財團法人台灣網路資訊中心因公出國人員報告書 107 年 11 月 9 日

報告人 姓　名	丁綺萍、 許淑芳	服務單位及 職稱	副執行長、 專案經理
出國期間	107/11/4-9	出國地點	Bangkok, Thailand
出國事由	參加 IETF 103 Bangkok 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 許淑芳 (簽章)

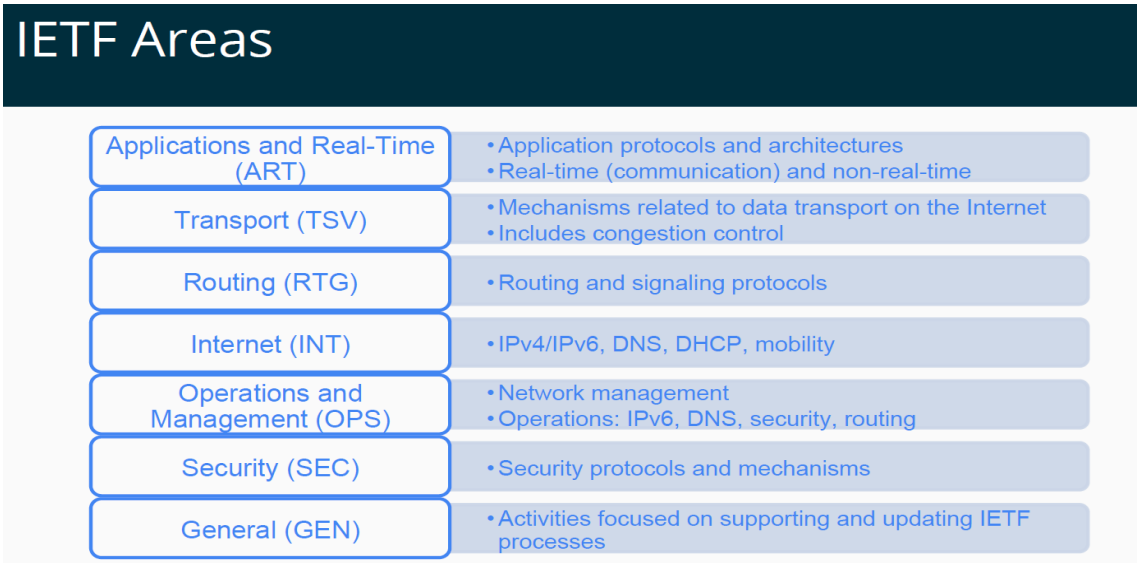
註：

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 103 Bangkok 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。此次會議在泰國曼谷召開，會議日期 11 月 3 日至 9 日共為期 7 天，這是 IETF 所舉行的第 103 次會議。本次會議約有 830 人參與，由 Huawei（華為）及 Cisco（思科）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/

二、 會議行程：

詳如會議網站 https://www.ietf.org/how/meetings/103/。
議程 https://datatracker.ietf.org/meeting/103/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
107/11/4 (日)	8:50	台灣桃園國際機場
	11:50	抵達曼谷國際機場
107/11/5 (一)	9:00	IETF Registration
	9:00-11:00	IPv6 Operations
	11:00-11:20	Beverage and Snack Break

	11:20-12:20	Crypto Forum
	12:20-13:50	Break
	13:50-15:50	Transport Layer Security
	15:50-16:10	Beverage and Snack Break
	16:10-18:10	IPv6 over Networks of Resource-constrained Nodes
107/11/6 (二)	9:00-11:00	IPv6 over Low Power Wide-Area Networks
	11:00-11:20	Beverage and Snack Break
	11:20-12:20	Web Authorization Protocol
	12:20-13:50	Break
	13:50-15:50	IPv6 Maintenance
	15:50-16:10	Beverage and Snack Break
	16:10-18:10	Thing-to-Thing
107/11/7 (三)	9:00-11:00	Trusted Execution Environment Provisioning
	11:00-11:20	Beverage and Snack Break
	11:20-12:20	Transport Layer Security
	12:20-13:50	Break
	13:50-15:20	IP Security Maintenance and Extensions
	15:20-15:40	Beverage Break
	15:40-17:10	Interface to Network Security Functions
	17:10-17:30	Beverage and Snack Break
	17:30-20:00	IETF Plenary
107/11/8 (四)	9:00-11:00	Software Updates for Internet of Things
	11:00-11:20	Beverage and Snack Break
	11:20-12:20	Quantum Internet Proposed Research Group
	12:20-13:50	Break
	12:45-13:30	Host Speaker Series Challenges of Evolution Towards Autonomous Network
	13:50-15:50	Extensions for Scalable DNS Service Discovery
	15:50-16:10	Beverage and Snack Break
	16:10-18:10	IPv6 over the TSCH mode of IEEE 802.15.4e
107/11/9 (五)	15:50	曼谷國際機場
	20:25	抵達台灣桃園國際機場

