財團法人台灣網路資訊中心因公出國人員報告書 108年12月3日

報告人 姓　名	丁綺萍、林志鴻、曲承則 顧靜恆、許乃文、林福寬	服務單位及 職稱	副執行長、組長、工程師 組長、組長、工程師
出國期間	11月15日-11月23日	出國地點	新加坡
出國事由	參加 IETF 106 會議		

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：
	丁綺萍(簽章)
	林志鴻(簽章)
	曲承則(簽章)
	顧靜恆(簽章)
	許乃文(簽章)
	林福寬(簽章)

附註

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。

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:

參加 IETF 106 Singapore 會議

二. 會議行程:

詳如會議網站 https://www.ietf.org/how/meetings/106/

議程 https://datatracker.ietf.org/meeting/106/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
108/11/15(五)	09:55	桃園機場出發(BR215)
	14:30	抵達新加坡樟宜機場
108/11/16(六)	08:30 - 22:00	IETF Hackathon
108/11/17(日)	08:30 - 16:00	IETF Hackathon
	17:00 - 19:00	Welcome Reception
108/11/18(一)	10:00 - 19:10	IETF Session I, II, III
108/11/19(二)	10:10 - 18:40	IETF Session I, II, III
108/11/20(三)	10:10 - 19:40	IETF Session I, II, III
108/11/21(四)	10:10 - 18:40	IETF Session I, II, III
108/11/22(五)	10:10 - 13:50	IETF Session I, II

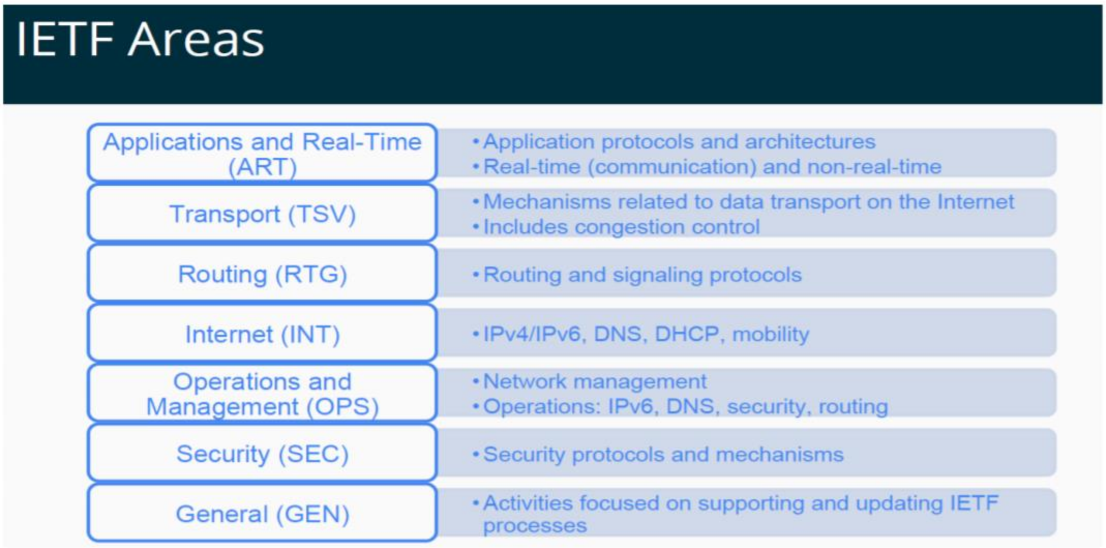
108/11/23(六)	15:45	樟宜機場出發(BR216)
	20:15	抵達桃園機場

三. 考察，訪問心得

甲、 前言

此會議為 IETF (網際網路工程任務小組，Internet Engineering Task Force) 所舉辦第 106 次會議，於 2019 年 11 月 16 日(六)至 2019 年 22 日(五)在新加坡召開，總共為期七天的會議，是由 NOKIA 主辦，Moratelindo 與 Equinix 贊助。本次參與會議人數高達 1539 人，其中有 540 人是利用遠端會議系統方式參與。其中有 9 成以上是來自國外與會者。在整體議程安排上，16 日及 17 日為技術人員舉行網路協定草案測試的 Hackthon，用以確認提案的可行性。17 日有專為首次參加 IETF 會議者舉辦的「Newcomer's Overview」介紹本次會議的總覽，18 日開始的議程著重在各種網路協定技術性標準之討論會議，由來自世界各地產學研的專家共同交換意見。在整體議程安排上，主題共分為以下 7 大項目：應用與即時架構領域(Application and Real Time Area, art)、一般領域(General Area, gen)、網際網路領域(Internet Area, int)、維運與管理領域(Operation & Management, opt)、網路路由領域(Routing Area, rtg)、安全領域(Security Area, sec)、封包傳遞領域(Transport Area, tsv)等網路領域，

另有 IRTF(Internet Engineering Task Force)的前瞻議題研究討論等議程，有高達 100 場資安相關討論會議與工作坊，提供與會者透過多元參與，掌握最新的資安技術標準與趨勢。



IETF Areas

Applications and Real-Time (ART)	•Application protocols and architectures •Real-time (communication) and non-real-time
Transport (TSV)	•Mechanisms related to data transport on the Internet •Includes congestion control
Routing (RTG)	•Routing and signaling protocols
Internet (INT)	•IPv4/IPv6, DNS, DHCP, mobility
Operations and Management (OPS)	•Network management •Operations: IPv6, DNS, security, routing
Security (SEC)	•Security protocols and mechanisms
General (GEN)	•Activities focused on supporting and updating IETF processes

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 1：IETF 106 大會報到處

圖 2：TWNIC 曲承則工程師，林志鴻組長，丁綺萍副執行長及許乃仁組長(左至右)

圖 3：IETF106 會場

在本次會議中主要參與的會議主題包含 Hackathon、Security、

IPv6、DNS 安全管理，隱私保護及 IoT 領域等相關議題。茲將本次所參加之各項會議主要議題之觀察與建議，分述如下：

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。

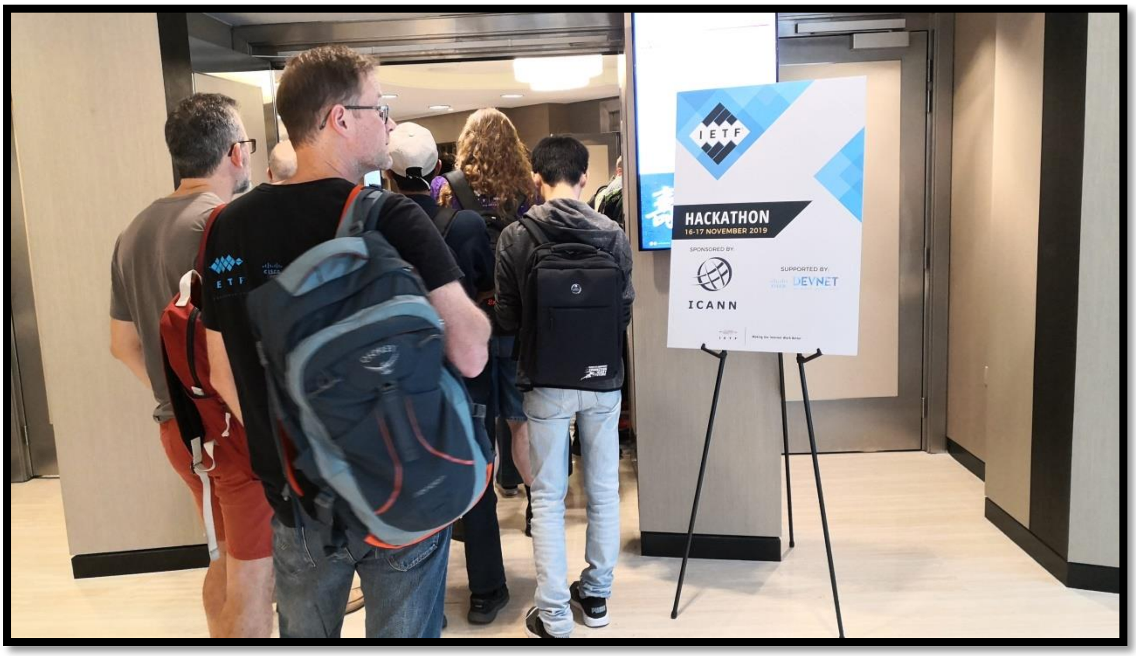


圖 4：Hackathon 報到處

本次 Hackathon 活動參與人數約有 398 名，分成 42 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，各分組的簡報內容可以在以下的連結下載：

https://github.com/IETF-Hackathon/ietf106-project-presentations

此次會議主要參與 DNS 小組，討論主題內容大致包含：

1. DNS privacy
   (1) DNS-over-TLS to authoritative
      - Unbound: set of net blocks + hostname verification

   (2) DNS-over-HTTPS
      - DoH design for BIND 9

   (3) DNS-over-HTTP/3
      - Proof of concept implementation using Quiche
      - Work in progress

