將政策專家，技術專家，開發人員和實際佈建者聯繫在一起，讓物聯網推向產業垂直生態鏈，使來自垂直產業生態系統和物聯網技術解決方案廠商聯合起來，通過物聯網實現產業的未來。

本次 2019 IoT World 有多項活動，除了 IoT World 研討會之外，還包括 IoT World 展覽會（Exhibition），新創公司後起之秀（Startup Elevate）展覽會，IoT World 開發者會議（Developers Conference），IoT World 黑客松（Hackathon），並且結合 Connected & Autonomous Vehicles 研討會一同舉行。

5 月 13 日至 14 日舉辦的 IoT World 黑客松（Hackathon），讓黑客與物聯網創新聯結，是本次物聯網世界開發者大會的一部分。本次黑客松挑戰的主題是：水，由於獲取和正確使用水對於農業的可持續性，增長和生計至關重要，黑客如何能夠發揮作用並找到解決這些問題的方法呢？

5 月 14 日至 16 日舉辦 IoT World 展覽會，展覽會場佔地 10 萬平方英呎，包含新興企業，超過 300 組的參展者攤位，展示為實現 IoT 夢想而設計的產品和服務，參展廠商包括物聯網晶片設計到應

用平台整個生態系統（Ecosystem），依據大會統計約有 1 萬 2,500 人次 IoT 領域專家前來參加，在會場接觸使用創新技術的解決方案，是觀察 IoT 最新動向的寶貴機會。

本次展覽會中特別規劃新創公司後起之秀區（Startup Elevate），本區域是獨特的新興企業輔助計畫與社群，以橋接特定投資人及相關業界與最具潛力的創新後起之秀。本次 Startup Elevate 特別由台灣科技部的國際科技創業基地（Taiwan Tech Arena，TTA）所贊助。

(1)

(2)

圖：TWNIC 顧靜恆組長於 IoT World 展覽場之 (1) Startup Elevate 會場 (2) Ecosystem Center Stage 會場

5 月 15 日至 16 日舉辦 IoT World 開發者會議 (Developer Conference)，重點在技術面，是以從事 IoT 解決方案開發的開發者、硬體技術人員、設計人員為對象的活動，在 2 天會期中舉行，包括世界主要企業的主管或開放原始碼專案負責人演講，可以收集到要成功開發 IoT 相關技術時的相關資訊。

圖：(左至右)TWNIC 顧靜恆組長與 IoT World 開發者大會主席 Joe Maglitta, Principal at Maglitta Communications 合影

今年 IoT World 還結合與 Connected & Autonomous Vehicles 研討會同時舉行，透過汽車業界與 IoT 的相遇，讓可以自由選擇使用電動化、自動化交通方式的時代即將來臨。此外藉由一併舉行展覽會，不只是汽車業界，也讓許多其他業界的專家齊聚一堂，針對 Connected Car 和自動駕駛汽車的實用化進行熱烈討論。

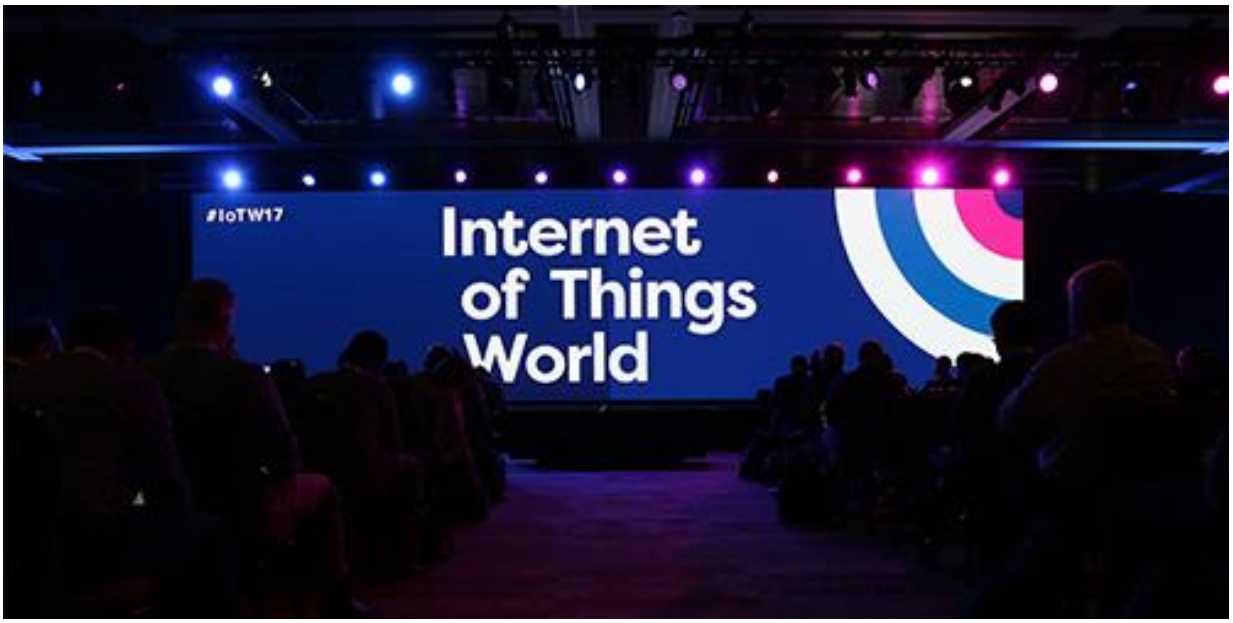
由於物聯網的應用非常廣泛，包括航空航天（Aerospace & Aviation），農業（Agriculture），汽車/運輸（Automotive/Transport），醫療保健（Healthcare），工業/製造（Industrial/Manufacturing），供應鏈與物流（Supply Chain & Logistics），智慧城市（Smart Cities），零售（Retail），能源與公用事業（Energy & Utilities），智慧建築（Smart Buildings），保險（Insurance），金融（Finance）等等。

本次世界物聯網研討會議場次共有 12 個分項，分別為

(1) 製造業（Manufacturing），
(2) 智慧建築與能源管理（Smart Buildings & Energy Management），

(3) 能源與資源生產（Energy and Resource Production），
(4) 智慧城市（Smart Cities），
(5) 連網消費品（Connected Consumer），
(6) 連網與自動駕駛汽車（Connected & Autonomous Vehicles），
(7) 物聯網連接（IoT Connectivity），
(8) 人工智能與機器學習（AI & Machine Learning），
(9) 開發人員會議：建構與佈署（Developers Conference: Build & Deploy），
(10) 供應鏈與物流（Supply Chain & Logistics），
(11) 物聯網安全（IoT Security），
(12) 邊緣計算（Edge Computing）等。

研討會詳細議程請參閱：
http://www.giievent.tw/itmc681315/agenda1.shtml。



圖：Internet of Things World 研討會場

圖：主辦單位 Informa Tech Maggie Miller 開幕致詞

2019 IoT World 贊助及參展廠商名錄：
http://www.giievent.tw/itmc681315/sponsors.shtml。

圖：IoT World 活動贊助廠商

二、 會議行程：

詳如 2019 IoT World 會議網站：
http://www.giievent.tw/itmc681315/。
2019 IoT World 議程：
http://www.giievent.tw/itmc681315/agenda1.shtml。
2019 IoT World Hackathon 網站：
https://iotworldhack.bemyapp.com/。

參與會議的行程安排如下表列：

日期	議程
108/5/13 (一)	Hackathon
108/5/14 (二)	Hackathon
	Exhibition Opening & Booth Crawl
	Silicon Valley AgTech Startup Pitch off
	Hackathon Pitch off Finals
108/5/15 (三)	Analyst Breakfast Briefings
	Keynotes
	Industry Vertical Networking
	Developers Conference: Build & Deploy
	IoT Connectivity - 5G & LPWAN
	Industry Vertical Exhibition Tours
	Startup Elevate Pitch offs
	Insider Session Workshops
108/5/16 (四)	Analyst Breakfast Briefings
	Keynotes
	Industry Vertical Networking
	Developers Conference: Build & Deploy
	IoT Security
	Industry Vertical Exhibition Tours
	Startup Elevate Pitch offs
	Insider Session Workshops

三、 考察、訪問心得：

（一）IoT World 會議及展覽會

本次會議參加廠商包括整個物聯網從晶片設計到應用平台的生態系統（Ecosystem），包括許多國際知名公司以及來自台灣的新創公司，以下針對幾個主要的公司及展示攤位做介紹，包括：(1)科技部國際科技創業基地（Taiwan Tech Arena，TTA），(2)研華科技（Advantech），(3)Amazon Web Services，(4)AT&T，(5)DELL Technologies，(6)IBM Watson，(7)MongoDB，(8)Software AG，(9)STMicroelectronics，(10)T-Mobile，(11)Verizon，(12)Wireless Communications Alliance，(13)UrsaLeo 等。

(1) 科技部國際科技創業基地（Taiwan Tech Arena，TTA）

科技部國際科技創業基地（Taiwan Tech Arena，TTA）由台灣科技部 (Ministry of Science and Technology，MoST) 根據前瞻基礎建設計畫成立。TTA 是一個技術創新和創業中心，將學術，研發人才，新創公司，國際加速器，企業和投資者聯繫在一起，實現一個串連技術、資金與國際交流的平台，以協助新創團隊的成功為最終目標。TTA 領導著名的台灣創業公司每年參加全球展覽，以協助他們連接全球市場和資本。

TTA 今年帶了七個團隊到場展演，包括手勢感測技術的酷手科技（Coolso）、IoT 設備能源解決方案供應商美商川盛科技（SWR Technology）、大數據加速處理平台偉薩科技（Waisa Technology）、企業與內部員工溝通 AI 機器人台灣易邁捷（Imageous Roby）、兒童語言治療輔助平台啟兒寶（PenguinSmart）、手機轉化即時麥克風簡報筆（Uniqcue）、幫助分析師及數據工作者建立模組的行動貝果（Mobagel）。分別介紹如下：

圖：國際科技創業基地（Taiwan Tech Arena，TTA）展示攤位

Coolso 公司開發了一種擁有自己專利技術的新型人機界面，用於可穿戴手勢控制和康復解決方案，詳細介紹請參閱：http://www.coolso.com.tw/。

圖：Coolso 展示攤位

SWR Technology 公司是 AIOT 世界中，智能設備的創新型中

長距離無線電源解決方案提供商，其技術可以減少電池使用量，從而更好地保護環境，並改變商業，工業或消費類應用中電力的供應，詳細介紹請參閱：https://www.swrtec.com/。

Wasai Technology 公司提供了基於 FPGA 卡的大數據加速平台，其解決方案包括 Apache Hadoop 和 Apache Spark 系統，用於大數據領域和生物醫學領域下一代序列的二級分析，詳細介紹請參閱：https://www.wasaitech.com/。

(1) (2)

圖：(1) SWR Technology 展示攤位 (2)Wasai Technology 展示攤位

Imageous' Roby 公司的 Roby 是一款支援聊天/語音的軟體，可處理所有請求，自動執行重複性任務，消除錯誤溝通，並縮短問題解決時間，提高員工滿意度，是唯一的會話 AI 服務中心，通過聊天或語音為員工提供單一的人機界面，詳細介紹請參閱：https://tellroby.com/。

PenguinSmart 公司幫助家長在家中提供有效的語言復健，其建立線上平台，提供早期治療諮詢。通過專家洞察和 AI 機器學習，

建立個性化的數據平台，實現“以家庭為中心”的早期治療模式，詳細介紹請參閱：https://www.mypenguinsmart.com/。

Uniqcue 公司希望改變我們觀看所有現場活動和媒體的方式，它用最明顯的替代品，我們的手機，取代傳統的麥克風和點擊，詳細介紹請參閱：http://uniqcue.com/。

Mobagel 行動貝果公司為企業打造 AI 數據分析系統，其 Decanter AI 提供快速、容易使用、準確、高解釋力的自動化機器學習，詳細介紹請參閱：https://mobagel.com/tw/。

(2) 研華科技 Advantech

隨著無線應用成為首選解決方案，研華推出了各種無線傳感設備，並一直保持物聯網傳感技術的領先。通過利用低功耗廣域網（LPWAN）和蜂巢式（Cellular）技術，研華科技的 WISE 系列可以成為室內和室外能源和環境監測應用的理想解決方案。 此外，通過提供各種雲平台連接以及支援 MQTT 和 CoAP 協定，WISE IoT 傳感設備可以促進和簡化物聯網時代的大數據採集應用。

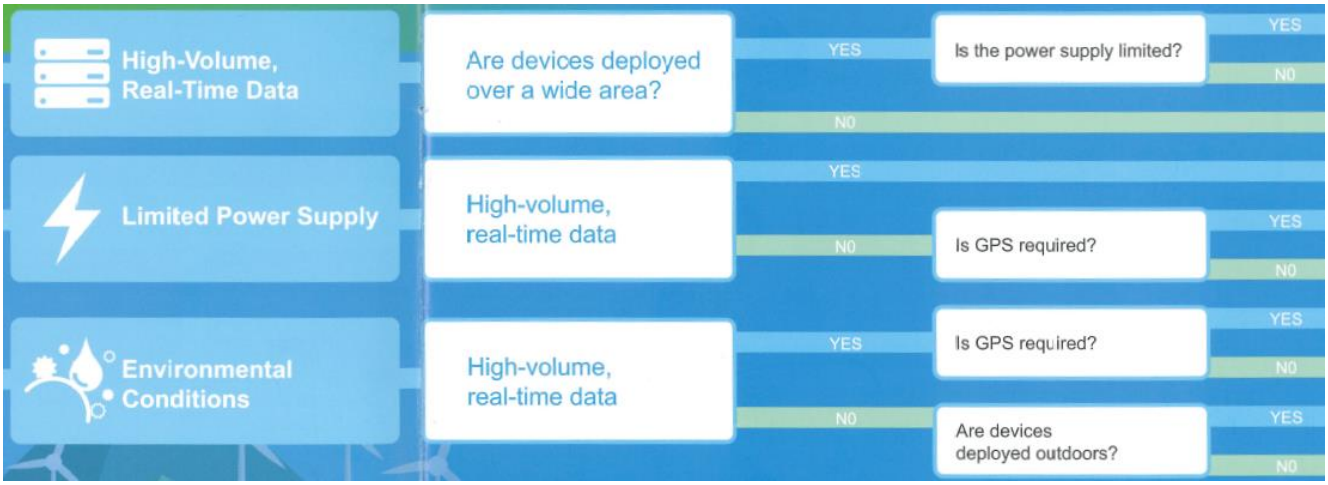
研華科技實踐了物聯網輕量級設備到雲端之架構，研華的綜合傳感設備支持多種物聯網通信協議，如 MQTT 和 RESTful，允許終端傳感器數據直接傳遞到雲端。這簡化了用於在物聯網應用中連接設備到雲解決方案的系統架構，同時降低了各個站點的系統構建成本。架構示意圖如下：

研華科技在物聯網相關的產品包括 WISE IoT 傳感設備 (Sensing Devices)，設備到雲端解決方案，以及無線 I/O 模塊 (I/O Module)。WISE IoT 無線 I/O 模塊包括有：WiFi，LPWAN(Low-Power Wide-Area Network)，LoRa，LoRaWAN，NB-IoT(Narrow Band IoT)，及 3G 等。

IoT 傳感設備作為大數據資料傳感的主要來源，在實現 IoT 系統中起著關鍵作用。為了獲得不同 IoT 應用的不同類型的數據，傳統的自動化架構和基本的數據採集已不再足夠，研華開發了 WISE-4000 系列無線傳感器節點（Wireless Sensor Node，WSN）。利用最新的 IoT 概念和技術，WISE-4000 是一個雲端數據傳感和通訊的工具，可以幫助實現 IoT 系統。應用範例包括：工廠環境，機房，食品和飲料產品線，倉庫，數據中心，水處理，農業，可再生能源等。其導入的 IoT 和大數據的相關技術包括，Cloud Integration，Modbus，RESTful，MQTT Protocol，以及 Wireless Communication 等。

研華提出在規劃要採用哪一類 IoT 產品時，需要考量幾個問題，

如下圖所示，再選擇適合的傳感設備。



WISE Wireless IoT Sensing Devices 詳細介紹請參閱：http://select.advantech.com/wise-iot-sensing-devices/。

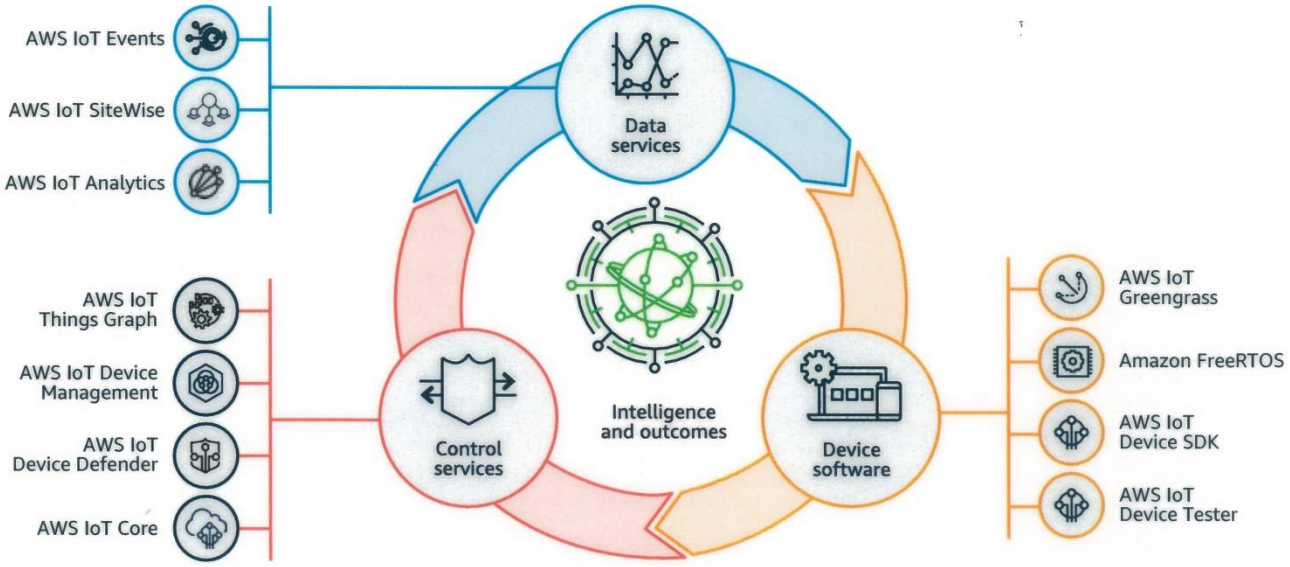
圖：研華科技 Advantech 展示攤位

(3) 亞馬遜公司 AWS

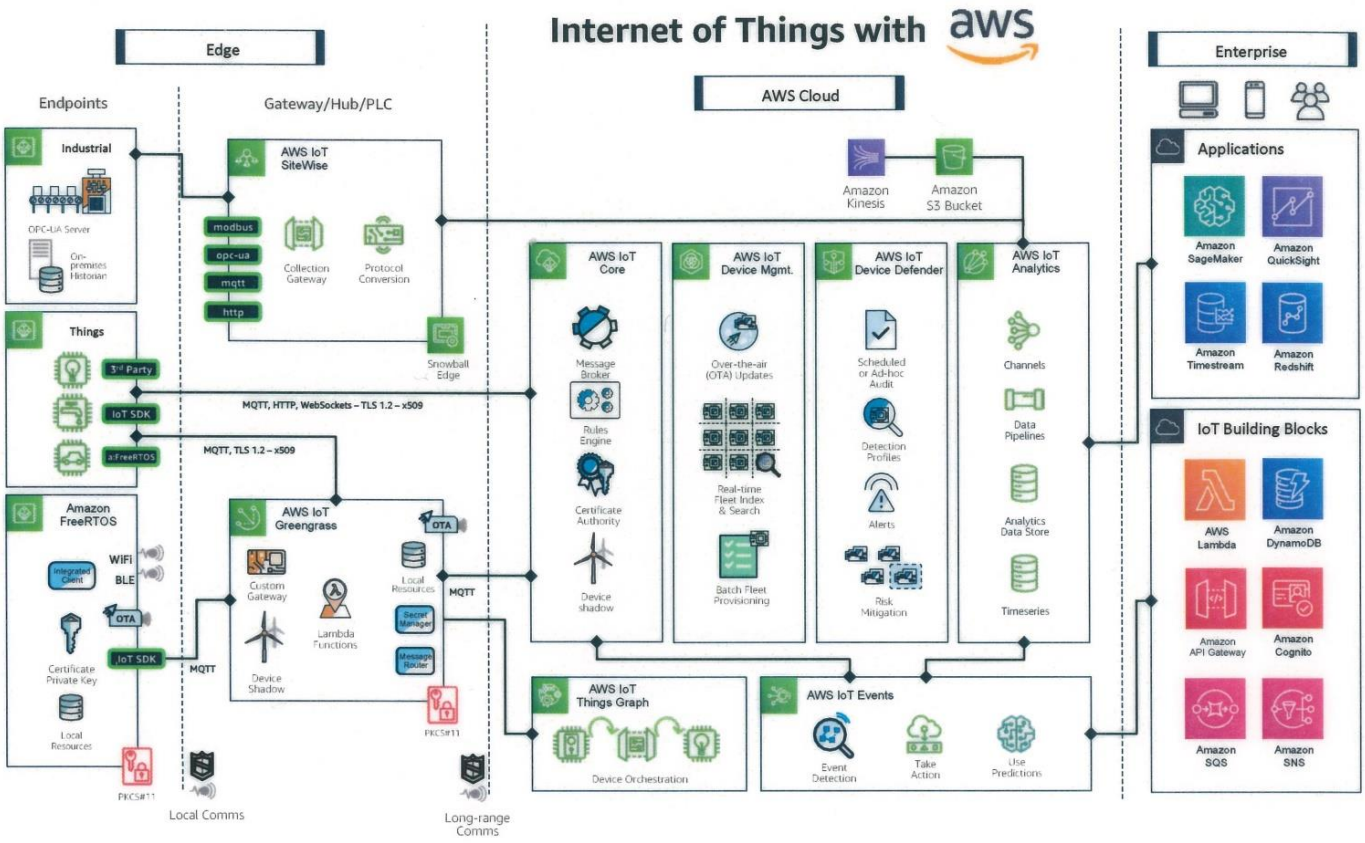
Amazon Web Services (AWS) 是全球最全面和廣泛採納的雲端平台，提供來自全球資料中心超過 165 多項功能完整的服務。

AWS IoT 是用於工業、消費者和商業解決方案的 IoT 服務。由於 AWS IoT 與多種 AI 服務整合，因此即使無法連接網際網路也能讓裝置變得更聰明。AWS IoT 建構在 AWS 雲端上，可隨著裝置數量的增加和業務需求的變化輕鬆擴展。AWS IoT 還提供最全面的安全功能，建立預防性安全政策並對潛在的安全問題立即採取行動。

AWS IoT 提供廣泛而深入的功能，跨越雲端，可以在各種設備上為幾乎任何案例建構物聯網解決方案。AWS IoT 架構所提供的解決方案如下圖所示，包含 Data Services，Device Software，以及 Control Services 等三個面向。



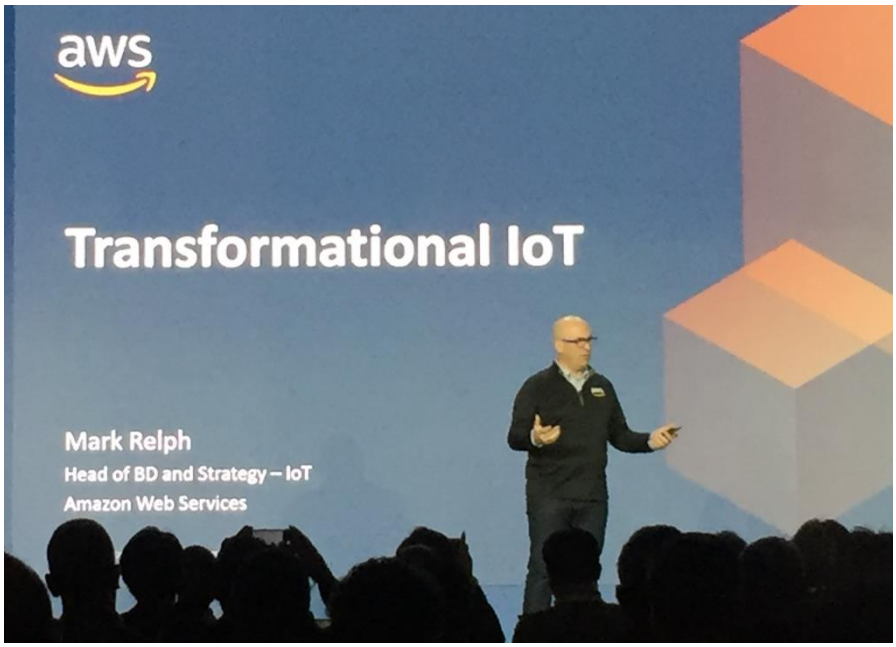
AWS IoT 的運作分三個層次，分別為 Edge，AWS Cloud，以及 Enterprise，其運作的關聯圖如下：



本次會議 Amazon Web Services Principal Solutions Architect of IoT 的 Craig Williams 在物聯網世界開發者大會，以 IoT Best Practices & Architecture 物聯網架構的最佳實踐為主題發表了演講。

此外，Amazon Web Services Head of BD and Strategy of IoT 的 Mark Relph 以 Transformational IoT 為主題於大會發表了專題演講，Mark Relph 如下圖所示：

AWS IoT 詳細介紹請參閱：https://aws.amazon.com/tw/iot/。
AWS IoT Atlas 詳細介紹請參閱：https://iotatlas.net。

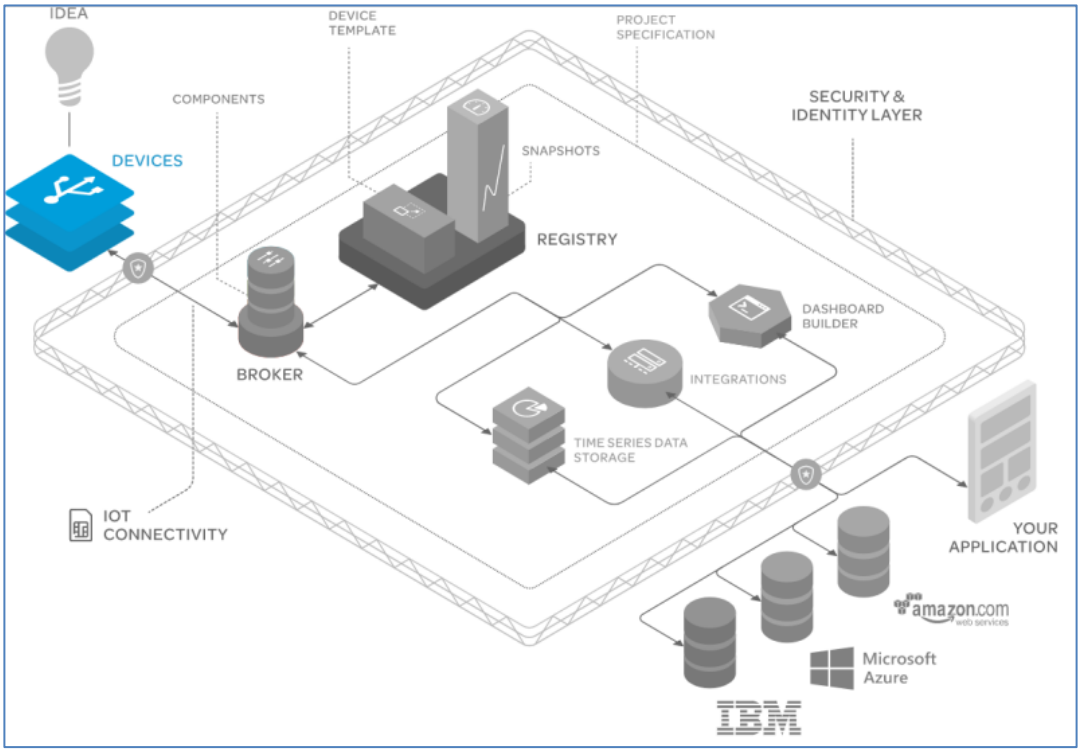


圖：Mark Relph, Amazon Web Services 介紹 Transformational IoT

圖：AWS 展示攤位

(4) AT&T

AT&T IoT 平台服務提供可擴展，快速的解決方案開發平台，由緊密集成的組件組成，包含 Data Flow 基礎設施，設備和設備適配器（Adapter），物聯網連接和管理等，其服務架構如下圖所示：



