1100218coco

# 110 年度「下世代電信網路號碼技術研析及管理」委託研究報告

# 附件

執行單位：財團法人電信技術中心

委託機關：交　　通　　部

中華民國　110　年　12　月

本報告為研究案並不代表交通部意見

1100218coco

# 110 年度「下世代電信網路號碼技術研析及管理」委託研究報告附件

著者：林永勝、卜慶玲、卓卿敏、陳志宇、
王彥中、簡嘉儀、夏慧馨

執行單位：財團法人電信技術中心

委託機關：交　通　部

中華民國　110　年　12　月

國家圖書館出版品預行編目資料

110 年度「下世代電信網路號碼技術研析及管理」委託研究報告 /林永勝,卜慶玲,卓卿敏,陳志宇,王彥中,簡嘉儀,夏慧馨著. -- 初版. -- 臺北市 : 交通部, 民 110.12
冊 ; 公分
ISBN 978-986-531-354-8(全套 : 平裝)

1.通訊工程 2.技術發展

448.73 110020588

著　　者：林永勝、卜慶玲、卓卿敏、陳志宇、王彥中、簡嘉儀、夏慧馨
出版機關：交通部
地　　址：10052 臺北市仁愛路一段 50 號
網　　址：http://www.motc.gov.tw
電　　話：(02)2349-2900
出版年月：中華民國 110 年 12 月
印 刷 者：大手印企業有限公司
版(刷)次冊數：初版一刷 30 冊
定　　價： 1200 元
本書同時登載於交通部網站
展售處：五南文化廣場 40042 臺中市中區中山路 6 號
電話: (04) 2226-0330 轉 10 或 28
http://www.wuan.com.tw
國家書店松江門市 10485 臺北市松江路 209 號 1 樓
電話: (02) 2518-0807
國家網路書店: http://www.govbooks.com.tw

GPN：1011002098
ISBN：978-986-531-354-8
著作財產權人：交通部
本著作保留所有權利，欲利用本著作全部或部分內容者，須徵求著作財產權人書面同意或授權。

# 交通部郵電司委託研究計畫出版品摘要表

<table>
<tr><td colspan="3">出版品名稱：110 年度「下世代電信網路號碼技術研析及管理」委託研究報告</td></tr>
<tr><td>國際標準書號(或叢刊書)</td><td>政府出版品統一編號</td><td>計畫編號</td></tr>
<tr><td>978-986-531-354-8</td><td>1011002098</td><td>1100218coco</td></tr>
<tr><td rowspan="2">主管：王廷俊<br>聯絡電話：02-23492200<br>傳真號碼：02-23813928<br>e-mail：<br>tc_wang@motc.gov.tw<br>承辦人：林姝宜<br>聯絡電話：02-23492181<br>傳真號碼：02-23813928<br>e-mail：sy_lin@motc.gov.tw</td><td rowspan="2">研究單位：財團法人電信技術中心<br>計畫主持人：林永勝<br>聯絡電話：02-8953-5971<br>傳真號碼：02-8953-5655<br>e-mail：BillLin@ttc.org.tw<br>研究人員：林永勝、卜慶玲、卓卿敏、陳志宇、王彥中、簡嘉儀、夏慧馨<br>通信地址：新北市板橋區遠東路 1 號 3 樓 B 室<br>聯絡電話：02-8953-5600</td><td>其他參與合作之研究團隊<br>無<br>研究期間<br>自 110.03<br>至 110.12<br>研究經費<br>壹仟參佰柒拾伍萬陸仟壹佰零貳元整</td></tr>
<tr><td colspan="3">關鍵詞：電信網路號碼、編碼技術、編碼標準、5G 物聯網、DNS 編碼</td></tr>
<tr><td colspan="3">摘要：<br>隨著 5G 時代來臨，物聯網、網路切片等新興應用服務快速發展，惟目前電信產業採用之 E.164、E.212 等電信編碼原則沿用已久，對應下世代嶄新的電信環境，在技術及管理上應有全面檢視之必要。本計畫核心架構係以國際 5G 前瞻技術趨勢及資通訊安全之政策走向，致力於 5G 網路切片技術之專網編碼系統與場域平臺之開發、建置與維運之整合性服務，並開發網域名稱系統(Domain Name System, DNS)與 5G 網路切片技術融合、跨場域編碼互通相關研究彙整成最終成果。本計畫研究報告書以四個分項架構進行撰寫。<br>分項一「下世代電信網路號碼技術及政策」部分，為超前部署下世代電信編碼技術與標準，報告盤點電信網路號碼資源 E.164、E.212、IPv6 及新創技術區段路由（Segment Routing IPv6, SRv6）之發展，與其他國家之號碼管理或應用情形，並研析物聯網編碼及新型態網路編碼的演進情形，以觀測下世代電信網路號碼技術及電信號碼未來之發展趨勢。<br>分項二「下世代電信網路號碼資安稽核」部分，透過研析歐盟網路與資訊安全指令、新加坡網路安全策略、美國網路安全框架等網路安全政策與法規，爬梳國際指標性國家在國家網路安全總體政策脈絡與資安體制之發展，以及未來網路的資安防護措施，並產出號碼管理資安稽核框架。<br>分項三「下世代電信網路號碼驗證機制」部分，以驗證 5G 專網環境，開發 DNS 編碼系統。</td></tr>
</table>

物聯網設備可透過 5G 核心網路進行認證，同時配發 IPv4 及 IPv6，並完成在同域或跨域之不同基站間移動測試，以利使用管理平臺儲存、管理及提供查詢相關 DNS 自動編碼的歷史軌跡資料。

分項四「下世代電信網路號碼人才培育」之目標為培養參與相關國際標準制訂工作及可擔任該等組織重要幹部之專業人才，以確保我國在資通訊領域的國際空間及影響力。

透過上述本計畫研究結論，綜整出以下政策建議。首先在下世代電信網路號碼技術及政策部分，建議號碼政策應以技術中立原則，依服務需求進行號碼之分配管理。而在下世代電信網路資安稽核部分，建議宜在我國資通安全管理法及其子法之法制體系下，建立利害關係人之風險溝通框架，以落實資安及國安之願景目標。另外不同於傳統公眾電信網路通用之 E.164 及 E.212 編碼，主要應用於人與人之通訊與識別，在下世代電信網路環境將會有人與物或物與物之通訊與識別情境，因此本計畫提出下世代電信網路號碼驗證機制，目的為提供使用者對物聯網裝置易於直覺式辨識及管理之編碼解決方案，以因應 5G 時代更加多元的 IoT 應用場景，並增加更多對移動性 IoT 設備之需求。本研究下世代電信網路號碼技術在國際實屬前瞻技術議題，為使我國掌握全球最新技術發展趨勢及確保在資通訊領域的國際空間，本計畫提出以四年為基準之人才培育短、中、長期參與策略與效益，透過參與國際相關組織會議，及強化與國際該等社群互動交流等策略，並加強所需之政策專業知能，以累積國際影響力及爭取擔任國際組織之幹部。

| 出版日期 | 頁數 | 定價 | 本出版品取得方式 |
|---|---|---|---|
| 110 年<br>12 月 | 1030 | 1200 | 凡屬機密性出版品均不對外公開，普通性出版品；公營、公益機關團體及學校，由本部依業務性質函送參考，其他需要者可函洽本部免費贈閱，或逕進入 www.motc.gov.tw 之出版品項下下載。 |

機密等級：

☐限閱☐密☐機密☐極機密☐絕對機密

(解密【限】條件：☐　年　月　日解密，☐公布後解密，☐附件抽存後解密，
☐工作完成或會議終了時解密，☐另行檢討後辦理解密)

☑普通

備註：本研究之結論與建議不代表交通部之意見

# 目次

附件一、110 年度「下世代電信網路號碼技術研析及管理」委託研究計畫期末審查會議簡報.....1

附件二、ICANN72 會議發表交通部計畫研究成果“PoC of DNS identifier”（「DNS 識別碼概念性驗證」）.....21

附件三、產學研者深度訪談規劃及紀錄 .....64

附件四、下世代電信網路號碼技術研析及管理資安稽核證照 .....84

附件五、下世代電信網路號碼驗證機制測試計畫暨測試報告書 .....89

附件六、下世代電信網路號碼我國參與國際組織之策略及效益 ....216

附件七、人才培育成果報告 .....228

# 附件一、110 年度「下世代電信網路號碼技術研析及管理」委託研究計畫期末審查會議簡報

# 壹、期末審查會議簡報

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER
110年度「下世代電信網路號碼技術研析及管理」委託研究計畫
-期末審查會議-
110年11月23日
版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

簡報大綱
一 研究目的與架構
二 分項一：下世代電信網路號碼技術及政策研析
三 分項二：下世代電信網路號碼資安稽核研究
四 分項三：下世代電信網路號碼驗證機制
五 分項四：下世代電信網路號碼人才培育
六 政策建議及結論
七 附件

# 研究目的與架構

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

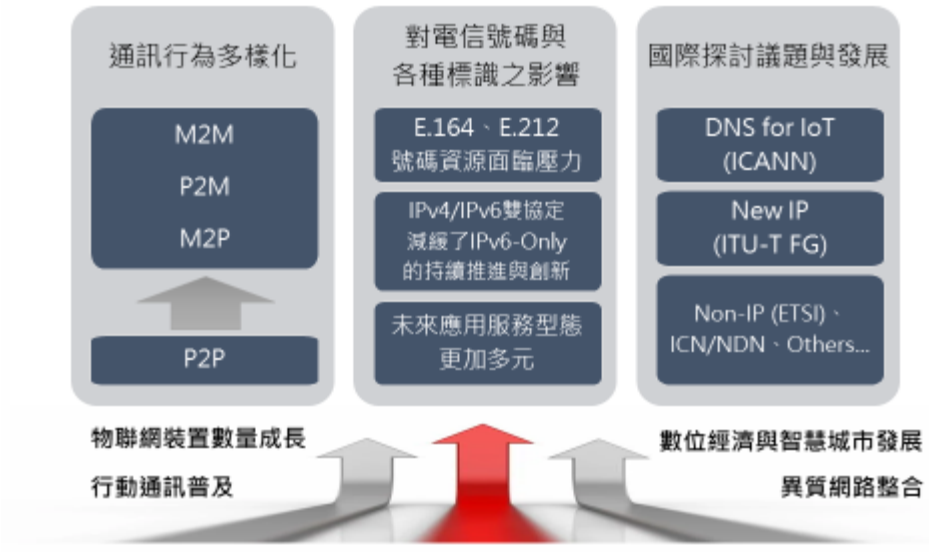
# 分項一
# 下世代電信網路號碼技術及政策研析

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.



## 下世代電信網路號碼技術背景與未來應用趨勢

■ 物聯網技術及應用的發展，將加速電信號碼與各種標識之匯流




版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

分項一

## 引導號碼與標識資源有效使用，方能助力物聯網及資料創新應用

| | 傳統關注重點 | 未來發展趨勢 |
|---|---|---|
| 電信層 | 安全、可靠、互通性 | • 更多的跨境服務（物聯網、低軌衛星上網）<br>• 隱私保護、資料在地化等治理議題 |
| 應用層 | 唯一識別性、存取權限管理 | 人與物、物與物的關係和關聯性 |

| | 優點 | 缺點 |
|---|---|---|
| 電信層 (E.164) | • 高度穩定性與可靠性<br>• 可全球互通 | • 電信號碼變更或擴充導致的行政成本高昂<br>• 屬國家資源，監管力道較高 |
| 應用層 (IP/DN) | • 高使用彈性及可擴充性<br>• 相對較低的監管程度 | • 需要DNS標識解析服務<br>• 易受資安攻擊，較高的資安風險 |

■ 跨境服務監管：以Starlink落地後使用IP/DN為例

**政策原則**

1. 使用我國IP(TWNIC)
2. 合作形態核備
3. 合作需經主管機關許可
4. 通訊監察
5. 資料在地化
6. 使用者實名制，包括外國人攜帶自有設備之入境申報與短暫使用規定等

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

6

分項一

## 超前部署下世代電信編碼技術與應用標準

■ 掌握電信網路號碼機制及網際網路主要標識與通訊協定相關之國際標準形成機制；主要包括ITU-T、IETF等組織運作與標準產生程序。

■ 各類標識皆有其特定用途，為能充分達到互聯互通，**標識解析(Identity Resolution)**將成為關鍵核心要素。

■ IPv4/IPv6雙協定僅為過渡機制，既無法充分發揮IPv6引領作用，且易受限於IPv4既存缺陷，故應更積極參與及持續觀測IETF等標準組織於**IPv6為基礎之上的通訊協定及創新應用研究**。

**E.164號碼**
- 維持使用於語音通話、簡訊收發等基礎電信服務（用戶識別）

**E.212號碼**
- 維持使用於UE接取網路的驗證、授權和帳務（設備識別）

**IP位址**
- IPv6協定加速過渡（替代IPv4/IPv6雙協定），更廣泛地使用於包括5G、Internet、物聯網裝置等所有連網設備（設備識別）

**網域名稱**
- 通用頂級域名 (gTLDs) 具備全球辨識性（無地域限制）
- DNS作為Internet重要基礎設施之一，持續修定運作及提升安全性仍是研究重點。

**物聯網標識之互通性**
- 須能提供連網物件的定址和識別等功能，並能在各種通訊協定間進行轉換，來達到資訊存取與傳遞的目的。
- DN, DOA/DOI, OID, NDN

IETF 5G 重要技術標準

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

8

# 「公眾電信網路號碼計畫」之調整建議

## ■ 公眾電信網路號碼計畫宜朝簡化、鬆綁、放寬等方向積極檢討

- 因應新興通訊技術或物聯網應用發展，應著眼於具體服務需求，來決定是否需在公眾電信網路號碼計畫中編定特別號碼區塊。
  例如：該項服務是否有提供語音功能的跨網互通性需求。
- 於現行號碼計畫中，0x0字頭號碼區塊之回收重整，建議應予優先考量，以儲備作未來之用。

**現況**

全區電信服務接取號碼(OAB)指配表

| 第 / 第 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | | 國際電話接取碼 | | | 國際電話接取碼 | 國際電話接取碼 | 國際電話接取碼 | 國際電話行動電話接取碼 | 國際電話接取碼 |
| 1 | VPS遠機專用網路服務 | | | | | 國際電話接取碼 | 國際電話接取碼 | 國際電話接取碼 | | 國際電話接取碼 |
| 2 | PBS短訊費率服務 | | 臺北市、新北市、基隆市 | | | 臺北市、新北市、基隆市 | | | | |
| 3 | CTS信用式電話服務 | | 桃園市 | | | 新竹縣市 | | 福建縣 | 花蓮縣 | 宜蘭縣 |
| 4 | 無線電話服務 | | 臺中市 | | | | | 彰化縣 | | 南投縣 |
| 5 | NKS一般費率服務 | | 嘉義縣市 | | | 雲林縣 | | | | |
| 6 | 智慧遠機碼服務(備用) | | 臺南市 | | | 臺南市 | | | | 澎湖縣 |
| 7 | ITS網路電話服務 | | 高雄市 | | | | | | | |
| 8 | PPS交通市行動服務 | 行動通信服務(備用) | 金門馬祖 | 馬祖 | 屏東縣 | 行動通信 | | 屏東縣 | | 臺東縣 |
| 9 | 行動通信服務 | | | | | | 衛星通信服務 | 行動通信服務 | | PPS個人號碼 |

**未來建議**

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 尚未核配，保留中 | 接取碼 | | | | | | | |
| 1 | 回收重整 | | | | | | | | | |
| 2 | | | 地理號碼 北部縣市 | | | | | | | |
| 3 | | | | | | | | | | |
| 4 | 物聯網 | | 地理號碼 中部縣市 | | | | | | | |
| 5 | 回收重整 | | | | | | | | | |
| 6 | | | 地理號碼 南部、東部縣市及離島 | | | | | | | |
| 7 | 網路電話 | | | | | | | | | |
| 8 | | | 地理號碼 | | | | | 地理號碼 | | |
| 9 | 非地理號碼 (行動、衛星、ecall) | | | | | | | | | |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.





# 電信編碼政策發展方向及策略

## ■ 經參考其他部會實務作法，建議成立專案小組並邀集領域專家共同參與編撰政策藍皮書。

| 章節安排 | 撰寫內容方向建議 |
|---|---|
| 第壹章 緒論 | • 我國電信號碼機制現況分析、當前挑戰與因應，以及未來願景之探究。 |
| 第貳章 現況分析 | • 公眾電信網路號碼計畫整備，包括：檢討現行各類智慧虛擬碼之存廢或整併，040及070字頭號碼於物聯網使用之區別，對Robocall使用地理性號碼（市話號碼）、手機號碼或智慧虛擬碼之限制或規定等。 |
| 第參章 議題探討 | • 資料在地化及跨境傳輸議題之探討。 |
| 第肆章 政策方向 | • 自廣泛的文獻探討及專家意見收攏聚焦出技術演進、標準制定及電信網路號碼資源編配管理相關組織之參與策略及其重要性。 |
| 第伍章 執行策略 | • 透過盤點技術缺口、科研投入、人才培育等系列舉措之規劃與執行，重點強化與ICANN、IETF等全球網際網路組織之連結，緊密跟隨國際IPv6+技術發展趨勢，俾為我國在電信網路領域積極布局、爭取更多的國際空間。 |
| 第陸章 結論建議 | |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 分項二
# 下世代電信網路號碼資安稽核研究

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.




## 國際網路安全政策與法規

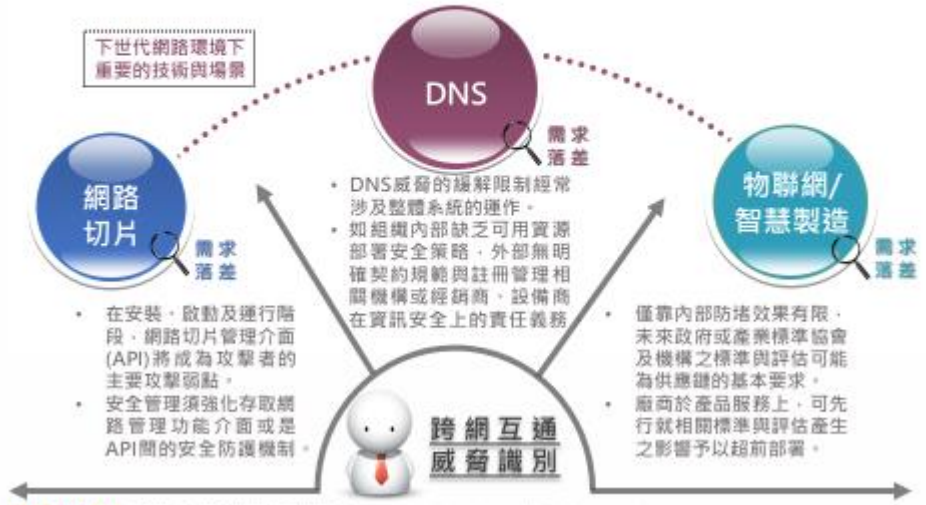
■ 觀測國際主要國家(美國、歐盟、新加坡)之網路安全策略走向，及網路安全體系發展重點，綜整分析**目前各國普遍重視供應鏈安全(ICT、物聯網)，並強化利害關係人情資共享機制。**

| 國家 | 主責機關 | | 網路安全策略走向 |
|---|---|---|---|
| 歐盟 | 策略 | 執委會(EC) | • 歐盟以「監管」、「投資」、「政策」為三大主軸，設立較為前瞻的資安願景；資安戰略則是以技術為導向，於資通訊科技(Information and Communications Technology, ICT)供應鏈引入更嚴格的資安規範。<br>• EC於2020年12月提出《網路與資訊系統安全指令》修正提案(Revised Directive on Security of Network and Information Systems, NIS 2 Directive)，引入更嚴格的監管措施以及更加嚴格的執法要求，例如整個歐盟的統一制裁，以及擴擴大NIS 2規管的範圍，以取代原有的NIS指令，進而加強安全要求，並進一步解決ICT供應鏈的安全問題以及同時有效要求更多部門和其他機構等採取措施，以提高歐盟的網路安全水準。 |
| | 技術標準 | 歐盟資通安全局(ENSIA) | |
| 美國 | 策略 | 網路安全暨基礎安全局(CISA) | • 美國資安防護由聯邦體系帶動民間建立資安框架，CISA作為國家級資安諮詢角色、頒布總體資安策略，再由NIST制定跨產業網路參考安全框架；伴隨技術與政策變遷，NIST已針對IPv6、DNS、物聯網安全發布系列特殊文件(SP)，2020年提出網路資源「零信任原則」，所有授權均須經過評估，注重內部網路的資料保護。<br>• 美國電機電子工程師學會(IEEE)參考NIST網路安全框架CSF1.1的架構設計，於2017年出版《域名系統安全管理》(DNS Security Management)，提出適用DNS之框架核心「DNS網路安全框架核心」(Cybersecurity Framework Core DNS Example)。 |
| | 技術標準 | 國家標準技術研究所(NIST) | |
| 新加坡 | 策略 | 網路安全局(CSA) | • 新加坡以邁向更安全網路空間為願景，制定三個長期願景之目標：一是「持續更新網路安全策略」、二是「建立彈性資訊關鍵基礎設施」、三是「發展網路安全生態系統」。<br>• 新加坡資訊通信媒體發展局(IMDA)於2020年3月發布物聯網網路安全指南(Internet of Things Cyber Security Guide)，提出物聯網系統層面的安全建議，提供物聯網開發者、供應者及使用者於物聯網系統實施或營運階段的網路安全基準建議，以及提供威脅建模清單(threat modelling checklist)與供應商自我揭露清單(vendor disclosure checklist)。 |
| | 技術標準 | 資訊技術標準委員會(ITSC) | |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## 下世代網路安全需求

■ 本計畫研析5G網路切片、DNS與物聯網/智慧製造應用場景之資安威脅，以因應**組織管理、內部網路環境之資安需求與應用場景**，並強化下世代電信網路跨網互通之資安管理。




版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.





## 指引與稽核框架擬定

分項二

## 相關安全策略指引擬定

- **建立本稽核框架之目的**：落實資安意識與全民資安防護、加強我國資通訊產業技術與防護能量。
- **政府機構使用框架之目的**：用於建構跨部門、跨域資料之共通基礎，以DNS編碼管理系統作為核心，完備下世代資料治理之推動架構。
- **使用框架預期可協助政府機構**：瞭解與定義**「政府組織內部議題、外部利害關係人重視之資安議題」**之界定，以符合我國下世代電信網路號碼管理政策主軸。

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

分項二

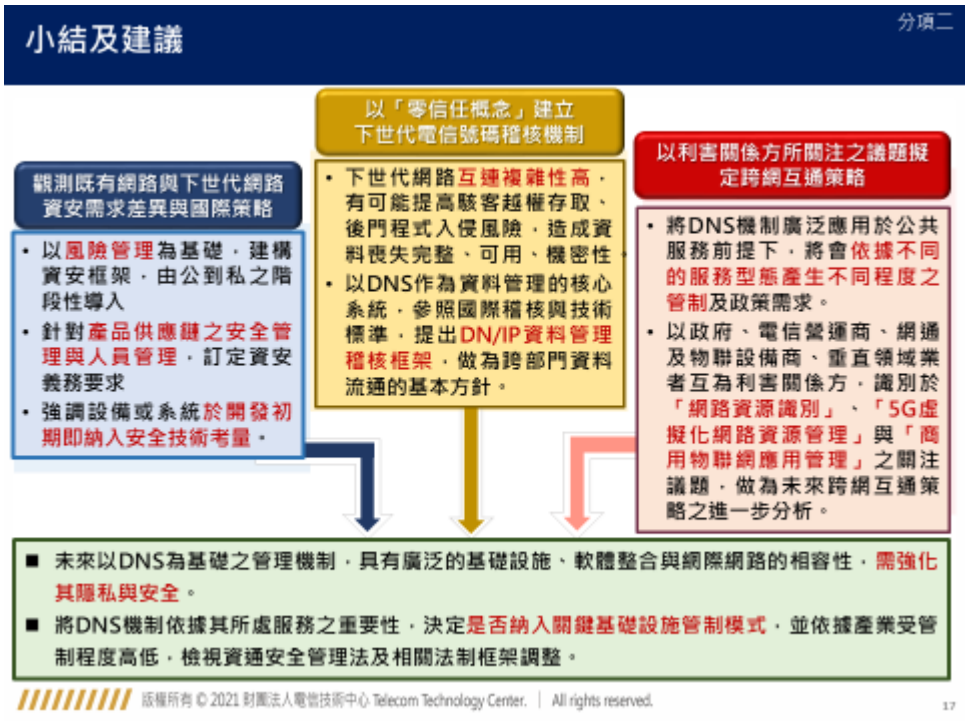
## 下世代電信號碼管理系統安全及跨網互通安全策略

- **檢視原則**：(1)針對三大議題，劃定政府機構、電信營運商、網通及物聯設備供應商、垂直領域業者為**彼此的利害關係人**。(2) 依據各利害關係人所關注之項目(或痛點)，**綜合考量組織本身對號碼管理安全需求程度**。

- 此架構可提供想要進行資安風險等級建立之組織**進行內部議題的鑑定**以及**瞭解利害關係方之外部議題**(以政府機構為例，黃色部分)，以進行風險規劃。
- 對政府機構而言，若外部利害關係方有**共通之外部議題**(灰色部分)，亦可協助其建立溝通機制。

| 需求 / 利害關係人 | 網路資源識別 | 5G虛擬化網路資源管理 | 商用物聯網應用管理 |
|---|---|---|---|
| 政府機構 | 開放資料與物聯網管理應用 | 數位基礎設施安全維護 | 設備產品是否合規 | 場域是否符合服務安全規範 |
| 電信營運商 | 電信資源分配與管理 | 服務導向商業競合考量(網路切片市場) | 設備產品安全 | 網路切片與專網之網路安全責任歸屬 |
| 網通及物聯設備供應商 | IPv6政策推廣 | 設備營運安全之責任歸屬 | 服務導向商業競合考量(OTA*市場) | 設備營運安全之責任歸屬 |
| 垂直領域業者 | 專網政策推廣 | 切片系統安全封包加密安全機密數據保護 | 設備產品與系統簡化與整合專網設備安全 | 服務導向商業競合考量(物聯應用市場) |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


小結及建議
分項二
觀測既有網路與下世代網路資安需求差異與國際策略
• 以風險管理為基礎，建構資安框架，由公到私之階段性導入
• 針對產品供應鏈之安全管理與人員管理，訂定資安義務要求
• 強調設備或系統於開發初期即納入安全技術考量。
以「零信任概念」建立下世代電信號碼稽核機制
• 下世代網路互連複雜性高，有可能提高駭客越權存取、後門程式入侵風險，造成資料喪失完整、可用、機密性。
• 以DNS作為資料管理的核心系統，參照國際稽核與技術標準，提出DN/IP資料管理稽核框架，做為跨部門資料流通的基本方針。
以利害關係方所關注之議題擬定跨網互通策略
• 將DNS機制廣泛應用於公共服務前提下，將會依據不同的服務型態產生不同程度之管制及政策需求。
• 以政府、電信營運商、網通及物聯設備商、垂直領域業者互為利害關係方，識別於「網路資源識別」、「5G虛擬化網路資源管理」與「商用物聯網應用管理」之關注議題，做為未來跨網互通策略之進一步分析。
■ 未來以DNS為基礎之管理機制，具有廣泛的基礎設施、軟體整合與網際網路的相容性，需強化其隱私與安全。
■ 將DNS機制依據其所處服務之重要性，決定是否納入關鍵基礎設施管制模式，並依據產業受管制程度高低，檢視資通安全管理法及相關法制框架調整。
版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.
17

分項三
下世代電信網路號碼驗證機制
版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.
18

## 國際標準及技術研析

- 以040為物聯網專用門號，**門號本身無法識別IoT設備特性**，參考GSMA發布之「E.164 regulatory exceptions for IoT connected services」，建議IoT管理應考量應用面及服務面，而非號碼範圍。另對應IP化電信網路環境及IoT設備數量成長趨勢，參考ICANN「5G Technology」，進行以網域名稱系統（Domain Name System, DNS）作為IoT設備自動編碼機制及管理之技術驗證。

**E.164號碼(用戶識別)**
藉由「冠碼」及「首碼」與不同電信服務對應，可辨識**地理區域**或**服務類型**。

**E.212 號碼(設備識別)**
E.212 號碼透過SIM卡與裝置結合，識別**裝置**並提供行動電話及行動寬頻服務。

**DN & IP**
命名（Naming）、定址（Addressing）與識別（Identifying）機制，是網路相互連通之基礎，得益於網路應用層的開放性，可進一步擴增號碼之功能，透過**DN命名**及**IP轉換解析機制**（即DNS系統），可強化對IoT設備之辨識性及管理性。

- 5G網路核心架構朝IP化及軟體化演進，帶動IoT應用服務蓬勃發展，IoT編碼須考量以下面向：
  1. 電信網路技術演進
  2. 大量設備及多元應用興起
  3. 設備移動情形管理
  4. 未來異質網路環境

- DNS編碼符合下世代電信網路號碼管理機制
  1. 自動化編碼及配置
  2. 直覺式辨識
  3. 設備位置追蹤管理
  4. 不同標識間的轉換、互通

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.




## DNS編碼機制

- DNS編碼機制之設計參考RFC 1034「Domain names – concepts and facilities」，並依以下4點原則進行編碼管理：
  1. DNS編碼碼長限制63個字元，域名總長度則不能超過255個字元。(RFC 1123)
  2. IoT設備具唯一標示規範。(GSMA IMEI Allocation and Approval Process)
  3. 地區與地域標示。(3GPP TS 29.561)
  4. 符合5G核心網路之DNS編碼。(GSMA IR.67、3GPP TS 23.003)

- DNS編碼機制為IoT設備配發具有**唯一性**之完全限定域名（Fully Qualified Domain Name, FQDN），透過FQDN，管理者可直覺式辨識IoT設備之①**廠牌、型號**、追蹤管理IoT設備所在②**位置**及③**網路切片特性**，自動化編碼及配置以達管理之效。

| 編碼標準 | GSMA IMEI Allocation and Approval Process | 3GPP TS 29.561 | | 3GPP TS 23.003 |
|---|---|---|---|---|
| DNS編碼組成規劃 | IMEI | Cell_ID | Domain_ID | sst, MNC, MCC |
| | (設備). | .(基站). | .(地區). | <sst>.nssf.5gc.mnc(mnc).mcc(mcc).3gppnetwork.org |
| 場域編碼範例 | 355979860003363 ① | Cell_1 ② | Domain_1 ② | <sst_1>.nssf.5gc.mnc001.mcc999.3gppnetwork.org* ③ |

註：mnc01.mcc999為ITU-T標準供測試使用

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

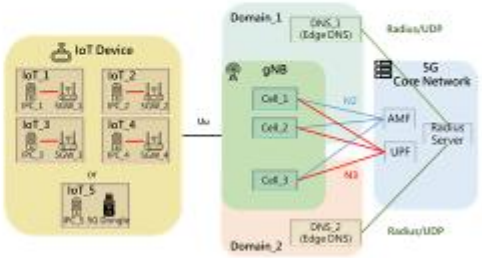
## 場域設置

■ **場域環境基本設定：**

1. 建置於封閉式專網環境
2. 支援R15標準之5G SA架構
3. 5G Wireless Network Slicing for eMBB、URLLC、MIOT

■ IoT設備以兩種方式接取5G網路：

1. 5G Gateway ：以5G Gateway作為網路連結之中介，是IoT應用廠商常用連網方式之一，例如：天候偵測器、停車位感測器。
2. 直連網路：透過5G Dongle，IoT設備可直接接取5G網路，例如：無人車（Automated Guided Vehicle, AGV）、機器人。




功能邏輯架構

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

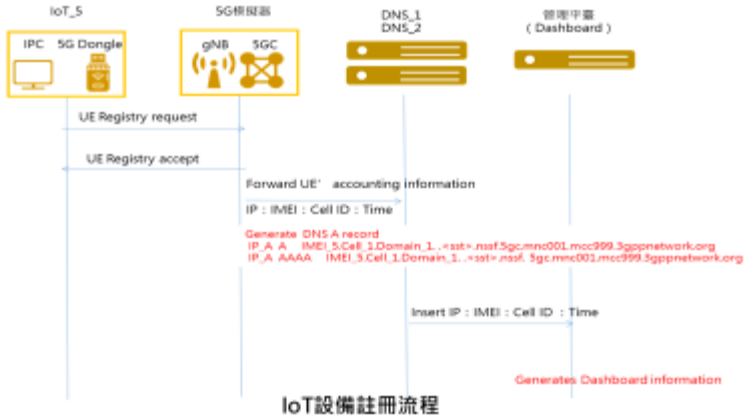




## 驗證平臺註冊流程

■ IoT設備連接5G網路後，將於5G核心網路註冊及配發IP，並在認證成功後透過Radius功能傳送UE的accounting information到DNS，依IPv4及IPv6網路為IoT設備配發A Record及AAAA Record。

■ 在IoT設備移動過程中，5G核心網路會隨時管理IoT設備的IP位址，包含動態分配與記住所分配的IP位址。




IoT設備註冊流程

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## 概念驗證(Proof of Concept, PoC)情境設計與驗證結果



■ 情境設計：以①**基本測試情境**及②**大量設備連結情境**，驗證DNS編碼機制於5G專網環境中，適用最新5G網路切片技術，動態追蹤IoT設備在同域或跨域不同基站間移動，以DNS完成自動編碼並透過Dashboard管理。

■ 基本測試情境驗證結果：提升設備動態追蹤管理效率。

■ 大量設備連結情境驗證結果：

1. 有效管理設備註冊及認證流程，自動化編碼提升IoT設備識別性。
2. 同時管理大量IoT設備。

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.



## 下階段PoS規劃



■ 延續今年PoC成果，下階段規劃在5G專網環境下之服務驗證場域（Proof of Service, PoS），以DNS編碼機制及管理平臺展示於智慧運輸系統（Intelligent Transportation System, ITS）之應用情境及服務驗證。(如智慧運輸系統管理環境、郵務物流管理系統）

智慧運輸裝置管理

郵局物流車管理及追蹤

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## 小結

1. PoC驗證成果在ICANN72「Tech Day」議程上，以線上方式發表專題演講：” PoC of DNS Identifier” ，獲得與會專家高度詢問及關注，為臺灣參與國際組織及展現資通訊應用創新能力提供良好示範。
2. 經由DNS編碼機制自動分配DNS識別碼予物聯網裝置，提供另一種適合大量物聯網環境使用的編碼方法，其直覺式辨識特性，有助於提升管理效率。
3. DNS編碼機制未來完成PoS後，預期可順利導入國內行動業者系統環境，與現行物聯網040編碼系統整合使用，提升管理彈性。

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 分項四
# 下世代電信網路號碼人才培育

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## 計畫目的與成果



■ **計畫目的：**

- 為掌握國際下世代電信網路號碼最新發展趨勢
- 促進我國5G IoT與網路切片相關產業技術與國際接軌
- 確保我國在國際資通訊領域的國際空間與影響力

■ **執行方式及成果：**

1. 建立國際鏈結：參與IETF、ICANN等國際會議及交流
2. 技術研究與自主開發：國際組織技術標準研析、座談會
3. 經驗傳承及教育訓練：經驗分享會、國際會議會前諮詢、訪談

**成果及效益**

- 人才培育
- 提出國際組織參與策略
- 強化技術能量
- 累積國際組織影響力

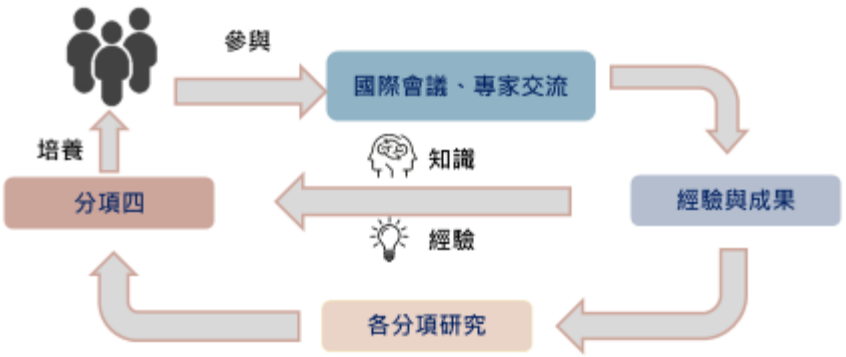
版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.



## 執行架構及流程



1. 參與ICANN、IETF及ITU國際會議，並與國際組織及成員進行交流。
2. 會議參與及交流之經驗與成果回饋予本計畫各分項研究。
3. 分析今年度參與國際組織及專家交流內容，綜整作為人才培育之策略。




版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## 人才培育成果

分項四

■ 今年參與國際相關會議及交流活動，主要獲得的經驗及成果，回饋與本計畫研究，並建議未來關注議題面向。

| | | | |
|---|---|---|---|
| 參與方式 | ICANN71<br>ICANN72<br>IROS mail | IETF111<br>IETF112<br>Guide Program | Digital World |
| 經驗及成果 | 1. 於ICANN 72 Tech Day發表「PoC of DNS identifier」<br>2. ICANN IROS建立交流管道 | 1. 鎖定IETF INT WG<br>2. 「電信網路與網際網路界接」、「DNS系統安全」等議題可作為制訂技術標依據 | 參與「未來5G網路及標準發展會議」及「未來網際網路、有線網路及無線網路發展趨勢」 |
| 回饋本研究內容 | 研析ICANN IROS及ICANN報告，如《5G Technology》、《New IP》《Non IP》、《NIS 2》及《Zero-Touch Universal IoT Device Identity》 | 1. 研析 IP技術(如NEW IP)、NDN編碼機制<br>2. 研析「物聯網設備的 DNS自動配置」標準草案 | 1. 研析低軌衛星服務及號碼議題<br>2. AI化、自動化及大量物聯網連接之技術趨勢，作為未來PoS規劃依據 |
| 未來關注議題 | 1.「歐盟網路安全原則性措施之指令草案（NIS2）」<br>2.《Zero-Touch Universal IoT Device Identity | 「電信網路與網際網路界接」、「DNS系統安全」 | 1. 5G/B5G/6G技術標準<br>2. 電信號碼編碼規範(e.164/e.212/e.214)<br>3. ITU-D、ITU-R、ITU-T參與方式 |

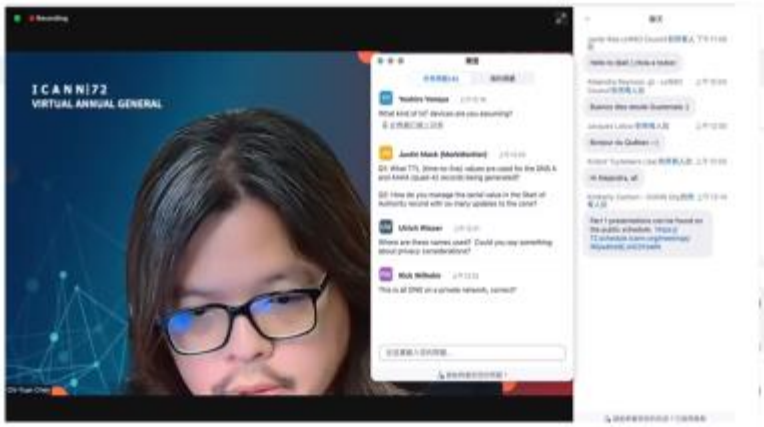
版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

29

## ICANN72「Tech Day」專題發表

分項四

■ ICANN72「Tech Day」會議上，由研究團隊成員國立宜蘭大學資工系陳麒元副教授代表，以虛擬會議發表專題演講"PoC of DNS identifier"，獲得與會專家高度詢問及關注，展現臺灣參與國際組織及資通訊應用創新能力。




版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

30

## IETF國際學者專家交流

分項四

- 研究團隊與IETF資深會員：美國加州大學洛杉磯分校(University of California, Los Angeles)的Dr. Zhang，交流與討論物聯網DNS自動生產編碼、TCP/IP及命名資料網路 (Named Data Networking, 簡稱NDN)等相關研究。

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## 經驗傳承及教育訓練

分項四

- 邀請參與國際標準組織經驗之國內專家學者及辦理國際會議會前諮詢會，培育專家學者及蒐集研提參與策略及效益。

**沈信雄顧任技正**
- 參與ICANN，應先多聽多看
- 並熟悉組織的相關規章

**黃勝雄執行長**
- 制訂RFC歷經4年
- 應長期投入資源
- 跨國或固定研究團隊
- 鎖定WG與研究議題

**吳國維前執行長**
- 討論技術應參與IETF
- 多參與ICANN會議及社群交流

**陳彥宏副教授**
- 組建官學研團隊
- 建立人才培育經驗傳承機制，強化產學合作

- **參與目標：參與**制訂技術標準(RFC)、爭取擔任國際組織幹部
- **參與策略：**
  1. 組建官學研團隊
  2. 選定具我國產業效益的技術標準議題
  3. 鎖定特定WG及研究議題
  4. 跨國、跨組織或跨單位的合作

ICANN

IETF

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## 國際組織參與策略及效益

分項四

■ 依據會議參與經驗及成果、專家學者及NII(含TWNIC)建議，除每年參與國際組織會議及活動外，提具4年期程人才培育執行策略方向及KPI。

| | | 第一年 | 第二年 | 第三年 | 第四年 |
|---|---|---|---|---|---|
| 策略方向 | | 蓄積技術能量<br>鎖定國際參與 | 提升技術能量<br>建立國際參與 | 強化技術能量<br>擴大國際參與 | 深化技術能量<br>增進國際參與 |
| 績效指標 | 人才培育 | • 人才培育成果報告≥1份 | • 培訓課程≥3場<br>• 培育課程資料≥1份 | • 培育課程≥3場<br>• IETF相關活動(研習或程式競賽)≥1場 | • 培育課程≥3場<br>• ICANN相關活動(研習或會議)≥1場 |
| | 國際合作(人員互動及國際交流) | • 國際會議成果發表≥1場(篇)<br>• 國際組織專家學者交流會議≥1場 | • 國際會議成果發表≥1場(篇)<br>• 參與國際組織社群≥2個 | • 國際會議成果發表≥1場(篇)<br>• 國際技術交流會≥1場 | • 國際技術研究成果發表≥1場(篇)<br>• 爭取擔任國際組織幹部 |
| | 研究報告 | • 人才培育參與策略報告1份 | • 國際組織及社群討論議題分析報告1份 | • 分析國際組織及社群電信網路技術討論報告1份 | • 我國資通訊領域國際參與及影響力分析報告1份 |

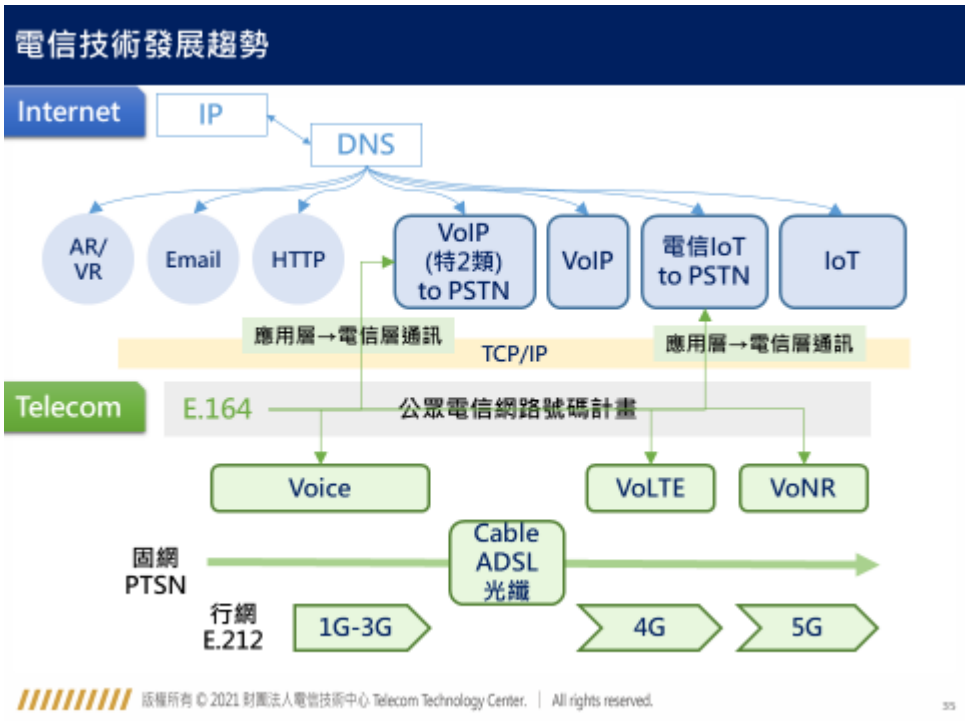
版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

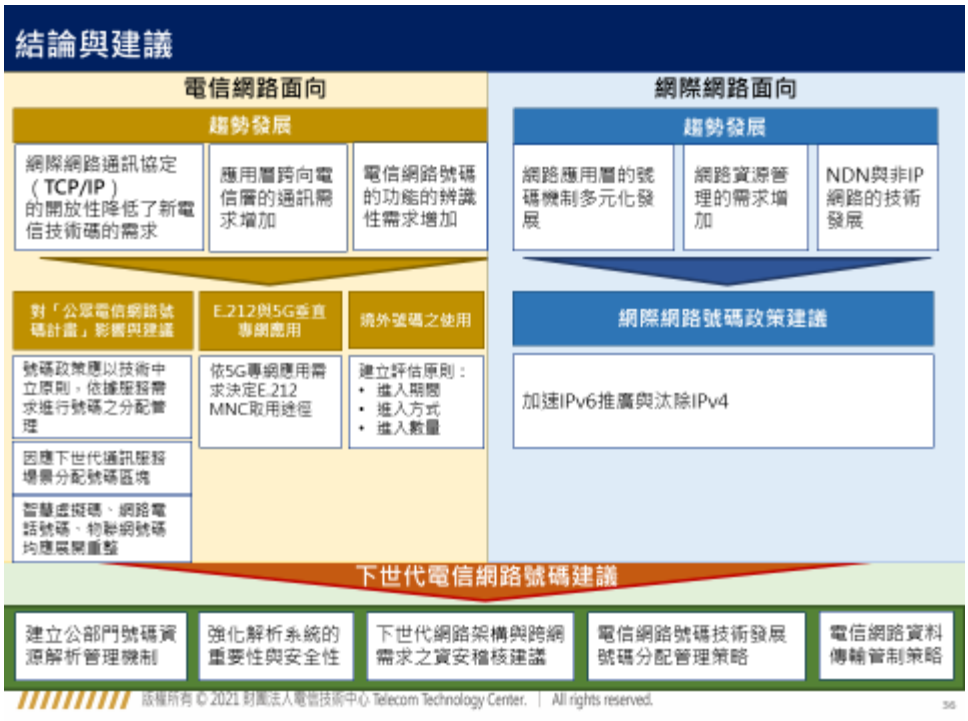
53

## 政策建議及結論

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

54


電信技術發展趨勢
Internet
IP
DNS
AR/ VR
Email
HTTP
VoIP (特2類) to PSTN
VoIP
電信IoT to PSTN
IoT
應用層→電信層通訊
TCP/IP
應用層→電信層通訊
Telecom
E.164
公眾電信網路號碼計畫
Voice
VoLTE
VoNR
固網 PTSN
Cable ADSL 光纖
行網 E.212
1G-3G
4G
5G
版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.
55


結論與建議
電信網路面向
趨勢發展
網際網路通訊協定（TCP/IP）的開放性降低了新電信技術碼的需求
應用層跨向電信層的通訊需求增加
電信網路號碼的功能的辨識性需求增加
對「公眾電信網路號碼計畫」影響與建議
E.212與5G垂直專網應用
境外號碼之使用
號碼政策應以技術中立原則，依據服務需求進行號碼之分配管理
因應下世代通訊服務場景分配號碼區塊
智慧虛擬碼、網路電話號碼、物聯網號碼均應與開重整
依5G專網應用需求決定E.212 MNC取用途徑
建立評估原則：
• 進入期間
• 進入方式
• 進入數量
網際網路面向
趨勢發展
網路應用層的號碼機制多元化發展
網路資源管理的需求增加
NDN與非IP網路的技術發展
網際網路號碼政策建議
加速IPv6推廣與汰除IPv4
下世代電信網路號碼建議
建立公部門號碼資源解析管理機制
強化解析系統的重要性與安全性
下世代網路架構與跨網需求之資安檢核建議
電信網路號碼技術發展號碼分配管理策略
電信網路資料傳輸管制策略
版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.
56

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

簡報完畢
敬請指教

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.



## 附錄-座談會討論及交流



■ **座談會辦理內容與產出成果：**為擴散國際電信號碼新知與發展，透過座談會討論交流，促進我國技術與產業能量升級，協助國內產業思考因應策略及市場布局。

| 座談會(一)：下世代電信網路號碼與物聯網編碼趨勢<br>參與人數：76位 | 座談會(二)：下世代電信號碼政策及資安機制<br>參與人數：54位 | 座談會(三)：下世代電信網路號碼研究及DNS編碼技術概念性驗證成果發表座談會<br>參與人數：66位 |
|---|---|---|
| •物聯網編碼技術面：<br>1. 目前物聯網產品、各廠商通常有自己的標識和編碼。<br>2. DNS編碼優勢：<br>✓ 電信級與非電信級物聯網都通用<br>✓ 電信網路及網際網路都有IP/DN定址<br>✓ 可快速分配與確認ID唯一性 | •資安稽核面：<br>1. 跨網互通：外網到內網仍需要縱深防禦及避免單點失效造成營運中斷。<br>2. 網路切片應有對應切片的身分驗證、切片資源分配限制、流量規則與政策。 | •政策面：<br>1. 物聯網編碼：德國開始討論5G專網的IoT聯網設備管理及編碼。<br>2. 網路切片編碼遵循3GPP國際技術標準：3GPP及GSMA標準已制定網路切片之編碼計畫，提供端到端網路切片識別之用途。 |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 附件二、ICANN72 會議發表交通部計畫研究成果“PoC of DNS identifier”（「DNS 識別碼概念性驗證」）

# 壹、財團法人電信技術中心於 ICANN72 會議發表交通部計畫研究成果(刊物發布佐證)

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

首頁 | 網站導覽 | 公開資訊 | 場地租借 | RSS訂閱 | EN

關於我們 專業服務 最新消息 採購公告 菁英招募 聯絡我們

最新消息

最新消息
- 研討會/教育訓練
- 報名查詢
- 新聞發佈
- 國內外產業通傳快訊
- 社會公益
- 活動花絮

首頁 > 最新消息 > 新聞發佈

## 財團法人電信技術中心於ICANN72會議發表交通部計畫研究成果

刊登日期： 2021-11-11 資料來源： 財團法人電信技術中心 新聞聯絡人：

分享：

財團法人電信技術中心（TTC）今年執行交通部委託研究計畫，研究團隊透過研析國際標準組織技術文件及自主開發程式後，由研究團隊成員國立宜蘭大學資工系陳麒元副教授代表，在素有網際網路聯合國美稱的ICANN72* 會議期間，於10月26日「Tech Day」進行線上專題演講，發表本計畫研究成果 "PoC of DNS identifier"（「DNS識別碼概念性驗證」）。

過去電信服務的發展係以提供人與人（P2P）溝通為主，主要為語音通話。隨著電信及網路技術進步，現代通訊由類比演進到數位化，服務內容也由語音通訊轉換到資訊交換，進而發展到下世代物聯網應用。目前公眾電信網路所適用的ITU E.164 / E.212編碼標準發展最初主要考慮應用於人與人的通訊與識別，基於「方便使用」及「易於記憶」而訂定。針對物聯網之發展及因應國內整體電信級物聯網發展需求，我國電信號碼及頻譜管理單位交通部為了在編碼技術及政策規劃上超前部署，今年委由TTC執行「下世代電信網路號碼技術研析及管理」委託研究計畫，期望推動我國編碼政策與前瞻號碼技術之發展與國際同步。

本次TTC於ICANN72會議中發表的研究成果，乃基於ICANN所發布「5G技術」（5G Technology）報告之概念，利用DNS作為物聯網識別碼進行技術概念性驗證（PoC）。在5G專網切片環境下，經由DNS識別碼機制自動分配DNS識別碼予物聯網裝置，提供另一種適合大量物聯網環境使用的編碼方法，其直覺式辨識及裝置群組分類的特性，有助於提升管理效率，為臺灣在電信網路編碼技術應用上創造新一波的國際聚焦。未來這項研究成果也可望應用在下世代5G / B5G切片下之大量物聯網場域。

此次研究成果發表獲得來自不同國家學術及網路社群等專業領域與會者的迴響，TTC期望藉由本次於ICANN72會議之發表契機，建立我國號碼技術與管理政策之國際交流管道、強化國際鏈結，並確保我國在資通訊領域的國際空間與影響力。

* 備註：ICANN為1998年10月依據美國加州法成立的非政府非營利組織，正式中文全名為「網際網路名稱與號碼指配機構」，為攸關全球網際網路順暢運作及協調管理的重要網路國際組織，主要負責監督管理網際網路技術管理功能、通訊協定參數及通訊埠之協調、DNS之管理、IP位址之分配暨指派，以及根伺服器系統之管理。為與全球網路利害關係人溝通，ICANN每年都會在全球不同地區召開三次國際大型會議。

圖1. TTC研究團隊成員於ICANN72會議發表研究成果

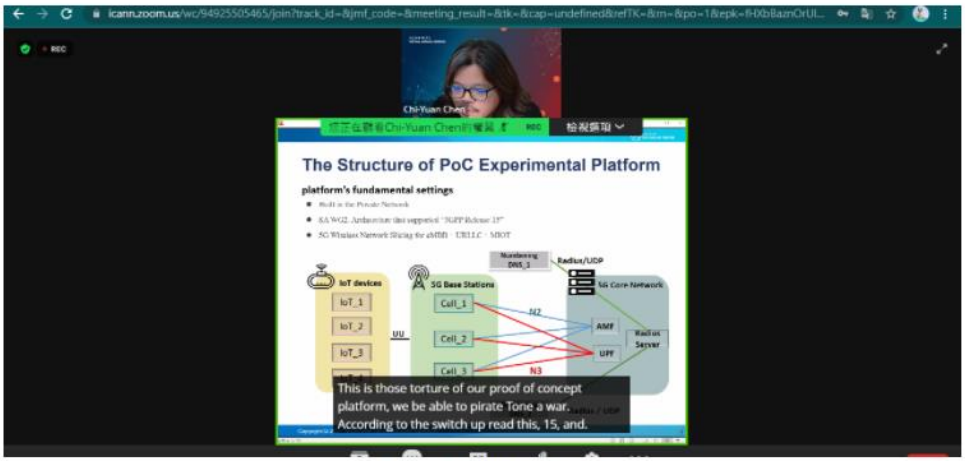



圖2. 本研究成果之概念性驗證架構

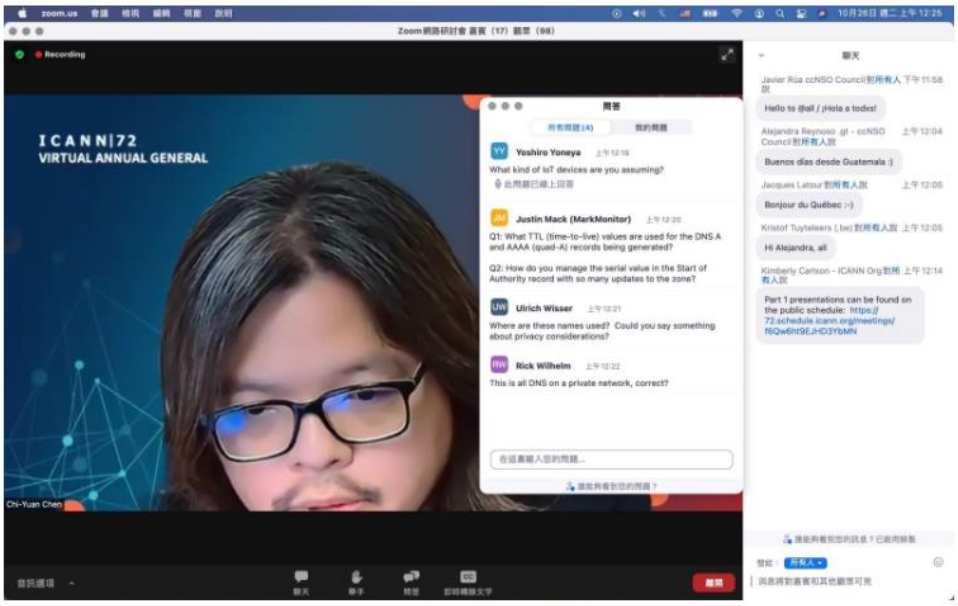
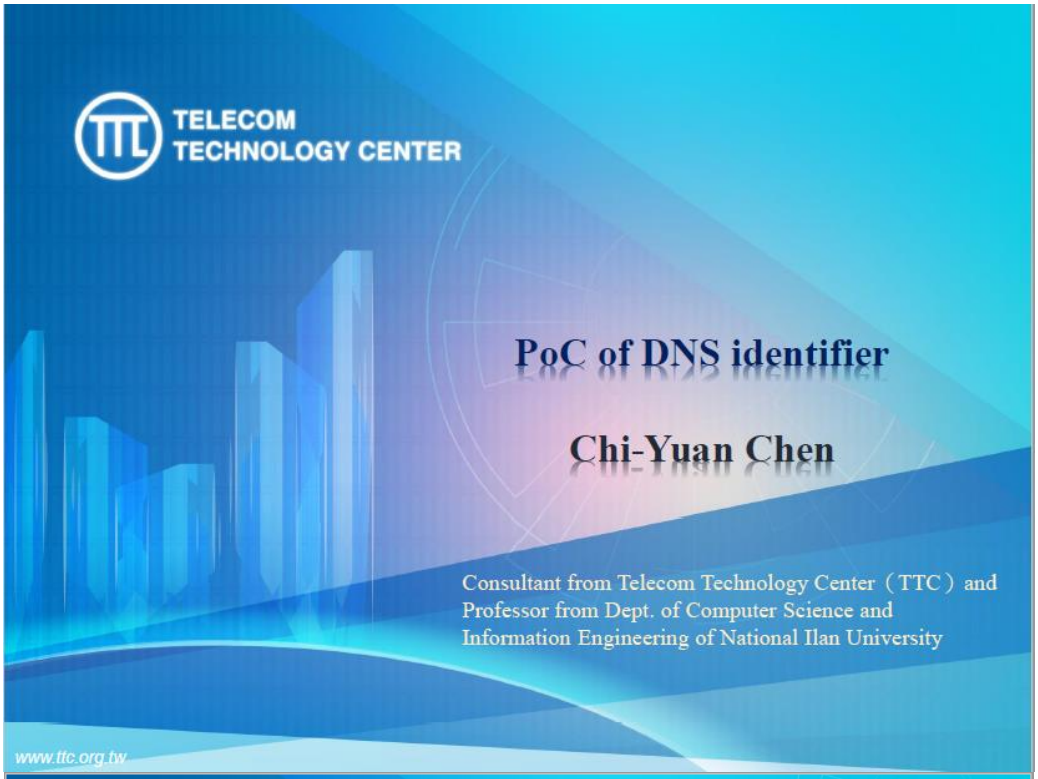
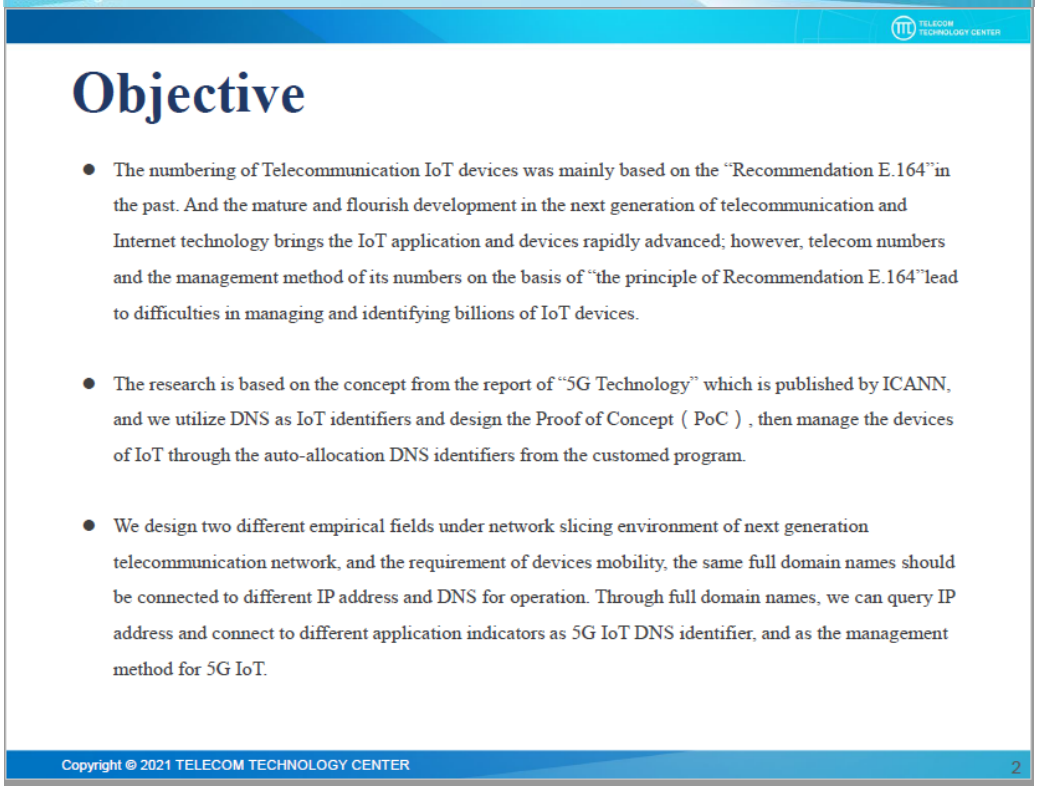



圖3. 與會專家針對發表內容即時提問

# 貳、PoC of DNS identifier”（「DNS 識別碼概念性驗證」）會議簡報



# Key innovations

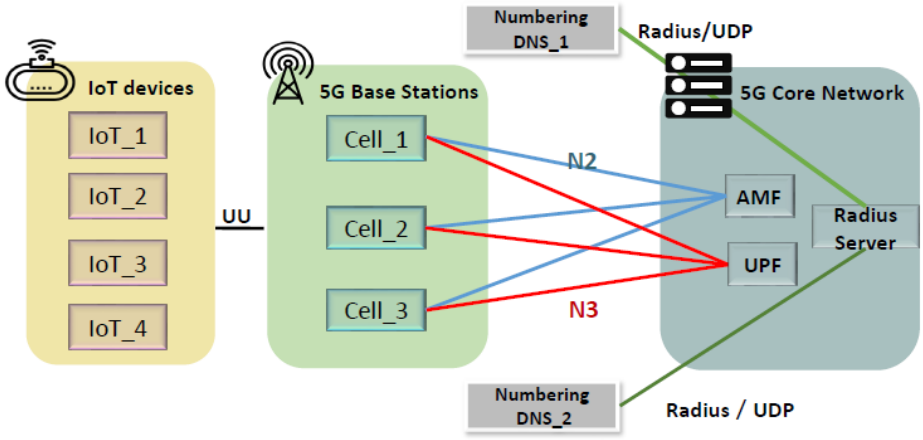
- Through the mechanism of DNS identifiers, the management of fixed and moving IoT devices under 5G is more efficient, and the IoT devices are improved their intuitive identifiability and managemental efficiency.
- In the context of 5G network slicing, Core Network（CN）sends APN, Cell ID, IMSI, MSISDN, IMEI, IP to Gn DNS to give identifiers on IoT devices according to Remote Authentication Dial-In User Service（RADIUS）

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# The Structure of PoC Experimental Platform

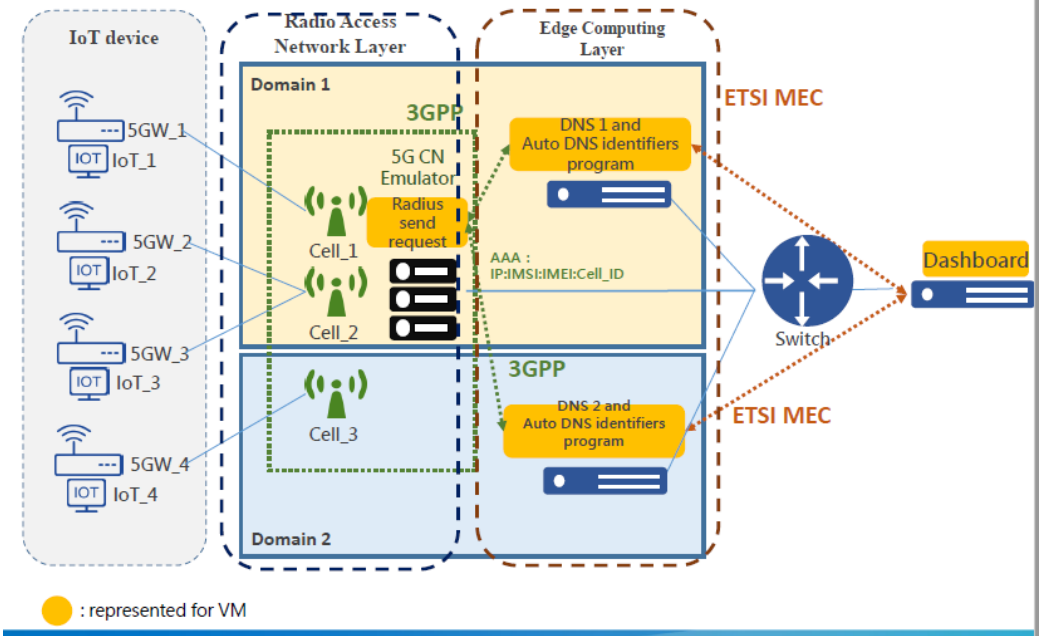
## platform's fundamental settings

- Built in the Private Network
- SA WG2. Architecture that supported "3GPP Release 15"
- 5G Wireless Network Slicing for eMBB、URLLC、MIOT




Copyright © 2021 TELECOM TECHNOLOGY CENTER

# The Structure of PoC Experimental Platform




: represented for VM

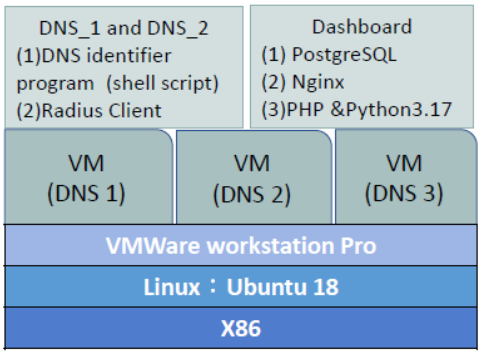
Copyright © 2021 TELECOM TECHNOLOGY CENTER


# The Structure of PoC Experimental Platform and its Equipment

PoC platform's Equipment and its Specification

| Equipment | Specification | Application |
|---|---|---|
| 5G Gateway Radio Access Network Device | DTA1164W 5G SA/NSA Gateway*4 | 5G Router with 5G SIM |
| IPC Equipment | ADLINK MXE-211-M2G*4 | Industrial Host PC in field experiment |
| 5G Simulator Equipment | Amarisoft Classic Callbox*1 | Simulator of gNB Based 5G R15 SA |
| Network Switch | Aruba 2930F-24G PoE+4SFP+ Swch*1 | Providing 5G simulator, DNS, Dashboard Network Interface |
| MEC Server | ADLINK MECS-6110*3 | Installed DNS and Dashboard System Software in field experiments |

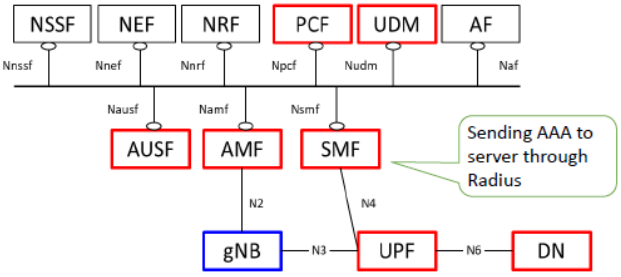
Applied Platform Structure




Copyright © 2021 TELECOM TECHNOLOGY CENTER

# The Structure of the Function Elements of 5G Simulator

With the aim of verifying PoC, we adopted 3GPP R15 based 5G simulator to imitate the standard behavior of gNB and 5GC. What interface among function elements adopted are listed below.




NSSF：Network Slice Selection Function
NEF：Network Exposure Function
NRF：Network Repository Function
PCF：Policy Control Function
UDM：Unified data management
AF：Application Function
AUSF：Authentication Server Function
AMF：Access Management Function
SMF：Session Management Function
gNB：Next Generation NodeB／Radio Access Network
UPF：User plane Function
DN：Data Network

Note: Red squares and words are the introduction of 5GC, and blue squares and words are the introduction of gNB.

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# The Initial Value of the Equipment's Parameter

| | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|
| **APN** | internet1 | internet2 | internet3 | internet4 |
| **IMEI** | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| **NSSAI** | eMBB | eMBB | URLLC | MIOT |
| **SST** | 1 | 1 | 2 | 3 |
| **Template** | AR/VR 8K Videos | AR/VR 8K Videos | Factory Automatic Machines | Smart City Sensors |
| **Throughput** | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |

Copyright © 2021 TELECOM TECHNOLOGY CENTER

# Identifier mechanism

The experimental platform referred to "3GPP TS 23.003", and the specifications of identifier proposed are below:

<IMEI>.<Cell_ID>.<Domain_ID>. <sst>.nssf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

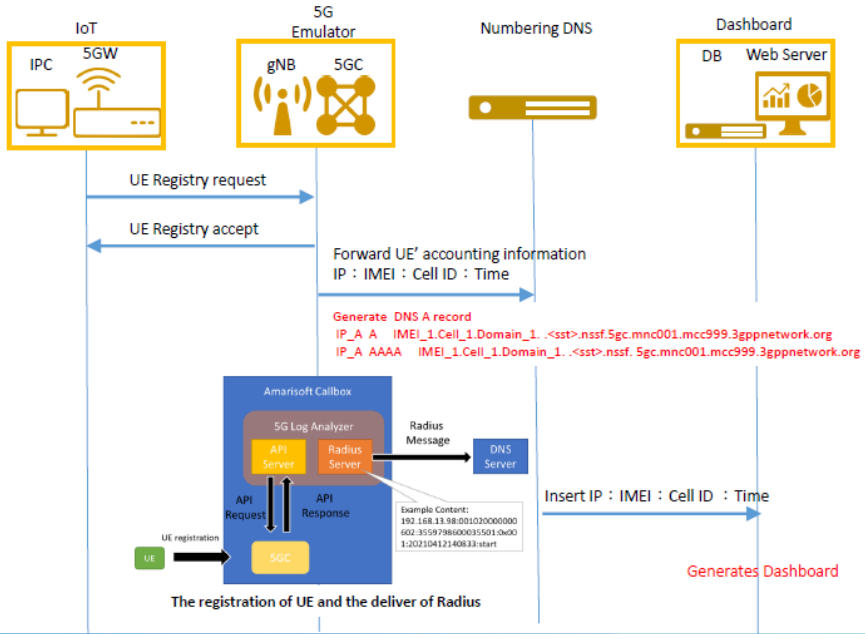
- According to "RFC952", A "name" ( Net, Host, Gateway, or Domain name ) is a text string up to 24 characters drawn from the alphabet ( A - Z ), digits ( 0 - 9 ), minus sign ( - ), and period ( . ).
- According to "RFC1123", host software MUST handle host names of up to 63 characters and SHOULD handle host names of up to 255 characters. Whenever a user inputs the identity of an Internet host, it SHOULD be possible to enter either (1) a host domain name or (2) an IP address in dotted-decimal ("#.#.#.#") form.

1. **IMEI**：Regarding the brand, model number, serial number and verification code of IoT, the numbering of IMEI device have uniqueness, which result in the uniqueness of the numbers that are generated form local host.
2. **Cell_ID**：ID of the Base Station
3. **Domain_ID**：geographical location
4. **SST**：Slice / Service Type
5. **MNC**：Mobile Network Code
6. **MCC**：Mobile Country Code

| Category | Terminal Layers of IoT | Radio Access Network Layer | Edge Computing Layer | Core Network Layer |
|---|---|---|---|---|
| Standard | GMSA TS.06 v18.2 | 3GPP TS29.061 | | 3GPP TS 23.003 |
| DNS identifier | IMEI | Cell_ID | Domain_ID | SST, MNC, MCC |
| | (equipment). | .(Cell). | .(area). | <sst>.nssf.5gc.mnc(mnc) .mcc(mcc).3gppnetwork.org |
| Example | 355979860003363 | Cell_1 | Domain_1 | <sst_1>.nssf.5gc.mnc001 .mcc999.3gppnetwork.org |

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Experimental Platform and Registration Process

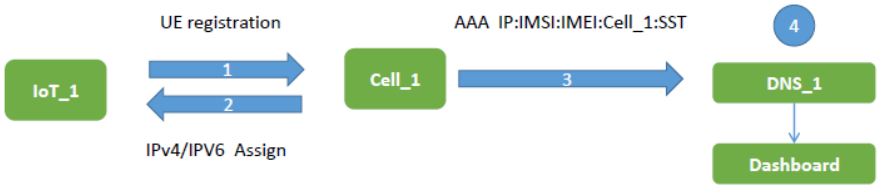



The registration of UE and the deliver of Radius

Copyright © 2021 TELECOM TECHNOLOGY CENTER

# IoT End Device Registration for the Auto DNS Identifiers

4 Generate DNS A record
IP_A A IMEI_1.Cell_1.Domain_1. <sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_1.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org



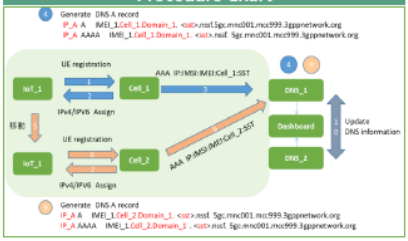

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Testing the PoC of DNS Identifiers

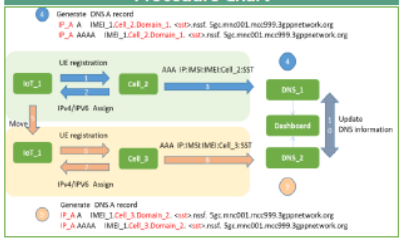
**the final result of PoC testing this year：**

1. Fixed and moving IoT devices under 5G network can be efficiently managed through DNS identifiers mechanism.
2. A huge amounts of IoT devices under 5G network will be efficiently auto-allocated numbers by the DNS identifiers mechanism.

Inter-Domain Verification Signaling Procedure Chart



Cross-Domain Verification Signaling Procedure Chart



Verification items in scenarios

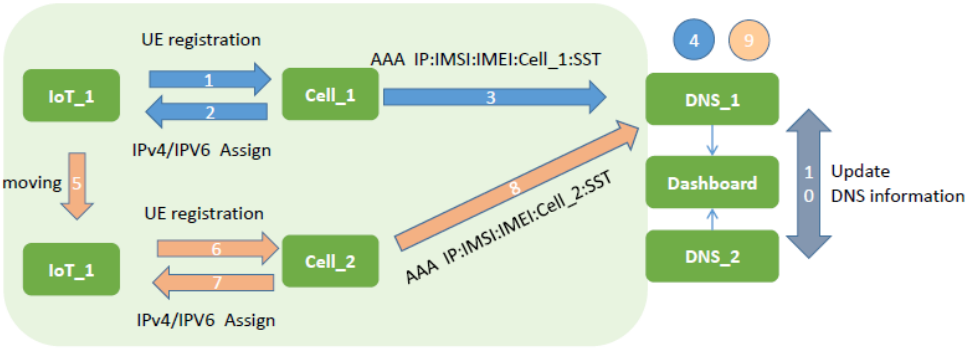
| item | Inter-Domain | Cross-Domain |
|---|---|---|
| 1 | Edge computing on data switching of MEC and DNS | Edge computing on data switching of MEC and DNS |
| 2 | Simulation of switching of IoT and DNS of IPv4／IPv6 | the simulation of switching of IoT and DNS of IPv4／IPv6 |
| 3 | Auto DNS identifiers mechanism and its management | the mechanism of auto-allocation DNS identifiers and its management |
| 4 | the behavior of multiple devices registered DNS in the meantime | |

Copyright © 2021 TELECOM TECHNOLOGY CENTER

# The Registration Process of IoT End Devices in Inter-Domain

**From Cell_1（Domain1）to Cell_2（Domain1）**

4 Generate DNS A record
IP_A A IMEI_1.Cell_1.Domain_1. <sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_1.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org




9 Generate DNS A record
IP_A A IMEI_1.Cell_2.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_2.Domain_1 . <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org

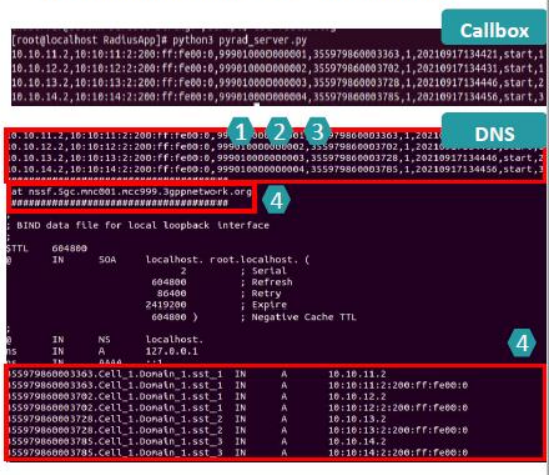
Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Inter-Domain's Test Steps

| Step | Procedure | Introduction of procedure |
|---|---|---|
| 1 | UE registration | IoT connects to Cell_1 and registered. |
| 2 | IPv4／IPv6 Assign | Callbox（MEC）assigns IP to IoT. |
| 3 | Send the registration information to DNS | Information like [IP:IMSI:IMEI:Cell_1:SST] is sent to DNS. |
| 4 | Generate DNS A record | DNS auto-generates domain names and DNS A record through auto-allocation program. |

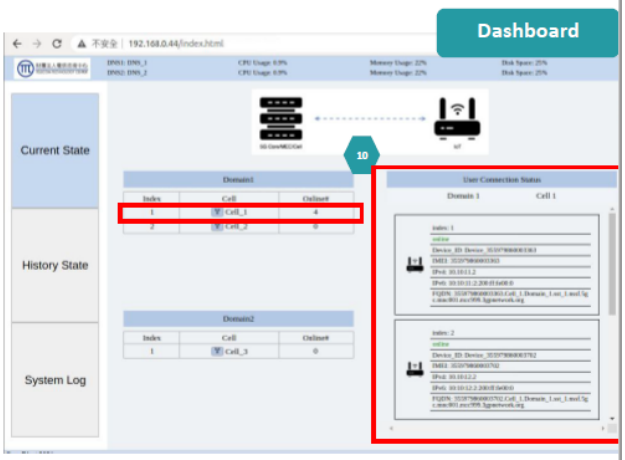
**Step 1 to Step 4**

**（the demonstration of system operation）**



## Inter-domain's test steps

| Step | Procedure | Introduction of procedure |
|---|---|---|
| 1 | UE registration | IoT connects to Cell_1 and registered. |
| 2 | IPv4／IPv6 Assign | Callbox（MEC）assigns IP to IoT. |
| 3 | Send the registration information to DNS | Information like [IP:IMSI:IMEI:Cell_1 :SST] is sent to DNS. |
| 4 | Generate DNS A record | DNS auto-generates domain names and DNS A record through auto-allocation program. |




Copyright © 2021 TELECOM TECHNOLOGY CENTER


## Inter-domain's test

**This chart shows some parameters that IoT register IP and auto-register DN.**
**（after step 1 to step 4）**

| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | APN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR 8K Videos | AR/VR 8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| Step 1、2 | Service IP IPv4 (DHCP) | 10.10.11.2/24 | 10.10.12.2/24 | 10.10.13.2/24 | 10.10.14.2/24 |
| Step 1、2 | Service IP IPv6 (DHCP) | 10:10:11.2::/80 | 10:10:12.2::/80 | 10:10:13.2::/80 | 10:10:14.2::/80 |
| Step 3、4 | DN | 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

Copyright © 2021 TELECOM TECHNOLOGY CENTER

# Inter-domain's test steps

| Step | Procedure | Introduction of procedure |
|---|---|---|
| 5 | UE moving | It moves from Cell_1 to Cell_2, and it is still Domain_1. |
| 6 | UE registration | IoT connects to Cell_2 and registered. |
| 7 | IPv4／IPv6 Assign | Callbox（MEC）assigns IP to IoT, and it utilizes the original IP because it is still Domain_1. |
| 8 | Send the registration information to DNS | Information like [IP:IMSI:IMEI:Cell_1:SST] is sent to DNS by Callbox（MEC）. |
| 9 | Generate DNS A record | DNS auto-generates domain names and DNS A record through auto-allocation program. |
| 10 | Update the DNS and Dashboard | Dashboard accesses the latest DNS A record. |

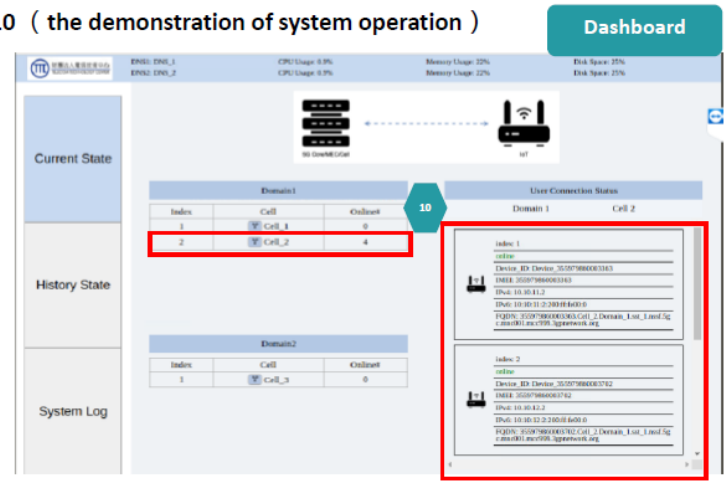
Step 5 to step 9
（the demonstration of system operation）

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Inter-domain's test steps

| Step | Procedure | Introduction of procedure |
|---|---|---|
| 10 | Update the DNS and Dashboard | Dashboard accesses the latest DNS A record. |

Step 10（the demonstration of system operation）




Copyright © 2021 TELECOM TECHNOLOGY CENTER

# Inter-domain's test

**This chart shows some parameters for step 6 to step 10**

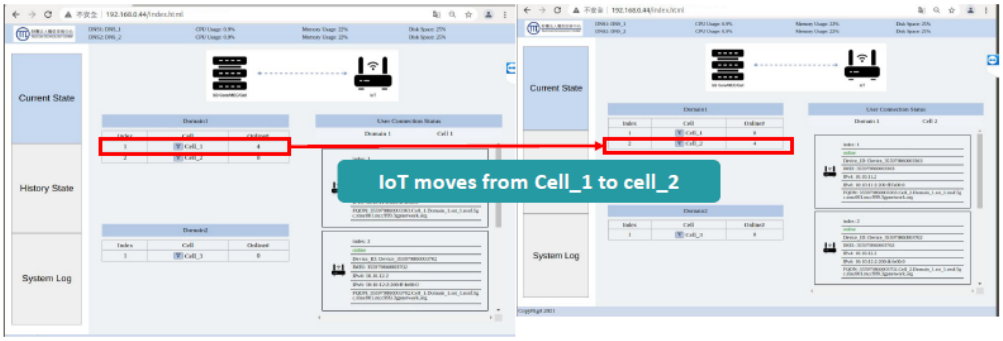
**When the IoT end device（IoT_1）move from Cell_1 to Cell_2, DN will change the name of Cell, but APN and IP remain unchanged.**

| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | APN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| Step 6 to 7 | Service IP IPv4 (DHCP) | 10.10.11.2/24 | 10.10.12.2/24 | 10.10.13.2/24 | 10.10.14.2/24 |
| Step 6 to 7 | Service IP IPv6 (DHCP) | 10:10:11.2::/80 | 10:10:12.2::/80 | 10:10:13.2::/80 | 10:10:14.2::/80 |
| Step 8 to 10 | DN | 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Inter-domain's test steps

**Check the Dashboard after the completion of the inter-domain test.**

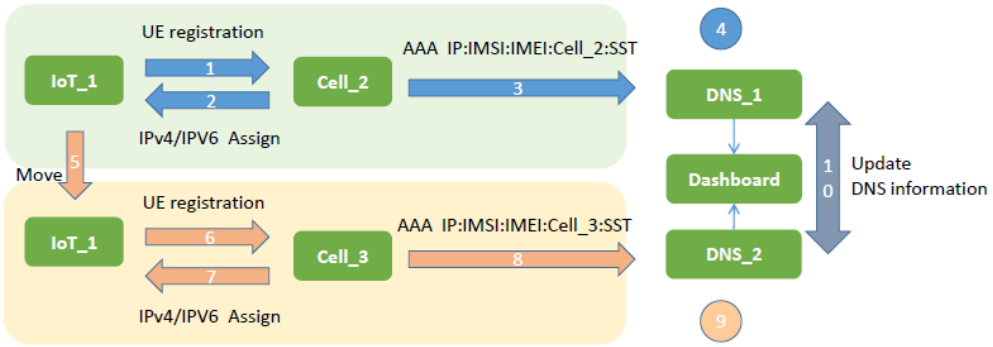



Copyright © 2021 TELECOM TECHNOLOGY CENTER

# The Registration Process of IoT End Devices in Cross-Domain

**The IoT end device move from Domain_1（ cell_2 ）to Domain_2（ cell_3 ）**

4 Generate DNS A record
IP_A A IMEI_1.Cell_2.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_2.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org



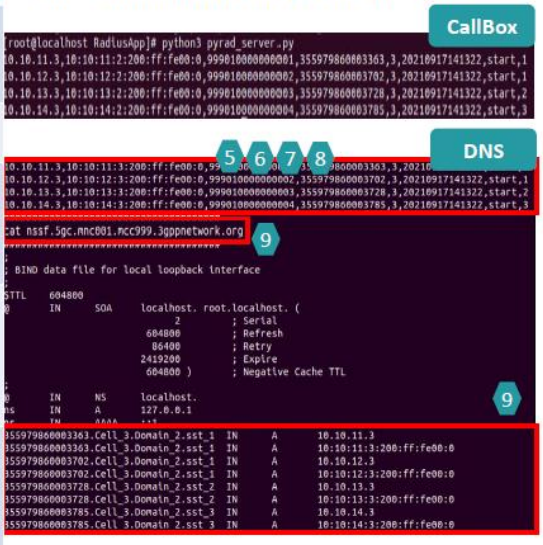

9 Generate DNS A record
IP_A A IMEI_1.Cell_3.Domain_2. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_3.Domain_2. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Cross-domain's test steps

| Step | Procedure | Introduction of procedure |
|---|---|---|
| 5 | UE moving | It moves from Cell_2 to Cell_3, and it moves from Domain_1 to Domain_2 . |
| 6 | UE registration | IoT connects to Cell_3 and registers. |
| 7 | IPv4／IPv6 assign | Callbox（MEC）assigns IP to IoT |
| 8 | Send the registration information to DNS | Information like [IP:IMSI:IMEI:Cell_1:SST] is sent to DNS by Callbox（MEC）. |
| 9 | Generate DNS A record | DNS auto-generates domain names and DNS A／AAA A record through auto-allocation program. |

**Step 5 to step 9**
**（ the demonstration of system operation ）**

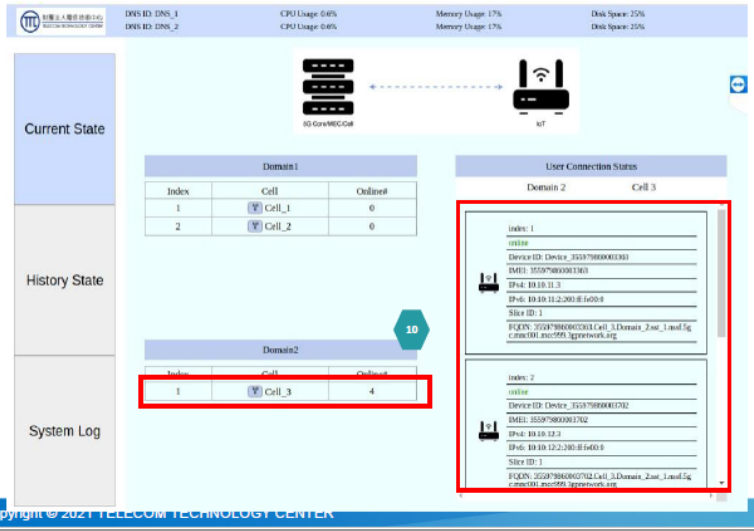



Copyright © 2021 TELECOM TECHNOLOGY CENTER

# Cross-domain's test steps

| Step | Procedure | Introduction of procedure |
|---|---|---|
| 10 | Update the DNS and Dashboard | Dashboard accesses the latest DNS A／AAAA record. |

**Step 10（the demonstration of system operation）**






# Cross-domain's test

**this chart shows some parameters for step 6 to step 10**

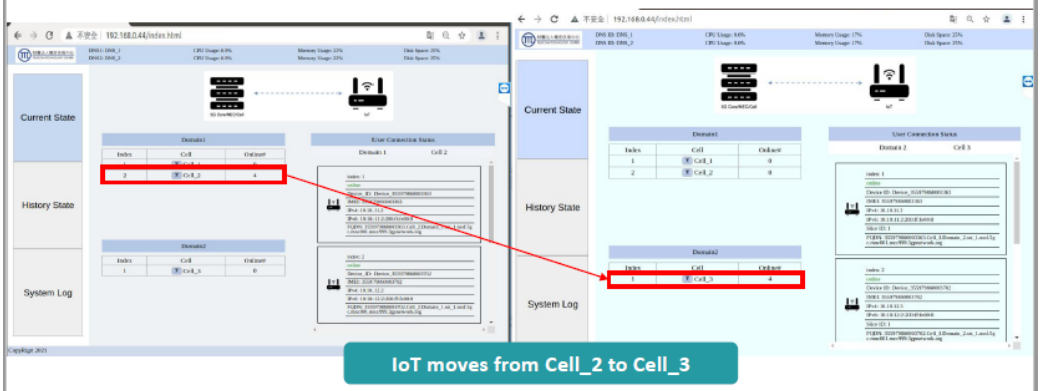
**When the IoT end device（IoT_1）moves from Cell_2 to Cell_3 and gets new IP through registration, DN will change the name of Cell.**

| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | APN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR 8K Videos | AR/VR 8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| Step 6、7 | Service IP IPv4 (DHCP) | 10.10.11.3/24 | 10.10.12.3/24 | 10.10.13.3/24 | 10.10.14.3/24 |
| | Service IP IPv6 (DHCP) | 10:10:11.3::/80 | 10:10:12.3::/80 | 10:10:13.3::/80 | 10:10:14.3::/80 |
| Step 8-10 | DN | 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

Copyright © 2021 TELECOM TECHNOLOGY CENTER

# Cross-domain's test

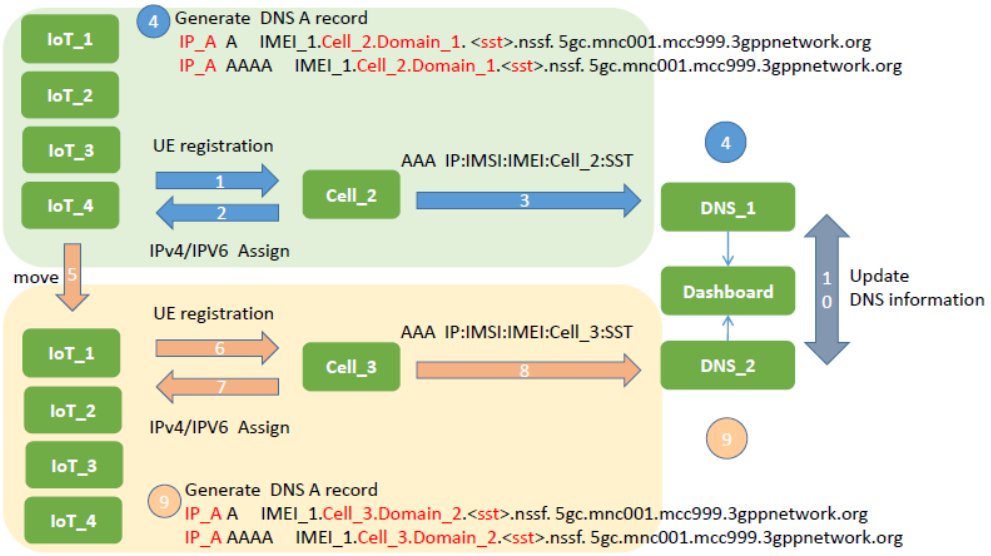
**Check the Dashboard after the completion of the cross-domain test**




Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Scenario 1:
# Large amounts of IoT devices are given identifiers automatically

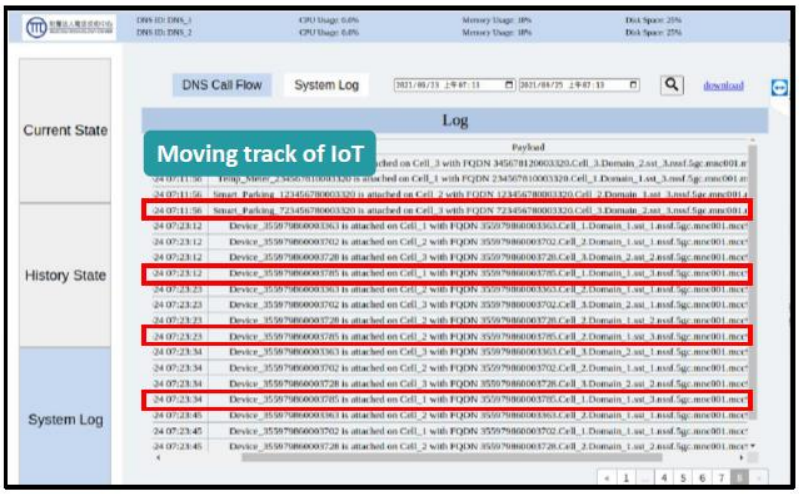
**Four sets of IoT equipment are used in 20 minutes and move among different Cells and Domains**




Copyright © 2021 TELECOM TECHNOLOGY CENTER

## Scenario 1:
## Testing large amounts of IoT devices are given identifiers automatically

**Identify the status of DN after the movement of IoT device through log**

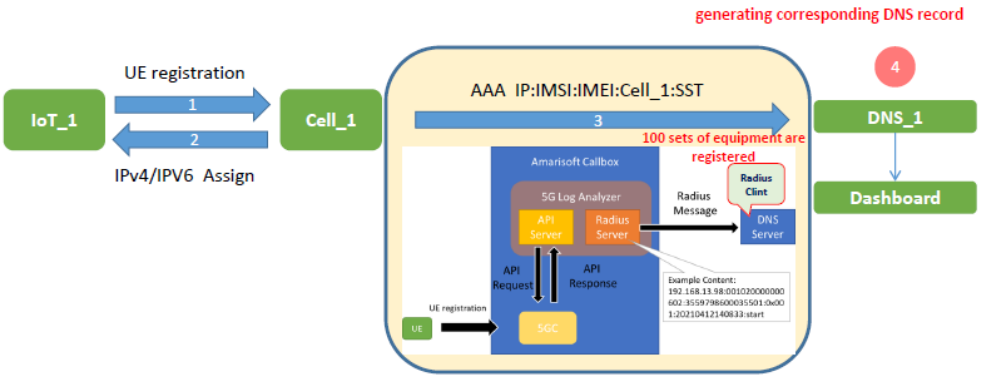



Copyright © 2021 TELECOM TECHNOLOGY CENTER


## Scenario 2:
## Testing large amounts of IoT devices are given identifiers automatically

**Register large amounts of IoT devices and then generate Radius record that will be sent to DNS server.**

4 Generate DNS A record
IP_A A IMEI_1.Cell_1.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_1.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org




Copyright © 2021 TELECOM TECHNOLOGY CENTER

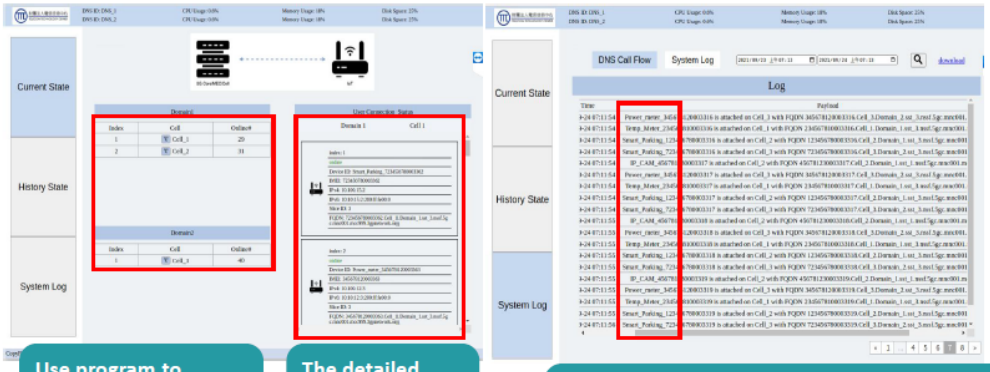
# Scenario 2:
# Testing large amounts of IoT devices are given identifiers automatically

| Name | IP_CAM | Power_Meter | Temp_Meter | Smart_Parking | Smart_Lamps |
|---|---|---|---|---|---|
| APN/DNN | IP_CAM | Power_Meter | Temp_Meter | Smart_Parking | Smart_Lamps |
| TAC (IMEI 8 code) | 45678123 | 34567812 | 23456781 | 12345678 | 72345678 |
| NSSAI | eMBB | MIOT | | | |
| SST | 1 | 3 | | | |
| Template | High quality Video | Smart City sensor | | | |
| Throughput | 100Mbps/100Mbps | 1Mbps/1Mbps | | | |
| Zone | nssf.5gc.mnc001.mcc999.3gppnetwork.org | | | | |
| Service IP IPv4 | 10.100.11.0/24 | 10.100.12.0/24 | 10.100.13.0/24 | 10.100.14.0/24 | 10.100.15.0/124 |
| Service IP IPv6 | 10.:100:11:(1-254):200:ff:fe00:00 | 10.:100:12:(1-254):200:ff:fe00:00 | 10.:100:13:(1-254):200:ff:fe00:00 | 10.:100:14:(1-254):200:ff:fe00:00 | 10.:100:15:(1-254):200:ff:fe00:00 |

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Scenario 2:
# Testing large amounts of IoT devices are given identifiers automatically

**Dashboard**




Use program to simulate 100 fixed IoT devices in 3 Cells

The detailed description of fixed IoT devices

<DNN>_<IMEI> are the IMEI identifier of IoT, and these logs are different IoT devices registered in 3 different Cells.

Copyright © 2021 TELECOM TECHNOLOGY CENTER

# Summary

- This Project was funded by MOTC .
- Through the mechanism of DNS identifiers, the management of fixed and moving IoT devices under 5G is more efficient, and the IoT devices are able to be given identifiers under 5G efficiently.
- The PoC of the research based on the context above verify the mechanism and methods of auto DNS identifiers, which can apply to the latest 5G slicing network context and manage the IoT devices efficiently.
- In the next phase of the research, we plan to do the Proof of Service（PoS）on the real 5G network context.

Copyright © 2021 TELECOM TECHNOLOGY CENTER


# Research Partners

TAIWAN TECH NATIONAL TAIWAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

ADLINK TECHNOLOGY INC.

國立宜蘭大學 National Ilan University NIU

O'PRUEB

鑑智實相科技 Digiforen Technology Co.,Ltd

網路中文 net-chinese.com.tw

Copyright © 2021 TELECOM TECHNOLOGY CENTER

TELECOM
TECHNOLOGY CENTER
Thank you
If you have questions or feedbacks,
you can send them via email.
Email: Emily.Chien@ttc.org.tw
www.ttc.org.tw

# 參、PoC of DNS identifier”（「DNS 識別碼概念性驗證」）會議逐字稿

ICANN72 | Virtual Annual General Meeting – Tech Day (1 of 3)
Monday, October 25, 2021 – 09:00 to 10:00 PDT

KIMBERLY CARLSON:

Hi, everyone. Happy start to ICANN 72 to you all and welcome to Tech
Day on the 25th of October. My name is Kim and along with Kathy, we are your participation managers for this session. Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior.

During the session, questions or comments will only be read aloud if submitted within the Q&A pod. We will read them aloud during the time set by the chair of moderator of the session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, you will be given permission to unmute your microphone. Kindly unmute your microphone at that time and speak.

All participants in this session may comment in the chat. Please use the dropdown menu in the chat pod and select “respond to all panelists and attendees.” This will allow everyone to view your comment. Please note that private chats are only possible among panelists in the Zoom webinar format. Any messages sent by a panelist or standard attendee to another standard attendee will also be seen by the session hosts, cohosts and other panelists.

This session also includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real-time transcript, click on the closed caption button in the Zoom toolbar. And with that, thank you again for joining and I’ll turn the call over to Dr. Eberhard Lisse, chair of the ccNSO Tech Working Group.

EBERHARD LISSE:

Good evening, good morning, or good day, everybody. Welcome to our fifth virtual Tech Day. This time, it's supposed to be in Seattle. I, myself, I am sitting in Germany at the moment, not in Namibia as usual, because I needed to visit some family and I wanted to test out the Starlink satellite dish that I got my sister on the roof. But due to sometechnical problem, we only get 10% of the speed. And they are very coland very helpful in remediating and sending us a new dish and cables.Next slide, please.

We usually go through the agenda in the beginning. I'll do my opening remarks as usual. And then, Justin Chen from University of Taiwan and also working with Net-Chinese. That's the one. We'll talk about—now I lost my train of thought—a proof of concept of DNS identifiers. That's what it was. Then Ed Lewis will speak about the DNS Core Census.

And we put Justin in the beginning because he has the worst daytime. Garth Miller is later on—also has a bad time zone but he came very late into the game so he had to take what he could get. We still put him as early as possible but due to the lengths of the presentation planned for Ed Lewis and him, we couldn't put him before lunch—before the break.

Then Eduardo Alvarez will speak about—Garth will speak about anRDAP-enabled security initiative that CoCCA has been working on for a while. And Eduardo Alvarez from ICANN will speak about ICANN's RDAP conformance tool. Then Roy Arends will speak about DNS magnitude, a way of measuring DNS—another way that he has come up with or some other colleagues of his and him. I don't know. Then Ed Lewis will talk about DNSSEC algorithm choices and Viktor Dukhovni will speak about DNS parameters for TLDs.

So as you can see, I've tried to group these things a little bit. And we actually got these last two together a little bit earlier so that they can choose which one is the better one for introduction.
Then we have another break. We are a bit flexible with the breaks. If we're under or over, we'll shorten or lengthen the breaks. It's not really that necessarily but we have to go with the flow of the ICANN meeting.

Greg Freeman will then speak about RPKI deployment experience at Lumen. Then Roy Arends will speak about the hyperlocal root zone service. I think we have heard all of this a little bit, that you can localize the root zones, which don't change much, so that less traffic comes with all this going up to the top. And then, Dmitry Kohmanyuk from the Ukraine will speak a little bit about ccTLD infrastructure. Do you want to do this yourself or do you want to farm this out?

And then, lastly, I have volunteered Jacques Latour, or rather he volunteered himself if nobody else did. He will then close the Tech Day as we usually do, giving a brief review of the presentations—what was interesting, what was not so interesting, what was helpful.

That means we can now, four minutes in front, start with the first presentation. Justin Chen from Taiwan has the floor.

CHI-YUAN CHEN:

Thank you, chair. Let me share my screen first. My permission is
disabled now.

EBERHARD LISSE:

Kim, can you enable him again, please?

KIMBERLY CARLSON:

It looks like he's still a co-host.

EBERHARD LISSE:

Okay. Just try again. We're not in a hurry. We have a few minutes to get this working. There you go.

CHI-YUAN CHEN:

Okay. Can you …?

EBERHARD LISSE:

There you go. Now we've got it. Go ahead.

CHI-YUAN CHEN:

Okay. Thank you. Hello, everyone. My name is Chi-Yuan Chen. I am a consultant from TTC in Taiwan. This talk is about a proof of concept of DNS identifiers for 5G mobile edge computing. And this project was funded by our government, MOTCCurrently, in telecom, the numbering was based on the ITURecommendation E.164. However, this numbering space is limited. This work is based on the concept of ICANN 5G Technology Report to use the DNS as an IoT identifier and the management of IoT devices is throughthe auto-location. We also designed two scenarios for the network slicing environment of next generation telecommunication network. This is our first-year result of our project and we focus on the 5G mobile edge computing only.

For our key innovations, first we showed, by using the DNS identifier, the management of fixed and moving IoT devices under 5G is more efficient. Second, based on the 5G network slicing, core network will send the APN, cell ID, IMSI, MSISDN, EMEI, IP to Gn DNS to give identifiers on IoT devices according to the RADIUS.

This is the structure of our proof of concept platform. We built a private core network according to the 3GPP Release 15. And we setup network slicing for eMBB, URLLC, and MIOT.

In all the proof of concept scenarios, we used 5G core network emulatorto create two domains, the domain one and the domain two, and sent the required information by RADIUS protocol. We also implemented a dashboard to monitor the network status.

This is our equipment list. We used a 5G router and IPC for IoT devices.And we used an Amarisoft Callbox for the gNodeB. For the DNS server and the dashboard, we implemented a program to collect information in virtual machines.

In our 5G simulator, the red and blue squares [implement] the functionelements. We use a broker program, Session Manager Function, SMF, to send the AAA information.

This is the IoT parameter list, including APN, IMEI for numbering,and NSSAI, SST, template, throughput for network slicing.

For identifier mechanism, we referred to the 3GPP and proposed the IMEI as the DNS identifier in the terminal layer for our private core network. IMEI is a unique number per device. This is a sample for our proof of concept.

In the registration process, the broker program will collect information from 5G Core API and forward UE information, including IP address, IMEI, cell ID, and the timestamp. In the DNS server, when it receives the information, it will generate a DNS A record, then serve the information to the dashboard.

This another sample for the DNS identifier generation. The fully qualified domain name for v4 and v6 were generated in step four.
There are two test cases in our first proof of concept scenario, the inter- domain and the cross-domain.

For the first test case, interdomain-the IoT devices were moved from server one to server two in the same domain. You will need to update information in the DNS record.

There are some data we collect from the Callbox and the DNS server during the registration process. The FQDNs were generated in step four, in the [py] server.

In the dashboard, we can see the [management] of IoT devices and domains and we can click on a button for the detailed information.

This table shows the status after our first registration process, the IP address received from the step one to the step two. And then the FQDN with cell one generated from step three to step four.

Later on, we moved the IoT device from the cell one to the cell two. There are some data we collected in the step five through the step 10.

In the dashboard, we can see the four IoT devices are moved to the cell two now.
For the step six through step 10, the FDQN will be updated with the new one in cell two. We

can see the label.

This screen shows the changes in the dashboard when IoT moves from the cell one to the cell two.

For the second test case, cross-domain, the IoT devices were moved from the cell two to the cell three in a different domain. It will also need to update its information in the DNS record with different DNS server.

There are some data we also collected in the step five through the step nine. And now we can see that four IoT devices are moved to cell three in domain two now.

Also, the FQDNs were updated with the cell three and the domain two now.

This shows the changes in the dashboard when the IoT device is moved from the domain one to the domain two.

For the scenario one, we show IoT devices were given identifiers automatically. We can also trace the movement of IoT devices in the dashboard.

For the scenario two, we showed that large amount of IoT devices are given identifiers automatically and that later, 100 IoT devices are registered in different cell in the different domain.

This table shows the parameter list of our 100 IoT devices. They have different data than in the slicing [parameters].

From the dashboard, we can see that 100 IoT devices are registered in the two domains in the different cells. And in this scenario, we used the DNN and the IMEI as the identifier of IoT device.

In this work, we verified a mechanism and method of auto DNS identifier. We can apply it to

the 5G slicing network and manage the IoT devices efficiently. In the next phase, we plan to do the proof of service on real and the public 5G network.

Especially thanks to the MOTC and ICANN and thanks to our panel.

EBERHARD LISSE:
Thank you very much. Technically, well beyond me but very interesting,

I think. IoT, we have had many presentations, or some, about IoT devices before. This is, in any case, where the future is. So probably, using the DNS to manage them is a good idea. I saw one hand, which I don't see anymore. Are there any questions? Please raise your hands and we will them open it, if there is one question. No more hands? One of the panelists has a question. Jacques Latour, you have the floor.

JACQUES LATOUR:
Yes. Thank you. So I understand the RADIUS and the domain name assignment are to allow the IoT device to move along and get provision. So my question is are the IoT devices themselves aware of that identity or that's something separate?

CHI-YUAN CHEN:
Okay. Can you hear my voice?

JACQUES LATOUR:
Yes.

EBERHARD LISSE:
Yes, we can.

CHI-YUAN CHEN:
Okay. Thank you. Yes. IoT devices can aware this identifier from the DNS query.

JACQUES LATOUR:

But is the IoT device aware of its own identity when it changes? Because presumably when it changes zones, like cells, the identifier changes, which means it changes the identity of the IoT device.

CHI-YUAN CHEN:
I think both the IoT device and the core network can use the DNS query to update the newest identifier and the related information.
JACQUES LATOUR:
Okay. Thank you

EBERHARD LISSE:
Thank you. Okay there are few questions in the Q&A. Yoshiro Yoneda asked, "What kind of IoT devices are you assuming?"

CHI-YUAN CHEN:
Okay. Wait a minute. We used the 5G gateway and the industrial IoT— many industrial personal computers, as our IoT device.

EBERHARD LISSE:
So it's just a proof of concept but he wanted to know what types of IoT devices would you be using this for—were you assuming that are to be used? I saw there were parking meters, and cameras, and so on. That's probably what he means.

CHI-YUAN CHEN:
Oh. It's the DNN, data network name, for the IoT device. And we used this name for our network slicing tool to our proof of concept.

EBERHARD LISSE:
Okay. Justin Mack from MarkMonitor asks, "What TTL, time to live, values are used for the A and AAAA records that are being generated?"

CHI-YUAN CHEN:
Sorry. Time to live?
EBERHARD LISSE:

Time to live, TTL value of the A and the AAAA records. Can you answer that? Do you understand the question? Did you understand the question or what is the problem? All right. I think we're having a communication issue here. Thank you very much. I will ask the people who asked this question to take it offline and send it directly to you on the e-mail address that was listed. Thank you very much.
Okay. Can we have the next presenter now, Ed Lewis? And un-share Justin's screen, please?

ED LEWIS:
I think he stopped sharing. I can start.

EBERHARD LISSE:
There you go.

ED LEWIS:
There we go. All right. Everybody, can you see and hear?

EBERHARD LISSE:
We can see and hear you very well.

ED LEWIS:
All right. I'm going to have a talk here called an update on the DNS Core Census, which might be promoting a little higher than I probably should because many people have never heard of my work on this. It's a small project. So I'm going to go through, basically, a coverage of some work I've been doing for the past couple of months and this is the agenda. Go through the census. What's DNS Core? What's the census? Then talk about the sources of the data that I'm playing with and the assembly of the data that I'm doing and then some commentary about making this public at some point.
So in a nutshell, the work here, the DNS Core Census is a small project that I've been working on for about a year and a half. It started out as a module to help me do other data collections, where I look at data and I want to split the data into pieces to make sense of out what's happening along certain lines, whether it's geographic, whether it's some other type of information, whatever is going on there. And TLDs are where I've spent all my time studying. I have a lot of history data on this.
So I had an earlier version of this. I numbered it 002, arbitrarily. And I presented it twice at

DNS-OARC in August of 2020, a year ago plus. And then I had another talk at LACTLD in September the same year. And I have the 002 on the web. It's actually accessible but I'm not promoting the URL for that anymore because I'm about to make a move. And there is at least one person who's accessed it over time and I've been in contact one-on-one with updates on that. So sooner or later, it will move and it will be in a new place. I'm not going to promise when right now.

So I do have some feedback from that and some other communication with other researchers. And there were three things that I decided to do, that I wanted to start over again. The number-one reason for starting over again was actually my third sub-bullet there where I had to make the process more rugged. I found out when data feeds disappeared, my program wasn't handling it very well and would just be absent for a day or two.
But there were a few comments. One was to rearrange how the data was being stored internally. I'll get into that a little bit later on. And then another person suggested some more [instances] that I might include, which I've managed to do in newer version, and gave me the idea that maybe I need to get some outside input on what should be or shouldn't be in this over time. And finally, making this version public. With this version, being the 010, public, it's an ongoing effort. And it may be out there who knows when. Again, I don't like to make promises.

The origin of this work, to go back to where this is coming from, I have to decide, a lot of times, whether a TLD that I'm looking at is a ccTLD or a gTLD. The reason for this is that gTLDs and ccTLDs run under different sets of rules. They behave very differently. When you're looking at behavior over time, you want to see does a certain policy seem to have a certain impact. Or if you see a lot of TLDs doing something, is it because they are independently thinking of that or are they all following a given set of rules.
It's not just the gTLD/ccTLD division that is interesting to me. There's some regional ones in there. IDN or not is another. And there's many other ones out there. To give you an example—not to harp on the data I'm showing here—but you see these pie charts. They're mostly red and green. And what's interesting in this is that the charts are different from place to place. This is divided from all TLDs, to all ccTLDs, to all gTLDs of the first division. That shows you a big difference between those two. And then, with the ccTLDs, I can divide again from the two-letter ccTLDs and the IDN ccTLDs.

So in the old day, the real problem I had was in the old days, it was simple to determine a TLD, whether it was gTLD or not. We had the two- letter codes everywhere. But when we go into

IDN ccTLDs, it made it a much more complicated question to answer that. And I had to do that for many people, over and over again, internally, when they asked me to work on some analysis for them. That's what started me on the effort to build a census.
I saw there was a hand raised. I'm deciding whether we should take questions as we go. I think I'll let questions

EBERHARD LISSE:
No. We'll take questions at the end. I don't know to interrupt the presenters. It's not good for the flow.

ED LEWIS:
All right. Okay. Cool. So the scope creep. Initially, I just wanted to know whether TLD was ccTLD or gTLD. But as you start looking at this, there are other factors. There is when did a TLD begin. How old is it? We have the legacy TLDs from before 2012. For a while, when I was doing this work, TLDs were very young. They might have been months old. Now they're usually a couple years old. We look at different phases of what goes on in them.
Another thing you can pull out of this information, if you dig deeply, is what TLDs share the same platform—at least share the same DNS. That's important because when you see a lot of TLDs suddenly adopt a new DNS feature, is it because a lot of people made the same decision—they ran off and said it was a really good idea—or did just one dominant player in DNS platforms decide, "I'm now going to assign everything." And with one flip of the switch, you see everything fly at one. And there's some examples of that. You can see that easily. In fact, my other talk will dive into that a bit.
Another one is geographical, geopolitical regions. I always get people going to a conference somewhere and saying, "I'd to have information about my audience's area of concern. They're from this part of the world. What do you know about that part of world or about that restriction?" and so on.

Also, you've got information about sizes. Are TLDs large, medium, small? What kind of cryptography have they chosen? There are many ways you want to carve this up for different types of analysis. And finally, too, where are the name servers on the network? The addresses, routes, autonomous system numbers are interesting.
One that inspired me to this work, too, is a lot of people like to divide the gTLDs into the new gTLDs and the old gTLDs. There are some finer distinctions to be made here so I really wanted to go in deeper and find out where I could split things up.

The novelty here is not so much getting this information. It's that this information is all over the place. It's scattered. I have a lot of sources that ICANN has published. And I wanted to simply put it in one place. And I also want to make it history so I can go back over time and do some of the historical analysis.

So, for example, of a different type of division here—and again, I'm not going to [inaudible] the underlying data. But these are pie charts representing one thing about DNSSEC across all the TLDs. And I have here the ICANN geographic divisions pulled apart. And you can see again, the pie charts, they all look pretty much different. They're red, and green, and one's larger in some area, and so on. The pattern is different depending on where you are in the world. Geography still rules, even on the Internet.

So coverage creep. Besides trying to put all this stuff together, how much of the DNS can we do? If we could have everything in the DNS in one place, that would be great but we don't have that. It's unmanageable to have that much data. On the other hand, if you pick just the root zone and its delegations, which is where I spent a lot of my time early on, it's too small a sample set to get an idea of what's going on, on the Internet.

So I want to say it's more of a right-size thing out there. So what's sensible? What's interesting. And that's kind of an open question. When I was initially doing this work internally, there were a lot of people wondering what I meant by "sensible." So in a nutshell—and I'll go through this again—I settled on ccTLDs and gTLDs, the reverse map zones and the RIRs, and then the zones that tie these together.

Other possible cores out there that could be interesting to do this kind of work on, but you'd have to do a lot more work to assemble the lists, are either the high-volume or popular zones. I see a lot of research that goes into the Alexa lists or Cisco's umbrella. I think that was the name of the other one.

This isn't the popular zones—not the zones that get a lot of hits, necessarily. You can go with genres like social media, or public sector, or anything like that. You might want to look at how an industry is working on the Internet. Again, that's interesting but not what I could easily put a rope around.

Or technically-complex zones. In the DNS, the root zone is actually a pretty simple DNS zone. It doesn't get updated in very fancy ways. But as you go down the stack, features pop in because at the leaf edges of the DNS, we use it in many other ways, like for traffic engineering. We like to point things different ways. So there are many perspectives here.

A lot of them are worthy or membership but it's very subjective and the lines aren't drawn clearly.

So defining what I call a DNS Core … And I'm using the DNS Core as … I just threw a name out there. It's the elements of the DNS close to the root zone which primarily exist to delegate other zones. Top-level domains are a part of that, including sub-parts of TLDs out there.
The Regional Internet Registries, I throw them in there because they are registries also, and they run DNS, and they're all part of this magic that goes on. And then there are a bunch of other zones that fill in the cracks of those areas that people forget about but they're worth adding to see how they run.

Generally, these are zones which are under guidelines set by a community and that's a very loose definition. They see themselves as a primary service—not that DNS is not important to social media giants because DNS is very important to what they do. But their social media platform is their leader—the lead interest at what they're doing.

And also, a lot of the TLDs tend to stick closer to the applicable standards. They don't look for innovations in the DNs. They try to make sure things are run well and flat as an even platform for all others. They're not trying to support some other purpose-built application.
So the DNS Core starts with the root zone. I go down to something else that I've invented called the commercial registration boundary. And that's the area where, basically, the registrants start paying for delegations. For example, customer.example. That's the typical example in the gTLD space. It could be a category below that. It could be a city province under a ccTLD, where payment may not be cash. It might be something else or some other qualification.

Or even if you go down to the reverse map, where do the service providers start delegating DNS for their PTR records, essentially. The concept is still experimental. Generally, the boundary is usually a third layer or it might be deeper.

So to add a little color here, this is a cartoon of the DNS Core, showing what I just covered—the root zone, the TLDs on top, the RIR component in the middle. Arpa and a lot of things that are under it would be in there, too. And sub-TLDs and sub-gTLDs. There are a few sub-gTLDs out there in the older TLDs.

So to give you an idea of what the core looks like—again, to add more color to my slides—the Core, there about 4,000 zones that I cover. 2,300 of them are sub-ccTLDs. That refers to the provinces or the regions within some of the ccTLDs that have really got very deep label usage.

There are about 1,300 gTLDs, 300 ccTLDs. That's what we're more commonly looking at when we look at the center of the DNS. There are about reverse map zones. That means some number .in-addr.arpa for IPv4 or the corresponding IPv6 delegations.

And I also have in these other zones these special use ones there because sometimes they pop up and you want to know that that was a special use. You shouldn't see it necessarily but you want to know that in research when you come across it because you will. I won't go through the rest of it but the test was interesting because there are 11 test TLDs out there that are inactive but they're still on the record books. And you may come across those if you're doing some research and some historical.

The other things about the scattered—or the zone depth, most things are actually three levels deep. Two levels is popular. And you can get all the way down to nine levels. There's some ccTLDs that have gone nine levels down before they go out to their registrants for whatever purpose that would actually be ccTLDs. It's not the reverse map off the top of my head.

Other things. There are 4,000 zones, 6,000 name servers. There's a lot of sharing. A lot of zones share name servers. Only about 10,000 addresses and a lot of addresses are shared between name servers. And route origins, there's only about 2,000 of them, and so on down the line. The bottom four numbers are just counts of what I grab as I go along through getting some of the data.

So the census itself, how it's embodied is it's compiled daily. I run a script. It takes about an hour and a half to go through it and collect everything. I store it in two things I'll mention later.

I have a database backend, which made it much—a tabular database. SQL-like is, I guess, the way to say that. I also have, for each run, nine CSV files. I have nine tables that correspond with CSV files. And also, I spit out nine equivalent JSON files, just to be cool with JSON again.

There's a little background to this. Why not lead with JSON? That's been a problem that's been at the back of my head. I had to put it on the slide here. Initially, I did something much more JSON-like. Let me see my next slide. Yeah. This is on my next slide. I did something that was much more richly-typed. It was a very hierarchical thing. I had three JSON files that came out. There was the zones, the name servers, and the addresses because they were shared. And I had a lot of ancillary information out of that.

To flatten that, though, I couldn't flatten that easily. So I had to restructure this for table bases into nine of them. Six of the tables, basically, are just the details that are in the original JSON structure. And this came about—the comment that I should be looking more at things like pandas.DataFrames, which is a tabular data type within Python. It just seems to be much more acceptable across the field of numerical analysis or data analysis out there. We like to use tables out there, not rich data structures out there.

So I did a lot of work to spin this backward in my mind from the JSON world back to CSV. It just seems kind of odd but it seems like that's the way a lot of the analysis work is going these days, is they want to be in that space.
So to go into what it is that's in my census, I'm going to list the sources of data and walk through them that I have here—a couple pages of this. From IANA, I have access to the root zone database, which is out there. It's the database itself in XML. It's the history of what's been built up over time—not the history. It's actually a snapshot of what it is over time.

There is a Repository of IDN Practices that was requested. It's a page which shows IDN tables—the policies used by certain TLDs out there. And that Special-Use Domain Names is one that's a registry that IANA is hosting which is, I guess, more … I don't know who the proper operator would be but the IETF documents define what's in there. And again, that's for reference to make sure we account for names that are special- use, that might pop into the

Internet. There's a lot of playing done with that.

From the ICANN sources here, I have a couple of websites and one other file in here. The ccTLD fast-track string evaluation gives a lot of metadata about the ccTLD IDNs that are in play. Registry agreement termination keeps track of the process to stop TLDs in running. So we have a history of why they may have been stopped. Sometimes, if the process itself doesn't succeed, we may actually have some gTLDs come back to life after the process is stopped. I found that interesting when I went through that page.
The ICANN geographic regions. The regions I've been using in the slides are the ICANN-assigned regions for some of the ccTLDs out there. There's a gTLD contract status page, which is known to some people that are involved with certificate authorities. It has a history back 10 years. It's not probably very well-visible. It's not an HMTL page. It's a JSON structure, which is very interesting.

And then there are various zone files that I can get my hands on, that most people can get out of CZDS. I'm sorry. In this line I'm including the zone files that ICANN publishes. If you go to that website, you'll see a list of what we have on some name servers that you can grab. That's not the CZDS. That's actually different, although I do have access to those, too.

Another source of data from the UN. It was requested that I bring in the regional tags that are used by the UN because if you're not an ICANN person, the UN probably is the place to go for regional definitions. There's a bunch of different levels that are added there. That's just metadata from the other data.

From the RIRs, first I was using RIPE's RPK validator. And when I started doing the slides, I realized that they had discontinued that just about a month ago. And I've since replaced it by a lookalike service which is running a local Routinator instance. I don't have a lot of detail here because I just did that it's picked up the pace since then, giving me the data. I know there are other options out there and we might want to look at some better … I have to see whether it's reliable or not. The data that it gives me seems to be very much equivalent to what I was getting from the RPKI validator. So far, so good on that.

And then also, I pulled the zone files that the RIRs publish. Some of them through FTPs, some through AXFR. Most of them are generally public. Two of them, I requested and got allowed to pull them, to work on them.

Also, beyond ICANN and the RIRs and IANA and the UN, the next series, I went out to some other public sources out there. There's a cool tool from Team Cymru. You ask about an IP address and it will tell you what routing information is available for it, what AS Numbers originate the route to that address. And also, it gives you some information about the name of the operator, which is cool to keep around.

I use the Public Suffix List but I don't use that as … We know that this is an interesting topic to get to the PSL. I use that as hints to help me figure out the commercial registration boundary. I don't republish that in whole. I just use it in some other work. I don't think I have any notes about the PSL membership of anything in the output here but I use that as an input to my work.

And then I do some DNS queries, of course. This is what takes some time. And this is done to fill in information that's not already covered— for example, the SOA, the DNS record and so on. And in particular, a lot of those I get from other sources but I sometimes want to get the DNSSEC information, whether it's available or not. And again, the DNS queries are chiefly to just get the commercial registration boundary poked at.
So this boundary, it's an estimation right now. I target a couple names that have been suspected of sub-elements. There's some out there that are pretty obvious. You might see .co or .ad or .gov are used across the board. I try those. And then I also through the Public Service List, which gives me another set of candidates. If they pop up to pass my little test, I include them as part of the boundary out there.

I'm not looking for the registrations in those areas. I'm not trying to discover what's outside the commercial registration boundary. I'm just trying to define where a registry leaves off and lets it go out to their registrations out there. It's experimental. There are a couple other ways

I could try to do this but I haven't spent whole lot of time with it. It's a little harder to do than it sounds.
So now, assembly of the data. What do I do with all this stuff? I grab all this stuff. It takes about … I'd say it's an hour and a half every day that it goes out and grabs everything. After my first attempt, I realized I didn't really want to generate much information. I just want to pass things through as much as possible in a straight-through phase. So you can always go back to the original source and get the original information and read on what it means. But just trying to collect it all in one place.

I use keywords. They hint at the source it comes from to help guide my way backwards but I also keep track of things come from. It's meant, ultimately, to be a utility for research, not a product of research. So it's not going to definitely tell you anything. The census doesn't tell you anything. You would use that as part of some research work and I've don't some examples of that. But again, being the one that wrote everything, I'm not really a good judge of whether I've been successful at that.

But there are these synthesized records. I have the start and end of the census, which of course, only I could come up with. I have the sources, which tells me where I got information from in a not-exactly-obvious way. It's more to help me debug things. Then I have a category, where I create my idea of gTLD, ccTLD and so on, and sub-gTLD to sub-ccTLD because in many places, it's just assumed that this list is a list of something. So I had to create the category.

The jurisdictions are the two-letter ISO codes. They most easily come from ccTLDs but then I assign a worldwide one for all the other elements that are gTLDs. I'm going to go through the next couple sides a little more quickly because I see there's some questions coming in and I want to leave time for that.

But for the zones, I have this information here. I've got the technical information, the zone cut information, all the bookkeeping you'd want to see, the root database, the gTLD, IDN metadata, agreement termination if it applies, and so on down the list there. There's just the list there.

The name servers, I have the addresses that are used for them, whether it's a registered address, meaning it's in the database somewhere. Cut- point, authoritative, and they should all agree but they don't always agree. And for cut-points, I also try to keep track of where the glue is coming from, what zone had that.

The glue information and authoritative is supposed to be the same. But as you go through the DNS core, it's not always true. There are some lingering differences over time. But for the most part, it's actually pretty clean.

Addresses, I have the address family. For some cases, I realized I had to keep track whether it was v4 or v6, even though some languages will let you do that automatically. Route origins, where is the route coming from? That's the BGP information, the CIDR notation of the network prefix and the AS Number. And then also, I keep track of the registered and glue values across the board. And also, I keep track of what name servers claim the address. And on the same servers slide, the name servers also keep track of what zones claim them. So you can look for all the sharing out there.

Route origins, I have the information about the route origins. And the AS Number table pretty much is the name of the operator, as I'm pulling that from Team Cymru.

DNSKEY records, DS records, RRSIG records. These are three tables that each have columns that correspond to the fields of those records. And whenever I find a record of those types, I store that. This way we can look at what parameters are being used in places, like what kind of keys, what algorithms are out there, for example, how the DS record has been hashed and so on throughout that.

And finally, the IDN practices. This pretty much the most passed- through of all things I have here. I read the IANA webpage. I convert it from the human-readable HTML that you can see, and visualize, and click on, to computer-readable, which is just these columns of what's in that information there.

Now, I don't have much about ccTLDs. I have that they exist. I have their technical data. But I don't go deep into them. I don't into the size of the ccTLD. I don't have population information for that. I know there are a lot of other sources for that. But I chose not to add bits and pieces. I wanted to be clean about this.

I don't have the complete coverage of the commercial registration boundary, which is more interesting in the ccTLD space—maybe enough to understand the depth and shape of ccTLD name spaces out there.

It would be great to have more coverage here but I'm trying to be mindful of being able to easily label this work—to say that it's just gTLDs with some ccTLD stuff out there. I know that some ccTLDs have name server zone files available. But until we have at least most of them, I don't really want to expand it into that area right now. I'd rather point to where they are or have them work with me in a different way. I don't want to exclude them. I just don't think it's convenient right now.

Presentation of the data. It's stored in an SQL-like database. It's a database, of course, which is not accessible to the public but it's built, ideally, for the Python data frames approach. I also have the data being generated into CSV and JSON text files but I haven't been able to get them in a place where anyone can play with it, at this point.

So my next steps. My next steps is to publish the dataset at some point. I do have documentation waiting to go, too, this time around. And I'm looking for feedback. Of course, you see my bottom. It says feedback requires published data. That will come along. In the meantime, expressions of interest would be appreciated.

But the feedback is, is this stuff worth the effort? Is this data worth the effort? I sometimes wonder about that because one thing I didn't put in the slides was that there's a lot of space taken up on disks to hold all this stuff. Maybe I don't want to do all that.

What other data would be helpful. I've gotten a few suggestions already in the past. I'm sure

there's more to go. And what's the best way to make this usable by researchers. I'm guessing from what I do one way but I may not be the best at doing this.
So with that, I am done with my slides and I see that there's some raised hands and questions. I guess I should turn it back to the moderator to work on this. Or should I just—

EBERHARD LISSE:
Thank you very much. I promised Viktor first crack. So, Viktor, can you unmute yourself, please?

VIKTOR DUKHOVNI:
Sure. I could use data like this, especially about where the commercial registration cuts are. I currently attempt to get that data from PSL with lots of exceptions. But it's not accurate and lots of work. How do you figure out where the boundaries are? And can I get that data?

ED LEWIS:
I'd be willing to share that. I have two things, right now, that I'm pulling. One is way back when I did a scrape of HTML, I did a hand-scrape of Wikipedia to find out what some ccTLDs advertise as their sub- elements. I threw all those names into a jumble and tried them across the board. That's one. I don't know that I have any statistics on whether that's a good strategy or not. But then the PSL is pretty much the other place I rely on. I have an idea of using some other passive DNS information but there's so much of that, I haven't been able to make much progress of it.
But I'd be willing to share the … Right now, at this point, I could send you my list of usual suspects in an e-mail, Viktor. That's probably the best way to do that.

VIKTOR DUKHOVNI:
All right. And I may have data for you. We should probably exchange
some. There are places that are difficult. Like Poland and Norway have lots of city or other things like that, that are hard to track for me.

ED LEWIS:
Yeah. I say I like to go naming no names. But you're not far from the truth on that. And they're not the only ones. There's a few others that are very deep. One TLD impresses me because they have the majority of the PSL names but they have it all in the same zone. It's amazing.

EBERHARD LISSE:
All right. Thank you. I want to get Steve Crocker, who has got his hand up for a while, please. You may unmute yourself now. There you go.

STEVE CROCKER:
Thank you. Ed, first of all, this is great work. I congratulate you on this.
I particularly like the focus on the backends and the name servers. That will give some interesting perspective on the underlying organization— emergent organization of the operations.

I know you're fully aware but for the benefit of the audience, I've been involved for a long time and helped create the database and the maps that are shown in the DNSSEC Workshop. So on Wednesday, for example, of this week there'll be a presentation of that. That work is older than I can remember, even though we started it and then transferred it over to the Internet Society, which has been publishing these maps on a weekly basis.
What's interesting is that underneath those maps is a full-scale database that has a complete history of everything that's gone into it. So there is rather richer data there than might first appear. It doesn't cover all the things that you have, by ay means. It was very focused on just tracking DNSSEC deployment.
But we did look at some of the same organizational issues. How do you classify a TLD into CCs versus Gs and some things that didn't fit very cleanly into that? What do you do with IDNs and so forth? So there's some areas where we have related statistics. It will be interesting to try to reconcile the numbers that are in that database versus what's in yours and so forth.
The commercial registration boundary, I think, is very important. And the Public Suffix List is a mixture of several different things. So I agree with you. There's partial information there.
One comment about tracking things. I think you've emphasized, as best I can tell, doing everything in as automated a fashion as possible. Obviously, that's desirable. What we discovered is that much of the data that we were interested in had to be collected by hand. That was the bad news.
The good news is, there isn't that much data. It doesn't change that often so that it's quite manageable. So for example, if you want to know what region, for example, a TLD is in, that's determined basically once. It doesn't have to be scanned, and rescanned, and rescanned over and over again. So I just wanted to mention all of those things.
I guess one additional comment is in looking at the backends, are you prepared for backends changing as they do once in a while, when the backend operation is transferred? A few examples

come to mind—for example, .au has moved, I think, twice now, if I recall correctly.
Oh, yes. One more thing. For the ccTLDs, do you keep track of the governance structure and is that of interest? Because I think there are some effects related to that, that might be interesting to track over a period of time. Thank you very much.

ED LEWIS:
To answer the first question I remember, in terms of backends changing, I've seen that. For the census, the census is just trying to track that. It's not impacted by that happening. Now, I have some analysis which goes over and does that, where it tries to discover what I call DNS houses and AS houses. I've run that for a time using the old census form. I need to rewrite it for the new census form.
It's interesting to watch that because you see when an operator may change. You can see in the newspaper that someone bought somebody else. And then, months go by and you start seeing a change at the IANA database, saying that they've changed the backend database there. And then maybe a few weeks or months go by and you see the DNS RNAME change. So by looking at different elements, you can get a heuristic for who's actually the backend operator.
Also it made me very much aware of this that when we do transition TLDs from one place to another, we don't transition the technology always at the same time. It takes technologists a few months or weeks to get everything smoothly run over there. So the census actually highlights the process even more so. And with another layer of coding, you can start dividing who are the co-managers? Who's managing all of these TLDs together. There's 240, at the time, players out there.

Oh. The second question, the ccTLD governance. My first answer was so long I almost ran out my memory buffer here. The governance there, I'm not exactly sure how to interpret that. But I do record the backend operators of the TLDs out there. I don't know that I have the registry administration, which might give you an inference as to whether—who is it that's running this. Is it a company running it? Or is it being run by the jurisdiction that owns the ccTLD name and so on.
When you say "governance," I'm not sure if that … We can talk more offline about that. But we can figure out what we want to record in thisSTEVE CROCKER: Yeah. The question is whether it's being run by the government, being run independently, or something [creative] thing.

EBERHARD LISSE:
Okay. Can we come to an end of the particular thread? Because we're running a little bit over time. There's one more question in the queue. Thank you very much, Steve. It was very interesting, though. Brett from Nominet, I think, asked, "Do you plan to make that data available to other interested parties? I understood you to say it's not research. It's a tool."

ED LEWIS:
Right. Yes. I very much plan to make it available to interested parties and also uninterested ones, too, if they want. Yeah. I plan to make this publicly available on the network. I'm getting closer to that but I can't promise how close I am. But yeah. It definitely will be out there.

EBERHARD LISSE:
Great stuff. Thank you very much. I'll look forward to the next … Sorry.
I muted myself just now. We are going to break now for half an hour until 17:30 UTC—that's 25 minutes—and then Garth Miller will start. Thank you.

KIMBERLY CARLSON: Thank you all. Please stop the recording.