三、 考察、訪問心得：

IETF 103 Bangkok 會議。

在此次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

有關 IPv6 技術討論會議，會中進行的主題包含以下內容：

1. CERNET2 IPv6-only Practice: Backbone, Servers, Clients and 4aaS

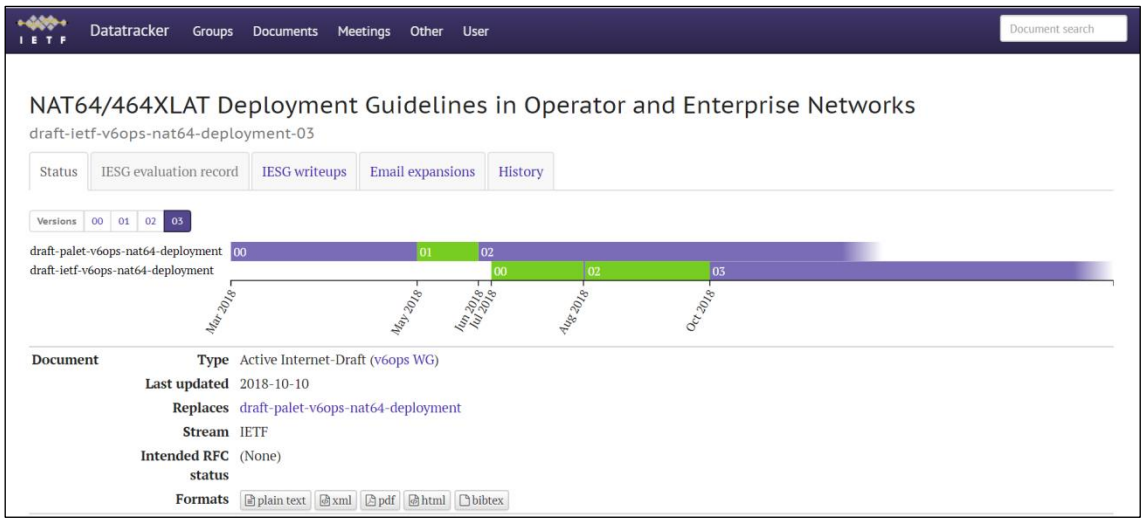
   CERNET（China Education and Research Network，中國教育研究網路）從 1994 開始投入計畫，由超過 2,000 以上的大學及研究機構參與，2003 年更進一步推展 CERNET2 計畫，採用純 IPv6 的骨幹網路，有超過 600 個以上的大學網路連結上 CERNET2 網路系統，中國利用此系統做為 IPv6 研究及實驗的網路系統。透過此實驗系統連結設備製造商、網路服務商及網路產業各領域共同參與推廣 IPv6。在此會議 IPv6 操作（v6ops）工作小組將分享 CERNET2 採用 RFC8305 Happy Eyeballs v2.0 的設計架構、運行狀況、及未來計畫。

2. NAT64/464XLAT Deployment Guidelines in Operator and Enterprise Networks

以下是有關〝NAT64/464XLAT Deployment Guidelines in Operator and Enterprise Networks〞草案，目前的狀況資訊。本草案的內容為描述如何在 IPv6 網路佈署 NAT64 和 464XLAT 的方式，不論是行動網路服務商、寬頻網路服務商還是企業內部的網路，當透過純 IPv6 的連結進入網路系統時，都需要考慮以下的問題：