2. DNS protocol improvement
   (1) DNS Server Cookies (draft-ietf-dnsop-server-cookies)
      - Updated (bis) specification and implementation of DNS cookies
      - Interoperable implementation between different open source DNS name server software

   (2) Extended error (draft-ietf-dnsop-extended-error)
      - Updated code in Unbound to the latest draft
      - Work in progress

3. DNS and services provisioning
   (1) Service binding and parameter specification via the DNS (draft-ietf-dnsop-svcb-httpssvc)
      - Previous hackathon implementation of first version of draft in Unbound
      - This hackathon update implementation to match with new & updated version of draft

4. DNS Measurements
   (1) New project for metrics of the root server operators
      - correctness of answers from the root servers
      - check the validation of a DNS response
      - extended getdns to return DNSSEC validation chain

圖 5：Hackathon 分組討論

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：

i. Maprg – Measurement and Analysis for Protocols
ii. TEEP – Trusted Execution Environment Provisioning
iii. Netmod – Network Modeling
iv. Httpbis – HTTP

會中進行的主題包含以下內容:

1. Ericsson’s 5G security

此演講說明 5G 安全性概況，涵蓋 5G 安全考量彈性(Resilience)、安全確保(Security assurance)、通訊安全(Communication security)、隱私(Privacy)與識別管理(Identity management)等議題，期能達成：彈性與安全的 EAP 認證架構、內部與跨網路間的零信任架構、網路功能與訊務分離、所有流量的加密與完整性保護、防止追蹤與識別使用者等目標。

過往駭客藉由 SS7 (Signaling System Number 7)協定的漏洞，取得電信網路的 SMS 等資訊，進而偽冒用戶進行金融交易。對此，5G 運用零信任架構(Zero Trust Architecture)，在 control plan 上使用 SBA (Service-based Architecture)介面，提供 Network Function (NF)的註冊與探索功能，透過 Ephemeral Diffie-Hellman 金鑰交換機制，使 NF 得以識別其他內網相關服務，並利用 N32 介面進行和核網與核網間的跨網識別與安全的連線。

為防止假冒行動基地台竊取 IMSI(International Mobile Subscriber Identi)資訊，5G 將進行永久識別碼加密、強制暫時識別碼更新、避免永久識別碼廣播、使用者流量的完整性保護、安全的無線移轉(radio redirections)、偽冒基地台偵測等機制，來防範相關攻擊。

SIM 卡內行動認證金鑰可遭駭客攔截封包進行破解，為降低此類攻擊造成的資安衝擊，5G 導入 PFS (Perfect Forward

Secrecy)機制，針對每個連線以 Ephemeral Diffie-Hellman 演算法，產生隨機的連線金鑰。當長期金鑰遭破解，亦不會導致先前的連線金鑰遭破解，來降低金鑰被破解的資安風險。

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-hrpc-5g-presentation

2. Open Trust Protocol

摘要內容如下:

This document specifies the Open Trust Protocol (OTrP), a protocol that follows the Trust Execution Environment Provisioning (TEEP) architecture and provides a message protocol that provisions and manages Trusted Applications into a device with a Trusted Execution Environment (TEE).

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-teep-opentrustprotocol-03.pdf
- https://tools.ietf.org/html/draft-tschofenig-teep-protocol-00
- https://github.com/ietf-teep/OTrP/issues

3. OTrP over HTTP

內容摘要如下:

This document specifies the HTTP transport for the Open Trust Protocol (OTrP), which is used to manage code and configuration data in a Trusted Execution Environment (TEE). An implementation of this document can run outside of any TEE, but interacts with an OTrP implementation that runs inside a TEE.

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-teep-sessa-teep-over-http
- https://tools.ietf.org/pdf/draft-thaler-teep-otrp-over-http-01.pdf
- https://github.com/ietf-teep/otrp-over-http

4. YANG Geo Location

草案摘要如下:

This document defines a generic geographical location object YANG grouping. The geographical location grouping is intended to be used in YANG models for specifying a location on or in reference to the Earth or any other astronomical object.

詳細內容請參考:

- https://tools.ietf.org/html/draft-ietf-netmod-geo-location-02
- https://datatracker.ietf.org/meeting/106/materials/slides-106-netmod-sessb-yang-geo-location-00.pdf

5. Comparison of NMDA datastores

草案摘要如下:

This document defines an RPC operation to compare management datastores that comply with the NMDA architecture.

詳細內容請參考:

- https://tools.ietf.org/html/draft-ietf-netmod-nmda-diff-03
- https://datatracker.ietf.org/meeting/106/materials/slides-106-netmod-sessb-comparison-of-nmda-datastores-01

6. A YANG Data model for Policy based Event Management

草案摘要如下:

[RFC8328] defines a policy-based management framework that allow definition of a data model to be used to represent high-level, possibly network-wide policies. This document defines an YANG data model for the policy based event management [RFC7950]. The policy based Event YANG provides the ability for the network management function (within a controller, an orchestrator, or a network element) to control the configuration and monitor state change on the network element and take simple and instant action when a trigger condition on the system state is met.

詳細內容請參考:

- https://tools.ietf.org/id/draft-wwx-netmod-event-yang-03.html
- https://datatracker.ietf.org/meeting/106/materials/slides-106-netmod-sessb-a-yang-data-model-for-policy-based-event-management-01

7. Framework for Use of ECA (Event Condition Action) in Network

草案摘要如下:

Event-driven management is meant to provide a useful method to monitor state change of managed objects and resources, and facilitate automatic triggering of a response to events, based on an established set of rules. This would provide rapid autonomic responses to specific conditions, enabling self-management behaviors, including: self-configuration, self-healing, self-optimization, and self-protection.

This document provides a framework that describes the architecture for supporting event-driven management of managed object state across devices. It does not describe specific protocols or protocol extensions needed to realize the objectives and capabilities discussed in the document.

詳細內容請參考:

- https://tools.ietf.org/html/draft-bwd-netmod-eca-framework-00
- https://datatracker.ietf.org/meeting/106/materials/slides-106-netmod-sessb-framework-for-use-of-eca-in-network-self-management-00

8. YANG Data Node Self Explanation Tags

草案摘要如下:

This document defines a method to tag data node associated with telemetry data in YANG Modules. This YANG data node tagging method can be used to filter queries of operational state on a server during a "pub/sub" service for YANG datastore updates when the state of all subscriptions of a particular Subscriber to be fetched is huge, so that the amount of data to be streamed out to the destination can be greatly reduced.

An extension statement to be used to indicate YANG data node tags that SHOULD be added by the module implementation automatically (i.e. outside of configuration).

A YANG module [RFC7950] is defined, which augment Module tag model and provides a list of data node entries to allow for adding or removing of data node tags as well as viewing the set of tags associated with a YANG module.

詳細內容請參考:

- https://tools.ietf.org/html/draft-tao-netmod-yang-node-tags-00
- https://datatracker.ietf.org/meeting/106/materials/slides-106-netmod-sessb-yang-data-node-self-explanation-tags-00

9. Losses in SATCOM systems: identification and impact (Nicolas Kuhn)

演講摘要如下:

This talk focuses on losses identification and impact on SATCOM end-to-end systems. We present three ways of assessing loss presence in SATCOM access: on the Wi-Fi link, in before the bottleneck and end-to-end. Despite having a quite reliable satellite access, most of the losses can be seen before the bottleneck (before the satellite link). This talk also presents the impact of losses on end-to-end protocols in such systems and discussing available solutions.

