財團法人台灣網路資訊中心因公出國人員報告書

112 年 04 月 11 日

報告人 姓　名	許乃文 林福寬	服務單位及職稱	技術組組長 技術組工程師
出國期間	112 年 03 月 24 日 至 112 年 04 月 01 日	出國地點	日本橫濱
機密等級	□機密　□密　■一般		
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

IETF(Internet Engineering Task Force, 網際網路工程任務組)是網際網路的首要標準開發組織(standards development organization, SDO)，他是一個開放的標準組織，負責推廣制定各種自願性的網際網路標準。這些標準經常被網際網路用戶、網路營運商或設備供應商採用，進而幫助塑造網際網路的發展軌跡。

IETF 第 116 次會議於 2023 年 03 月 25 日(星期六)至 03 月 31 日(星期五)於日本橫濱(Yokohama)舉辦。本次會議為期 7 天，是由 WIDE Project 主辦，總共有 1,773 人報名參加會議(1,008 人現場參加、765 人遠端參與)。

會議主題(TETF Areas)共分為以下 7 大項目：

1. Applications and Real-Time Area (art)
2. General Area (gen)
3. Internet Area (int)
4. Operations and Management Area (ops)
5. Routing Area (rtg)
6. Security Area (sec)
7. Transport Area (tsv)

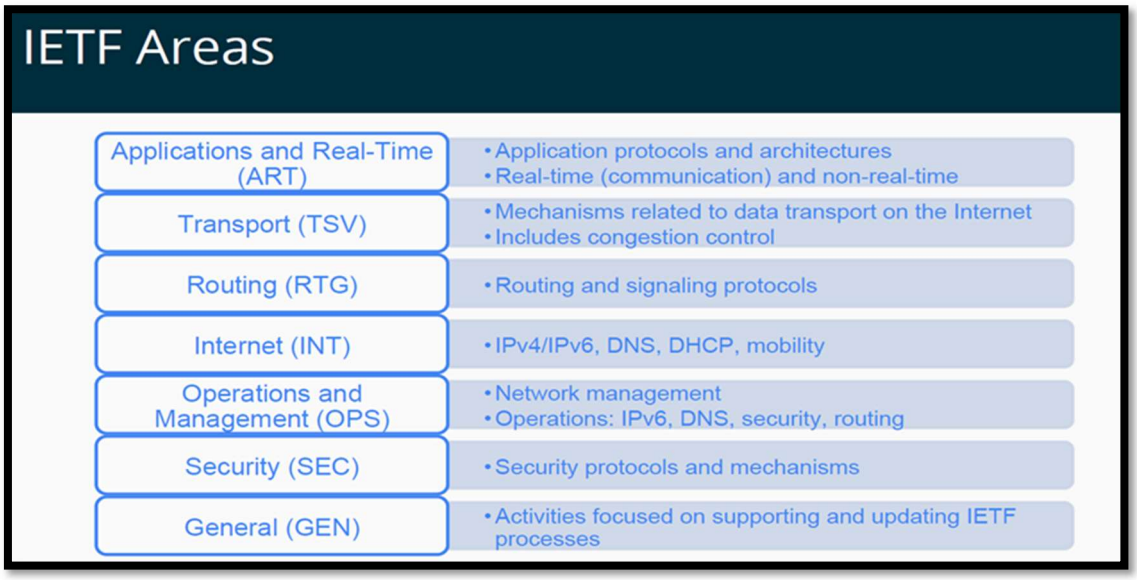

圖 1：IETF Areas

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、及 QUIC 等相關議題。

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

二、會議議程

IETF 第 116 次會議議程表請參閱附錄及會議網站：

https://datatracker.ietf.org/meeting/116/agenda/

三、考察、訪問心得

Hackathons

IETF Hackathons 活動是透過不同主題的分組討論及交換彼此的想法，並展示範例程式及尋求解決方案，將開源的協作精神與效率引入至 IETF 的標準活動中，用以改良現有的網際網路標準或制定新的規範，並且利用這樣的活動將開發人員帶入 IETF 並對其產生興趣。