- DNS64
- 使用 IPv4 地址的應用或設備
- 非 IPv6 相容的 APIs
- 純 IPv4 的主機或應用。

此草案的目的即為解決這些議題。



3. IPv6-Ready DNS/DNSSSEC Infrastructure

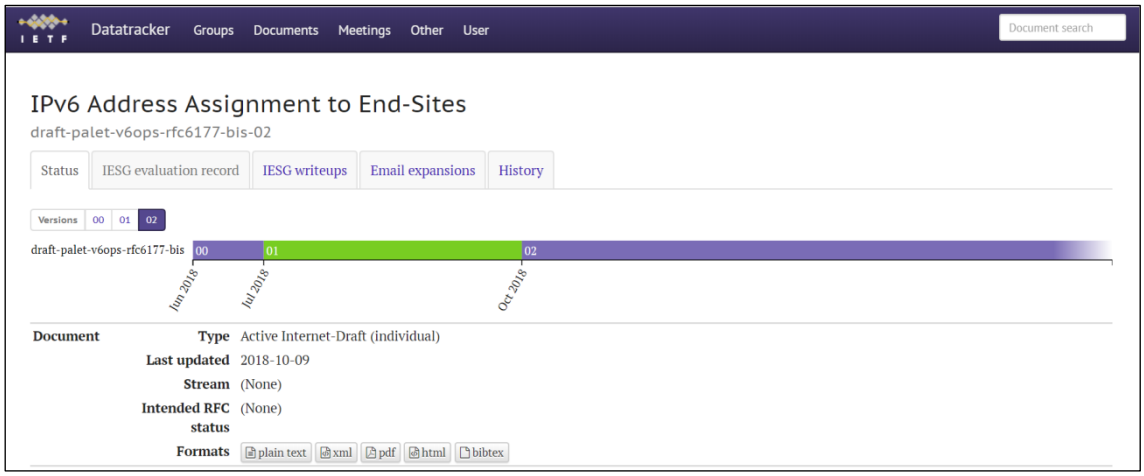
以下是有關〝IPv6-Ready DNS/DNSSSEC Infrastructure〞草案，目前的狀況資訊。本草案定義了實現全球 IPv6-Ready DNS 和 DNSSEC 基礎設施的時機，以利促進全球 IPv6-only 的佈署。為解決在某些情況下，網路系統無法彼此溝通，其關鍵問題是需要全球網路都能支持 DNSSEC 和 DNS64。這個文件說明任何 DNSSEC 簽署的資源記錄，都應該包含 IPv6 資源記錄，以做為最完整的紀錄路徑，用於解決與 DNS64 和 DNSSEC 任何佈建的衝突。

4. IPv6 Address Assignment to End-Sites

以下是有關〝IPv6 Address Assignment to End-Sites〞草案，目前的狀況資訊。各個區域網路註冊管理機構（RIR），對於建議能分配給終端網站的可用位址區段的政策，有不同的看法。目前只允許最多/48，但並未對此限制加以說明理由，並清楚地說明應該如何為終端網站分配多少地址空間的確切選擇方式，而是由每個網路服務業者自行決定。

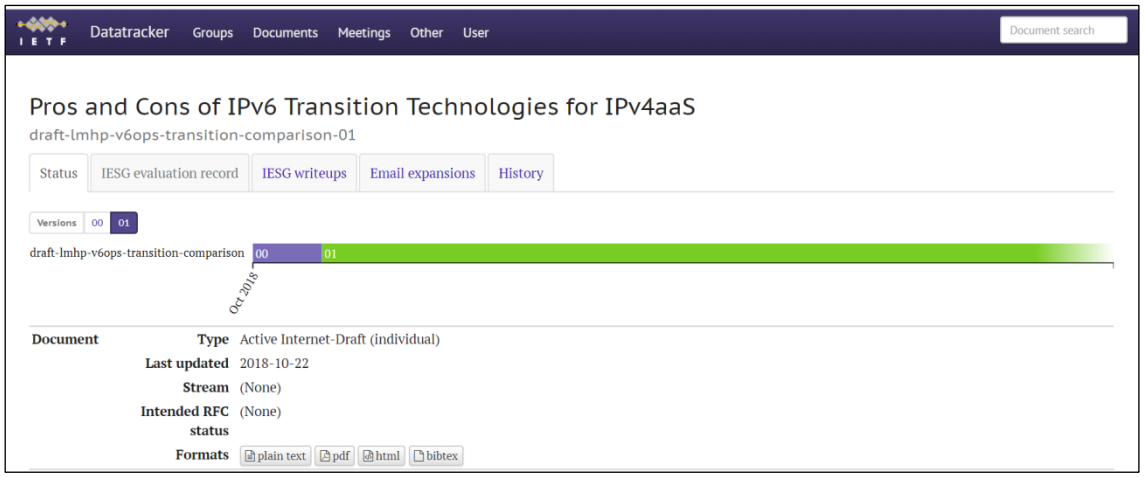
本草案依內容終端網站的架構和運作的條件，作為分配地址空間的依據，並重申各 RIR 的分配政策方針。此修訂版本特別強調 IPv6 協議演進，及因應不斷增加的子網路需求，因此分配策略不建議為單一子網站做地址分配。