詳細內容請參考:

- ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-maprg-losses-in-satcom-systems-identification-and-impact

10.TLS Beyond the Browser: Combining End Host and Network Data to Understand Application Behavior (Blake Anderson and David McGrew (Cisco Systems))

演講摘要如下:

The Transport Layer Security (TLS) protocol has evolved in response to different attacks and is increasingly relied on to secure Internet communications. Web browsers have led the adoption of newer and more secure cryptographic algorithms and protocol versions, and thus improved the security of the TLS ecosystem. Other application categories, however, are increasingly using TLS, but too often are relying on obsolete and insecure protocol options, as we found through a study of applications that use TLS at global enterprises. To understand in detail what applications are using TLS, and how they are using it, we developed a novel system for obtaining process information from end hosts and fusing it with network data to produce a TLS fingerprint knowledge base. This data has a rich set of context for each fingerprint, is representative of enterprise TLS deployments, and is automatically updated from ongoing data collection. Our dataset is based on 96 million endpoint-labeled and 2.4 billion unlabeled TLS sessions obtained from enterprise edge networks in five countries, plus millions of sessions from a malware analysis sandbox. We actively maintain an open source dataset that, at 2,200+ fingerprints and counting, is both the largest and most informative ever published. In this paper, we use the knowledge base to identify trends in enterprise TLS applications beyond the browser: application categories such as storage, communication, system, and email. We study fingerprint prevalence, longevity, and succession across application versions, and identified a rise in the use of TLS by non-browser applications and a corresponding decline in the fraction of sessions using version 1.3. Finally, we highlight the shortcomings of na\"{i}vely applying TLS fingerprinting to detect malware, and we present recent trends in malware's use of TLS such as the adoption of cipher suite randomization.

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-maprg-tls-beyond-the-browser
- http://delivery.acm.org/10.1145/3360000/3355601/p379-Anderson.pdf

11.Characterizing JSON Traffic Patterns on a CDN (Santiago Vargas and Aruna Balasubramanian (Stony Brook University), Moritz Steiner and Utkarsh Goel (Akamai))

演講摘要如下:

Content delivery networks serve a major fraction of the Internet traffic, and their geographically deployed infrastructure makes them a good vantage point to observe traffic access patterns. We perform a large-scale investigation to characterize Web traffic patterns observed from a major CDN infrastructure. Specifically, we discover that responses with 'application/json' content-type form a growing majority of all HTTP requests. As a result, we seek to understand what types of devices and applications are requesting JSON objects and explore opportunities to optimize CDN delivery of JSON traffic. Our study shows that mobile applications account for at least 52% of JSON traffic on the CDN and embedded devices account for another 12% of all JSON traffic. We also find that more than 55% of JSON traffic on the CDN is uncacheable, showing that a large portion of JSON traffic on the CDN is dynamic. By further looking at patterns of periodicity in requests, we find that 6.3% of JSON traffic is periodically requested and reflects the use of (partially) autonomous software systems, IoT devices, and other kinds of machine-to-machine communication. Finally, we explore dependencies in JSON traffic through the lens of ngram models and find that these models can capture patterns between subsequent requests. We can potentially leverage this to prefetch requests, improving the cache hit ratio.

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-maprg-characterizing-json-traffic-patterns-on-a-cdn-santiago-vargas
- http://delivery.acm.org/10.1145/3360000/3355594/p195-Vargas.pdf

12.Tighten language around DELETE request bodies

詳細內容請參考:

https://github.com/httpwg/http-core/issues/258
Updating stored headers

探討 RFC 7234 提及 stored headers 需更新為 304 或 HEAD

回應以及其延伸之問題。

詳細內容請參考:

- https://github.com/httpwg/http-core/issues/165

13.Clarification of weak validators

探討 RFC7232 提及之 weak validator，定義參考:

https://www.rfc-editor.org/errata/eid5236

詳細內容請參考:

- https://github.com/httpwg/http-core/issues/163

14.Quoted cache-control directives

徵求更改規格意見以因應 CACHE 無法識別 Cache-Control: max-age=”3600”

詳細內容請參考:

- https://github.com/httpwg/http-core/issues/128

15.RateLimit Header Fields for HTTP – Roberto Polli

討論內容主要針對 HTTP 之 RateLimit-Limit, RateLimit-Remaining, RateLimit-Reset header 欄位，以解決”Retry-After”回傳”429 Too Many Requests”或是”503 Service Unavailable”回應問題(RFC7231)。

草案摘要如下:

- https://tools.ietf.org/html/draft-polli-ratelimit-headers-01

16.Borders and Gateways: Measuring and Analyzing National AS Chockpoints

演講摘要如下:

Internet topology reflects economic and political constraints that change over time. Although autonomous systems (AS) topology has been measured and modeled for many years, focusing primarily on economic relationships, earlier studies have not quantified how topology is changing with respect to nation-state boundaries. National boundaries are natural points of control for surveillance, censorship, tariffs and data localization. This paper introduces a measure, national chokepoint potential (NCP), to characterize how a country’s AS topology is organized in terms of BGP paths that can carry traffic across international borders. To study country level chokepoints, we developed BGP-SAS, an open source, cross platform, efficient set of tools for simulating BGP routing and calculating national chokepoint measures. We use these tools to assess how AS topologies have changed over a ten-year span, finding significant variability among countries, with some increasing their chokepoint potential and others remaining constant, fluctuating, and in some cases declining. Overall, however, most national Internet boundaries have either become more pronounced or remained constant, despite new infrastructure buildouts and increased Internet usage. When compared to independent measures of Internet freedom, we find statistically significant relationships between NCP and Internet freedom

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-hrpc-borders-and-gateways-presentation
- https://forrest.biodesign.asu.edu/data/publications/2019-compass-chokepoints.pdf

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：

i. 6man - IPv6 Maintenance
ii. Spring - Source Packet Routing in Networking
iii. RTGWG - Routing Area Working Group
iv. IPsecME WG – IP Security Maintenance and Extensions
v. 6tisch – IPv6 over the TSCH mode of IEEE 802.15.4e

會中進行的主題包含以下內容:

1. Path MTU Hop-by-Hop Option Update

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 host 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.

詳細內容請參考:

- https://tools.ietf.org/html/draft-ietf-6man-mtu-option

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

   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.

   詳細內容請參考:

   - https://tools.ietf.org/html/draft-ietf-6man-spring-srv6-oam

3. Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers

   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 updates [RFC4861] to allow routers to proactively create a Neighbor Cache entry when a new IPv6 address is assigned to a host. It also updates [RFC4862] and [RFC4429] recommending hosts to send unsolicited Neighbor Advertisements upon assigning a new IPv6 address. The proposed change will minimize the delay and packet loss when a host initiate connections to off-link destination from a new IPv6 address.

   詳細內容請參考:

   - https://tools.ietf.org/html/draft-linkova-6man-grand

4. IPv6 Extension Header for the Alternate Marking Method

   草案摘要如下:

This document describes how the alternate marking method in [RFC8321] and [I-D.ietf-ippm-multipoint-alt-mark] can be used as the passive performance measurement method in an IPv6 domain and reports implementation considerations. It proposes how to define a new Extension Header Option to encode alternate marking technique and also considers the Segment Routing Header TLV alternative.

詳細內容請參考:

- https://tools.ietf.org/html/draft-fz-6man-ipv6-alt-mark

5. IPv6 Formal Anycast Addresses and Functional Anycast Addresses

草案摘要如下:

Currently, IPv6 anycast addresses are chosen from within the existing IPv6 unicast address space, with the addresses nominated as anycast addresses through configuration. An alternative scheme would be to have a special class of addresses for use as anycast addresses. This memo proposes a distinct general anycast addressing class for IPv6, and a more specific scheme for functional anycast addresses.

詳細內容請參考:

- https://tools.ietf.org/html/draft-smith-6man-form-func-anycast-addresses

6. Asymmetric IPv6 for IoT Networks

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.

詳細內容請參考:

- https://tools.ietf.org/html/draft-jiang-asymmetric-ipv6

7. Support Postcard-Based Telemetry for SRv6 OAM

草案摘要如下:

Applications such as SRv6 TE may require to collect detailed performance data on SR paths. Existing in-situ OAM techniques incur encapsulation and header overhead issues. This document describes a method based on Postcard-based Telemetry with Packet Marking for SRv6 on-path OAM, which avoids the extra overhead for encapsulating telemetry-related instruction and metadata in SRv6 packets.

詳細內容請參考:

- https://tools.ietf.org/html/draft-song-6man-srv6-pbt

8. SRv6 network programming

此演講主要針對為 SRv6 Network Programming 之草案演進狀況。

草案摘要如下:

This document describes the SRv6 network programming concept and its most basic functions.