圖 2：Hackathons Kickoff

Hackathons 是開放給所有人免費參加，他是一項合作活動，而不是一場比賽。在 Hackathons 分組討論的主題，幾乎涵蓋所有 IETF Work Areas 的範圍，包括 DNS、HTTP 2.0、QUIC、WebRTC、IPv6 等等。

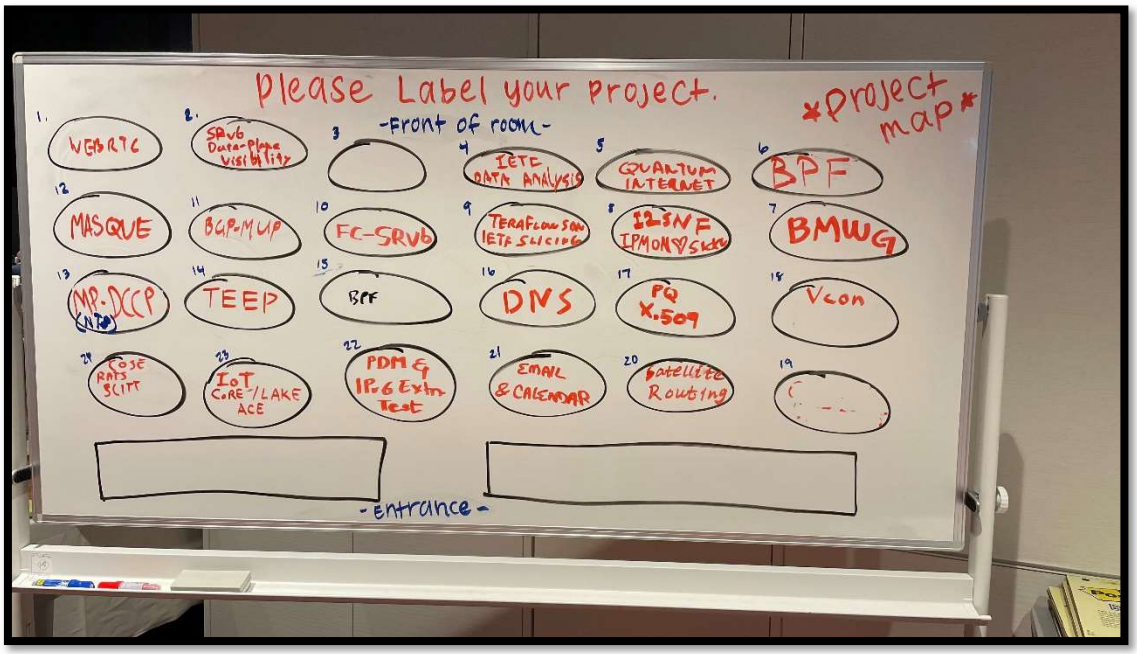

圖 3：Hackathons 分組討論位置表

這次的分組討論中，有一「量子網際網路(Quantum Interne

t)」的主題滿特別的，原來量子科技不只能運用在電腦運算，也能利用其特性組建成資料傳遞速度超越光速的網際網路，這樣的科技運用，著實令人期待。若想對量子網際網路多做了解的話，也能參閱該單位所提供之電子書籍(https://github.com/sfc-aqua/Overview-of-Quantum-Communications-E)。

Hackathons 簡報資料：https://github.com/IETF-Hackathon/ietf116-project-presentations/

DNS 相關

在 DNS 的議程中，提到目前多數的網路提供商，在提供服務時（例：ACME, Automatic Certificate Management Environment)，需要客戶使用 DNS 記錄來驗證是否擁有該域名的管理權限？而在驗證完成後，客戶往往忘記刪除該筆記錄，當這些無用資料累積到一定數量時，還可能會影響 DNS 查詢的回應。因此，有講者提出在 TXT 記錄中，增加到期的標籤(expiry)，讓系統知道該筆記錄何時可以刪除。