[END OF TRANSCRIPTION]

# 附件三、產學研者深度訪談規劃及紀錄

# 壹、產學研者深度訪談規劃

## 一、 訪談目的

本計畫下世代電信網路號碼技術及政策研析部分，除由計畫團隊觀測國際趨勢及各國政策發展外，亦規劃於 110 年 8 月 20 日前，訪談至少 3 位之電信號碼專業領域及參與相關會議之專家產學研者，請其分享國際下世代電信號碼機制及其他國家政策發展情形，並提供其觀點及建議，期藉由深度訪談，掌握國際下世代電信號碼機制及各國政策發展趨勢，並瞭解專業面之觀點及建議，以強化本計畫技術研析，促使我國政策擬議更為周全並符合國際發展趨勢；亦可將該等技術新知提供予計畫之專業人才，強化其技術能量，增進本計畫人才培育效益。

## 二、 訪談題目及大綱

本次訪談預計請受訪者分享國際下世代電信號碼機制及其他國家政策發展情形、5G 網路技術等，並提供其觀點及建議，題目及大綱如下表：

| 題目 | 大綱 |
|---|---|
| 國際 5G 物聯網號碼機制及各國政策發展情形 | 1、國際 5G 物聯網號碼發展現況：ITU-T E.164、E.212 建議書對物聯網編碼選項。<br>2、主要國家 5G 物聯網號碼政策：美國、中國、歐盟之政策及市場發展。 |
| 5G 網路技術 | 1、編碼機制：國際電信編碼、命名、尋址及識別資源 (NNAI) 。<br>2、網路切片：標準發展、專網架構下之應用。<br>3、多接取邊緣運算：標準發展、專網架構下之應用。<br>4、網路分裂議題。<br>5、下一步的發展：3GPP R16/R17 針對 5G 垂直應用場景所發展之關鍵增強技術。. |

| 題目 | 大綱 |
| --- | --- |
| 下世代電信號碼演變研析 | ITU Network-2030、ETSI Non-IP、IETF Protocols for IoT 及 ICANN DNS 於 5G 網路應用等。 |

## 三、 訪談對象

本訪談規劃以具備下列條件人員作為訪談對象：

(一)具備電信號碼專業或長期投入電信號碼相關技術研究。

(二)曾參與我國政府通訊技術相關計畫，具有政策制定經驗。

(三)曾參與國際電信號碼相關活動或會議（如：「網際網路網域名稱及位址指配機構」（ICANN）、「網際網路工程任務組」（IETF）等）內部工作或擔任其幹部。

| 項次 | 姓名/單位 | 資歷 | 訪談理由及目的 |
| --- | --- | --- | --- |
| 1 | 陳彥宏/<br>臺北護理健康大學資訊管理系副教授<br>(優先) | ・國立臺灣科技大學資通安全研究與教學中心研究團隊成員<br>・行政院科技會報辦公室 副研究員(2013.11~2016.9)，於 2016 年獲行政院公告褒獎<br>・德國柏林科技大學訪問學者(2012~2013) | 陳教授長期專精於網路安全、網路通訊協定等研究，並曾參與政府重要電信計畫，期透過訪談了解專業面之電信編碼觀點及我國電信編碼政策可執行之方向。 |
| 2 | 黃勝雄/<br>財團法人台灣網路資訊中心<br>執行長<br>(優先) | ・ICANN 根域中文標識生成委員會副主席<br>・IETF RFC3743 網際網路技術規範作者<br>・美國 PIR (.org Registry)註冊管理局 | 黃博士擔任 ICANN 重要幹部，並具 IETF 技術規範擬訂專業，期透過訪談了解國際上最新討論方向及 DNS 作為電信網路編碼之可行性。 |

| 項次 | 姓名/單位 | 資歷 | 訪談理由及目的 |
| --- | --- | --- | --- |
| | | 董事<br>· ICANN 新頂級域名 New gTLD 審查委員會委員<br>· ICANN 全球 IP 位址委員會副主席暨亞太區代表 | |
| 3 | 劉明翰/<br>友訊科技 IoT 策略事業群處長<br>(優先) | · IETF RFC 8585 技術標準主要作者 | 劉處長為業界人士，曾參與 IETF RFC 標準制定，期透過訪談了解 IETF 標準制定過程、實務上執行電信網路編碼之方式及我國電信編碼可執行方向。 |
| 4 | 林咨銘/<br>工業技術研究院技術經理<br>(備選 1) | · 3GPP RAN/SA 全體會議參與經驗<br>· 台灣資通產業標準協會(TAICS) TC1-WG1 組長 | 林博士曾參與 ITU 會議並長期觀測該組織重要討論議題，期透過訪談了解目前 ITU 在電信網路編碼最新資訊。 |
| 5 | 廖婉君/<br>臺灣大學電機工程系教授<br>(備選 2) | · 教育部 5G 行動寬頻人才培育計畫總顧問<br>· 5G/6G, AI, 物聯網, 區塊鏈技術專家 | 廖教授為 5G/6G 及物聯網專家，期透過訪談了解目前學界在電信網路編碼研究成果，以提供我國電信編碼可執行之方向。 |
| 6 | 蔡敦仁/<br>文化大學資工系教授 | · 經濟部標準技術委員會分組召集人（資訊安全、資訊軟體、通信 | 蔡教授具有通訊技術專業及標準制定經驗，期透過訪談了解目前學界在電信網路編碼標準 |

| 項次 | 姓名/單位 | 資歷 | 訪談理由及目的 |
| --- | --- | --- | --- |
| | (備選 3) | 技術等）<br>· 個資保護與資訊安全技術專家 | 制定之研究成果。 |
| 7 | 林盛琪/<br>是方電訊網路服務部資深經理<br>(備選 4) | · 台灣網路維運社群(TWNOG)多方利害關係人小組會議<br>· 070 網路電話技術專家 | 林經理為業界 IoT 人士，期從業界的角度提供實務上執行電信網路編碼方式。 |

## 四、 預期成果

有鑑於受訪者多具備電信號碼等通訊技術相關專業背景，部分曾參與我國政府通訊技術相關計畫，具有豐富之政策制定經驗，亦有參與國際上電信號碼相關活動或會議（如： ICANN、IETF 等）工作之經驗，故預期本次深度訪談應有以下成果：

(一)強化計畫技術研析能量，並使我國未來在擬議電信號碼相關政策時更能貼進國際發展趨勢，與國際接軌。

(二)促使本計畫專業人才在參與國際會議時，更能掌握電信號碼最新技術及討論方向，進而提升該等人員於國際組織內之重要性，增加其擔任重要工作或幹部之機會。

## 貳、第一場深度訪談會議紀錄

一、 訪談時間：2021 年 6 月 3 日(四)下午 5 時

二、 訪談對象：國立臺北護理健康大學資訊管理系陳彥宏副教授

三、 出席人員：

| 單位 | 姓名 | 職稱 |
|---|---|---|
| 國立臺北護理健康大學<br>資訊管理系 | 陳彥宏 | 副教授 |
| 財團法人電信技術中心 | 陳志宇 | 資深經理 |
| | 王彥中 | 研究員 |
| | 夏慧馨 | 助理研究員 |
| | 簡嘉儀 | 副管理師 |

四、 紀錄：簡嘉儀 (副管理師)

五、 討論事項：

| 題目 | 紀錄 |
|---|---|
| 「下世代電信網路號碼技術研析及管理」之研究方向及意義 | 1. B5G 因為網路切片改變了目前既有的通訊協定，5G 切片的目標是把整個異質網路整合在一起，但目前每個異質網路都有不同的編碼。<br>2. 目前不同的編碼有分成兩大類，第一類是 ITU 的電信網路陣營，透過 E.164 編碼規則，並使用 SIM 卡定址綁定設備。第二類的編碼是定址網路服務，區域網路是用 MAC Address、廣域網路是用 IP Address、電腦服務是用 Port Number，為了方便人類記憶也會用 DNS，這種語意位置使定址是有意義的。此外，若有 MAC Address、IP Address 和 Port Number 及 DNS，則可以做網路切片的定址。<br>3. 自主調適網路(例如 SDN)使號碼本身可以加密，因此我們可以看到兩個號碼陣營都有優勢和劣 |

| 題目 | 紀錄 |
| --- | --- |
| | 勢。ITU 的 E.164 跟 E.212 優勢是可以綁定設備，劣勢是號碼不能加密我且無法帶有意思訊息，並且無法跨其他異質網路；第二個 Domain Name 號碼陣營 IP Address 的優勢是號碼本身可以帶有意義，以及可以加密，但缺點就是無法綁定設備。<br>4. 號碼議題與我國的關係在於，我國不是 ITU 的會員國，因此無法加入 Telecom 陣營，而目前我國使用的國碼+886 只是當區的保留號，因此導致我國在電信上面是沒有辦法跟其他國家做共通共連的測試，所以才會出現在 ENUM( 6.8.8.e164.arpa) 的申請案被 ITU 否決之案例，原本在做 ENUM 是為了異質網路的互通，然而因為我國不屬於 ITU 會員國，因此該申請案未能通過。<br>5. 另一個研究方向是 IP/DNS，IP/DNS 主管機關不是聯合國，而是美國商務部，所以說我國較容易使用用臺灣名義或中華民國名義，參與 ICANN 活動，以利我國在參與及穩固 Datacom 號碼，我國無法參與 ITU 的情況下，至少能確保在 ICANN 組織的地位及角色。 |
| 國際 5G 物聯網號碼發展趨勢 | 1. ICANN 的技術主席表示，未來 ICANN 爭取網路切片編碼的主導權及使用 DNS 的編碼。<br>2. 5G 號碼案例如將中華郵政郵務車目前使用 Telecom 的編碼轉化成使用 DNS 的編碼，把原本使用 SIM 卡追蹤車輛的方式，轉為 Datacom 的方式。另外，建議透過目前在任的幹部或是未來接任的幹部，代表我國到 ICANN 倡議該號碼解決方案，以利我國在下世代電信網路發展上的技術含量。<br>3. 今年度若有一個模擬的場域，展現網路切片及設 |

| 題目 | 紀錄 |
| --- | --- |
| | 備(例如無人機)從 A 場域跨到 B 場域，以利強化本案的技術能量。<br>4. 網路切片(企業專網)是二維走向，X 軸是低客製化(公眾網路切片)到高客製化的通話，技術層部分有針對 Core network 的切片、針對網路協定的切片、頻寬的切片、天線的切片及 QoS 的切片，因此會產生企業專網屬於何種網路切片，因此網路切片間須要橫向及縱向間的協調，有些企業專網有 L3、L4、L5，而這個差別就會在企業專網切片的程度。<br>5. 未來若有公眾網路切片及企業專網切片間的互通互連問題，就必須先解決 Telecom 號碼及 Datacom 的號碼如何互連的技術問題。 |
| 網路互連間的資安問題 | 1. 網路切片互通互連間的號碼資安議題，因此建議分項二撰寫時，不要以技術研析的角度，而是要以政策制訂的角度切入；而從計畫面的角度是擬訂一個稽核分項三系統的資安稽核框架，系統是否有符合規範，因此分項二要將分項三當作一個 PoC 及案例分析的標的，以利未來資安稽核標準規範是可執行的。<br>2. 分項二不是一份技術報告，而是須有具體的政策產出。建議分項二在今年度產出，一資安稽核政策，且主要著重在切片及切片之間的號碼互連安全之資安稽核政策，另外產出資安稽核如何稽核分項三的方式及規劃。<br>3. 在 GSMA 網路切片互連區塊間可能都有號碼互連的議題，但可能隨著時間及技術的演進，與假設有所差異，建議研究團隊可以研究及分析相關議題。 |
| 5G 網路及網路切片技術 | 1. 4G 和 5G 最大的差異在於一根天線可收到各家電信業者的電波，此時由於裝置設備同時收到不同 |

| 題目 | 紀錄 |
| --- | --- |
| | 電信業者的訊號，因此應該有號碼電信資費的依據。<br>2. 未來低軌衛星可以用地面波的頻段從地面打下來，換言之設備裝置有可能收到從衛星傳輸的資料，及地面電信業者傳輸的資料，而設備裝置要如何收費，這也是與號碼議題相關須研析的部分。 |
| 下世代電信網路號碼驗證機制能力 | 1. 建議設計一個測試及實際情境。<br>2. 建議今年度的成果可以到 ICANN 展示，以展現我國具備下世代電信號碼及網路切片編碼的實力。 |

## 參、第二場深度訪談會議紀錄

一、 訪談對象：友訊科技 劉明翰技術長

二、 出席人員：

| 單位 | 姓名 | 職稱 |
|---|---|---|
| 友訊科技 | 劉明翰 | 處長 |
| 財團法人電信技術中心 | 卓卿敏 | 資深經理 |
| | 陳志宇 | 研究員代資深經理 |
| | 王彥中 | 研究員 |
| | 簡嘉儀 | 副管理師 |
| | 李昕甯 | 助理研究員 |
| | 彭俞蓉 | 助理研究員 |

三、 訪談日期：2021 年 8 月 17 日(二)上午 10 時至 12 時

四、 紀錄：簡嘉儀 (副管理師)

五、 討論事項：

| 題目 | 紀錄 |
|---|---|
| 隨著科技的快速發展與物聯網時代的來臨，下一波的連網設備將不再侷限於電腦與行動電話等智慧型手持裝置，機器與機器之間的通訊將成為常態，此外 ITU、3GPP R16/R17 等國際組織陸續針對 5G 技術提出相關技術文件及報告，在此趨勢下，我國物聯網實務應用及產業發展 | 1. 數位時代下，傳統電話號碼已不再被大眾記憶的識別符號，例如人們會透過 SIRI 找到聯絡人。基於這個背景之下，IPv6 及 DNS 在某程度可做到管理物聯網的功能。<br>2. 基本上自從有 IPHONE 及大量數位化之後，電話號碼不再是被大家記憶的東西，因此數位管理變得更為重要。<br>3. IPv6 從 RFC2460 發佈到現在，歷經了 20 年，整個過渡歷程仍相當緩慢。但幸好有 DNS 架構，可以有 AAAA record，換言之 IPv6 有 128 |

| 題目 | 紀錄 |
| --- | --- |
| 趨勢為何 | 個 bits，這個數量級上真正是靠後面的管理，而 DNS 資源也越來越少，因此不管事 E.164 的編碼還是 IP 的編碼，當進入物聯網的世界，當我們期待所有東西都能聯網，如何管理 DEVICE 勢必是未來討論的話題趨勢，要解決的問題是如何用統一有效的語言及具有識別性的管理，因此物聯網編碼勢必是未來討論的及趨勢。<br>4. IoE 或 IoT 的管理開始有越來越多的討論，討論的重點是使用一個有效及統一的編碼方式，以利物聯網管理。 |
| 對於電信級物聯網連接技術（如 LTE-M、NB-IoT 及未來 5G NR IoT 等）和非電信級物聯網裝置連線上網（使用 Bluetooth、LoRa、SigFox、Wi-Fi、ZigBee…等），使用 DNS 域名解析服務作為裝置身分管理（Identity Management）和端點管理機制/方案在國內的應用前景如何？以 DNS 為基礎的方案是否能作為下世代物聯網裝置編碼之解決方案？ | 1. 預估未來聯網裝置不管實體連接網路方式（Bluetooth、LoRa、SigFox、Wi-Fi、ZigBee…等）為何，目前只要是上網路，都可以支援 IPv6，例如可基於 ZigBee 的新 Protocol 名稱為 matter。Matter 跑在 IPv6 的網路上，然而 IPv6 在發展 20 年期間，如果沒有激勵情況下，轉換進程相當緩慢，目前統計上 IPv6 普及率大約 35%至 37%左右。而在下世代電信網路的物聯網 IP 化應該將成為趨勢，另一部分物聯網使用案例，例如 IIOT 等 Private IP，不一定會暴露在 Public IP。<br>2. 編碼與暴露在 Public IP 乍看下沒有太大的關聯性，然而當一個 Private IP 不用 Internet Routing 的情況下，IPv6 定義了 unique local address (簡稱，ULA)，雖然他當時設計出來不是作為 Private IP，但 IPv6 的 address 基本上都有 global unique address(簡稱，GUA)定 |

| 題目 | 紀錄 |
| --- | --- |
| | 址(除了 link local 外)。<br>3. 目前 IPv6 有網路位址轉換(Network Address Translation，簡稱，NAT)，但是 GUA 轉 GUA，並不是 GUA 轉非 GUA。<br>4. 從成本及技術導入觀察，DNS 是目前最適合做管理的編碼方式。 |
| 以工業物聯網（Industrial Internet of Things, IIoT）的智慧感測技術應用為例，其編碼需求與可用方案為何？未來是否有導入或建立具可互通性的數位物件架構（Digital Object Architecture, DOA）之必要？ | 從技術的角度來看，一定有必要，但整個來看還是 use case，但技術觀點來看是需要的，因為一開始沒有這個概念及沒有這個架構，之後才要建立這個架構會相對來說困難，對設備商及供應商來說都會是相當困難架構。 |
| 有關政府規劃推動在 IETF 下世代電信網路人才培育，是否有相關推動建議。 | 1. 台灣的產業形態是以硬體為主，Layer3 以上的產品相對來說是較於薄弱，而 IETF 比較偏向軟體的規格制訂。<br>2. IETF 參與應該由政府推動，而 IETF 技術性高，因此應該由產學合作的方式進行，以利鼓勵學生吸收及學習技術能量。<br>3. IETF 除了技術性高之外，但參與的門檻相對成本較低，並且該組織不具政治性，因為在 mailing lists 及網路上的討論即可，透過 mailing lists 參與可以獲取許多新技術。 |

## 肆、第三場深度訪談會議紀錄

一、 訪談時間：2021 年 6 月 30 日(三)下午 4 時

二、 訪談對象：財團法人台灣網路資訊中心 黃勝雄執行長

三、 出席人員：

| 單位 | 姓名 | 職稱 |
|---|---|---|
| 財團法人台灣網路資訊中心 | 黃勝雄 | 執行長 |
| 財團法人電信技術中心 | 陳志宇 | 資深經理 |
| | 王彥中 | 研究員 |
| | 彭俞蓉 | 助理研究員 |
| | 李昕甯 | 助理研究員 |
| | 夏慧馨 | 助理研究員 |
| | 柯盈池 | 工程師 |
| | 簡嘉儀 | 副管理師 |
| | 郭怡萱 | 助理管理師 |

四、 紀錄：郭怡萱 (助理管理師)

五、 討論事項：

| 題目 | 紀錄 |
|---|---|
| 本計畫是下世代網路電信網路號碼計畫，目前觀察國際 5G 物聯網趨勢都沒有在未來考慮到物聯網之相關議題，就您觀察，是否有其他的電信編碼機制之相關規範？ | 因為現在的假設是 Layer2 使用 E.164 的編碼方式。現在問題是如果說要進到 TCP/IP 或網際網路領域的時候，是否需要網際網路編碼，有些電信服務不需要經過網際網路編碼，若需要網際網路編碼，基本上現在發放的是 IPv6 的編碼。 |
| 目前其他的國家(美國、中國、歐盟)當中是否有針對 5G 物聯網號碼，在政策上的更新或技術上的研究？ | 物聯網是很多國家的政策重點，不管是技術、政策或制訂標準規範，所以研究團隊在蒐集其他國家的物聯網政策，包括頻率、編碼政策或未來應用的場域。 |

| 題目 | 紀錄 |
| --- | --- |
| 中國或俄羅斯在很早之前就有網路分裂議題，5G 的下世代電信技術的一個特性就是網路切片，網路切片會不會也造成另一種網路分裂的情況，ICANN 在這個議題上目前是否有新的研究或相關社群在討論這個議題？ | 基本上除非做電信的會討論相關議題，在網際網路領域很少會討論到網路切片造成網路分裂，因為可能性不大。舉例來說，因為網路切片是在營運商的管理網頁裡面去切，在可用的資源做更有效的使用，這個是屬於營運商內部的資源配置，從網際網路來看，基本上就是一樣的東西，無論切成幾個段落，對網際網路來說就是不同的載具。那你連接上來就是看你的分配的 IP 的區塊，決定你的路由，所以對網際網路說來講是沒有所謂切片造成的分裂問題。包括中國的防火長城或俄羅斯的網路獨立法，對網際網路來說影響都非常的有限。 |
| 在網際網路跟公眾電信網路互通的技術之下，是否有網路切片所造成的網路分裂的情況？ | 公共網路或是網際網路，在網際網路看的應是使用的編碼方式進到網際網路，如果不是用網際網路編碼方式，則是使用一個國家內部的網路，可能是公共、私有或企業網路。對網際網路來看，還是整個區塊來跟我鏈接。<br>所以接到網際網路區塊，就看 IP 的連接屬性路由 IP 的編碼方式。至於公共網路跟網際網路或網路切片會不會因為實體層分割造成分裂，基本上，會或不會從網際網路的角度是看不到的，因為分裂與否都是屬於同一個管轄或服務供應商去決定是否斷裂，可能基於 VPN 服務給特定專用專網使用，所以看起來專網只能從內部使用，不會與外面鏈接。對服務供應商來講他決定就是屬於內部用的網路。<br>因此無法連結不會把它視為網際網路分裂的一環，因為他本來就是屬於私有網路。 |
| 請問 CDN 的管理問題是否 | 部分的影響會比起剛剛所提的國家以管轄 |

| 題目 | 紀錄 |
| --- | --- |
| 造成網際分裂？ | 權的方式影響大，因為 CDN 跟網路的吻合密度非常高，假設現在網路所用的串流服務都是透過 CDN 提供，所以當 CDN 有問題的時候，對網際網路就會造成很大的衝擊。<br>舉例來說，2021 年 6 月 8 日有一個 CDN 的供應商斷線，全球網路包括美國、英國政府的官網、Twitter 的主要網站沒辦法接取，就是 CDN 的故障導致網路的斷裂。<br>再來 CDN 跟網路的路由，因為路由變成不是原先供應商設定的路由配置，所以確實 CDN 跟網際網路在公共治理領域上有衝突。至於會不會造成網際網路分裂，應該說是涵蓋在公共治理裡面，但是他的衝擊若發生狀況就會造成很大影響。從商業的角度，會盡他最大的能力讓商業穩定運作，但並不是屬於公共稽核的領域範圍，所以對網路治理來講是一個很大的一個缺口。 |
| 是否可預見 ICANN 或是網路治理領域未來會將 CDN 的管理問題造成的分裂議題列入討論或是解決此問題？ | 這個議題會列入討論但答案並不容易，因為這些 CDN 服務的提供者屬於私領域，沒有所謂的公共政策的參與機制，所以即便拿到 ICANN 或其他領域討論，基本上只能產出一些想法但是沒有辦法產出一些具體可執行的政策建議。 |
| 所以是否可以解釋目前已存的現象，CDN 在 protocol 方面還是會用到 TCP 或是單純的 IP protocol，因為他自己的獨特技術，會去改變原先預設好的路由。但在幾個使 | 目前的政策或規範，假設網路層跟傳輸層沒有違反，所以以目前的結構來看，從 IP 位址及 Domain Name 及 protocol 的政策完全無違反，所以完全符合網路治理的政策要求。<br>對 ICANN 來講，要介入會比較困難。因為這個問題會持續發酵，包括很多資安問題， |

| 題目 | 紀錄 |
| --- | --- |
| 用的條件下，是否存在既存違反的例如 ICANN 或是網路上既存的原則或規定？或是即使違反但無規範的空間？ | 過去也沒有涵蓋在網路治理範圍內，但若無法從源頭來解決，會衍伸很多資安的問題，基本上是頭痛醫頭腳痛醫腳。這些區塊來也慢慢都納進來。不過這個困難度還是蠻高的，因為畢竟不屬於公共領域範疇。 |
| 有關企業內部提供一個 DNS 或識別的管理，跨到網際網路上，目前本計畫的想法是需要用到既有網路 DNS 來做橋接。因為網路 DNS 是由一些組織，如 ICANN 來命名，如何在企業專網的命名跟網際網路的命名中間，有一個轉換或橋接？目前本計畫的實驗是採取營運商內部的認證欄位組成 DNS，像我們場域就是用 IMEI+基站位置+Follow 3GPP 標準的營運商識別碼，作為內部 IoT 的管理或識別，甚至寶 IoT 的 IP 併入 DNS 管理。但目前都是內部制定的規則，想請教若希望 IoT 達到跨域、上到網際網路或是 IoT 與 IoT 在網際網路的溝通，勢必需要網路上的 DNS 相互結合，請問在 ICANN 上是否針對 IoT 建立一個新的 gTLD。 | 如果說企業內部沒有對外解析，那就是企業內部處理；如果對外解析，就是透過網際網路的命名方式，是掛在什麼地方、在第幾層，那就到網際網路的 delegation 的架構做標示與編碼。假設需要跟網際網路鏈接，就在主結構上依照網際網路命名，不論是 gTLD、ccTLD，依照命名方式取得第二層、第三層授權，再接續往下發放。 |

| 題目 | 紀錄 |
| --- | --- |
| | |
| 關於 gTLD 在 2012 年首次發放期間也陸續受理跟核准將近 1 千多個頂級網域之後，目前有所謂在新一輪發放的討論，在今年一月份的時候有一個最終報告，以現況來說，進度是否已到 ICANN 的董事會，最後就是等到董事會通過之後才會去做新一輪的受理申請？ | 是的，目前計畫書已經送上去了，ICANN 董事會在確定之前需要做概念設計規劃，確定實務運作上可實施，之後董事會決議通過後，就會依著時程表進行。 |
| 剛剛有提到，有關政策制定過程中的規劃和架構的設計階段，是否會涉及 RFC 文件的制定？ | 要兼顧到很多需求，因為在概念技術設計部分需考慮發放出來的有哪些應該規避的原則或發放限制，必須把技術、政治、文化、地理區域或特定單位的限制排除。舉例來說，NIL 美國軍方用的頂級網域名稱就會限制使用，或是一些保留字或容易造成混淆的字就必須排除。<br>名稱是地理保護名稱，如 amazon 去申請.amazon，南美洲有 7 個國家認為 amazon 是他們的地理區域名稱，不可使用。這些概念設計的就必須把這些可能產生的衝突點逐一盤點，然後形成一個政策建議書。 |
| 有關區塊鏈議題，可能是依附在某個 gTLD 下面，是否存在內部 Domain 與外部 Domain 轉換的問題，或是區塊鏈的 Domain 可能帶有 | 如果提出來的是基於在某一個 gTLD，後面就會依照區塊鏈上所訂定的規範，做往下分配的設計。至於內部分配的機制是否對網際網路有影響，基本上不會有這方面的顧慮，一旦發放授權到某個地方，分散管理就交由註冊管理 |

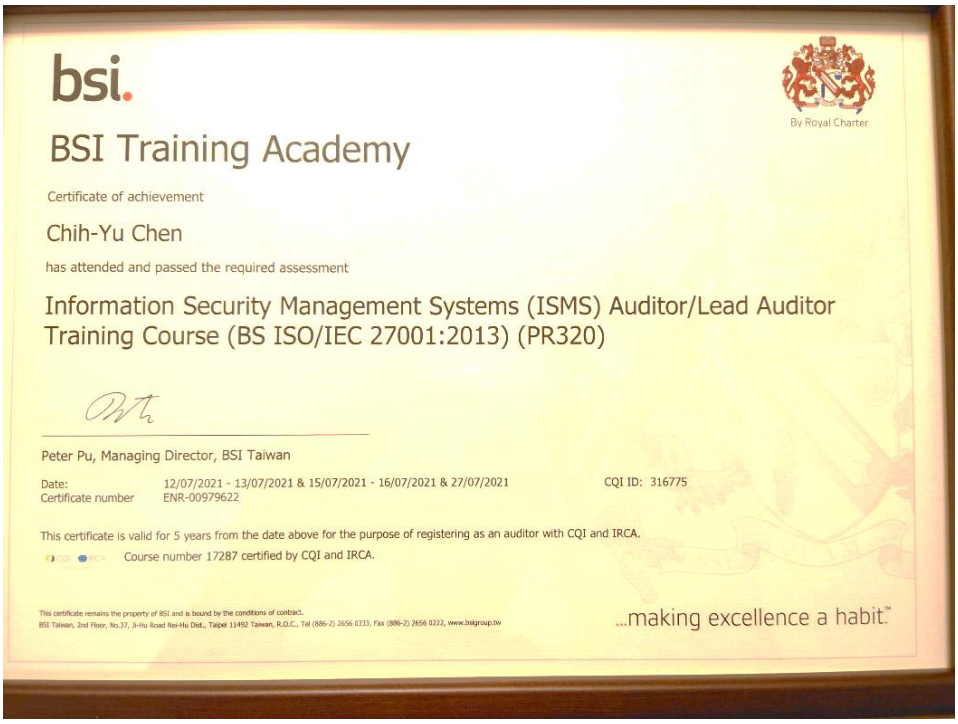
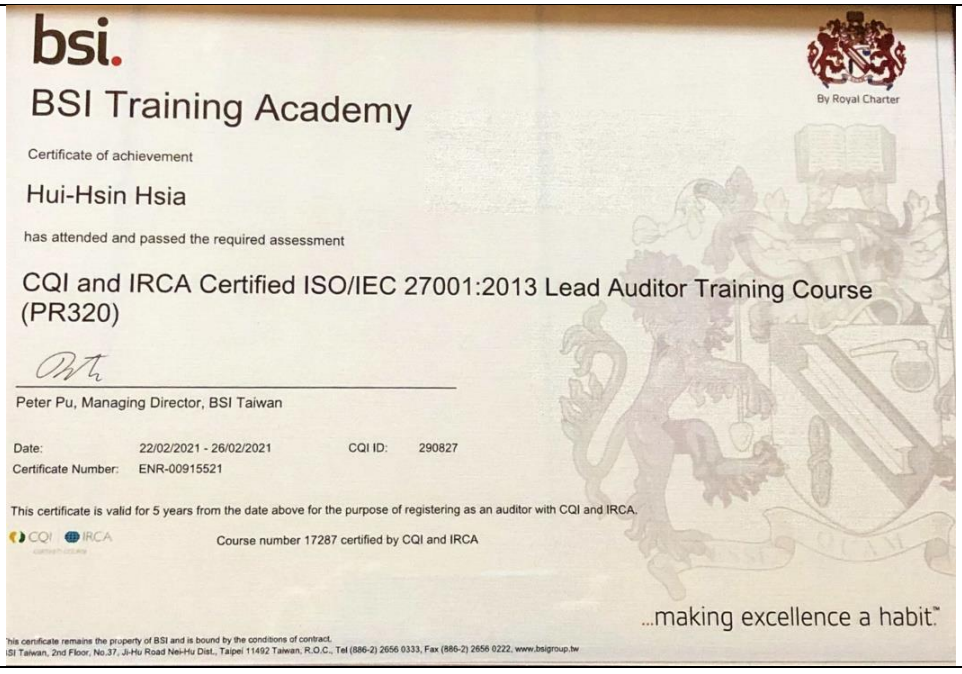
| 題目 | 紀錄 |
| --- | --- |
| 與資安疑慮相關的資訊，並把內部命名規則暴露在網際網路的相關憂慮？ | 局全權負責。 |
| TCP/IP 似乎有一點侷限性在於應用層或接取層的新發展。目前現象的討論，再往下一步來說，是否會漸進發展 TCP/IP 在網際網路有它存在的作用，或是有 non-IP 或 New IP 被提出？目前他們在設想一個下世代網路的應用情境，會提到例如全息投影等技術，需要更高傳輸及低延遲的功能需求，相關標準組織亦會界定現行 TCP/IP 的局限性或極限，是否已達到發展下一代新興應用服務的目的。 | TCP/IP 共存，並發展編碼或識別系統這個情況在現實已經發生，如區塊鏈、IoT、SDN 等，目前也有人提出用 DNS 取代 Router，用 URAL 做 Routing。從網際網路及 TCP/IP 核心社群看，就是在基礎上開發應用，屬於應用層的部分。<br>至於是否衝突，目前也有提出 IPv9 或其他 IP 編碼，所以你剛提到的這情況都有存在，也有直接衝突的，那就是輪到各個不同的市場去找他的區塊，所以有直接衝突的，也有往上面去堆疊。 |
| IETF 的 RFC 文件中， 除了網際網路標準，我們案子有一個實例，想要在行動網路去設計並追蹤管理物聯網，引用 DNS 的一個自動命名編碼的形式做有效的管理。在實作跟應用方面，是否適合把他描述或包裝成 Experimental RFC，並不一定指標準建立，而是將實作的東西在社群提出討論。 | 不論是 Experimental RFC 或是 Informational RFC，基本上，分類是最後一哩路在做的事。前面的第一哩路就是提出問題、是否提出 Chapter 都與您提的沒有關聯，當提出討論後，已經要變成國際標準的時候，才會進行協商或分類定義為 Experimental RFC 或是 BCP。<br>前置作業是提出議題、經過 RFC 後成立 Chapter、進行相關議題解決方案的討論，跟後面階段的類別沒有關係。本計畫最重要應該關注在議題本身，是否有足夠利害關係人引起共 |

| 題目 | 紀錄 |
| --- | --- |
| | 鳴並有足夠的支持人，因為議題內容決定是否該繼續討論。 |
| 參與 RFC 制定是一個長期的過程，就您的經驗，當時您參與 RFC 的過程，台灣部分參與的組成方式為何？ | 當初有學術界、財團法人、政府單位都有，最主要的有穩定的財源當然是最好，不過其實參與國際上的討論，情況變化非常大，且台灣、日本及韓國或 IETF 其他國家的情況都不一樣，每個人的背景也不一樣，無法說出哪個情況是最適合。<br>基本上，如果真正要在標準制定上有貢獻，我個人的看法是人數可能不是最主要的關鍵，而是對於議題的掌握程度及對議題的投入研究程度比較重要。這個跟研究一樣，如果這個根本就不是 IETF 偏好的研究議題，那就沒有意義，因為要解決的問題可能就完全不一樣。 |
| 各國參與 IETF 的年齡大概落在哪個區間？ | 年齡沒有依據國家有普遍不一致，綜整看 IETF 各國成員年紀都偏長。<br>IETF 很多參與者都是科技公司的 CTO 等級，對公司的技術產品或是網際網路架構都有一定程度的掌握，所以比較能夠了解議題對整個網際網路的重要程度。<br>所以 IETF 從過去到現在參與的人，年齡有逐漸老化現象，這也是一個問題。 |
| 本計畫其中一個重要目標就是培育可以擔任國際組織重要幹部的人才，誠如您剛剛所提到，如果擔任 Area | 政府的支持當然也很重要，但就我的觀點來看，另一個重點是培育人才亦應將每個人的生涯規劃列入考量，若培育參與國際組織的人才對其無生涯規劃上的幫助，基本上就找不到 |

| 題目 | 紀錄 |
| --- | --- |
| director 的話其實年齡都比較偏高且在技術面掌握度高。請問就您自己本身，在參與 ICANN 是否有短、中、長期規劃？或是過程中政府是否挹注支援來支持。 | 足夠的誘因鼓勵更多人參與。因為投入國際組織並非僅指為一個職位名稱而已，需要投入大量的時間及資源，若無個人的生涯規劃及興趣，很難達到效果。<br>所以在目標達成上，建議可以從較不顯著方面著手並逐漸深入組織，例如，假設參與 IETF 成本不高，可以多鼓勵人參與，將有效樣本數拉高；ICANN 方面，若有個人或組織與 ICANN 業務相關，如註冊管理局、受理註冊管理機關、智財權、法律學者等，找出與職涯相關領域切入，也是讓培育者更有動機做下去或是更深入發展的誘因。 |
| 若本計畫欲完成培育人才的目的，需要將重點放在篩選人才方面，如動機、職涯規劃是否吻合方面著手？ | 沒錯，因為參與國際組織會議是一個很大的成本，不可能培育一個無相關性的人才參與。舉個例子，ICANN 董事在面試時的第一個問題就是：你願意一個禮拜、一個月、一年，提供你 1/3 的時間參與 ICANN 的公共業務嗎？這個問題不僅是 ICANN，在任何一個網際網路領域的組織都是必答的題目。我相信個人投入的這些時間，應該不會有任何政府或商業機關替你負擔這些時間成本或轉換為薪資，所以個人動機及生涯規劃吻合很重要。 |

# 附件四、下世代電信網路號碼技術研析及管理資安稽核證照

# 壹、ISO/IEC 27001:2013 及 ISO/IEC 27701:2013 證照

| 證照資訊 | 佐證資料 |
| --- | --- |
| **ISO/IEC 27001:2013**<br>陳志宇資深經理 |  |
| **ISO/IEC 27001:2013**<br>夏慧馨助理研究員 |  |

| | |
|---|---|
| **ISO/IEC 27001:2013**<br>**張允亭助理研究員** | |

bsi.

By Royal Charter

BSI Training Academy

Certificate of achievement

Yun-Ting Chang

has attended and passed the required assessment

CQI and IRCA Certified ISO/IEC 27001:2013 Lead Auditor Training Course (PR320)

Peter Pu, Managing Director, BSI Taiwan

Date: 22/02/2021 - 26/02/2021 CQI ID: 290861

Certificate Number: ENR-00934806

Issue Date: 06/04/2021

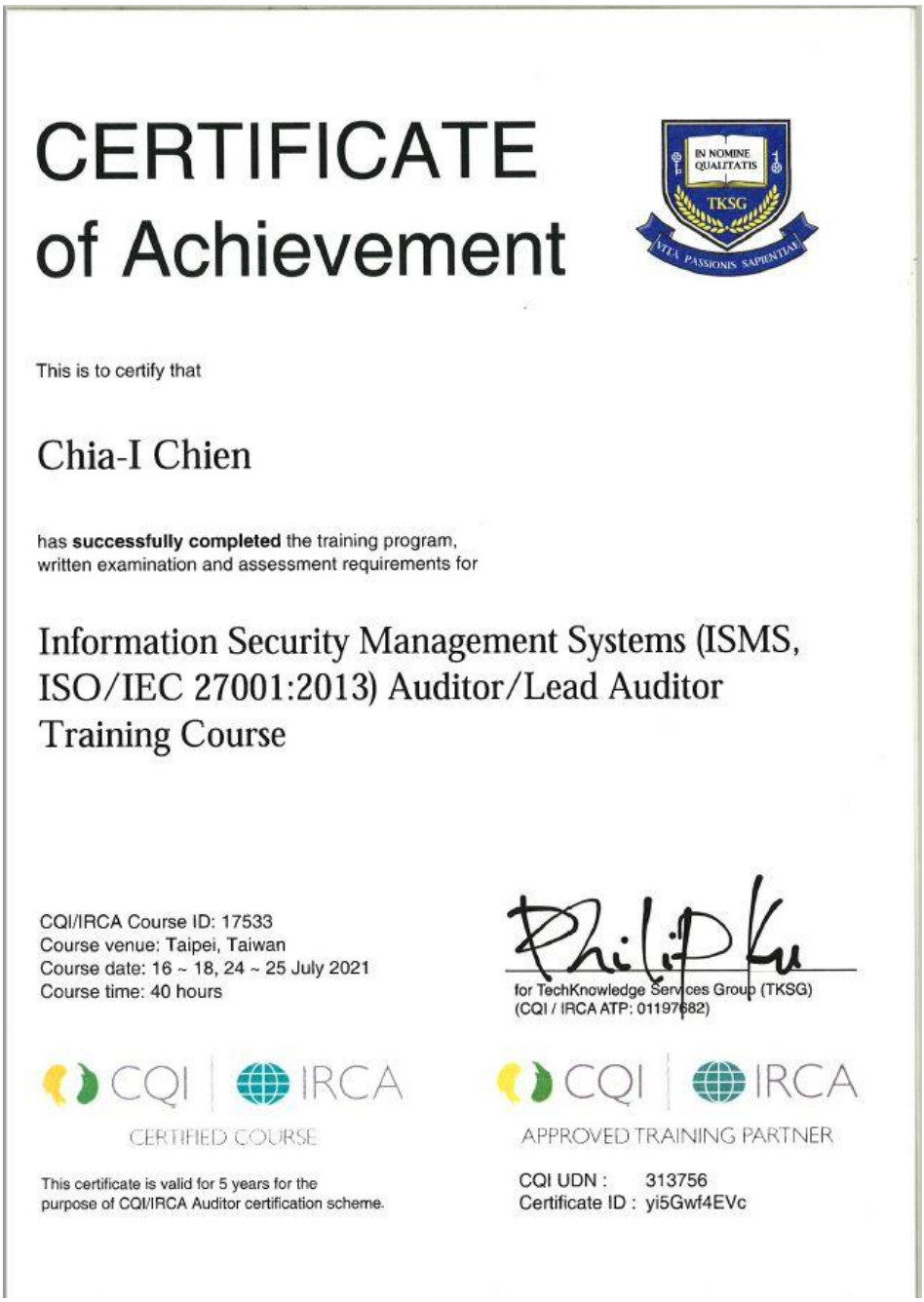
This certificate is valid for 5 years from the date above for the purpose of registering as an auditor with CQI and IRCA.

Course number 17287 certified by CQI and IRCA

...making excelle

This certificate remains the property of BSI and is bound by the conditions of contract.
BSI Taiwan, 2nd Floor, No.37, Ji-Hu Road Nei-Hu Dist., Taipei 11492 Taiwan, R.O.C., Tel (886-2) 2656 0333, Fax (886-2) 2656 0222, www.bsigroup.tw

**ISO/IEC 27001:2013**
**簡嘉儀副管理師**



# CERTIFICATE of Achievement

This is to certify that

Chia-I Chien

has **successfully completed** the training program, written examination and assessment requirements for

Information Security Management Systems (ISMS, ISO/IEC 27001:2013) Auditor/Lead Auditor Training Course

CQI/IRCA Course ID: 17533
Course venue: Taipei, Taiwan
Course date: 16 ~ 18, 24 ~ 25 July 2021
Course time: 40 hours

for TechKnowledge Services Group (TKSG)
(CQI / IRCA ATP: 01197682)

CQI | IRCA
CERTIFIED COURSE

This certificate is valid for 5 years for the purpose of CQI/IRCA Auditor certification scheme.

CQI | IRCA
APPROVED TRAINING PARTNER

CQI UDN : 313756
Certificate ID : yi5Gwf4EVc

**ISO/IEC 27701:2013**
**夏慧馨助理研究員**

# CERTIFICATE of Achievement

This is to certify that

## HUI HSIN HSIA

has **successfully completed** the training program, written examination and assessment requirements for

ISO/IEC 27001:2013 Extension to ISO/IEC 27701:2019 Lead Auditor (PIMS, Privacy Information Management System) Training Course

Course ID: 886_27701_2021
Course venue: Taipei, Taiwan
Course date: 27 September ~ 01 October 2021
Course time: 40 hours

for TechKnowledge Services Group (TKSG)
(CQI / IRCA ATP: 01197682)

Certificate ID : YOcG4DGH7d

# 附件五、下世代電信網路號碼驗證機制測試計畫暨測試報告書

## 壹、實測驗證平臺架構說明

依據本案場域邏輯示意圖以及功能需求，擬定本平臺之整體架構規劃，架構說明如下：

- 邊緣運算層：採用一臺 Amarisoft Classic Callbox 設備模擬 5G 核心網路,以及兩臺凌華 MECS-6110 伺服器安裝 Edge DNS Server 與 DNS 編碼程式，分別為 DNS_1 與 DNS_2。
- Edge DNS Server：安裝於兩臺凌華 MECS-6110 伺服器上，分別為 DNS_1 與 DNS_2。
- 無線接取層：Amarisoft Classic Callbox 5G 核心網路模擬設備提供 3 個符合 3GPP gNB 規範的 5G 基站天線（Cells），做為無線接取層。3 個 Cells 劃分為 2 個 Domain，Cell_1 與 Cell_2 屬於 Doamin_1，Cell_3 屬於 Domain_2。
- IoT 設備：提供五組 IoT 設備，四組終端設備由一臺凌華 MXE-211-M2G IoT device 與一臺 DTA1164W 5G SA/NSA Gateway 所組成。IoT device(IoT_1、IoT_2、IoT_3、IoT_4)分別透過 ethernet Cat6 銅纜與 5G Gateway 介接，由 5G Gaetway(5GW_1、5GW_2、5GW_3、5GW_4)分配動態 IP。5G Gateway 均安裝 5G SIM 卡連至 Amarisoft Classic Callbox。一組終端設備由一臺凌華 MXE-211-M2G IoT device 與一臺 APAL TRIBUTO 5G Dongle 所組成
- DNS 編碼管理：客製自動化組成 DNS 編碼程式，安裝於 DNS_1 與 DNS_2。

一、 軟硬體設備規劃

本案規劃軟硬體清單如表 1 及表 2。

表 1、硬體設備清單

| 項次 | 設備功能 | 廠牌 | 型號 | 數量 | PoC 實測驗證平臺之架構部署關係說明 |
|---|---|---|---|---|---|
| 1 | 伺服器 | 凌華科技股份有限公司 | MECS-6110 | 3 臺 | 兩臺伺服器運用於多重接取邊緣運算層，一臺伺服器運用於系統管理 |
| 2 | IoT 裝置 | 凌華科技股份有限公司 | MXE-211-M2G | 4 臺 | 終端設備 |
| 3 | 網路交換器 | HPE Aruba | Aruba 2930F | 1 臺 | 於多重接取邊緣運算層裡作連接三臺 MEC 伺服器之用 |
| 4 | 5G 核心網路模擬設備 | Amarisoft | Amarisoft Classic Callbox | 1 臺 | gNB Based 5G R15 SA 模擬器，無線接取層及 5G 核心網路 |
| 5 | 5G 閘道器 | 新漢股份有限公司 | DTA1164W/5G SA/NSA Gateway | 4 臺 | 終端設備之 5G 無線模組 |
| 6 | 5G 行動網卡 | 皇鋒通訊股份有限公司 | APAL TRIBUTO 5G Dongle | 1 個 | 終端設備之 5G 無線模組 |

表 2、軟體清單

| 項次 | 軟體名稱 | 功能說明 | 數量 |
|---|---|---|---|
| 1 | Edge DNS Server 系統軟體 | DNS 安裝與設定 | 2 套 |
| 2 | DNS 編碼程式 | 自動生成與 5G UE 對應 DNS A/AAAA Record | 2 套 |
| 3 | Dashboard | 場域展示用網站，顯示各設備狀態與展示運作流程 | 1 套 |

| 項次 | 軟體名稱 | 功能說明 | 數量 |
|---|---|---|---|
| 4 | Radius 資料傳送 | 將 UE 設備註冊資料，傳送到 DNS | 1 套 |
| 5 | MEC 伺服器系統軟體 | 1. Ubuntu<br>2. PostgreSQL<br>3. Nginx | 1 式 |

二、 系統設計

實測驗證平臺包含有 5 組 IoT 設備（包含 IoT 設備、5G Gateway 及 5G Dongle）、一臺 5G 模擬器與三臺伺服器（包含兩臺 DNS 與一臺 Dashboard）。其中三臺伺服器的作業系統與所需要的執行軟體環境架構如圖 1。

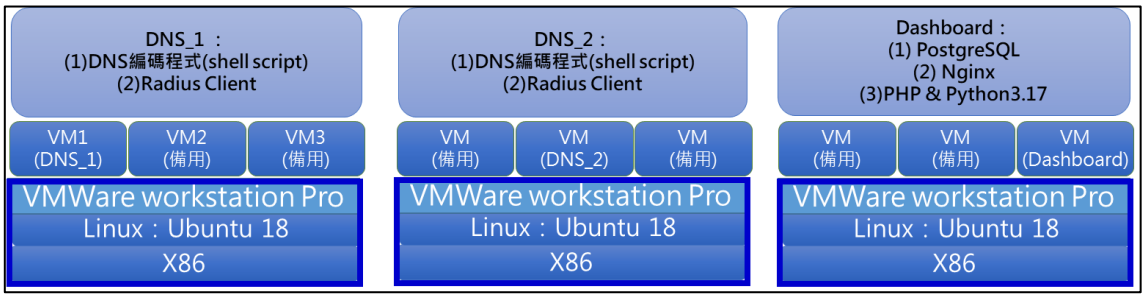



圖 1、MEC 伺服器軟體系統架構

三、 客製化軟體功能

本案開發四個客製化軟體，包括(1) Edge DNS Server 系統軟體(2) DNS 編碼程式(3) Dashboard 與(4)Radius 資料傳送。當 UE 註冊時，Radius 資料傳送模組會將註冊資訊傳送到 Edge DNS Server，DNS 編碼程式會進行解析，並將 IP 以及域名資訊寫到 DNS 上，最後 Dashboard 會到 DNS 上擷取資訊，並採用圖形化介面呈現。

## 貳、實測驗證平臺之驗證情境說明

- 情境一：由 IoT 設備連結至 5G 閘道器（5G Gateway）之情形。以凌華 MXE-211-M2G 設備與 DTA1164W 5G SA/NSA Gateway 組成 IoT 設備，場域中共有四組 IoT 設備，依序編號 IoT_1、IoT_2、IoT_3、IoT_4，如圖 2。

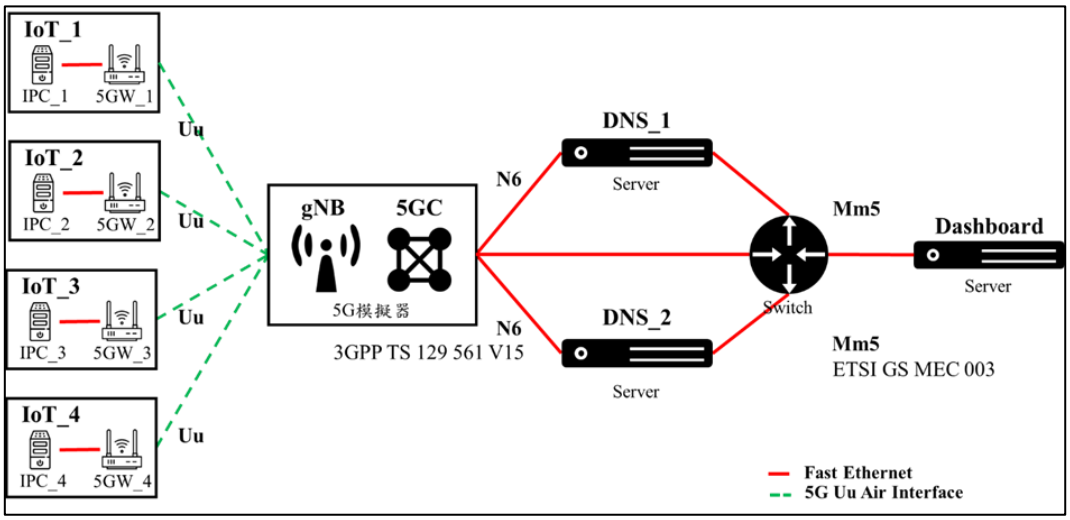



圖 2、實測驗證平臺實體架構示意圖(情境一：以 5G Gateway 連線)

- 情境二：由 IoT 設備安裝 5G 行動網卡（5G Dongle）連網之情形。以凌華 MXE-211-M2G 設備安裝 APAL 5G Dongle 組成一組 IoT 設備，加上以凌華 MXE-211-M2G 設備與 DTA1164W 5G SA/NSA Gateway 組成三組 IoT 設備，依序編號為 IoT_1、IoT_2、IoT_3、IoT_5，如圖 3。

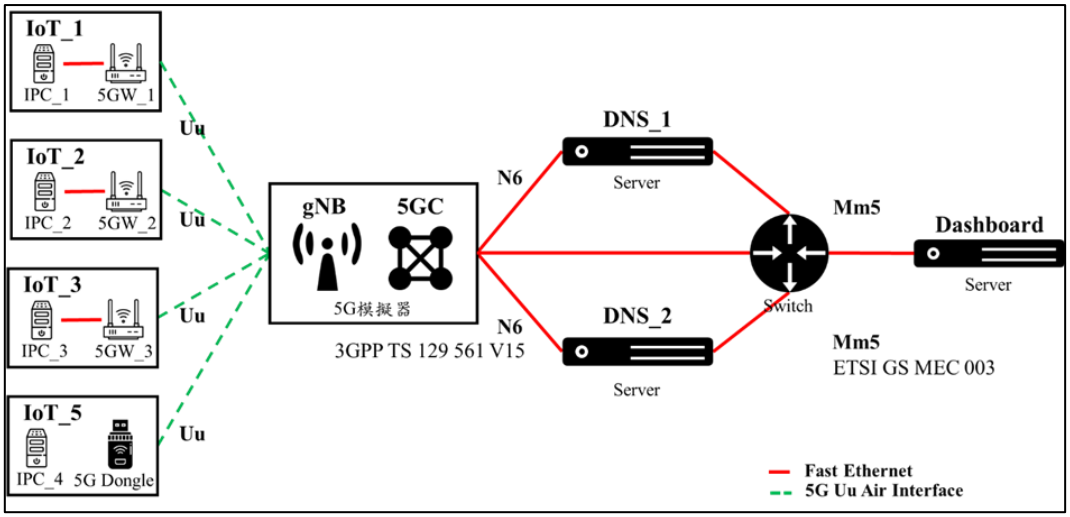



圖 3、實測驗證平臺實體架構示意圖(情境二：以 5G Dongle 連線)

當 IoT 設備連線到 Amarisoft Classic Callbox 進行註冊時，Callbox 會依照 IoT 設備裡 IMSI 與 DNN 設定配發 IP 位址給 IoT 設備，同時會依照 3GPP TS 29.0611定義，透過 Radius 協議將 DNN(Data Network Name，在 3GPP Release15 中，APN 已經以 DNN 名稱取代2)、Cell ID、IMSI、MSISDN、IMEI、IP、SST 等資料，依據 Domain 傳給 DNS_1 或 DNS_2。DNS 收到資料後動生成 A Record，編碼格式如下：

[IMEI.Cell_ID.Domain_ID.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org]

(依 ITU-T 標準，mnc001.mcc999 供測試使用)

在 Callbox 中設定，將 IoT 設備連線到不同的 Cell_ID 重新註冊，用來模擬 IoT 設備在場域中移動的情境。DNS Server 上亦會動態更改 A Record，並與其他 Domain 上的 DNS Server 交換更新 FQDN 資訊，達到同一個 IoT 設備在網路間的互相通訊與辨識，自動配置與管理專網號碼(DN)，功能邏輯架構圖如圖 4 所示。

[1] BIND 9 Security Considerations，P1，2020，https：//bind9.readthedocs.io/en/v9_16_4/security.html

[2] Digital cellular telecommunications system (Phase 2+) (GSM);Universal Mobile Telecommunications System (UMTS);Numbering, addressing and identification(3GPP TS 23.003 version 15.4.0 Release 15)，P37，2018/07，https：//www.etsi.org/deliver/etsi_ts/123000_123099/123003/15.04.00_60/ts_123003v150400p.pdf

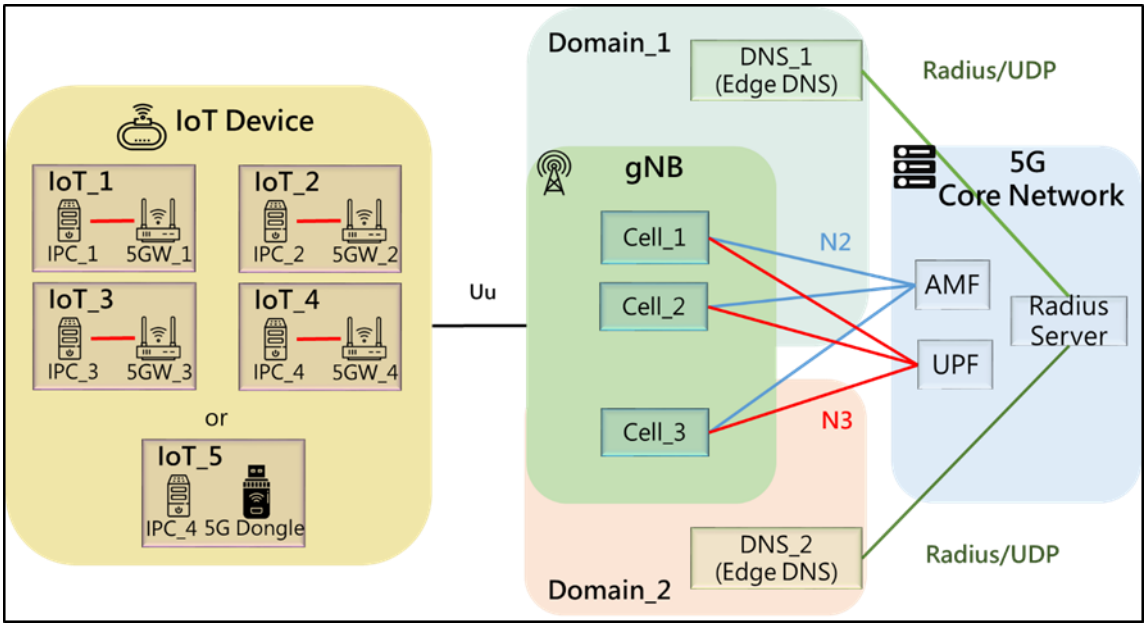

IoT Device
IoT_1
IPC_1
5GW_1
IoT_2
IPC_2
5GW_2
IoT_3
IPC_3
5GW_3
IoT_4
IPC_4
5GW_4
or
IoT_5
IPC_4 5G Dongle
Uu
Domain_1
DNS_1
(Edge DNS)
Radius/UDP
gNB
Cell_1
Cell_2
Cell_3
N2
N3
5G
Core Network
AMF
UPF
Radius
Server
DNS_2
(Edge DNS)
Radius/UDP
Domain_2

圖 4、功能(邏輯)架構圖

# 參、測試使用工具說明

## 一、 Wireshark

Wireshark 輔助工具提供完整的過濾器和統計分析的功能，其操作介面如下圖 5 分成幾個主要的部份，包括最上方的功能表和各種工具列、網路封包的清單、封包的標頭和封包的內容，並且以不同的顏色來代表各種不同的通訊協定或是過濾條件。這樣的設計讓使用者在擷取網路封包的過程中，就能夠即時瞭解目前網路上所傳送的網路封包類型。由於 Wireshark 可以解析超過七百種的通訊協定，因此幾乎所有協定都能夠解碼，就算將來有新的通訊協定推出，也會因為其採用開放原始碼的授權方式。

在網路封包清單中，可以針對不同的網路通訊協定或過濾規則指定顏色，這種設計方式可以協助使用者快速辨識各種不同通訊協定，或是過濾規則符合目前網路流量的情況，能夠更直覺地進行後續處理。

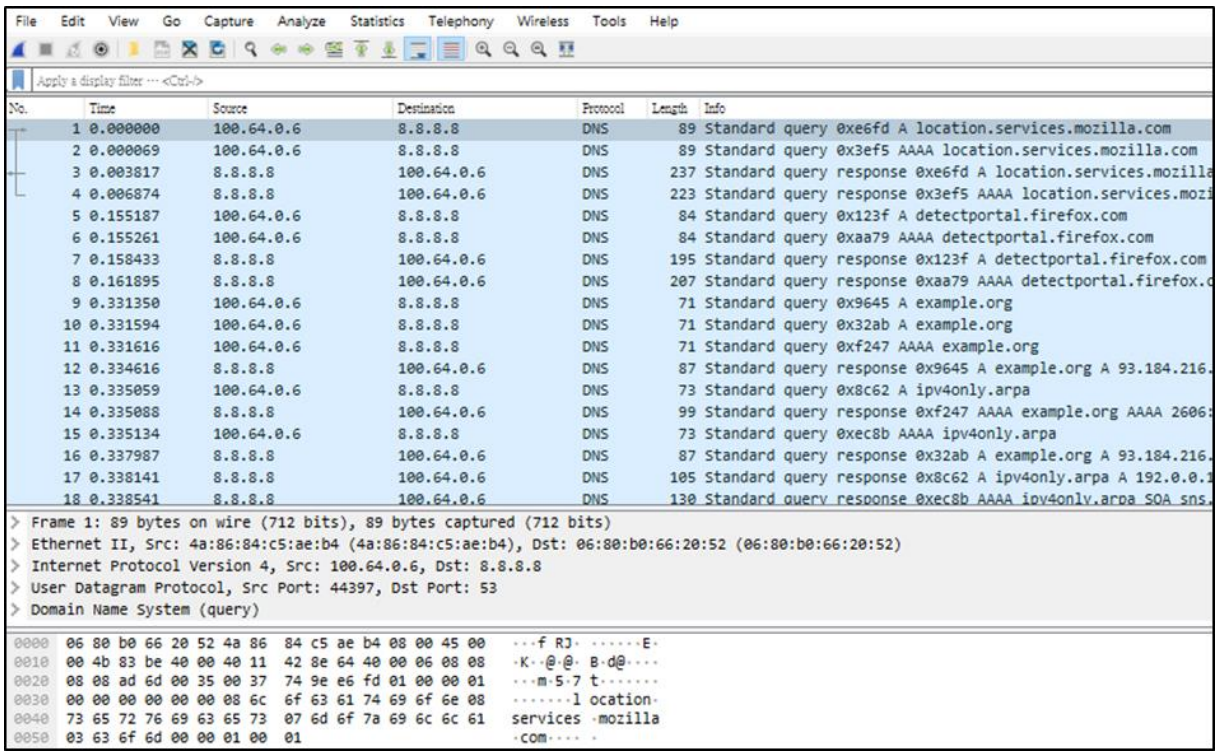



圖 5、Wireshark 封包圖

## 二、 Iperf

Iperf 輔助工具是一個 TCP/IP 和 UDP/IP 的性能測量工具，能夠提供網路吞吐率信息，以及震動、丟包率、最大段和最大傳輸單元大小等統計信息；從而能夠幫助我們測試網路性能，定位網路瓶頸。

通用參數如下說明，輸出圖如圖 6：

- -f [k|m|K|M] 分別表示以 Kbits, Mbits, KBytes, MBytes 顯示報告，預設以 Mbits 為單位
- -i sec 以秒為單位顯示報告間隔
- -l 緩衝區大小，預設是 8KB
- -m 顯示 tcp 最大 mtu 值
- -o 將報告和錯誤信息輸出到檔案
- -p 指定服務器端使用的端口或客戶端所連接的端口
- -u 使用 udp 協議
- -w 指定 TCP 窗口大小，預設是 8KB
- -B 綁定一個主機地址或通訊埠
- -C 兼容舊版本
- -M 設定 TCP 資料封包的最大 mtu 值
- -N 設定 TCP 不延時
- -V 傳輸 ipv6 資料封包

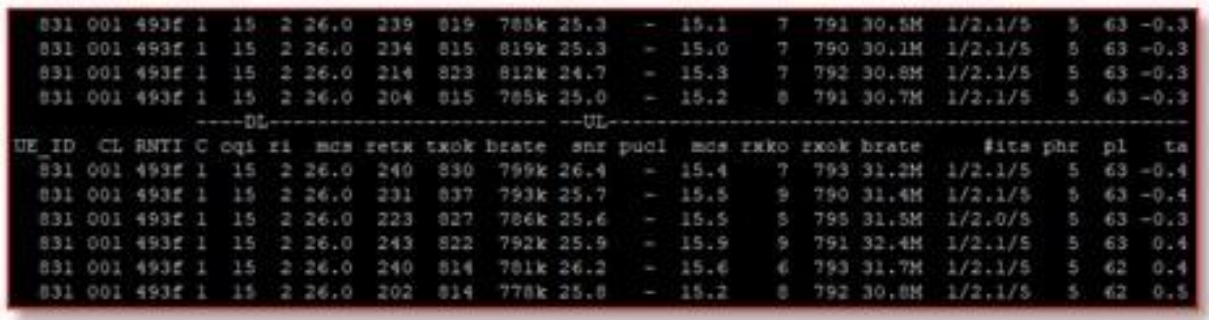



圖 6、Iperf 輸出圖

三、 Ping

Ping 輔助工具是用來測試封包能否透過 IP 協定到達特定主機。Ping 的運作原理是向目標主機傳出一個 ICMP 的請求回顯封包，並等待接收回顯回應封包。程式會按時間和成功回應的次數估算遺失封包率（丟包率）和封包往返時間（網路時延，Round-trip delay time）。使用方式如下：

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
[-4] [-6] target_name

表 3、Ping 命令集表

| 命令集 | 敘述 |
|---|---|
| -t | Ping 指定的主機，直到停止。 |
| | 若要查看統計資料並繼續，請按 Control-Break; |
| | 若要停止，請按 Control-C。 |
| -a | 將位址解析為主機名稱。 |
| -n count | 要傳送的回應要求數目。 |
| -l size | 傳送緩衝區大小。 |
| -f | 在封包中設定 Don't Fragment 旗標 (僅 IPv4)。 |
| -i TTL | 存留時間。 |
| -v TOS | 服務類型 (僅 IPv4。此設定已過時，而且對 IP 標頭中的 服務類型欄位沒有影響)。 |
| -r count | 紀錄路由以供計算躍點 (僅 IPv4)。 |
| -s count | 供計算躍點的時間戳記 (僅 IPv4)。 |
| -j host-list | 鬆散的主機清單的來源路由 (僅 IPv4)。 |
| -k host-list | 嚴格的主機清單來源路由(僅 IPv4)。 |
| -w timeout | 每個回覆的等候逾時 (單位為毫秒)。 |
| -R | 也使用路由標頭測試反向路由 (僅 IPv6)。 |
| | 根據 RFC 5095，已不再使用此路由標頭。如果使用此標頭， |

| 命令集 | 敘述 |
| --- | --- |
| | 某些系統可能會捨棄回應要求。 |
| -S srcaddr | 要使用的來源位址。 |
| -c compartment | 路由區間識別碼。 |
| -p | 對 Hyper-V 網路虛擬化提供者位址執行 Ping。 |
| -4 | 強制使用 IPv4。 |
| -6 | 強制使用 IPv6。 |

圖 7、Ping 操作圖

# 肆、單元測試計畫

一、 MEC Server

表 4、凌華 MECS-6110 單元測試

| 受測設備 ： 凌華 MECS-6110 | | |
|---|---|---|
| 項次 | 測試內容 | 操作方式 |
| 1 | 硬體配備<br>CPU 為 D-2177NT 或同等級以上 | 實機操作顯示相關資訊 |
| 2 | 系統記憶體 128G(含)以上 | 實機操作顯示相關資訊 |
| 3 | 硬碟 2.5" SATA 5400RPM 1T HDD*1 | 實機操作顯示相關資訊 |
| 4 | 100/1000BASE-T Ethernet port 2 個(含)以上 | 實機操作顯示相關資訊 |
| 5 | 安裝 Ubuntu 15.04 或以上版本與 VMware Workstation 16 Pro 單機版或以上版本 | 實機操作顯示相關資訊 |

二、 IoT 裝置

表 5、凌華 MXE-211-M2G 單元測試

| 受測設備 ： 凌華 MXE-211-M2G | | |
|---|---|---|
| 項次 | 測試內容 | 操作方式 |
| 1 | CPU 為 Intel E3950 或同等級以上 | 實機操作顯示相關資訊 |
| 2 | 系統記憶體 2GB(含)以上 | 實機操作顯示相關資訊 |
| 3 | 100/1000BASE-T Ethernet port 2 個(含)以上 | 實機操作顯示相關資訊 |
| 4 | USB PORT 1 個(含)以上 for 無線網路接取之用 | 實機操作顯示相關資訊 |
| 5 | USB PORT 2 個(含)以上 for PoS 環境感測情境展示應用。 | 實機操作顯示相關資訊 |

| 受測設備 ： 凌華 MXE-211-M2G | | |
|---|---|---|
| 項次 | 測試內容 | 操作方式 |
| 6 | 安裝 Ubuntu 15.04 或以上版 | 實機操作顯示相關資訊 |
| 7 | 支援可配置 IP 網段版本：IPv4、IPv4v6、IPv6 | 實機操作顯示相關資訊 |

三、 網路交換器

表 6、Aruba 2930F 單元測試

| 受測設備 ： Aruba 2930F 24G PoE+ 4SFP+ Swch | | |
|---|---|---|
| 項次 | 測試內容 | 操作方式 |
| 1 | 具備 24 埠 10/100/1000 Base-T Ethernet 界面及 4 個 1/10G SFP/SFP+ 介面，UTP 介面具備 Auto MDI/MDI-X。 | 實機操作與書面審查 |
| 2 | 具備 PoE 及 PoE+功能，最高可提供 370W 供電效能。 | 實機操作與書面審查 |
| 3 | 提供 IPv6 Host 管理功能、Dual Stack (IPv4/IPv6)。 | 實機操作，顯示相關設定 |
| 4 | 具備 IPv4 路由協定設定，包括 Static Route、RIPv1/RIPv2、OSPF。 | 實機操作，顯示相關設定 |
| 5 | 具備 IPv6 Layer 3 靜態路由與動態路由 RIPng、OSPF v3。 | 實機操作，顯示相關設定 |
| 6 | 提供 DHCP Server 功能。 | 實機操作,顯示相 7 關設定 |
| 7 | 具備頻寬限制(Rate Limiting)功能，可依據 Per-Port ingress 配置 | 實機操作，顯示相關設定 |
| 8 | 具備 NTP/SNTP 網路校時功能 | 實機操作，顯示相關設定 |
| 9 | 具備 STP BPDU Port Protection 保護機制。 | 實機操作，顯示相關設定 |
| 10 | 具備 SNMPv1/v2c/v3 管理功能 | 實機操作，顯示相關設定 |

四、 5G 核心網路模擬設備

表 7、Amarisoft Classic Callbox 單元測試

| 受測設備 ： Amarisoft Classic Callbox | | |
|---|---|---|
| 項次 | 測試內容 | 操作方式 |
| 1 | LTE eNB 功能是否能正常啟動及連線 | 實機操作 |
| 2 | EPC 功能是否能正常啟動及連線 | 實機操作 |
| 3 | 5G gNB 功能是否能正常啟動及連線 | 實機操作 |
| 4 | 模擬設備是否可以模擬 3 個 5G cells | 實機操作 |
| 5 | 5G 5GC 是否支援註冊認證 | 實機操作 |
| 6 | 是否支援分配 IP 網段版本：IPv4 | 實機操作 |
| 7 | 是否支援分配 IP 網段版本：IPv4v6 | 實機操作 |
| 8 | 是否支援分配 IP 網段版本：IPv6 | 實機操作 |

五、 5G 無線接入設備

表 8、DTA1164W 單元測試

| 受測設備 ： DTA1164W 5G SA/NSA Gateway | | |
|---|---|---|
| 項次 | 測試內容 | 操作方式 |
| 1 | 是否具備 2 個 1GbE RJ45 cooper ports 且可正常運作 | 實機操作 |
| 2 | 是否支援 5G SA (3GPP Release 15) 架構 | 實機操作與書面說明 |
| 3 | 是否支援 5G NSA (3GPP Release 15) 架構 | 實機操作與書面說明 |
| 4 | 是否支援分配 IP 網段版本：IPv4 | 實機操作 |
| 5 | 是否支援分配 IP 網段版本：IPv4v6 | 實機操作 |
| 6 | 是否支援分配 IP 網段版本：IPv6 | 實機操作 |

# 伍、單元測試結果

## 一、 MEC Server

### (一)測試項目

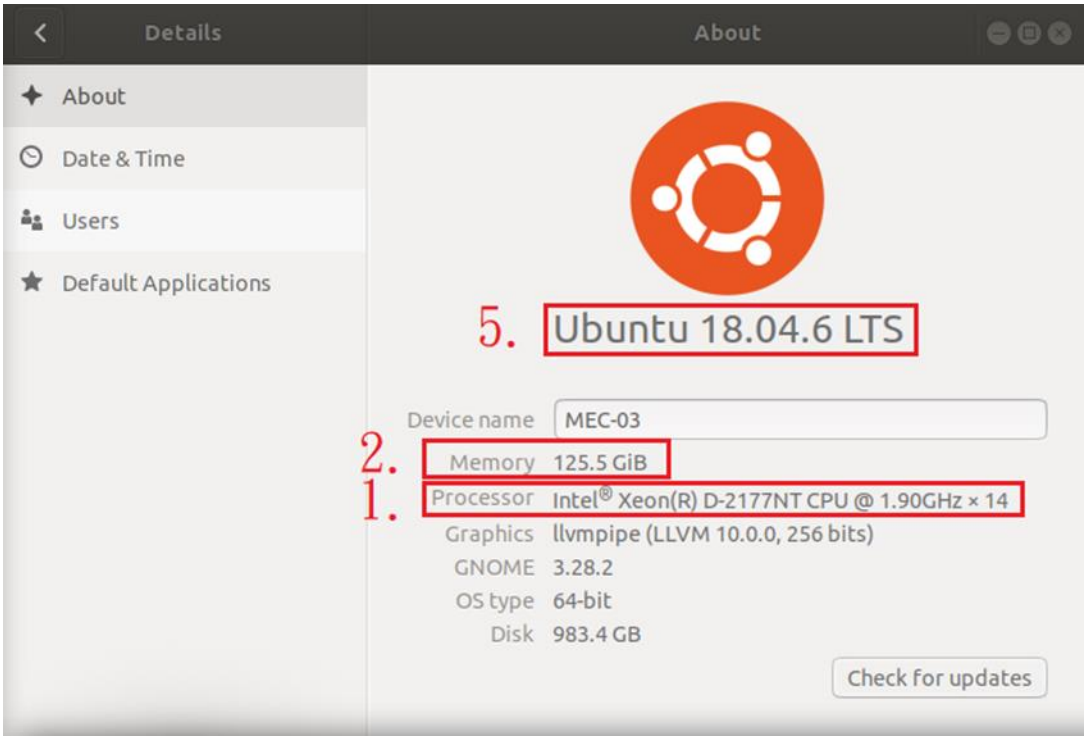
表 9、凌華 MECS-6110 單元測試

| 受測設備 ： 凌華 MECS-6110 | | | |
|---|---|---|---|
| 項次 | 測試內容 | 操作方式 | 是否符合 |
| 1 | 硬體配備 CPU 為 D-2177NT 或同等級以上 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 2 | 系統記憶體 128G(含)以上 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 3 | 硬碟 2.5" SATA 5400RPM 1T HDD*1 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 4 | 100/1000BASE-T Ethernet port 2 個(含)以上 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 5 | 安裝 Ubuntu 15.04 或以上版本與 VMware Workstation 16 Pro 單機版或以上版本 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |

(二)佐證內容(文件說明或實機操作畫面)

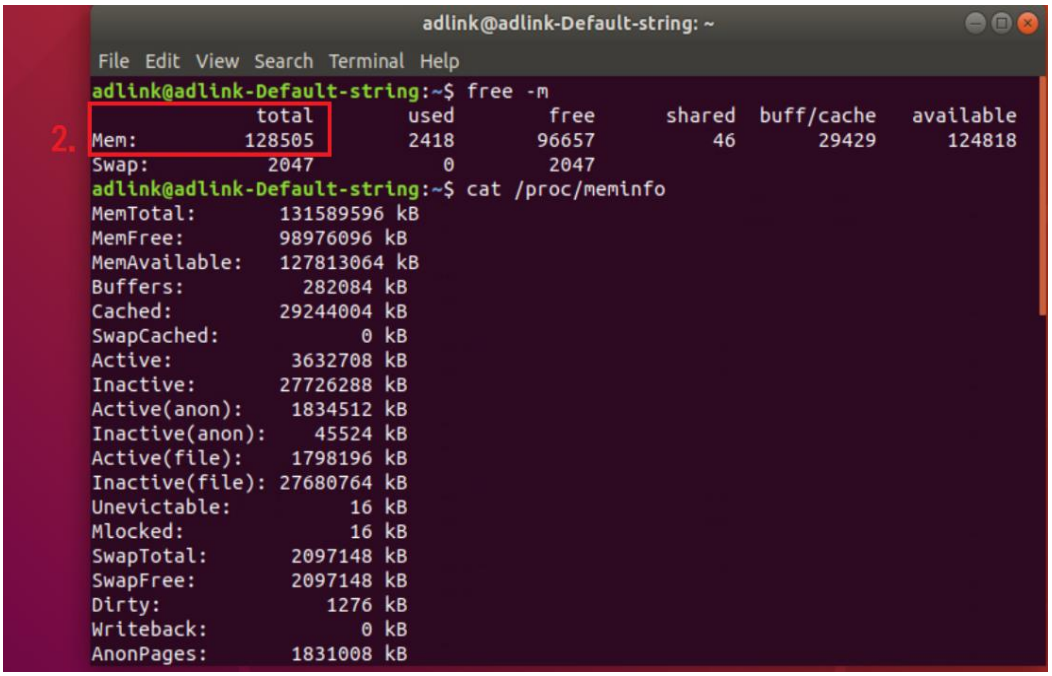
- 項次 1：硬體配備 CPU 為 D-2177NT 或同等級以上

  實機操作：顯示 CPU 為 D-2177NT。



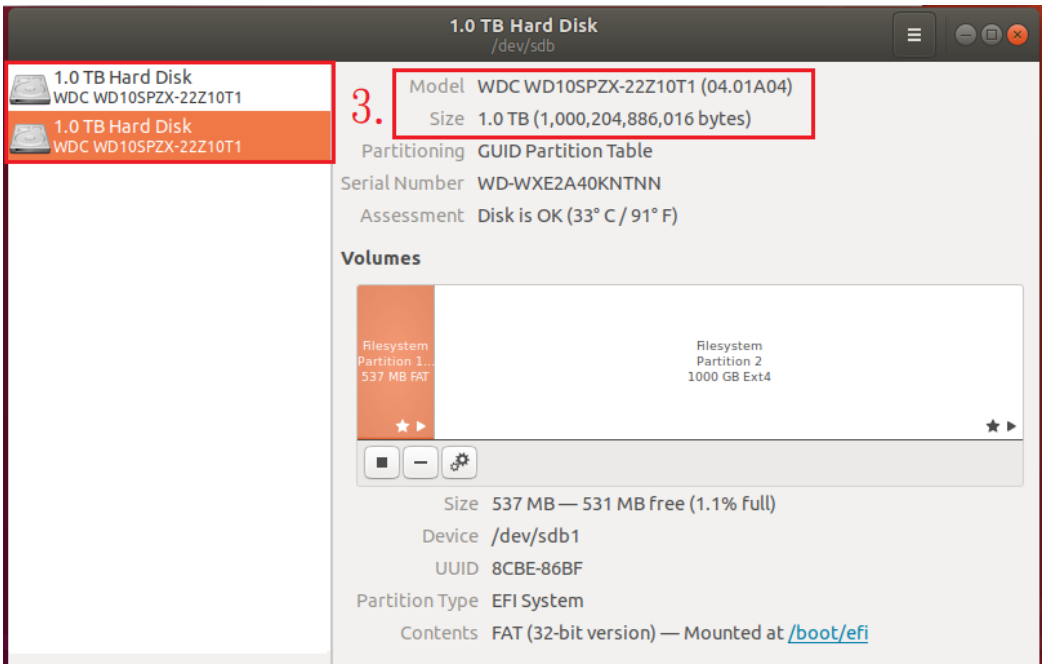

- 項次 2： 系統記憶體 128G(含)以上

  實機操作：顯示系統記憶體 128G(含)以上。



➢ 項次 3： 硬碟 2.5" SATA 5400RPM 1T HDD*1

實機操作步驟 1：顯示硬碟為 1TB。




實機操作步驟 2：書面佐證資料，顯示硬碟 2.5" SATA 5400RPM。

Western Digital WD Blue™ 2.5 吋 HDD

產品簡介

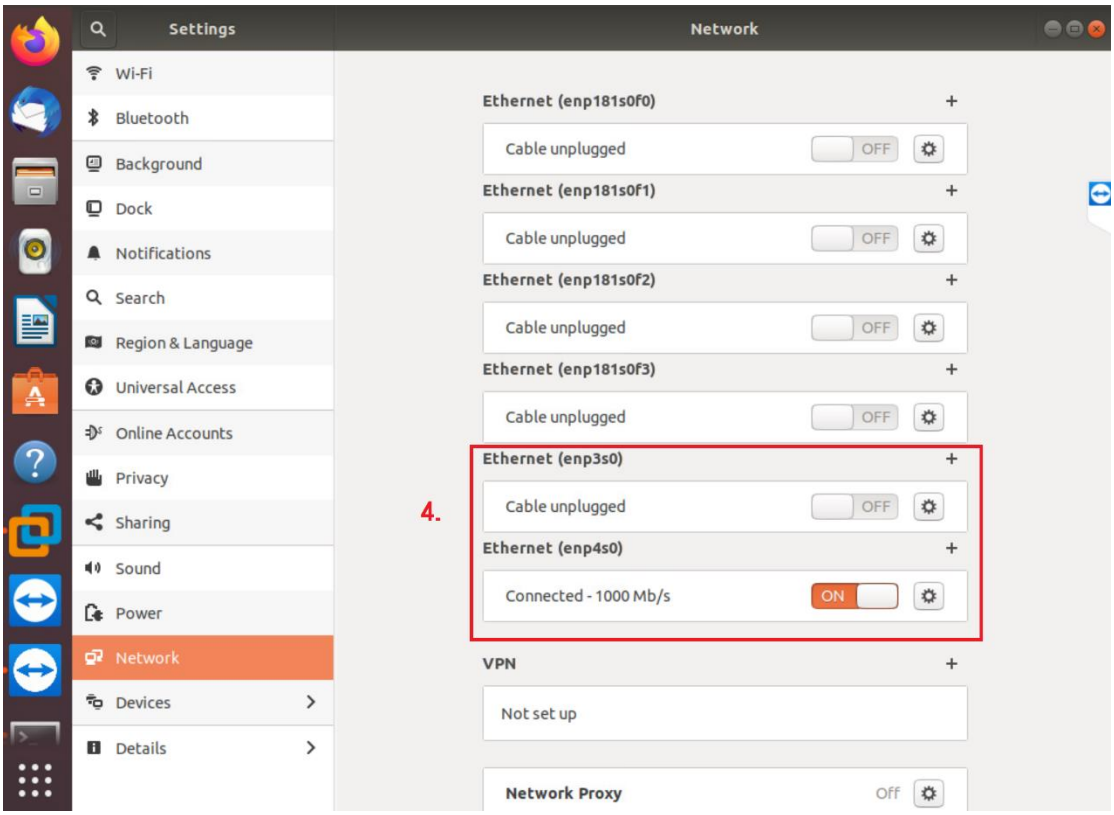
規格

3.

| | 2TB | 1TB | 500GB | 500GB | 320GB | 320GB |
|---|---|---|---|---|---|---|
| 型號[2] | WD20SPZX | WD10SPZX | WD5000LPCX | WD5000LPVX<br>WD5000LQVX[9] | WD3200LPCX | WD3200LPVX |
| 錄製技術[10] | SMR | SMR | CMR | CMR | CMR | CMR |
| 格式化容量[1] | 2TB | 1TB | 500 GB | 500 GB | 320 GB | 320 GB |
| 外型規格 | 2.5 吋 | 2.5 吋 | 2.5 吋 | 2.5 吋 | 2.5 吋 | 2.5 吋 |
| 先進格式化（AF） | 是 | 是 | 是 | 是 | 是 | 是 |
| 符合 RoHS 的規範[3] | 是 | 是 | 是 | 是 | 是 | 是 |
| **效能** | | | | | | |
| 資料傳輸速率（最高）[1]<br>介面速度 | 6 Gb/s | 6 Gb/s | 6 Gb/s | 6 Gb/s | 6 Gb/s | 6 Gb/s |
| 快取記憶體 (MB)1 | 128 | 128 | 16 | 8 | 16 | 8 |
| 效能等級 | 5400 RPM | 5400 RPM | 5400 RPM | 5400 RPM | 5400 RPM | 5400 RPM |
| 平均磁碟機就緒時間（秒） | 3.5 | 2.8 | 2.8 | 2.8 | 2.8 | 2.8 |
| **可靠性/資料完整性** | | | | | | |
| 載入/載出循環次數[4] | 600,000 | 600,000 | 600,000 | 600,000 | 600,000 | 600,000 |
| 每位元讀取發生無法復原的讀取錯誤 | <1/10[14] | <1/10[14] | <1/10[14] | <1/10[14] | <1/10[14] | <1/10[14] |
| 有限保固年限[5] | 2 | 2 | 2 | 2 | 2 | 2 |

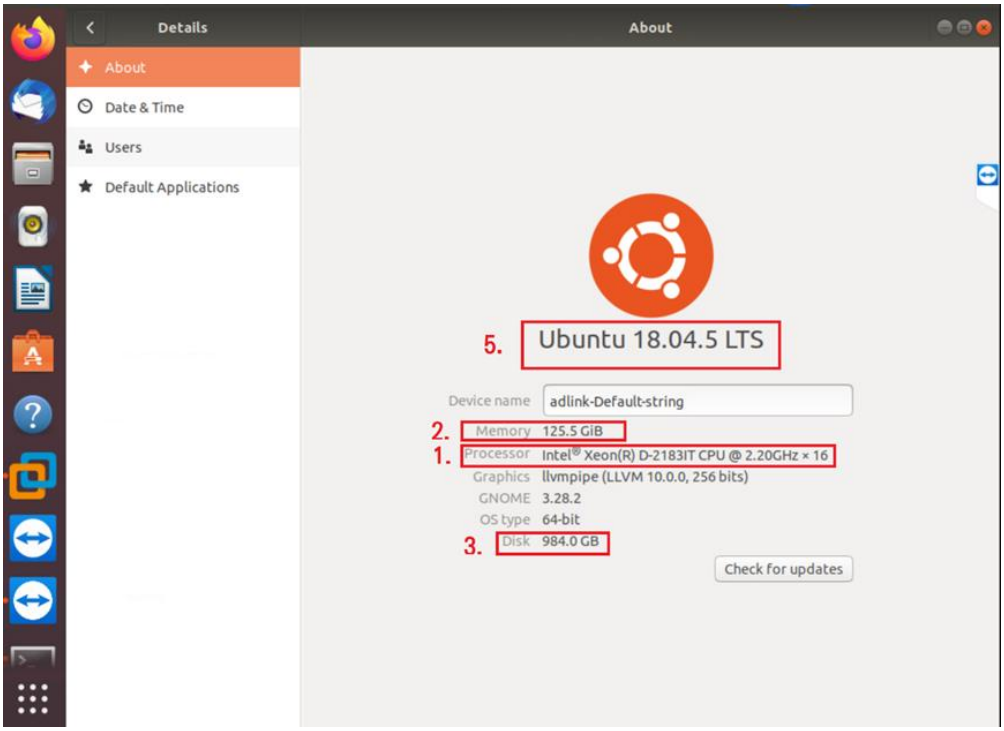
- 項次 4： 100/1000BASE-T Ethernet port 2 個(含)以上

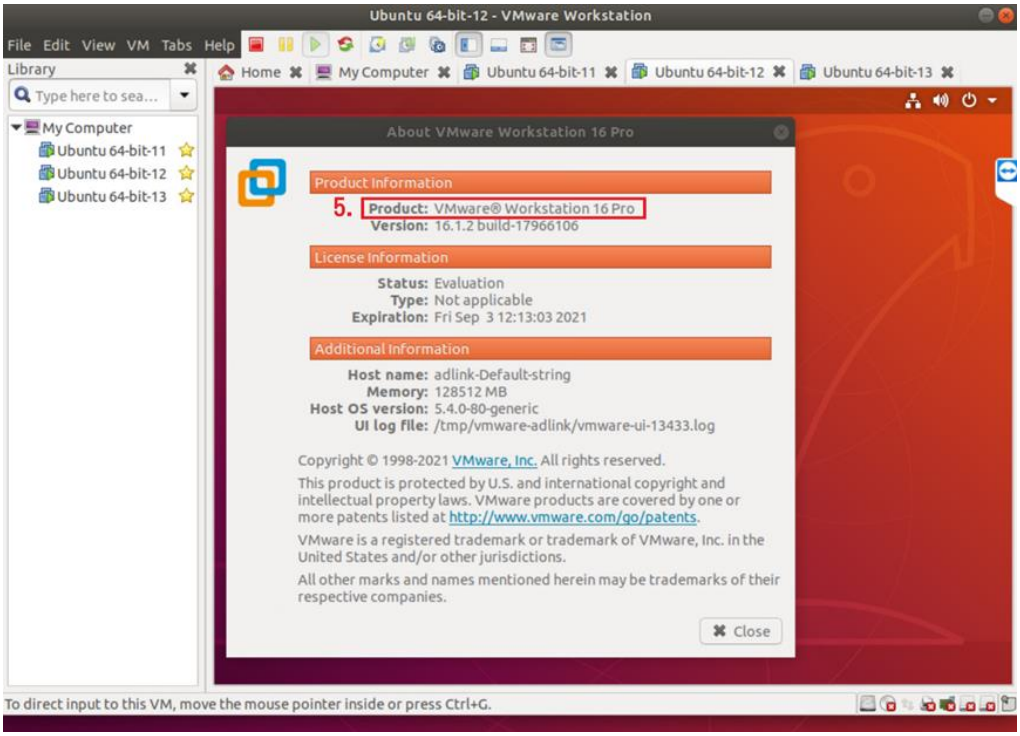
  實機操作：顯示乙太網路介面。



- 項次 5：安裝 Ubuntu 15.04 或以上版本與 VMware Workstation 16 Pro 單機版或以上版本

  實機操作：顯示安裝 Ubuntu15.04 以上版本與 VMware Workstation 16 Pro。



## 二、 IoT 裝置

### (一)測試項目

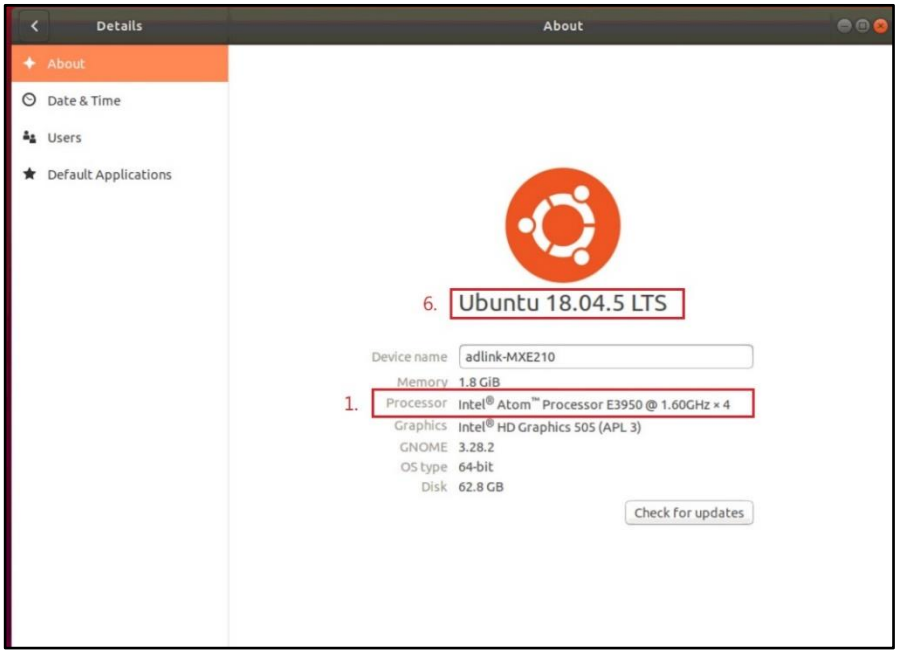
表 10、凌華 MXE-211-M2G 單元測試

| 受測設備 ： 凌華 MXE-211-M2G | | | |
|---|---|---|---|
| 項次 | 測試內容 | 操作方式 | 是否符合 |
| 1 | CPU 為 Intel E3950 或同等級以上 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 2 | 系統記憶體 2GB(含)以上 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 3 | 100/1000BASE-T Ethernet port 2 個(含)以上 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 4 | USB PORT 1 個(含)以上 for 無線網路接取之用 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 5 | USB PORT 2 個(含)以上 for PoS 環境感測情境展示應用。 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 6 | 安裝 Ubuntu 15.04 或以上版本 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |
| 7 | 支援可配置 IP 網段版本：IPv4、IPv4v6、IPv6 | 實機操作顯示相關資訊 | ■符合<br>□不符合 |

(二)佐證內容(文件說明或實機操作畫面)

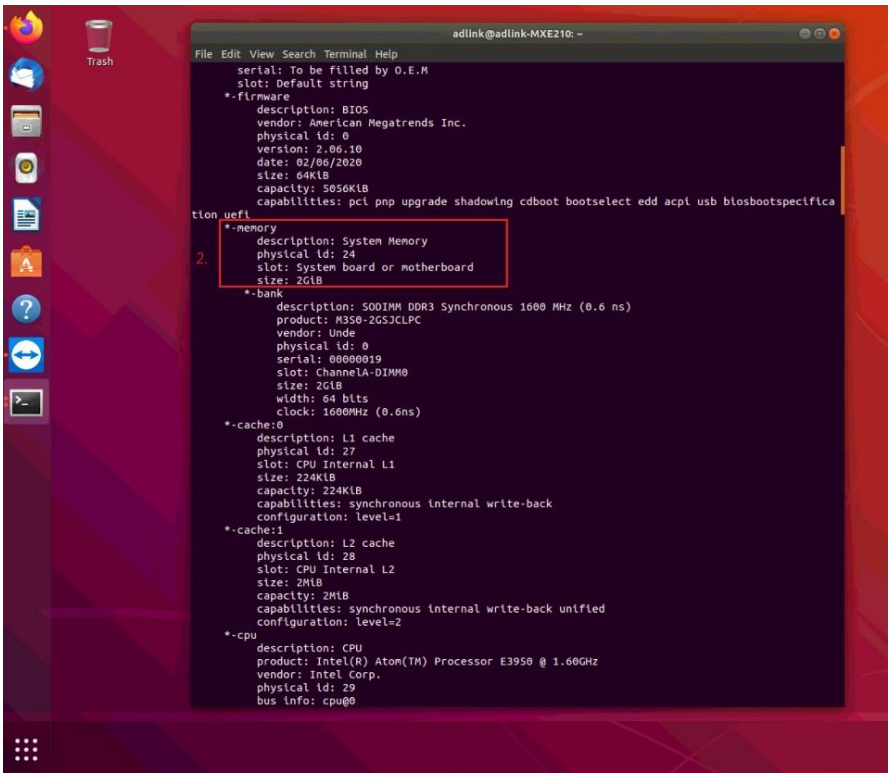
- 項次 1：CPU 為 Intel E3950 或同等級以上

  實機操作：顯示 CPU 為 Intel E3950。



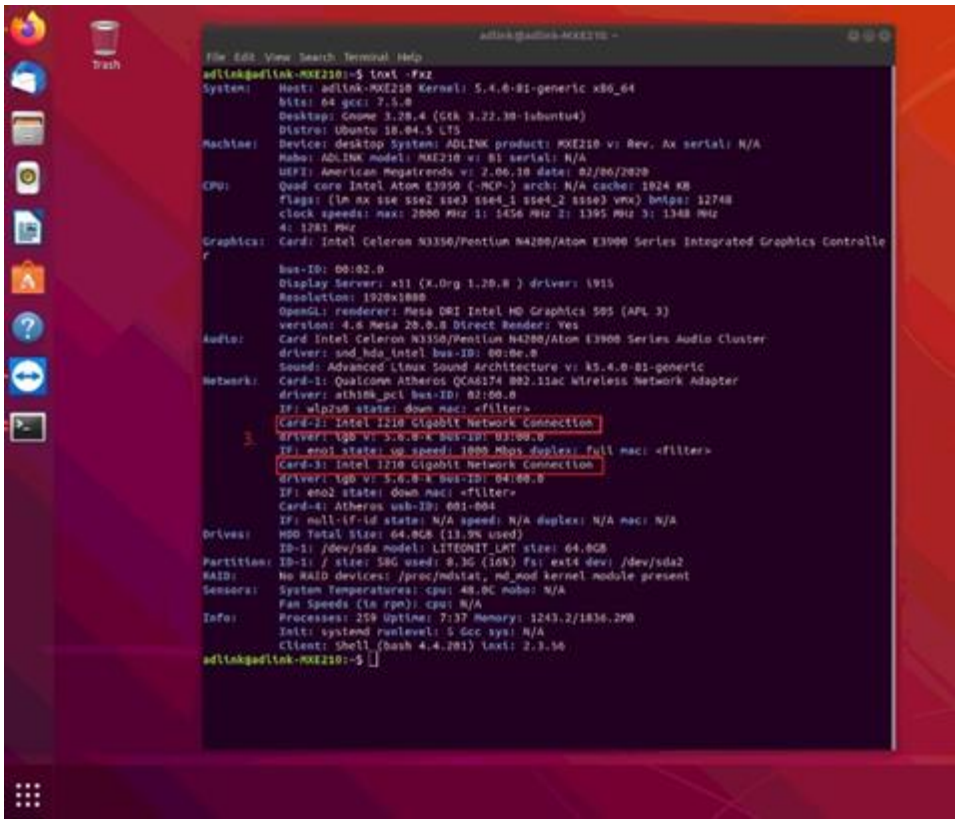

- 項次 2：系統記憶體 2GB(含)以上

  實機操作：顯示系統記憶體 2GB。



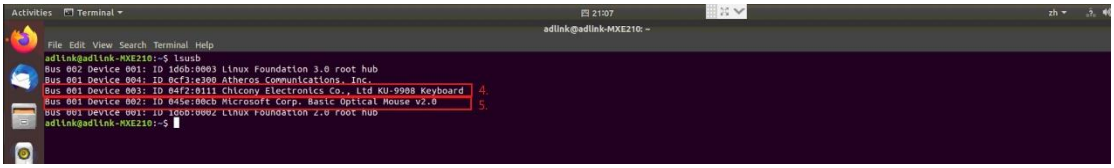
- 項次 3： 100/1000BASE-T Ethernet port 2 個(含)以上

  實機操作：顯示兩個 100/1000BASE-T Ethernet port。



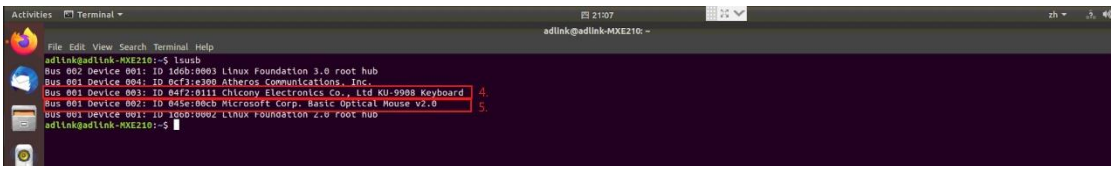

- 項次 4： USB PORT 1 個(含)以上 for 無線網路接取之用

  實機操作：顯示 USB PORT，2 個 USB 2.0、2 個 USB 3.0。



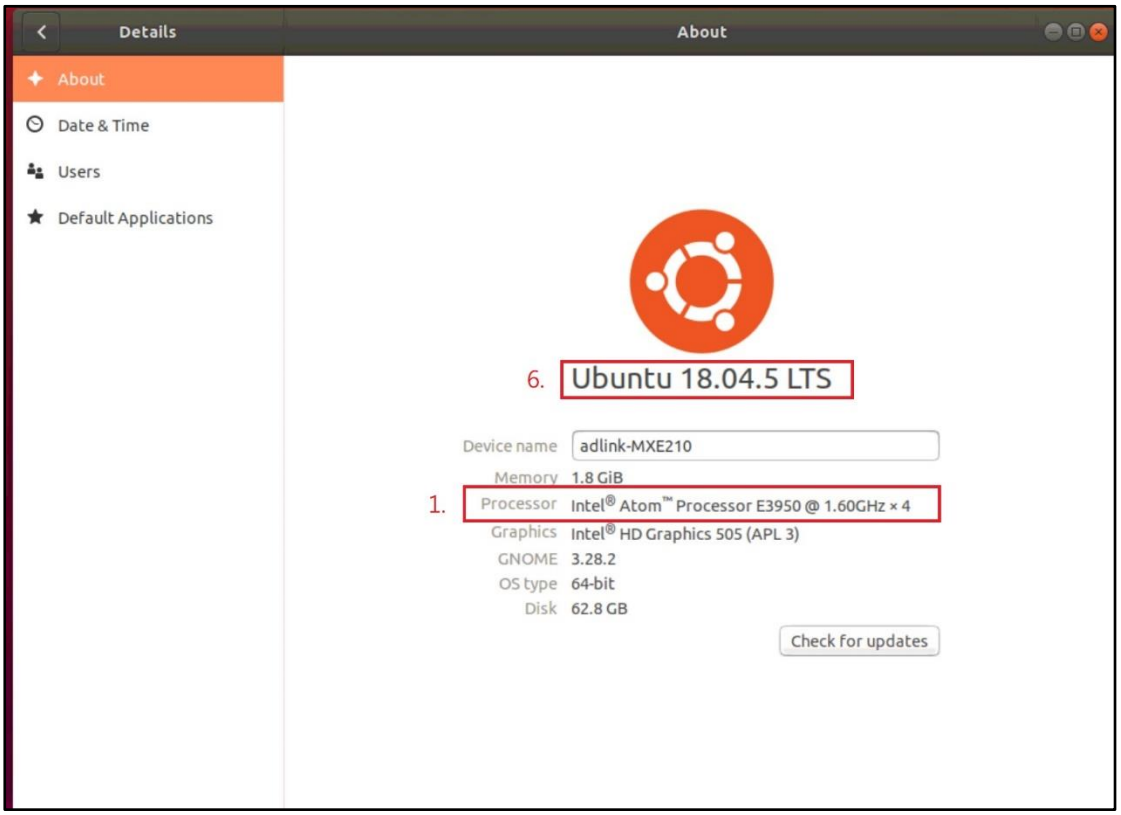

- 項次 5： USB PORT 2 個(含)以上 for PoS 環境感測情境展示應用

  實機操作：顯示 USB PORT，2 個 USB 2.0、2 個 USB 3.0。



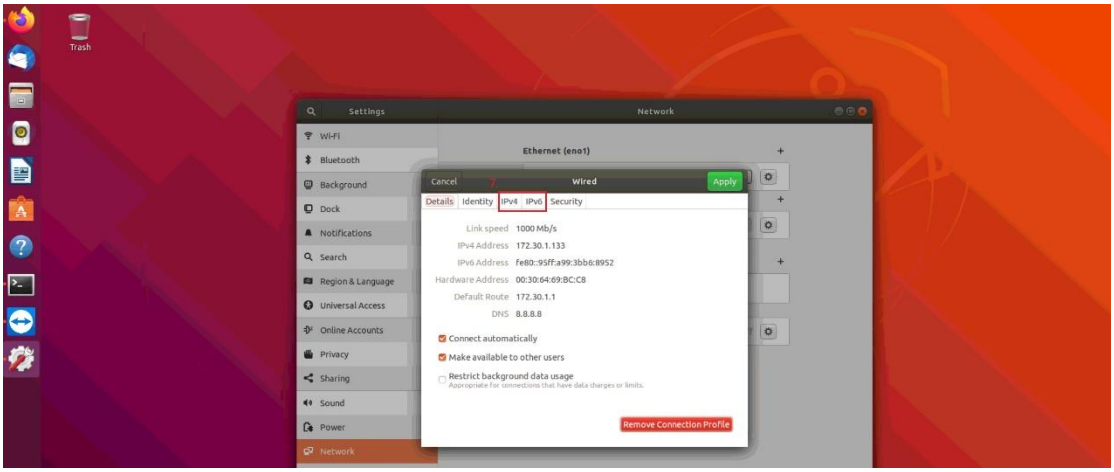
➢ 項次 6：安裝 Ubuntu 15.04 或以上版本

實機操作：顯示 Ubuntu 18.04.5 版本。




➢ 項次 7：支援可配置 IP 網段版本：IPv4、IPv4v6、IPv6

實機操作：顯示 IPv4、IPv4v6、IPv6。



三、 網路交換器

(一)測試項目

表 11、Aruba 2930F 單元測試

| 受測設備 ： Aruba 2930F 24G PoE+ 4SFP+ Swch | | | |
|---|---|---|---|
| 項次 | 測試內容 | 操作方式 | 是否符合 |
| 1 | 具備 24 埠 10/100/1000 Base-T Ethernet 界面及 4 個 1/10G SFP/SFP+介面，UTP 介面具備 Auto MDI/MDI-X。 | 實機操作與書面審查 | ■符合<br>□不符合 |
| 2 | 具備 PoE 及 PoE+功能，最高可提供 370W 供電效能。 | 實機操作與書面審查 | ■符合<br>□不符合 |
| 3 | 提供 IPv6 Host 管理功能、Dual Stack (IPv4/IPv6)。 | 實機操作，顯示相關設定 | ■符合<br>□不符合 |
| 4 | 具備 IPv4 路由協定設定，包括 Static Route、RIPv1/RIPv2、OSPF。 | 實機操作，顯示相關設定 | ■符合<br>□不符合 |
| 5 | 具備 IPv6 Layer 3 靜態路由與動態路由 RIPng、OSPF v3。 | 實機操作，顯示相關設定 | ■符合<br>□不符合 |
| 6 | 提供 DHCP Server 功能。 | 實機操作，顯示相 7 關設定 | ■符合<br>□不符合 |
| 7 | 具備頻寬限制(Rate Limiting)功能，可依據 Per-Port ingress 配置 | 實機操作，顯示相關設定 | ■符合<br>□不符合 |
| 8 | 具備 NTP/SNTP 網路校時功能 | 實機操作，顯示相關設定 | ■符合<br>□不符合 |
| 9 | 具備 STP BPDU Port Protection 保護機制。 | 實機操作，顯示相關設定 | ■符合<br>□不符合 |
| 10 | 具備 SNMPv1/v2c/v3 管理功能 | 實機操作，顯示 | ■符合 |

| | | | |
|---|---|---|---|
| | | 相關設定 | □不符合 |

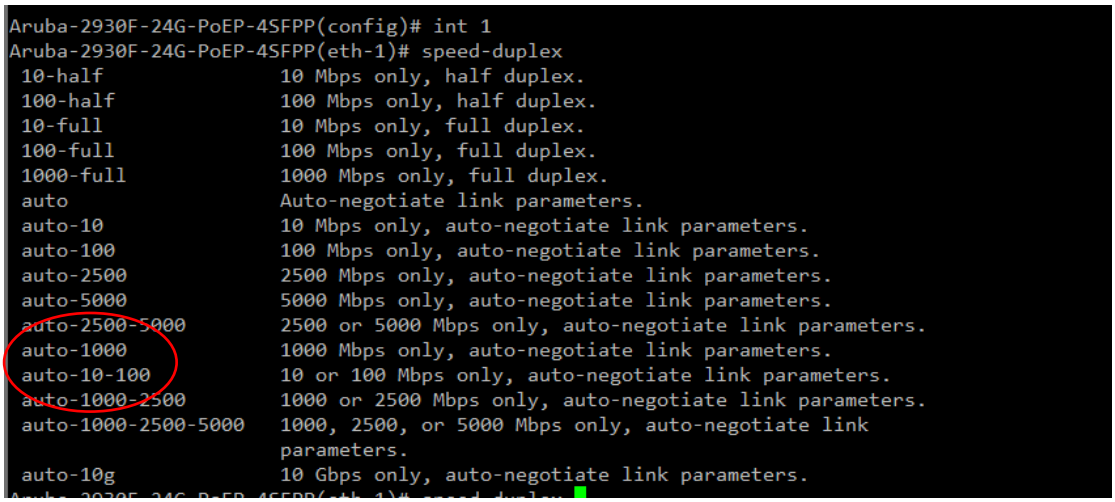
(二)佐證內容(文件說明或實機操作畫面)

- 項次 1:具備 24 埠 10/100/1000 Base-T Ethernet 界面及 4 個 1/10G SFP/SFP+介面，UTP 介面具備 Auto MDI/MDI-X。

  實機操作步驟 1：顯示介面，共有 24 個 UTP 介面以及 4 個 SFP/SFP+介面，UTP 介面具備 Auto MDI/MDI-X。

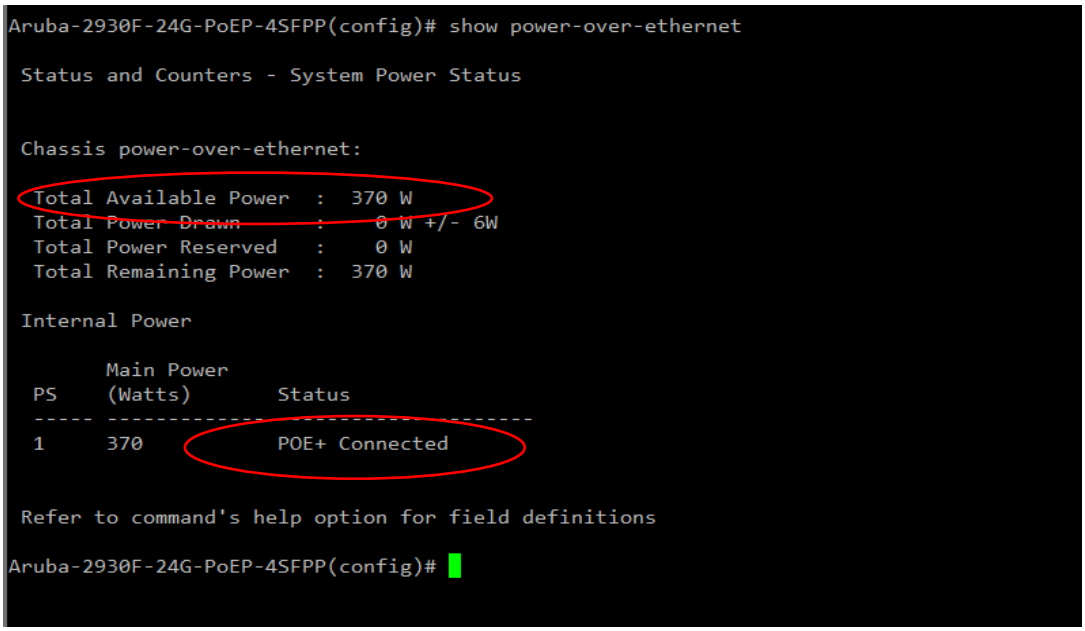
```
Aruba-2930F-24G-PoEP-4SFPP(config)# show interfaces brief

 Status and Counters - Port Status

                         | Intrusion                          MDI  Flow Bcast
 Port          Type      | Alert     Enabled Status Mode       Mode Ctrl Limit
 ------------- --------- + --------- ------- ------ ---------- ---- ---- -----
 1             100/1000T | No        Yes     Down   1000FDx    NA   off  0
 2             100/1000T | No        Yes     Down   1000FDx    Auto off  0
 3             100/1000T | No        Yes     Down   1000FDx    Auto off  0
 4             100/1000T | No        Yes     Down   1000FDx    Auto off  0
 5             100/1000T | No        Yes     Down   1000FDx    Auto off  0
 6             100/1000T | No        Yes     Down   1000FDx    Auto off  0
 7             100/1000T | No        Yes     Up     1000FDx    MDIX off  0
 8             100/1000T | No        Yes     Down   1000FDx    Auto off  0
 9             100/1000T | No        Yes     Down   1000FDx    Auto off  0
 10            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 11            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 12            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 13            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 14            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 15            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 16            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 17            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 18            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 19            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 20            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 21            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 22            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 23            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 24            100/1000T | No        Yes     Down   1000FDx    Auto off  0
 25                      | No        Yes     Down   .              off  0
 26                      | No        Yes     Down   .              off  0
 27                      | No        Yes     Down   .              off  0
 28                      | No        Yes     Down   .              off  0

Aruba-2930F-24G-PoEP-4SFPP(config)#
```

實機操作步驟 2：顯示 UTP 介面可選擇 10/100/1000 的 port speed。



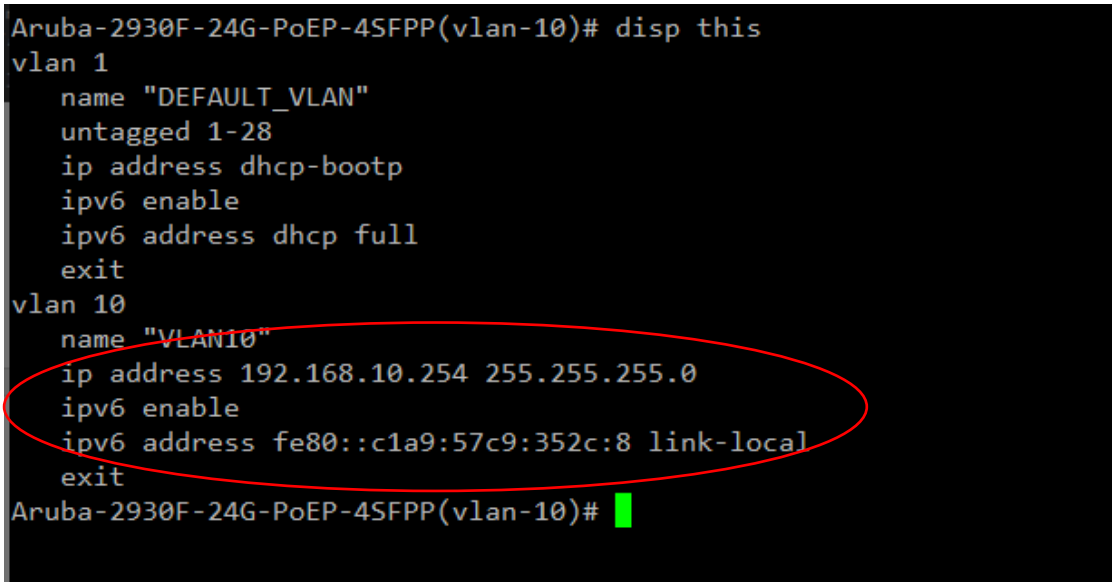

- 項次 2：具備 PoE 及 PoE+功能，最高可提供 370W 供電效能。

  實機操作：顯示 PoE 及 PoE+功能，最高可提供 370W 供電。



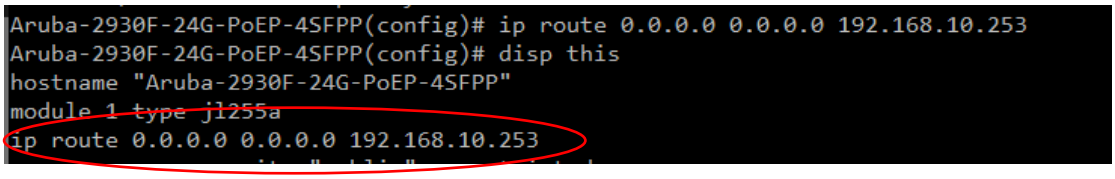
- 項次 3：提供 IPv6 Host 管理功能、Dual Stack (IPv4/IPv6)。

  實機操作：可同時啟用 IPv4/IPv6。

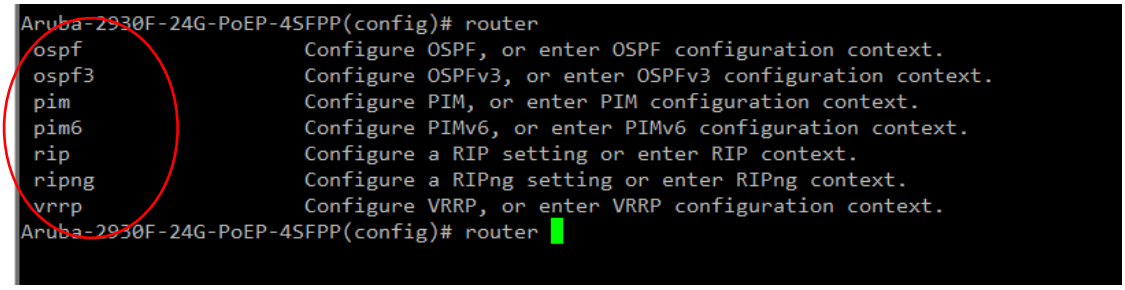



- 項次 4:具備 IPv4 路由協定設定，包括 Static Route、RIPv1/RIPv2、OSPF。

  實機操作步驟 1：顯示 Static route

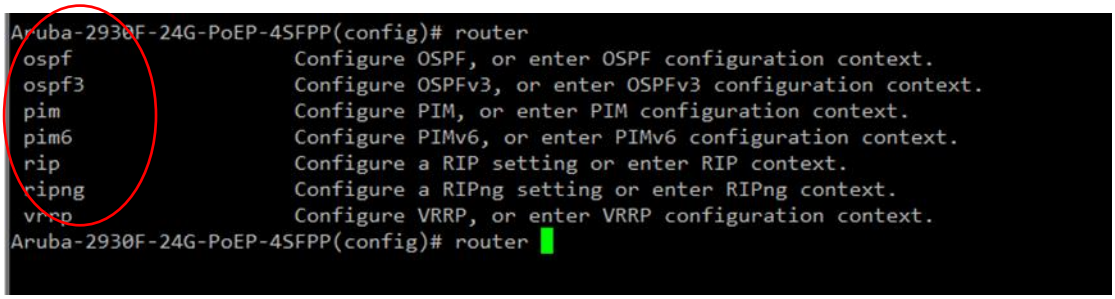



  實機操作步驟 2：顯示 RIPv1/RIPv2、OSPF。



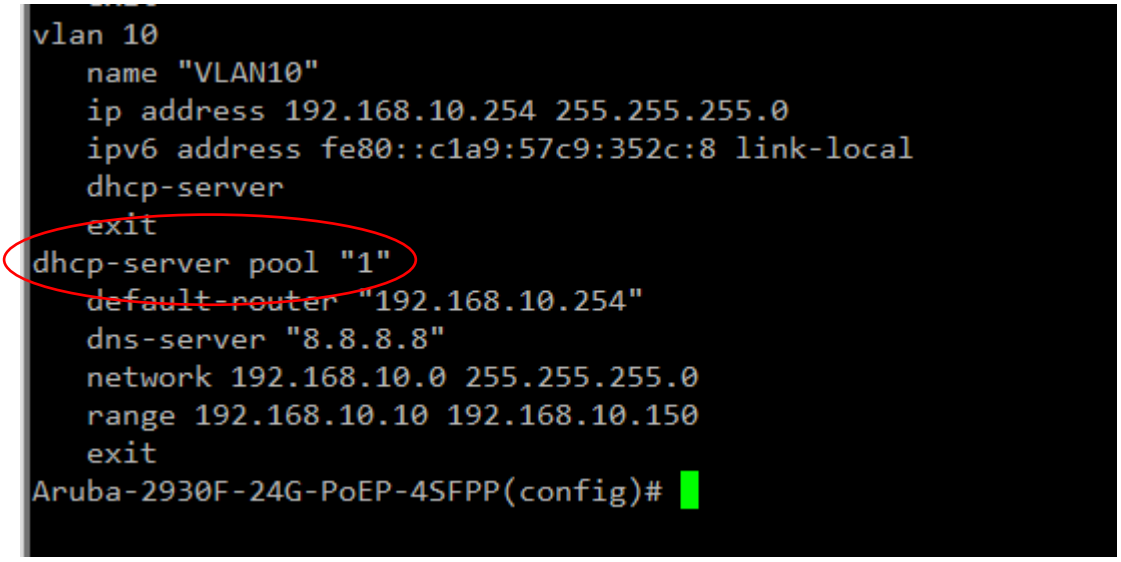
- 項次 5:具備 IPv6 Layer 3 靜態路由與動態路由 RIPng、OSPF v3。

  實機操作：顯示 RIPng、OSPFv3。



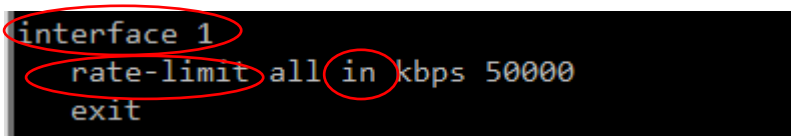

- 項次 6：提供 DHCP Server 功能。

  實機操作：顯示 DHCP Server 功能。




- 項次 7:具備頻寬限制(Rate Limiting)功能，可依據 Per-Port ingress 配置

  實機操作：顯示依據 Rate Limiting 功能，依據 Per-Port ingress 配置。



➢ 項次 8 具備 NTP/SNTP 網路校時功能

實機操作：顯示 NTP/SNTP 網路校時功能。

```
Aruba-2930F-24G-PoEP-4SFPP(config)# timesync
 ntp                    Update the system clock using NTP.
 sntp                   Update the system clock using SNTP.
 timep                  Update the system clock using TIMEP.
 timep-or-sntp          Update the system clock using TIMEP or SNTP.
Aruba-2930F-24G-PoEP-4SFPP(config)# timesync
```

➢ 項次 9 具備 STP BPDU Port Protection 保護機制。

```
Aruba-2930F-24G-PoEP-4SFPP(config)# show spanning-tree bpdu-protection

 Status and Counters - STP Port(s) BPDU Protection Information

 BPDU Protection Timeout (sec) : 0
 BPDU Protected Ports : 1-2


Aruba-2930F-24G-PoEP-4SFPP(config)# show spanning-tree bpdu-protection 1-2

 Status and Counters - STP BPDU Protection Information

 BPDU Protection Timeout (sec) : 0
 BPDU Protected Ports : 1-2


  Port  Type       Protection State        Errant BPDUs
  ----- ---------- ---------- ------------ ------------
  1     100/1000T  Yes        Disabled     0
  2     100/1000T  Yes        Disabled     0
```

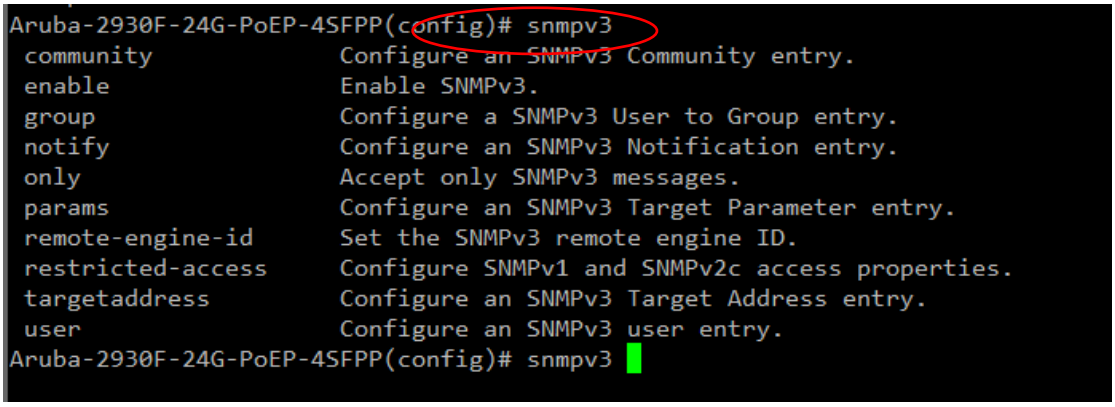
實機操作：顯示 STP BPDU Port Protection 保護機制。

➢ 項次 10 具備 SNMPv1/v2c/v3 管理功能

實機操作步驟 1：顯示 SNMPv1/v2c 管理功能。

```
Aruba-2930F-24G-PoEP-4SFPP(config)# snmp-server
 community              Add/delete SNMP community.
 contact                The name of the switch administrator.
 enable                 Enable SNMPv1/v2.
 engine-id              Set the SNMPv3 Engine ID.
 host                   Define SNMP traps and their receivers.
 location               A description of the switch location.
 mib                    Configure SNMP access security for specific MIBs.
 response-source        Specify the source ip-address policy for the response
                        pdu.
 trap-source            Specify the source ip-address policy for the trap pdu.
Aruba-2930F-24G-PoEP-4SFPP(config)# snmp-server en
 enable
 engine-id
Aruba-2930F-24G-PoEP-4SFPP(config)# snmp-server
```

實機操作步驟 2：顯示 SNMPv3 管理功能。



四、 5G 核心網路模擬設備

(一)測試項目

表 12、Amarisoft Classic Callbox 單元測試

| 受測設備 ： Amarisoft Classic Callbox | | | |
|---|---|---|---|
| 項次 | 測試內容 | 操作方式 | 是否符合 |
| 1 | LTE eNB 功能是否能正常啟動及連線 | 實機操作 | ■符合<br>□不符合 |
| 2 | EPC 功能是否能正常啟動及連線 | 實機操作 | ■符合<br>□不符合 |
| 3 | 5G gNB 功能是否能正常啟動及連線 | 實機操作 | ■符合<br>□不符合 |
| 4 | 模擬設備是否可以模擬 3 個 5G cells | 實機操作 | ■符合<br>□不符合 |
| 5 | 5G 5GC 是否支援註冊認證 | 實機操作 | ■符合<br>□不符合 |
| 6 | 是否支援分配 IP 網段版本：IPv4 | 實機操作 | ■符合<br>□不符合 |
| 7 | 是否支援分配 IP 網段版本：IPv4v6 | 實機操作 | ■符合<br>□不符合 |
| 8 | 是否支援分配 IP 網段版本：IPv6 | 實機操作 | ■符合<br>□不符合 |

(二)佐證內容(文件說明或實機操作畫面)

➢ 項次 1：具備 LTE eNB 功能是否能正常啟動及連線。

- 測試步驟：

  1.啟動 Amarisoft 服務

  2.分別對 mme 與 enb 輸入指令，查詢 RAN_ID

- 期望結果：

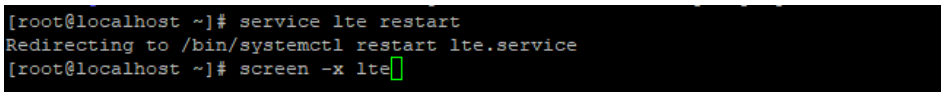
  服務正常啟動，基站與核心網路 RAN_ID 相同

- 操作流程：

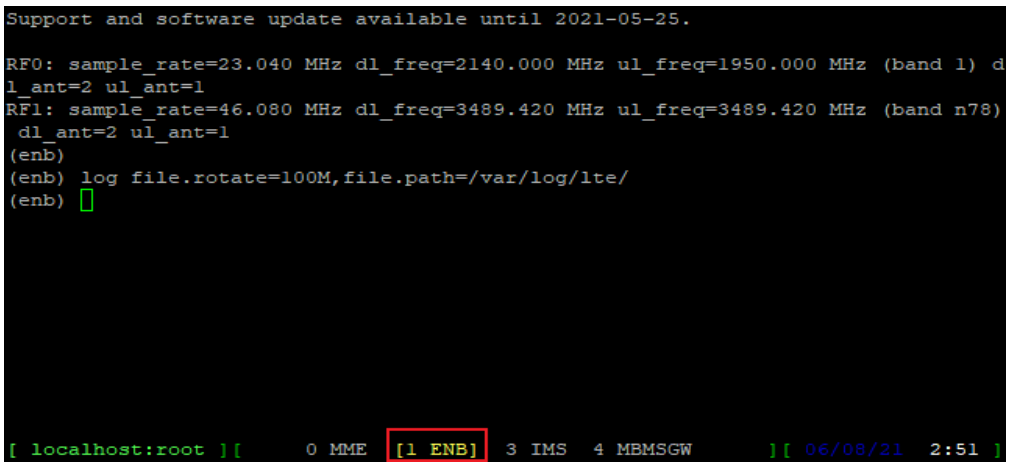
  實機操作步驟 1：啟動 Amarisoft 服務

  啟動 Amarisoft 服務指令：service lte restart

  切換螢幕至 lte 指令： screen –x lte

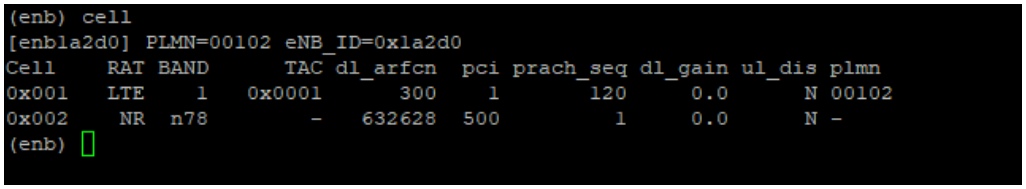



使用 ctrl+a 切換至 MME 畫面，如下圖右下角 MME 標籤，若畫面中顯示日誌資料夾路徑且並無錯誤訊息，表示 EPC 功能正常啟動。

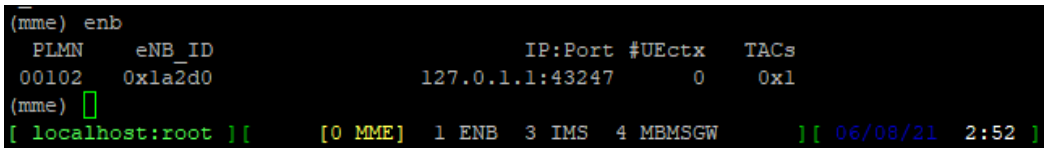



實機操作步驟 2：分別對 mme 與 enb 輸入指令，查詢 RAN_ID

列出 eNB 中可用 cell 指令：cell




列出 mme 中連結之 eNodeBs，指令：enb




- 實際結果：服務正常啟動，基站與核心網路 RAN_ID 相同

➢ 項次 2：具備 EPC 功能是否能正常啟動及連線。

- 測試步驟：

  1.啟動 Amarisoft 服務

  2.對 enb 輸入指令確認 s1 接通

- 期望結果：

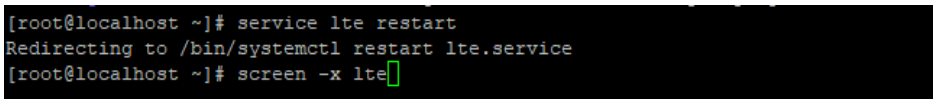
  服務正常啟動，enb s1 應接通

- 操作流程：

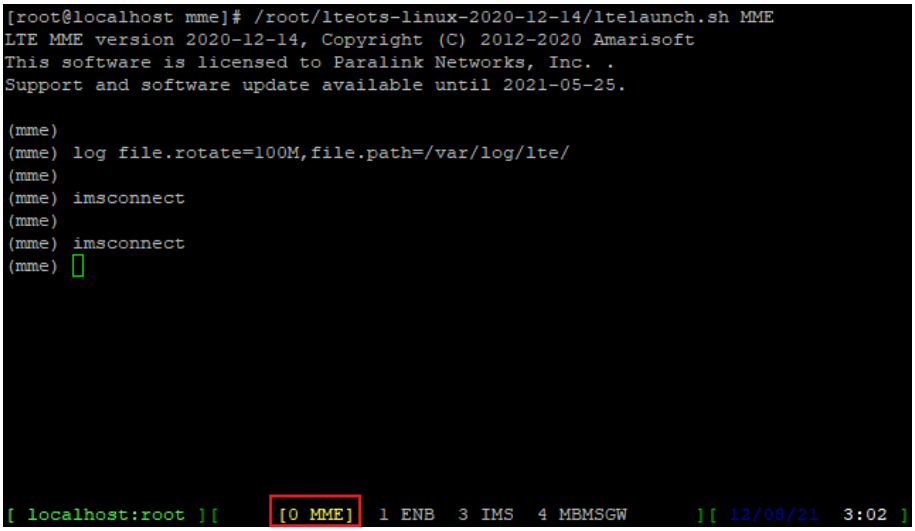
  實機操作步驟 1：啟動 Amarisoft 服務

  服務啟動指令：service lte restart

  切換螢幕至 lte，指令：screen –x lte

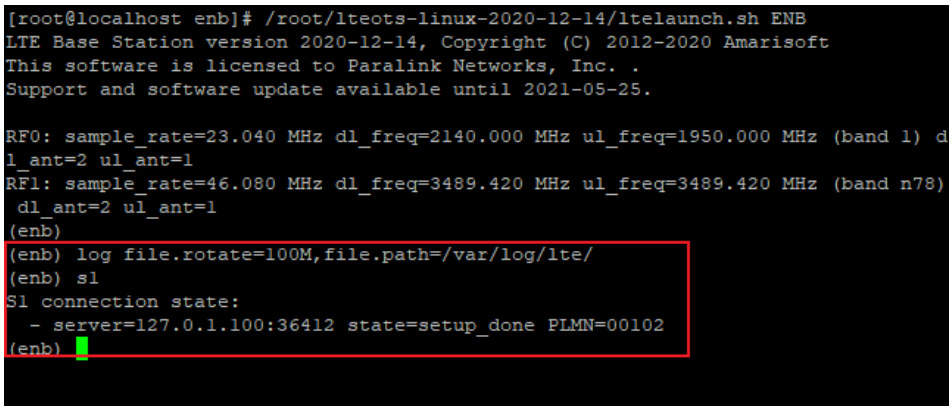



使用 ctrl a 切換至 MME 畫面，如下圖右下角 MME 標籤，若畫面中顯示日誌資料夾路徑且並無錯誤訊息，表示 EPC 功能正常啟動。




實機操作步驟 2：對 enb 輸入指令確認 s1 接通

列出 s1 狀態指令：s1




- 實際結果：服務正常啟動，確認 enb s1 接通

➢ 項次 3：提供 5G gNB 功能是否能正常啟動及連線。

- 測試步驟：

  1.啟動 Amarisoft 服務

  2.分別對 mme 與 gnb 輸入指令，查詢 RAN_ID

- 期望結果：

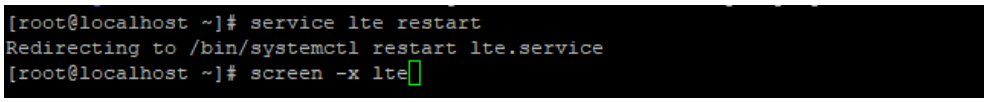
  服務正常啟動，基站與核心網路 RAN_ID 應相同

- 操作流程：

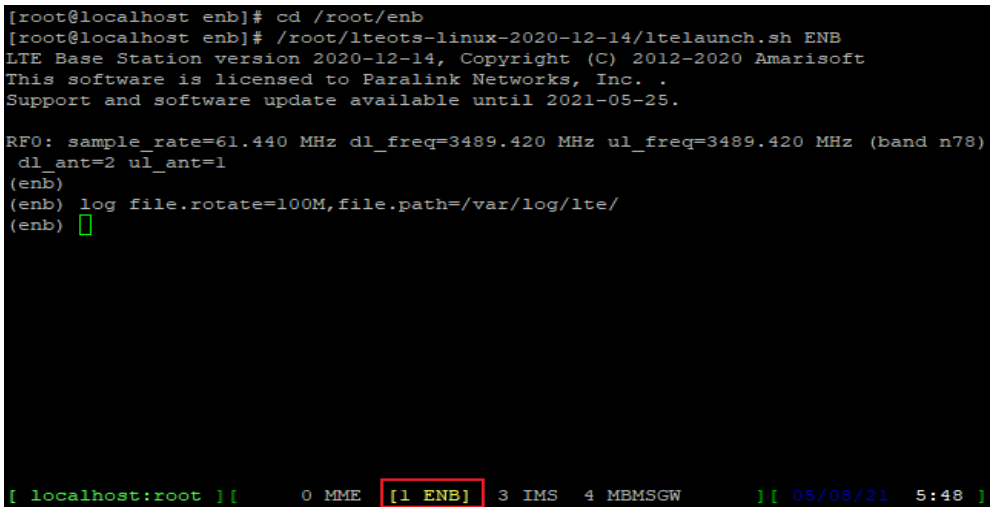
  實機操作步驟 1：啟動 Amarisoft 服務

  服務啟動服務，指令：service lte restart

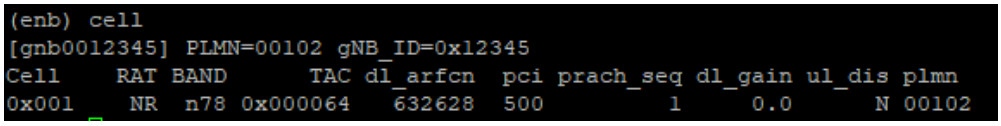
  切換螢幕至 lte，指令：screen –x lte




使用 ctrl a 切換至 ENB 畫面，如下圖右下角 ENB 標籤，若畫面中顯示日誌資料夾路徑且並無錯誤訊息，表示 gNB 功能正常啟動

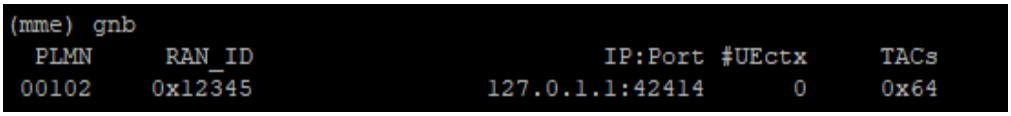



實機操作步驟 2：分別對 mme 與 gnb 輸入指令，查詢 RAN_ID




列出 gNB 中可用 cell 指令：cell

列出 mme 中連結之 gNodeBs，指令：gnb




檢視 gNB 之 gNB_ID 與 mme gnb 之 RAN_ID 是否一致，若相同即表示連線正常

- 實際結果：服務正常啟動，基站與核心網路 RAN_ID 相同

➢ 項次 4：具備模擬設備是否可以模擬 3 個 5G cells。

- 測試步驟：

  1.確認 Amarisoft config 之 gNB.cfg 中具有三個 cells

  2.啟動 Amarisoft 服務

  3.對 gnb 輸入指令，查詢 cell 數量

- 期望結果：

  對 gnb 輸入指令，查詢 cell 數量期望結果：服務正常啟動，基站與核心網路 RAN_ID 應相同

- 操作流程：

  實機操作步驟 1：確認 Amarisoft config 之 gNB.cfg 中具

有三個 cells

```
nr_cell_list: [
{
  rf_port: 0,
  cell_id: 1,
  n_id_cell: 1,
  band: 78,
  dl_nr_arfcn: 632628,
  ncell_list: [
  {
    cell_id: 2,
  },
  {
    cell_id: 3,
  },
  ],
},
{
  rf_port: 0,
  cell_id: 2,
  n_id_cell: 2,
  band: 78,
  dl_nr_arfcn: 632928,
  ncell_list: [
  {
    cell_id: 1,
  },
  {
    cell_id: 3,
  },
  ],
},
{
  rf_port: 1,
  cell_id: 3,
  n_id_cell: 3,
  band: 78,
  dl_nr_arfcn: 633228,
  ncell_list: [
  {
    cell_id: 1,
  },
  {
    cell_id: 2,
  },
  ],
},
], /* nr_cell_list */
```