此草案正式通過後將用於取代目前的 RFC6177。



5. Pros and Cons of IPv6 Transition Technologies for IPv4aaS

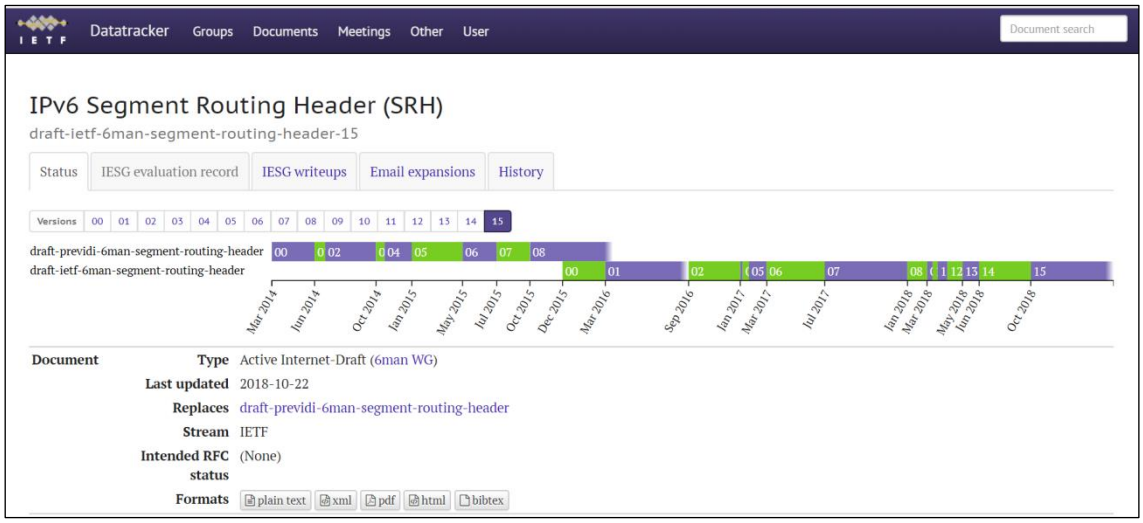
以下是有關〝Pros and Cons of IPv6 Transition Technologies for IPv4aaS〞草案，目前的狀況資訊。對於只有 IPv6 服務的網路服務業者（ISP），目前有多種 IPv6 過渡技術可供採用，以向客戶提供 IPv4 服務（IPv4aaS）。不同的技術各有其優點和缺點， 在本次的 IETF 會議中有許多討論及分析。如何選擇最適合的解決方案，大家都有共識是需根據網路服務業者（ISP）的系統架構條件和偏好。本次會議中分別分析了五 5 種最著名的 IPv4aaS 技術，以便作為網路服務業者選擇最適合的技術參考。