有一個新草案，是討論到目前 DNSSEC 的查詢中，針對「無設定資料(NODATA)」及「域名不存在(NXDOMAIN)」有不同的處理(回應)方式。在 NODATA 的時候，DNS 伺服器只需要回應 1 筆 NSEC 記錄，但在 NXDOMAIN 的情況，則可能需要回應 2~3 筆 NSEC 記錄，這導致在 NXDOMAIN 的狀況時，DNS 查詢所回應的資料比 NODATA 多了許多，不僅浪費網路頻寬資源、也使 DNS 伺服器的性能損耗增加，因此，提出此草案來討論及改善，這些回應的資料是否可以精簡或比照 NODATA 的處理方式即可？

另外，針對 CDS/CDNSKEY 的 RFC 標準，也有人提出一些可能

產生潛在安全疑慮的地方，例如：自動 DS 管理機制、詢問單一 DNS 伺服器、在乎 SOA 中比較新的序號資料而非考慮資料一致性、多個 DNS 代管商可能會出現嚴重錯誤…等。

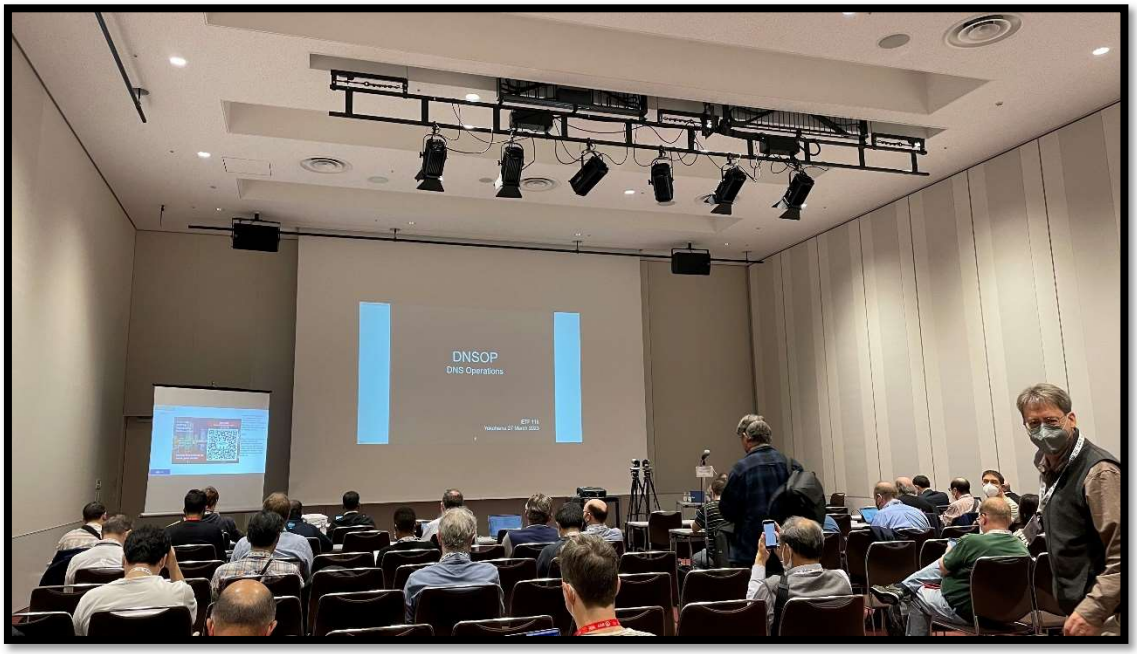

圖 4：DNSOP 會議主題現場

EPP 相關

可擴展供應協議(EPP,Extensible Provisioning Protocol)是提供域名註冊管理機構與註冊商之間，一種靈活的資料傳遞的。根據講者的研究後發現，在一些頂極域名(TLD, Top-level Domain)營運商在 DNS 設定授權的 TTL(Time to Live)時間過久，因此提出建議，以 EPP 的方式，來讓域名註冊商可以自行指定 TTL 的時間。規劃在<create>、<update>及<info>項目中，針對 NS、DS、A 及 AAAA 這 4 種記錄提供 TTL 的設定(EX: <ttl:secs>3600</ttl:secs>)。