實機操作步驟 2：啟動 Amarisoft 服務

服務啟動服務，指令：service lte restart

服務啟動後，切換頁面致 ENB

```
[root@localhost enb]#
[root@localhost enb]# cd /root/enb
[root@localhost enb]# /root/lteots-linux-2020-12-14/ltelaunch.sh ENB
LTE Base Station version 2020-12-14, Copyright (C) 2012-2020 Amarisoft
This software is licensed to Paralink Networks, Inc. .
Support and software update available until 2021-05-25.

RF0: sample_rate=30.720 MHz dl_freq=3491.670 MHz ul_freq=3491.670 MHz (band n78) dl_ant=1 ul_ant=1
RF1: sample_rate=23.040 MHz dl_freq=3498.420 MHz ul_freq=3498.420 MHz (band n78) dl_ant=1 ul_ant=1
(enb)
(enb) log file.rotate=100M,file.path=/var/log/lte/
(enb)
```

實機操作步驟 3：對 gnb 輸入指令，查詢 cell 數量

列出 gNB 中 cell 列表指令：cell

```
(enb) cell
[gnb0012345] PLMN=00102 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1     0.0      N 00102
0x002    NR  n78 0x000064   632928    2         1     0.0      N 00102
0x003    NR  n78 0x000064   633228    3         1     0.0      N 00102
(enb)
```

- 實際結果：Amarisoft 可支援模擬三個 cell 於不同頻率位置同時啟動服務

➢ 項次 5：具備 5G 5GC 是否支援註冊認證。

- 測試步驟：

  1.啟動 Amarisoft 服務

  2.啟動 UE 並發送指令取得 IP

  3.對 mme 輸入指令確認是否有 UE 裝置

  4.進入瀏覽器日誌確認 UE 是否有註冊訊息

- 期望結果：

  核心網路日誌訊息中應包含 UE 註冊認證訊息

- 操作流程：

  實機操作步驟 1：啟動 Amarisoft 服務

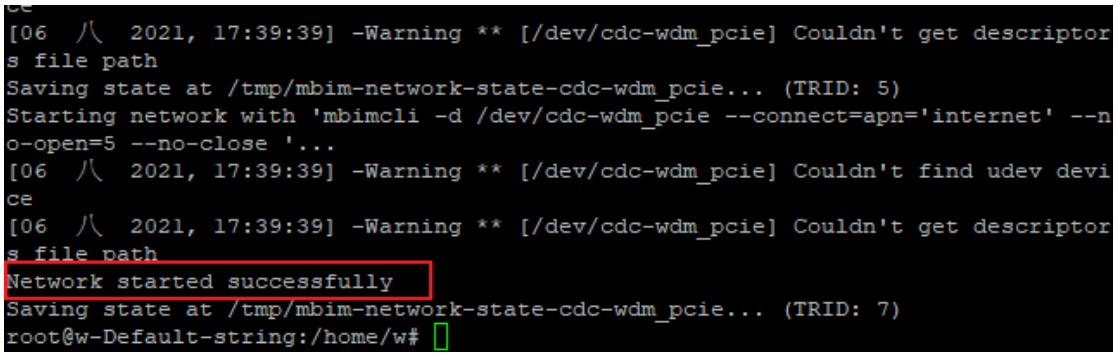
  服務啟動服務，指令：service lte restart

  實機操作步驟 2：啟動 UE 並發送指令取得 IP

  啟動 UE(需以 root 權限執行)啟動成功後結果如附圖所示，出現 Network started successfully 字樣，網路啟動指令如下：

  mbim-network /dev/cdc-wdm_pcie start

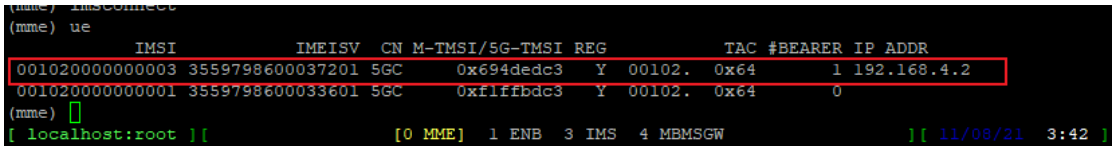
UE 取得 DHCP 配發之 IP 指令如下，此時會顯示 DHCP 配發之 IP 位址：udhcpc -nqfi mbim_mhi0




實機操作步驟 3：對 mme 輸入指令確認是否有 UE 裝置

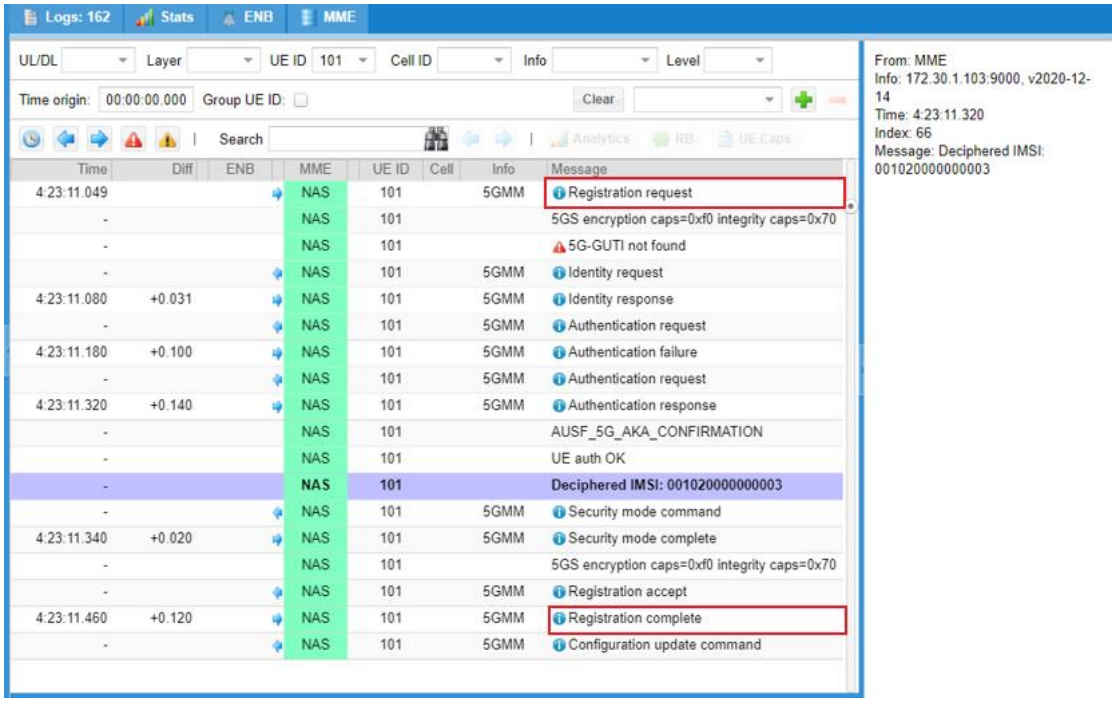
核心網路取得 UE 列表指令： ue

從 UE 列表中可以確認 IP 位址與 UE 取得之 IP 相同




實機操作步驟 4：進入瀏覽器日誌確認 UE 是否有註冊訊息

開啟模擬器日誌，確認 UE 的註冊與認證之相關訊息如下圖所示，其中需確認 UE 之 IMSI 是否與發送 UE 端相同。




實際結果：核心網路日誌訊息中包含 UE 註冊認證訊息

➢ 項次 6：支援分配 IP 網段版本：IPv4。

- 測試步驟：

  1.確認 Amarisoft config 路徑之 mme.cfg

  2.啟動 Amarisoft 服務

  3.啟動 UE 發送指令取得 IP，並查詢 UE 的 IP 網域相關參數

  4.對 mme 輸入指令確認 UE 裝置

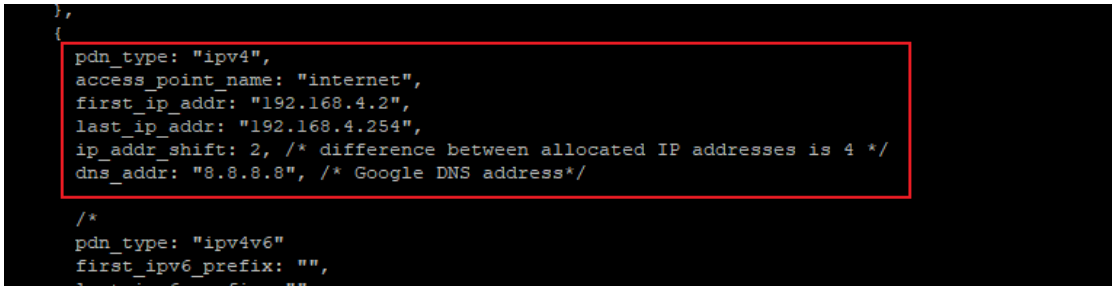
- 期望結果：

  確認 UE 裝置取得之 IP 位址應落於 mme.cfg 中設定的 IPv4

- 操作流程：

  實機操作步驟 1：確認 Amarisoft config 路徑之 mme.cfg

  確認 mme.cfg 中 pdn_list 之 pdn_type 為 IPv4




  實機操作步驟 2：啟動 Amarisoft 服務

  服務啟動服務，指令：service lte restart

  實機操作步驟 3：啟動 UE 發送指令取得 IP，並查詢 UE 的 IP 網域相關參數

  啟動 UE (需以 root 權限執行)

  進入 minicomtc 指令：minicom -D /dev/at_pcie

  查詢 UE IMSI 指令：at+cimi

  啟動成功結果如附圖所示，出現 Network started successfully 字樣，

  指令：mbim-network /dev/cdc-wdm_pcie start

```
[06 八 2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't get descriptor
s file path
Saving state at /tmp/mbim-network-state-cdc-wdm_pcie... (TRID: 5)
Starting network with 'mbimcli -d /dev/cdc-wdm_pcie --connect=apn='internet' --n
o-open=5 --no-close '...
[06 八 2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't find udev devi
ce
[06 八 2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't get descriptor
s file path
Network started successfully
Saving state at /tmp/mbim-network-state-cdc-wdm_pcie... (TRID: 7)
root@w-Default-string:/home/w#
```

UE 取得 DHCP 配發之 IP 指令如下，此時會顯示 DHCP 配發之 IP

位址：udhcpc -nqfi mbim_mhi0

查詢 UE 的 IP 網域相關參數，指令：ifconfig

```
mbim_mhi0: flags=65<UP,RUNNING>  mtu 65535
        inet 192.168.4.2  netmask 255.255.255.252
        inet6 fe80::200:ff:fe00:0  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000
 (UNSPEC)
        RX packets 29817  bytes 463272096 (463.2 MB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 54503  bytes 4179799 (4.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

實機操作步驟 4：對 mme 輸入指令確認 UE 裝置

核心網路取得 UE 列表指令：ue

```
(mme) disconnect
(mme) ue
            IMSI           IMEISV  CN M-TMSI/5G-TMSI REG          TAC #BEARER IP ADDR
 001020000000003 3559798600037201 5GC      0x8f8a35f7   Y  00102.  0x64       1 192.168.4.2
 001020000000001 3559798600033601 5GC       0x4cc6c64   Y  00102.  0x64       0
(mme)
[ localhost:root ][            [0 MME]  1 ENB  3 IMS  4 MBMSGW            ][ 11/08/21  5:45 ]
```

- 實際結果：UE 裝置取得之 IP 位址落於 mme.cfg 中設定的 IPv4

➢ 項次 7：支援分配 IP 網段版本：IPv4v6

- 測試步驟：

1.確認 Amarisoft config 路徑之 mme.cfg

2.啟動 Amarisoft 服務

3.啟動 UE 發送指令取得 IP，並查詢 UE 的 IP 網域相關參數

4.對 mme 輸入指令確認 UE 裝置

- 期望結果：

確認 UE 裝置取得之 IP 位址應落於 mme.cfg 中設定的 IPv4v6

- 操作流程：

實機操作步驟 1：確認 Amarisoft config 路徑之 mme.cfg

確認 mme.cfg 中 pdn_list 之 pdn_type 為 IPv4v6

```
    },
    {
      pdn_type: "ipv4v6",
      access_point_name: "internet",
      first_ip_addr: "192.168.4.2",
      last_ip_addr: "192.168.4.254",
      first_ipv6_prefix: "2001:468:3000:1::",
      last_ipv6_prefix: "2001:468:3000:ffff::",
      ip_addr_shift: 2, /* difference between allocated IP addresses is 4 */
      dns_addr: ["8.8.8.8", "2001:4860:4860::8888"],/* Google DNS address*/

      /*
      pdn_type: "ipv4v6"
      first_ipv6_prefix: "",
```

實機操作步驟 2：啟動 Amarisoft 服務

服務啟動服務，指令：service lte restart

實機操作步驟 3：啟動 UE 發送指令取得 IP，並查詢 UE 的 IP 網域相關參數

啟動 UE (需以 root 權限執行)

進入 minicomtc 指令： minicom -D /dev/at_pcie

查詢 UE IMSI 指令：at+cimi

```
at+cimi
001020000000003

OK
```

啟動成功結果如附圖所示，出現 Network started successfully 字樣，指令：mbim-network /dev/cdc-wdm_pcie start

```
[06  八  2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't get descriptor
s file path
Saving state at /tmp/mbim-network-state-cdc-wdm_pcie... (TRID: 5)
Starting network with 'mbimcli -d /dev/cdc-wdm_pcie --connect=apn='internet' --n
o-open=5 --no-close '...
[06  八  2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't find udev devi
ce
[06  八  2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't get descriptor
s file path
Network started successfully
Saving state at /tmp/mbim-network-state-cdc-wdm_pcie... (TRID: 7)
root@w-Default-string:/home/w#
```

UE 取得 DHCP 配發之 IP 指令：udhcpc -nqfi mbim_mhi0

查詢 UE 的 IP 網域相關參數，指令：ifconfig

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

mbim_mhi0: flags=65<UP,RUNNING>  mtu 65535
        inet 192.168.4.2  netmask 255.255.255.252
        inet6 2001:468:3000:1:200:ff:fe00:0  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::200:ff:fe00:0  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000
 (UNSPEC)
        RX packets 17  bytes 2396 (2.3 KB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 20  bytes 1840 (1.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@w-Default-string:/home/w#
```

實機操作步驟 4：對 mme 輸入指令確認 UE 裝置

至核心網路確認該 UE 分配到的 IP 與 UE 介面取得的

IP 是否一致。

核心網路取得 UE 列表指令： e

```
(mme) ue
          IMSI           IMEISV  CN M-TMSI/5G-TMSI REG          TAC #BEARER IP_ADDR
 001020000000001 3559798600033601 5GC     0x9f18e3c5   Y  00102.  0x64       0
 001020000000003 3559798600037201 5GC     0x9d069f5c   Y  00102.  0x64       1 192.168.4.2 2001:468:3000:1::
(mme)
[ localhost:root ][                  [0 MME]  1 ENB  3 IMS  4 MBMSGW                    ][ 06/08/21  5:55 ]
```

- 實際結果：確認 UE 裝置取得之 IP 位址落於 mme.cfg 中設定的 IPv4v6

➢ 項次 8：支援分配 IP 網段版本：IPv6

- 測試步驟：

  1.確認 Amarisoft config 路徑之 mme.cfg

  2.啟動 Amarisoft 服務

  3.啟動 UE 發送指令取得 IP，並查詢 UE 的 IP 網域相關參數

  4.對 mme 輸入指令確認 UE 裝置

- 期望結果：

  確認 UE 裝置取得之 IP 位址應落於 mme.cfg 中設定的 IPv6

- 操作流程：

  實機操作步驟 1：確認 Amarisoft config 路徑之 mme.cfg

  確認 mme.cfg 中 pdn_list 之 pdn_type 為 IPv6

```
},
{
  pdn_type: "ipv6",
  access_point_name: "internet",
  first_ipv6_prefix: "2001:468:3000:1::",
  last_ipv6_prefix: "2001:468:3000:ffff::",
  dns_addr: "2001:4860:4860::8888",/* Google DNS address*/

  /*
  pdn_type: "ipv4v6"
  first_ipv6_prefix: "",
  last_ipv6_prefix: "",
```

  實機操作步驟 2：啟動 Amarisoft 服務

  服務啟動服務，指令：service lte restart

  實機操作步驟 3：動 UE 發送指令取得 IP，並查詢 UE 的 IP 網域相關參數

  啟動 UE (需以 root 權限執行)

  進入 minicomtc 指令： minicom -D /dev/at_pcie

  查詢 UE IMSI 指令：at+cimi

```
at+cimi
001020000000003

OK
```

啟動成功結果如附圖所示，出現 Network started successfully 字樣，

指令：mbim-network /dev/cdc-wdm_pcie start

```
[06 八 2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't get descriptor
s file path
Saving state at /tmp/mbim-network-state-cdc-wdm_pcie... (TRID: 5)
Starting network with 'mbimcli -d /dev/cdc-wdm_pcie --connect=apn='internet' --n
o-open=5 --no-close '...
[06 八 2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't find udev devi
ce
[06 八 2021, 17:39:39] -Warning ** [/dev/cdc-wdm_pcie] Couldn't get descriptor
s file path
Network started successfully
Saving state at /tmp/mbim-network-state-cdc-wdm_pcie... (TRID: 7)
root@w-Default-string:/home/w#
```

UE 取得 DHCP 配發之 IP 指令如下，此時會顯示 DHCP 配發之 IP 位址：udhcpc -nqfi mbim_mhi0

查詢 UE 的 IP 網域相關參數，指令： ifconfig

```
mbim_mhi0: flags=65<UP,RUNNING>  mtu 65535
        inet6 2001:468:3000:1:200:ff:fe00:0  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::200:ff:fe00:0  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000
 (UNSPEC)
        RX packets 31521  bytes 475432948 (475.4 MB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 56489  bytes 4354092 (4.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@w-Default-string:/home/w#
```

實機操作步驟 4：對 mme 輸入指令確認 UE 裝置

核心網路取得 UE 列表指令： ue

```
(mme) ue
          IMSI          IMEISV  CN M-TMSI/5G-TMSI REG          TAC #BEARER IP_ADDR
001020000000003 3559798600037201 5GC     0x28617e01   Y  00102.  0x64       1 2001:468:3000:1::
(mme)
[ localhost:root ][              [0 MME]  1 ENB  3 IMS  4 MBMSGW                ][ 11/08/21 21
```

- 實際結果：UE 裝置取得之 IP 位址落於 mme.cfg 中設定的 IPv6

五、 5G 無線接入設備

(一)測試項目

表 13、DTA1164W 單元測試

| 受測設備 ： DTA1164W 5G SA/NSA Gateway | | | |
|---|---|---|---|
| 項次 | 測試內容 | 操作方式 | 是否符合 |
| 1 | 是否具備 2 個 1GbE RJ45 cooper ports 且可正常運作 | 實機操作 | ■符合<br>□不符合 |
| 2 | 是否支援 5G SA (3GPP Release 15) 架構 | 實機操作與書面說明 | ■符合<br>□不符合 |
| 3 | 是否支援 5G NSA (3GPP Release 15) 架構 | 實機操作與書面說明 | ■符合<br>□不符合 |
| 4 | 是否支援分配 IP 網段版本：IPv4 | 實機操作 | ■符合<br>□不符合 |
| 5 | 是否支援分配 IP 網段版本：IPv4v6 | 實機操作 | ■符合<br>□不符合 |
| 6 | 是否支援分配 IP 網段版本：IPv6 | 實機操作 | ■符合<br>□不符合 |

(二)佐證內容(文件說明或實機操作畫面)

- 項次 1：具備 2 個 1GbE RJ45 cooper ports 且可正常運作。

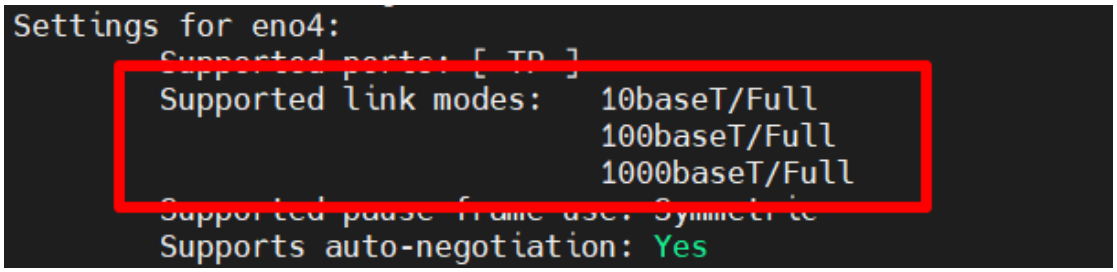
實機操作步驟 1：第一個 cooper ports 資訊

```
Settings for eno3:
        Supported link modes:   10baseT/Full
                                100baseT/Full
                                1000baseT/Full
        Supports auto-negotiation: Yes
```

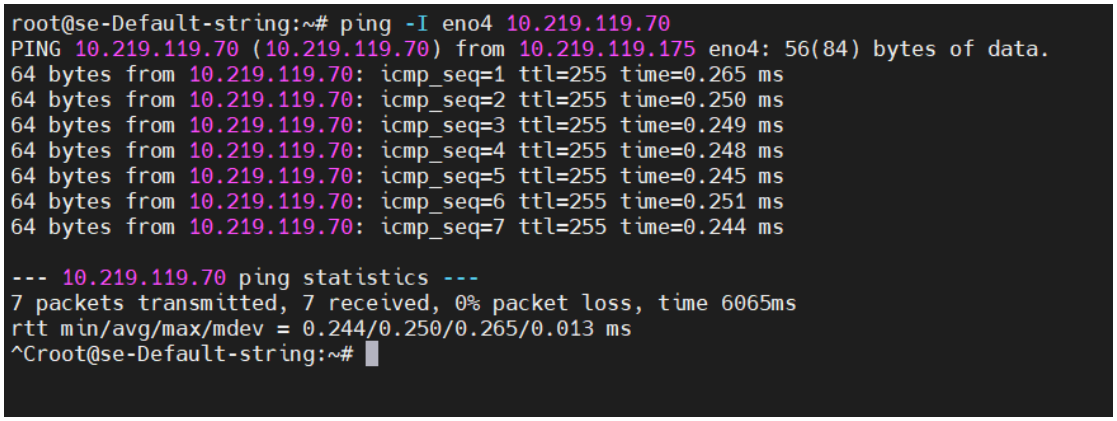
實機操作步驟 2：網路測試工具測試 Ping 可運作

```
^Croot@se-Default-string:~# ping -I eno3 10.219.119.70
PING 10.219.119.70 (10.219.119.70) from 10.219.119.174 eno3: 56(84) bytes of data.
64 bytes from 10.219.119.70: icmp_seq=1 ttl=255 time=0.475 ms
64 bytes from 10.219.119.70: icmp_seq=2 ttl=255 time=0.254 ms
64 bytes from 10.219.119.70: icmp_seq=3 ttl=255 time=0.264 ms
64 bytes from 10.219.119.70: icmp_seq=4 ttl=255 time=0.245 ms
64 bytes from 10.219.119.70: icmp_seq=5 ttl=255 time=0.242 ms
64 bytes from 10.219.119.70: icmp_seq=6 ttl=255 time=0.246 ms
64 bytes from 10.219.119.70: icmp_seq=7 ttl=255 time=0.247 ms
^C
--- 10.219.119.70 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6133ms
rtt min/avg/max/mdev = 0.242/0.281/0.475/0.082 ms
root@se-Default-string:~#
```

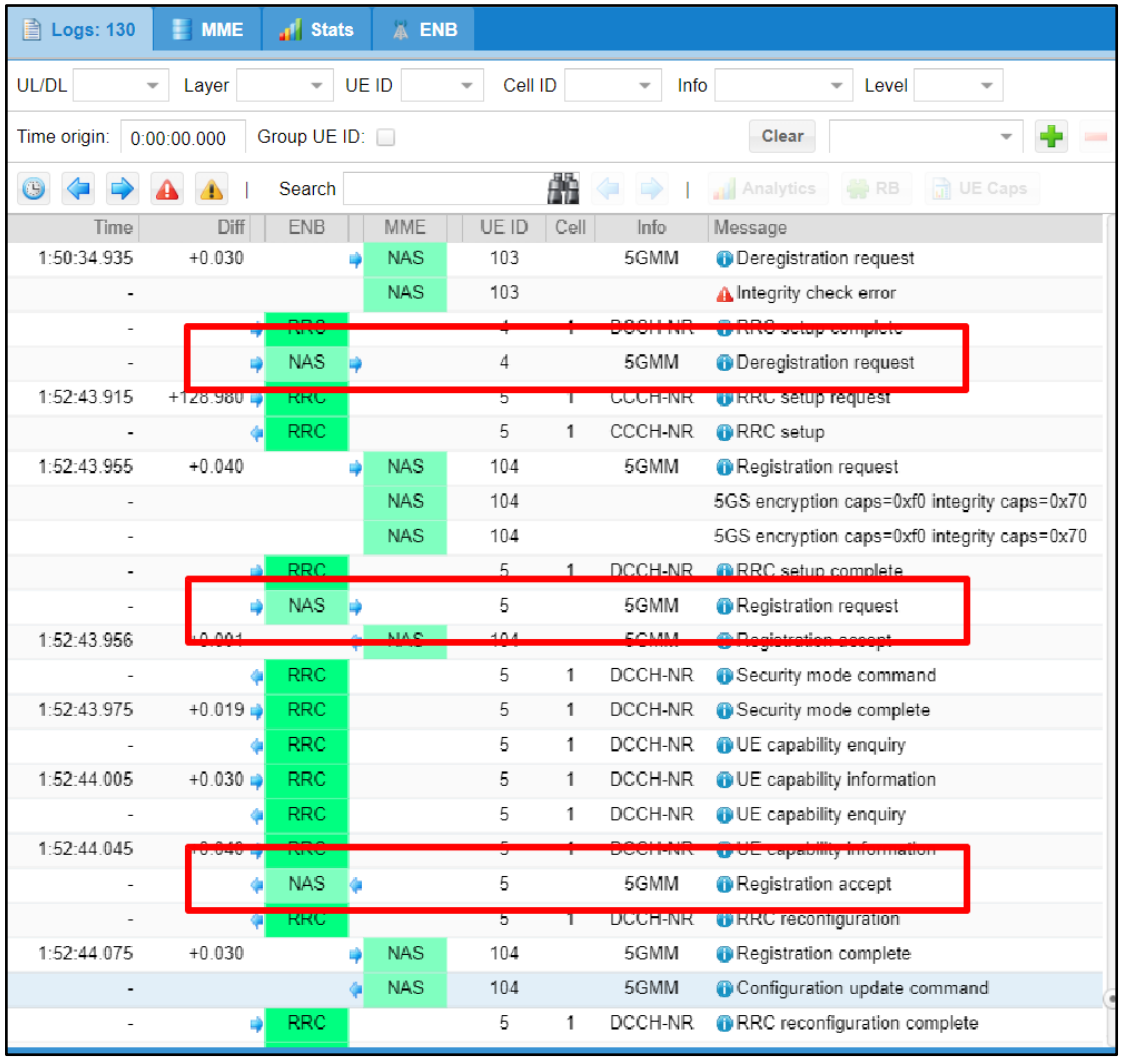
實機操作步驟 3：第二個 cooper ports 資訊



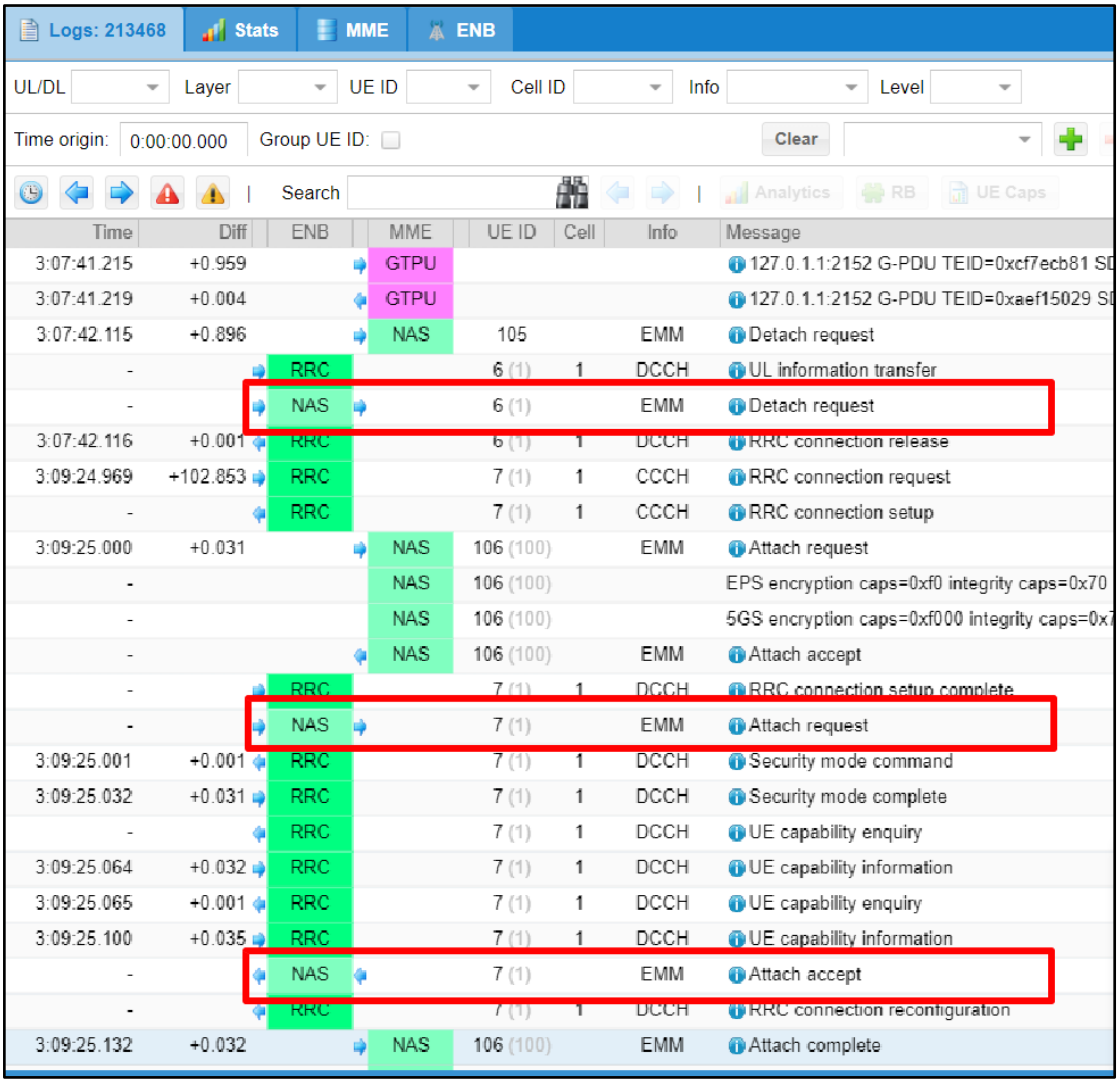

實機操作步驟 4：網路測試工具測試 Ping 可運作



➢ 項次 2：支援 5G SA (3GPP Release 15) 架構。

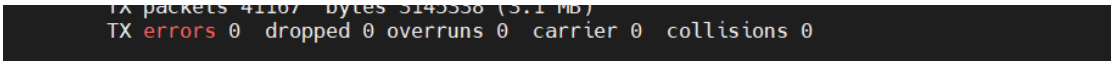


➢ 項次 3 支援 5G NSA (3GPP Release 15) 架構。



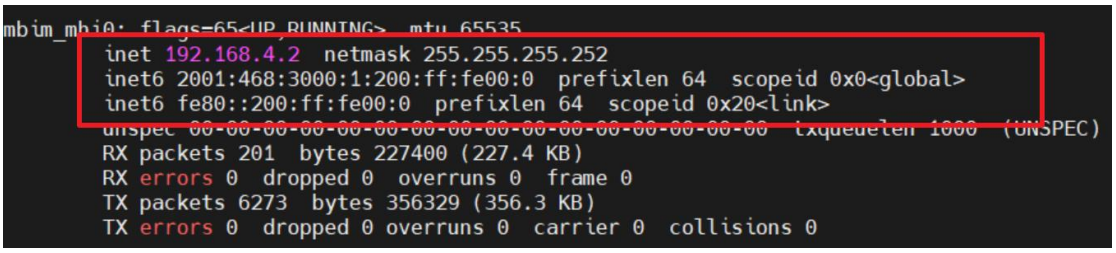
➢ 項次 4 支援分配 IP 網段版本：IPv4。

實機操作：進入操作畫面顯示 IPv4 設定。



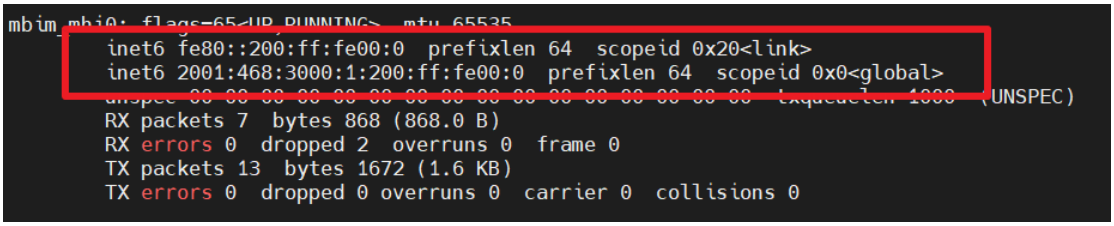

➢ 項次 5 是否支援分配 IP 網段版本：IPv4v6。

實機操作：進入操作畫面顯示 IPv4v6 設定。




➢ 項次 6 支援分配 IP 網段版本：IPv6。

實機操作：進入操作畫面顯示 IPv4v6 設定。



# 陸、介接測試計畫

## 一、 介接測試項目

實測驗證平臺系統邏輯元件之介接測試、實測驗證平臺系統邏輯元件之連線或信令測試，介接測試項目詳列如下表 14。

表 14、介接測試項目

| 項次 | 測試內容 | 操作方式 |
|---|---|---|
| 1 | 5G radio band scanning | UE 可掃描搜尋到 5G N78 頻段之無線電廣播訊號 |
| 2 | UE attached with successful | UE 註冊至 5G 網路成功 |
| 3 | UE attached with failure | UE 註冊至 5G 網路失敗 |
| 4 | UE de-attached with successful case | UE 從 5G 網路離線成功 |
| 5 | UE integrity protection | UE 發送之控制封包具備完整性資安保護 |
| 6 | UE data traffic interoperability | UE 可正常透過 5G 網路與其他設備聯通 |
| 7 | Network slicing access privileges | gNB 與 5GC 建立 NG 協定連線時，只有設定合法 network slicing 的 gNB 才能成功建立連線 |

## 二、 測試內容說明

### (一)5G radio band scanning

為驗證 5G gateway 可確實掃描搜尋到 5G 模擬器所廣播 5G N78 頻段之無線電廣播訊號，確認設備之間介接具備基本的互通性，執行以下測試步驟如圖 8：

- 步驟 1: 啟動 5G 模擬器，確認 5G 核心網路元件與基地台功能正常啟動
- 步驟 2: 啟動 5G gateway 系統，使 5G gateway 於系統開啟後進

入 5G 頻段廣播訊號掃描模式，開始掃描 5G gateway 可以接收到之 5G SA 廣播訊號 MIB、SIB1

- 步驟 3: 確認 5G gateway 所掃描到的 5G SA 訊號包含 5G 模擬器所發送之訊號，可明確辨識到 5G 模擬器所發送包含 PLMN ID 為 99901 之無線電訊號

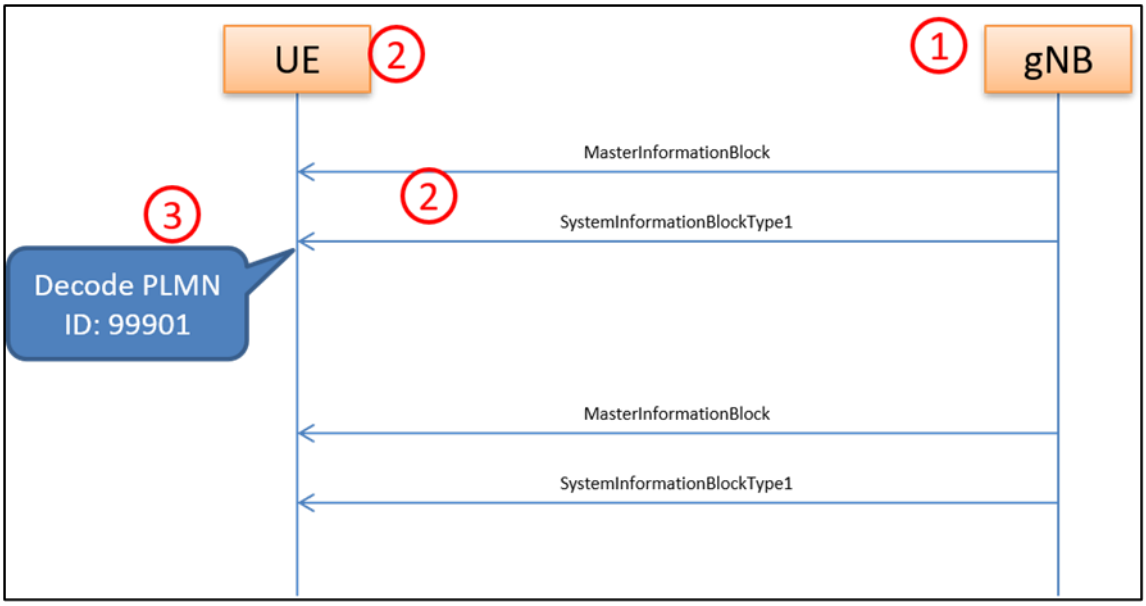



圖 8、5G radio band scanning 訊息流程圖

(二)UE attached with successful

為驗證 5G gateway 與 5G 模擬器可依照 3GPP 標準註冊流程進行網路註冊與連線，執行以下測試步驟如圖 9：

- 步驟 1: 啟動 5G 模擬器，確認 5G 核心網路元件與基地台功能正常啟動
- 步驟 2: 啟動 5G gateway 系統，使 5G gateway 於系統開啟後自動進行 5G 網路掃描與註冊動作，與 5G 模擬器進行標準註冊流程
- 步驟 3: 檢查訊息流程與內容，註冊流程相關資訊中確實完成 UE 與 gNB 之間 AS RRC 層連線設定：

1. 於 Registration Request 中包含 5G gateway 所設定之 UE IMSI 資訊，
2. 經由 5G 模擬器中核心網路元件完成終端使用者認證與鑒權流程，

3. 隨後進行 UE 與 gNB 之間、UE 與核心網路之間所使用訊息加密與正確性保護資訊安全演算法協商流程，
4. 最後由 5G gateway 接收到 5G 模擬器所發重之 Registration Accept 訊息，完成 5G 註冊流程，並符合下圖之訊息流程。

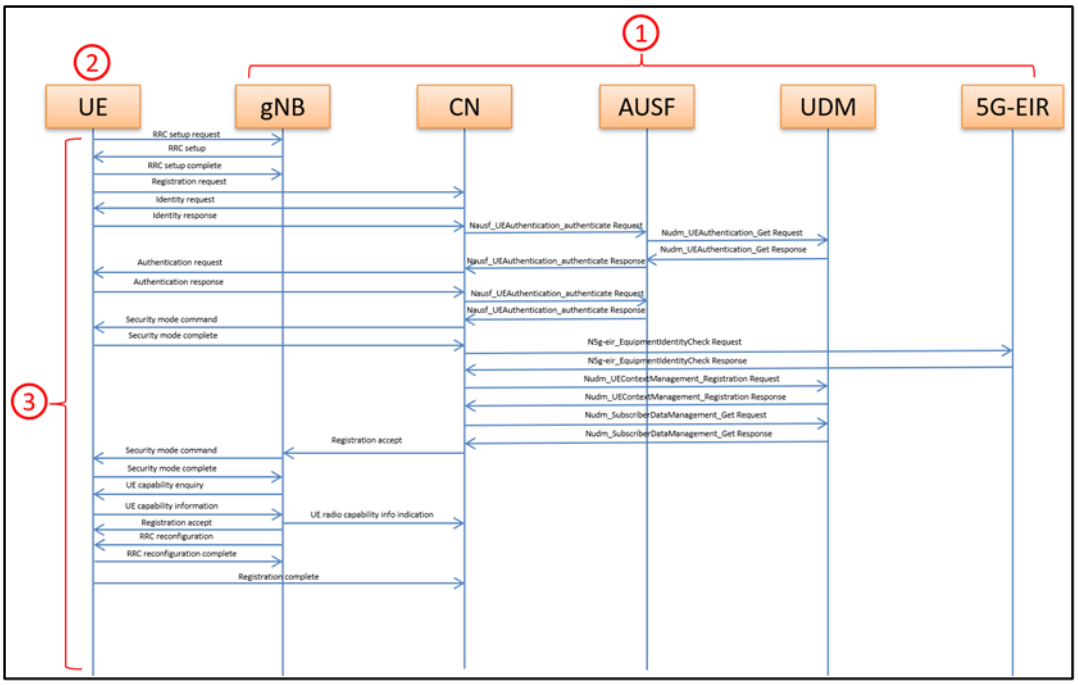



圖 9、UE attached with successful 訊息流程圖

(三)UE attached with failure

為驗證 5G 系統依照 3GPP 標準流程驗證 5G 終端資訊，確保 5G 網路不被未知裝置或使用者接入，執行以下測試步驟如圖 10：

- 步驟 1: 刪除 5G 核網中已加入之 5G Gateway UE IMSI 等使用者資訊設定
- 步驟 2: 重新啟動 5G 模擬器，使新設定可讀取進入 UDM 資料庫
- 步驟 3:重新啟動 5G gateway 系統，使系統開機後嘗試接入 5G 網路進行註冊流程
- 步驟 4: 檢查訊息流程與內容，註冊流程相關資訊中確實包含 5G gateway 所設定之 UE IMSI 資訊，並接收到由 5G 核心網路所發送之 Registration reject 控制訊令，並符合下圖之訊息流程。

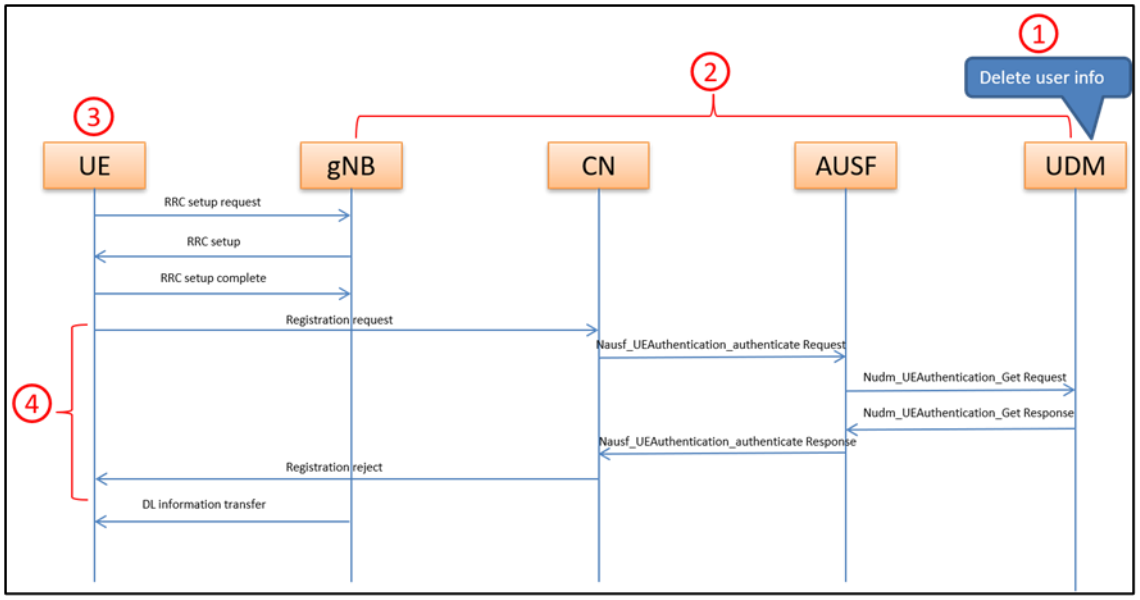



圖 10、UE attached with failure 訊息流程圖

(四)UE de-attached with successful

為驗證 5G gateway 正常提供符合 3GPP 標準離線流程，並確保整體 5G 網路的穩固性及安全性，執行以下測試步驟如圖 11：

- 步驟 1: 確認 5G gateway 已註冊進 5G 網路，並獲得 IP 位址
- 步驟 2: 關閉 5G gateway 電源，5G gateway 依照 3GPP 標準流程進行 Deregistration 流程
- 步驟 3: 檢查訊息流程與內容確實包含 5G gateway 註冊所獲得之 5G-GUTI 參數以及 gNB 確實發送 RRC release，並符合下圖之訊息流程

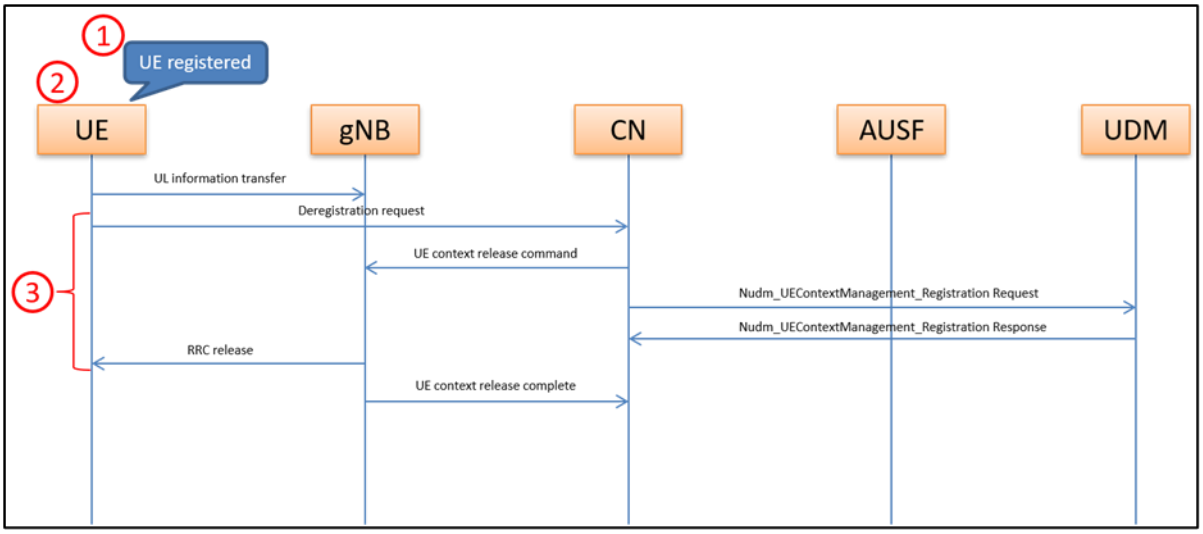



圖 11、UE de-attached with successful 訊息流程圖

(五)UE integrity protection

為驗證 UE 發送之控制封包具備完整性資安保護，執行以下測試步驟如圖 12：

- 步驟 1: 啟動 5G 模擬器，確認 5G 核心網路元件與基地台功能正常啟動
- 步驟 2: 啟動 5G gateway 系統，使 5G gateway 於系統開啟後自動進行 5G 網路掃描與註冊動作，與 5G 模擬器進行標準註冊流程
- 步驟 3: 檢查訊息內容與流程，SecurityModeCommand 訊息中指定之完整性保護演算法不為 NIA0，並且之後的 NAS 層訊息皆包含依據訊息內容雜湊之 MAC-I 值，未出現 Integrity check failed 之訊息

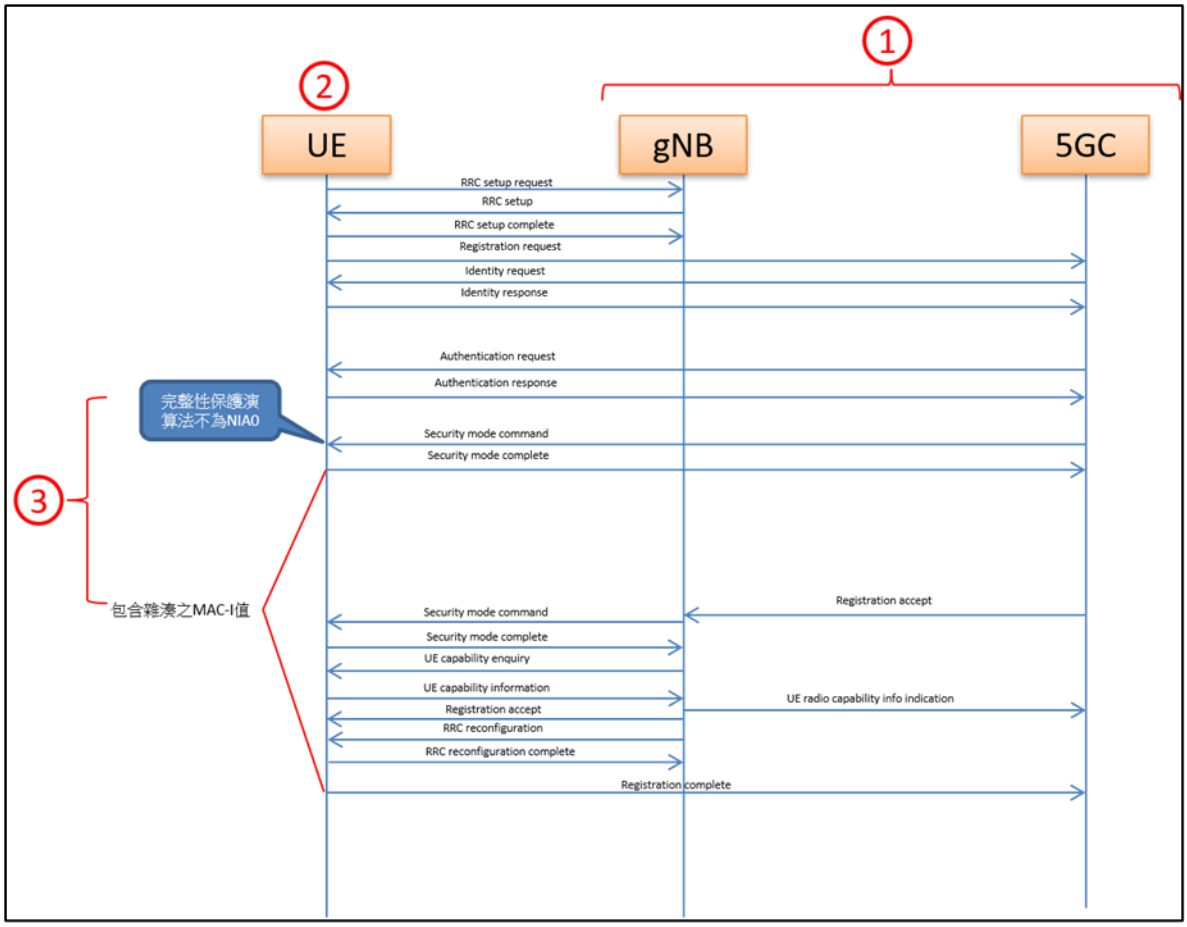



圖 12、UE integrity protection 訊息流程圖

(六)UE data traffic interoperability

為驗證 UE 可正常透過 5G 網路與其他設備聯通，確保資料平面介接互通性，執行以下測試步驟如圖 13：

- 步驟 1:啟動 5G 模擬器，確認 5G 核心網路元件與基地台功能正常啟動
- 步驟 2:啟動 5G gateway 系統，使 5G gateway 於系統開啟後自動進行 5G 網路掃描與註冊動作，與 5G 模擬器進行標準註冊流程
- 步驟 3:5G gateway 發起 PDU Session Establishment Request 請求，接收 PDU Session Establishment Response 後取得由 5GC 配發之 IPv4 位址，獲得資料平面傳輸能力
- 步驟 4:使用 Ping 工具與其他設備聯通，確認 5G gateway 獲得 ICMP Echo Response 證明具備資料平面互通性

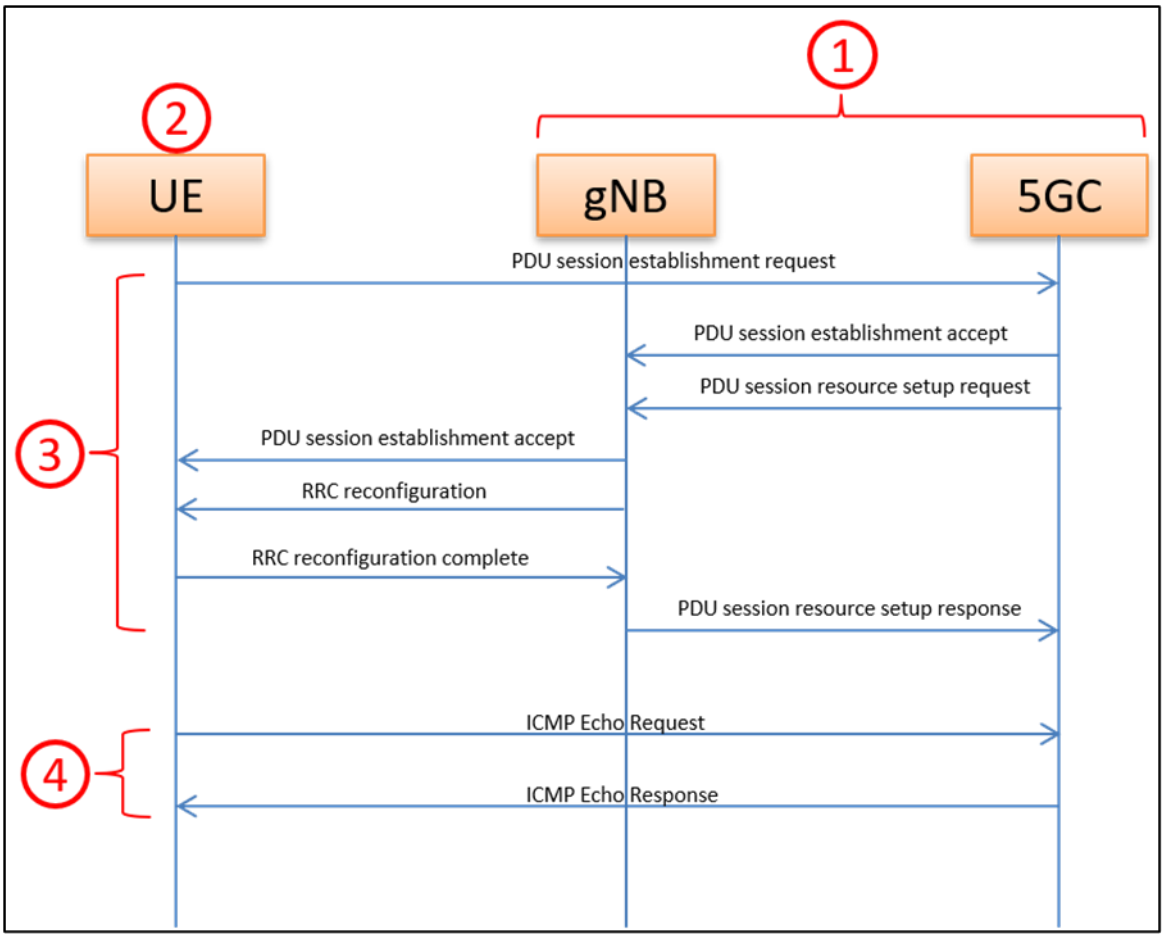



圖 13、UE data traffic interoperability 訊息流程圖

(七)Network slicing access privileges

為符合本案 5G 網路切片之情境，驗證只有設定合法網路切片參數 NSSAI 的正確數值才可以正常與 5GC 建立 NG 連線，驗證其網路切片功能正常運作，執行以下測試步驟如圖 14：

- 步驟 1:啟動 5G 模擬器，設定 5GC 可接受之網路切片參數 NSSAI SST 值為 1，啟動 5GC 元件
- 步驟 2:設定 gNB 可服務之網路切片參數 NSSAI SST 值為 2，啟動 gNB 元件與 5GC 建立 NG 協定連線
- 步驟 3:檢查訊息內容，5GC 應正確回覆 NG setup failure 訊息，並且失敗原因為 slice-not-supported
- 步驟 4:關閉 gNB 元件，修改 gNB 設定 NSSAI SST 值為 1，啟動 gNB 元件與 5GC 建立 NG 協定連線
- 步驟 5:檢查訊息內容，5GC 應正確回覆 NG setup response 訊息

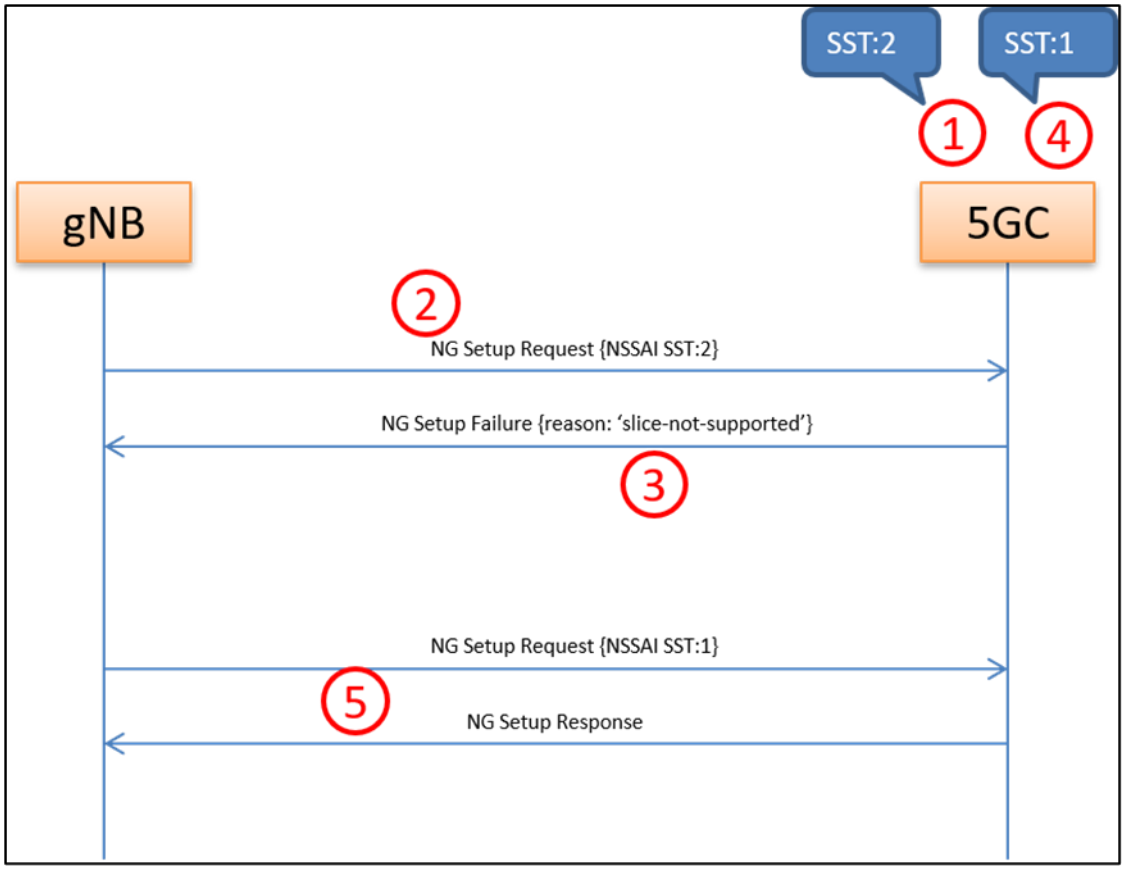



圖 14、Network slicing access privileges 訊息流程圖

# 柒、介接測試結果

一、 介接測試項目

實測驗證平臺系統邏輯元件之介接測試、實測驗證平臺系統邏輯元件之連線或信令測試，介接測試結果詳列如下表 15。

表 15、介接測試結果

| 項次 | 測試內容 | 預期結果 | 測試結果 |
|---|---|---|---|
| 1 | 5G radio band scanning | UE 可掃描搜尋到 5G N78 頻段之無線電廣播訊號 | UE 掃描搜尋到 5G 模擬器，其掃描結果包含 99901 之 5G 網路訊號 |
| 2 | UE attached with successful | UE 註冊至 5G 網路成功 | UE 註冊成功，UE 成功接收到 5G 模擬器所發送之 Registration Accept 訊息 |
| 3 | UE attached with failure | UE 註冊至 5G 網路失敗 | 將 UE 資訊移除後，使 UE 註冊遭拒，UE 收到 5G 模擬器所發送之 Registration reject 訊息 |
| 4 | UE de-attached with successful case | UE 從 5G 網路離線成功 | 關閉 5G gateway 功能與電源，5G gateway 依照 3GPP 標準流程傳送 Deregistration request，內容包含 5G gateway 註冊所獲得之 5G-GUTI 參數並接收到 gNB 發送之 RRC release |
| 5 | UE integrity protection | UE 發送之控制封包具備完整性資安保護 | SecurityModeCommand 訊息中指定之完整性保護演算法為 5G NIA1，與 NAS 層訊息皆包含依據訊息內容雜湊之 MAC-I 值，且註冊過程中未出現 Integrity check failed 之訊 |

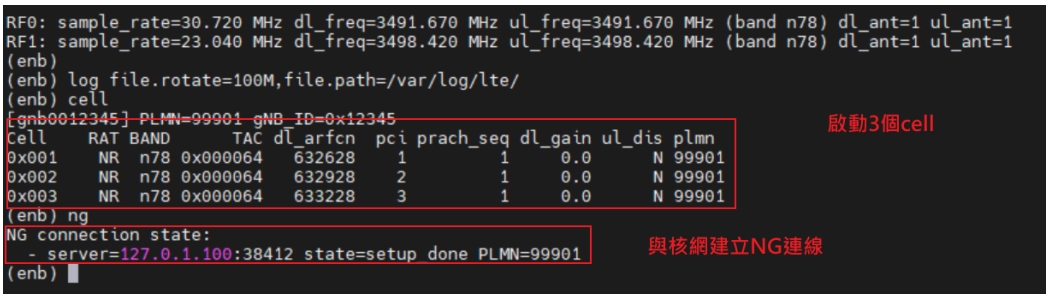
| 項次 | 測試內容 | 預期結果 | 測試結果 |
|---|---|---|---|
| | | | 息 |
| 6 | UE data traffic interoperability | UE 可正常透過 5G 網路與其他設備聯通 | UE 可取得 5GC 所配發之 IPv4 位址，並順利使用 Ping 工具與其他設備聯通，5G gateway 接收到 Google DNS 回覆之 ICMP Echo Response 證明具備資料平面互通性 |
| 7 | Network slicing access privileges | gNB 與 5GC 建立 NG 協定連線時，只有設定合法 network slicing 的 gNB 才能成功建立連線 | gNB 與 5GC 建立 NG 協定連線時，只有設定合法 network slicing 的 gNB 才會成功建立連線並回覆 NG setup response 訊息 |

二、 測試結果說明

(一)5G radio band scanning

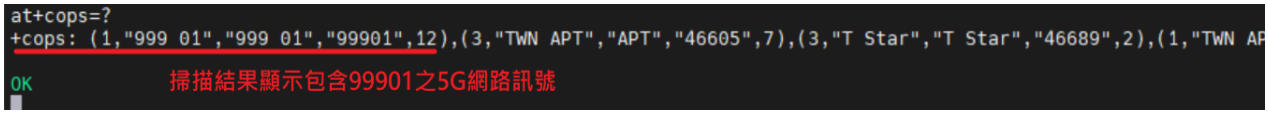
為驗證 5G gateway 可確實掃描搜尋到 5G 模擬器所廣播 5G N78 頻段之無線電廣播訊號，確認設備之間介接具備基本的互通性，執行以下測試步驟：

- 步驟 1： 啟動 5G 模擬器，5G 核心網路元件與基地臺功能正常啟動



- 步驟 2： 啟動 5G gateway 系統，使 5G gateway 於系統開啟後進入 5G 頻段廣播訊號掃描模式，開始掃描 5G gateway 可以接收到之 5G SA 廣播訊號 MIB、SIB1

- 步驟 3： 確認 5G gateway 所掃描到的 5G SA 訊號包含 5G 模擬器所發送之訊號，可明確辨識到 5G 模擬器所發送包含 PLMN ID 為 99901 之無線電訊號

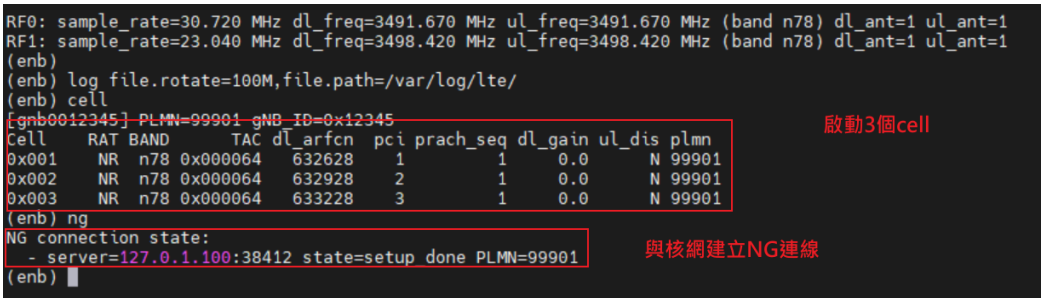



- 期望結果：UE 可掃描搜尋到 5G N78 頻段之無線電廣播訊號
- 實際測試結果：UE 掃描搜尋到 5G 模擬器，其掃描結果包含 99901 之 5G 網路訊號

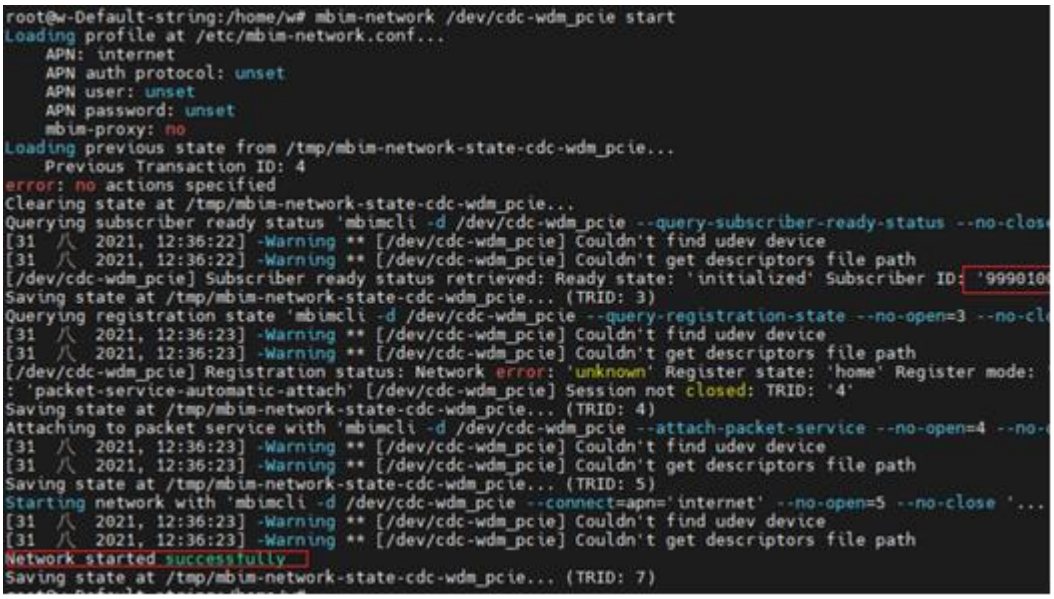
(二)UE attached with successful

為驗證 5G gateway 與 5G 模擬器可依照 3GPP 標準註冊流程進行網路註冊與連線，執行以下測試步驟：

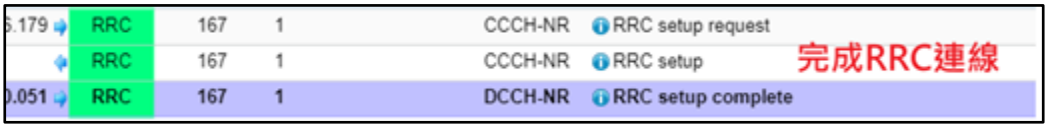
- 步驟 1： 啟動 5G 模擬器，5G 核心網路元件與基地臺功能正常啟動。

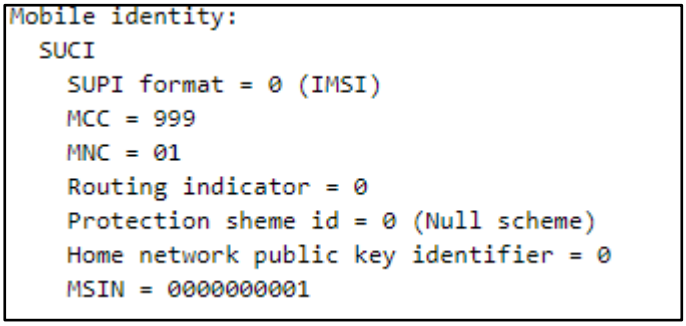


➢ 步驟 2： 啟動 5G gateway 系統，使 5G gateway 於系統開啟後自動進行 5G 網路掃描與註冊動作，與 5G 模擬器進行標準註冊流程。

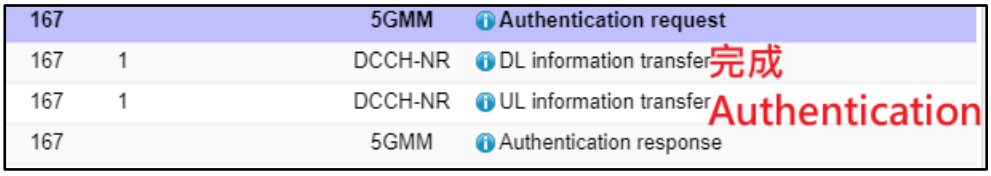



➢ 步驟 3： 檢查訊息流程與內容，註冊流程相關資訊中確實完成 UE 與 gNB 之間 AS RRC 層連線設定，於 Registration Request 中包含 5G gateway 所設定之 UE IMSI 資訊，

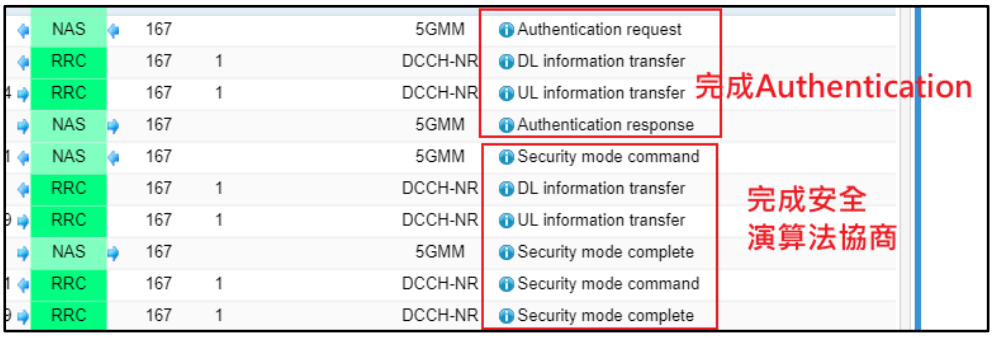



經由 5G 模擬器中核心網路元件完成終端使用者認證與鑒權流程



隨後進行 UE 與 gNB 之間、UE 與核心網路之間所使用訊息加密與正確性保護資訊安全演算法協商流程。




最後由 5G gateway 接收到 5G 模擬器所發重之 Registration Accept 訊息，完成 5G 註冊流程，並符合下圖之訊息流程。

```
Protocol discriminator = 0x7e (5GS Mobility Management)
Security header = 0x2 (Integrity protected and ciphered)
Auth code = 0x596e42b3
Sequence number = 0x01
Protocol discriminator = 0x7e (5GS Mobility Management)
Security header = 0x0 (Plain 5GS NAS message, not security protected)
Message type = 0x42 (Registration accept)
5GS registration result = 0x09 (Emergency registered=0, NSSAA to be performed=0, SMS allowed=1, 3GPP access)
5G-GUTI:
  5G-GUTI
    MCC = 999
    MNC = 01
    AMF Region ID = 128
    AMF Set ID = 4
    AMF Pointer = 1
    5G-TMSI = 0xb502cc99
TAI list:
  Length = 7
  Data = 00 99 f9 10 00 00 64
Allowed NSSAI:
  S-NSSAI
    Length of S-NSSAI contents = 1 (SST)
    SST = 0x01
  S-NSSAI
    Length of S-NSSAI contents = 1 (SST)
    SST = 0x02
  S-NSSAI
    Length of S-NSSAI contents = 1 (SST)
    SST = 0x03
T3512 value:
  Value = 30
  Unit = 5 (1 minute)
```

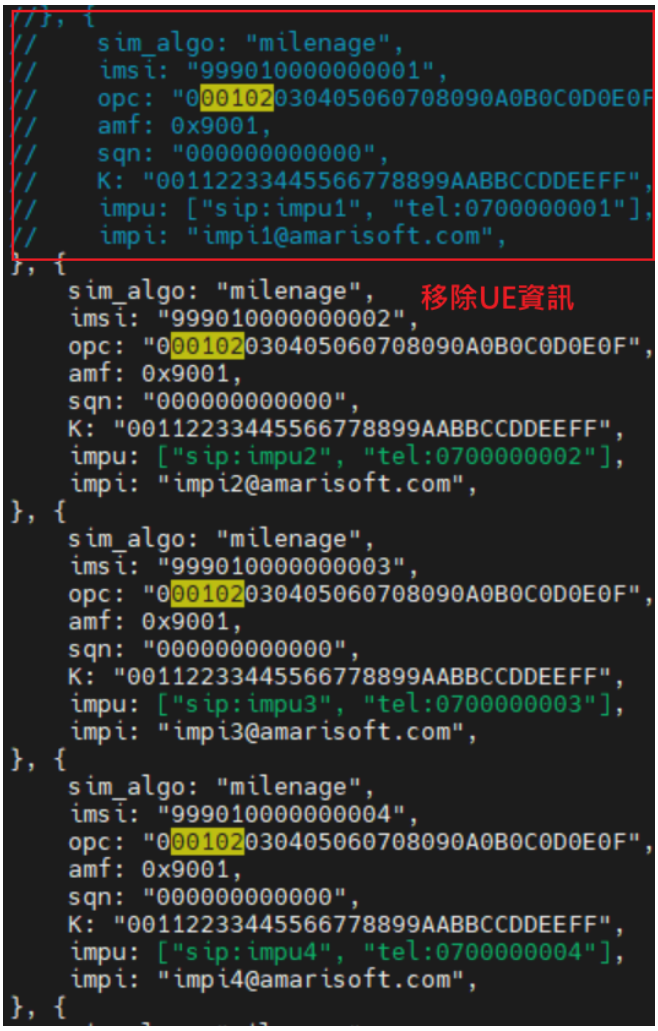
UE成功註冊，接收到Accpet訊息

- 期望結果：UE 註冊至 5G 網路成功
- 實際測試結果：UE 註冊成功，UE 成功接收到 5G 模擬器所發送之 Registration Accept 訊息

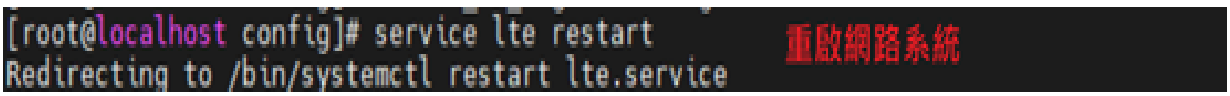
(三)UE attached with failure

為驗證 5G 系統依照 3GPP 標準流程驗證 5G 終端資訊，確保 5G 網路不被未知裝置或使用者接入，執行以下測試步驟：

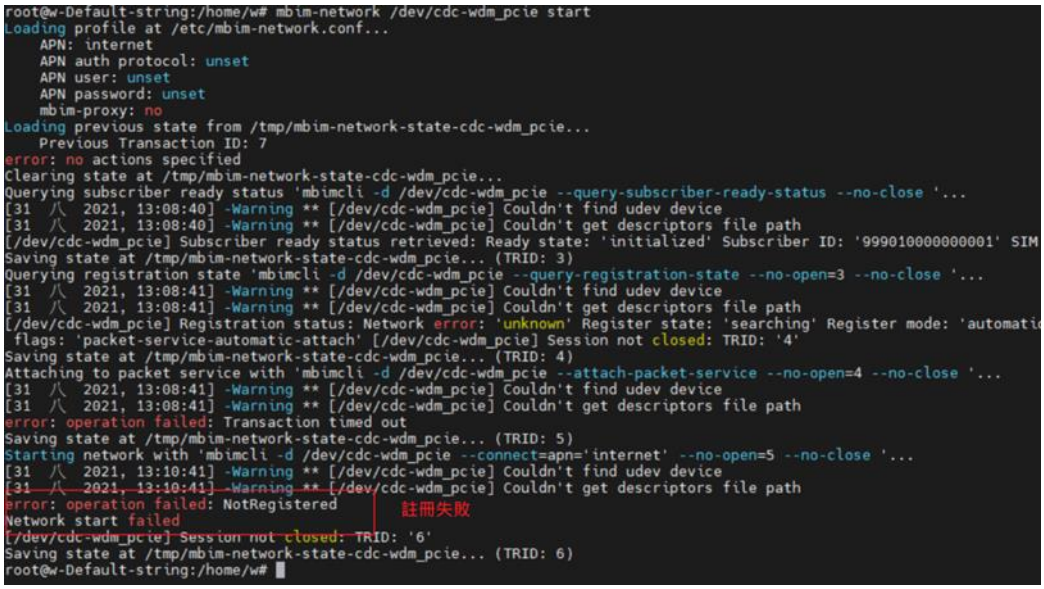
- 步驟 1：刪除 5G 核網中已加入之 5G Gateway UE IMSI 等使用者資訊設定



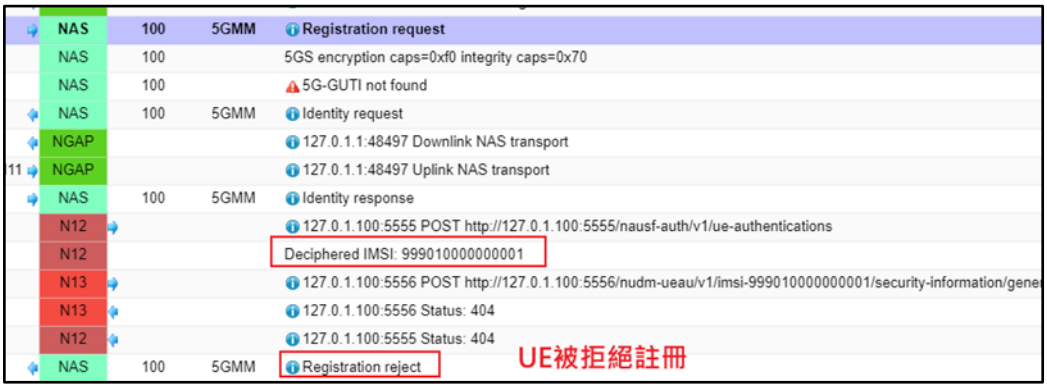

- 步驟 2：重新啟動 5G 模擬器，使新設定可讀取進入 UDM 資料庫



- 步驟 3：重新啟動 5G gateway 系統，使系統開機後嘗試接入 5G 網路進行註冊流程




- 步驟 4： 檢查訊息流程與內容，註冊流程相關資訊中確實包含 5G gateway 所設定之 UE IMSI 資訊，並接收到由 5G 核心網路所發送之 Registration reject 控制訊令，並符合下圖之訊息流程。

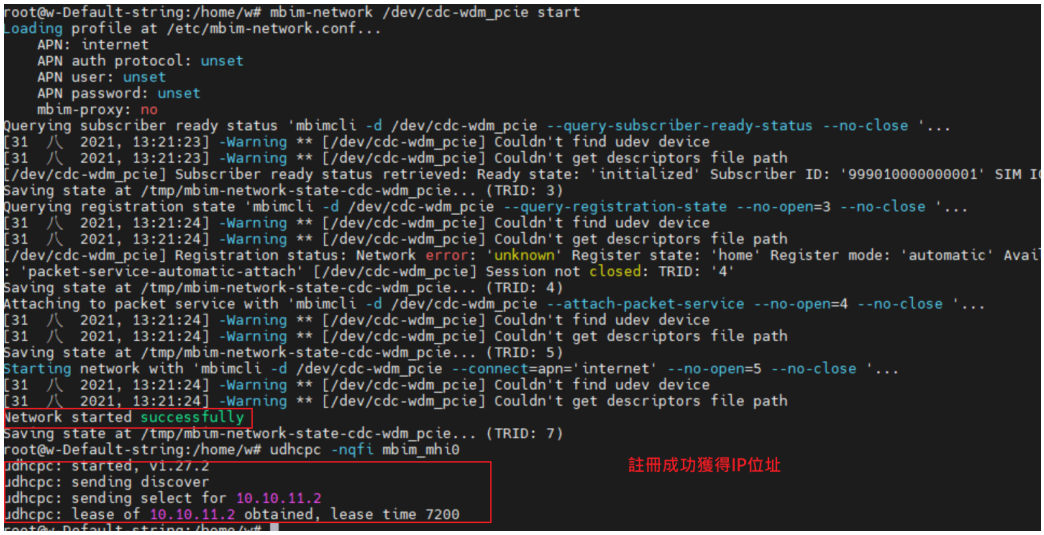



- 期望結果：UE 註冊至 5G 網路失敗
- 實際測試結果：將 UE 資訊移除後，使 UE 註冊遭拒，UE 收到 5G 模擬器所發送之 Registration reject 訊息

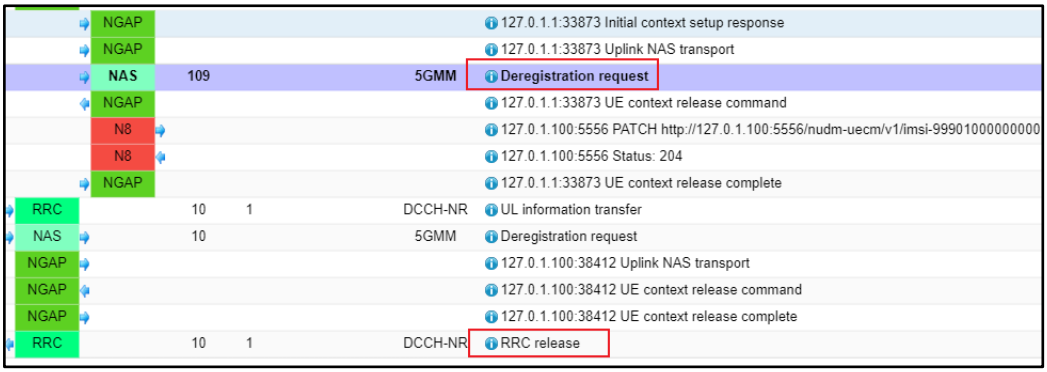
(四)UE de-attached with successful

為驗證 5G gateway 正常提供符合 3GPP 標準離線流程，並確保整體 5G 網路的穩固性及安全性，執行以下測試步驟：

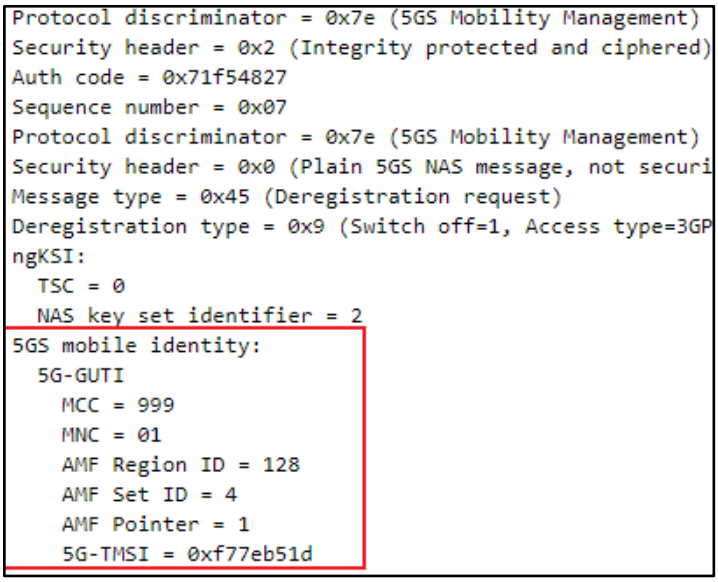
- 步驟 1： 確認 5G gateway 已註冊進 5G 網路，並獲得 IP 位址




- 步驟 2： 關閉 5G gateway 電源，5G gateway 依照 3GPP 標準流程進行 Deregistration 流程



- 步驟 3： 檢查訊息流程與內容確實包含 5G gateway 註冊所獲得之 5G-GUTI 參數以及 gNB 確實發送 RRC release。

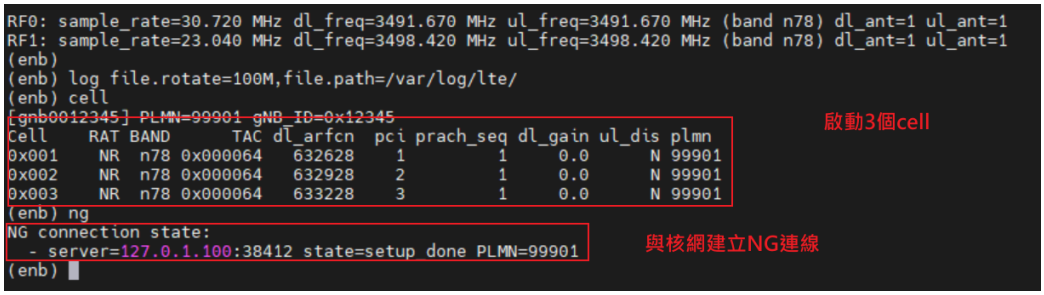



- 期望結果：UE 從 5G 網路離線成功
- 實際測試結果：關閉 5G gateway 功能與電源，5G gateway 依照 3GPP 標準流程傳送 Deregistration request，內容包含 5G gateway 註冊所獲得之 5G-GUTI 參數並接收到 gNB 發送之 RRC release

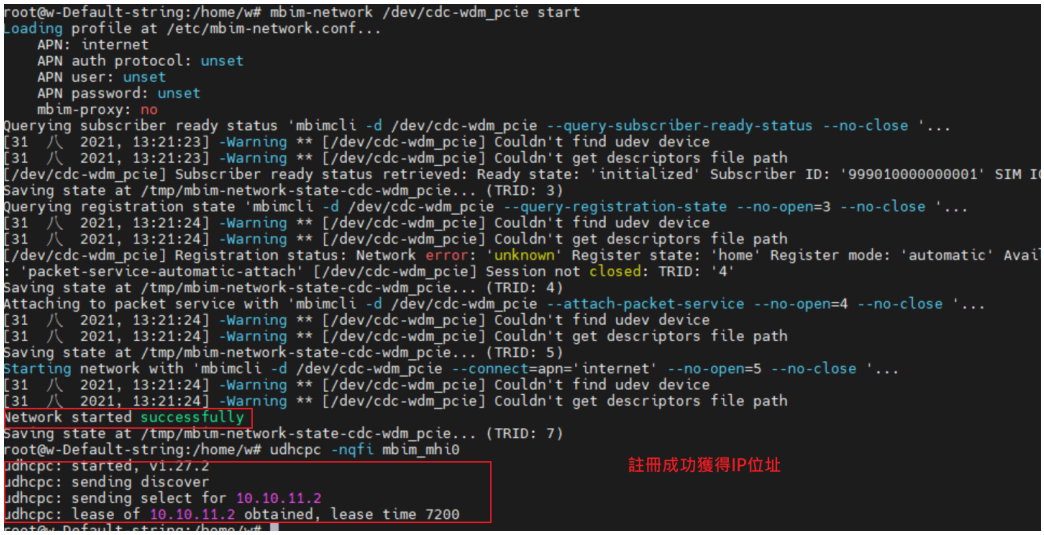
(五)UE integrity protection

為驗證 UE 發送之控制封包具備完整性資安保護，執行以下測試步驟：

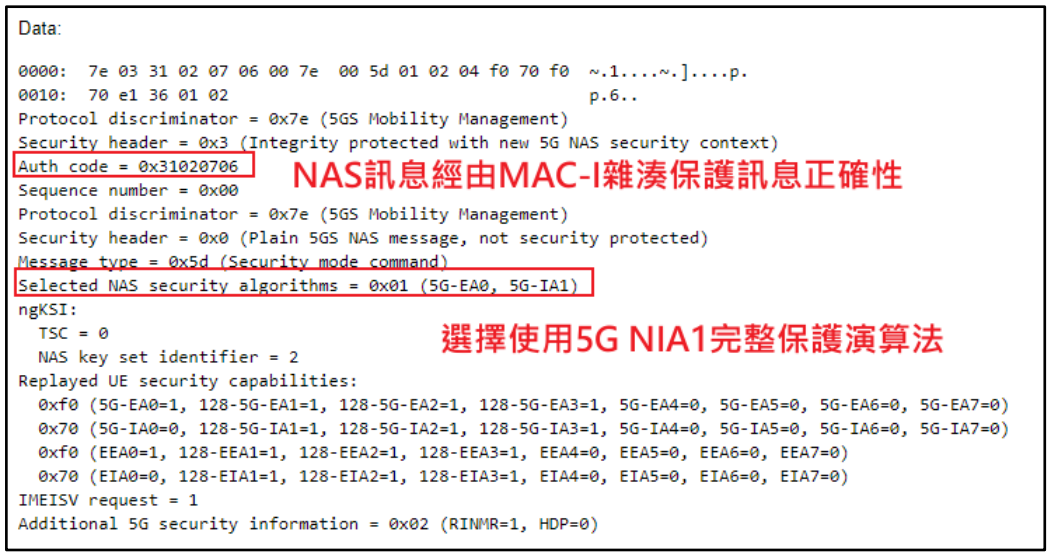
- 步驟 1： 啟動 5G 模擬器，確認 5G 核心網路元件與基地臺功能正常啟動




- 步驟 2： 啟動 5G gateway 系統，使 5G gateway 於系統開啟後自動進行 5G 網路掃描與註冊動作，與 5G 模擬器進行標準註冊流程



- 步驟 3： 檢查訊息內容與流程，SecurityModeCommand 訊息中指定之完整性保護演算法不為 NIA0，並且之後的 NAS 層訊息皆包含依據訊息內容雜湊之 MAC-I 值，未出現 Integrity check failed 之訊息

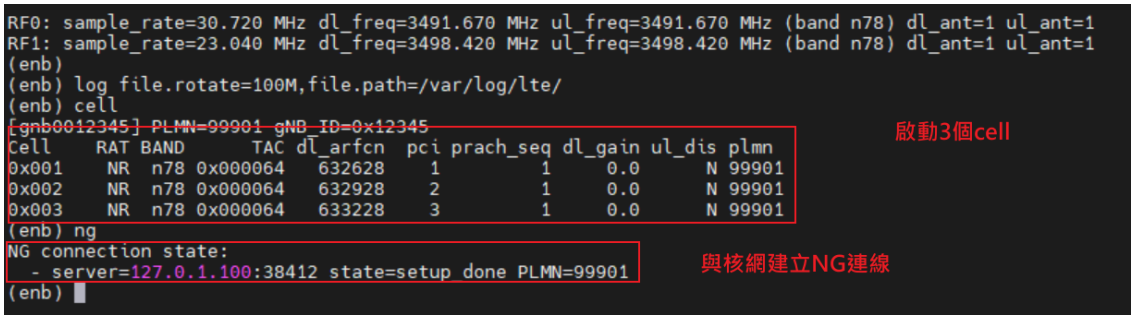


- 期望結果：UE 發送之控制封包具備完整性資安保護
- 實際測試結果： SecurityModeCommand 訊息中指定之完整性保護演算法為 5G NIA1，與 NAS 層訊息皆包含依據訊息內容雜湊之 MAC-I 值，且註冊過程中未出現 Integrity check failed 之訊息

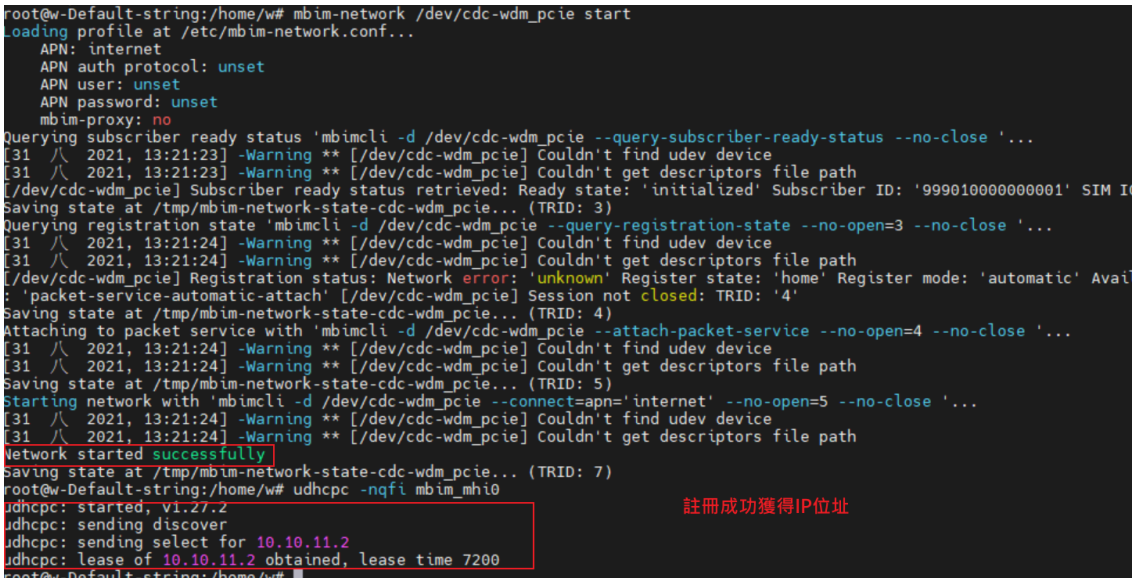
(六)UE data traffic interoperability

為驗證 UE 可正常透過 5G 網路與其他設備聯通，確保資料平面介接互通性，執行以下測試步驟：

- 步驟 1： 啟動 5G 模擬器，確認 5G 核心網路元件與基地臺功能正常啟動




- 步驟 2： 啟動 5G gateway 系統，使 5G gateway 於系統開啟後自動進行 5G 網路掃描與註冊動作，與 5G 模擬器進行標準註冊流程



- 步驟 3： 5G gateway 發起 PDU Session Establishment Request 請求，接收 PDU Session Establishment Response 後取得由 5GC 配發之 IPv4 位址，獲得資料平面傳輸能力

```
Protocol discriminator = 0x2e (5GS Session Management)
PDU session identity = 1
Procedure transaction identity = 1
Message type = 0xc2 (PDU session establishment accept)
Selected PDU session type = 0x1 (IPv4)
Selected SSC mode = 0x1 (1)
Authorized QoS rules:
  QoS rule 1:
    QoS rule identifier = 1
    Rule operation code = 1 (create new QoS rule)
    DQR = 1 (the QoS rule is the default QoS rule)
    Number of packet filters = 1
    Packet filter identifier = 15
      Packet filter direction = 3 (bidirectional)
      Match-all
    QoS rule precedence = 255
    QFI = 1
Session AMBR:
  Session-AMBR for downlink = 3000000 kbps
  Session-AMBR for uplink = 1000000 kbps
5GSM cause = 0x32 (PDU session type IPv4 only allowed)
PDU address:
  SI6LLA = 0
  PDU session type = 1 (IPv4)
  IPv4 = 10.10.11.2
S-NSSAI:
  Length of S-NSSAI contents = 1 (SST)
  SST = 0x01
```

5GC 配發之IP

- 步驟 4： 使用 Ping 工具與其他設備聯通，確認 5G gateway 獲得 ICMP Echo Response 證明具備資料平面互通性

```
root@w-Default-string:/home/w# ping 8.8.8.8 -I mbim_mhi0
PING 8.8.8.8 (8.8.8.8) from 10.10.11.2 mbim_mhi0: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=177 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=16.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=35.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=34.2 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=56 time=33.2 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=56 time=32.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=56 time=32.2 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=56 time=30.2 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=56 time=29.1 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=56 time=29.7 ms
^C
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 16.571/45.166/177.902/44.529 ms
```

可與Google dns連通

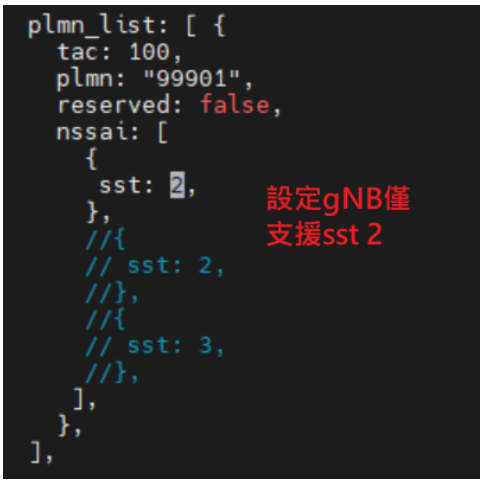
- 期望結果：UE 可正常透過 5G 網路與其他設備聯通
- 實際測試結果：UE 可取得 5GC 所配發之 IPv4 位址，並順利使用 Ping 工具與其他設備聯通，5G gateway 接收到 Google DNS 回覆之 ICMP Echo Response 證明具備資料平面互通性

(七)Network slicing access privileges

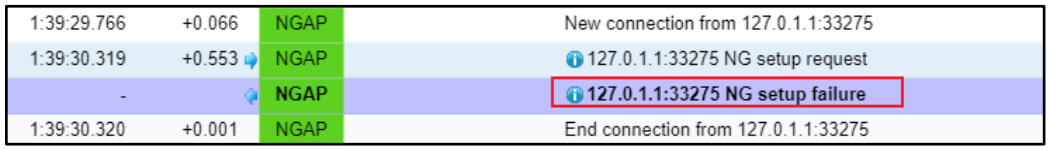
為符合本案 5G 網路切片之情境，驗證只有設定合法網路切片參數 NSSAI 的正確數值才可以正常與 5GC 建立 NG 連線，驗證其網路切片功能正常運作，執行以下測試步驟：

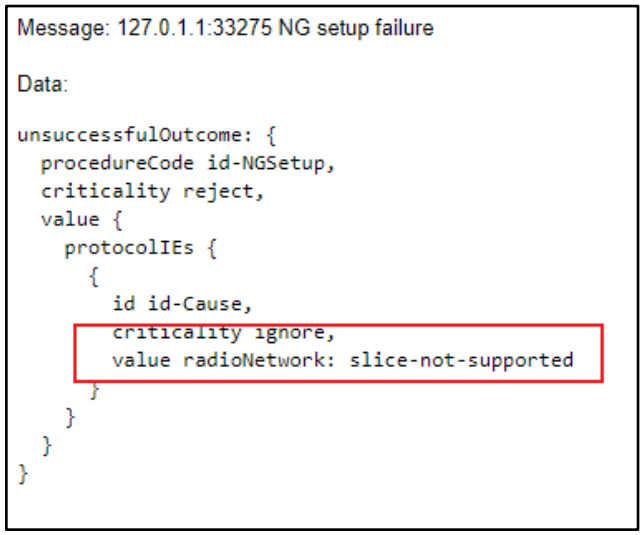
- 步驟 1:啟動 5G 模擬器，設定 5GC 可接受之網路切片參數 NSSAI SST 值為 1，啟動 5GC 元件。

- 步驟 2： 設定 gNB 可服務之網路切片參數 NSSAI SST 值為 2，啟動 gNB 元件與 5GC 建立 NG 協定連線。

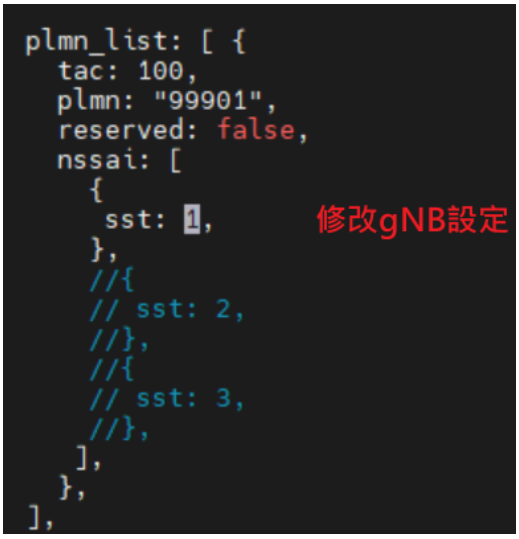


➢ 步驟 3： 檢查訊息內容，5GC 應正確回覆 NG setup failure 訊息，並且失敗原因為 slice-not-supported。




➢ 步驟 4： 關閉 gNB 元件，修改 gNB 設定 NSSAI SST 值為 1，啟動 gNB 元件與 5GC 建立 NG 協定連線。



- 步驟 5： 檢查訊息內容，5GC 應正確回覆 NG setup response 訊息。

Message: 127.0.1.1:54755 NG setup response

Data:

```
successfulOutcome: {
  procedureCode id-NGSetup,
  criticality reject,
  value {
    protocolIEs {
      {
        id id-AMFName,
        criticality reject,
        value "amarisoft.amf.5gc.mnc001.mcc999.3gppnetwork.org"
      },
      {
        id id-ServedGUAMIList,
        criticality reject,
        value {
          {
            gUAMI {
              pLMNIdentity '99F910'H,
              aMFRegionID '80'H,
              aMFSetID '0000000100'B,
              aMFPointer '000001'B
            }
          }
        }
      },
      {
        id id-RelativeAMFCapacity,
        criticality ignore,
        value 50
      },
      {
        id id-PLMNSupportList,
        criticality reject,
        value {
          {
            pLMNIdentity '99F910'H,
            sliceSupportList {
              {
                s-NSSAI {
                  sST '01'H
                }
```

- 期望結果：gNB 與 5GC 建立 NG 協定連線時，只有設定合法 network slicing 的 gNB 才能成功建立連線
- 實際測試結果：gNB 與 5GC 建立 NG 協定連線時，只有設定合法 network slicing 的 gNB 才會成功建立連線並回覆 NG setup response 訊息

## 捌、情景測試 (情境一)

本節測試主要驗證當 IoT 設備在不同 Domain 之間移動時，IoT 設備會自動取得 IP 位址，同時，DNS Server 上也會動態更改 A Record，並與其他 Domain 上的 DNS Server 交換 FQDN 資訊，達到 IoT 設備在專網間的互相通訊與辨識，自動配置(Autoconfig)與管理專網號碼。

當完成 IoT 設備在不同 Cell 之間移動進行自動註冊後，繼續將 IoT 設備在不同 Cell 之間持續移動，觀察 System Log 變化情形，另外採用程式模擬方式產生大量靜態物聯網裝置，檢視其支援大量設備自動註冊的能力。IoT 設備初始設定的參數如下表 16：

表 16、IoT 設備初始參數

| | IoT_1 | IoT _2 | IoT _3 | IoT _4 |
|---|---|---|---|---|
| DNN | internet1 | internet2 | internet3 | internet4 |
| IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| NSSAI | eMBB | eMBB | URLLC | MIOT |
| SST | 1 | 1 | 2 | 3 |
| Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic<br>Machines | Smart City<br>Sensors |
| Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |

一、 同域測試項目

IoT 設備從 Cell_1 移動到 Cell_2，觀察 IP 與域名變化，同域測試內容如表 17。

表 17、同域測試

| 項次 | 測試內容 | 預期結果 |
|---|---|---|
| 1 | 5G 模擬器及 DNS 間的編碼核配與管理 | 5G 模擬器可以透過 Radius 協議將 IP：IMSI：IMEI：Cell ID 資訊傳給 DNS |
| 2 | Device 取得 IP (IPv4/IPv6)與 DNS mapping | 5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致 |
| 3 | DNS 編碼核配與管理 | DNS 可以依據 5G 模擬器產生 Radius 內容自動產出 A Record |
| 4 | 多個 Device 註冊 DNS 與核配編碼 | 比對各 5G 模擬器及 DNS：Device IP、IMSI、IMEI 及 Cell ID 結果一致 |

(一)IP 註冊與 DNS 動態管理流程

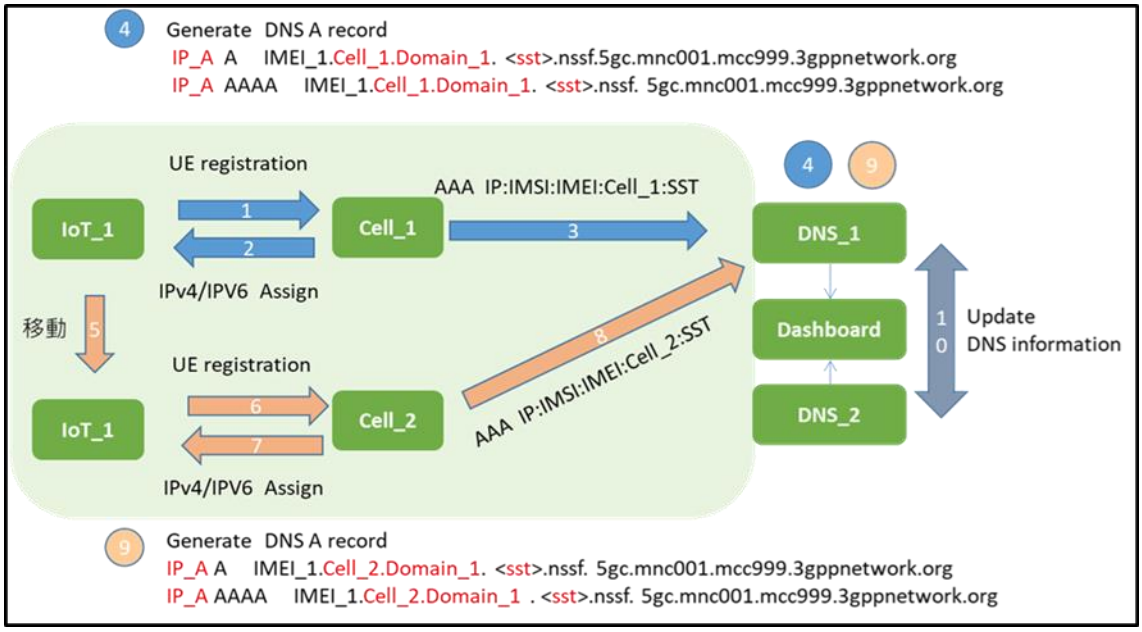



圖 15、同域移動之 IP 註冊與 DNS 動態管理流程

(二)驗證測試步驟及操作結果

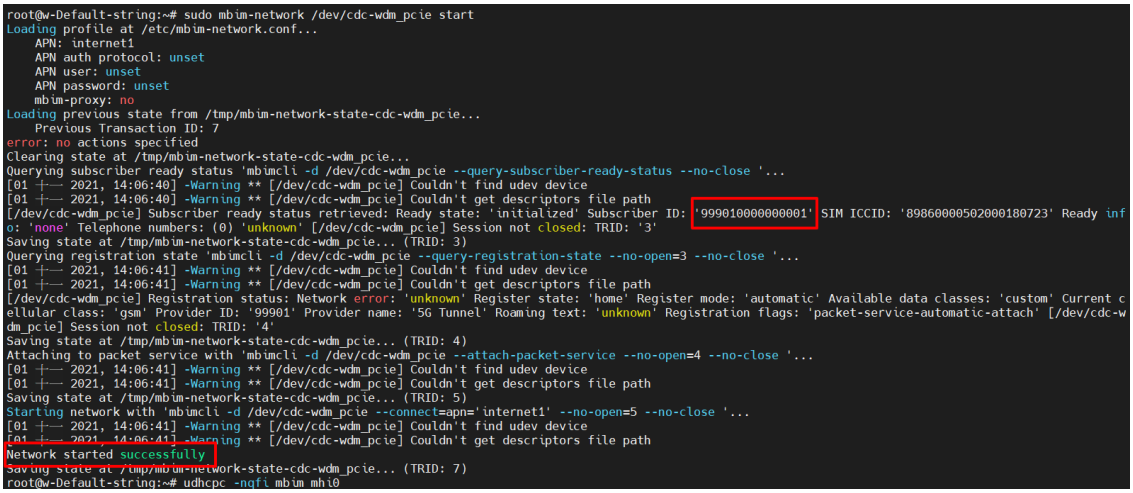
同域移動測試步驟說明如表 18。

表 18、同域移動之 IP 註冊與 DNS 動態管理流程

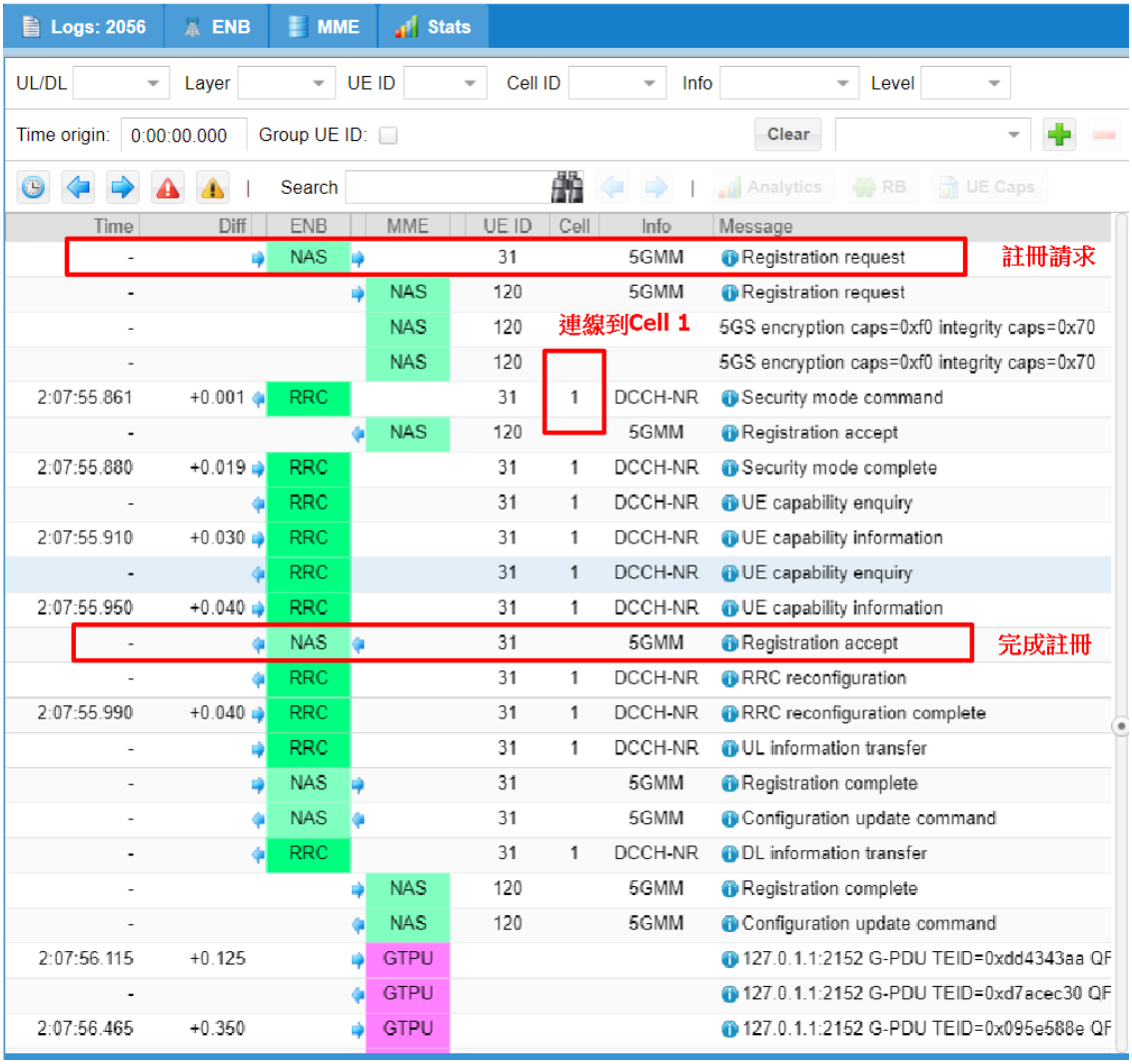
| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_1，並進行註冊 |
| 2 | 配發 IPv4/IPV6 位址 | 5G 模擬器配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | 傳送[IP：IMSI：IMEI：Cell_1：SST]等資訊至 DNS |
| 4 | Generate DNS A Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 5 | UE 移動 | IoT 從 Cell_1 移動至 Cell_2，同為 Domain_1 |
| 6 | UE registration | IoT 連線到 Cell_2，並進行註冊 |
| 7 | 配發 IPv4/IPV6 位址 | 5G 模擬器配發 IP 給 IoT，因為是同一 Domain，使用原來的 IP |
| 8 | 傳送註冊資訊至 DNS | 5G 模擬器傳送[IP：IMSI：IMEI：Cell_2：SST]等資訊至 DNS |
| 9 | Generate DNS A/AAAA Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 10 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA Record 資訊 |

➢ 步驟 1：IoT 註冊

啟動 IoT 設備連線到 5G 模擬器，並進行進行標準註冊流程

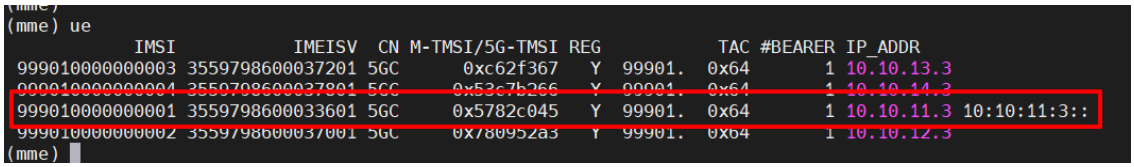



5G 模擬器顯示 IoT 設備連線至 Cell_1 並完成註冊

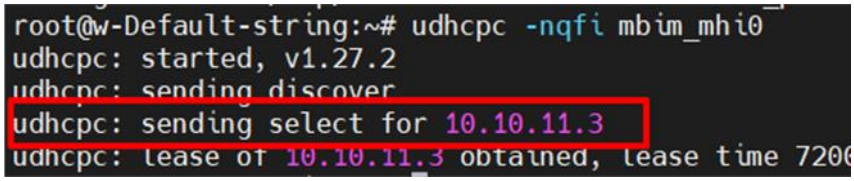


➢ 步驟 2：配發 IPv4/IPV6 位址

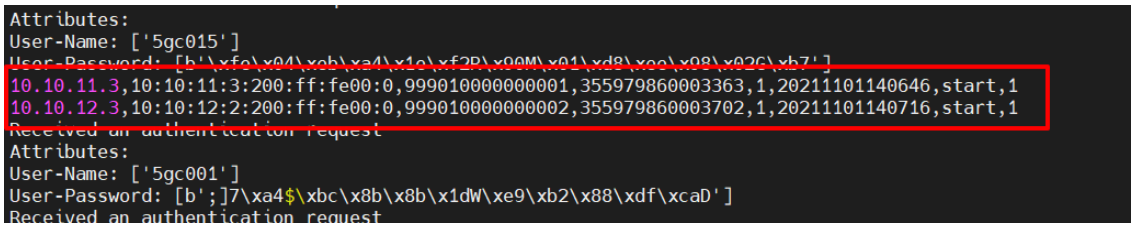
IoT 設備向 5G 模擬器要求 IP，5G 模擬器配發 IP 給 IoT 設備。

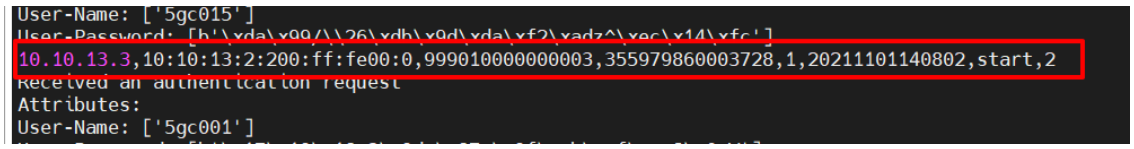


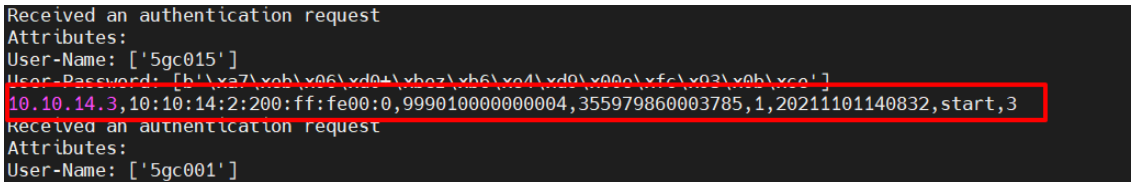

➢ 步驟 3：傳送註冊資訊至 DNS




傳送[IP：IMSI：IMEI：Cell_1：SST]等資訊至 DNS



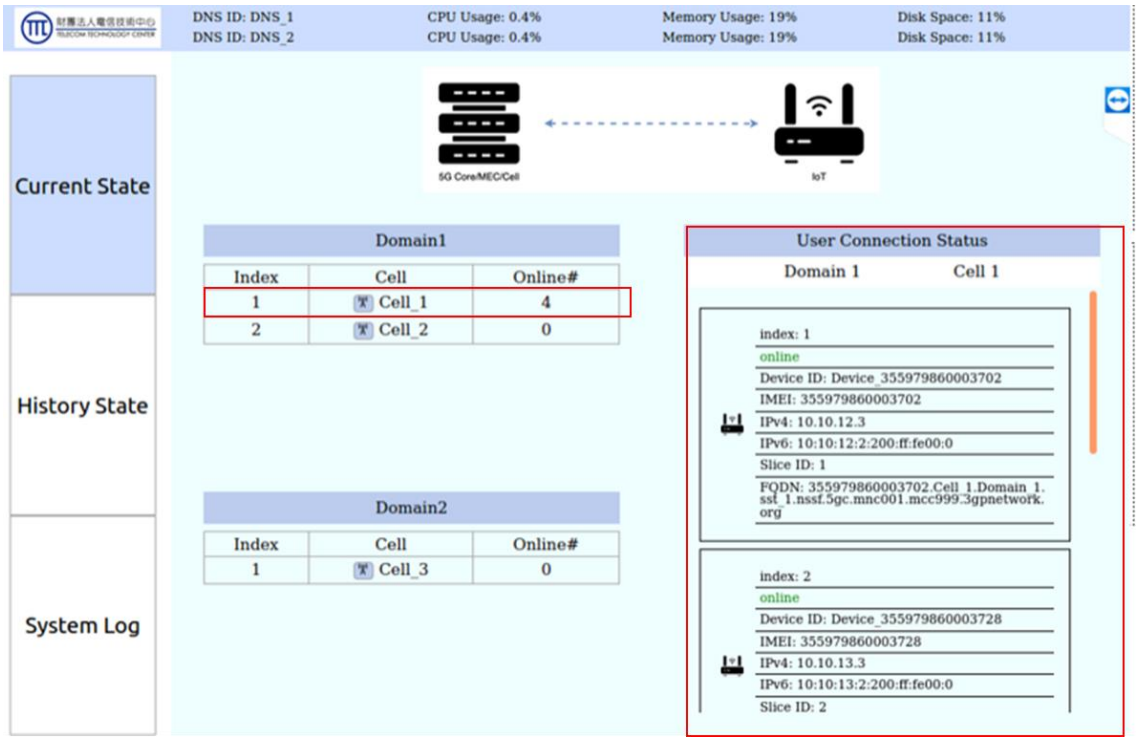



➢ 步驟 4：Generate DNS A Record

DNS 透過自動編碼程式自動產生域名以及 DNS A Record

```
cat: /home/dnsserver/script/radius.log: No such file or directory
########################################
cat nssf.5gc.mnc001.mcc999.3gppnetwork.org
########################################
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
ns      IN      A       127.0.0.1
os      IN      AAAA    ::1
355979860003363.Cell_1.Domain_1.sst_1  IN      A       10.10.11.3
355979860003363.Cell_1.Domain_1.sst_1  IN      A       10:10:11:3:200:ff:fe00:0
355979860003702.Cell_1.Domain_1.sst_1  IN      A       10.10.12.3
355979860003702.Cell_1.Domain_1.sst_1  IN      A       10:10:12:2:200:ff:fe00:0
355979860003728.Cell_1.Domain_1.sst_2  IN      A       10.10.13.3
355979860003728.Cell_1.Domain_1.sst_2  IN      A       10:10:13:2:200:ff:fe00:0
355979860003785.Cell_1.Domain_1.sst_3  IN      A       10.10.14.3
355979860003785.Cell_1.Domain_1.sst_3  IN      A       10:10:14:2:200:ff:fe00:0
```

檢視 Dashboard 畫面，可以看到 Cell_1 有 4 臺上線的 IoT 設備，點選進去可以看到這 4 臺裝置的系統資訊。



完成 1-4 步驟後，IoT 設備註冊 IP 以及自動註冊 DN 如下圖：

| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | DNN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟 1,2 | Service IP IPv4 (DHCP) | 10.10.11.3 | 10.10.12.3 | 10.10.13.3 | 10.10.14.3 |
| 步驟 1,2 | Service IP IPv6 (DHCP) | 10:10:11:3:200:ff:fe00:0 | 10:10:12:2:200:ff:fe00:0 | 10:10:13:2:200:ff:fe00:0 | 10:10:14:2:200:ff:fe00:0 |
| 步驟 3,4 | DN | 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

- 步驟 5：IoT 設備移動

  從 Cell_1 移動至 Cell_2，同為 Domain_1

```
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        34           123 0x001 0x4622
        32           121 0x001 0x4620
        30           119 0x001 0x461e
        28           117 0x001 0x461c
(enb) cell_gain 2 0
(enb) cell_gain 1 -60
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        67             - 0x002 0x4643
        32           121 0x002 0x4642
        52             - 0x002 0x4634
        45             - 0x002 0x462d
(enb)
(enb)
(enb)
(enb)
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        32           121 0x002 0x4642
(enb)
```

- 步驟 6：IoT 設備 registration

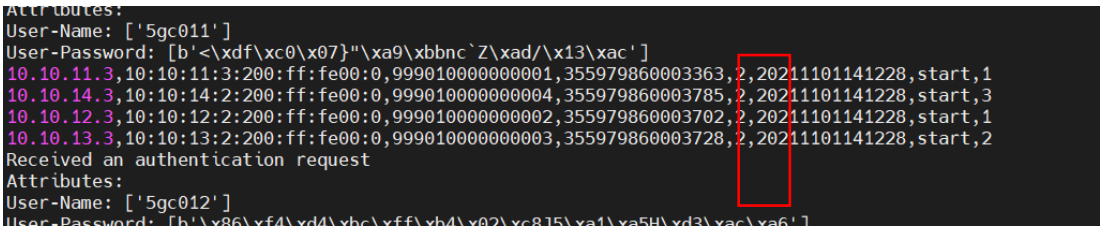
  IoT 設備連線到 Cell_2，並進行註冊

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2:12:24.590 | +1.765 | RRC | 45 | 2 | CCCH-NR | RRC reestablishment request |
| - | | RRC | 45 | 2 | DCCH-NR | RRC reestablishment |
| 2:12:24.655 | +0.065 | RRC | 52 | 2 | CCCH-NR | RRC reestablishment request |
| - | | RRC | 52 | 2 | DCCH-NR | RRC reestablishment |
| 2:12:24.795 | +0.140 | RRC | 66 (32) | 2 | CCCH-NR | RRC reestablishment request |
| - | | RRC | 66 (32) | 2 | DCCH-NR | RRC reestablishment |
| 2:12:24.815 | +0.020 | RRC | 67 | 2 | CCCH-NR | RRC reestablishment request |
| - | | RRC | 67 | 2 | DCCH-NR | RRC reestablishment |
| 2:12:24.960 | +0.145 | RRC | 66 (32) | 2 | DCCH-NR | RRC reestablishment complete |
| - | | RRC | 66 (32) | 2 | | Changing UE_ID to 0x20 |
| - | | RRC | 32 | 2 | DCCH-NR | RRC reconfiguration |
| 2:12:25.010 | +0.050 | RRC | 32 | 2 | DCCH-NR | RRC reconfiguration complete |

- 步驟 7：配發 IPv4/IPV6 位址

  5G 模擬器配發 IP 給 IoT 設備，由於是同一 Domain，所以使用原來的 IP

- 步驟 8：傳送註冊資訊至 DNS

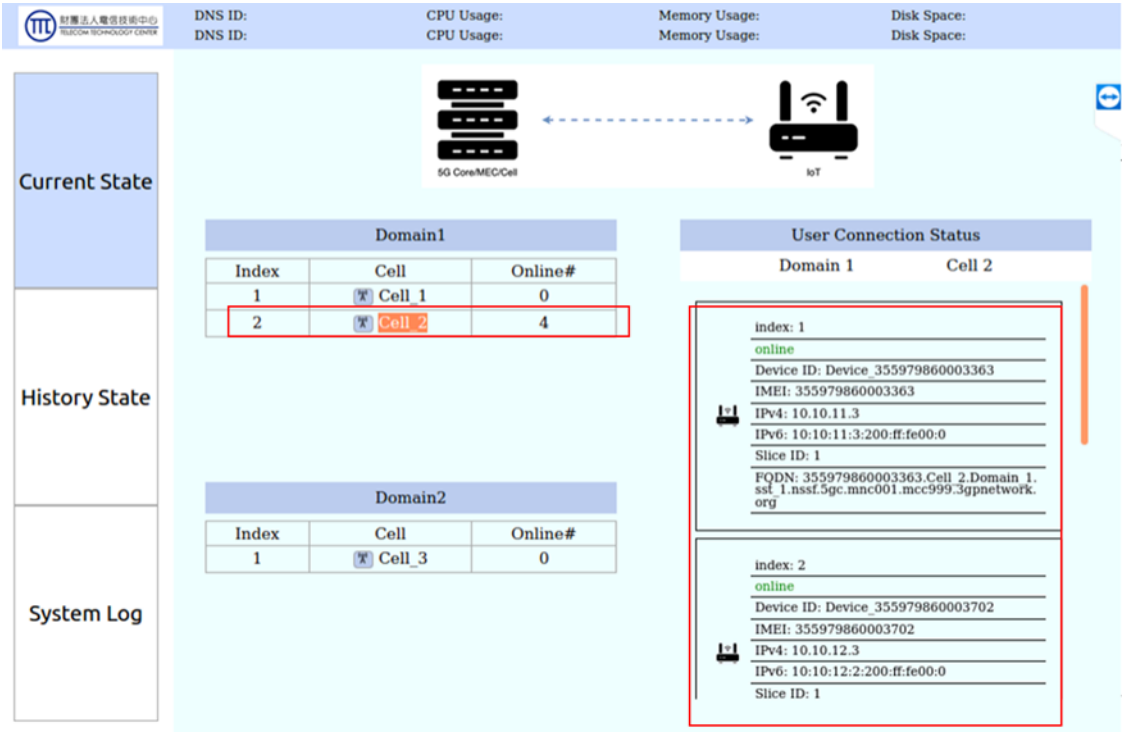


- 步驟 9：Generate　DNS A Record

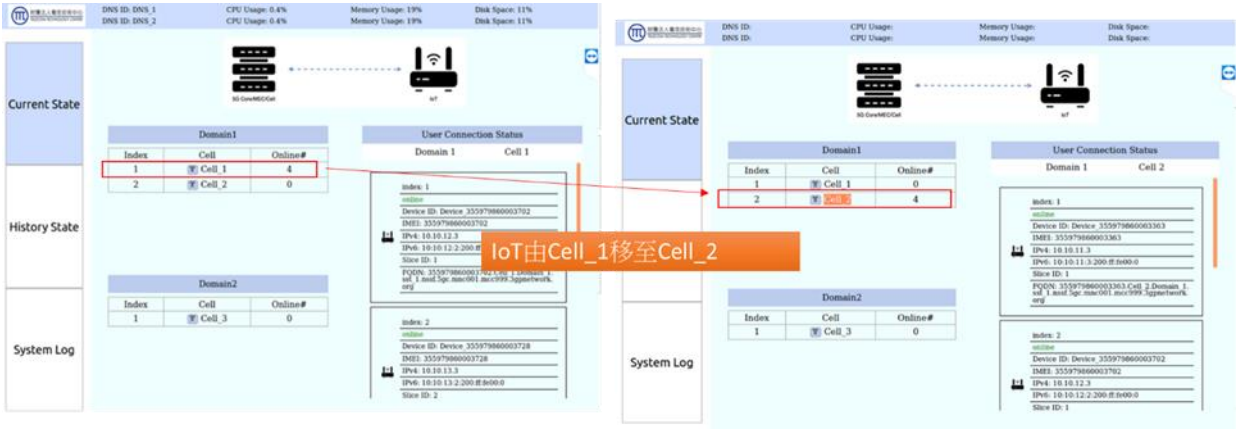
  DNS 透過自動編碼程式自動產生域名以及 DNS A Record，在 DNS 上顯示 DN 已更新

```
cat: /home/dnsserver/script/radius.log: No such file or directory
########################################
cat nssf.5gc.mnc001.mcc999.3gppnetwork.org
########################################
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
ns      IN      A       127.0.0.1
ns      IN      AAAA    ::1
355979860003363.Cell_2.Domain_1.sst_1  IN      A       10.10.11.3
355979860003363.Cell_2.Domain_1.sst_1  IN      A       10:10:11:3:200:ff:fe00:0
355979860003785.Cell_2.Domain_1.sst_3  IN      A       10.10.14.3
355979860003785.Cell_2.Domain_1.sst_3  IN      A       10:10:14:2:200:ff:fe00:0
355979860003702.Cell_2.Domain_1.sst_1  IN      A       10.10.12.3
355979860003702.Cell_2.Domain_1.sst_1  IN      A       10:10:12:2:200:ff:fe00:0
355979860003728.Cell_2.Domain_1.sst_2  IN      A       10.10.13.3
355979860003728.Cell_2.Domain_1.sst_2  IN      A       10:10:13:2:200:ff:fe00:0
```

檢視 Dashboard 畫面，可以看到 Cell_1 的上線裝置變為 0 個，Cell_2 的上線裝置變成 4 個。



➢ 步驟 10：DNS 與 Dashboard 更新資料




(三)同域移動設備參數內容

IoT 在同域的不同 Cell 移動時，DNN 與 IP 不更換，DN 會更改 Cell 名稱。進入系統檢視 IoT 設備參數異動，如下圖所示：

| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | DNN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟 6,7 | Service IP IPv4 (DHCP) | 10.10.11.3 | 10.10.12.3 | 10.10.13.3 | 10.10.14.3 |
| | Service IP IPv6 (DHCP) | 10:10:11:3:200:ff:fe00:0 | 10:10:12:2:200:ff:fe00:0 | 10:10:13:2:200:ff:fe00:0 | 10:10:14:2:200:ff:fe00:0 |
| 步驟 8-10 | DN | 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

(四)同域測試結果

經由以上的測試，整理測試結果如下表 19：

表 19、同域測試結果

| 項次 | 測試內容 | 預期結果 | 測試結果 |
|---|---|---|---|
| 1 | 5G 模擬器及 DNS 間的編碼核配與管理 | MEC 可以透過 Radius 協議將 IP：IMSI：IMEI：Cell ID 資訊傳給 DNS | 於步驟 3 以及 9，5G 模擬器會透過 Radius 協議將 IP：IMSI：IMEI：Cell ID：SST 資訊傳給 DNS。 |
| 2 | Device 取得 IP (IPv4/IPv6)與 DNS mapping | MEC 分配給 UE 的 IP 與傳送給 DNS 的內容一致 | IoT 設備於步驟 1、2 以及步驟 5、6、7 完成註冊後，自動取得 IP 位置。<br>檢視 5G 模擬器與 DNS 系統上所看到的 IP 資訊一致。 |
| 3 | DNS 編碼核配與管理 | DNS 可以依據 MEC 產生 Radius 內容自動產出 A Record | 於步驟 4、9，DNS 透過 Radius 協議得到的 IP：IMSI：IMEI：Cell ID：SST 資訊，自動產生 A Record。 |
| 4 | 多個 Device 註冊 DNS 與核配編碼 | 比對各 MEC 及 DNS：Device IP、IMSI、IMEI 及 Cell ID 結果一致 | 於 Dashboard 檢視各 IoT 設備的 IP、IMSI、IMEI 及 Cell ID 的資訊，與 5G 模擬器傳送的資料一致。 |

(五)System Log 及說明

從 Dashboard 上顯示同域測試過程中，IoT 設備註冊、移動、自動編碼產生 DN 的 System Log。

表 20、IoT 設備註冊後之 **Dashboard System Log**

| **Datetime** | **Payload** | **Type** |
|---|---|---|
| 2021/11/1 14:07 | Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:07 | Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:08 | Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:08 | Device_355979860003785 is attached on Cell_1 with FQDN 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

二、 跨域測試項目

IoT 設備從 Cell_2 移動到 Cell_3，觀察 IP 與域名變化，跨域測試內容如表 21。

表 21、跨域測試

| 項次 | 測試內容 | 預期結果 |
|---|---|---|
| 1 | 5G 模擬器及 DNS 間的編碼核配與管理 | 5G 模擬器可以透過 Raius 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS |
| 2 | 跨網域 Device 取得 IP（IPv4/IPv6）與 DNS mapping | 5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致 |
| 3 | 跨網域 Device 的 DNS 編碼核配與管理 | DNS 可以依據 5G 模擬器產生 Radius 內容自動產出 A/AAAA Record |

(一)IP 註冊與 DNS 動態管理流程

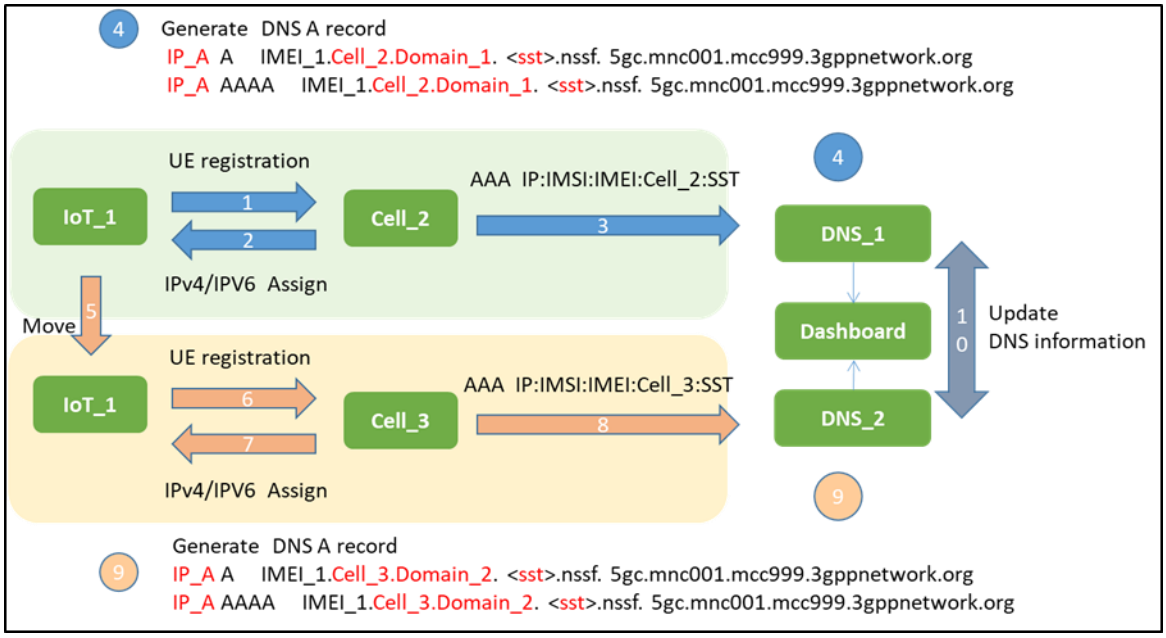



圖 16、跨域移動之 IP 註冊與 DNS 動態管理流程

跨域移動測試各步驟說明如表 22：

表 22、跨域移動之 IP 註冊與 DNS 動態管理流程

| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_2，並進行註冊 |
| 2 | 配發 IPv4/IPV6 位址 | 5G 模擬器配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | 5G 模擬器傳送 [IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS |
| 4 | Generate DNS A/AAAA Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 5 | UE 移動 | IoT 從 Cell_2 移動至 Cell_3，從 Domain_1 移動至 Domain_2 |
| 6 | UE registration | IoT 連線到 Cell_3，並進行註冊 |
| 7 | 配發 IPv4/IPV6 位址 | 5G 模擬器配發 IP 給 IoT |
| 8 | 傳送註冊資訊至 DNS | 5G 模擬器傳送 [IP:IMSI:IMEI:Cell_3:SST]等資訊至 DNS |
| 9 | Generate DNS A/AAAA Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 10 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA Record 資訊 |