6. IPv6 Segment Routing Header

以下是有關〝IPv6 Segment Routing Header〞，目前的狀況資訊。新的路由擴增檔頭，可以讓區段路由（Segment Routing）被應

用於 IPv6 的資料傳送上。本內容是用於描述區段路由的擴增檔頭，及如何應用於區段路由的結點上。



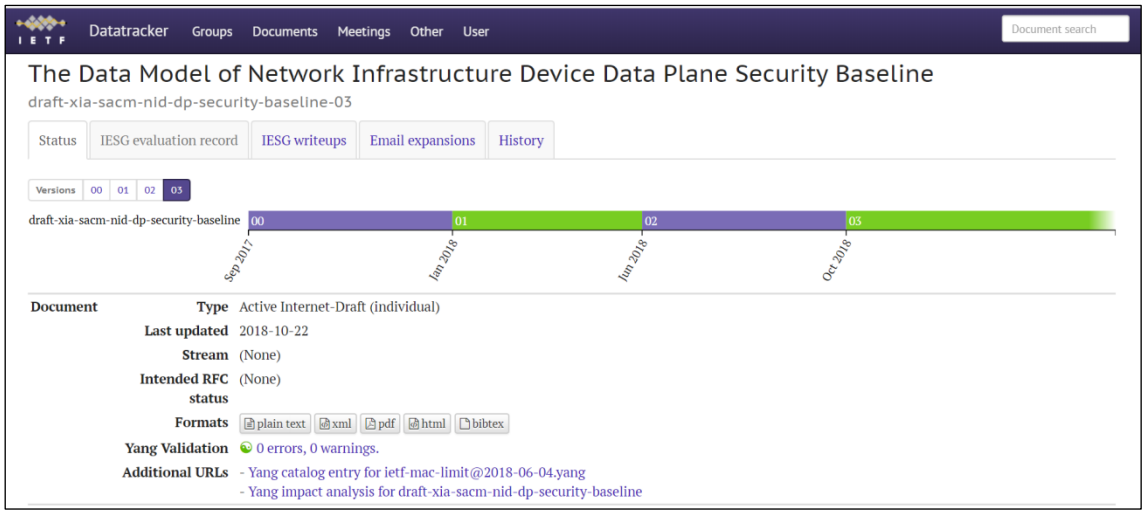
Security 相關技術討論

有關 Security 技術討論會議，會中進行的主題包含以下內容：

1. Data Model of Network Infrastructure Device Data Plane Security Baseline

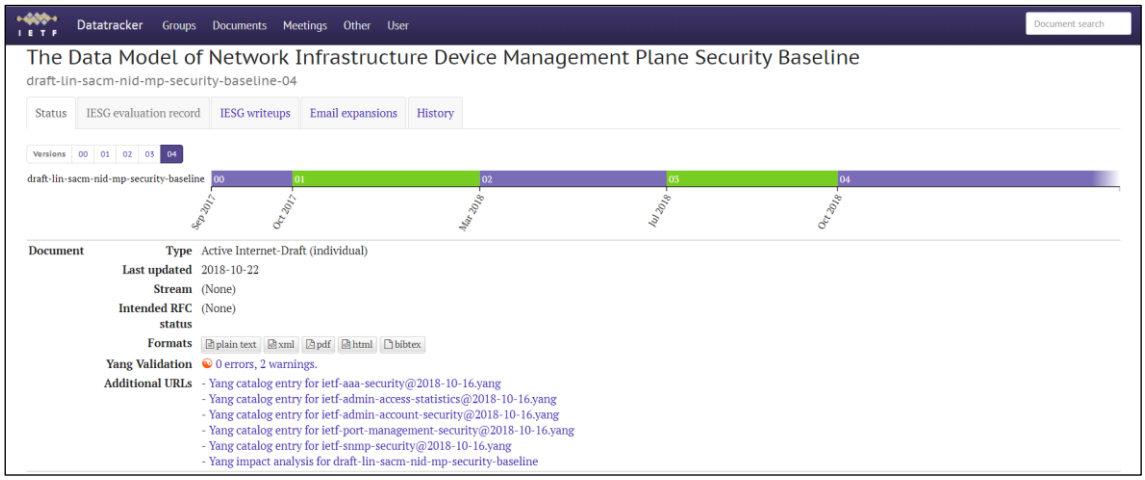
   以下是有關〝Data Model of Network Infrastructure Device Data Plane Security Baseline〞草案，目前的狀況資訊。此草案提出部份和網路安全相關的議題，有關網路基礎設備（即路由器，交換機，防火牆等）的資料安全。另外有關其他網路安全的草案，分別提列在以下 2 個草案：

   - [I-D.ietf-lin-sacm-nid-mp-security-baseline]，管理資料平面安全（Management plane security baseline）。
   - [I-D.ietf-dong-sacm-nid-infra-security-baseline]，基礎設施層安全（infrastructure layer security baseline）。



2. The Data Model of Network Infrastructure Device Management Plane Security Baseline

以下是有關〝The Data Model of Network Infrastructure Device Management Plane Security Baseline〞草案，目前的狀況資訊。本草案內容定義網路設備管理平面的安全，由 YANG 數據模型表示。此數據模型的相對設定值和狀態值可以在安全自動化和持續監控（SACM）元件之間傳輸，並可用於網路設備安全狀態評估。