HTTP/3(QUIC)相關

QUIC(Quick UDP Internet Connection)是基於 UDP 協定的

新一代網際網路傳輸協議，原本是由 Google 於 2013 提出，而 IETF 於 2018 年將他重新命名為 HTTP/3，利用此協議，可以降低連線交握的時間至 1 個 RTT(Round Trip Time)。在此議題上，有講者提出幾個問題點。第一點是在傳輸較大的 TLS 資料時，會觸發多個 RTT 交握(handshake)，在針對約 25 萬個使用 QUIC 的網站中，大約有 38%的網站出現此一現象；第二點是伺服器遭遇到不完整的交握(例：反射性的 DDoS 攻擊)而認為資料遺失而重新發送資料時，可能發生高的放大係數；第三點是在 CDN(Content Delivery Network 或 Content Distribution Network)設置中，針對了低延遲進行了優化，卻也會導致更大的交握資料。在多個 CDN 配置中，QUIC 伺服器可以分開存取及處理 TLS 資料，但這可能會增加延遲並使用戶端對於 RTT 的估計錯誤。

其他網路相關

在處理網路擁塞的議題上，也有針對未來的網路是否會全面走向 BBR(Bottleneck Bandwidth and RTT)主導的網際網路環境為主題,去比較使用 CUBIC 及 BBR 兩種演算法之間的差異或影響。CUBIC 是使用 CWND(Congestion Window)為基準，利用「封包遺失」來判斷網路是否擁塞，而 BBR 則是使用 RTT_{min} 及頻寬估算來判斷是否擁塞。講者以數學模型來預測在使用兩種演算法的網際網路環境中，CUBIC 與 BBR 之間互相競爭的吞吐量份額(throughput shares)，隨著瓶頸處(bottleneck)BBR 流量的增加，他的吞吐量優勢會隨之下降。

四、建議意見

1. 持續關注相關各 WGs 動態及相關訊息。

2. 持續關注 DNS 的相關技術發展，以掌握最新的發展趨勢。
3. 持續了解 EPP 的政策規範，以配合修改相關作業流程。
4. 持續參與 IETF 以掌握相關技術規範的演進及狀態。

五、其他相關事項或資料

IETF 第 116 次會議的會議錄影畫面，可以至以下的網站觀看。

https://www.meetecho.com/ietf116/recordings

IETF 下一次的會議(第 117 次)，預計於 2023 年 07 月 22 日(星期六)至 07 月 28 日(星期五)於美國舊金山舉辦。相關會議資訊可以參閱 IETF 官網。

IETF 116 (Yokohama)會議的議程表如下：

Saturday, March 25, 2023	
時間	議程
09:30 - 20:30	Hackathon
10:00 - 18:00	Code Sprint
10:30 - 11:00	Hackathon Kickoff

Sunday, March 26, 2023	
時間	議程
09:30 - 16:00	Hackathon
10:00 - 12:00	IEPG Meeting
10:00 - 18:00	IETF Registration
10:30 - 11:30	TSV ADs Office Hours
12:30 - 13:30	Tutorial: New Participants' Overview
14:00 - 16:00	Hackathon Project Results
16:00 - 17:00	New Participants' Quick Connections (Note that pre-registration is required)
16:00 - 17:00	RTG ADs Office Hours
17:00 - 20:00	Welcome Reception & Meeting Host Demonstrations
18:00 - 20:00	Hot RFC Lightning Talks

Monday, March 27, 2023	
時間	議程
08:15 - 09:15	Systers Networking Event
08:30 - 09:30	*Continental Breakfast*
08:30 - 18:00	IETF Registration
09:30 - 11:30	**Monday Session I**
—	Dispatch (Joint with ARTAREA)
—	Distributed Mobility Management
—	Computing in the Network Research Group