- 步驟 1 到步驟 4：請參考同域測試的步驟 6 到步驟 9。
- 步驟 5： IoT 設備移動

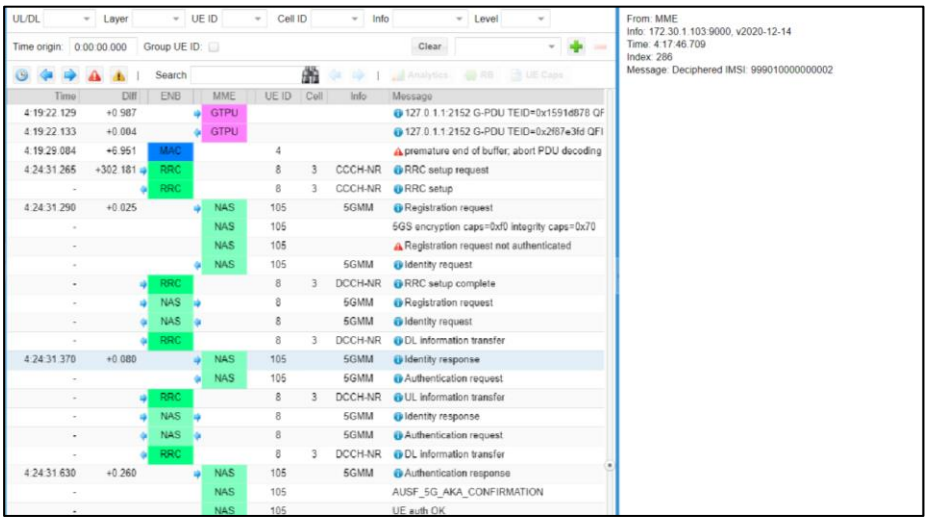
  IoT 設備從 Cell_2 移動至 Cell_3，從 Domain_1 移動至 Domain_2

```
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        32           121 0x002 0x4642
(enb)
(enb)
(enb)
```

```
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1   -60.0      N 99901
0x003    NR  n78 0x000064   633228    3         1     0.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        92           137 0x003 0x465c
        90           135 0x003 0x465a
        88           133 0x003 0x4658
        87           132 0x003 0x4657
(enb)
```

- 步驟 6： IoT 設備 registration

  IoT 設備連線到 Cell_3，並進行註冊



➢ 步驟 7： 配發 IPv4/IPV6 位址

5G 模擬器配發 IP 給 IoT 設備

```
(mme) ue
           IMSI           IMEISV  CN M-TMSI/5G-TMSI REG          TAC #BEARER IP_ADDR
 999010000000004 3559798600037801 5GC     0x6c4cb370   Y  99901.  0x64       1 10.10.14.4
 999010000000001 3559798600033601 5GC     0x4469d5c4   Y  99901.  0x64       1 10.10.11.4 10:10:11:4::
 999010000000002 3559798600037001 5GC     0x94068454   Y  99901.  0x64       1 10.10.12.4
 999010000000003 3559798600037201 5GC     0xb9d8478b   Y  99901.  0x64       1 10.10.13.4
```

➢ 步驟 8： 傳送註冊資訊至 DNS

傳送[IP：IMSI：IMEI：Cell_3：SST]等註冊資訊至 DNS

```
User-Password: [b'\xa2\xc8\xba\x180\xde%\x86\x18\xbf4\xd1$0\x8a\xf3']
Received an authentication request
Attributes:
User-Name: ['5gc015']
User-Password: [b'w+&y\xd2\x81\x8a\xace\xc5\xc4uJW\x95\xaf']
10.10.11.4,10:10:11:4:200:ff:fe00:0,999010000000001,355979860003363,3,20211101141826,start,1
10.10.12.4,10:10:12:3:200:ff:fe00:0,999010000000002,355979860003702,3,20211101141901,start,1
10.10.13.4,10:10:13:3:200:ff:fe00:0,999010000000003,355979860003728,3,20211101141926,start,2
Received an authentication request
Attributes:
User-Name: ['5gc001']
User-Password: [b'\xee*\xdd\x92\xe3\xe5\x9b-\xde\x14`lf\x9c\xe0\xdf']
Received an authentication request
```

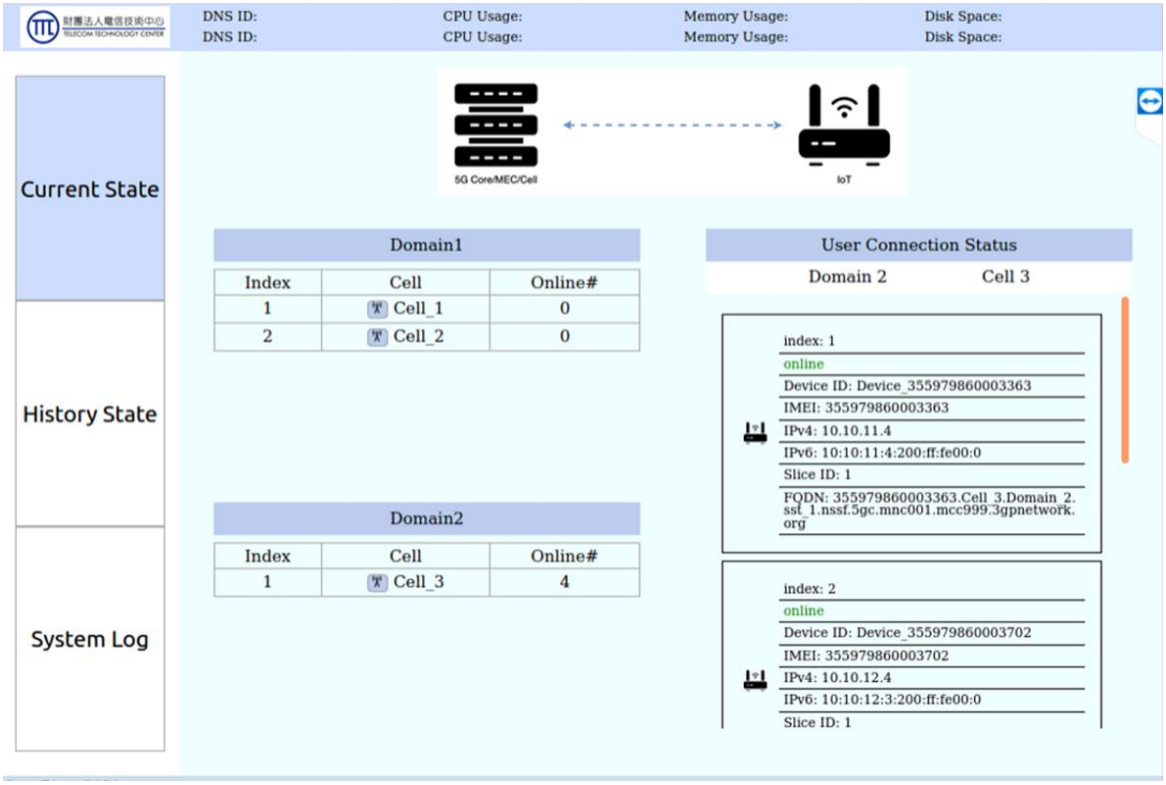
```
Received an authentication request
Attributes:
User-Name: ['5gc015']
User-Password: [b'\x9e_o\xb9\xcc\xd2s0X\xe4\xb1\xbb\xe7\xd8\xddA']
10.10.14.4,10:10:14:3:200:ff:fe00:0,999010000000004,355979860003785,3,20211101141956,start,3
Received an authentication request
Attributes:
User-Name: ['5gc001']
User-Password: [b'!q^z\x9e\xc1\xcb\r\x13\x83\xe2\x07\x15\xb052']
Received an authentication request
Attributes:
```

➢ 步驟 9： Generate DNS A Record

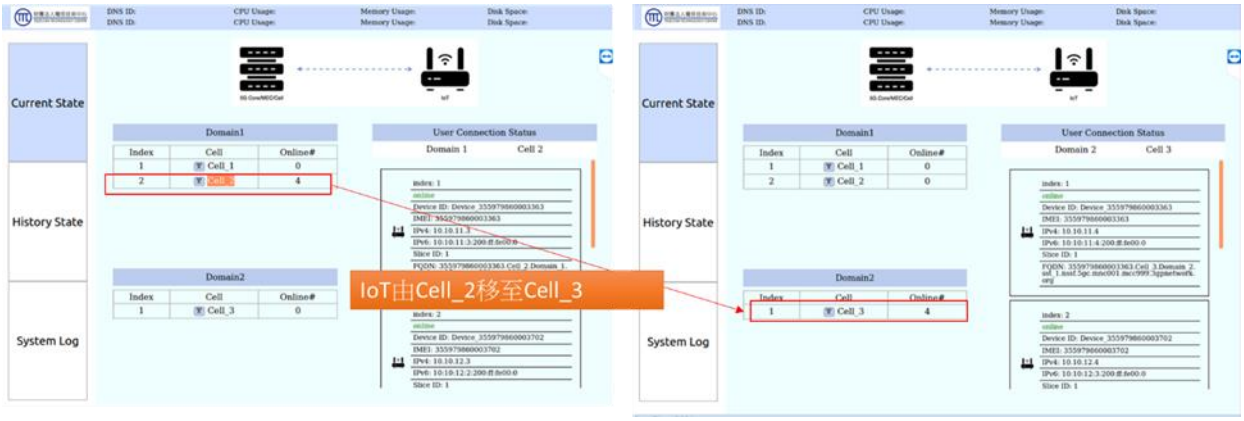
DNS 透過自動編碼程式自動產生域名以及 DNS A Record，在 DNS 上顯示 DN 已更新

```
{"message": "Upload success"}{"message": "Upload success"}
10.10.14.4,10:10:14:3:200:ff:fe00:0,999010000000004,355979860003785,3,20211101141956,start,3
########################################
cat nssf.5gc.mnc001.mcc999.3gppnetwork.org
########################################
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
ns      IN      A       127.0.0.1
ns      IN      AAAA    ::1
355979860003363.Cell_3.Domain_2.sst_1  IN      A       10.10.11.4
355979860003363.Cell_3.Domain_2.sst_1  IN      A       10:10:11:4:200:ff:fe00:0
355979860003702.Cell_3.Domain_2.sst_1  IN      A       10.10.12.4
355979860003702.Cell_3.Domain_2.sst_1  IN      A       10:10:12:3:200:ff:fe00:0
355979860003728.Cell_3.Domain_2.sst_2  IN      A       10.10.13.4
355979860003728.Cell_3.Domain_2.sst_2  IN      A       10:10:13:3:200:ff:fe00:0
355979860003785.Cell_3.Domain_2.sst_3  IN      A       10.10.14.4
355979860003785.Cell_3.Domain_2.sst_3  IN      A       10:10:14:3:200:ff:fe00:0
```

檢視 Dashboard 畫面，可以看到 Cell_2 的上線裝置變為 0 個，Cell_3 的上線裝置變成 4 個。




➢ 步驟 10： DNS 與 Dashboard 更新資料



(二)跨域移動設備參數內容

UE 在跨域移動時，會取得新的 IP，同時也會更改 DN 的 Cell 與 Domain 名稱，進入系統檢視 5GW 設備參數異動，如下圖所示：

| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | DNN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR 8K Videos | AR/VR 8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟 6,7 | Service IP IPv4 (DHCP) | 10.10.11.4 | 10.10.12.4 | 10.10.13.4 | 10.10.14.4 |
| | Service IP IPv6 (DHCP) | 10:10:11:4:200:ff:fe00:0 | 10:10:12:3:200:ff:fe00:0 | 10:10:13:3:200:ff:fe00:0 | 10:10:14:3:200:ff:fe00:0 |
| 步驟 8-10 | DN | 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

(三)跨域測試結果

經由以上的測試，整理測試結果如下：

| 項次 | 測試內容 | 預期結果 | 測試結果 |
|---|---|---|---|
| 1 | 5G 模擬器及 DNS 間的編碼核配與管理 | 5G 模擬器可以透過 Radius 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS | 於步驟 3 以及 9，5G 模擬器會透過 Radius 協議將 IP:IMSI:IMEI:Cell ID:SST 資訊傳給 DNS。 |
| 2 | Device 取得 IP (IPv4/IPv6)與 DNS mapping | 5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致 | IoT 設備於步驟 1、2 以及步驟 5、6、7 完成註冊後，自動取得 IP 位置。<br>檢視 5G 模擬器與 DNS 系統上所看到的 IP 資訊一致。 |
| 3 | DNS 編碼核配與管理 | DNS 可以依據 5G 模擬器產生 Radius 內容自動產出 A/AAAA Record | 於步驟 4、9，DNS 透過 Radius 協議得到的 IP:IMSI:IMEI:Cell ID:SST 資訊，自動產生 A/AAAA Record。 |

(四)System Log 及說明

從 Dashboard 上顯示跨域測試過程中，IoT 設備註冊、移動、自動編碼產生 DN 的 System Log。

表 23、IoT 設備跨域移動測試後之 Dashboard System Log

| Datetime | Payload | Type |
|---|---|---|
| 2021/11/1 14:14 | Device_355979860003363 is detached from Cell_2 | INFO |
| 2021/11/1 14:14 | Device_355979860003702 is detached from Cell_2 | INFO |
| 2021/11/1 14:14 | Device_355979860003728 is detached from Cell_2 | INFO |
| 2021/11/1 14:14 | Device_355979860003785 is detached from Cell_2 | INFO |
| 2021/11/1 14:19 | Device_355979860003702 is attached on Cell_3 with FQDN 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:19 | Device_355979860003363 is attached on Cell_3 with FQDN 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:19 | Device_355979860003728 is attached on Cell_3 with FQDN 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:19 | Device_355979860003785 is attached on Cell_3 with FQDN 355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

三、 大量物聯網裝置情境(1)測試項目

完成 IoT 設備在不同 Cell 之間移動進行自動註冊後，繼續將 IoT 設備在不同 Cell 之間持續移動，觀察 System Log 變化情形，另外採用程式模擬方式產生大量物聯網裝置的 Radius 資料，傳送到 DNS Server，驗證系統支援大量設備自動註冊的能力。

表 24、大量物聯網裝置情境(1)測試

| 項次 | 測試內容 | 預期結果 |
|---|---|---|
| 1 | 模擬程式產生大量物聯網裝置資料 | 可從 Dashboard 顯示物聯網裝置數量以及展示物聯網裝置資訊 |
| 2 | DNS 編碼核配與管理 | DNS 可以依據 Radius 內容自動產出 A/AAAA Record |

(一) IP 註冊與 DNS 動態管理流程

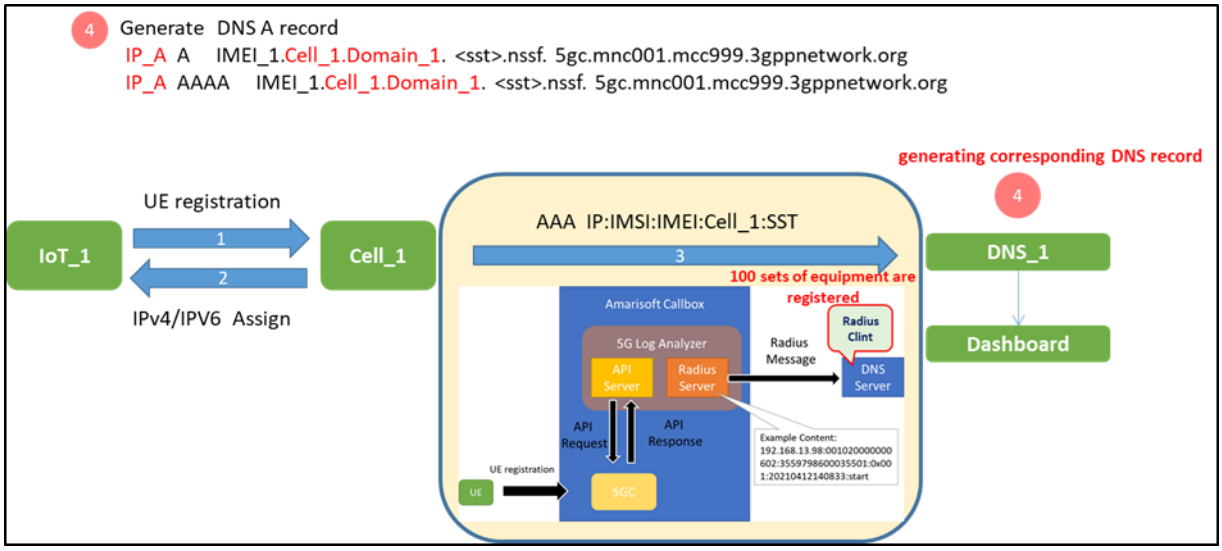



圖 17、大量 IoT 設備註冊並產生 Radius 資料流程

(二) 驗證測試步驟及操作結果

大量物聯網裝置測試步驟說明如表 25。

表 25、大量物聯網裝置情境一 IP 註冊與 DNS 動態管理

| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | 使用模擬程式產生大量 Radius 資料 |
| 2 | Generate DNS A/AAAA Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 3 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA Record 資訊 |

- 步驟 1： UE 註冊

開發程式以產生 100 臺 IoT 設備的 Radius 資料，傳送到 DNS Server。IoT 設備參數設計如下表：

| **Name** | **IP_CAM** | **Power_Meter** | **Temp_Meter** | **Smart_ Parking** | **Smart_Lamps** |
|---|---|---|---|---|---|
| DNN | IP_CAM | Power_Meter | Temp_Meter | Smart_Parking | Smart_Lamps |
| TAC（IMEI 前 8 碼） | 45678123 | 34567812 | 23456781 | 12345678 | 72345678 |
| NSSAI | eMBB | MIOT | | | |
| SST | 1 | 3 | | | |
| Template | High quality Video | Smart City sensor | | | |
| Throughput | 100Mbps/100Mbps | 1Mbps/1Mbps | | | |
| Zone | nssf.5gc.mnc001.mcc999.3gppnetwork.org | | | | |
| Service IP IPv4 | 10.100.11.0/24 | 10.100.12.0/24 | 10.100.13.0/24 | 10.100.14.0/24 | 10.100.15.0/124 |
| Service IP IPv6 | 10.:100:11:(1-254):200:ff:fe00:00 | 10.:100:12:(1-254):200:ff:fe00:00 | 10.:100:13:(1-254):200:ff:fe00:00 | 10.:100:14:(1-254):200:ff:fe00:00 | 10.:100:15:(1-254):200:ff:fe00:00 |

- 步驟 2： Generate DNS A/AAAA Record

  系統自動產生 DNS A/AAAA Record 。

```
234567810003317.Cell_1.Domain_1.sst_3  IN      A       10:10:13:17:200:ff:fe00:0
123456780003317.Cell_2.Domain_1.sst_3  IN      A       10.100.14.17
123456780003317.Cell_2.Domain_1.sst_3  IN      A       10:10:14:17:200:ff:fe00:0
723456780003317.Cell_3.Domain_2.sst_3  IN      A       10.100.15.17
723456780003317.Cell_3.Domain_2.sst_3  IN      A       10:10:15:17:200:ff:fe00:0
456781230003318.Cell_2.Domain_1.sst_1  IN      A       10.100.11.18
456781230003318.Cell_2.Domain_1.sst_1  IN      A       10:10:11:18:200:ff:fe00:0
345678120003318.Cell_3.Domain_2.sst_3  IN      A       10.100.12.18
345678120003318.Cell_3.Domain_2.sst_3  IN      A       10:10:12:18:200:ff:fe00:0
234567810003318.Cell_1.Domain_1.sst_3  IN      A       10.100.13.18
234567810003318.Cell_1.Domain_1.sst_3  IN      A       10:10:13:18:200:ff:fe00:0
123456780003318.Cell_2.Domain_1.sst_3  IN      A       10.100.14.18
123456780003318.Cell_2.Domain_1.sst_3  IN      A       10:10:14:18:200:ff:fe00:0
723456780003318.Cell_3.Domain_2.sst_3  IN      A       10.100.15.18
723456780003318.Cell_3.Domain_2.sst_3  IN      A       10:10:15:18:200:ff:fe00:0
456781230003319.Cell_2.Domain_1.sst_1  IN      A       10.100.11.19
456781230003319.Cell_2.Domain_1.sst_1  IN      A       10:10:11:19:200:ff:fe00:0
345678120003319.Cell_3.Domain_2.sst_3  IN      A       10.100.12.19
345678120003319.Cell_3.Domain_2.sst_3  IN      A       10:10:12:19:200:ff:fe00:0
234567810003319.Cell_1.Domain_1.sst_3  IN      A       10.100.13.19
234567810003319.Cell_1.Domain_1.sst_3  IN      A       10:10:13:19:200:ff:fe00:0
123456780003319.Cell_2.Domain_1.sst_3  IN      A       10.100.14.19
123456780003319.Cell_2.Domain_1.sst_3  IN      A       10:10:14:19:200:ff:fe00:0
723456780003319.Cell_3.Domain_2.sst_3  IN      A       10.100.15.19
723456780003319.Cell_3.Domain_2.sst_3  IN      A       10:10:15:19:200:ff:fe00:0
456781230003320.Cell_2.Domain_1.sst_1  IN      A       10.100.11.20
456781230003320.Cell_2.Domain_1.sst_1  IN      A       10:10:11:20:200:ff:fe00:0
345678120003320.Cell_3.Domain_2.sst_3  IN      A       10.100.12.20
345678120003320.Cell_3.Domain_2.sst_3  IN      A       10:10:12:20:200:ff:fe00:0
234567810003320.Cell_1.Domain_1.sst_3  IN      A       10.100.13.20
234567810003320.Cell_1.Domain_1.sst_3  IN      A       10:10:13:20:200:ff:fe00:0
123456780003320.Cell_2.Domain_1.sst_3  IN      A       10.100.14.20
123456780003320.Cell_2.Domain_1.sst_3  IN      A       10:10:14:20:200:ff:fe00:0
723456780003320.Cell_3.Domain_2.sst_3  IN      A       10.100.15.20
723456780003320.Cell_3.Domain_2.sst_3  IN      A       10:10:15:20:200:ff:fe00:0
dnsserver@mecs-6110-01:~/script$
```

➢ 步驟 3：DNS 與 Dashboard 更新資料

執行完模擬程式之後，100 個 IoT 設備自動註冊，可從 Dashboard 顯示在 Cell_1 有 29 個上線設備，Cell_2 有 31 個上線設備，Cell_3 有 40 個上線設備，並可檢視每個 IoT 設備的資訊，如圖 18、圖 19。

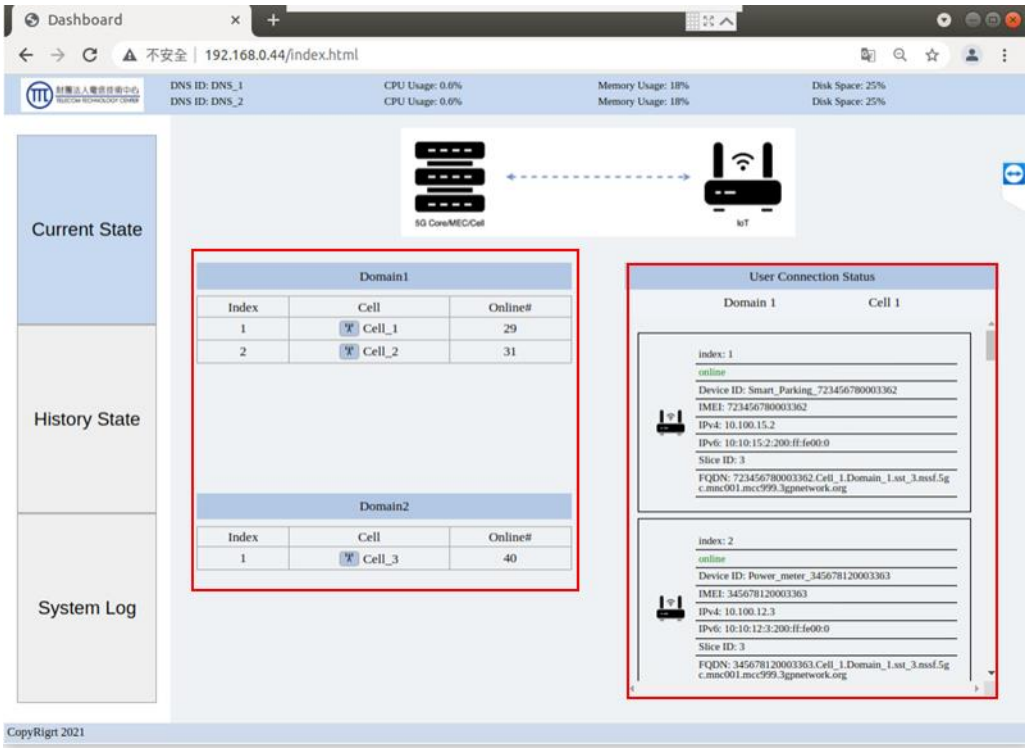



圖 18、100 個 IoT 自動註冊展示畫面

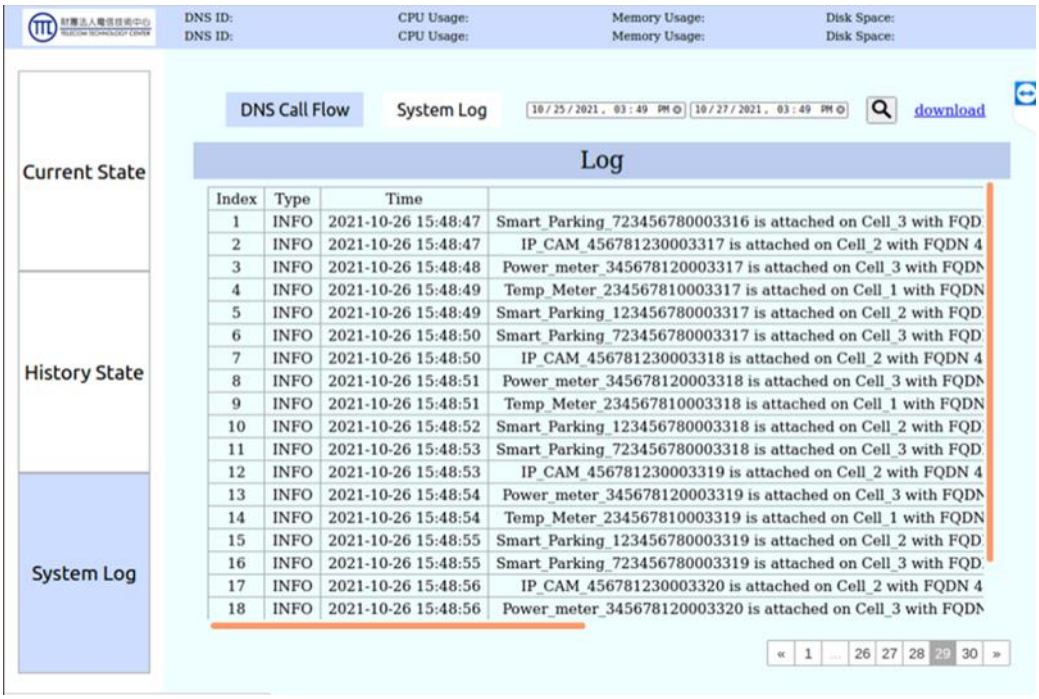



圖 19、100 個 IoT 自動註冊 System Log

(三) 大量物聯網裝置情境(1)測試結果

表 26、100 臺 IoT 設備註冊測試結果

| 項次 | 測試內容 | 預期結果 | 測試結果 |
|---|---|---|---|
| 1 | 模擬程式產生大量物聯網裝置資料 | 可從 Dashboard 顯示物聯網裝置數量以及展示物聯網裝置資訊 | 於 Dashboard 上顯示 100 台的 IoT 設備資訊 |
| 2 | DNS 編碼核配與管理 | DNS 可以依據 Radius 內容自動產出 A/AAAA Record | DNS 自動產出 A/AAAA Record |

(四) System Log 及說明

大量物聯網裝置情境(1)程式模擬 100 臺 IoT 設備裝置自動註冊，以下節錄部分 System Log：

| Datetime | Payload | Type |
|---|---|---|
| 2021/10/26 12:10 | IP_CAM_456781230003361 is attached on Cell_3 with FQDN 456781230003361.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Power_meter_345678120003361 is attached on Cell_1 with FQDN 345678120003361.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Temp_Meter_234567810003361 is attached on Cell_2 with FQDN 234567810003361.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Smart_Parking_723456780003361 is attached on Cell_1 with FQDN 723456780003361.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Smart_Parking_123456780003361 is attached on Cell_3 with FQDN 123456780003361.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | IP_CAM_456781230003362 is attached on Cell_3 with FQDN 456781230003362.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Power_meter_345678120003362 is attached on Cell_1 with FQDN 345678120003362.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

| Datetime | Payload | Type |
|---|---|---|
| 2021/10/26 12:10 | Temp_Meter_234567810003362 is attached on Cell_2 with FQDN 234567810003362.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Smart_Parking_123456780003362 is attached on Cell_3 with FQDN 123456780003362.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Smart_Parking_723456780003362 is attached on Cell_1 with FQDN 723456780003362.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Power_meter_345678120003363 is attached on Cell_1 with FQDN 345678120003363.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | IP_CAM_456781230003363 is attached on Cell_3 with FQDN 456781230003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Temp_Meter_234567810003363 is attached on Cell_2 with FQDN 234567810003363.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Smart_Parking_123456780003363 is attached on Cell_3 with FQDN 123456780003363.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Smart_Parking_723456780003363 is attached on Cell_1 with FQDN 723456780003363.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | IP_CAM_456781230003364 is attached on Cell_3 with FQDN 456781230003364.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Power_meter_345678120003364 is attached on Cell_1 with FQDN 345678120003364.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Smart_Parking_123456780003364 is attached on Cell_3 with FQDN 123456780003364.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Temp_Meter_234567810003364 is attached on Cell_2 with FQDN 234567810003364.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

| Datetime | Payload | Type |
|---|---|---|
| 2021/10/26 12:10 | Smart_Parking_723456780003364 is attached on Cell_1 with FQDN 723456780003364.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Power_meter_345678120003365 is attached on Cell_1 with FQDN 345678120003365.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | IP_CAM_456781230003365 is attached on Cell_3 with FQDN 456781230003365.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Temp_Meter_234567810003365 is attached on Cell_2 with FQDN 234567810003365.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 12:10 | Smart_Parking_123456780003365 is attached on Cell_3 with FQDN 123456780003365.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

四、 大量物聯網裝置情境(2)測試項目

20 分鐘內使用 4 臺 IoT 設備，在不同 Cell 與 Domain 間移動，System Log 須呈現移動後之變化，測試內容如表 27。

表 27、大量物聯網裝置情境(2) 測試

| 項次 | 測試內容 | 預期結果 |
|---|---|---|
| 1 | 物聯網裝置於 20 分鐘內移動 | 可從 System Log 中檢視物聯網裝置移動軌跡 |
| 2 | DNS 編碼核配與管理 | DNS 可以依據移動軌跡自動產出 A/AAAA Record |

(一)IP 註冊與 DNS 動態管理流程

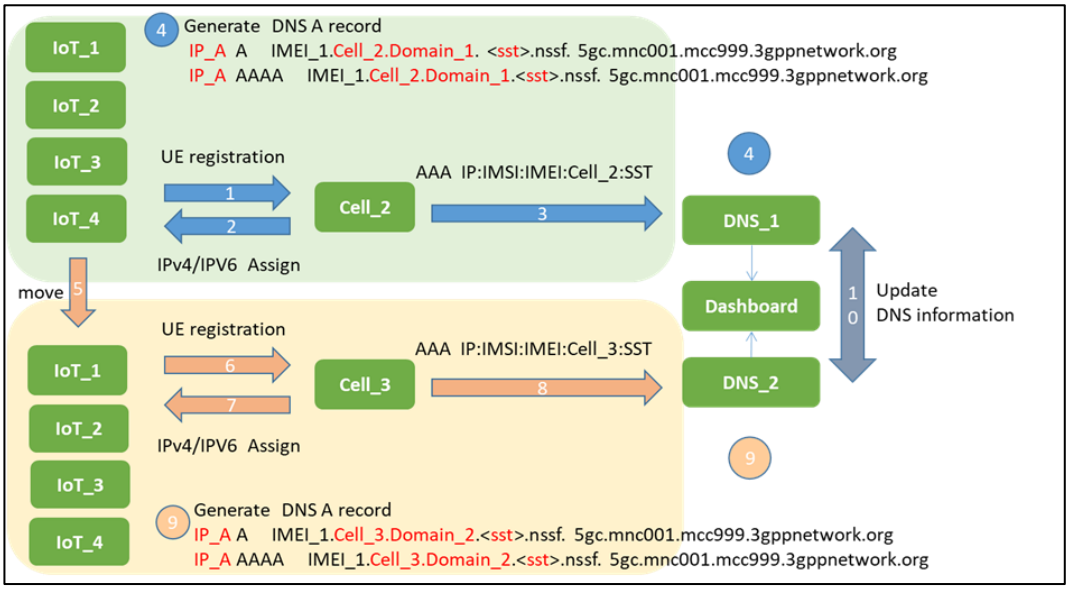



圖 20、大量 IoT 設備跨域移動之 IP 註冊與 DNS 動態管理流程

(二)驗證測試步驟及操作結果

大量物聯網裝置測試步驟說明如表 28：

表 28、大量物聯網裝置情境(2)IP 註冊與 DNS 動態管理

| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 持續移動 | IoT 在 Cell_1、Cell_2 與 Cell_3 之間移動 |
| 2 | Generate DNS A/AAAA Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 3 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA Record 資訊 |

- 步驟 1： UE 持續移動

當完成同域與跨域測試後，在 5G 模擬器上設定讓 IoT 設備在不同 Cell 之間移動。

```
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        34           123 0x001 0x4622
        32           121 0x001 0x4620
        30           119 0x001 0x461e
        28           117 0x001 0x461c
(enb) cell_gain 2 0
(enb) cell_gain 1 -60
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        67             - 0x002 0x4643
        32           121 0x002 0x4642
        52             - 0x002 0x4634
        45             - 0x002 0x462d
(enb)
(enb)
(enb)
(enb)
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        32           121 0x002 0x4642
(enb)
```

```
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        32           121 0x002 0x4642
(enb)
(enb)
(enb)
```

- 步驟 2 ： Generate DNS A/AAAA Record

```
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1   -60.0      N 99901
0x003    NR  n78 0x000064   633228    3         1     0.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        92           137 0x003 0x465c
        90           135 0x003 0x465a
        88           133 0x003 0x4658
        87           132 0x003 0x4657
(enb)
```

- 步驟 3 ：DNS 與 Dashboard 更新資料

```
@       IN      NS      localhost.
ns      IN      A       127.0.0.1
ns      IN      AAAA    ::1
355979860003363.Cell_2.Domain_1.sst_1  IN      A       10.10.11.3
355979860003363.Cell_2.Domain_1.sst_1  IN      A       10:10:11:3:200:ff:fe00:0
355979860003702.Cell_2.Domain_1.sst_1  IN      A       10.10.12.3
355979860003702.Cell_2.Domain_1.sst_1  IN      A       10:10:12:2:200:ff:fe00:0
355979860003728.Cell_2.Domain_1.sst_2  IN      A       10.10.13.3
355979860003728.Cell_2.Domain_1.sst_2  IN      A       10:10:13:2:200:ff:fe00:0
355979860003785.Cell_2.Domain_1.sst_3  IN      A       10.10.14.3
355979860003785.Cell_2.Domain_1.sst_3  IN      A       10:10:14:2:200:ff:fe00:0
```

測試結果：可以從 System Log 中下載 excel 表格，完整檢視 IoT 設備移動軌跡。

| | | |
|---|---|---|
| 590 | 2021/10/26 16:24 Device_355979860008363 is attached on Cell_1 with FQDN 355979860008363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 591 | 2021/10/26 16:24 Device_355979860008702 is attached on Cell_1 with FQDN 355979860008702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 592 | 2021/10/26 16:24 Device_355979860008728 is attached on Cell_1 with FQDN 355979860008728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 593 | 2021/10/26 16:25 Device_355979860008785 is attached on Cell_1 with FQDN 355979860008785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 594 | 2021/10/26 16:26 Device_355979860008363 is attached on Cell_2 with FQDN 355979860008363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 595 | 2021/10/26 16:26 Device_355979860008785 is attached on Cell_2 with FQDN 355979860008785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 596 | 2021/10/26 16:26 Device_355979860008728 is attached on Cell_2 with FQDN 355979860008728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 597 | 2021/10/26 16:26 Device_355979860008702 is attached on Cell_2 with FQDN 355979860008702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 598 | 2021/10/26 16:27 Device_355979860008363 is detached from Cell_2 | INFO |
| 599 | 2021/10/26 16:30 Device_355979860008702 is detached from Cell_2 | INFO |
| 600 | 2021/10/26 16:30 Device_355979860008728 is detached from Cell_2 | INFO |
| 601 | 2021/10/26 16:30 Device_355979860008785 is detached from Cell_2 | INFO |
| 602 | 2021/10/26 16:31 Device_355979860008363 is attached on Cell_3 with FQDN 355979860008363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 603 | 2021/10/26 16:31 Device_355979860008702 is attached on Cell_3 with FQDN 355979860008702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 604 | 2021/10/26 16:31 Device_355979860008728 is attached on Cell_3 with FQDN 355979860008728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 605 | 2021/10/26 16:31 Device_355979860008785 is attached on Cell_3 with FQDN 355979860008785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 606 | 2021/10/26 16:32 Device_355979860008363 is detached from Cell_3 | INFO |
| 607 | 2021/10/26 16:32 Device_355979860008728 is detached from Cell_3 | INFO |
| 608 | 2021/10/26 16:32 Device_355979860008785 is detached from Cell_3 | INFO |
| 609 | 2021/10/26 16:32 Device_355979860008702 is detached from Cell_3 | INFO |
| 610 | 2021/10/26 16:34 Device_355979860008363 is attached on Cell_1 with FQDN 355979860008363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 611 | 2021/10/26 16:35 Device_355979860008702 is attached on Cell_1 with FQDN 355979860008702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 612 | 2021/10/26 16:35 Device_355979860008728 is attached on Cell_1 with FQDN 355979860008728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 613 | 2021/10/26 16:36 Device_355979860008785 is attached on Cell_1 with FQDN 355979860008785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 614 | 2021/10/26 16:37 Device_355979860008363 is detached from Cell_1 | INFO |
| 615 | 2021/10/26 16:37 Device_355979860008702 is detached from Cell_1 | INFO |
| 616 | 2021/10/26 16:37 Device_355979860008785 is detached from Cell_1 | INFO |
| 617 | 2021/10/26 16:37 Device_355979860008728 is detached from Cell_1 | INFO |
| 618 | 2021/10/26 16:40 Device_355979860008363 is attached on Cell_3 with FQDN 355979860008363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 619 | 2021/10/26 16:40 Device_355979860008728 is attached on Cell_3 with FQDN 355979860008728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 620 | 2021/10/26 16:40 Device_355979860008702 is attached on Cell_3 with FQDN 355979860008702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 621 | 2021/10/26 16:40 Device_355979860008785 is attached on Cell_3 with FQDN 355979860008785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 622 | 2021/10/26 16:42 Device_355979860008702 is detached from Cell_3 | INFO |
| 623 | 2021/10/26 16:42 Device_355979860008728 is detached from Cell_3 | INFO |
| 624 | 2021/10/26 16:42 Device_355979860008363 is detached from Cell_3 | INFO |
| 625 | 2021/10/26 16:42 Device_355979860008785 is detached from Cell_3 | INFO |
| 626 | 2021/10/26 16:43 Device_355979860008363 is attached on Cell_2 with FQDN 355979860008363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 627 | 2021/10/26 16:43 Device_355979860008702 is attached on Cell_2 with FQDN 355979860008702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 628 | 2021/10/26 16:43 Device_355979860008728 is attached on Cell_2 with FQDN 355979860008728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 629 | 2021/10/26 16:44 Device_355979860008785 is attached on Cell_2 with FQDN 355979860008785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

圖 21、4 個 IoT 持續移動 System Log

(三)大量物聯網裝置情境(2)測試結果

| 項次 | 測試內容 | 預期結果 | 測試結果 |
|---|---|---|---|
| 1 | 物聯網裝置於 20 分鐘內移動 | 可從 System Log 中檢視物聯網裝置移動軌跡 | 從 Dashboard 的 System Log 中可以展示連網裝置移動軌跡 |
| 2 | DNS 編碼核配與管理 | DNS 可以依據移動軌跡自動產出 A/AAAA Record | DNS 自動產出 A /AAAA Record |

(四)System Log 及說明

持續移動 IoT 設備 20 分鐘，可透過 System Log 檢視特定 IoT 設備裝置的移動軌跡。

| Datetime | Payload | Type |
|---|---|---|
| 2021/10/26 16:20 | Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:20 | Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:20 | Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:20 | Device_355979860003363 is detached from Cell_1 | INFO |
| 2021/10/26 16:20 | Device_355979860003702 is detached from Cell_1 | INFO |
| 2021/10/26 16:20 | Device_355979860003728 is detached from Cell_1 | INFO |
| 2021/10/26 16:24 | Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:24 | Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

| Datetime | Payload | Type |
|---|---|---|
| 2021/10/26 16:24 | Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:25 | Device_355979860003785 is attached on Cell_1 with FQDN 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:26 | Device_355979860003363 is attached on Cell_2 with FQDN 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:26 | Device_355979860003785 is attached on Cell_2 with FQDN 355979860003785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:26 | Device_355979860003728 is attached on Cell_2 with FQDN 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:26 | Device_355979860003702 is attached on Cell_2 with FQDN 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:27 | Device_355979860003363 is detached from Cell_2 | INFO |
| 2021/10/26 16:30 | Device_355979860003702 is detached from Cell_2 | INFO |
| 2021/10/26 16:30 | Device_355979860003728 is detached from Cell_2 | INFO |
| 2021/10/26 16:30 | Device_355979860003785 is detached from Cell_2 | INFO |
| 2021/10/26 16:31 | Device_355979860003363 is attached on Cell_3 with FQDN 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:31 | Device_355979860003702 is attached on Cell_3 with FQDN 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:31 | Device_355979860003728 is attached on Cell_3 with FQDN 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

| Datetime | Payload | Type |
|---|---|---|
| 2021/10/26 16:31 | Device_355979860003785 is attached on Cell_3 with FQDN 355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:32 | Device_355979860003363 is detached from Cell_3 | INFO |
| 2021/10/26 16:32 | Device_355979860003728 is detached from Cell_3 | INFO |
| 2021/10/26 16:32 | Device_355979860003785 is detached from Cell_3 | INFO |
| 2021/10/26 16:32 | Device_355979860003702 is detached from Cell_3 | INFO |
| 2021/10/26 16:34 | Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:35 | Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:35 | Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:36 | Device_355979860003785 is attached on Cell_1 with FQDN 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:37 | Device_355979860003363 is detached from Cell_1 | INFO |
| 2021/10/26 16:37 | Device_355979860003702 is detached from Cell_1 | INFO |
| 2021/10/26 16:37 | Device_355979860003785 is detached from Cell_1 | INFO |
| 2021/10/26 16:37 | Device_355979860003728 is detached from Cell_1 | INFO |
| 2021/10/26 16:40 | Device_355979860003363 is attached on Cell_3 with FQDN 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:40 | Device_355979860003728 is attached on Cell_3 with FQDN 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

| Datetime | Payload | Type |
|---|---|---|
| 2021/10/26 16:40 | Device_355979860003702 is attached on Cell_3 with FQDN 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:40 | Device_355979860003785 is attached on Cell_3 with FQDN 355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:42 | Device_355979860003702 is detached from Cell_3 | INFO |
| 2021/10/26 16:42 | Device_355979860003728 is detached from Cell_3 | INFO |
| 2021/10/26 16:42 | Device_355979860003363 is detached from Cell_3 | INFO |
| 2021/10/26 16:42 | Device_355979860003785 is detached from Cell_3 | INFO |
| 2021/10/26 16:43 | Device_355979860003363 is attached on Cell_2 with FQDN 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:43 | Device_355979860003702 is attached on Cell_2 with FQDN 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:43 | Device_355979860003728 is attached on Cell_2 with FQDN 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/10/26 16:44 | Device_355979860003785 is attached on Cell_2 with FQDN 355979860003785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

## 玖、情景測試項目(情境二)

本節測試主要驗證當 IoT 設備在不同 Domain 之間移動時，IoT 設備會自動取得 IP 位址，同時，DNS Server 上也會動態更改 A Record，並與其他 Domain 上的 DNS Server 交換 FQDN 資訊，達到 IoT 設備在專網間的互相通訊與辨識，自動配置(Autoconfig)與管理專網號碼。

IoT 設備初始設定的參數如表 29

表 29、IoT 設備初始參數

| | IoT_1 | IoT _2 | IoT _3 | IoT _5 |
|---|---|---|---|---|
| DNN | internet1 | internet2 | internet3 | Internet5 |
| IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 359047100170495 |
| NSSAI | eMBB | eMBB | URLLC | MIOT |
| SST | 1 | 1 | 2 | 3 |
| Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic Machines | Smart City Sensors |
| Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/<br>500Mbps | 1Mbps/1Mbps |

一、 同域測試

IoT 設備從 Cell_1 移動到 Cell_2，觀察 IP 與域名變化，測試內容如表 30。

表 30、同域測試

| 項次 | 測試內容 | 預期結果 |
|---|---|---|
| 1 | 5G 模擬器及 DNS 間的編碼核配與管理 | MEC 可以透過 Radius 協議將 IP：IMSI：IMEI：Cell ID 資訊傳給 DNS |
| 2 | Device 取得 IP (IPv4/IPv6)與 DNS mapping | MEC 分配給 UE 的 IP 與傳送給 DNS 的內容一致 |
| 3 | DNS 編碼核配與管理 | DNS 可以依據 MEC 產生 Radius 內容自動產出 A Record |
| 4 | 多個 Device 註冊 DNS 與核配編碼 | 比對各 MEC 及 DNS：Device IP、IMSI、IMEI 及 Cell ID 結果一致 |

(一)IP 註冊與 DNS 動態管理流程

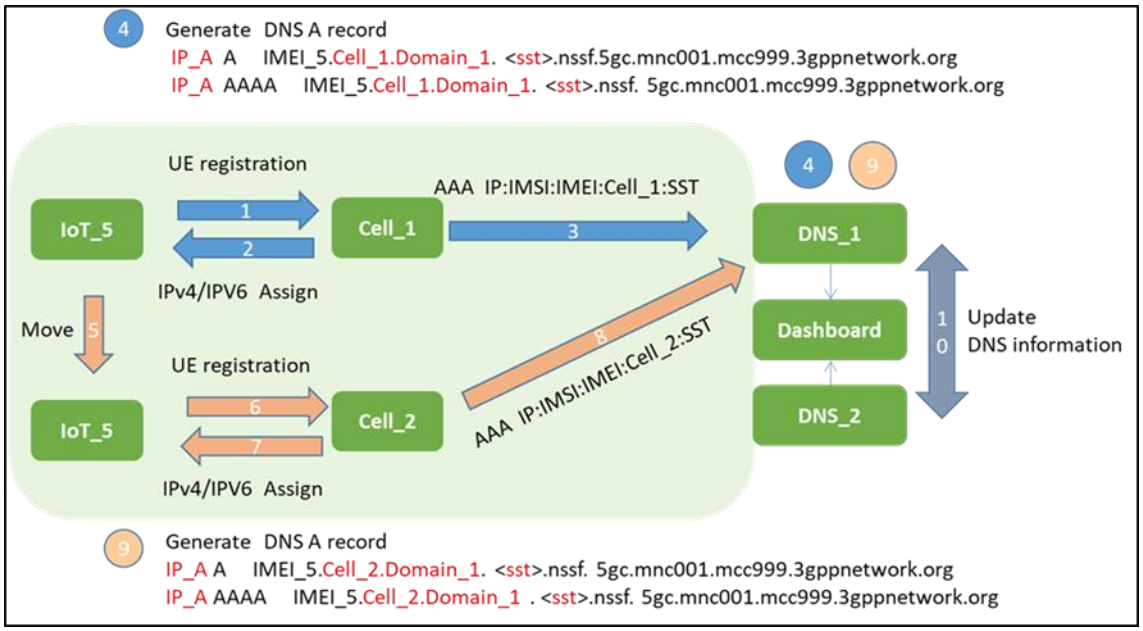



圖 22、同域移動之 IP 註冊與 DNS 動態管理流程

(二)驗證測試步驟及操作結果

下表 31 為各步驟說明：

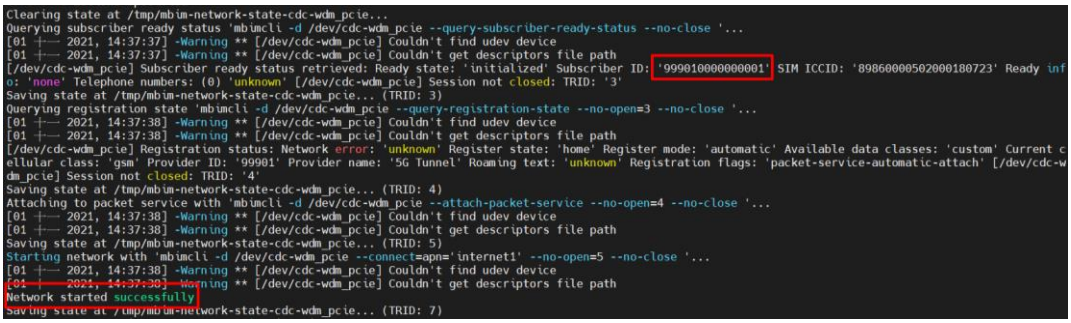
表 31、同域移動之 IP 註冊與 DNS 動態管理流程

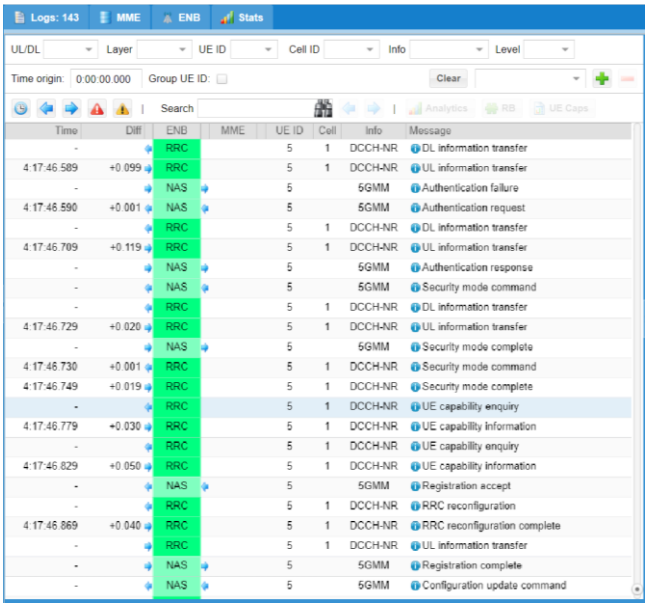
| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_1，並進行註冊 |
| 2 | 配發 IPv4/IPV6 位址 | 5G 模擬器配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | 傳送[IP：IMSI：IMEI：Cell_1：SST]等資訊至 DNS |
| 4 | Generate DNS A Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 5 | UE 移動 | IoT 從 Cell_1 移動至 Cell_2，同為 Domain_1 |
| 6 | UE registration | IoT 連線到 Cell_2，並進行註冊 |
| 7 | 配發 IPv4/IPV6 位址 | 5G 模擬器配發 IP 給 IoT，因為是同一 Domain，使用原來的 IP |
| 8 | 傳送註冊資訊至 DNS | 5G 模擬器傳送[IP：IMSI：IMEI：Cell_2：SST]等資訊至 DNS |
| 9 | Generate DNS A/AAAA Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 10 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA Record 資訊 |

➢ 步驟 1：IoT 註冊

啟動 IoT 設備連線到 5G 模擬器，並進行進行標準註冊流程

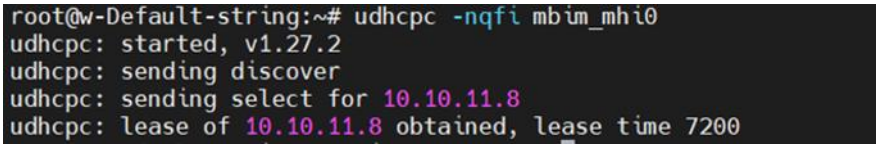
5G 模擬器顯示 IoT 設備連線至 Cell_1 並完成註冊

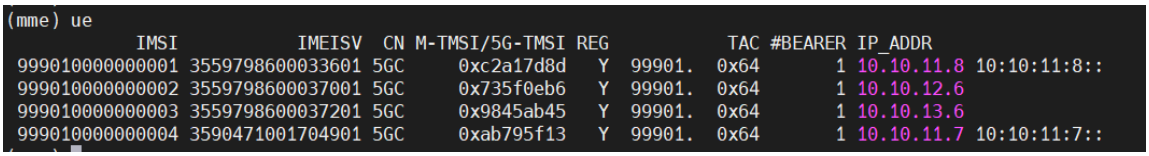



➢ 步驟 2：配發 IPv4/IPV6 位址

IoT 設備向 5G 模擬器要求 IP，5G 模擬器配發 IP 給 IoT 設備。



- 步驟 3：傳送註冊資訊至 DNS

  傳送[IP：IMSI：IMEI：Cell_1：SST]等資訊至 DNS

```
Attributes:
User-Name: ['5gc015']
User-Password: [b'\x08\xc8/\x82\x13\xc3\x1e\x83\xf6gb\xfc)/\xf7Y']
10.10.11.8,10:10:11:8:200:ff:fe00:0,999010000000001,355979860003363,1,20211101145309,start,1
10.10.12.6,10:10:12:4:200:ff:fe00:0,999010000000002,355979860003702,1,20211101145324,start,1
10.10.13.6,10:10:13:4:200:ff:fe00:0,999010000000003,355979860003728,1,20211101145334,start,2
Received an authentication request
Attributes:
User-Name: ['5gc001']
User-Password: [b'\x11\xc2\xe3\x1e\xce.c\xb7\x04\xfd\x05g\t\xb3\xf4\x7f']
```

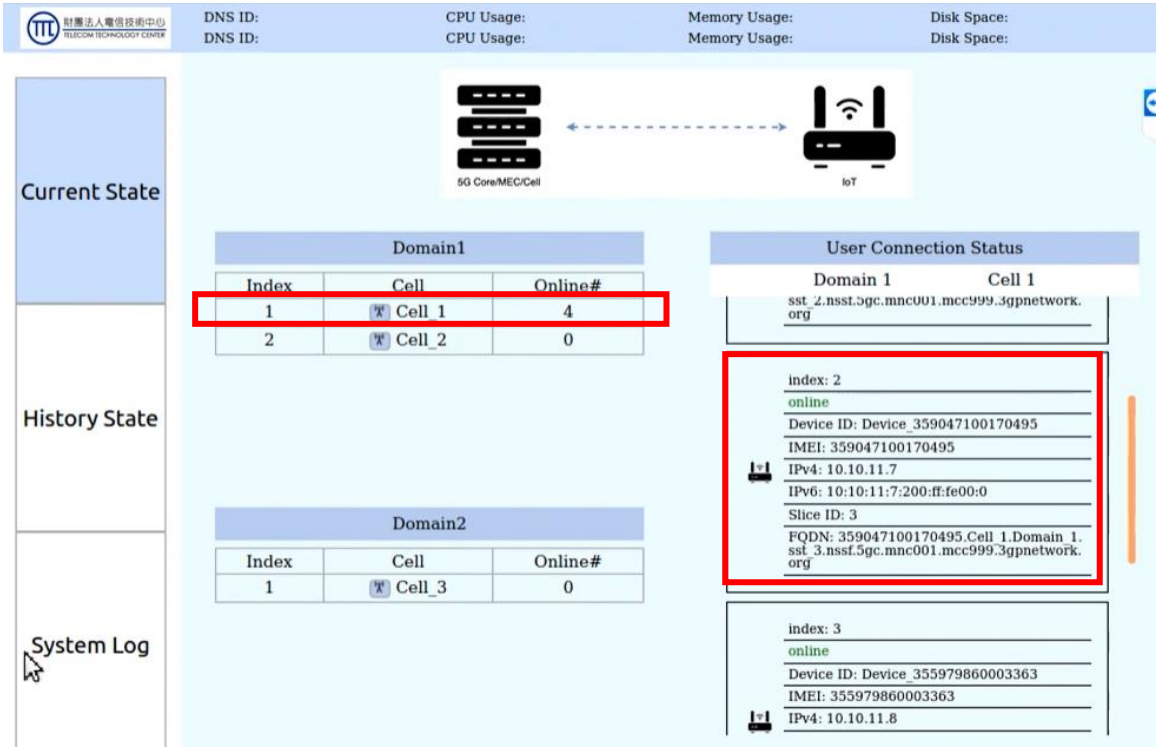
```
Received an authentication request
Attributes:
User-Name: ['5gc015']
User-Password: [b'z\x87\x8d\xb3\x8a\xd6\x8c\xfc"\xe20\x97X\xf3\x0fX']
10.10.11.7,10:10:11:7:200:ff:fe00:0,999010000000004,359047100170495,1,20211101144953,start,3
Received an authentication request
Attributes:
User-Name: ['5gc001']
User-Password: [b'\xa0\xa1P\x84\x17\x10S\x81\xd6\xce\x06\xa5\x81\x01\xf0I']
```

- 步驟 4：Generate DNS A Record

  DNS 透過自動編碼程式自動產生域名以及 DNS A Record

```
{"message": "Upload success"}{"message": "Upload success"}
10.10.12.6,10:10:12:4:200:ff:fe00:0,999010000000002,355979860003702,1,20211101145324,start,1
10.10.13.6,10:10:13:4:200:ff:fe00:0,999010000000003,355979860003728,1,20211101145334,start,2
10.10.11.8,10:10:11:8:200:ff:fe00:0,999010000000001,355979860003363,1,20211101145309,start,1
########################################
cat nssf.5gc.mnc001.mcc999.3gppnetwork.org
########################################
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
ns      IN      A       127.0.0.1
ns      IN      AAAA    ::1
359047100170495.Cell_1.Domain_1.sst_3  IN      A       10.10.11.7
359047100170495.Cell_1.Domain_1.sst_3  IN      A       10:10:11:7:200:ff:fe00:0
355979860003702.Cell_1.Domain_1.sst_1  IN      A       10.10.12.6
355979860003702.Cell_1.Domain_1.sst_1  IN      A       10:10:12:4:200:ff:fe00:0
355979860003728.Cell_1.Domain_1.sst_2  IN      A       10.10.13.6
355979860003728.Cell_1.Domain_1.sst_2  IN      A       10:10:13:4:200:ff:fe00:0
355979860003363.Cell_1.Domain_1.sst_1  IN      A       10.10.11.8
355979860003363.Cell_1.Domain_1.sst_1  IN      A       10:10:11:8:200:ff:fe00:0
```

檢視 Dashboard 畫面，可以看到 Cell_1 有 4 臺上線的 IoT 設備，點選進去可以看到 IoT_5 終端的系統資訊。




完成 1-4 步驟後，IoT 設備註冊 IP 以及自動註冊 DN 如下圖：

| | | IoT_1 | IoT_2 | IoT_3 | IoT_5 |
|---|---|---|---|---|---|
| | DNN | internet1 | internet2 | internet3 | internet5 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 359047100170495 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR 8K Videos | AR/VR 8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟 1,2 | Service IP IPv4 (DHCP) | 10.10.11.8 | 10.10.12.6 | 10.10.13.6 | 10.10.11.7 |
| 步驟 1,2 | Service IP IPv6 (DHCP) | 10:10:11:8:200:ff:fe00:0 | 10:10:12:4:200:ff:fe00:0 | 10:10:13:4:200:ff:fe00:0 | 10:10:11:7:200:ff:fe00:0 |
| 步驟 3,4 | DN | 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | 359047100170495.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org |

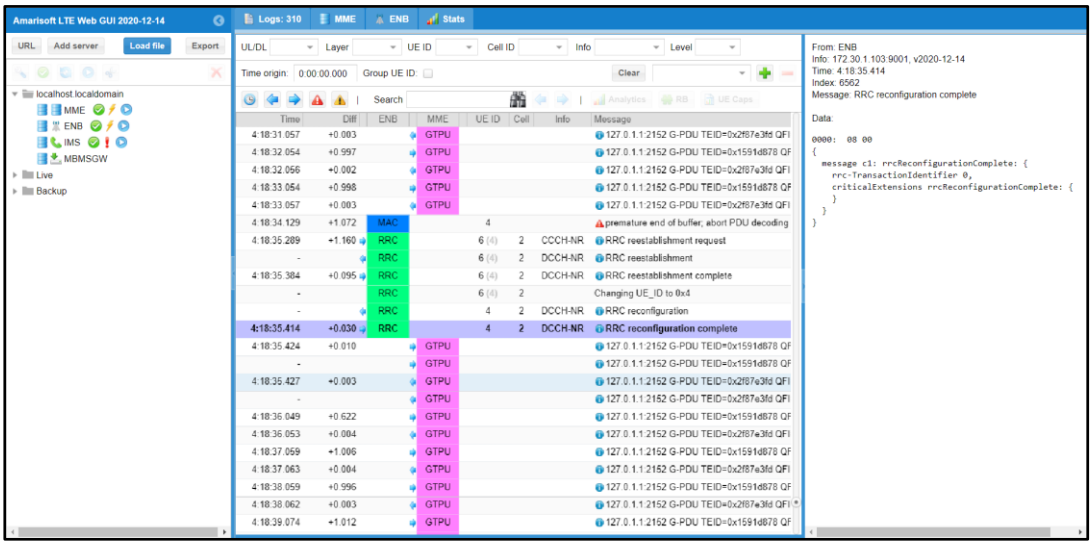
➢ 步驟 5： IoT 設備移動

從 Cell_1 移動至 Cell_2，同為 Domain_1

```
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        34           123 0x001 0x4622
        32           121 0x001 0x4620
        30           119 0x001 0x461e
        28           117 0x001 0x461c
(enb) cell_gain 2 0
(enb) cell_gain 1 -60
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        67             - 0x002 0x4643
        32           121 0x002 0x4642
        52             - 0x002 0x4634
        45             - 0x002 0x462d
(enb)
(enb)
(enb)
(enb)
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        32           121 0x002 0x4642
(enb)
[ localhost:root ][                                    0 MME  [1 ENB]  3 IMS  4 MBMSGW
```

➢ 步驟 6： IoT 設備 registration

IoT 設備連線到 Cell_2，並進行註冊



- 步驟 7： 配發 IPv4/IPV6 位址

  5G 模擬器配發 IP 給 IoT 設備，由於是同一 Domain，所以使用原來的 IP

- 步驟 8： 傳送註冊資訊至 DNS

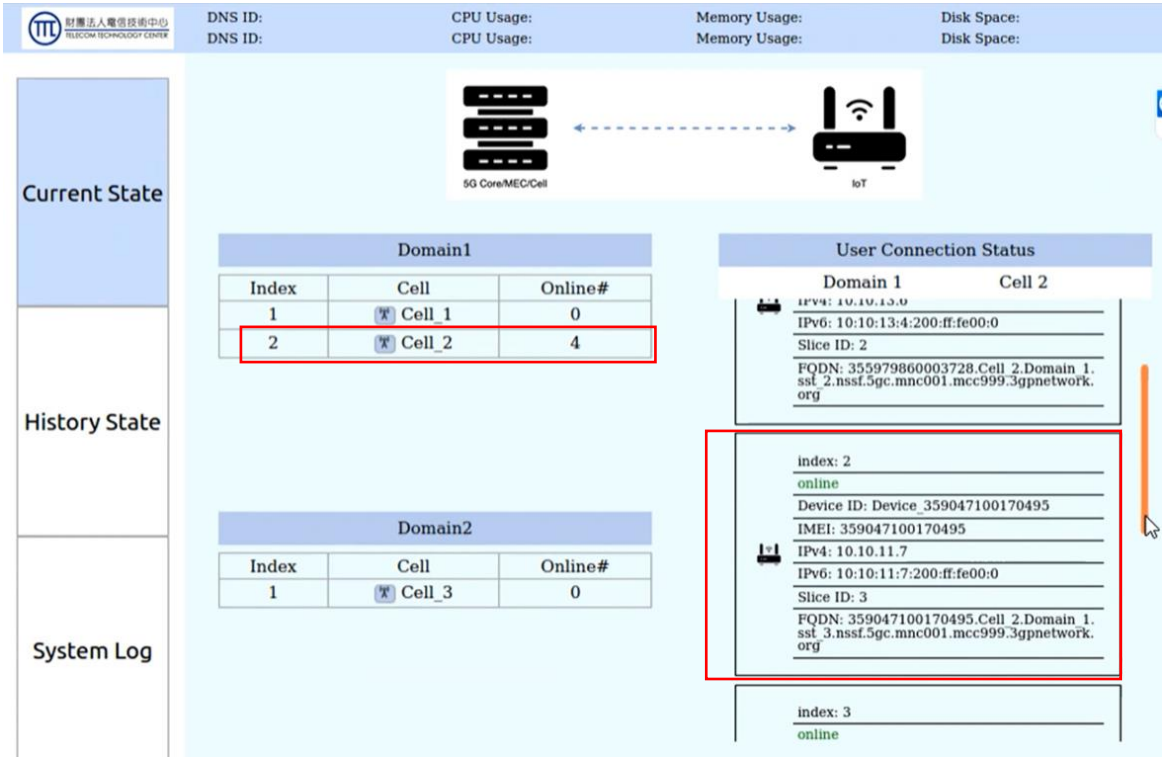
```
10.10.11.7,10:10:11:7:200:ff:fe00:0,999010000000004,359047100170495,2,20211101150037,start,3
10.10.11.8,10:10:11:8:200:ff:fe00:0,999010000000001,355979860003363,2,20211101150037,start,1
10.10.12.6,10:10:12:4:200:ff:fe00:0,999010000000002,355979860003702,2,20211101150037,start,1
10.10.13.6,10:10:13:4:200:ff:fe00:0,999010000000003,355979860003728,2,20211101150037,start,2
```

- 步驟 9： Generate　DNS A Record

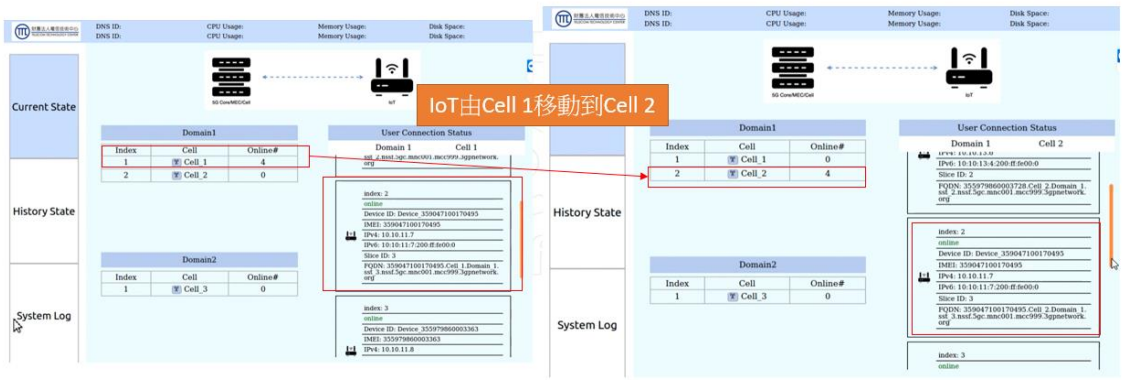
  DNS 透過自動編碼程式自動產生域名以及 DNS A Record，在 DNS 上顯示 DN 已更新

```
####################################
cat nssf.5gc.mnc001.mcc999.3gppnetwork.org
####################################
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
ns      IN      A       127.0.0.1
ns      IN      AAAA    ::1
359047100170495.Cell_2.Domain_1.sst_3  IN      A       10.10.11.7
359047100170495.Cell_2.Domain_1.sst_3  IN      A       10:10:11:7:200:ff:fe00:0
355979860003363.Cell_2.Domain_1.sst_1  IN      A       10.10.11.8
355979860003363.Cell_2.Domain_1.sst_1  IN      A       10:10:11:8:200:ff:fe00:0
355979860003702.Cell_2.Domain_1.sst_1  IN      A       10.10.12.6
355979860003702.Cell_2.Domain_1.sst_1  IN      A       10:10:12:4:200:ff:fe00:0
355979860003728.Cell_2.Domain_1.sst_2  IN      A       10.10.13.6
355979860003728.Cell_2.Domain_1.sst_2  IN      A       10:10:13:4:200:ff:fe00:0
```

檢視 Dashboard 畫面，可以看到 Cell_1 的上線裝置變為 0 個，Cell_2 的上線裝置變成 4 個。




➢ 步驟 10： DNS 與 Dashboard 更新資料



(三)同域移動設備參數內容

IoT 在同域的不同 Cell 移動時，DNN 與 IP 不更換，DN 會更改 Cell 名稱。

進入系統檢視 IoT 設備參數異動，如下圖所示：

| | | IoT_1 | IoT_2 | IoT_3 | IoT_5 |
|---|---|---|---|---|---|
| | DNN | internet1 | internet2 | internet3 | internet5 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 359047100170495 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR 8K Videos | AR/VR 8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟 6,7 | Service IP IPv4 (DHCP) | 10.10.11.8 | 10.10.12.6 | 10.10.13.6 | 10.10.11.7 |
| 步驟 6,7 | Service IP IPv6 (DHCP) | 10:10:11:8:200:ff:fe00:0 | 10:10:12:4:200:ff:fe00:0 | 10:10:13:4:200:ff:fe00:0 | 10:10:11:7:200:ff:fe00:0 |
| 步驟 8-10 | DN | 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 359047100170495.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

(四)同域測試結果

經由以上的測試，整理測試結果如下：

| 項次 | 測試內容 | 預期結果 | 測試結果 |
|---|---|---|---|
| 1 | 5G 模擬器及 DNS 間的編碼核配與管理 | 5G 模擬器可以透過 Radius 協議將 IP:IMSI: IMEI:Cell ID 資訊傳給 DNS | 於步驟 3 以及 9，5G 模擬器會透過 Radius 協議將 IP:IMSI:IMEI:Cell ID:SST 資訊傳給 DNS。 |
| 2 | Device 取得 IP (IPv4/IPv6)與 DNS mapping | 5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致 | IoT 設備於步驟 1、2 以及步驟 5、6、7 完成註冊後，自動取得 IP 位置。<br>檢視 5G 模擬器與 DNS 系統上所看到的 IP 資訊一致。 |
| 3 | DNS 編碼核配與管理 | DNS 可以依據 5G 模擬器產生 Radius 內容自動產出 A/AAAA Record | 於步驟 4、9，DNS 透過 Radius 協議得到的 IP:IMSI:IMEI:Cell ID:SST 資訊，自動產生 A/AAAA Record。 |
| 4 | 多個 Device 註冊 DNS 與核配編碼 | 比對各 5G 模擬器及 DNS：Device IP、IMSI、IMEI 及 Cell ID 結果一致 | 於 Dashboard 檢視各 IoT 設備的 IP、IMSI、IMEI 及 Cell ID 的資訊，與 5G 模擬器傳送的資料一致。 |

(五)System Log 及說明

Dashboard 上顯示同域測試過程中，IoT 設備註冊、移動、自動編碼產生 DN 之 System Log：

| Datetime | Payload | Type |
|---|---|---|
| 2021/11/1 14:50 | Device_359047100170495 is attached on Cell_1 with FQDN 359047100170495.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:53 | Device_355979860003728 is attached on Cell_1 with FQDN 355979860003728.Cell_1.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:53 | Device_355979860003702 is attached on Cell_1 with FQDN 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 14:53 | Device_355979860003363 is attached on Cell_1 with FQDN 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 15:01 | Device_359047100170495 is attached on Cell_2 with FQDN 359047100170495.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 15:01 | Device_355979860003363 is attached on Cell_2 with FQDN 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 15:01 | Device_355979860003728 is attached on Cell_2 with FQDN 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 15:01 | Device_355979860003702 is attached on Cell_2 with FQDN 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

## 二、 跨域測試

IoT 設備從 Cell_2 移動到 Cell_3，觀察 IP 與域名變化，測試內容如表 32。

表 32、跨域測試

| 項次 | 測試內容 | 預期結果 |
|---|---|---|
| 1 | 5G 模擬器及 DNS 間的編碼核配與管理 | 5G 模擬器可以透過 Raius 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS |
| 2 | 跨網域 Device 取得 IP（IPv4/IPv6）與 DNS mapping | 5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致 |
| 3 | 跨網域 Device 的 DNS 編碼核配與管理 | DNS 可以依據 5G 模擬器產生 Radius 內容自動產出 A/AAAA Record |

### (一)IP 註冊與 DNS 動態管理流程

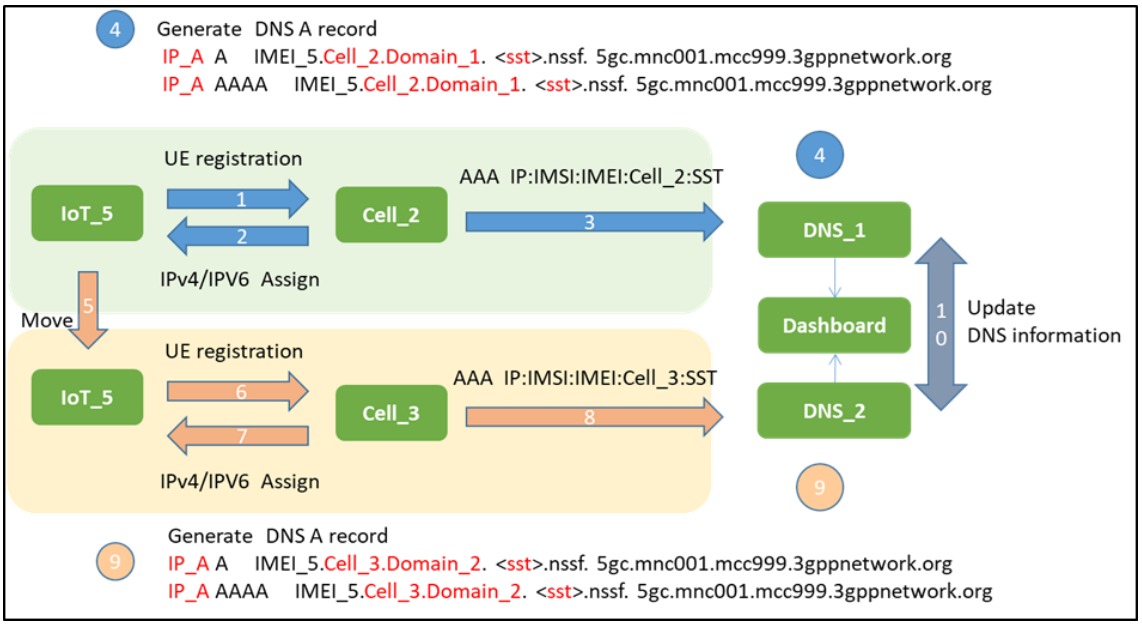



圖 23、跨域移動之 IP 註冊與 DNS 動態管理流程

(二)驗證測試步驟及操作結果

跨域移動之 IP 註冊與 DNS 動態管理各步驟說明如表 33。

表 33、跨域移動之 IP 註冊與 DNS 動態管理流程

| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_2，並進行註冊 |
| 2 | 配發 IPv4/IPV6 位址 | 5G 模擬器配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | 5G 模擬器傳送 [IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS |
| 4 | Generate DNS A/AAAA Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 5 | UE 移動 | IoT 從 Cell_2 移動至 Cell_3，從 Domain_1 移動至 Domain_2 |
| 6 | UE registration | IoT 連線到 Cell_3，並進行註冊 |
| 7 | 配發 IPv4/IPV6 位址 | 5G 模擬器配發 IP 給 IoT |
| 8 | 傳送註冊資訊至 DNS | 5G 模擬器傳送 [IP:IMSI:IMEI:Cell_3:SST]等資訊至 DNS |
| 9 | Generate DNS A/AAAA Record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA Record |
| 10 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA Record 資訊 |

驗證測試步驟及操作結果：

- 步驟 1 到步驟 4：請參考同域測試步驟 6~9
- 步驟 5：IoT 設備移動

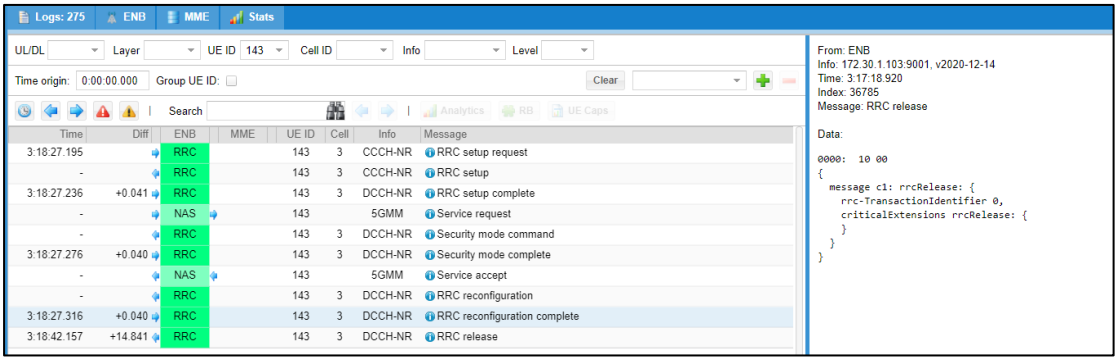
  IoT 設備從 Cell_2 移動至 Cell_3，從 Domain_1 移動至 Domain_2

```
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1     0.0      N 99901
0x003    NR  n78 0x000064   633228    3         1   -60.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        80           126 0x002 0x4650
        79           125 0x002 0x464f
        76           124 0x002 0x464c
        32           121 0x002 0x4642
(enb)
(enb)
(enb)
```

```
(enb) cell
[gnb0012345] PLMN=99901 gNB_ID=0x12345
Cell    RAT BAND      TAC dl_arfcn  pci prach_seq dl_gain ul_dis plmn
0x001    NR  n78 0x000064   632628    1         1   -60.0      N 99901
0x002    NR  n78 0x000064   632928    2         1   -60.0      N 99901
0x003    NR  n78 0x000064   633228    3         1     0.0      N 99901
(enb) ue
 RAN_UE_ID      CN_UE_ID  Cell   RNTI
        92           137 0x003 0x465c
        90           135 0x003 0x465a
        88           133 0x003 0x4658
        87           132 0x003 0x4657
(enb)
```

- 步驟 6：IoT 設備 registration

  IoT 設備連線到 Cell_3，並進行註冊




- 步驟 7：配發 IPv4/IPV6 位址

  5G 模擬器配發 IP 給 IoT 設備

```
(mme) ue
            IMSI              IMEISV  CN M-TMSI/5G-TMSI REG          TAC #BEARER IP_ADDR
 999010000000004 3590471001704901 5GC      0x1592bd3e   Y  99901.  0x64       1 10.10.11.9 10:10:11:9::
 999010000000001 3559798600033601 5GC      0xad850b6c   Y  99901.  0x64       1 10.10.11.10 10:10:11:a::
 999010000000002 3559798600037001 5GC      0xd7c256d3   Y  99901.  0x64       1 10.10.12.7
 999010000000003 3559798600037201 5GC      0x66417c34   Y  99901.  0x64       1 10.10.13.7
```

- 步驟 8：傳送註冊資訊至 DNS

  傳送[IP：IMSI：IMEI：Cell_3：SST]等註冊資訊至 DNS

```
User-Name: ['5gc015']
User-Password: [b'=\xf5\x96\x01\xf3I\x14\x8a\xee\x12\xefR\x93\x9bBL']
10.10.11.10,10:10:11:a:200:ff:fe00:0,999010000000001,355979860003363,3,20211101152230,start,1
Received an authentication request
Attributes:
User-Name: ['5gc001']
```

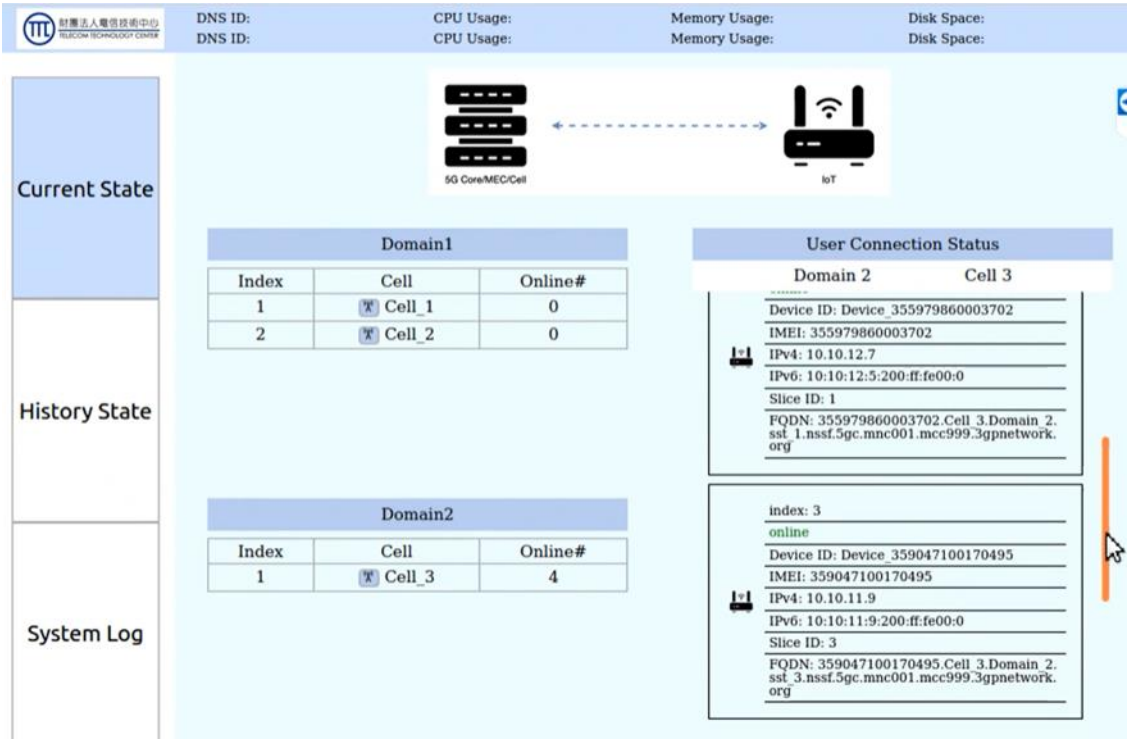
```
Attributes:
User-Name: ['5gc015']
User-Password: [b'\xe4\xd7-n \xa7\xa5\xd7\xa4;\xffp\x194\x91\x08']
10.10.12.7,10:10:12:5:200:ff:fe00:0,999010000000002,355979860003702,3,20211101152240,start,1
10.10.13.7,10:10:13:5:200:ff:fe00:0,999010000000003,355979860003728,3,20211101152245,start,2
Received an authentication request
Attributes:
User-Name: ['5gc001']
User-Password: [b'6\xb3\xb0\xc5\xbe+\x92\x90t\x1c\xbaig`\x88\x15']
```

- 步驟 9：Generate DNS A Record

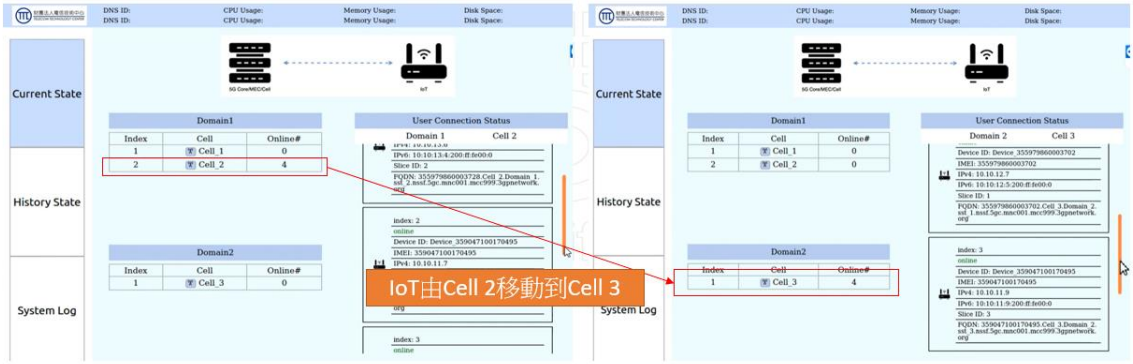
  DNS 透過自動編碼程式自動產生域名以及 DNS A Record，在 DNS 上顯示 DN 已更新

```
########################################
cat nssf.5gc.mnc001.mcc999.3gppnetwork.org
########################################
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
ns      IN      A       127.0.0.1
ns      IN      AAAA    ::1
359047100170495.Cell_3.Domain_2.sst_3  IN      A       10.10.11.9
359047100170495.Cell_3.Domain_2.sst_3  IN      A       10:10:11:9:200:ff:fe00:0
355979860003363.Cell_3.Domain_2.sst_1  IN      A       10.10.11.10
355979860003363.Cell_3.Domain_2.sst_1  IN      A       10:10:11:a:200:ff:fe00:0
355979860003702.Cell_3.Domain_2.sst_1  IN      A       10.10.12.7
355979860003702.Cell_3.Domain_2.sst_1  IN      A       10:10:12:5:200:ff:fe00:0
355979860003728.Cell_3.Domain_2.sst_2  IN      A       10.10.13.7
355979860003728.Cell_3.Domain_2.sst_2  IN      A       10:10:13:5:200:ff:fe00:0
```

檢視 Dashboard 畫面，可以看到 Cell_2 的上線裝置變為 0 個，Cell_3 的上線裝置變成 4 個。




➢ 步驟 10：DNS 與 Dashboard 更新資料



(三)跨域移動設備參數內容

UE 在跨域移動時，會取得新的 IP，同時也會更改 DN 的 Cell 與 Domain 名稱，進入系統檢視設備參數異動，如下圖所示：

| | | IoT_1 | IoT_2 | IoT_3 | IoT_5 |
|---|---|---|---|---|---|
| | DNN | internet1 | internet2 | internet3 | internet5 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 359047100170495 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR 8K Videos | AR/VR 8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟 6,7 | Service IP IPv4 (DHCP) | 10.10.11.10 | 10.10.12.7 | 10.10.13.7 | 10.10.11.9 |
| | Service IP IPv6 (DHCP) | 10:10:11:a:200:ff:fe00:0 | 10:10:12:5:200:ff:fe00:0 | 10:10:13:7:200:ff:fe00:0 | 10:10:11:9:200:ff:fe00:0 |
| 步驟 8-10 | DN | 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 359047100170495.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

(四)跨域測試結果

整理跨域移動測試結果如表 34：

表 34、跨域移動測試結果

| 項次 | 測試內容 | 預期結果 | 測試結果 |
|---|---|---|---|
| 1 | 5G 模擬器及 DNS 間的編碼核配與管理 | 5G 模擬器可以透過 Radius 協議將 IP:IMSI:IMEI:Cell ID 資訊傳給 DNS | 於步驟 3 以及 9，5G 模擬器會透過 Radius 協議將 IP:IMSI:IMEI:Cell ID:SST 資訊傳給 DNS。 |
| 2 | Device 取得 IP（IPv4/IPv6）與 DNS mapping | 5G 模擬器分配給 UE 的 IP 與傳送給 DNS 的內容一致 | IoT 設備於步驟 1、2 以及步驟 5、6、7 完成註冊後，自動取得 IP 位置。<br>檢視 5G 模擬器與 DNS 系統上所看到的 IP 資訊一致。 |
| 3 | DNS 編碼核配與管理 | DNS 可以依據 5G 模擬器產生 Radius 內容自動產出 A/AAAA Record | 於步驟 4、9，DNS 透過 Radius 協議得到的 IP:IMSI:IMEI:Cell ID:SST 資訊，自動產生 A/AAAA Record。 |

(五)System Log 及說明

跨域測試 System Log：從 Dashboard 下載資料中截取 IoT 設備跨域移動測試後自動編碼產生 FQDN 之 System Log 如表 35。

表 35、IoT 設備跨域移動測試後之 Dashboard System Log

| Datetime | Payload | Type |
|---|---|---|
| 2021/11/1 15:06 | Device_355979860003363 is detached from Cell_2 | INFO |
| 2021/11/1 15:06 | Device_355979860003702 is detached from Cell_2 | INFO |
| 2021/11/1 15:06 | Device_355979860003728 is detached from Cell_2 | INFO |
| 2021/11/1 15:06 | Device_359047100170495 is detached from Cell_2 | INFO |
| 2021/11/1 15:20 | Device_359047100170495 is attached on Cell_3 with FQDN 359047100170495.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 15:22 | Device_355979860003363 is attached on Cell_3 with FQDN 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 15:22 | Device_355979860003702 is attached on Cell_3 with FQDN 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |
| 2021/11/1 15:22 | Device_355979860003728 is attached on Cell_3 with FQDN 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gpnetwork.org | INFO |

# 附件六、下世代電信網路號碼我國參與國際組織之策略及效益

# 壹、我國參與國際組織之策略及效益

盤點國際組織之背景與宗旨、性質、結構及近年議題趨勢等，分析與本計畫主題之相關性後，綜整提出我國參與策略與效益，以擘劃我國未來國際交流藍圖。

1. 國際電信聯盟(International Telecommunication Union，簡稱 ITU)

(1) 背景與宗旨：ITU 成立於 1985 年，為聯合國轄下的國際組織，其成立宗旨為規劃全球無線電通訊的管理制度和標準、管理無線電頻譜和衛星軌道及促進全球的電訊發展。國際電信聯盟定期為政府、產業和中小型企業舉辦全球技術盛會，例如在世界各地所舉行的電訊展(TELECOM)活動，此活動中所展出的為電訊產業前瞻之產品及服務，並為政府機關和電訊政策及電訊產業有關的人士設立論壇，讓其有一個適當的論壇討論和分析最新的產業議題。

(2) 組織性質：政府間國際組織(IGOs)。

(3) 組織結構：國際電信聯盟的最高機構是全權代表大會(Plenipotentiary Conference)，現任秘書長為中國籍趙厚麟，任期至 2022 年。國際電信聯盟目前共區分為無線通信部門(ITU-R)、電信標準部門(ITU-T)和電信發展部門(ITU-D)三個主要領域：

a. 無線通信部門(ITU-Telecommunication Radiocommunication Sector，簡稱 ITU- R)：ITU- R 主要任務在於確保所有無線通訊業者能以合理適當、有效率且符合經濟效益的方式使用無線電頻譜。此一部門也從事和無線電通訊相關的研究並提出建議。

b. 電信標準化部門(ITU-Telecommunication Standardization Sector，簡稱 ITU - T)：ITU - T 主要任務在於電信技術標準，此一部門藉由研究技術標準、技術標準的運作和關稅問題，規劃國際電信聯盟的電信標準化事宜。

c. 電信發展部門(ITU-Telecommunication Development Sector，簡稱 ITU-D)：ITU-D 任務包括促使國際電信聯盟

成為聯合國下轄的專業機構，並且在聯合國的發展體制下負責執行各種有關計畫。電信發展部門也致力於推動技術合作和援助活動，以提升電信之發展。[3]

(4) 成為會員之方式：成為 ITU 成員須向 ITU 依單位身分填具申請，其分為企業單位及學術單位等兩類，填具申請表後，須向 ITU 成員國(即國家)之國家電信主管部門批准，然而我國目前仍未加入 ITU 成員國，因此正規之申請方式受阻。

(5) 須投入資源：依據 ITU 成員資格條款和條件規定，每年會員應繳交年費，而年費依據申請資格及國家屬性繳交費用。以下是 ITU-R、ITU-T 及 ITU-D 的費用表。換言之，倘若依學術成員身分申請加入 ITU 的 ITU-T，每年須投入至少新臺幣 60,773 元。

表 1、ITU 會費一覽表

單位：新臺幣元

| 部門 | 部門成員 | 部門準成員 | 學術成員 |
|---|---|---|---|
| ITU-R<br>(無線電通信) | $972,368<br>$121,546[4] | $324,122<br>$120,781[5]<br>$60,773[6] | $121,546<br>$60,773 [4] |
| ITU-T<br>(電信標準化) | $972,368<br>$120,781 [3] | $324,122<br>$120,781 [4]<br>$60,773 [5] | |
| ITU-D<br>(發展) | $7,950<br>$120,781[7] | $120,781 [4]<br>$60,773 [5] | |

說明：(費率換算基準)

---

[3] 經濟部標準檢驗局（2008 年 8 月 15 日）。國際通信聯盟(ITU)。檢自：https://www.bsmi.gov.tw/wSite/ct?xItem=16648&ctNode=9175&mp=1（最後瀏覽日：2021/5/10）

[4] 年人均收入低於 2,000.00 美元（UNDP 標準）的發展中國家，尚未加入該部門或兩個部門並且不是總部設在發達國家的跨國公司的子公司。

[5] 發達國家的中小型企業。

[6] 發展中國家和最不發達國家的中小型企業。

[7] 發展中國家和最不發達國家。

**資料來源：ITU 官方網站**[8]

(6) 擔任幹部之方式：選舉投票制。

(7) 近年議題趨勢：ITU 成立的主要目的在於劃分全球的無線電頻譜、衛星軌道及制定技術標準[9]，因此會議中的討論議題包含了通訊監管及全球電信發展等。然近年隨著 5G、人工智慧等新興技術的發展，國際電信聯盟的視角也開始轉向物聯網及人工智慧等議題，並且因新冠疫情影響，近年議題也包含人工智慧在應對流行病中的角色等。

(8) 參與建議：依據上述該組織之結構可得知，ITU-T 所關注的電信技術標準及電信標準化事宜，與本計畫下世代電信網路號碼技術及管理具有高度相關性，然而依據上述分析我國國際處境特殊，~~我國也~~未能加入 ITU，因此參與 ITU 必須透過其他國家或與國外單位合作。今年度評估參與國際會議及活動方式以培養專家學者及蒐集與國際下世代電信網路議題相關資料，有鑑於此，今年度參與 ITU Digital World 公開會議。

ITU Digital World 於 2021 年 9 月至 12 月召開，該會議主要由各國政府、企業、科技中小企業匯聚一堂，共同分享未來電信發展技術及趨勢，及各國未來政策及戰略目標等。

2. 第三代合作夥伴計畫(3rd Generation Partnership Project，簡稱 3GPP)

(1) 背景與宗旨：3GPP 於 1998 年 12 月成立，其成立宗旨為推廣符合 IMT-2000 技術規範的 3G 通用行動通訊系統(Universal Mobile Telecommunication System，簡稱 UMTS)。而成立目的在於準備、批准及維護可用於 3G 網路的技術標準規格，此技術標準規格又以 Evolved GSM core network 及 Universal Terrestrial Radio Access(UTRA)為基礎，並由會員

[8] MyITU (Membership).https://www.itu.int/zh/myitu/Membership/Become-a-Member/Fees. （最後瀏覽日：2021/5/12）

[9] ITU（2021 年 4 月 13 日）。國際電聯是主管信息通信技術事務（ICT）的聯合國機構。檢自：https://www.itu.int/zh/about/Pages/overview.aspx（最後瀏覽日：2021/5/12）

將其發展成可供商業市場使用的技術及商業化應用。該組織目前成員包括歐洲電信標準協會(ETSI)、日本的電波產業協會(ARIB)和日本情報通訊技術委員會(TTC)、中國通信標準化協會(CCSA)、韓國電信技術協會(TTA)、北美洲的電信工業解決方案聯盟(ATIS)和印度的電信標準開發協會。

(2) 性質：非營利機構(NPO)。

(3) 結構：3GPP 主要是由一個「專案統籌小組(Project Coordination Group, PCG)」和數個專門的「技術規範小組(Technical Specification Groups, TSGs)」組成。技術規範小組在需要時可以建立「工作組(Working Groups)」，而組織夥伴需有例會制度。在作法上，3GPP 採用快速和電子化的工作程序以及簡化標準審批流程，以縮短「技術規範(Technical Specifications)」和「技術報告(Technical Reports)」從被定義到被批准接受的時間。[10]

3GPP 的成員類型主要包括「組織夥伴(Organizational Partner)」，必須經過一國或一地區之官方授權或認可，且有權利在該國或該地區之技術領域具全面或局部性定義、出版及建立標準之工作；「市場代表夥伴(Market Representation Partner)」則是被 3GPP 的組織夥伴邀請參加並致力於建立標準之相關工作，但無權力在該國或該地區就技術面進行全面或局部性定義、出版和建立標準之企業或研發等單位。

(4) 成為會員之方式：3GPP 為 NPO 組織，不同於 ITU 具有強烈的官方色彩，而是以公司、政府部門或教育機構名義，向組織合作夥伴的成員部門申請[11]。

(5) 擔任幹部之方式：選舉投票制。

(6) 近年議題趨勢：3GPP 每年會在全球不同區域召開會議，其工作組下分別為服務與系統方面(service and System Aspects, SA）、無線電接入網(Radio Access Network, RAN )及核心網

[10] 經濟部標準檢驗局（2009 年 6 月）。產業技術標準活絡及推廣委辦計畫深入國際標準化組織。檢自：https://www.bsmi.gov.tw/wSite/public/Data/f1352964204876.pdf（最後瀏覽日：2021/5/13）

[11] TWNIC，ICANN 組織簡介（一），台網中心電子報，2017 年 7 月，https://www.3gpp.org/about-3gpp/membership（最後瀏覽日：2021/5/13）

路與終端( Core Network and Terminals, 簡稱 CT )等技術規格小組(TSG)發展會議，對 5G 標準進行討論。目前最新 5G 標準版本為 Release 16，為 5G 應用加入不少升級，全力完善「獨立 5G 網路」，就是無需靠 4G 硬體和標準之純 5G 網路，新規格可支援各行業實務應用，如自動駕駛、工業網路、智慧物流和遠距醫療等。下一階段 Release 17 5G 標準，在 2021 年下半年完成，然目前因疫情影響，皆改為電子會議方式舉行，原先規劃於 2021 年發行之 Release 17 第 2 階段功能及第 3 階段協議之時程則於 2022 年凍結。

3. 網際網路名稱與數字位址分配機構
(Internet Corporation for Assigned Names and Numbers，簡稱 ICANN)

(1) 背景與宗旨：ICANN 為全球性的非政府非營利組織，1998 年 10 月成立於美國加州，負責監督管理網際網路技術管理功能(Internet technical management functions)、通訊協定參數及通訊埠(Protocol Parameters and Port)之協調、域名系統(Domain Name System，DNS)之管理、IP 位址之分配及指派，以及根伺服器系統(Root server system)的管理。由於 ICANN 為攸關全球網路順暢運作及協調管理的重要網路國際組織，有別於傳統國際組織由上而下的運作過程，ICANN 在政策制定方面採取的是多方利益共同體(multi-stakeholders)參與模式，將個人、企業、非商業利益組織及政府置於同等地位，並以全體 ICANN 社群為基礎形成的共識決，以符合全球網際網路結構「無國界」、「對所有人開放」的特點。

(2) 性質：非營利機構(NPO)。

(3) 結構：ICANN 的組織結構主要包括 ICANN 董事會(Board of Directors)、3 個支援組織(Supporting Organization, SO)、4 個諮詢委員會(Advisory Committee, AC)、ICANN 組織職員(CEO/Staff)以及 ICANN 監察部門。SO 的成員多為政府以外的參與者，透過由下而上的流程制定政策；擬定政策通過 ICANN 董事會決議後，再交付 ICANN 組織職員據以實施。

AC 的責任則是向 ICANN 董事會提出建議，而後者可選擇接受或拒絕這些諮詢建議。ICANN 董事會主要負責監督政策發展過程及 ICANN 管理，並對政策建議有最終決定權。董事會由 16 名票選會員及 5 名聯絡代表(liaison representative)組成，董事會主席也是票選會員其中一員。[12]

(4) 成為會員之方式：個人、企業、非商業利益組織及政府都可參加 ICANN 會議。

(5) 擔任幹部之方式：投票選舉制度。

(6) 近年議題趨勢：ICANN 每年都會在全球不同地區召開 3 次國際大型會議，議程安排除了 ICANN 大會、公眾論壇、跨社群論壇，亦包含 ICANN 內部各社群的內部議程、各政策制定(Policy Development Procedure, PDP)工作小組會議(GNSO Policy Development Process)，以及由技術社群主辦的網域名稱(Domain Name)技術研討會等。ICANN 會議任何人都可免費報名參加。此外，ICANN 的公開議程都有網路直播，也開放線上參與。以往會議期間約舉辦 200 多場議程，2021 年 3 月舉辦之 ICANN 70 因疫情關係改為線上參與形式，會議議程也縮減至 100 場以內。綜觀 ICANN 於 2021 年國際會議設定的主題，多項是延續 2020 年議題，大致上包括域名問題，例如通用頂級域名(Generic Top Level Domain，簡稱 gTLD)、國家及地區頂級域名(Country Code Top-Level Domain，簡稱 ccTLD)等議題；DNS 議題(例如 DNSSEC 和安全研討會、KINDNS 演示和研討會、ICANN 授權的未來和 DNS 的發展：下一代的聲音)與網路治理等相關議題。

[12] TWNIC，ICANN 組織簡介（一），台網中心電子報，2017 年 7 月，http://www.myhome.net.tw/2017_07/p08.htm。（最後瀏覽日：2021/5/13）

(7) 今年會議場次：

表 2、ICANN 會議場次盤點

| 2021 年場次 | 主題 | 時間 |
|---|---|---|
| ICANN 70 | Community Forum | 22-25 March 2021 |
| ICANN 71 | Policy Forum | 14-17 June 2021 |
| ICANN 72 | Annual General Meeting | 23-28 October 2021 |

4. 網際網路工程任務組(Internet Engineering Task Force，簡稱 IETF)

(1) 背景與宗旨：IETF 為隸屬於網際網路協會(Internet Society，簡稱 ISOC)的國際組織，其由全球關心網際網路發展的網際網路設計者、操作者、使用者和研究者所組成，負責網際網路標準的研究發展和制定，例如網際網路上使用的通訊協定(protocols)、程序 (procedures)和慣例(conventions)等的制定。

(2) 性質：非營利機構(NPO)

(3) 結構：IETF 是由工作群組(working groups)委員會所組成，其工作群組大多屬於任務性編組，因針對特殊問題或議題而暫時成立，當任務結束後或目標完成，該工作群組將停止或解散。IETF 工作群組包括網路工程指導小組(Internet Engineering Steering Group, IESG)、網路研究工程組(Internet Research Task Force)、網路架構委員會(Internet Architecture Board)、董事會(Directorates)等。其中，網路工程指導小組負責 IETF 活動和網路標準流程的技術管理；網路架構委員會為網路標準提供長期的技術指導；網路研究工程組則為專注於網路協議、應用、體系結構和技術相關主題的長期研究小組。

(4) 成為會員之方式：沒有會員制度，個人均可參加或發表文件，參與對象以個人為主，而不是國家、公司或團體。

(5) 擔任幹部之方式：IETF Chair 由 ISOC 指派，因此爭取 IETF Chair 職位較為困難，然而 7 大工作領域的董事(Area Director，簡稱 AD)是由自願參加的候選人中隨機選出，但必須在最近 5 次的 IETF 會議中，參加過 3 次以上才能有候選人資格，相較之下參選 AD 較為可行。但由於 IETF 為技術性國際組織，若想要參選 AD，必須在專業工作領域相當熟悉，經評估持續且積極參與 IETF 會議及 Mailing lists 討論 3 年以上才有爭取擔任幹部之機會。

(6) 近年議題趨勢：IETF 每年舉辦三次會議，對於參與會議的參加者無資格上的限制，並針對網際網路協定等相關議題進行討論。例如，IETF 110 中有五場與 DNS 相關的會議，並已針對物聯網設備的 DNS 名稱自動配置提出了草案。IETF 有 7 大領域，包括 ART (Applications and Real-Time Area)、GEN(General Area) 、 INT(Internet Area) 、 OPS(Ops & Management Area)、RTG(Routing Area)、SEC(Security Area)及 TSV(Transport)，有 130 餘個工作小組分屬其中，每個領域設置 2 名 Directors，Directors 與 IETF 主席組成 IESG(Internet Engineering Steering Group)，共同處理業務及標準審查。與本案相關之領域為 INT(Internet)、RAI(Real-time Applications & Infrastructure)及 RTG(Routing)領域，今年度專家學者及計畫研究團隊參與及觀察 4 個工作領域的會議及先前發布的草案，並從 4 個工作領域中鎖定 1 至 2 個工作小組，作為未來積極參與 Mailing lists 及議題設定的目標。

5. GSM 協會(Groupe Speciale Mobile Association，簡稱 GSMA)

(1) 背景與宗旨：GSMA 成立於 1995 年，是一個由行動通訊業者及相關公司為了全球行動通訊系統(Global System for Mobile Communications, GSM)的共通標準建置及推動所贊助成立的協會，是世界行動通訊界的三大國際組織之一。GSMA 代表全球行動營運商的共同權益，成員包括全球 218 個國家和地區逾 750 家行動通訊營運商和 400 多家企業，

其中包括手機與裝置製造商、軟體公司、設備供應商、網際網路企業以及金融、醫療、媒體、交通和公共事業等領域的企業。

GSMA 每年在西班牙巴塞隆納、美國洛杉磯和中國上海舉辦業界領先的世界行動通訊大會(Mobile World Congress, MWC)，是全球具影響力的專注於行動通訊領域的展覽會之一。除盛名遠播的 MWC 巴塞隆納世界行動通訊大會，尚有 MWC 洛杉磯世界行動通訊大會、MWC 上海世界行動通訊大會以及行動 360 系列區域會議等會議。行動 360 系列是 GSMA 於全球不同區域舉辦之研討平臺，邀集各國通訊傳播監理機關、行動通訊領域專家學者、行動通訊業者及相關垂直應用行業代表等，共同就行動通訊相關發展主題進行在地案例及全球經驗之討論，期藉由交流、學習成功經驗，促進各國行動通訊環境之提升，為人民及消費者帶來福祉。[13]但是截至今年四月底尚未公布今年行動 360 系列區域會議日程。

今年雖因新冠肺炎(COVID-19)疫情影響，GSMA 仍堅持舉辦 MWC 會議，但將巴塞隆納世界行動通訊大會展覽活動由原訂 3 月 1 至 4 日延後至 6 月 28 日至 7 月 1 日舉辦，並以實體及部分線上方式辦理。根據 GSMA 官網的資料，GSMA 每年在西班牙巴塞隆納、美國洛杉磯和中國上海舉辦的 MWC 合計約有 19 萬人參與。[14]

(2) 性質：非政府組織(NGO)

(3) 結構：GSMA 的組織結構分為主席、總幹事、GSMA 諮詢董事會、GSMA 組織成員、區域利益集團和高級顧問等。要成為 GSMA 企業會員需繳交會費，每年的年度會費基於公司上一年的年收入，其中營運商會員資格(Operator Membership)開放給使用 GSM 系列技術的許可行動網路營運商、報告人會員資格(Rapporteur Membership)開放給行動

[13] 國家通訊傳播委員會，出席 GSMA 行動 360 系列—數位化社會會議出國報告書，2018 年 11 月，https://www.ncc.gov.tw/chinese/files/19091/5012_41986_190917_1.pdf。（最後瀏覽日：2021/5/23）

[14] 駐西班牙台北經濟辦事處，西班牙「Expansión 日報」9 月 24 日報導：行動通訊協會(GSMA)宣布，2021 年在西班牙巴塞隆納舉辦之世界行動通訊大會(MWC)將延至 6 月辦理，2020 年 9 月，https://www.roc-taiwan.org/es/post/13735.html。（最後瀏覽日：2021/5/23）

虛擬網路營運商(Mobile Virtual Network Operator, MVNO)和非 GSM 許可營運商、企業成員資格(Sector Membership)開放給相關企業組織。

(4) 成為會員之方式：成員主要以企業為主

(5) 近年議題趨勢：主題較為多元，包含手機與裝置製造商、設備供應商、網際網路企業以及金融、醫療、媒體、交通和公共事業等領域。經盤點後，該組織討論議題與研究關聯性較低，將不續行蒐集相關該組織資料。

6. 國際標準化組織(International Organization for Standardization，簡稱 ISO)

(1) 背景與宗旨：1946 年 10 月 14 日，來自 25 個國家的代表在倫敦召開會議，決定發起成立一個新的國際組織，目的是促進國際間的合作和各領域標準的統一，故 ISO 於 1947 年 2 月 23 日正式成立，其總部則設在瑞士的日內瓦。宗旨為制定、發佈和推廣國際標準、協調世界範圍內的標準化工作、組織各成員國和技術委員會進行交流，並與其他國際組織共同研究有關標準化議題。[15]

(2) 性質：非政府性國際組織(INGO)

(3) 結構：國際標準化活動最早開始於電機領域，在 1906 年成立了世界上最早的國際標準化機構「國際電工委員會(International Electrotechnical Commission, IEC)」；非電機的技術領域工作，則由成立於 1926 年的「國家標準化協會國際聯盟(International Federation of the National Standardizing Associations, ISA)」負責，ISA 重點在於機械工程方面。國家標準化協會國際聯盟(ISA)和聯合國標準協調委員會(UNSCC)皆可視為 ISO 的前身。ISO 成員屬性可分為正式成員、通訊成員及註冊會員。與 ISO 有聯繫的國際組織、政府或非政府組織都可參與工作。根據需要可下設分技術

[15] 經濟部標準檢驗局(2009 年 9 月)。深入國際標準化組織。檢自：http://www.standards.org.tw/CKEdit/upload/21/files/201506080817.pdf（最後瀏覽日：2021/5/23）

委員會(SC)和工作組(WG)。技術委員會(TC)及 SC 由各成員國自願參加，TC 及 SC 之主席與秘書經選舉產生。ISO 還與國際電工委員會(IEC)共同建立了聯合技術委員會(JTC)。

(4) 參與方式：國家或地區才能申請為 ISO 會員，個人或公司不能成為 ISO 成員。

(5) 近年議題趨勢：ISO 設有 5 大機構，包括全體大會、理事會、中央秘書局主要官員、政策制定委員會、技術管理局，這些主要機構之下還設有多種的技術性委員會，例如特別諮詢小組、標準物質委員會、技術委員會、技術諮詢小組等[16]，技術諮詢小組又可分為技術委員會及工作小組，各自依需求發展多次相關技術會議，每年皆會在世界各地舉辦約 26 場技術會議。ISO 全體大會是國際標準化組織的最高權力機構。每年召開會議一次，針對年度報告中有關項目的工作情況、策略計畫及財政預算、支出等做出決議。

[16] 新世紀智庫論壇第 54 期(2011 年 6 月 30 日)。國際標準化組織(ISO)。檢自：http://www.taiwanncf.org.tw/ttforum/54/54-18.pdf（最後瀏覽日：2021/5/23）

# 附件七、人才培育成果報告

# 貳、第一場國際會議：ICANN 71

## 一、 ICANN 71 會議簡介及議程

ICANN 每年會在全球的不同地區召開三次國際公開會議。由於 COVID-19 持續流行，ICANN 將 ICANN 社群、董事會與工作人員的健康、安全為首要考量，故原定於 2021 年 6 月 14 日至 17 日在荷蘭海牙舉行之 ICANN71 會議，仍維持虛擬會議方式召開。ICANN71 虛擬會議時區為 UTC+2，與我國時差 6 個小時，使用會議軟體為 Zoom Meeting Virtual Room。

ICANN71 為政策論壇，故許多會議將側重於特定的政策制定工作或跨社群討論。ICANN71 會期也將舉辦三場由跨社群的全體會議，主題包含近期的網路監管發展、ICANN 在網際網路治理生態系統中的角色，以及討論「網域註冊信譽阻止列表提供商」（Domain Registration Reputational Block List Provider）之運作方式。

目前 ICANN71 虛擬會議規劃召開之會議超過 70 場次，而為掌握國際下世代電信網路號碼趨勢，建議參與以下會議：

| 臺灣時間 | 會議名稱 | 效益分析 |
|---|---|---|
| 14, June<br>15:00-16:00 | DNSSEC and Security Workshop (1 of 2) | 1. 希望透過會議中的分享，了解 DNS 安全及資安相關議題及政策發展方向，做為我國擘劃 DNS 及網路安全政策之參考。<br>2. 此外，相關資安議題，也可透過會議中的討論，作為後續研究之參考。 |
| 14, June<br>16:30-18:00 | DNSSEC and Security Workshop (2 of 2) | |
| 14, June<br>18:30-20:00 | Plenary Session: Impact of Regulatory Developments on ICANN Policy Topics[17] | 1. 希望透過會議中的分享，了解各國國內法在 ICANN 各項政策的影響，及後續可能進展的方向，進而推測未來國際網際 |

[17] 原議程名稱為 Plenary Session 1: Governmental Regulatory Developments, WHOIS, Data Protection, and Cybersecurity，會議討論內容不變。

| 臺灣時間 | 會議名稱 | 效益分析 |
| --- | --- | --- |
| | | 網路政策發展方向，做為我國擘劃網路政策之參考。<br>2. 此外，相關資安議題，也可透過會議中的討論，作為後續網路運作（無論是固定網路、行動網路或是物聯網）相關行為規範制定的參考。 |
| 14, June<br>20:30-22:00 | Tech Day (1 of 2) | 1. 透過技術性議題的分享，可獲悉與網域名稱產業(註冊業務、DNS、網路安全等）相關的技術知識。<br>2. 透過會議的召開，結識更多各專業領域的著名專家，擴展技術人際脈絡。 |
| 16, June<br>16:30-18:00 | GNSO - CPH DNS Abuse Work Group Community Update | 本會議旨在更 ICANN 締約方（CPH，即註冊管理機構與受理註冊機構）DNS 濫用工作小組進度。透過 GNSO 締約方對 DNS 濫用行為的研析與應對行為報告，藉此了解 ICANN 部分社群對 DNS 濫用行為的相關規範制定方向與採取措施，以做為未來相關場域規範、限制與濫用行為認定之參考。 |
| 17, June<br>20:30-22:00 | SSAC Public Meeting | 透過「安全與穩定諮詢委員會」（SSAC）與公眾的互動和對談，進一步了解該社群特性與參與社群的成員的行業屬性，以此做為我國未來啟動新型態網路建設， |

| 臺灣時間 | 會議名稱 | 效益分析 |
|---|---|---|
| | | 在組建網路安全與「服務提供水層級」(Service Level)維持相關的機制時，可有一足供參照且持續運作之對象。 |
| 17, June 22:30-23:30 | The Post-Pandemic Future of ICANN Public Meetings | 1. 該議程將討論下次 ICANN 會議的形式及討論議程。<br>2. 希冀透過參加該會議，掌握 ICANN72 討論議題主軸，以利本計畫提前準備研究及相關事宜。 |

## 二、 ICANN 71 會議紀錄

### (一) 網域名稱系統安全擴充和安全性研討會 1/2 及技術日(DNSSEC and Security Workshop 1 of 2 and Tech Day)

| 日期 | 6/14(一) | 參與會議場次 | ICANN71 |
|---|---|---|---|
| 會議主題 | DNSSEC and Security Workshop (1 of 2) and Tech Day (1 of 2)<br>網域名稱系統安全擴充和安全研討會（2-1）和技術日（2-1） | | |
| 會議交流 | 在 DNSSEC and Security Workshop (1 of 2)這場會議中，由 Ericsson 公司的 Daniel Migault 主講 TLS Identity Pinning（TLS 身分綁定）這個題目，這個演講分享一個想法，就是目前客戶端（Client）要確認它所連結的伺服器端（Server）是真正的伺服器端，而不是其他偽冒的假伺服器端，且是運用憑證技術，例如：X.509 憑證。但目前可頒發憑證的頒發機構（Certificate Authority，簡稱 CA）甚多，在一個瀏覽器裡的預設可信任的憑證頒發機構就有約 75 個。另外，憑證的管理也常出現問題，容易被有心人運用漏洞而躲開運用憑證來證明客戶端所連結的伺服器是否為真的這個機制。還有，伊朗的駭客曾成功地使用中間人（Man-in-the-Middle，簡稱 MITM）攻擊，將正確的伺服器端位址，經由假扮上層 DNS 伺服器並提出更改 DNS 紀錄的要求至下層 DNS 伺服器，而成功地暫時將某些 client 正常的伺服器請求流量，導入假的伺服器上，藉此拿到重要的 SSL 憑證或 | | |

| | |
|---|---|
| | email 憑證（credentials）。所以，Daniel Migault 提出要在伺服器端使用第二個身分辨識方法（或方式）的機制（Server-side 2FA）來加強伺服器端目前只有憑證的身分辨識機制。<br>那麼這第二個身分辨識機制的目標是甚麼呢？就是確保每次 client 連結 TLS server 時，其所連結的 TLS server 要能證明它就是上次這個 client 連結的 TLS server。這就是 server identity 的概念。那麼，如何實踐這個概念呢？Daniel Migault 提出一個簡單的協定，運用 client 在第一次連結 TLS server 時，在這個安全的通道，傳送一個自己生成的秘密值給 server，日後，client 再連結 TLS server 時，server 的回覆訊息裡面必須含有這個秘密值，來證明自己就是 client 第一次連結的 server。Daniel Migault 認為這個機制很適合企業內部的網路來實踐，因為這個機制對 client 沒有額外的管理負擔、client 與 server 都只需要實作 TLS 通道的能力即可、這機制與 TLS 憑證可以相互搭配使用、這機制適合 B2B 的通訊使用。我向 Daniel Migault 問了兩個問題：(1)這個機制對 TLS server 的運行負擔為何？(2)這個機制適合 M-to-M（機器對機器）通訊使用嗎？Daniel Migault 認為他們提出的這個機制對 TLS server 的運行負擔不會太大，也可以使用在 M-to-M（機器對機器）通訊，雖然他們一開始並沒有朝這方面規劃。 |
| 會議過程 | 這次參加 ICANN71 會議，被指派參與兩個場次的會議：DNSSEC and Security Workshop (1 of 2) and Tech Day (1 of 2)。這兩個會議場次多為與 DNS 相關的新技術議題，或是報告最近各國使用 DNSSEC 資安強化機制的整體情況，也有一些新的工具、服務或架構的介紹。在 DNSSEC and Security Workshop (1 of 2)這場會議中，首先是 Dan York 針對 DNSSEC Workshop 的整體性介紹，談及目前的主要組成分子（Program Committee）、主要支持這個工作坊的組織（ICANN SSAC, Internet Society）、DNSSEC 等三個機制（DNSSEC, DANE, RPKI）目前在全世界的部署情形。<br>再來是 Ericsson 公司的 Daniel Migault 介紹 TLS Identity Pinning 機制，目標是確保每次 client 連結 TLS server 時，其所連結的 TLS server 要能證明它就是上次這個 client 連結的 TLS server。 |

| | |
|---|---|
| | Daniel Migault 認為這個機制很適合企業內部的網路來實踐。因為這個機制對 client 沒有額外的管理負擔、client 與 server 都只需要實作 TLS 通道的能力即可、這機制與 TLS 憑證可以相互搭配使用、這機制適合 B2B 的通訊使用。<br>第三場演講是 CIRA 的技術長( chief technology officer )Jacques Latour，他講使用 DNSSEC 機制於物聯網裝置的身分管理之挑戰。他提出的概念是使用 DNSSEC 機制實踐雙向 TLS 身分辨識來進行物聯網裝置的身分管理。這裡就需要假設物聯網裝置皆會裝 eSIM 晶片卡，那麼，我們就可以使用 eSIM 裡內建的公私鑰進行簽章行為來支援雙向 TLS 身分辨識。在實務的系統建置上，CIRA 提出在物聯網裝置內使用 eSIM 卡，加上 CIRA 實作的物聯網裝置中介軟體，來進行雙向 TLS 身分辨識及網路連結。在雲端方（即伺服器端）也需要使用 CIRA 建置的安全物聯網登錄服務，這個服務支援伺服器端的中介軟體與 API、CA 及硬體加密器（Hardware Security Module，簡稱 HSM）、DNS 服務及 DNSSEC 機制等。CIRA 的目標是在伺服器端運用 TLSA 與 DNSSEC 機制，在物聯網裝置端運用 eSIM 及 TLS 身分辨識機制，來打造出可管理物聯網裝置身分的整個系統架構。<br>在 Tech Day (1 of 2)這場會議中，Dr. Eberhard Lisse 先做了一個開場介紹。第一場演講是歐盟（European Union）的 Jordi Iparraguirre 報告了一個歐盟的 EURid 所開發的防止在網際網路上設置網站來進行詐騙的偵測與減少損害機制。這個機制檢查網站設立者的註冊資料（WHOIS 資料），來進一步判斷這個網站設立者是否有問題，若有疑慮，就將所發現的資訊轉給其他有權力進行進一步調查的機構，請它們接手處理。這個機制使用四個步驟：避免/過濾（Prevention）、偵測（Detection）、檢查（Check）、溝通分享（Communication）。<br>在每個步驟使用的技術或做法是：(1)導入歐盟開發的 APEWS 黑名單系統來進行初步的網站過濾，這個系統使用大數據分析方法建立過濾模型，且定期進行模型更新。(2)對看來正常的網站網域名稱（Domain Name），使用後委託檢查機制（Post-Delegation Check） |

| | |
|---|---|
| | 來進行偵測，看這個網站是否有異常紀錄或時常被更換 Domain Name。(3)使用人工（EURid 裡的法律人員）再度檢查認為可疑的案件，這裡運用金融界常用的 Know Your Customer 做法。(4)分享可疑的 Domain Name 給其他國際機構或組織，例如：EUROPOL、FOD Economy、Global Cyber Alliance、eCommerce Foundation 等。<br>第二場是 SIDN 實驗室的主任 Cristian Hesselman 介紹一個新的清除分散式阻斷攻擊的架構，叫做 DDoS Clearing House for Europe。這個架構的主要概念是當一個服務提供者的網路被 DDoS 攻擊了，那麼，將可以即時蒐集這次 DDoS 攻擊的特徵數值，形成其攻擊模式的指紋（Fingerprint）資料，這個資料將傳至 Clearing House 的伺服器並分享給其他還沒被攻擊的服務提供者，這些服務提供者就可以更新它們既有的防護機制的資料，事先認識這種新模式的 DDoS 攻擊，進而提早預防。這個架構中，在 Clearing House 的伺服器上，有開發多個服務來協助達成攻擊模式的指紋的分析、呈現、轉檔、分享。每個服務目前是由不同的研發團隊負責，進度也不一，這些服務包含：API Threat Intel Platform、MISP Exporter、IP Address Analyzer、DDoS Visualizer。<br>另外，這個架構也需要在服務提供者端裝設一些元件與服務：Dissector、DDoS Tool Analyzer。這是一個仍在進行的計畫，由歐盟 CONCORDIA 計畫及荷蘭 Anti-DDoS-Coalitie 聯盟支持。第三場是 Internet Systems Consortium 的 DNS operations director, Ray Bellis 來介紹 ISC 所開發的一個互動式資料視覺化呈現系統，叫做 Root System Visualiser。這個系統是可視全球的 DNS root systems 的運作情形，可以放大或縮小要觀察的區域，經由視覺化呈現的資料，可以知道哪個區域的哪個 root system 目前回應的延遲時間，藉以判斷這裡的 root system 是否需要進一步檢視。 |

| | |
|---|---|
| 會議心得 | 這次參與的兩個會議，大約每個會議都有 150~160 個人左右參加。但是因為是線上的虛擬會議，參加者無法在會議中，私下交換意見或認識新朋友。ICANN 的會議內容都十分緊湊，一個小時內安排 3-4 場次的題目討論或技術報告。每個場次的報告都相對簡短，與會者若沒有相關的知識與技術背景，很難立刻融入議題的情境並參與討論或發問。每個會議都有主持人，會精確地控制時間，不讓會議時間拖延，因為每個會議之間幾乎沒有甚麼時間換場。我深深地感受到要在 ICANN 有一定影響力，必須要長期投入，與裡面主要的參與者熟識，才能掌握 ICANN 組織的脈動。我看到所參與的會議場次裡面的主持人與每個講員都很熟識。 |
| 與本計畫關聯 | 本次參與的兩場會議中，與本計畫有關聯性的演講或報告如下：<br>(1) DNSSEC and Security Workshop (1 of 2)的第三場演講，CIRA 的技術長（chief technology officer）Jacques Latour 討論使用 DNSSEC 機制於物聯網裝置的身分管理之挑戰。他提出的概念是使用 DNSSEC 機制實踐雙向 TLS 身分辨識來進行物聯網裝置的身分管理。這裡就需要假設物聯網裝置皆會裝 eSIM 晶片卡，加上 CIRA 實作的物聯網裝置中介軟體，來進行雙向 TLS 身分辨識及網路連結。在雲端方（即伺服器端）也需要使用 CIRA 建置的安全物聯網登錄服務，這個服務支援伺服器端的中介軟體與 API、CA 及硬體加密器（Hardware Security Module，簡稱 HSM）、DNS 服務及 DNSSEC 機制等。CIRA 的目標是在伺服器端運用 TLSA 與 DNSSEC 機制，在物聯網裝置端運用 eSIM 及 TLS 身分辨識機制，來打造出可管理物聯網裝置身分的整個系統架構。<br>(2) 在 Tech Day (1 of 2)的第一場演講，歐盟（European Union）的 Jordi Iparraguirre 報告了一個歐盟的 EURid 所開發的防止在網際網路上設置網站來進行詐騙的偵測與減少損害機制。這個機制使用四個步驟：避免/過濾（Prevention）、偵測（Detection）、檢查（Check）、溝通分享（Communication）。在每個步驟使用的技術或做法是：(1)導入歐盟開發的 APEWS 黑名單系統來進行初步的網站過濾，這個系統使用大數據分析方法建立過濾模型，且定期進行模型更新。(2)對看來正常的網站網域名稱（Domain Name），使用後委託 |

| | |
|---|---|
| | 檢查機制（Post-Delegation Check）來進行偵測，看這個網站是否有異常紀錄或時常被更換 Domain Name。(3)使用人工（EURid 裡的法律人員）再度檢查認為可疑的案件，這裡運用金融界常用的 Know Your Customer 做法。(4)分享可疑的 Domain Name 給其他國際機構或組織，例如：EUROPOL、FOD Economy、Global Cyber Alliance、eCommerce Foundation 等。 |
| 回饋 | 本次參與的兩場會議中，我認為本國政府可以借鏡的是思考如何結合 DNS 系統來預防或減少 DDoS 攻擊的損害。這可以參考 SIDN 實驗室的主任 Cristian Hesselman 提出的這個新的清除分散式阻斷攻擊的架構，叫做 DDoS Clearing House for Europe。<br>這個架構是仍在進行的計畫，由歐盟 CONCORDIA 計畫及荷蘭 Anti-DDoS-Coalitie 聯盟支持。我國可以藉由參與這類計畫增加能見度並結識各國相關組織的人才。 |
| 建議 | 個人認為研究團隊未來參與國際會議安排或規劃時，應思考長遠的戰略布局，多年期的支持計畫與確認一批可長期參與特定國際相關會議的人才，是不可少的。建議思考長期參與的人才應有政府部門的常任事務官、學界的學者、財團法人形式的研究機構的專業人員，以形成長期合作相互支援的團隊。這樣，在設定國際參與的議題主軸時，比較能抓住長期努力的議題方向，使我們認識國際組織內的成員們、培養良好互動並了解國際間真正關注的議題等方面能有持續性。如此，我們若提出議案，就比較能合乎國際朋友們的期待與受到重視，議案的能見度與成功性才會大幅增加。 |

**(二) 網域名稱系統安全擴充和安全性研討會 2/2(DNSSEC and Security Workshop 2 of 2)**

| 日期 | 6/14(一) | 參與會議場次 | ICANN71 |
|---|---|---|---|
| 會議主題 | DNSSEC and Security Workshop (2 of 2)<br>網域名稱系統安全擴充和安全性研討會（2-2） | | |
| 會議交流 | 因 COVID-19 疫情影響，ICANN71 採線上會議舉辦形式，會議講題安排緊湊且圍繞 DNSSEC Provisioning Automation 主軸，與本計畫關聯性較低，因此並無針對主題發言，亦無法與與會者交流。 | | |

| | |
|---|---|
| 會議過程 | DNSSEC and Security Workshop (2 of 2)會議議程：<br>DNSSEC and Security Workshop (2 of 2)的第一場次主持人為 Steve Crocker，其為 IETF RFC 1 的作者，這次會議的主軸是 DNSSEC Provisioning Automation（DNSSEC 配置自動化），在簡單的開場後即開始第一個講題 DNSSEC Provisioning Automation Overview，該主題自 2020 年的 ICANN67 至 ICANN71 舉辦了 5 場 Meeting，其主要為了解決的議題有二：<br>1. Automation of DS updates：在週期性的金鑰更新中，child's zone 需要新的 parent DS record，因此受理註冊機構（registrar）需要存取 parent，在受理註冊機構（registrar）提供 signed DNS service 的情形下不會有問題，但第三方 DNS provider 無法存取註冊管理機構（registry）。<br>2. Multiple DNS Providers：每個 DNS provider 透過其擁有的金鑰（RFC 8901 Model 2）進行簽章，其需包含其他 provider 的 ZSKs，但目前並無定義共享金鑰的做法，因此需要 Multi-DNS Provider Coordination （Multi-Signer）。<br>第二個講題為 RIPE NCC 的 Ondřej Caletka 所發表關於 CDS records 掃描專案的成果，此專案是為了支援資料庫中 DS records 的自動化，並提出一個 private DNS provider 的解決方案。第三個講題 The State of DNSSEC Provisioning Automation 為 University of Twente 的學士專題成果，其由 Software Support、TLD Support 及 Domain Support 三個面向調查目前的現況。第四個講題是由 DNS-Labs - The Swedish Internet Foundation 發表其單位對於 Bind、Knot 及 PowerDNS 等 Name Server Software 對於 Multi-Signer 的支援現況及相關測試。第五個講題由 Internet Systems Consortium 發表 Bind 對於 Multi-Signer 及 DNS Update 的支援現況，第六個講題則是由 PowerDNS 發表 PowerDNS 對於 Multi-Signer 的支援現況。<br>第二場次的主持人為 CIRA CTO Jacques Latour，其亦為 ICANN SSAC 成員，第一個講題是由 ICANN Technical Engagement 的 Vice President - Adiel Akplogan 發表 ICANN KINDNS（Knowledge-sharing and Instantiating Norms for DNS and Naming Security）專案的發展與 |

| | |
|---|---|
| | 未來規劃。第二個講題是由 SWITCH 的 Michael Hausding 介紹 DNS resilience 專案。 |
| 會議心得 | DNSSEC and Security Workshop 安排的主題皆是實務導向，此次參與的場次 DNSSEC and Security Workshop (2 of 2)主要是為了解決 DNSSEC 中 Automation of DS updates 與 Multiple DNS Providers 的相關議題，透過 ICANN 的主導，以及許多產業及學術團體的專案投入，並且主要的 DNS Software 組織也參與其中，能夠有效的產出解決方案並且驗證。 |
| 與本計畫關聯 | 本會議場次主要討論議題與發表成果圍繞 DNSSEC 中的 DS update 與 Multi-Signer，與本計畫目標較無直接關聯，ICANN KINDNS（Knowledge-sharing and Instantiating Norms for DNS and Naming Security）專案目前已成立暫時性 Wiki page（https://community.icann.org/pages/viewpage.action?pageId=160728236），可提供本計畫在 DNS 安全性方面的參考資料。 |
| 回饋 | 本會議場次主要討論議題與發表成果圍繞 DNSSEC 中的 DS update 與 Multi-Signer，與本計畫目標較無直接關聯。其中由 SWITCH (.ch 及.li 的 registry)的 Michael Hausding 介紹 DNS resilience 專案所規劃的 DNSSEC Measurements RFP 可以作為我國 DNSSEC 推展相關專案的參考。 |

**(三) 技術日(Tech Day)**

| 日期 | 6/14(一) | 參與會議場次 | ICANN71 |
|---|---|---|---|
| 會議主題 | Tech Day (2 of 2)<br>技術日（2-2） | | |
| 會議交流 | 因 COVID-19 疫情影響，ICANN71 採線上會議舉辦形式，會議講題安排與本計畫關聯性較低，因此並無針對主題發言，亦無法與與會者交流。 | | |
| 會議過程 | Tech Day (2 of 2)第一個講題是由 PLISK 的 CEO Jothan FRAKES 所發表的 PUBLIC SUFFIX LIST，其介紹 PSL 專案（https://github.com/publicsuffix/list）主要提供應用程式在處理域名上可以利用的工具，PSL 是由 ICANN/IANA 的頂級域名（Top-level | | |

| | |
|---|---|
| | Domain，簡稱 TLD）清單及私人部門（Private section）所提供的清單所組成。<br>第二個講題是由 Donuts 公司的 Howard Eland 所發表的 rm -f SHA-1: Algorithm Rolls En Masse，ICANN 在 2020 年已呼籲在網域名稱系統安全擴充（Domain Name System Security Extensions，簡稱 DNSSEC）中停用 SHA-1 雜湊函式演算法，因其具有安全性弱點，該講題展示使用 SHA-256 來進行規模測試的一些成果。 |
| 會議心得 | 本場會議安排兩個講題，PUBLIC SUFFIX LIST 應用在域名的處理上，以及 DNSSEC 中 SHA-1 的轉置（migration）經驗，與本計畫目標無直接關聯性，較適合研發工程師與維運工程師參與學習。 |
| 與本計畫關聯 | 本場會議安排講題與本計畫目標無直接關聯性，但可作為 DNSSEC 方面安全性基礎的參考。 |
| 建議 | ICANN Tech Day 的主題亦可多鼓勵或安排研發工程師參與。 |

**(四) 全體會議：監管發展對 ICANN 政策主題的影響(Plenary Session: Impact of Regulatory Developments on ICANN Policy Topics)**

| 日期 | 6/14(一) | 參與會議場次 | ICANN71 |
|---|---|---|---|
| 會議主題 | Plenary Session: Impact of Regulatory Developments on ICANN Policy Topics<br>全體會議：監管發展對 ICANN 政策主題的影響 | | |
| 會議交流 | 本次會議為 ICANN71 開幕第一天的大會討論活動，主要由政府官員對多方利害關係人報告近期與網際網路相關的政策與法規，開放各社群提問與討論政府政策及法規之內容以及對於網際網路社群之影響等等。會中係由歐盟官員報告歐盟的近期法規發展與網域名稱系統（Domain Name System，簡稱 DNS）的關係，以及《布達佩斯網路犯罪公約》（Budapest Convention on Cybercrime）的進度等等，與會者非常多，台灣亦有其他人士參與。 | | |

| | |
|---|---|
| 會議過程 | • 會議進行首先由 Olivier Bringer(Head of Unit at the European Commission)說明歐洲近期法規動態，主要是歐盟“Proposal for a Directive on measures for a high common level of cybersecurity across the Union （NIS2）”以及“Proposal for a Regulation on a Single Market For Digital Services”數位服務法（Digital Services Act，簡稱 DSA）。接者由 Alexander Seger （Head of Cybercrime Division, Council of Europe）介紹《布達佩斯網路犯罪公約》（Budapest Convention on Cybercrime）之最新發展。之後進行專家討論是否 ICANN 應該要回應這些政府的舉動，多方利害關係人應如何考量政府法規變遷，從過去的歷史來看，ICANN 對於類似之議題應如何因應。最後開放社群討論。<br>• Olivier Bringer 報告歐盟 NIS2 草案核心，歐盟希望各成員國均能加入網路安全（Cybersecurity）的協防架構中，各成員國應要求其境內管理網域名稱系統（Domain Name System，簡稱 DNS）之機構，致力於維護其註冊資料之正確，紀錄 DNS 登記人之聯絡資訊，公布非屬個人資料之資訊，如遇正當請求時應立刻提供相關資訊。而數位服務法（Digital Services Act，簡稱 DSA）草案則是依照數位業者在產業鏈所扮演之不同角色以及經營規模，賦予不同之保護消費者之義務。例如非常大規模之平台，即負有最多之保護消費者之義務。<br>• Alexander Seger 報告《布達佩斯網路犯罪公約》（Budapest Convention on Cybercrime）之最新發展，其中定義網路犯罪（Cybercrime）之內容以及規模，各國防治網路犯罪（Cybercrime）應採取之措施，其中第 83 條要求各國應訂定法律，要求網域名稱登記機構有協助執法機關調查並提供資料之義務。<br>• 專家討論時，(i) Fred Baker 表示根伺服器（root server）看起來被包入 NIS2 而且被認定為係 registrar/registry 的一種，但其實本質並不相同，無法依照 NIS2 要求運作。(ii) Philippe Fouquart，GNSO 代表認為由於這些國際條約還需要內國政策制定，最終後果不明，雖然相關之手段在 WHOIS 資料庫（database）Phase |

| | |
|---|---|
| | 1 Phase 2 都已經討論過，大家都很熟悉，未來待觀察。(iii) Matthias Hudobnik，At-large 代表認為，為代表終端使用者（end-user）之利益，教育使用者非常重要，GDPR 的發展是很好的模式。(iv)Alejandra Reynoso，ccNSO 代表認為 ccNSO 社群內代表相當多不同之利益，統整不易，需要多方溝通，ccNSO 的做法就是示範實例給社群成員，以便溝通整合意見。<br>• 社群討論時，大家仍十分專注於因應 GDPR 之要求，WHOIS 資料庫（database）目前不提供各界查詢註冊人之個人資訊，依照 EDPD Phase 1 以及 Phase 2 之建議未來將為執法單位以及智慧財產權權利人提供查詢管道，但進度未明，是以各國執法單位如何向 DNS registrar/registry 取得註冊人資料，歐盟的三個公約草案產生之交互作用，也有詢問 ICANN 如何處理各國規範不同之狀況。 |
| 會議心得 | 由於".tw"的域名登記服務是由台灣向全球提供的，歐盟境內之人士也有可能登記".tw"的域名，所以本人十分好奇 TWNIC 會不會被認定是數位服務法（Digital Services Act，簡稱 DSA）裡面的中介產業（intermediary），Oliver Bringer 沒有正面回答，但是表示如果有對 EU 提供服務時，即有可能。<br>另與會者發言諸多意旨也提及 ICANN 除了符合歐盟法規以外，對於世界上其他國家的 WHOIS 資料庫（database）如何管理如何交代？本人也提出類似問題，與會專家反而回答歐盟模式已經是各國所接受之模式，沒有這種顧慮。綜合觀察全場討論之狀況，現場十分熱絡，各自依照所代表之利害關係發言，不過一談到實際之執行措施，通常都會以應建立工作小組廣徵各利害關係人之意見為答覆，具有 ICANN 獨特之模式與思維，是以相較於其他模式，決策與執行之時程必定耗時較長。 |

| | |
|---|---|
| 與本計畫關聯 | 本次討論主要係討論歐盟新條約草案對於 ICANN 社群之影響以及 ICANN 社群應有的應對，由於歐盟此次草案有兩項專注於打擊網路犯罪，希望 ICANN 旗下的域名發放與登記單位能夠配合執法單位提供可疑違法人士之個人資料，雖然與電信號碼相關之主題較為無關，但確是網際網路界未來重要的國際趨勢，ICANN 對於歐盟的各草案之意見以及未來之因應措施，也會影響整個 DNS 生態系，是以應列為重點觀察之國際趨勢。 |
| 回饋 | 我國與歐盟交流密切之 NIS2、DSA、Budapest Convention on Cybercrime 預計均會有域外效力，應密切觀察相關立法進度以為國內企業及早因應。NIS2、DSA、Budapest Convention on Cybercrime 對於 ICANN 旗下的域名發放與登記單位就註冊人之資料搜集與利用等，未來將有具體義務誕生，應持續觀察此類議題。 |
| 建議 | 相關議題對國內業者未來可能有重要影響，且為重要國際趨勢，應持續觀察相關議題。 |