圖：AT&T 物聯網平台 DataFlow Infrasturecuture

AT&T IoT 平台服務提供全球連接和管理，設備服務，數據協作，數據可視化，解決方案自動化等服務。全球連接和管理方面，利用無縫購買，配置和管理設備的 SIM 卡，利用 AT&T LTE-M 網路實現低功耗蜂窩網路連接，以及 AT&T 全球 SIM 卡連接，從而提供更高的可靠性，安全性和移動性。設備服務方面，提供面板，監控和管理您的設備，消息和部署。數據協作方面，提供在任何地方可路由，轉換和儲存您的數據，並使用全面的 IoT Platform API 構建您的應用系統。數據可視化方面，提供在可自行定義的物聯網儀表板中聚合，比較和跟踪您的設備數據，以獲得對您的設備的即

時觀察。解決方案自動化方面，使用規則引擎在業務流程中，讓行業垂直解決方案模組來識別事件並觸發操作和通知。

利用 AT&T 物聯網平台的應用實例如：智能水錶，用以控制和改善用水量；連線冰箱，用以遠距冰箱管理；車輛解決方案，利用位置跟踪，路線優化和預測性維護來改進流程並降低成本；資產管理，在地理感知儀表板上管理全球分佈式資產，該儀表板顯示即時診斷數據和事件驅動通知。

AT&T IoT Platform 詳細介紹請參閱：https://iotplatform.att.com/。

AT&T IoT Platform 車輛解決方案應用展示請參閱：https://iotplatform.att.com/solutions/vehicle-solutions。

AT&T IoT Platform 資產管理應用展示請參閱：https://iotplatform.att.com/solutions/asset-management。

(5) DELL Technologies 戴爾技術

戴爾技術物聯網部門通過將 IoT 物聯網（Internet of Things）轉變為 IQT(IQ of Things)來推動人類進步，讓事物變得更有智慧，提供智能的物聯網。人工智能（AI）和機器學習技術與物聯網基礎設施協同工作，提供更智能，更具預測性的系統。戴爾技術認為人工智慧與物聯網必須被視為跨邊緣（Edge）、核心（Core）與雲端（Cloud）的單一相依生態系統（Ecosystem）。

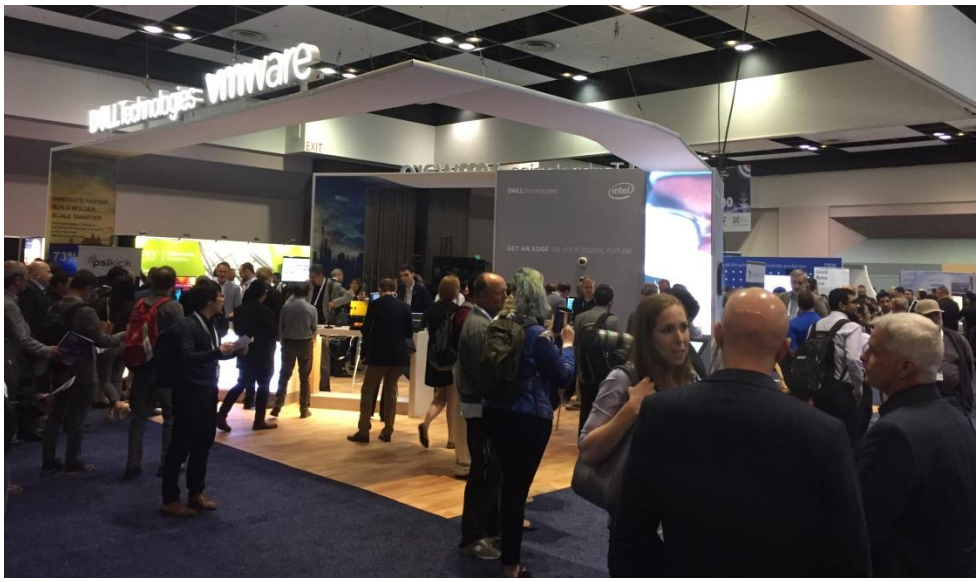
戴爾技術物聯網方案中邊緣、核心、雲端，然後返回的概念，目的是要能充分發揮物聯網的潛能，需要將智慧新增至每個階段。在邊緣更聰明地收集資料、在核心更聰明地運算，以及雲端運算階段更深入地學習。將所有情報加總並送回邊緣，提升物聯網的 IQ，並推動全新境界的組織創新。

戴爾客戶可以利用跨越網路，數據中心和雲的分析方案，實現

分析驅動的行動。戴爾產品組合，藉由合作夥伴生態系統，垂直和領域專業知識以及協作方式，提供端到端的物聯網解決方案。為了啟動物聯網順利運作，戴爾以內嵌個人電腦和 Edge Gateway 連接未互聯的裝置。

戴爾的邊緣分析方案 Dell Edge Gateway 系列旨在聚合，保護和中繼來自各種傳感器和設備的數據，讓資訊隨手可得：從位於 IoT 網路邊緣的有線與無線感應器收集、彙總及處理資料，提供即時的回應，並將有意義的資料轉送至後端系統。其使用案例包括：遠端資產監控、預測性維護、能源管理、重要基礎建設管理、冷凍設備監控、監視系統及智慧型農業等。

DELL IoT 解決方案詳細介紹請參閱：https://www.delltechnologies.com/zh-tw/what-we-do/iot/index.htm 及 https://www.dell.com/learn/us/en/555/oem/oem-internet-of-things。



圖：DELL 展示攤位

(6) IBM Watson IoT Platform

IBM 認為物聯網提供數據，AI 啟動這些數據的涵義。利用 AI

和IoT的結合可釋放數據的力量,創新資產管理,優化房產和設施，改進軟體和系統工程，推進數位轉型。

IBM Watson IoT Platform（物聯網平台）提供安全地連接，管理物聯網環境和分析物聯網數據。此平台是雲端託管服務，旨在簡化從物聯網設備中獲取價值的過程,專門設計用來協助輕鬆從物聯網裝置中衍生價值。

Watson IoT 平台，可以快速，輕鬆地安全地連接，收集和開始處理物聯網數據。由於它使用 IBM Cloud，因此可以快速擴展和適應不斷變化的業務需求，而不會影響安全性，隱私或風險級別。

IBM Watson 認為從物聯網數據中獲取最大價值的四個步驟，第 1 步：收集數據（Gather data），第 2 步：樣態可視化（Visualize patterns），第 3 步：推進分析（Advance to analytics），第 4 步：注入人工智能（Infuse with Artificial Intelligence）。

IBM Watson IoT 探索應用服務的重點包括工業設備,建築物，車輛,以及民用基礎建設。其解決方案的重點之一是企業資產管理（Enterprise asset management，EAM），包括核心企業資產管理（Core enterprise asset management），資產績效管理（Asset performance management），生產優化（Production optimization），生產質量洞察（Production quality insights），工人安全洞察（Worker safety insights）等方面。通過為營運增加分析，讓物聯網和人工智慧的強大功能，降低風險，降低成本並提高效率

本次會議 IBM David Meek 以關於未來智慧工廠的主題發表了演講，介紹未來智慧工廠中 AI 如何改變製造業，David Meek 的演講如下圖所示：

圖：David Meek, IBM Watson 介紹未來智慧工廠中 AI 如何改變製造業

此外，IBM Watson IoT Advocacy 的 CTO John Walicki，在物聯網世界開發者大會上發表演講，主題是 From Sensors to Insights with Watson IoT Applying AI to IoT Data 從傳感器到內涵：將 AI 應用於物聯網數據，展示關於開發人員如何在幾分鐘內完成物聯網營運和財務上的價值。

John Walicki 現場操作 IBM Watson 物聯網平台，帶領與會者進行快節奏的旅程，從追踪物聯網傳感器數據的產生到邊緣網關進行分析，經由加密，到雲端，Watson IoT，Node-RED 處理，雲存儲，Watson Studio，Jupyter 電腦中的 Apache Spark 分析，PixieDust 可視化和機器學習算法等步驟。所有處理過程都是即時的！John Walicki 的演講如下圖所示：

圖：John Walicki, CTO, IoT Advocacy, IBM Watson 在物聯網世界開發者大會介紹從傳感器到內涵：將 AI 應用於物聯網數據

IBM Watson IoT 詳細介紹請參閱：https://www.ibm.com/internet-of-things。

IBM Watson 物聯網平台解決方案詳細介紹請參閱：https://www.ibm.com/internet-of-things/solutions/iot-platform 及 https://www.ibm.com/tw-zh/marketplace/internet-of-things-cloud。

IBM Cloud 試用請參閱：https://console.ng.bluemix.net/registration/?target=/catalog/services/internet-of-things-platform。

圖：IBM 展示攤位

(7) MongoDB

MongoDB 提供企業物聯網數據平台。由於沒有兩個物聯網解決方案完全相同，從邊緣到雲，MongoDB 是技術決策者，架構師和開發人員的理想合作夥伴。

使用 MongoDB 進行物聯網，可以存儲任何類型的數據，即時分析，並在樣態發生時更改模型。其特點如下：

新設備和數據：MongoDB 的文檔模型能夠存儲和處理任何結構的數據：事件，時間序列數據，地理空間坐標，文本和二進制數據以及其他任何內容。您可以通過添加新字段來調整文檔架構的結構，從而使處理 IoT 應用程序生成的快速變化數據變得簡單。

水平可伸縮性：MongoDB 的自動分片功能可以跨商品服務器分發數據，具有完整的應用程序透明性。有多種擴展選項，包括基於範圍，基於散列和區域共享，MongoDB 每秒可以支持數千個節點，數 PB 的數據和數十萬個操作，而無需建構自定義分區和緩存層。

就地分析：憑藉其豐富的索引和查詢支持，包括輔助，地理空

間和文本搜索索引，聚合框架和 Apache Spark 的本機支持，MongoDB 可以針對傳感器數據就地運行複雜的臨時或報告分析。

安全：強大的身份驗證，授權，審核和加密控制可保護有價值的傳感器數據及其提供的分析。

本次會議 MongoDB 的 Product Marketing Manager Robert Walters 在物聯網世界開發者大會，以探索物聯網數據的發展與挑戰發表了演講。

MongoDB IoT 詳細介紹請參閱：https://www.mongodb.com/use-cases/internet-of-things。

MongoDB Atlas 雲端服務詳細介紹請參閱：https://www.mongodb.com/cloud/atlas。

圖：MongoDB 展示攤位

(8) Software AG

Software AG 的 Cumulocity IoT，是開放、獨立、與設備無關的（device agnostic）平台，支援多種預整合設備（pre-integrated device）和多種工業協議（industrial protocol），以確保快速、輕鬆與任何事物的安全連線。

Software AG 藉由提供易於使用的 IoT PaaS 讓客戶能專注於其創新和差異化，以實現業務的數位轉型。企業若使用 Cumulocity IoT 就能迅速從有限規模的雲端 IoT 項目開始，隨著複雜性不斷成長建立與其一起成長的 IoT 平台和服務。

Cumulocity IoT 的獨特之處在於它提供了 IoT 即服務（IoT-as-a-Service）解決方案，其中包括增強的高可用性和多叢集部署（multi-cluster deployment）選項。此外，Cumulocity IoT 還包括多種營運商級功能，包括支援 LPWAN、用於長期低頻寬遠程監控的設備的無程式碼整合，如 NB-IoT、LWM2M 和 LoRa 等。

Software AG IoT 解決方案詳細介紹請參閱：https://www.softwareag.com/corporate/products/internet_of_things/default.html。

圖：Software AG 展示攤位

(9) STMicroelectronics 意法半導體

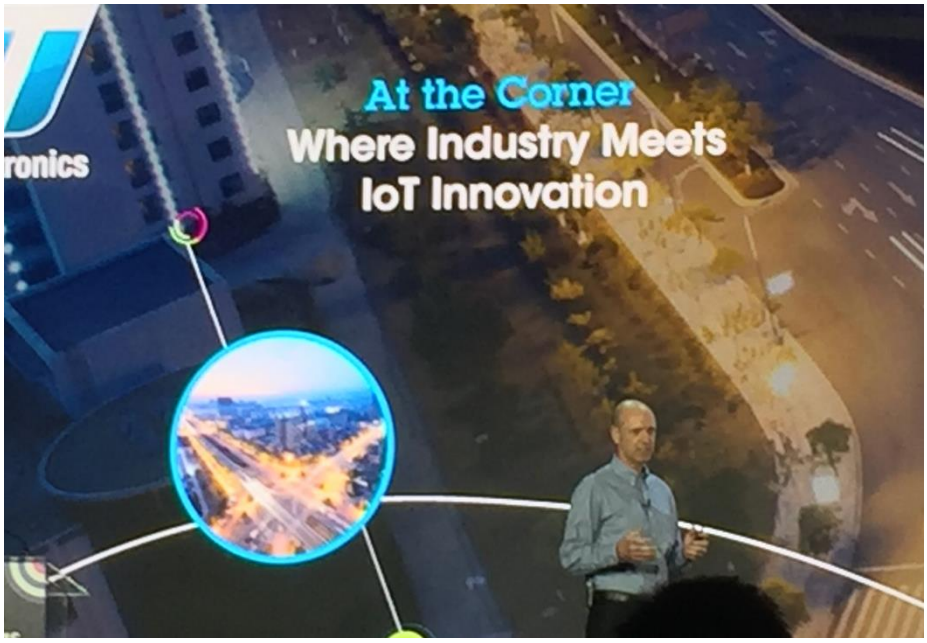
意法半導體（STMicroelectronics）是一家國際性的半導體生產商，總部位於瑞士日內瓦。本次會議舉辦了一場實作工作坊，主題是 Bluetooth Low Energy 5.0 and 802.15.4 Made Easy with the STM32WB。雙核，多協議無線 STM32WB55 微控制器基於 64 MHz 運行的 Arm® Cortex® -M4 內核（應用處理器）和 32 MHz 的 Arm® Cortex® -M0 +內核(網絡處理器)，支持 Bluetooth™5 和 IEEE 802.15.4 無線標準。

STM32WB55 微控制器得益於這兩個完全獨立的內核，這種創新架構針對實時執行（無線電相關軟件處理）以及靈活的資源使用和電源管理進行了優化，從而降低了 BOM 成本並提供了更好的用戶體驗。STM32WB 系列採用與我們的超低功耗 STM32L4 微控制器相同的技術開發，提供相同的數字和模擬外設，適用於需要延長電池壽命和復雜功能的應用。

無線連接方面經過Bluetooth™5認證的STM32WB55微控制器可支持 Mesh 1.0 網絡，多種配置文件以及集成專有 BLE 堆棧的靈活性。通用 IEEE 802.15.4 MAC 層確保 STM32WB55 可以運行專有協議或堆棧，包括 ZigBee 和 Thread 低功耗網狀網絡協議，為設計人員提供了更多選項，可將設備連接到物聯網（IoT）。此外，這些超低功耗 32 位微控制器可同時運行 Bluetooth™5 和 802.15.4 無線協議。STM32WB 相關資訊請參閱：http://st.com/STM32WB。

本次會議 STMicroelectronics 的 VP IoT Strategy Tony Keirouz 以 Embedded Intelligence for the Next Wave of Smart Systems - Opportunities and Challenges on the Edge 為主題發表了演講，介紹邊緣運算的機會和挑戰，Tony Keirouz 如下圖所示：

STMicroelectronics 詳細介紹請參閱：https://www.st.com/。



圖：Tony Keirouz, STMicroelectronics 介紹邊緣運算的機會和挑戰

圖：STMicroelectronics 意法半導體展示攤位

(10) T-Mobile

T-Mobile 主要針對物聯網的應用提供合適的網路服務。T-Mobile 針對物聯網提供多元網路產品組合以支持廣泛的應用案利。從最簡單的傳感器到大部分數據密集型系統，T-Mobile 都有適合需求的網路。例如：5G，NB-IoT，CAT-1，及 4G LTE 等。

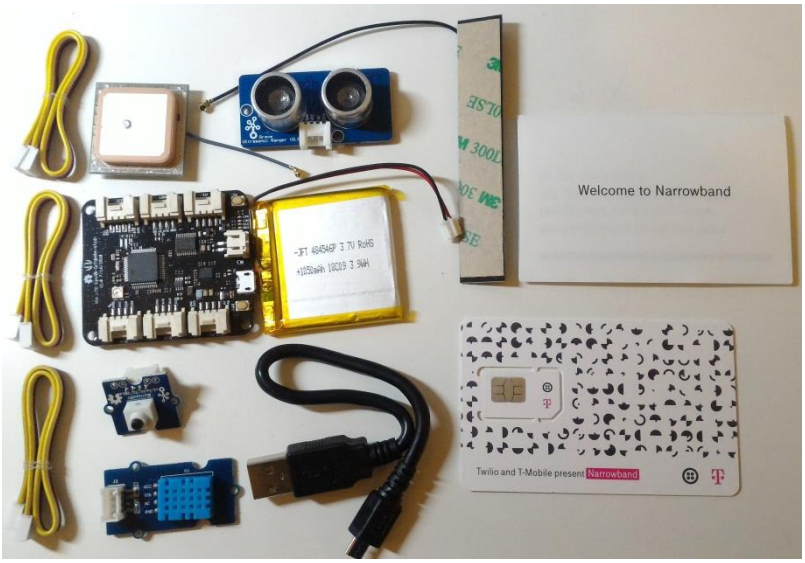
T-Mobile 佈署 5G 網路使用多個頻段-mmWave 和 600 MHz，實現全國範圍的移動性。NB-IoT 網路在現有網路的專用保護頻段上運行，可以有效地傳輸數據，而不會與其他網路流量競爭，是低頻寬和長電池壽命的物聯網解決方案。對於智能建築，互聯城市，資產跟踪等，是一個出色的解決方案。CAT-1 網路使用全頻譜的低頻段，中頻段和高頻段，因此語音和數據會不斷優化以提高效率，有助於控制業務成本並保持速度。4G LTE 網路提供工業標準，為物聯網業務提供前沿技術。而且，T-Mobile 繼續擴展 LTE 範圍，為 5G 奠定基礎。

T-Mobile 網路也和合作夥伴提出多種解決方案，應對各種垂直行業，為各行各業提供真正的商業價值。列舉下列幾項解決方案，包括：資產追踪（Asset Tracking），智慧城市（Smart Cities），智能建築（Smart Buildings）及車隊（Fleet）等。資產追踪通過窄帶物聯網（NB-IoT）使監控資產比以往更簡單，更強大。智慧城市從智能街道照明到複雜的公共安全系統，提供優化的網路。智能建築連接和集中傳感器，控制器，安全攝影機以及全國幾乎任何類型的設備。車隊在院子裡或在路上，藉由全國性網路幫助定位和監控您的所有車輛。

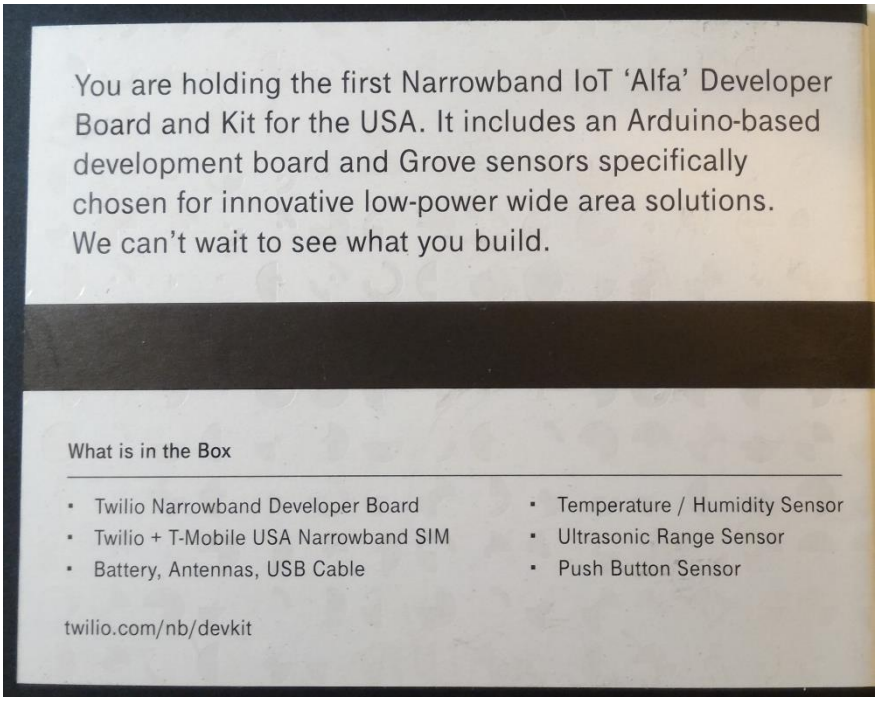
本次會議 T-Mobile 的 Senior Director of Leading IoT Technology Mesut Guven 在物聯網世界開發者大會，以通過 NB-IoT 實現創新為主題發表了演講。

圖：T-Mobile Mesut Guven 介紹通過 NB-IoT 實現創新

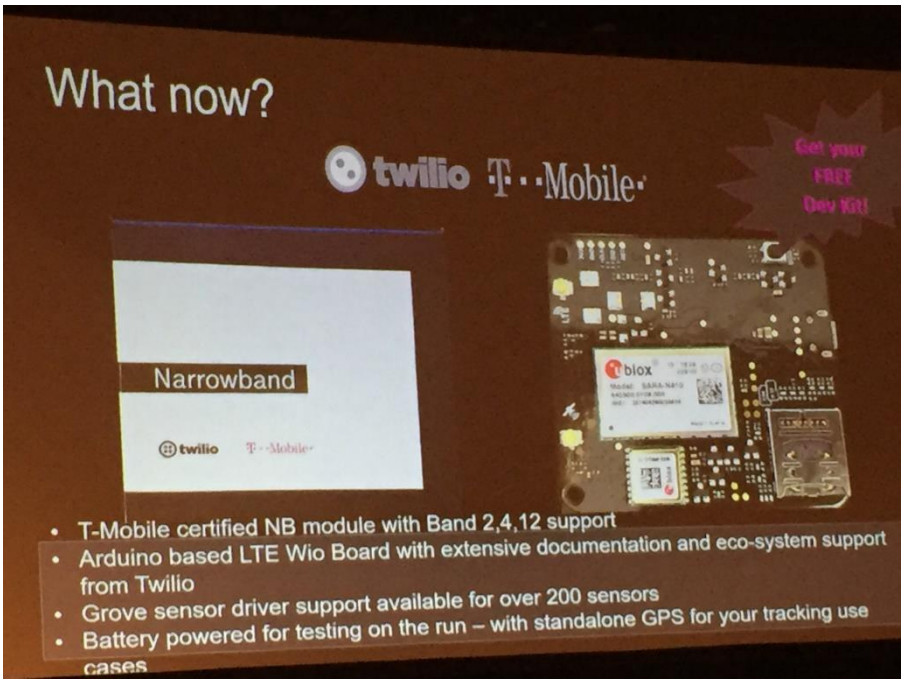
此外，T-Mobile 提供與會者 Narrowband IoT ‘Alfa’ Developer Board and Kit for the USA，此支援 NB-IoT 的 IoT 開發套件盒內容及說明如下圖所示：



圖：T-Mobile Narrowband IoT ‘Alfa’ Developer Board and Kit 開發套件內容



圖：T-Mobile Narrowband IoT 'Alfa' Developer Board and Kit 開發套件說明



圖：T-Mobile Narrowband Board 規格

T-Mobile IoT 詳細介紹請參閱：https://iot.t-mobile.com/。

(11) Verizon

Verizon 為所有物聯網產品提供連接解決方案，從工業和消費產品到車輛和建築物，讓一切工作都更加安全，高效和經濟。Verizon 不僅僅專注於提供連接,還創建了 Verizon 開放開發計畫，旨在允許和鼓勵開發社群創建新產品，應用程序和服務。

Verizon 物聯網解決方案 ThingSpace，是物聯網開發平台，此集中開發和管理解決方案，幫助物聯網生態系合作夥伴，如企業和原始設備製造商，進行創建，測試，連接，並將物聯網創意推向市場的物聯網平台。

Verizon 的物聯網應用之一是著重在實踐智慧城市和社區，其中應用包括：智慧照明（Intelligent Lighting）、智慧交通流量管理（Intelligent Traffic Management）、交通數據服務（Traffic Data Services）、交叉路口安全分析（Intersection Safety Analytics）等等。一個智慧城市的物聯網應用是無處不在，Verizon 從能源，交通管理和公共安全等方面考慮，幫助創造更有效和可持續的服務，以提供更好的社區公民服務。

Verizon 於智慧城市解決方案的運作，是利用緊密編織的無線網路技術的組合來利用和分析數據。傳感器和設備在邊緣工作以收集數據。無論是分析流量模式,監控公用事業和資源還是其他方面,智慧城市解決方案將少量訊息集合起來，以提供全面的可視性。Verizon 智慧城市解決方案可幫助近乎實時地了解數據，處理和分析數據，然後提供向公眾傳播這些結果的方法。舉例如下：

智慧照明（Intelligent Lighting）：通過智慧街道照明技術節省能源並改善公共安全。Verizon 智慧照明可以單獨或按組遠程操作燈光，或根據接近傳感器數據或預設定義進行編程以打開，關閉或調暗，有助降低能源成本並提高安全性。通過 City Hub，更可以在適應性強且易於使用的雲平台上連接更多物聯網解決方案。

智慧交通流量管理（Intelligent Traffic Management）：利用智

慧交通技術推動交通流量的改善。在大多數社區，交通非常頻繁，信號時序缺乏與現場數據相結合，容易造成燃料浪費，排放增加，駕駛員受挫以及業務損失等。Verizon 幫助司機花更少的時間到達目的地。Verizon 智慧交通流量管理是一種基於雲的端到端軟體即服務（end-to-end software-as-a-service）解決方案，使用機器對機器（M2M）技術和無線網絡來收集流量數據。提供更好的方法來監控流量，改善信號時序和管理流量。

交通數據服務（Traffic Data Services）：交通堵塞不僅使人們感到沮喪，而且司機每年因浪費燃料和浪費時間而造成損失。Verizon 4G LTE 網路的無線數據可以幫助交通管理人員和交通規劃人員改善人們穿越城市的方式。Verizon 交通數據服務使用匿名的個人數據提供即時交通訊息和歷史紀錄，從全國網路收集街道資訊提高準確性。該方案提供有關人口流動模式和交通性能的可操作數據，改善管理和規劃多模式運輸方式。

交叉路口安全分析（Intersection Safety Analytics）：幫助行人，騎自行車者和駕駛員保持安全。對於試圖提高安全性並實現 Vision Zero 目標的城市不再需要依靠手動收集交通事故數據。Verizon 交叉路口安全分析提供使社區更安全所需的數據，還有助於交通規劃和擁堵管理。其軟體即服務解決方案，可以輕鬆地使用全天候數據，幫助行人，騎自行車者和司機安全到達目的地。

Verizon 如何讓城市變得更聰明，其中關鍵組成部分是 5G 網路戰略，稱為 Verizon 5G 動力智慧城市。5G 是第五代無線技術，用戶會將其視為目前世界上最快，最強大的技術之一。這意味著不僅可以更快地下載，還可以獲得更豐富的沉浸式體驗，這些體驗對我們的生活，工作，學習和娛樂方式產生巨大影響。5G 的連接優勢將使企業更高效，並使消費者能夠以前所未有的速度訪問更多信息。自動駕駛汽車，智能社區，工業物聯網，遠程醫療保健等都將依賴 5G。這就是 Verizon 建構自己的 5G 技術以加速測試並推動全球 5G 標準開發的原因。並將持續與其他技術合作夥伴合作，進一步推進 5G 技術，並在實現全面佈署的道路上實現重要里程碑。

此外，Verizon 亦推出 Narrowband Internet of Things（NB-IoT，窄頻物聯網）和 LTE M（Cat M1）網路，使客戶可以自由選擇最適合特定應用的連接，並具有安全，可擴展和可靠的蜂窩 LTE 網路的所有優勢。

NB-IoT 是用於物聯網應用中受歡迎的 LPWA 技術之一。它提供了恰當的功能組合。低頻窄帶信號點播具有可以穿透牆壁和金屬導管的長距離傳播特性。電源要求足夠低，使得由單個電池供電的設備的壽命可以超過 10 年。它的數據速率恰好適用於物聯網應用，如儀表讀數，控制路燈，停車位監控，工業數據監控和一些其他低數據速率應用等，提供經濟高效，安全且可擴展的連接選項。

另外，LTE CAT M1 使用現有的 LTE 網路進行操作，但是不同於 NB-IoT 的是，LTE CAT M1 在與用於蜂窩應用中的相同 LTE 頻帶內進行工作。其優點之一是它具有從一個小區站點向另一個小區站點之間切換的能力，這使得可以在移動應用中使用該技術；而 NB-IoT 不允許從一個小區站點移動切換至另一個小區站點，因此只能用於固定應用，即僅限於單個小區站點覆蓋的區域內的應用。

由於 LTE Cat M1 技術能夠與 2G，3G 和 4G 行動網路共存，因此它具有行動網路的所有安全和隱私功能的優點，例如支持用戶身份保密性，實體認證，機密性，數據完整性以及對移動設備鑑定的功能等。

表：NB-IOT 與 LTE CAT-M1 的關鍵規格比較

	LTE Cat M1	NB-IoT
Deployment	In-Band LTE	In-Band LTE, LTE Guard Bands, Standalone
Downlink Modulation	OFDMA, 16 QAM	OFDMA
Downlink Datarate	Up to 1 Mbps	250 kbps