—	IPv6 Operations
—	Link State Routing
—	EAP Method Update
—	Remote ATtestation ProcedureS
—	IP Performance Measurement
11:30 - 13:00	*Break*
11:30 - 12:45	Story Telling Event sponsored by JPRS
12:00 - 12:45	SEC ADs Office Hours
13:00 - 15:00	**Monday Session II**
—	Content Delivery Networks Interconnection
—	Building Blocks for HTTP APIs
—	BPF/eBPFBoF
—	IRTF Open Meeting
—	Network Configuration
—	Protocols for IP Multicast
—	CBOR Object Signing and Encryption
—	Privacy Preserving Measurement
15:00 - 15:30	*Beverage and Snack Break*
15:30 - 17:00	**Monday Session III**
—	Secure Media Frames
—	Quantum Internet Research Group
—	Media OPerationS
—	Path Computation Element
—	Time-Variant Routing
—	Javascript Object Signing and Encryption
—	Trusted Execution Environment Provisioning
—	TCP Maintenance and Minor Extensions
17:00 - 17:30	*Beverage Break*
17:30 - 18:30	**Monday Session IV**
—	Media Type Maintenance

—	Extensions for Scalable DNS Service Discovery
—	MAC Address Device Identification for Network and Application Services
—	Routing Area Working Group
—	Security Dispatch
—	Application-Layer Traffic Optimization
18:30 - 19:30	Hackdemo Happy Hour
18:45 - 20:45	New Participants Dinner (Open to newcomers. Note that pre-registration is required and a $15USD fee will be charged.)

Tuesday, March 28, 2023	
時間	議程
08:30 - 09:30	*Continental Breakfast*
08:30 - 09:30	IETF Chair Office Hours
08:30 - 17:30	IETF Registration
09:30 - 11:30	**Tuesday Session I**
—	Structured EmailBoF
—	Information-Centric Networking
—	Operations and Management Area Working Group (Combined OpsAWG/OpsAREA)
—	RFC Series Working Group
—	Pseudowire And LDP-enabled Services (Joint PALS/MPLS/DETNET)
—	Web Authorization Protocol
—	Delay/Disruption Tolerant Networking
—	Transport Area Working Group
11:30 - 13:00	*Break*
11:30 - 13:00	IETF-3GPP Coordination
13:00 - 15:00	**Tuesday Session II**
—	Audio/Video Transport Core Maintenance
—	Constrained RESTful Environments
—	JSON Mail Access Protocol (Joint JMAP/EXTRA session)

—	Path Aware Networking RG
—	Benchmarking Methodology
—	Locator/ID Separation Protocol
—	Supply Chain Integrity, Transparency, and Trust
—	Transport Layer Security
14:30 - 15:30	INT ADs Office Hours
15:00 - 15:30	*Beverage and Snack Break*
15:30 - 16:30	**Tuesday Session III**
—	Domain-based Message Authentication, Reporting & Conformance
—	HTTP
—	Transfer dIGital cREdentialS Securely
—	Drone Remote ID Protocol
—	Multiprotocol Label Switching
—	Routing Over Low power and Lossy networks
—	DANE Authentication for Network Clients Everywhere
—	Transport Area Open Meeting
16:30 - 17:00	*Beverage Break*
17:00 - 18:00	**Tuesday Session IV**
—	Domain BoundariesBoF
—	System for Cross-domain Identity Management
—	Internet Area Working Group
—	Network Time Protocols
—	Routing In Fat Trees
—	Oblivious HTTP Application Intermediation
—	RADIUS EXTensions