IoT 相關技術討論

有關 Iot 技術討論會議，會中進行的主題包含以下內容：

1. Automated IoT Security

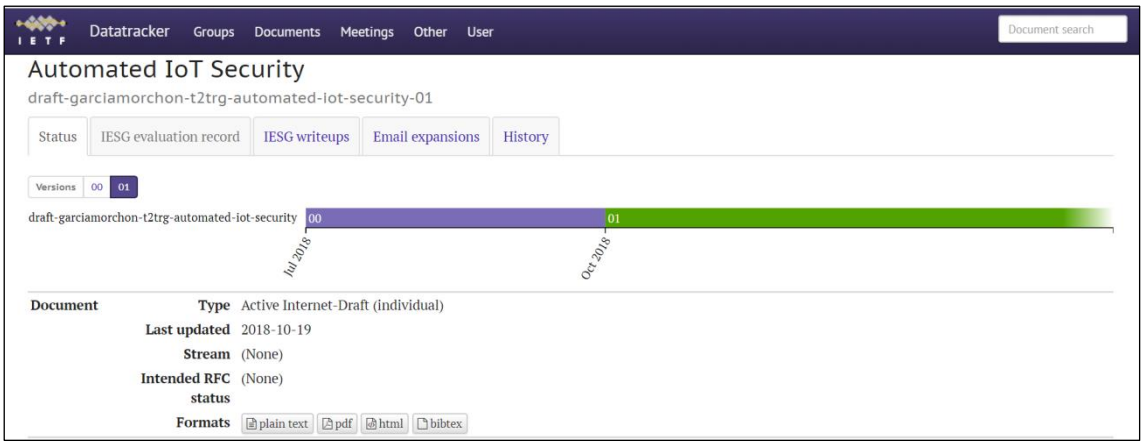
以下是有關〝Automated IoT Security〞草案，目前的狀況資訊。物聯網（IoT）概念是指使用標準網際網路協議，實現人與物（human-to-thing）及物與物（thing-to-thing）之間的溝通。因此其安全的設計需要經過廣泛的認可才能被採用，但物聯網應用和系統的設計非常複雜，因此也面臨各式各樣類型網路攻擊的威脅。

特別的是，網路攻擊的威脅不斷發展，而大多數的物聯網系統卻很少更新，但是通常物聯網系統會運作數十年，而且不會做大幅度的變動。此草案內容定義一個安全框架，用以整合既有的安全流程，如物聯網應用中對物件的生命週期的風險評估或漏洞評估等。此安全方法的核心主要是依賴於 2 個協議：

- 自動安全配置協議（PASC）。
- 自動漏洞評估協議（PAVA）。

PASC 是在物聯網系統中，當物件在網路系統中執行，PASC 負責自動執行風險評估，並做適當的設備或系統安全配置，以抵禦已識別的風險。其所分配的安全設置可以適用於設備的應用程序在特定環境和威脅模型下運作。

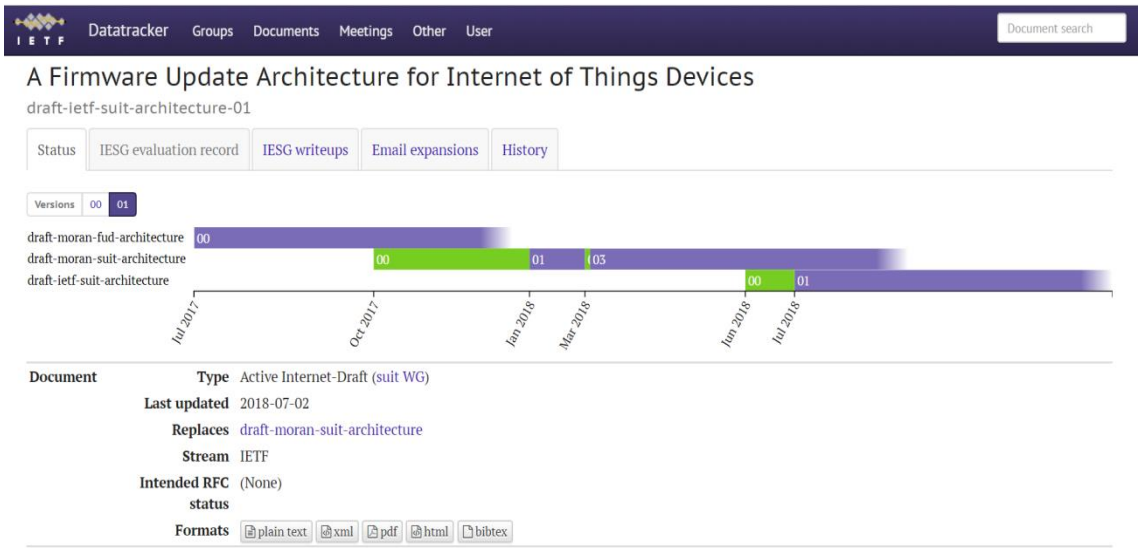
PAVA 在物聯網的物件運作期間執行，並確保以主動方式發掘物件和物聯網系統中的漏洞。此 2 個協議以透過自動化的方式，讓使用者、製造商、和網路服務業者，在安全的物聯網環境都能受益。