**(五) SSAC 公開會議(SSAC Public Meeting)**

| | | | |
|---|---|---|---|
| 日期 | 6/17(四) | 參與會議場次 | ICANN71 |
| 會議主題 | SSAC Public Meeting<br>SSAC 公開會議 | | |
| 會議交流 | 本次會議為 Security and Stability Advisory Committee（SSAC）對大眾的公開會議，由各工作小組向社群報告 SSAC 的工作進度以及近況更新。 | | |
| 會議過程 | ● 會議進行首先由主席 Rod Rasmussen 就 SSAC 之組成、工作任務等進行簡介。<br>● Jeff Bedser 負責就 SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS 進行進度報告，該報告之目的為降低使用者受 DNS Abuse 之損害並就互通性（interoperable）的處理方式提出建議，目前建議應該由各方利害關係人協力建立一個通報系統，要求 registry/registrar/registrar reseller/hosting provider 合作於時限內進行通報（各自有 24 小時通報期限，96 小時完成），最後建議另 | | |

| | |
|---|---|
| | 外成立一個可信賴的第三方機構，作為服務多方利害關係人的一般濫用回應協調員（Common Abuse Response Facilitator）。<br>● James Galvin 等報告域名衝突分析計畫 （Name Collision Analysis Project，簡稱 NCAP），說明目前的進度、預計建立的處理架構以及未來之資訊敏感性分析等等。<br>● 介紹 SSAC 下設的特別工作組（working parties）一共 11 個。<br>● 介紹 SSAC 需要的技能（skills）以招募新成員。 |
| 會議心得 | 有關於 DNS Abuse 通報的 Common Abuse Response Facilitator，如現在開始成立另外一個獨立第三方公正機構擔任此任務恐曠日費時，是以本人於會中提議應由 ICANN 本身勇於任事承擔重任，但被 SSAC 嚴詞拒絕，表示 ICANN 已經承擔太多任務，組織龐大，不適合再承擔多餘任務。由於 ICANN 多方利害關係人作成決定耗時冗長，實際執行亦勢必曠日費時，如此 DNS Abuse 通報系統恐怕不是短期可以成就的，未來實際執行時是否可以追上 Abused 端的科技發展，亦有待觀察。 |
| 回饋 | SAC115 之提議受到利害關係人普遍關注，所提出之處理模式以及建議較為具體可行，如未來定案後果真成立獨立第三方公正機構擔任 Common Abuse Response Facilitator，預計將為重要之防止利用網域名稱侵權之組織，我國應密切觀察以及適時參與。 |
| 建議 | 本次 SSAC 討論之議題，雖與電信號碼並不直接相關，但由於防止 DNS Abuse 為網際網路重要議題，應持續關注。 |

**(六) GNSO - CPH DNS 濫用工作小組社群更新會議(GNSO - CPH DNS Abuse Work Group Community Update)**

| 日期 | 6/16(三) | 參與會議場次 | ICANN71 |
|---|---|---|---|
| 會議主題 | GNSO - CPH DNS Abuse Work Group Community Update<br>GNSO - CPH DNS 濫用工作小組社群更新會議 | | |
| 會議交流 | 本次會議為 GNSO 關於 CPH（Contracted Parties House）DNS Abuse Work Group 的進度報告，由工作小組向社群報告 CPH DNS Abuse Work Group 的工作進度以及近況更新。 | | |

| | |
|---|---|
| 會議過程 | 會議進行首先由主席 James Galvin Donuts 開場，工作小組報告 CPH DNS Abuse Work Group 最新工作進度，最後開放社群提問。<br>● CPH 對於 DNS Abuse 的定義包含五種對於 DNS 有害的行為：惡意軟體（malware）、殭屍網路（botnets）、網路釣魚（phishing）、網址嫁接（pharming）以及垃圾郵件（spam）（現於作為其他形式 abuse 之傳送系統時之 spam）。<br>● Registries Stakeholder Group 工作進度報告：(1) 對於域名濫用報告（Domain Abuse Activity Reporting，簡稱 DAAR）建議增加受理註冊機構（registrars）；(2)提出“Registry Operator Available Actions”清單，以便註冊管理機構（registry）在遇到 DNS Abuse 時有所依循，其中列出註冊管理機構（Registry Operator）可以採取的技術措施（暫緩、移轉或鎖定）、區別惡意登記域名以及被侵入之域名等。<br>● Public Safety Working Group 工作進度報告：提出對於 Domain Generating Algorithms（DGAs）相關之 Malware 以及 Botnets 之對策，表示工作小組已經與 ICANN 達成初步共識，對於會不斷利用軟體程式大量自動申請登記網域名稱的行為，registry 以及 registrar 可以一次性取得授權處理此種經自動申請註冊之域名，而無需一一取得授權。<br>● Registries Stakeholder Group DNS Abuse Work Group 與 Registrars Stakeholder Group DNS Abuse Work Group 共同報告對於 Trusted Notifiers 之進度，各方均認為應對下列有更明確之指標：(1) 如何成為 Trusted Notifier、(2) Trusted Notifier 應做之盡職調查；(3) 如何作成紀錄？ (4)對於註冊人之保障。<br>● CTTRT Recommendations Working Group：新進成立之工作小組，對於 DNS Abuse 提出建議。<br>● IDN Homoglyph Attacks Working Group：對於國際化域名（Internationalized Domain Name，簡稱 IDN）相關之 DNS Abuse 作出建議。<br>● Registrars Stakeholder Group 介紹各個已經出版的報告以及正在草擬之報告。 |

| | |
|---|---|
| 會議心得 | 社群討論時提到幾個可以處理 DNS Abuse 的作法，其中一個是修改 registry 與 registrar 之合約，以便要求 registrar 針對 DNS Abuse 就 DAAR 進行比對，顯示 ICANN 社群處理問題時，除了從技術面分析可行性外，亦涵蓋利用私人約定之契約來處理各項議題與建立規範。若各個 registry 以及 registrar 針對 DNS Abuse 簽訂相同之契約條文，透過私契約的利用，即可達到統一處理模式與規範之目的，也不失為一種解決方案。 |
| 與本計畫關聯 | DNS Abuse 工作小組之目標為消除 DNS Abuse，與本計畫之電信號碼相關議題較無關聯，但 DNS Abuse 之防範為重要國際趨勢，值得觀察。 |
| 回饋 | 會議主要針對 Contracted Parties，亦即 registrars 以及 registries 對於 DNS Abuse 議題應如何互相分工合作嚇阻以及處理，在國內主要涉及 TWNIC 以及其授權域名註冊商未來之分工、權利義務等等議題，似與本研究計畫主題較不相關。但 DNS Abuse 之防範為重要國際趨勢，值得觀察。 |
| 建議 | 本議題似與本研究計畫主題較不相關。惟由於 DNS Abuse 是近年來 ICANN 處理之重大議題之一，如果要持續參與 ICANN 活動，應該對於此議題 ICANN 的動向加以了解，值得持續觀察。 |

# 參、第二場國際會議：ICANN72

## 一、ICANN 72 會議簡介及議程

本次會議係 ICANN「年度大會」(Annual General Meeting，簡稱「AGM」)，於本（2021）年 10 月 25 日至 10 月 28 日以「全球遠端參與形式」舉行，議程共有 4 天。

| 臺灣時間 | 會議名稱 | 效益分析 |
|---|---|---|
| 15, Oct 04:00-05:00 | Introducing the DNS Security Facilitation - Technical Study Group (DSFI-TSG) | 藉由參加該會議，了解包括 DNS 可用性、利用 DNS 的安全威脅、DNS 關鍵基礎建設中的信任憑證及加密等安全議題，作為我國擘劃 DNS 及網路安全政策之參考。 |
| 26, Oct 00:00-01:00 01:30-03:00 03:30-05:00 | Tech Day（1 of 3） | 透過於會議中發表 DNS 及安全性等相關技術成果及與各領域專家討論技術性議題，可獲悉與網域名稱產業（註冊業務、DNS、網路安全等）相關的技術知識。 |
| | Tech Day（2 of 3） | |
| | Tech Day（3 of 3） | |
| 27, Oct 03:30-05:00 | SSAC Public Meeting | SSAC Public Meeting 是對安全與穩定諮詢委員會 SSAC 工作的公開介紹，主要內容包含 SSAC 概述、SSAC 近期活動及 SSAC 即將展開的工作等，透過參加該會議，對於 ICANN SSAC 的組織運作可以有更深的了解，幫助擴展組織內人際脈絡。。 |
| 27, Oct 07:30-08:30 | Joint Meeting: ICANN Board and SSAC | 該會議由 ICANN Board 和 SSAC 針對相關議題共同討論，希冀透過參與該聯合會議，了解 ICANN Board 和 SSAC 的共同戰略計畫及目標。 |
| 28, Oct 03:30-05:00 | DNSSEC and Security Workshop（1 of 3） | 希望透過會議中的分享，了解 DNS 安全及資安相關議題與政策發展方向，以作為我國擘劃 DNS 及網路安全政策之參考。 |

## 二、ICANN 72 會議紀錄

### (一) 網域名稱系統安全擴充和安全性研討會 3/3 及技術日及 ICANN 董事會與 SSAC 聯席會議(DNSSEC and Security Workshop 3of 3 and Tech Day Joint Meeting: ICANN Board and SSAC)

| | | | |
|---|---|---|---|
| 日期 | 10/26(二)、10/27(三)、<br>10/28(四) | 參與會議場次 | ICANN72 |
| 會議主題 | DNSSEC and Security Workshop 3of 3 and Tech Day and Joint Meeting: ICANN Board and SSAC | | |
| 會議交流 | 在 Tech Day (3 of 3)這場會議中，由烏克蘭的 Dmitry Kohmanyuk 主講 ccTLD Infrastructure DIY 這個題目，他曾是烏克蘭的 ccTLD(country code top-level domain)經理，目前是 Hostmaster Ltd.之共同創辦人及 Intuix LLC 的合夥人，烏克蘭 ccTLD 的 administrative contact。由於 Dmitry Kohmanyuk 本身具管理烏克蘭的國家頂級域名(ccTLD)經驗，故透過演講分享關於動手建立一個國家頂級域名所需之基礎建設環境，說明需要準備事項內容，例如：給頂級域名及你自己本身域名使用之 DNS 服務、DNSSEC 的簽章與金鑰管理、WHOIS 與 RDAP 服務、給註冊者使用的 EPP 服務、email 或其他聯絡他人的工具、資料中心的空間、網際網路連線、軟體開發測試與維護能力、系統及網路行政管理與維運能力、會計與律師等等。然當考量上述準備事項是由自己著手辦理時，會發現耗費極大時間成本，或是根本沒有足夠能力做。故須考量將工作外包。然需注意外包之內容不應涵蓋商業或財務維運事務。討論外包議題，亦需注意成本控制問題，因為新技術的出現，以往合理的某些系統外包，可能已經可用其他方式取代，例如：雲端化或使用自身團隊進行敏捷式開發。注意，若想重建系統，很可能成本會過高。<br>在這個演講後的討論中，許多人有些回饋意見，會議主持人也說 ICANN 很希望看到這類實務的議題與討論，認為這有助於與會者在實踐網際網路的安全、穩定、可相互操作各方面的作業與管理上，能有相互交流的機會。 | | |

| | |
|---|---|
| 會議過程 | 我個人這次參加 ICANN 72 會議，被指派參與三個場次的會議：Tech Day (3 of 3), DNSSEC and Security Workshop (3of 3) and Joint Meeting: ICANN Board and SSAC。在 Tech Day (3 of 3)這場會議中，首先是 Greg Freeman 討論使用 RPKI(Resource Public Key Infrastructure)來增進路由安全的議題，他是 Lumen Technologies 的網路與客戶轉型(Network and Customer Transformation)部門的副總。這個演講使用 Lumen 公司所管轄的網際網路上的自治系統(autonomous system)來進行說明與討論，全球最大的自治系統就是 Lumen 公司所管理。Lumen 公司有超過 450,000 英哩的光纖網路，超過 314,000 個 IP 裝置，每月有超過 25 billion 的通話分鐘數。<br>RPKI 這個技術，主要是用來防止 BGP 路由被惡意劫持，使用此技術可以確認某個特定自治系統中，被授權使用那些 IP 位址前綴(IP prefix)；因此，IP 服務提供者可使用 RPKI 確認宣告的 IP 路由是否正確。然而，RPKI 不能阻止大多數的路由被惡意手段劫持。在部署 RPKI 的經驗中，Lumen 公司學習到幾件事：商業方案需要調整、RPKI 的軟體有瑕疵、軟硬體需要升級、如何實作認證伺服器很重要、要做好與客戶的溝通、其他還包含 RPKI 會增加路由平台的負擔、要發展路由政策(routing policy)、要注意維運與員工訓練、需要相信 Regional Internet Registries (RIRs)。<br>Greg Freeman 認為成功的 RPKI 部署，將會對網際網路社群帶來許多好處，Lumen 公司在成功部署 RPKI 後，許多客戶能拿回被劫持的 IP 位址範圍(IP ranges)。Roy Arends 是 ICANN CTO 辦公室的 Principal Research Scientist，他的講題是 Hyperlocal Root Zone，主要是討論解析器(Resolver)使用在地區域的根轄區(root zone)取得網域解析的資料，而不用根伺服器(root servers)。這個概念是 2003 年 Paul Mockapetris 提出的，於 2004 年由 David Malone 做了進一步的研究。<br>這個概念已經被許多網路服務提供者實作了，所以 Roy Arends 想要進行一下技術分析。他認為 Hyperlocal 這個技術對解析器有多方面的影響。(1)查詢的隱私：這個技術減少了根伺服器蒐集更多由解析器傳來的資訊，因而增強了客戶端(client)的隱私保護；(2) 根轄 |

| | |
|---|---|
| | 區(root zone)的完整性：目前實務上 hyperlocal 技術會伴隨使用 HTTPS/PGP 簽章或 TSIG，這使得此技術有更好的資料完整性；(3)查詢的延遲：hyperlocal 這個技術可以降低查詢延遲的時間，得到更好的流通量(throughput)；(4)減少遙測數值的蒐集：有些值得關注的數值如 v4/v6 的比例、UDP/TCP 的比例等，會無法觀測到；(5)操作的複雜性：這個技術的部署上，仍存在許多要一一解決的實務事項，也就是說，這個技術有其作業上的複雜性。<br>Dmitry Kohmanyuk 主講 ccTLD Infrastructure DIY 這個題目，他目前是烏克蘭 ccTLD 的 administrative contact。由於 Dmitry Kohmanyuk 自己就在管理烏克蘭的國家頂級域名(ccTLD)，他在這場演講就分享自身的經驗，對於如何自己動手建立一個國家頂級域名所需的基礎建設環境，指出需要準備的事項。Dmitry Kohmanyuk 提醒大家要所有事情都自己動手做，可能太花時間，或是根本沒有足夠能力做。所以，就要考慮外包一些工作給別人做。注意最好不要外包你的商業或財務維運事務。當討論到外包，就要注意成本控制問題。因為新技術的出現，以往合理的某些系統外包，可能現在已經可以用其他方式取代，例如：雲端化或使用自身團隊進行敏捷式開發。若想重建系統，要注意很可能成本會過高。<br>在 Joint Meeting: ICANN Board and SSAC 中，討論了三個網際網路治理議題：(1)與歐盟一般資料保護規範(GDPR)有關的議題，討論法人與自然人的註冊資料之異同(面對 GDPR，處理規則是否要不同？)，SSAC 建議要有三個值：Natural, Legal, Unspecified，一開始 Unspecified 這個值將會佔大多數，希望日後註冊者會逐漸修正此值至 Natural(自然人)或 Legal(法人)。有關使用標準化且匿名的電子郵件信箱地址做為唯一連絡人的可能性(指 generic top-level domain 註冊資料中的連絡人資訊)，SSAC 建議暫緩提出實作方法。(2)建立一個早期預警系統(Early Warning System)來警告所有根伺服器系統服務者，如果目前的根區域擴編(Root Zone Scaling)已經太大而會導致正常服務失敗的結果。這個治理議題被 SSAC 否決，認為以目前的環境無法確定能建構有效的系統，做到期望的預警功效。(3)持續增加 gTLD(generic top-level domain)至根名稱空間(root namespace)是 |

| | |
|---|---|
| | ICANN 想要看到的結果嗎？這樣會使網際網路更安全、穩定、可相互操作(interoperable)嗎？在面對增加 gTLD namespace 這事情上，所有系統化的考量(例如：確認、監控並減輕整個 DNS 解析鏈的影響)都清楚且可以做到嗎？<br>此外，惡意使用 DNS(abuse DNS)的事件有增多的趨勢，我們需要在尚未想出解決惡意使用 DNS 的辦法之前，就增加 gTLD namespace，給惡意使用 DNS 的攻擊者更多機會嗎？SSAC 建議 ICANN Board 要多思考所有情況，提供參考教材給新的註冊服務提供者(new registry service providers)，參考 the Name Collision Analysis Project 的結果報告。<br>在 DNSSEC and Security Workshop (3of 3)這場會議中，首先是 IANA Services 的副總，也是 ICANN Public Technical Identifiers 總裁的 Kim Davies，介紹由 Trusted Community Representatives(某些 ICANN 相信的人)之中，挑出幾位成為 Recovery Key Shareholders，並給予每位一把金鑰稱為 Recovery Key。ICANN 使用秘密分享(Secret Sharing)機制，通常是 7 位 Recovery Key Shareholders 中，有 4 位若能到齊，則 4 把 Recovery Keys 可以還原 DNS Root Key Signing Key。這是 ICANN 在遭遇重大事件，需要使用 Root Key Signing Key 時，還原金鑰的機制。這個機制是希望大眾能相信 ICANN 不會也不能自行拿到並使用最重要的 DNS Root Key Signing Key。但這個機制有些重大缺陷是當初未曾想到的。<br>這次的演講就是在分享一個實際案例：十年前分到一把 Recovery Key 的 Dan Kaminsky 突然於 2021 年 4 月去世了，他的家人也不知道他把 Recovery Key 放到哪裡去了。這使得 ICANN 花了許多功夫，經由律師的協助與 Dan Kaminsky 家人的幫忙，才終於由一間在紐約銀行的保險箱裡拿到當初給 Dan Kaminsky 的密封袋，裡面是他負責保管的 Recovery Key。Kim Davies 分享經過這事後，ICANN 做了一些調整，也必須認真思考有沒有其他更好的信任機制來實踐分別保管 Recovery Keys。<br><br>第二場演講是由 SIDN 的 Stefan Ubbink 主講 Disaster Recovery |

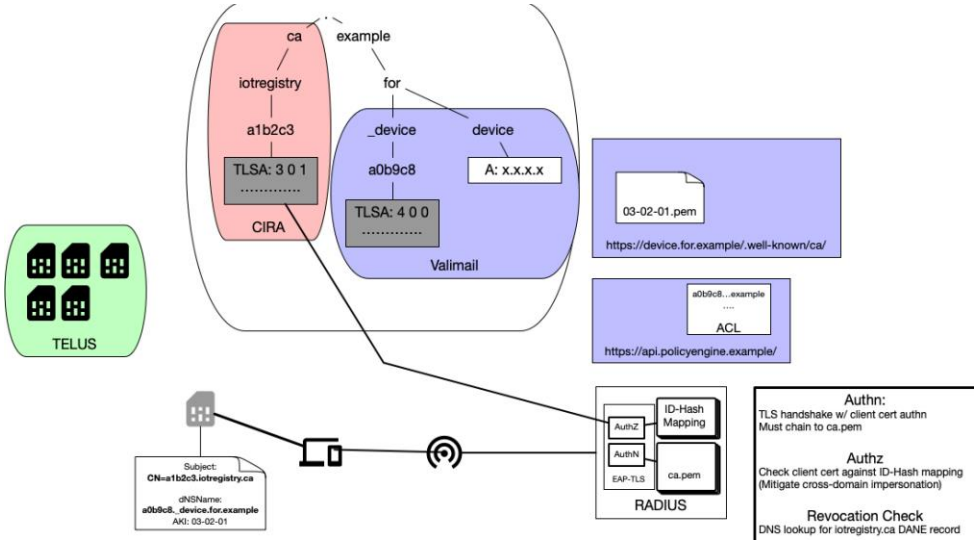
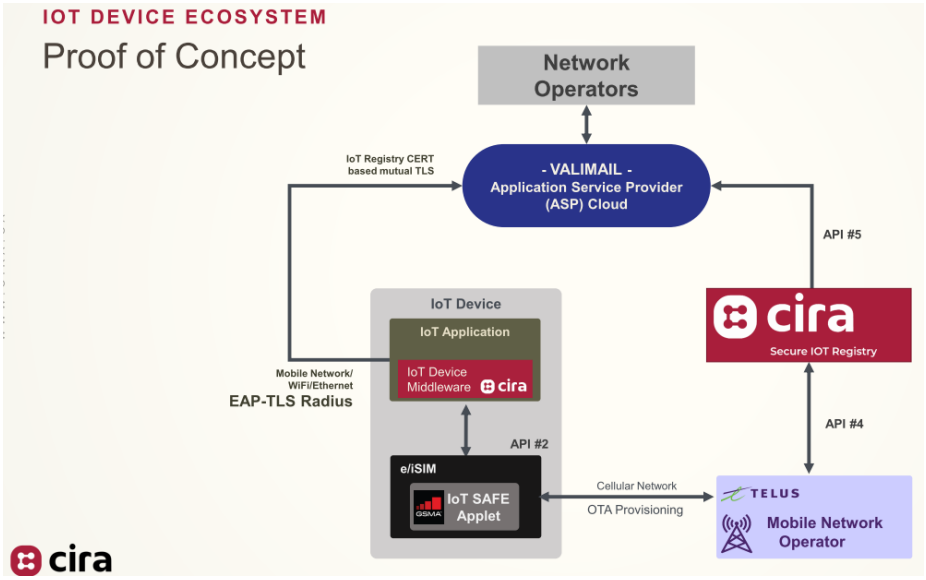
| | |
|---|---|
| | with DNSSEC，這個機制使用 online Key Signing Key (KSK)來代替傳統的 2 台 Hardware Security Module (HSM)的 Disaster Recovery 架構。這個機制可以由自動化的 backup 程序來產生新的 ZSK(zone signing key)，比起傳統的人工作業要花約 7 個工作天才能讓一個 zone 的 DNS 服務恢復，新機制會快很多，但需要規劃如何進行自動化 backup。 |
| 會議心得 | 這次參與的幾個場次的會議，可以看出 ICANN 的基本性質是在於關注對網際網路的治理或管理方面的事情，由這些管理面向所衍生出的實務技術交流與探討，很多時候是實際個案的經驗分享與討論，也會是 ICANN 有興趣的事物。或許，臺灣有網際網路經營管理的組織(例如：TWNIC)或公司(例如：中華電信)，可以嘗試至 ICANN 會議報告實務的網際網路的治理方面的經驗，並提出要討論的事項。這可以增加我國在 ICANN 的能見度。 |
| 與本計畫關聯 | 本次參與的三場會議都是討論 DNS 的維運或是金鑰管理相關議題，並無直接與物聯網裝置的命名、名稱空間、裝置或服務找尋等議題相關聯。 |
| 回饋 | 本次參與的三場會議中，我認為本國政府可以借鏡的是像 ICANN 組織學習思考要如何與國際接軌，治理網際網路。例如：這次會議中，ICANN Board and SSAC(The Security and Stability Advisory Committee)的聯合會議場次，就討論了幾個有趣且重要的網際網路治理議題，我國相關單位與組織(例如：NCC、TWNIC)也應注意其未來發展：(1)與歐盟一般資料保護規範(GDPR)有關的議題，討論法人與自然人的註冊資料之異同(面對 GDPR，處理規則是否要不同？)及使用標準化且匿名的電子郵件信箱地址做為唯一連絡人的可能性(指 generic top-level domain 註冊資料中的連絡人資訊)。(2)建立一個早期預警系統(Early Warning System)來警告所有根伺服器系統服務者，如果目前的根區域擴編(Root Zone Scaling)已經太大而會導致正常服務失敗的結果。(3)持續增加 gTLD(generic top-level domain)至根名稱空間(root namespace)是 ICANN 想要看到的結果嗎？這樣會使網際網路更安全、穩定、可相互操作(interoperable)嗎？在面對增加 gTLD namespace 這事情上，所有系統化的考量(例 |

| | |
|---|---|
| | 如：確認、監控並減輕整個 DNS 解析鏈的影響)都清楚且可以做到嗎？此外，惡意使用 DNS(abuse DNS)的事件有增多的趨勢，我們需要在尚未想出解決惡意使用 DNS 的辦法之前，就增加 gTLD namespace，給惡意使用 DNS 的攻擊者更多機會嗎？ |
| 建議 | 個人認為 ICANN 主要是關注對網際網路的治理或管理方面的事情，建議將來的延續計畫可以考慮邀請在網際網路的治理方面有實際經驗的組織，派員參與 ICANN 去分享網際網路管理經驗並提出相關需要討論的議題，以形成長期合作相互支援的團隊。如此，我們也可就網際網路治理方面提出議案，比較能合乎 ICANN 的設立目的並獲得重視，議案的能見度與成功性才會大幅增加。 |

**(二)網域名稱系統安全擴充和安全性研討會 1/3 (DNSSEC and Security Workshop 1of 3 )**

| 日期 | 10/28(四) | 參與會議場次 | ICANN72 |
|---|---|---|---|
| 會議主題 | DNSSEC and Security Workshop (1 of 3) | | |
| 會議交流 | 在 Q&A 的階段，本計畫顧問陳麒元透過 QA Pod 發問:<br>：CHI-YUAN CHEN: Could the IoT device be equipped only with the cellular network interface and eSIM?<br>：JASON BLAKEY: Yeah, it certainly could. Right now we're using a Cat-M1 network to get our provisioning data. And also in a previous POC, we were using Cat-M1 for data as well. And if the eSIM supports IoT SAFE, it should be all happy about it. So, yes.<br>：JACQUES LATOUR: I think you did a presentation yesterday or the day before on identity management. So maybe you can reach out—there are synergies there—and integrate in a little bit of both together.<br>CIRA 是透過 eSIM 和 Cellular 來進行公私鑰憑證的取得，再透過 DANE 架構來進行 Universal Namespace 的 IoT 註冊，因此網路的部分並不是特別需要限定，主持人也提到我們在昨天也有展示 PoC，也許我們可以互相交流或整合。<br>第四個講題 Verisign: ZONEMED 由 Duane Wessels 所發表，其概念 | | |

| | |
|---|---|
| | 是希望再 DNS Zone 中嵌入 Zone Digest 成為 Zone resource record，由 zone publisher 計算產生，zone recipient 負責驗證。 |
| 會議過程 | DNSSEC and Security Workshop (1 of 3)共安排有四個講題，如下:<br><br>**DNSSEC and Security Workshop – Part 1 12:30 – 14:00 Local Seattle (19:30 – 21:00 UTC)**<br>**1. 12:30 – 12:45 (19:30 – 19:45 UTC) – Presentation: Dan York, *DNSSEC Workshop Introduction, Program, Deployment Around the World – Counts, Counts, Counts***<br>**Moderator: Jacques Latour**<br>**2. 12:45 – 13:05 (19:45 – 20:05 UTC) – Mark Elkins, DNS/ZACR: DNSSEC, automation observations**<br>**3. 13:05 – 13:30 (20:05 – 20:30 UTC) – Ash Wilson, Valimail, Jason Blakey, CIRA: ZERO-Touch Universal IoT Device Identity**<br>**4. 13:30 – 13:50 (20:30 – 20:50 UTC) – Duane Wessels, Verisign: ZONEMED**<br>**5. 13:50 – 14:00 (20:50 – 21:00 UTC) – Q&A**<br><br>1. DNSSEC Workshop Introduction, Program, Deployment Around the World – Counts, Counts, Counts 由 Dan York 開始先介紹 DNSSEC Workshop 的成員，並說明 DNSSEC Workshop 是由 ICANN SSAC 及 Internet Society 所支持。接著 Dan York 展示目前國際上關於 DNSSEC、DANE 及 RPKI 的發展現況。<br>2. DNS/ZACR: DNSSEC, automation observations 的講者 Mark Elkins 則分別從 Registry 及 Registrar 的面向摘要 DNS 管理的觀察現象，接著再切入至 DNSSEC 管理面，並摘要在 Cloudflare 上觀察到的 DNSSEC 問題。<br>3. CIRA: ZERO-Touch Universal IoT Device Identity，首先由 Ash Wilson 講述 PKI-based Device Identity 可以達成 E2E Message Security、Transport authentication 及 Network Authentication，但卻也面臨實作的一些挑戰議題，所幸 DANE project 可以解決這些問題，其中也提到了關於 Namespace 的重要問題，在 CSA 的 Summary Guidance for Identity and Access Management in the IoT-Step 1a: Define a common namespace for IoT devices 中有相關的描述，CIRA 的 Project 意圖以 DNS 來建立新的 Universal Namespace 如下圖。 |

| | |
|---|---|
| |  <br>接著由 Jason Blakey 呈現 CIRA 在 PoC 的驗證架構，其透過 eSIM 及電信網路先進行 OTA Provisioning，取得憑證與金鑰，接著基於使用 DANE 在 Wifi 網路進行 IoT 註冊驗證。<br>  |
| 會議心得 | 第三個講題 CIRA: ZERO-Touch Universal IoT Device Identity 與本計畫皆是 DNS 作為 IoT Device Identity 的目標，然而 CIRA Project 考量的是在 Internet 上基於 DANE 架構來達成 Universal Namespace 的管理與驗證，而本計畫考量的是在 5G 專網的架構下進行 Identifier 編碼與整合管理，各有其優點。 |

| | |
|---|---|
| 與本計畫關聯 | 第三個講題 CIRA: ZERO-Touch Universal IoT Device Identity 與本計畫最為相關,能夠作為參考的對象並持續關注 CIRA Project 及 DANE 的發展。 |
| 回饋 | IoT Identity Management 的相關議題在 ICANN 及 IETF 皆是近年受到重視的議題，恰巧在此次 ICANN 會議 CIRA 及本計畫皆展示了各自以 DNS 作為 IoT Identity 的 PoC，因此這方向確實為眾所認可的解決方案之一。 |

**(三) SSAC 公開會議(SSAC Public Meeting)**

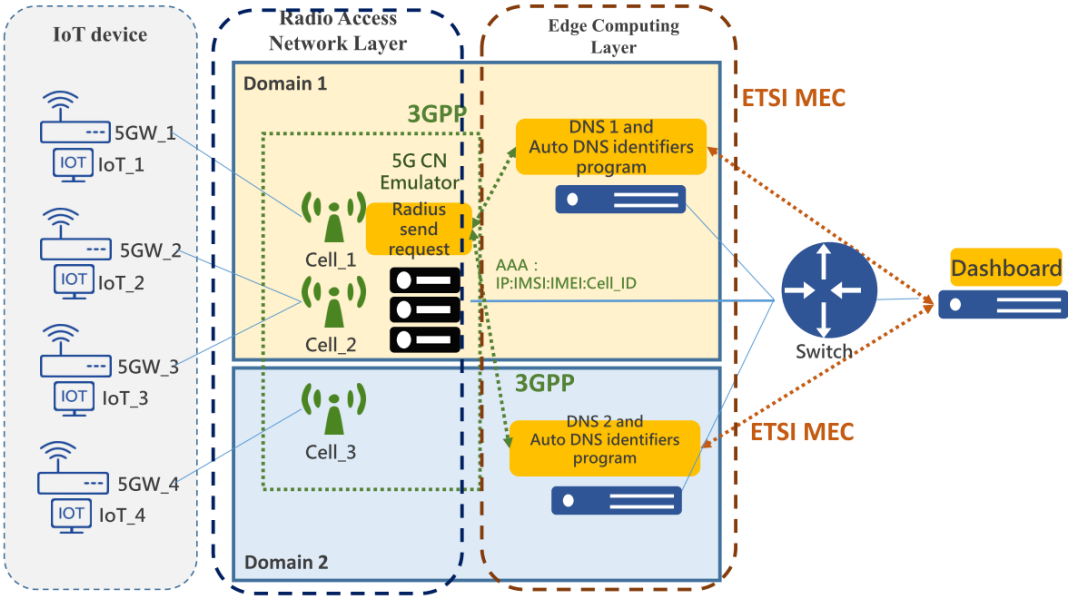
| 日期 | 10/27(三) | 參與會議場次 | ICANN72 |
|---|---|---|---|
| 會議主題 | SSAC Public Meeting | | |
| 會議過程 | SSAC Public Meeting 主要是對於 Security and Stability Advisory Committee (SSAC)的相關活動現況進行說明，議程首先是由 SSAC Chair Rod Rasmussen 進行簡單的開場，並且開始介紹 SSAC 組職現況及架構。<br>接著交由 Geoff Huston 摘要 SAC117 工作,SAC117 摘要了許多 Root Service Early Warning Systems 主題相關的發表文章。再由 Steve Crocker 摘要 SAC118 工作，首先說明目前 EPDP(Expedited Policy Development Process) Phase 2A 的主題，並且提出了一些建議。Steve Crocke 亦對 SAC119 GNSO Transfer Policy Review PDP WG 進行簡單的摘要說明。以及 NCAP Co-Chairs James Galvin 對 Name Collision Analysis Project 工作進行說明。<br>議程最後由主席 Rod Rasmussen 結論目前 SSAC 共有 36 位成員，自 2002 年來發表了 119 份出版文件，並且 SSAC 正尋求具備以下技術背景的專家能夠加入，特別是非洲、拉丁美洲及亞太平洋等地區的會員。<br>• ISP operations<br>• Large-scale measurement<br>• Registrar Operations<br>• Browser Development/Testing<br>• Mobile Apps Development/Testing | | |

| | |
|---|---|
| | • Low bandwidth resource constrained Internet connectivity<br>• Red Team experience<br>• Risk management<br>• Law Enforcement experience |
| 與本計畫關聯 | 本議程安排的議題與本計畫較無直接的關聯性，但可以了解目前 SSAC 關注的議題與發展現況。 |
| 回饋 | 本會議討論之主題與本計劃僅有間接相關，屬於本計畫主軸實現之後的下一步進展與配套，可作為未來計畫之參考。 |

**(四)技術日 Tech Day (1 of 3)**

| | | | |
|---|---|---|---|
| 日期 | 10/27(三) | 參與會議場次 | ICANN72 |
| 會議主題 | Tech Day (1 of 3) | | |
| 會議交流 | 本次會議交流名單如下：<br>BERHARD LISSE, 議程主席, Chair of the ccNSO Tech Working Group<br>JACQUES LATOUR, CTO at the Canadian Internet Registration Authority (CIRA)<br>Yoshiro Yoneya<br>Justin Mack, MarkMonitor<br>Ulrich Wisser<br>Rick Wilhelm<br>Anupam Agrawak | | |
| 會議過程 | Tech Day 首場安排的時間有一個小時，議程安排如下:<br>**16:00** Opening Remarks: Lisse<br>**16:10** PoC of DNS Identifiers: Chen<br>**16:30** DNS Core Census: Lewis<br>**17:00** Break<br>首先由議程主席 EBERHARD LISSE 簡單的進行開場，並介紹這場會議安排的兩個講題，PoC of DNS Identifiers 及 DNS Core Census。 | | |

第一個講題 PoC of DNS Identifiers 由本計畫團隊顧問陳麒元代為發表，首先陳述本計畫團隊為解決巨量物聯網裝置之管理問題，提出以 DNS Identifier 作為編碼管理解決方案的想法，並說明此次 PoC 驗證的實驗架構圖如下:




以及結合電信核心網路和邊緣運算層後，以 DNS Identifier 作為 5G 專網物聯網裝置編碼的可行格式及範例:

| Category | Terminal Layers of IoT | Radio Access Network Layer | Edge Computing Layer | Core Network Layer |
|---|---|---|---|---|
| Standard | GMSA TS.06 v18.2 | 3GPP TS29.061 | | 3GPP TS 23.003 |
| DNS identifier | IMEI | Cell_ID | Domain_ID | SST, MNC, MCC |
| | (equipment). | .(Cell). | .(area). | <sst>.nssf.5gc.mnc(mnc) .mcc(mcc).3gppnetwork.org |
| Example | 355979860003363 | Cell_1 | Domain_1 | <sst_1>.nssf.5gc.mnc001 .mcc999.3gppnetwork.org |

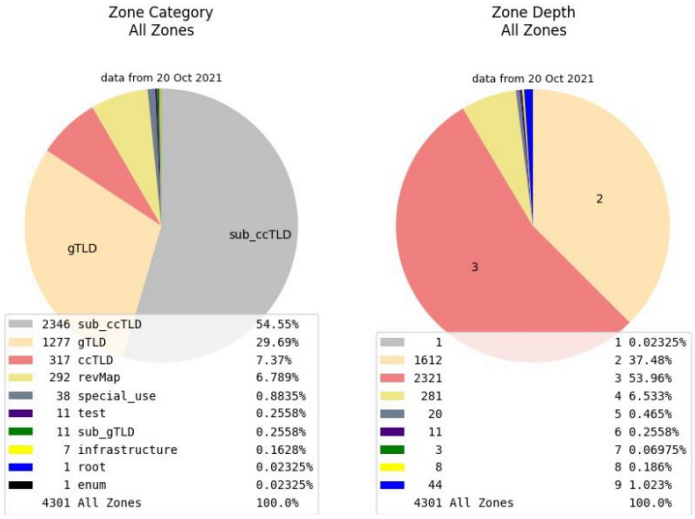
接著透過簡報畫面呈現 5G 專網物聯網裝置編碼管理的 PoC 驗證測試:

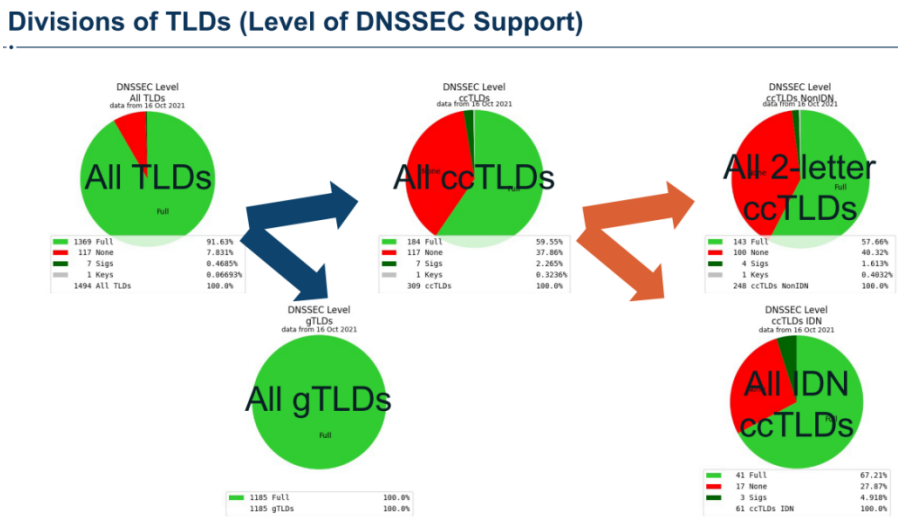
- 情境 1: DNS Identifier PoC 驗證測試分為 Inter-Domain 及 Cross-Domain 兩種測試場景。
- 情境 2: 大量物聯網裝置之 DNS Identifier PoC 驗證 (100 個)。

PoC of DNS Identifiers 介紹結束後我們收穫了許多的提問如下:

1. JACQUES LATOUR: So I understand the RADIUS and the domain name assignment are to allow the IoT device to move along and get provision. So my question is are the IoT devices themselves aware of that identity or that's something separate?
   CHI-YUAN CHEN: Yes. IoT devices can aware this identifier from

| | |
|---|---|
| | the DNS query.<br>JACQUES LATOUR: But is the IoT device aware of its own identity when it changes? Because presumably when it changes zones, like cells, the identifier changes, which means it changes the identity of the IoT device.<br>CHI-YUAN CHEN: I think both the IoT device and the core network can use the DNS query to update the newest identifier and the related information.<br>透過 DNS Query 可以讓裝置得知自身的相關改變，但的確可能需要花上一些時間才能取得最新的更新。<br>2. Yoshiro Yoneya: What kind of IoT devices are you assuming?<br>CHI-YUAN CHEN: We used the 5G gateway and the industrial IoT—many industrial personal computers, as our IoT device. DNN, data network name, for the IoT device. And we used this name for our network slicing tool to our proof of concept.<br>3. Justin Mack: Q1: What TTL (time-to-live) values are used for the DNS A and AAAA (quad-A) records being generated? Q2: How do you manage the serial value in the Start of Authority record with so many updates to the zone?<br>講者視訊軟體出了狀況未能及時回覆(以下問題將會後再答覆)，這個問題提及在 DNS 伺服器管理大量 record 時該如何去設置 TTL 及 serial，目前 PoC 採用的是預設值，該議題確實是未來實務上需要考慮的議題。<br>1. Ulrich Wisser: Where are these names used? Could you say something about privacy considerations?<br>2. Rick Wilhelm: This is all DNS on a private network, correct?<br>3. Anupam Agrawak: If the IoT devices are not moving in an Industrial Internet scenario, what's the use case for changing cell towers?<br>第二的講題是由 Edward Lewis 所發表的 DNS Core Census，其為 DNS 核心普查計畫，其目標包含的 DNS Core 如下: |

<table>
<tr>
<td></td>
<td>


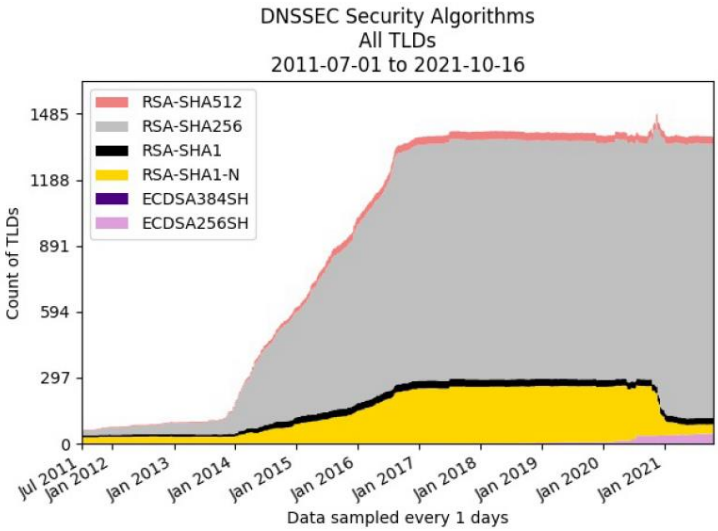
<ul>
<li>Other scattered numbers
<ul>
<li>4,301 Zones</li>
<li>6,458 Name servers</li>
<li>9,928 Addresses</li>
<li>2,265 Route Origins</li>
<li>524 AS Numbers</li>
<li>8,038 DNSKEY records</li>
<li>7,077 DS records</li>
<li>20,639 RRSIG records</li>
<li>14,144 IDN Tables</li>
</ul>
</li>
</ul>
其中亦呈現了目前對於 DNSSEC 的支援現況:


</td>
</tr>
<tr>
<td>會議心得</td>
<td>與會者許多都是在 DNS 技術或管理專精的專家，對於此次本計畫團隊展示的 PoC 驗證，很快便能指出其中一些值得探討的議題，整理如下:<br>1. FQDN 更新延遲<br>2. DNS Server 面對巨量 record 管理<br>3. FQDN 安全隱私問題</td>
</tr>
<tr>
<td>與本計畫關聯</td>
<td>ICANN 在 5G Technology 報告中指出 DNS 可以作為物聯網裝置管理的解決方案之一，本計畫藉此次會議展示本年度計畫的 PoC 驗證測試結果，希望藉此與 ICANN 專家學者交流想法。</td>
</tr>
</table>

| | |
|---|---|
| 回饋 | 彙整專家提問議題，對於 DNS Identifier 作為 5G 物聯網管理的解決方案，後續應持續針對以下兩個方向深入研究:<br>1. 巨量物聯網裝置下的 DNS 伺服器維運管理<br>2. DNS 編碼的安全隱私問題 |

**(五)技術日 Tech Day(2 of 3)**

| | | | |
|---|---|---|---|
| 日期 | 10/26(二) | 參與會議場次 | ICANN72 |
| 會議主題 | Tech Day (2 of 3) | | |
| 會議過程 | Tech Day 第二場安排的時間有一個半小時，議程安排如下:<br>**17:30** RDAP Enabled Security Initiative: Miller<br>**17:50** ICANN's RDAP Conformance Tool: Alvarez<br>**18:10** DNS-Magnitude: Arends<br>**18:30** DNSSEC Algorithm Choices: Lewis<br>**18:40** DNSSEC Parameters for TLDs: Dukhovni<br>**19:00** Break<br>在第一個講題 RDAP Enabled Security Initiative 中，講者 GARTH MILLER 首先陳述在 Registry、Registrar 及 Registrant 三者不同面向遭遇的惡意行為及安全管理議題，藉著提出透過測試開源工具 RDAP (Registration Data Access Protocol)測試的程序，並且陳述為何採用 RDAP 的原因:<br>1. WHOIS services are not helpful: server output often differs, rate limiting is common, required data is often redacted.<br>2. RDAP: easy integration via an existing industry standard API<br>3. ccTLD managers retain full control of personal and commercially sensitive data<br>第二個講題 ICANN's RDAP Conformance Tool 的講者 EDUARDO ALVAREZ 則是展示一個由 IETF 開發出可以對 RDAP 伺服器進行合規性測試(Conformance Test)的開源工具，採用 gTLD RDAP profile 作為範例，並且列出測試中發現的常見議題。<br>第三個講題 DNS Magnitude 的講者 Roy Arends 則是首先說明 | | |

| | |
|---|---|
| | Magnitude 來表示 DNS 量級的定義，該詞彙最早是在 2017 年的 ICANN 58 會議中由 Alexander Mayrhofer 所提出，並說明其定義 DNS Magnitude 的三個原則:<br>1. Count unique hosts per domain instead of queries per domain<br>2. Use a logarithmic scale<br>3. Normalize the result<br>計算出的量級代表的意義為「A high magnitude value indicates that a top-level domain is queried for by a large number of networks and presents a high collision risk.」。<br>第四個講題 DNSSEC Algorithm Choices 的講者 Edward Lewis 則是展示在數年間 Top-Level Domains 的 DNSSEC security algorithm 使用情形(如下)，並針對不同層級區域等分類另行呈現討論。<br>  <br><br>第五個講題 DNSSEC Parameters for TLDs 的講者 VIKTOR DUKHOVNI 則是針對 RFC 8624 中定義的簽章及驗證演算法 RSASHA256(8)及 ECDSAP256SHA256(13)進行金鑰長度及參數的分析，並探討目前實作上遭遇的困難。 |
| 會議心得 | ICANN Tech Day 所安排的講題許多都是目前正在進行的實務專案成果，主要針對 Top-Level Domains 管理及 DNSSEC 落實等兩個面向，其中不難觀察到安全性的議題占了很大的比例。 |
| 與本計畫關聯 | 本議程安排的議題與本計畫較無直接的關聯性，但可以了解目前國際上關注的實務議題。 |

| | |
|---|---|
| 回饋 | 目前對於 DNSSEC 落實及相關安全管理上的議題是相當受到重視的，本計畫亦規劃有相對應的分項進行研究。 |

**(六)GNSO - CPH DNS 濫用工作小組社群更新會議(GNSO - CPH DNS Abuse Work Group Community Update)**

| 日期 | 10/26(二) | 參與會議場次 | ICANN72 |
|---|---|---|---|
| 會議主題 | GNSO - CPH DNS 濫用工作小組社群更新會議(GNSO - CPH DNS Abuse Work Group Community Update) | | |
| 會議交流 | 在線上與 Perkins Coie 之律師 Griffin Barnett 就 DNS Abuse 的上訴機制簡短交換意見。Griffin 認為上訴機制應有 ICANN 參與，更瑩回覆他但是上次 ICANN 71 的時候有提到 ICANN 的組織太大，應由第三方機構負責。<br>線上向主持人提問，ICANN 的 registry agreement 會不會因為 Trusted Notifier 的機制或是其他防止 DNS Abuse 的機制而修正，與談人 Brian Cimbolic 回答，Trusted Notifier 的關係乃係建立於 Registry/Registrar/Trusted Notifier 之間，並不需要修正 ICANN 合約以達成。 | | |
| 會議過程 | 會議主要介紹 CPH DNS Abuse Work Group 最近的進展，主要係發布三篇新的文件，包括：<br>1. Appeals Mechanisms following DNS Abuse Mitigation<br>2. Approaches to Business Email Compromise (BEC) scams<br>3. CPH Trusted Notifiers Framework<br>會議集中介紹 CPH Trusted Notifiers Framework，解釋 Registry 及 Registrar 和 Trusted Notifier 如何建立關係，如何互動，有關之盡職調查、能力、法律背景等等。 | | |
| 會議心得 | 在會議 Q&A 的過程中，從主持人 Reg Levy 的回覆以及反應發現 Registry 及 Registrar 和 Trusted Notifier 的互動與關係並不透明，主持人提到為了保護 Trusted Notifier，她不會公開 Trusted Notifier 的身份，雖然她可以分享互動之經驗，她鼓勵想成為 Trusted Notifier 的機構或個人自行去接觸合適的 Registry 及 Registrar，形成其等之間之信賴關係。如此 Trusted Notifier 對於 Registry 及 Registrar 之關 | | |

| | |
|---|---|
| | 係與線民與警察之關係頗為類似，與一般 ICANN 的組織採取公開透明化之運作方式不盡相同。惟 DNS Abuse 的防止以及相關行動大多會與執法系統產生互動，如此 Trusted Notifier 的角色以及所能提供的助力其實十分關鍵，也需要堅實之基礎，才能支援 Registry 及 Registrar 對抗 DNS Abuse。 |
| 與本計畫關聯 | DNS Abuse 的 Trusted Notifier Framework 與本計畫的號碼指配或是 network slicing 比較沒有直接相關，但是一旦未來技術上可以使用 DNS 來分配電信號碼，DNS Abuse 的防範對於系統之安全與穩定及十分重要，Trusted Notifier 就會是其中之助力之一。 |
| 回饋 | 本會議討論之主題與本計劃僅有間接相關，屬於本計畫主軸實現之後的下一步進展與配套，可作為未來計畫之參考。 |
| 建議 | 有關 ICANN 對於 DNS Abuse 之防範與發展為 ICANN 最近重要之主題，雖然與本計畫並不直接相關，但是如果未來擬更積極加入 ICANN 組織或活動，此一主題值得密切關注與加入資源討論與發展。 |

# 肆、第三場國際會議：IETF111

## 一、 IETF111 會議簡介及議程

IETF111 虛擬會議訂於 2021 年 7 月 26 日至 7 月 30 日，共計 5 日。此次會議由「瞻博網路」(Juniper)、CISCO、ICANN 等等單位贊助主辦，為因應新型冠狀病毒疫情影響，以「全球遠端參與形式」舉行，共計 1,411 名遠端參與者。

由於 IETF 主要負責網際網路標準的研究發展和制定，例如網際網路上使用的通訊協定(protocols)、程序 (procedures)和慣例(conventions)等的制定其組織架構，與本研究議題關聯性高，並非採取會員制度，而是以個人名義皆可參與或發表文件，參與對象以個人為主，而不是國家、公司或團體，經評估後於該組織擔任國際組織幹部之可行性較高，因此今年度將安排 2 名專業人才分別參與 IETF111 及 IETF112 兩場會議，以強化國際鏈結及掌握國際相關議題趨勢。

IETF111 議程安排主要為「網際網路工程任務小組」(Internet Engineering Task Force，簡稱「IETF」) 及「網際網路研究任務小組」(Internet Research Task Force，簡稱「IRTF」)各工作小組進行中「草案」(Draft) 目前進展及未來規劃，同時包含社交活動 Newcommers'Coffee Break 及 IETF 全體大會。

| 臺灣時間 | 會議名稱 | 效益分析 |
|---|---|---|
| 27, July<br>7:00-9:00 | Domain Name System Operations<br>(簡稱 Dnsop) | Dnsop 工作小組的主要工作是為 dns 的軟體開發、服務運作及管理制做相關的工作指引，可透過參與本議程，了解目前技術規畫方向，及了解該小組作業方式。 |
| 27, July<br>7:00-9:00 | IoT Operations<br>(簡稱 IoTops) | IoTops 工作小組是負責討論物聯網相關設備的運作問題，尤其是設備的起動與生命週期的管理；因為與物聯網相關的 IETF 工作小組很多，本工作小組也希望在討論各種物聯網相關的技術組 |

| 臺灣時間 | 會議名稱 | 效益分析 |
| --- | --- | --- |
| | | 合時能發揮積極的作用。 |
| 28, July<br>5:00-5:30 | Newcomers' Coffee Break | 藉由新進成員活動，多方面了解 IETF 生態及領域社群。 |
| 28, July<br>5:30-6:30 | Extensions for Scalable DNS Service Discovery (簡稱 dnssd) | dnssd 工作小組主要的任務是為延伸可擴展 DNSSD（DNS service Discovery）開發解決方案，討論以 mDNS（RFC6762）、DNS-SD（RFC6763）為基礎在多網段的應對方案。 |
| 29, July<br>7:00-8:40 | IETF Plenary | 藉由參與 IETF 全體大會，了解其重要核心成員對整體組織的領導方向及評估各領域議題的側重方向，以提供專案成員擘劃未來專案主軸。 |
| 30, July<br>3:00-4:00 | DNS PRIVate Exchange (簡稱 dprive) | DNS 傳輸交換隱私工作小組（Dprive）主要工作是保障 DNS 訊息交換間的機密性及找尋可能性的解決方案並評估工作小組所提供的技術方案應對各種 DNS 監控攻擊的有效性。 |
| 30, July<br>4:30-5:30 | DNS PRIVate Exchange (簡稱 dprive) | |
| 30, July<br>7:00-7:30 | Newcommers’Coffee Break | 藉由新進成員活動，多方面了解 IETF 生態及領域社群。 |
| 30, July<br>7:30-8:30 | Domain Name System Operations (簡稱 Dnsop) | Dnsop 工作小組的主要工作是為 dns 的軟體開發、服務運作及管理制做相關的工作指引，可透過參與本議程，了解目前技術規畫方向，及了解該小組作業方式。 |
| 31, July<br>7:00-9:00 | Operations and Management Area Working Group (簡稱 opsawg) | opsawg 工作小組的主要工作是為不在目前工作小組分類內且不適合另建新工作小組的技術提案文件（RFC）提供運作與管理的討論平台。 |

## 二、 IETF111 會議紀錄

### (一) IRTF 公開會議、IETF 全體會議、DNS 傳輸交換隱私工作小組、確定性網路及營運與管理領域工作小組(IRTF Open Meeting, IETF Plenary, DNS PRIVate Exchange, Deterministic Networking, Operations and Management Area Working Group Joint OpsAWG / OpsAREA)

| | | | |
|---|---|---|---|
| 日期 | 7/27(二)、7/29(四)、<br>7/30(五)、7/31(六) | 參與會議場次 | IETF 111 |
| 會議主題 | IRTF Open Meeting, IETF Plenary, DNS PRIVate Exchange, Deterministic Networking, Operations and Management Area Working Group Joint OpsAWG / OpsAREA | | |
| 會議交流 | 這是本人第一次參加 IETF 會議，所以有向 IETF 會議申請找一位有經驗的參與者(導師)來協助我，了解 IETF 會議的內容、進行方式、參與規則，以及如何獲得各種協助，如何參與會議討論等事項。我的導師(mentor)是 Paul Wouters，他是很有名的網路資安專家，他是 Libreswan (以前稱為 Openswan) IPsec/IKE 的主要開發者，也在 ICANN 組織中擔任過 liason 以及 Root Rollover Design committee。<br>Paul Wouters 目前是 No Hats 這家公司的董事長(President)，他的公司專注於 DNSSEC 及 IPsec 的顧問工作。他是 IETF 標準 RFC 7929、RFC 7901、RFC 7828、RFC 7670、RFC 7619、RFC 7250 的制定者之一。這次因為都是線上會議，全球的時差問題也造成會議後，很難找到其他參與者進行交流活動。希望，日後能有更多機會與 Paul Wouters 交流，或邀請他來台灣訪問交流。 | | |
| 會議過程 | 本次會議個人參加了幾場不同主題的 Session，這裡報告未寫在其他報告項目的幾場會議參與情形。IETF Plenary 主要是報告各項有關於 IETF 的整體營運狀況、需要進行的組織選舉以及其他組織事務。主要的重點是：(1)每次 IETF 會議的參與人數約在 1500 人左右，歐美的專業人士仍是主要參與的力量。(2)COVID-19 確實造成影響，IETF 會議必須改為線上會議，參與人數也降低。(3) Internet Architecture Board 及 Internet Research Task Force 都進行了工作報告。 | | |

| | |
|---|---|
| | (4) RFC Editor 功能改善。(5) 提名委員會針對如何找到合適的志願工作者進入各位置，所進行的一些實驗結果進行報告。(6)IETF 行政對下次 IETF112 馬德里會議及後續會議的地點等行政事務進行報告。<br>此外，IETF 針對其發出的社群問卷的分析結果也進行了報告。Deterministic Networking 工作小組的 session 主要是討論 10 份進行中的草案。確定性網路(Deterministic Networking)是為即時應用，例如音頻和視頻流、工業自動化與車輛控制等，所需要的網路特性，所發展的一套網路標準；這些網路特性包含：極低的資料丟失率與有限制的端對端延遲。Operations and Management Area Working Group Joint OpsAWG / OpsAREA session 主要是討論 7 份進行中的草案。營運與管理領域工作小組所發展的草案，主要是運用 YANG (Yet Another Next Generation) modeling language 來建構一個可用的模型，以保障網路服務品質及監控網路效能。<br>此外，這些草案也對相關的支援事務進行標準的發展，例如：建議儘快使用 PCAPng 取代 PCAP 來處理封包抓取事宜、增加設備上的軟體的透明度及確認軟體可能的弱點(Vulnerabilities)。 |
| 會議心得 | 這次參與 IETF 111 次會議，感受到這個會議是一群長時間投入、非常熱愛使用網路技術來解決實際網際網路問題的人，所組成的團體組織。IETF 會議中，各個 session chair 與各工作小組報告工作進度的成員們，看來都相互非常熟悉，很多人都相識甚久的感覺。本次參與會議的人數，官方的統計是 1369 人，對照歷年參與人數，沒有太多的改變，不過，依照 IETF 執行長的報告，長期趨勢而言，參與 IETF 會議的新面孔增加的並不多，也不快。這倒是給了我們一些想法，若台灣有計畫地投入 IETF 會議，可能更有機會進入組織核心。因為 COVID-19 疫情的影響，這次 IETF 111 會議採用線上方式進行。這個結果就是對某些時區(例如：亞太區)的參與者而言，重要會議 sessions 的時段都不理想，常是在半夜或清晨開會，身心都受不了太長的時間連續這樣進行 5 天。<br>因為主要的會議 session 主持人多在美國或歐洲國家，而會議時間的選擇就偏向他們比較方便參與的時段。我認為實體的會議才能有更深入的互動與交流，線上會議在互動交流上，實在有許多的不便與 |

| | |
|---|---|
| | 限制，大多數參與會議者，也都是會議 session 一結束，就直接離開會議下線了，無法有效進行交流對話。 |
| 與本計畫關聯 | 在 DNS PRIVate Exchange WG(Working Group)這個會議 Session，主要是討論了四個有關 DNS 的技術。其中，兩個技術是屬於既有的工作項目，另兩個技術是屬於新成立的工作項目。兩個既有的工作項目是：(1) DNS over QUIC (DoQ)，< draft-ietf-dprive-dnsoquic>：QUIC 是一個剛於 2021 年 5 月成為 IETF RFC9000 標準的網路傳輸層協定，QUIC 提供低延遲且安全的網路封包傳輸以嘗試取代傳統 TCP 網路傳輸協定。DoQ 這個技術目標是使用 QUIC 協定放到 DNS 的資訊傳輸工作上，以保護傳輸的資料的隱私性，同時，降低資訊傳輸的延遲時間。<br>簡而言之，DoQ 的目的是達成類似於 DoT (DNS over TLS)的隱私保護能力並同時達到 DNS over UDP 協定的低延遲傳輸能力。目前這個技術草案更新至第 3 版，做了以下幾個修改：(a)這個版本重新聚焦於三個方向上：RDoQ、ADoQ、XoQ；(b)同時，修改了串流映射(stream mapping)的規格；(c)釐清如何處理協定錯誤資訊的方式；(d)依照 IANA 的意見，這個協定將使用與 DNS over DTLS 協定一樣的埠號 853，也可能使用埠號 784 做為測試用。<br>這版也並未對一些議題提出解決方案，例如：對於新提出的 Zone Transfer 的 connection mapping 的一般性支援與其範圍為何、DoQ-i02 的實作實驗也仍在進行中、針對 ADoQ 的身分辨識模型已故意地延後研發、訊息整體長短(message size limits)的限制也沒有定案。(2) Recursive to Authoritative DNS with Unauthenticated Encryption，< draft-ietf-dprive-unauth-to-authoritative>：這項工作發布了第三版草案來進一步說明如何運用未確認身分的加密(Unauthenticated Encryption) 將連接 DNS recursive resolver 與 authoritative server 的通訊管道加密；因為某些 DNS recursive resolver 認為在 Internet 的環境中，無論如何，有多一些加密操作總比沒有加密操作來得好，即使進行加密者的身分 |

| | |
|---|---|
| | 尚未被確認。這個機制對目前的 DNS 作業環境而言，只是一個選擇項，並非一定要實作進 DNS 作業情境。這版草案仍有三個議題未能解決：(a)如何應對 port probing？(b) 目前草案是基於 TCP 協定，但更應該基於 DoQ 協定來實作提出的方法。(c) 需要考慮到 IANA 組織的意見。<br>兩個新成立的工作項目是：(3) New Record Types in Parent Zones，<draft-schwartz-dprive-name-signal-00>：這個工作項目是嘗試在上層 DNS(parent DNS)使用 SVCB 紀錄，這樣的話，需要做許多改變現有 DNS 環境架構的事，很可能需要花費多年的時間。目前工作小組建議不要急著找出可立刻實踐的方法(workarounds)，應該想清楚議題再往前進。(4) Signaling Authoritative DNS Encryption，<draft-rescorla-dprive-adox>：這個工作項目連動於上一個工作項目，主要是要建立一個方法讓 recursive resolver 可以由 authoritative server 得到額外的訊息，知道它要訪問的目的節點(伺服器)是支援加密操作的。這個額外的訊息預計是由 SVCB 紀錄來提供，但是如何做到將 SVCB 紀錄傳播至上層 DNS 是個需要解決的大問題(這是前一個工作項目要做的事)。 |
| 回饋 | 本次參加的 IRTF Open Meeting，主持人是 Colin Perkins。他先說明 IRTF 的 14 個研究群組中，有 4 個群組在本次會議沒有議程，有 1 個群組已經提早開完會了，剩下 9 個群組會在本次會議中開會討論進度。<br>IRTF 也在 6 月提出了兩個 RFCs：PANRG 研究群組提出 RFC 9049、ICNRG 研究群組提出 RFC 9064。最後，他介紹 Applied Networking Research Prize，這個獎頒給在網路應用(applied networking)領域中，研究結果最傑出的團隊。本次會議有兩個得獎的團隊來正式報告他們的研究成果。(1) Rüdiger Birkner 及他的團隊報告 Config2Spec: Mining Network Specifications from Network Configurations。這個研究是想建構一個可以自動找出支援使用者要求的網路規範的可用網路，研究團隊探索 Intent-based Networking 的可行性，運用 Networking Configuration Synthesis 工具及 Configuration Validation and Verification 工具來自動化搜尋並建構支援使用者要求 |

| | |
|---|---|
| | 的網路規範的可用網路。他們也進行了實驗以證明這個構想是有可能實現的。 (2) Sadjad Fouladi 及他的團隊報告 Salsify: Low-latency Network Video through Tighter Integration between a Video Codec and a Transport Protocol。這個研究是建構一個新的即時視訊傳輸架構，目標是在即時視訊傳輸時，視訊品質不會因為傳輸過程的網路環境的改變(例如：傳輸頻寬突然變小等)，而受到明顯的影響(視訊接收者可以感受到一段時間的品質急遽下降)。<br>此研究成果是將視訊編解碼器與網路傳輸協定更直接地整合在一起，是一個非常實用的技術。我認為臺灣的學術界或網路產業界都有能力研發出這類可實用化的研究成果，若我們找出並鼓勵這些團隊，將其研發成果來投稿 IRTF 每年與 ACM、ISOC 合辦的 Applied Networking Research Workshop，或可得到 Applied Networking Research Prize 的肯定並有機會於 IETF 會議中行報告。 |

**(二) 網絡上 IPv6 的限制資源節點會議(IPv6 over Networks of Resource-constrained Nodes)**

<table>
<tr><td>日期</td><td>7/29(四)</td><td>參與會議場次</td><td>IETF 111</td></tr>
<tr><td>會議<br>主題</td><td colspan="3">IPv6 over Networks of Resource-constrained Nodes</td></tr>
<tr><td>會議<br>過程</td><td colspan="3">IPv6 over Networks of Resource-constrained Nodes 會議場次安排共計一小時，議程如下安排：<br><table><tr><th>主題</th><th>講者</th></tr><tr><td>Introduction and draft status</td><td>Bhandari/Gomez</td></tr></table>Agenda bashing; blue sheets; scribe; Jabber scribe<br>議程主席首先簡單開場並說明議程的安排，最後摘要目前工作小組內的草案處理情形。<br><table><tr><th>主題</th><th>講者</th></tr><tr><td>Update of Applicability and Use Cases draft</td><td>Yong-Geun Hong</td></tr></table>https://datatracker.ietf.org/doc/html/draft-ietf-6lo-use-cases-11<br>該講題摘要簡述 draft-ietf-6lo-use-cases-11 草案工作，已於 2020 進</td></tr>
</table>

<table>
<tr><td></td><td>入工作小組 Last Call，並說明對於收到評論的回應與修正。<br><table><tr><th>主題</th><th>講者</th></tr><tr><td>Transmission of SCHC-compressed Packets over IEEE 802.15.4</td><td>Carles Gomez</td></tr></table>https://datatracker.ietf.org/doc/html/draft-gomez-6lo-schc-15dot4-00<br>該講題摘要簡述 draft-gomez-6lo-schc-15dot4-00 草案工作，該草案為新提案，主要提出 SCHC 標頭壓縮的協定格式定義，搭配 6Lo(WPAN)的標頭壓縮，理論上能夠改善 IEEE 802.15.4 的電池存活時間達至高接近 40%。<br><table><tr><th>主題</th><th>講者</th></tr><tr><td>Native Short Address for Internet Expansion</td><td>Guangpeng Li</td></tr></table>https://datatracker.ietf.org/doc/html/draft-li-native-short-address-00<br>該講題摘要簡述 draft-li-native-short-address-00 草案工作，該草案為新提案，作者來自 Huawei，主要為提出 Native Short Addresses (NSA) 定義，以縮減標頭長度。<br><table><tr><th>主題</th><th>講者</th></tr><tr><td>Fragment forwarding and FEC</td><td>Amaury Bruniaux</td></tr></table>該講題首先講述 RFC4944 的轉送機制與缺點，提出 VRB (Virtual Reassembly Buffer)以改善此問題，並且提出三個 6LoWPAN 的 Forward Error Correction (FEC)機制，XorFec、RFec 及 NCFec。</td></tr>
<tr><td>與本計畫關聯</td><td>透過 6lo 工作小組安排的相關草案討論，可以獲取目前 6LoWPAN 標準發展的現況與趨勢。</td></tr>
<tr><td>回饋</td><td>從議程安排的草案講題中可以觀察到中國大陸已有許多電信與網通業者積極參與草案的撰寫工作，我國在這方面的參與度較低，建議應鼓勵相關業者考量投入。</td></tr>
</table>

**(三) ACM/IRTF 應用網絡研究研討會：新網路協定與具實用性的壅塞控制及 DNS 隱私以及應用程式與規格(ACM/IRTF Applied Networking Research Workshop: New Internet Protocols & Practical Congestion Control and Privacy & Applications)**

| | | | |
|---|---|---|---|
| 日期 | 7/27(二)、7/29(四) | 參與會議場次 | IETF 111 |
| 會議主題 | ACM/IRTF Applied Networking Research Workshop: New Internet Protocols & Practical Congestion Control and ACM/IRTF Applied Networking Research Workshop: Privacy & Applications | | |
| 會議過程 | ACM/IRTF Applied Networking Research Workshop 第一個場次會議共兩個小時，分為兩個 Session，New Internet Protocols 與 Practical Congestion Control<br>New Internet Protocols 共有五個講題，分述如下：<br>1. Adaptive Cheapest Path First Scheduling in a Transport-Layer Multi-Path Tunnel Context 中，作者證明了將 CPF (Cheapest Path First) 與 MP-DCCP 通道一起使用可能會導致次最佳化性能。這是由於排乘與點到點通道擁塞控制之間的不利互動。 因此作者設計了自適應最便宜路徑優先 (ACPF) 排程，它限制了主要瓶頸中的佇列建構，並更早地將流量移動到次要路徑。 CPF 相比，ACPF 將平均傳輸量提高了 24% 到 86%。<br>2. Leveraging the 0-RTT Convert Protocol to improve Wi-Fi/Cellular convergence，作者提及行動數據使用量正在增加，行動網路運營商希望將部分流量轉移到 Wi-Fi 網絡上。 MPTCP 和 0-RTT TCP Convert 協定可以實現通訊網路和 Wi-Fi 網路的融合。其先介紹這兩個協定，然後討論可能的部署方式，最後展示一些來自智慧手機的測量結果。<br>3. Cooperative Performance Enhancement Using QUIC Tunneling in 5G Cellular Networks，Multiplexed Application Substrate over QUIC Encryption (MASQUE) 是一種新的協定，目前正在 IETF 標準化程序。 MASQUE 定義了 HTTP CONNECT 方法的擴展，以支持基於 QUIC 的通道以及 UDP 和 IP 流量轉發。 作者討論基於 MASQUE 的代理設置的使用案例，以解決通訊網 | | |

| | |
|---|---|
| | 路中性能最佳化的挑戰。 所呈現的使用案例基於三個方面（即客戶端、代理和目標伺服器）之間支持的合作級別來實現不同的服務。<br>4. CCID5: An implementation of the BBR Congestion Control algorithm for DCCP and its impact over multi-path scenarios 中，作者提及提供多連接服務是下一代無線網路的一個重要目標，其中多重存取網路需要融合到有效支持可靠和不可靠流量的解決方案中。 基於虛擬網路介面和路徑擁塞控制通道，MP-DCCP 的多路徑存取聚合框架提出了一種新穎的解決方案，可靈活支持不同的路徑排程和擁塞控制演算法以及重新排序模組。 MP-DCCP 框架的程式碼包括新的 CCID5 已開放原始程式碼。<br>5. Toward greater scavenger congestion control deployment: implementations and interfaces 中，作者提出 (1) 兩個最近的 scavenger 提案 PCC Proteus（基於 QUIC）和 LEDBAT++ 的開源實作； (2) 兩者在現實網路設置中的測試； (3) 討論應用程式利用 scavenger 擁塞控制所需的 API。<br>Privacy & Applications 會議共有五個講題，分述如下：<br>1. Encryption without Centralization: Distributing DNS Queries Across Recursive Resolvers 作者陳述為了實現增加去中心化和提高靈活性的目標，其展示重構 DNS 解析器架構的設計和實作，該架構允許去中心化名稱解析，保留加密 DNS 的優勢，同時滿足其他所需屬性，包括效能和隱私 .<br>2. Institutional Privacy Risks in Sharing DNS Data 的作者將在權威伺服器上收集 DNS 數據帶來的新風險稱為機構隱私，即使在通過 DNS 遞迴快取和聚合之後也是如此。 作者宣稱是首個通過查看電子郵件交換洩漏的通訊樣式和存取敏感網站的洩漏來證明這種風險的，這兩者都會損害機構的公眾形象。 其定義了一種方法來識別來自機構的查詢並識別洩漏。<br>3. DNS over TCP Considered Vulnerable 展示了 IP 碎片攻擊也適用於 TCP 的伺服器。其在前 10 萬個 Alexa 網域中，有 393 個網域，其名稱伺服器可被強制進行分封 IP 封包且包含 TCP |

| | |
|---|---|
| | segments。 相反，當通過 UDP 發送時，這些網域則不能強制分封。<br>4. Tools for Disambiguating RFCs 應用 NLP 來識別 RFC 中歧義或定義不足的句子，並在歧義被澄清時自動產生協定的實作。該系統還遠非通用或可部署，為了進一步減少歧義句子的成本和錯誤，提高該系統的通用性，還有很多工作要做，以發展一個完全通用且有用的系統，來緩解 RFC 程序中的自然語言挑戰。<br>5. Manus Manum Lavat: Media Clients and Servers Cooperating with Common Media Client/Server Data 其討論新修訂的 CTA 標準—Common Media Client Data (CMCD)，其允許內容提供商深入了解其大規模串流媒體操作的性能。它的姊妹標準—Common Media Server Data（CMSD）正在開發中，將允許伺服器向其他伺服器和客戶端發送提示。CMCD/CMSD 組合是期待已久的 HTTP 可適應串流媒體系統的升級。 |
| 會議心得 | Applied Networking Research Workshop 為 ACM 與 IRTF 合作舉辦的 Workshop，提供一個研究交流的平台，發表的議題較接近學界的研究論文，但相當重視實作，參與會議可以了解最新的協定實作議題。 |

**(四) 用於物聯網服務強化的 DANE 身份驗證會議(DANE AutheNtication for Iot Service Hardening)**

| | | | |
|---|---|---|---|
| 日期 | 7/28(三) | 參與會議場次 | IETF 111 |
| 會議主題 | DANE AutheNtication for Iot Service Hardening | | |
| 會議過程 | 該議程為 DANISH(DANE AutheNtication for Iot Service Hardening)的 Birds of a Feather(BOF)議程，以組成 DANISH 工作小組。DANISH 工作小組目標為使用憑證或 RPK(Raw Public Keys)以擴展 DANE(DNS-Based Authentication of Named Entities)來涵蓋 TLS 客戶端驗證機制。<br>在其問題定義的部分提及 IoT 生態體系的挑戰，目前 Private PKI 無所不在，但要建立 private PKI 網域間的信任是難困難的，並且沒 | | |

有可以避免 PKI 網域間的命名碰撞的技術。因此希望能夠擴展 DANE 與 TLS 客戶端驗證機制來達到 IoT 與 SMTP 的傳輸安全。該講題亦展示兩種客戶端識別命名格式如下:

## Client DNS Naming Convention

Draft is not proscriptive, but proposes 2 naming formats that may be generally suitable for many applications.

Format 1: Service specific client identity

_service.[client-domain-name]

e.g. _smtp-client.relay1.example.com

1st label identifies the application service name. The remaining labels are composed of the client domain name. Allows the same client to have distinct authentication credentials for distinct application services.

## Client DNS Naming Convention

Format 2: IOT Device Identity

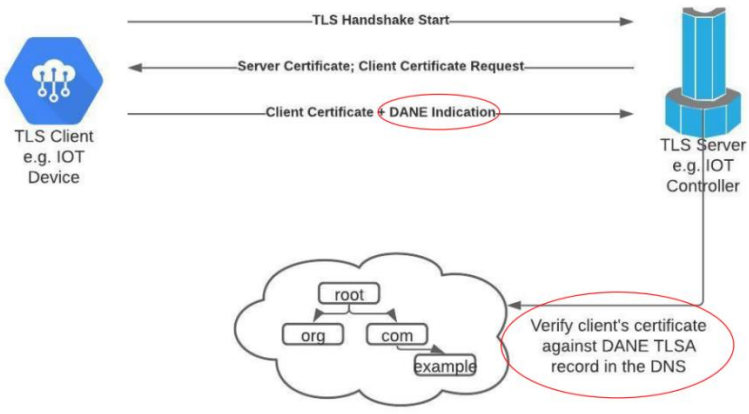
[deviceid]._device.[org-domain-name]

e.g.

a1b2c3._device.subdomain.example.net.

- a1b2c3: device identifier (could be multiple leftmost labels)
- _device: identity grouping label
- subdomain: organizational label (optional)
- example.net: organizational domain

架構如下圖：




工作小組目前對於草案的工作安排如下:

| | |
|---|---|
| | DANISH architecture document (9 months)<br>DANE for device certificates (current draft) (6 months)<br>DANE for TLS client authentication (current draft) (6 months) |
| 會議心得 | DANISH 工作小組的目標是在網際網路與 PKI 的基礎上強化 IoT 的服務安全性，而本計畫是基於電信網路架構發展編碼識別機制。 |
| 與本計畫關聯 | DANISH 工作小組的目標是在網際網路與 PKI 的基礎上強化 IoT 的服務安全性，包含安全驗證識別與命名空間的碰撞問題，因此與本計畫的目標有部分重合，值得參考借鏡並持續關注。 |

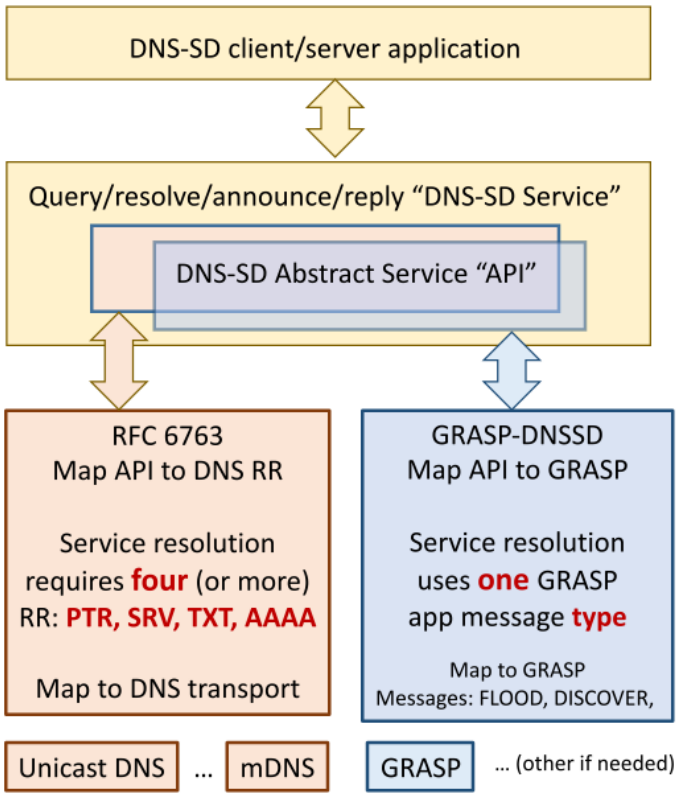
**(五)DNS 營運(Domain Name System Operations - Session I and Session II)**

| 日期 | 7/27(二) | 參與會議場次 | IETF 111 |
|---|---|---|---|
| 會議主題 | Domain Name System Operations - Session I and Session II | | |
| 會議過程 | 1. Domain Name System Operations - Session I 開場先由主席先介紹目前 Working Group 內相關的標準文件現況，接著安排以下的報告程序:<br>Current Working Group Business:<br>Guidance for NSEC3 parameter settings<br>https://datatracker.ietf.org/doc/draft-ietf-dnsop-nsec3-guidance/<br>Wes Hardaker, wjhns1@hardakers.net, 10 min<br>該講題摘要簡述 draft-ietf-dnsop-nsec3-iterations 草案工作，NSEC 是在 DNSSEC 機制中提供不存在域名的證明，NSEC3 避免了直接接露域名組的問題，該草案提供了 NSEC3 參數的設定指引，並討論定義其互動的指引。<br>• Glue is not optional<br>https://datatracker.ietf.org/doc/draft-ietf-dnsop-glue-is-not-optional/<br>shuque@gmail.com, 15 min<br>該講題摘要簡述 draft-ietf-dnsop-glue-is-not-optional 草案工作，Glue record 是在 child zone 中的名稱伺服器 address record，此次講題進行 Sibling Glue 的定義及範例，並且討論 Orphan Glue。<br>• Fragmentation Avoidance in DNS | | |

| | |
|---|---|
| | https://datatracker.ietf.org/doc/draft-ietf-dnsop-avoid-fragmentation/<br>fujiwara@jprs.co.jp, 15 min<br>該講題摘要簡述 draft-ietf-dnsop-avoid-fragmentation 草案工作，目前已有討論認為 DNS over TCP 是不安全的(ANRW 2021)，其存在著碎片攻擊的漏洞，然而 IP_DONTFRAG 選項目前未被任何 RFC 所定義，RFC3542 定義了相似的 IPV6_DONTFRAG，該草案提出對於相關 RFC 的更新。<br>• Revised IANA Considerations for DNSSEC<br>https://datatracker.ietf.org/doc/draft-ietf-dnsop-dnssec-iana-cons/<br>paul.hoffman@icann.org, 10 min<br>該講題摘要簡述 draft-ietf-dnsop-dnssec-iana-cons 草案工作，該草案更新 RFC6014 及 RFC8624 以增加對於新演算法的需求。<br>• New Working Group Business:<br>Survey of Domain Verification Techniques using DNS<br>https://datatracker.ietf.org/doc/draft-sahib-domain-verification-techniques/<br>shuque@gmail.com, 15 min<br>該講題摘要簡述 draft-sahib-domain-verification-techniques 草案工作，許多服務提供商需要使用者證明其能控制特定的網域，例如 Let's Encrypt，該講題提供了現有機制的調查，並提出了建議。<br>• DNSSEC automation<br>https://datatracker.ietf.org/doc/draft-wisser-dnssec-automation/<br>ulrich@wisser.se, 15 min<br>該講題摘要簡述 draft-wisser-dnssec-automation 草案工作，此次展示的對於名稱伺服器軟體功能的調查，包含 Bind、Knot 及 PowerDNS，DNS 服務提供商的能力調查(尚未全完成)，並且進行演算法及 Multi-Signer Controller 測試工作。<br>• DNS Access Denied Error Page<br>https://datatracker.ietf.org/doc/draft-reddy-dnsop-error-page/<br>danwing@gmail.com, 10 min<br>該講題摘要簡述 draft-reddy-dnsop-error-page 草案工作，該草案提出可以提供 error page URI 的機制，定義 Error Page URI EDNS0 選項格式。 |

| | |
|---|---|
| | • Structured Data for DNS Access Denied Error Page<br>https://datatracker.ietf.org/doc/draft-wing-dnsop-structured-dns-error-page/<br>danwing@gmail.com, 15 min<br>該講題摘要簡述 draft-wing-dnsop-structured-dns-error-page 草案工作，該草案為新提案，其目的為定義一個機制以闡述 DNS 過濾的原因，並提供 HTTPS URI 以取得詳細資訊，其以 JSON 作為範例。<br>2. Domain Name System Operations - Session II 開場先由主席說明議程安排，接著安排以下的報告程序:<br>• New Working Group Business:<br>Empty Non-Terminal Sentinel for Black Lies<br>https://datatracker.ietf.org/doc/draft-huque-dnsop-blacklies-ent/<br>shuque@gmail.com, 10 min<br>該講題摘要簡述 draft-huque-dnsop-blacklies-ent 草案工作，主要定義 Empty Non-Terminal Names 的 Synthetic Type。<br>• Current Working Group Business:<br>Liaison reply ISO 3166-1 user defined codes for private-use-tld<br>Suzanne Woolf/DNSOP chairs, 20 min<br>private-use-tld proposed next steps<br>Joe Abley/Roy Arends (combined with the above agenda item)<br>兩個講題摘要簡述 draft-ietf-dnsop-private-use-tld-01 草案工作，包含與 ISO 聯絡官的溝通，以及對於隱喻定義的討論。<br>• Prioritisation of WG activities (incl. discussion)<br>DNSOP chairs, 25 min<br>該講題首先彙整目前工作小組的 17 件 Active Internet-Drafts，並對這些工作進行排序討論。 |
| 會議心得 | 目前在 DNS 維運工作小組進行的相關草案中，與 DNSSEC 及安全性議題占大多數。透過 DNS 維運工作小組安排的相關討論，可以獲取目前 DNS 標準發展的現況與趨勢。 |
| 與本計畫關聯 | 透過 DNS 維運工作小組安排的相關草案討論，可以獲取目前 DNS 標準發展的現況與趨勢。 |

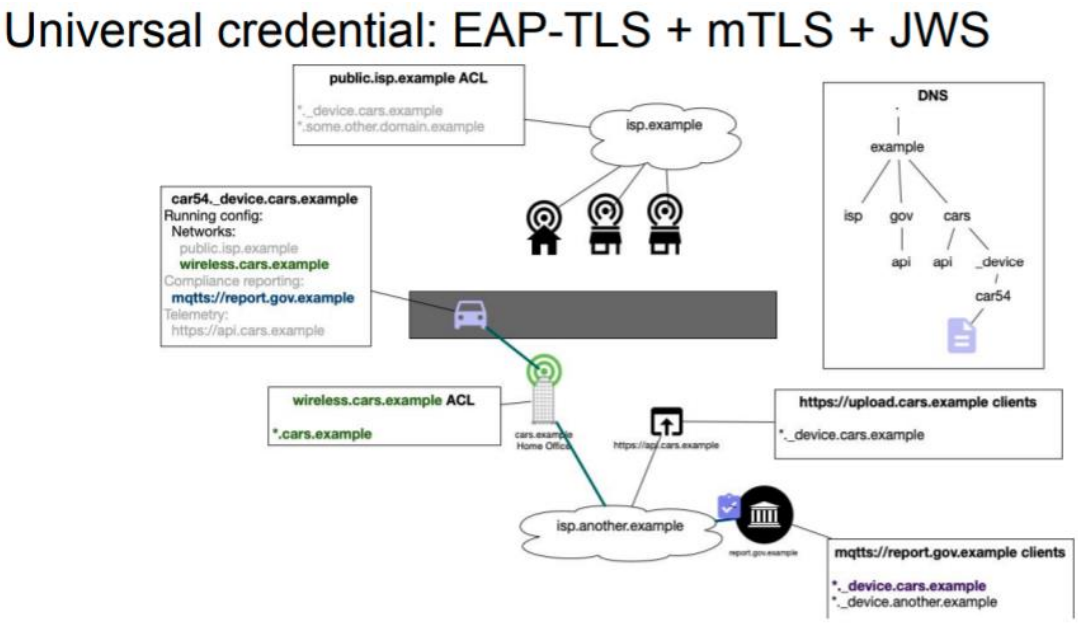
**(六)基於可擴展 DNS 的服務發現(Extensions for Scalable DNS Service Discovery)**

| 日期 | 7/28(三) | 參與會議場次 | IETF 111 |
|---|---|---|---|
| 會議主題 | Extensions for Scalable DNS Service Discovery | | |
| 會議過程 | DNSSD 工作小組議程共計一小時，議程安排如下:<br>Administrivia and Status Update: dnssd Chair slides (5 minutes)<br>首先由主席簡單開場並介紹議程安排。<br>DNS-SD Compatible Service Discovery in GeneRic Autonomic Signaling Protocol (GRASP)<br>* Toerless Eckert, 5 minutes -- may be extended by a few minutes if there is broad interest expressed<br>[draft-eckert-anima-grasp-dnssd](https://datatracker.ietf.org/doc/draft-eckert-anima-grasp-dnssd/)<br>該講題簡述摘要 draft-eckert-anima-grasp-dnssd 草案現況，其提出 DNS-SD 抽象服務 API 的概念以使用 RFC6763 或 GRASP-DNSSD，如下圖。<br>  <br> | | |

| | |
|---|---|
| | Service Registration Protocol for DNS-Based Service Discovery<br>* Ted Lemon<br>* [draft-ietf-dnssd-srp](https://datatracker.ietf.org/doc/draft-ietf-dnssd-srp/)<br>Advertising Proxy for DNS-SD Service Registration Protocol<br>* Ted Lemon<br>*[draft-sctl-advertising-proxy](https://datatracker.ietf.org/doc/draft-sctl-advertising-proxy/)<br>兩個講題合併簡述摘要 draft-ietf-dnssd-srp 及 draft-sctl-advertising-proxy 草案現況，draft-srp-10 已進入 Last Call 階段，draft-sctl-advertising-proxy-02 已準備等工作小組採納。 |
| 與本計畫關聯 | 透過 DNSSD 工作小組安排的相關草案討論，可以獲取目前 DNS 標準發展的現況與趨勢。 |

# 伍、第四場國際會議：IETF112 會議紀錄

| 日期 | 11/12(五) | 參與會議場次 | IETF 112 |
|---|---|---|---|
| 會議主題 | DANE Authentication for Network Clients Everywhere | | |
| 會議過程 | Deterministic Networking 議程共計 2 小時，安排如下:<br>Chairs Introduction - 10m:<br>議程開場首先由主席 Wes Hardaker 介紹工作小組的相關工作情況。<br><br>Use case presentations - 40m:<br>TLSA use case for DNS - Bill Woodcock - 10m<br>該講題的全名為" Use cases for DANE and bidirectional TLS authentication in the DNS"，在如下圖的 DNS publishing chain，如果透過 DNSSEC 的授權和驗證內容，正常的狀況下所有人看到的內容都一樣，但這並沒有解決 party authorization 的問題。我們需要能夠在任何 DNS transaction 中都可以驗證雙方的機制，如 TLS 雙向驗證，因此我們需要在 DNS 透過 DANE 發布 TLS client 及 server 的金鑰，並進行雙向的 TLS 驗證。<br> <br><br><br>Device-to-cloud - Ash Wilson - 10m<br>該講題講述 HTTPS use case，討論 HTTPS 及 mTLS 協定遭遇的 client identity 挑戰，Web app 通常位於 TLS-offloading balancer 後方，用戶端通常會有許多的 private PKI，造成 Identifier collisions 與 Impersonation 等安全問題，因此可以透過 TLS-Cooperative DANE client authentication 解決該問題。<br><br>EAP-TLS use case - Ash Wilson - 10m<br>該講題講述 EAP-TLS use case，討論 TLS client identity 及 EAP-TLS 的挑戰，EAP-TLS supplicant authentication 的問題是成本昂貴 | | |

| | |
|---|---|
| | 與互通的困難，因此可以使用 DANE 來提供 EAP-TLS supplicant ID，裝置的識別即透過 DNS。<br><br>Architecture document presentations - Ash Wilson - 30m<br>https://www.ietf.org/archive/id/draft-wilson-dance-architecture-00.txt<br>該講題講述 draft-wilson-dance-architecture-00(An Architecture for DNS-Bound Client and Sender Identities)草案的工作，其問題源自於 PKI-based client identity 限制多過，沒有互通性，並且操作繁重。根據 CSA, Identity and Access Management for the IoT Summary Guidance 的 Step 1a: Define a common namespace for IoT devices，但如果不去建立一個新的 namespace，而是使用現有的 DNS 該如何實現。透過 DANE 實現 Client Identity 的作法，主要將 PKI namespace 綁至 DNS，組織就能透過 pre-provisioned identities 獲取裝置，其使用 Autonomous Cars 作為範例:<br>  <br><br><br>Solution documents - Shumon Huque - 30m:<br>https://datatracker.ietf.org/doc/html/draft-huque-dane-client-cert<br>https://datatracker.ietf.org/doc/html/draft-huque-tls-dane-clientid<br>該講題講述 draft-huque-dane-client-cert-07 及 draft-huque-tls-dane-clientid-05 草案的工作，其目的是使用 DANE 驗證 TLS 連線的用戶端，使用案例是鎖定 IoT 裝置驗證與 SMTP 傳輸安全。其作法是 |

提出新的 TLS extension 以承載用戶端的 DANE identity，並且定義用戶端的 DNS 命名規則:

Format 1: Service specific client identity

_service.[client-domain-name]

e.g.

_smtp-client.relay1.example.com

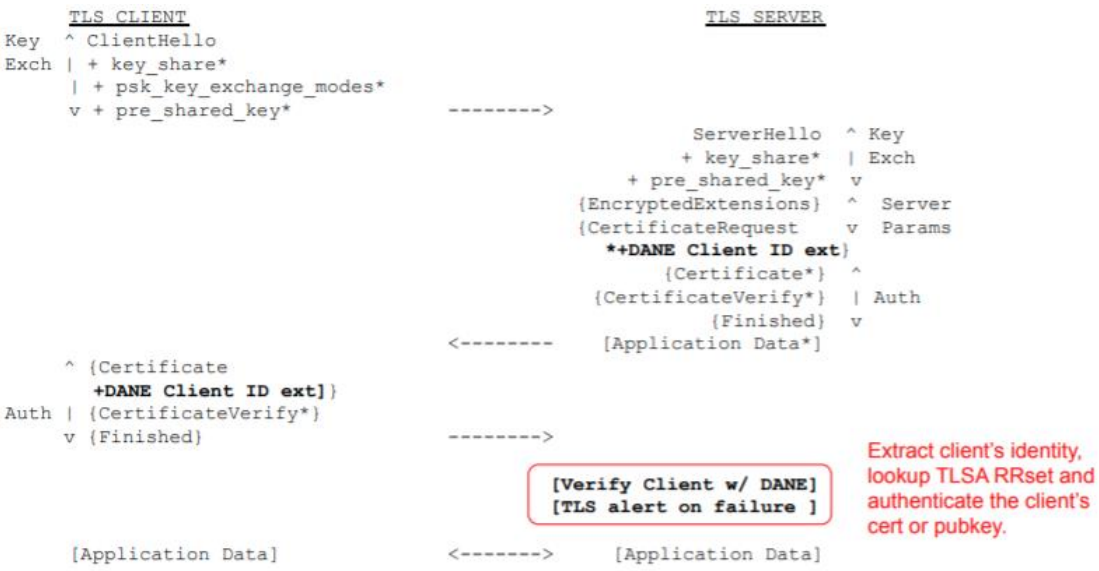
Format 2: (IOT?)

Device Identity [deviceid]._device.[org-domain-name]

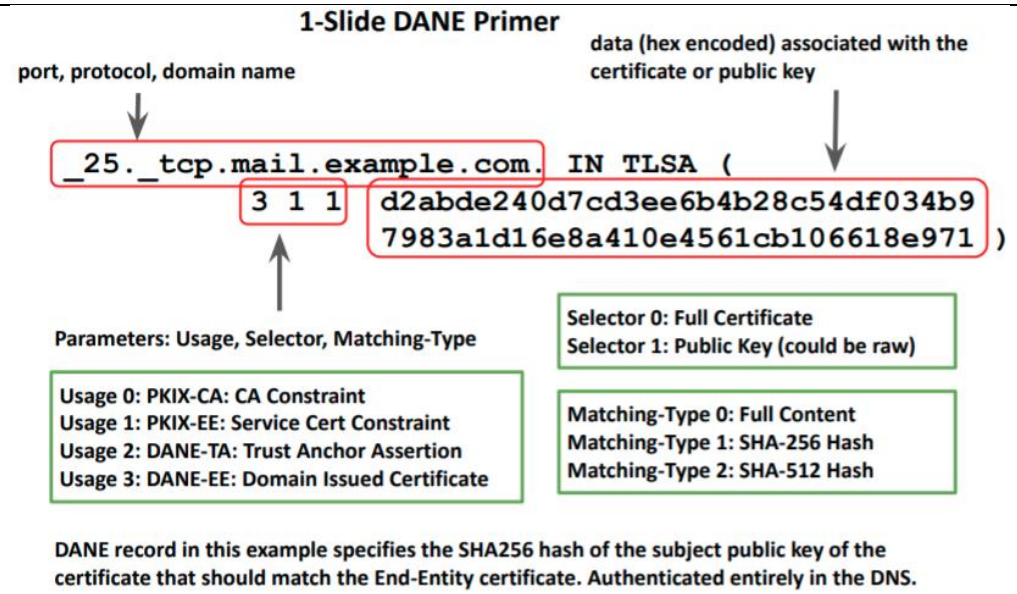
e.g.

a1b2c3._device.subdomain.example.net.

其協定如下:




DANE 的 record 如下:

| | |
|---|---|
| |  <br>在討論中也許多專家對於 record 的 TTL(Time To Live)及 key rotation 的問題進行討論，並提及後續將討論關於 namespace 的部分，最後主席採用線上舉手投票的表決以決定是否接受該兩草案，22 票通過 1 票不贊成 |
| 會議心得 | DANCE 工作小組的目標是在網際網路與 DANE 的基礎上提供用戶端或 IoT 的 identity，而本計畫是基於電信網路架構發展編碼識別機制。 |
| 與本計畫關聯 | DANCE 工作小組的目標是在網際網路與 DANE 的基礎上提供用戶端或 IoT 的 identity，包含安全驗證識別與命名空間的碰撞問題，因此與本計畫的目標有部分重合，值得參考借鏡並持續關注 |

# 陸、第五場國際會議：ITU-T 未來網際網路、有線網路及無線網路發展趨勢會議報告

## 一、 前言與目的

本場會議為 2021 年 ITU 數位世界開幕會議，會議中專家小組成員就如何開發和擴展作為所有連結背後的底層基礎設施網路，以高速、高可靠性的提供高質量、豐富的內容與服務為目標探討了從光纖到衛星、固定無線、後端骨幹網路、5G、網路自動化、基礎設施共享和新監管方法等一系列的技術和解決方案。

## 二、 會議議程

會議時間為 2021 年 9 月 1 日星期三，下午 13:30 至 14:45 CET 時間。

| 未來網際網路、有線網路及無線網路發展趨勢 | |
|---|---|
| 時間 | 演講主題 |
| 13:30 – 13:35 | Phan Tam：會議引言 I |
| 13:35 – 13:40 | HouLin Zhao：會議引言 II |
| 13:40 – 13:55 | 基礎設施 |
| 13:55 – 14:05 | 自動化網路 |
| 14:05 – 14:35 | 無線、光纖和衛星替代方案 |
| 14:35 – 14:45 | 5G 商業案例 |
| 13:45 – 13:55 | 重新考慮監管方法 |

Phan Tam 先生現任越南信息通信部副部長。 他自 2015 年起擔任該職位。他曾被任命為越南電信管理局局長和副局長，協助信息和通信部部長。Tam 先生擁有法國波爾多大學的博士學位。

HouLin Zhao 先生於 2014 年 10 月在韓國釜山舉行的第 19 屆全權代表大會上當選 ITU 秘書長。 2015 年 1 月 1 日上任。趙先生 1950 年出生於中國江蘇，畢業於南京郵電大學，並擁有英國埃塞克斯大學遠程信息處理碩士學位。 2007 年至 2014 年，他擔任 ITU 副秘書長，與 ITU 其他當選官員密切合作，有效協助 ITU 秘書長管理國際電聯戰略計劃的實施和 ITU 的運作。ITU 秘書處，特別是為了提高組織的透明度和效率。他負責實施重要創新，包括推廣向全球學術界開放的新會員類別、內部效率措施，例如轉向近乎無紙化的工作環境、更多地使用遠程參與系統，以及增加銷售和成本回收服務的收入。他還密切關注成員驅動的優先事項，包括維持和擴大 ITU 對無障礙獲取、多語言以及多利益相關方廣泛參與 ITU 工作的承諾。在此之前，趙先生於 1999 年至 2006 年擔任 ITU 電信標準化局（TSB）主任。與行業成員合作，同時加強促進 ITU 在全球 ICT 標準制定方面的領導地位。 1986 年至 1992 年，趙先生在當時的 CCITT 擔任高級職員，1993 年至 1998 年在 TSB 擔任高級職員。在擔任 ITU-T 研究組顧問的職責中，他是與其他國際技術機構（包括 ISO 和 IEC）合作的協調員。在加入 ITU 之前，趙先生曾在中國郵電部設計院擔任工程師，積極參加了中國電信標準和國家規劃專家會議，並作為專家參加了 CCITT 研究組會議。中國代表。他為許多著名的中國技術出版物撰寫了重要文章，並於 1985 年獲得郵電部科學技術成就獎。作為 ITU 第 19 任秘書長，趙先生致力於通過鼓勵更多來自世界各地的行業成員和學術界加入 ITU 大家庭，進一步擴大 ITU 的社區。他還發起了一項更加開放的政策，以歡迎其他利益相關者和合作夥伴，並促進中小企業更多地參與聯盟的工作。

Vaishali Rastogi 女士 是波士頓諮詢集團技術、媒體和電信 (TMT) 業務的全球領導者。她曾擔任多個領導職位，包括領導 BCG 在東南亞的業務—涵蓋所有東盟市場 - 在此期間，她帶領業務快速擴展到數位化、分析和轉型。Vaishali 還是 BCG 全球銷售工作的聯合領導者、快速發展經濟體

的市場推廣領導者以及 BCG 營銷、銷售和定價實踐的亞太區領導者。她一直是 BCG 全球執行委員會的成員。Vaishali 在幫助許多市場的電信公司、技術和其他面向消費者的企業轉型方面擁有豐富的經驗。她發表了多份關於東南亞數位化轉型、上市和消費者的報告。她還致力於研究 COVID-19 後的新現實將如何影響 TMT 的不同子行業，以及公司如何反彈並重新構想其商業模式和運營以在逆境中抓住優勢。

MiroSalem 先生作為樂天移動的人工智能和自主網絡全球負責人，他的使命是實現自主網絡的願景，從研究到產品。 Miro 的職業生涯始於一些最大的移動網絡供應商，即 Sprint、AT&T 和 Verizon。 在加入樂天移動之前，他創立了 3TEN8，這是一個人工智能和機器學習平台，可幫助工程師預測和診斷無線網絡的退化和中斷； 該公司被移動運營商和投資者評為排名第一的人工智能新創公司。 他熱衷於追求技術和社會進步的實用創新。

Jocelyn Karakula 先生於 1987 年加入法國電信，並在 Ecole Nouvelle d'Ingenieur en Telecommunications (Lille-France) 獲得工程師學位。他於 1996 年加入法國電信國際網絡部，擔任專案經理，負責傳輸和交換領域的關鍵技術改造。從 2000 年起，他進入 Orange 的國際批發部門，首先擔任服務交付總監，然後從 2005 年起擔任國際批發產品和服務的銷售總監。2013 年，Jocelyn 被任命為 Orange 中東和非洲的副 CTIO，並於 2021 年 2 月被任命為 Orange MEA 的 CTIO，覆蓋 18 個國家/地區的 ITN 區域。

Aarti Holla-Maini 女士 自 2004 年以來一直擔任 ESOA 秘書長。她是世界經濟論壇全球未來空間理事會、WEF 全球 5G 聯盟網絡和 WEF 基本數位基礎設施和服務網絡的成員。在 Aarti 的領導下，ESOA 及其成員 CEO 帶頭努力展示衛星通信對建設更具包容性和安全性的社會的好處—這對於彌合世界數位鴻溝、實現聯合國可持續發展目標和實現 5G 生態系統至關重要。自加入該協會以來，Aarti 帶領 ESOA 從一個歐洲協會擴展到一個代表 22 個全球和區域衛星運營商利益的協會。她直接向他們的首席執行官報告。Aarti 在航空航天行業擁有 23 年的經驗，從德國的戴姆勒-奔馳航空航天/EADS（現為空中巴士）開始。 2000 年，她搬到布魯塞爾，代表空中巴士公司在歐洲衛星導航計劃：伽利略。Aarti 擁有法國 HEC

和美國紐約市斯特恩商學院的工商管理碩士學位。她於 1995 年獲得英國最高法院的律師資格，持有倫敦大學國王學院和德國帕紹大學的德國法學士學位，2:1 等級法學學士榮譽學位。她也是國際空間大學的校友。 Aarti 是英印裔，擁有英國和比利時國籍。她住在布魯塞爾，有 3 個孩子，會說 5 種語言。

Neha 女士 是 Astrome 的聯合創始人兼首席執行官，Astrome 是一家科技創業公司，通過其獲得專利的毫米波電信無線電和衛星通信產品加速 5G 和農村電信基礎設施的部署。 她擁有德克薩斯 A&M 大學的博士學位和印度科學研究所 (IISc) 的航空航天工程碩士學位。 在攻讀博士學位期間，她獲得了崇塔基金會 (Zonta Foundation) 頒發的著名的 Amelia Earhart 獎學金。 獲得博士學位後，她在佛羅里達大學與美國空軍研究實驗室合作，擔任博士後研究助理。 2020 年，Neha 獲得了 Unreasonable Fellowship，這是一個由精選的成長階段企業家、機構和投資者組成的全球社區，旨在以盈利的方式解決緊迫的全球問題。 她還是 WEQ 研究員，該獎項由 AnitaB.org、USISTEF 和印度政府聯合頒發。 她還是國際電聯 EQUALS 獎學金的獲得者。

Konstantinos Masselos 教授於 2018 年 2 月被任命為希臘電信和郵政委員會 (EETT) 主席。2006 年加入伯羅奔尼撒大學，現任信息與電信系教授，計算機系統研究組組長。 2012-2017 年任上述大學校長。他還曾擔任計算機科學系主任（2009-2011）、副校長（2010-2012）和研究委員會主任（2010-2013）。2010-2016 年期間，他擔任倫敦帝國理工學院電氣與電子工程系榮譽講師。此外，從 2005 年到 2008 年，他在同一所大學擔任數位系統講師。從 2001 年到 2004 年，他加入了希臘的 Intracom Telecom SA，在那裡他參與了有關無線通信系統的研究和開發項目。他參與了多個研究和開發項目，並在各個行業、初創公司和公共組織中擁有諮詢經驗。自 2005 年以來，他還經常作為專家參與歐盟委員會不同部門的工作。 2015 年至 2017 年，他是歐洲科技合作科學委員會 (COST) 組織的成員。他的主要研究興趣包括編譯器、高級綜合（HLS）、FPGA、高性能計算和空間計算系統。他在國際期刊和會議上發表了 120 多篇論文。Konstantinos Masselos 教授在希臘帕特雷大學獲得電氣工程學士學位（1994 年），並在英國曼徹斯特

科技大學獲得 VLSI 系統工程碩士學位（1996 年）。 2000 年 4 月，他與比利時大學間微電子中心（IMEC）合作，獲得希臘帕特雷大學電氣和計算機工程博士學位，1997 年至 1999 年在那裡擔任研究員。

Mikael Rylander 是 Nokia 的技術領導官，專注於在軟體驅動的開放網絡系統時代引導技術創新。

## 三、 會議過程及內容

本次會議將著眼於所謂的有線、無線在全球範圍內的網絡下一步發展。現在我們知道網路在這場大流行中發揮了巨大的作用，如果疫情發生在 2000 年，只有不到 0.2% 的勞動力能夠遠端工作，不到 1%的人可以擁有真正的寬頻。因此，就真正使我們能夠在家工作與推動教育而言，網路絕對重要。

在基礎設施方面，作為網路和連接提供商而言，同時關注能效技術和 CSR 參與是重要的。產業界應該專注於開發更多高效鋰電池並且更加適應太陽能，具適應性的關鍵 AI 算法可以預測電力系統中的某些操作。第二，有時非常難以到達的一個或多個地區，必須推廣一些技術，使遠程部署升級發布可以順利進行。開放式運行可能是一項非常有前途的技術，這取決於處理能源效率的方式以及達到成本效益水平的方式。在商業部分，目前正在推動並研究的是低頻段微波。低頻段意味著低於 6 GHz，包括 LTE 中繼後端骨幹網路。因為通過大容量呼叫獲得 30、40 或 50 公里的可能性非常重要。第二：衛星。具有傳統系統的衛星無法真正處理這些地區的可持續數位包容性。地球軌道早期衛星具有未來發展性，具有一些可以盈利的商業模式，以便以低延遲和顯著容量提供服務。對我們來說非常重要的是解決這個問題，也許可以用額外的參與者來改變模型，比如可以處理整個事情的完整集成商。另一方面是數位包容和能力挑戰。這四種技術並行是已經確定的，因此其面臨著巨大的挑戰。首先是通過使用已經使用的 DSS 技術進行優化來管理頻譜和容量，在未來幾個月或幾年內會有更多的技術公告。另一件事是管理所有這些複雜的自動化， AI 算法也將會是關鍵。我們無法在如此復雜的傳統模式下進行管理，比如說宣布的網路和現代網絡。那麼在此基礎上解決的挑戰是什麼?非洲會保留這個 2G、3G 網絡多年是因為 4G 和 5G 的滲透。4G 設備確實存在問題，實際上這與智能手機對

低收入人群的負擔能力有關。因此，期待技術將解決並能夠降低生產和製造的價格，以促進和發展。最終這可能會對內部連接和服務的使用產生非常重大的影響。

作為一家毫米波無線公司來說，為農村地區開發解決方案，長達到 40 到 50 公里的距離，後端骨幹網路(Backhaul)無法使用或非常微弱。所以一般認為為毫米波無線後端骨幹網路與非授權頻段後端骨幹網路的組合也基本上是低頻與微波。微波無線電可以達到更遠的距離和可能更低的吞吐量，以及可以達到中等距離但更高吞吐量的毫米波無線後端骨幹網路。對於大多數這些情況，這兩者的組合可能是一個非常好的解決方案。一旦你向附近的人口提供容量，重要的是降低網路的成本和穩定性，而且 Wi-Fi mesh 網絡是一項非常好且有趣的技術。事實上，將低頻和高頻無線解決方案結合起來解決後端骨幹網路和接入問題可能是一個有趣的組合。最後當然 LEO（低地球軌道）星群是解決後端骨幹網路問題的一個非常好的替代方案。

世界上有五分之二的人口可以上網，還有 13 億孩子在家中沒有互聯網連接。自主運營自動化網絡所創造的經濟效益是我們能夠在以前無法解決的領域解決這些問題。所以必須發生的根本轉變是網路正確運行的經濟學，我們都顯著降低了無線和訪問互聯網的成本。它只能通過改變經濟來改變我們做事的方式來做到這一點。我們真正談論的是一些設計原則，如果我們擁有就可以創建自治網絡，並擁有一個可以訪問互聯網的世界，以及所有人都擁有的相同特權，所以它始於經濟學。如果我們能夠改變經濟，將獲得自動化網路解決方案，從而為每個人提供所有人都擁有的訪問權限。在未來兩三年內將會出現許多自動化網路。但不會在一年內從現在的狀態發展到 100 個自動化網絡。這就像進化的運作方式。這是一種進化，隨著時間的推移將會到達那裡。在未來兩年內實現一定程度的自動化網路。

現今我們經歷了電信網路向軟體化的轉變，這也嚴重影響了電信網絡的部署和成本。所以接著需要關注雲端引入的軟體定義網絡硬體軟體化趨勢，這些趨勢正在討論整個電信行業，品牌專用硬體的時代變得非常快。過去的事情和商品服務器甚至正在接管電信核心網絡中最傳統和遺留的功能，對它們進行抽象和虛擬化。因此，軟體定義網絡和網絡功能虛擬化領域的

發展成本更低。並簡化現代電信基礎設施的設置和運營，這在傳統上一直是該行業新進入者的主要市場入口。在接下來的四五年內，這一趨勢引發的該領域的競爭將對電信提供商施加壓力，他們拒絕接受精進運營模式，無法適應並專注於更適合其專業知識和企業文化的細分市場。所以我們的網路一代給我們帶來的成本需要密集的光纖部署。但這可以通過謹慎的資源共享和規劃以及降低核心網絡運營成本來實現，因為它們成為軟體定義的商品並得到虛擬化。

光纖到戶(FTTH)確實是一項關鍵技術。這不是當今唯一有意思的存取技術。因此，研究工作已經提供了許多連接技術，它們在部署時間和成本、維護覆蓋範圍、功能速度延遲可擴展性以及面向未來的客戶端設備成本方面呈現出不同的權衡。因此，沒有一種技術解決方案足以適用於任何特定案例或國家。高質量且價格合理的連接通常需要混合技術解決方案。在我看來，考慮到其國家地區的具體特徵，例如形態人口分佈季節性問題等。以希臘作為此方面的例子。組合解決方案將使用正確的技術組合來優化連接基礎設施的部署和維護成本。消費者價格也是如此。從這個角度來看，將會看到許多技術是實現高質量和仍然負擔得起的連接目標的關鍵光纖到駐地（用戶所在地）技術提供高速規模、性能可靠性與低能耗，並且似乎是人口稠密的強大選擇區域固定無線接入，但也使用未經許可的毫米波無線電，如 60 GHz 頻譜似乎是光纖到家庭或光纖到場所提供高速但也更容易部署。這非常適合郊區或農村地區。我們不應忘記衛星寬頻網絡，包括由低延遲低地球軌道 (LEO) 衛星提供的網絡，它們確實提供了另一種有希望的選擇。也許今天我們認為低地球軌道衛星網絡是農村地區的一個不錯的選擇。但該領域的快速技術發展將使低軌道衛星網絡能夠比農村地區做得更多。然而所有上述固定接入技術都有一個共同點， 5G 行動網路也是。所有這些情況都需要光纖網路。因此，除了從光纖到駐地部署之外，應該牢記光纖到天線的部署，尤其是在預計基站密度將激增的 5G 環境中。因此，光纖到戶到 5G 融合需要在不同網路之間分擔網路部署成本，這使得這些網路的程式碼設計成為必要，以優化網路部署成本。

如果需要寬頻，尤其是在需要高速和大範圍覆蓋的地區，光纖到戶確實是最好的選擇。光纖到戶是非常有未來性的，目前在業界以 2.5 Gbps 的

速度脫穎而出,現在廠商提供 10 和 25Gbps,並正在開發 50 和 100Gbps。光纖到戶的運營成本也是最低的。如果在工廠外部查看實際網路它是被動式的,因此功耗非常低。一旦部署該網絡還可以用於為其他客戶提供服務,不僅是住宅或小型企業,還包括 5G 小基地台。這是一種點對多點技術,主要是全球 95% 的布建都是點對多點。所以實際上可以使用新技術從銅軸電纜線中擠壓出 100Mbps。但我們也可以看到,在電信公司中,大多數人都有一個策略,導致部署越來越多的光纖到戶。與有線電視運營商一樣,他們有一點優勢,因為他們擁有自己的有線電視網絡,但他們繼續投資和升級,但我們現在也可以看到,已經提到的固定式無線接入網路(FWA)光纖部署的理想補充,適用於光纖業務不適用的地區,可能是低密度的農村地區或部署光纖需要很長時間的地區。綜上所述,光纖到戶是目前發展中的寬頻主流技術。

事實上,衛星已經是一種經濟高效的方式,可以讓人們上網,尤其是那些地面網路無法覆蓋的人。現在正看到技術的巨大演變。但它既存在於太空,也存在於地面。這正在增加為整體連接生態系統提供的衛星服務。更高容量的服務,每位元成本正在下降,當然 NGSO 系統將帶來更低的延遲,這也是某些應用程序所需要的。到目前為止,後端骨幹網路一直是討論的重要組成部分。事實上,這是衛星多年來所做的事情,但不僅僅是行動通訊的後端骨幹網路。還有社區 W-iFi 解決方案的後端骨幹網路,這對於讓人們上網越來越重要。但就產業的發展而言,要注意兩件事。首先,多項試驗表明 5G 後端骨幹網路已經可以通過衛星完成,並且在 3GPP 系統架構組內的非地面網絡 NTN 也正在發生通過衛星實現特定的 5G 後端骨幹網路功能,這些功能將在明年第 17 版中出現.但值得注意的是,地面部門投資衛星的勢頭確實證明了移動運營商對後端骨幹網路的重視,無論我們是否看到 Barti Airtel(印度電信業者) 將其在 Oneweb 上的投資翻倍,這是眾所皆知的,甚至是像匈牙利 4iG 這樣鮮為人知的投資,收購了以色列衛星運營商 AMOS Spececom 的多數股權。這一切都非常有說服力,我認為這有不同的原因。首先是需要無縫連接體驗,這是許多 5G 垂直領域的特徵,無論談論的是互聯交通、移動醫療保健、全球資產跟踪,還是確保出於安全原因可能非常關鍵的軟體更新,以確保這些可以達到他們需要的所有設備或車輛,無論他們在哪裡。第二個原因是需要推動增長。所以我們知道移動

運營商面臨著推出 5G 的巨大壓力。但是現在隨著疫情大流行也確實將連接擴展到更多人，而這兩個目標都需要巨額投資。這意味著運營商需要新用戶，因此連接未連接的用戶是衛星解決方案的一個明顯組成部分。衛星還可以幫助優化行動網路的效率，正如所說的多播，將內容廣播到基地台到邊緣地帶。並且透過此方式將移動網路從大量內容中卸載下來，這一部分帶給運營商很少的收入。行動網路運營商對衛星如此感興趣的最後一個原因正是 3GPP 中技術的發展和標準工作。這兩種想法都將使將衛星和傳統網絡集成到經常聽到的 5G 網路中變得更加容易。所以所有關於電信部門融合的說法都表明移動固定和衛星之間的傳統分歧正在緩慢消散，但可以肯定的是，人們對衛星的興趣日益增加，這在很大程度上證明了連接的最佳解決方案確實存在技術結合，匯集不同技術的優勢，共同提供高彈性、更高的可用性，並為更多的用戶提供更高的可用性。所以是的，衛星絕對是更廣泛的電信生態系統的一部分，行動網路運營商更多地使用它們，不僅用於後端骨幹網路，而且行動網路運營商越來越多地提供更加可靠的服務。例如，從英國的 BT 了解到，將衛星作為其網絡的一部分確實可以增加其網絡的正常運行時間。在疫情大流行期間，看到了很多演變，一些成員看到新訂閱增加了 50%，事實上，衛星運營商工程師被指定為必不可少的工作人員，僅僅是因為非常需要連接，這是建立連接的唯一方法，因此，由於對高吞吐量衛星的大量投資，新訂閱數量和提供的容量都有了很大的增加。正如 Startlink 這樣的 LEO 寬頻時指出的那樣，是的，它在那裡。但它現在僅處於 beta 測試階段。這當然不適合發展中國家。即使它可以擴展，它和消費設備的價格可能會下降。必須記住，GEO 與否 NGSO 的設備基本上是相同的，移除了多個組件，因此 GEO 設備也會隨著對衛星寬帶需求的增加而擴展，而且它會更便宜。

固定無線接取網路可以成為光纖網路的有價值補充，特別是在沒有固定基礎設施的地區，實際上可以成為占主導地位的寬頻提供商技術。因此，固定無線接取將在彌合數位鴻溝方面發揮關鍵作用。如果您開始向網路加載數據。這對無線電網絡是一個挑戰，尤其是當您還想提供類似光纖的速度時。可以採用幾種策略，使用高增益固定無線 CPS，這意味著將以有效方式使用無線電容量。您可以使用 MIMO 高階或 MIMO CPS。這將為每個小區提供更多的用戶。當然可以在這裡使用更多的頻譜，或許可以以一

種沒有在全球大規模部署的方式來談論新技術。毫米波就是這樣一種技術。可以使用更多的頻譜。還有多用戶大規模 MIMO 類型的應用。我們看到了固定無線接取的未來。但我們不應忘記也可以使用逐步方法修復無線訪問。如果不想擁有非常高的速度。可以使用室外 CPS，使用直接 LoS，將獲得強大而高效的固定無線網絡。以諾基亞為例，在哪裡引入它來連接肯尼亞以前沒有連接過的學校，所以這是諾基亞、 Safaricom 和 UNICEF 之間的合作。因此，您可以使用固定訪問作為逐步方法。當然，您可以使用我們在此處討論的許多技術來完成後端骨幹網路。

固定服務可以發揮作用並且是衛星的補充。與傳統的固定業務不同，FWA 顯然是為了指向多點服務。這意味著它可以擁有採用 FWA 技術的基地台，可以同時指向更多用戶，如學校、網咖、家庭等。但儘管 FWA 可以連接更多用戶，幾點需要注意，它並不像我們對 4G、 5G 移動連接所期望的那樣移動。最重要的是，當查看 FWA 的實際部署時。到目前為止，它實際上只發生在城市地區。僅僅是因為它需要連接到主幹網路。所以在發表關於 4G 的聲明時需要小心，5G 必須具有彌合數位鴻溝的潛力。這肯定不是作為獨立的解決方案，因為它們都需要是後端骨幹網路，為此需要混合使用包括衛星在內的技術。在沒有光纖的地方非常好， FWA 真正做的首先是幫助運營商應對沒有光纖的地區的容量需求。但它並沒有以任何有意義的方式擴展城市地區以外的連接範圍。其次，它允許運營商在不使用移動頻譜或等待新的 5G 移動頻譜分配的情況下提供更多連接。因此，在一個聲明中談論 FWA 和數位鴻溝是困難的，而且這對政策制定者尤其具有誤導性，完全談論數位鴻溝的唯一方法是指混合技術。

5G 的市場，在亞洲、美國和西歐都看到了強勁的進展。這是由 CSPs、WEB-scales 和企業公司之間的新夥伴關係驅動的。CSP 現在正在努力重新定位和重新調整其組織能力，這是為了能夠解決和學習如何將 5G 技術注入 B2B 環境。可以看到，當涉及到新的基礎設施新技術時，該行業正在學習如何以相當驚人的速度集成和操作高級 SLA(Service Level Agreement)，實際上是自然而然的。有一個學習曲線需要克服。還可以重申網 Web-scales、CSPs 和所有從事該行業的 OMS。目前可看到很多新的合作正在發生，其中很好的例子是德意志電信威瑞森和 AT&T。可以看到新架構和運營模式

的巨大適應性。這將實現以前從未見過的規模的創新配置和性能。那麼現在可以從 5G 中看到什麼好處呢？每位元的功耗。因此，可以以更低的功耗在網絡中傳輸更多的位元。我們已經討論了固定線路接取技術，在這些應用中，都可以使用更多頻寬，但也可以使用 5G 中的新頻譜效率功能。5G 核心網可用於切片和性能被認為是關鍵的地方。我們有提供電力天然氣、電動汽車充電、網路電視的公用事業公司的例子。他們有一家特定公司，擁有私人 5G 的區域 3.7GHz 許可證。並且在他們的網絡中進行內部感知和遠程控制。而且他們還為企業和企業內部提供固定無線連接。引擎整體維護我們談到了 Covid 疫情大流行。要讓訓練有素、有能力的工程師飛出去進行發動機檢查是非常困難的。對於航空公司而言，例如一家大型歐洲航空公司使用 5G AR/VR 技術檢查製造商的發動機。在北美，可以看到地方政府正在購買少量頻譜，以覆蓋未得到服務的社區和企業。這是為了彌合消費者和企業的數位鴻溝，我們可以在賓夕法尼亞州、俄亥俄州和科羅拉多州的社區中看到這一點。我們可以看到很多大學校園都啟用了 AR/VR 功能。北美的所有 CSP 都為體育場館提供增強的運動體驗。還有一段無人機視訊，可以在其中看到 5G 支持 2D 和 3D 映射。在亞洲，日本、新加坡、韓國等多家汽車製造商（如本田豐田）正在使用 5G 來增強其工廠製造流程。接下來將在韓國、日本、紐西蘭使用 V2X 毫米波頻譜（在這些情況下為 28GHz）進行自動駕駛試驗。諾基亞 CSP 也在建立聯合創新實驗室和開放創新實驗室，例如諾基亞或與美國的 T-mobile 合作。但可以肯定的是，目前正處於用例演變的新領域的開端。在工業環境中看到合工業環境中的高性能的超低延遲。在這裡可以看到主導產業是製造業公用事業建設部分和機場。該行業將使用 6G 以下頻譜毫米波的組合。CSP 有機會通過解決校園和高性能工業環境在 18 個月內推動高達 8% 的收入增長。

在邁向 6G 的過程中，還沒有看到 5G 的全部潛力。將繼續看到 5G 可能向 5.5G 演進，速度更快，延遲更低，可靠性更高。所以仍然看到很多關於 5G 及其演變的想法，也會以某種方式看到人工智能與 5G 的融合。所以將從萬物互聯走向智能萬物互聯。但與 5G 的這種演進並行，我們已經開始研究 6G，其中的挑戰或多或少與所看到的 5G 相似。所以想要更高的速度、更高的數據速率、更好的覆蓋範圍、使用毫米波頻率等。因此，從 5G 中吸取的經驗教訓將對 6G 的發展非常有用。6G 戰略應該優先考慮電

信、微電子、光子學、軟件和開發高質量人力資源資本以及這些領域的知識產權等領域的研究。當然，監管機構應該創造一個友好的環境，支持創新並支持圍繞新技術的 6G 商業模式。

## 四、 總結

從本次會議中各位小組專家成員對於未來網際網路、有線網路及無線網路發展趨勢從各自的領域進行經驗分享以及對於未來發展的想像進行闡述。首先就網路基礎設施的發展應對付能力的挑戰進行討論，專家提到需要從節能與電力系統管理著手，如果能滿足成本效益與能源效率挑戰，提供遠程部署的相關技術在偏遠地帶與農村地區可能會非常有前途。另外，關於頻譜的成本以及設備的製造成本如何降低將會大大影響網路的推廣。此外，在無線、光纖與衛星的替代方案議題中，各位專家提到 FTTH 極具未來性，在許多國家網路尚未普及的地區距離可用的光纖網路範圍還有一段距離，使用無線網路及衛星網路可將此一部分彌補起來，在未來此三種技術的組合搭配可以為更多用戶提供更高的彈性與可用性。在 5G 商業案例的議題中，專家們提到了在西歐、亞洲及美國市場正在利用 5G 建立新的 B2B 環境，在大學校園、智能工廠、機器人技術、機場與海港等應用領域找於新的機會。在新的監管方法議題中，專家們呼籲監管機構需要支持網路和頻譜共享以減少在頻譜許可的支出從而鼓勵網路未來的發展。在最後 ITU 秘書長趙先生對於技術與資源共享的互補連結，特別是關於基礎建設的連結可負擔性表示贊同，並強調需要好好利用現有容量包含網路共享、衛星與海底電纜。並且呼籲中小企業提供 IoT 物聯網解決方案與應用，以推動網路使用及增加收入並且平衡運營商之間的資源共享與競爭。投資新技術和改善基礎設施對於網路世界的發展至關重要。

# 柒、第六場國際會議：ITU-T 未來 5G 網路及標準發展會議報告

## 一、 前言與目的

本場會議將從全球和不同利益相關的角度來探討“5G 後”時代，未來網路標準化的期望和挑戰。本場會議講者由系統供應商和行動通訊營運商組成的專家小組，分享他們對未來網路發展、標準化、問題和前景的看法。

而本場會議內容將探討以下主題：

- 5G 在部建及相關企業努力下的全球市場趨勢方面的當前狀態如何，相關企業將如何從 5G 推出朝向 6G 及更高版本？
- 未來的網路將提供哪些新服務，這些服務將如何改善全世界人們的生活
- 實現未來網路的要求是什麼，包括極高的比特率、低延遲和低功耗？
- 標準化在提供未來網路方面應該扮演什麼角色，後 5G 時代的藍圖是什麼樣的？

## 二、 會議議程與講者介紹

會議時間為 2021 年九月十日星期五，下午 13:30 至 14:45 CET 時間

| 未來 5G 網路及標準發展 | |
|---|---|
| 時間 | 演講主題 |
| 13:30 -13:35 | Memiko Otsuki：未來 5G 網路及標準發展會議引言 |
| 13:35- 13:45 | Masayoshi Shintani：日本的後 5G 的戰略 |
| 13:45- 14:00 | Seizo ONOE：對新一代和全球可持續發展的市場預測 |
| 14:00- 14:15 | Erik Ekudden：如何成為通往 6G 之路 |
| 14:15- 14:30 | Durga Malladi：5G 與後 5G 的市場應用 |

| | |
|---|---|
| 14:30- 14:45 | Ryosuke Takahashi：數據的隱私洩露的加密機制與 Quick MPC |

- Memiko Otsuki 女士是日本總務省 (MIC) 全球戰略司的助理司長。在其任職期間，她一直為國際電信的多項活動做出貢獻，包括國際電信理事會、國際電信活動、大會和全會及其籌備會議。最近，她被任命為 APT WTDC-21 的工作組主席。Memiko 女士在電信/ICT 領域擁有超過 15 年的專業經驗，並且在政策和監管問題方面擁有專業知識。此前，她曾擔任 NTT DOCOMO, Inc.企業戰略與營運商規劃部與監管事務辦公室聯絡員，積極參與國際政策和標準化工作，搭建政府與手機企業的橋樑。Memiko 女士擁有國立澳大利亞大學（澳大利亞堪培拉）的公共政策碩士學位和國際基督教大學（日本東京）的商業管理專業文學學士學位。她目前正在九州大學（日本福岡）攻讀經濟學博士學位。
- Masayoshi Shintani 先生自 2020 年 9 月起擔任日本總務省 (MIC) 國務大臣。他於 2001 年開始了醫生職業生涯，並曾擔任醫院院長。在工作過程中，開始相信正確的政策對於改善社區的健康和福利以及所有公民的生活質量至關重要，並於 2012 年首次當選眾議院議員 (HR) .他帶來了豐富的健康和福利經驗，曾擔任多個高級職位，包括自民黨青年部副主任；自民黨國土交通旅遊司副司長；自民黨厚生勞動省副廳長；自民黨衛生福利相關組織委員會主席；土地、基礎設施、運輸和旅遊委員會主任、人力資源和；厚生勞動省議會秘書。Masayoshi 先生畢業於帝京大學醫學院和東京大學經濟學院。
- Seizo ONOE 先生是 NTT CORP. 的標準策略辦公室主席和 NTT DOCOMO, INC. 的研究員。在擔任現職之前，他於 2015 年 6 月至 2021 年 6 月擔任 DOCOMO Technology, Inc. 總裁。 2012 年 6 月至 2017 年 6 月，Seizo 先生，擔任 NTT DOCOMO 首席技術官兼執行副總裁兼董事會成員。 2002 年 7 月至 2012 年 6 月，他擔任 NTT DOCOMO 研發組織的董事總經理，擔任高級副總裁和副總裁。一直負責類比蜂巢式系統 (1G)、數位蜂巢式系統 (2G)、W-CDMA/HSPA (3G)、LTE/LTE-Advanced (4G)、5G 及更高版本的研究

和開發的先進前瞻計劃。自 1982 年以來，他一直在 NTT 和 NTT DOCOMO 工作，積累了 30 多年的經驗。 Onoe 先生擁有京都大學工學研究生院的電子學碩士學位。

- Erik Ekudden 先生為愛立信的 CTO，負責為愛立信制定整體戰略和技術領先方向。 在加利福尼亞州聖克拉拉待了近七年後，他於 2017 年搬到了瑞典的 Kista。Ekudden 先生對集團的關注重點是在行動通訊、雲端計算、人工智能和物聯網方面的戰略決策和投資。 這建立在他在技術戰略和企業活動方面與 2G 到 5G 及其他領域的領先客戶和合作夥伴長達數十年的職業生涯的基礎上。Ekudden 先生 於 1993 年首次加入愛立信從事行動通訊系統相關工作，迅速成為研究和技術領域的領導者。 他曾擔任研究領域主任和技術戰略、標準化和企業副總裁。Ekudden 先生擁有瑞典斯德哥爾摩皇家理工學院電氣工程理學碩士學位。 他是瑞典皇家工程科學院 (IVA) 的成員。
- Durga Malladi 先生是高通(Qualcomm Technologies, Inc.) 5G 行動寬頻和基礎設施部門高級副總裁兼總經理。 Durga 於 1998 年加入 Qualcomm，擔任高級工程師。在過去的 24 年裡，他曾在 3G、4G 和 5G 技術方面擔任過各種研發和業務職務。Malladi 先生在 2008-15 年間，在 Qualcomm Research 擔任 4G LTE 和 LTE-Advanced 的項目工程師，致力於載波聚合、小型蜂窩、HetNets、中繼、許可輔助存取 (LAA)、物聯網（eMTC、NB- IoT) 和蜂窩 V2X。從 2015-18 年，他在 Qualcomm 領導了 Sub6 和毫米波頻段的 5G 研究，專注於增強型行動寬頻 (eMBB)、超可靠低延遲通訊 (URLLC)、工業物聯網、5G 車載通信 (C-V2X)、集成存取和後端網路系統、未經許可/共享頻譜和大規模物聯網 (mIoT)。職責涵蓋系統設計、標準化、原型測試平台、商業化前營運商互操作性測試和試驗。自 2018 年起，擔任 5G、行動寬頻和基礎設施高級副總裁兼總經理，負責蜂窩調製解調器(Cellular Modem)、定位、基礎設施射頻網路和專有網路業務、基頻和收發器調製解調器技術藍圖和特性、軟體產品與 5G 生態系統企業夥伴的合作。他推動跨業務部門的整體 5G 調製解調器射頻網路藍圖和解決方案，跨越行動通訊、基礎設施、物聯網和汽車領域。Malladi 先生獲得高通 IP 卓越獎、高通項目領導傑出貢獻者

獎和 HSPA 和 LTE 的傑出貢獻成就獎。Malladi 先生擁有印度理工學院馬德拉斯分校的技術學士學位，以及加州大學洛杉磯分校碩士和博士學位。博士論文是序列檢測和自適應估計技術，他的研究興趣包括訊號處理、通信理論、人工智能和量子計算。他是 IEEE 成員，擁有 536 項美國專利。

- Ryosuke Takahashi 先生在大學時就開始擔任工程師。憑藉其作為個人 Web 應用程序開發人員和多家企業實習生的經驗於 2018 年 6 月創立了 Acompany。Takahashi 先生經歷了一個開發數位密鑰管理系統的項目，參與了數位資產管理團隊。他還在多個創業公司的商業計劃競賽中獲得了一些獎項，包括 2021 年內政和通信部 NICT 企業家博覽會的二等獎。Acompany 被選為愛知縣加速升級計劃。在該計劃中，用於區塊鏈上管理製造業的供應鏈數據。Ryosuke Takahashi 先生在聽取一些公司的意見時遇到了問題。問題是數位數據使用和數據隱私保護之間的權衡。他聽到大公司的聲音說“想更實際地利用公司的數據，但不想將其提供給外部”。他意識到了名為“安全多方計算(MPC)”的解決方案，並決定將他的商業業務轉向。Acompany 開發並發布了獨創的資安多方運算引擎“Quick MPC”，並在多家公司的示範實驗中取得成功。Acompany 正在最前沿致力於多方計算技術的社會化實現。

## 三、 會議過程及內容

這個會議將討論解決科技與國際標準變得更加多樣化和複雜衍生的社會問題，而且很多國家開始討論下一代通訊技術 6G，不僅是 5G 的發展需求，也已經需要後 5G 的標準，對此而言，預期將有更多樣化和有品質的產品和服務，在更多數服務下，並鼓勵供應商減少成本。後 5G 時代的技術也更有潛力，來實現彈性的網路，並增進社會和經濟發展。日本也制定了後 5G 的戰略，目的再實現一個相容、可持續發展和可靠的數據驅動型社會。該藍圖基於全球生態、創新和集中資源三項基本政策。 它的成立是為了政府、企業和其他利益相關者共同努力，以實現後 5G 的環境和國際連結。日本政府將與企業以及地方和國際政府合作展開，一系列國際標準化活動。