詳細草案請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-srv6-network-programming
- https://tools.ietf.org/html/draft-ietf-spring-srv6-network-programming-05#section-8.4

9. YANG Data Model for SRv6 Base and Static

草案摘要如下:

This document describes a YANG data model for Segment Routing IPv6 (SRv6) base. The model serves as a base framework for configuring and managing an SRv6 subsystem and expected to be augmented by other SRv6 technology models accordingly. Additionally, this document also specifies the model for the SRv6 Static application.

詳細草案請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-srv6-yang-model
- https://tools.ietf.org/html/draft-raza-spring-srv6-yang-05

10.YANG Data Model for Segment Routing Policy

草案摘要如下:

Segment Routing architecture leverages the paradigm of source routing. It can be realized in a network data plane by prepending the packet with a list of instructions, a.k.a. segments. A segment can be encoded as a Multi-Protocol Label Switching (MPLS) label, IPv4 address, or IPv6 address. Segment Routing can be applied in the MPLS data plane by encoding segments in an MPLS label stack. It also can be applied to the IPv6 data plane by encoding a list of segment identifiers in IPv6 Segment Routing Extension Header (SRH). In this document is described the use of unified segment identifiers in use cases where interworking between SR-MPLS and SRv6 is required.

詳細草案請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-sr-policy-yang
- https://tools.ietf.org/html/draft-raza-spring-sr-policy-yang-02

11.Unified Identified usecase in IPV6 Segment Routing Networks

草案摘要如下:

Segment Routing architecture leverages the paradigm of source routing. It can be realized in a network data plane by prepending the packet with a list of instructions, a.k.a. segments. A segment can be encoded as a Multi-Protocol Label Switching (MPLS) label, IPv4 address, or IPv6 address.

Segment Routing can be applied in the MPLS data plane by encoding segments in an MPLS label stack. It also can be applied to the IPv6 data plane by encoding a list of segment identifiers in IPv6 Segment Routing Extension Header (SRH). In this document is described the use of unified segment identifiers in use cases where interworking between SR-MPLS and SRv6 is required.

詳細草案請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-unified-sid-in-srv6
- https://tools.ietf.org/html/draft-wmsaxw-6man-usid-id-use-00

12.Unified Identifier in IPv6 Segment Routing Networks

草案摘要如下:

Segment Routing architecture leverages the paradigm of source routing. It can be realized in a network data plane by prepending the packet with a list of instructions, a.k.a. segments. A segment can be encoded as a Multi-Protocol Label Switching (MPLS) label, IPv4 address, or IPv6 address. Segment Routing can be applied in MPLS data plane by encoding segments in MPLS label stack. It also can be applied to IPv6 data plane by encoding a list of segment identifiers in IPv6 Segment Routing Extension Header (SRH). This document extends the use of the SRH to unified identifiers encoded as MPLS label or IPv4 address, to compress the SRH, and support support more detailed network programming and interworking between SR-MPLS and SRv6 domains.

詳細草案請參考:

- https://tools.ietf.org/html/draft-mirsky-6man-unified-id-sr-04

13.Segment Routing Mapped To IPv6 (SRm6)

草案摘要如下:

This document describes Segment Routing mapped to IPv6 (SRm6). SRm6 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. SRm6 is optimized for ASIC-based forwarding devices that operate at high data rates.

詳細草案請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-draft-bonica-spring-srv6-plus
- https://tools.ietf.org/html/draft-bonica-spring-srv6-plus-06

14.Path Segment for SRv6 (Segment Routing in IPv6)

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 an MPLS data plane as well as an IPv6 data plane.

Further, Path Segment has been defined in order to identify an SR path in SR-MPLS networks, and used for various use-cases such as end-to-end SR Path Protection and Performance Measurement (PM) of an SR path. Similar to SR-MPLS, this document defines the Path Segment in SRv6 networks in order to identify an SRv6 path.

詳細草案請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-srv6-path-segment
- https://tools.ietf.org/html/draft-li-spring-srv6-path-segment-04

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

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:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-segment-routing-header-encapsulation-for-in-situ-oam-data
- https://tools.ietf.org/html/draft-ali-spring-ioam-srv6-02

16.An Experiment of SRv6 Service Chaining at Interop Tokyo 2019 ShowNet

草案摘要如下:

This document reports lessons learned from an experimental deployment of service chaining with Segment Routing over the IPv6 data plane (SRv6) at an event network. The service chaining part of the network was comprised of four SRv6-capable nodes (three products from different vendors), five SRv6 proxy nodes (two products from different vendors and three open source software), and six services. This network was deployed at Interop Tokyo 2019, and it successfully provided network connectivity and services to all the exhibitors and visitors on the event.

詳細草案請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-an-experiment-of-srv6-service-chaining-at-interop-tokyo-2019-shownet
- https://tools.ietf.org/html/draft-upa-srv6-service-chaining-exp-00

17.SRv6 Tagging proxy

草案摘要如下:

This document describes the tagging method of SRv6 proxy. SRv6 proxy is an SR endpoint behavior for processing SRv6 traffic on behalf of an SR-unaware service.

詳細草案請參考:

- ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-srv6-tagging-proxy
- ➢ https://tools.ietf.org/html/draft-eden-srv6-tagging-proxy-00

18.SRv6 for Deterministic Networking (DetNet)

草案摘要如下:

Deterministic Networking provides service with low jitter, bounded latency and low loss rate, using technologies of explicit route, resource reservation and service protection.This document specifies how to implement Deterministic Networking (DetNet) in a SRv6 Network.

詳細草案請參考:

- ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-spring-sessa-srv6-for-deterministic-networking
- ➢ https://tools.ietf.org/html/draft-geng-spring-srv6-for-detnet-00

19.DetNet SRv6 Data Plane Encapsulation

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:

- ➢ https://tools.ietf.org/html/draft-geng-detnet-dp-sol-srv6-01

20.Dynamic Network to Hybrid Cloud DCs

草案摘要如下:

This document analyzes the technological gaps when using SDWAN to dynamically interconnect workloads and applications hosted in rd various 3 party cloud data centers.

詳細內容請參考:

- https://datatracker.ietf.org/doc/draft-ietf-rtgwg-net2cloud-gap-analysis/
- https://datatracker.ietf.org/doc/draft-ietf-rtgwg-net2cloud-problem-statement/

21.Application-aware IPv6 Networking (APN6) Problem statement & usecases and Framework

草案摘要如下:

Network operators are facing the challenge of providing better network services for users. As the ever developing 5G and industrial verticals evolve, more and more services that have diverse network requirements such as ultra-low latency and high reliability are emerging, and therefore differentiated service treatment is desired by users. However, network operators are typically unaware of which applications are traversing their network infrastructure, which means that only coarse-grained services can be provided to users. As a result, network operators are only evolving their infrastructure to be large but dumb pipes without corresponding revenue increases that might be enabled by differentiated service treatment. As network technologies evolve including deployments of IPv6 and SRv6, the programmability provided by IPv6 and SRv6 encapsulations can be augmented by conveying application related information into the network. Adding application knowledge to the network layer allows applications to specify finer granularity requirements to the network operator.

This document analyzes the existing problems caused by lack of application awareness, and outlines various use cases that could benefit from an Application-aware IPv6 Networking (APN6) architecture.

詳細內容請參考

- https://tools.ietf.org/html/draft-li-apn6-problem-statement-usecases-01
- https://tools.ietf.org/html/draft-li-apn6-framework-00

22.SRv6 Path Egress Protection

草案摘要如下:

This document describes protocol extensions for protecting the egress node of a Segment Routing for IPv6 (SRv6) path or tunnel.

詳細內容請參考

- https://datatracker.ietf.org/doc/draft-hu-rtgwg-srv6-egress-protection/

23.Architecture for use of BGB as Central Controller

草案摘要如下:

BGP is a core part of a network including Software-Defined Networking (SDN) system. It has the traffic engineering information on the network topology and can compute optimal paths for a given traffic flow across the network.

This document describes some reference architectures for BGP as a central controller. A BGP-based central controller can simplify the operations on the network and use network resources efficiently for providing services with high quality.