2. A Firmware Update Architecture for Internet of Things Devices

以下是有關〝A Firmware Update Architecture for Internet of

Things Devices〞之草案，以目前的狀況資訊相關訊息。物聯網（IoT)設備的安全漏洞所引發對資訊安全的韌體更新機制的需求全球都認知是日益增加的一種現象。安全專家建議採用此類更新機制來修復漏洞，更新設備的設定及增加新功能。本草案的內容即描述適用於物聯網設備的韌體更新機制的架構。
該架構與韌體映像（firmware images）和描述資料（meta data）的傳輸無關。此版本的內容適用於非對稱加密（asymmetric cryptography）和公鑰（public key）的基礎架構。未來版本將加入描述對稱密鑰（symmetric key）方法應用於物聯網中特定的設備。



量子網路（Quantum Internet）

本次會議 IRTF(Internet Research Task Force)的量子網路研究團隊，介紹了量子網路(Quantum Internet)的概念，發展狀況及未來計畫，量子網路聯盟(Quantum Internet Alliance)預計在西元 2020 年，於荷蘭阿姆斯特丹(Amsterdam)、萊頓(Leiden)、海牙(The Hague)、及台夫特(Delft)，佈建 4 個測試點，以作為量子網路的展示平台。
有關量子網路聯盟(Quantum Internet Alliance)相關資訊請參考網站：
http://quantum-internet.team/

Host Speaker Series

這次會議華為以主辦單位的身分，在 11/8 舉辦一場主辦單位演講，由 Chang Yue 華為的網路產品架構總監發表主題為〝Challenges of Evolution Towards Autonomous Network〞的演講。內容主要是針對網路

時代因應雲端應用的快速成長，且雲端應用越來越和大量的儲存資源及計算結合，而網路配置需要在幾秒鐘內反應，因此形成極大挑戰。網路自治為回應此一挑戰，因此必須簡化網路協定系統。

網路自治透過網路的虛擬化和軟體化將有助於將網路配置和底層資源分離，這使的網路服務佈署的速度，和計算及存儲資源的速度能相匹配。此外智慧網路能根據網路狀態的大數據應用於網路的即時診斷決策及配置更改可大大提升網路的效率。

四、 建議意見：

<u>建議事項</u>

- ☐ 建議持續關注相關各 WGs 動態及相關訊息。
- ☐ 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。
- ☐ 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。
- ☐ 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。

IETF 下一次會議將於 2019 年 3 月 23-29 日於 Prague 舉行，相關資訊請參考 https://www.ietf.org/how/meetings/104/。

五、 會議議程：

以下為 IETF 103 Bangkok 的完整議程表：

日期	時間	議程
107/11/3 (六)	8:30-22:00	IETF Hackathon
	9:30-18:00	Code Sprint
107/11/4 (日)	8:30-16:00	IETF Hackathon
	10:00-12:00	IEPG Meeting
	10:00-19:00	IETF Registration
	12:30-13:30	Tutorial: Newcomer's Overview
	12:30-13:30	Tutorial: Traffic Engineering
	13:45-14:45	Tutorial: Bringing New Work to the IETF
	13:45-14:45	Tutorial: INT Area Overview
	15:00-16:00	Newcomer's 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
107/11/5 (一)	8:00-9:00	Beverage Break
	8:00-18:00	IETF Registration
	9:00-11:00	Dispatch Joint with ARTAREA

		Human Rights Protocol Considerations
		Coding for efficient NetWork Communications Research Group
		Network Configuration
		IPv6 Operations
		Locator/ID Separation Protocol
		Routing Over Low power and Lossy networks
		Web Authorization Protocol
	11:00-11:20	Beverage and Snack Break
	11:20-12:20	Secure Telephone Identity Revisited
		Crypto Forum
		Global Routing Operations
		Pseudowire And LDP-enabled Services
		Traffic Engineering Architecture and Signaling
		Transport Area Open Meeting
	12:20-13:50	Break
	13:50-15:50	Constrained RESTful Environments
		Autonomic Networking Integrated Model and Approach
		Domain Name System Operations
		BGP Enabled ServiceS
		Path Computation Element
		Transport Layer Security
		Transport Area Working Group
	15:50-16:10	Beverage and Snack Break
	16:00-17:00	NomCom Office Hours
	16:10-18:10	OPS ADs Office Hours
	16:10-18:10	IPv6 over Networks of Resource-constrained Nodes
		IRTF Open Meeting
		Routing Area Working Group
		EAP Method Update
		Managed Incident Lightweight Exchange
		Messaging Layer Security
		TCP Maintenance and Minor Extensions
	18:30-20:00	Hackdemo Happy Hour
107/11/6 (二)	8:00-9:00	Beverage Break
	8:00-9:00	Systers' Networking Event
	8:00-18:00	IETF Registration
	9:00-11:00	Hypertext Transfer Protocol
		IPv6 over Low Power Wide-Area Networks
		Decentralized Internet Infrastructure
		Network Modeling
		Link State Routing
		Limited Additional Mechanisms for PKIX and SMIME

