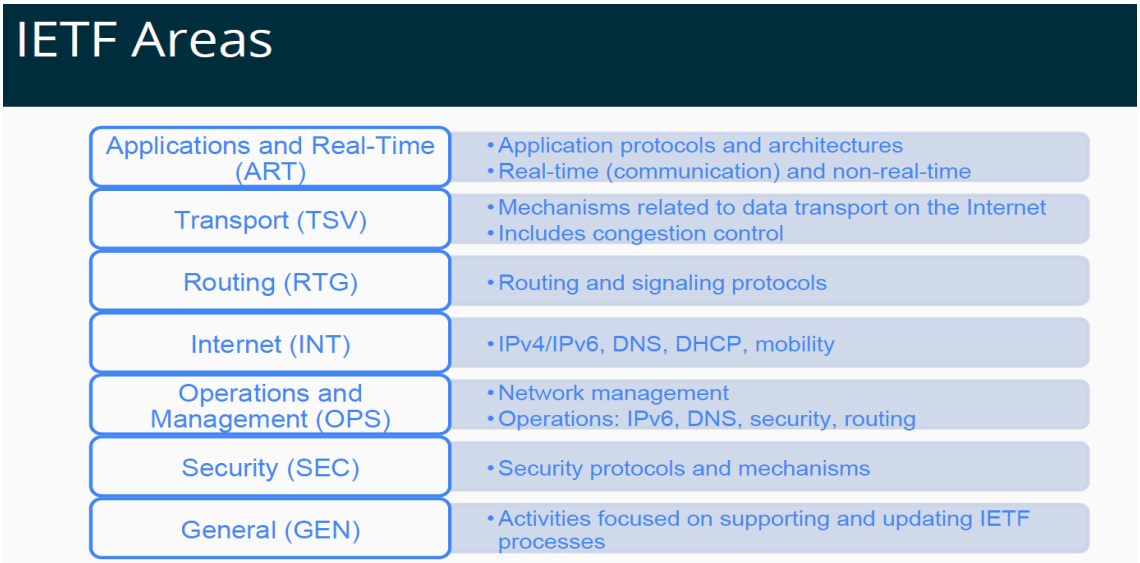
財團法人台灣網路資訊中心因公出國人員報告書 108 年 4 月 18 日

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：
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 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 (三)	9:00-11:00	Security Events WG
	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：

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