詳細內容請參考

- https://datatracker.ietf.org/doc/draft-cth-rtgwg-bgp-control/

24.Implicit IV for Counter-based Ciphers in Encapsulating Security Payload (ESP)

草案摘要如下:

Encapsulating Security Payload (ESP) sends an initialization vector (IV) in each packet. The size of IV depends on the applied transform, being usually 8 or 16 octets for the transforms defined by the time this document is written. Some algorithms such as AES-GCM, AES-CCM and ChaCha20-Poly1305 when used with IPsec, take the IV to generate a nonce that is used as an input parameter for encrypting and decrypting. This IV must be unique but can be predictable. As a result, the value provided in the ESP Sequence Number (SN) can be used instead to generate the nonce. This avoids sending the IV itself, and saves in the case of AES-GCM, AES-CCM and ChaCha20-Poly1305 8 octets per packet. This document describes how to do this.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-ipsecme-implicit-iv-11.pdf

25.IKEv2 Notification Status Types for IPv4/IPv6 Coexistence

草案摘要如下:

This document specifies new IKEv2 notification status types to better manage IPv4 and IPv6 co-existence.
This document updates RFC7296.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-ipsecme-ipv6-ipv4-codes-04.pdf

26.Postquantum Preshared Keys for IKEv2

草案摘要如下:

The possibility of Quantum Computers pose a serious challenge to cryptography algorithms deployed widely today. IKEv2 is one example of a cryptosystem that could be broken; someone storing VPN communications today could decrypt them at a later time when a Quantum Computer is available. It is anticipated that IKEv2 will be extended to support quantum secure key exchange algorithms; however that is not likely to happen in the near term. To address this problem before then, this document describes an extension of IKEv2 to allow it to be resistant to a Quantum Computer, by using preshared keys.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-ipsecme-qr-ikev2-08.pdf

27.Intermediate Exchange in the IKEv2 Protocol

草案摘要如下:

This documents defines a new exchange, called Intermediate Exchange, for the Internet Key Exchange protocol Version 2 (IKEv2). This exchange can be used for transferring large amount of data in the process of IKEv2 Security Association (SA) establishment. Introducing Intermediate Exchange allows re-using existing IKE Fragmentation mechanism, that helps to avoid IP fragmentation of large IKE messages, but cannot be used in the initial IKEv2 exchange.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-ipsecme-ikev2-intermediate-02.pdf

28.IP Traffic Flow Security

草案摘要如下:

This document describes a mechanism to enhance IPsec traffic flow security by adding traffic flow confidentiality to encrypted IP encapsulated traffic. Traffic flow confidentiality is provided by obscuring the size and frequency of IP traffic using a fixed-sized, constant-send-rate IPsec tunnel. The solution allows for congestion control as well.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-hopps-ipsecme-iptfs-01.pdf

29.Labeled IPsec Traffic Selector support for IKEv2

草案摘要如下:

This document defines a new Traffic Selector (TS) Type for Internet Key Exchange version 2 to add support for negotiating Mandatory Access Control (MAC) security labels as a traffic selector of the Security Policy Database (SPD). Security Labels for IPsec are also known as "Labeled IPsec". The new TS type is TS_SECLABEL, which consists of a variable length opaque field specifying the security label. This document updates the IKEv2 TS negotiation specified in RFC 7296 Section 2.9.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-ipsecme-labeled-ipsec-02.pdf

30.Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2)

草案摘要如下:

This document describes how to extend Internet Key Exchange Protocol Version 2 (IKEv2) so that the shared secret exchanged between peers has resistance against quantum computer attacks. The basic idea is to exchange one or more post-quantum key exchange payloads in conjunction with the existing (Elliptic Curve) Diffie-Hellman payload.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-tjhai-ipsecme-hybrid-qske-ikev2-04.pdf

31.IKEv2 Optional SA&TS Payloads in Child Exchange

草案摘要如下:

This document describes a method for reducing the size of the Internet Key Exchange version 2 (IKEv2) exchanges at time of rekeying IKE SAs and Child SAs by removing or making optional of SA & TS payloads. Reducing size of IKEv2 exchanges is desirable for low power consumption battery powered devices. It also helps to avoid IP fragmentation of IKEv2 messages.

詳細內容請參考:

- ➢ https://tools.ietf.org/pdf/draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt-02.pdf

32.Deprecation of IKEv1 and obsoleted algorithms

草案摘要如下:

This document deprecates Internet Key Exchange version 1 (IKEv1) and additionally deprecates a number of algorithms that are obsolete.

詳細內容請參考:

- ➢ https://tools.ietf.org/pdf/draft-pwouters-ikev1-ipsec-graveyard-02.pdf

33.An Alternative Approach for Postquantum Preshared Keys in IKEv2

草案摘要如下:

An IKEv2 extension defined in [I-D.ietf-ipsecme-qr-ikev2] allows IPsec traffic to be protected against someone storing VPN communications today and decrypting it later, when (and if) Quantum Computers are available. However, this protection doesn't cover an initial IKEv2 SA, which might be unacceptable in some scenarios. This specification defines an alternative way get the same protection against Quantum Computers, which allows to extend it on the initial IKEv2 SA.

詳細內容請參考:

- ➢ https://tools.ietf.org/pdf/draft-smyslov-ipsecme-ikev2-qr-alt-00.pdf

34.Multiple SAs in one create child SA exchange

草案摘要如下:

IPsec packet processing with one Security Association (SA) per core is more efficient than having a SA shared by the multiple cores. This document optimizes the negotiation of multiple unidirectional SAs in order to minimize the impact SAs being shared by multiple cores.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-mglt-ipsecme-multiple-child-sa-00.pdf

35.In-Flight IPv6 Extension Header Insertion Considered Harmful

草案摘要如下:

In the past few years, as well as currently, there have and are a number of proposals to insert IPv6 Extension Headers into existing IPv6 packets while in-flight. This contradicts explicit prohibition of this type of IPv6 packet proccessing in the IPv6 standard. This memo describes the possible failures that can occur with EH insertion, the harm they can cause, and the existing model that is and should continue to be used to add new information to an existing IPv6 and other packets.

詳細內容請參考:

- https://tools.ietf.org/html/draft-smith-6man-in-flight-eh-insertion-harmful-01

36.SRH insertion within an SR Domain

草案摘要如下:

SRv6 is deployed in multiple provider networks. This document describes the usage of SRH insertion and deletion within the SR domain and how security and end-to-end integrity is guaranteed.

詳細內容請參考:

- https://tools.ietf.org/html/draft-voyer-6man-extension-header-insertion-08

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

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.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-6tisch-architecture-28.pdf

38.Minimal Security Framework for 6TiSCH

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.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-6tisch-minimal-security-13.pdf

39.6tisch Zero-Touch Secure Join protocol

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].

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-6tisch-dtsecurity-zerotouch-join-04.pdf

40.draft-ietf-6tisch-enrollment-enhanced-beacon

草案摘要如下:

In TSCH mode of IEEE STD 802.15.4, 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.

詳細內容請參考:

- https://tools.ietf.org/html/draft-ietf-6tisch-enrollment-enhanced-beacon-06

41.draft-ietf-6tisch-msf

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.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-6tisch-msf-08.pdf

DNS 相關技術討論

本次參與有關 DNS 技術討論會議，包括下列幾個工作小組:

i. abcd – Application Behavior Considering DNS
ii. DNSOP – Domain Name System Operations

過往 DNS 查詢機制多以明碼傳輸，易遭中間人(Man-in-the-middle, MITM)攻擊，針對 DNS 查詢或回應封包內容進行攔截、監控或竄改，造成使用者隱私侵害或導引至惡意網域。有鑑於此，IETF 研擬一系列的 DNS 隱私強化標準，包括：DNS over TLS (DoT)、DNS over HTTPS (DoH)、DNS-over-HTTP/3 等。

雖然 DoH 可解決 DNS 查詢遭監控與 MITM 攻擊等議題，但為避免使用者的 DNS 查詢歷史遭單一 DNS 提供者所掌握，與會者提出外部加密 DNS 服務搜尋機制。處於不受信任的網域時，如何利用 PROXY 進行查詢的機制。

It's Always DNS Themes

Group of DNS software engineers, working on:

- DNS privacy
- DNS protocol improvement
- DNS and services provisioning
- DNS monitoring