Uplink Modulation	SC-FDMA, 16 QAM	SC-FDMA
Uplink Datarate	Up to 1 Mbps	250 kbps (multi-tone), 20 kbps (single tone)
Bandwidth	1.08 MHz	180 khz
Duplexing Technology	Full Duplex, Half Duplex, FDD & TDD	Half Duplex and FDD
Latency	10 to 15 milli seconds	1.6 to 10 seconds
Link Budget	155.7 dB	164 dB
Power Class	23 dBM, 20 dBM	23 dBM, 20 dBM

Verizon IoT 詳細介紹請參閱：https://www.verizon.com/about/our-company/internet-things。

Verizon IoT 企業解決方案詳細介紹請參閱：https://enterprise.verizon.com/products/internet-of-things/。

圖：Verizon 展示攤位

(12) Wireless Communications Alliance (WCA)

無線通信聯盟（WCA）成立於 1994 年，是一個致力於為無線行業提供教育，連接和社區的非營利性商業聯盟。WCA 通過舉辦研討會/小組來實現這些目標; 提供交流機會; 鼓勵和支持初創企業和企業家; 並幫助建立和維護商業和學術界之間的橋樑。支持學術

和技術教育是 WCA 的主要目標。WCA 位於舊金山灣區，靠近幾所世界一流的大學，學院和智庫。儘管移動技術迅速崛起，但研究表明只有 5%的大學新生認為無線是職業目標。為了確保未來十年強大的人才庫，WCA 邀請大學生免費參加舉辦的活動，希望無線行業的曝光能夠鼓勵他們將專業和課程重點轉向無線。

本次活動 WCA 舉辦了一場 Tech Talk，主題是 Privacy-centric cloud service for mobile operators，介紹雲存儲的重新發明已經開始。來自 0Chain 的產品 OBox 是一個分散的存儲平台，可以保護我們的數據透明。在 Meetup 中，分散式分類帳公司 0Chain 的首席執行官 Saswata Basu 討論服務提供商如何利用以隱私為中心的雲產品 0Box 來減少客戶流失並增加收入。有關詳細信息，請訪問 https://Ochain.net。0Chain 是一個以“第 1 層”區塊鏈協議啟動分散的應用程序（如 0Box 和 0Wallet），能夠抽象基礎架構和“零信任”協議。WCA 本年度的活動還包括：Sensors Expo & Conference on 25 June 2019，IoT Forum on Computer Vision on 26 June 2019，Gadgets & Gizmos: An hands-on IoT Experience on 23 July 2019 等。

WCA 詳細介紹請參閱：https://wca.org/。

(13) UrsaLeo

UrsaLeo 是一個平台即服務（PaaS）公司，它從工業建築，設備和設備以及商店中獲取數據，顯示和處理 Google 雲中的數據。他們擁有一些獨特的可視化和分析功能，例如以低成本在設施規模的 3D 模型上顯示傳感器數據。他們現在有一個測試版產品，在 7 個國家/地區擁有客戶，將在 2019 年第二季初發布 MVP（最簡可行產品，Minimum Viable Product）。目標客戶是中型製造，物流和數據中心。 其針對發送到雲端的數據，以 MB 為基礎做計量收費。

UrsaLeo 在本次會議中獲得 Startup Elevate Innovation of Things Pitchoff Winner。

詳細 UrsaLeo 介紹請參閱網站：https://ursaleo.com/。

圖：Startup Elevate Pitchoff Winner UrsaLeo 展示攤位

（二）Hackathon 會議

本次 IoT World Hackathon 於 5 月 13-14 日舉辦兩天，議程如下：

May 13th	
8:00am	Doors Open
9:00am	Kickoff / Hacking Begins
12:00pm	Crash Tests
3:00pm	Team Registration Due
6:00pm	Drone Races
11:59pm	Leave

May 14th	
8:00am	Doors Open / Tech Support Resumes
10:00am	“Giving Your Pitch” mini-workshop
12:00pm	Coding Ends
12:30pm	Round 1 Presentations
4:00pm	Top 3 Teams Present at Exhibitor Happy Hour
4:30pm	Winners Announced
5:00pm	End

此次 Hackathon 開發專案挑戰的主題是：水(Water)，說明如下：水是一種影響生活各方面的珍貴商品。對於一些人來說，這種資源很容易獲得並且供應充足。然而，在農業領域，情況並非總是如此。獲取和正確的使用水，對於農業的可持續性，成長和生計至關重要。您如何能夠找到並發揮解決這些問題的方法？

本次物聯網世界 Hackathon 是物聯網世界開發者大會的一部分，今年首要贊助商是 SAIC，主辦單位提供專案開發的支援配備包括：STMicroelectronics 公司提供的 ST25R3911B 高性能 HF 讀取器/NFC 啟動器，ST25 軟體開發套件 ST25SDK 作為 NFC 資料接收的

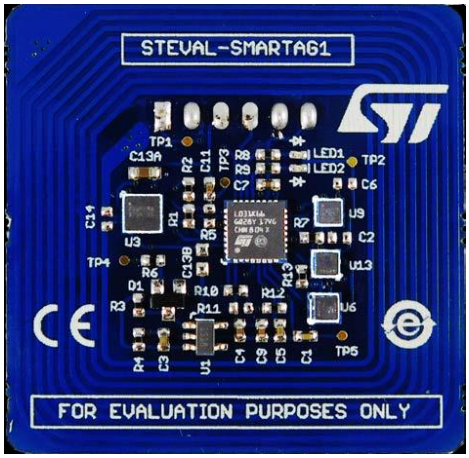
GUI，NFC Sensor Tag，USB 連接線，電池，ST 產品規格手冊，以及 USDA(U.S. Department of Agriculture) 歷年 DataSets 數據集作為專案驗證測試使用。（註：HF 全名為 High frequency，高頻；NFC 全名為 Near-field communication，近距離無線通訊）

圖：IoT World Hackathon 專案開發支援配備

ST25R3911B 介紹如下：ST25R3911B 為高性能 HF 讀取器/ NFC 啟動器，ST25R3911B-DISCO 是一款即用型開發套件，用於評估高性能 HF 讀卡器/ NFC 啟動器 ST25R3911B 在讀卡器模式下的功能，適用於非接觸式應用。ST25R3911B-DISCO 通過 USB 連接到 PC，以顯示 ST25R3911B 晶片的功能。 可使用 STSW-ST25R001 軟體來控制開發工具包的所有功能。
ST25R3911B-DISCO PCB 如下圖：

STEVAL-SMARTAG1 介紹如下：STEVAL-SMARTAG1 是 NFC Dynamic Tag sensor node evaluation board，具有 NFC 收集功能。這款智能靈活的 NFC Tracker 評估板帶有傳感器，包括一個全面的軟體函式庫和一個範例應用，用於從 Android 或 iOS 設備透過 NFC 監控和記錄傳感器上的數據。

此超低功耗傳感器節點評估板安裝了 ST25DV NFC 標籤，STM32L0 ARM Cortex M0 +，環境傳感器（溫度，濕度和壓力）和運動(加速度計)傳感器等。STEVAL-SMARTAG1 NFC sensor tag 如下圖：



The STEVAL-SMARTAG1 evaluation board 詳細元件和功能請參考： https://www.st.com/en/evaluation-tools/steval-smartag1.html。

ST NFC Sensor TAG evaluation board 之使用者手冊（User Manual），請參考：
https://www.st.com/content/ccc/resource/technical/document/user_ma

nual/group1/9b/5c/d5/3e/e3/0b/4d/90/DM00511300/files/DM00511300.pdf/jcr:content/translations/en.DM00511300.pdf。

本次主辦單位提供美國農業部 USDA 歷年降雨資料作為專案開發參考。“水土資源保護法”（RCA，The Soil and Water Resources Conservation Act）給美國農業部（USDA，U.S. Department of Agriculture）為提供廣泛的自然資源戰略評估和規劃的權限。 RCA 的目的是確保美國農業部保護土壤，水和相關資源的計畫能夠滿足國家的長期需求。詳細 RCA Report - Interactive Data Viewer 請參考：https://www.nrcs.usda.gov/wps/portal/nrcs/rca/national/technical/nra/rca/ida/。

本次有 10 組隊伍報名專案開發，10 組專案報告及展示後選出優勝前三名，分別為 AFS(Automated Farm Surveyor)，Smart Ag 以及 RAM 等三隊，最後獲得 Hackathon 第一名的隊伍是 SmartAg。

圖：IoT World Hackathon 評審與前三名隊伍成員合影

四、 建議意見：

建議事項

- ☐ 本次會議的各家廠商都強調物聯網服務的成功，需要倚靠建立整個產業的生態系統（Ecosystem），包括從物聯網感測晶片設計，傳感系統，數據傳輸，分析，管理的物聯網雲平台，以及特定應用的智慧樣態和洞察分析，這些都需要有專業公司來提供服務，非常值得台灣在未來物聯網產業垂直整合發展上參考。
- ☐ 物聯網的應用層面可以很廣泛，本次會議已經有許多公司展示成功案例，也有許多新創公司展現其創新的應用構想，台灣的新創公司也積極的參與了此次盛會，台灣未來在物聯網的應用上，仍有很大的空間可以發揮，可多鼓勵新創構想以發展物聯網應用。
- ☐ 美國主要 ISP 如：Verizon，T-Mobile，AT&T 等，在物聯網無線傳輸環境的基礎建設上都已可提供 5G，NB-IoT，CAT-1，及 4G LTE 等不同傳輸標準，以因應不同物聯網的應用，並且積極整合特定應用的合作夥伴，提出整合的物聯網解決方案，值得台灣 ISP 未來提供物聯網無線傳輸的基礎建設以及探索相關應用的參考。
- ☐ AWS IoT 的運作分三個層次，分別為 Edge，Cloud，以及 Enterprise，從物聯網應用的資料流架構上，這三個層次確實環環相扣，台灣在雲端服務的成熟度上及在邊緣運算的佈建上都是一大挑戰，此架構可以做為未來台灣物聯網服務提供及系統整合廠商的參考。
- ☐ 本次會議舉辦的物聯網 Hackathon，各隊為了要完成一個 IoT Hackathon 專案，必須結合問題探討，資料分析，以及感測硬體元件，軟體開發，訊號傳輸，視覺介面設計等系統整合等，才能完成一個雛形系統進行專案報告和展示。尤其物聯網的應用需要依據問題和目標，整合多種技術，在短時間內結合多人的技術專長，發揮團隊分工與合作，很值得在台灣推廣試驗。
- ☐ 許多國際業者會舉辦物聯網的技術研討和實作工作坊，也陸續舉辦多場展覽會，建議可多參與，並與國外相關單位及業者進行更密切及多元的交流及經驗分享，作為台灣發展的參考。

Internet of Things World 下一次會議將於 2020 年 4 月 6-9 日於美國聖荷西舉行，相關資訊請參考：https://tmt.knect365.com/iot-world/。

五、 會議議程：

以下為 2019 Internet of Things World 的完整議程表：

Monday, May 13, 2019: Pre-Conference Workshops and Hackathon	
時間	議程
09:00-16:00	Intelligent Transport Systems Workshop
09:30-17:00	
	Silicon Valley AgTech Conference
	Eclipse IoT Developers Day
	IoT in the Channel
	IoT Saving Lives
	Hackathon

Tuesday, May 14, 2019: Executive Keynote Day and Hackathon	
時間	議程
08:15-08:45	Pre-Keynotes Industry Briefing
08:40-16:00	Executive Keynotes Day
16:00-18:00	Exhibition Opening & Booth Crawl
16:20-16:50	Silicon Valley AgTech Startup Pitch off
17:00-17:30	Hackathon Pitch off Finals
18:30-21:00	Hyatt Pool Party

Wednesday, May 15, 2019: Morning Keynotes, 11 Conference Tracks and Exhibition	
時間	議程
07:30-08:30	Analyst Breakfast Briefings
08:40-10:40	Keynotes
10:40-11:40	Industry Vertical Networking
11:30-16:40	Conference Tracks - Industrial Verticals
	Manufacturing
	Smart Buildings & Energy Management
	Smart Cities - Investment/PPPs/Infrastructure
11:30-16:40	Conference Tracks - Consumer Verticals
	Connected Consumer: Technology
	Connected & Autonomous Vehicles
11:30-16:40	Conference Tracks - IoT Capabilities
	IoT Connectivity - 5G & LPWAN

	AI & Machine Learning
11:30-16:40	IoT World Developer Conference
10:00-18:00	Expo Hall - Exhibition Open Hours
10:30-17:00	Ecosystem Stage
10:30-17:00	Startup Elevate Pitch offs
10:30-16:30	Insider Session Workshops
16:00-17:00	IoT World Official Press Event
15:40-16:40	Industry Vertical Exhibition Tours
16:40-17:40	VIP Networking Power Hour
18:00-21:00	IoT World Awards Ceremony and Gala Dinner

Thursday, May 16, 2019: Morning Keynotes, 9 Conference Tracks and Exhibition	
時間	議程
07:30-08:30	Analyst Breakfast Briefings
08:30-10:30	Morning Keynotes
10:40-11:40	Industry Vertical Networking
11:30-16:40	Conference Tracks - Industrial Verticals
	Energy Production & Distribution
	Supply Chain & Logistics
	Smart Cities - Mobility & Transportation
11:30-16:40	Conference Tracks - Consumer Verticals
	Connected Consumer: Delivery & Services
	Connected & Autonomous Vehicles
11:30-16:40	Conference Tracks - IoT Capabilities
	IoT Security
	Edge Computing
11:30-16:40	IoT World Developer Conference
15:30-16:30	Industry Vertical Exhibition Tours
10:00-16:00	Expo Hall - Exhibition Open Hours
10:30-16:00	Ecosystem Stage
	Startup Elevate Pitch offs
	Insider Session Workshops

『MWC19 Shanghai』出國報告

財團法人台灣網路資訊中心因公出國人員報告書 108 年 7 月 10 日

報告人 姓　名	許淑芳	服務單位及 職稱	專案經理
出國期間	108/6/25-29	出國地點	Shanghai, China
出國事由	參加 MWC19 Shanghai		
報告書內容包含： 一、 出國目的 二、 會議行程 三、 考察、訪問心得 四、 建議意見			
授　權 聲 明 欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人： 許淑芳 (簽章)		

註
二、請於授權聲明欄簽章，授權本中心重製發行公開利用。
附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

一、出國目的：

參加由 GSM 協會（Group Special Mobile Association，GSMA）所主辦的 MWC19 Shanghai（Mobile World Congress 2019 Shanghai，全球行動通訊大會-上海）會議及展覽。GSMA 成立於 1995 年，是為 GSM 行動電話系統的共通標準、建置及推動而設立，由行動通訊業者以及相關公司贊助成立的協會。其歷史可追溯到 1982 年由 CEPT（Confederation of European Posts and Telecommunications）組成 GSM（Group Special Mobile），主要目的為設計歐洲行動通訊技術，到 1995 年協會才正式成立。GSMA 每年舉辦全球行動通訊大會最大的年度盛事—包含全球行動通訊大會-巴塞隆納、全球行動通訊大會-上海、全球行動通訊大會-洛杉磯、GSMA NFC 與行動商務高峰會、GSMA-mHA 健康行動高峰會等。GSMA 由 220 多個國家及區域，將近 800 家的行動通訊業者，和 200 多家設備製造商構建了行動生態體系，包含手持式行動裝置製造商、軟體公司、行動裝置晶片設計製造商、網際網路業者、媒體與娛樂業者等。

此次是全球行動通訊大會-上海的第八屆會議及展覽，也是亞洲行動通訊的年度大型會議及展覽之一，會議日期為 6 月 26 日至 28 日共 3 天。會議和展覽期間共有來自 100 國家，超過 7.5 萬人到場參與，今年主題〝智聯萬物〞，描繪了高速靈活的 5G 網路、物聯網、人工智慧、大數據及邊緣計算等新科技的結合，達到聯結萬物，共建美好未來。中國工信部於今年 6 月 6 日，也就是展期前 3 週，正式向中國電信、中國移動、中國聯通及中國廣電 4 家電信營運商發放了 5G 商用執照，象徵中國進入 5G 元年，這比原本預期的時間提早了一年，可以強烈感受到全球對 5G 的熱度及競爭態勢。因此此次會展期間舉辦了相當多場 5G 技術研討會，並可看到參展業者對 5G 技術商品及應用著墨甚多，各個展廳都有 5G 相關的展示和體驗，此次整個展覽會場也布建 5G 連網環境，讓與會者可以體驗 5G 行動連網的真實感受。

智聯萬物標誌著一個新時代的來臨，讓人可以隨時隨地享受多樣化

及個性化體驗。2019 年 MWC 上海會展，以智聯萬物為題，圍繞八個核心主題。會展期間活動包含主題演講、產業峰會、合作夥伴活動、導覽以及研討會等。會展的八個核心主題如下：

（一）人工智慧

截至 2020 年，人工智慧市場產值預計將達到 700 億美元，這無疑將對全球消費者、企業及政府產生相當程度的影響。人工智慧產業不斷開發出各式各樣的應用，展現的人工智慧真正潛力，本主題將深入探討各產業該如何運用此革命性技術及其對人類生活的影響。

◆ 相關行業包括:

廣告與零售業、政府、IT、搜索、電信。

（二）連接

5G 具有高速性、靈活性及敏捷性，能夠提供遠比現在更加可靠的服務與性能。〝連接〞 這一主題的目地在強調讓 5G 願景成為現實所需的相關需求，從真正實施到案例、業務模式、頻譜與法規監管，再到新興與多元市場或產業中面臨的商業及文化挑戰。

◆ 相關行業包括:

航空航天、緊急支援服務、智慧城市、電信。

（三）資訊安全

近幾年出現的一些資訊安全事件，大大降低大眾對於數位生態系統的信任度。隨著人工智慧時代的來臨，針對數據使用的隱私與道德規範，將引入更多法規約定，且引起更多的強烈關注。資訊安全須肩負分析實現消費者、政府和監管機構間良好平衡所需的重要責任。

◆ 相關行業包括:

數位身份、金融科技、政府、媒體與公關、隱私、安全。

（四）數位健康

各行各業數位化滲透大眾生活的各個面向，以透過智慧手機的管道對人類生活產生的影響及變化最大，所以行動網路也包含在其中。由於智慧手機普及，讓人對科技的依賴性，所引發對心理健康問題的影響，也引起了廣泛的關注及討論。

◆ 相關行業包括:

生物科技、醫療保健、軌道交通、可再生能源、智慧城市、旅遊。

（五）顛覆性創新

因為創新及推廣速度持續加快，顛覆性創新貫穿了會展的各個面向。企業需要保持警覺與具備靈活性，才能積極應對產業及市場的快速變化。

◆ 相關行業包括:

企業社會創新與影響力投資、管理顧問、新創公司。

（六）沉浸式內容

隨著消費者對擴增實境(Augmented Reality，AR)、虛擬實境(Virtual Reality，VR)及其他更為豐富的體驗式內容的需求與期望不斷增長，其對網路、活動場地及整體消費者參與度的影響也在不斷擴大。〝沉浸式內容〞深入探討我們所面臨的挑戰、獲利模式及消費增長與網路容量之間的關係。

◆ 相關行業包括:

AR/VR、遊戲、媒體與視頻、音樂、體育與電子競技。

（七）工業 4.0

工業 4.0 由物聯網、虛實整合系統(cyber physical systems，CPS)、雲端和認知計算(cognitive computing)構建，主要在分析這些構成要素的實施方法與為產業帶來的廣泛影響。

◆ 相關行業包括:

汽車、物聯網平台與分析供應商、物流、維護、製造。

（八）美好未來

美好未來這一主題將以更長遠的眼光看待未來 10 年的技術發展，探究其將如何塑造 2028 年及之後的世界面貌。

◆ 相關行業包括:

6G、腦機接口(Brain-Computer Interface)、量子計算、創業公司。

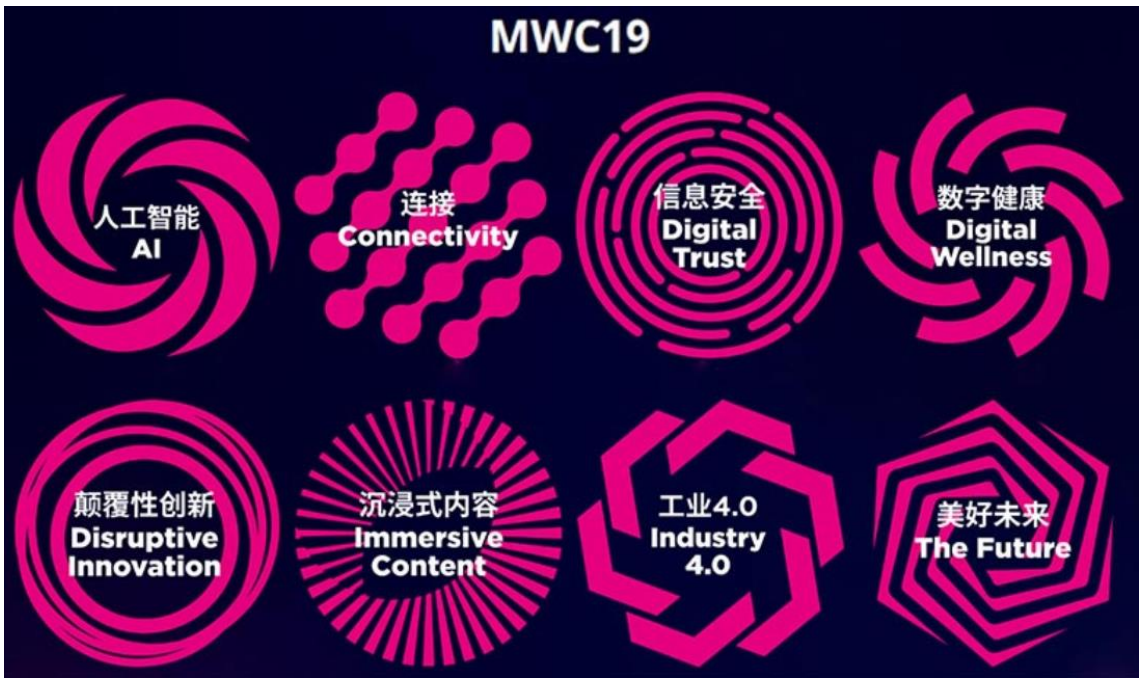


圖 1、MWC19 上海會展主題

本次 MWC19-Shanghai 同時進行多類活動，主要分為展覽、會議、活動及體驗 4 大類，各類活動所舉辦的分項內容包含：

（一）展覽

MWC19 上海的展期為 6 月 26 日至 28 日為期 3 天，展覽會場有 7 大展館面積接近 10 萬平方公尺，比 2012 年第一次 MWC 上海會展增加近 3 倍。此次展覽主題類別如下所述：

1. GSMA 創新城市展

GSMA 創新城市展示行動通訊行業創新技術及應用，主要重點將聚焦在 MWC19-上海主題智聯萬物的解決方案，從 5G 時代中行動網路、智慧平台、人工智慧和物聯網設備數據的多項技術結合中受益。深入探索這些技術對大眾生活所產生的影響，包括娛樂、交通、公共服務、企業、環境可持續性及網路與雲端連接。

主辦單位 GSMA 和 BICS、中國移動咪咕、G7 智慧物聯網、華為、myFC、上海雷塔智能科技和新加坡電信等業者，打造行動通訊連網、未來網路和物聯網等重點項目，展示行動互聯產品和服務如何改善市民、企業和政府的日常生活。

圖 2、GSMA 創新城市展區

2. 超級展館

這是 MWC 上海第二次規劃超級展館(Super Hall)，也是本次展覽的重量級舞台，集結業界領先企業齊聚在同一展館，展示與5G、人工智慧(AI)、物聯網(IoT)等新技術相關的創新解決方案。

圖 3、超級展館展出業者

3. 未來智慧交通展區

在該展區參展的公司包括 Helix Technologies、Imagination Technologies 和 UROS，以及汽車行業主辦機構廣東寰球國際會展(GIE)，將攜手智慧互聯汽車合作夥伴，包括百傑騰、深鑑科技、國圖顧問、星輿科技等，共同展示未來行動智慧交通的生

態發展。除展覽外，該展區還將包括未來智慧交通舞台，探討顛覆未來智慧交通生態系統的創新技術及應用。

下圖為中國信科在未來智慧交通展區，所展示的遠端駕駛平台。

圖 4、中國信科遠端駕駛平台

4. 國際智慧城市博覽會

國際智慧城市博覽會已經正式成為 MWC 上海展覽的一部分，此次上海浦東智慧城市博覽會將行動互聯與智慧城市連結。展會以智慧城市建設與發展為題，建立政府及企業面對面的交流平台。除展覽外同時舉行智慧城市國際合作論壇上海峰會，目地在促進中外智慧城市領域的合作及交流，論壇特別邀請國際智慧城市負責人到場進行介紹和案例分享。並由中國智慧城市的領導以及知名企業代表，在論壇上分享成功經驗。

亞信科技結合 5G、智慧政務、智慧社區/養老、智慧金融、智慧出行、智慧零售以及企業數位化等七大領域解決方案。下圖為亞信科技展位上所展出的智慧社區解決方案。

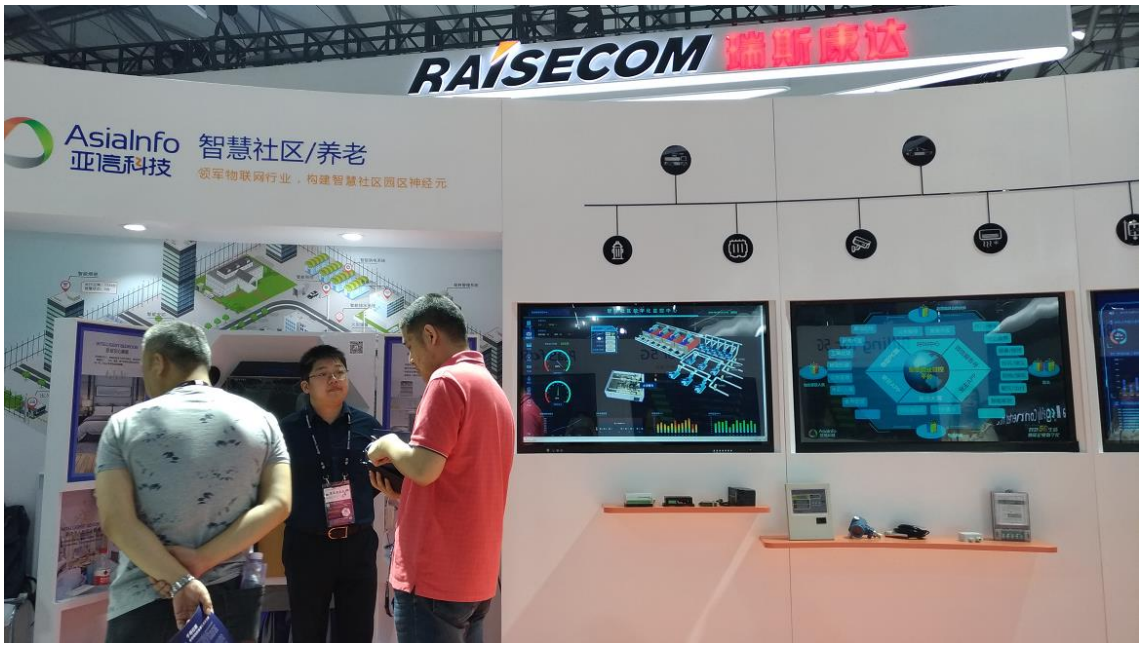


圖 5、亞信科技的智慧社區解決方案

5. 國際新型顯示技術展

國際新型顯示技術展是一個集新型顯示、顯示終端為一體的技術、產品、學術年度交流及貿易平台。2017 年首次舉辦，今年折疊行動智慧手機產品將從設計概念落實為真正應用，OLED、AMOLED 顯示技術開始向車載系統產業延伸、高解析度顯示上下游產業鏈也不斷有突破性發展，對國際新型顯示產業的技術、市場、產品和競爭格局也都產生一定程度的變化。

因應 5G 與新型顯示技術融合發展趨勢日益明顯，2018 年開始 MWC 上海的同期活動，加入了國際新型顯示技術展共同宣傳。在國際新型顯示技術展中，以展示及推廣柔性、高解析度顯示，5G 通信技術及產品為展場主題。

6. 全球 5G 沉浸式體驗

全球 5G 沉浸式體驗展用好看、好聽、好玩的互動展示方式，打造 5G 應用體驗，為參觀者帶來互動 5G 之旅。展館由中國移動推出和 5G 有關應用，針對行動互聯網領域中國移動設立子公司咪咕文化科技，負責數位內容領域產品提供、營運及服務，其所經營的內容包含音樂、遊戲、閱讀及動漫四大領域數位內