從市場對 4G 的開始。 4G 這個術語在標準化的早期並不是那麼流行，LTE 在 2008 年被注意到。然而隔年 3G HSPA+就在這之前為人們關注的焦點。但經由 LTE 的釋出，HSPA+很快地就被 LTE 的聲勢取代。以各自推出年份來說，一開始的一年內 3G 與 LTE 的營運商數量相比，LTE 比 3G 大得多，所以說 LTE 是非常成功商業部建。你還記得 2015 年嗎。通過計算世界移動大會每日新聞頭條中流行語的數量來衡量 5G 熱潮。這熱潮到今天為止，它仍處於膨脹階段，並在預期的高峰值附近，就看未來 6G 的浪潮，繼續延燒。而這個 5G 熱潮的早期，大約在 2015 年或 2016 年，那時 5G 的熱潮感到有點新奇。因為大家都在說 5G，但又不知何為真正的 5G。

而帶領 5G 潮流，當然也是需要一段時間的，5G 有很多商業發展機會，人們對 5G 的期望也很高，這種期望也開始涉與其他特定行業領域的整合，如何引起各種協議的交流，創造跨企業合作及更多新的商業機會。實際上，跨企業合作將是 5G 成功的關鍵。今天，大多數人或許認為許多活動沒有持續進行，因為疫情暫時中斷，但事實是 5G 能處於高度發展與部建階段，並且 6G 的討論也已經開始了，相比 5G 使用案例的討論，來的時間更早，希望能持續討論 5G 的進一步的標準，而不是匆匆忙忙，快速開啟 6G 或以後的下世代，相比技術的發展，網路的技術滲透率，也是一項網路部建的重點。

各地區的通訊普及率，總結了這三年前趨勢。加入對 5G 的猜測，目前仍然不確定階段，但希望隨著持續時間的增加，快速的地區或國家落實。讓我們簡單地看看我可以說 5G 的部建甚至大於 4G。

新一代技術的傳播，將伴隨著地區間的傳播。新世代的改變與升級。人們認為新一代技術在導入的時候，相比舊技術下有了很大的躍進。然而，現實是不同的。新一代的技術價值，是在於確保發展持續性 每隔一段時間，它的推出並不是性能比的躍進，新一代的推出也可能不是每年都必須推出的，對於世代數而言，能力比技術名稱更重要，我們在這幾代中看到了一些正相關因素。世代進化仍有技術進步的風險，而世代升級也可能不是所有地區提升寬頻的主要手段，但這些正相關因素可能會支持它的理論，對於某些非高度發展的國家，或許仍不需有高度發展的技術，並面對成本考量下，世代升級就沒有迫切的需求。

談到了對 5G 的期望領導跨企業合作的明確結果，並討論挑戰減少地區差異的新世代滲透率。目前階段發展的 5G 與後 5G，以及將持續發展至 6G。因此在全球範圍內更快速地部建 5G 作為目標之一，目前已經擁有大約 170 個 5G 網路服務供應商，擁有超過 900 種智慧型手機。預測到今年年底，我們將擁有 580 百萬個訂閱使用用戶，而在未來五年內，預計將擁有多達 88 億個 3GPP 網路的訂閱用戶。而其中 5G 將佔有 35 億個，占比其中很大一部分。此外，廣域蜂窩型物聯網訂閱用戶的增長非常驚人，僅在五年內就達到了約 54 億。因此，到 2030 年，實際上看到在談論的官方或企業部門合作，也已經發生，但從現在起，到 10 年後將更加占主導地位，因為 5G 和許多其他技術會成為公共基礎設施。 5G 營運商將達 7000 億美元的業務收入。

而智能製造，正是一個使用案例，現在正在經歷一場巨大的轉變，從主要未連接或固定連接的設備到無線連接的世界。到 2030 年，智能製造中將有大約 47 億個無線連接。當然，這是商業模式和其他技術的巨大變化。但對於企業來說，這是一個很好的機會。國際標準和全球無線發展規模確實為過去以及未來五到十年，展開了提前部屬。事實上，這個生態系統和在 ITU 3GPP 行業中創新能力，確實促成了這種的高價值創造。

我們現在正在經歷從集成的網路轉到橫向網路的轉變。基本上，在跨無線通訊網路的核心網路邁向雲端的旅程中，我們引入了邊緣計算，以便能夠將工作負載移到基礎設施中更接近使用者的地方，來降低延遲並提高用戶體驗。但這也意味著我們必須跟上頻寬、更高的頻率，並且當我們需要如載波聚合之類的技術時，我們需要有這些來降低延遲並能夠為新服務提供服務，亦在消費者領域和企業領域都出現了這類技術。而關鍵工具之一就是通過網路切片提供更好的性能及更好的保證。這項技術已經醞釀了很長時間，現在它正在商業部建中，無線通訊網路、核心網路、傳輸網路、編排層，以及同樣實施網路切片的愛立信 5G 無線路由器等設備中。因此，高性能部分正在成為 5G 的一個關鍵特性。此技術實際上建立在獨特的硬體之上。Ericsson 獨特的晶片，我們正在全球範圍內部建它，可以讓功耗越來越低、效率更高，而且與更通用的解決方案相比，它還能提高性能。加速器是雲端轉型的關鍵部分。現在愛立信雲端運算是那個其中的一部分。

但值得一提的是，這也是企業再持續發展、持續融入網路方面的轉型。這帶來了更高的效率、更快的部建軟體功能，可以每小時升級和更新，而不是每月或每年。為了應對複雜性，整合 AI 是自動化的一部分。但在未來 5 到 10 年內，我們將在整合 AI 更多方面。這確實為分散式基礎設施的演進，當我們擁有邊緣運算的能力，在本次會議介紹中提到的關鍵基礎設施的靈活彈性和穩定性。

其中的一個例子，是數位分身技術，在這種情況下，是基於雲端動態協調的基站。以目前而言，5G 通過頻寬和儲存以及低延遲可以實現這一點。啟用 5G 的無人機可以幫助我們追踪存貨，確保可以得到正確的資訊，還能夠應對基站以外的新挑戰。用於各種維護和監視應用程式。如果我們切換到未來後多一點預期技術。我們看到 5G 已經啟用的新使用案例，實際上得到進一步增強，將獲得更高的頻寬、更低的延遲和更強的穩定性。因此，其中一個領域是將觸覺反饋以及使用者和遊戲領域，所做的事情中的體驗，轉化為氣味和其他味道到現實世界，當然還有多感官交流中的一切環境。所有連接到智能裝置有關，這些智能裝置，需要互聯駕駛來實現相互操作性，而且還需要從網路基礎設施中獲得更佳性能。我在前面的例子中展示的數位分身也非常重要，當數位和物理世界中結合在一起。早期例子，例如我們自己的智能製造，真正為創建基於網路技術、5G 和 5G 後數位世界。最後，在使用案例中，我們有機會在 2030 年之前使用 5G 和數位技術顯著減少碳排放的互聯世界。事實上，我們的估計表明，超過 15%使用最新的 ICT 技術，尤其是 5G，可以減少全球碳排放，這當然是轉型變革或轉型推動，但它也是許多其他需要轉型的必要基礎 為實現可持續發展的世界而努力。作為一個行業，我們可以做更多的事情來處理我們自己企業的排放和情況，但真正支持汽車改造、物流、改造、各種旅行，但所有進入零售業的東西 我們在金融部門看到我們在衛生部門看到的所有部門都將從它和數位技術中受益匪淺。

如果以 5G 而言，表明我們現在仍處於早期發展部建階段，現在思考 5G 之後的一代需要面臨什麼。從多個方面來看，數據速率、延遲、定位、覆蓋等能力，能源效率也可能是更重要的特徵之一，但延展到新維度的極端的能力，其中如靈活性、彈性、服務可用性、服務多功能性、促進分散式

應用程式、極端設備感知以及進一步的部建靈活性，將在未來世代中變得更加重要。在自動化過程中的位置，那麼未來 5 到 10 年，網路方面再做各方數據的融合，以及人工智能和 5G 人工智能和 6G 的結合。這就是認知網路和由意圖來驅動的網路而非數據驅動，網路不僅擁有運算能力，而且還利用所有營運數據和數據基礎設施整合在一起。就可以機會開始看到驚人的收益。所以效率方面，也看到的高性能了。但當然其他企業如何利用網路平台進行的重大改革，用 5G 升級的創新平台將演變為 6G。看到在各行業對長期演進規劃時間來看，創新將來自開放的標準化，創新將來自不斷挑戰自我並將新技術構建為新標準。但 ITU 開始的項目之一，將在 2023 年產生願景報告，從前幾代的標準學到了什麼，需要多長時間才能建立新基礎，從需求的研究活動一直到標準化和商業化，需考慮未來 10 年的時間，ITU 進到 2023 年期間，在此還有很多工作，在未來的幾年裡國際標準化機構之間的合作非常好，開放的標準化機構可以擴大受益行業的規模。如何利用已經完成標準，繼續發展並推動新穎性和標準化過程，我們看到了對不僅是消費者端和設備端，企業的效益，事實上基於 5G 的住宅固定無線存取是另一個很好的例子，已有 160 多家服務提供商提供商業固定無線存取服務。如果您真正渴望更好的用戶體驗，消費者的接受度和興趣，對新設備外形的體驗，那麼與 5G 結合在一起的應用服務在早期市場，確實取得了成功。但如果沒有 3GPP 所代表的國際合作和標準化，5G 就不會出現。所以這就是為什麼我們現在非常確定我們必須說一個最好的起點，也可以延伸到 5 年後的 6G。這確實需構建新矽晶元、高性能、低能耗和高的時間來實現。需要基礎架構中，成熟的基礎技術。但它也來自對使用者的學習和要求苛刻的使用案例。這真的指向感官互聯網或真正超出我們當前能力的事物，並將我們的想像力延展到假設 2030 年可能實現的事物。所以感謝有機會分享對未來幾年的一些想法，包括標準化可以讓你感覺新奇的事情。

於今天而言，網路連通性對每個人來說都是至關重要。對於醫療保健、教育等方面的工作亦是。連通性對於實現強勁經濟增長和更具彈性的社會的未來。鑑於我們在過去 18 個月中目睹了數據流量的顯著增加。Covid-19 的影響，加強對 5G 的需求，以提供未來十年後大規模數據增長所需的性能和容量。5G 更是全球趨勢的一部分，每個人和一切都可以智能連接，超

快速 5G 連接、高性能、低功耗運算和設備人工智能技術的整合以及雲端的大規模增長的推動。5G 設備可以無時無刻連接到雲端，通過不斷增加的應用程式處理能力和儲存量來提供新的體驗。推動了互聯智能邊緣端的出現，數十億智能互聯設備將被部建各行業上，並產生重大影響。 5G 人工智能與雲端的整合，將成為全球創新和經濟增長的催化劑。在 Covid-19 過程中，我們看到各行業和企業加快了數位化轉型的步伐。雖然無線網路發揮了作用，但 5G 是未來不可或缺的一部分，它支持新的商業模式、新服務和新的收入。 5G 行動技術，已得到行動產業的證實，有望推動其他產業的進步和創新，5G 的經濟影響將是巨大的。根據分析師的預測，到 2035 年，5G 將在製造、物流、醫療保健、教育、娛樂等多個領域實現超過 13 萬億美元的全球銷售活動。通過加入 5G，政府可以為國內創新和經濟增長創造重大機遇。但為了充分利用 5G 並在網路、企業和家庭中實現它，我們需要多樣化、可延展、安全和適應性強的下一代基礎設施。它還需要在室內和室外提供高性能服務，並支援公共或專用網路。這些需求正在推動向更加虛擬化的模組化，和可互操作的蜂窩基礎設施，開放虛擬化和模組化，無線網路存取的靈活性和可延展性將加速蜂窩基礎設施的創新，降低成本，並支持軟體可升級的網路架構。這種現代網路方法取代了專門構建的專有無線電存取硬體，使用在現成的計算機服務器和路由器中運行的軟體定義技術，使無線電網路存取更加靈活、可延展和更具成本效益。開放運行支持基於標準且可互操作的市場，該市場更加開放、穩健、創新和具有競爭力。因此，現代網路有望促進小型、大型和新創公司在公共和私有網路中的更大創新。虛擬化和開放網路的商業化正在進行中。例如，樂天正在日本推出虛擬化網路，其他主要營運商已在美國、歐洲等地區展開試驗。

Qualcomm 與 NTT DoCoMo 和其他十幾個生態系統領導者聯手創建了 5G openRAN 生態鏈系統，以開放運行在全球的延展。去年支持開放授權的全新 Qualcomm 5G 運行平台的推出得到了 15 家全球營運商的支持。5G 可以為人們、企業和經濟成長做很多事情，但當我們充分利用時，它的影響力甚大。這包括利用所有頻譜，這是 5G 的目的。現有的較低頻段和低於 6 GHz 的頻段提供廣域覆蓋，以實現服務連續性。低於 6 GHz 中頻段的 5G 可提供額外的容量和頻寬。 5G 毫米波以部建密集的城市點、提供固定無線存取、企業和工業應用數 Gbps 的數據速率、大容量以及低延遲。

它將成為許多新使用案例的關鍵部分，例如雲端中的 8k 影片編輯、協作多維空間中的虛擬學習和 4k 視訊會議以及支持交通樞紐、購物中心和體育場等擁擠場所的高容量需求.毫米波已經通過意大利、新加坡、澳大利亞和美國的商業網路走向全球，未來還會有更多。在日本，所有行動網路營運商現在都可以在不到六個月的時間內提供商用 5G 毫米波。

日本的 5G 毫米波基站數量從 2020 年 9 月的約 2300 個增加到今年 3 月的近 8100 個，增加了三倍，佔 5G 毫米波基站總數的近 45%。對於營運商來說，重要的是知道毫米波不是部建的優先事項，而是移動營運商網路戰略的一個增強選項。毫米波部署具有成本效益，分析師數據顯示，在容量需求較高的地方，具有毫米波和中頻段頻譜的系統的總擁有成本，低於單獨部建中頻段的成本。最多可節省 35%。 5G 毫米波也代表著進一步經濟增長。在歐洲，英國和歐盟近半數國家已經分配或計劃分配 5G 毫米波頻譜。分析師估計，到 2040 年，5G 毫米波部署將在 30 個歐洲國家和中國產生超過 1400 億歐元的累計 GDP 增長，我們正與生態鏈系統成員密切合作，在 2022 年北京冬季奧運會上展示 5G 毫米波。根據GSMA 的數據，到 2034 年，毫米波的使用帶來的經濟效益預計將超過 1000 億美元。

在性能方面，5G 毫米波速度令人驚嘆，尤其是在 Qualcomm 的 Snapdragon 數據上顯示，我們的 Snapdragon 5G 調製解調器射頻系統提供的毫米波數據速率比 5G sub 6 GHz 快 16 倍，比 LTE 快 38 倍。作為毫米波領域的全球領導者，Qualcomm 開發了許多計劃，我們將在未來幾個月內推出這些計劃，以幫助加速採用。除了對經驗和企業的影響。 5G 毫米波也將成為解決重要社會問題的有力工具。在 Covid-19 期間變得更加突出的一個問題是寬帶差距。它影響了教育、小企業，尤其是農村和低收入社區。 5G 毫米波固定無線存取將有助於將高速連接到缺乏寬帶服務的學校、圖書館和家庭。它為城市郊區和農村地區提供了一種具有成本效益的最後一英里技術，有助於縮小數位鴻溝和寬帶存取差距，並將互聯經濟增長的好處延展到服務不足的新社區。 5G 毫米波固定無線提供強大的性能也就不足為奇了。在最近與 US Cellular 和諾基亞的合作中，我們實現了每秒 1 Gpbs 的固定無線數據連接，距離超過 6 英里，創下了世界紀錄。同樣重要

的是 5G 毫米波無線具有成本效益。5G 毫米波和 sub 6 頻譜的組合允許美國農村的營運商提供固定互聯網存取，與單獨使用 sub 6 相比，總成本節省 40%。 Qualcomm 在美國的無線存取業務取得顯著增長，部分原因在於我們企業領先的 5G 固定無線解決方案組合。在我們忙於引領 5G 跨地區商業化的同時，我們繼續大力投資研發，通過即將發布的新 5G 規範，推動 5G 藍圖的演變，以幫助在今天建立的 5G 技術基礎上實現 5G 的全部潛力，新的 5G 版本將帶來增強的功能和特性，使全新的行業能夠支持下一代服務和商業模式，並創造令人興奮的新使用案例和體驗。一些 5G 延展領域包括增強的 5G 物聯網支持，為工使用案例提供超可靠、低延遲的連接，以及 5G 的縮小版本和我們稱之為 light 的標準。對於傳感器和變量等低複雜性設備，改進了端到端 5G 系統性能並優化了 5G 增強實境體驗，包括新的邊緣器和 5G 使用衛星運行的能力。 5G 藍圖的可能性確實是無限的。他們還致力於關鍵的長期研究，最終將引領通往 6G 的道路，包括更具可延展性的網路架構，以及雲端到設備的分解和虛擬化。新的無線電設計可以提供差異化的性能和效率、採用安全設計方法的通信彈性、人工智能和無線機器學習，支持數據驅動的無線設計方法，以及動態和自適應協調頻譜共享，甚至更高的頻段。 6G 的願景開始形成。然而，距離正式確定 6G 定義系統設計目標和推動有意義的實施建議還有幾年的時間。Qualcomm 正在積極參與學術界和政府以及支持大學研究中心的 6G 討論。我們仍處於 5G 商業化的早期階段，要在全球範圍內推廣 5G 並將 5G 延展到新的使用案例和企業，還有很長的路要走。

日本在利用數位技術方面落後於，快速增長的歐洲 IT 公司。對於未來數據鏈接分散式的重要性，也提出了幾點，展示下一代數據利用應該是什麼。另一方面，數據競爭的進步或隱私能力，對於數據競爭中的隱私洩露事件變得顯而易見，造成了巨大的損害或影響。它也影響公司或組織的品牌形象。在很多情況下，它會傳播到商業夥伴和客戶等，尤其在處理隱私時，保護資料也是公司和組織的社會責任。因此，我們很難充分利用數據資料。換句話說，是數據利用與數據隱私保護之間的權衡。我們可以通過使用資安運算來解決這個問題，我們的資安運算產品 Quick MPC 是我們開發的一款獨特的軟體，可以保護數據和隱私。它也努力地利用數據。資安運算是處理數據同時保持加密的技術的通用術語。換句話說，它是一種允許在執

行的同時進行運算的技術。能夠在利用數據的同時保護數據，另一方面，運算有望成為非常強大的下一代密碼學，因為它可以在每次使用時實現數據保護。好的，將介紹產品 Quick MPC 並研究具有安全多路徑補償的資安運算。Quick MPC 是用於構建安全多方運算系統的軟體。建立一個安全的計算系統很複雜，因為它需要高度技術能力。Quick MPC 可以通過使用我們的軟體來構建它。資安運算通道或程序正在分析我們的多總數據組合。多公司數據聯用的客戶問題就是我們的例子。他們想要數據聯用的分析結果，但又不希望自己的數據被其他公司看到。因為很難按原樣向外界提供原始數據。在這種情況下，都會降低數據的準確性。但是，資安運算可以在這樣的事情中解決這個問題。數據競爭將是其中一種手段，如何進行數據競爭。在對數據保密的同時進行競爭處理，採用了一種稱為秘鑰共享方案的方式。對於機密訊息，依據日期分成幾條稱為共享的訊息。將這些共享訊息，分佈在多個服務器上。並通過資安運算實現，安全的資料收集和分析來延展的業務。例如，一家公司想使用大營銷數據或其他公司，可以在服務上將兩個數據集成到資安運算上。通過這樣做，可以構建一個平台，使分析或潛在客戶能夠分析新的業務目標，同時保護用戶的隱私。此外，現在醫療旅遊和數據尚未對外共享，因為它是資全問題和醫院本身的機密訊息。我們現在正在與一家大學醫院合作。我們糾正他們的醫療履歷和日期，同時保持秘密自行競爭，來優化醫院的資源管理。當今技術上沒有完美的開源軟體，實施安全的多方競爭、或多個高度專業化的技術堆疊。

## 四、 總結

本次會議從全球和多方利益相關者的角度討論了未來網路和標準化對 5G 以上的期望和挑戰。讓我們對市場方面的期望或新一代網路的價值有了深刻的見解。我們得到一些有趣的內容和想法，來理解數位技術的演進以及我們生活和社會的未來會是什麼樣子。以及對網路的普及速度，也快速的增長，相較 3G/4G 網路，5G 的成長動能更為快速，部建約兩年多就多達百家的營運商，這也是人們對於新技術的渴望，加速市場創新的速度。我們也了解要實現這樣的未來需要什麼技術。我們還機會了解一家初創公司創造的有趣且創新的技術，對於資料的使用以及加密，使得更保有資料的隱私，如果可能用來做更大量的數據分析，增進未來社會使用的資料庫。

## 第一場「下世代電信網路號碼與物聯網編碼趨勢」專家座談會

## 一、第一場座談會簡介及議程

我國電信號碼編碼採 ITU E.164 國際編碼方式，電信級設備以「國碼」+「區碼」+「電話號碼」格式即可互通互連。隨著下世代電信網路技術來臨，物聯網(Internet of Things, IoT)、網路切片及專網等成為快速發展的新興應用服務，惟目前電信產業採用之 E.164、E.212 等電信編碼原則對應下世代嶄新的電信環境，在技術及管理上應有全面檢視之必要。有鑑於國際組織 ICANN、ITU 及各國陸續展開電信號碼技術及標準研究，如 ICANN 於 106 年 11 月會議展示使用網域名稱系統作為取代 E.164 編碼方式之可能性，此外該組織又於 109 年發布「5G Technology」報告，說明以 DNS 系統作為物聯網設備編碼之可行性，希冀凝聚各界之共識。

政府為加速推動 5G 基礎建設，營造友善 5G 發展的環境，同時強化我國 5G 專網服務，帶領掌握 5G 及下世代電信契機，驅動產業創新，期藉超前部署「新世代電信編碼之技術與標準發展」，以保持我國於世界資通訊產業領先國的地位。

財團法人電信技術中心承接交通部 110 年度「下世代電信網路號碼技術研析及管理」委託研究計畫，將於 8 月 19 日（四）舉辦線上專家座談會，針對下世代電信號碼與物聯網編碼趨勢，邀請各方專家代表出席討論，希冀廣納各方意見，以充實本案研析報告並提供主管機關未來政策評估。

| 時間 | 議程 | | 主講人 |
|---|---|---|---|
| 13:30-14:00 | 報到 | | |
| 14:00-14:05 | 主持人致詞 | | 電信技術中心<br>林永勝主任 |
| 14:05-14:30 | 引言報告 | 下世代電信網路號碼技術及發展趨勢 | 電信技術中心<br>王彥中研究員 |
| 14:30-15:00 | 引言報告 | IETF 國際會議參與技術交流分享 | 國立宜蘭大學<br>陳麒元副教授 |

| 時間 | 議程 | | 主講人 |
|---|---|---|---|
| 15:00-16:20 | 專家座談<br>意見交流 | 討論題綱：<br>1. 國際下世代電信網路號碼發展趨勢綜合討論<br>2. 我國下世代電信網路號碼之實務應用及產業趨勢討論 | 電信技術中心<br>林永勝主任 |
| 16:20-16:30 | 主持人總結 | | 電信技術中心<br>林永勝主任 |

## 二、第一場座談會會議紀錄

(一) **主持人**：財團法人電信技術中心 林永勝主任

(二) **會議時間**：2021 年 8 月 19 日（四）下午 2 時 00 分

(三) **會議地點**：線上會議

(四) **與會成員**：交通部郵電司、經濟部工業局、國家通訊傳播委員會、台灣資通產業標準協會、財團法人工業技術研究院、國立臺灣科技大學電子工程系王瑞堂、國立臺灣科技大學電子工程系陳文雄、國立成功大學電信管理研究所陳文字、國立臺北護理健康大學資訊管理系陳彥宏、國立宜蘭大學資訊管理系陳麒元、中華電信股份有限公司、台灣大哥大股份有限公司、台灣之星股份有限公司、亞太電信股份有限公司、遠傳電信股份有限公司、台灣諾基亞通信股份有限公司、台灣愛立信股份有限公司、財團法人電信技術中心

(五) **會議紀錄**：彭俞蓉助理研究員、郭怡萱助理管理師

(六) **會議討論事項**：

**國際下世代電信網路號碼發展趨勢綜合討論：從國際下世代電信網路號碼發展趨勢來看，對我國相關電信號碼規劃及使用上的可能影響為何？**

1. 陳彥宏副教授(國立台北護理健康大學)：
   (1)建議計畫團隊將研究成果及結論，綜整及分析一份政策文件，以利業者得聚焦此政策文件進行討論及意見交流。
   (2)計畫團隊係以 5G 實質網路及實體網路設備基礎下進行研析號碼政策，若在此前提下，號碼政策仍是依據現行 ITU E.164 號碼規則無疑，而在下世代電信網路技術下(如 5G、B5G、6G)，未來網路不全然是實體網路設備，其中包含虛擬 Container、雲端化無線存取網路、虛擬私有雲、虛擬硬碟及虛擬網路等技術，此外上述技術將會使用網路切片方式，這些技術是需要編碼定址及一套互通機制，目前建議可用 Domain Name 技術處理定址方式，然而倘若計畫團隊僅針對 5G 實質網路及實體網路設備進行研析，則無法將軟體、網路虛擬化技術納入編碼範疇，也無法探討更深入的數據安全治理規範及評估等議題，建議計畫團隊能修正及調整研究範疇。
2. 陳志宇資深經理(計畫團隊)：謝謝陳教授的建議，由於下世代電信網路編碼議題涉及新興技術議題，因此希冀透過本場座談會先行徵詢各電信業者之建議，第三場座談會聚焦政策議題。
3. 陳彥宏副教授(國立台北護理健康大學)：建議第三場座談會可將雲端網路、虛擬演算等編碼議題納入討論。
4. 陳文字教授(國立成功大學)：
   (1)研析電信號碼議題應先區分號碼涉及對象是人使用或是機器使用，倘若是人使用，則編碼機制應謹慎處理，若是提供物聯網使用，因數量龐大，因此需透過機器設備進行管理。
   (2)號碼互聯涉及 IP Base、Domain Name service，而通訊互聯過程中會衍生出安全性議題，各裝置不論透過 5G 或是網際網路都需要透過 IP address 相互連線，然而 IPv6 已經是世界標準，依循此標準核配及管理即可。若涉及電信業者計價收費之 IMSI Base，建議主管機關依循目前電信業者自己的管理機制即可。
5. 王瑞堂助理教授(國立臺灣科技大學電子工程系)：
   (1) 之前物聯網設備都是使用非電信網路聯網，也就是所謂的 Wi-Fi，ZigBee，或者是有線網路。此情況下，電信營運商是無法管理相關物聯網設備。按此前提之下，電信營運商要先掌管物聯網設備，才有辦

法來思考電信編碼機制。

(2) 就目前電信編碼的發展來看，尚未有針對物聯網設備的編碼機制與演算法。

6. 陳文雄專案經理(國立臺灣科技大學電子工程系)：

(1) 目前主管機關核配給 040 物聯網號碼，但無法確定業者是否將門號提供給物聯網使用，因此本研究所採用 DNS 作為物聯網編碼，可以看出所使用的設備裝置(如手機、燈泡等)及設備使用情形，以利設備管理。

(2) 目前物聯網號碼是使用 E.164，例如 02 或 886，而物聯網上網是使用 E.212，換言之，物聯網設備需透過電信業者提供的 E.164 及 E.212 兩個號碼，而國際組織 ICANN 討論 DNS 編碼議題是假設物聯網設備不需要通話服務及簡訊服務下，則不需要配發 E.164 這個號碼，而僅在需要通話及簡訊服務的產品，才需要配發 E.164 號碼。而 ICANN 是管理 DN 的國際組織，因此建議物聯網裝置可以使用其他的運算符號，如透過 IMSI、IMEI、OID 等識別符號轉換 DNS 作為物聯網裝置的命名標準，而個人認為 IMEI 是需要在 GSMA 註冊，因此可以透過 IMEI 知道製造商、物聯網設備產品，透過 IMEI 編碼方式具有可識別性外，還可以知道產品為何。

(3) 實際上 3GPP 裝置連網都是使用 IMSI 通訊，電信業者不一定要將每一筆的 MSISDN 與 IMSI 作對應，所以未來電信號碼可以只要針對有使用通話及簡訊通訊的號碼進行 E.164 編碼調配，物連網號碼只需維持既有 IMSI 控管即可，對電信監管業務影響不大。電信業者不須將每筆 MSISDN/IMSI 作對應，也有助於減少資料庫維護及電信號碼的資安監管資源投入。

7. 盧添壽副處長(台灣資通產業標準協會)：

(1) 隨著物聯網的快速發展，各種類型的通訊終端和設備已經廣泛應用在生活的各個方面。對於物聯網產品、各廠商通常有自己的標識和編碼方式，是否需建立設備的唯一性識別號碼機制，取決於法規對於物聯網產品的監管機制。

(2) 在一般情況下物聯網設備是機器對人，但未來有可能是機器對機器，因此也必須考量機器對機器的編碼方式，以利識別裝置的位置及設

備狀態。

8. 連彥宗高級研究員(中華電信研究院寬網所)：

(1) 未來物聯網將會是機器對人的通訊情境，因此E.164的編碼方式仍有其必要性，然而在下世代電信網路路由方式，將採用ENUM/DNS的機制，而DNS解析則會採用全碼解析方式，因此未來編碼在新服務上的號碼可有更具彈性。

(2) 未來下世代電信網路將朝向行固融合之趨勢發展，未來行網、固網E.164管理若可以滿足緊急服務需求，固網E.164服務則可提供具有移動特別的商業服務。

(3) 未來新服務物聯網部分，應考量管理方式；在 IP 端對端及語音通訊服務，目前已經使用 DNS 的模式，mapping 端對端的位置，若未來在機器對人的通訊情境下，也可以使用 DNS 的編碼方式。

9. 林永勝高級工程師(中華電信行分經營規劃處)：電信編碼有 IT 網路及行動網路等不同討論觀點，而在行動網路的觀點目前主要是依循 ITU E.164 及 E.212 規則編碼，依循這兩種編碼方式制定的系統運作架構、商業運作、通聯紀錄及通訊監察等，因此從行動網路的角度認為，若未來有新的編碼方式建議採用 3GPP 標準或全球一致標準，以確保物聯網裝置之安全性及系統開發能與國外設備規格一致。

10. 楊博森主任工程師(台灣大哥大股份有限公司系統設計處)：台灣大哥大與中華電信的意見一致，針對國際下世代電信網路號碼發展，若採用新電信編碼制度，建議應採全球一致性標準，此外若採新的編碼制度，建議主管機關應考量新舊號碼(用戶) 如何互撥?是否需建置轉換平臺?業者既有設備是否能支援?等管理議題。

**我國下世代電信網路號碼在實務應用及產業趨勢討論：我國物聯網及電信產業應用及發展趨勢為何?**

1. 王瑞堂助理教授(國立臺灣科技大學電子工程系)：

(1) 要找到物聯網與電信網路之間有效的雙贏商業模式。換言之，建議未來可探討在電信網路下使用物聯網的原因。

(2) 目前5G特性的傳輸高、低延遲與大連結，應該會有特定場景必須使用電信網路，例如自駕車等，而在此情境，還是需要有適合的商業模式來配合。

2. 陳文雄專案經理(國立臺灣科技大學電子工程系)：台灣電信產業未來會逐漸朝向電信產品提為國產化比例及 5G 企業專網應用發展，在室外涵蓋面對 SpaceX 衛星通訊的快速發展威脅及 WiFi 6 網路的發展，預估未來電信會朝衛星、5G 以及 WiFi 的共存發展。例如：室內通訊、AR/VR、影片以 WiFi 為主，但是需要超低延遲的 MR 直播、異地共演、遠端遙控以及遠端手術會以 5G 服務為主。戶外的郊區、山區、沙漠、海上通訊以及災難現場，會以衛星通訊為主，其餘智慧城市、都市城鄉一般移動用戶聯網、超低延遲的車連網、無人機，會以 5G 服務為主。

3. 盧添壽副處長(台灣資通產業標準協會)：過去 2G、3G 電路交換核心網路提供 CSFB 語音服務，所以傳統的 E.164（MSISDN）及 E.212（IMSI）均會存在，但 E.164（MSISDN）未來可能在沒有電路交換的核心網路後逐漸消失。E.212（IMSI）因可作為認證註冊之用，安全機制也較完備，因此仍可能繼續使用，然而在設備定址的方式在 All-IP 的核心網路下，勢必漸進過渡到長期的 IP 位址。

4. 謝文生主任級研究員(中華電信研究院智聯所)：我國物聯網應用發展趨勢，依國發會在 2021 年 4 月發布「物聯網黃金十年」新聞指出，國內市場物聯網產值繼 2018 年突破兆元後，2020 年已增至新臺幣 1.54 兆元，全球市占率約 4.61%；國發會進一步指出「亞矽 2.0」擴大 AIoT 科技導入後，預估物聯網產值將於 2023 年突破新臺幣 2 兆元，並在 2025 年達到全球市占率 5%；另預期物聯網市場將在 AI、Surveillance、Enterprise Service、Telecommunications、Cloud、Health Tech…等應用領域持續發光發熱。依據各項物聯網市場研調報告分析指出，驅動物聯網市場大幅成長的主要因素可歸納為幾點：

(1) 大型跨國企業積極採用物聯網平臺應用服務，例如：微軟、AWS、Google 等大型跨國企業在市場中扮演領頭羊的角色；藉由良性競爭、異業結盟等策略合作，拓展垂直應用物聯網服務市場，使得各項應用服務能不斷推陳出新，驅動市場持續成長。

(2) 政府推動「亞矽2.0」計畫，持續引領物聯網產業創新研發及健全創新創業生態系，透過資金、法規、人才與擴大發展創新聚落等推動作法，將加速產業進化，預期國內物聯網產業將會有更多元化和高附加價值的服務和產品推出，持續帶動物聯網產業發展。

(3) 受 COVID-19影響，對全球物聯網「解決方案的需求」雖然造成全球物聯網整體成長趨緩。不過「短空長多」，也因為疫情衝擊進而提高「部分新科技的採用度與依賴性」；近期疫情升溫更促使各行業別企業加速評估「數位轉型」，提升企業在「數位化方案」採用的意願，預估在疫情過後，物聯網在軟體與服務等智慧應用領域將會出現顯著成長。

(4) 電信業如中華電信近幾年在物聯網各項應用服務上，也展現了許多成果，未來將聚焦5G+AIoT 創新應用，持續投入整體資通訊基礎設施、雲端機房及5G 網路建設，以集團能量研發產品、提供各項智慧應用服務，包含智慧工廠、智慧軌道、智慧交通、智慧製造、智慧城市、智慧電表、無人機、智慧港口、太陽能及風電等解決方案，更強調聚焦行業別的經營，深入各行業別發展5G＋人工智慧物聯網各式應用，協助企業加速轉型。

5. 林永勝高級工程師(中華電信行分經營規劃處)：3GPP 標準之行動網路係以 E.212 及 E.164 進行身分驗證、識別、提供服務及通訊監察等運作，此機制仍為 5G SA(非獨立選網)沿用，目前 3GPP 不具備 DNS 編碼運作方式及識別終端裝置，未來若有新型態編碼規則應能納入 3GPP 標準，以確保 IoT 裝置 DNS 編碼可順利運行於行動網路。

**我國下世代電信網路號碼在實務應用及產業趨勢討論：非 3GPP 標準下之 IoT 裝置(如透過 Wi-Fi 連線到 5G Gateway)，是否規劃編碼應用範圍?**

1. 王瑞堂助理教授(國立臺灣科技大學電子工程系)：對於需要修改基於電信網路基礎的電信編碼機制，理由如下：

(1) 因爲基於 Wi-Fi 聯網是沒有辦法看到 IMSI 等電信網路相關 ID。

(2) 5G deployment option 也有一些整合網路機制，也需要配合電信網路機制來完成編碼機制。

2. 陳文雄專案經理(國立臺灣科技大學電子工程系)：除了 IMEI 外，也可以用具有唯一性的 MAC。但 5G 通訊下有規定必須經過 EIR 認證，而 EIR 是透過 IMEI 進行認證，因此個人認為如果用 IMEI 作為唯一識別碼，有助於對物聯網裝置的管理。
3. 盧添壽副處長(台灣資通產業標準協會)：同意陳文雄專案經理所述，可以用 MAC 作為裝置唯一識別碼的定址，以利管理及查詢物聯網位置。對於物聯網可能涉及的編碼方式，應考慮連接網路是公眾電信網路（固定通訊網路或行動通訊網路），在網際網路上應用的物聯網服務，其使用之網域名稱與位址（IPv4 或 IPv6）的編製格式與現行網際網路上的各種應用服務一致，不需做變更，基本上不屬於電信網路的範圍。
4. Andy Lee 技術長(台灣愛立信股份有限公司)：
   (1) 其實有關號碼資源議題與商業模型有關，由於 IP 及 MSISDN 都涉及設備商的商業成本考量，但從 3GPP 規範中也是可以節省 MSISDN 使用，例如可使用 3GPP 定義之 MSISDN Last 協定，因此可以節省 MSISDN 網路使用資源。
   (2) 物聯網設備商以 Gateway 作為連接中介，包括 Wi-Fi 及非 IP 應用（例如：藍牙），建議需探討兩者是否皆需納入監管及如何監管。最重要的是在法規上需清楚定義監管邊界，才可談如何及運用何種號碼方法來監管。因為其實從技術層面而言兩者皆為可行方案。
5. 林永勝高級工程師(中華電信行分經營規劃處)：
   (1) 3GPP 標準之行動網路，主要以 E.212及 E.164進行身分驗證、識別、提供服務及通訊監察等運作，非3GPP 標準 IoT 裝置因不具備 E.212及 E.164編碼機制，無法於行動網路中使用。
   (2) 非3GPP 標準 IoT 裝置如利用透過 Wi-Fi 連線到支援 E.212及 E.164編碼機制之5G Gateway 使用服務，行動網路僅能就前述5G Gateway 之 E.212及 E.164編碼進行身分驗證、識別、提供服務及通訊監察，無法識別及管理經 Wi-Fi 接取之個別 IoT 裝置。
   (3) 未來若有新型態編碼規則，應能納入3GPP 標準依循3GPP 標準使用行動網路之 IoT 裝置，以確保 IoT 裝置 DNS 編碼可順利運行於行動網路（含跨境漫遊）。

**我國下世代電信網路號碼在實務應用及產業趨勢討論：物聯網應用的編碼需求與可用方案為何?是否有建立統一標準編碼之必要? DNS 編碼是否能作為下世代物聯網設備編碼之解決方案?**

1. 王瑞堂助理教授(國立臺灣科技大學電子工程系)：基於 DNS 會是一個很好的建議。主要的理由是：
   (1) 電信網路與非電信網路都可以通用。
   (2) 大量查詢可以用分散計算環境來解決。
   (3) 可快速分配與確認具有唯一性之 ID。
2. 盧添壽副處長(台灣資通產業標準協會)：
   (1) 可參照現有移動終端設備的 TAC 和 IMEI 編制統一的編碼體系，並將編碼範圍由接入公眾網的移動終端設備擴展到其他物聯網設備。
   (2) 考量未來監管及資安需求，統一標準編碼有其必要性。
   (3) 可將 DNS 編碼作為下世代物聯網設備編碼之解決方案列為考量，不過仍需參考國際標準做法。
3. CA Li 經理(台灣諾基亞通訊股份有限公司)：5G 網路基本上是針對物聯網（主要為企業物聯網）提供服務，3GPP 建議制訂把非 3GPP 的行動裝置都納入統一的核心網路中，事實上國外有 4G 業者擁有不需 MSISDN 的物聯網裝置，這些物聯網裝置經配對到號碼以控管 API。5G 網路應用將涉到大連結的物聯網服務，包括固網或行動裝置都希望可納入到同一 5G 平臺提供服務，因此集中式平臺有助於控管，所以在制定規範時，建議可參照國外或者 3GPP 針對不同連接裝置的控管方式。
4. 林永勝高級工程師(中華電信行分經營規劃處)：
   (1) 物聯網應用包含各種通訊技術接取方式，除服務應用本身有認證及識別機制外，各種通訊技術接取均有各自認證及識別機制，行動網路依循3GPP 標準以 E.212及 E.164進行認證、識別及提供行動通訊服務（如簡訊及語音）。
   (2) 目前行動物聯網以 E.164 040字頭為編碼，廣泛使用於3GPP 標準下之 IoT 裝置（含跨國行動網路漫遊），除作為裝置識別，亦提供物聯網簡訊服務（目前物聯網簡訊作為控制信令用，另語音服務部分

基於法規目前未開放），DNS 編碼倘作為下世代物聯網設備編碼，若未列入3GPP 標準，行動網路內部運作機制仍需使用 E.212及E.164編碼進行認證、識別及通訊監察。

5. 楊博森主任工程師(台灣大哥大股份有限公司系統設計處)：針對未來產業趨勢將「電腦化」，其範圍將可能包含電動車、路燈、水電錶等日常生活所及數量相當龐大，而如何與其「溝通」則將是一重大課題。因此，建議可制訂符合國內法規的統一標準制度，以因應未來的電腦（物）互聯互通使用。
6. 陳文字教授(國立成功大學電信管理研究所)：建議釐清 5G 企業專網號碼是誰要用、編碼目的何在，並建議計畫團隊應把企業專網納入考量，有助於釐清編碼方式。

(七) **散會：下午 4 時 30 分**

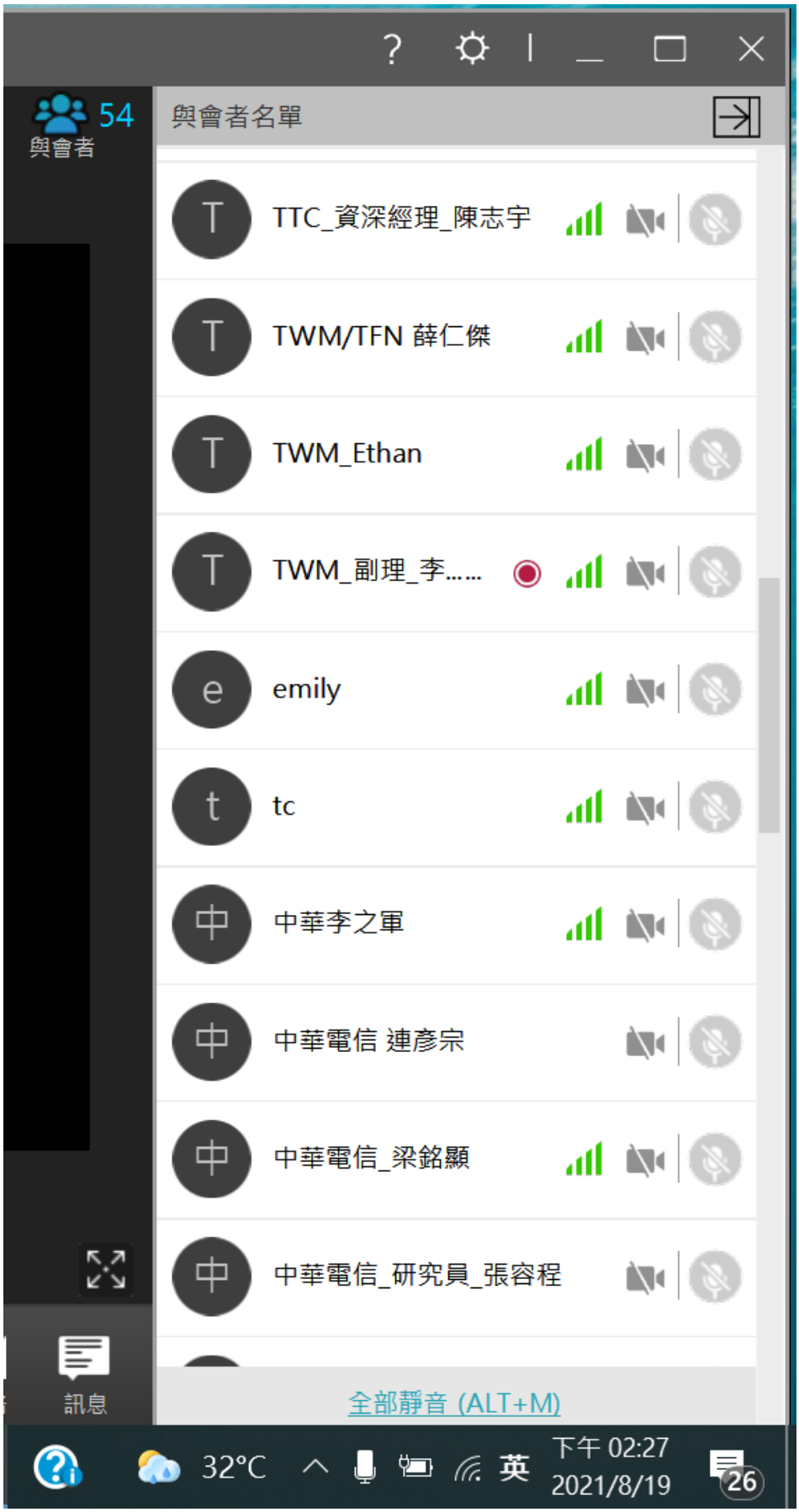
(八) **參與人員名單及簽到表**

| 編號 | 單位 | 姓名 | 職稱 |
|---|---|---|---|
| **政府機關** | | | |
| 1. | 交通部郵電司 | 林姝宜 | 專員 |
| 2. | 交通部郵電司 | 陳日暉 | 技士 |
| 3. | 交通部郵電司 | 高境良 | 技正 |
| 4. | 經濟部工業局 | 葉武松 | 代表出席 |
| 5. | 國家通訊傳播委員會 | 林永裕 | 科長 |
| **公協會** | | | |
| 6. | 台灣資通產業標準協會 | 戴武聰 | 副秘書長 |
| 7. | | 盧添壽 | 副處長 |
| 8. | 財團法人工業技術研究院<br>資訊與通訊研究所 | 林咨銘 | 技術經理 |
| **學者專家** | | | |
| 9. | 國立臺灣科技大學電子工程系 | 王瑞堂 | 助理教授 |
| 10. | | 陳文雄 | 專案經理 |
| 11. | 國立宜蘭大學資訊管理系 | 陳麒元 | 副教授 |
| 12. | 國立成功大學電信管理研究所 | 陳文字 | 教授 |
| 13. | 國立臺北護理健康大學 | 陳彥宏 | 副教授 |

| 編號 | 單位 | 姓名 | 職稱 |
|---|---|---|---|
| | 資訊管理系 | | |
| **電信業者** | | | |
| 14. | 中華電信股份有限公司 | 白洪政 | 高級工程師 |
| 15. | | 梁銘顯 | 高級工程師 |
| 16. | | 李之軍 | 高級工程師 |
| 17. | | 張容程 | 研究員 |
| 18. | | 唐崇實 | 高級研究員 |
| 19. | | 連彥宗 | 高級研究員 |
| 20. | | 謝文生 | 主任級研究員 |
| 21. | | 林永勝 | 高級工程師 |
| 22. | | 陳瑞全 | |
| 23. | 台灣大哥大股份有限公司 | 黃振杉 | 主任工程師 |
| 24. | | 楊博森 | 主任工程師 |
| 25. | | 李佳原 | 副理 |
| 26. | | 劉傳譯 | 主任管理師 |
| 27. | | 薛仁傑 | 副理 |
| 28. | | 胡里昂 | |
| 29. | | 林瀚杰 | 副理 |
| 30. | 台灣之星電信股份有限公司 | 任致遠 | 專案副理 |
| 31. | 亞太電信股份有限公司 | 方俊傑 | 經理 |
| 32. | | 許文宏 | 高級工程師 |
| 33. | | 許鈺宸 | 副理 |
| 34. | | 張栢芳 | 專員 |
| 35. | 遠傳電信股份有限公司 | 徐子祥 | 資深工程師 |
| 36. | | 廖鈺鳴 | 資深專員 |
| 37. | | 高家惠 | |
| 38. | | 黃志雯 | 副理 |
| 39. | | 郭禾蓁 | |
| **產業代表** | | | |
| 40. | 台灣諾基亞通信股份有限公司 | 謝巧君 | 行銷公關協理 |
| 41. | | Eric Wu | |
| 42. | | CA Li | |
| 43. | 台灣愛立信股份有限公司 | Andy Lee | 技術長 |
| 44. | | 王方平 | 資深協理 |
| TTC | | | |
| 45. | 財團法人電信技術中心 | 卜慶玲 | 副執行長 |
| 46. | | 林永勝 | 主任 |

| 編號 | 單位 | 姓名 | 職稱 |
| --- | --- | --- | --- |
| 47. | | 卓卿敏 | 資深經理 |
| 48. | | 陳志宇 | 資深經理 |
| 49. | | 王彥中 | 研究員 |
| 50. | | 夏慧馨 | 助理研究員 |
| 51. | | 李昕甯 | 助理研究員 |
| 52. | | 彭俞蓉 | 助理研究員 |
| 53. | | 簡嘉儀 | 副管理師 |
| 54. | | 陳佳瑀 | 副管理師 |
| 55. | | 郭怡萱 | 助理管理師 |

54
與會者
與會者名單
TTC- Crystal
主持人
TTC-副管理師-簡嘉儀
TTC-副管理師-陳佳瑀
TTC-助理研究員-...
TTC-助理研究員-...
主持人
TTC-助理管理師-...
TTC-研究員-王彥中
主持人
TTC_主任_林永勝Bill
TTC_助理研究員_夏.....
TTC_資深經理_卓卿敏
訊息
全部靜音 (ALT+M)
32°C
英
下午 02:27
2021/8/19
26


54
與會者
與會者名單
TTC_資深經理_陳志宇
TWM/TFN 薛仁傑
TWM_Ethan
TWM_副理_李.....
emily
tc
中華李之軍
中華電信 連彥宗
中華電信_梁銘顯
中華電信_研究員_張容程
訊息
全部靜音 (ALT+M)
32°C
英
下午 02:27
2021/8/19
26

54
與會者
與會者名單
中華電信_陳瑞全
中華電信_高研_唐崇實
中華電信_高級工程師_...
中華電信_高級工程師_白.....
亞太-張栢芳
亞太-許文宏
亞太-許鈺宸
北護-陳彥宏
台灣之星_任致遠
台灣大哥大 胡里昂
全部靜音 (ALT+M)
網路
訊息
32°C
英
下午 02:28
2021/8/19
26

54
與會者
與會者名單
台灣大哥大-林瀚杰
台灣大哥大-楊博森
台灣大哥大_黃振杉
台灣諾基亞-方案經理-...
台科大—王瑞堂
宜大-陳麒元
成大陳文字教授
經濟部工業局_代理出...
臺科大電子工程系-專...
謝文生
全部靜音 (ALT+M)
網路
訊息
32°C
英
下午 02:28
2021/8/19
26

54
與會者
與會者名單
會議室人員名單 (54)
您可以將另一名與會者的麥克風設為靜音。在設為靜音後，
您仍可以再按一下，請他們再度開啟。
APT_方俊傑
Ericsson Andy Lee
ITRI-技術經理-林咨銘
MOTC_林姝宜
MOTC_陳日暉
MOTC_高境良
NCIC-廖鈺鳴
TAICS-盧添壽
TAICS_副秘書長_戴武...
全部靜音 (ALT+M)
網路
訊息
32°C
英
下午 02:26
2021/8/19
26

54
與會者
與會者名單
宜大-陳麒元
成大陳文字教授
經濟部工業局_代理出...
臺科大電子工程系-專...
謝文生
通傳會_科長_林永裕
遠傳-高嘉惠
遠傳_副理_黃志雯
遠傳郭禾蓁
遠傳電信-徐子祥
全部靜音 (ALT+M)
訊息
32°C
英
下午 02:28
2021/8/19
26

## (九) 產官學研專家座談會會議照片

圖 1 、陳彥宏副教授就本案議題給予建議與指導

# 三、第一場座談會會議簡報

Chinese Name:陳志元
English Name : Chi-Yuan Chen (Justin)

03-9317374
http://sites.google.com/site/chiyuanchen/
chency@niu.edu.tw

## About Me

國立東華大學 電機工程學系 博士

經歷

- 國立宜蘭大學 資訊工程學系 副教授
- IEEE Senior Member, 2020.
- 中華民國資訊安全學會 副秘書長兼出版委員會主委, 2018~
- 台灣軟體模擬學會 副秘書長, 2014.2 – present
- Assistant Secretary In General, Internet Society Taipei Chapter, 2014.2~present
- Secretary and Treasurer, ACM SIG Mobility Taiwan Chapter, 2012-2013.2
- Executive Editor-in-Chief, Journal of Internet Technology (JIT), Since 2014.2 ~ present
- Editor-in-Chief, Communications of CCISA, Since 2019.1 ~ present

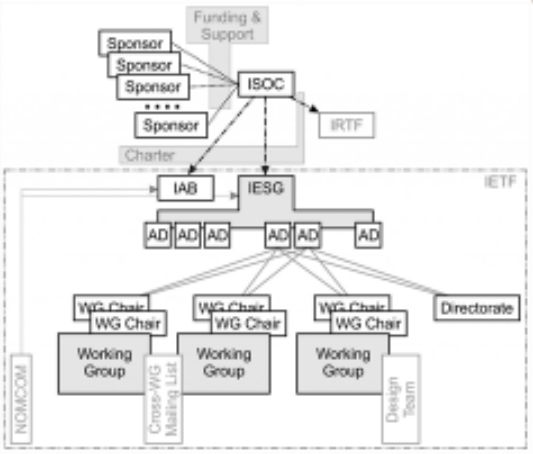
## The IETF

- Internet Engineering Task Force formed in 1986
- The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet [RFC 3935]
- The IETF is a Standards Development Organization (SDO)
- With self-selected individual participants, no formal membership

I E T F

# The Big Picture

- Internet Society (ISOC)
- Internet Architecture Board (IAB)
- Internet Research Task Force (IRTF)
- Internet Engineering Steering Group (IESG)
- Area Director (AD)




Source: Russ White 2015

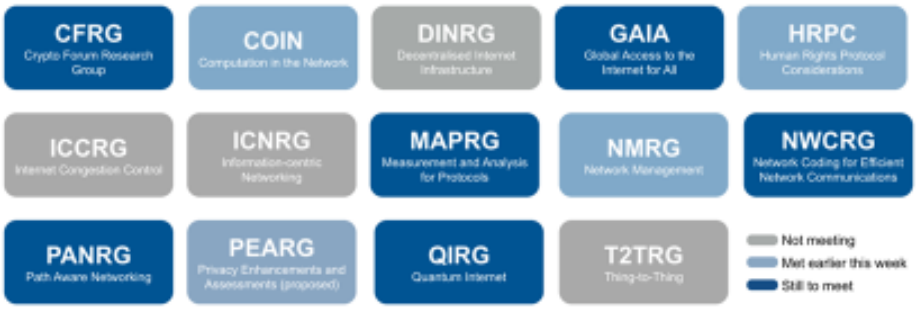
# IETF Areas

| | |
|---|---|
| Applications and Real-Time (ART) | • Application protocols and architectures<br>• 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<br>• Operations: IPv6, DNS, security, routing |
| Security (SEC) | • Security protocols and mechanisms |
| General (GEN) | • Activities focused on supporting and updating IETF processes |

Source: IETF

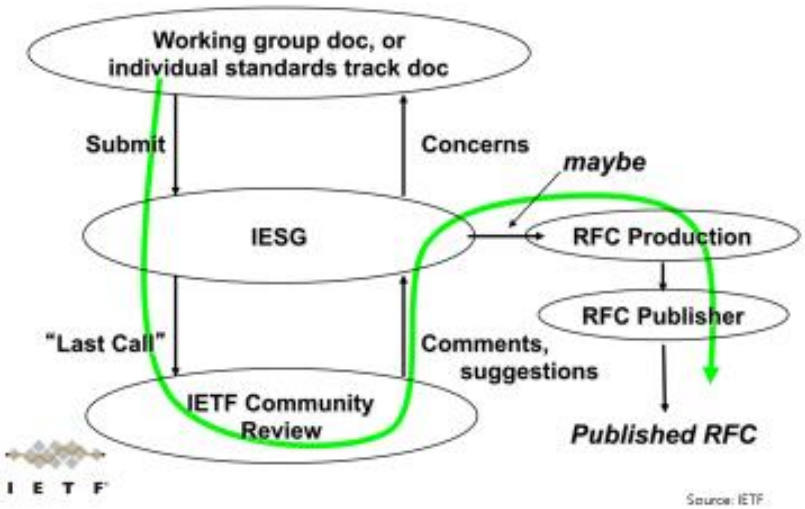
# IRTF RGs

- The IRTF conducts research; it is not a standards development organisation




Source: IETF 111

# IETF Submissions




Source: IETF

## The IETF and Consensus

- IETF mantra:
  - "We reject kings, presidents and voting. We believe in rough consensus and running code."
  – David Clark
- Humming – a way of measuring consensus that is not voting
- The session chair is usually the arbiter of consensus, but WG session consensus must yield to WG mailing list consensus
- "On Consensus and Humming in the IETF", P. Resnick [RFC 7282]

## The IETF and Consensus

# An IETF Meeting week

- Organized events on the agenda include:
  - Working Group sessions: ~130 working groups (some subset meeting)
  - Birds of a Feather sessions (BOFs)
  - IRTF sessions: ~ 15 research groups (some subset meeting)
  - Area-wide sessions, IETF-wide plenary(s), invited talks
  - Hackathon and Code Sprint
  - Social Events
  - Tutorials, Deep Dives & Lunch Sessions
  - Hot RFC Lightning Talks
  - Side Meetings, Open Time
- IETF 111 was held online 26-30 July 2021

# IETF 111 Participant Statistics

- Registration fee:
  - $280 USD
- Early Bird:
  - $230 USD
- 1369 registrations
- 8 from TW
- 1K to 1.5K people at 3/year meetings

# Future meeting locations and venues

| MEETING LOCATION | VENUE | DATES | HOSTS |
|---|---|---|---|
| **IETF 112 – Madrid** | Melia Castilla Hotel | November 6 – 12, 2021 | * |
| **IETF 113 – Bangkok** | Marriott Marquis Queen's Park | March 19 – 25, 2022 | * |
| **IETF 114 – Philadelphia** | Philadelphia 201 Hotel | July 23 – 29, 2022 | Comcast/NBCUniversal |
| **IETF 115 – Europe** | TBA | November 5-11, 2022 | * |
| **IETF 116 – Asia** | TBA | March 25-31, 2023 | * |
| **IETF 117 – San Francisco** | Hilton Union Square | July 22-28, 2023 | * |
| **IETF 118 – Prague** | Hilton Prague | November 4-10, 2023 | * |
| **IETF 119 - Asia** | TBA | March 16-22, 2024 | * |

Source: IETF 111

# IETF 111

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

Source: IETF

# Active Internet-Draft

| Areas | Working Groups | Active Internet-Draft | IETF 111 |
|---|---|---|---|
| OPS | Operations and Management Area Working Group（opsawg） | Operational Considerations for use of DNS in IoT devices | Y |
| OPS | IOT Operations (iotops) | Requirements and Scenarios for Industry Internet Addressing | Y |
| INT | DNS PRIVate Exchange（dprive） | Specification of DNS over Dedicated QUIC Connections | Y |
| INT | IP Wireless Access in Vehicular Environments（ipwave） | DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks | N |
| INT | Distributed Mobility Management（dmm） | Transport Network aware Mobility for 5G | N |
| INT | Extensions for Scalable DNS Service Discovery（dnssd） | Service Registration Protocol for DNS-Based Service Discovery | Y |
| SEC | DANE AutheNtication for Iot Service Hardening (danish) | TLS Client Authentication via DANE TLSA records | Y |

# DANE AutheNtication for Iot Service Hardening

draft-huque-dane-client-cert-06

TLS Client Authentication via DANE TLSA records

Internet Engineering Task Force
Internet-Draft
Updates: 6698, 7671 (if approved)
Intended status: Standards Track
Expires: 3 November 2021

S. Huque
Salesforce
V. Dukhovni
Two Sigma
A. Wilson
Valimail
2 May 2021

## DANE AutheNtication for Iot Service Hardening

draft-huque-dane-client-cert-06

- The DANE AutheNtication for Iot Service Hardening (DANISH) WG seeks to extend DANE to encompass TLS client authentication using certificates or Raw Public Keys (RPK)
- IoT Ecosystem Challenges
  - Private PKI needs a broadly useful lookup mechanism
  - Specifically, we need a lookup mechanism which:
    - works across private PKI (enabling mutual TLS authentication)
    - prevents naming collisions
    - makes credential rotation easier
    - works well for constrained platforms
  - Create safe bridges between islands of trust

## DANE AutheNtication for Iot Service Hardening

draft-huque-dane-client-cert-06

- Client DNS Naming Convention

Format 1: Service specific client identity

_service.[client-domain-name]

e.g. _smtp-client.relay1.example.com

1st label identifies the application service name. The emaining labels are composed of the client domain name. Allows the same client to have distinct authentication credentials for distinct application services.

## DANE AutheNtication for Iot Service Hardening

draft-huque-dane-client-cert-06

- Client DNS Naming Convention

  Format 2: IOT Device Identity

  [deviceid]._device.[org-domain-name]

  e.g. a1b2c3._device.subdomain.example.net.

  - a1b2c3: device identifier (could be multiple leftmost labels)
  - _device: identity grouping label
  - subdomain: organizational label (optional)
  - example.net: organizational domain

## DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks

draft-jeong-ipwave-iot-dns-autoconf-10

| Document | | |
|---|---|---|
| | Type | Active Internet-Draft (individual) |
| | Authors | Jaehoon (Paul) Jeong, Sejun Lee, Park Jung-Soo |
| | Last updated | 2021-02-21 |
| | Stream | (None) |
| | Intended RFC status | (None) |

IPWAVE Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 25, 2021

J. Jeong
Sungkyunkwan University
S. Lee
Ericsson-LG
J. Park
ETRI
February 21, 2021

## DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks

draft-jeong-ipwave-iot-dns-autoconf-10

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   unique_id.object_identifier.OID.domain_name    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

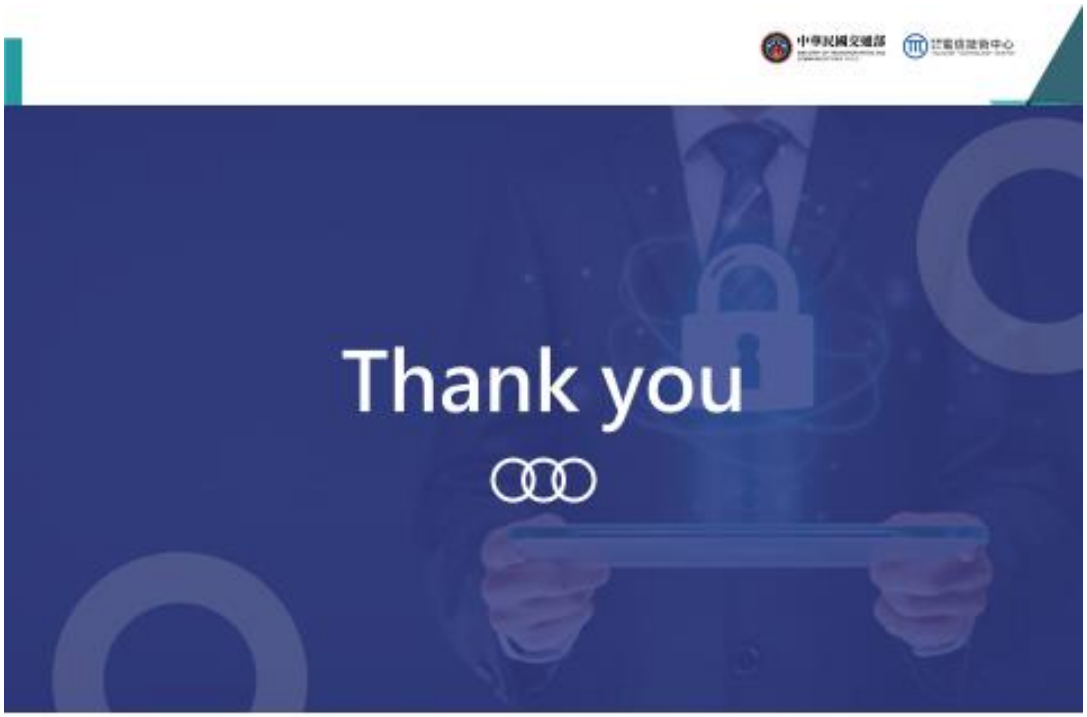
- IoT Device DNS Name Format with OID
  - unique_id: unique identifier to guarantee the uniqueness of the DNS name in ASCII characters. The identifier MAY be alphanumeric with readability, e.g., product name plus a sequence number
  - object_identifier: device's object identifier that consists of a higher arc, that is, M2M node indication ID (i.e., the concatenation of the managing organization, administration, data country code, and M2M node) and a sequence of four arcs (i.e., manufacturer ID, model ID, serial ID, and expanded ID) as defined in [oneM2M-OID]. The fields are separated by an underscore '_'
  - OID: subdomain for the keyword of OID to indicate that object_identifier is used
  - domain_name: domain name that represents a DNS domain for the network having the IoT devices

## DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks

draft-jeong-ipwave-iot-dns-autoconf-10

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| unique_id.object_identifier.OID.mic_loc.mac_loc.LOC.domain_name |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Location-Aware DNS Name Configuration
  - mic_loc: device's micro-location, such as an offset in a road segment and coordinates in 2-dimensional (or 3-dimensional) space
  - mac_loc: device's macro-location, such as a road segment and 2-dimensional (or 3-dimensional) space
  - LOC: subdomain for the keyword of LOC to indicate that mac_loc and mic_loc are used




中華民國交通部
MINISTRY OF TRANSPORTATION AND COMMUNICATIONS R.O.C

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

## 【二、引言報告】

## 下世代電信網路號碼技術及發展趨勢

中華民國交通部
MINISTRY OF TRANSPORTATION AND COMMUNICATIONS R.O.C

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

# 下世代電信網路號碼技術及發展趨勢

王彥中 研究員
財團法人電信技術中心
2021.08.19

## 行動通訊系統的演進：主要應用及能力

**1980's (1979) - 1G**
- 類比語音通話
- 可移動性

**1990's (1991) - 2G**
- 數位語音通話、簡訊
- 基本的數據服務

**2000's (2002) - 3G**
- 行動及無線上網、內容、社群媒體
- 行動蜂代固網 (FMS)

**2010's (2009) - 4G**
- 真正的行動寬頻體驗
- 應用程式App化，帶來更為便捷的數位生活

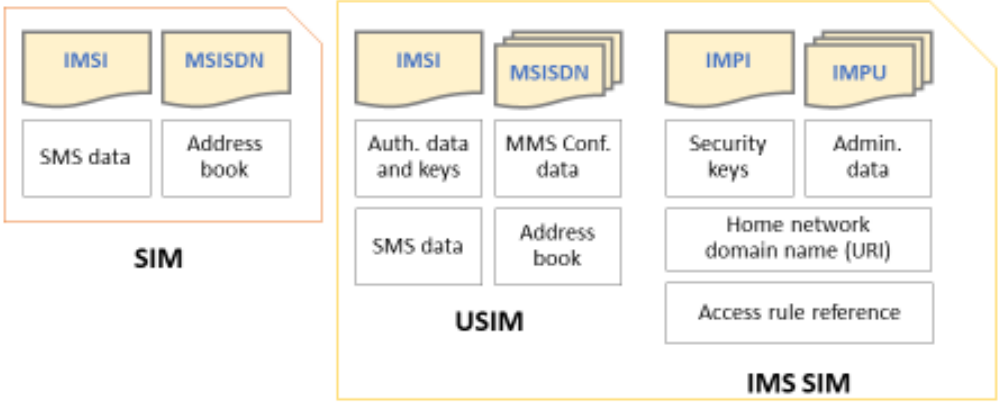
**2020's (2019) - 5G**
- 探索垂直領域應用：企業專網、工業物聯網、關鍵任務（行控/公安/電網）

**2030's (202?) - 6G**
- Digital Twins, Mixed Reality, Metaverse, Tactile Internet, Telepresence, ...

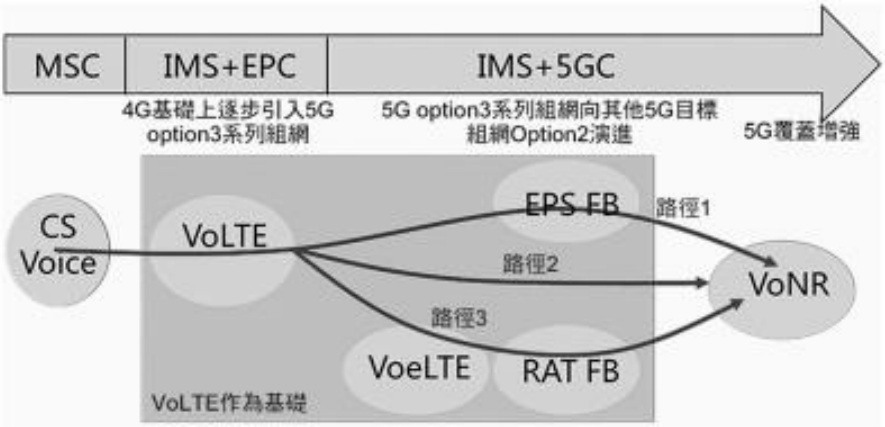
## 行動通訊系統的演進：信令、服務及識別

| 2G/3G CS + PS | 4G EPS + IMS* (All-IP, CUPS) | | 5G 5GS + IMS* (All-IP, CUPS, SBA) | |
|---|---|---|---|---|
| SS7 | Diameter | | HTTP/2 | |
| Voice call, SMS, Basic Data Services | VoLTE*, SMS*, Mobile Broadband | | VoNR*, SMS*, eMBB / mMTC / uRLLC | |
| HLR / VLR | HSS | IMS | UDM | IMS |
| MSISDN (ITU-T E.164), IMSI (ITU-T E.212) | MSISDN, IMSI | IMPI, IMPU | MSISDN, IMSI | IMPI, IMPU |

## 行動通訊系統的演進：用戶識別卡

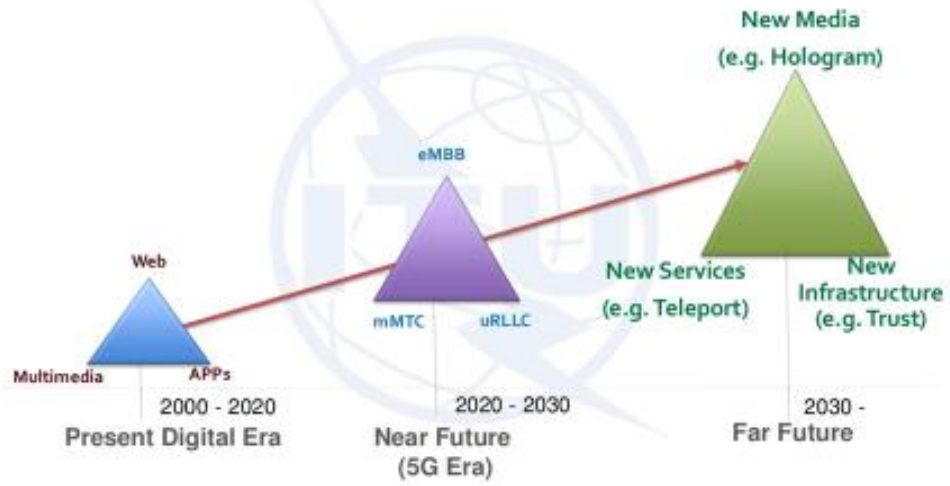


# 行動通訊系統的演進：語音通話服務

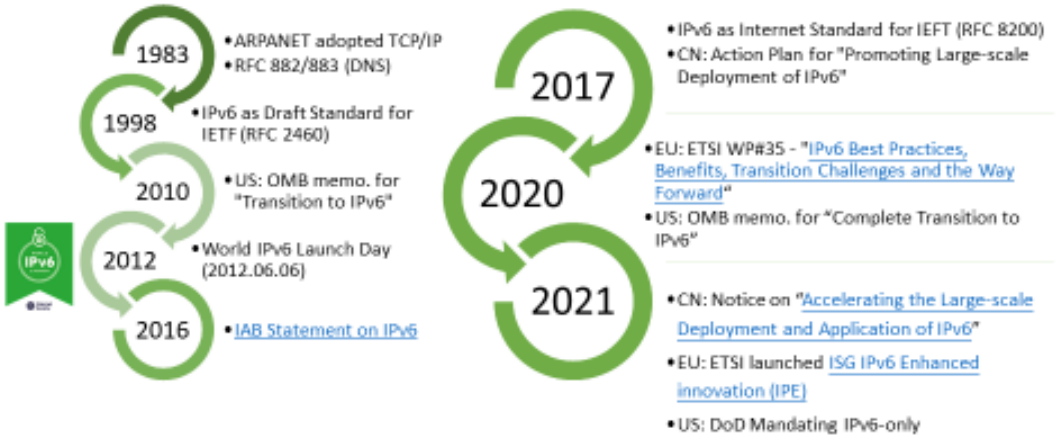



# 行動通訊系統的演進：訊息服務

# 行動通訊系統的演進：下一步?




# 網際網路的唯一識別碼：IP位址



# 從IPv4過渡到IPv6：現況

https://public.tableau.com/app/profile/rene.wilhelm/viz/APNICIPv6changes/Dashboard1

# 物聯網識別碼的發展：命名機制

**應用層**

- **應用識別碼**：用於識別物聯網各項應用服務組成元素
  - 業務接取號碼、資訊服務接取功能變數名稱或位址等
  - 可使用功能變數名稱、URL 等。

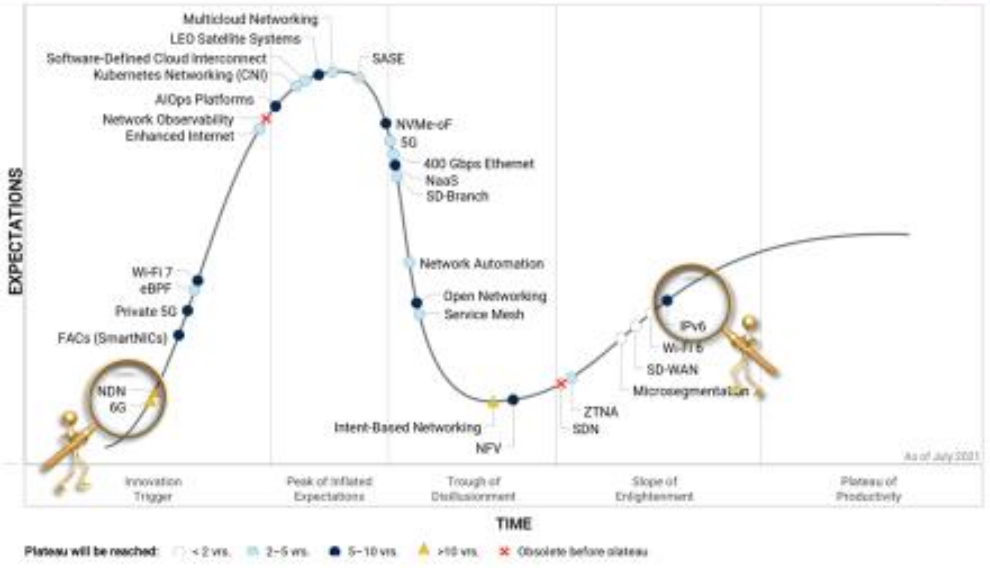
**網路層**

- **通訊識別碼**：用於識別具備通訊能力的網路節點
  - 使用者手機、RFID 讀寫器、感測器節點、網路設備等
  - 可使用E.164號碼、IP位址等

**感知層**

- **物件識別碼**：用於識別各種實體資源
  - 被動式：條碼（EAN碼、UPC碼、128碼）、RFID無線射頻標籤（EPC碼、ucode碼）
  - 通過人機介面從物聯網終端獲取：物件識別碼（OID）、統一資源名稱（URN）、數位物件架構/識別碼（DOA/DOI）、Handle 等

# Gartner: 企業網路技術成熟度曲線




https://www.gartner.com/doc/reprints?id=1-26Y6WGOP&ct=210726

# 小結：

| | |
|---|---|
| E.164號碼 | 持續使用於語音通話、訊息收發等電信服務（用戶識別） |
| E.212號碼 | 持續使用於終端設備接取網路的AAA機制（設備識別） |
| IP位址 | • IPv6協定加速過渡（替代IPv4）<br>• 將更廣泛地使用於包括5G、Internet、物聯網裝置等所有連網設備（設備識別） |
| 網域名稱 | • 通用頂級域名 (gTLDs) 具備全球辨識性（無地域限制）<br>• DNS作為Internet的重要基礎設施之一，持續穩定運作及提升其安全性仍是研究的重點。 |
| 物聯網號碼技術 | • 除提供連網物件的定址和識別等功能，並能在各種通訊協定間進行轉換，來達到資訊存取與傳遞的目的。<br>• IP位址, 網域名稱/域名解析系統 (DN/DNS), 統一資源名稱 (URN), 其它... |

# 捌、第二場「下世代電信號碼政策及資安機制」專家座談會

## 一、第二場座談會簡介及議程

隨著下世代電信網路技術來臨，國際電信聯盟電信標準化部門(ITU-T)下的 2030 網路技術焦點組，於 108 年 5 月發表「科技、應用及 2030 市場驅動藍圖」，揭櫫未來 2030 年新興科技應用趨勢、願景、重點發展領域及對既有網路之影響，而世界各國當前的資安政策，也陸續因應未來網路、社會、經濟發展面向，並規劃及確立國家網路安全總體政策脈絡與資安體制發展。

有鑑於此，我國行政院於 108 年 5 月 10 日核定「台灣 5G 行動計畫」（108 年至 111 年），其中為完備 5G 技術核心及資安防護能量，制訂 5G 資安國家整體政策，打造 5G 國產品資安防護機制，並強化 5G 關鍵基礎設施及營運資安防護能力，推動國內廠商進入國際 5G 可信賴供應鏈。

交通部為掌握我國下世代電信號碼資安稽核機制，蒐集相關下世代電信號碼管理系統安全及跨網互通安全政策建議，因此透過座談會邀集國內產官學研界專家學者，廣泛並深入瞭解各界意見。

財團法人電信技術中心承接交通部 110 年度「下世代電信網路號碼技術研析及管理」委託研究計畫，將於 8 月 26 日（四）舉辦線上專家座談會，針對下世代電信號碼政策及資安機制議題，邀請各方專家代表出席討論，希冀廣納各方意見，以充實本案研析報告並提供主管機關未來政策評估之參考。

| 時間 | 議程 | | 主講人 |
|---|---|---|---|
| 13:30-14:00 | 報到 | | |
| 14:00-14:05 | 主持人開場 | | 電信技術中心<br>卜慶玲副執行長 |
| 14:05-14:35 | 引言報告 | 下世代電信網路號碼技術發展下之政策初探 | 電信技術中心<br>陳志宇資深經理 |

| 時間 | 議程 | | 主講人 |
|---|---|---|---|
| 14:35-15:15 | 引言報告 | 下世代電信網路號碼資安威脅及電信資安稽核機制初探 | 電信技術中心<br>莊淑閔主任 |
| 15:15-16:20 | 專家座談意見交流 | 討論題綱：<br>1. 下世代電信網路號碼技術發展下之政策建議綜合討論<br>2. 下世代電信號碼管理系統安全及跨網互通安全政策討論 | 電信技術中心<br>卜慶玲副執行長 |
| 16:20-16:30 | 主持人總結 | | 電信技術中心<br>卜慶玲副執行長 |

## 二、第二場座談會會議紀錄

(一) **主持人**：財團法人電信技術中心 卜慶玲副執行長

(二) **會議時間**：2021 年 8 月 26 日（四）下午 2 時 00 分

(三) **會議地點**：線上會議

(四) **與會成員**：交通部郵電司、經濟部工業局、國家通訊傳播委員會、台灣資通產業標準協會、財團法人工業技術研究院、國立臺灣科技大學電子工程系王瑞堂、國立臺灣科技大學電子工程系陳文雄、國立成功大學電信管理研究所陳文字、國立臺北護理健康大學資訊管理系陳彥宏、國立宜蘭大學資訊管理系陳麒元、中華電信股份有限公司、台灣大哥大股份有限公司、台灣之星股份有限公司、亞太電信股份有限公司、遠傳電信股份有限公司、台灣諾基亞通信股份有限公司、台灣愛立信股份有限公司、財團法人電信技術中心

(五) **會議紀錄**：彭俞蓉助理研究員、郭怡萱助理管理師

(六) **會議討論議題**：

**引言報告：「下世代電信網路號碼技術發展下之政策初探」及「下世代電信網路號碼資安威脅及電信資安稽核機制初探」**

1. 朱建國協理(遠傳電信股份有限公司)：依據簡報所示 DNS 服務(Domain Name Service)偏向關鍵基礎設施，然而該服務應明確定義提供者是 ISP 業者或是應用服務業者，倘若是應用服務業者則提供服務機制及系統，有可能透過跨境服務的方式，而該模式我國政府規管較為不易，因此我司建議研究團隊應將 DNS 服務業者先清楚界定後，再進一步分析相關服務規管事宜。
2. 卜慶玲副執行長(財團法人電信技術中心)：根據遠傳電信上述建議初步回覆，在台灣 DNS 解析服務是財團法人台灣網路資訊中心(簡稱 TWNIC)處理，事實上 DNS 目前是由國際組織 ICANN 管理。
3. 紀廷運副理事長(中華民國電腦學會)：Domain Name 除透過 TWNIC 管理外，也是全球互通的資源，此外全球或是任何業者均可使用 DNS 編碼，因此建議未來若將 DNS 作為重要唯一識別碼，可能需要更明確的資源分配及嚴謹的法規規範。
4. 朱建國協理(遠傳電信股份有限公司)：呼應上述紀廷運副理事長說明，若我國擬將 DNS 作為重要的唯一識別碼，建議應有一套完整的規管機制，此外若 DNS 服務業者不在我國，則無法對 DNS 進行解析，因此須建立 DNS 服務提供商之相關管理機制。
5. 劉莘相董事長(網路中文資訊股份有限公司)：目前全世界網域名稱僅中國有完整實名制，換言之台灣的網域名稱註冊資料是沒有完整實名制的；另外，我國政府若針網域名稱實施實名制，也僅能對 TWNIC 核發的.tw、.台灣系列進行管理，而 TWNIC 核發的網域名稱僅佔全台灣使用的近六成，政策法規的有效性與普遍適用性尤須評估；第三點則是必須考慮到 DNS 解析服務管制是否提供公平競爭之轉換機制。

**針對國際下世代電信網路技術發展趨勢下，我國電信網路的通訊安全、裝置安全可能面臨之威脅與挑戰為何？**

1. 陳彥宏副教授(國立台北護理健康大學)：目前網路服務及硬體服務，會產生多的號碼，這些多個號碼可能來自跨組織、跨國業者，請問計畫團隊是否有針對該議題，提出一個處理原則? 號碼管理是否有信託代理的

制度?其責任歸屬為何?

2. 陳志宇資深經理(財團法人電信技術中心)：事實上若牽涉到國外業者，政府規管力道確實會受到影響，這個計畫團隊會納入研析議題。
3. 戴豪君副教授(世新大學)：
   (1) 在電信管理法第 5 條，提供電信服務，且有與他電信事業進行互連協商或申請裁決、申請核配第 56 條規定以外之無線電頻率、申請核配設置公眾電信網路之識別碼或信號點碼及申請核配用戶號碼行為之一者，應向主管機關辦理電信事業之登記，其中申請核配設置公眾電信網路之識別碼、信號點碼之公眾網路識別碼及申請核配用戶號碼，為目前討論之編碼原則標的，換言之，在決定識別碼的範圍時，主管機關應有對應的管理措施。
   (2) 再者，有關 E.164、E.212、DNS、NDN 等編碼，目前電信管理法分為兩種管制模式，一是「電信號碼核配及管理辦法」及電信管理法第 71 條，需由法人組織辦理，換言之，上述編碼是規管力道較強。第二種是「網際網路位址及頂級網域名稱註冊管理業務監督辦法」，為公私協力治理的方式，兩種規範之規管強度不同，而未來是否會有第三種管制方式及何種管制模式，提供後續議題討論。
   (3) 另外，過去 DNS、NDN 域名的名稱本身可能具有意義(或是具有商標名稱)，因此涉及到智財權的爭議，建議將該議題納入研究方向。
   (4) 最後建議從資安角度，觀察歐盟近期更新 NIS2 修訂草案，歐盟將 DNS 納入政府監管及查詢措施，這部份建議可納入研究議題。
4. 葉榮明部經理(台灣大哥大股份有限公司資通訊暨個資安全管理處)：
   (1) 從資通安全面來看，第五代行動通訊系統資通安全維護計畫參考框架，NCC 與 TTC 在相關風險論述有深入的探討，針對 5G 系統面臨的資通安全風險、威脅與挑戰，各家業者皆有依資通安全框架要求，規劃資通安全防護措施，以因應上述的風險議題，相關簡述如下：

   A. 缺乏通訊技術及產品品質保證、單一供應商之依賴性、供應鏈上下游之依賴性及第三方對於供應鏈之干預。
   B. 物聯網設備攻擊 5G 系統，與 3G、4G 系統整合面臨既有 3G、4G 系統之風險。

C. 提供第三方服務提供者多重接取邊緣運算服務，或開放允許設置之相關系統於 5G 系統網路邊緣，可能產生的資源濫用、翻牆、滲透與入侵等風險。

D. 租用或共用他方之傳輸線路，包含線路提供者，或是線路共用所可能帶來的風險。

E. 網路切片可能遭受惡意攻擊威脅。

(2) 從網路技術面來看，電信網路於 5G 技術發展下，全面朝向 IP 化與虛擬化，分析最主要威脅與挑戰如下：

A. 設備的威脅：由於設備本身為虛擬化軟體，以軟體做為出發點攻擊是主要的威脅，種類有透過軟體漏洞、病毒、木馬等手法。因此除了公司內部須教育全體員工資安觀念外，同時設備原廠也必須保證符合國際標準資安認證，並定期進行弱點掃瞄與滲透測試，確保軟體的安全性。

B. 裝置的威脅：主要來自於客戶裝置上的不法軟體 APP、漏洞、病毒、木馬等，由於一般客戶端資安觀念薄弱，裝置端相較於設備端更容易成為資安破口，尤其現今行動電子商務盛行，除個資竊取外，行動支付盜刷事件也層出不窮。另外是 IoT 物聯網裝置，由於成本相對低廉，資安功能也較少，容易被發動大量 DDoS 攻擊。因此除不定期舉辦資安說明會、媒體文宣加強宣導及教育客戶資安觀念外，在網路端也須有資安防護機制。

5. 劉莘相董事長(網路中文資訊股份有限公司)：相較中國，我國政府或業者參與國際性技術組織的力道稍有不足，對相關技術的掌握，大多在相關技術標準成形後，再依循著指導文件(RFC)採用，較缺乏創新性的想法及思維，不易取得先機。

**一、我國下世代電信網路號碼技術發展之政策建議為何？**

1. 連彥宗高級研究員(中華電信研究院寬網所)：

(1) 關於物聯網使用 E.164 的配置，建議維持現狀指配專區方式，並且核配到最大碼長(040xxxxxxxxx)，如此可達 1 百億的容量。指配的數量上可以用小區塊，如萬或千為單位，以減少分割損失，提高配出號碼使用率。專用區塊也可在未來有新技術出現時(如 DNS)，可

整批轉換，不影響既有 E.164 在網路上的運行。

(2) 在配發的管理政策上，針對機器與人的物聯網號碼提供不同核發政策。關於 E.212 的部分，因為 MNC 為稀有資源，建議仍配給予電信業者，再從管理規則的制定來確保物聯網的永續發展。

2. 葉榮明部經理(台灣大哥大股份有限公司資通訊暨個資安全管理處)：目前電信產業採用 E.164 編碼，對下世代嶄新的電信環境恐有不敷使用之疑慮，有鑑於國際組織未來可能使用網域名稱系統取代 E.164 編碼，相關政策應與國際接軌並保持彈性。

3. 劉莘相董事長(網路中文資訊股份有限公司)：建議多加關注相關國際組織(ITU、IANA(PTI)、ICANN)在該議題的討論，以利作為我國下世代電信網路號碼技術發展之政策參考。

**二、下世代電信網路安全與稽核重點探討：跨網互通（網路切片之內網、外網）、營運科技系統（Operational Technology）、工控系統、IoT 物聯網應用場景的資安需求下，建議的稽核重點為何?**

6. 郭憲誌總經理(代表中華民國資訊安全學會)：

(3) 跨網互通，外網到內網仍需要縱深防禦及避免單點失效造成營運中斷，外網相關資安防禦設備，內網區隔及備援機制等，可採用識別、偵測、防護、應變四個構面去思考，並在設備部署，事前、事中、事後階段建立管理制度。

(4) OT及工控系統可依照業務屬性做適當區隔，OT Gateway端的防禦機制及偵測，OT設備白名單機制，降低非授權軟體使用，從OT設備制定設備資安檢查清單，如惡意程式檢測，推行實驗室資安設備檢測標章機制，OT設備部署前再執行資安測試確認，測試通過後再移轉至營運區降低風險，定期設備資安檢測配合軟體白名單機制可大幅度降低營運衝擊。

(5) IoT物聯網應用場景則是前三項的整合，從設備購買時可推行實驗室檢測標章制度，到場域運用的部署資安測試再確認，再到全場域網路規劃相關的設定、變更管理都需要有預先檢測項目，經確認後再執行。只是場域有分大小，大場域需要檢測的行程會很長，倘若只有部分資安公司或實驗室，則效果較難彰顯成效。

7. 許真民工程師(中華電信網路處)：有關跨網互通，包括切片內網及外網，有以下幾點說明。
   (1) 網路切片應有其對應安全分級與對應級別之安全的網路隔離、分片隔離、功能隔離以及資源隔離。
   (2) 網路切片所存取之 Network Function 應具有存取權限限制、服務之間的認證與授權、過濾 以及 SCP(Service Communication Proxy)。
   (3) 網路切片應設有存取限制、對應切片的身分驗證、切片資源分配限制、流量規則與政策。
   (4) 對應的組態設定如共享參數、切片資源限制、切片組合方式等應禁止客戶變更設定，並設有良好的驗證與變更流程。
   (5) 跨網或跨電信商通訊的輔助驗證或者其他自訂介面等所需資料或參數(如 Header Information)應有對應良好的數位資源命名管理。
   (6) 網路切片之間若存在不可避免的通訊，需嚴格限制且定義, 每個切片必須作為一個單獨的網路進行獨立管理。
   (7) 切片必須具有獨立的安全功能，例如根據服務而制定的防火牆規則、存取策略、資料檢查等，並使用全新且獨立的金鑰進行加密保護。
   (8) 若網路切片之營運管理系統須提供外部系統介接，需採取點對點最小限縮開放原則，並給予最小所需之 API 權限，輔以日誌機制以利稽核。
   (9) 網路切片運行之雲平台，需進行必要之資訊安全防護機制與安全組態設定。
8. 謝文生主任級研究員(中華電信研究院智聯所)：目前網路上運行的主要稽核重點取決於可否區分為物聯網應用或非物聯網應用？若可區分，則需要另外制定專門用於物聯網應用的網路安全規範；否則應可直接參考一般的網路安全規範、較不會有執行上如何認定的議題。除了上述的網路安全外，物聯網應用所使用的終端設備非常多元，有固定式的、有移動性的、有高階的、有低階的，不一定會有(完整)作業系統、也不一定會有固定 IP，但一般最後都會串接使用到公眾的網際網路，應較有可能需要一合適的出廠檢驗規範、來確保網路安全。
9. 葉榮明部經理(台灣大哥大股份有限公司資通訊暨個資安全管理處)：
   (1) 以往 OT 設置隔離封閉之網路及專用軟硬體架構，該架構遭受外部

攻擊可能性較低，但未來物聯網在連網及互聯需求持續增長下，恐導致安全風險產生變化。

(2) 工業系統的生命週期通常較長，系統設計製造以穩定運作目標為優先，較少納入安全需求考量，原廠傾向避免軟硬體異動，如要停機來執行安全更新，恐導致系統無法運作產生重大損失。上述條件限制下，系統可能充滿安全漏洞，一但連上網路，既有防護水準無法抵擋物惡意攻擊；為降低連網風險，安全防護觀念與等級必須提升與改變，包含軟體安全、上下游供應鏈安全性、防範惡軟體機制、組態配置與安全修補、開發測試與線上區隔、實體安全防護、存取控制、身分驗證、遠端連線安全等等議題，可能都需要仰賴先前在 Internet 系統的經驗作強化，以及作為內部控制與稽核查核重點。

(3) 無論是 OT 或 IoT 應用場景，在網路功能、擴展性及安全性方面都有特定的需求，包括管理大量設備、提供覆蓋範圍，以及可靠低延遲的通訊。網路切片使前述場景成為可能，透過切片都可針對特定需求進行調整與優化，在流量與資源方面提供了切片之間的隔離與控制，防止不同應用場景互相影響，避免受 DDoS 攻擊；在資源區隔的管控上，防止未授權存取切片資源，確認網路切片管控能力會是查核上的重點。

10. 劉莘相董事長(網路中文資訊股份有限公司)：目前各式各樣的跨網通訊，不僅是在移動網路出現，在物聯網上更是因為個別設備的工作及發展特性不同，所以有不同的通訊協定及安全標準，建議在研析一體適用的稽核工具前，應充分研析及紀錄行動網路及物聯網路的應用情形，以利綜整及分析相關資訊較為妥適。

**不同網路需求下之資安稽核概念援用：資訊安全管理系統（Information System Management System, ISMS）與（自動化）工業控制系統（Industrial (Automation) and Control System, I(A)CS）、（自動化）監控與數據採集系統（ Supervisory Control and Data Acquisition, SC(A)DA）之間的關聯、管理概念是否可相容與交互應用？可如何引用適用?**

6. 郭憲誌總經理(代表中華民國資訊安全學會)：依照目前的各管理制度來看，都有發展出一套檢核項目，而不同管理機制個人認為是可相容，其理由在於在制定查核表時，均從識別、偵測、防護、應變等四個構面去思考，而設備之事前、事中、事後部署及管理機制等流程。例如事前的規劃，大部分都是規劃導入設備，而這一段其實可以藉由實驗室設備檢測，讓乙方可以採購已經合格的資安產品；而事中、事後階段可採用定期進行環境安全檢測跟日常維運相關資安落實度查核，搭配監控裝置確認各設備的狀況，另外就是資安意識教育訓練、變更管理、委外管理及緊急應變演練來強化營運管理能力。
7. 陳銘德工程師(中華電信網路處)：基本上資安防護應該針對其特性和重點，並選擇適當的稽核標準，例如 ISO 27001 的稽核項目就比較偏 IT，而 IEC 62443 工控資安標準則偏 OT 方面，雖然其管理概念大致相通，但實施上仍有其差異，考量資源有限的情況下，一般通常建議將資源先投入於關鍵項目上，針對場域特性選擇適當的標準來落實，當然若組織內很複雜，既有 IT 又有 OT，建議應各自挑選適當的標準導入。
8. 葉榮明部經理(台灣大哥大股份有限公司資通訊暨個資安全管理處)：
   (1) 製造業或工業不同產業別，倘若導入 ISO 27001 通用性的資通安全標準，則可提供資通安全管理的架構；但對於提升特定產品安全，仍需要參考專用標準，方能貼近產業特性，例如電信業依循 ISO 27011 標準、工業自動化及控制系統產業依循 IEC 62443 標準。
   (2) IEC 62443 標準著重於產品開發的流程、服務及系統整合，雖然與 ISO 27001 的著重面向不同，但在部分的安全控制項目可對照使用，例如組態管理可視為 A.12 的延伸，事件管理可搭配 A.16、A18 的查核等。故 ISO 27001 可用於保護工業系統的資通安全；然而，若將焦點專注於確保工業系統開發過程，即可評估 IEC 62443 定義的安全控制項目。透過 ISO 27001 管理制度評估重要性及風險，再把資源放在較優先處理的部分，並利用 IEC 62443 的安全規範，以評估及延伸查核項目。
9. 劉莘相董事長(網路中文資訊股份有限公司)：在探討本題之前，先行概述資安稽核概念之間的目的及差異，首先 ISMS 的核心精神是 PDCA 循環檢核及改善的過程(Plan-Do-Check-Action)，其目的改善流程及管理品質；而 IACS((Industrial Automation and Control Systems/工業自動化和控

制系統)目的是確保工業控制設施的各種運作具有可用性和安全性；SDCA(Standardize-Do-Check-Action)則是標準化和維持穩定運作的流程；PDCA 是使企業管理效能不斷提升的驅動力；SDCA 則是防止企業管理效能下滑的制動力；IACS 則是確保整體企業運轉的可靠性及安全性，這三者可以組成穩定(IACS)-改進(PDCA)-維持(SDCA) 的工作循環，可以讓企業不斷穩定的向上提升。沒有標準化措施，企業就無法維持在較高的管理效能。

(七) **散會：下午 4 時 30 分**

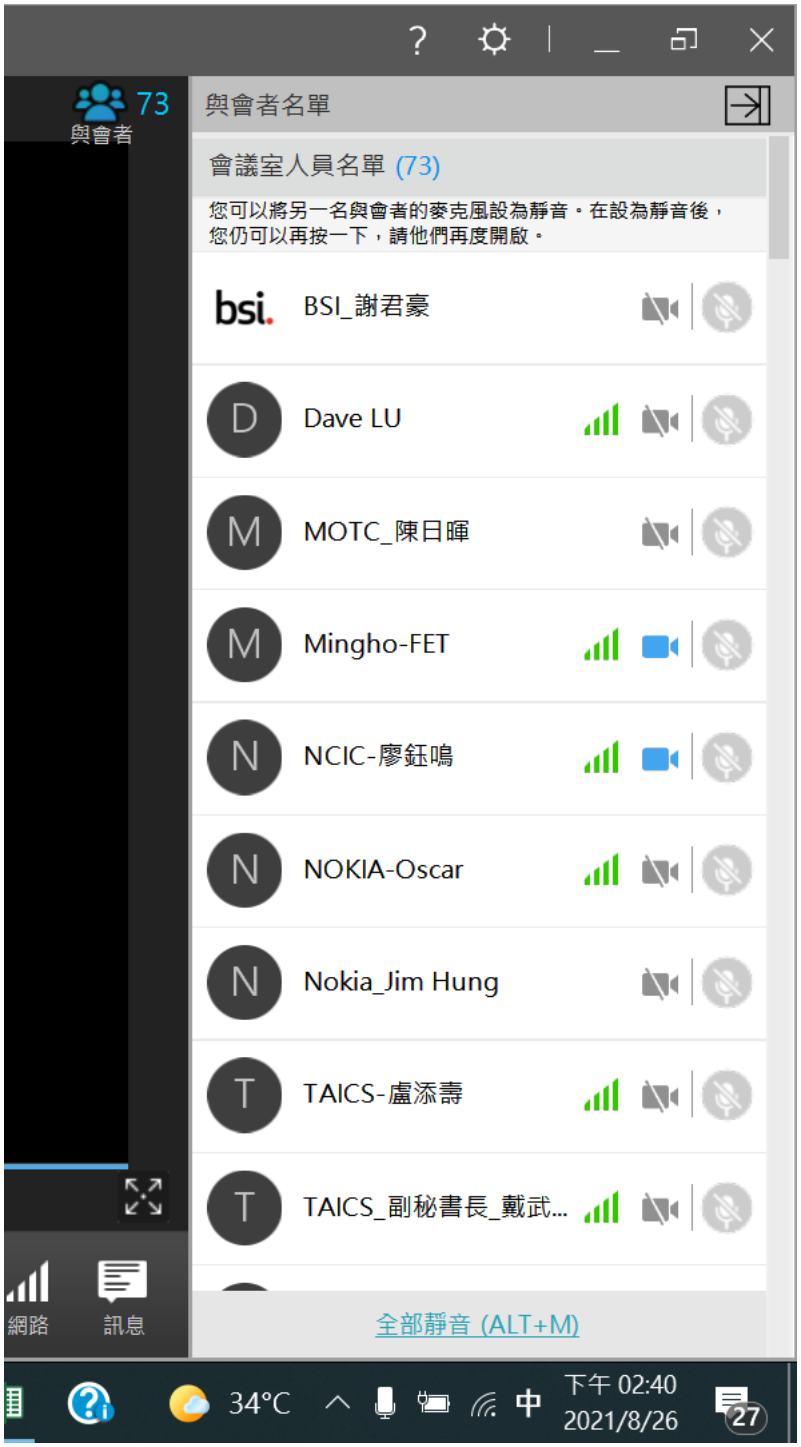
(八) **參與人員名單及簽到表**

| 編號 | 單位 | 姓名 | 職稱 |
|---|---|---|---|
| **政府機關** | | | |
| 1. | 交通部郵電司 | 林姝宜 | 專員 |
| 2. | 交通部郵電司 | 蕭家安 | 科長 |
| 3. | 交通部郵電司 | 陳日暉 | 技士 |
| 4. | 國家通訊傳播委員會<br>射頻與資源管理處 | 林永浴 | 科長 |
| **公協會** | | | |
| 5. | 中華民國電腦學會 | 紀廷運 | 副理事長 |
| 6. | 台灣電信產業發展協會 | 劉莉秋 | 副秘書長 |
| 7. | 台灣資通產業標準協會 | 戴武聰 | 副秘書長 |
| 8. | | 盧添壽 | 副處長 |
| 9. | 國立臺灣科技大學 | 羅乃維 | 教授 |
| 10. | 國立宜蘭大學 | 陳麒元 | 副教授 |
| 11. | 理律法律事務所 | 曾更瑩 | 律師 |
| 12. | 國立台北護理健康大學 | 陳彥宏 | 助理教授 |
| 13. | 世新大學 | 戴豪君 | 副教授 |

| 編號 | 單位 | 姓名 | 職稱 |
|---|---|---|---|
| **電信業者** | | | |
| 14. | 中華電信網路處 | 白洪政 | 高級工程師 |
| 15. | 中華電信網路處 | 陳瑞全 | 高級工程師 |
| 16. | 中華電信網路處 | 陳銘德 | 工程師 |
| 17. | 中華電信經營規劃處 | 梁銘顯 | 高級工程師 |
| 18. | 中華電信法務處 | 李之軍 | 高級工程師 |
| 19. | 中華電信研究院無線所 | 張容程 | 研究員 |
| 20. | 中華電信研究院寬網所 | 連彥宗 | 高級研究員 |
| 21. | 中華電信行分經營規劃處 | 林永勝 | 高級工程師 |
| 22. | 中華電信 | 王阜毓 | |
| 23. | | 林尚達 | |
| 24. | | 王奕勛 | |
| 25. | | 蔡佩彣 | |
| 26. | 台灣大哥大股份有限公司<br>系統設計處 | 侯全成 | 部經理 |
| 27. | 台灣大哥大股份有限公司<br>系統設計處 | 胡政嘉 | 資深主任工程師 |
| 28. | 台灣大哥大股份有限公司<br>資通訊暨個資安全管理處 | 葉榮明 | 部經理 |
| 29. | 台灣大哥大股份有限公司<br>資通訊暨個資安全管理處 | 瞿鴻斌 | 高級管理師 |
| 30. | 台灣大哥大股份有限公司<br>法規暨同業關係處 | 林瀚杰 | 副理 |
| 31. | 台灣之星電信股份有限公司 | 陳明勇 | 處長 |

| 編號 | 單位 | 姓名 | 職稱 |
| --- | --- | --- | --- |
| 32. | 台灣之星電信股份有限公司 | 王志強 | 經理 |
| 33. | 台灣之星電信股份有限公司 | 許正倫 | 經理 |
| 34. | 台灣之星電信股份有限公司 | 葉兆軒 | 專案工程師 |
| 35. | 台灣之星電信股份有限公司 | 馬文怡 | 資深專案<br>工程師 |
| 36. | 台灣之星電信股份有限公司 | 任致遠 | 專案副理 |
| 37. | 亞太電信股份有限公司 | 方俊傑 | 經理 |
| 38. | 亞太電信股份有限公司 | 張佰芳 | |
| 39. | 亞太電信股份有限公司 | 許鈺宸 | |
| 40. | 遠傳電信股份有限公司<br>法務法規暨採購群 | 廖鈺鳴 | 資深專員 |
| 41. | 遠傳電信股份有限公司<br>法務法規暨採購群 | 黃漢臣 | 經理 |
| 42. | 遠傳電信股份有限公司 | 郭禾蓁 | |
| 43. | | 高家惠 | |
| 44. | | 陳榮志 | |
| 45. | | 侯淑婉 | |
| 46. | | 陳素齡 | |
| 47. | | 徐子祥 | |
| 48. | | 朱家銘 | |
| 49. | | 陳名河 | |
| 50. | | 朱建國 | |

| 編號 | 單位 | 姓名 | 職稱 |
| --- | --- | --- | --- |
| 產業代表 | | | |
| 51. | 勤業眾信聯合會計事務所風險諮詢服務 | 林彥良 | 副總 |
| 52. | BSI 英國標準協會台灣分公司 | 謝君豪 | 營運長 |
| 53. | 網路中文資訊股份有限公司 | 劉莘相 | 董事長 |
| 54. | 台灣諾基亞通信股份有限公司 | Jim Hung 洪牧村 | Sales Solution Consultant, Cloud & Network Services, Nokia Taiwan |
| 55. | 數聯資安股份有限公司 | 郭憲誌 | 總經理 |


73
與會者
與會者名單
會議室人員名單 (73)
您可以將另一名與會者的麥克風設為靜音。在設為靜音後，
您仍可以再按一下，請他們再度開啟。
BSI_謝君豪
Dave LU
MOTC_陳日暉
Mingho-FET
NCIC-廖鈺鳴
NOKIA-Oscar
Nokia_Jim Hung
TAICS-盧添壽
TAICS_副秘書長_戴武...
全部靜音 (ALT+M)
網路
訊息
34°C
中
下午 02:40
2021/8/26
27

73
與會者
與會者名單
TST-資深專案工程師-馬文怡
TST_工程師_Jack Yeh
TST_經理_王志強
TST_許正倫
TTC-副執行長-卜慶玲
主持人
TTC-副管理師-簡嘉儀
TTC-研究員-王彥中
TTC-莊淑閔主任
TTC_副管理師_陳佳瑀
TTC_助理研究員_夏.....
網路
訊息
全部靜音 (ALT+M)
34°C
中
下午 02:40
2021/8/26
27

74
與會者
與會者名單
TTC_助理研究員_彭.....
TTC_助理研究員_...
TTC_助理研究員_黃.....
主持人
TTC_助理管理師_...
TTC_林永勝_Bill
TTC_資深經理_陳志宇
TWM 林瀚杰
TWM_部經理_葉榮明
ttc0826
ttc0826
全部靜音 (ALT+M)
網路
訊息
34°C
中
下午 02:41
2021/8/26
27

74
與會者
與會者名單
世新智傳所戴豪君
中華_高級工程師_林永勝
中華李之軍
中華民國資安學會/數...
中華民國電腦學會 紀.....
中華電 王奕勛
中華電信 工程師 陳銘德
中華電信 連彥宗
中華電信_張容程
中華電信_林尚達
網路
訊息
全部靜音 (ALT+M)
33°C
下午 02:41
2021/8/26
27

74
與會者
與會者名單
中華電信_梁銘顯
中華電信_王阜毓
中華電信_蔡佩彣
中華電信_高級工程師_白……
亞太-張栢芳
亞太-許文宏
亞太-許鈺宸
亞太_方俊傑
劉莉秋
北護 陳彥宏
全部靜音 (ALT+M)
網路
訊息
33°C
中
下午 02:41
2021/8/26
27

74
與會者
與會者名單
台灣之星-處長-陳明勇
台灣大哥大 主任管理師 瞿.....
台灣大哥大 胡政嘉
台灣大哥大-侯全成
台灣科技大學羅乃維.....
宜大-陳麒元
理律 曾更瑩
網中-劉莘相
網路中文 - Aria
網路中文(ALEX)
全部靜音 (ALT+M)
網路
訊息
33°C
中
下午 02:42
2021/8/26
27

74
與會者
與會者名單
網路中文EVONNE
網路中文 - Tom孟
通傳會_林永裕
遠傳 徐子祥
遠傳 朱家銘Dirk Chu
遠傳 營運支援 侯淑婉
遠傳 郭禾蓁
遠傳 陳榮志
遠傳-高嘉惠
遠傳_陳素齡
全部靜音 (ALT+M)
網路
訊息
33°C
中
下午 02:42
2021/8/26
27

74
與會者
與會者名單
網路中文EVONNE
網路中文 - Tom孟
通傳會_林永裕
遠傳 徐子祥
遠傳 朱家銘Dirk Chu
遠傳 營運支援 侯淑婉
遠傳 郭禾蓁
遠傳 陳榮志
遠傳-高嘉惠
遠傳_陳素齡
全部靜音 (ALT+M)
網路
訊息
33°C
中
下午 02:42
2021/8/26
27

74
與會者
與會者名單
遠傳 朱家銘Dirk Chu
遠傳 營運支援 侯淑婉
遠傳 郭禾蓁
遠傳 陳榮志
遠傳-高嘉惠
遠傳_陳素齡
遠傳電信-黃漢臣
遠傳電信_朱建國
郵電司林姝宜
郵電司蕭家安
全部靜音 (ALT+M)
訊息
33°C
中
下午 02:42
2021/8/26
27

## (九) 產官學研專家座談會會議照片

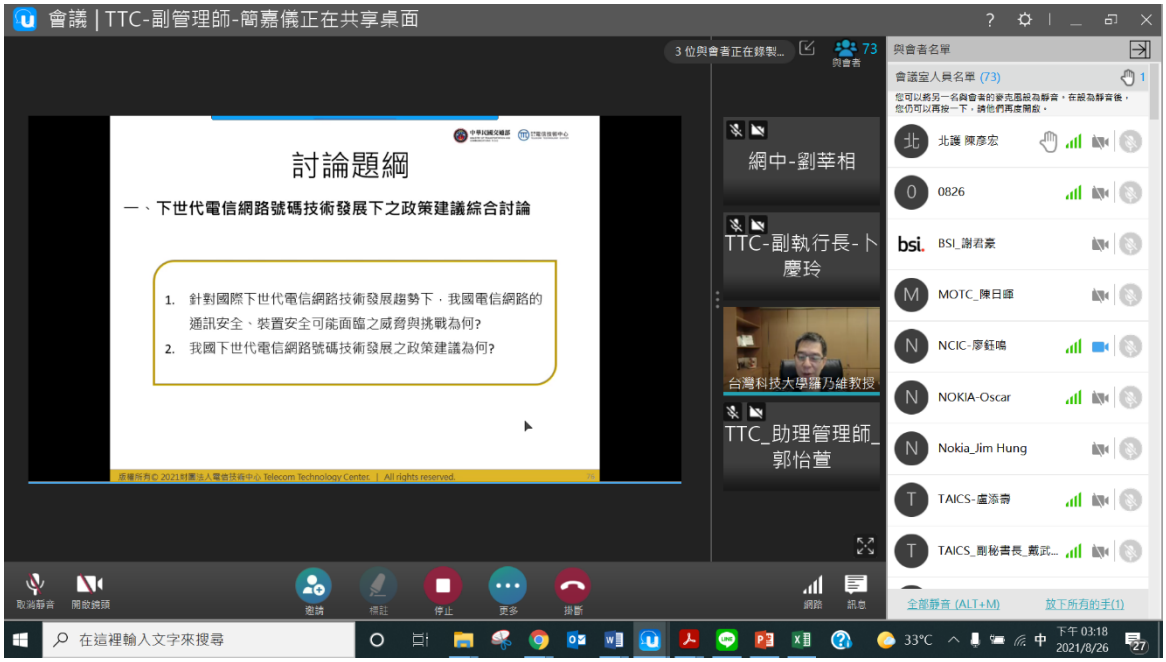



圖 1、羅乃維教授擔任本次專家座談會之主持人

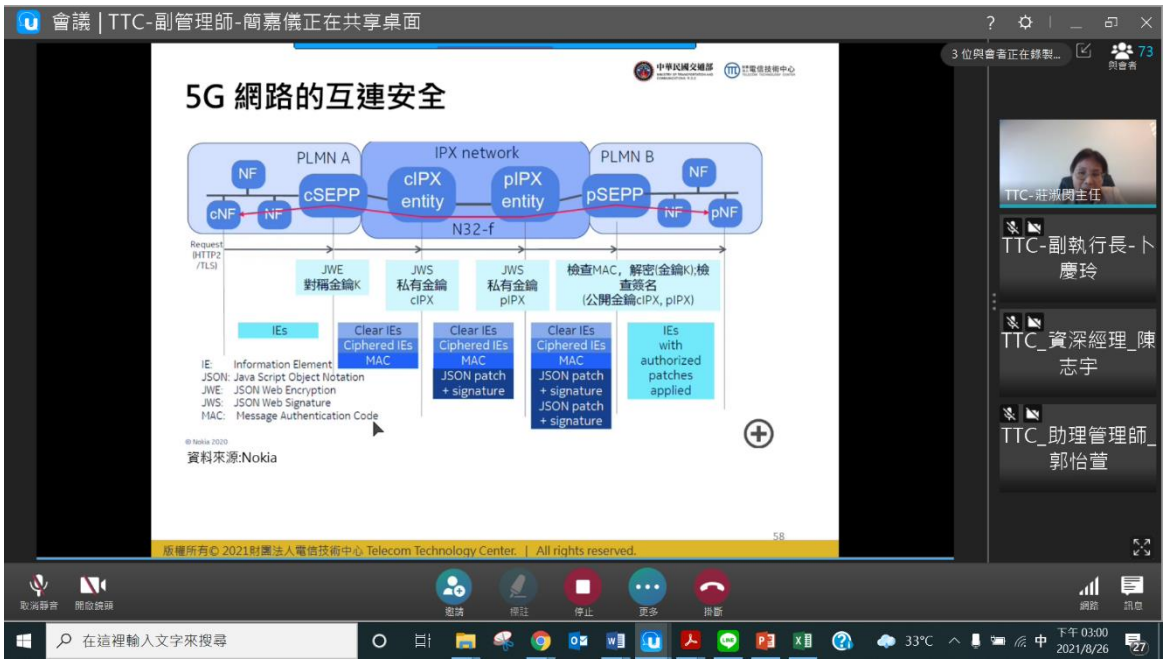



圖 2、本中心資安組莊淑閔主任針對下世代電信網路號碼資安議題進行分享

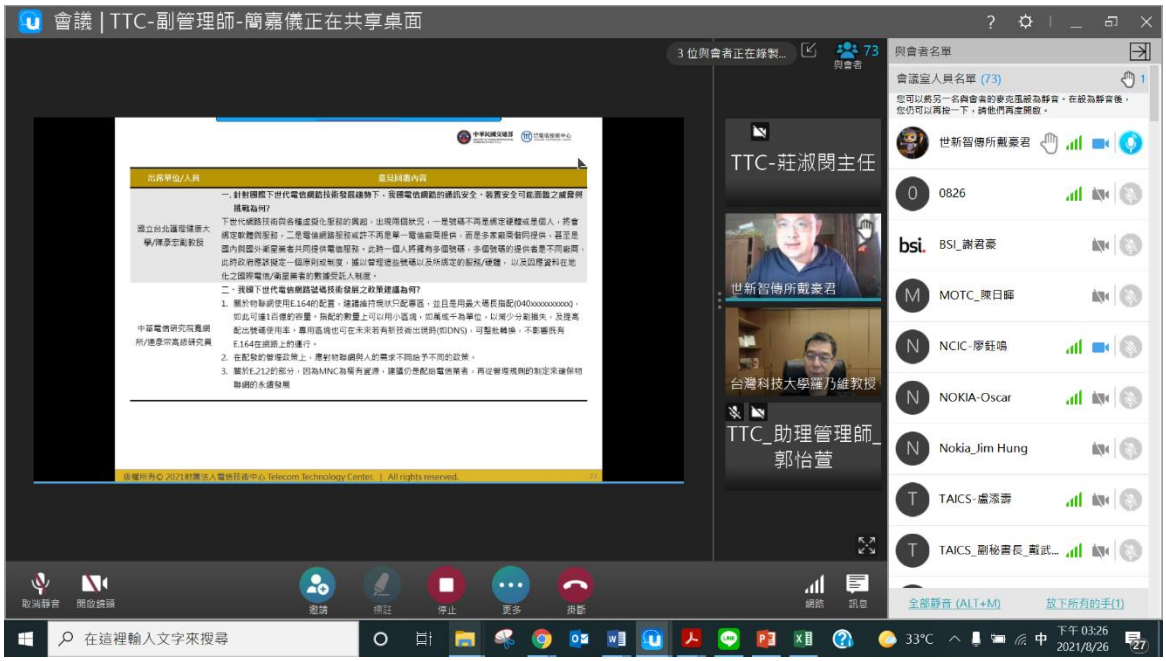
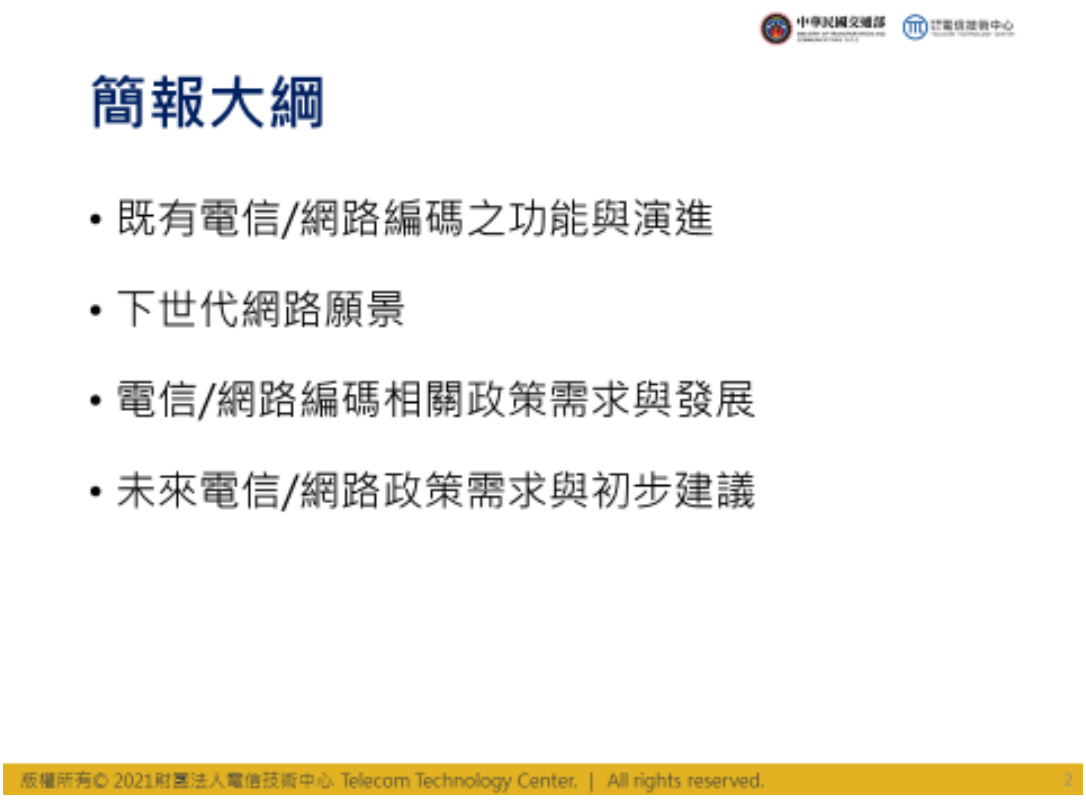



圖 3、世新大學戴豪君副教授就本案議題給予建議與指導

# 三、第二場座談會會議簡報



# 電信及網路編碼的功能與演進

| | 固網 | 行網 | 網際網路 | 物聯網 | 備註 |
|---|---|---|---|---|---|
| 用戶識別碼 | E.164 | E.164 | Domain Name | E.164<br>Domain Name<br>OID/DOA | 分配後變動性低 |
| 通訊技術/協定 | | | TCP/IP | | |
| | 光纖<br>/Cable/xDSL | 4G/5G | | | |
| 通訊對象位址 | 固定路由<br>（硬體內碼） | 基站→E.212<br>（IMSI） | IP Based | IP Based | |
| 識別與位址解析 | 電信網路 | 電信網路 | 網際網路<br>DNS | 網際網路<br>DNS/DOA | 將固定識別轉換至變動位址 |
| 雙向互通 | Y | Y | N | N | |

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 電信及網路編碼的功能與演進

■ 編碼之分配
- **國家監管機關：E.164、E.212**
- **公私協力之中間機構管理：「.TW」Domain Name 、IP位址**
- 商業機制運作：OID、DOA/DOI

■ 網路通訊的互通性需求
- **基礎電話服務（固網、行網）**
- **基礎網際網路（DNS/IP）**

■ 新型態編碼的系統組成（From ITU-T X.1255：Framework for discovery of identity management information）
- 識別/解析系統：identifier/resolution system
- 存儲庫系統：repository system
- 註冊系統：registry system

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 邁向下世代網路網路願景

**01 新垂直應用**

現今網路技術能量將向垂直層級進行更緊密的整合，能滿足高時間感知工程、全自動化等產業應用場景。

**02 新媒介技術**

創新網路技術例如全息投影，滿足民眾在遠距溝通之互動需求，此類技術需要更大容量和更高傳輸能力的網路。

**03 異質網路特徵**

各種異質網路架構逐步成熟，太空網路、行動網路、固網互連，將形成多重網路現象。

**多接取邊緣運算(MEC)的形成**

當MEC此種具智慧性、能協同作業的基礎設施應用漸趨普及，邊緣網路的安全設計須有效提升。

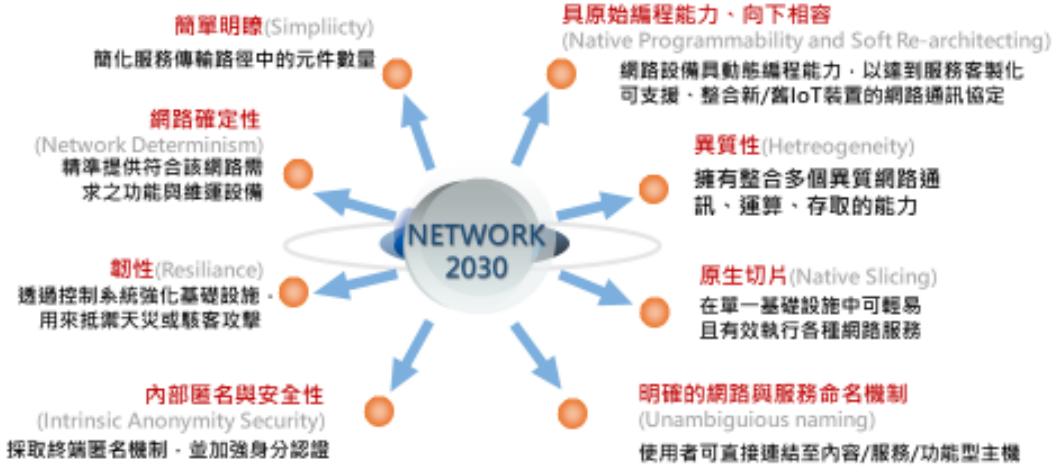
**網路的「路由與定址」更加複雜化**

不同網路層的通訊協定整合，將會更依賴於完善路由與定址設計，使資料快速交換與傳輸。

**04 提高網路韌性、網路服務安全**

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 下世代網路網路應具備之特徵




**簡單明瞭(Simpliicty)**
簡化服務傳輸路徑中的元件數量

**具原始編程能力，向下相容**
(Native Programmability and Soft Re-architecting)
網路設備具動態編程能力，以達到服務客製化可支援，整合新/舊IoT裝置的網路通訊協定

**網路確定性**
(Network Determinism)
精準提供符合該網路需求之功能與維運設備

**異質性(Hetreogeneity)**
擁有整合多個異質網路通訊、運算、存取的能力

**韌性(Resiliance)**
透過控制系統強化基礎設施，用來抵禦天災或駭客攻擊

**原生切片(Native Slicing)**
在單一基礎設施中可輕易且有效執行各種網路服務

**內部匿名與安全性**
(Intrinsic Anonymity Security)
採取終端匿名機制，並加強身分認證

**明確的網路與服務命名機制**
(Unambiguious naming)
使用者可直接連結至內容/服務/功能型主機

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## Network 2030願景下的電信及網路編碼需求

- 明確的網路服務/命名機制
- 傳輸路徑簡單明確
- 強化匿名性、安全性
- 相容性

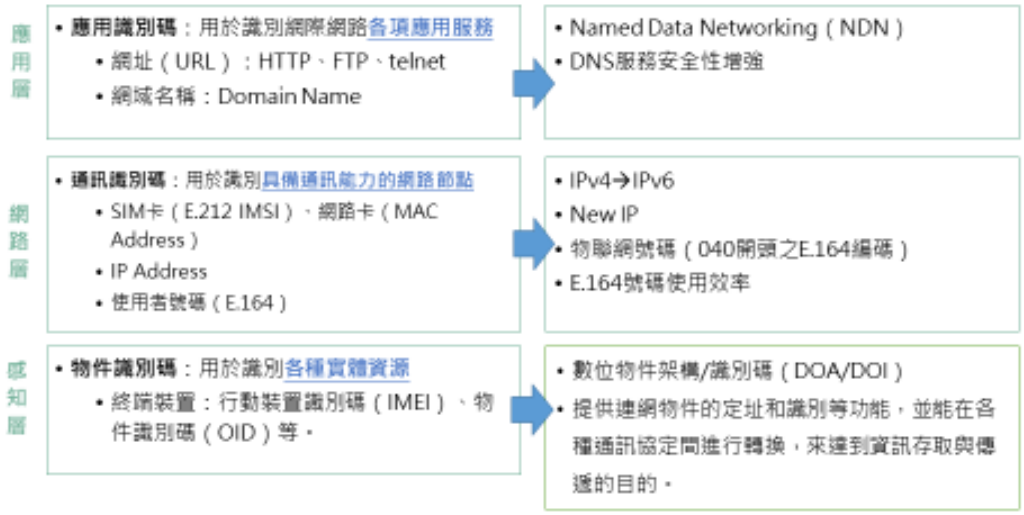
版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

## 各種網路識別碼的功能與議題發展

- 號碼機制演進
  - 新編碼機制的提出
    - NDN、DOA/DOI
  - 既有編碼機制的強化
    - E.164、E.212
    - DN/IP
    - New IP
- 號碼機制的不變需求
  - 具唯一性、全球互通
  - 中立平等的分配管理
  - 在通訊協定間轉換
  - 可彈性納入其他識別需求，如國家、地理區域及服務類型等

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# 各種網路識別碼的功能與議題發展




版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# 各種網路識別碼的功能與議題發展

- E.164：
  - 用於各國基礎電信服務
  - 具唯一性、全球互通
  - 識別用戶
  - 編碼規則中基本含有國家、地理區域及服務類型識別
- 衍生之政策議題：
  - 固網市場萎縮，物聯網及行動網路需求持續上升，
    - 檢討是否維持地理區域的辨識、區碼之整併
    - 臺灣人口及市場規模有限，編碼不足之問題並不嚴重

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# 各種網路識別碼的功能與議題發展

- E.212（國際行動用戶識別碼, IMSI）
  - 用於各國行動電信服務
  - 具唯一性、全球互通
  - 識別服務網路
  - 編碼規則中含有國家及行動網路業者識別
- 行動網路技術演進：
  - 6G or 衛星通訊，業者跨國提供服務之辨識

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 各種網路識別碼的功能與議題發展

■ Doa（Digital Object Architecture）/Doi（Digital Object Identifier）

- 運作結構來自於ITU-T X.1255
- DOA是 Internet結構的邏輯延伸，相較於原本的Internet功能為數位化資訊的傳輸，DOA可進一步支援資訊管理的功能需求，其架構開放，可跨不同的網路平台使用，由DONA基金會所維護。
- 其認證稱為「多重主要管理者（Multi-Primary Administrators, MPA）」
- 其為架構性技術，提供給不同的單位或機構自行開發用途，如DOI屬於國際DOI基金會（INTERNATIONAL DOI FOUNDATION）所開發維護。

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 各種網路識別碼的功能與議題發展

■Named Data Networking（NDN）

- NDN係以資訊為中心的網路結構（information centric networking, ICN），目前仍處於研發實驗階段，其目的為改革既有以IP為基礎（IP-Based）網路的各種問題。
- 概念上，當前網際網路透過DNS系統將網域名稱（Domain Name）轉換為IP，IP的指向通常為儲存資訊的伺服器主機（HOST），而非直接指向資訊；ICN則強化使用者輸入查詢資訊所在，而能直接取得資訊本身。
- 屬於網路運作架構之改變，其以資訊為中心，故其概念上並不仰賴編碼機制。（但在資訊名稱及用語上如何統一是個問題，尤其是中文）

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# 各種網路識別碼的功能與議題發展

■New IP

- 由華為提出
- 在既有的IP通訊基礎上，提出網路傳輸層的技術改進，為通訊協定的技術革新概念
- 因IETF反對，僅提出概念而無任何具體實現

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# 各種網路識別碼的功能與議題發展

■DNS機制的隱私與安全性強化

- DNS的初始設計為DN--IP之解析機制，未考慮安全性與隱私需求。
- 具有廣泛的基礎設施、軟體整合與網際網路的相容性。
- 其名稱之分配管理兼有國家及商業用途。
- 使用廣泛，從而架構不易變動；增強安全性後可能面臨網路效能下降，延遲增加。

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 小結：

| | |
|---|---|
| E.164號碼 | 持續使用於語音通話、訊息收發等電信服務（用戶識別） |
| E.212號碼 | 持續使用於終端設備接取網路的AAA機制（設備識別） |
| IP位址 | • IPv6協定加速過渡（替代IPv4）<br>• 將更廣泛地使用於包括5G、Internet、物聯網裝置等所有連網設備（設備識別） |
| DNS/IP | • 域名具備全球或地區辨識性<br>• 為最成熟、支援度最高的編碼識別/解析機制，除提供連網物件的定址和識別等功能，並能在各種通訊協定間進行轉換，來達到資訊存取與傳遞的目的。<br>• DNS作為Internet的重要基礎設施之一，持續穩定運作及提升其安全性仍是研究的重點。 |

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 下世代網路的號碼需求與角色

■在電信網路的發展上，目前仍以E.164與E.212號碼作為識別基礎
- ➢觀察E.164/E.212編碼於衛星—行動網路整合化的發展趨勢

■新類型編碼的發展仍待觀察其重要性與影響性

■DNS/IP編碼機制具有因應未來網路需求之彈性與潛力（ITU、ICANN）
- ➢DNS運作為網際網路的關鍵基礎
  1. 優點：
     - 具有極大的編碼命名空間
     - 相容性
     - 基礎建設普及度高
  2. 缺點：
     - DNS機制重視低延遲，其通訊安全性低
  3. 衍生政策需求：
     - DNS系統的安全性強化
     - 業界有共識的編碼規則

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 下世代網路的號碼需求與角色

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 下世代網路的號碼需求與角色

- DNS機制的如何因應未來網路需求
  - DNS運作結構與IYU-TX.1255相近（識別/解析、存儲、註冊）
  - 可因應5G虛擬化網路資源管理需求
    - 其層級式命名架構，可依據網路切片以及虛擬資源的管理加以擴增
    - 其層級式的名稱解析運作架構，可透過邊緣運算（MEC）加快物聯網端的解析，彌補網路延遲
  - 可因應物聯網大量裝置需求，設計自動化編碼與管理機制
    - 例如車聯網

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 下世代網路的號碼需求與角色

網路互連情形將會更甚以往，TCP/IP與DNS轉換將成為下世代網路下的關鍵，DNS重要性提升，DN/IP與號碼的對應關係，將成為討論重點，要快速、安全的識別。

當網路切片技術興起，多網、私有網路形成，網路不見得需互連，可以直通消費者，形成網路分裂現象。如何將IP整合進入電信網路，避免來自應用層的經濟/技術壟斷，以及網路分裂?

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 編碼政策初步建議

- 持續觀測各種具重要性的新編碼機制的發展
  - 涉及國家、地理名稱之識別與分配
  - 涉及基礎網路通訊技術的變革
  - 區別其屬於電信網路或網際網路
  - 影響基礎電信服務、具有全球互通性需求
- 編碼機制運作之解析/註冊/存儲系統，可能成為資訊關鍵基礎設施（分項二）
- 為產業需求提出一套編碼規則與運作機制（分項三）
  - 遵守DN層級化命名規則，並具備唯一識別性
  - 透過自動化系統加以命名與管理
  - 與既有DNS機制相容
  - 尤其在涉及跨網服務、公共服務時，需有一套可遵循的編碼規則
    - 例如公共安全服務、車聯網

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

中華民國交通部
MINISTRY OF TRANSPORTATION AND COMMUNICATIONS R.O.C

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

# 下世代電信網路號碼資安威脅及電信資安稽核機制初探

莊淑閔 主任
財團法人電信技術中心

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# 簡報大綱

- ITU-Network 2030介紹
  - Tactile Internet
  - Holographic Type Communications
- 下世代電信網路資安威脅
- 電信資安稽核機制

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


## Convergence of Satellite Networks and Terrestria Networks

| Co. | Support (Data are from the Internet, not yet verified) | Scale |
|---|---|---|
| Starlink | SpaceX (Elon Musk) | 4K by 2019, th 12K |
| Oneweb | Softbank | 650 by 2019 |
| Boeing | Apple (spec) | 2956, 1350 in 6 yrs |
| O3Nb | Virgin group, SES | 400 |
| CASIC | China | 300 (54 trial) |

| Distances | Bandwidth | delay |
|---|---|---|
| (LEO) 900-1200 KM | 1—200 Gbps | 35ms |
| (MEO) ~2000 KM | 1-200 Gbps | ~60ms |
| Space to space | ~100 KM – ~Tbps<br>~1000 KM ~10 Gbps | |

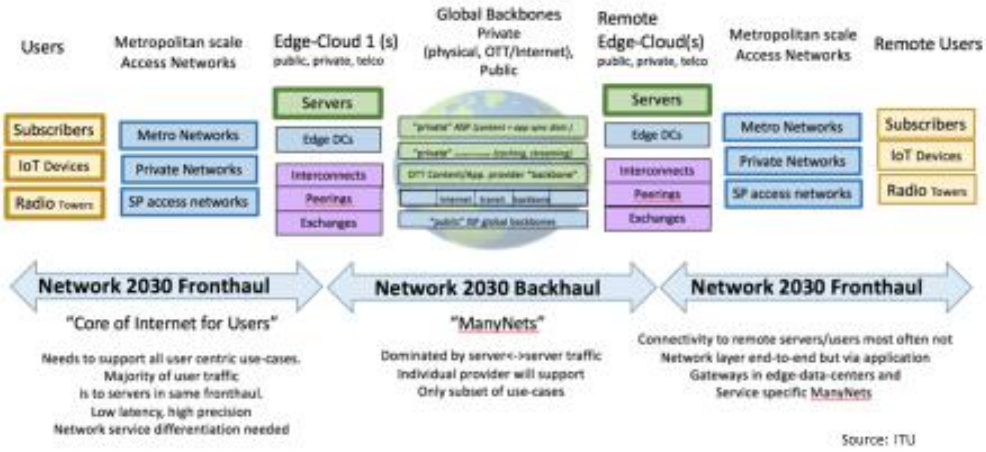
Use Cases
- Satellite as access, and terrestrial networks as backhaul
- Satellite as transport
- Hybrid and Integrated

Requirements
- Uniform Addressing and Converged Routing
- Bandwidth capacity at the satellite side
- Admission control by satellites
- Edge storage and computing

Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# Expected Evolution of Network2030 Architecture




Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# ManyNets: Embracing Diversity, Variety, and Economy

Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# ITU-Network 2030
## New IP Frontier – Market and Business Drivers

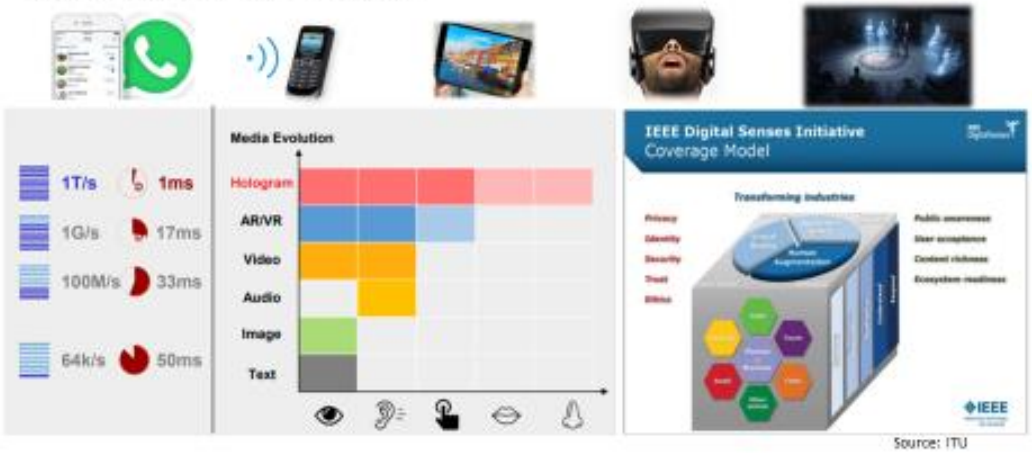
- Holographic type communications (HTC)
- Tele-driving, cloud driving and integrated driving
- Space-terrestrial integrated network (STIN)
- Industrial IoT (IIoT) with fully cloudified PLC
- Intelligent operation network (ION)
- Light-field 3D communications (LF3D)
- Tactile internet (TAC)
- Network computing convergence (NCC) Digital Twin and Holographic Twin (DT/HT)

Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# Holographic Type Communications

Attach Digital Senses to Holograms




Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

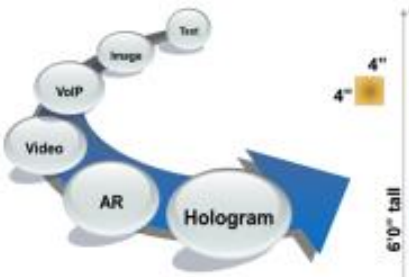
# Holographic Type Communications

- Immersive holographic spaces will render artefacts from a distant location into a room, rendering local users into the remote location.
- Remote troubleshooting and repair applications will allow technicians to interact with holographic renderings of items at remote and hard-to-reach locations, such as on an oil drilling platform or inside a space probe.

Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

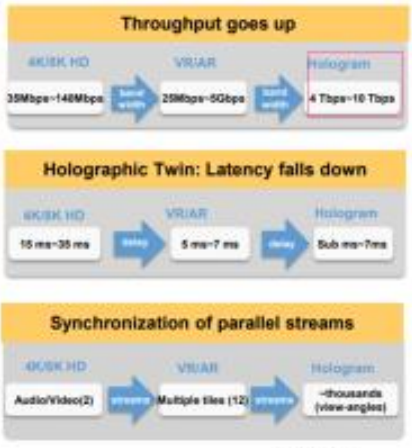
# Holograms and Holographic Type Communications




| | Dimensions | Bandwidth |
|---|---|---|
| Tile | 4 x 4 inches | 30 Gbps |
| Human | 72 x 20 inch | 4.32 Tbps |

- Raw data; no optimization or compression.
- color, FP (full parallax), 30 fps

*(reference: 3D Holographic Display and its Data Transmission Requirement, 10.1109/IPOC.2011.6122872), derived from for 'Holographic three-dimensional telepresence'; N. Peyghambarian, University of Arizona)*




Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# Tactile Internet

Enabling tactile and haptic sensations to human-to-machine interaction

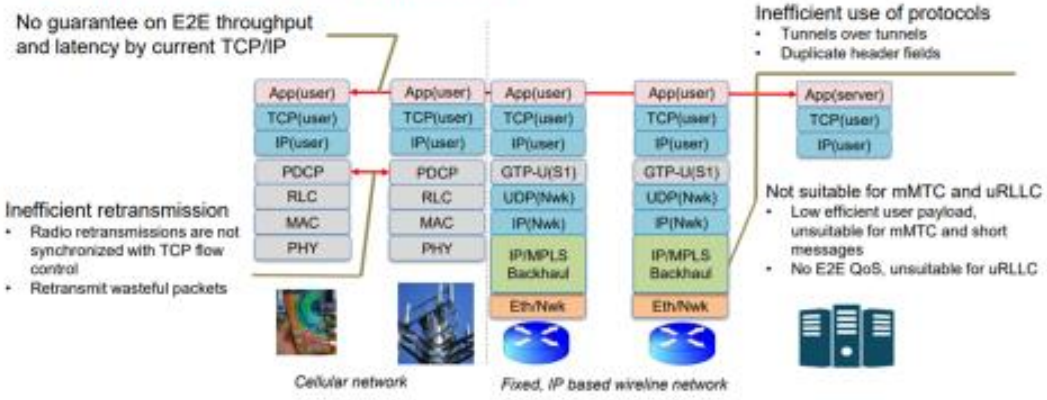
- Ultra-low latency: Sub-millisecond to 5 milliseconds.
- Ultra-low loss: Loss of packets is almost intolerable
- Ultra-high bandwidth: From 360-degree video to holograms. VR feed: 5 Gbps; Holograms: Tbps
- Stringent synchronization: Different human-brain reaction times to different sensory inputs (tactile: 1ms, visual: 10ms, or audio: 100ms). Real-time feedback from different inputs must be synchronized accordingly.
- Differentiated prioritization levels: Prioritizing streams based on their immediate relevance.

Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# End-to-End Precise Requirements

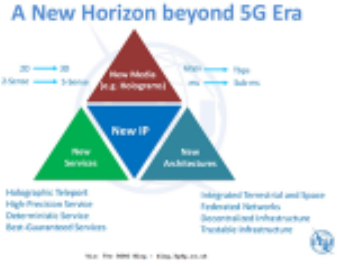
RAN has evolved, but IP/MPLS networks stay the same




Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# Imagine a new IP packet as a FedEx-like Datagram



- ❑ A packet carries a contract from an application to the network
- ❑ The network and routers process the contract

**New IP**

1) The packet arrives in 35ms
2) The packet arrives at 35ms later sharp
3) I require a throughput of 12Gbps
4) No packet loss. If lost, you get a compensation
5) Track it

**FedEx**

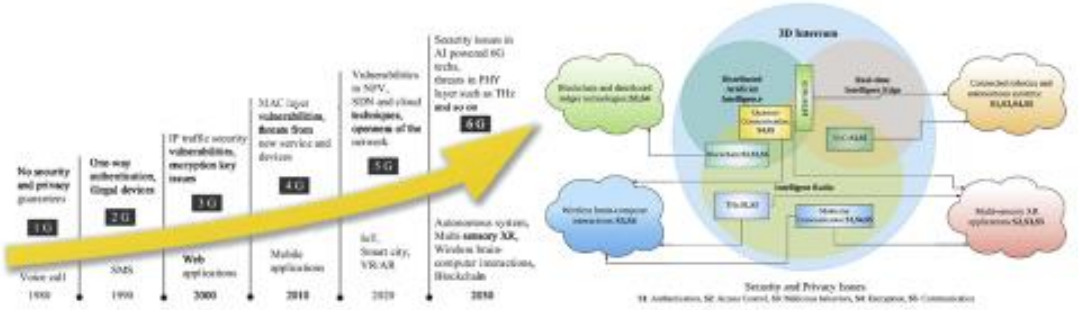
1) The package arrives in 1 day
2) The packages arrives at 9:00AM next day
3) The weight is 12kg
4) No package loss. If lost, you get a refund of $$$
5) Status Track

Source: ITU

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 6G 網路安全與隱私議題

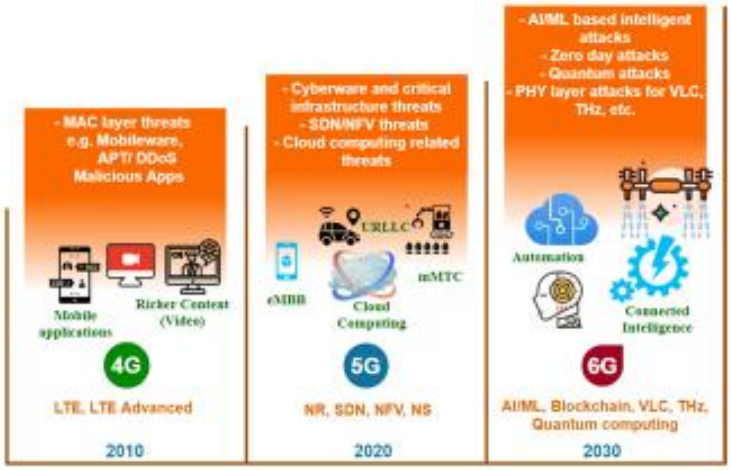
Evolution of security and privacy issues in wireless systems.




Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

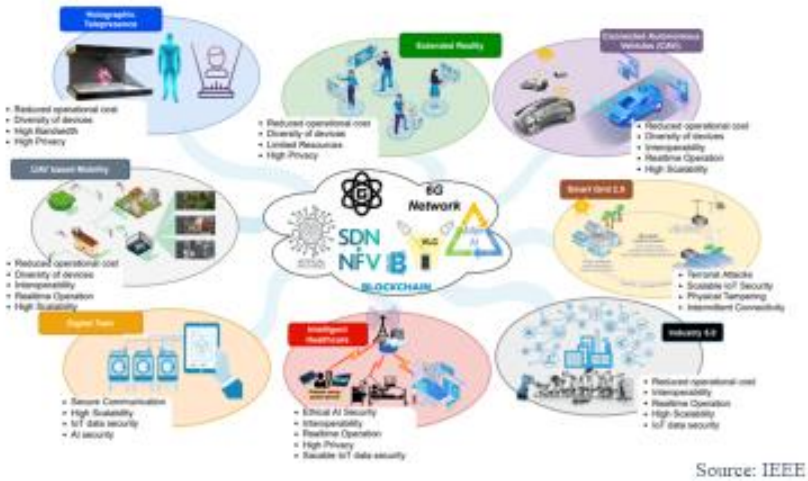
# 4G to 6G 網路資通安全全景圖




Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 6G 應用需求與主要資通訊安全議題




Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 6G 應用需求與資通訊安全

## 6G Security Threat Landscape

## 6G Security Threat Requirements

Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 6G 應用的資通訊安全需求挑戰

| Potential 6G Applications | Security Requirements | | | | | | Expected Security and Implantation Challenges | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Ultra Lightweight Security | Zero-touch Security | High Privacy | Proactive Security | Security via Edge | Domain specific security | Limited resources | Diversity of Devices | High Mobility | Physical Tempering | Terrorist Attacks | Intermittent Connectivity | Localized environment | Lack of Security Standards | E2E Security orchestration | Energy Efficiency |
| UAV based mobility | M | H | L | M | H | L | H | M | H | M | H | L | L | L | H | H |
| Holographic Telepresence | M | L | H | L | M | L | H | M | L | M | L | L | M | M | H | H |
| Extended Reality | H | M | H | L | H | L | H | M | M | H | L | L | L | H | H | H |
| Connected Autonomous Vehicles | L | H | M | H | H | H | L | M | H | M | H | L | L | L | H | M |
| Smart Grid 2.0 | H | M | M | H | L | H | H | L | L | H | H | H | L | L | L | M |
| Industry 5.0 | M | H | L | H | H | H | H | H | M | L | M | L | H | M | H | H |
| Hyper-Intelligent Healthcare | H | M | H | M | H | H | H | H | M | M | L | M | H | M | H | H |
| Digital Twin | M | H | L | L | M | M | L | M | L | L | H | M | L | L | H | M |

L Low Level Requirement/Impact  M Medium Level Requirement/Impact  H High Level Requirement/Impact

Source: IEEE

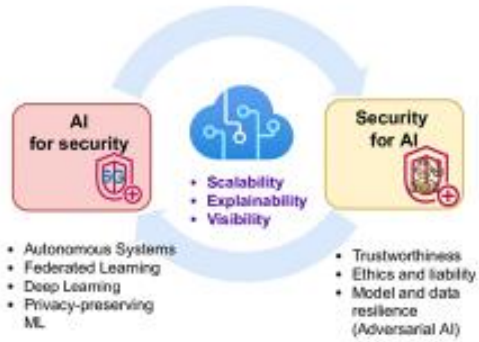
版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 隱私總類與保護

Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 6G 資通訊安全與AI安全




Role of quantum computing in 6G

Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 6G 資通安全設計思維

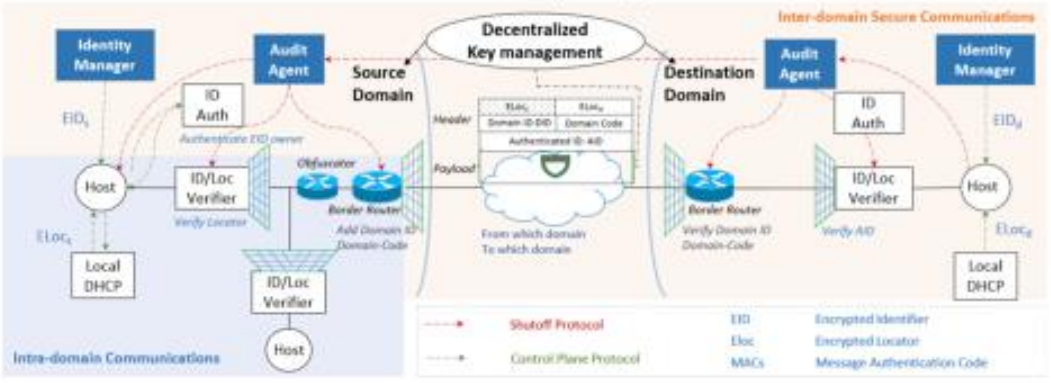
| KPI | Description | 6G impact |
|---|---|---|
| Protection level | The guaranteed level of protection against certain threats and attacks | More stringent due to the pervasive utility of 6G and burgeoning risk level |
| Time to Respond (mean, max, ...) | Time for security functions to counteract in case of malicious activity | Much smaller due to compressed timescale of 6G networks, e.g., an attack can cause havoc at an order or faster |
| Coverage | The coverage of security functions over the 6G service elements and functions | More challenging due to diverse 6G technologies and ultra-distributed functions |
| Autonomicity level | A measure of how autonomic security controls can act | Expected to be easier to implement with pervasive AI, but also may be counter-beneficial due to AI security issues |
| AI robustness | The robustness of AI algorithms in the network hardened for security | More difficult to maintain consistently system-wide but more critical due to AI's role in 6G |
| Security AI model convergence time | Time for learning models working for security to converge | Although more advanced AI/ML models are emerging and hardware capabilities are improving, the data availability and complexity are challenging factors for this KPI. |
| Security Function Chain round-trip-time | Time for chained security functions to process for ingest, analyse, decide and act (related to "Time to respond" KPI) | Security architecture in 6G supposed to be more distributed, leading to challenges. But at the same time, device-centric and edge-centric solutions will help. |
| Cost to deploy security functions (mean, max, ...) | Various cost metrics for measuring the cost of deployment | Substantially increases due to complexity, thus harder to meet target KPI values |

Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 下世代電信網路資通防護架構
## Network Architecture with Intrinsic Security

NAIS for source authentication and privacy



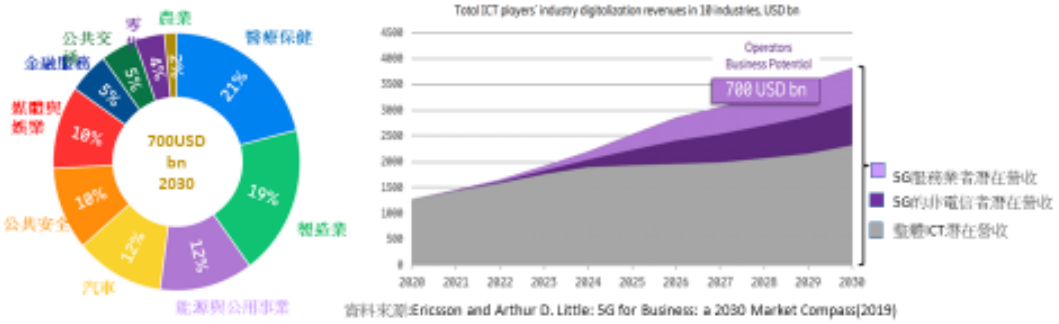

Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 5G電信在數位轉型的營收預測

➢ 全球ICT收入5G電信業者的佔比預估(2030)

- 資通訊技術參與者收入因各產業數位化轉型有望達到約3.8兆美元
- 電信業在製造業、能源與公用事業、公共安全、醫療保健、公共交通、媒體與娛樂、汽車、金融服務、零售業和農業領域的5G市場相關產值可達7千億美元




資料來源:Ericsson and Arthur D. Little: 5G for Business: a 2030 Market Compass(2019)

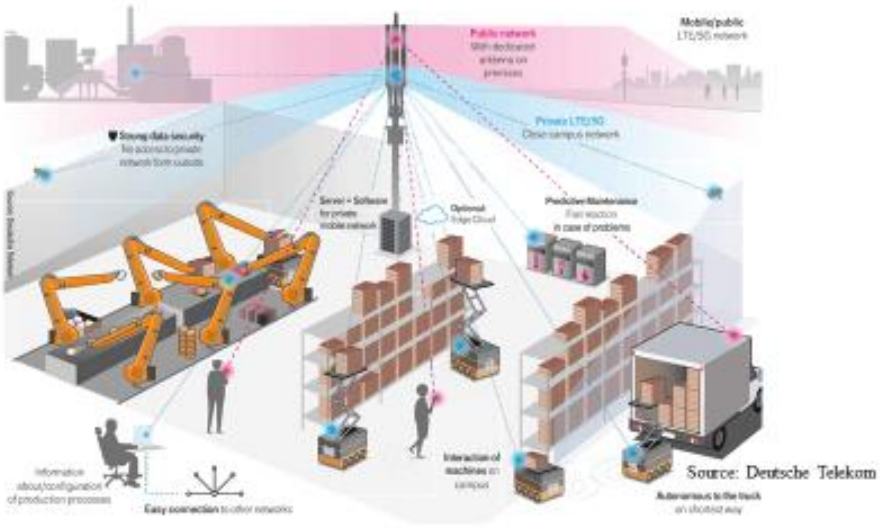
版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 5G網路與工業物聯網應用項目

Source: Qualcomm

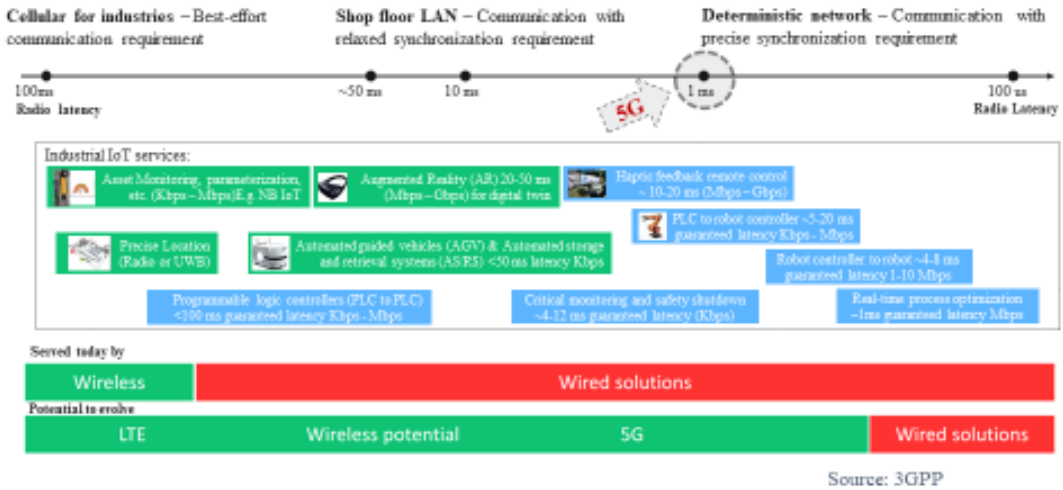
版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 5G企業網路與工業物聯網情境




版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

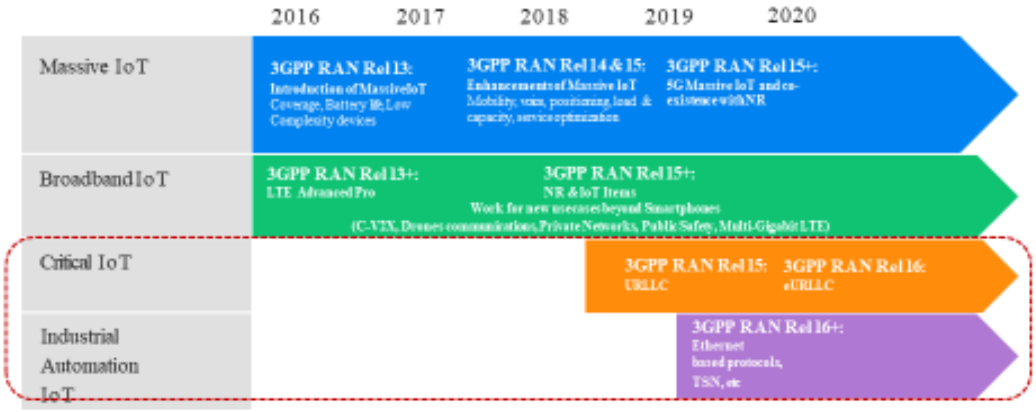
# Industrial IoT and set foundation for 5G




Source: 3GPP

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

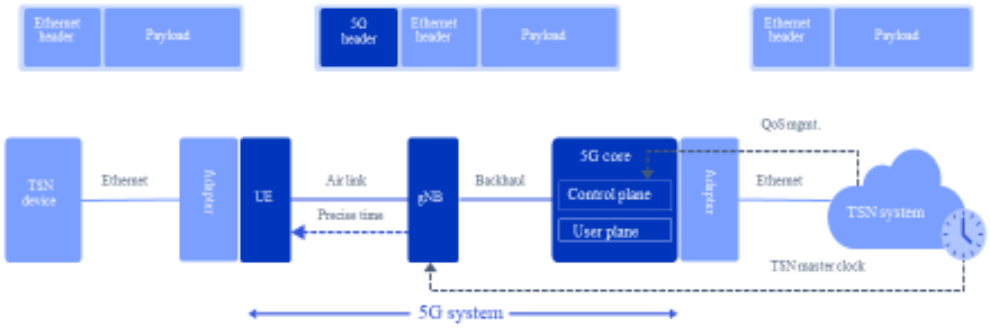
# 5G Roadmap for Industrial IoT




Source: 3GPP

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 5G 支持 Time Sensitive Networking (TSN)




**Ethernet over 5G**
- Transport Ethernet frames over 5G
- Efficient transport of broadcast packets, including loop prevention
- Automatic address discovery

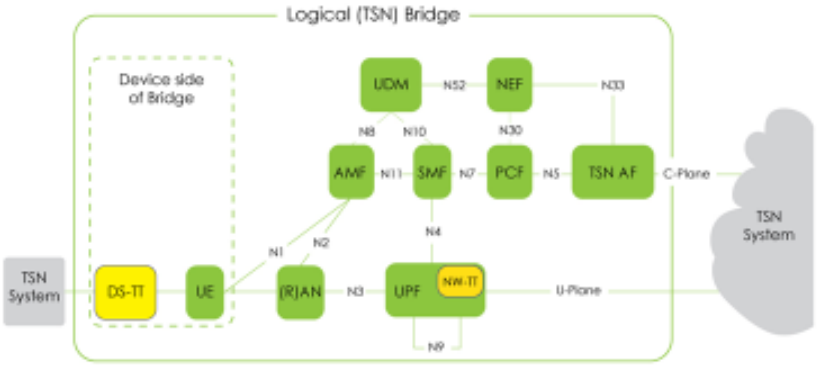
**Quality of Service (QoS)**
- Interface between 5G control plane and TSN for QoS management
- Define new 5G QoS identifier for industrial Ethernet
- Admission control & interaction with TSN QoS framework

**Time synchronization**
- Time synchronization architecture
- Microsecond synchronization for all nodes
- Broadcasting precise time by gNB

Source: Qualcomm

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 3GPP 定義Time-Sensitive Network標準



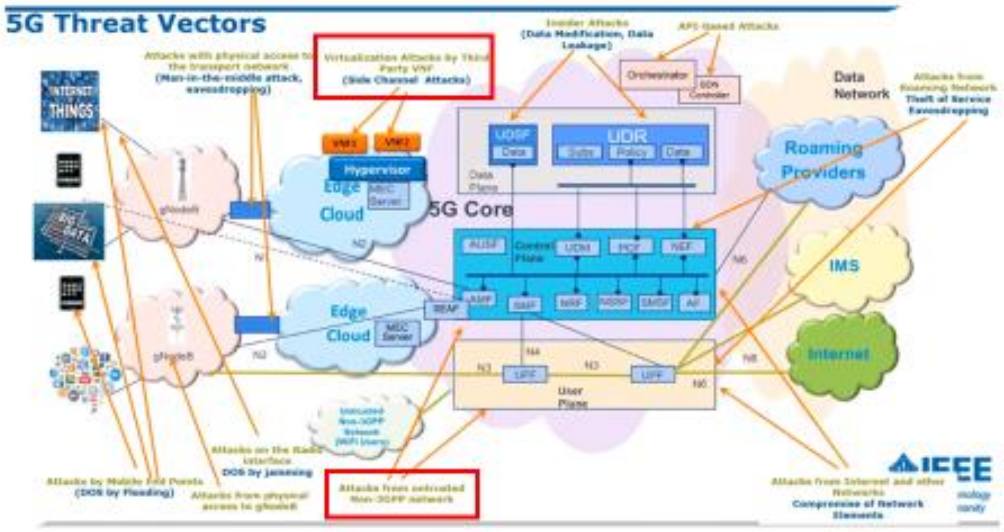

System architecture view with 5GS appearing as a Time-Sensitive Networking bridge

TS 23.501

Source: 3GPP

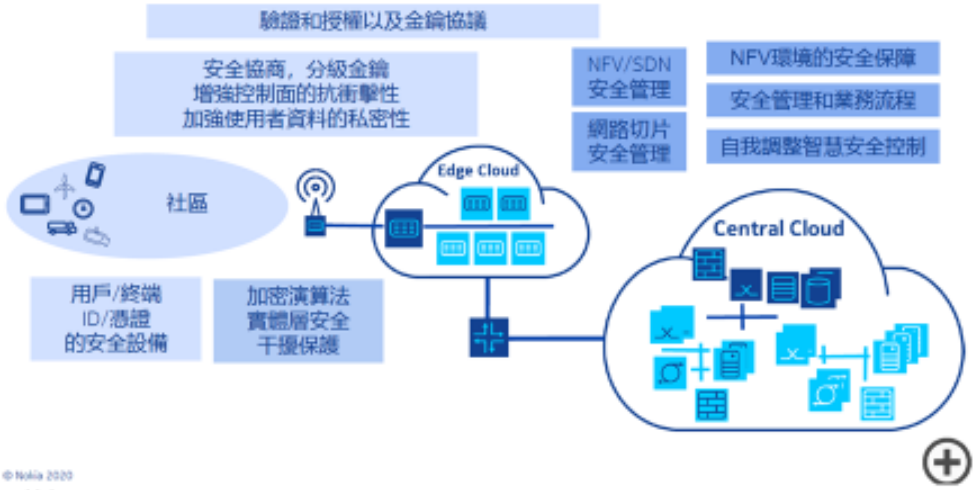
版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 5G SA威脅向量圖




版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 5G 安全架構的基本元素



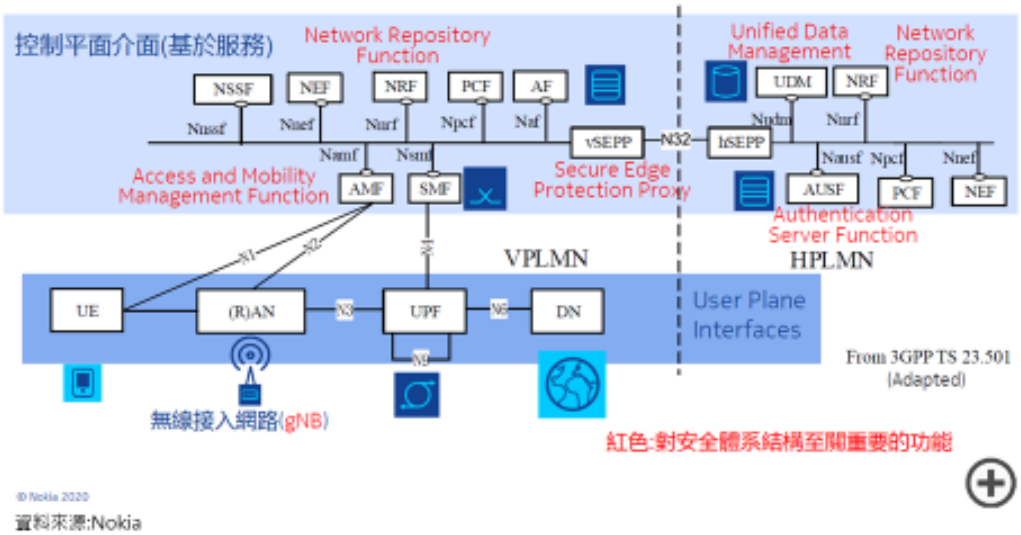

© Nokia 2020

資料來源:Nokia

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

51

# 3GPP 5G系統的關鍵安全功能



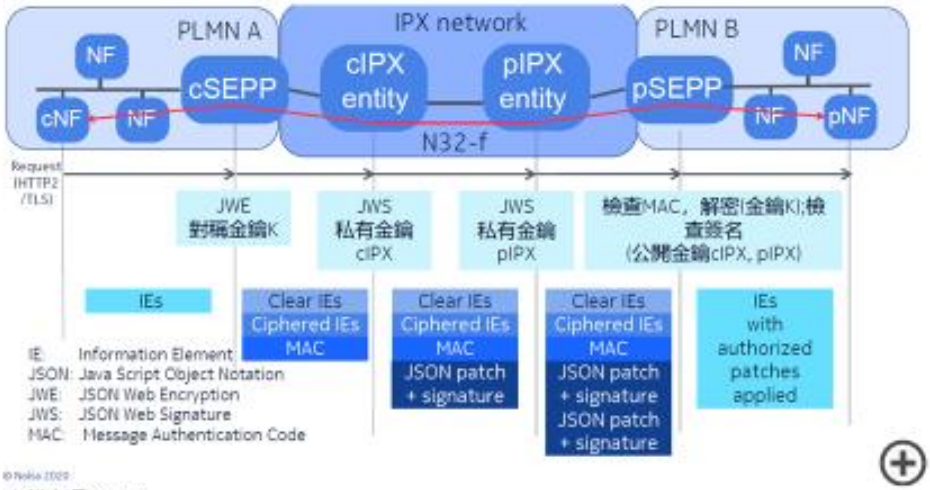

© Nokia 2020

資料來源:Nokia

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

52

# 5G 網路的互連安全

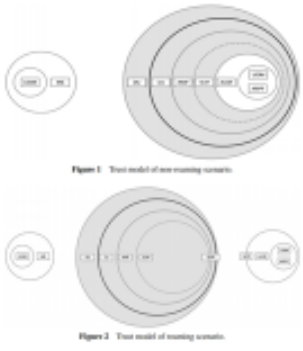


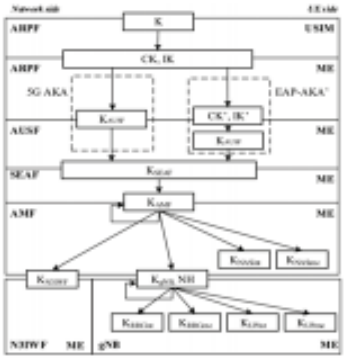

資料來源:Nokia

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 金鑰的階層架構

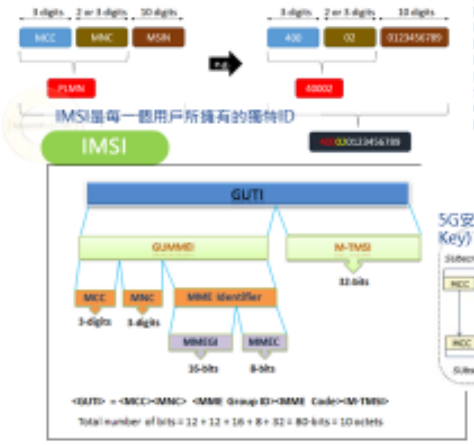
- 2 types of authentication, primary authentication that all devices have to perform for accesing the mobile network services, and secondary authentication to an external data network (DN)
- Data network (DN) by performing strong authentication used to EAP-AKA' or EAP-TLS authentication methods with the presence of a USIM on a UICC in the user equipment to securely store and handle the credentials used to access the DN.





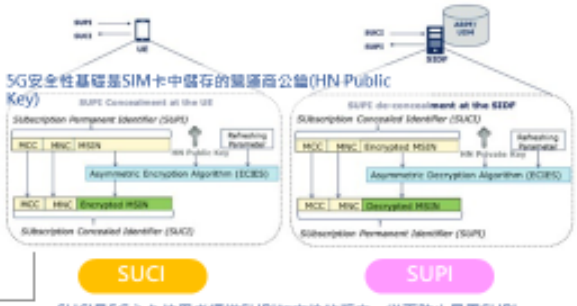

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# Authentication Schemes in 5G System
# IMSI / GUTI / SUCI / SUPI Format




MCC: Mobile Country Codes
MNC: Mobile Network Code
MSIN: Mobile Subscription Identification Number
PLMN: Public Land Mobile Network
IMSI: International Mobile Subscriber Identity
GUTI: Globally Unique Temporary Identity

MME: Mobility Management Entity
M-TMSI: MME Temporary Mobile Subscriber Identity
GUMMEI: Mobile Subscription Identification Number



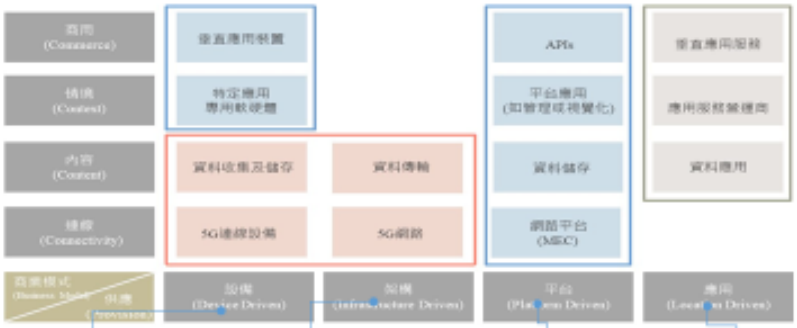

GUMMEI是用作辨別 MME，代表用戶是在哪一個MME下面
M-TMSI是用戶在單一個MME底下的身分識別

SUCI是5G永久使用者標識SUPI加密後的版本，從而防止暴露SUPI，SUCI使用營運商的公鑰，由SUPI生成。

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 建立5G資安防護環境

5G 網路涉及不同類型的終端設備、多種接入方式和接入憑證、多種時延要求、隱私保護要求




① 通訊安全
② 數據儲存安全
③ 實體安全
④ 特定垂直應用安全
⑤ 消費者使用安全

① 接取網路設備安全
② 核心網路設備安全
③ 通訊傳輸安全
④ 網路管理及維運安全

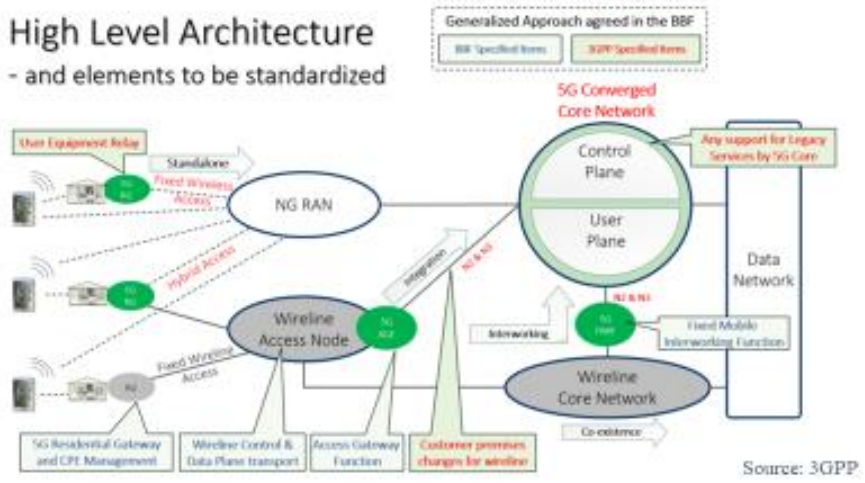
① 身分識別與存取安全
② 資料儲存安全
③ 應用程式安全
④ 威脅偵測與管理安全

① 端對端（E2E）垂直應用安全
② 終端設備、通訊網路、應用服務等提供商安全責任

資料來源：TTC，科會辦整理，2019年4月

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 5G網路的 Fixed-Mobile Convergence

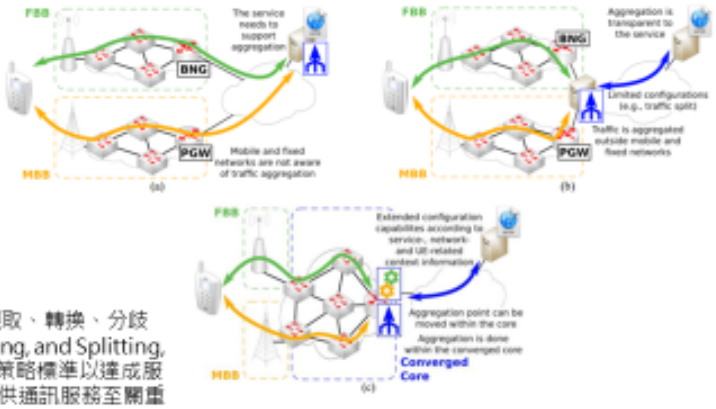



Source: 3GPP

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# 5G 時代中Fixed-Mobile Convergence(續)

FBB and MBB 三種架構
(a) traffic aggregation performed at the end-side service,
(b) FMC with a HAG interconnecting fixed and mobile networks,
(c) FMC with converged core network.

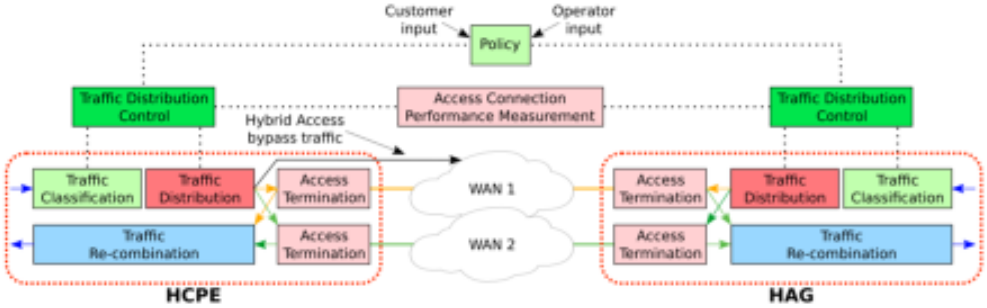



整合核心網路:落實制定接取流量選取、轉換、分歧（Access Traffic Steering, Switching, and Splitting, ATSSS）策略，訂出特定接取服務策略標準以達成服務品質要求。依照服務品質限制提供通訊服務至關重要，如高可靠度和低延遲通訊（Ultra-reliable Low Latency Communications, URLLC）即能避免接取失敗的情況。同時，服務提供商得以提供最佳連線品質，終端使用者也可以體驗最佳化網路體驗。不僅如此，無論用戶設備為何，電信業者皆可以保證相同的協定堆疊（Protocol Stack）支援同一套ATSSS 策略

Source: 3GPP

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# Hybrid Access reference architecture

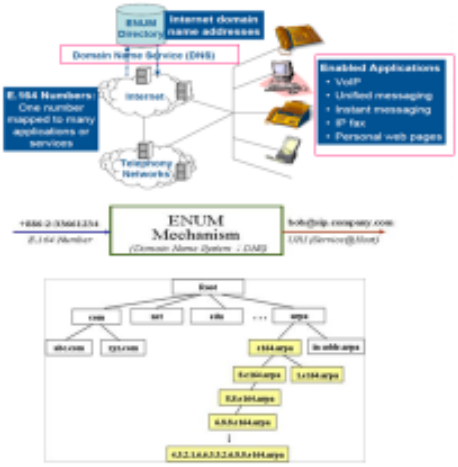



- Hybrid customer premises equipment (HCPE)through a hybrid access gateway (HAG). The HCPE aggregates and distributes traffic in the upstream while the HAG, which can be placed either at either the BNG or PGW
- HAG and the HCPE, BBF mainly considers different transport options: layer 3 (L3)overlay tunneling, L3 network-based tunneling and L4 multipath, like MPTCP

Source: SGPF

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

# 電話號碼對應
# Electronic Telephone Number Mapping, ENUM

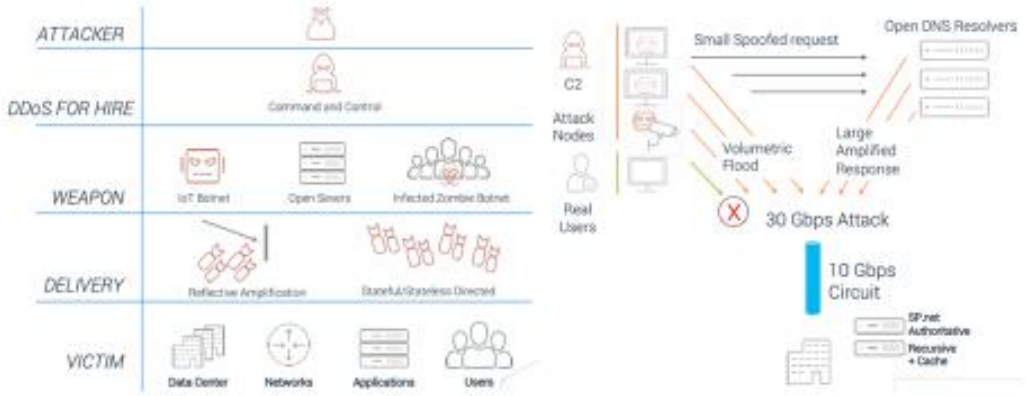



- ENUM是電話號碼對映URI(s) (Uniform Resource Identifier)協定
- ENUM技術是架構在網際網路上既有的DNS (Domain Name System，網域名稱系統)機制上，將一個傳統E.164電話號碼，對映成一個網際網路上的網域名稱（Domain Name），再利用此網域名稱向具有ENUM資料的DNS伺服器進行解析查詢，而得到該電話號碼所關聯的服務識別位址

Source: NCC

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved. 

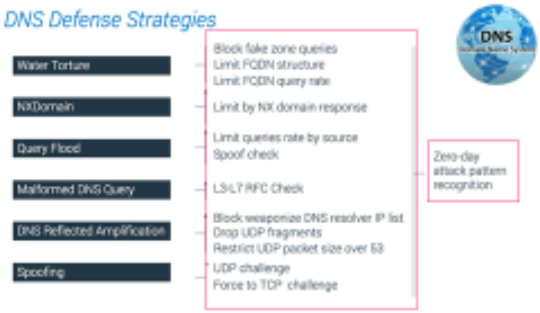
# DNS 攻擊手法




Source: Infblox

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# DNS 攻擊方式與防禦策略



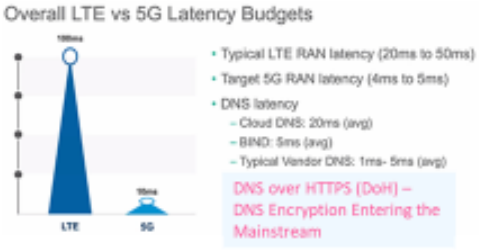

- Transmission Control Protocol synchronize (TCP SYN) flood
  - Internet Control Message Protocol/User Datagram Protocol (ICMP/UDP) flood
- Non-DNS reflected amplification (e.g. NTP, SSDP, etc)
- Packet anomalies

- **Water torture:**
Also known as pseudo-random subdomain attacks, water torture attacks bombard DNS resolvers with legitimate domains followed by random labels, forcing the DNS to work harder.
- **NXDomain:**
By repeatedly requesting non-existent domains (NXDomains), attackers can cause DNS resolvers and servers to become overwhelmed.
- **Query flood:**
A multitude of queries flood either the DNS resolvers or the authentication servers.
- **Malformed DNS query:**
These types of queries force the DNS to complete additional processes and use additional resources.
- **DNS reflected amplification:**
DNS is always looking and listening for queries, which makes it an ideal target for reflected attacks.

Source: IEEE

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 5G 網路六大關鍵DNS 設計要求



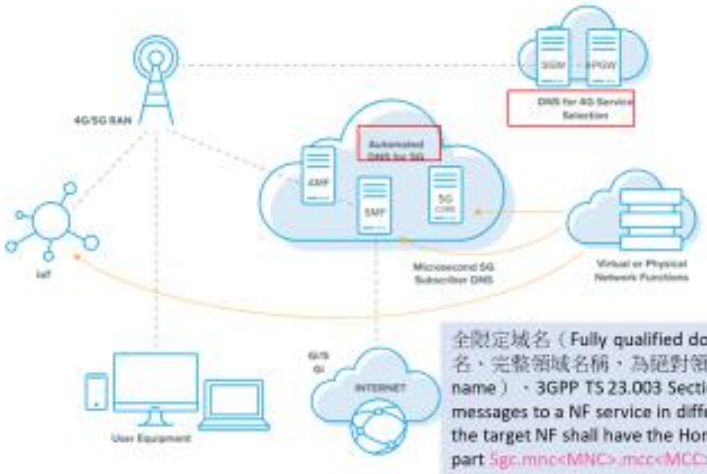

5G 網路六大關鍵DNS 設計要求
1.Low latency
2.Scaling by orders of magnitude
3.Network-wide awareness
4.Edge security
5.Secure high-performance control plane
6.Real-time monitoring and management
Flexibility

- 加密的HTTPS協定進行DNS解析請求，避免原始DNS協定中使用者的DNS解析請求被竊聽或者修改的問題（例如中間人攻擊）來達到保護使用者隱私的目的

Source: Infblox

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 自動化DNS安全設計確保 5G 與4G 核心網路




全限定域名（Fully qualified domain name）完全資格域名，完整領域名稱，為絕對領域名稱（absolute domain name），3GPP TS 23.003 Section 28.5. For HTTP/2 request messages to a NF service in different PLMN, the FQDN of the target NF shall have the Home Domain as the trailing part 5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Source: Infblox

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 5G風險掌握-虛擬化及軟體化威脅

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 第五代行動通信系統資通安全維護計畫參考框架

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 電信資安稽核機制初探

- 稽核依據
  - 《資通安全管理法》第16條第6項及第17條第4項授權訂定之《國家通訊傳播委員會所管特定非公務機關資通安全管理作業辦法》
  - 《電信管理法》第15條第3項授權訂定之《電信事業資通安全管理辦法》
    - 明定本會應每年擇定特定非公務機關/設置使用電信資源之公眾電信網路，以現場實地稽核之方式，稽核其資通安全維護計畫實施情形。
- 稽核對象及方法
  - 依通傳會所管特定非公務機關資通安全管理作業辦法及電信事業資通安全管理辦法規定，擇定受稽對象之考量原則：
    - 資通安全責任等級
    - 資通安全事件發生之頻率與程度
    - 資通安全演練之成果
    - 受稽核之頻率與結果
    - 其他與資通安全相關之因素

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 電信資安稽核機制初探:稽核內容

審酌受稽機構之資安維護計畫共有17項次，內容涵蓋受稽機構之資通安全組織、資安防護、資安事件通報、應變、演練與情資分享以及用戶隱私與個資的保護等面向，爰據以擬定四大類重點稽核項目：

- 稽核重點分為4大類
  - 類別一：確認受稽機構完備及精進其資通安全組織
  - 類別二：確認受稽機構落實資安防護
  - 類別三：確認受稽機構依法辦理資安事件通報、應變、演練與情資分享
  - 類別四：確認受稽機構依法落實因服務而產生之用戶個資及隱私保護

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 電信資安稽核機制初探:稽核項目

類別一：為督導受稽機構健全及精進其5G資通安全組織，將其資安維護計畫之「四、資通安全推動組織」、「五、專責人力及經費之配置」、「六、資通安全長之配置」、「十三、所屬人員辦理業務涉及資通安全事項之考核機制」及「十四、資通安全維護計畫及實施情形之持續精進及績效管理機制」，納入為第一類重點稽核。

類別二：為確認受稽機構落實5G系統資安防護，將資安維護計畫之「七、資訊及資通系統之盤點規劃」、「九、資通安全防護及控制措施」、「十二、資通系統或服務委外辦理之管理措施」及「十五、資通安全偵測與防護之建置及執行方案」，納入為第二類重點稽核。本年度更將「核心網路」、「無線電接取網路」、「傳輸網路」以及「業務支援系統」4大區塊之中高風險威脅之控制措施，作為「九、資通安全防護及控制措施」以及「十五、資通安全偵測與防護之建置及執行方案」之稽核項目。

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 電信資安稽核機制初探:稽核項目(續)

類別三：為確認受稽機構依法辦理5G資安事件通報、應變、演練與情資分享，將資安維護計畫之「十、資通安全事件通報、應變及演練相關機制」及「十一、資通安全情資之評估及因應機制」，納入為第三類重點稽核。

類別四：為確認受稽機構依法落實因5G服務而產生之用戶個資及隱私保護，將資安維護計畫之「十六、執行前述執行方案所蒐集、儲存、處理及利用用戶資料之安全保護措施」納入為第四類重點稽核。

版權所有© 2021財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 玖、第三場「下世代電信網路號碼研究及 DNS 編碼技術概念性驗證成果暨實測說明」專家座談會

## 一、第三場座談會簡介及議程

大規模、大頻寬、低延遲物聯網與專網服務為我國下世代通訊技術發展重心，電信網路號碼技術將成為各類型網路互聯重要議題。ICANN、IETF、ITU 等國際組織均已陸續展開電信號碼技術及標準研究，如：ICANN 於 106 年 11 月會議上，展示使用 DNS 系統作為物聯網編碼方式之可能性，又於 109 年發布「5G Technology」報告，探討以 DNS 系統作為物聯網設備編碼之相關技術及解決方案，並持續對此議題進行討論。

交通部 110 年度委託財團法人電信技術中心(簡稱本中心)辦理「下世代電信網路號碼技術研析及管理」委託研究計畫，期藉由觀察國際下世代電信號碼發展趨勢，研析我國下世代電信號碼編碼機制，超前部署「新世代電信編碼之技術與標準發展」，協助推動下世代電信網路基礎建設，建立研發能量，並掌握 5G 及下世代電信契機，以確保我國相關技術及政策能與國際先進國家並駕齊驅。

本中心訂於 110 年 9 月 29 日（星期三）下午 2 時至 5 時舉辦「下世代電信網路號碼研究及 DNS 編碼技術概念性驗證成果座談會」，展示本計畫完成之 DNS 編碼技術概念性驗證，並邀請各方產官學研界專家學者蒞臨指導，希冀藉由廣納各方意見及進行交流討論充實本計畫之研究內容，以作為交通部未來擬議政策之參考。

| 時間 | 議程 | 主講人 |
|---|---|---|
| 13:30-14:00 | 會議報到 | |
| 14:00-14:05 | 開場致詞 | 電信技術中心<br>林輝堂執行長 |
| 14:05-14:35 | 【專題報告】<br>DNS 編碼技術概念性驗證 | 電信技術中心<br>林永勝主任 |

| 時間 | 議程 | 主講人 |
|---|---|---|
| 15:00-15:10 | Q&A | |
| 15:10-15:30 | 中場休息 | |
| 15:30-15:45 | 【專題報告】<br>下世代電信網路號碼對我國產業及政策影響 | 電信技術中心<br>陳志宇資深經理 |
| 15:45-16:50 | 【專家論壇】<br>1. 下世代電信網路虛擬化/網路切片對編碼應用之影響<br>2. 下世代電信網路號碼初步政策建議方案討論 | 電信技術中心<br>林輝堂執行長 |
| 16:50-17:00 | 總結 | |

## 二、第三場座談會會議紀錄

(一)**主持人**：財團法人電信技術中心 林輝堂執行長

(二)**會議時間：2021 年 9 月 29 日（三）下午 2 時 00 分**

(三)**會議地點**：集思交通部國際會議中心 201 會議室及線上會議

(四)**與會成員**：行政院資安處、郵電司、國家通訊傳播委員會、財團法人台灣網路資訊中心、財團法人工業技術研究院、財團法人資訊工業策進會、台灣電信產業發展協會、國立臺灣科技大學資訊工程系周詩梵、國立臺灣科技大學電子工程系陳文雄、國立成功大學電信管理研究所陳文字、國立宜蘭大學資訊管理系陳麒元、中華電信股份有限公司、台灣大哥大股份有限公司、台灣之星股份有限公司、亞太電信股份有限公司、遠傳電信股份有限公司、網路中文資訊股份有限公司、友訊科技股份有限公司。

(五)**會議紀錄**：郭怡萱助理管理師

(六)**會議討論議題：**

**專題報告：「DNS 編碼技術概念性驗證」及「下世代電信網路號碼對我國產業及政策影響」**

1. 劉明翰處長(友訊科技)：專題報告中說明實驗情境為設定一百個物聯網裝置，其中若每個物聯網裝置都有 GUA Address 存在的情況下，請問在 IPv6 Numbering 情境，如何對 DNS 進行編碼?
2. 計畫團隊：在使用 Gateway 情況下，物聯網裝置連線情況下會得到一個 IP；本計畫研究範圍內，編碼機制是跟著 SIM 卡，所以在對外 SIM 卡註冊時，會自動生成 Domain Name。而計畫團隊後續將持續研究物聯網裝置加入編碼。GUA 在 R17 才會有，現在透過 Radius 或 SMF 的環境，物聯網裝置本身不會將 IPv6 的 EUA 納入，但在 3GPP 的 R17 版本中，有針對這部分的問題做描述。
3. 李隆奇經理(遠傳電信)：當特定的物聯網裝置認定有嚴重的漏洞，是否可透過 DNS 編碼的機制做有效的運用？在 3GPP TR23.003 有保留環境應用的彈性空間或是在 DNS 的 zone 或 domain 設計上做特別的標示或註記？
4. 計畫團隊：在 3GPP 的規規範下，物聯網裝置、IMEI 須向 GSMA 註冊，IMEI 前 8 碼是廠牌及設備名稱，後 6 碼是生產國、生產日期、序號等，您提的疑問是可以制止的。假設有漏洞出現時，可以透過 IMEI 前 8 碼判斷場域內設備的裝置，就可以遠端更新防禦機制。
5. 林咨銘技術經理(工業技術研究院)：在進行測試時，物聯網的 hand off 是假設何應用情境，因為在智慧工廠 AR/VR 等應用，很難聯想有甚麼相關需求。另外，在有關 Latency 的效能方面，專題報告中規劃十幾個步驟，在編碼轉換測試，實際過程造成 Latency 的過程有何影響。
6. 陳文字教授(國立成功大學)：有關 Latency 的議題，目前實際應用情境通常是在連線時先有目的地的 Domain Name，然後由主機向 Domain Name Server 去查詢目的地 IP Address，此為獨一無二的 Address。這個過程是需要傳輸時間及處理時間，而且所需時間和主機與 Domain Name Server 位置有關。特別是在應用場域中，設有路由器的架構，會產生可觀的 Latency。所以主機去 Domain Name Server 查詢目的地 IP Address 的 Latency，在物聯網這個應用領域，需要審慎評估及考慮。

7. 計畫團隊:DNS Latency 問題確實是關鍵,DNS 在 5G 網路回應約 25ms,若在時間敏感網路物聯網間需要不斷聯繫情況下,確實會影響專網裝置的連線效能,但若為 Meter 這類的讀表服務就較無影響。

**下世代電信網路具有網路虛擬化及網路切片等特性,對物聯網編碼使用產生影響為何?**

1. 黃勝雄執行長(財團法人台灣網路資訊中心):若預設條件為電信編碼意涵 IP 位址及網域名稱,則對物聯網編碼無影響。目前亦需關注國家是否有發布訂定制度的權利,以國家的角度來看,哪些欄位政府應該介入,及針對第二層需制定如列入 CI 或加強基礎設施方面之規管措施。
2. 林咨銘技術經理(工業技術研究院):詳簡報
3. 周詩梵助理教授(國立臺灣科技大學資訊工程系):網路虛擬化和網路切片的功能省去下世代電信網路的硬體佈建成本,而能依應用服務與需求客製化資源的配置,給予更大的資源運用靈活度,並提升資源利用率。然而,在大量物聯網裝置共存的環境中,除需考量 IP 位址的配置外,亦需考量 DNS 編碼問題。由於每個物聯網設備具備一組唯一的 DNS 編碼,為了成功將感測器的資料傳送到目的地、實現機器間訊息的交換與共享和建造可識別、監控和管理的智慧化網路系統,物品編碼解析技術扮演至關重要的角色,才能將物聯網設備 ID 轉換成網路可識別的 IP 位址,使網路認識該設備。因此,如何透過 DNS 系統實現區域網路和互聯網的連接,以完成不同區域網路裡設備的通訊,是個亟需探討的問題。尤其是在網路虛擬化和網路切片的應用中,除了基礎硬體設備的識別外,還需識別因不同應用所發展的邏輯網路型態。當幾億個物聯網裝置同時有存取 DNS 系統的需求時,該如何確保彼此間訊息的交換以維持網路正常運作,是應優先考量的議題,其中又牽涉到網路基礎設施的佈建、惡意程式攻擊等問題。
4. 鄭嘉逸專案經理(資訊工業策進會):5G 專網在國內的發展脈絡是一個曖昧不明的情況,業界(製造業)可能會覺得 5G 專網是促進數位轉型以及運作更有效率的方式,但對於電信業者來說,會擔心 5G 專網導致外溢並侵蝕相關服務功能。在 5G 專網中主要探討假設一個智慧工廠場域下,如何更有效率管理相關設備。回到本計畫編碼議題,管理場域設備是很重要的議題,牽涉到如何完善管理及具移動性設備到外場域

之後，是否可與其他網路連結，不論是其他的 5G 專網或是禁用的公眾網路。若要達到此效益，需探討在編碼議題上如何幫助及提升。例如德國在 2020 年就開始討論 5G 專網的 IoT 聯網設備，應如何管理及編碼，進而對提供 IMSI 作為管理機制議題提出討論，然在法律上就會出現問題，因為 IMSI 是被高度管制，只提供公眾網路電信事業使用。再者，過往專用網路無法跨網域連結，是在一個封閉的場域中，如同專題報告提及，ITU 有針對獨立封閉型網路提供如 MCC 999 或 998、MNC 02 之場域測試，然目前趨勢仍有連網必要，故須提供 IMSI 管理，但各國家對 IMSI 資源相對有限。因此德國提出讓有對外聯通及跨場域的專網業者，在 Mobile Network Code 共享 MCC+MNC，等於可共享大量的 IMSI 號碼。又，牽涉到是否須建立一個管理機構、組織或公協會管理這些可共享的 IMSI 號碼，以及一個或多個 Mobile Network Code 該如何管理，也是值得探討的問題。

許真民工程師(中華電信)：網路虛擬化及網路切片對物聯網編碼使用應無影響，3GPP 及 GSMA 標準已制定網路切片之編碼計畫，提供端到端網路切片識別之用途。

**固行網融合的趨勢對電信編碼機制需求及影響為何？**

1. 黃勝雄執行長(財團法人台灣網路資訊中心)：若預設條件為電信編碼意涵 IP 位址及網域名稱，則對電信編碼機制需求無影響。談到電信網路跟 Internet 整個過程是很痛苦的，從原生生態、操作習慣到關注焦點都完全不一樣。電信網路關注核心網路；Internet 關注的則是 Edge，DNS 亦類似於 IBM 名稱的轉換。目前大家對 DNS 應用有很多的期待，如搜尋引擎、內容獲利等，但在公共數位領域卻很困難達成，因為牽扯到註冊政策、規範及個資保護等，基本上不會允許讓 Intermediary Operator 介入式操控。然在技術面問題，把 Domain name 換成 IP 在技術上非常困難及複雜，因為在 name 轉換成 IP 的過程中，光在標準建立指引，RFC 就有 8 千多頁內容說明。簡單來說 DN 有一些特性，也有發展的地方，但限制亦非常多。
2. 林咨銘技術經理(工業技術研究院)：詳簡報
3. 周詩梵助理教授(國立臺灣科技大學資訊工程系)：隨著通訊傳播匯流的發展，在不同平台或載具上傳輸各式數位服務已是普遍存在的情境，

為因應固網和行動網路的異質網路整合，通訊傳播相關產業亦需整併，電信編碼機制也因此需要做相對應的調整，以符合異質網路通訊需求。在如此的潮流趨勢下，考量到服務類型、網路型態、匯流層級 (終端設備、網路和號碼等) 的差異，現存號碼區塊的使用或編配新號碼區塊的方式都將是亟需探討的議題。其中，因固網和行動號碼分屬不同的號碼區塊，網路接取和號碼區塊的配置方式都需符合電信法規的規範。若能簡化電信編碼機制，盡可能在原有號碼區塊支援新服務，將有利於固行網的融合。

4. 許真民工程師(中華電信)：固行網融合對電信編碼機制並無特殊需求，3GPP 及 GSMA 標準已針對固行網融合制定所需編碼機制，主要沿用現有行動(3GPP)電信編碼及固網(IETF)編碼機制，應可達成固行網融合目標。

5. 連彥宗高級研究員(中華電信)：固行網融合的趨勢對電信編碼機制需求及影響有以下幾點，包括：
   A. 固行網融合的趨勢主要分為設備與網路架構面的融合及業務面的融合二種獨立的情境。
   B. 固行網設備及網路架構朝向雲原生及雲化發展，並融合於同一系統及網路，在功能模組化後，透過共用及專屬模組的組合，仍可分別提供固網及行網的服務。與現行固、行網分開的架構所提供的服務一樣，使用相同的電信編碼機制需求，沒有不同。因此，不影響目前的電信編碼。
   C. 業務面的融合又有好多種，但只要是維持目前固行網各自的計費機制，目前的編碼機制仍須維持。
   D. 目前國內電信編碼仍具備識別服務及費率的功能，若未來國內出現新型態固行網融合的服務及計費，才有新的編碼需求

6. 陳文雄專案經理(國立台灣科技大學)：主要是管理方便，尤其是企業專網應用的垂直場域未來也會橫向擴充，具有網路及切片特性的物件命名會更容易管理與互聯，例如，都是車聯網、溫濕度壓力等讀表服務、錄影或是人臉辨識等應用，但光是 QoS 及 Firewall Policy 的管理就不相同。

**在網路虛擬化及網路切片的管理上，是否需依據服務的重要性制定一致的電信號碼編碼規則(例如涉及關鍵設施)?**

1. 林咨銘技術經理(工業技術研究院)：詳簡報
2. 周詩梵助理教授(國立臺灣科技大學資訊工程系)：網路虛擬化和網路切片為 5G 裡的關鍵技術。目前的電信基礎設施主要由 RAN 無線接取網路和核心網路所組成，而現行 5G 網路主要分成非獨立組網架構 (與 4G 網路使用一樣的核心網路，並配備獨立 5G 基地台) 和獨立組網架構 (使用 5G 核心網路並配備獨立 5G 基地台) 兩種部署方式。由於一些重要網路切片功能皆定義在獨立組網架構中，像是服務導向架構 (Service Based Architecture)，為了真正發揮網路切片的功能，以靈活使用或切分可利用的網路資源，並建立各種滿足不同應用的切片網路，許多電信商 (例: 中華電信、台灣大哥大、遠傳、日本樂天行動等) 已紛紛投入與布局獨立組網架構。在應用服務與網路資源管理的角度切入，可依應用服務的性質與要求區分重要性層級 (例: 低延遲、大頻寬等)，而在如此高複雜度的通訊傳輸與基礎設施建設的階段，使用一致的電信號碼編碼規則有助於確立服務的重要性層級，以支援車聯網、工業物聯網及各種創新應用，並益於下世代基礎網路設施的建設。
3. 鄭嘉逸專案經理(資訊工業策進會)：有多個網路認定方式，假設在某工廠中給定某號段 Mobile Network Code，有了這些 IMSI 號碼就可以進行分類及管理。例如 3GPP 在處理 IMSI 號碼議題上，在 Release16 版本中，提到 NIB 概念，也就是 Country Code+ Network Code 的概念，後端則使用不同數字編碼分段，分別代表不同的場域及設備，用設備去定義不同電信的編碼，這些都是對既有的電信、號碼資源有限的概念的擴張及延伸。故從技術發展面來說，當接取網、核網及對 IMSI 的處理達到成熟階段，這種延伸的方法變動成本是最小的。
4. 顏聖原技正(國家通訊委員會)：在傳統電信號碼部分，MNC 如果是市話號碼是可以分區的，因此我們討論過，號碼若進行匯流融合階段會讓民眾無法接受，因此可用 ENON 機制跟 DN 一樣進行 Mapping 方式解決，但最主要還是在市話電話機終端，市話桌機按鍵有限的問題。再來是 5G 專網的部分，在 MCC 方面，台灣僅只一個 MCC 代碼，不像美國、中國、日本等，可向 ITU-T 申請多個 MCC；NMC 方面，台灣有 2

碼，組合成一百億個，有相關機制可進行擴充。其次，E.164 議題，我個人認為並非枯竭而是沒有人使用，在未來通訊網路需要使用哪個 Identifier 確認位置，都很有討論空間。

5. 許真民工程師(中華電信)：3GPP 及 GSMA 標準已依據服務重要性制定一致性之網路切片(eMBB、URLLC、MIoT 及 V2X)及服務 QoS (5QI)等編碼計畫，應無需針對網路虛擬化及網路切片管理再另訂一致的電信號碼編碼規則。
6. 連彥宗高級研究員(中華電信)：關鍵設施通常涉及生命財產及安全的議題，一般都是由政府單位來負責，所有的網路切片應會連到相同的關鍵設施，有需要制定一致的電信號碼編碼。
7. 陳文雄專案經理(國立台灣科技大學)：關鍵基礎建設可以視為是不同專網場域，也就是不同網路切片，所以這題我認為答案是肯定。

**DNS 編碼註冊、分配及存儲系統之管理上是否納入關鍵基礎設施(CI)管制？在管理上如何依據其重要性，以選擇由主管機關管制、公私協力或業者自律?**

1. 黃勝雄執行長(財團法人台灣網路資訊中心)：頂級網域註冊管理機構 Registry 可能可歸屬關鍵資訊基礎設施；Registry 若為關鍵資訊基礎設施且為公務機關或特定非公務機關，就受資通安全管理法管制。若 Registry 非公務機關或非特定公務機關，受 ICANN Registry Agreement 及相關規範所規管，DNS 在目前現行的電信事業相關法規中並無限定 DNS。回到法制面，網路(數位)空間規則由誰訂定之？學者提出四個構面，包括：法律面、通訊協定、市場帶動之需求、參與者之多方利害關係人訂定之相關規範。當在考慮全球性或是偌大的數位空間，絕對不是技術的問題，而是生態系統的問題，需要清楚了解生態系統中最主要的利害關係人、扮演何角色及可以決定的力道為何，方可知道自己的定位。
2. 林咨銘技術經理(工業技術研究院)：下世代電信網路重要性越來越高，會成為如瓦斯水電般的公共設施，DNS 編碼註冊就是 Address 及定址，也是整個電信網路中重要的技術性資料。在規管方面，如何使用取決於不同功能對應不同的效能，亦影響在規管上的困難度。在定址議題上是否讓 DNS 編碼足夠成為關鍵的基礎設施，我建議應該列入規管，建立有序的規管機制且不影響電信網路基本的功能性。

3. 周詩梵助理教授(國立臺灣科技大學資訊工程系)：隨著物聯網的蓬勃發展，通訊設備數量已逐年呈爆炸性增長，對於 DNS 編碼的需求也隨之大幅增加，DNS 編碼註冊、分配和儲存管理將會是個重要的議題，攸關網路的整體運作。以嚴謹的角度來審視，若使用關鍵基礎設施的管制模式，能方便與統一化 DNS 的操作，同時減少和避免 DNS 的不當使用和安全性威脅，不過仍仰賴相關法規的配合。否則，至少應採取公私協力管制，來約束和監管 DNS 的使用。
4. 鄭嘉逸專案經理(資訊工業策進會)：在法規上會去探討一個系統的管理，是否應該納入關鍵基礎設施，廣義上來看就是是否符合關鍵基礎設施相關要件，若是，就應受政府管制；若非，可能就有更大的彈性空間，如公私協力或自律方式。
5. 劉莘相董事長(網路中文資訊股份有限公司)：
   (1) 目前我國相關法規（電信管理法、網際網路位址及頂級網域名稱註冊管理業務監督辦法），並未對網域名稱系統的運作與管理上有細部的法規限制。綜觀 DNS 的運作結構，在實際的解析過程中要避免的是：因為單點錯誤（Single Point Fault）的發生，造成解析失敗的狀況。
   (2) DNS 的整個服務架構，本來就是一個分散式（非集中）的資訊共享架構，所以重點應該是放在「解析來源的正確性確保」與「解析資訊取得的順暢性」。
   (3) 在解析來源的正確性確保上，目前技術上是以 DNSSEC 的方式確保解析來源的正確；而解析資訊取得的順暢性以我國的網路架構而言，一方面是仰賴各大 ISP 業者所提供的線路解析伺服器（例：Hinet 的 168.95.1.1 及 168.95.192.1），另一方面則是大型的公共 DNS 解析伺服器（例：Google 的 8.8.8.8）所提供的 DNS 快取服務，來讓使用者可以快速的取得 DNS 相關資訊。所以如果要穩定整體的 DNS 運作，有兩個面向是可以推動的：
      A. 推廣國內各類型的網域名稱啟動 DNSSEC（或許可採標章認可制）。
      B. 組成 DNS 營運機構組織或是協會，透過行業的自律及稽核機制，讓良幣驅逐劣幣，使整體 DNS 的解析環境愈趨健全。

6. 丁立彥經理(遠傳電信)：我們這邊有觀察到 DNS 在電信業扮演重要的角色，尤其是 DNS cache 的功能，所有的 mobile user 進入 Internet 都需要透過 DNS cache server。希望未來可更深入討論以下有關電信業者 DNS cache 的議題：

   A. 是否要將 DNS 納入關鍵基礎設施的管控。

   B. 目前 NCC 要求各業者的 DNS 進行加密動作，未來若客戶使用 Google 的 DNS，將無法取得 DNS 的資料供檢調使用，從業者角度看，是否可管控客戶 DNS 的使用行為。

   C. Apple 手機 IOS 15 版本中內含有 iSecurity 付費服務，此服務 Apple 在未經同意的情況下，把 DNS 查詢的功能變成其商業產品，在未來的寬頻服務提供者反而無法提供 DNS 服務。Apple 此行為是否有資安上的顧慮呢？

## (七)散會：下午 5 時 30 分

## (八)參與人員名單及簽到表

- 實體名單

| 編號 | 單位 | 姓名 | 職稱 |
|---|---|---|---|
| **政府機關** | | | |
| 56. | 交通部郵電司 | 林姝宜 | 專員 |
| 57. | 交通部郵電司 | 陳日暉 | 技士 |
| 58. | 國家通訊傳播委員會 | 顏聖原 | 技正 |
| **公協會** | | | |
| 59. | 財團法人台灣網路資訊中心 | 黃勝雄 | 執行長 |
| 60. | 財團法人資訊工業策進會 | 鄭嘉逸 | 專案經理 |
| 61. | 財團法人工業技術研究院 | 林咨銘 | 技術經理 |
| **學者專家** | | | |
| 62. | 國立臺灣科技大學電子工程系 | 周詩梵 | 助理教授 |
| 63. | 國立宜蘭大學資訊工程系 | 陳麒元 | 副教授 |
| **電信業者** | | | |
| 64. | 遠傳電信股份有限公司 | 黃志雯 | 副理 |
| **產業代表** | | | |
| 65. | 網路中文資訊股份有限公司 | 劉莘相 | 董事長 |
| 66. | | 魏駿光 | 資深營運經理 |
| 67. | | 賴俞帆 | 專案經理 |
| 財團法人電信技術中心 | | | |
| 68. | 財團法人電信技術中心 | 林輝堂 | 執行長 |
| 69. | | 卜慶玲 | 副執行長 |

| 編號 | 單位 | 姓名 | 職稱 |
|---|---|---|---|
| 70. | | 林永勝 | 主任 |
| 71. | | 卓卿敏 | 資深經理 |
| 72. | | 陳志宇 | 資深經理 |
| 73. | | 王彥中 | 研究員 |
| 74. | | 李昕甯 | 助理研究員 |
| 75. | | 彭俞蓉 | 助理研究員 |
| 76. | | 簡嘉儀 | 副管理師 |
| 77. | | 陳佳瑀 | 副管理師 |
| 78. | | 郭怡萱 | 助理管理師 |
| 79. | | 邱雯琪 | 助理管理師 |
| 計畫團隊 | | | |
| 80. | 鑑智實相科技股份有限公司 | 陳彥吉 | 專案經理 |
| 81. | 國立台灣科技大學 | 陳文雄 | 專案經理 |
| 82. | 銓準科技有限公司 | 王浩丞 | |

- 線上名單

| 編號 | 單位 | 姓名 | 職稱 |
|---|---|---|---|
| **政府機關** | | | |
| 83. | 行政院資安處 | 陳崧銘 | |
| 84. | 交通部郵電司 | 高境良 | 技正 |
| **公協會** | | | |
| 85. | 台灣電信產業發展協會 | 劉莉秋 | 副秘書長 |
| **學者專家** | | | |
| 86. | 國立成功大學電信管理研究所 | 陳文字 | 教授 |
| **電信業者** | | | |
| 87. | 中華電信股份有限公司 | 白洪政 | 高級工程師 |
| 88. | | 陳瑞全 | 高級工程師 |
| 89. | | 陳銘德 | 工程師 |
| 90. | | 許真民 | 工程師 |
| 91. | | 梁銘顯 | 高級工程師 |
| 92. | | 李之軍 | 高級工程師 |
| 93. | | 張容程 | 研究員 |
| 94. | | 余聲旺 | 主任級研究員 |
| 95. | | 唐崇實 | 高級研究員 |
| 96. | | 連彥宗 | 高級研究員 |
| 97. | | 謝文生 | 主任級研究員 |
| 98. | | 林永勝 | 高級工程師 |
| 99. | | 林方傑 | 工程師 |
| 100. | | 周柏伸 | 工程師 |
| 101. | 台灣大哥大股份有限公司 | 楊博森 | 主任工程師 |
| 102. | | 林瀚杰 | 副理 |
| 103. | | 林益申 | 高級工程師 |
| 104. | | 任致遠 | 專案副理 |

| 編號 | 單位 | 姓名 | 職稱 |
|---|---|---|---|
| 105. | 台灣之星電信股份有限公司 | 潘科諺 | 主任 |
| 106. | | 陳慶宏 | 主任工程師 |
| 107. | 亞太電信股份有限公司 | 許文宏 | 高級工程師 |
| 108. | | 唐興銘 | 經理 |
| 109. | | 張栢芳 | 專員 |
| 110. | 遠傳電信股份有限公司 | 賴建良 | 經理 |
| 111. | | 盧祖耀 | 資深協理 |
| 112. | | 楊東敏 | 技術經理 |
| 113. | | 黃漢臣 | 經理 |
| 114. | | 丁立彥 | 經理 |
| 115. | | 李隆奇 | 經理 |
| **產業代表** | | | |
| 116. | 新世紀資通股份有限公司 | 廖鈺鳴 | 專員 |
| 117. | 友訊科技股份有限公司產品中心 | 劉明翰 | 處長 |
| **計畫團隊** | | | |
| 118. | 理律律師事務所 | 曾更瑩 | 律師 |

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

### —下世代電信網路號碼研究及DNS編碼技術概念性驗證成果—

## 會議簽到單

**會議時間**：110年9月29日(星期三)下午2時至5時

**會議地點**：集思交通部國際會議中心201會議室

(臺北市中正區杭州南路1段24號2樓)

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 交通部郵電司 | 林姝宜 | 林姝宜 |
| 經濟部工業局 | 李純孝 | |
| 國家通訊傳播委員會 | 顏聖原 | 顏聖原 |
| 國立臺灣科技大學資訊工程系 | 周詩梵 | 周詩梵 |
| 財團法人台灣網路資訊中心 | 黃勝雄 | 黃勝雄 |
| 工業技術研究院 | 林容銘 | 林容銘 |
| 財團法人資訊工業策進會 | 鄭嘉逸 | 鄭嘉逸 |
| 宜蘭大學 | 陳顧元 | 陳顧元 |

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

### —下世代電信網路號碼研究及DNS編碼技術概念性驗證成果—

## 會議簽到單

**會議時間**：110年9月29日(星期三)下午2時至5時

**會議地點**：集思交通部國際會議中心201會議室

(臺北市中正區杭州南路1段24號2樓)

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 網路中文資訊股份有限公司 | 劉莘相 | |
| 網路中文資訊股份有限公司 | 魏駿光 | |
| 網路中文資訊股份有限公司 | 賴俞帆 | |
| 遠傳電信 | 黃志雯 | |
| 交通部 | 陳日暉 | 陳日暉 |
| | | |
| | | |
| | | |

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

### —下世代電信網路號碼研究及DNS編碼技術概念性驗證成果—

## 會議簽到單

**會議時間**：110年9月29日(星期三)下午2時至5時

**會議地點**：集思交通部國際會議中心201會議室

(臺北市中正區杭州南路1段24號2樓)

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 財團法人電信技術中心 | 林輝堂 | 林輝堂 |
| 財團法人電信技術中心 | 卜慶玲 | 卜慶玲 |
| 財團法人電信技術中心 | 林永勝 | 林永勝 |
| 財團法人電信技術中心 | 陳志宇 | 陳志宇 |
| 財團法人電信技術中心 | 卓卿敏 | 卓卿敏 |
| 財團法人電信技術中心 | 王彥中 | 王彥中 |
| 財團法人電信技術中心 | 李昕甯 | 李昕甯 |
| 財團法人電信技術中心 | 彭俞蓉 | 彭俞蓉 |
| 財團法人電信技術中心 | 簡嘉儀 | 簡嘉儀 |

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

### —下世代電信網路號碼研究及DNS編碼技術概念性驗證成果—

## 會議簽到單

**會議時間**：110年9月29日(星期三)下午2時至5時

**會議地點**：集思交通部國際會議中心201會議室

(臺北市中正區杭州南路1段24號2樓)

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 財團法人電信技術中心 | 陳佳瑀 | 陳佳瑀 |
| 財團法人電信技術中心 | 郭怡萱 | 郭怡萱 |
| 財團法人電信技術中心 | 邱雯琪 | 邱雯琪 |
| | | |
| | | |
| | | |
| | | |
| | | |

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

### —下世代電信網路號碼研究及DNS編碼技術概念性驗證成果—

## 會議簽到單

**會議時間**：110年9月29日(星期三)下午2時至5時

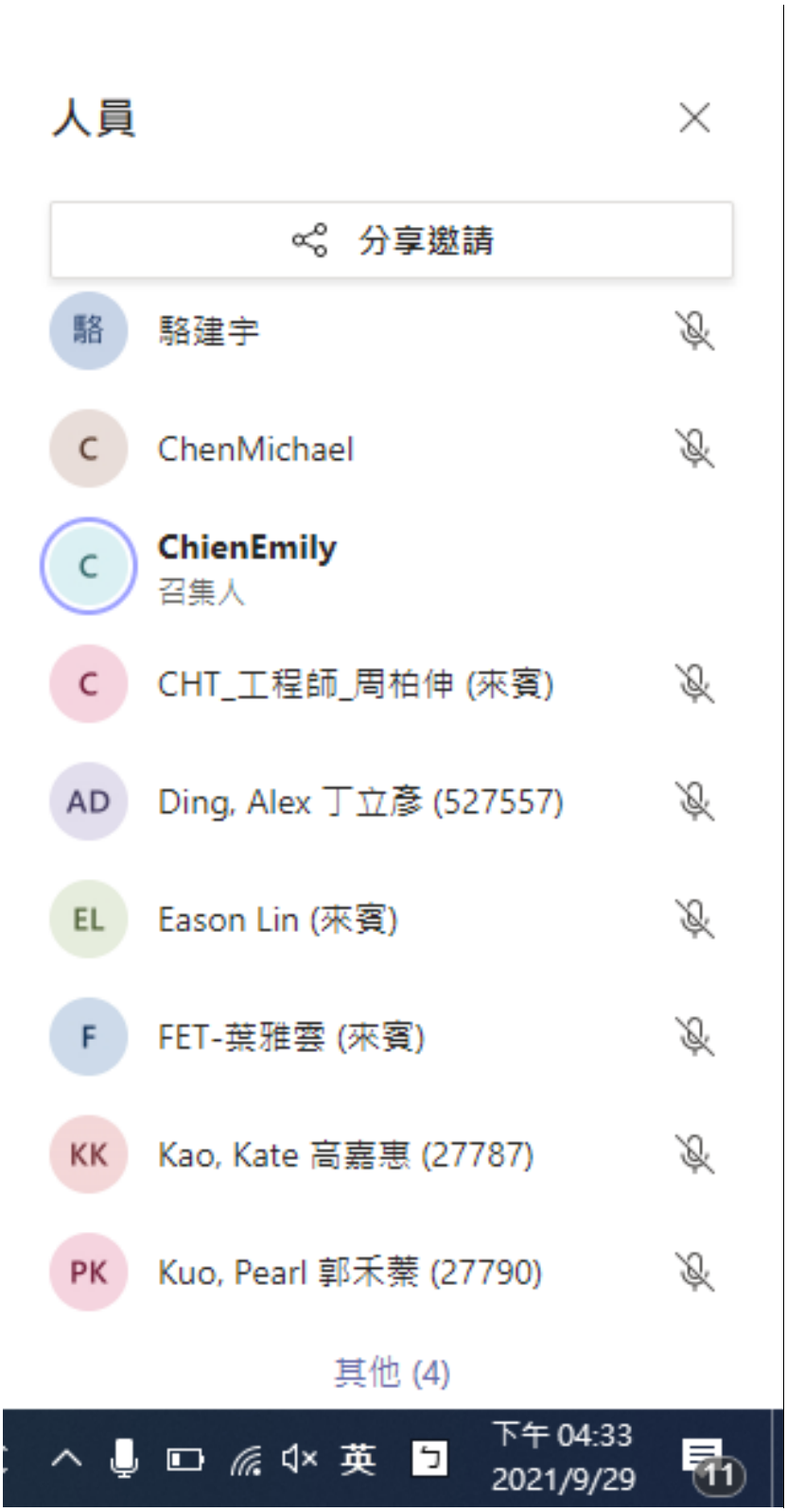
**會議地點**：集思交通部國際會議中心201會議室

(臺北市中正區杭州南路1段24號2樓)

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 台灣科大 | 陳文生 | 陳文生 |
| 鑑智實相 | 陳彥吉 | 陳彥吉 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

人員
分享邀請
目前在此會議中 (41)
T
TTC-助理研究員-彭俞蓉 (來賓)
台楊
台灣大哥大 楊博森 (來賓)
台
台灣之星_潘科諺 (來賓)
成
成大陳文字教授 (來賓)
行陳
行政院資安處 陳崧銘 (來賓)
李
李之軍
亞
亞太_方俊傑 (來賓)
亞何
亞太電信 何伯陽 (來賓)
亞李
亞太電信 李明峰 (來賓)
亞
亞太電信_唐興銘 (來賓)
時多雲
中
下午 02:31
2021/9/29

人員
分享邀請
亞太電信-許文宏 (來賓)
林永勝
范揚麟
連彥宗
曾更瑩（理律）(來賓)
郵電司_高境良 (來賓)
遠傳電信 - 黃漢臣 (來賓)
遠傳電信-廖鈺鳴 (來賓)
駱建宇
英
下午 04:32
2021/9/29
11


人員
分享邀請
駱 駱建宇
C ChenMichael
C ChienEmily
召集人
C CHT_工程師_周柏伸 (來賓)
AD Ding, Alex 丁立彥 (527557)
EL Eason Lin (來賓)
F FET-葉雅雲 (來賓)
KK Kao, Kate 高嘉惠 (27787)
PK Kuo, Pearl 郭禾蓁 (27790)
其他 (4)
英
下午 04:33
2021/9/29
11

人員
分享邀請
目前在此會議中 (29)
AD Ding, Alex 丁立彥 (527557)
EL Eason Lin (來賓)
F FET-葉雅雲 (來賓)
KK Kao, Kate 高嘉惠 (27787)
PK Kuo, Pearl 郭禾蓁 (27790)
CL Lee, Charles 李隆奇 (525405)
T TTC-李昕甫 (來賓) 保留中
T TTC一助理管理師-郭怡萱 (來...
W Webber (來賓)
英
下午 04:34
2021/9/29
11

人員
分享邀請
目前在此會議中 (29)
T
TTC-Test (來賓)
台楊
台灣大哥大 楊博森 (來賓)
台
台灣之星_潘科謬 (來賓)
成
成大陳文字教授 (來賓)
行陳
行政院資安處 陳崧銘 (來賓)
李
李之軍
保留中
亞
亞太電信_唐興銘 (來賓)
亞
亞太電信-張栢芳 (來賓)
亞
亞太電信-許文宏 (來賓)
英
下午 04:32
2021/9/29
12

## (十) 實測說明會會議照片

圖 1、電信技術中心主任報告研究背景及內容

圖 2、計畫團隊進行實測驗證報告

圖 3、PoC 實測驗證平臺設備

## (十一)產官學研專家座談會照片

圖 4、專家論壇

圖 5、工研院林咨銘博士就本案議題給予建議與指導

圖 6、與會來賓大合照

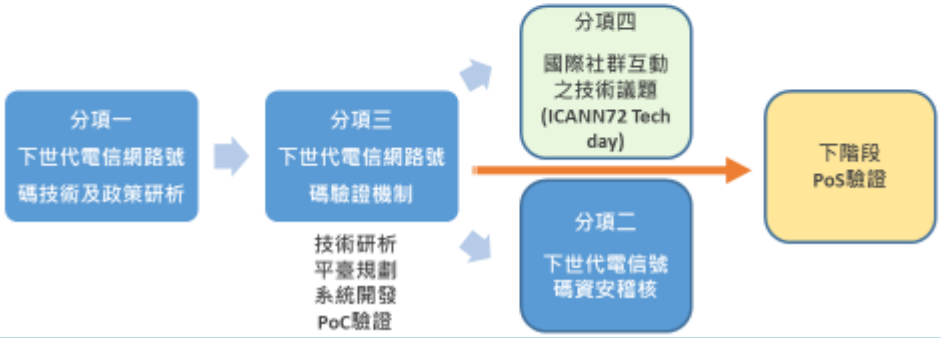
# 三、第三場座談會會議簡報

# 研究背景及內容

**研究背景**

5G時代後，物聯網、網路切片及專網等應用服務快速發展，國際組織ICANN於2020年發表「5G Technology」文件，其中探討以DNS技術作為物聯網設備之編碼方式。本計畫據其構想，參照ITU、3GPP、ICANN及ETSI標準，設計規劃本次技術概念性驗證(PoC)。

目前電信業者依E.164標準進行物聯網裝置之編碼(我國為040開頭共13碼)，適用數量有其限制，且無法直接從號碼上識別裝置特性；運用DNS技術進行物聯網裝置自動編碼之機制，可透過編碼直覺辨識裝置相關特性，建立即時、有效之管理。



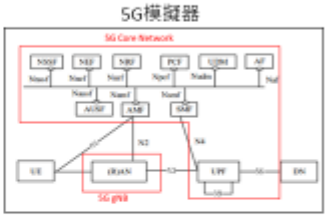


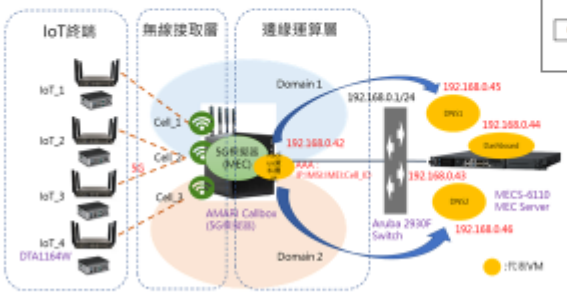

# PoC 實測驗證平臺架構

**平臺基本設定**

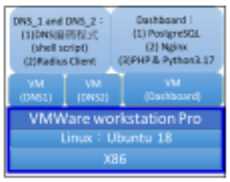
- 建置於專網環境
- 支援R15標準之5G SA架構
- 5G Wireless Network Slicing for eMBB、URLLC、MIOT

5G模擬器






MECS系統架構



# PoC 實測驗證平臺設備

# 實證場域初始狀態設備參數內容

| | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|
| APN | internet1 | internet2 | internet3 | internet4 |
| IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| NSSAI | eMBB | eMBB | URLLC | MIOT |
| SST | 1 | 1 | 2 | 3 |
| Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic Machines | Smart City Sensors |
| Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |

# 編碼機制

**本實測驗證平臺參照3GPP TS 23.003 DNS編碼原則，提出編碼規則如下：**

**<IMEI>.<Cell_ID>.<Domain_ID>. <sst>.nssf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org**

- 依據RFC952定義，域名由字母（a-z、A-Z）、數字（0-9）、「-」及「.」所組成。
- 依據RFC1123定義，每一級域名不超過63字元，總長不超過255字元，並可由域名轉譯為"#.#.#.#"形式之IP address。

1. **IMEI**：IoT裝置之品牌、型號、生產序號及驗證碼，IMEI裝置編碼具有唯一性，使本機制所產生之編碼也具有其唯一性。
2. **Cell_ID**：基地臺之識別碼
3. **Domain_ID**：地理位置
4. **SST**：Slice / Service Type
5. **MNC**：行動裝置之網路碼
6. **MCC**：裝置之國家代碼

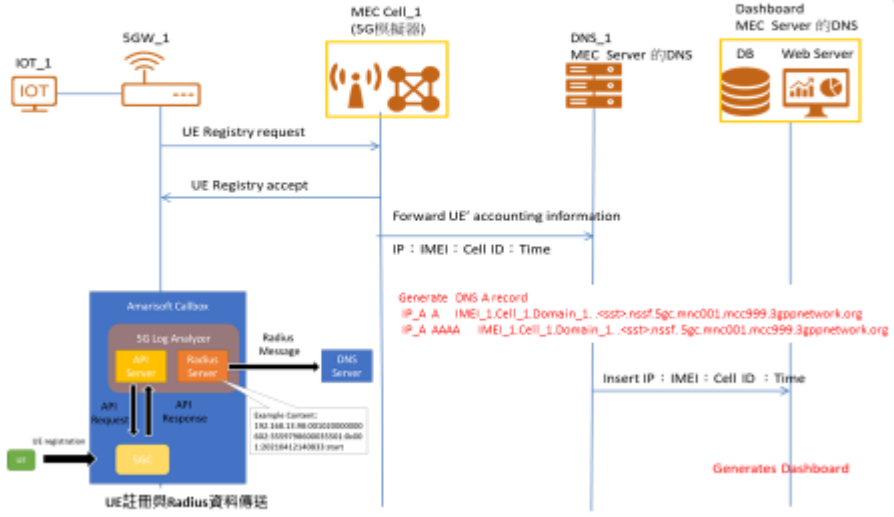
| 類別 | IoT終端層 | 無線接取層 | 邊緣運算 | 網路核心層 |
|---|---|---|---|---|
| 參考標準 | GMSA TS.06 v18.2 | 3GPP TS29.061 | | 3GPP TS 23.003 |
| DNS編碼組成規劃 | IMEI | Cell_ID | Domain_ID | SST, MNC, MCC |
| | (設備). | .(基站). | .(地區). | <sst>.nssf.5gc.mnc(mnc) .mcc(mcc).3gppnetwork.org |
| 場域編碼範例 | 355979860003363 | Cell_1 | Domain_1 | <sst_1>.nssf.5gc.mnc001 .mcc999.3gppnetwork.org |

註：mnc01.mcc999為ITU-T標準供測試使用

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. 』All rights reserved.



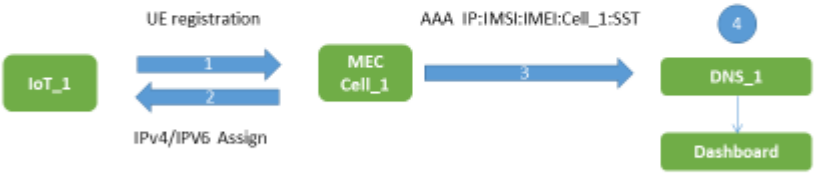
# 實測驗證平臺與註冊流程




版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. 』All rights reserved.

# IoT終端註冊自動編碼

4 Generate DNS A record
IP_A A IMEI_1.Cell_1.Domain_1.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_1.Domain_1.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org

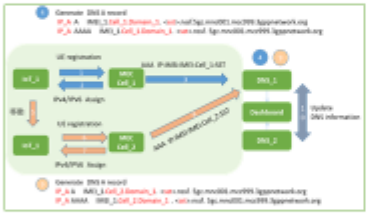





# DNS編碼技術概念性驗證測試

**本年度PoC最終成果演示：**

1. DNS編碼機制能有效管理5G網路下固定及移動位置之IoT裝置
2. DNS編碼機制能有效進行5G網路下大量IoT裝置自動編碼

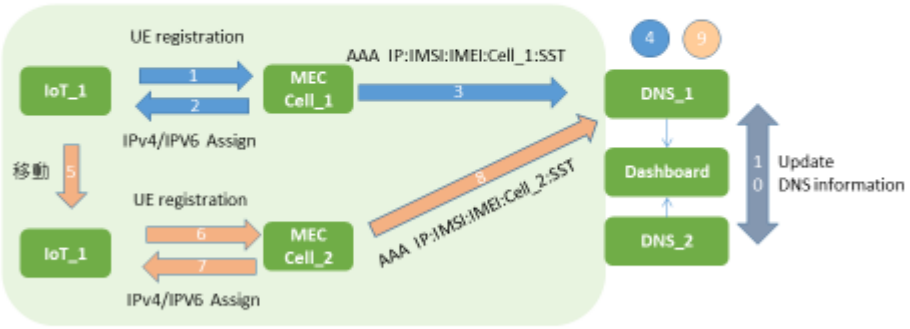
| 同域驗證信令流程圖 | 跨域驗證信令流程圖 |
|---|---|
|  | |

| 情境驗證項目 | 項次 | 同域 | 跨域 |
|---|---|---|---|
| | 1 | 邊緣運算MEC及DNS間的資料交換 | 邊緣運算MEC及DNS間的資料交換 |
| | 2 | 模擬IPv4/IPv6的IoT與DNS轉換 | 模擬IPv4/IPv6的IoT與DNS轉換 |
| | 3 | 自動生成DNS名稱機制與管理運用 | 自動生成DNS名稱機制與管理運用 |
| | 4 | 同時多個Device註冊DNS行為 | |

# IoT終端同域移動註冊流程

**從Cell_1(Domain1)移動到Cell_2( Domain1)**

4 Generate DNS A record
IP_A A IMEI_1.Cell_1.Domain_1. <sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_1.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org



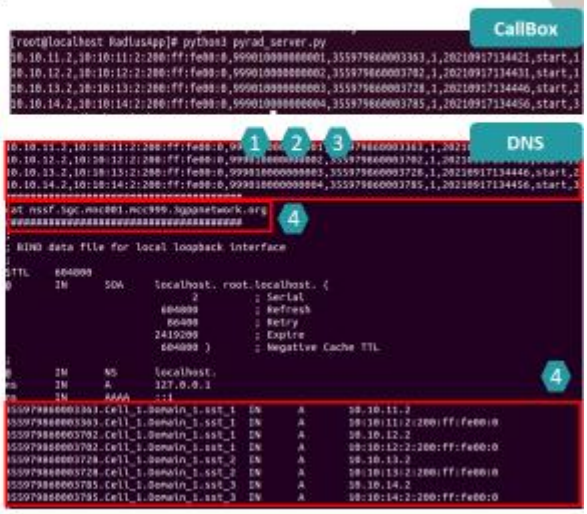

9 Generate DNS A record
IP_A A IMEI_1.Cell_2.Domain_1. <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_2.Domain_1 . <sst>.nssf. 5gc.mnc001.mcc999.3gppnetwork.org

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. 』All rights reserved.


# 同域測試步驟

**步驟1至步驟4(系統操作畫面)**

| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_1，並進行註冊 |
| 2 | 配發 IPv4/IPv6 位址 | Callbox(MEC)配發 IP 給 IoT |
| 3 | 傳送註冊認證至 DNS | 傳送[IP:IMSI:IMEI:Cell_1:SST]註冊訊息至 DNS |
| 4 | Generate DNS A record | DNS 透過同動編碼程式自動產生域名以及 DNS A/AAAA record |
| 5 | UE 移動 | IoT 從 Cell_1 移動至 Cell_2，同為 Domain_1 |
| 6 | UE registration | IoT 連線到 Cell_2，並進行註冊 |
| 7 | 配發 IPv4/IPv6 位址 | Callbox(MEC)配發 IP 給 IoT，因為同一 Domain，使用原來的 IP |
| 8 | 傳送註冊認證至 DNS | Callbox(MEC)傳送[IP:IMSI:IMEI:Cell_2:SST]註冊訊息至 DNS |
| 9 | Generate DNS A/AAAA record | DNS 透過同動編碼程式自動產生域名以及 DNS A/AAAA record |
| 10 | DNS 與 Dashboard 註冊資訊 | Dashboard 取得最新的 DNS A/AAAA record 資訊 |

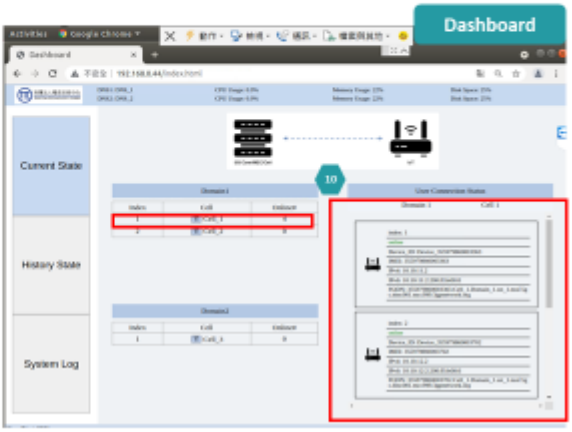



版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. 』All rights reserved.

# 同域測試步驟

步驟1至步驟4(Dashboard顯示畫面)

| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_1，並進行註冊 |
| 2 | 配置 IPv4/IPv6 位址 | Callbox(MEC)配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | 傳送[IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS |
| 4 | Generate DNS A record | DNS 透過自動產碼程式自動產生域名以及 DNS A/AAAA record |
| 5 | UE 移動 | IoT 從 Cell_1 移動至 Cell_2，同時 Domain_1 |
| 6 | UE registration | IoT 連線到 Cell_2，並進行註冊 |
| 7 | 配置 IPv4/IPv6 位址 | Callbox(MEC)配發 IP 給 IoT，因為是同一Domain，使用原來的 IP |
| 8 | 傳送註冊資訊至 DNS | Callbox(MEC) 傳送[IP:IMSI:IMEI:Cell_2:SST]等資訊至 DNS |
| 9 | Generate DNS A/AAAA record | DNS 透過自動產碼程式自動產生域名以及 DNS A/AAAA record |
| 10 | DNS 與 Dashboard 顯示資料 | Dashboard 取得重新訂 DNS A/AAAA record 資訊 |




版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 同域測試步驟

完成步驟1至步驟4後，IoT註冊IP以及自動註冊DN (相關參數)

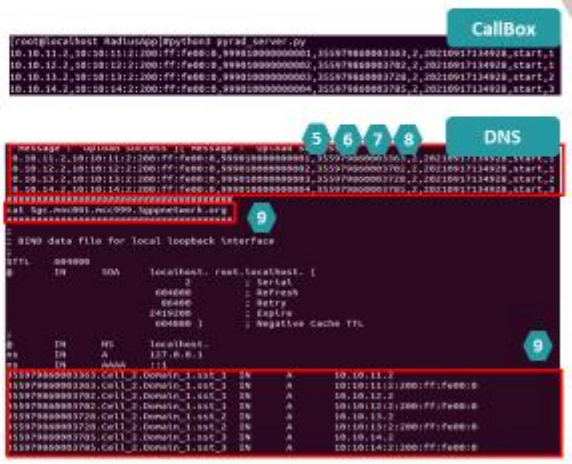
| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | APN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟1, 2 | Service IP IPv4 (DHCP) | 10.10.11.2/24 | 10.10.12.2/24 | 10.10.13.2/24 | 10.10.14.2/24 |
| 步驟1, 2 | Service IP IPv6 (DHCP) | 10:10:11.2::/80 | 10:10:12.2::/80 | 10:10:13.2::/80 | 10:10:14.2::/80 |
| 步驟3, 4 | DN | 355979860003363.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_1.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_1.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 同域測試步驟

## 步驟5至步驟9(系統操作畫面)

| 步驟 | 說明 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_1，並進行註冊 |
| 2 | 配發 IPv4/IPV6 位址 | Callbox(MEC)配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | 傳送[IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS |
| 4 | Generate DNS A record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA record |
| 5 | UE 移動 | IoT 從 Cell_1 移動至 Cell_2，同為 Domain_1 |
| 6 | UE registration | IoT 連線到 Cell_2，並進行註冊 |
| 7 | 配發 IPv4/IPV6 位址 | Callbox(MEC)配發 IP 給 IoT，因為是同一 Domain，使用原來的 IP |
| 8 | 傳送註冊資訊至 DNS | Callbox(MEC)傳送[IP:IMSI:IMEI:Cell_2:SST]等資訊至 DNS |
| 9 | Generate DNS A/AAAA record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA record |
| 10 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA record 資訊 |

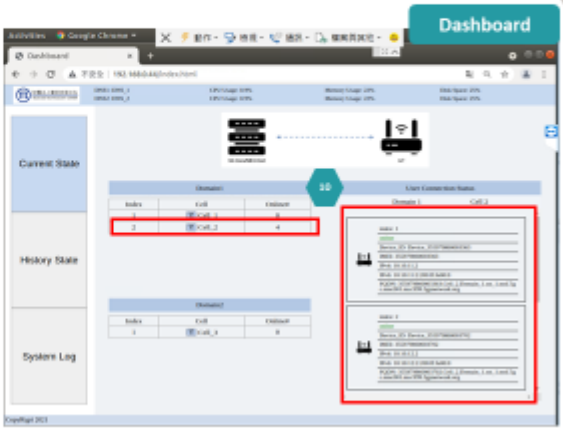





# 同域測試步驟

## 步驟10(Dashboard顯示畫面)

| 步驟 | 說明 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_1，並進行註冊 |
| 2 | 配發 IPv4/IPV6 位址 | Callbox(MEC)配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | 傳送[IP:IMSI:IMEI:Cell_1:SST]等資訊至 DNS |
| 4 | Generate DNS A record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA record |
| 5 | UE 移動 | IoT 從 Cell_1 移動至 Cell_2，同為 Domain_1 |
| 6 | UE registration | IoT 連線到 Cell_2，並進行註冊 |
| 7 | 配發 IPv4/IPV6 位址 | Callbox(MEC)配發 IP 給 IoT，因為是同一 Domain，使用原來的 IP |
| 8 | 傳送註冊資訊至 DNS | Callbox(MEC)傳送[IP:IMSI:IMEI:Cell_2:SST]等資訊至 DNS |
| 9 | Generate DNS A/AAAA record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA record |
| 10 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA record 資訊 |



# 同域測試

**步驟6至步驟10(相關參數)**

IoT終端(IoT_1)由Cell_1 移動到Cell_2，APN與IP不更換，DN會更改Cell名稱

| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | APN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic<br>Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟6,7 | Service IP IPv4 (DHCP) | 10.10.11.2/24 | 10.10.12.2/24 | 10.10.13.2/24 | 10.10.14.2/24 |
| 步驟6,7 | Service IP IPv6 (DHCP) | 10:10:11.2::/80 | 10:10:12.2::/80 | 10:10:13.2::/80 | 10:10:14.2::/80 |
| 步驟8-10 | DN | 355979860003363.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_2.Domain_1.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_2.Domain_1.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_2.Domain_1.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 同域測試步驟

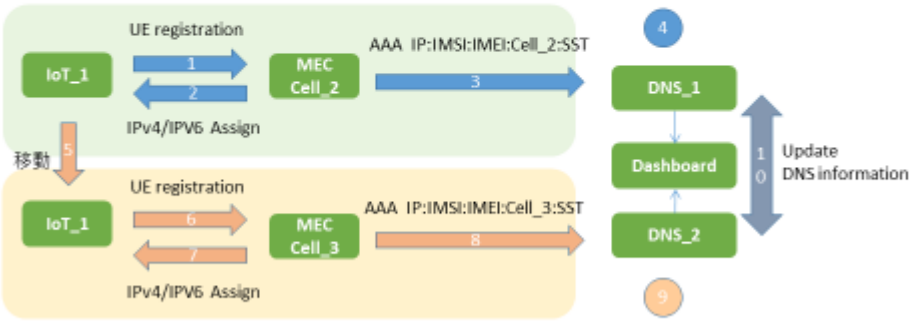
**同域測試完成，檢視Dashboard畫面**

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# IoT終端跨域移動註冊流程

**從Domain_1(cell_2)移動到Domain_2(Cell_3)**

4 Generate DNS A record
IP_A A IMEI_1.Cell_2.Domain_1.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_2.Domain_1.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org



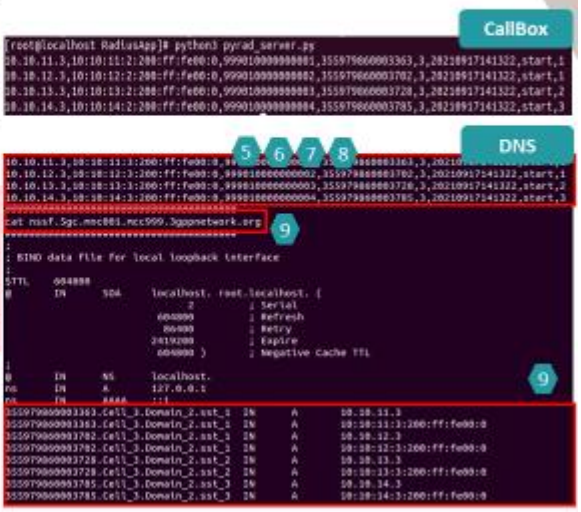

9 Generate DNS A record
IP_A A IMEI_1.Cell_3.Domain_2.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_3.Domain_2.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org

All rights reserved.


# 跨域測試步驟

**步驟5至步驟9(系統操作畫面)**

| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 感測器 Cell_2，並進行註冊 |
| 2 | 配發 IPv4/IPv6 位址 | Callbox(MEC)配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | Callbox(MEC)傳送 [IP:IMSI:IMEI:Cell_2:SST]註冊資訊至 DNS |
| 4 | Generate DNS A/AAAA record | DNS 透過自動編譯程式自動產生域名以及 DNS A/AAAA record |
| 5 | UE 移動 | IoT 從 Cell_2 移動至 Cell_3，從 Domain_1 移動至 Domain_2 |
| 6 | UE registration | IoT 感測器 Cell_2，並進行註冊 |
| 7 | 配發 IPv4/IPv6 位址 | Callbox(MEC)配發 IP 給 IoT |
| 8 | 傳送註冊資訊至 DNS | Callbox(MEC)傳送 [IP:IMSI:IMEI:Cell_2:SST]註冊資訊至 DNS |
| 9 | Generate DNS A record | DNS 透過自動編譯程式自動產生域名以及 DNS A/AAAA record |
| 10 | DNS 與 Dashboard 更新資料 | Dashboard 取得更新的 DNS A/AAAA record 資訊 |




All rights reserved.

# 跨域測試步驟

## 步驟10(Dashboard顯示畫面)

| 步驟 | 流程 | 說明 |
|---|---|---|
| 1 | UE 註冊 | IoT 連線到 Cell_2，並進行註冊 |
| 2 | 配發 IPv4/IPV6 位址 | Callbox (MEC)配發 IP 給 IoT |
| 3 | 傳送註冊資訊至 DNS | Callbox (MEC)傳送 [IP:MSI:IMEI:Cell_1:SST]等資訊至 DNS |
| 4 | Generate DNS A/AAAA record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA record |
| 5 | UE 移動 | IoT 從 Cell_2 移動至 Cell_3，從 Domain_1 移動至 Domain_2 |
| 6 | UE registration | IoT 連線到 Cell_3，並進行註冊 |
| 7 | 配發 IPv4/IPV6 位址 | Callbox (MEC)配發 IP 給 IoT |
| 8 | 傳送註冊資訊至 DNS | Callbox (MEC)傳送 [IP:MSI:IMEI:Cell_1:SST]等資訊至 DNS |
| 9 | Generate DNS A record | DNS 透過自動編碼程式自動產生域名以及 DNS A/AAAA record |
| 10 | DNS 與 Dashboard 重新查詢 | Dashboard 取得重新的 DNS A/AAAA record 資訊 |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 跨域測試

## 步驟6至步驟10(相關參數)

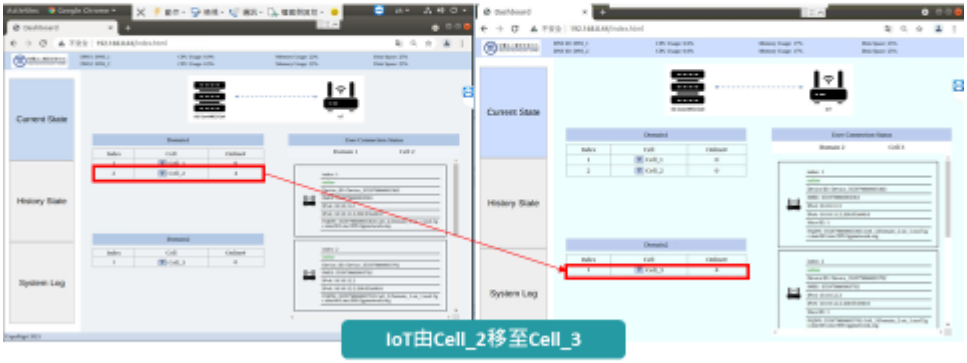
IoT終端(IoT_1)由Cell_2 移動到Cell_3，註冊到新的IP，DN會更改Cell名稱

| | | IoT_1 | IoT_2 | IoT_3 | IoT_4 |
|---|---|---|---|---|---|
| | APN | internet1 | internet2 | internet3 | internet4 |
| | IMEI | 355979860003363 | 355979860003702 | 355979860003728 | 355979860003785 |
| | NSSAI | eMBB | eMBB | URLLC | MIOT |
| | SST | 1 | 1 | 2 | 3 |
| | Template | AR/VR<br>8K Videos | AR/VR<br>8K Videos | Factory Automatic Machines | Smart City Sensors |
| | Throughput | 1Gbps/1Gbps | 1Gbps/1Gbps | 500Mbps/500Mbps | 1Mbps/1Mbps |
| 步驟6,7 | Service IP IPv4 (DHCP) | 10.10.11.3/24 | 10.10.12.3/24 | 10.10.13.3/24 | 10.10.14.3/24 |
| | Service IP IPv6 (DHCP) | 10:10:11.3::/80 | 10:10:12.3::/80 | 10:10:13.3::/80 | 10:10:14.3::/80 |
| 步驟8-10 | DN | 355979860003363.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003702.Cell_3.Domain_2.sst_1.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003728.Cell_3.Domain_2.sst_2.nssf.5gc.mnc001.mcc999.3gppnetwork.org | 355979860003785.Cell_3.Domain_2.sst_3.nssf.5gc.mnc001.mcc999.3gppnetwork.org |

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 跨域測試

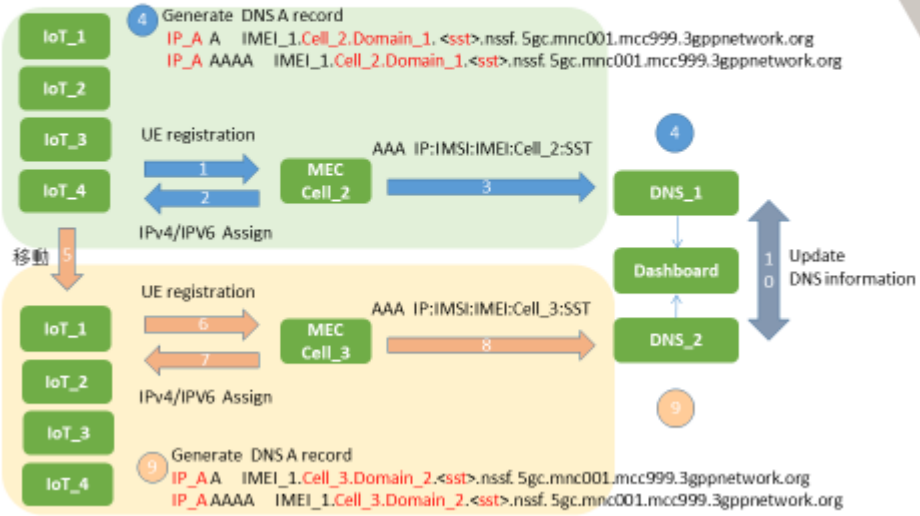
跨域測試完成，檢視Dashboard畫面





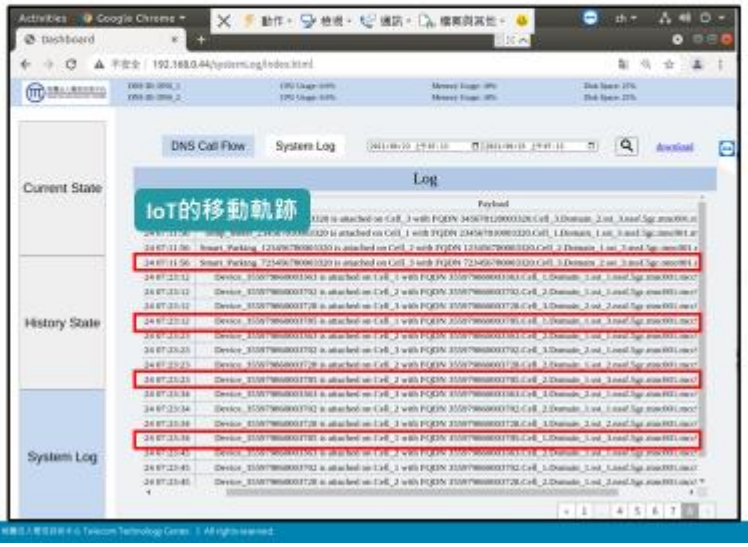

# 大量IoT裝置自動編碼測試情境1

20分鐘內使用4台IoT設備，在不同Cell與Domain間移動。



# 大量IoT裝置自動編碼測試情境1

透過log，確認IoT設備移動後的DN變化

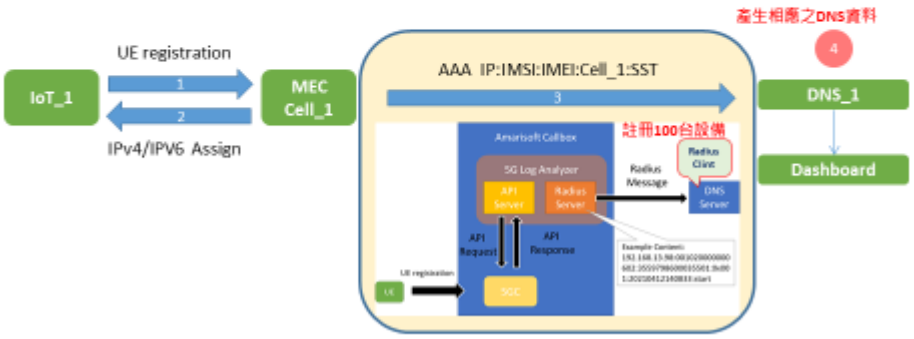





# 大量IoT裝置自動編碼測試情境2

進行大量設備註冊並產生Radius資料，傳送到DNS Server

4 Generate DNS A record
IP_A A IMEI_1.Cell_1.Domain_1.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org
IP_A AAAA IMEI_1.Cell_1.Domain_1.<sst>.nssf.5gc.mnc001.mcc999.3gppnetwork.org



# 大量IoT裝置自動編碼測試情境2

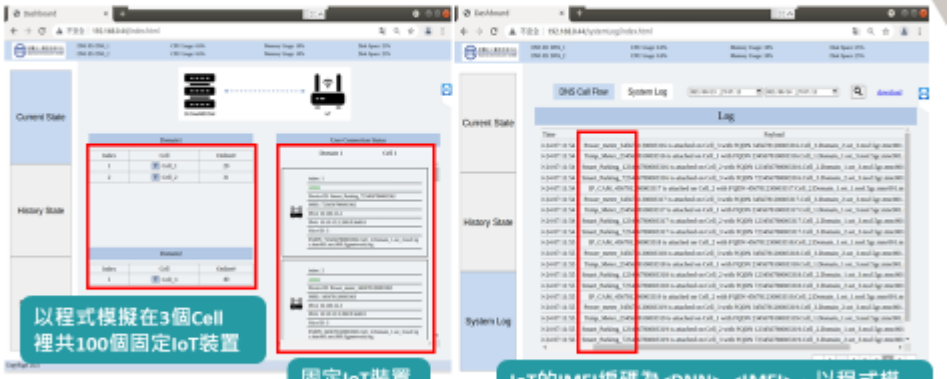
參數設計

| Name | IP_CAM | Power_Meter | Temp_Meter | Smart_Parking | Smart_Lamps |
|---|---|---|---|---|---|
| APN/DNN | IP_CAM | Power_Meter | Temp_Meter | Smart_Parking | Smart_Lamps |
| TAC (IMEI前8碼) | 45678123 | 34567812 | 23456781 | 12345678 | 72345678 |
| NSSAI | eMBB | MIOT | | | |
| SST | 1 | 3 | | | |
| Template | High quality Video | Smart City sensor | | | |
| Throughput | 100Mbps/100Mbps | 1Mbps/1Mbps | | | |
| Zone | nssf.5gc.mnc001.mcc999.3gppnetwork.org | | | | |
| Service IP IPv4 | 10.100.11.0/24 | 10.100.12.0/24 | 10.100.13.0/24 | 10.100.14.0/24 | 10.100.15.0/124 |
| Service IP IPv6 | 10.:100:11:(1-254):200:ff:fe00:00 | 10.:100:12:(1-254):200:ff:fe00:00 | 10.:100:13:(1-254):200:ff:fe00:00 | 10.:100:14:(1-254):200:ff:fe00:00 | 10.:100:15:(1-254):200:ff:fe00:00 |



# 大量IoT裝置自動編碼測試情境2

Dashboard展示



# 結語

本計畫概念性驗證(PoC)，透過以下情境：
- DNS編碼機制能有效管理5G網路下固定及移動位置之IoT裝置
- DNS編碼機制能有效進行5G網路下大量IoT裝置自動編碼

驗證DNS自動編碼之機制與方法，可運用於最新5G網路切片環境，並以有效方式管理IoT裝置。

下階段規劃在實際5G網路環境，導入電信服務情境進行服務驗證(PoS)。

## Q & A

Telecom Technology Center. All rights reserved.

中華民國交通部
MINISTRY OF TRANSPORTATION AND COMMUNICATIONS R.O.C

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

## 【二、專題報告】
## 下世代電信網路號碼對我國產業及政策影響

All rights reserved.


中華民國交通部
MINISTRY OF TRANSPORTATION AND COMMUNICATIONS R.O.C

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

# 下世代電信網路技術號碼政策發展

陳志宇 資深經理
財團法人電信技術中心

All rights reserved.

# 簡報大綱

- 電信/網路編碼之功能角色
- 電信/網路發展下之衍生政策議題
- 未來電信/網路編碼政策建議



# 未來號碼需求與角色

從固網至3G行動網路，號碼的功能除了傳統之通話、定址、SMS功能；4G、5G時代TCP/IP整合、連網、IoT技術持續推展，號碼功能亦隨時代需求而變遷。

數位化下的變革網路結構更趨複雜，APP、數位平臺等應用花開發百花齊放，逐步體現於三方面

5G核心網路演進為IP化網路架構，網路切片形成虛擬化的網路功能（NFV），虛擬化的網路資源需要一套具有彈性、相容於既有IP網路架構、易於辨識與管理的命名機制。

1.基礎設施AI化、IP化

2.物聯裝置、路由設備移動性增加

3.太空網路、行動網路、固定網路透過技術整合

當「IP」的重要性漸增，電信號碼通話、定址功能性降低，加上通訊之傳輸，接收方的關係不再固定，如何透過號碼有效識別身份／裝置，如何有效配合下世代網路互連，將會是下世代電信號碼面臨的挑戰。

# 電信及網路編碼的功能角色

- 電信網路號碼之功能（E.164、E.212）
  - **識別與定位使用者**
  - **網路互連互通**
  - **隨公眾語音通訊（參酌PSTN）之定義擴展**
- 網際網路編碼之功能（DN+IP）
  - **定位網站（IP）**
  - **識別網站（DN）**
- 新型態網際網路編碼之功能（From ITU-T X.1255：Framework for discovery of identity management information）：
  - **定位網路資源（NDN、OID、DOA）**

© 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 各種網路識別碼的功能與議題發展：

| | | |
|---|---|---|
| 應用層 | • **應用識別碼**：用於識別網際網路各項應用服務<br>• 網址（URL）：HTTP、FTP、telnet<br>• 網域名稱：Domain Name | • Named Data Networking（NDN）<br>• DNS服務安全性增強 |
| 網路層 | • **通訊識別碼**：用於識別具備通訊能力的網路節點<br>• SIM卡（E.212 IMSI）、網路卡（MAC Address）<br>• IP Address<br>• 使用者號碼（E.164） | • IPv4→IPv6<br>• New IP<br>• 物聯網號碼（040開頭之E.164編碼）<br>• E.164號碼使用效率 |
| 感知層 | • **物件識別碼**：用於識別各種實體資源<br>• 終端裝置：行動裝置識別碼（IMEI）、物件識別碼（OID）等、、 | • 數位物件架構/識別碼（DOA/DOI）<br>• 提供連網物件的定址和識別等功能，並能在各種通訊協定間進行轉換，來達到資訊存取與傳遞的目的。 |

© 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

# 電信技術的發展對編碼機制的影響

■低軌道衛星通訊

- SpaceX帶起低軌道衛星寬頻通訊的風潮：因其僅提供寬頻服務，未提供基礎電信語音通話，故尚無分配電信號碼（E.164/E.212）的需求。
- 在6G將衛星通訊納入整合後，即可能產生需分配E.164/E.212之需求。
  - 若採代理模式，則國際業者由ITU分配取得全球性號碼。
  - 若業者落地進入我國，則由我國分配E.164/E.212號碼。

■5G切片下的虛擬化資源管理

- 由於5G核心網路IP化，各虛擬運算資源也將各自分配IP。
- 利用DNS機制加以管理，有利於網路資源管理與分享。

■物聯網深入應用於不同產業垂直領域

- 利用DNS機制及自動配置（Autoconfiguration），識別網路設備，以便對其進行監控和遠端控制。
- 網路中的設備有相互通訊需求時，例如車間通訊（V2V）時，同樣可透過DNS機制加以管理、相互識別與通訊。

Telecom Technology Center. All rights reserved.


# 數位轉型與資料治理對編碼機制的需求

■數位基礎建設

- 公部門及公共物聯網
  - 利用DNS機制管理及開放政府資源。
- 資料開放與治理
  - 國發會針對政府機關或組織團體推動「物件識別碼」（OID）使用，但成效與普及有限。
  - 以數位物件架構（Digital Object Architecture, DOA），建立我國資料開放基礎。

Telecom Technology Center. All rights reserved.

# 電信及網路編碼機制的管制需求分析

■編碼之分配
- **ITU→各國通傳主管機關：E.164、E.212**
- **公私協力之中間機構管理：「.TW」Domain Name 、IP位址**
- **資料治理主責機關：DOA/DOI應用於資料開放與治理**

■網路通訊的互通性需求
- **基礎電話服務（固網、行網→衛星）**
- **基礎網際網路（DNS/IP→安全性及重要性管理）**

■未來編碼系統的重要性：（ITU-T X.1255）
- 運用於電信網路：單純進行DN/IP轉換的功能→電信網路本為關鍵基礎設施
- 運用於重要公部門服務：DN/IP轉換及網路資源管理→獨立納入CI
- 運用於一般商業服務：DN/IP轉換及網路資源管理→無須納入CI

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.


# 電信及網路編碼政策建議

■因應新電信技術演進，新電信網路發展，擴展E.164/E.212之分配範圍。
- 6G與低軌道衛星通訊：當前衛星通訊提供寬頻網路服務，並無傳統語音通訊，故尚無納入E.164編碼，當行動通訊演進至6G時，應會納入E.164號碼使用

■然而，E.164/E.212此種由ITU分配之號碼資源，有其限制性。特別是ITU會員資格與國家資格的關連性，時常不利於我國爭取分配相關資源。
- ■DNS的運作機制（ICANN）的國家限制性較低，同時，DN資源與IP位址（IPv4 & IPv6）的分配彈性較高，當資源不足時可較容易由國際組織取得新資源。
- ■持續關注新電信編碼之可能發展。

■DNS機制的延伸應用
- 公部門公共服務
- 開放資料網路資源識別
- 5G網路虛擬化網路資源管理
- 商業物聯網應用管理

■新型態編碼的使用（DOA架構）
- 政府資開放與治理

版權所有 © 2021 財團法人電信技術中心 Telecom Technology Center. | All rights reserved.

## DNS編碼機制未來政策建議

■DNS機制的隱私與安全性強化

- DNS的初始設計為DN--IP之解析機制，未考慮安全性與隱私需求。
- 具有廣泛的基礎設施、軟體整合與網際網路的相容性。
- 其名稱之分配管理兼有國家及商業用途。
- 使用廣泛，從而架構不易變動；增強安全性後可能面臨網路效能下降，延遲增加。

■假設DNS編碼機制成功作為下世代網路號碼管理系統，並廣泛應用於公共服務，將會依據不同的服務型態產生不同程度之管制，並產生相應的政策需求。

■管制程度之決定

- 將DNS機制依據其所處服務之重要性，決定是否納入關鍵基礎設施（Critical Infrastructure, CI）之管制模式（例如智慧電網）。
- 納入CI後，依據產業受管制程度高低，決定採取主管機關管制（如電網）、公私協力（例如TWNIC）、業者自律(例如企業專網)之管制機制，進而檢視資通安全管理法及相關子法之條文規範與法制框架調整。

All rights reserved.


## 結語

打造高效能、高安全的數位基礎建設，創造有利數位經濟與創新發展之環境。

因應整體網路發展趨勢，滾動檢視與調整必要法規增訂之需求

促進產業轉型，提升數位創新應用動能，驅動我國邁向智慧國家

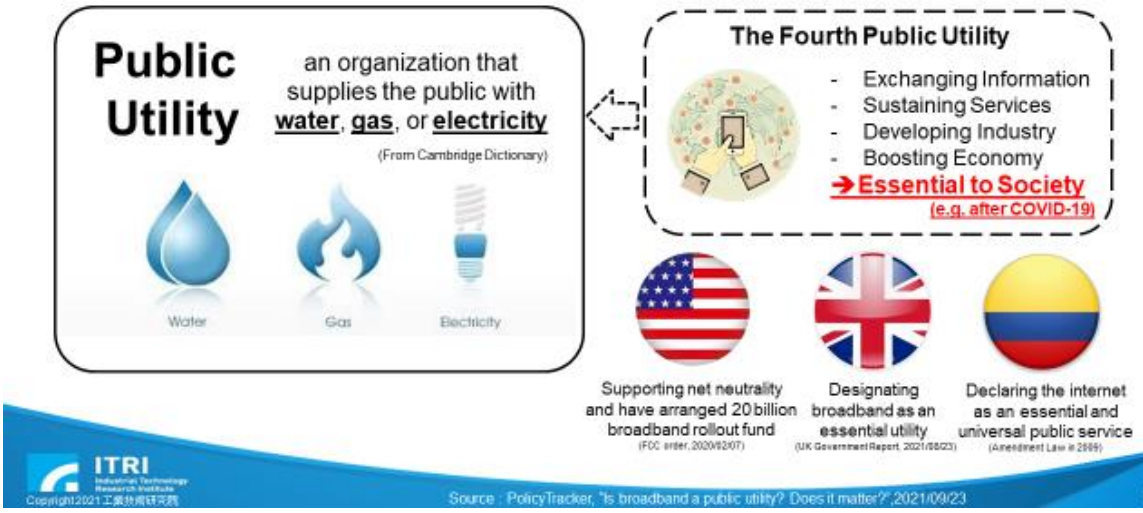
All rights reserved.