IETF 106 Hackathon – It's Always DNS

圖 6：DNS 會議

對於域名的部分，亦有與會者建議比照 Private IP、Private ASN 模式，於 DNS 管理上提供 Private DN。目前 Private DN 的規範有 RFC 6762 的 .LOCAL、研議中的有.LOACAL、.ALT、.INTERNAL 等域名，但這些域名過於冗長致不易推廣。本次會議，Roy Arends 建議在尚未被 ISO3901、ISO4217、ISO6166、及其他國際組織如:ICAO (International Civil Aviation Organization)、IATA (International Air Transport Association)、WIPO (World Intellectual Property Organization) 等使用的二字元域名中，挑選 .ZZ 作為 Private DN。

本次 DNS Hackathon 針對：DNS 隱私、DNS 協定改善、DNS 與服務供應、及 DNS 監控等議題進行實作探討。DNS 隱私部

分研議：DoT 與威權伺服器的連結、DoH 與 bind 9 的整合設計、並探討 DNS-over-HTTP/3 的可行性等。在 DNS 協定改善部分，討論有 DNS Server Cookies 的強化，並進行可與不同開源 DNS 系統溝通的實作。此外，亦討論 DNS Extended error 的強化，使相關協定能滿足當前 DNS 維運所需。DNS 與服務供應部分，探討新協定的對 DNS 服務參數的影響。DNS Monitoring 部分，則討論並驗證 root server 回應的正確性，同時提供監控工具。

會中進行主題包含以下內容:

1. Adaptive DNS Privacy (Application Behavior Considering DNS (ABCD))

   此演講針對三個主要議題進行探討:

   1. How can clients discover encrypted DNS resolvers?
   2. How can network advertise local policy?
   3. How can clients choose the right resolvers to use?

   草案摘要如下:

   This document defines an architecture that allows clients to dynamically discover designated resolvers that offer encrypted DNS services, and use them in an adaptive way that improves privacy while co-existing with locally provisioned resolvers. These resolvers can be used directly when looking up names for which they are designated. These resolvers also provide the ability to proxy encrypted queries, thus hiding the identity of the client requesting resolution.

   詳細內容請參考:

- ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-abcd-adaptive-dns-privacy
- ➢ https://tools.ietf.org/pdf/draft-pauly-dprive-adaptive-dns-privacy-01.pdf

2. Mozilla Canary Domain

   此演講針對 DNS over HTTPS 進行探討，包括 DoH bypass 基於 DNS 的 parental controls，以及其可能解決此問題之手法與應用說明。

   詳細內容請參考:

   - ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-abcd-mozilla-canary-domain

3. A Look at the ECS Behavior of DNS Resolvers (Rami Al-Dalky and Michael Rabinovich (Case Western Reserve University), Kyle Schomp (Akamai Technologies))

   演講摘要如下:

   Content delivery networks (CDNs) commonly use DNS to map end-users to the best edge servers. A recently proposed EDNS0-Client-Subnet (ECS) extension allows recursive resolvers to include end-user subnet information in DNS queries, so that authoritative nameservers, especially those belonging to CDNs, could use this information to improve user mapping. In this paper, we study the ECS behavior of ECS-enabled recursive resolvers from the perspectives of the opposite sides of a DNS interaction, the authoritative nameservers of a major CDN and a busy DNS resolution service. We find a range of erroneous (i.e., deviating from the protocol specification) and detrimental (even if compliant) behaviors that may unnecessarily erode client privacy, reduce the effectiveness of DNS caching, diminish ECS benefits, and in some cases turn ECS from facilitator into an obstacle to authoritative nameservers' ability to optimize user-to-edge-server mappings.

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-maprg-a-look-at-the-ecs-behavior-of-dns-resolvers-kyle-schomp
- http://delivery.acm.org/10.1145/3360000/3355586/p116-Al-Dalky.pdf

4. Message Digest for DNS Zones

摘要內容如下:

This document describes an experimental protocol and new DNS Resource Record that can be used to provide a message digest over DNS zone data. The ZONEMD Resource Record conveys the message digest data in the zone itself. When a zone publisher includes an ZONEMD record, recipients can verify the zone contents for accuracy and completeness. This provides assurance that received zone data matches published data, regardless of how the zone data has been transmitted and received. ZONEMD is not designed to replace DNSSEC. Whereas DNSSEC protects individual RRSets (DNS data with fine granularity), ZONEMD protects protects a zone’s data as a whole, whether consumed by authoritative name servers, recursive name servers, or any other applications. As specified at this time, ZONEMD is not designed for use in large, dynamic zones due to the time and resources required for digest calculation. The ZONEMD record described in this document includes fields reserved for future work to support large, dynamic zones.

詳細內容請參考:

- https://tools.ietf.org/pdf/draft-ietf-dnsop-dns-zone-digest-02.pdf

5. Extended DNS Errors

摘要內容如下:

This document defines an extensible method to return additional information about the cause of DNS errors. Though created primarily to extend SERVFAIL to provide additional information about the cause of DNS and DNSSEC failures, the Extended DNS Errors option defined in this document allows all response types to contain extended error information. Extended DNS Error information does not change the processing of RCODEs.

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-dnsop-sessb-extended-error-00
- https://tools.ietf.org/pdf/draft-ietf-dnsop-extended-error-12.pdf

6. Service binding and parameter specification via the DNS (DNS SVCB and HTTPSSVC)

摘要內容如下:

This document specifies the "SVCB" and "HTTPSSVC" DNS resource record types to facilitate the lookup of information needed to make connections for origin resources, such as for HTTPS URLs. SVCB records allow an origin to be served from multiple network locations, each with associated parameters (such as transport protocol configuration and keying material for encrypting TLS SNI). They also enable aliasing of apex domains, which is not possible with CNAME. The HTTPSSVC DNS RR is a variation of SVCB for HTTPS and HTTP origins. By providing more information to the client before it attempts to establish a connection, these records offer potential benefits to both performance and privacy. TO BE REMOVED: This proposal is inspired by and based on recent DNS usage proposals such as ALTSVC, ANAME, and ESNIKEYS (as well as long standing desires to have SRV or a functional equivalent implemented for HTTP). These proposals each provide an important function but are potentially incompatible with each other, such as when an origin is load-balanced across multiple hosting providers (multi-CDN). Furthermore, these each add potential cases for adding additional record lookups in-addition to AAAA/A lookups. This design attempts to provide a unified framework that encompasses the key functionality of these proposals, as well as providing some extensibility for addressing similar future challenges. TO BE REMOVED: The specific name for this RR type is an open topic for discussion. "SVCB" and "HTTPSSVC" are meant as placeholders as they are easy to replace. Other names might include "B", "SRV2", "SVCHTTPS", "HTTPS", and "ALTSVC".

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-dnsop-sessb-svcb-02
- https://tools.ietf.org/pdf/draft-ietf-dnsop-svcb-httpssvc-01.pdf

7. Interoperable Domain Name System (DNS) Server Cookies

摘要內容如下:

DNS cookies, as specified in RFC 7873, are a lightweight DNS transaction security mechanism that provides limited protection to DNS servers and clients against a variety of denial-of-service and amplification, forgery, or cache poisoning attacks by off-path attackers. This document provides precise directions for creating Server Cookies so that an anycast server set including diverse implementations will interoperate with standard clients.

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-dnsop-sessb-interoperable-dns-server-cookies-00
- https://tools.ietf.org/pdf/draft-ietf-dnsop-server-cookies-02.pdf

隱私保護相關技術討論

本次參與有關 Privacy 技術討論會議，包括下列幾個工作小組：

i. Pearg – Privacy Enhancements and Assessments Research Group
ii. HRPC - Human Rights Protocol Considerations

會中進行的主題包含以下內容:

1. Data privacy risks of machine learning (Prof Reza Shokri, N-CRiPT)

   此演講針對機器學習對於資料隱私性之威脅介紹。各種行為如網頁點'讚'，歷史地理位置，都可為提取個人訊息之來源。即使此類資料被某種程度去識別化，仍可透過機器學習來提取整體資料，或是學習的模組本身既可視為個資。此演講也提出幾個可以保護資料的一些方法如 data synthesis 等.