容。本次體驗展以咪咕創新星球為主題，展示 5G+生態，讓觀眾和 5G 應用進行互動體驗。

圖 6、全球 5G 沉浸式體驗展場現場

展出的內容包含 8K 電影院，5G 高解析度賽事直播、博物館在移動、AR/VR 展區及 5G 咪咕熊貓樂園等共五個展示區。

- ◆ 8K 電影院展現超高解析度 8K 內容的視聽新體驗。
- ◆ 5G 高解析度賽事直播，打造 5G 超高解析度賽場籃球訓練營的概念，以投影方式營造和現場觀眾進行互動式遊戲，及進行 5G 4K/8K 高解析度賽事直播。
- ◆ 博物館在移動透過新科技與中華傳統文化的傳承、創新與發展做融合，開啟大眾與博物館之間的交流，活化文化資源，增強博物館服務效能。
- ◆ AR/VR 展區，匯聚最新 VR/AR 設備及內容廠商，透過影音及互動雙重體驗內容，讓參觀者以最直觀的方式感受 AR/VR 所帶來的視覺感官體驗，拓展 VR/AR 展示，推動 VR/AR 雲端+終端+內容展示產品的商業化。

圖 7、5G 高解析度賽事直播及互動遊戲現場

圖 8、AR/VR 展區現場

◆ 5G 咪咕熊貓樂園是為紀念科學發現大熊貓 150 週年，〝全球 5G 沉浸式體驗展〞咪咕咖啡區域以熊貓作為主要設計元素，將咪咕的產品、業務及咖啡餐飲服務融為一體相結合。咖啡展區連結展會主題，展示 5G+AI 的技術發展的核心產品和能力，目的在用技術拓展更多體驗場景。

（二）會議

除了展覽外本次 MWC19-上海並舉辦多項論壇及研討會，希望與會者可透過論壇與研討會，了解 GSMA 組織所推動各項技術，及各項關聯性產業計畫的發展趨勢。通過參加研討會、聆聽全球產業專家的想法，拓展與會者對產業發展趨勢的了解，並獲取全球先進知識。論壇與研討會活動於 6/26 及 6/27 舉行，場次分為：

1. 未來智慧交通舞台：

在 MWC19 上海未來智慧交通舞台上，將探究加速未來智慧交通生態系統發生變革的創新推動因素，探索現有產業和新業者應如何在市場中找到定位，以把握新的發展機會。

2. GSMA 未來網路研討會：

主要是以富通信訊息（Rich Communication Services，RCS）傳送業務如何改變消費者的使用體驗為題，透過業內重要業者的意見及經驗分享。探討富通信業務消息傳送市場的現狀及成果，及此平台帶來的商機及市場潛力，以及富通信的戰略願景等。

圖 9、GSMA 未來網路研討會現場

3. GSMA 未來物聯網大會：

未來物聯網大會將匯集政府、行動通信服務商和企業代表，共

同探討物聯網、5G 和大數據的最新發展。物聯網發展迅速，5G 建構起支持物聯網發展的基礎，足以展示 5G 與物聯網的無限潛能。本次未來物聯網大會透過行動通信商分享物聯網數據平台和數據服務，如何提供客戶連接以外的其他重要服務，為客戶帶來物聯網創新商機。

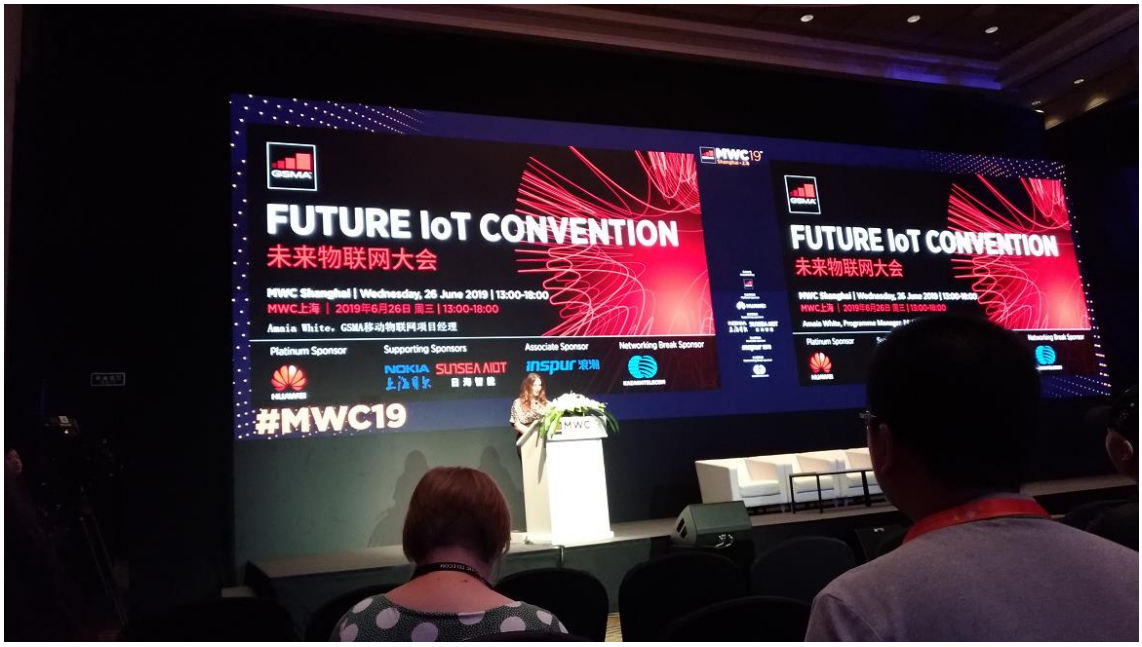


圖 10、GSMA 未來物聯網大會現場

4. GSMA 富通信訊息傳送業務宣傳實驗室：

此活動和未來網路專題相關由 LivePerson 贊助的第 25 屆 GSMA 富通信訊息傳送業務實驗室活動。實驗室目的在與初次接觸富通信的企業交流，及讓與會者了解通信服務商在富通信服務、GSMA 配置文件標準、富通信生態系統（通信服務商、品牌、科技公司和營銷公司）、富通信全球部署、手機應用、客戶體驗、品牌試驗、商業模式和隱私，及安全與信任等資訊。

5. 中國數位身份認證美好未來：

隨著亞洲數位服務不斷整合，對於企業而言，身份認證與數據都將扮演重要地位。企業更希望能擴展並將身份認證數據套現。本次研討會將由 GSMA 身份認證團隊舉辦，探索通信服務商如何與企業建立穩固關係，及如何將服務擴展到 5G 和物聯網

等新技術。並展示供應商如何提供境外交易安全保障。

6. 第 4 屆 5G 頻譜和政策論壇：

GSMA 攜手合作夥伴 GSA 共同舉辦 MWC19 上海第 4 屆 5G 頻譜和政策年度論壇。亞洲地區 5G 發展態勢強勁，多個國家和地區已開始發放 C 波段等頻譜(C 波段指的是全球頻譜分配給通信衛星使用的 3.4-4.2GHz 頻段)，為商業網路部署做好準備。與此同時，2019 年世界無線電通信大會(WRC-19)將隆重舉行，屆時將確定適用於 5G 的毫米波頻譜中的新頻段，2019 年將是 5G 發展的一個重要里程碑。

7. 智慧網路論壇：

在電腦計算能力不斷突破的今日，人工智慧技術被廣泛應用在各個領域及應用上，迎來蓬勃發展的時代。然而行動通信服務商最關心的是，如何將人工智慧技術應用於網路規劃建設、系統維護優化、性能提升、安全防護等方面，在提升網路智慧化的同時提升業務服務的質量和體驗，並降低網路成本及節省能源開支。會中將邀請在該領域積極探索的行動通信服務商和相關產業的業者，分享人工智慧技術應用於網路的實際案例和應用成效，並探討下一步如何推動產業發展更趨於成熟。

8. 未來寬頻論壇-5G 時代的光網路戰略：

今年全球將迎來大規模的 5G 部署需求及第一批 5G 商業服務。在網路經濟的挑戰下，怎樣的智慧光纖策略能全面支持 5G 部署，同時開啟 ICT 融合的新時代：是工業 4.0?還是超大規模物聯網應用?本次活動將探討 5G 帶來的新 ICT 趨勢，重點關注 5G 的傳輸和網路需求，解決 5G 時代的前端傳輸(Fronthaul)架構及邊緣數據中心連接。探討全球光纖生態發展趨勢將如何影響 5G？

圖 11、未來寬頻論壇現場

9. 未來智慧交通舞台：

在社會、經濟和技術趨勢的強力推動下，智慧交通革命正穩步前進，同時帶來商業與社會形態轉變。人工智慧、電氣化、自動駕駛技術與加強連結性的快速發展，正推動全球運輸行動服務（Mobility as a Service，MaaS）的快速發展。預計到 2030 年，乘車共享等運輸行動服務帶來的收入將達到近 1.2 萬億歐元，遠超過傳統汽車製造業的潛在獲利能力。在 MWC19 上海未來智慧交通舞台，將探究加速未來智慧交通生態系統發生變革的推動因素，探索產業和新興業者如何在市場中找到定位，以充分把握產業發展機會。

10.eSIM 論壇：

自蘋果 2018 年發布 eSIM 手機以來，整個行業引頸期盼的時刻現已到來：eSIM 是否會成為時尚智慧手機的標準配置? 並且開啟行動新時代?毫無疑問 2019 年 eSIM 將在消費者及工業物聯網領域被廣泛應用。各行各業如何利用這一不斷發展演進的 SIM 技術並從中獲益?在大規模應用的過程中將遇到哪些阻礙，例如監管政策、用戶體驗管理、技術複雜性以及數位信任方面的不確定性等議題。

11.5G 網路論壇：

今年全球迎來 5G 網路商用元年，伴隨大規模的網路部署的需求，3GPP 將採用的網路及終端設備標準，以及行動通訊服務商在 5G 網路部署的進度和時間表將吸引相關產業業者關注，初期 5G 的網路業務能力和實際性能足以支撐哪些服務和應用？而 5G 標準制定的網路切片(Network Slicing)、邊緣計算(Edge Computing)、及以服務導向的網路架構等對垂直產業應用有關的重要網路能力在早期部署場景中是否能符合服務需求? 4G 發展初期所遭遇的室內覆蓋問題，在 5G 頻率更高的情況下該如何解決?面對 5G 建設週期長投資成本高的業界共識，行動通訊服務商將如何選擇技術演進的進程：未來全功能 5G 網路將如何演進? 非獨立網路(No-Standalone，NSA) 和獨立網路(Standalone，SA)是否可以共存及如何共存等問題探討，都將是此會議的重點。

圖 12、5G 網路論壇現場

12.亞太及中國地區對人工智慧信任專題探討：

大多數人工智慧和人工智慧信任的會議多集中在西方進行，藉

此次專家對話 GSMA 邀請亞太地區專家探討區域內當前人工智慧和對人工智慧信任的趨勢與機會。專家對話將會分為三個組別進行，其中兩組專注於亞太地區，另一組專注於中國的發展討論。

（三）活動

亞洲行動通訊大獎頒獎典禮，得獎對象涵蓋各項技術，從突破性行動終端及科技，在亞洲市場使用或專為其開發的行動應用及服務等。本次得獎業者如下：

圖 13、MWC19 上海亞洲行動通訊大獎得獎業者

（四）體驗

1.4YFN 創新系列活動

4YFN (4 Years From Now) 是由全球行動通信大會 (Mobile World Congress)聯合全球通訊協會 GSMA 專為科技新創企業建立的交流平台，透過專題演講、一對一投資媒合會、新創企業簡報競賽和聯誼活動，致力於為新創業者建立國際聯結。這是 MWC19 上海第四次舉辦此創業競賽活動，目的是加速業務發展和新技術投資。入圍決賽創新提案共有 5 組，將於展會期間向 MWC 上海的評審委員、投資者、企業和與會觀眾介紹其產品或服務。每個創業公司都有四分鐘的時間來發表精彩的演講，兩分鐘的評審提問時間。參與決賽提案簡報有 4 組包括：

◆ YouBeWon（中國）：其設計概念根據網路營運商的網路，建立一個大數據服務平台和產品。其核心團隊成員來自華為，聯想，海航等科技公司。該業務已經吸引了數百萬美元的天使投資，並有知名房地產和電信行業的合作夥伴成為客戶。

◆ ClareKnows（中國）：提案內容是透過交互式人工智慧作為經營及銷售推薦的解決方案。透過使用人工智慧自然語言聊天來吸引現有和潛在客戶，並向客戶，合作夥伴和員工提供產品推薦和訊息。

◆ RefundMe（荷蘭）：提案內容是一個使用 RFID 和物聯網為造訪歐洲的遊客提供數位化退稅流程的平台。

◆ Ambeent（美國）：提案內容是一款透過使用預測性 AI，減少容量的浪費和來自相鄰路由器的干擾，以優化 Wi-Fi 的應用。

得獎者是 RefundMe，杰羅姆·伊瓦涅斯（Jerome Ibanez）代表團隊做提案演說，對改革機場退稅制度計畫進行了精采的介紹。歐洲遊客購買商品後，由於機場冗長且效率低落的手動流程，每年只有少數遊客獲得退稅。RefundMe 使用 RFID 和物聯網，將流程數位化，可以每秒驗證多達 1,000 件物品，讓遊客更方便完成退稅流程。目前該公司正在進行試驗階段，與史基浦（Schiphol）機場做試點改造計畫。

2. Women4Tech 項目

MWC19 上海展會期間，安排第二屆 Women4Tech 項目，重點關注多元化企業文化帶來的轉型價值，從而加強組織績效，改善我們所服務社群的生活品質。

Women4Tech 計畫此次重返上海，將推出更多以縮小行動通信產業性別差異為目標的活動。該計畫以 Women4Tech 峰會為核心，期間將推出多個主題演講和小組討論，探討性別平等、職業發展指導、以及行動通信產業中的女性、女性企業家與創新者等話題。愛立信是今年 Women4Tech 峰會的主要贊助商，演講嘉賓包含來自摩根大通亞洲、KDDI、聯想、LinkIn、萬事達

卡、聯合國兒童基金會及香港大學等的高階管理人。

3. 主題導覽

會展期間將提供四大主題導覽，透過產業專家指導，以滿足與會者和參展業者的需求。透過導覽互動式內容，能更了解參展業者的產品與服務。導覽主題為：

◆ 5G 和虛擬網路導覽

透過互動式導覽，以了解虛擬網路如何與下一代無線應用結合。了解 SDN 和虛擬網路的地位和影響、虛擬實現達成過程中的的初始案例，及下一代網路架構所需考量的技術需求。

◆ 以人工智慧為基礎的技術

GSMA 預測，截至 2025 年，互聯裝置數量將達 250 億，這些物聯網設備將產生龐大的數據資料，其中大部分為非結構化數據資料。本次導覽將把重點放在企業利用各類人工智慧的技術，例如機器學習、機器視覺和深度學習等，將物聯網所收集之數據的巨大潛能產生價值，打造體驗式互聯網。

◆ 產業重塑的新技術

當前企業正積極尋找新技術，以期能創造全新的產業經營模式，產生創新業務發展。此導覽將重點放在雲端服務、語音界面、與企業系統搭配使用的擴增實境/虛擬實境、多機器人和服務機器人以及聊天機器人如何創造新營收、簡化流程並改變人類的工作方式。

◆ 物聯網基礎

互聯時代人工智慧(AI)、5G、雲端計算、機器對機器(M2M)、機器人技術以及車聯網，只是少數技術成果的展現。透過與物聯網產業領先企業互動交流，從基礎設施到消費者終端，讓參展觀眾能夠對物聯網如何應用於業務發展有更深入的了解。

4. 客製化體驗

客製化體驗項目是會展所提供的一項諮詢服務，目的在滿足個別公司的需求，確保該公司在 MWC 上海期間達成會展目標。

透過確認具體的活動要求、針對有興趣重要領域、潛在業務合作夥伴以及相關活動，幫助公司實現目標。

5. 數位領導者計畫

縱觀全球，人類和企業越來越依賴智慧連接和數位解決方案以獲得更好地生活和更有效地擴展業務。對行動產業及更多垂直產業而言，攜手打造數位化未來意義深遠。數位領導者計劃基於此目的，邀請數位產業有影響力的領導者，共同探討產業面臨的挑戰和發現未來商機。透過跨產業交流，加速行動產業和其他產業之間的相互了解，推動跨行業創新，實現全面的數位化未來。

6. INSEAD 大師班課程

GSMA 首次在 MWC19 上海期間推出大師班課程。大師班課程特別為負責領導和實施企業改革的中高層管理人員設置。教授學員與企業如何在智慧連接時代面對挑戰、掌握機會。完成課程的學員將能掌握在高科技融合時代能快速應變的實用管理方法，並能夠在實際工作中創造可執行的管理計劃。

7. MWC 上海展示路演(Roadshows)

MWC 上海展示路演(Roadshows)，陸續於各大城市展開，詳細資訊請參考以下連結：

https://www.mwcshanghai.cn/experiences/opendays/

論壇及研討會議程，詳細資訊請參考以下連結：

https://www.mwcshanghai.com/conference-programmes/agenda/#day=7516

圖 14、5G Summit 會議現場

WMC19 上海贊助商名錄，詳細資訊請參考以下連結：
https://www.mwcshanghai.cn/about/sponsors-partners/
參展商名錄，詳細資訊請參考以下連結：
https://www.mwcshanghai.cn/exhibition/exhibitors/

圖 15、MWC19-上海活動贊助廠商

二、 會議行程：

WMC19 上海會議網站，請參考以下連結：
https://www.mwcshanghai.com/。
WMC19 上海議程，詳細資訊請參考以下連結：
https://www.mwcshanghai.com/conference-programmes/agenda/#day=7516。
WMC19 上海會議展覽資訊，請參考以下連結：
https://www.mwcshanghai.com/exhibition/。

圖 16、TWNIC 許淑芳於 MWC19 上海展覽會場入口、試用 5G 互動影像

圖 17、MWC19 上海展覽會場登記處

參與會議的行程安排如下表所列：

日期	時間	議程
108/6/26 (星期三)	**GSMA Future Networks Seminar**	
	10:00-10:25	RCS Transformation：from communication tool into business ecosystem
	10:25-10:50	Connecting carriers to the global conversational grid
	10:50-11:15	RCS 商業富媒體訊息的創新實踐
	11:15-12:40	RCS/MaaP status in Japan
	11:40-12:00	The evolution of RCS business models
	GSMA Future IoT Convention	
	13:00-13:05	Opening of Future IoT Convention at MWC Shanghai
	13:05-13:15	GSMA Opening Speech
	13:15-14:15	Opening Keynotes –The Future of IoT, 5G and Big Data
	14:15-15:30	Mobile IoT in the 5G World
	15:30-16:00	Break
	16:00-17:00	IoT Beyond Connectivity
	17:00-18:00	Security to Scale the Long Term Future of the IoT
108/6/27 (星期四)	**Future Broadband Forum**	
	09:30 - 09:35	Welcome Remarks
	09:35 - 09:50	KT's 5G and Use Cases
	09:50 - 10:05	Unlocking 5G for the Enterprise IoT Market
	10:05 - 11:10	Network Economics in 5G Era - GSMA Beta Lab
	11:10 - 12:00	What a Smart Fiber Strategy Endorse Sustainable 5G Introduction? Fiber-5G Partnership?
	12:00 - 12:35	How Immersive Innovation & Development Trends in Fiber and Optics Will Affect the 5G Era
	12:35 - 12:40	Wrap Up and Networking
	5G Network Forum(5G 論壇)	
	14:00-14:10	Welcome Remarks
	14:10-15:10	5G Network: Deployment Strategies and Network Capabilities
	15:10-15:40	Panel Discussion: A Deep Dive into 5G

		Indoor Coverage
	15:40-16:25	5G Network: Evolution Roadmap and Future Challenges
	16:25-16:55	5G New Core: Challenges and Strategies
	16:55-17:00	Closing Remarks
108/6/28 (星期五)	**5G Summit(5G 高峰會)**	
	09:30-10:00	5G Connected Surgeon
	10:00-10:20	What Will Proper 5G Networks Look Like?
	10:20-10:40	5G PODS
	10:40-11:00	Shaping the Smart Future with 5G Converged Scenarios
	11:00-11:30	Business Model and Operation of 5G Network Slicing
	11:30-12:30	Digital Bank at the 5G Edge
	12:00-12:25	Monetising 5G
	12:25-12:50	5G Gear, Making New Digital Era a Reality

三、考察、訪問心得：

（一）MWC19 上海論壇及研討會

1. GSMA Future Networks Seminar

未來網路研討會，集結終端業者、解決方案服務商及行動電信服務商等共同參與研討會，將就未來富通信訊息（Rich Communication Suite，RCS）市場機會與技術創新展開探討，並有業者做案例分享。

RCS 是由 GSMA 主導的基於 IMS(IP Multimedia Subsystem，IP 多媒體子系統）架構對基礎通信業務的整合和增強，主要提供多媒體訊息、群組聊天、文件傳輸、影像通話、通話過程中的內容共享等業務功能，目標是實現全球統一標準的富媒體通信解決方案，保證通信服務商之間的業務可以互相聯通。而 GSMA 最新發布的 RCS Universal Profile 2.3 在原有基礎上，升級為 MaaP（Messaging as a Platform，訊息即平台），目的在透過電信服務商訊息平台，將短訊升級為 RCS 訊息，以〝RCS + Platform + Chatbot (聊天機器人)〞的方式，讓使用者可以在訊息服務內完成搜尋、訊息交換、及支付等

完整的服務體驗，這讓商業富媒體訊息國際標準更為完善，進一步擴展 RCS 商業富媒體訊息的產品形態、豐富度及應用場景。2018 年 RCS 發展非常迅速，全球已經有 74 個商用網路在營運 RCS 業務，RCS 商業富媒體訊息市場潛力相當大。在此次研討會上主要是希望電信商、終端設備業者等能共同攜手，推動 RCS 的普及，並遵循最新 RCS 商業富媒體訊息國際規範進行升級,構建新一代訊息服務平台，提升商業信息平台價值，加速 RCS 使用率在全球的成長。

全新的RCS商業富媒體訊息產業鏈有著相當大的價值潛力，在未來將會為通信產業帶來一定的市場機會，但同時也需要電信商、終端設備商等共同努力，透過不斷推陳出新的技術帶給用戶更好的訊息體驗，共同推動產業生態的發展。

RCS/MaaP status in Japan 主題中，由 KDDI 分享 RCS 在日本的發展現況，2018 年由日本 3 家電信業者 KDDI、NTT Docomo 及 Softbank 聯手合作開發新的訊息服務+Message，可提供用戶發送照片、電影、貼圖、語音訊息及群組聊天等功能。該服務符合 GSMA 在 Rich Communication Services（RCS）所訂定的標準規範。3 家電信商共同合作推出此服務的優點是：

◆ 相同的規格

◆ 相同的服務名稱

◆ 相同的使用者介面及使用經驗

但各自的電信商會經營自己的後台，如果使用者換到不同的電信業者，也不會有帳號無法使用，需適應新的應用或服務的問題而造成使用者流失的狀況，3 家電信商可就自己的後台發展更多的加值內容及服務。KDDI 正式讓+Message 在日本上線後，在 Android 及 iPhone 上的使用者目前已經累積超過 9 百萬的用戶，但主要還是來自於 Android 手機用戶，因為 Android 手機可以預設安裝電信業者指定 APP，但 iPhone 的主導權在 APPLE 手上，且 iPhone 手機使用者在日本的比例相當高，這也是業者在推展上遇到的難題。

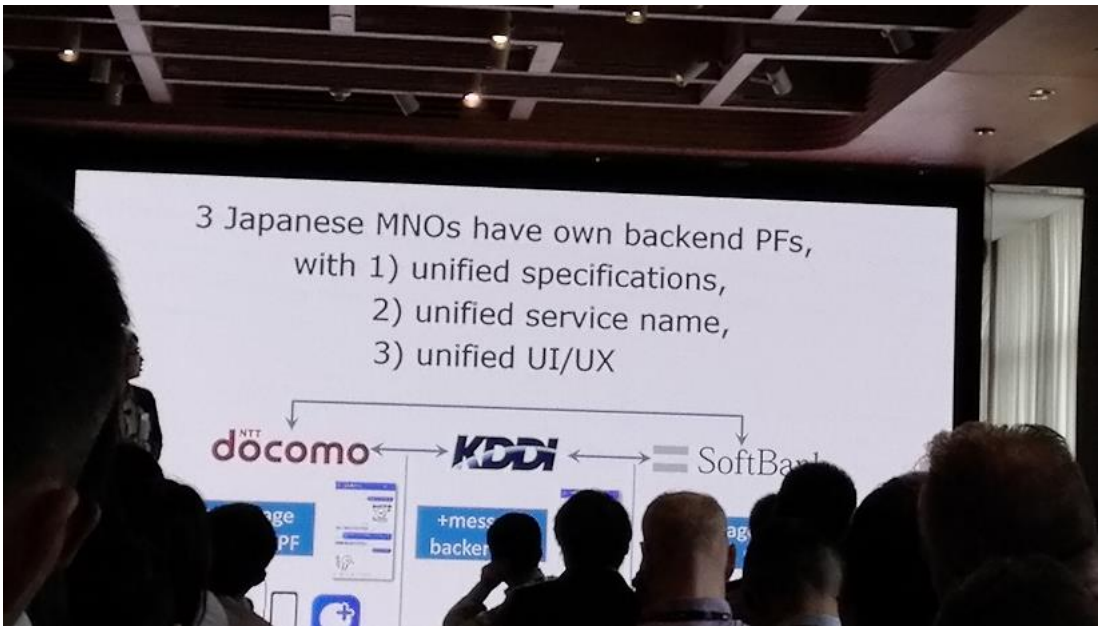


圖 18、RCS/MaaP status in Japan 會議現場

針對 RCS Business messaging（MaaP）的優點為：

- ◆ 可做為身分認證，在消費者購買的使用經驗上可以減少需輸入身分驗證的次數。
- ◆ 相較於 e-mail 的使用，使用者開啟 Business messaging 的機率及便利性上更高。
- ◆ 收費上比電話來的低，能以更低成本做商業訊息推廣使用。

MaaP 的 RCS 平台將改變店家、企業與用戶的互動方式。店家、企業能透過 RCS 平台讓訊息直接接觸使用者，由人工智慧與聊天機器人為使用者提供〝永遠在線〞的服務，不僅能節省成本，還能提升服務品質。使用者也能享受到更豐富便捷的消費體驗，在 RCS 訊息窗應用就能完成搜索、訊息交換和支付等。可以應用於和聊天機器人進行機票查詢、購票、訂位，餐廳點餐，進行商品選擇、下單、支付等。

2. GSMA Future IoT Convention

當前，物聯網發展態勢強勁且迅速，世界各國都在積極部署

5G 網路，構建 5G 生態系統以支援物聯網的發展。越來越多的服務正式的商用化，顯示 5G 與物聯網的無限潛力。5G 如何為物聯網產業帶來革命性的創新？在 5G 領域，物聯網發展將會帶來哪些機會與挑戰？本次未來物聯網大會將探討物聯網、5G 以及大數據等下一代全球技術發展。演講內容共分 4 大主題：

◆ 物聯網、5G 和大數據未來發展

物聯網未來發展前景良好，其所展現出的價值比以往更為清晰。開幕主題演講重點將闡述未來的發展及機會，及行動業者將如何把握此機會。

開場由 GSMA, Head of IoT Program, Graham Trickey 就物聯網在全球的發展現況做介紹，由下圖中可顯示出全球電信業者積極參與物聯網的發展，例如國內的中華電信、遠傳、台灣大哥大及亞太電信等行動通訊業者也積極努力布局，中華電信支援 IoT 的行動通訊協定標準上，可達到支援 NB-IoT 及 LTE-M 兩種標準，顯示業者對市場潛力具有信心及積極希望打開市場的決心。而行動物聯網的應用場景不論是在：

- 工業 4.0：工廠管理、自動化工廠、自動警示系統、維修通報等應用。
- 環境：公共環境應用如智慧電表、智慧路燈、水資源監測等應用。
- 智慧居家：智慧家電、居家防護等應用。

未來的潛力相當可觀。而 5G 的高傳輸及低延遲的特性，將讓自動化工廠、自駕車、AR/VR、即時視訊會議及智慧城市等應用，能夠真正實現。而 NB-IoT 及 LTE-M 將會成為 5G 家族的一部分，補足窄帶物聯網設備的需求，尤其是 NB-IoT，業界普遍認為 NB-IoT 和 5G 並存的可能性相當高。