Wednesday, March 29, 2023	
時間	議程
08:15 - 09:20	Wednesday EDM Program

—	Evolvability, Deployability, & Maintainability
08:30 - 09:30	*Continental Breakfast*
08:30 - 17:30	IETF Registration
09:30 - 11:30	Wednesday Session I
—	vConBoF
—	IPv6 Maintenance
—	Usable Formal Methods Proposed Research Group
—	BGP Enabled ServiceS
—	Common Control and Measurement Plane
—	Source Address Validation in Intra-domain and Inter-domain Networks
—	Limited Additional Mechanisms for PKIX and SMIME
—	Multiplexed Application Substrate over QUIC Encryption
11:30 - 13:00	*Break*
11:45 - 12:45	WG Chairs Forum (For WG Chairs Only)
13:00 - 15:00	Wednesday Session II
—	WebTransport
—	General Area Dispatch
—	Internet Congestion Control
—	Privacy Enhancements and Assessments Research Group
—	Autonomic Networking Integrated Model and Approach
—	SIDR Operations
—	Source Packet Routing in Networking
—	Key TransparencyBoF
15:00 - 15:30	*Beverage Break*
15:30 - 16:30	IETF Trust Office Hours
15:30 - 17:00	Wednesday Session III
—	Secure Telephone Identity Revisited
—	Stub Network Auto Configuration for IPv6
—	Measurement and Analysis for Protocols

—	Network Management
—	MBONE Deployment
—	Computing-Aware Traffic Steering
—	IP Security Maintenance and Extensions
—	Open Specification for Pretty Good Privacy
17:00 - 17:30	*Beverage and Snack Break*
17:30 - 19:30	IETF Plenary

Thursday, March 30, 2023	
時間	議程
08:30 - 09:30	*Continental Breakfast*
08:30 - 17:00	IETF Registration
09:30 - 11:30	Thursday Session I
—	More Instant Messaging Interoperability
—	Decentralized Internet Infrastructure
—	Global Access to the Internet for All
—	Domain Name System Operations
—	Deterministic Networking
—	Inter-Domain Routing
—	Lightweight Authenticated Key Exchange (Joint ACE/LAKE session)
—	QUIC
11:30 - 13:00	*Break*
11:30 - 13:00	Liaison Coordinators Office Hours
11:45 - 12:45	Host Speaker Series: Quantum Internet
13:00 - 14:30	Thursday Session II
—	Media Over QUIC
—	IPv6 over Low Power Wide-Area Networks (Joint session with SCHC)
—	Research and Analysis of Standard-Setting Processes Proposed Research Group
—	Global Routing Operations

—	Traffic Engineering Architecture and Signaling
—	Interface to Network Security Functions
—	Software Updates for Internet of Things
14:30 - 15:00	*Beverage Break*
15:00 - 16:00	Thursday Session III
—	Concise Binary Object Representation Maintenance and Extensions
—	Registration Protocols Extensions
—	IAB Open Meeting
—	Dynamic Host Configuration
—	Operational Security Capabilities for IP Network Infrastructure
—	Traffic Engineering Architecture and Signaling
—	Automated Certificate Management Environment
—	Messaging Layer Security
16:00 - 16:30	*Beverage and Snack Break*
16:30 - 17:30	Thursday Session IV
—	Serialising Extended Data About Times and Events
—	WebRTC Ingest Signaling over HTTPS
—	Adaptive DNS Discovery
—	Routing Area Open Meeting
—	Security Area Open Meeting
—	Transport Area Working Group
17:45 - 18:45	New Participants' Social Hour
17:45 - 18:45	Systers Happy Hour
19:00 - 21:30	IETF 116 Social Event at Osanbashi Pier - Hosted by WIDE

Friday, March 31, 2023	
時間	議程
08:30 - 09:30	*Continental Breakfast*
08:30 - 12:30	IETF Registration

09:30 - 11:30	Friday Session I
—	HTTP
—	Secure Asset Transfer Protocol
—	IPv6 over Networks of Resource-constrained Nodes
—	Crypto Forum
—	Human Rights Protocol Considerations
—	Network Modeling
—	Routing Area Working Group
—	Web Authorization Protocol
11:30 - 12:00	*Beverage and Snack Break*
12:00 - 13:30	Friday Session II
—	Media Over QUIC
—	IOT Operations
—	Bit Indexed Explicit Replication
—	Reliable and Available Wireless
—	Grant Negotiation and Authorization Protocol
—	Post-Quantum Use In Protocols
—	Privacy Pass
—	Network File System Version 4