   詳細內容請參考:

   - https://datatracker.ietf.org/meeting/106/materials/slides-106-pearg-pearg-106-shokri
   - https://datatracker.ietf.org/meeting/106/materials/slides-106-pearg-pearg-106-shokri-00.pdf

2. Preserving Privacy via Homomorphic Encryption (Prof Xianhui Lu, SCRiPTS NTU)

   此演講針對使用 Homomorphic Encryption (HE) 來保護隱私，兩種 HE 的種類，partial 與 fully HE，以及他們的應用與技術性挑戰，效能等。演算法介紹以及根據不同資料產生客製化或是一般性的 HE 加密。

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-pearg-homomorphic-encryption-lu
- https://datatracker.ietf.org/meeting/106/materials/slides-106-pearg-homomorphic-encryption-lu-00.pdf

3. Personal Information Tagging for Logs (PITFoL) (Sandeep Rao, Grab)

此演講針對紀錄檔內個資進行標記之說明。尤其對於紀錄黨內的個資進行偵測，如何去識別化等議題探討以及手法介紹。

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-pearg-pitfol-sandeep
- https://datatracker.ietf.org/doc/slides-106-pearg-pitfol-sandeep/

4. Network-based Website Fingerprinting (Chris Wood)

此演講針對利用網站之 metadata 的洩漏資訊來攻擊終端使用者連結隱私進行議題探討。攻擊手法如利用 TLS metadata 來學習已加密的應用程式資訊與透過封包 IP 位置來學習伺服器資訊。

詳細內容請參考:

- https://datatracker.ietf.org/meeting/106/materials/slides-106-pearg-ietf106-pearg-website-fingerprinting
- https://datatracker.ietf.org/doc/slides-106-pearg-ietf106-pearg-website-fingerprinting/

5. Introduction to MEDUP (Bernie Hoeneisen)

此演講針對 Pervasive Monitoring (RFC 7258)進行議題探討。PM 通常為透過大範圍侵入性監視方式蒐集協議 metadata 如 headers, 流量分析等，攻擊機構與使用者的隱私。需透過協議設計減輕與預防此類攻擊。

詳細內容請參考:

- ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-pearg-medup-intro-bernie
- ➢ https://datatracker.ietf.org/doc/slides-106-pearg-medup-intro-bernie/

6. Privacy and Security Threat Analysis for Private Messaging (Iraklis Symeonidis)

此演講針對私訊(電子郵件與即時訊息)的隱私與安全威脅分析進行議題討論如威脅點，攻擊手法與案例分析。

詳細內容請參考:

- ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-pearg-private-messaging-analysis-iraklis
- ➢ https://datatracker.ietf.org/doc/slides-106-pearg-private-messaging-analysis-iraklis/

7. I-D association

此演講為針對 rfc8280，探討網路架構如何提供集會與組織權力以及草稿大綱探討。

詳細內容請參考:

- ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-hrpc-i-d-association
- ➢ https://tools.ietf.org/pdf/draft-irtf-hrpc-association-03.pdf

8. I-D political

此演講目的為探討政治與網路協議標準的關係，針對人權議題不同面向之提案草稿

詳細內容請參考:

- ➢ https://datatracker.ietf.org/meeting/106/materials/slides-106-hrpc-i-d-political
- ➢ https://tools.ietf.org/pdf/draft-irtf-hrpc-political-07.pdf

9. I-D guidelines

此演講目的為基於 RFC8280，制定人權規範。

詳細內容請參考:

- ➢ https://tools.ietf.org/pdf/draft-irtf-hrpc-guidelines-03.pdf

IoT 相關技術討論

本次參與有關 IoT 技術討論會議，包括以下工作小組：

i. T2TRG

會中進行的主題包含以下內容:

1. RESTful Design for Internet of Things Systems

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).

詳細內容請參考:

➢ https://tools.ietf.org/html/draft-irtf-t2trg-rest-iot-05

2. Secure IoT Bootstrapping: A Survey

草案摘要如下:

This document presents a survey of secure bootstrapping mechanisms available for smart objects that are part of an Internet of Things (IoT) network. It aims to provide a structured classification of the available mechanisms. The document does not prescribe any one secure bootstrapping mechanism and rather presents IoT developers with different options to choose from, depending on their use-case, security requirements and the user interface available on their smart objects.

詳細內容請參考:

➢ https://tools.ietf.org/html/draft-sarikaya-t2trg-sbootstrapping-07

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。

□ 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 2020 年 3 月 21 日至 2020 年 3 月 27 日於 Vancouver 舉行，相關資訊請參考：
https://www.ietf.org/how/meetings/107/

五. 會議議程:

以下為 IETF 106 Singapore 的完整議程表:

Saturday, November 16, 2019	
時間	議程
0830-2200	IETF Hackathon
0930-1800	Code Sprint

Sunday, November 17, 2019	
時間	議程
0830-1600	IETF Hackathon
1000-1200	IEPG Meeting
1000-1800	IETF Registration
1230-1300	Tutorial: Newcomers' Overview
1345-1445	Tutorial: Service Discovery for IP Applications
1500-1600	SEC AD Office Hours
1600-1700	Newcomers' Quick Connections (Open to Newcomers. Note that pre-registration is required)
1700-1900	Welcome Reception
1800-2000	Hot RFC Lightning Talks

Monday, November 18, 2019	
時間	議程
0800-0900	Beverage Break
0800-0900	Systers Networking Event
0830-0945	Side Meetings / Open Time
0830-1830	IETF Registration
0900-1000	NomCom Office Hours
1000-1200	
	Dispatch Joint with ARTAREA
	Dynamic Host Configuration
	Internet Congestion Control
	Information-Centric Networking
	Source Packet Routing in Networking
	MatheMatical Mesh
	IP Performance Measurement

1200-1330	Break
1330-1530	Calendaring Extensions 1330 - 1430
	Email mailstore and eXtensions To Revise or Amend 1430 – 1530
	Secure Telephone Identity Revisited
	Extensions for Scalable DNS Service Discovery Joint with HOMENET
	Home Networking Joint with DNSSD
	Decentralized Internet Infrastructure
	Privacy Enhancements and Assessments Research Group
	Link State Routing
	Transactional Authorization and Delegation
	Transport Area Working Group
1530-1550	Beverage and Snack Break
1550-1750	
	HTTP
	Distributed Mobility Management
	IRTF Open Meeting
	Network Configuration
	IPv6 Operations
	Multiprotocol Label Switching
	Routing Over Low power and Lossy networks
	EAP Method Update
1650-1750	TSV AD Office Hours
1750-1810	Beverage Break
1810-1940	Hackdemo Happy Hour
1810-1910	
	General Area Dispatch
	Extensions for Scalable DNS Service Discovery
	Light-Weight Implementation Guidance
	Measurement and Analysis for Protocols
	Inter-Domain Routing
	Network Virtualization Overlays
	Limited Additional Mechanisms for PKIX and SMIME
1930-2100	Newcomers' Dinner (Open to Newcomers. Note that pre-registration is required and a $25USD fee will be

	charged.)

Tuesday, November 19, 2019	
時間	議程
0830-0900	Beverage Break
0830-0945	Side Meetings / Open Time
0830-1830	IETF Registration
0830-0945	Community Process for RSE Model Evolution
0900-1000	NomCom Office Hours
1000-1200	
	Trustworthy Multipurpose Remote ID
	Human Rights Protocol Considerations
	Network Modeling
	Locator/ID Separation Protocol
	Routing Over Low power and Lossy networks
	Security Automation and Continuous Monitoring
	Trusted Execution Environment Provisioning
	QUIC
1200-1330	Break
1330-1500	
	Application Behavior Considering DNS
	Global Access to the Internet for All
	Babel routing protocol
	Link State Vector Routing
	Traffic Engineering Architecture and Signaling
	Software Updates for Internet of Things
	RTP Media Congestion Avoidance Techniques
1500-1520	Beverage and Snack Break
1520-1650	
	GitHub Integration and Tooling
	IPv6 over Low Power Wide-Area Networks
	Network Modeling
	BGP Enabled ServiceS
	Authentication and Authorization for Constrained Environments
	Remote ATtestation ProcedureS

	Transport Services
1650-1710	Beverage Break
1710-1840	Internet Area AD Office Hours
1710-1840	
	JSON Mail Access Protocol
	Quantum Internet Proposed Research Group
	Autonomic Networking Integrated Model and Approach
	Domain Name System Operations
	Bidirectional Forwarding Detection
	Traffic Engineering Architecture and Signaling
	Security Dispatch
	Multipath TCP
1900-2300	IETF 106 Social Event at the ArtScience Museum Marina Bay Sands - Hosted by Nokia