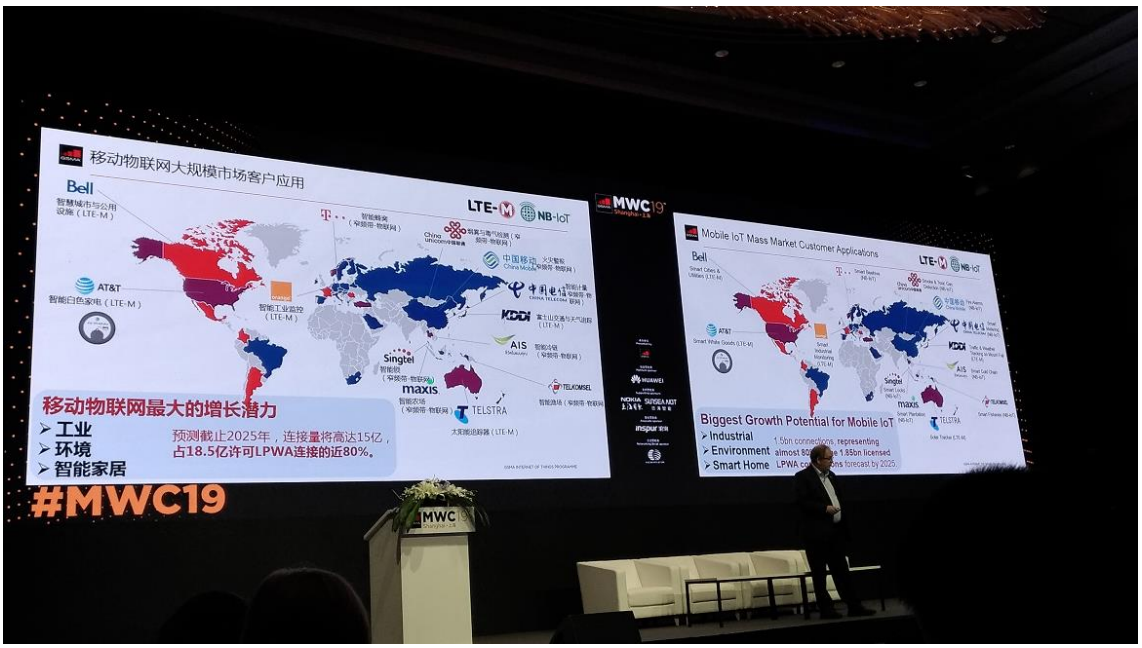


圖 19、未來物聯網大會主題演講現場

Nokia CEO 以誰將受益於未來物聯網和 5G 為題發表演說提及，現在全球有 70 億設備連網，預測到 2025 年將有 1,000 億設備連網，未來的發展相當驚人，但當前主要受益者以原本數位化程度高的公司，傳統產業需要有更完整的解決方案，才有機會加快經由科技的創新而獲益。5G 的高頻寬和低延遲特性，連結大量的資訊；而 AI 在機器感知、認知、大數據處理及自動控制等方面技術不斷的提升；兩者的整合，正為全球科技業帶來極大的變革。物聯網經過多年發展，經由 5G 所帶來的高速連網基礎，讓物聯網的未來能真正落實。智慧物聯網 (AIoT)將整合人工智慧、區塊鏈、雲端計算、大數據、邊緣計算及物聯網，為未來帶來極大的變化及創新。

圖 20、Nokia CEO 未來物聯網演講現場

◆ 5G 未來的行動物聯網發展

行動物聯網網路不斷增加，同時推升 5G 解決方案的熱度。此專題將邀請行動通信業者講述5G和行動物聯網產業、醫療保健及汽車市場，提供物聯網服務的全新解決方案。

中國電信在會中分享中國物聯網發展的現在與未來，到今年底中國預測將有 31 億的物聯網設備連網，到 2022 年底將成長到 70 億的規模，3 年就超過一倍以上的成長率，物聯網設備連網已經來到大成長期，5G 推升物聯網的應用。以下為 5G 及物聯網應用案例：

- 北京世園會：應用於智慧路燈、環境監測、電車管理、智慧煙霧感測及智慧灌溉等應用。
- 智慧警務應用：無人機做自動巡邏，勤務人臉識別系統等應用。
- 電視節目春晚 4K/VR 直播。

對於未來發展的預測NB-IoT適用於低流量窄帶應用上，和 5G 並存的機會高；2G 和 3G 將逐步退出市場，而 4G 和 5G 應該還會並存一段時間。

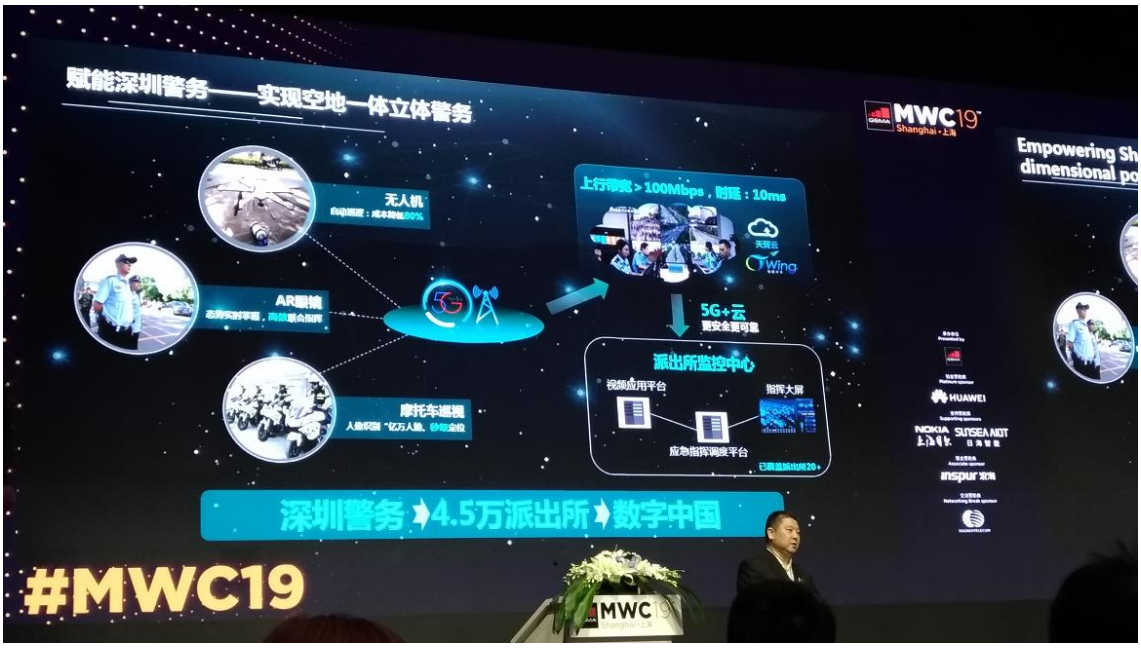


圖 21、中國電信未來物聯網演講現場

◆ 物聯網不止是連接

物聯網、大數據分析和人工智慧可以為企業提供連網領域外的商機。電信商與垂直產業如何制定新策略，突破連網領域界線，會中將以真實案例分享業者的經驗。

物聯網除了連網外，並加入感知元件，因此以前網路連接人與人，到物聯網時代網路連接人與物、物與物等，如何讓物聯網應用更廣泛? AI 和智慧學習是下一步重要關鍵。

國內業者研華科技在會中介紹研華 WISE-PaaS 工業物聯網平台，及部分案例分享。其平台服務包含物聯網雲端服務、物聯網安全服務、WISE-PaaS 物聯網軟體服務、及研華 EIS 邊緣智慧伺服器套裝解決方案等。實際應用案例包含：

- 中央空調遠程運作及維修管理應用。
- CNC 設備 5G 聯網解決方案。

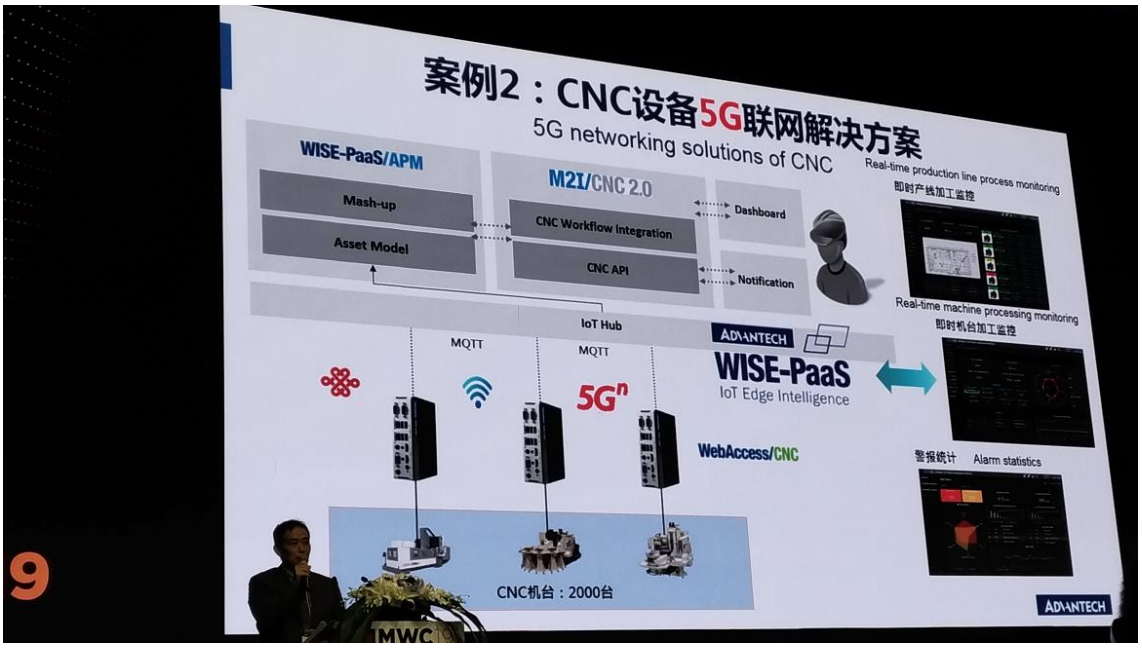


圖 22、研華科技未來物聯網演講現場

◆ 物聯網安全

安全在物聯網發展上扮演相當重要的因素。本次專題討論將重點放在物聯網價值鏈中，企業如何將安全納入考量。

在 2016 年以前物聯網的攻擊比較少見，但近年來網路駭客針對物聯網設備的攻擊不斷增加。由物聯網(IoT)組成的殭屍網路(Botnet)於 2016 年開始橫行全球，其中又以惡意軟體 Mirai 所造成的幾次分散式阻斷服務攻擊(DDoS)最為惡名昭彰。Mirai 與其他類似的惡意軟體能夠感染 IoT 裝置，將其納入由命令和控制伺服器(C&C Server)所操縱的殭屍網路，對特定目標發動攻擊。但有些物聯網設備製造商並非網路安全專家，因此忽略安全認證的重要性；再者業者考量加入安全性模組會增加設備製造成本，而不願意採取行動。但業者忽略了如果商品遭受攻擊，讓消費者產生安全性疑慮所帶來的商譽損失，遠比加入安全性考量所需付出成本來的高。

各國政府也意識到，物聯網安全威脅的問題逐漸加溫，因此各國也訂定出相關規範，希望能提高各界對物聯網

安全議題的重視。例如：

- 美國 2019 年的《物聯網網路安全改進法案》（Internet of Things Cybersecurity Improvement Act）。目標是建立一個框架，政府可以使用這個框架來確保安全聯網設備所需的特徵清單。該法案將確定安全設備要求的任務分配給熟知技術的美國國家標準與技術研究院（NIST）。由管理和預算辦公室（OMB）來指導聯邦機構如何採用 NIST 的指南。
- 英國數位文化媒體體育部(The Department for Digital, Culture, Media & Sport, DCMS)於 2018 年公佈關於「Secure by Design」的規範。除公告給製造商的「消費者物聯網設備安全實務作業規範」(Code of Practice for Consumer IoT Security)外，並有智慧家庭裝置的規範。更新版本包含 13 條主要規範內容，由 DCMS 及英國國家網路安全中心(NCSC)共同制定，並參考實務及學術界的相關建議。DCMS 指出，遵循本作業規範，可幫助個人資料保護的法律遵循作業，如 GDPR 要求安全處理個人資料。DCMS 強調，優先遵循前 3 條規範，可帶來安全效益。規範條文如下：
  (1) 禁止使用預設密碼：所有 IoT 設備的密碼應該都是唯一的，且不得被重設為出廠預設值。
  (2) 實施漏洞揭露政策：所有提供連接網路設備及服務的公司，應提供公開的連絡資訊作為漏洞揭露政策的一部分，使安全研究人員及其他人能夠提告問題。被公開的漏洞應及時處理。
  (3) 保持軟體更新：IoT 終端設備應公佈其生命週期政策，明確說明支援設備軟體更新的最短時間，以及採用此時間的原因。每次更新都應該向用戶清楚說明，而且需容易執行。對於無法執行更新的設備，可對其進行隔離或更換。

(4) 安全保存身分驗證資訊及安全敏感資料(security-sensitive data)：任何憑證都需安全地存放在服務和設備上。不可使用固定編碼在設備軟體中的憑證。

(5) 通訊安全：安全敏感性資料（包括所有遠端系統管理和控制資料）在傳輸過程中應該採用適當技術和使用方法進行加密，金鑰應該實施安全管理。

(6) 最小化暴露的攻擊面：所有設備和服務都應基於「最小許可權原則」運行；未使用的連接埠應關閉，硬體不得提供不必要的存取權限，服務在未開啟使用時應不可用，並應儘量減少代碼，僅保留使服務正常運行所需的最少代碼。軟體應以適當的許可權運行，同時考慮安全性和功能。

(7) 確保軟體的完整性：應使用安全啟動機制驗證 IoT 設備上的軟體。如果檢測到未經授權的更改，設備應向使用者/管理員發出警報。

(8) 確保個人資料受到保護：設備製造商和 IoT 服務提供者都應向消費者提供清晰、透明的資訊，說明其個人資料的使用方式、使用者以及使用目的。這也適用於可能涉及的任何第三方協力廠商（包括廣告商），若個人資料依據消費者的授權進行處理，則此授權應以合法、有效的方式獲得，並允許消費者隨時撤回。

(9) 使系統能從故障中迅速恢復：考量網路中斷或電力中斷的可能性，根據 IoT 設備和服務的用途或依賴於此的系統，若 IoT 設備和服務需要具備恢復機制，則應具備相對應內建恢復機制。

(10) 監控系統的遙測資料(telemetry data)：若利用 IoT 設備和服務收集遙測資料，如果使用和測量資料，則應監控是否存在安全異常。

(11)用戶能輕鬆的刪除個人資料：設備和服務的設置應允許消費者在轉讓設備所有權、刪除資料或處置設備時更容易刪除個人資料，且應向消費者提供有關如何刪除個人資料之明確說明

(12)使設備的安裝和維護簡單化：IoT 設備的安裝和維護應採用最少的步驟，並應遵循安全最佳做法，另外應向消費者提供有關如何安全設置設備的指引。

(13)驗證輸入的資料：通過使用者介面輸入的資料，以及通過應用程式設計發展介面 (API) 傳輸的資料或在服務和設備之間的網路傳輸的資料均應執行驗證。

- 歐盟ENISA(歐盟網路與資訊安全局,European Union Agency for Network and Information Security）所發佈物聯網用於關鍵資訊基礎建設的資訊安全基本線建議（Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures），目的在於為歐洲的物聯網奠定安全基礎。

圖 23、物聯網安全演講現場

3. Future Broadband Forum

在未來寬頻論壇中，邀請到韓國 KT 電信分享韓國 5G 的展望，韓國政府於今年 4 月正式商用 5G 網路服務，成為第一個進入 5G 時代的國家。韓國的 5G 發展速度很快，不到一個月就有了 26 萬用戶，到 6 月底已經超過百萬用戶。用戶成長速度相當快，其成功的原因，以採取低資費，並有中、高資費無限制流量及多裝置共享，多種方案可選。

除一般用戶連網，韓國 KT 電信也提出 5G 其他商業用途規劃，例如：

- 5G 救難用飛船，當發生重大災難時，機器人和搜救團隊在地面負責搜救任務，並透過天空的飛船建構臨時網路和外界連繫。
- KCITY 監控中心負責保障市民安全，例如當駕駛在高速公路上突然發生意外狀況、無法再駕駛時，KCITY 監控中心人員可以遠端操控車輛，將車子安全地停靠在路邊等應用。
- 智慧工廠應用，韓國 KT 電信和微軟、愛立信等大廠攜手，藉由 AR 和 MR 的虛實同步，透過 5G 執行遠端控制，幫助現場人員突破環境限制，達成檢修、組裝、監控目的。

圖 24、韓國 KT 電信分享 5G 展望演講現場

4. 5G Network Forum(5G 論壇)

今年是 5G 商用元年，在此論壇中將對 5G 的技術做探討，並對 5G 標準制定的網路切片（Networking Slicing），邊緣計算及網路服務架構和應用面的關聯進行分析及解說，會中就以下四個主題進行演說：

◆ 5G 網路：部署方案及網路能力

5G 的 8 大競爭優勢，包括高傳輸速度、高頻寬、低延遲、行動性、連接性、能源效率、部署規模及高可靠性。儘管 5G 商用標準明年才會定案，但在美國、歐洲、澳洲、韓國等國家，已有不少電信業者紛紛開跑，搶先推出 5G 服務，其餘各國也不甘示弱，加快 5G 部署腳步，5G 連網裝置及新款手機也從今年開始大爆發，全球 5G 市場正加速起飛。

國際電信標準制定組織 3GPP 相繼通過 R15 版的 5G 標準，包含 NR 標準的 NSA（Non-Standalone）和 SA（Standalone）版本，意味著相關設備商、電信營運商有更清楚的規格依循，能夠及早進行相容於標準的設備及系統開發或網路測試部署工作。NSA 版本用於非獨立組

網，用來規範在 4G 核心網路及無線接取網路（Radio Access Network）時，如何額外建置 5G 的無線接取網路，提供 4G+5G 的服務，例如在都會區提供速度更快的 5G，郊區或農村則仍以 4G 涵蓋；而 SA 版本的標準則可用於獨立組網，可用於電信業者從核心網路到無線接取網路均採用 5G 規格的情況。會議中，中國移動和中興等業者對 NSA 及 SA 版本的技術分析，並分享其布建規畫，先期以提供 NSA 加快服務上線，最終以實現 SA 為目標，且預測 NSA 及 SA 將會共存一段時間，共同協作提供 5G 服務。

◆ 室內覆蓋的挑戰及對策

5G 雖然具備多項優勢，但無線訊號的頻率越高，傳播效果越差，穿越障礙物的能力也越弱。室內接收對 5G 是一項挑戰，特別是更高頻毫米波訊號無法穿透牆壁。4G 時代行動通信商以支援雙模(蜂巢/Wi-Fi)手機來解決容量問題，Wi-Fi 分擔大量無線網路流量，證實雙模運作對於緩解日益增長的流量問題是有效的解決方案。5G 室內基地站參考設計的發佈，也被外界普遍解讀爲一種趨勢。5G 超密集組網的技術特點，將讓各大運營商考慮大量引入小型基地站以解決室內覆蓋問題，室內基地站因具備高度靈活性、容易部署和容易管控等技術特點，使其成爲 5G 室內通信的重要解決方案。對比傳統 Wi-Fi 技術不具備完備的移動性管理和安全管理能力，所以無法取代室內基地站。在 5G 時代，Wi-Fi 雖不能代替室內基地站，但 Wi-Fi 可作爲把 5G 網路轉化爲區域網路的技術手段，肩負起將室內設備接入 5G 的任務，因此 Wi-Fi 將會被併入 5G 的網路架構中。萬物互聯是 5G 特徵之一， 5G 室內基地站將會把家庭打造成一個完整的網路體系。未來從密碼鎖到室內空調、冰箱等家用電器的控制，甚至 VR 遊戲或其他 AI 智慧設備都需要底層 5G 網路連結，而 5G 室內基地

站，將實現家庭智慧生活的可行性。

◆ 5G 網路的演進路線和未來挑戰

5G 讓實現萬物互聯成為可能，而 5G 的網路切片技術在人和物的連結上扮演重要的角色，例如工業物聯網的應用，對應工廠內部各種複雜的應用場景，5G 支援網路切片(Network Slicing)將可依據終端應用需求，將網路「切開」給不同場景與族群使用，例如其低延遲特性可應用於要求零時差的工業控制需求，而高頻寬特性則可對應工廠內多媒體需求應用。網路切片可在單一網路「切片」成多個虛擬網路，每一個「切片」可以加以客製化滿足特定應用、服務和裝置的需求，同時提供一個安全的空間，用來儲存、分享和分析資料。更重要的是，每一個虛擬網路或「切片」可以隔離開來，可根據不同應用需求設定不同安全機制，一旦發生網路攻擊意外，可避免災情蔓延所有網路，提供更安全的網路環境。

而 AI 的引入讓 5G 應用更多元，例如工廠內的物流設備—自動導引車(Automated Guided Vehicle；AGV)過去須透過實體軌道鋪設固定其路線，當未來工廠面對彈性生產，產線更動將趨於頻繁，製造業者無法隨時配合硬體改造，而現有 AGV 可整合人工智慧(AI)與導航技術，利用即時定位、繪圖與機器視覺等技術在多變的工廠環境中計算最佳路徑，而這背後便是透過 5G 高速傳輸達到即時計算。

◆ 5G 新核心網的技術挑戰及對策

5G 帶動邊緣計算的興起，如果說 4G 是雲端計算的時代，那麼 5G 就是邊緣計算時代，因為 5G 的高傳輸速率和高度連結能力讓數據量大增，同時啟動物聯網市場的發展，5G 要連結萬物，需要在網路邊緣部署大量小規模或容易攜帶式數據中心，以滿足高可靠、低延遲的通訊需求，這就是邊緣計算。邊緣計算溝通真實世界和數位世界，

以功能定義其融合網路、計算、存儲、應用核心能力的分佈式開放平台，就近提供邊緣智慧服務，滿足產業數位化的連結、即時業務、數據優化、應用智慧化、安全與隱私保護等需求。邊緣計算的主要價值在於減少大流量對網路損耗，為各種應用提供低延遲和開放的網路能力，實現系統和服務智慧化。邊緣計算很難有標準化的可能，業界可透過成功案例分享，再擴展到不同領域的應用上，以提高數據使用效率並提升產能及創造更多的價值。

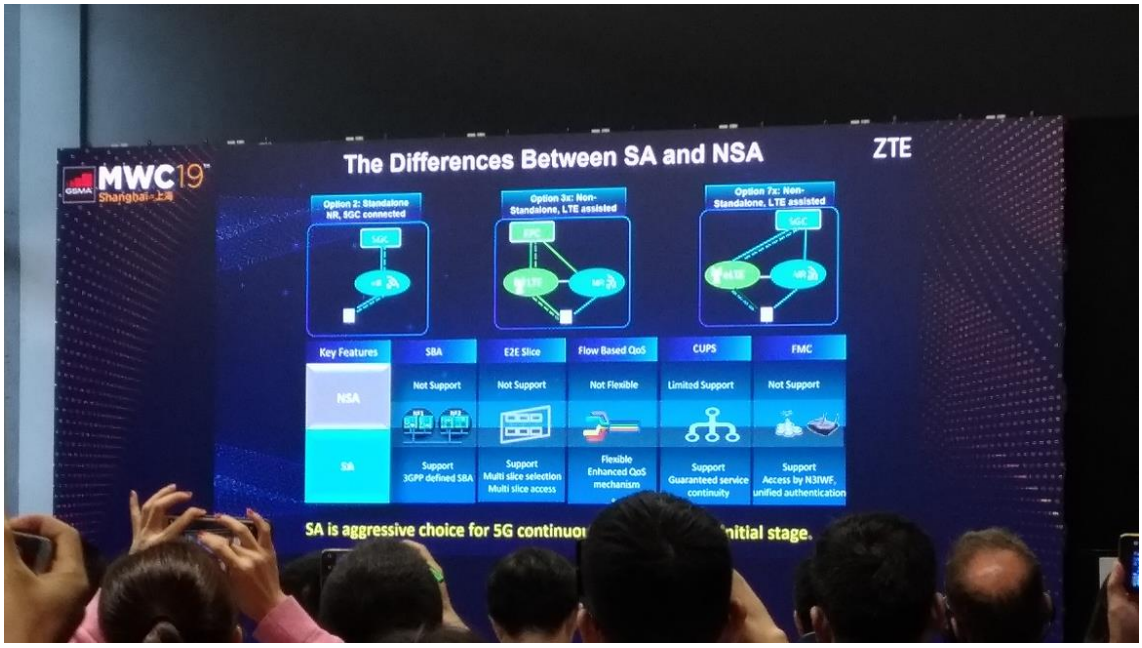


圖 25、5G 論壇演講現場

5. 5G Summit(5G 高峰會)

今年將有更多電信通訊服務商開始營運並商用化 5G 服務，但一般使用者所談論的 5G 可能與業界所努力研發的服務方向大相徑庭，此外，5G 的早期部署本質上是提供更快及更大的頻寬，還有 5G 另一個大目標是希望透過其所提供的動態網路切片以支援行動網路不同服務，目前要達到這個目標，實際仍存在著相當大的差異，這需要基礎設施建置及所有者、政府和專用網路及衛星服務供應商等之間合作，對現有的網

路架構做相當程度上的改變及調整，及建立新的合作夥伴關係。這關係到網路營運，服務層級協議（Service Level Agreement，SLA）管理，使用者界面與關係管理。透過這些元素的改變都有可能打造出全新的服務，而且這些服務也能在 4G LTE 網路仍然存在的情況下發揮作用。今年的 5G 高峰會，將回顧重要的業界所發佈的新聞，了解在推動實現 5G 目標的技術與業務方面有哪些進展，以及通訊服務商的業務發展。

本次 5G 高峰會的開場由巴塞隆納臨床醫院腸胃手術服務負責人 Antonio De Lacy 博士發表演說，主題為〝5G 遠距手術（5G Remote Surgery）〞。全球醫療環境仍然未達到所有區域都可提供高品質的醫療條件，每天在全球的各個角落不斷發生因無法獲得好的醫療而發生令人遺憾的事，而 5G 高頻寬及低延遲的特性，可應用於醫療手術上，讓國際醫療專家遠距指導，讓手術過程更加順利及提高成功率，為外科帶來革命性的改變，透過 MWC19 上海會展已經布建 5G 行動網路，Antonio De Lacy 博士在演說過程中和上海市東方醫院手術現場 Chuang-Gang Fu 博士所帶領的醫療團隊連線，作為第一次 5G 遠距醫療連線的展示，為 5G 醫療應用帶來全新的一頁，下圖為現場連線照片。

圖 26、5G 遠距手術演講和上海醫院手術現場連線

上海市東方醫院目前將 5G 應用在救護車的救治上，當病人上了救護車後，立刻透過 5G 將病人狀況經由高解析度的圖像送給醫院醫療團隊，在救護車上就可以開始進行醫療行為，當病人到達醫院時即可進入手術房開始進行手術，完成無縫的急救醫療過程。5G 在醫療上可以廣泛被利用，包含：

- ◆ 遠距醫療：經由國際專家提供指導，縮短區域醫療的差距。
- ◆ 醫療教學及會議：分享醫療技術。
- ◆ 透過遠距操作機器人進行醫療行為。
- ◆ 醫院管理：提高醫療資源的應用及改善醫院管理。

5G 除了相對 4G 有更高的頻寬、更快的傳輸速度及低延遲外，其在終端設備及網路傳輸端都有對資訊安全做加強，因此提高實現 5G 在醫療端應用的可行性。利用科技讓醫療平等化，為人類帶來更好的未來。

（二）MWC19 上海會場展覽

展覽會場主要電信服務和設備商，都集中精力展示在 5G 技術領域取得的成果及應用。5G 應用，下載一部 1080P 電影僅需不到 10 秒鐘，4K/8K 影片直播成為可能；5G 雲端游戲，借助雲端數據

中心，遊戲時間延遲可達到低於 30 毫秒；5G 機器人，透過連接雲端智慧大腦平台，可以陪人聊天說話，可以透過遠端操作執行任務，實現工業 4.0；AR/VR 應用，在 5G 及雲端技術基礎下，醫療、設計、社交、娛樂，透過 AR/VR 技術提供消費者全新的體驗。

1. 4K/8K 直播

   在 5G 低延遲、大頻寬的特性下，影音服務市場不僅持續 4G 時代的蓬勃發展，且更加擴大，電視台的實況直播就是其中一個例子。華為發表 5G 背包，在背包內搭載可隨處攜帶的 CPE（客戶終端設備），記者背在身上時，就成為一個 5G 基站，可以搭載 5G 傳播功能的攝影機連接，隨處就可進行「4K+5G」直播。

   中央廣播電視台在現場設置高解析互動體驗區，由中國移動提供 5G 遠程傳輸 8K 高解析電視節目，展現 5G 高傳輸及大頻寬的特性，相較 4K 影像內容，8K 超高解析內容色彩鮮豔、影像細節都明顯高出許多。

   除 4K/8K 影響直播外，在中國移動沉浸式體驗館，結合影像畫面數據分析 AI 人工智慧及 5G 賽事直播，為觀眾提供精采畫面分析和多視角畫面，提供觀眾不同以往的體育賽事轉播體驗。

圖 27、中央電視台 4K 直播

圖 28、中國移動和 SHARP 合作展示 5G+8K 直播

圖 29、5G 賽事直播及精采畫面分析展示

2. 機器人

5G 無人配送吸引眾多關注。中國聯通攜手美團、華為進行了 5G 網路的無人配送聯合示範。中國聯通將與合作夥伴一起，應用 5G 網路低延遲、大頻寬和高可靠性的優點，推動無人配送的商用化服務。該業務預計將於年底在北京冬奧園區試營運。