		Token Binding
		IP Performance Measurement
	11:00-11:20	Beverage and Snack Break
	11:20-12:20	Audio/Video Transport Core Maintenance
		Content Delivery Networks Interconnection
		IP Wireless Access in Vehicular Environments
		Operational Security Capabilities for IP Network Infrastructure (CANCELLED)
		Link State Routing
		Web Authorization Protocol
		TCP Maintenance and Minor Extensions
	12:20-13:50	Break
	12:20-13:35	RTG AD Office Hours
	13:50-15:50	Registration Protocols Extensions
		IPv6 Maintenance
		Global Access to the Internet for All
		SIDR Operations
		Multiprotocol Label Switching
		Protocols for IP Multicast
		Remote ATtestation ProcedureS
		QUIC
	15:50-16:10	Beverage and Snack Break
	16:00-17:00	NomCom Office Hours
	16:10-18:10	Network Time Protocol
		Measurement and Analysis for Protocols
		Thing-to-Thing
		MBONE Deployment
		Operations and Management Area Working Group Combined OpsAWG / OpsAREA
		Traffic Engineering Architecture and Signaling
		Security Dispatch
107/11/7 (三)	8:00-9:00	Beverage Break
	8:00-17:30	IETF Registration
	9:00-11:00	Concise Binary Object Representation Maintenance and Extensions
		DNS PRIVate Exchange (CANCELLED)
		Bit Indexed Explicit Replication
		Common Control and Measurement Plane
		Source Packet Routing in Networking
		Security Events
		Trusted Execution Environment Provisioning
		QUIC
	11:00-11:20	Beverage and Snack Break
	11:20-12:20	Light-Weight Implementation Guidance
		Network Management
		Multiprotocol Label Switching

		Transport Layer Security
		Transport Area Working Group
	12:20-13:50	Break
	12:35-13:35	WG Chairs Forum (For WG Chairs Only)
	13:50-15:20	JSON Mail Access Protocol
		WGs Using GitHub
		Home Networking
		Path Aware Networking RG
		Network Virtualization Overlays
		IP Security Maintenance and Extensions
	15:00-16:00	NomCom Office Hours
	15:20-15:40	Beverage Break
	15:40-17:10	Internet Area Working Group
		Privacy Enhancements and Assessments Proposed Research Group
		Babel routing protocol
		Routing In Fat Trees
		Interface to Network Security Functions
		Transport Services
	17:10-17:30	Beverage and Snack Break
	17:10-17:30	IAOC / LLC Office Hours
	17:30-20:00	IETF Plenary
107/11/8 (四)	8:00-9:00	Beverage Break
	8:00-9:00	Newcomers Feedback Session
	8:00-17:00	IETF Registration
	9:00-11:00	Hypertext Transfer Protocol
		Information-Centric Networking
		Benchmarking Methodology
		Routing Area Working Group
		DDoS Open Threat Signaling
		Software Updates for Internet of Things
		Delay/Disruption Tolerant Networking
	11:00-11:20	Beverage and Snack Break
	11:20-12:20	Captive Portal Interaction (CANCELLED)
		Constrained RESTful Environments
		Session Initiation Protocol Core
		Quantum Internet Proposed Research Group
		Bit Indexed Explicit Replication
		Mobile Ad-hoc Networks
		Messaging Layer Security
		RTP Media Congestion Avoidance Techniques
	12:20-13:50	Break
	12:20-13:50	Systers Lunch
	12:45-13:30	Host Speaker Series Challenges of Evolution Towards Autonomous

		Network
	13:50-15:50	TSV AD Office Hours
	13:50-15:50	Email mailstore and eXtensions To Revise or Amend
		Multiparty Multimedia Session Control
		Distributed Mobility Management
		Extensions for Scalable DNS Service Discovery
		Deterministic Networking
		Link State Vector Routing
		Service Function Chaining
		Security Area Open Meeting
	15:50-16:10	Beverage and Snack Break
	16:00-17:00	NomCom Office Hours
	16:10-18:10	Real-Time Communication in WEB-browsers
		IPv6 over the TSCH mode of IEEE 802.15.4e
		Internet Congestion Control (CANCELLED)
		Network Modeling
		Routing Area Open Meeting
		Authentication and Authorization for Constrained Environments
		Automated Certificate Management Environment
		Security Automation and Continuous Monitoring