Wednesday, November 20, 2019	
時間	**議程**
0800-0900	Beverage Break
0830-0945	Side Meetings / Open Time
0830-1710	IETF Registration
0900-1000	NomCom Office Hours
0900-0945	Routing AD Office Hours
1000-1200	
	Constrained RESTful Environments
	Registration Protocols Extensions
	Network Time Protocol
	Operations and Management Area Working Group Combined OpsAWG / OpsAREA
	Reliable and Available Wireless
	Trusted Execution Environment Provisioning
	QUIC
1200-1330	Break
1215-1315	WG Chairs Forum (For WG Chairs Only)
1330-1500	
	WebTransport
	IPv6 over Networks of Resource-constrained Nodes

	Crypto Forum
	Benchmarking Methodology
	Routing Area Working Group
	Web Authorization Protocol
1500-1520	Beverage Break
1520-1650	
	Web Packaging
	Autonomic Networking Integrated Model and Approach
	SIDR Operations
	BGP Enabled ServiceS
	Mobile Ad-hoc Networks
	Lightweight Authenticated Key Exchange
1650-1710	Beverage and Snack Break
1710-1940	IETF Plenary

Thursday, November 21, 2019	
時間	**議程**
0800-0900	Beverage Break
0800-0900	Newcomers' Feedback Session
0830-0945	Side Meetings / Open Time
0830-1800	IETF Registration
0900-1000	NomCom Office Hours
1000-1200	
	Relay User Machine
	Network Management
	Thing-to-Thing
	Media OPerationS
	Bit Indexed Explicit Replication
	Common Control and Measurement Plane
	Transport Layer Security
	Transport Area Working Group
1200-1330	Break
1215-1315	Systers Lunch
1230-1315	Host Speaker Series
1330-1530	
	HTTP

	IPv6 Maintenance
	Coding for efficient NetWork Communications Research Group
	Domain Name System Operations
	Protocols for IP Multicast
	Routing In Fat Trees
	Security Area Open Meeting
	Delay/Disruption Tolerant Networking
1530-1550	Beverage and Snack Break
1550-1720	
	Internet Area Working Group
	MBONE Deployment
	Deterministic Networking
	Source Packet Routing in Networking
	CBOR Object Signing and Encryption
	IP Security Maintenance and Extensions
	Web Authorization Protocol
	Application-Layer Traffic Optimization
1720-1740	Beverage Break
1740-1840	
	Concise Binary Object Representation Maintenance and Extensions
	IPv6 Maintenance
	Deterministic Networking
	Inter-Domain Routing
	Transport Layer Security
	Transport Area Open Meeting

Friday, November 22, 2019	
時間	**議程**
0800-0900	Beverage Break
0830-0945	Side Meetings / Open Time
0830-1230	IETF Registration
1000-1200	
	IPv6 over the TSCH mode of IEEE 802.15.4e
	DNS PRIVate Exchange

	Computing in the Network Proposed Research Group
	Path Computation Element
	Routing Area Working Group
	Messaging Layer Security
	Remote ATtestation ProcedureS
	TCP Maintenance and Minor Extensions
1200-1220	Beverage and Snack Break
1220-1350	
	Audio/Video Transport Core Maintenance
	Constrained RESTful Environments
	Network Management
	Path Aware Networking RG
	Global Routing Operations
	Link State Routing
	Automated Certificate Management Environment
	DDoS Open Threat Signaling

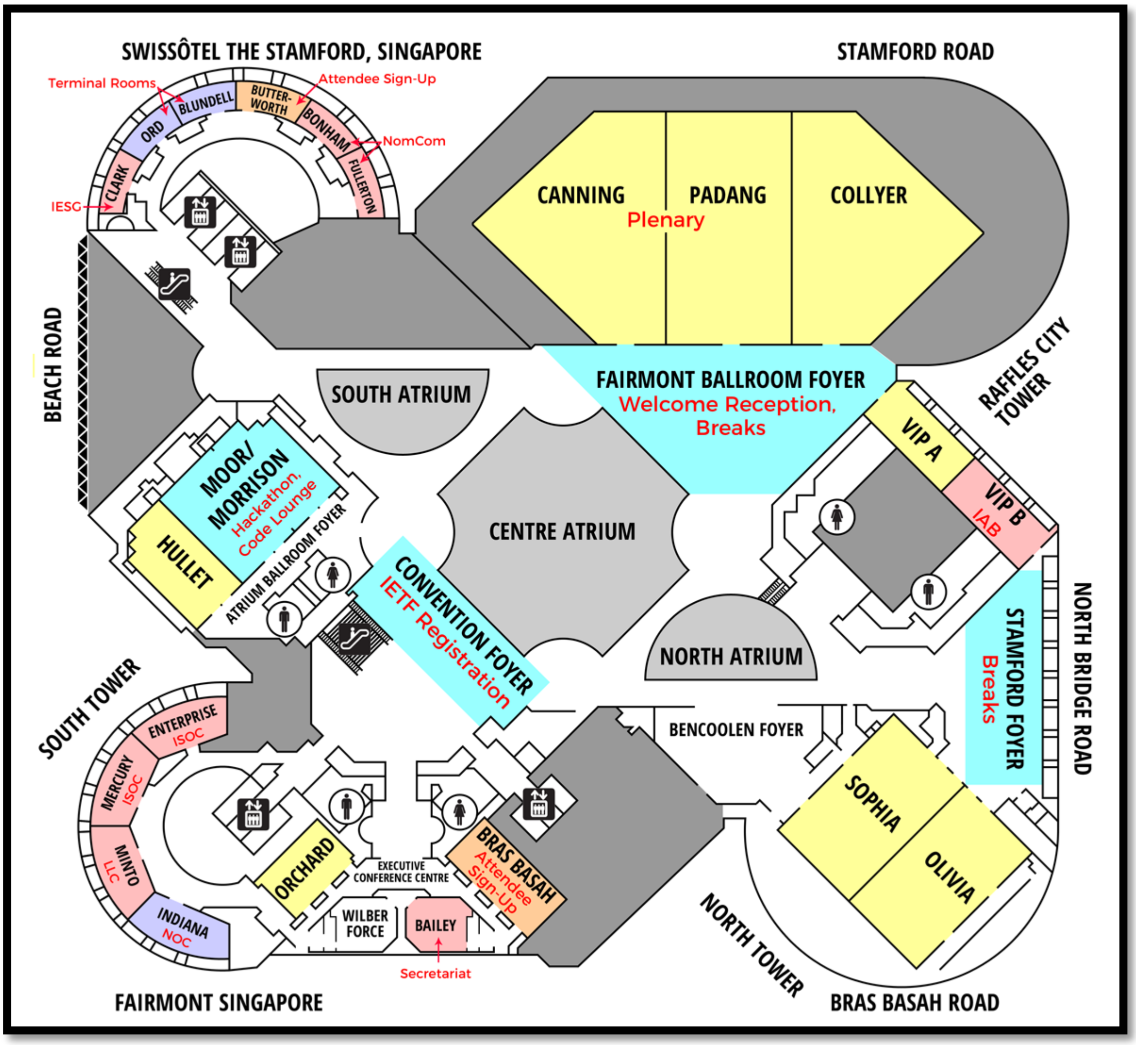

SWISSÔTEL THE STAMFORD, SINGAPORE
STAMFORD ROAD
Terminal Rooms
Attendee Sign-Up
BLUNDELL
BUTTER-WORTH
ORD
BONHAM
NomCom
FULLERTON
CLARK
IESG
CANNING
PADANG
COLLYER
Plenary
BEACH ROAD
SOUTH ATRIUM
FAIRMONT BALLROOM FOYER
Welcome Reception,
Breaks
RAFFLES CITY TOWER
VIP A
VIP B
IAB
MOOR/ MORRISON
Hackathon, Code Lounge
HULLET
ATRIUM BALLROOM FOYER
CENTRE ATRIUM
CONVENTION FOYER
IETF Registration
NORTH ATRIUM
STAMFORD FOYER
Breaks
NORTH BRIDGE ROAD
SOUTH TOWER
ENTERPRISE
ISOC
MERCURY
ISOC
MINTO
LLC
INDIANA
NOC
ORCHARD
EXECUTIVE CONFERENCE CENTRE
WILBER FORCE
BAILEY
Secretariat
BRAS BASAH
Attendee Sign-Up
BENCOOLEN FOYER
SOPHIA
OLIVIA
NORTH TOWER
FAIRMONT SINGAPORE
BRAS BASAH ROAD

圖 7：會議場地配置圖