5G 醫院物流機器人，是華為與合作夥伴在中國醫科大學附屬第一醫院、華中科技大學同濟醫學院附屬同濟醫院、四川大學華西第二醫院等諸多醫院已經合作成功的案例。一個 5G 醫療機器人能夠代替 2-3 名醫護人員工作量，一個月替代醫護人員行走 220 公里；機器人與雲端能夠即時傳輸醫院環境視訊影像，進行障礙物識別和追踪，指引機器人在醫院複雜環境中順利行進；同時院內多台機器人能夠編隊運作，在 5G 高速網路運作下，安全性相對提升。

愛立信展示 5G 智慧工廠，在智慧工廠大規模機器人及機器手臂替代人力。5G 時代，機器人所組成建立的生產線的運作，將成為智慧製造的基本元素。機器人的靈活及彈性，簡化生產程序，提高工廠製造效率。

中國電信的展位上利用猜拳機器人展示 4G 和 5G 在傳輸速度及延遲性上的差別，5G 的低延遲特性，感測器捕捉使用者手勢的延遲低，在使用者出拳的那一刻，機器人捕捉到之後，就以超快的運算和通訊速度立即給出能贏使用者的結果，讓使用者看不出來，5G 的延遲可以低到人眼無法察覺的程度。對比 4G 通訊卻反應慢半拍，一眼就能看出它在作弊。

在智慧製造領域，機械手臂和機器人都可以不需要用到有線網路，內部整合 5G 的射頻(RF)系統就能做到和有線網路一致的即時性。美團、華為、中國聯通合作的 5G 無人派送就是典型示範。機器人身上載有高解析的攝影機，因此需要高頻寬傳送速率將資料回傳給控制台，現場工作人員表示：「現在就是從北京遠端控制這台上海的車。攝影機的影像資料直接傳到北京。」。其他如中興機器人演奏鋼琴、中國信科 5G 遠程駕駛、中國移動展位上的 5G 智慧製造示範，現場展台上的微型縮小機械臂和傳送帶可做真實示範等。

圖 30 、中興機器人演奏鋼琴

圖 31、中國移動展位上 5G 機器人示範

圖 32、美團和華為及中國聯通合作的配送機器人

圖 33、中國移動展位上的 5G 智慧製造示範

3. AR/VR

5G 商用更帶動 AR/VR 熱潮，在展場中可看到多個攤位展出 AR/VR 技術。

中國移動和 htc 合作，將 5G+4K+AR/VR 沉浸式互動體驗搬到 MWC 現場，包含清明上河圖、敦煌夢幻等在現場展示，讓觀眾有如親臨現場的體驗

vivo 在展位上除有 5G 手機外，AR 眼鏡引起相當多的關注，未來這款眼鏡將支援 AR 遊戲、辦公、電影院，及物體辨識、人臉辨識五大應用場景。vivo AR 眼鏡正面搭載了三顆鏡頭。中間的鏡頭負責拍照、人臉辨識的「圖像擷取」功能；左右兩顆則負責偵測環境，讓眼鏡可以達到定位追蹤功能。

在高通（Qualcomm）的展位上，vivo 和高通合作展出 AR 眼鏡 nreal light，只要和搭載高通 Snapdragon 855 處理器、並透過高通認證的手機，透過 USB-Type C 線連結，手機就可以成為眼鏡的運算主機，並分享網路給眼鏡。

中國電信展位也展出一系列的智慧社區應用，其中 AR 巡邏眼鏡，整合人臉辨識技術，透過 AR 眼鏡及時回覆結果，以保障社區安全。

圖 34、中國移動和 htc 合作 VR 體驗

圖 35、vivo nreal 5G AR 展示

4. 5G 設備

此次展覽 5G 為熱門話題，展場中可看到多家廠商展出 5G 設備。中國多家電信營運商除和華為合作外，也和國際大廠如諾基亞和愛立信等合作。諾基亞貝爾展位上展示和中國移動聯合推出的 AirScale mMIMO 天線(MAA)，這是一款目的在滿足中國市場在 5G 過渡的過程中所產生的大規模頻寬和覆蓋需求的產品。愛立信與中國移動一同做智慧工廠、應用網路、5G 網路切片技術、遠程醫療等項目。

中興展出一款約 A4 大小的 5G 小型基站，及 5G 室內路由器等產品。

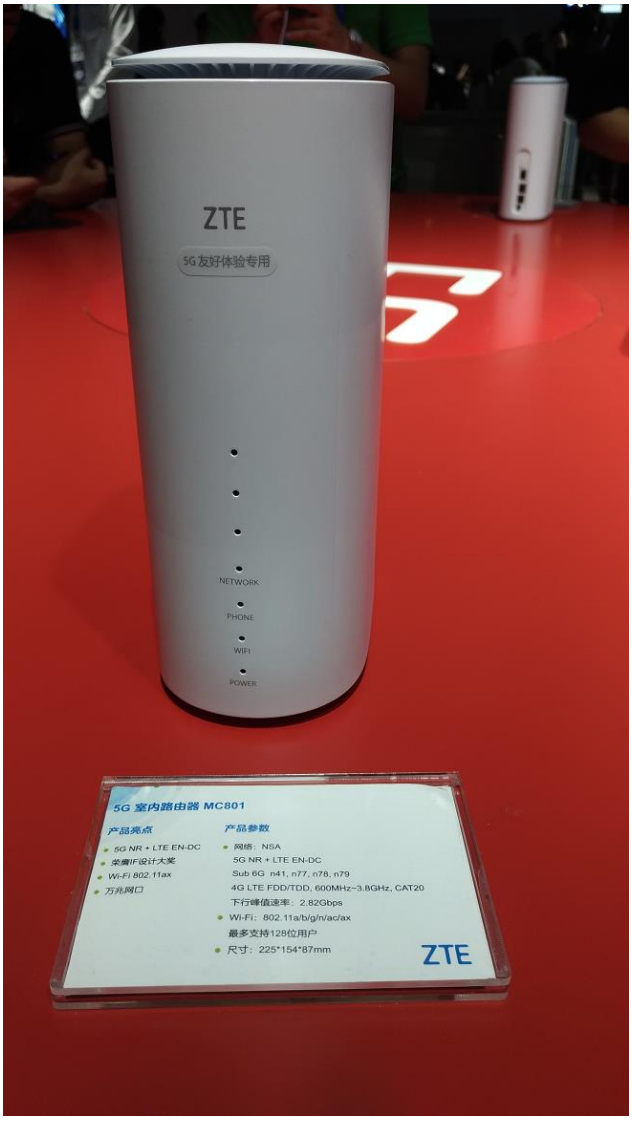


圖 36、中興 5G 室內路由器

5. 智慧城市

5G服務透過各種產業實現,也讓智慧城市的架構更為完整。近期上海強制推動垃圾分類，引發各方熱烈討論，中國電信趕上當地的話題潮流，推出智慧垃圾回收站，強調其功能包括監控、秤重、兌幣及身分識別，針對各種可回收垃圾即時秤重、計算價格，超過限定重量時會立刻通知管理人員，節省人力進行巡邏檢查成本。

6. 日月光

日月光本次也參與 MWC 智慧城市展，會場展示的一款自行車，內部包含環境光感測器、姿勢感測器、動作感測器等，功能包括智慧防盜、自動解鎖、UV 監控、透過動作辨識打方向燈、生命體監測、安全警報等多項功能。

圖 37、日月光參與智慧城市展

四、建議意見：

建議事項

- ☐ 本次會議過程中，以往同業之間大多以競爭者的姿態發表演說，但進入 5G 時代，一方面業者希望能更快為消費者提供服務，另一方面 5G 雖然有龐大的商機，但同時也需要龐大的投資，因此有些業者也希望透過合作聯盟的方式，以減少風險共創商機的想法，拋出同業合作的可能性，例如日本 KDDI、NTT Docomo 及 Softbank 合作富通信訊息應用，中國的電信業者也暢談合作議題，值得國內產業參考。
- ☐ 在 5G 之前時代，電信業者所扮演的角色大多停留在連網服務提供者上，但到了 5G 時代電信業者已經有明顯的角色轉變，業者談的是如何提供開放式的平台，攜手合作夥伴提供更好的應用服務，這種產業思維的轉變，值得國內 ISP 深入思考。
- ☐ 5G 的布建需要龐大的投資，尤其中國幅員廣大，要能提供大量覆蓋 5G 服務，對中國 ISP 業者是一大挑戰，因此業者為了能快速進入商用化市場，採取分階段執行由 NSA 先行，再到 SA 布建，及網路切片技術的應用等，值得國內業者參考，但也要考慮到分階段實行如何能滿足不同時期使用者及使用者所使用的終端設備能力的需求。
- ☐ 5G 正式進入商用化年代，全球預測物聯網裝置將以飛快的速度成長，物聯網裝置的安全也成了產業界關注的焦點，因此英國、美國及歐盟等，為物聯網裝置的安全性，訂定了安全規範及認證機制，為因應國內物聯網產業發展，政府相關單位也須重視此議題，訂立規範為產業發展鋪路。
- ☐ 5G 和物聯網是新一代數位科技發展的重點，近年相關國際技術研討和展覽活動非常頻繁，透過參與國際技術研討和展覽活動，吸取國際經驗，並與國際進行交流及經驗分享，有助國內產業政策制定，及作為國內產業發展方向的參考。

MWC 目前每一年會在巴塞隆納、上海及洛杉磯各舉辦一場，下一次會議及展覽將於 2019 年 10 月 22-24 日於美國洛杉磯舉行，相關資訊請參考 https://www.mwclosangeles.com/。

『IETF 105 Montreal Meetings』出國報告

財團法人台灣網路資訊中心因公出國人員報告書 108 年 8 月 2 日

報告人 姓　名	顧靜恆 許乃文 林福寬	服務單位及 職稱	組長 組長 工程師
出國期間	108/7/19-28	出國地點	Montreal, Canada
出國事由	參加 IETF 105 Montreal Meetings		

報告書內容包含：
一、 出國目的
二、 會議行程
三、 考察、訪問心得
四、 建議意見
五、 會議議程

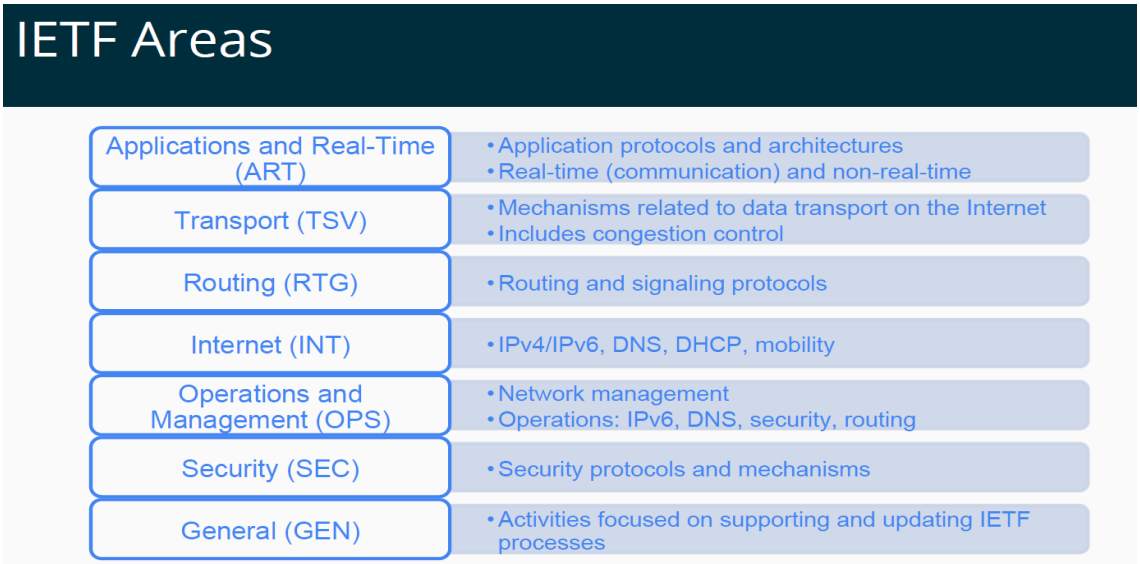
授　權 聲 明 欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人： 顧靜恆 許乃文 林福寬 (簽章)

註
二、請於授權聲明欄簽章，授權本中心重製發行公開利用。
附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

一、出國目的：

參加 IETF 105 Montreal 會議。

這是 IETF（網際網路工程任務小組, Internet Engineering Task Force）所舉辦的第 105 次會議，於 2019 年 07 月 20 日（星期六）至 2019 年 07 月 26 日（星期五）在加拿大蒙特婁召開，總共為期七天的會議，是由 COMCAST 與 NBCUniversal 共同主辦。本次參與會議人數高達 1,961 人，其中有 859 人是利用遠端會議系統的方式參與。會議主題共分為以下 7 大項目：

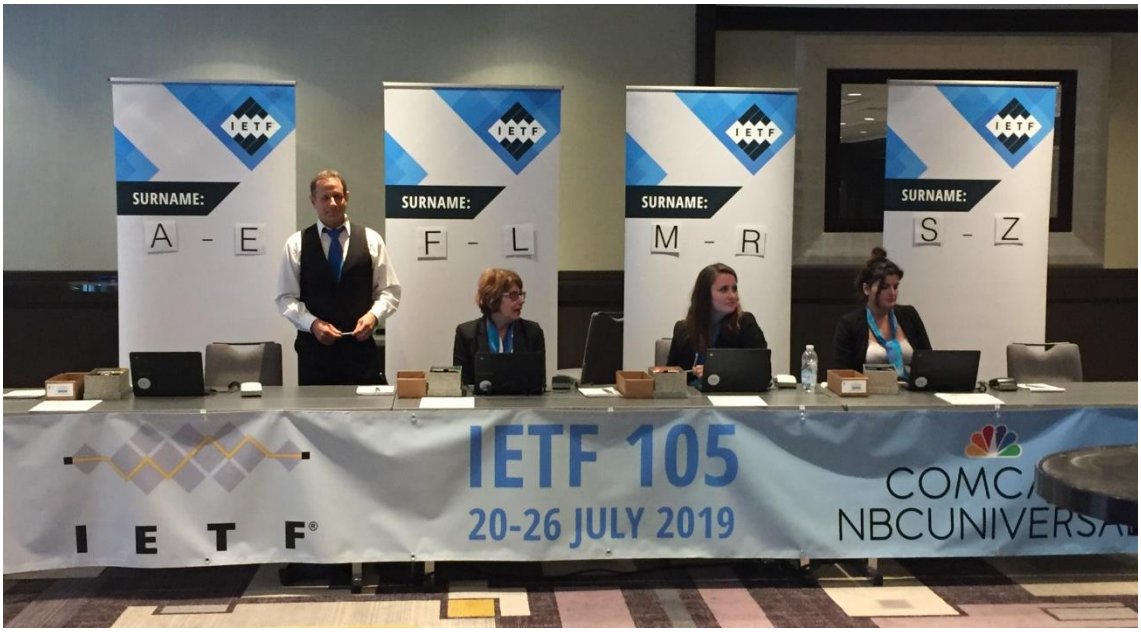


中心參加此次會議的主要目的為參與及了解各 WGs（Working Groups，工作小組）技術發展的趨勢及討論方向，包含 DNS、Security、EPP、IPv6 及 IoT 等相關議題。

Working Groups 是制定 IETF 技術規格和規範的主要機制，各小組負責不同技術規格的討論，並接收各方的意見加以修改，最終目的是要讓技術規格成為網際網路運作的標準或建議書，提供網際網路的技術開發團隊能有技術標準規格可做為依循，及保障全球網際網路能通行無礙。WGs 的運作方式是透過建立一個新的章程，該章

程定義特定問題及成果(包含建議、標準規範等)。各 Working Group 會有一位主席追蹤小組的運作狀況，並在章程規定小組的工作範圍，列出如何完成此項工作的目標和里程碑等資訊，每個 Working Group 都是由和其本身工作領域相關的技術人員參與。當完成目標後，Working Group 就會結束，但有些 Working Group 會隨著環境及應用的變化，不斷改進已建立的標準協議，則此 Working Group 就會持續維持運作狀態。所有進行中的 Working Group 可以在 IETF Datatracker 找到完整列表。

IETF Datatracker 查詢網站：https://datatracker.ietf.org/



圖：IETF 105 大會報到處

二、 會議行程：

詳如會議網站 https://www.ietf.org/how/meetings/105/ 。

議程 https://datatracker.ietf.org/meeting/105/agenda.html 。

IETF 網站 https://www.ietf.org/ 。

參與會議的行程安排如下表列：

日期	時間	議程
108/7/20 (六)	8:30-22:00	IETF Hackathon
108/7/21 (日)	8:30-16:00	IETF Hackathon
	10:00	IETF Registration
	12:30-13:30	Tutorial: Newcomers' Overview
	16:00-17:00	Newcomers' Quick Connections
108/7/22 (一)	8:00-9:00	Continental Breakfast
	9:00-19:10	IRTF Applied Networking Research Workshop (ANRW)
	10:00-12:00	Routing Area Working Group
	12:00-13:30	Break
	13:30-15:30	IPv6 over Networks of Resource-constrained Nodes WG
	15:30-15:50	Beverage and Snack Break
	15:50-17:50	IPv6 Operations WG
	18:10-19:10	Domain Name System Operations WG
108/7/23 (二)	8:00-9:00	Continental Breakfast
	10:00-12:00	Domain Name System Operations WG
	11:30-12:00	IP Wireless Access in Vehicular Environments WG
	12:00-13:30	Break
	13:30-15:00	Applications Doing DNS WG
	13:30-15:00	Security Events WG
	15:00-15:20	Beverage and Snack Break
	15:20-16:50	SIDR Operations WG
	17:10-18:10	IPv6 Maintenance
108/7/24 (三)	8:00-9:00	Continental Breakfast
	10:00-12:00	Software Updates for Internet of Things WG
	12:00-13:30	Break

	13:30-15:30	Thing-to-Thing WG
	15:30-15:50	Beverage Break
	15:50-16:50	Global Routing Operations WG
	16:50-17:10	Beverage and Snack Break
	17:10-18:10	IETF Technical Plenary
	18:20-19:50	IETF Administrative/Operations Plenary
108/7/25 (四)	8:00-9:00	Continental Breakfast
	10:00-12:00	Interface to Network Security Functions WG
	12:00-13:30	Break
	13:30-15:30	Extensions for Scalable DNS Service Discovery WG
	15:30-15:50	Beverage and Snack Break
	15:50-17:20	IPv6 Maintenance WG
	15:50-17:20	DNS PRIVate Exchange WG
	17:20-17:40	Beverage Break
	17:40-19:10	IPv6 over the TSCH mode of IEEE 802.15.4e WG
108/7/26 (五)	8:00-9:00	Continental Breakfast
	10:00-12:00	IPv6 over Low Power Wide-Area Networks WG
	12:00-12:20	Beverage and Snack Break
	12:20-13:50	Inter-Domain Routing WG

三、 考察、訪問心得：

IETF 105 Montreal 會議

圖：IETF 105 會場

於本次會議中，主要參與的主題包含 Hackathon、ANRW(Applied Networking Research Workshop)、DNS、註冊協議擴展(Registration Protocols Extensions)、IPv6 及 IoT 等領域的相關議題，分別整理如下：

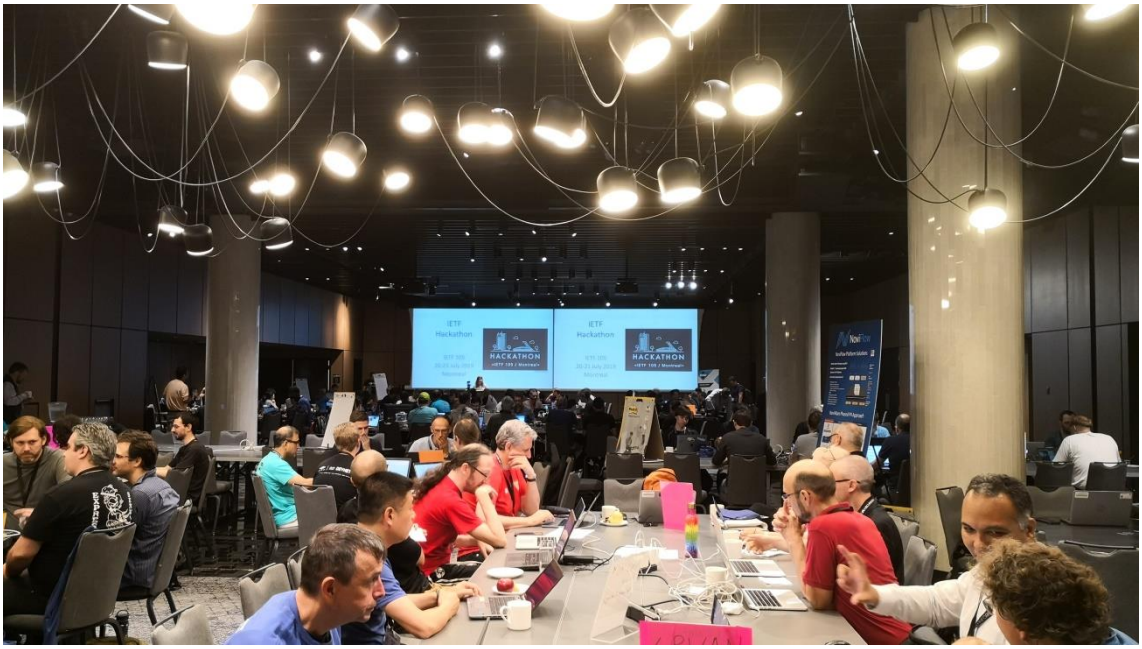
Hackathon

Hackathon 活動是 IETF 為鼓勵開發人員能在一個開放且協作的環境中，依據不同的主題分組面對面討論、交換彼此的想法、演示程式代碼、及尋求解決方案。任何的競爭都是良性的，並且秉持著持續發展新的或改良現有互聯網標準的精神前進。

本次 Hackathon 活動參與人數約有 384 名，分成 30 個不同的主題分組討論，並於第二天下午由各組進行 3 分鐘的簡短報告(下載連結)。此次會議主要參與 DNS 主題，內容包含：

1. DNS privacy：Zone transfers over TLS、DoH proxy plugin for any webserver、Preparing BIND for DoT/DoH。
2. DNS support for specific network environments：Identifier/Locator Network Protocol RRs、DNS64 prefix discovery。

3. DNS provisioning：Interoperable DNS server cookies、Timeout RR、HTTPSSVC。



圖：Hackathon 活動分組討論現況

詳細的 Hackathon 說明及參與方式，可以參考以下網址：
https://trac.ietf.org/trac/ietf/meeting/wiki/105hackathon

ANRW(Applied Networking Research Workshop)

ANRW 2019 是一個學術研討會，為研究人員、供應商、網路營運商和網際網路標準社群提供一個展示和討論研究新成果的論壇，也提供了一個機會，讓研究學者們，可以將其研究轉為 IETF 標準或協議，並且可以從討論的過程及公開的問題中，獲得新的靈感。本次研討會是由 ACM SIGCOMM 公司及 IRTF(Internet Research Task Force)所贊助。

此次 ANRW 所報告的主題，包含以下的內容：

1. A Performance Perspective on Web Optimized Protocol Stacks: TCP+TLS+HTTP/2 vs. QUIC

   比較現有瀏覽網頁的連線方式（TCP+TLS+HTTP/2）與未來預計使用的 QUIC 連線方式，兩者之間的性能差異。雖然傳統的連線方式，可以利用 TCP 參數的優化，讓 Web 堆疊的性

能直接產生顯著的改進，但，QUIC 的性能仍高於優化後的 TCP。這種性能優勢主要是由於 QUIC 在連接建立期間減少了 RTT 設計，並且由於其能夠繞過線路阻塞而導致網絡損耗。

2. Performance Measurements of QUIC Communications

在數據封包遺失、延遲和抖動方面的性能量測，是現代網路封包交換的關鍵。這些數值也明確地呈現出網路供應商的服務品質(QoS)，特別是在用戶使用諸如語音、視訊會議之類的實時通信時影響最大。因此，針對 QUIC 提出了一種新的性能量測方法，並與該領域的現有方式進行比較，透過對測試環境的實驗驗證和評估來顯示這些結果。

3. Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path

用戶使用網路透過 DNS 服務來解析域名時，可以使用 ISP（Internet Service Providers）預設提供的 DNS 主機、也可以自由選擇喜歡的公共 DNS 主機（例如：168.95.1.1 或 8.8.8.8）。但，少數 ISP 公司可能會利用路由設定，將向公共 DNS 主機的查詢秘密攔截轉由自身的 DNS 主機回應，而產生隱私和安全的問題。因此，本文分析大量 DNS 攔截的特徵後，設計了新的檢測 DNS 攔截方法，並利用全球 148,478 個家用及行動網路的 IP 位址，在檢查的 3,047 個 ASec 中，發現有 259 個出現 DNS 攔截的行為。為了解決此類問題，提供了新的見解。

4. Oblivious DNS: Practical Privacy for DNS Queries

使用網際網路服務時，幾乎都需要使用到 DNS 查詢服務，因此，用戶所拜訪（查詢）過的網站（域名）、及用戶的 IP 位址皆因此而被 DNS 主機記錄，而存在隱私漏洞的隱憂。因此，本文提出了一個新的 Oblivious DNS(ODNS)概念，在用戶端與 DNS 主機之間加入一個模糊層，利用他當緩衝而隱藏用戶的 IP 位位，並且相容於現有的 DNS 架構。

5. Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web

新型態的 DNS 查詢方式(Dot、DoH)，相較於傳統查詢方式(Do53)，雖然可以保護隱私，不會被窺視查詢的域名資料，

但，卻必須額外付出成本（回應時間增加）。因此，本文比較這三種查詢方式，分析當網路流量正常、壅塞等狀況時，對於瀏覽網頁時的載入速度影響程度為何？實驗結果得知，在正常狀況時，DoT 的網頁載入速度優於 Doh 及 Do53；但當網路壅塞時，Do53 載入速度最快。文中也提到，可以採取 opportunistic partial responses 或 wire format caching 方式，就能輕鬆提升 DNS 性能。

6. What Can You Learn from an IP?

由於原始網際網路的設計並不符合安全性，為避免竊聽者取得（或推測）使用者瀏覽的網頁內容，因此發展出許多加密體系，例如：加密的 DNS、HTTPS 等。但，加密不一定能保證匿名性或隱私性，只需要觀察使用者設備流量上的目標 IP 位址，依然可以推測出訪問的網站（域名）。

詳細的 ANRW 介紹，可以參考以下網址：https://irtf.org/anrw/2019/

DNS 相關技術討論

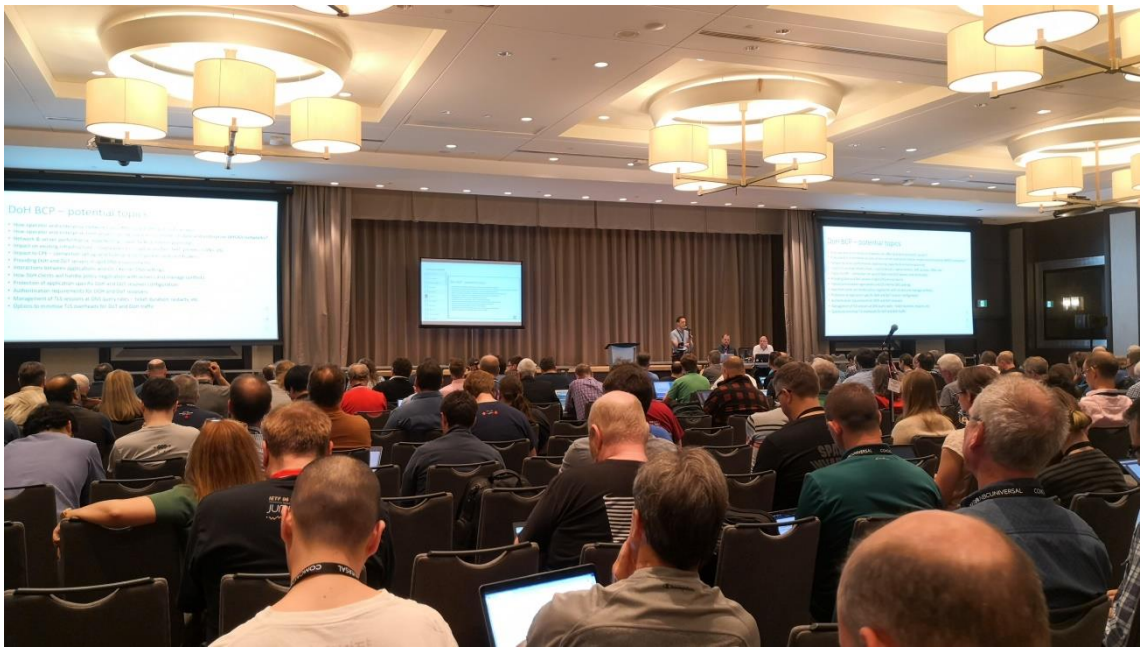
DNS 在工作小組的報告項目中，有幾個新式資源記錄雖然目前還在草案階段，但，值得留意未來發展的動向：