# 意見徵詢

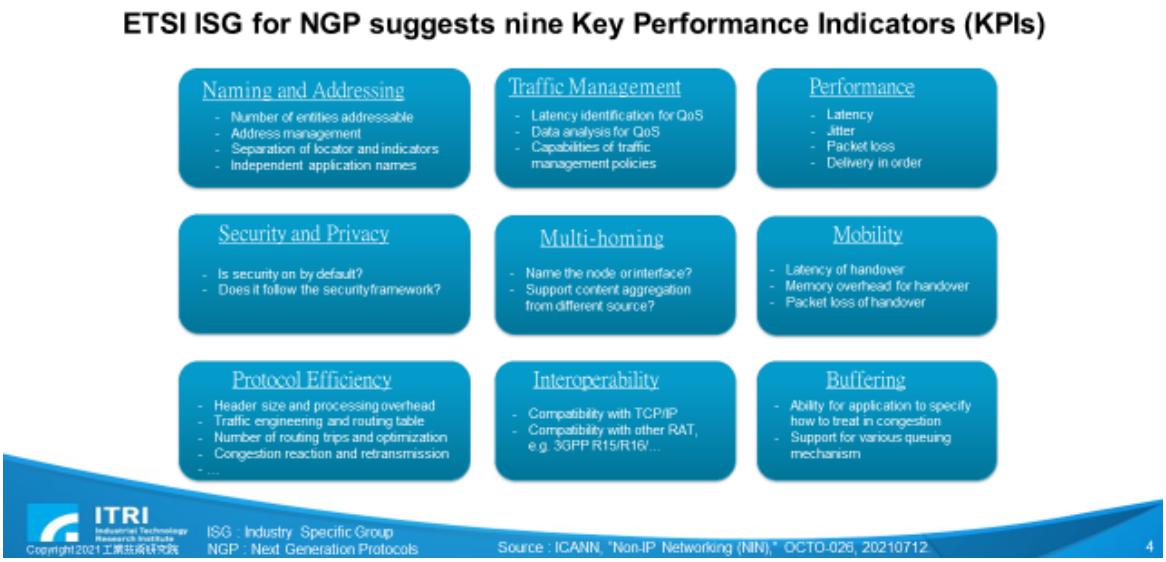
- 下世代電信網路虛擬化/網路切片對電信編碼應用之影響?
  - 下世代電信網路具有網路虛擬化及網路切片等特性，對物聯網編碼使用產生影響為何?
  - 固行網融合的趨勢對電信編碼機制需求及影響為何?
  - 在網路虛擬化及網路切片的管理上，是否需依據服務的重要性制定一致的電信號碼編碼規則(例如涉及關鍵設施)?
- 下世代電信號碼初步政策建議方案討論
  - DNS編碼註冊、分配及存儲系統之管理上應納入關鍵基礎設施(CI)管制、公私協力管制或業者自律？

ITRI
Copyright 2021 工業技術研究

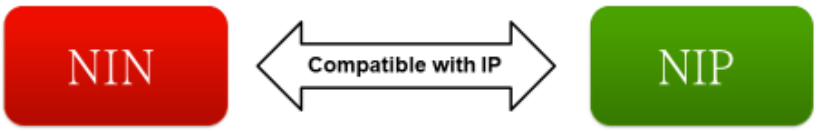
# 未來電信網路將成為第四公用事業




# 下世代電信發展與管理議題 - 1



# 下世代電信發展與管理議題 - 2




**Non IP Network**
- Label replacement (Small IP)
- Virtual circuit to separate control and data plan
- Allow to removal of IP headers in packets

**New IP**
- Define new IP header (Big IP)
- Datagram to enable QoS features
- Enforced by intermediary routers

ITRI Industrial Technology Research Institute
Copyright2021工業技術研究院
Source : ICANN, "Non-IP Networking (NIN)," OCTO-026, 20210712


# 總結與建議

- 未來電信網路將可被視為公共事業
- 下世代電信可依據不同效能指標進行管理
- NIN與NIP的發展與競合值得追蹤關注

ITRI Industrial Technology Research Institute
Copyright 2021 工業技術研究

# 壹拾、交通部 110 年度「下世代電信網路號碼技術研析及管理」委託研究計畫經驗分享會議紀錄

## 一、 國際電信技術發展趨勢暨國際會議經驗談

**(一)**時間：2021 年 6 月 1 日(二)下午 2 時

**(二)**地點：線上會議

**(三)**講者：沈信雄 科長

**(四)**與會人員：

| 單位 | 姓名 | 職稱 |
|---|---|---|
| 顧問團隊 | 曾更瑩 | 顧問 |
| | 羅乃維 | 顧問 |
| | 陳麒元 | 顧問 |
| 中心本部 | 卜慶玲 | 副執行長(協同主持人) |
| 研企組 | 陳志宇 | 研究員代資深經理 |
| | 王彥中 | 研究員 |
| | 李昕甯 | 助理研究員 |
| | 夏慧馨 | 助理研究員 |
| 應服組 | 林永勝 | 主任(計畫主持人) |
| | 卓卿敏 | 資深經理 |
| | 柯盈池 | 工程師 |
| | 洪希真 | 管理師 |
| | 謝伊凡 | 副管理師 |
| | 簡嘉儀 | 副管理師 |
| | 郭怡萱 | 助理管理師 |

**(五)**綜合討論發言紀錄：

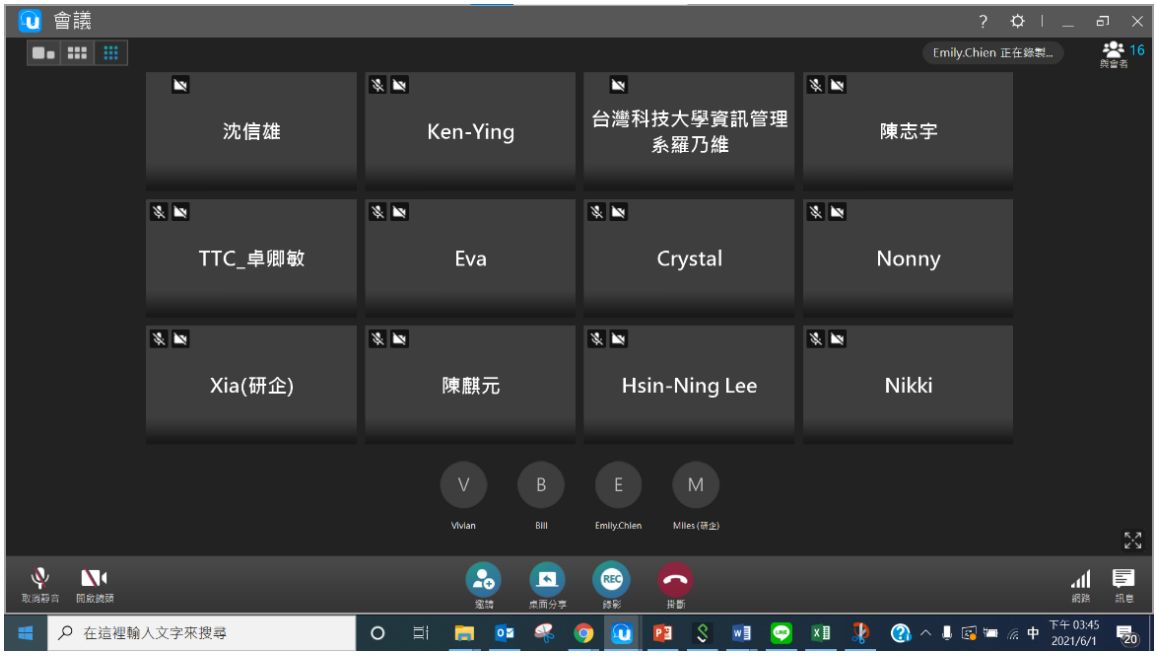
| 題目 | 紀錄 |
|---|---|
| 號碼核配是由 NCC 核配嗎？ | 因為台灣不是 ITU 會員，業者可以依據 GSMA 業者組織網路管道獲得 MNC，並通報 NCC 備查。 |
| 目前 NCC 執行交通部計畫，申請一個實驗性的網路號 | 若有跟裝置連接，僅連接 1 個裝置，需留意與當前號碼不可重複； |

| 題目 | 紀錄 |
| --- | --- |
| 碼，需要跟 NCC 備查嗎？ | 若需與全世界裝置連接，則需與 ITU 申請網路號碼，有一個 999，9 開頭的可作為連線之實驗裝置，(詳細規範可參考 1.212)；若無與裝置連接，僅在封閉場域中實驗，則不受規範。 |
| 想請教沈科長，我國目前在 ITU 參與情況 | 因進去 ITU 會議通常皆需查看護照，持台灣護照無法進入會場會議，目前已知工研院有參與 ITU-R，是用美國公司+美國護照方式進入。台灣電信廠商若需得知會議資訊，皆需透過其他國家取得會議內容後，於會後提供資料。 |
| 先前與交通部開會，交通部長官曾經說過中華電信有參與 ITU-T 經驗。 | 參加 ITU 的方式，若是以個人名義，或是有些會議場次對與會人員資格要求無特別規範，是可以參與會議的，並不是特別困難，但這樣的方式並不是所謂的進入 ITU 組織。 |
| 想了解 ICANN 是否會用 DNS 核發號碼嗎？ | ICANN 不會發電信電話號碼，ICANN 不會做超過 Level Domain Name 的事。例如：LINE 不須用共種網路或電信，所以用 LINE 打電話不需 Domain Name。 |
| 目前計畫是以 DNS 作為電信號碼網路編碼，其中一個分項是培育人才參與國際組織，想請教沈科長是否有參與策略方針。 | 參與國際組織以個人名義參與沒什麼問題，但台灣要如何打入國際組織，組織規章都訂得很清楚，要實際加入有難度。要深入瞭解組織國際組織如何運作及規章很重要。 |
| 請問科長過去 ICANN 的參與經驗 | 以參與 ICANN 來說，就是先多聽多看，組織的相關規章，實際參與了解會議如何操作，與各國代表交流，將會議內容帶回來，討論我們能深入組織的機會。 |

**(六)**散會：下午 4 時 30 分

**(七)**「國際電信技術發展趨勢暨國際會議經驗談」簽到單

本次會議共 16 名人員參與，詳如下列：



## 二、 國際電信技術趨勢與參與國際會議經驗談

**(一)**時間：2021 年 6 月 30 日(三)下午 3 時

**(二)**地點：線上會議

**(三)**名稱：國際電信技術趨勢與參與國際會議經驗談

**(四)**講者：黃勝雄 董事長

**(五)**與會人員：

| 單位 | 姓名 | 職稱 |
|---|---|---|
| 顧問團隊 | 曾更瑩 | 顧問 |
| | 羅乃維 | 顧問 |
| | 陳麒元 | 顧問 |
| 中心本部 | 卜慶玲 | 副執行長(協同主持人) |
| 研企組 | 陳志宇 | 研究員代資深經理 |
| | 王彥中 | 研究員 |
| | 邱儀萱 | 研究員 |
| | 彭俞蓉 | 助理研究員 |
| | 王資寧 | 助理研究員 |
| | 胡依淳 | 助理研究員 |
| | 李昕甯 | 助理研究員 |
| | 夏慧馨 | 助理研究員 |
| 應服組 | 林永勝 | 主任(計畫主持人) |
| | 卓卿敏 | 資深經理 |
| | 柯盈池 | 工程師 |
| | 簡嘉儀 | 副管理師 |
| | 郭怡萱 | 助理管理師 |

**(六)**綜合討論發言紀錄：

針對分享會會議簡報部份，問題及答覆如下：

| 問題 | 答覆 |
|---|---|
| 請黃董事長具體分享完成 RFC 文件制定,需投入多少人力、經費及時間等資源。 | 就提出 RFC-3743 的經驗分享經驗。RFC-3743 於 2004 通過標準，2000 年開始與日本、中國、香港、澳門、韓國、新加坡，共同於日本開會，針對漢字訂定國際標準。日本針對本計畫編列 100 萬美金，台灣是由 TWNIC 編列預算及個人名義出資，各國花費 2 年時間共同完成。2 年之 |

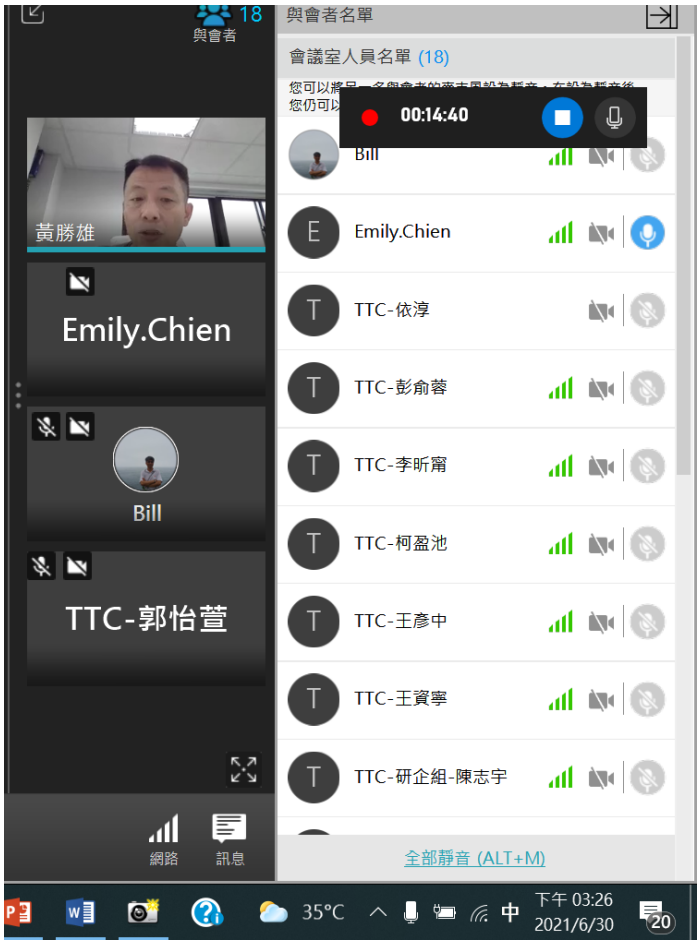
| | |
|---|---|
| | 後，各自國家的資源結束。直到最後通過 RFC 標準，共耗費 4 年時間才完成。中、日、韓集結了幾百個工程師、幾百個人月，僅訂定其中一個標準。 |
| 請問可否分享您在 IETF 的會議提 proposal 文件方面討論的經驗分享。 | 在 IETF 會議中，不僅是針對 proposal 文件討論，在 IETF 會議前已經就討論相關技術規格開會，去 IETF 報告的第一次會議就被要求必須做 demonstration，例如這個規範會耗費多少系統資源，須在現有經濟可行的系統方案及數位環境之可實行，因此在 IETF 會議前做了很多技術的實作，除了 propose 外還有許多實作，光實作就耗費了前兩年時間。討論技術方向，若未達成共識可能須走回頭路，也會耗費很多時間。 |
| 請問具體說明 BCP 及 RFC 的標準制定流程。 | BCP 或 IETF 的 RFC 的標準審查程序是一樣的，走的路徑及審查力度也大同小異，皆需要在實務驗證上須確認在目前資訊環境是可實施的。差異是後面程序會歸類 BCP 或 RFC，於後面的路徑做調整。 |
| 國內主管機關希望 TTC 在國際組織中扮演一些關鍵角色，可否提供一些建議？ | 可以當作一個理想或目標，從現況到目標需要一個推動的藍圖，如何落實或是最後是否落實是一回事，目前看來從現況到藍圖的部分是比較薄弱，且藍圖的推動不能僅依靠單一部會，可能與人才培育、外界技術合作者、與國外合作夥伴及與國際政治互動等問題有關。IETF 政治介入相對難度低，所以考量技術與可落實性，做好就很有機會可以發展。除政府期待外，還需考慮參與者的意願及意義。 |
| 就講者經驗，可否提供台灣參與 IETF 需投入的方向？ | 在領域方面，台灣在資通訊產業很強，廠商在設計能力很強，但他們在國際標準制定無太多涉略，台灣在開發能力很強，不用擔心能力，在 IETF 的 Routing、Security、Transport Area 在參與上都有很大的著力點，總結：<br>台灣有相關能力及實力的都有，只是他們 |

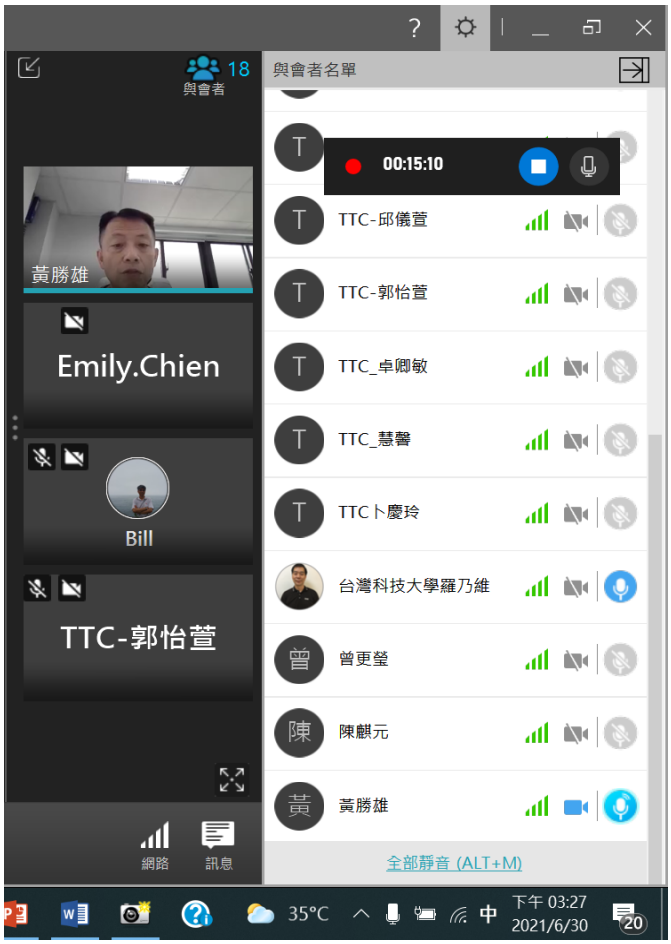
| | |
|---|---|
| | 比較少參與國際標準制定 2.在研究人員、研究單位、廠商等在制定標準經驗薄弱 3.廠商、研究機構、研究人員等須足夠的參與動機。4.國家政策的動力推進上也很重要，需設計誘因讓更多人有參與動機。 |
| 參與 IEFT 情境上，鼓勵政府部門跟學界及業界合作，在實作面方面，最後與業界合作，將標準付諸實行，TTC 角色則是由第三方中立角色從中協助，是否為一理想的方向。 | 資源分配方面，沒有學界的參與相對力道會薄弱很多，學界有研究屬性，在 IETF 提新方案，研究思維有必要，產界方面，我所了解業界在參與標準制定的商業動機很薄弱。在資源配置上有研究能量投入，在學界的既有研究在去轉型，推進的進度會比較快。<br>IETF 還是以研發為主，若台灣的學術研發能量加入，進而推進標準制定，較適切。 |
| 就講者經驗來看，過去拿到 RFC 標準是多國人員合作還是單一國家？東亞國家之研究學者在參與 IETF 參與尚有甚麼策略？ | 參與國際標準討論，不太可能是單一國家提出想法，聚集相關利害關係人，爭取支持，界定反對者有哪些，凸顯問題顯著性，相關利害關係人需要一起合作，在一開始就需要了解提案會有多少人支持與合作。 |
| 本計畫需參與 ICANN 國際會議及與 ICANN IROS 互動交流，請問可否針對 ICANN IROS 互動模式、實際產出內容及衡量標準提供建議？ | ICANN 在政策制定上與 IETF 完全不同，ICANN 也不同的利害關係人及生態系統，複雜程度會比較高，ICANN 涵蓋範圍又更高，有技術、資源管理、使用者權益、商業、公共利益為導向，不同面項皆需取得一個平衡點，所以在網路治理面向上複雜性高。在爭議處理機制上，也比 IETF 高蠻多。所謂利害關係人是：1.需確保他是多方利害關係人 2.需有開放透明的政策治理程序 3.不同意見衝突時的爭議解決方式。 |
| 本計畫核心是與電信號碼相關，若要在 ICANN 上就相關主題進行動員或討論，或在群組發起相關討論以帶動政策，有何建議？ | 政策面需先了解屬於哪個屬性，因為 ICANN 是很大的社群，可以針對某個社群，進入特定議題討論。若以電信號碼為主，可以針對議題特性去聚焦，也不一定是 ICANN 或 IETF 組織為主。所以須先聚焦社群再進入討論。 |

**(七)**散會：同日下午 16 時 00 分。

(八)「國際電信技術趨勢與參與國際會議經驗談」簽到單

本次會議共 18 名人員參與，詳如下列：



## 三、 下世代電信網路號碼技術研析及管理諮詢會議

**(一)**時間：2021 年 10 月 14 日(四)下午 2 時

**(二)**地點：財團法人電信技術中心_板橋_大會議室

**(三)**名稱：下世代電信網路號碼技術研析及管理諮詢會議

**(四)**講者：鄧添來前司長

**(五)**會議紀錄：郭怡萱助理管理師

**(六)**出席人員：

| 單位 | 姓名 | 職稱 |
|---|---|---|
| | 鄧添來 | 交通部前司長 |
| 電信技術中心研企組 | 陳志宇 | 資深經理 |
| | 王彥中 | 研究員 |
| | 彭俞蓉 | 助理研究員 |
| | 李昕甯 | 助理研究員 |
| | 夏慧馨 | 助理研究員 |
| 電信技術中心<br>應服組 | 卓卿敏 | 資深經理 |
| | 簡嘉儀 | 副管理師 |
| | 陳佳瑀 | 副管理師 |
| | 郭怡萱 | 助理管理師 |

**(七)**討論內容：

1. 計畫內容建議：

(1) 我國電信編碼係採用 ITU 所發布的 E.164 建議書，而該編碼機制優點為有彈性、可擴充、易辨識；而在網際網路定址，國際上則是採用 ICANN 所定義的 DN 編碼，其主要是供人記憶，並透過 IP 搜尋位置，建議計畫團隊可分別將 IP 及 E.164 號碼分析及比較。

(2) 由於在下世代電信技術仍處於發展階段，國際上亦未有新的編碼方式，因此建議計畫團隊持續觀測 ITU 及 ICANN 在電信號碼及網際網路定址發展。

2. 立法院擬答表建議：

(1) 立法委員較關注政策發展、社會及民生相關議題，建議擬訂「下世代電信政策如何因應」、「參與國際會議經費及效益」等政策方向議題，以利提供交通部參考。

(2) 計畫團隊提擬之擬答表相關建議如下：

| 計畫團隊提問 | 建議回覆 |
| --- | --- |
| 未來 Starlink 落地後，倘是用美國核發之IP/DN或自己研發之 IP/DN，我國如何監管？可否逼迫該公司使用台灣核發之IP/DN？處理原則為何？ | 因通訊監察法的問題，故低軌衛星需要在台灣設立 Gateway 地面站，故不會有監測漏洞。當行動電話 IP 進入我國區域，仍需至原註冊廠商進行註冊，取得用戶資料。類似目前網際網路 DN，之前網址無.tw，在台灣使用，Gateway 仍可監控及保留相關紀錄。 |
| 本計畫與其他部會在執行的資安防護相關計畫有什麼不同？相對之優、缺點各為何？以及如何串接上其他部會的資安防護機制？ | 本計畫是政府整體計畫的一小環，上游是經濟部製造商。下游是電信營運商，本計畫角度是中間銜接的橋樑，會將國內的設備和電信營運商做試驗測試證實可行。 |
| 本計畫號碼驗證能否通過 5G OTIC 驗證，或是有否通過驗證之時程規劃，且必須提出介面與各項驗證所依循之指引或標準名稱。 | 通過 OTIC 是本計畫需努力的目標，但不能保證驗證一次通過。會詢問有關 OTIC 的委員我認為也不多，請參考會前提供的經濟部台美 5G 合作參考資料，說明較大方向的問題，從資料中找題目及答案，不須從太深入技術的角度切入。題目亦同步修改成與產業、民眾有關之議題。 |
| 本計畫參與之國際會議為何？參與策略？是否訂定 KPI？訂定原則？ | 擔任國際組織幹部一事，仍須考量許多變數，除人才本身能力之外，仍須考量專業人才是否獲得國際組織成員支持及利益團體遊說等因素，因此建議將該項目目標(KPI)設定為「培育有能力擔任幹部之人才」，而驗證方式為擔任國際會議主持人。 |

3. 新進交通部郵電司文官之課程文件，以使所培育專家學者協助新進事務官代表官方推動資安外交/資訊外交之課程框架：

(1) 事務官應先提升及瞭解電信技術，爾後方能進行政策制定等事務

推動，有鑑於此建議新進文官可透過交通部內部訓練，亦或是中華電信訓練所等課程進行技術培訓。

(2)另外建議可參與美國電信訓練機構(United States Telecommunications Training Institute，USTTI)，有鑑於該訓練機構匯集各國電信政策制定者及工程師，因此透過該機構強化專業技能外，亦能建立與國際電信政策交流互動之管道。

4. 人才培育短、中、長期培育規劃：

有關人才培育短、中、長期培育規劃，建議人才可多參加國際會議，並長期投入資源，此外建議將該項目目標(KPI)設定為「培育有能力擔任幹部之人才」，而驗證方式為擔任國際會議主持人。

5. 針對諮詢會議內容提問內容：

| 問題 | 答覆 |
| --- | --- |
| 綜觀 ITU、ICANN 及 IETF，全球網際網路是靠各國的電信網路所構成，彼此互聯有一全球性架構，如海纜及目前發展中的低軌衛星，所以掌控權在誰手上就會是個非常重要的議題。長遠來看，低軌衛星部分，衛星與衛星間使用雷射光通訊，可以減少地面上傳輸的路徑及延遲，未來是否可預見低軌衛星取代海纜。<br>國內現行法規有一定程度的保護，若提供電信服務需要配合通訊監察監管，但面對新興通訊發展的業務，網際網路功能已不如以往強調對通話的意義。從郵電司角度來 | 1. 低軌衛星取代海纜議題還為之過早。衛星軌道的位置需要向 ITU 登記，台灣的衛星是向新加坡登記，但新加坡有一些問題，需要再向鄰近國家連結。所以掌控權在誰手上也是一個問題。若討論衛星取代地表通訊，尤其台灣人口密集，故還為之過早，可將焦點放在 HAPS 系統研究等適合台灣等小型國家。<br>2. 就編碼而言，重點是可互通、連接及受大家認可。ITU 的 E.164 是因為過去交換機的使用，從中央政府、地方政府等分層分配連接，有一個邏輯性的系統供辨識，並沿用幾十年。過去媒體常常爭論，台灣使用 886 國碼是否會被收回，答案是不會。雖然 ITU 在 886 登記非台灣，為特別保留碼，但編碼的實際應用並無想像中容易，國碼需與各國交換機進行設定，並無法輕易改變。號碼方面，在研究過程 |

| | |
|---|---|
| 看，如何定義下世代編碼，是否應該設定一套國內願意配合且遵守的專屬編碼機制，或是編碼機制回歸到應用面，建立轉換及互通機制，請問哪一條路是比較適當的考量及選擇？ | 中，需注意應取得國際認可號碼及廣泛性的建議，且面臨改變亦是很複雜的問題。作為物聯網、通訊的號碼必須由國際認可才可以連接。若未來可以結合 ITU 及 ICANN 號碼的轉換器，是深入研究的方向。 |
| 有關本案分項四人才培育，需要開設人才培訓課程，培訓交通部郵電司事務官，課程目的是了解目前計畫內容，供政府後續推動資安外交及資訊外交工作，以供未來併入數發布之政策建議。 | 以我觀點看，郵電司新進員工對工作內容涉入不深，尤其是技術面的知識。故首先應先到電信訓練(電信學院)所或相關驗證中心，通過一系列課程，建立技術知識再談後續政策規劃。<br>有關資安外交及資訊外交等議題，TWNIC 在資安的部分也有經驗，在驗證資安過程，請駭客分享經驗，所以建議可找駭客專家進行訪談。 |
| 執行案子過程中，業主希望計畫團隊設想未來如網路切片的應用發展。目前訪問業者得到回答是還在研發階段或有相關成本考量，仍傾向使用專網而非網路切片。就司長經驗來看，從交通部郵電司的角度看，需要設想的前瞻內容情境為何？ | 行政機關需維持開放中立態度，業者專網可以自建，也容許建立合作關係。重點是需要考慮將來使用頻譜的收費方式及人才的能力等。請業者自行評估之後，選擇使用何種方式，結果亦自行承擔。 |

**(八)**散會：同日下午 4 時

**(九)**下世代電信網路號碼技術研析及管理諮詢會議_簽到單

本次會議共 11 名人員參與，詳如下列：

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

### —下世代電信網路計畫諮詢會議—

## 會議簽到單

**會議時間**：110年10月14日(星期四)下午2時至5時

**會議地點**：財團法人電信技術中心_板橋_大會議室

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 行政院科技會報辦公室 | 鄧添來 | |
| 財團法人電信技術中心 | 卓卿敏 | |
| 財團法人電信技術中心 | 陳志宇 | |
| 財團法人電信技術中心 | 王彥中 | |
| 財團法人電信技術中心 | 李昕甯 | |
| 財團法人電信技術中心 | 彭俞蓉 | |
| 財團法人電信技術中心 | 簡嘉儀 | |
| 財團法人電信技術中心 | 陳佳瑀 | |
| 財團法人電信技術中心 | 郭怡萱 | |
| 財團法人電信技術中心 | 余曜成 | |

1

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

### —下世代電信網路計畫諮詢會議—

## 會議簽到單

**會議時間**：110年10月14日(星期四)下午2時至5時

**會議地點**：財團法人電信技術中心_板橋_大會議室

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 鑑智資相 | 陳彥吉 | 陳彥吉 |
| 研企 | 夏聖陳 | 夏聖陳 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## (十)會議照片

| | |
|---|---|
| | |
| 交通部周添來司長給予本計畫指導及建議 | |

# 壹拾壹、交通部 110 年度「下世代電信網路號碼技術研析及管理」國際會議行前諮詢會議紀錄

## 四、 ICANN72 行前諮詢會議會議紀錄

(一)會議時間：110 年 10 月 18 日（星期一）下午 3 時

(二)實體暨線上會議：

1. 地點：財團法人電信技術中心板橋大會議室（新北市板橋區遠東路 1 號 3 樓 B 室）
2. 線上：會議連結 https://u.cyberlink.com/meeting/698496863

(三)出席人員：

| 單位 | 姓名 | 職稱 |
|---|---|---|
| NII 產業發展協進會 | 吳國維 | 顧問 |
| | 梁理璇 | 副執行長 |
| 網路中文資訊股份有限公司 | 魏駿光 | 資深營運經理 |
| | 賴俞帆 | 專案經理 |
| 顧問團隊 | 曾更瑩 | 律師 |
| | 羅乃維 | 教授 |
| | 陳麒元 | 副教授 |
| 財團法人電信技術中心 | 卜慶玲 | 副執行長 |
| | 林永勝 | 主任 |
| | 卓卿敏 | 資深經理 |
| | 王彥中 | 研究員 |
| | 彭俞蓉 | 助理研究員 |
| | 李昕甯 | 助理研究員 |
| | 夏慧馨 | 助理研究員 |
| | 簡嘉儀 | 副管理師 |
| | 陳佳瑀 | 副管理師 |
| | 郭怡萱 | 助理管理師 |

(四)會議紀錄：網路中文

(五)會議報告事項摘要

**1. ICANN 國際組織參與經驗分享會：**

由前 ICANN 董事吳國維概要介紹 ICANN 組織、組織運作及屬性，並分享參與該組織建議事項。

**2. ICANN72 議程簡介：**

(1) 本次會議係 ICANN「年度大會」(Annual General Meeting，簡稱「AGM」)，於本（2021）年 10 月 25 日至 10 月 28 日以「全球遠端參與形式」舉行，議程共有 4 天。

(2) 本專案將參與之會議列表：

| 台灣日期 | 台灣時間 | 會議名稱 |
|---|---|---|
| Oct, 15 | 04:00-05:00 | Introducing the DNS Security Facilitation - Technical Study Group (DSFI-TSG) |
| Oct, 26 | 00:00-01:00 | Tech Day（1 of 3） |
| | 01:30-03:00 | Tech Day（2 of 3） |
| | 03:30-05:00 | Tech Day（3 of 3） |
| Oct, 27 | 03:30-05:00 | SSAC Public Meeting |
| Oct, 27 | 07:30-08:30 | Joint Meeting: ICANN Board and SSAC |
| Oct, 28 | 03:30-05:00 | DNSSEC and Security Workshop（1 of 3） |
| | 05:30-07:00 | DNSSEC and Security Workshop（2 of 3） |
| | 07:30-08:30 | DNSSEC and Security Workshop（3 of 3） |

**3. Q&A：**

| 問題 | 回答 |
|---|---|
| 本專案需與 ICANN IROS 進行交流，然而與 OCTO 書信往來杳無音訊，故改與 Tech Day 進行交流。針對技術部分，請問此是否可行？或有其他方法得以與 ICANN 進行交流、聯繫或合作？ | 吳國維顧問表示針對技術部分，與 ICANN 交流並不容易，ICANN 技術人員都是 IETF 的人，不善於社交，若提出問題不夠專業，可能不會回應。技術交流部分，可以請黃勝雄執行長協助牽線。 |
| 本次 ICANN72 會議議題及重點為何？ | 1. 網路中文表示大部分 ODA、ODP 或是 PDP 處於剛開始或臨近結案，之前也盤點目前正在啟動之 |

| | |
|---|---|
| | 工作小組予 TTC。會後會提出 ICANN72 參與建議供參(如附件)。<br>2. 吳國維顧問表示 Whois、普遍適用（Universal Acceptance）以及 New gTLD 議題隨時都可以參與。 |

(六)會議討論及決議：

無。

(七)散會：同日下午 5 時 12 分。

(八)「 ICANN72 行前諮詢會議」簽到單

本次會議共 17 名人員參與，詳如下列：

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

### —ICANN 72 會前諮詢會議暨經驗分享會—

## 簽到單

**會議時間**：110年10月18日(星期一)下午3時至5時

**會議地點**：財團法人電信技術中心板橋_大會議室
(新北市板橋區遠東路 1 號 3 樓 B 室)
線上會議

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| NII產業發展協進會 | 吳國維 | |
| NII產業發展協進會 | 梁理旋 | |
| 網路中文資訊股份有限公司 | 魏駿光 | |
| 網路中文資訊股份有限公司 | 賴俞帆 | |
| 財團法人電信技術中心 | 卜慶玲 | |
| 財團法人電信技術中心 | 林永勝 | |
| 財團法人電信技術中心 | 陳志宇 | — |
| 財團法人電信技術中心 | 王彥中 | |
| 財團法人電信技術中心 | 夏慧馨 | |
| 財團法人電信技術中心 | 李昕甯 | |

# 交通部「下世代電信網路號碼技術研析及管理」

## 委託研究計畫

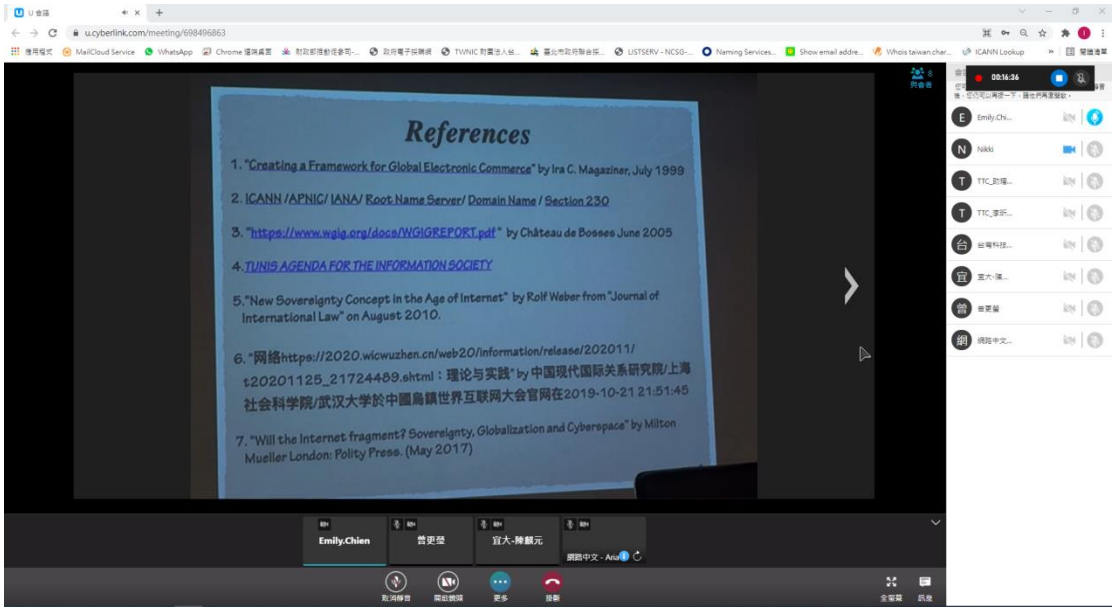
### —下世代電信網路計畫諮詢會議—

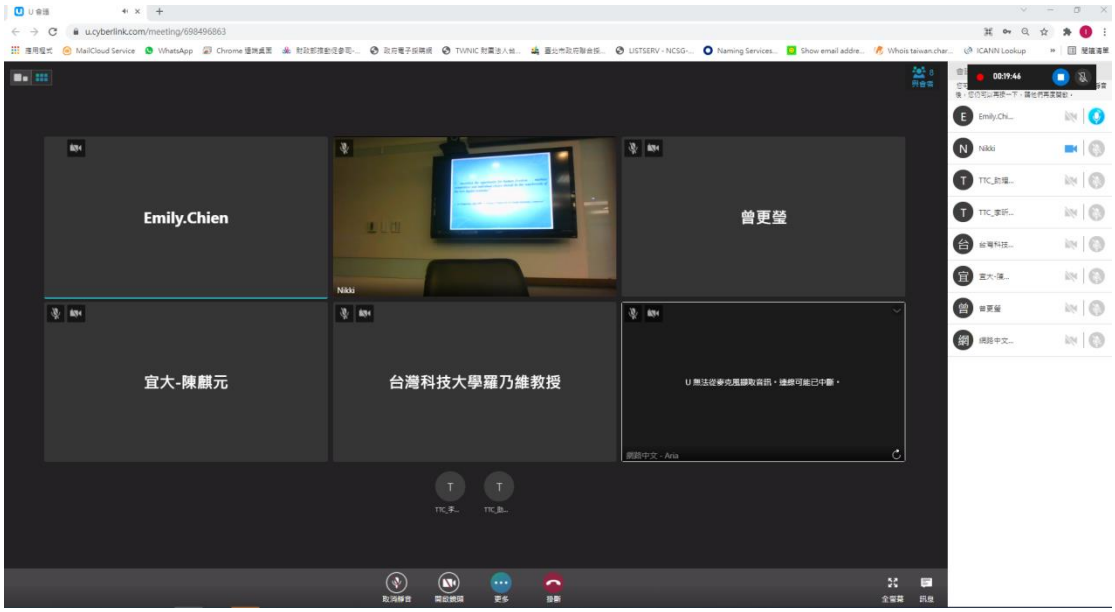
## 簽到單

**會議時間**：110年10月14日(星期四)下午2時至5時

**會議地點**：財團法人電信技術中心板橋_大會議室
(新北市板橋區遠東路1號3樓B室)
線上會議

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 財團法人電信技術中心 | 彭俞蓉 | 彭俞蓉 |
| 財團法人電信技術中心 | 簡嘉儀 | 簡嘉儀 |
| 財團法人電信技術中心 | 陳佳瑀 | 陳佳瑀 |
| 財團法人電信技術中心 | 郭怡萱 | 郭怡萱 |
| | | |
| | | |
| | | |
| | | |
| | | |


References
1. "Creating a Framework for Global Electronic Commerce" by Ira C. Magaziner, July 1999
2. ICANN /APNIC/ IANA/ Root Name Server/ Domain Name / Section 230
3. "https://www.wgig.org/docs/WGIGREPORT.pdf " by Château de Bosses June 2005
4. TUNIS AGENDA FOR THE INFORMATION SOCIETY
5. "New Sovereignty Concept in the Age of Internet" by Rolf Weber from "Journal of International Law" on August 2010.
6. "网络https://2020.wicwuzhen.cn/web20/information/release/202011/t20201125_21724489.shtml：理论与实践" by 中国现代国际关系研究院/上海社会科学院/武汉大学於中國烏鎮世界互联网大会官网在2019-10-21 21:51:45
7. "Will the Internet fragment? Sovereignty, Globalization and Cyberspace" by Milton Mueller London: Polity Press. (May 2017)
Emily.Chien
曾更瑩
宜大-陳麒元


Emily.Chien
曾更瑩
宜大-陳麒元
台灣科技大學羅乃維教授

(九)會議照片

- 邀請 NII 產業發展協進會吳國維顧問經驗分享

## 五、 IETF111 會前諮詢會議會議紀錄

(一)會議時間：2021 年 7 月 13 日（星期二）下午 4 時

(二)線上會議：會議連結 https://u.cyberlink.com/meeting/415944029

(三)出席人員：

| 單位 | 姓名 | 職稱 |
|---|---|---|
| 網路中文資訊股份有限公司 | 魏駿光 | 資深營運經理 |
| | 賴俞帆 | 專案經理 |
| | 潘怡萍 | 助理 |
| 顧問團隊 | 曾更瑩 | 律師 |
| | 羅乃維 | 教授 |
| | 陳麒元 | 副教授 |
| 財團法人電信技術中心 | 林永勝 | 主任 |
| | 卓卿敏 | 資深經理 |
| | 王彥中 | 研究員 |
| | 彭俞蓉 | 助理研究員 |
| | 李昕甯 | 助理研究員 |
| | 夏慧馨 | 助理研究員 |
| | 彭俞蓉 | 助理研究員 |
| | 柯瑩池 | 工程師 |
| | 簡嘉儀 | 副管理師 |
| | 郭怡萱 | 助理管理師 |

(四)會議紀錄：網路中文

(五)會議報告事項摘要

1. IETF 組織與社群運作簡介：

(1) 認識 IETF：

「網際網路工程任務小組」（Internet Engineering Task Force，簡稱「IETF」）是一個網際網路技術制定的組織，成立於 1985 年底，其主要任務是負責網際網路相關技術規範的研發、制定。

(2) IETF 會議之使命：

IETF 參與者為志願人員，透過 IETF 每年召開的三次會議來完成該組織的如下使命：

- 鑑定網際網路之運行與技術問題，並提出解決方案；
- 詳細說明網際網路協定之發展或用途，解決相應問題；
- 向 IESG 提出針對網際網路協定標準及用途之建議；
- 促進向網際網路社群推廣 IRTF 的技術研究成果；
- 為包含網際網路使用者、研究人員、行銷商、承包商及管理者等提供訊息交流的論壇。

(3) IETF 之領域與工作小組：

目前 IETF 共有 7 大研究領域及 121 個處於活動狀態的工作小組，7 大研究領域說明如下：

- 「即時應用領域」(Applications and Real-Time Area，簡稱「art」)，共有 29 個工作小組。
- 「通用領域」(General Area，簡稱「gen」)，共有 2 個工作小組。
- 「網際網路領域」(Internet Area，簡稱「int」)，共有 17 個工作小組。
- 「營運與管理領域」(Operations and Management Area，簡稱「ops」)，共有 15 個工作小組。
- 「路由領域」(Routing Area，簡稱「rtg」)，共有 23 個工作小組。
- 「安全領域」(Security Area，簡稱「sec」)，共有 24 個工作小組。
- 「傳輸領域」(Transport Area，簡稱「tsv」)，共有 11 個工作小組。

2. IETF111 會議議程內容：

(1) IETF 第 111 次會議於本（2021）年 7 月 26 日至 7 月 30 日以「全球遠端參與形式」舉行。

(2) 網路中文依 2021 年 6 月 24 日工作會議指示，依據 TTC 目前研

究與 DNS、DNS&IoT 及網路切片相關之議題，選定及建議可參與 IETF111 會議場次如下，並說明各場次的參與效益分析，詳見下表。

| 台灣<br>日期 | 台灣<br>時間 | 會議名稱 | 會議參與效益分析 |
|---|---|---|---|
| 7/27 | 7:00-9:00 | Domain Name System Operations( 簡 稱 Dnsop) | Dnsop 工作小組的主要工作是為 dns 的軟體開發、服務運作及管理制做相關的工作指引，可透過參與本議程，了解目前技術規畫方向，及了解該小組作業方式。 |
| | 7:00-9:00 | IoT Operations(簡稱 IoTops) | IoTops 工作小組是負責討論物聯網相關設備的運作問題，尤其是設備的起動與生命週期的管理；因為與物聯網相關的 IETF 工作小組很多，本工作小組也希望在討論各種物聯網相關的技術組合時能發揮積極的作用。 |
| 7/28 | 5:00-5:30 | Newcomers' Coffee Break | 藉由新進成員活動，多方面了解 IETF 生態及領域社群。 |
| | 5:30-6:30 | Extensions for Scalable DNS Service Discovery( 簡 稱 dnssd) | dnssd 工作小組主要的任務是為延伸可擴展 DNSSD（DNS service Discovery）開發解決方案，討論以 mDNS（ RFC6762 ）、 DNS-SD（RFC6763）為基礎在多網段的應對方案。 |
| 7/29 | 7:00-8:40 | IETF Plenary | 藉由參與 IETF 全體大會，了解其重要核心成員對整體組 |

| 台灣<br>日期 | 台灣<br>時間 | 會議名稱 | 會議參與效益分析 |
|---|---|---|---|
| | | | 織的領導方向及評估各領域議題的側重方向，以提供專案成員擘劃未來專案主軸。 |
| 7/30 | 3:00-4:00 | DNS PRIVate Exchange( 簡稱 dprive) | DNS 傳輸交換隱私工作小組（Dprive）主要工作是保障 DNS 訊息交換間的機密性及找尋可能性的解決方案並評估工作小組所提供的技術方案應對各種 DNS 監控攻擊的有效性。 |
| | 4:30-5:30 | DNS PRIVate Exchange( 簡稱 dprive) | |
| | 7:00-7:30 | Newcommers'Coffee Break | 藉由新進成員活動，多方面了解 IETF 生態及領域社群。 |
| | 7:30-8:30 | Domain Name System Operations( 簡稱 Dnsop) | Dnsop 工作小組的主要工作是為 dns 的軟體開發、服務運作及管理制做相關的工作指引，可透過參與本議程，了解目前技術規畫方向，及了解該小組作業方式。 |
| 7/31 | 7:00-9:00 | Operations and Management Area Working Group (簡稱 opsawg) | opsawg 工作小組的主要工作是為不在目前工作小組分類內且不適合另建新工作小組的技術提案文件（RFC）提供運作與管理的討論平台。 |

3. The Guide Program：Guide Program 為 IETF 指導員計畫，透過 IETF 資深參與者帶領新進者（參與實體會議五次以下）方式，以協助新人縮短成為活躍成員(active member)的時間。該計畫主要具體目標如下：

- 使參與者更了解 IETF 及技術標準開發過程的相關知識
- 使參與者遭遇問題時，不會求助無門
- 面對個別參與者的需求時，都可以提供最即時的協助
- 給予具主動學習意願之參與者，正向的回饋
- 培育 IETF 新一代的活躍成員

(六)會議討論及決議：

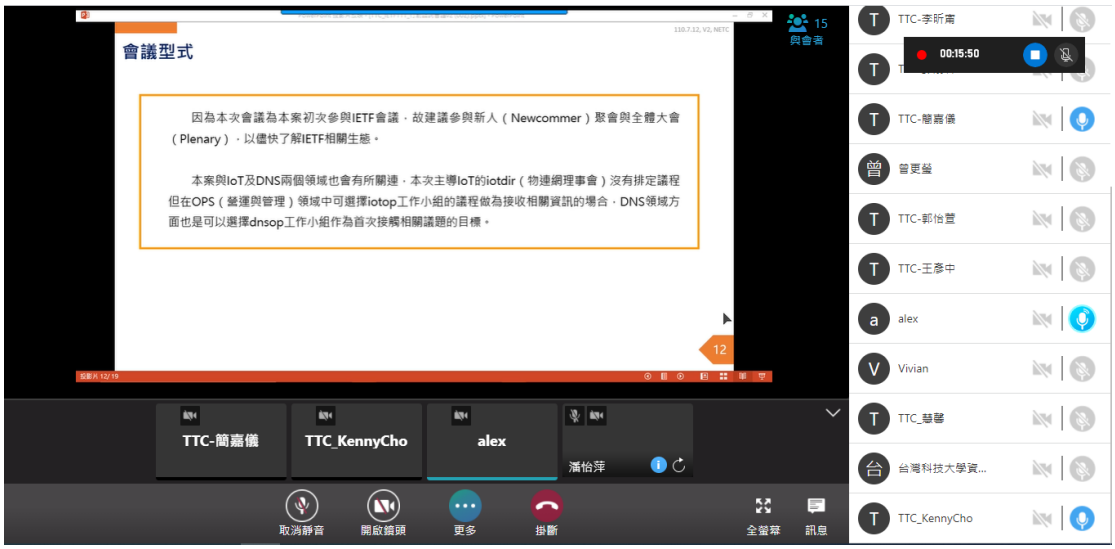
**1.** 請 TTC 參考網路中文提供的 IETF111 參與建議場次表，及安排會議參與人員。

**2.** 有鑑於交通部期中研究報告審查會議時委員指出，因參與線上會議無法互動，建議 TTC 可透過相關單位熟識社群人員等方式執行互動及交流，因此網路中文詢問 IETF 後有關 Guide Program 計畫目的、方式及申請流程後(詳見附件)，建議 TTC 可與顧問共同參與 IETF Guide Program，並與交通部溝通執行方式，網路中文將可協助辦理申請事宜。

(七)散會：同日下午 5 時 39 分。

(八)「IETF111 會前諮詢會議」簽到單

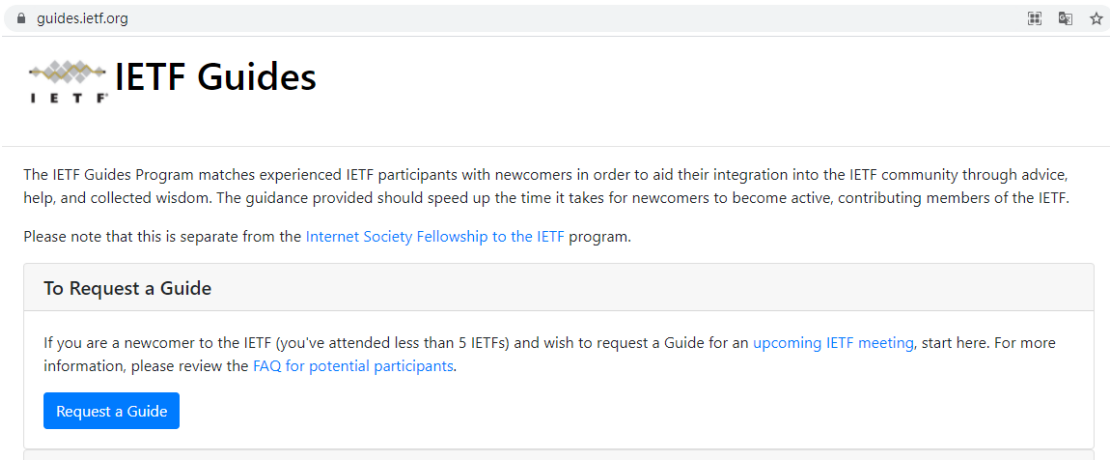
本次會議共 15 名人員參與，詳如下列：，



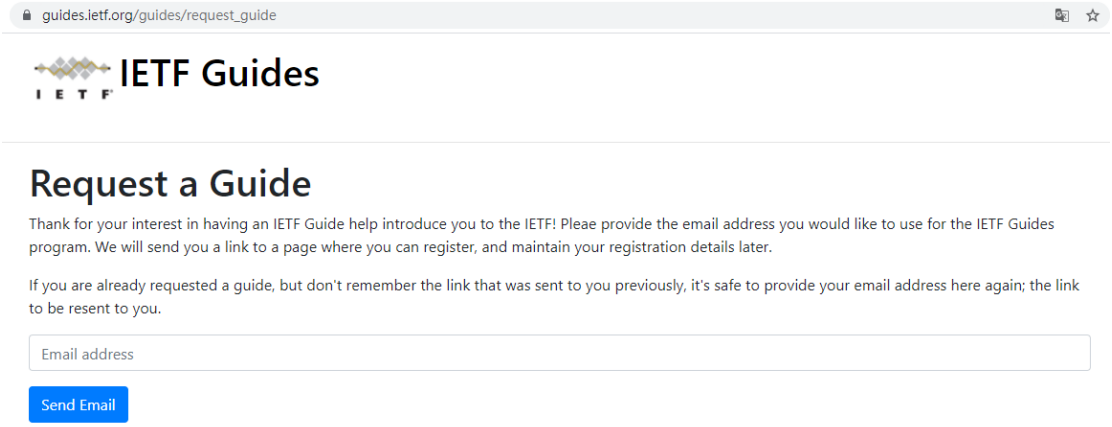
(九)附錄：The Guide Program 申請步驟及表格翻譯

1. 申請步驟（申請網址：https://guides.ietf.org/）

(1) 步驟 1：點選「To Request a Guide」。




(2) 步驟 2：輸入「電子郵件地址」後，點選「Send Email」，並至電子郵箱收信，點選信件內（表格）連結。




(3) 步驟 3：填寫表格。填寫完畢後，按「Save」鍵。若想要修改表格內容，可以隨時透過步驟 2 郵箱信件內的表格連結，進行編輯。

(4) IETF Guide Program 會根據申請人所填寫表格之訊息（如：領域、語言），配對適合的指導員。

2. 貳、表格翻譯

- Will you be attending the next IETF? 是否會參加下一次的 IETF 會議？
- Will you be attending remotely? 是否以遠端形式參與 IETF 會議？
- Given name 名字
- Surname 姓氏
- Affiliation 工作單位

- Country of residence 居住國家
- Preferred conversational language 首選對話語言

  選項：
  - English 英文
  - Cantonese 粵語
  - Mandarin 中文
- Number of IETFs attended 參與 IETF 會議次數？

  選項：
  - This is my first IETF meeting 這是我第一次參與 IETF 會議
  - This is my second IETF meeting 這是我第二次參與 IETF 會議
  - This is my third IETF meeting 這是我第三次參與 IETF 會議
  - This is my fourth IETF meeting 這是我第四次參與 IETF 會議
- What technical topics brought you to the IETF? 哪些技術主題吸引您參與 IETF？

  回答可參考諮詢會議簡報
- What IETF area(s) most interest you? 您對哪些 IETF 領域有興趣？

  選項：
  - ART: Applications and Real-Time 即時應用領域
  - INT: Internet 網際網路領域
  - OPS: Operations and Management 營運與管理領域
  - RTG: Routing 路由領域
  - SEC: Security 安全領域
  - TSV: Transport 傳輸領域
  - UNKNOWN: I don't know yet 不知道
- Which working groups are you most interested in? 您對哪一個工作小組最有興趣？（工作小組參考網頁：https://www.ietf.org/how/wgs）

  回答可參考諮詢會議簡報
- Guide gender preference 指導員性別偏好

  選項：
  - I don’t have a preference. 沒有偏好。
  - I would prefer to work with a male guide.我傾向與男性指導員一同工作。
  - I would prefer to work with a female guide. 我傾向與女性指導員一同工作。
- Is there anything else you would like to share with us? 是否有其他事情想要與我們分享？

## 六、 IETF112 行前諮詢會議會議紀錄

**(一)會議時間：110 年 11 月 01 日（星期一）下午 3 時**

**(二)實體暨線上會議：**

- 地點：財團法人電信技術中心板橋大會議室（新北市板橋區遠東路 1 號 3 樓 B 室）
- 線上：會議連結 https://u.cyberlink.com/meeting/519498745

**(三)出席人員：**

| 單位 | 姓名 | 職稱 |
|---|---|---|
| 網路中文資訊股份有限公司 | 魏駿光 | 資深營運經理 |
| | 賴俞帆 | 專案經理 |
| | 潘怡萍 | 助理 |
| 顧問團隊 | 曾更瑩 | 律師 |
| | 羅乃維 | 教授 |
| | 陳麒元 | 副教授 |
| 財團法人電信技術中心 | 林永勝 | 主任 |
| | 卓卿敏 | 資深經理 |
| | 彭俞蓉 | 助理研究員 |
| | 彭俞蓉 | 助理研究員 |
| | 陳佳瑀 | 副管理師 |
| | 簡嘉儀 | 副管理師 |
| | 郭怡萱 | 助理管理師 |

**(四)會議紀錄：網路中文**

**(五)會議報告事項摘要**

## 1. 2021 年追蹤之 IETF WG 草稿：

| | 領域 (Area) | 工作小組(WG) | 草稿 |
|---|---|---|---|
| 1 | OPS | Operations and Management Area Working Group（opsawg） | Operational Considerations for use of DNS in IoT devices |
| 2 | INT | DNS PRIVate Exchange（dprive） | Specification of DNS over Dedicated QUIC Connections |
| 3 | | IP Wireless Access in Vehicular Environments（ipwave） | DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks |
| 4 | | Distributed Mobility Management（dmm） | Transport Network aware Mobility for 5G |
| 5 | | Extensions for Scalable DNS Service Discovery（dnssd） | Service Registration Protocol for DNS-Based Service Discovery |

## 2. IETF112 會議簡介：

(1) IETF 第 112 次會議於 2021 年 11 月 08 日至 11 月 12 日以「全球遠端參與形式」舉行。

(2) 下列為網路中文建議本專案參與之會議列表：

| 台灣日期 | 台灣時間 | 領域 (Area) | 工作小組 (WG) | 會議名稱 |
|---|---|---|---|---|
| 3-Nov | 21:30-23:00 | | | IETF Plenary |
| 8-Nov | 22:30-23:30 | int | 6lo | IPv6 over Networks of Resource-constrained Nodes |
| 9-Nov | 20:00-22:00 | ops | opsawg | Operations and Management Area Working Group Combined OpsAWG / OpsAREA |
| 10-Nov | 00:00-02:00 | irtf | irtfopen | IRTF Open Meeting |
| 10- | 20:00- | rtg | detnet | Deterministic Networking |

| 台灣日期 | 台灣時間 | 領域 (Area) | 工作小組 (WG) | 會議名稱 |
|---|---|---|---|---|
| Nov | 22:00 | | | |
| 11-Nov | 20:00-22:00 | int | dprive | DNS PRIVate Exchange |
| 12-Nov | 00:00-02:00 | ops | dnsop | Domain Name System Operations |
| | 22:30-23:30 | | | |
| 13-Nov | 00:00-01:00 | ops | iotops | IOT Operations |

**3. Q&A：**

| 問題 | 回答 |
|---|---|
| IETF112 是否係 IETF111 延續？ | 是，草稿議題係連續性，各工作小組持續討論草稿。 |
| IETF 對於電信相關議題並不熱烈？ | 是，該組織較重視網際網路，針對電信方面，著墨較少。 |

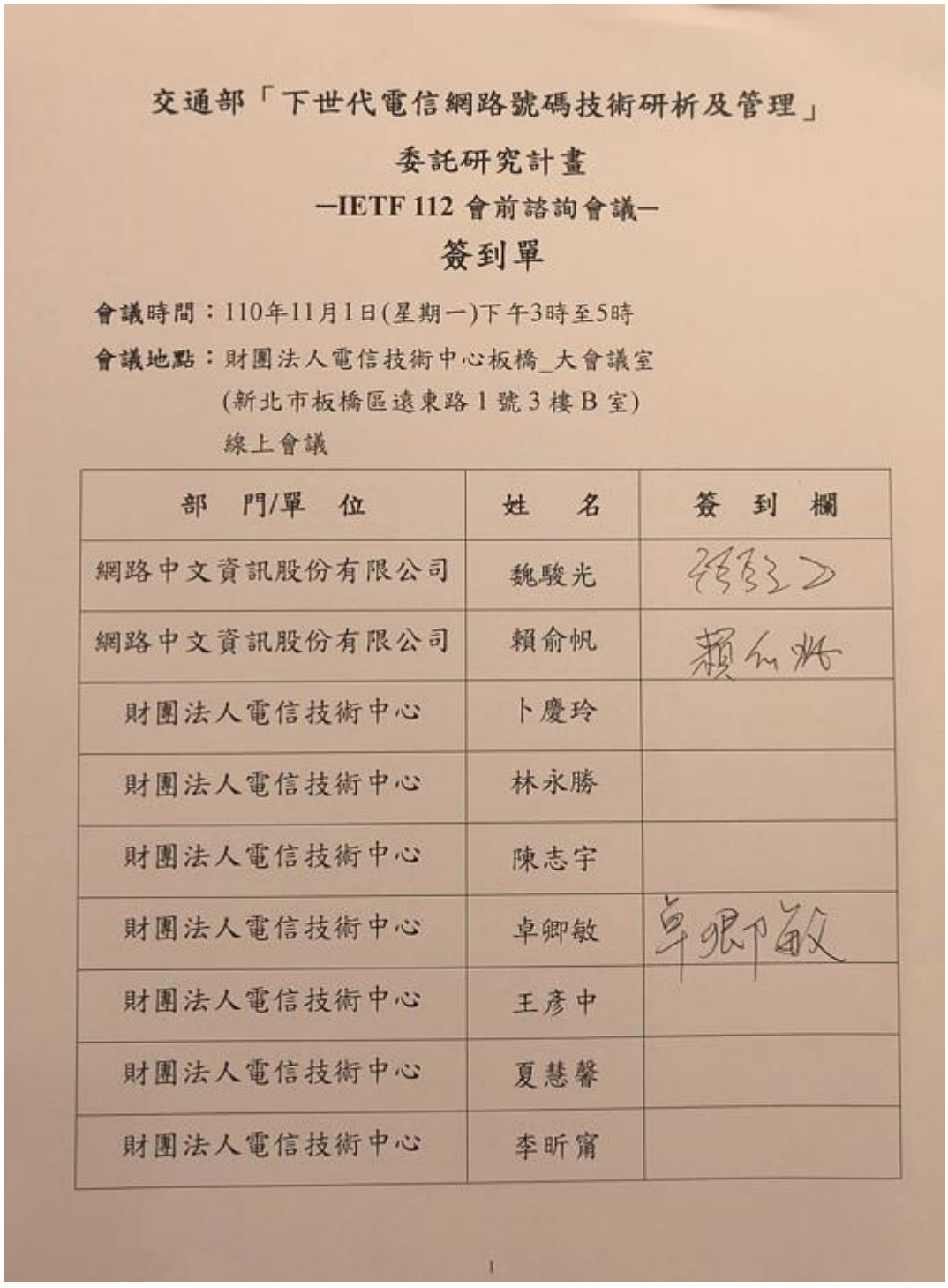
**(六)會議討論及決議：**

1. 羅乃維教授建議專案後續可考慮將電信下編碼成為其中一種特殊假設，並對此假設提出解決方案；另可著墨各個可介接 DNS 情境的假設，研究目前是否已有普遍之情境，若無，則可深入研究並提出相關建議。
2. 建議參與之議程新增陳麒元教授所提之 IP Wireless Access in Vehicular Environments（ipwave）及 DANE Authentication for Network Clients Everywhere（dance）工作小組之會議（詳參附件三建議參與之議程）。

**(七)散會：同日下午 3 時 55 分。**

## (八)「 IETF112 行前諮詢會議」簽到單

本次會議共 12 名人員參與，詳如下列：



交通部「下世代電信網路號碼技術研析及管理」

委託研究計畫

—IETF 112 會前諮詢會議—

簽到單

會議時間：110年11月1日(星期一)下午3時至5時

會議地點：財團法人電信技術中心板橋_大會議室
(新北市板橋區遠東路 1 號 3 樓 B 室)
線上會議

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 網路中文資訊股份有限公司 | 魏駿光 | |
| 網路中文資訊股份有限公司 | 賴俞帆 | |
| 財團法人電信技術中心 | 卜慶玲 | |
| 財團法人電信技術中心 | 林永勝 | |
| 財團法人電信技術中心 | 陳志宇 | |
| 財團法人電信技術中心 | 卓卿敏 | |
| 財團法人電信技術中心 | 王彥中 | |
| 財團法人電信技術中心 | 夏慧馨 | |
| 財團法人電信技術中心 | 李昕甯 | |

1

交通部「下世代電信網路號碼技術研析及管理」

委託研究計畫

—IETF 112 會前諮詢會議—

## 簽到單

**會議時間**：110年11月1日(星期一)下午3時至5時

**會議地點**：財團法人電信技術中心板橋_大會議室
(新北市板橋區遠東路1號3樓B室)
線上會議

| 部　門/單　位 | 姓　名 | 簽　到　欄 |
|---|---|---|
| 財團法人電信技術中心 | 彭俞蓉 | 彭俞蓉 |
| 財團法人電信技術中心 | 簡嘉儀 | 簡嘉儀 |
| 財團法人電信技術中心 | 陳佳瑀 | 陳佳瑀 |
| 財團法人電信技術中心 | 郭怡萱 | 郭怡萱 |
| 網路協會 | 潘明萍 | 潘明萍 |
| | | |
| | | |
| | | |
| | | |

會議參與者 (7)
您可以將另一名與會者的麥克風設為靜音。在設為靜音後，您仍可以再按一下，請他們再度開啟。
Bill
Nikki
TTC_卓卿...
TTC_彭俞...
台灣科技...
宜大-陳...
網路中文...

與會者名單
Nikki
TTC_卓卿敏
TTC_彭俞蓉
台灣科技大學資訊管...
宜大-陳麒元
網路中文_Aria
要求所有人取消靜音

TTC_卓卿敏
TTC_彭俞蓉
台灣科技大學資訊管理系羅乃維
網路中文_Aria

(九)附錄：「**IETF112 建議參與之議程**」

| 台灣日期 | 會議開始 | 會議結束 | 領域(Area) | 工作小組(WG) | IETF 會議 |
|---|---|---|---|---|---|
| 3-Nov | 21:30 | 23:00 | | | IETF Plenary |
| 8-Nov | 22:30 | 23:30 | int | 6lo | IPv6 over Networks of Resource-constrained Nodes |
| 9-Nov | 20:00 | 22:00 | ops | opsawg | Operations and Management Area Working Group Combined OpsAWG / OpsAREA |
| 10-Nov | 00:00 | 02:00 | irtf | irtfopen | IRTF Open Meeting |
| 10-Nov | 20:00 | 22:00 | rtg | detnet | Deterministic Networking |
| 11-Nov | 20:00 | 22:00 | int | dprive | DNS PRIVate Exchange |
| 12-Nov | 00:00 | 02:00 | ops | dnsop | Domain Name System Operations |
| 12-Nov | 20:00 | 22:00 | sec | dance | DANE Authentication for Network Clients Everywhere |
| 12-Nov | 22:30 | 23:30 | ops | dnsop | Domain Name System Operations |
| 13-Nov | 00:00 | 01:00 | ops | iotops | IOT Operations |

備註：IETF112 並未舉行 IP Wireless Access in Vehicular Environments

（ipwave）

# 壹拾貳、國際組織交流清單

## 一、 ICANN IROS 交流

本年度與 ICANN 交流重點可分為兩個部分，一個係 ICANN IROS；另一個係 ICANN ccNSO Tech Day。本年度與 ICANN IROS 交流過程中發現，ICANN IROS 對於本案設定之命題不如預期熱烈，且後期所發送之信件杳無音信，因此專案團隊拓展交流範圍，轉與 ccNSO Tech Day 進行交流，以爭取我國國際能見度。

據此，安排參與 ICANN72 Tech Day 會議展示本案初步研究成果，除該場會議上發表本年度團隊研究成果外，並與社群進行互動，為團隊奠定合作交流管道基礎，以俾下一年度之交流目標進行。

## 二、 IETF Working Group(WG)討論議題蒐集及資料

本年度 IETF WG 交流重點為資料蒐集及議題追蹤，協助掌握國際標準發展趨勢，以利專案團隊研究及方向發展；專案團隊追蹤之 5 份草稿，大多沒有明顯更動之處，惟《Specificatio n of DNS o ver Dedicated QUIC Connections》為「會話恢復」（Session Resumption）新增相關敘述與傳輸隱私風險考量及建議。此外透過參與 IETF111 及 IETF112 會議，進一步了解 IETF 社群運作方式、草稿撰寫流程及各工作小組工作內容及目標，同時，藉由參與會議新人活動，接觸社群，建立熟悉度，以俾下一年度發展目標。

# 三、 ICANN IROS 年度交流

## (一)ICANN IROS 年度交流概覽

### 1. IROS

#### 1.1 5 月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/3/29 | 電子郵件／OCTO | 詢問 OCTO，ICANN 目前對於 DNS、5G、識別碼的相關規劃與進展。 |
| 2021/3/29 | 電子郵件／OCTO | 系統自統回復，說明信件已收到。 |
| 2021/4/22 | Skype 電話／ICANN 全球客服－新加坡 | 詢問我方 2021 年 3 月 29 日發送之電子郵件至今尚無下文。 |
| 2021/4/23 | 電子郵件／ICANN 全球客服－新加坡 | ICANN 說明會聯繫 OCTO。 |
| 2021/4/23 | 電子郵件／ICANN 全球客服－新加坡 | ICANN 通知我方，我方問題已轉知 OCTO。 |
| 2021/5/6 | Skype 電話／ICANN 全球客服－美國加州總部 | 說明 OCTO 正在研擬回復文件。 |
| 2021/5/18 | 電子郵件／OCTO | 我方詢問進度。 |
| 2021/5/18 | 電子郵件／OCTO | Matt Larson 轉請 Alain Durand 回覆。 |
| 2021/5/19 | 電子郵件／OCTO | Alain Durand 詢問 Matt Larson 回覆方式。 |
| 2021/5/19 | 電子郵件／OCTO | 我方請 Alain Durand 書面回覆。 |
| 2021/5/28 | 電子郵件／OCTO | Alain Durand 回復我方問題，同時提供相關 OCTO 報告鏈結。 |

## 1.2 6 月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/6/1 | 電子郵件／OCTO | 詢問 OCTO，DNS 及網路識別碼 Internet Identifiers 是否會是《5G 科技》《OCTO-004》其中一個主題。 |
| 2021/6/4 | 電子郵件／OCTO | Alain Durand 回復我方問題。 |
| 2021/6/10 | 電子郵件／OCTO | 詢問 OCTO，ICANN 針對新類型的 5G 識別碼、網路切片、及網路／DNS 碎片化相關規劃及進展，同時詢問討論方式。 |
| 2021/6/10 | 電子郵件／OCTO | Alain Durand 回復我方問題。 |
| 2021/6/30 | 電子郵件／OCTO | 詢問 OCTO，IETF draft 相關規劃及 DNS 與下世代電信在網路切片的特性研究計畫，同時附件《CENTRstats Global TLD Report》。 |

## 1.3 7 月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/7/16 | Skype 電話／ICANN 全球客服－美國加州總部 | ICANN 說明該員為客服部門，不清楚 OCTO 相關事情,請我方自行以電子郵件聯繫 OCTO。 |
| 2021/7/26 | 電子郵件／OCTO | 我方發信詢問,（1）ICANN72，OCTO 會不會開會說明／討論？（2）詢問有無 DNS Performance/Efficiency 相關計畫？ |

## 1.4 8 月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/8/3 | 電子郵件／OCTO | 我方發信詢問，當 5G 切片等技術應用漸趨成熟，未來將處於多重網路環境，也因此產生更 |

| 日期 | 聯繫方式與對象 | 概述 |
| --- | --- | --- |
| | | 多的攻擊目標，攻擊規模與嚴重程度也將同步擴大。現應強化網路布局架構、網路終端與基礎設施防護，以提升整體資安管理效能。因此我國開始研究 5G 切片現況與未來網路趨勢，例如 DNS 參數改寫、暫存資料入侵，現階段有提到的如 DNSSEC 等防護機制；IPv6 部分則是建議導入純 IPv6 的網路環境以及如何在 IPv4IPv6 共存環境下降低資安風險。針對該趨勢 ICANN IROS 是否有相關研究，或是認同我們研究對這趨勢的判斷呢? |

## 2. ccNSO Tech Day

### 2.1 6 月

| 日期 | 聯繫方式與對象 | 概述 |
| --- | --- | --- |
| 2021/6/8 | 電子郵件／ccNSO | 詢問 ccNSO，在 ICANN72 或未來的 Tech Day 上簡報分享的相關資訊。 |
| 2021/6/8 | 電子郵件／ccNSO | ccNSO 回復我方問題。 |

### 2.2 7 月

| 日期 | 聯繫方式與對象 | 概述 |
| --- | --- | --- |
| 2021/7/9 | 電子郵件／ccNSO | 我方詢問，能否提供繳交欲在 ICANN72 分享研究成果提案之截止日期？ |
| 2021/7/9 | 電子郵件／ccNSO | Tech Day 表示沒有固定截止日期，只要在會議前還有時間，同時該發表十分引人注目，則會進行安排。並再次請求我方提供分享主題之相關資料。 |

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/7/15 | 電子郵件／ccNSO | 我方回應，待團隊整理好研究內容後，將盡快交給 Tech Day 進行考量。 |
| 2021/7/15 | 電子郵件／ccNSO | Tech Day 回應，目前希望能知道主題，不是演講內容或發現，單純主題即可。 |

## 2.3 8 月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/8/3 | 電子郵件／ccNSO | 負責人變更。 |
| 2021/8/3 | 電子郵件／ccNSO | 我方發信告知研究主題「以 DNS 為基礎電信網路號碼裝置自動配置」，如需要其他資料請隨時告知。 |
| 2021/8/3 | 電子郵件／ccNSO | Tech Day 詢問，是否可以為議程提供一簡短標題？ |
| 2021/8/5 | 電子郵件／ccNSO | 我方發信詢問，Tech Day 對於短標題的長度偏好為何？ |
| 2021/8/13 | 電子郵件／ccNSO | 我方回應短標題，並附上研究簡介。 |
| 2021/8/13 | 電子郵件／ccNSO | Tech Day 回應，短標題過長。 |
| 2021/8/16 | 電子郵件／ccNSO | 我方詢問 ICANN72 Tech Day 簡報繳交時間？ |
| 2021/8/16 | 電子郵件／ccNSO | Tech Day 回應，最慢在 Tech Day 前一個禮拜天晚上前提交簡報。 |
| 2021/8/16 | 電子郵件／ccNSO | 我方詢問何時可以收到能於 ICANN72 上演講的通知？ |
| 2021/8/16 | 電子郵件／ccNSO | Tech Day 回應已錄取。 |

## 2.4 9 月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/09/07 | 電子郵件／ccNSO | 我方會盡快提交簡報。 |

## 2.5 10 月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/10/11 | 電子郵件／ccNSO | Tech Day 詢問進度及短標題。基於時區，將是第一個報告。 |
| 2021/10/12 | 電子郵件／ccNSO | 我方回應正在製作簡報，預計本周六提交，短標題為「DNS 編碼技術概念性驗證」。 |
| 2021/10/12 | 電子郵件／ccNSO | Tech Day 詢問 POC 意思、報告順序以及提醒簡報寄送時間。 |
| 2021/10/12 | 電子郵件／ccNSO | Tech Day 寄送第一版會議議程，詢問報告順序，提醒簡報提交時間及檔案格式。 |
| 2021/10/13 | 電子郵件／ccNSO | 我方回覆 POC 意思、報告順序以及講者訊息。 |
| 2021/10/19 | 電子郵件／ccNSO | Tech Day 寄送第二版會議議程，提醒簡報提交時間及檔案格式。 |
| 2021/10/19 | 電子郵件／ccNSO | Tech Day 通知修改議程。 |
| 2021/10/19 | 電子郵件／ccNSO | 我方回覆修改講者名字及由我方控制簡報。 |
| 2021/10/19 | 電子郵件／ccNSO | Tech Day 回應會修改講者名字，並詢問是否需要提前測試裝置。 |
| 2021/10/19 | 電子郵件／ccNSO | 我方詢問測試時間。 |
| 2021/10/19 | 電子郵件／ccNSO | Tech Day 回應控場人員會直接與我方聯繫。 |
| 2021/10/21 | 電子郵件／ccNSO | Tech Day 詢問負責人終版議程進度，提醒講者 |

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| | | 簡報提交時間及 Tech Day 報告時間。 |
| 2021/10/21 | 電子郵件／ccNSO | Tech Day 負責人回應今天會寄終版議程。 |
| 2021/10/22 | 電子郵件／ccNSO | Tech Day 寄送終版議程，提醒會議註冊。 |
| 2021/10/22 | 電子郵件／ccNSO | 我方詢問是否需提供資料以便於會議上確認講者身分，及測試設置時間。 |
| 2021/10/22 | 電子郵件／ccNSO | Tech Day 負責人回應無論如何請寄送 PDF 版簡報，我方講者會是專家小組成員。 |
| 2021/10/22 | 電子郵件／ccNSO | Tech Day 控場人員回覆進入 Zoom 時，係以專家小組身分，報告前，以聯席主持人身分，給予適當權限分享螢幕。會議開始前 45 分鐘開啟會議室，可於此時進行測試。 |
| 2021/10/24 | 電子郵件／ccNSO | 我方寄送簡報。 |
| 2021/10/24 | 電子郵件／ccNSO | Tech Day 回覆收到簡報。 |
| 2021/10/25 | 電子郵件／ccNSO | Tech Day 傳送會議連結。 |
| 2021/10/26 | 電子郵件／ccNSO | 我方表達感謝之意，並詢問回應與會者問題之方式。 |

# 3. 移轉政策

## 3.1 7 月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/7/15 | 電子郵件／ICANN | 詢問 ICANN，是否有收到移轉政策 PDP 註冊表單。 |
| 2021/7/15 | 電子郵件／ICANN | ICANN 回覆已收到。 |
| 2021/7/15 | 電子郵件／ICANN | 表達謝意。 |

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/7/15 | 電子郵件／ICANN | ICANN 回覆謝意。 |

## (二)ICANN IROS 年度聯繫信件中英並陳

# 1. IROS

## 1.1 5 月

### (1) 2021 年 3 月 29 日，致 OCTO

To whom it might concern,

**敬啟者，**

I am fortunate to find your "5G Technology" report, dated 23rd January, 2020, and also to have participatedin your meeting on this topic last year.

**我很幸運找到 OCTO 於 2020 年 1 月 23 日的《5G 科技》（5G Technology）報告；去年也曾參加此主題的會議。**

I am currently running an independent research, and would greatly appreciate if OCTO can provide me withICANN's plans and development regarding DNS, Identifiers and 5G, please. I would like to ask thefollowing questions:

**目前我正在進行一項獨立研究，若 OCTO 可以提供 ICANN 針對 DNS、識別碼及 5G 的規劃及發展，我會非常感謝。我想請教幾個問題：**

1. What is the current status of ICANN's research and investigation into DNS and 5G?

   **請問 ICANN 針對 DNS 及 5G 的研究及調查現況如何？**

2. What is the current status on each of the 5 aspects that was stated in the report? Namely: "Latency","Network Slicing", "Will 5G Result in introduction of new identifiers?", "ITU-T", "Opportunities fornon-IP solutions".

   **請問報告中所提及的五個面向的現況如何？即「延遲」（Latency）、「網路切片」（Network Slicing）、「5G 是否會產生新的識別碼導入？」（Will 5G Result in introduction of new identifiers?）、「國際電信聯盟電信標準化部門」（ITU-T）、「非 IP 解決方案的機會」（Opportunity for non-IP solutions）。**

3. What are ICANN's future plans on the above mentioned aspects?

**針對上述所提的面向，請問 ICANN 未來的計劃是什麼？**

Thank you very much for your time.

**感謝您百忙之中閱讀此信件。**

## (2) 2021 年 4 月 23 日

### I. ICANN 說明會聯繫 OCTO

Thank you for contacting ICANN Global Support. It was a joy speaking with you today.

**感謝您聯繫 ICANN 全球支援中心（Global Support），今日與您聊得很愉快。**

As we have discussed, I have communicated with our OCTO team regarding your inquiry.

**如同我們所討論的，我已針對您的提問向 OCTO 團隊溝通了。**

If you have questions, please let me know.

**如果您還有任何問題，請務必讓我知道。**

## II. ICANN 通知我方已轉知 OCTO

Good day to you.

**日安，**

I would like to inform you our OCTO team has already received your inquiry. A member of the team will reply to you assoon as possible.

**我來通知您 OCTO 團隊已收到您的問題，團隊成員會盡快回覆您。**

You may also follow-up with the team directly by emailing to octo@icann.org. They should receive your follow-up request.

**您也可通過寄送郵件至 octo@icann.org 直接與團隊聯繫，團隊會收到您後續的請求。**

I hope this was of assistance to you. I will now close this inquiry.

**希望這對您有幫助，現在我將結束此次詢問。**

If you have questions, please contact us anytime.

**如果您有任何問題，請隨時與我們聯繫。**

### (3) 2021 年 5 月 18 日

## I. 致 OCTO

I would like to ask about the status of ticket#1383995? It has been more than a month since my previous email, and I have not received any response from yet.

**我想要詢問編號#1383995 郵件的狀況，自從上封郵件寄出，已經過了一個多月了，但至今尚未收到任何回覆。**

I look forward to your kind and sincere reponse. I wish you all well and healthy.

**期待收到貴組織友好及真摯的回覆，祝福各位幸福健康。**

## II. OCTO 指派人員回覆

Matt Larson commented on ticket #1383995

**Matt Larson 對編號#1383995 郵件發表評論**

Alain, could you please answer these questions?

**Alain，可否請您回答這些問題？**

### (4) 2021 年 5 月 19 日

#### I. Alain Durand 詢問回覆方式

Sure. Do you want me to reach out to him directly for a conversation oranswer by email?

當然，請問是要直接聯繫對話亦或是以郵件方式回覆？

#### II. 我方請 Alain Durand 書面回覆

Thank you for your attention to my email.

感謝您注意到我的信件。

Is it possible for you to please reply by email?

可否請您以郵件方式回覆？

### (5) 2021 年 5 月 28 日，OCTO 正式回覆

Please find my response to your questions.

請查看我對您的問題之回覆：

1. What is the current status of ICANN's research and investigation into DNS and 5G?

   請問 ICANN 針對 DNS 及 5G 的研究及調查現況如何？

   - OCTO wrote a paper OCTO-004 (https://www.icann.org/en/system/files/files/octo-004-23jan20-en.pdf) on DNS and 5G. We are planning for an update of that paper at some point in the future.

   OCTO 已針對「DNS」及「5G」撰寫一份報告，即《OCTO-004》（**https://www.icann.org/en/system/files/files/octo-004-23jan20-en.pdf**），我們計畫未來會再更新此份報告。

2. What is the current status on each of the 5 aspects that was stated in the report? Namely: "Latency","Network Slicing", "Will 5G Result in introduction of new identifiers?", "ITU-T", "Opportunities fornon-IP solutions".

   請問報告中所提及的五個面向的現況如何？即「延遲」（**Latency**）、「網

**路切片」（Network Slicing）、「5G 是否會產生新的識別碼導入？」（Will 5G Result in introduction of new identifiers?）、「國際電信聯盟電信標準化部門」（ITU-T）、「非 IP 解決方案的機會」（Opportunity for non-IP solutions）。**

- Not much has changed about the topics of latency, Network slicing and new identifiers since we wrote OCTO-004. OCTO wrote a paper on "New IP" in OCTO-017 (https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf) and is finalizing a paper on the ETSI ISG "Non IP".

**自 OCTO 完成《OCTO-004》報告以來，「延遲」、「網路切片」及「新識別碼」議題並未有太多改變。OCTO 已完成一篇有關「新 IP」的報告，即《OCTO-017》(https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf)，而 OCTO 現在正在定稿一份有關「歐洲電信標準協會產業規範小組」（ETSI ISG）「非 IP」的報告。**

3. What are ICANN's future plans on the above mentioned aspects?

**針對上述所提的面向，請問 ICANN 未來的計劃是什麼？**

- As mentioned above, we are finalizing a paper on Non-IP and will update the 5G paper when enough would have change to warrant a new version.

**如同上述所述，我們正在定稿關於「非 IP」的報告，當有足夠的變化且需要新版本的時候，我們將會更新「5G」報告。**

## 1.2 6 月

### (1) 2021 年 6 月 1 日，致 OCTO

Dear Mr Alan Duran,

**親愛的 Mr Alan Duran，**

I have received your reply.

**我已收到您的回覆了。**

I have a follow-up question that I would like to kindly ask, and the question is as follows:

**我有個問題想要詢問您，問題如下：**

Regarding the new updated "5G Technology"(OCTO-004) report, would "DNS and internet identifiers" be one of its theme topics, or what else would be instead, from what

you know and can foresee at this point.

**針對新版本的《5G 科技》（5G Technology）《OCTO-004》報告，從您現在已知及所能預見的情況來看，請問「DNS」及「網路識別碼」（Internet Identifiers）會是 5G 科技其中一個主題嗎？還是其他內容才是呢？**

I look forward to your reply, and I wish you and the OCTO team a wonderful week ahead.

**期待您的回覆，並提前祝福您及 OCTO 團隊有個美好的一週。**

Best regards

**誠摯祝福**

### (2) 2021 年 6 月 4 日，OCTO 正式回覆

I do not expect to publish an update of OCTO-004 this calendar year, so it is too early to say what exactly will come in it.

**我不期望今年能發布最新版本的《OCTO-004》，現在說都為時過早。**

Best regards,

**誠摯的祝福。**

### (3) 2021 年 6 月 10 日

#### I. 致 OCTO

Dear Mr Alan Durand,

**親愛的 Mr Alan Durand，**

I have received your reply.

**我已收到您的回覆了。**

I am wondering if ICANN have or would have any plan to initiate any policy or regulatory research or study on any of the following issues:(1)new-types of 5G identifiers; or (2) network slicing; or (3)fragmentation of Internet/DNS? My colleague and I are willing to see where we can provide input, and if possible maybe we can try to schedule for a call or ZOOM meeting during ICANN71, should you be interested.

**我想知道 ICANN 是否已經針對下述的議題開展政策或監管研究：（1）新類型的 5G 識別碼（New-Types of 5G Identifiers）；（2）網路切片（Network Slicing）；（3）網路／DNS 碎片化（Fragmentation of Internet／DNS）。我與同事想知道哪裡可以提供意見，若是您有興趣，ICANN71 期間我們可以安排電話會議或是 Zoom 會議。**

I look forward to your reply.

**期待您的回覆。**

Best regards,

**誠摯祝福**

## II. OCTO 正式回覆

We don't have any immediate plans around those issues.

**針對這些議題，我們目前沒有任何計畫。**

Best regards,

**誠摯祝福**

## (4) 2021 年 6 月 30 日，致 OCTO

To whom it might concern,

**敬啟者，**

Our team is doing a research on mobile network and DNS, and we would like to ask a few

questions regarding those topics. Questions are as follows:

**我們團隊正在進行關於行動網路及 DNS 的研究，針對該主題，有幾個問題想要請教，問題如下：**

1. In January, 2020, ICANN have published “5G Technology” report, which describes the feasibility of DNS as an IoT identifier. Is there any plan to update these two articles “DOA over DNS” and “DNS Object Exchange”, which published in 2017, in the IETF draft?

   **2020 年 1 月 ICANN 發布了「5G Technology」報告，該報告說明了 DNS 做為物聯網編碼的可行性報告後，請問是否針對這兩篇文章《DOA over**

**DNS》及《DNS Object Exchange》，將在 IETF draft 進行更新的計畫。**

2. From your perspective of DNS as an IoT identifier, shall we consider the feature and characteristic of network slicing in the next generation telecommunication? For instance, when the action of crossing the network happens between public network and private network, it may challenge the allocation method of the existing Internet address and mobile network numbers. Is there any research project related to this issue?

   **就您認為在 DNS 做為物聯網編碼，未來是否應考量下世代電信在網路切片的特性，例如可能公眾網路與專用網路之間可以相互跨網，當公眾網路與專用網路之間可以相互跨網恐將挑戰現有的網際網路定址及行動網路號碼的編碼方式，請問您是否有對此相關的研究計畫。**

We look forward to your kind response.

**期待您的回覆，**

Yours sincerely,

**誠摯祝福**

## 1.3 7 月

### (1) 2021 年 7 月 26 日，致 OCTO

We appreciate your kind responses and information since March this year.
**感謝您自今年三月以來友善的回覆。**

I would like to understand, during ICANN72, would OCTO have your own session to present your reports and findings? My team would like to offer a chance to exchange views and information.
**我想知道 OCTO 團隊於 ICANN72 是否有分享研究報告及發現之會議？我方想與貴團隊交流觀點及資訊。**

To prepare for our possible discussion, we would like to understand OCTO's current and future plans on "DNS Performance/Efficiency."
**為準備討論，我方希望可以知道貴團隊近期及未來針對 DNS 表現及效率（DNS Performance/Efficiency）的計畫。**

Your response will be much appreciated.
**若您回覆，將不勝感激。**

Best regards,
**誠摯祝福，**

## 1.4 8 月

### (1) 2021 年 8 月 3 日，致 OCTO

Mr. Alex Wei has been assigned a new position, I will be responsible for future communications.

**Alex Wei 已經調職，未來的聯繫事項將由我接手。**

With the utilization of 5G technology gradually maturing, the future of 5G technologies will be amidst a multi-network environment, thereby creating more targets for possible attacks, and the scale and severity of the attacks will also increase synchronously. Now is the time to enhance network structure placement, network terminal and infrastructure protection, in order to enhance overall cyber security management performance. For this reason, we have started research on 5G network slicing and future Internet trends, for example DNS parameter rewrite, cache data invade, as mentioned in current stage, e.g.: DNSSEC, and other protection mechanisms; in terms of IPv6, we provide recommendations on "the introduction of pure IPv6 network environment" and "measures to reduce cyber security risk in an environment that IPv4 and IPv6 co-exists". Do you, the ICANN IROS, have any relevant research, or does ICANN IROS agree with our judgment / opinion on future trends in our research?

**當 5G 切片等技術應用漸趨成熟，未來將處於多重網路環境，也因此產生更多的攻擊目標，攻擊規模與嚴重程度也將同步擴大。現應強化網路布局架構、網路終端與基礎設施防護，以提升整體資安管理效能。因此我國開始研究 5G 切片現況與未來網路趨勢，例如 DNS 參數改寫、暫存資料入侵，現階段有提到的如 DNSSEC 等防護機制；IPv6 部分則是建議導入純 IPv6 的網路環境以及如何在 IPv4IPv6 共存環境下降低資安風險。針對該趨勢 ICANN IROS 是否有相關研究，或是認同我們研究對這趨勢的判斷呢?**

Look forward to your kind response, thank you.

**期待您友善的回覆，感謝。**

Kind regards

**祝福。**

# 2. ccNSO Tech Day

## 2.1 6 月

### (1) 2021 年 6 月 8 日

#### I. 致 ccNSO-Tech Day

To whom it may concern,

**敬啟者，**

I am currently running an independent research and looking for public forums or webinars to share my findings.

**最近我正在進行一項獨立研究，並尋找公共論壇或網路研討會分享我的研究發現。**

I happened to learn about the chance of giving a presentation on Tech Day from the Agenda Page, so I am writing to seek for further details if I would be granted to share my findings in ICANN72 or future Tech Days.

**從議程網頁中，我得知一個可以在 TechDay 上簡報分享的機會，故想藉此封郵件詢問，若我能在 ICANN72 或未來的 Tech Day 上分享我的研究發現，是否能給予更多細節。**

I am looking forward to hearing from you soon.

**期待您的回覆。**

## II. ccNSO-Tech Day 正式回覆

please tell us a little more on the content (but not necessarily the findings) of your research.

**請告訴我們更多關於您研究的內容（不一定為發現）。**

If it is in some way related to the DNS (including DNSSEC or IDN), IP Addressing, or the Management of a Registry or Registrar or it is very interesting (the best of course would be both :-)-O) we usually offer 20 minutes (and can give 30 if required).

**如您的研究內容是和 DNS（包含 DNSSEC 或 IDN）、IP 位址或註冊管理機構或受理註冊機構管理相關，抑或是非常有趣的研究（最好可上述兩者兼具），我們會提供 20 分鐘給您進行報告（如有需要，可以提供 30 分鐘）。**

We would then note it for ICANN72 so you don't have to answer the next Call for Presentations.

**隨後我們會予以紀錄在 ICANN72 的議程上，如此您不必再回復下一次徵求講者的資訊。**

## 2.2 7 月

### (1) 2021 年 7 月 9 日

#### I. 致 ccNSO-Tech Day

Could you please tell me when is the deadline for me to submit the proposal of presenting my findings at ICANN72?

**請問 ICANN72 提交研究發現提案的截止日期是？**

Best regards

**誠摯祝福**

#### II. ccNSO-Tech Day 回覆

we don't have a fixed deadline, really. If there are open spaces the day before we will take presentations if they are compelling.

**我們沒有固定的截止日期，真的。如果前一天仍有時間且簡報內容夠吸引人，我們會進行安排。**

Could you tell us a little more, please (as below)? You are in any case on the top of the list :-)-O

**請問能告訴我們更多細節嗎（如下）？無論如何，您都是名單中的首位 :-)-O**

The Program Group reads in copy.

**計劃小組閱讀副本。**

## (2) 2021 年 7 月 15 日

### I. 致 ccNSO-Tech Day

Thank you for your kind response.

**感謝您友善的回應。**

We are still organizing our research content.

**我方仍在組織研究內容。**

As soon as I obtain the content of the research from the researchers in our researching team, I will submit it to you via email.

**待我收到來自研究團隊的資料後，會盡快透過電子郵件提交給您。**

Best regards

**誠摯祝福**

### II. ccNSO-Tech Day 回覆

Not a problem,

**沒問題。**

please keep in touch. I have added a placeholder into the agenda, to avoid forgetting.

**請保持聯繫。我已在議程中註記，避免忘記。**

However I must have an indication what the topic is about. Not the presentation or findings, just the topic.

**但我仍需要知道主題是什麼，並非研究發現的描述，僅是主題。**

## 2.3 8 月

### (1) 2021 年 8 月 3 日

#### I. 致 ccNSO-Tech Day

I would like to let you know that I have been assigned a new task.
**我想讓您知道我收到新的工作任務。**

My replacement will be Ms. Amy Hsu, who will be responsible for future communications on the Tech Day presentation matter.
**之前的工作將由 Amy Hsu 小姐接手，其將負責未來與 Tech Day 簡報相關事務的聯繫。**

I'd like to thank you for your kind and timely responses over these past few months.
**感謝您過去幾個月友善的回應、即時的回覆。**

Best regards
**誠摯的祝福。**

#### II. 致 ccNSO-Tech Day

Ms. Dora Chen has been assigned a new task, so I will be responsible for future Tech Day presentation matters.
**Dora Chen 小姐接到新任務，接下來 Tech Day 簡報相關事項將由我負責。**

We are one of the research teams of Telecom Technology Center in Taiwan, specialized in DNS and network trends related research.
**我們是台灣電信技術中心其中一個研究團隊，研究著重在 DNS 及網路相關趨勢。**

The topic of our recent research is "The DNS in Automatic Allocation of Telecommunication Network Identifier Devices". We hope to present the content and the findings of our research at ICANN72. If you need any further information about our

research, please do not hesitate to contact us.

**近期團隊的研究主題為「以 DNS 為基礎電信網路號碼裝置自動配置」，希望可以於 ICANN72 展現研究內容及發現，若您還需要近一步的資訊，請務必與我聯繫。**

### III. ccNSO-Tech Day 回覆

please correspond with ccNSO-techday@icann.org for record keeping purposes, and can I please have a short title for the agenda?

**請與 ccNSO-techday@icann.org 聯繫以進行紀錄保存，請問是否可以為議程提供一簡短標題？**

greetings, el

**問候**

### (2) 2021 年 8 月 5 日，致 ccNSO-Tech Day

Thank you for your response and reminding.

**感謝您的回應及提醒，**

In terms of short title for the agenda, what is your preferable length of short title?

**請問 Tech Day 對於短標題的長度偏好為何？**

Regards,

**祝福**

### (3) 2021 年 8 月 13 日

### I. 致 ccNSO-Tech Day

Thank you for your email on August 3rd, asking for short title for the agenda.

**感謝您八月三日寄信詢問議程的短標題。**

After discussing with my team, we think "DNS Auto-allocation of Telecom Network Devices" is the suitable short title for Tech Day agenda, as well as entirely presents what

we are going to share with others.

**與團隊討論之後，我們認為適合 Tech Day 議程的短標題為「電信網路裝置之 DNS 自動網路分配」，完整呈現我們想與他人分享的內容。**

In addition, the attachment is the brief of our research that we are going to present at ICANN72. If you need any further information, please do not hesitate to contact us.

**此外，附件為即將在 ICANN72 呈現的研究簡述，若您需要進一步的資訊，請與我們聯繫。**

Regards

**誠摯祝福**

### II. ccNSO-Tech Day 回覆

thanks,

**感謝，**

much too long, I'll figure something out to fit on one line :-)-O (for the agenda slide only)

**但標題仍太長，我會想出一個適合的標題（僅針對議程簡報）**

## (4) 2021 年 8 月 16 日

### I. 致 ccNSO-Tech Day

Yes no problem.

**好的，沒問題。**

In addition, I wonder when we need to provide the slide to ccNSO-TechDay if we are granted to share our research at ICANN72?

**此外，若保證參與 ICANN72 ccNSO Tech Day 分享研究內容，請問何時需要提供簡報？**

Regards

**誠摯祝福**

## II. ccNSO-Tech Day 回覆

you must provide the slides at the latest on the Sunday evening before TechDay (in efficiently compressed PDF without transitions). And, they will be put up on our web page for future reference.

**您最慢在 Tech Day 前一個禮拜天晚上前提交簡報（請將檔案轉成 pdf 檔），之後簡報會上傳至網頁上作為參考資料。**

Greetings

**祝福**

## III. 致 ccNSO-Tech Day

Thank you for your rapid and kind reply!

**感謝您迅速且友善的回應！**

So when can we get the notice of whether we are granted to present at ICANN72?

**請問何時可以收到於 ICANN72 演講的通知呢？**

Regards,

**誠摯祝福**

## IV. ccNSO-Tech Day 回覆

you have been accepted :-)-O

**貴團隊已錄取。**

## 2.4 9 月

### (1) 2021 年 9 月 7 日，致 ccNSO-Tech Day

Thank you for your information!

**感謝您的資訊！**

We will submit our slide to ccNSO-TechDay asap.

**我方會盡快提交簡報予 ccNSO TechDay。**

If you and TechDay need any further information, please do not hesitate to contact us!

**若您與 TechDay 團隊需要進一步的資訊，請隨時與我聯繫。**

Regards

**誠摯祝福，**

## 2.5 10 月

### (1) 2021 年 10 月 11 日，ccNSO-Tech Day 寄信

where are we on this?

**目前進度如何？**

I need a title for the presentation or to be told that I can remove the placeholder. Given the time zones, you would present first.

**我需要報告標題或是告知可以移除議程註記。因為時差問題，您將是第一個報告。**

Please reply at your very earliest convenience

**請您盡速回覆。**

### (2) 2021 年 10 月 12 日

#### I. 我方回覆

We are making slides right now, and we are expected to submit the slides this Saturday. Besides, “POC of DNSidentifier” will be the short title of our presentation. And we would like to ask if there is other information that we need to provide in addition to the PDF version of the slide?

**我們現在正在製作簡報中，預計本周六提交。此外，報告短標題為「DNS 編碼技術概念性驗證」，另想請問您除了簡報 pdf 檔之外，是否需要提交其他資訊？**

Regards,

**誠摯問候，**

#### II. ccNSO Tech Day 回覆

thank you,

**感謝。**

can you please give me a two liner for my introduction? I am not sure what POC stands for.

**針對我的介紹，可否簡述？我不太確定此處「POC」意旨。**

The slides must be received by Kimberly Carlson (who reads in copy) on 2021-10-24 by 17:00 UTC and we do not exercise any editorial control, so they do not have to be sent to us for "approval" beforehand :-)-O

**由 Kimberly Carlson（郵件副本者）需於 2021 年 10 月 24 日下午 5 點（UTC）之前收到簡報，我們並不會修改簡報，故 Kimberly Carlson 他們不會提前寄給我們審閱。**

As before I'll put you on at 16:10 UTC straight after my opening remarks, which is the earliest I can do. I could also put you on as the (currently) last speaker around 19:30 UTC. Please advise which is more convenient for you from the dime zone difference

perspective.
**我將您的報告時間直接安排至下午 4 點 10 分（UTC），我的開場致詞後，這也是我可安排最早的時間；也可將您安排至目前最後一名講者後面，時間大約是晚上 7 點 30 分（UTC），基於時差問題，請您提供您最方便之時間。**

Greetings
**問候，**

## III. ccNSO Tech Day 回覆

All,
**大家好，**

please find enclosed the first draft agenda, not for publication yet. Agendas will be dated (until it is final), so we don't mix them up.
**請閱覽附件第一版會議議程，這不是公告版本。會議議程會持續更新至定版，我們並不會將議程參雜在一起。**

The topic titles can still change slightly, if I messed things up, but should fit on one line for agenda purposes. The actual Presentation Titles can be longer.
**如果議程上的主題標題不足以表達內容，標題可稍微改變，但仍應符合會議議程一行限制，實際簡報上的主題標題可以更長。**

Please confirm availability/convenience of the times, Amy Hsu and Garth Miller have the first choices due to their locations and otherwise I tried to group topics together a little.
**請確認有空／方便的時間，基於地區因素，Amy Hsu 及 Garth Miller 擁有第一選擇權，否則我會嘗試以主題分組。**

As usual we like PDFs without transitions or other effects as they will go onto our web site. As we are using Zoom we can also accept PowerPoint or KeyNote presentations for loading onto the presentation laptop but only if accompanied by the PDF.

**如同以往，我們喜歡 PDF 檔格式，係因為將簡報上傳至網站時，不會有跑版或是其他影響。因我們使用 Zoom，故接受 Power Point 及 KeyNote 檔案格式簡報，之後會下載至簡報專用筆電，但前提是附有 PDF 檔。**

If you want to present from your own laptop, please advise Kim Carlson (who reads in copy) and me accordingly, but will will load the presentation anyway, as a backup.
**若您想要用自己的電腦呈現簡報，請通知我和 Kim Carlson（郵件副本者），但我們仍會儲存簡報作為備份。**

Kim needs the presentations before 17:00 UTC on Sunday (before the TechDay) 2021-10-24. We do not exercise any editorial control so earlier sending in and/or for approval is not required, but we would appreciate if Kim could have everything lined up in time.
**2021 年 10 月 24 日星期天下午 5 點（UTC）（Tech Day 前）之前 Kim Carlson 需要收到簡報，我們並不會針對簡報進行任何編輯工作，故不需要提前寄送及／或給予我們審閱，但若 Kim Carlson 及時將一切準備就緒，我們會很感激。**

If you know of speakers who can not resist their urge :-)-O please email me or the TechDay email address, the third block goes up to 21:00 UTC, so we can add on even on short notice.
**如果您的講者無法抑制自己的衝動想講更多:-)-O，請以電子郵件聯繫我或是 Tech Day 團隊，第三堂 Tech Day 到晚上 9 點（UTC），一經通知立即安排。**

If I have overlooked someone, please advise as well :-)-O
**若我少提到誰，請通知我。:-)-O**

greetings,
**問候，**

### (3) 2021 年 10 月 13 日

#### I. 我方回覆

Thank you for your information.

**感謝您的資訊。**

Q: can you please give me a two liner for my introduction? I am not sure what POC stands for.

**Q：針對我的介紹，可否簡述？我不太確定此處「POC」意旨。**

A: The "POC" stands for "Proof of Concept", which means something that demonstrates the feasibilityof a concept. And the brief introduction of our research attached this email.

**A：「POC」代表「概念性驗證」（Proof of Concept），意旨展示某個概念之可行性，此封郵件附件為研究簡述。**

Q: As before I'll put you on at 16:10 UTC straight after my opening remarks, which is the earliest Ican do. I could also put you on as the (currently) last speaker around 19:30 UTC. Please advise which is more convenient for you from the dime zone difference perspective.

**Q：我將您的報告時間直接安排至下午 4 點 10 分（UTC），我的開場致詞後，這也是我可安排最早的時間；也可將您安排至目前最後一名講者後面，時間大約是晚上 7 點 30 分（UTC），基於時差問題，請您提供您最方便之時間。**

A: For the sequence of presentation, it is our pleasure to be the first speaker in this session.

**A：針對報告順序，我們很榮幸成為第一個講者。**

Q: Please confirm availability/convenience of the times, Amy Hsu and Garth Miller have the first choices due to their locations and otherwise I tried to group topics together a little.

**Q：請確認有空／方便的時間，基於地區因素，Amy Hsu 及 Garth Miller 擁有第一選擇權，否則我會嘗試以主題分組。**

A: Our speaker for Tech Day is Justin Chen from the Department of Computer Science

and Information Engineering of National Ilan University.

**A：我們 Tech Day 講者為國立宜蘭大學資工系陳麒元教授。**

Regards

**祝福，**

### (4) 2021 年 10 月 19 日

## I. ccNSO-Tech Day 寄信

All,

**大家好，**

please find enclosed the second draft agenda which looks very close to final. If we had a latecomer I would put him/her at the end, we have time until 21:00 UTC.

**請閱覽附件第二版草稿議程，此版議程已非常接近終版議程。如果後續有新的講者加入，我們會直接將其放在議程最後，會議係到晚上 9 點才結束（UTC）。**

I like to publish and post it by tomorrow 20:00 UTC, and therefor would like someone to volunteer to do the usual closing.

**我希望議程可以在明晚 8 點前（UTC）公布，因此希望有人志願進行結尾。**

I will be in transit to Europe Wednesday/Thursday. As usual we like PDFs without transitions or other effects as they will go onto our web site. As we are using Zoom we can also accept PowerPoint or KeyNote presentations for loading onto the presentation laptop but only if accompanied by the PDF.

**周三及周四我將會到歐洲，如同往常，我們希望上傳至網站上之檔案係 PDF 檔案，沒有轉場或其他特效。因為我們使用 Zoom 進行會議，故接受 Power Point 或 Key Note 形式簡報，但寄送同時需附上 PDF 版本。Power Point 或 KeyNote 形式簡報會下載至簡報專用電腦。**

If you want to present from your own laptop, please advise Kim Carlson (who reads in copy) and me accordingly, but will will load the presentation anyway, as a backup.

若您想要用自己的電腦呈現簡報，請通知我和 **Kim Carlson**（郵件副本者），但我們仍會儲存簡報作為備份。

Kim needs the presentations before 17:00 UTC on Sunday (before the TechDay) 2021-10-24. We do not exercise any editorial control so earlier sending in and/or for approval is not required, but we would appreciate if Kim could have everything lined up in time.
**2021 年 10 月 24 日星期天下午 5 點（UTC）（Tech Day 前）之前 Kim Carlson 需要收到簡報，我們並不會針對簡報進行任何編輯工作，故不需要提前寄送或給予我們審閱，但若 Kim Carlson 能及時將一切準備就緒，我們會很感激。**

Roy, I need a little more for the (Hyperlocal) topic in the Agenda (must fit on one line, please).
**Roy，我需要更多關於議程中的（超地方）主題（請盡可能一行）。**

greetings,
問候，

## II. ccNSO-Tech Day 回覆

There was a small timing issue when swapping Ed's and Viktor's presentations. It is fixed for the next edition.
**Ed 及 Viktor 報告時間出現小小的問題，下一版本之議程會修改。**

## III. 我方回覆

Thank you for your information.
**感謝您的資訊。**

For the draft agenda, we would like to revise the name of the speaker, please change to "Chen" instead.
**針對草稿議程，我們想要修改講者名字，請更換成 Chen。**

In addition, we want to present from our own laptop.
**此外，我們想要用自己的電腦報告。**

Thank you for your assistance. If you need further information, please let us know
**感謝您的協助，若您需要其他資訊，請通知我們。**

## IV. ccNSO-Tech Day 回覆

will change the name of the presenter of course. Can I have the complete name and since I am unfamiliar with Chinese names also the gender, for my introduction, please?
**我們將會更改講者名字，請問可否提供講者全名及性別，因為我對中文不太熟悉，此將用於介紹中。**

Please note that we insist on an identical PDF to be sent to Kim as requested, because all presentations will be posted on our web site afterwards.
**請注意我們堅持要求寄給 Kim 的 PDF 檔案需一致，因為之後所有簡報都會公布在網站上。**
Do you wish to test the setup with Kim beforehand?
**請問您希望提前和 Kim 測試裝備及設置嗎？**
Greetings
**問候**

## V. 我方回覆

Thank you for your email,
**感謝您的來信。**

The information below is our speaker's background.
**下方資訊為講者背景，**

Name：Justin Chen
**姓名：陳麒元**

Gender: Male
**性別：男性**

Position: Consultant from Telecom Technology Center（TTC）(Taiwan) and Professor from Dept. of Computer Science and Information Engineering of National Ilan University (Taiwan)

**職位：TTC 顧問及宜蘭大學教授**

Besides, thank you for your reminder, we will submit the PDF version of slides by 17:00 UTC October 24, 2021.

**此外，感謝您的提醒，我們會在 2021 年 10 月 24 日下午 5 點（UTC）之前提交 PDF 檔案簡報。**

When will we test the setup with Mrs. Kim Carlson? And what should we need to prepare beforehand?

**請問何時與 Kim Carlson 進行設備測試？請問需提前準備什麼嗎？**

If you need other information, please let us know.

**若您需要其他資訊，請通知我們。**

Best Regards

**誠摯祝福，**

## VI. ccNSO-Tech Day 回覆

thank you.

**謝謝您，**

Kim reads in copy, she will reply directly.

**Kim 讀取副本後，將直接與你們聯繫。**

## (5) 2021 年 10 月 21 日

### I. ccNSO-Tech Day 寄信

Please let me know if this agenda is ready for posting and distribution.
**若議程可以公布，請讓我知道。**

Presenters: Please send your presentations (ppt & pdf) before Sunday - preferably sooner. IF you prefer to display your slides yourself or do a live demo, we will need to know ahead of time to give you the proper permissions in Zoom
**講者：請於星期天前提交您的簡報（PPT 及 PDF），最好可以早點。如果您選擇自行控制簡報，我們需提前知道，以便給予您 Zoom 適當之權限。**

Monday 25 October 2021
**2021 年 10 月 25 日**

Tech Day Part 1, 2 and 3 | 1600-1700, 1730-1900, 1930-2100 UTC | Blocks 1, 2, 3
**Tech Day 第 1、2 及 3 場| 1600-1700, 1730-1900, 1930-2100 UTC | Blocks 1, 2, 3**

Thank you,
**謝謝您**

### II. ccNSO-Tech Day 回覆

thanks,I just arrived in Germany, will send agenda today
**謝謝，我剛抵達德國，今天會寄送議程。**

## (6) 2021 年 10 月 22 日

### I. ccNSO-Tech Day 回覆

Here with the final agenda, which will now be published and added to the ICANN (ccNSO) Calendar.

**附件為終版議程，其將會被公布及新增至 ICANN（ccNSO）日曆。**

Presenters MUST send us (Kim Carlson) a PDF which we shall publish on the website and MAY send us additionally also a PPT(X) if they so desire, from which to present. We needs them by Sunday close of business (UTC).

**講者必須將簡報（PDF）寄給我們（Kim Carlson），我們會將其公布至網站上；可另外寄送 PPT 形式簡報，以進行報告。我們需要在本周日工作時間結束前收到簡報。**

All Presenters will form part of a "panel" in terms of Zoom access levels, and log in to the (normal) Meeting URL to be "promoted" my the Chairs/Co-Chairs

**根據 Zoom 存取權限，所有講者為專家小組，登入（一般）會議連結，提升為主持人或聯席主持人。**

the Meeting URL wil be pusblished the day before (and we shall post it here here onto this list in any case), in any case, but technically Registration is a requirement for participation in ICANN meetings.

**會議連結會在前一天公布（總之，我們會公告在這裡），此外，參與 ICANN 會議需要先註冊。**

All presenters who have not registered for the meeting on the ICANN Meetings website https://events.icann.org/ICANNEventsPortal/icannmeetings/portal

**若有尚未於 ICANN 會議網站註冊之講者，連結如下：https://events.icann.org/ICANNEventsPortal/icannmeetings/portal**

should therefor please do so, and if you do not want to have your participation be visible,

please choose accordingly.

**請務必完成註冊，若您不想要公開參與資訊，請您根據選項選擇。**

Please don't hesitate to ask if there are any questions left.

**若有任何問題，請盡情發問。**

greetings,

**問候**

## II. 我方回覆

We would like to demonstrate the slides by ourselves, and for this part, I would like to ask few questions as below:

**我們想要自己控制簡報，對此，有幾個問題想要請教您，**

1. Do we need to provide the registration email or account of Zoom beforehand to let you check the identity of the speaker at the meeting, and then you could do the promoting?

   **請問我們需要先提供註冊電子郵件或 Zoom 帳號，以便讓您於會議上確認講者身分，進而提升 Zoom 存取權限？**

2. When do we test the set up? Should we need to do some preparation?

   **請問何時測試設置呢？我們是否需要準備什麼？**

Look forward to your reply

**期待您的回覆**

Best Regards,

**誠摯祝福**

### III. ccNSO-Tech Day 回覆

Please send the PDF anyway, and liaise with Kim, but it's a straight screen share, actually, you will be a "panel"member.

**無論如何請寄送 PDF 檔簡報，並與 Kim 聯絡；將是直接分享螢幕，實際上，您將成為「專家小組」成員。**

### IV. ccNSO-Tech Day 回覆

Thank you both. I will still need the presentation for back-up/redundancy and for posting.

**謝謝兩位。我仍需要簡報做為備份及公布。**

When you join, you will be moved in Zoom to the "panelist" side and made a cohost right before your presentationtime. You will then have the proper permissions to share your screen.

**進入 Zoom 時，您係以專家小組身分，報告前，則以聯席主持人身分，並給予適當權限分享螢幕。**

Zoom will be open 45 mins before the session starts if you wish to test.

**若想測試設置，Zoom 會議室將會於會議開始前 45 分鐘開啟。**

Thank you,

**謝謝，**

## (7) 2021 年 10 月 24 日

### I. 致 ccNSO-Tech Day

Thanks for your email, the attachment of this email is the slides (PPT&PDF) for the presentation.

**感謝您的回覆，此封郵件附件為簡報 PDF 檔及 PTT 檔。**

In addition, our speaker will use his private account to log in ICANN and Zoom, I am not sure how you have him as a panel in Zoom,therefore, we would like to provide his

information.

**此外，我方講者將使用私人帳號登入 ICANN 及 Zoom，因不確定您是如何使其於 Zoom 中成為專家小組成員，故提供其資訊予您：**

Name: Chi-Yuan Chen (Justin Chen)

**姓名：陳麒元**

Email:chency@niu.edu.tw

**電子郵件：chency@niu.edu.tw**

(Please send me the notification and Meeting URL; I am responsible for the administrative support for contact with Tech Day and our speaker)

**請將通知及會議連結寄給我，我係負責行政支援（聯繫 Tech Day 及支援講者）。**

And is it the agenda on the website (https://community.icann.org/display/ccnsowkspc/vTech+Day+%7C+25+October+-+Agenda) be revised again? It is because our speaker's name is wrong, it is Chen, not Hsu.

**請問下方網站上之議程會進行修改嗎？（https://community.icann.org/display/ccnsowkspc/vTech+Day+%7C+25+October+-+Agenda），我方講者名字為 Chen，並非 Hsu。**

Best Regards,

**誠摯問候，**

## II. ccNSO-Tech Day 回覆

Amy, thank you, will be fixed. In the published PDF it's correct.

**Amy，感謝您，將會修改網站議程，簡報為 PDF 檔，係對的。**

Justin, Technically you should register on the ICANN web site, and if you so wish you

can keep his registration unpublished. I shall try to remember to keep you in the loop as well as Amy when corresponding (which is our usual practice). Or staff will be on the lookout for you entering the Zoom conference which will be easy if your Zoom handle is Chen or something similarly recognizable. You can also use the Chat mote to correspond with the Panel and let us know you are there. As soon as we find you, you'll be "promoted" to the panel (so you can share the screen).

**Justin，從技術上來說，您應該在 ICANN 網站註冊，並根據您的意願，選擇是否公開註冊資訊。我會盡量記得讓您與 Amy 保持聯繫（這是我們的慣例）。比較簡單的狀況是工作人員會留意您進入 Zoom 會議，如果是 Chen 或其他人控制您的 Zoom，您可以使用聊天室告訴我們您進來了。我們一找到您，就會將您升級為專家小組成員，以便您共享螢幕。**

Kim, please fix as requested and while you are at it, please change Roy Arends' title from "Hyperlocal" to "Hyperlocal Root Zone Service".

**Kim，請依據要求進行修改，同時將 Roy Arends 的報告標題從「Hyperlocal」更改為「Hyperlocal Root Zone Service」。**

Alejandra, I see the three blocks have been added to the ccNSO Google Calendar, don't you usually put in each topic?

**Alejandra，我看到 ccNSO Google Calendar 已新增了三場會議，通常不是將每個主題都放入嗎？**

greetings,

**問候，**

## (8) 2021 年 10 月 25 日

### I. ccNSO-Tech Day 回覆

Tech Day (1 of 3)

**Tech Day (1 of 3)**

When: Monday, October 25, 2021 at 16:00-17:00 UTC

**時間：2021 年 10 月 25 日星期一，晚上 4 點至 5 點（UTC）**

Location: Zoom 2 (ccNSO)

**會議室：Zoom2（ccNSO）**

Tech Day (2 of 3)

**Tech Day (2 of 3)**

When: Monday, October 25, 2021 at 17:30-19:00 UTC

**時間：2021 年 10 月 25 日星期一，晚上 5 點 30 分至 7 點（UTC）**

Location: Zoom 2 (ccNSO)

**會議室：Zoom2（ccNSO）**

Tech Day (3 of 3)

**Tech Day (3 of 3)**

When: Monday, October 25, 2021 at 19:30-21:00 UTC

**時間：2021 年 10 月 25 日星期一，晚上 7 點 30 分至 9 點（UTC）**

Location: Zoom 2 (ccNSO)

**會議室：Zoom2（ccNSO）**

Zoom

Link:

https://icann.zoom.us/j/94925505465?pwd=TUJkamZyQnlMVnAyRXBNTEhIOEhrUT09

**Zoom：**

**Link:**

**https://icann.zoom.us/j/94925505465?pwd=TUJkamZyQnlMVnAyRXBNTEhIOEhrUT09**

Zoom Session ID:949 2550 5465

**Zoom 會議 ID：949 2550 5465**

Zoom Session Passcode:B!ZCCH8KLe

**Zoom 會議密碼：**B!ZCCH8KLe

Zoom International Dial-In Numbers:https://icann.zoom.us/u/acXUO2eMdh

**Zoom 國際撥打號碼：https://icann.zoom.us/u/acXUO2eMdh**

Zoom Phone Passcode:382 013 7837

**Zoom 手機密碼：382 013 7837**

### (9) 2021 年 10 月 26 日

#### I. 我方寄信

Thank you for your kind responses and assistance these days,

**感謝您近期友善之回應及協助。**

This Tech Day offered us a great opportunity to share our research, thank you.

**此次 Tech Day 給予我們機會向大眾分享研究成果，謝謝您。**

In addition, we would like to ask if there is any possible way to reply to questions from the audiences (online and Q&A Pod)?

**此外，請問可以怎麼回應觀眾於會議上詢問之問題呢？**

Best Regards,

**誠摯祝福，**

# 3. 移轉政策

## 3.1 7 月

### (1) 2021 年 7 月 15 日

#### I. 致 ICANN

I added two of my team members to sign up as an observer to GNSO Transfer Policy Review PDP because they are also interested in Transfer Policy, and hope to receive the latest updates.

**我有兩位團隊成員對移轉政策很感興趣，並希望收到最新資訊，所以我新增兩位以觀察員的身份註冊 GNSO 移轉政策審查 PDP。**

I have already submitted the Google sign up form that you gave me on May, 17th.

**我已經提交您於 5 月 17 日給予的 Google 註冊表單。**

Two people I added are:

1. Chien, Chia-I

2. Lai, Yu-Fan

**兩名新增團員為：**

**1. 簡嘉儀**

**2. 賴俞帆**

Please check whether you receive my request and if I need to provide additional information for signing up.

**請確認是否已收到我的表單，以及是否需要提供額外的註冊訊息。**

I'm looking forward to hearing from you soon.

**期待您的回覆。**

Best regards

**誠摯祝福**

## II. ICANN 回覆

I received both of their completed sign up forms, thank you! I have just added them to the mailing list as an observer, and I am sending them the next meeting invite; observers can now join the meetings on a listen-only mode.

**我收到他們填寫的註冊表單了，謝謝！我剛剛已經將他們以觀察員的身分新增至郵件列表中，現在正在向他們寄送下一次會議的邀請；現在觀察員只能「聆聽」會議。**

Thank you ever so much!

**真的非常感謝你！**

Best,

**誠摯祝福**

## III. 致 ICANN

Thank you for your assistance. Have a nice day!

**謝謝您的幫助。祝您有個愉快的一天！**

Best regards

**誠摯祝福**

## IV. ICANN 回覆

It's my pleasure! Enjoy your day also!

**這是我的榮幸！也享受您的一天！**

## 四、 IETF Working Group(WG)討論議題蒐集及資料

### (一)IETF 組織結構及工作小組

IETF 隸屬於「網際網路協會」(Internet Society，簡稱「ISOC」)，組織由上而下分別是 ISOC、「網際網路架構委員會」(Internet Architecture Board，簡稱「IAB」)、IETF，IETF 內部設有「網際網路工程指導小組」(Internet Engineering Steering Group，簡稱「IESG」，領導「工作小組」(Working Group)，標準之制定工作具體由工作小組承擔。

IAB 成員由 IETF 會議參與人員選出，主要是監管各個工作小組的工作狀況。IESG 的主要職責是接收各個工作小組的報告，對工作小組之工作進行審查，並對工作小組提出的各種標準、建議提出指導性的意見，甚至從工作的方向上、品質上與程序上給予一定的指導。

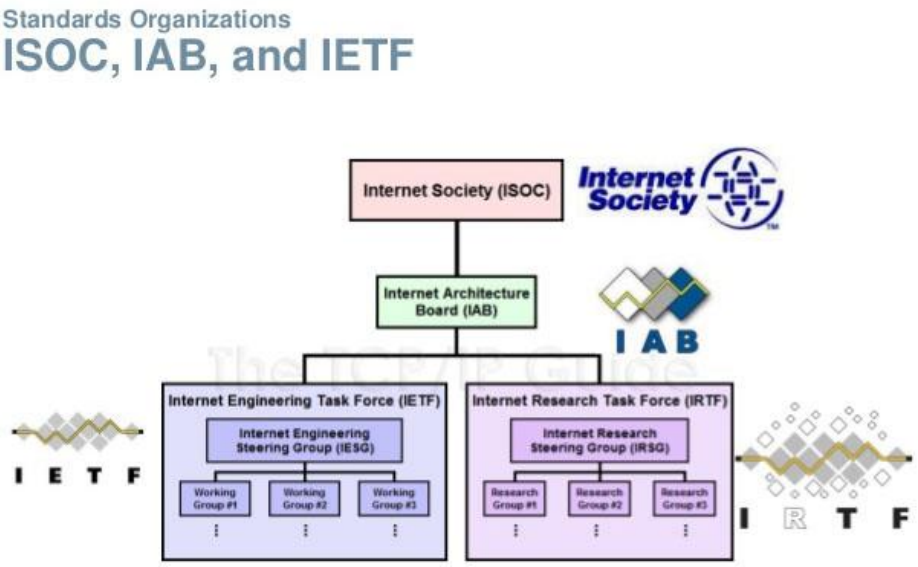



圖 1、ISOC、IAB 與 IETF 之結構

IETF 工作小組根據主題不同劃分為若干個「領域」(Area)。每個領域由一到兩名「指導員」(Director) 負責管理，所有的領域指導員組成 IESG。IETF 工作小組透過「郵件列表」(Mailing List) 進行工作，另輔以 IETF 每年召開三次實體會議。

目前，IETF 共包括七個研究領域，121 個處於活動狀態的工作小組。

1. 「即時應用領域」（Applications and Real-Time Area，簡稱「art」），共有 29 個工作小組。
2. 「通用領域」（General Area，簡稱「gen」），共有 2 個工作小組。
3. 「網際網路領域」（Internet Area，簡稱「int」），共有 17 個工作小組。
4. 「營運與管理領域」（Operations and Management Area，簡稱「ops」），共有 15 個工作小組。
5. 「路由領域」（Routing Area，簡稱「rtg」），共有 23 個工作小組。
6. 「安全領域」（Security Area，簡稱「sec」），共有 24 個工作小組。
7. 「傳輸領域」（Transport Area，簡稱「tsv」），共有 11 個工作小組。

下方為與本案相關草案之彙整列表：

| | 領域 | 工作小組 | 草稿 |
|---|---|---|---|
| 一 | OPS | Operations and Management Area Working Group(opsawg) | Operational Considerations for use of DNS in IoT devices[18] |
| 二 | INT | DNS PRIVate Exchange (dprive) | Specification of DNS over Dedicated QUIC Connections[19] |
| 三 | | IP Wireless Access in Vehicular Environments (ipwave) | DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks[20] |
| 四 | | Distributed Mobility Management (dmm) | Transport Network aware Mobility for 5G[21] |
| 五 | | Extensions for Scalable DNS Service Discovery (dnssd) | Service Registration Protocol for DNS-Based Service Discovery[22] |

[18] IETF，Operational Considerations for use of DNS in IoT devices，https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud-iot-dns-considerations/，最後更新日：2021 年 2 月 21 日。

[19] IETF，Specification of DNS over Dedicated QUIC Connections，https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsoquic/，最後更新日：2021 年 2 月 22 日。

[20] IETF，DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks，https://datatracker.ietf.org/doc/draft-jeong-ipwave-iot-dns-autoconf/，最後更新日：2021 年 2 月 21 日。

[21] IETF，Transport Network aware Mobility for 5G，https://datatracker.ietf.org/doc/draft-ietf-dmm-tn-aware-mobility/，最後更新日：2021 年 3 月 9 日。

[22] IETF，Service Registration Protocol for DNS-Based Service Discovery，https://datatracker.ietf.org/doc/draft-ietf-dnssd-srp/，最後更新日：2021 年 1 月 11 日。

## (二)IETF 與本計畫相關之工作小組草稿年度更新

### 1. Operations and Management Area Working Group(opsawg)

#### 1.1 六月資訊

| | | |
|---|---|---|
| **領域** | | OPS |
| **Active Internet-Draft** | | Operational Considerations for use of DNS in IoT devices |
| **日期** | | 2021/2/21 |
| **狀態** | | I-D Exists |
| **摘要** | **中文** | 該文件詳細說明了物聯網設備如何使用 IP 位址與 DNS 名稱的問題。<br>隨著網路運營商開始佈署《RFC8520 製造商使用說明(MUD)定義》來控制設備存取，這個問題變得刻不容緩。<br>該文件透過一系列可能出錯的案例來解釋問題，並提出設備製造商如何最好地處理這些問題之建議。這些建議會對設備與網際網路協定設計產生影響。 |
| | **英文** | This document details concerns about how Internet of Things devices use IP addresses and DNS names. The issue becomes acute as network operators begin deploying RFC8520 Manufacturer Usage Description (MUD) definitions to control device access.<br>This document explains the problem through a series of examples of what can go wrong, and then provides some advice on how a device manufacturer can best make deal with these issues.The recommendations have an impact upon device and network protocol design. |

| | |
|---|---|
| **作者** | Michael Richardson |
| **服務單位** | Sandelman Software Works |

### 1.2 七月資訊更新

| | |
|---|---|
| **領域** | OPS |
| **Active Internet-Draft** | Operational Considerations for use of DNS in IoT devices |
| **更新日期** | 2021/7/21 |
| **主要更動處** | 1. 新增一名共同編輯人：W. Pan（華為）。<br>2. 在使用 SNI 辨識時，因 TLS 1.3 提供將 SNI 加密為 ESNI，故無法採用，建議用 TLS 1.2 連接。<br>3. 在 CDN 環境（Amazon AWS）時，應改用虛擬託管模式（AWS S3 Virtual Hosting）。 |

### 1.3 八月資訊更新

| | |
|---|---|
| **領域** | OPS |
| **Active Internet-Draft** | Operational Considerations for use of DNS in IoT devices |
| **更新日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 1.4 九月資訊更新

| | |
|---|---|
| **領域** | OPS |
| **Active Internet-** | Operational Considerations for use of DNS in IoT |

| | |
|---|---|
| **Draft** | devices |
| **更新日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 1.5 十月資訊更新

| | |
|---|---|
| **領域** | OPS |
| **Active Internet-Draft** | Operational Considerations for use of DNS in IoT devices |
| **更新日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

## 2. DNS PRIVate Exchange (dprive)

### 2.1 六月資訊

| | | |
|---|---|---|
| **領域** | | INT |
| **Active Internet-Draft** | | Specification of DNS over Dedicated QUIC Connections |
| **日期** | | 2021/2/22 |
| **狀態** | | I-D Exists |
| **摘要** | **中文** | 該文件描述了使用 QUIC 為 DNS 提供傳輸隱私性。<br>QUIC 提供的加密與 TLS 提供的加密具有相似的特性，而 QUIC 傳輸消除了 TCP 固有的 HOL（隊頭阻塞）問題，並提供了比 UDP 更有效的錯誤更正。<br>DNS over QUIC（DoQ）具有類似於《RFC7858》中指定的 DNS over TLS（DoT）的隱私屬性，以及類似於傳統 DNS over UDP 的延遲特性。 |
| | **英文** | This document describes the use of QUIC to provide transport privacy for DNS.<br><br>The encryption provided by QUIC has similar properties to that provided by TLS, while QUIC transport eliminates the head-of-line blocking issues inherent with TCP and provides more efficient error corrections than UDP. DNS over QUIC (DoQ) has privacy properties similar to DNS over TLS (DoT) specified in RFC7858, and latency characteristics similar to classic DNS over UDP. |
| **作者** | | Christian Huitema<br>Allison Mankin<br>Sara Dickinson |

| | |
|---|---|
| **服務單位** | Private Octopus Inc.<br>Salesforce<br>Sinodun IT |

### 2.2 七月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Specification of DNS over Dedicated QUIC Connections |
| **日期** | 2021/7/12 |
| **主要更動處** | 列明 QUIC 傳輸 RFC 為《RFC9000》與《RFC9001》，DoQ 部分是參照[ID.ietf-dnsop-rfc8499bis]。<br>將先前版本中有需要對照到 RFC 文件的部分，在本次修改中補充完全。 |

### 2.3 八月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Specification of DNS over Dedicated QUIC Connections |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

## 2.4 九月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Specification of DNS over Dedicated QUIC Connections |
| **日期** | 2021/09/03 |
| **主要更動處** | 主要更動為：<br>1. 將「QUIC 遺失檢測和擁塞控制」指向至《QUIC Loss Detection and Congestion Control》（RFC 9002）。<br>2. 新增 5.3.1 傳輸取消的相關過程敘述。<br>3. 詳細敘述 5.5「會話恢復」（Session Resumption）內容中，伺服器端必須採取的對應作為。<br>4. 在 6.1「驗證」（Authentication）內容中，區域傳輸規格由 ID.ietf-dprive-xfr-over-tls 改為《DNS Zone Transfer over TLS》（RFC-9103）。<br>5. 新增 6.5.3 會話恢復相關敘述與傳輸隱私風險考量。<br>6. 在 6.8 流量控制機制中，將相關規範指向至《RFC-9002》。<br>7. 在 9.1－9.3 中，說明允許 0-RTT 所帶來的傳輸性能提昇（前一版本建議關閉 0-RTT），以及本草案如何避免會話恢復發生隱私問題（本草案 5.5 及 6.5.3 之相關敘述）。<br>8. 在 10.3 與 10.4 中，將相關詳細的錯誤代碼列出並加以說明。 |

## 2.5 十月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Specification of DNS over Dedicated QUIC Connections |
| **日期** | 2021/10/20 |
| **主要更動處** | 主要更動為：<br>1. 版次更新至第六版，進入工作小組最後調整階段。<br>2. 加強文件中敘述內容。<br>3. 增加 5.3.4 替代用錯誤代碼，除了 5.3.1 至 5.3.3 已指定的特定錯誤代碼外，增列 DOQ_NO_ERROR 與 DOQ_ERROR_RESERVED 來做匡列。<br>4. 增加 9.4「延長會話持續狀態的隱私問題」(Issues With Long Duration Sessions)，延長會話持續狀態可以視為「替代會話恢復」(Session Resumption)的方法，其也具有類似的效果，相關的隱私問題也可由 6.5.4 節中的建議來獲得緩解。<br>5. 新增附錄 B 補充說明與先前版本不同之處，主要是在 5.2 節所提到的「串流映射」(Stream Mapping)與第二版草案《Draft-02》是不相容的；此外，本附錄會於正式版本公布時移除。 |

## 3. IP Wireless Access in Vehicular Environments (ipwave)

### 3.1 六月資訊

| | | |
|---|---|---|
| **領域** | | INT |
| **Active Internet-Draft** | | DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks |
| **日期** | | 2021/2/21 |
| **狀態** | | I-D Exists |
| **摘要** | **中文** | 該文規定了基於 IP 的車載網路中「裝置探索」（Device Discovery）和「服務探索」（Service Discovery）的自動配置方案。透過裝置探索，該文支持對感測器、執行器和車載單元等「物聯網」（IoT）裝置進行全球（或區域）DNS 命名。透過該方案，物聯網裝置的 DNS 名稱可以在有線和無線目標網路（例如車輛、路網、家庭、辦公室、購物中心和智慧電網）中使用裝置的型號資訊自動配置。透過服務探索，網路（或區域網路）中的物聯網使用者（例如司機、乘客、家庭住戶和顧客）可以輕鬆識別目標網路中的每個裝置以進行監測和遙控。 |
| | **英文** | This document specifies an autoconfiguration scheme for device discovery and service discovery in IP-based vehicular networks.<br><br>Through the device discovery, this document supports the global (or local) DNS naming of Internet-of-Things (IoT) devices, such as sensors, actuators, and in-vehicle units. By this scheme, the DNS name of an IoT device can be autoconfigured with the device's model information in wired and wireless target networks (e.g., vehicle, road network, home, office, shopping mall, and smart grid). Through the service discovery, IoT users |

| | | |
|---|---|---|
| | | (e.g., drivers, passengers, home residents, and customers) in the Internet (or local network) can easily identify each device for monitoring and remote-controlling it in a target network. |
| **作者** | | J. Jeong<br>Sejun Lee<br>Park Jung-Soo |
| **服務單位** | | Sungkyunkwan University<br>Ericsson-LG<br>ETRI |

### 3.2 七月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 3.3 八月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 3.4 九月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 3.5 十月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

## 4. Distributed Mobility Management (dmm)

### 4.1 六月資訊

| | | |
|---|---|---|
| **領域** | | INT |
| **Active Internet-Draft** | | Transport Network aware Mobility for 5G |
| **日期** | | 2021/3/9 |
| **狀態** | | I-D Exists<br>WG Document |
| **摘要** | **中文** | 該文件詳細說明了從 5g 行動系統中的切片到 ip、第 2 層和第 1 層傳輸網路中的傳輸切片的框架和對應。<br>5g 系統中的切片的特點是延遲範圍、「預留保證」(Reservation Guarantees)、「抖動性」(Jitter)、資料速率、可用性、行動速度、「使用密度」(Usage Density)、關鍵性和優先度。<br>這些特性應對應到傳輸網路切片的特性，包括頻寬、延遲和標準，例如隔離、方向性和分離的路由。需要將行動切片標準對應到無線側網路功能和用戶平面功能（閘道器）之間的回程、中途和前程連通性分段中提供的適當的傳輸切片和功能。<br>該文件描述了行動網路功能如何將其切片標準對應到 IP 和第 2 層資料包中的識別碼，傳輸網路網段用於在 UE 行動場景中授予傳輸層服務。還討論了此框架和基礎傳輸網路的適用性，它們可以啟用不同的切片屬性。這基於行動和傳輸參考底圖(L2、分段路由、IPv6、MPLS 和 IPv4）之間的對應。 |
| | **英文** | This document specifies a framework and mapping from slices in 5G mobile systems to transport slices in IP, Layer 2 and Layer 1 transport networks. Slices in 5G |

| | | |
|---|---|---|
| | | systems are characterized by latency bounds, reservation guarantees, jitter, data rates, availability, mobility speed, usage density, criticality and priority. These characteristics should be mapped to the transport network slice characteristics that include bandwidth, latency and criteria such as isolation, directionality and disjoint routes. Mobile slice criteria need to be mapped to the appropriate transport slice and capabilities offered in backhaul, midhaul and fronthaul connectivity segments between radio side network functions and user plane function(gateway).<br><br>This document describes how mobile network functions map its slice criteria to identifiers in IP and Layer 2 packets that transport network segments use to grant transport layer services during UE mobility scenarios. Applicability of this framework and underlying transport networks, which can enable different slice properties are also discussed. This is based on mapping between mobile and transport underlays (L2, Segment Routing, IPv6, MPLS and IPv4). |
| 作者 | | Uma Chunduri<br>John Kaippallimalil<br>Sridhar Bhaskaran<br>Jeff Tantsura<br>Praveen Muley |
| 服務單位 | | Futurewei<br>Altiostar<br>Juniper Networks<br>Nokia |

### 4.2 七月資訊更新

| | |
|---|---|
| 領域 | INT |

| | |
|---|---|
| **Active Internet-Draft** | Transport Network aware Mobility for 5G |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 4.3 八月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Transport Network aware Mobility for 5G |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 4.4 九月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Transport Network aware Mobility for 5G |
| **日期** | 2021/03/09 |
| **主要更動處** | 此份草稿「過期」(Expired)。 |

### 4.5 十月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Transport Network aware Mobility for 5G |
| **日期** | 2021/09/22 |
| **主要更動處** | 主要係重新啟動草案工作：版次更新為第一版，草案存活期限延長至 2022 年 3 月 22 日。 |

## 5. Extensions for Scalable DNS Service Discovery (dnssd)

### 5.1 六月資訊

| | | |
|---|---|---|
| **領域** | | INT |
| **Active Internet-Draft** | | Service Registration Protocol for DNS-Based Service Discovery |
| **日期** | | 2021/1/11 |
| **狀態** | | I-D Exists<br>WG Document |
| **摘要** | **中文** | 「基於 DNS 的服務探索的服務註冊協定」（Service Registration Protocol for DNS-Based Service Discovery）使用標準的 DNS 更新機制，以僅使用單點資料封包來啟用基於 DNS 的服務探索。<br>這樣就可以在不使用多點的情況下部署 DNS 服務探索，從而極大地提高了可伸縮性，並在多點服務不是最佳選擇的網路（尤其是 802.11（Wi-Fi）和 802.15.4（IoT）網路）上提高了性能。<br>DNS-SD 服務註冊使用公開金鑰和 SIG(0)來允許服務保護其註冊免受攻擊。 |
| | **英文** | The Service Registration Protocol for DNS-Based Service Discovery uses the standard DNS Update mechanism to enable DNS-Based Service Discovery |

| | | |
|---|---|---|
| | | using only unicast packets. This makes it possible to deploy DNS Service Discovery without multicast, which greatly improves scalability and improves performance on networks where multicast service is not an optimal choice, particularly 802.11 (Wi-Fi) and 802.15.4 (IoT) networks. DNS-SD Service registration uses public keys and SIG(0) to allow services to defend their registrations against attack. |
| **作者** | | Ted Lemon<br>Stuart Cheshire |
| **服務單位** | | Apple Inc. |

### 5.2 七月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Service Registration Protocol for DNS-Based Service Discovery |
| **日期** | 2021/7/21 |
| **主要更動處** | 在 SRP 更新時，需注意《RFC6736》中 7.1 所說明關於 SRP Subtype 的狀況。 |

### 5.3 八月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Service Registration Protocol for DNS-Based Service Discovery |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 5.4 九月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Service Registration Protocol for DNS-Based Service Discovery |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

### 5.5 十月資訊更新

| | |
|---|---|
| **領域** | INT |
| **Active Internet-Draft** | Service Registration Protocol for DNS-Based Service Discovery |
| **日期** | 無 |
| **主要更動處** | 此份草稿無更新。 |

## (三)IETF 年度交流資料

### 1. IETF 年度交流概覽

#### 1.1 六月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/6/30 | 電子郵件／IETF | 詢問 OCTO，IETF draft 相關規劃及 DNS 與下世代電信在網路切片的特性研究計畫。 |

#### 1.2 七月

| 日期 | 聯繫方式與對象 | 概述 |
|---|---|---|
| 2021/7/12 | 電子郵件／IETF | 詢問 IETF,更多指導員計畫相關資訊。 |
| 2021/7/13 | 電子郵件／IETF | IETF 回覆指導員及參與者在一周開始的時候（或前一周）會面，回答新進參與者任何問題，並嘗試讓其在一周內保持高效的正確方向。 |
| 2021/7/14 | 電子郵件／IETF | 詢問 IETF，指導員計畫申請、截止日期及配對工作執行時間長度。 |
| 2021/7/20 | 電子郵件／IETF | IETF 建議 7 月 20 日當周完成申請，配對工作也會於該周執行。 |

## 2. 年度聯繫信件中英並陳

### 2.1 六月

#### (1) 2021 年 6 月 30 日，致 IETF

To whom it might concern,

**敬啟者，**

Our team is doing a research on mobile network and DNS, and we would like to ask a few questions regarding those topics. Questions are as follows:

**我們團隊正在進行關於行動網路及 DNS 的研究，針對該主題，有幾個問題想要請教，問題如下：**

1. In January, 2020, ICANN have published “5G Technology” report, which describes the feasibility of DNS as an IoT identifier. Is there any plan to update these two articles “DOA over DNS” and “DNS Object Exchange”, which published in 2017, in the IETF draft?

   **2020 年 1 月 ICANN 發布了「5G Technology」報告，該報告說明了 DNS 做為物聯網編碼的可行性報告後，請問是否針對這兩篇文章《DOA over DNS》及《DNS Object Exchange》，將在 IETF draft 進行更新的計畫。**

2. From your perspective of DNS as an IoT identifier, shall we consider the feature and characteristic of network slicing in the next generation telecommunication? For instance, when the action of crossing the network happens between public network and private network, it may challenge the allocation method of the existing Internet address and mobile network numbers. Is there any research project related to this issue?

   **就您認為在 DNS 做為物聯網編碼，未來是否應考量下世代電信在網路切片的特性，例如可能公眾網路與專用網路之間可以相互跨網，當公眾網路與專用網路之間可以相互跨網恐將挑戰現有的網際網路定址及行動網路號碼的編碼方式，請問您是否有對此相關的研究計畫。**

We look forward to your kind response.

**期待您的回覆，**

Yours sincerely,

**誠摯祝福**

## 2.2 七月

### (1) 2021 年 7 月 12 日，致 IETF

To whom it may concern,

**敬啟者，**

Our team is doing an independent research on “The DNS in Network Slicing and IoT Communication Mechanism”, and we will be newcomers of IETF111. Recently, we found that there is a IETF Guides Program on the official website. Regarding this program, could you provide more detailed information? For example, what is the guide working? How frequently the guide contacts with newcomers? What do we learn from the guide?

**我們團隊針對「以 DNS 為基礎的網路切片及 IoT 裝置運行通訊機制」正在進行一項獨立的研究，此外，我們也是 IETF111 的新進參與者。最近，我們在 IETF 官方網站上發現 IETF 指導員計畫，針對此計畫，可否請貴團隊提供更詳盡的資訊？例如：指導員的工作內容？指導員聯繫新進參與者的頻率？我們可以向指導員學到什麼？**

We look forward to your kind response.

**期待您的回覆。**

Yours sincerely,

**誠摯的祝福**

### (2) 2021 年 7 月 13 日，IETF 正式回覆

Essentially we try to provide an experienced someone for participants that wish to request a guide. The guide and the participant meets typically at the beginning of the week (or the week before) to advise the newcommer what the IETF is like, what the conference is like, ask answer any questions, and generally try to get the new attendee headed in the right direction to be productive during the week.

**我們嘗試為希望請求指導員的參與者提供經驗豐富的人。指導員及參與者通常在一周開始的時候（或前一周）會面，向新進參與者說明 IETF 是什麼樣的，會議是什麼樣的，回答任何問題，並嘗試讓新進參與者在一周內保持高效的正確方向。**

How many people are you planning on bringing? it might be good to have just one person register and put in the form that a number from your group are coming together, and we can assign one guide to the entire group.

**您打算帶多少人呢？最好讓一個人註冊並填寫表格，使您的小組得以聚集在一起，我們可以為整個小組分配一名指導員。**

### (3) 2021 年 7 月 14 日，致 IETF

Thank you for kind response.

**感謝您友善的回覆。**

For the IETF Guide Program, we have the following questions：

**針對 IETF 指導員計畫，想要請教您以下幾個問題：**

(1) When can we apply for the Guide Program? When is the deadline of the application of the Guide Program?

**何時可以申請指導員計畫？何時為指導員計畫申請截止日？**

(2) How many days will the matching work of the program take?

**計畫的配對工作需要多久呢？**

We are looking forward to your kind response.

**期待您的回覆。**

Sincerely,

**誠摯的祝福**

### (4) 2021 年 7 月 20 日，IETF 正式回覆

"gm.public" <gm.public@net-chinese.com.tw> writes:

**「gm.public」<gm.public@net-chinese.com.tw> 寫到：**

> Thank you for kind response.

**感謝您友善的回覆。**

Sorry for the delay.

**抱歉，耽擱回覆。**

> (1) When can we apply for the Guide Program? When is the deadline of the application of the Guide Program?

**何時可以申請指導員計畫？何時為指導員計畫申請截止日？**

You can apply now (https://guides.ietf.org) and you should do so before the end of this week ideally.

**您可以現在申請（https://guides.ietf.org），最好這周前完成申請。**

> (2) How many days will the matching work of the program take?

**計畫的配對工作需要多久呢？**

We tend to make matches this week. My co-leaders of the guides program and I will try to make some probably Wednesday or so.

**我們傾向這周執行配對工作，我的同事及我預計在週三做些配對工作。**

ISBN：978-986-531-354-8

GPN：1011002098
定價：1200 元