1. ANAME

由於目前 CNAME 使用上會有所限制，例如：域名本身(example.tw)無法設定 CNAME 到別的域名，只能多指定一層 subdomain(www.example.tw)才能使用 CNAME 記錄。因此，當網站使用 CDN 服務時，域名本身卻只能設定 A 或 AAAA 記錄，而造成諸多不便。網站使用 CDN 的優勢，就是透過 CNAME 到 CDN 所提供的域名，讓 CDN 根據地區、服務等條件，自動對應到合適的 IP，以提供最佳的網站服務。因此，產生了新的 RR 類型(ANAME)的概念（目前是草案第 04 版），以解決 CNAME 無法設定域名本身的問題。

域名本身設定為 ANAME 時，當查詢該域名的 A 記錄時，Resolver 回傳的資料中，在 ANSWER 的區塊中，顯示該筆域名的 ANAME 及 A 記錄，並將 AAAA 記錄顯示在 ADDITIONAL

區塊中；反之，查詢 AAAA 記錄時，則將 A 記錄顯示在 ADDITIONAL 區塊中。若查詢該域名的 ANAME 記錄時，則將 A 與 AAAA 記錄顯示在 ADDITIONAL 中。



圖：DNSOP 工作小組討論現況

2. HTTPSSVC

新的 HTTPSSVC 類型（目前是草案第 03 版），則是希望當使用者要連線至 Web Server 時，可以先藉由事前的 DNS 查詢，將該網站的相關資料先行取得，以減少與網站在連線前階段的溝通次數，以加快與網站的連線速度。而且，HTTPSSVC 類型，也可以像 ANAME 類型一樣，將域名本身指定到另一個域名的相關記錄上。

每一筆 HTTPSSVC 記錄中，可以包含幾個主要資訊：

(1) ALIAS 域名：指定轉至那一筆 A 或 AAA 記錄。
(2) HTTP 版本：指定使用 HTTP/2 或 HTTP/3 的方式連線。
(3) PORT 編號：若不是使用預設的 443 port 時，可以指定 Web Server 使用的 port 編號。
(4) ESNIKEY 資料：將該網站使用的 ESNI 公鑰的資料放在 DNS 記錄中，讓使用者事先查詢 DNS 時，即可取得。

不過，因為該 RR 類型，將原本由 Web Server 的工作，提前至 DNS 主機，當網站流量增加時，是否也會造成 DNS 主機的過量負荷？則須持續關注該記錄類型的後續發展。

有關於域名註冊服務，使用 EPP(Extensible Provisioning Protocol)執行移轉註冊商時，為避免移轉未獲合法授權而被冒名盜取域名所有權，有一個新草案規範了此移轉流程，但，這因為涉及 ICANN 的政策決定，而不是技術問題，因此，最後是否會成為標準，必須持續觀察。此草案的重點敘述如下：

1. 原註冊商(registrar)僅在用戶提出移轉(transfer)申請時，才產生（設定）授權碼(authinfo code)並提供給用戶，這個授權碼是有有時效性，待時間到期，註冊商須將授權碼移除。
2. 註冊商不儲存授權碼資料，他是存放在註冊局(registry)。
3. 註冊局是儲存授權碼經過 HASH 後的資料，而非明碼儲存。因此，註冊商無法查詢原來的授權碼資料，只能以重新設定的方式更新授權碼資料。
4. 待域名成功移轉至新註冊商時，註冊局必須將授權碼資料移除。

IPv6 相關技術討論

本次參與有關 IPv6 技術討論會議，包括下列幾個工作小組：

1. v6ops Working Group - IPv6 Operations
2. 6MAN Working Group - IPv6 Maintenance，
3. 6lo Working Group - IPv6 over Networks of Resource-constrained Nodes，

各工作小組的介紹如下：

1. v6ops Working Group - IPv6 Operations

IPv6 運營工作組（v6ops）為新的和現有的 IPv6 網路的佈署和操作制定了指南。v6ops 工作組的目標是：

(1).徵求網路營運商和用戶的意見，以確定 IPv6 網路營運的問題，並確定這些問題的解決方案或解決方法。

(2).徵求網路營運商和用戶的意見，以確定與 IPv4 網路的營運交互問題，並確定這些問題的解決方案或解決方法。

(3).徵求對僅 IPv6 操作中的問題和機會的討論和記錄，以及由此產生的創新。

(4).已確定問題的營運解決方案應在 v6ops 中制訂，並記錄在訊息或 BCP 草案中。
(5).記錄 IPv6 網路的操作要求。

詳細 v6ops 工作組章程請參考：
https://datatracker.ietf.org/group/v6ops/about/

2. 6MAN Working Group - IPv6 Maintenance

6man 工作組負責維護和推進 IPv6 協議規範和尋址架構。工作組將解決在佈署和運行期間發現的協議限制/問題。6man 是 IPv6 協議擴展和修改的設計權威。

詳細 6MAN 工作組章程請參考：
https://datatracker.ietf.org/group/6man/about/

3. 6lo Working Group - IPv6 over Networks of Resource-constrained Nodes

6lo 專注於通過約束節點網路促進 IPv6 連接的工作，具有以下特點：
*有限的功率，內存和處理資源；
*狀態，代碼空間和處理週期的硬上限；
*能源和網路頻寬使用的優化；
*缺少一些第 2 層服務，如完整的設備連接和廣播/多播。
6lo 適用於小型，重點突出的工作，但不承擔更大的跨層工作。只要合理和可能，工作組將繼續重用現有的協議和機制。

詳細 6lo 工作組章程請參考：
https://datatracker.ietf.org/group/6lo/about/
會中進行的主題包含以下內容：

1. 464XLAT Optimization

本文為第三版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，提出了可能的解決方案，以避免當目的地可用於 IPv6 時，IP / ICMP 轉換算法（SIIT）的某些缺點。 當 SIIT 用作 NAT46 且僅 IPv4 設備或應用程序啟動到雙協定 CDN（內容交付網絡），高速緩存或其他網路資源（在營運商網路或 Internet 中）的流量時，這些流量將轉通過 NAT64 換回 IPv4。這是

464XLAT 和 MAP-T 的情況。

詳細草案請參考：draft-palet-v6ops-464xlat-opt-cdn-caches-03

2. Neighbor Cache Entries on First-Hop Routers: Operational Considerations

本文為第一版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

Neighbor Discovery (RFC4861) is used by IPv6 nodes to determine the link-layer addresses of neighboring nodes as well as to discover and maintain reachability information. This document discusses how the neighbor discovery state machine on a first-hop router is causing user-visible connectivity issues when a new (not being seen on the network before) IPv6 address is being used.

詳細草案請參考：draft-linkova-v6ops-nd-cache-init-01

3. Operational Security Considerations for IPv6 Networks

本文為第 17 版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

Knowledge and experience on how to operate IPv4 securely is available: whether it is the Internet or an enterprise internal network. However, IPv6 presents some new security challenges. RFC 4942 describes the security issues in the protocol but network managers also need a more practical, operations-minded document to enumerate advantages and/or disadvantages of certain choices.

This document analyzes the operational security issues in several places of a network (enterprises, service providers and residential users) and proposes technical and procedural mitigations techniques. Some very specific places of a network such as the Internet of Things are not discussed in this document.

詳細草案請參考：draft-ietf-opsec-v6-17

4. IS-IS Multi Topology Deployment Considerations

本文為第 2 版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

This document analyzes IS-IS Multi Topology (MT) applicability in various deployments (Core/Mobile Backhaul/Data Center underlays). This document explores the nuances around the terminology and usage of various IS-IS address families, topologies with different considerations, for choosing the right combination for a specific deployment scenario.

This document also discusses various ways one can deploy IPv6 only IS-IS topology.

詳細草案請參考：draft-chunduri-lsr-isis-mt-deployment-cons-02

5. IPv6 Point-to-Point Links

本文為第 3 版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

This document describes different alternatives for configuring IPv6 point-to-point links, considering the prefix size, numbering choices and prefix pool to be used.

詳細草案請參考：draft-palet-v6ops-p2p-links-03

6. IPv6-Only Terminology Definition

本文為第 4 版發表於 IPv6 維運（IPv6 Operations，v6ops）工作小組，草案摘要如下：

This document defines the terminology regarding the usage of expressions such as "IPv6-only", in order to avoid confusions when using them in IETF and other documents. The goal is that the reference to "IPv6-only" describes the actual native functionality being used, not the actual protocol support.

詳細草案請參考：draft-palet-v6ops-ipv6-only-04

7. IPv6 Segment Routing Header (SRH)

本文為第 21 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Segment Routing can be applied to the IPv6 data plane using a new type of Routing Extension Header. This document describes the Segment Routing Extension Header and how it is used by Segment Routing capable nodes.

詳細草案請參考：draft-ietf-6man-segment-routing-header-21

8. ICMPv6 errors for discarding packets due to processing limits

本文為第 3 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Network nodes may discard packets if they are unable to process protocol headers of packets due to processing constraints or limits. When such packets are dropped, the sender receives no indication so it cannot take action to address the cause of discarded packets. This document defines ICMPv6 errors that can be sent by a node that discards packets because it is unable to process the protocol headers. A node that receives such an ICMPv6 error may be able to modify what it sends in future packets to avoid subsequent packet discards.

詳細草案請參考：draft-ietf-6man-icmp-limits-03

9. IPv6 Minimum Path MTU Hop-by-Hop Option

本文為第 2 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document specifies a new Hop-by-Hop IPv6 option that is used to record the minimum Path MTU along the forward path between a source to a destination host. This collects a minimum recorded MTU along the path to the destination. The value can then be communicated back to the source using the return Path MTU field in the option.

This Hop-by-Hop option is intended to be used in environments like Data Centers and on paths between Data Centers, to allow them to better take advantage of paths able to support a large Path MTU.

詳細草案請參考：draft-hinden-6man-mtu-option-02

10. IPv6 Neighbor Discovery on Wireless Networks

本文為第 3 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document describes how the original IPv6 Neighbor Discovery and Wireless ND (WiND) can be applied on various abstractions of wireless media.

詳細草案請參考：draft-thubert-6man-ipv6-over-wireless-03

11. IPv6 Neighbor Discovery Unicast Lookup

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document updates RFC 8505 in order to enable unicast address lookup from a 6LoWPAN Border Router acting as an Address Registrar.

詳細草案請參考：draft-thubert-6lo-unicast-lookup-00

12. Discovering PREF64 in Router Advertisements

本文為第 3 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document specifies a Router Advertisement option to communicate NAT64 prefixes to clients.

詳細草案請參考：draft-ietf-6man-ra-pref64-03

13. IPv6 Support for Segment Routing: SRv6+

本文為第 4 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document describes SRv6+. SRv6+ is a Segment Routing (SR) solution that leverages IPv6. It supports a wide variety of use-cases while remaining in strict compliance with IPv6 specifications. SRv6+ is optimized for for ASIC-based forwarding devices that operate at high data rates.

詳細草案請參考：draft-bonica-spring-srv6-plus-04

14. The IPv6 Compressed Routing Header (CRH)

本文為第 5 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document defines a new IPv6 Routing header type, called the Compressed Routing Header (CRH). SRv6+ nodes use the CRH to steer packets from segment to segment along SRv6+

paths.

詳細草案請參考：draft-bonica-6man-comp-rtg-hdr-05

15. The Per-Path Service Instruction (PPSI) Option

本文為第 6 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

SRv6+ encodes Per-Path Service Instructions (PPSI) in a new IPv6 option, called the PPSI Option. This document describes the PPSI Option.

詳細草案請參考：draft-bonica-6man-vpn-dest-opt-06

16. The Per-Segment Service Instruction (PSSI) Option

本文為第 4 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

SRv6+ encodes Per-Segment Service Instructions (PSSI) in a new IPv6 option, called the PSSI Option. This document describes the PSSI Option.

詳細草案請參考：draft-bonica-6man-seg-end-opt-04

17. Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)

本文為第 3 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document defines building blocks for Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Dataplane (SRv6). The document also describes some SRv6 OAM mechanisms.

詳細草案請參考：draft-ali-6man-spring-srv6-oam-03

18. Service-aware IPv6 Network

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

A multitude of applications are carried over the network,

which have varying needs for network bandwidth, latency, jitter, and packet loss, etc. Some applications such as online gaming and live video streaming have very demanding network requirements thereof require special treatments in the network. However, since the current network is lack of enough information of service requirements of such applications it is difficult to guarantee the SLA or it may take long time to provide such guarantee. This document proposes the solution to make use of IPv6 extensions header to convey the service requirement information along with the packet to the network to facilitate the service deployment and network resource adjustment to guarantee SLA for applications. Then it defines the service-aware options which can be used in the different IPv6 extension headers for the purpose.

詳細草案請參考：draft-li-6man-service-aware-ipv6-network-00

19. Consideration of IPv6 Encapsulation for SFC and IFIT

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Service Function Chaining (SFC) and In-situ Flow Information Telemetry (IFIT) are important path services along with the packets. In order to support these services, several encapsulations have been defined. The document analyzes the problems of these encapsulations in the IPv6 scenario and proposes the possible optimized encapsulation for IPv6.

詳細草案請參考：draft-li-6man-ipv6-sfc-ifit-01

20. Encapsulation of Path Segment in SRv6

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

Segment Routing (SR) allows for a flexible definition of end-to-end paths by encoding paths as sequences of sub-paths, called "segments". Segment routing architecture can be implemented over IPv6 data plane, called SRv6. In some use-cases such as end-to-end SR Path Protection and Performance Measurement (PM), SRv6 path need to be identified. This document defines the encoding and processing of Path Segment in SRv6 networks.

詳細草案請參考：draft-li-6man-srv6-path-segment-encap-00

21. Segment Routing Header encapsulation for In-situ OAM Data

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

OAM and PM information from the SR endpoints can be piggybacked in the data packet. The OAM and PM information piggybacking in the data packets is also known as In-situ OAM (IOAM). IOAM records operational and telemetry information in the data packet while the packet traverses a path between two points in the network. This document defines how IOAM data fields are transported as part of the Segment Routing with IPv6 data plane (SRv6) header.

詳細草案請參考：draft-ali-spring-ioam-srv6-01

22. DetNet SRv6 Data Plane Encapsulation

本文為第 1 版發表於 IPv6 維護（IPv6 Maintenance，6MAN）工作小組，草案摘要如下：

This document specifies Deterministic Networking data plane operation for SRv6 encapsulated user data.

詳細草案請參考：draft-geng-detnet-dp-sol-srv6-01

23. Transmission of IPv6 Packets over Near Field Communication

本文為第 15 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

Near field communication (NFC) is a set of standards for smartphones and portable devices to establish radio communication with each other by touching them together or bringing them into proximity, usually no more than 10 cm apart. NFC standards cover communications protocols and data exchange formats, and are based on existing radio-frequency identification (RFID) standards including ISO/IEC 14443 and FeliCa. The standards include ISO/IEC 18092 and those defined by the NFC Forum. The NFC technology has been widely implemented and available in mobile phones, laptop computers, and many other

devices. This document describes how IPv6 is transmitted over NFC using 6LoWPAN techniques.

詳細草案請參考：draft-ietf-6lo-nfc-15

24. Packet Delivery Deadline time in 6LoWPAN Routing Header

本文為第 5 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document specifies a new type for the 6LoWPAN routing header containing the deadline time for data packets, designed for use over constrained networks. The deadline time enables forwarding and scheduling decisions for time critical IoT machine to machine (M2M) applications that operate within time-synchronized networks that agree on the meaning of the time representations used for the deadline time values.

詳細草案請參考：draft-ietf-6lo-deadline-time-05

25. 6LoWPAN Fragment Forwarding

本文為第 3 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document provides a simple method to forwarding 6LoWPAN fragments. When employing adaptation layer fragmentation in 6LoWPAN, it may be beneficial for a forwarder not to have to reassemble each packet in its entirety before forwarding it. This has always been possible with the original fragmentation design of RFC4944. This method reduces the latency and increases end-to-end reliability in route-over forwarding. It is the companion to the virtual Reassembly Buffer which is a pure implementation technique.

詳細草案請參考：draft-ietf-6lo-minimal-fragment-03

26. 6LoWPAN Selective Fragment Recovery

本文為第 5 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，

草案摘要如下：

This draft updates RFC 4944 with a simple protocol to recover individual fragments across a route-over mesh network, with a minimal flow control to protect the network against bloat.

詳細草案請參考：draft-ietf-6lo-fragment-recovery-05

27. IPv6 over Constrained Node Networks (6lo) Applicability & Use cases

本文為第 6 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document describes the applicability of IPv6 over constrained node networks (6lo) and provides practical deployment examples. In addition to IEEE 802.15.4, various link layer technologies such as ITU-T G.9959 (Z-Wave), BLE, DECT-ULE, MS/TP, NFC, PLC (IEEE 1901.2), and IEEE 802.15.4e (6tisch) are used as examples. The document targets an audience who like to understand and evaluate running end-to-end IPv6 over the constrained node networks connecting devices to each other or to other devices on the Internet (e.g. cloud infrastructure).

詳細草案請參考：draft-ietf-6lo-use-cases-06

28. IPv6 Neighbor Discovery Unicast Lookup

本文為第 1 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，草案摘要如下：

This document updates RFC 8505 in order to enable unicast address lookup from a 6LoWPAN Border Router acting as an Address Registrar.

詳細草案請參考：draft-thubert-6lo-unicast-lookup-00

29. Asymmetric IPv6 for IoT Networks

本文為第 1 版發表於資源受限節點上的 IPv6 網路（IPv6 over Networks of Resource-constrained Nodes，6lo）工作小組，

草案摘要如下：

This document describes a new approach to IPv6 header compression for use in scenarios where minimizing packet size is crucial but routing performance must be maximised.

詳細草案請參考：draft-jiang-asymmetric-ipv6-01

IoT 相關技術討論

本次參與有關 IoT 技術討論會議，包括下列幾個工作小組：

1. suit Working Group - Software Updates for Internet of Things；
2. 6TiSCH Working Group - IPv6 over the TSCH mode of IEEE 802.15.4e；(TSCH is the abbreviation of Time Slotted Channel Hopping)
3. lpwan Working Group - IPv6 over Low Power Wide-Area Networks；
4. t2trg Working Group - Thing-to-Thing。

各工作小組的介紹如下：

1. suit Working Group - Software Updates for Internet of Things；

物聯網（IoT）設備中的漏洞引發了對安全韌體更新機制的需求，該機制也適用於受約束設備。安全專家，研究人員和監管機構建議所有物聯網設備都配備這樣的機制。

韌體更新解決方案包含多個組件，包括：

*將韌體映像傳輸到相容設備的機制。

*提供有關韌體映像的後設資料(meta-data)清單（例如韌體包標識符，程序包需要運行的硬體以及對其他韌體包的依賴性），以及用於保護韌體映像的加密信息。

*韌體映像本身。

詳細 suit 工作組章程請參考：
https://datatracker.ietf.org/group/suit/about/

2. 6TiSCH Working Group - IPv6 over the TSCH mode of IEEE 802.15.4e；(TSCH is the abbreviation of Time Slotted Channel Hopping)

低功耗和有損網路（Low-power and Lossy Networks，LLN）

將可能因大量的資源受限節點互連以形成無線網狀網路。IEEE802.15.4TSCH 網路中的節點通過遵循時分多址（TDMA）調度進行通訊。該調度中的時隙提供了為相鄰節點之間的通訊分配的頻寬單位。可以對分配進行編程，使得可預測的傳輸模式與流量匹配。

這些技術為 LLN 提供了一系列新的使用案例，包括：

- 無線過程控制網路中的控制環路，其中需要高可靠性和完全確定性的行為。
- 從不同的獨立客戶端傳輸數據的服務提供商網路，營運商需要流量隔離和流量整形。
- 包括能量收集節點的網路，其需要極低且可預測的平均功耗。

詳細 6TiSCH 工作組章程請參考：
https://datatracker.ietf.org/group/6tisch/about/

3. lpwan Working Group - IPv6 over Low Power Wide-Area Networks；

新一代無線技術以低功耗廣域（LPWA）的通用名稱出現，具有許多共同特徵，使這些技術成為物聯網應用的獨特和破壞性。

為了釋放 LPWA 技術及其生態系統的全部功能，需要將它們與其他生態系統相結合，通過引入網路層來保證交互工作，並為管理和安全性以及共享應用程序配置文件啟用通用組件。IETF 可以通過提供 IPv6 連接做出貢獻，並提出保護操作和管理設備及其網關的技術。

工作組將重點關注通過以下選擇的低功耗廣域技術實現 IPv6 連接：SIGFOX，LoRa，WI-SUN 和 NB-IOT。

詳細 lpwan 工作組章程請參考：
https://datatracker.ietf.org/group/lpwan/about/

4. t2trg Working Group - Thing-to-Thing。

該物對物的研究組（T2TRG）將開放研究一個真正的“物聯網”變為現實的問題。物聯網其中低資源節點能夠之間溝通自己和與更廣泛的互聯網，以參與無權創新。T2TRG 的重點將從設備連接到 IP 的適配層開始，並在應用層結束。具有用於通訊和

製作數據和管理功能的架構和 API（包括安全功能）。

工作組已經確定了一些感興趣的領域，包括：

*了解單用途筒倉和網關的動機，促進小塊鬆散地連接（因此“物到物”）；支持擴展單個網路中的應用程序數量。

*部署注意事項； 規模考量； 擁有成本。

*“物”的管理和操作。

*生命週期方面（包括但不限於安全性考慮）。

*與 W3C 的合作，例如，數據模型，格式和語義。

詳細 t2trg 工作組章程請參考：
https://datatracker.ietf.org/group/t2trg/about/

會中進行的主題包含以下內容：

1. A Firmware Update Architecture for Internet of Things Devices

本文為第 5 版發表於物聯網軟體更新（Software Updates for Internet of Things，suit）工作小組，草案摘要如下：

Vulnerabilities with Internet of Things (IoT) devices have raised the need for a solid and secure firmware update mechanism that is also suitable for constrained devices. Incorporating such update mechanism to fix vulnerabilities, to update configuration settings as well as adding new functionality is recommended by security experts.

This document lists requirements and describes an architecture for a firmware update mechanism suitable for IoT devices. The architecture is agnostic to the transport of the firmware images and associated meta-data.

This version of the document assumes asymmetric cryptography and a public key infrastructure. Future versions may also describe a symmetric key approach for very constrained devices.

詳細草案請參考：draft-ietf-suit-architecture-05

2. Firmware Updates for Internet of Things Devices - An Information Model for Manifests

本文為第 3 版發表於物聯網軟體更新（Software Updates for Internet of Things，suit）工作小組，草案摘要如下：

Vulnerabilities with Internet of Things (IoT) devices have raised the need for a solid and secure firmware update mechanism that is also suitable for constrained devices. Incorporating such an update mechanism to fix vulnerabilities, to update configuration settings, as well as adding new functionality is recommended by security experts.

One component of such a firmware update is a concise and machine-processable meta-data document, or manifest, that describes the firmware image(s) and offers appropriate protection. This document describes the information that must be present in the manifest.

詳細草案請參考：draft-ietf-suit-information-model-03

3. SUIT CBOR manifest serialisation format

本文為第 5 版發表於物聯網軟體更新（Software Updates for Internet of Things，suit）工作小組，草案摘要如下：

This specification describes the format of a manifest. A manifest is a bundle of metadata about the firmware for an IoT device, where to find the firmware, the devices to which it applies, and cryptographic information protecting the manifest.

詳細草案請參考：draft-moran-suit-manifest-05

4. An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4

本文為第 24 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document describes a network architecture that provides low-latency, low-jitter and high-reliability packet delivery. It combines a high-speed powered backbone and subnetworks using IEEE 802.15.4 time-slotted channel hopping (TSCH) to meet the requirements of LowPower wireless deterministic applications.

詳細草案請參考：
draft-ietf-6tisch-architecture-24

5. Minimal Security Framework for 6TiSCH

本文為第 12 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document describes the minimal framework required for a new device, called "pledge", to securely join a 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e) network. The framework requires that the pledge and the JRC (join registrar/coordinator, a central entity), share a symmetric key. How this key is provisioned is out of scope of this document. Through a single CoAP (Constrained Application Protocol) request-response exchange secured by OSCORE (Object Security for Constrained RESTful Environments), the pledge requests admission into the network and the JRC configures it with link-layer keying material and other parameters. The JRC may at any time update the parameters through another request-response exchange secured by OSCORE. This specification defines the Constrained Join Protocol and its CBOR (Concise Binary Object Representation) data structures, and configures the rest of the 6TiSCH communication stack for this join process to occur in a secure manner. Additional security mechanisms may be added on top of this minimal framework.

詳細草案請參考：draft-ietf-6tisch-minimal-security-12

6. 6tisch Zero-Touch Secure Join protocol

本文為第 4 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document describes a Zero-touch Secure Join (ZSJ) mechanism to enroll a new device (the "pledge") into a IEEE802.15.4 TSCH network using the 6tisch signaling mechanisms. The resulting device will obtain a domain specific credential that can be used with either 802.15.9 per-host pair keying protocols, or to obtain the network-wide key from a coordinator.

The mechanism describe here is an augmentation to the one-touch mechanism described in [I-D.ietf-6tisch-minimal-security], and is a profile of the constrained voucher mechanism [I-D.ietf-anima-constrained-voucher].

詳細草案請參考：draft-ietf-6tisch-dtsecurity-zerotouch-join-04

7. IEEE802.15.4 Informational Element encapsulation of 6tisch Join and Enrollment Information

本文為第 1 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

In TSCH mode of IEEE802.15.4, as described by [RFC8180], opportunities for broadcasts are limited to specific times and specific channels. Nodes in a TSCH network typically frequently send Enhanced Beacon (EB) frames to announce the presence of the network. This document provides a mechanism by which small details critical for new nodes (pledges) and long sleeping nodes may be carried within the Enhanced Beacon.

詳細草案請參考：
draft-ietf-6tisch-enrollment-enhanced-beacon-01

8. 6TiSCH Minimal Scheduling Function (MSF)

本文為第 5 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This specification defines the 6TiSCH Minimal Scheduling Function (MSF). This Scheduling Function describes both the behavior of a node when joining the network, and how the communication schedule is managed in a distributed fashion. MSF builds upon the 6TiSCH Operation Sublayer Protocol (6P) and the Minimal Security Framework for 6TiSCH.

詳細草案請參考：draft-ietf-6tisch-msf-05

9. Robust Scheduling against Selective Jamming in 6TiSCH Networks

本文為第 2 版發表於 IPv6 基於 IEEE 802.15.4e 的 TSCH 模式（IPv6 over the TSCH mode of IEEE 802.15.4e，6TiSCH）工作小組，草案摘要如下：

This document defines a method to generate robust TSCH schedules in a 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4-2015) network, so as to protect network nodes against selective jamming attack. Network nodes independently compute the new schedule at each slotframe, by altering the one originally

available from 6top or alternative protocols, while preserving a consistent and collision-free communication pattern. This method can be added on top of the minimal security framework for 6TiSCH.

詳細草案請參考：draft-tiloca-6tisch-robust-scheduling-02

10.LPWAN Static Context Header Compression (SCHC) and fragmentation for IPv6 and UDP

本文為第 18 版發表於 IPv6 低功耗廣域網路(IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This document defines the Static Context Header Compression (SCHC) framework, which provides both header compression and fragmentation functionalities. SCHC has been designed for Low Power Wide Area Networks (LPWAN).

SCHC compression is based on a common static context stored in both the LPWAN device and the network side. This document defines a header compression mechanism and its application to compress IPv6/UDP headers.

This document also specifies a fragmentation and reassembly mechanism that is used to support the IPv6 MTU requirement over the LPWAN technologies. Fragmentation is needed for IPv6 datagrams that, after SCHC compression or when such compression was not possible, still exceed the layer-2 maximum payload size.

The SCHC header compression and fragmentation mechanisms are independent of the specific LPWAN technology over which they are used. This document defines generic functionalities and offers flexibility with regard to parameter settings and mechanism choices.

This document standardizes the exchange over the LPWAN between two SCHC entities. Settings and choices specific to a technology or a product are expected to be grouped into profiles, which are specified in other documents. Data models for the context and profiles are out of scope.

詳細草案請參考：draft-ietf-lpwan-ipv6-static-context-hc-18

11.SCHC over Sigfox LPWAN

本文為第 1 版發表於 IPv6 低功耗廣域網路（IPv6 over Low

Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

The Static Context Header Compression (SCHC) specification describes a header compression scheme and a fragmentation functionality for Low Power Wide Area Network (LPWAN) technologies. SCHC offers a great level of flexibility that can be tailored for different LPWAN technologies.

The present document provides the optimal parameters and modes of operation when SCHC is implemented over a Sigfox LPWAN.

詳細草案請參考：draft-ietf-lpwan-schc-over-sigfox-00

12.Static Context Header Compression (SCHC) over LoRaWAN

本文為第 2 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

The Static Context Header Compression (SCHC) specification describes generic header compression and fragmentation techniques for LPWAN (Low Power Wide Area Networks) technologies. SCHC is a generic mechanism designed for great flexibility, so that it can be adapted for any of the LPWAN technologies.

This document provides the adaptation of SCHC for use in LoRaWAN networks, and provides elements such as efficient parameterization and modes of operation. This is called a profile.

詳細草案請參考：draft-ietf-lpwan-schc-over-lorawan-02

13.Data Model for Static Context Header Compression (SCHC)

本文為第 1 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This document describes a YANG data model for the SCHC (Static Context Header Compression). A generic module is defined, that can be applied for any headers and also a specific model for the IPv6 UDP protocol stack is also proposed. Note that this draft is a first attempt to define a YANG data module for SCHC, more work is needed to use all the YANG facilities.

詳細草案請參考：draft-toutain-lpwan-schc-yang-data-model-00

14.LPWAN Static Context Header Compression (SCHC) for CoAP

本文為第 9 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

This draft defines the way SCHC header compression can be applied to CoAP headers. CoAP header structure differs from IPv6 and UDP protocols since the CoAP use a flexible header with a variable number of options themself of a variable length. Another important difference is the asymmetry in the header format used in request and response messages. Most of the compression mechanisms have been introduced in [I-D.ietf-lpwan-ipv6-static-context-hc], this document explains how to use the SCHC compression for CoAP.

詳細草案請參考：draft-ietf-lpwan-coap-static-context-hc-09

15.OAM for LPWAN using Static Context Header Compression (SCHC)

本文為第 1 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

With IP protocols now generalizing to constrained networks, users expect to be able to Operate, Administer and Maintain them with the familiar tools and protocols they already use on less constrained networks.

OAM uses specific messages sent into the data plane to measure some parameters of a network. Most of the time, no explicit values are sent is these messages. Network parameters are obtained from the analysis of these specific messages.

This can be used:

- To detect if a host is up or down.
- To measure the RTT and its variation over time.
- To learn the path used by packets to reach a destination.

-AM in LPWAN is a little bit trickier since the bandwidth is limited and extra traffic added by OAM can introduce perturbation on regular transmission.

Two scenarios can be investigated:

- OAM coming from internet. In that case, the NGW should act as a proxy and handle specifically the OAM traffic.
- OAM coming from LPWAN devices: This can be included into regular devices but some specific devices may be installed in the LPWAN network to measure its quality.

The primitive functionalities of OAM are achieved with the

ICMPv6 protocol.

ICMPv6 defines messages that inform the source of IPv6 packets of errors during packet delivery. It also defines the Echo Request/Reply messages that are used for basic network troubleshooting (ping command). ICMPv6 messages are transported on IPv6.

This document describes how basic OAM is performed on Low Power Wide Area Networks (LPWANs) by compressing ICMPv6/IPv6 headers and by protecting the LPWAN network and the Device from undesirable ICMPv6 traffic.

詳細草案請參考：draft-barthel-lpwan-oam-schc-00

16.RTO considerations in LPWAN

本文為第 1 版發表於 IPv6 低功耗廣域網路（IPv6 over Low Power Wide-Area Networks，lpwan）工作小組，草案摘要如下：

Low-Power Wide Area Network (LPWAN) technologies are characterized by very low physical layer bit and message transmission rates. Moreover, a response to a message sent by an LPWAN device may often only be received after a significant delay. As a result, Round-Trip Time (RTT) values in LPWAN are often (sometimes, significantly) greater than typical default values of Retransmission TimeOut (RTO) algorithms. Furthermore, buffering at network elements such as radio gateways may interact negatively with LPWAN technology transmission mechanisms, potentially exacerbating RTTs by up to several orders of magnitude. This document provides guidance for RTO settings in LPWAN, and describes an experimental dual RTO algorithm for LPWAN.

詳細草案請參考：draft-gomez-rto-considerations-lpwan-00

17.RESTful Design for Internet of Things Systems

本文為第 4 版發表於物到物（Thing-to-Thing，t2trg）工作小組，草案摘要如下：

This document gives guidance for designing Internet of Things (IoT) systems that follow the principles of the Representational State Transfer (REST) architectural style. This document is a product of the IRTF Thing-to-Thing Research Group (T2TRG).

詳細草案請參考：draft-irtf-t2trg-rest-iot-04

18.YANG Object Universal Parsing Interface

本文為第 1 版發表於物到物（Thing-to-Thing，t2trg）工作小組，草案摘要如下：

YANG Object Universal Parsing Interface (YOUPI) specification describes generic way to encode and decode binary data based on a YANG model for use of constrainted devices. YOUPI is a generic mechanism designed for great flexibility, so that it can be adapted for any of the constainted devices.

詳細草案請參考：draft-petrov-t2trg-youpi-00

19.Problem Statement of IoT integrated with Edge Computing

本文為第 1 版發表於物到物（Thing-to-Thing，t2trg）工作小組，草案摘要如下：

This document describes new challenges such as strict latency, uplink cost, uninterrupted services, privacy and security, for IoT services originated from the IoT environmental changes. In order to address those new challenges, the integration of Edge computing and IoT has been emerged as a promising solution. This document discribes the concept of IoT integrated with Edge computing as well as the state-of-the-art of IoT Edge computing. It also proposes an architecture of IoT Edge computing. The direction of Edge computing for IoT should be discussed in the IETF/IRTF.

詳細草案請參考：draft-hong-t2trg-iot-edge-computing-00

路由安全維運相關技術討論

本次參與有關路由安全維運技術的討論會議，sidrops 工作小組，sidrops Working Group - SIDR Operations 工作小組的介紹如下：

SIDR 的全球部署，正在進行包括 RPKI，BGP 來源公告驗證和 BGPSEC，以創建一個由 SIDR 感知和非 SIDR 感知網路組成的網際網路路由系統。

此部署必須正確處理，以避免將 Internet 劃分為單獨的網路。Sidrops 負責鼓勵部署 SIDR 技術，同時確保在過渡期間盡可能保證全

球路由系統的安全。

SIDR 營運工作組（sidrops）為 SIDR 感知網路的營運制定指南，並提供有關如何在現有網路和新網路中部署和運行 SIDR 技術。

sidrops 工作組專注於 SIDR 技術的部署和營運問題及經驗，這些技術包括全球路由系統，以及構成 SIDR 架構的存儲庫和 CA 系統。

詳細 sidrops 工作組章程請參考：
https://datatracker.ietf.org/group/sidrops/about/

SIDR 營運工作組（sidrops）於會中進行的主題包含以下內容：

1. A Profile for Autonomous System Provider Authorization

   本文為第 1 版發表於 SIDR 營運（SIDR Operations，sidrops）工作小組，草案摘要如下：

   This document defines a standard profile for Autonomous System Provider Authorization in the Resource Public Key Infrastructure. An Autonomous System Provider Authorization is a digitally signed object that provides a means of verifying that a Customer Autonomous System holder has authorized a Provider Autonomous System to be its upstream provider and for the Provider to send prefixes received from the Customer Autonomous System in all directions including providers and peers.

   詳細草案請參考：draft-ietf-sidrops-aspa-profile-00

2. Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization

   本文為第 1 版發表於 SIDR 營運（SIDR Operations，sidrops）工作小組，草案摘要如下：

   This document defines the semantics of an Autonomous System Provider Authorization object in the Resource Public Key Infrastructure to verify the AS_PATH attribute of routes advertised in the Border Gateway Protocol.

   詳細草案請參考：draft-ietf-sidrops-aspa-verification-01

3. Signaling Prefix Origin Validation Results from an RPKI Origin Validating BGP Speaker to BGP Peers

   本文為第 3 版發表於 SIDR 營運（SIDR Operations，sidrops）

工作小組，草案摘要如下：

This document describes the use of BGP large communities, as well as its usage, to signal prefix origin validation results from an RPKI Origin validating BGP speaker to other BGP peers. Upon reception of prefix origin validation results, peers can use this information in their local routing decision process.

詳細草案請參考：draft-ietf-sidrops-validating-bgp-speaker-03

4. RPKI Signed Object for Trust Anchor Keys

本文為第3版發表於SIDR營運（SIDR Operations，sidrops）工作小組，草案摘要如下：

Trust Anchor Locators (TALs) [I-D.ietf-sidrops-https-tal] are used by Relying Parties in the RPKI to locate and validate Trust Anchor certificates used in RPKI validation. This document defines an RPKI signed object for Trust Anchor Keys (TAK), that can be used by Trust Anchors to signal their set of current keys and the location(s) of the accompanying CA certiifcates to Relying Parties, as well as changes to this set in the form of revoked keys and new keys, in order to support both planned and unplanned key rolls without impacting RPKI validation.

詳細草案請參考：draft-ietf-sidrops-signed-tal-03

四、建議意見：

建議事項

☐ 建議持續關注相關各 WGs 動態及相關訊息。
☐ IPv6 技術規範已有 IPv6-only 以及因應物聯網需求的草案提出，建議持續關注IPv6的相關技術規範發展，強化新一代網路基礎建設。
☐ 物聯網相關技術規範，廣泛地從架構，軟體，安全，應用，格式等各方面都有草案提出，建議持續關注 IoT 的相關技術規範發展，以取得新一代網路應用技術，作為創新產業的基礎。
☐ 建議持續關注 DNS 的相關技術發展，以掌握最新的發展趨勢。
☐ 建議持續了解 EPP 的政策規範，以配合修改相關作業流程。
☐ 建議與國外相關單位進行更密切及多元的交流及經驗分享。
☐ 建議持續參與 IETF 以掌握相關技術規範的演進及狀態。

IETF 下一次會議將於 2019 年 11 月 16-22 日於新加坡舉行，相關資訊

請參考 https://www.ietf.org/how/meetings/106/。

五、 會議議程：

以下為 IETF 105 Montreal 的完整議程表：

Saturday, July 20, 2019 (EDT)	
時間	議程
8:30-22:00	IETF Hackathon
9:30-18:00	Code Sprint

Sunday, July 21, 2019 (EDT)	
時間	議程
8:30-16:00	IETF Hackathon
10:00-12:00	IEPG Meeting
10:00-18:00	IETF Registration
12:30-13:30	Tutorial: Newcomers' Overview
13:45-14:45	Tutorial: Writing Security Considerations
16:00-17:00	Newcomers' Quick Connections (Open to Newcomers. Note that pre-registration is required)
17:00-19:00	Welcome Reception
18:00-20:00	Sunday Hot RFC lightning talks

Monday, July 22, 2019 (EDT)	
時間	議程
8:00-9:00	Continental Breakfast
8:00-9:00	Systers Networking Event
8:30-9:45	Side Meetings / Open Time
8:30-18:30	IETF Registration
9:00-19:10	IRTF Applied Networking Research Workshop (ANRW)
10:00-12:00	Internet Area AD Office Hours
10:00-12:00	**Monday Morning session I**
	Captive Portal Interaction 1000 – 1100
	Secure Telephone Identity Revisited 1100 - 1200
	Benchmarking Methodology
	Network Configuration
	Routing Area Working Group
	Automated Certificate Management Environment

	Trusted Execution Environment Provisioning
	Local Optimizations on Path Segments (BOF)
12:00-13:30	Break
12:15-13:15	SEC AD Office Hours
13:30-15:30	**Monday Afternoon session I**
	IPv6 over Networks of Resource-constrained Nodes
	Media OPerationS (BOF)
	Network Modeling
	Locator/ID Separation Protocol
	Link State Routing
	Security Dispatch
	Transport Services
15:30-15:50	Beverage and Snack Break
15:50-17:50	**Monday Afternoon session II**
	Hypertext Transfer Protocol
	Network Time Protocol
	Network Modeling
	IPv6 Operations
	Multiprotocol Label Switching
	Lightweight Authenticated Key Exchange (BOF)
	Multipath TCP
18:10-19:40	Hackdemo Happy Hour
18:10-19:10	**Monday Afternoon session III**
	Dispatch Joint with ARTAREA
	Domain Name System Operations
	Link State Routing
	Managed Incident Lightweight Exchange
19:30-21:00	Newcomers' Dinner

Tuesday, July 23, 2019 (EDT)	
時間	議程
8:00-9:00	Continental Breakfast
8:30-9:45	Side Meetings / Open Time
8:30-17:30	IETF Registration
8:30-9:45	**Tuesday Side meetings / open time**
	Technology Deep Dive : How NICs Work Today

10:00-12:00	**Tuesday Morning session I**
	Concise Binary Object Representation Maintenance and Extensions 1000-1130
	IP Wireless Access in Vehicular Environments 1130-1200
	Human Rights Protocol Considerations
	Information-Centric Networking
	Autonomic Networking Integrated Model and Approach
	Domain Name System Operations
	Routing Area Working Group
	Trusted Execution Environment Provisioning
	QUIC
12:00-13:30	Break
13:30-15:00	**Tuesday Afternoon session I**
	Applications Doing DNS (BOF)
	Global Access to the Internet for All
	Internet Congestion Control
	Autonomic Networking Integrated Model and Approach
	Traffic Engineering Architecture and Signaling
	Limited Additional Mechanisms for PKIX and SMIME
	Security Events
15:00-15:20	Beverage and Snack Break
15:20-16:50	**Tuesday Afternoon session II**
	Relay User Machine
	Internet Area Working Group
	IRTF Open Meeting
	SIDR Operations
	BGP Enabled ServiceS
	Traffic Engineering Architecture and Signaling
	IP Security Maintenance and Extensions
	Web Authorization Protocol
17:10-18:10	**Tuesday Afternoon session III**
	Audio/Video Transport Core Maintenance
	Constrained RESTful Environments
	IPv6 Maintenance
	Bidirectional Forwarding Detection
	Mobile Ad-hoc Networks
	Transport Layer Security

18:30-22:00	IETF 105 Social Event

Wednesday, July 24, 2019 (EDT)	
時間	議程
8:00-9:00	Continental Breakfast
8:30-9:45	Side Meetings / Open Time
8:30-17:10	IETF Registration
9:00-9:45	Routing AD Office Hours
10:00-12:00	**Wednesday Morning session I**
	Distributed Mobility Management
	Decentralized Internet Infrastructure
	Operations and Management Area Working Group
	Routing Over Low power and Lossy networks
	Source Packet Routing in Networking
	DDoS Open Threat Signaling
	Software Updates for Internet of Things
	QUIC
12:00-13:30	Break
12:15-13:15	WG Chairs Forum
13:30-15:30	**Wednesday Afternoon session I**
	IETF Meeting Network Requirements (BOF)
	Privacy Enhancements and Assessments Research Group
	Thing-to-Thing
	Bit Indexed Explicit Replication
	Deterministic Networking
	Inter-Domain Routing
	EAP Method Update
	IP Performance Measurement
15:30-15:50	Beverage Break
15:50-16:50	TSV AD Office Hours
15:50-16:50	**Wednesday Afternoon session II**
	Calendaring Extensions
	Global Routing Operations
	Babel routing protocol
	Deterministic Networking
	Remote ATtestation ProcedureS
16:50-17:10	Beverage and Snack Break

17:10-18:10	**IETF Technical Plenary**
18:20-19:50	**IETF Administrative/Operations Plenary**

Thursday, July 25, 2019 (EDT)	
時間	**議程**
8:00-9:00	Continental Breakfast
8:00-9:00	Newcomers' Feedback Session
8:30-9:45	Side Meetings / Open Time
8:30-18:00	IETF Registration
10:00-12:00	**Thursday Morning session I**
	Constrained RESTful Environments
	Registration Protocols Extensions
	Link State Vector Routing
	Path Computation Element
	Interface to Network Security Functions
	Transport Layer Security
	Application-Layer Traffic Optimization
	Transport Area Working Group
12:00-13:30	Break
12:15-13:15	Systers Lunch
13:30-15:30	**Thursday Afternoon session I**
	Extensions for Scalable DNS Service Discovery
	Computing in the Network Proposed Research Group
	Path Aware Networking RG
	Common Control and Measurement Plane
	Protocols for IP Multicast
	Security Area Open Meeting
	Network File System Version 4
	TCP Maintenance and Minor Extensions
15:30-15:50	Beverage and Snack Break
15:50-17:20	**Thursday Afternoon session II**
	Hypertext Transfer Protocol
	IPv6 Maintenance
	DNS PRIVate Exchange
	Crypto Forum
	MBONE Deployment
	Routing In Fat Trees

	Remote ATtestation ProcedureS
	Transport Area Open Meeting
17:20-17:40	Beverage Break
17:40-19:10	**Thursday Afternoon session III**
	IPv6 over the TSCH mode of IEEE 802.15.4e
	Network Management
	BGP Enabled ServiceS
	Authentication and Authorization for Constrained Environments
	Security Automation and Continuous Monitoring
	RTP Media Congestion Avoidance Techniques

Friday, July 26, 2019 (EDT)	
時間	**議程**
8:00-9:00	Continental Breakfast
8:30-9:45	Side Meetings / Open Time
8:30-12:20	IETF Registration
10:00-12:00	**Friday Morning session I**
	IPv6 over Low Power Wide-Area Networks
	Measurement and Analysis for Protocols
	Coding for efficient NetWork Communications Research Group
	Inter-Domain Routing
	Messaging Layer Security
	Web Authorization Protocol
	Delay/Disruption Tolerant Networking
12:00-12:20	Beverage and Snack Break
12:20-13:50	**Friday Afternoon session I**
	JSON Mail Access Protocol
	Inter-Domain Routing
	Network Virtualization Overlays
	CBOR Object Signing and Encryption
	Transport Area Working Group

『APNIC 48』出國報告

財團法人台灣網路資訊中心因公出國人員報告書

108 年 9 月 17 日

報告人 姓　名	黃勝雄 丁綺萍 顧靜恆 林志鴻 王彥傑 陳玟羽 詹婷怡 陳映竹	服務單位及職稱	執行長 副執行長 IP 組組長 網資組組長 IP 組工程師 IP 組管理師
出國期間	108 年 9 月 8 日 至 108 年 9 月 13 日	出國地點	泰國清邁
出國事由	報告書內容應包含： 一、出國目的 二、考察、訪問過程 三、考察、訪問心得 四、建議意見 五、其他相關事項或資料 （內容超出一頁時，可由下頁寫起）		
授權聲明欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人： （簽章）		

附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。

註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。

一、出國目的

APNIC(Asia Pacific Network Information Centre)為掌管亞太地區 IP 位址與 AS 號碼發放的機構，為能廣納會員對於 IP 位址及 AS 號碼相關政策之意見，並進行網路管理相關技術交流，APNIC 每半年召開會議，以供各界對於其 IP 位址及 AS 號碼資源之政策作一個公開的討論，藉由對 IP 位址及 AS 號碼資源管理政策提案之公開討論的方式，依照與會的會員所達成共識的結果制訂成相關政策。

APNIC 48 會議於 2019 年 9 月 5 日至 12 日在泰國清邁(CHIANG MAI, THAILAND)舉行，本次會議共有 422 人參與，會議內容涵蓋了網際網路維運、技術及發展等。本次會議有許多 NIR 代表、網路技術專家、政府代表、網路業者代表、Internet 工程師等共同參加。

此次參加會議之目的為參與相關議題及進行台灣最新發展現況報告，瞭解亞太地區各國網際網路發展狀況與網路運作之政策。另外，本中心參與此會議中，負責主持 APNIC IPv6 Deployment 場次，Cooperation SIG 場次，並共同主持 Policy SIG 場次，IPv6 Deployment 場次中包含 5 個 IPv6 佈建相關專題報告與經驗分享，以促進亞太地區 IPv6 發展；Cooperation SIG 場次邀請了 5 位講者針對 Internet Jurisdiction 主題進行座談；Policy SIG 場次共討論了 5 個 Policy Proposals 政策提案。

二、參與議程與議題
APNIC 48 會議，相關議程及會議錄影等資訊如下：

APNIC 48 CHIANG MAI, THAILAND

Tuesday, 10 September 2019

Conference, Day 6

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

Wednesday, 11 September 2019

Conference, Day 7

時間	議程	
09:00	**APNIC - FIRST Security** 09:00 to 10:30	**IPv6 Deployment** 09:00 to 10:30
11:00	**APNIC - FIRST Security** 11:00 to 12:30	**Technical Session 3** 11:00 to 12:30

14:00	**APNIC - FIRST Security** 14:00 to 15:30	**RPKI - Industry Trends and Initiatives** 14:00 to 15:30
16:00	**APNIC - FIRST Security** 16:00 to 17:30	**Lessons learned from RPKI Deployments** 16:00 to 17:30
17:30	**RPKI BoF** 17:30 to 18:30	
18:30	**Meet the APNIC EC Cocktail** 18:30 to 19:00	
19:00	**ROA signing Social** 19:00 to 21:00	

Thursday, 12 September 2019

Conference, Day 8

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

本次會議參與的 APNIC 48 的 Session 如下：

議程名稱	說明
APNIC IPv6 Deployment	IPv6 佈建相關專題報告討論與經驗分享。
Cooperation SIG	討論網路管轄權及意見交流座談
NIR SIG	各國 NIR 半年來的活動與狀況經驗分享報告。
Policy SIG	對於現行網路資源管理政策提出修正意見之提案。
NIR Hostmaster Workshop	與會對象為各 NIR 之 Hostmaster，目的是提供 APNIC 與 NIRs 的 Hostmaster 交流溝通管道，以檢討 IP 審理發放作業及增進彼此的 IP 管理技術，並進行 RPKI 佈建經驗交流。
APNIC Member Meeting (AMM)	與會對象為全體 APNIC 會員，目的是向會員報告 APNIC 近半年的狀況，同時總結各 SIG 所討論之提案，並尋求參與會員之共識，並選出 APNIC NRO NC。

三、參加心得

1. Cooperation SIG

Cooperation SIG 由 TWNIC 丁綺萍副執行長主持，時間為 9 月 10 日的 09:00-10:30，此次共有四個專題演講，包括：

- Internet and Jurisdiction - Nepali Perspective (Bikram Shrestha)
- Internet Jurisdiction - Emerging Issues and Ways Forward (Nicole T I Chan)
- IP Address and Cross-border Cooperation for Resolving the Cyber Attribution Challenge (Eun Chang Choi)
- Educating Internet Ethics, Moral Development and Awareness Raising Activities of Myanmar (Dr Mie Mie Su Thwin)

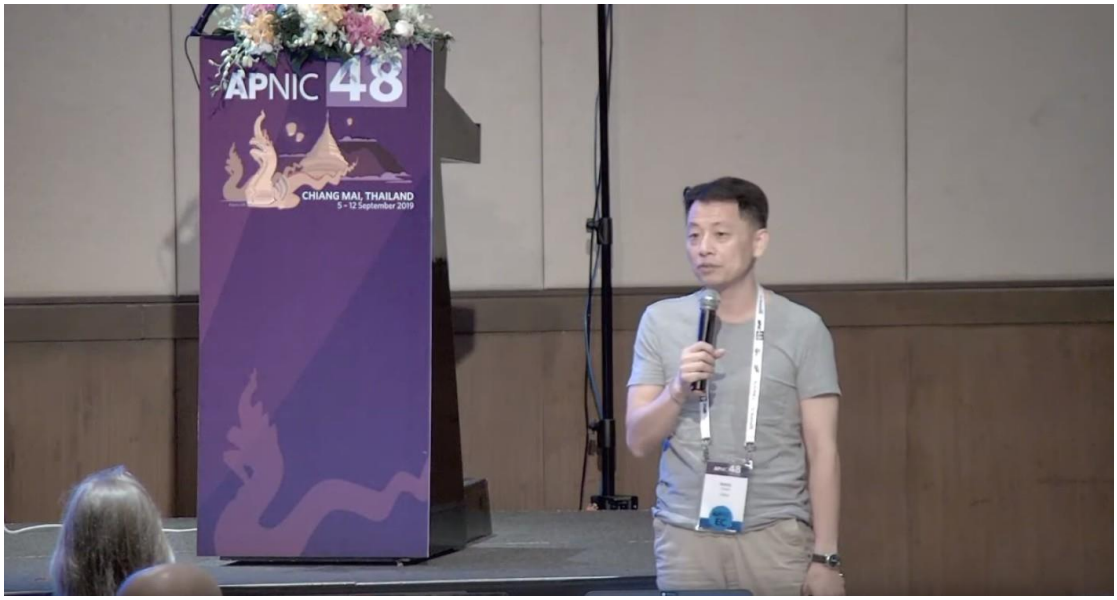
圖一：詹婷怡律師於 Cooperation SIG 分享網路管轄權的新興問題與未來展望

2. APNIC IPv6 Deployment

APNIC IPv6 Deployment 為 TWNIC 黃勝雄執行長主持，時間為 9 月 11 日的 09:00-10:30，共有 5 個講者進行報告如下：

- Tanapon Chandavasu –IPv6 Deployment in Thailand
- Geoff Huston –IPv6 Performance
- Koji Yasukagawa –IPv6 Deployment for Mobile Network
- Nguyen Hong Thang–IPv6 Deployment in Vietnam
- Maile Halatuituia –Islands in the IPv6 World

本次會議由不同國家的講者分享 IPv6 Deployment 的經驗。本場次約有 100 多人參加，現場討論熱烈。



圖二：黃勝雄執行長主持 IPv6 Deployment 場次

3. Policy SIG

此次 Policy SIG 由 TWNIC 顧靜恆組長擔任共同主持人，共包含有五個 Policy Proposals，包括 prop-124: Clarification on IPv6 sub-assignments、prop-126: PDP update、prop-130: Modification of transfer policies、prop-131: Editorial changes in IPv6 policies 及 prop-132: RPKI ROAs for unallocated and unassigned APNIC address space (was: AS0 for Bogons)，其中 prop-131 跟 prop-132 在 Policy SIG 及 AGM 中皆達成共識，其餘提案都沒有達成共識，這些提案退回到 mailing list 讓社群回饋意見後再做修改。

此外，Policy SIG 中還有以下兩份資訊報告：

- Implementation Update - Sunny Chendi
- Resource Hijacking is an APNIC Policy Violation - Jordi Palet

圖三：顧靜恆組長共同主持 Policy SIG 場次

4. NIR SIG

本次 NIR SIG 共有 TWNIC、CNNIC、VNNIC、IRINN、IDNIC、KRNIC、JPNIC 等 7 個 NIR 上台報告，各 NIR 主要報告其各項業務推動狀況。TWNIC 在此會議中報告會員狀況、IP 核發狀況及相關活動，如第 32nd TWNIC IP OPM、2019 TWNIC-APNIC Joint Training - Routing Workshop、Taiwan IPv6 User Availability、TWNIC RPKI 統計及 TWNIC RPKI Training 等與各 NIR 和與會者進行交流。

圖四：TWNIC 陳玟羽管理師在 NIR SIG 報告目前 TWNIC IP 業務狀況

圖五：TWNIC 王彥傑工程師在 NIR SIG 報告目前 TWNIC RPKI 狀況

圖六：NIR SIG 講者合照

5. AMM 會議

9 月 12 日召開 APNIC AMM 會員大會，會議由 APNIC Executive Council (EC)主席 Gaurab Raj Upadhaya 擔任主持人，共 8 位 APNIC EC 於台上參與。

圖七：八位 APNIC Executive Council 進行 AMM

APNIC 主要針對目前的各業務進行相關報告與宣佈 APNIC NRO NC 投票結果，APNIC EC 成員中負責 Treasure 為 TWNIC 黃勝雄執行長，黃執行長於會員大會中進行 APNIC EC Treasurer Report，報告 APNIC 2019 上半年財務經費及活動預算的執行狀況。

本次會議進行 APNIC NC 選舉，共 11 位候選人，最後由 Aftab Siddiqui 當選。

此外，AMM 會員大會中也邀請黃勝雄執行長針對 IPv6 Deployment 場次、丁綺萍副執行長針對 Cooperation SIG 做總結報告，APNIC 並於閉幕式致贈本中心贊助會議之感謝狀。

圖八: 丁綺萍副執行長進行 Cooperation SIG 報告

四、建議事項

1. 目前國際上各國家都積極在推動 IPv6，愈來愈多國家的 ISP 業者都預設啟用 IPv6，建議國內 ISP 參考此方式推動使用 IPv6，也建議持續對國際 IPv6 發展持續關注。
2. Policy 是推動網路發展的重要依據，在 Policy 形成之前，需先進行 Proposal 的提案及討論，由於 proposal 的討論需尊重整個社群的意見，建議國內 ISP 及相關單位能了解並參與相關的討論，以便能與國際接軌及健全國內網路的持續發展。
3. RPKI 在 APNIC 48 會議場次比例提高許多，可見 APNIC 對於 RPKI 的重視，未來台灣仍應持續推動 RPKI 並提升 ROA 覆蓋率以及 ROV valid 比例。

五、其他相關事項或資料

APNIC 48 會議各場次簡報投影片及 YouTube 錄影均提供於活動網站上，歡迎點閱下載，活動網址如下：
https://conference.apnic.net/48/