『前瞻及完整之 IPv6 生態系推動方案』

附錄九
『物聯網服務與應用研析及網際網路技術標準研析』

109 年委託研究報告

『物聯網服務與應用研析及網際網路技術標準研析』
期末報告

計畫委託機關：台灣網路資訊中心

中華民國 109 年 12 月

109 年委託研究報告

物聯網服務與應用研析及
網際網路技術標準研析

受委託單位

東海大學資訊管理學系

計畫主持人

林正偉

研究人員

賴囿嘉、陳晏羚、陳示珮、胡詠翔、

吳宜庭、古庭瑋、彭鍾碩、張巧宜、

陳臻、吳光軒、許桓禎、王品力

研究期程：中華民國 109 年 4 月至 109 年 12 月

研究經費：新臺幣 70 萬元

本報告不必然代表台灣網路資訊中心意見

中華民國 109 年 12 月

目　　次

表　　次 …… VI

圖　　次 …… VIII

提　　要 …… XVII

第一章 計畫執行狀況與檢討 1

第一節　計畫執行內容說明 1

一、　背景分析 1

二、　計畫動機與主題 2

三、　工作架構與施行方法 3

四、　預期成果 4

第二節　與計畫符合情形 6

一、　目標達成狀況 6

二、　進度符合情形 7

第三節　資源運用檢討 9

一、　人力運用情形 9

二、　經費運用情形 10

第二章 成果說明 11

第一節　物聯網服務與應用研析 11

一、　物聯網的基礎架構 11

二、　物聯網的應用 14

第二節　主題式網際網路技術標準研析 14

一、　IETF 系列標準 14

第三節　ISP 之 IPv6 網路安全防護準則 15

一、　IPv6 的發展現況與趨勢 15

二、 ISP 服務架構 16

第三章 物聯網的應用 18

第一節 食的物聯網 – 全程冷鏈不斷鏈管理 18

一、 現況與挑戰 18

二、 願景 19

三、 服務架構 21

四、 應用與展示 31

五、 參展紀錄 33

六、 致謝 34

第二節 醫的物聯網 - LincGO 服務架構與技術 36

一、 現況與挑戰 36

二、 願景 39

三、 服務架構 41

四、 應用與展示 51

五、 得獎紀錄 59

第三節 住的物聯網 – 雲端智慧綠能管理系統(iGEMS) 61

一、 現況與挑戰 61

二、 願景 61

三、 服務架構 62

四、 應用與展示 70

五、 得獎記錄 71

第四節 行的物聯網 – 中華電信智慧停車物聯網 75

一、 現況與挑戰 75

二、 願景 75

三、 服務架構 76

四、 應用與展示 84

第五節　育的物聯網 – 工業 4.0 模擬研發實驗室 88

一、　現況與挑戰 88

二、　願景 88

三、　服務架構 89

四、　應用與展示 100

五、　參展紀錄 102

第六節　樂的物聯網 - 智慧導覽與實境遊戲平台 104

一、　現況與挑戰 104

二、　願景 106

三、　服務架構 107

四、　應用與展示 114

五、　參展紀錄 115

第四章 IETF 系列標準 118

第一節　IP (Internet Protocol) 118

一、　IPv6 基本介紹 118

二、　IETF IPv6 標準制定現況 133

第二節　DN (Domain Name).....169

一、　DNS 歷史 169

二、　DNS 結構 170

三、　運作方式 178

四、　訊息格式 188

五、　資源紀錄 193

六、　協議擴展 195

七、　動態更新 196

八、　安全問題 198

九、　隱私問題 200

第三節 BGP (Border Gateway Protocol) 202
一、 前言 202
二、 RFC List 205
三、 相關知識 214
四、 BGP 運行 217
第四節 RPKI (Resource Public Key Infrastructure) 231
一、 前言 231
二、 RFC List 232
三、 資源憑證與子物件 234
四、 管理 242
五、 發布 243
六、 驗證 246
七、 路由決策 249
第五節 DNSSEC (DNS Security Extensions) 251
一、 RFC List 251
二、 簡介 252
三、 歷史 253
四、 DNS 常見攻擊 255
五、 資源紀錄 257
六、 演算法 258
七、 尋找過程 264
八、 信任錨(Trust anchors) 268
九、 信任鏈(Chain of trust) 271
十、 簽名和區域簽名 273
十一、 密鑰管理 274
十二、 部署 277
十三、 工具 286

十四、 IoT 與 DNSSEC 287

第六節 SIP (Session Initiation Protocol) 293

一、 SIP 介紹 293

二、 協定架構 302

三、 通訊流程 308

四、 SIP 的應用 336

五、 相關議題 344

六、 IETF 活躍中的 Working Groups 346

第五章 參與技術活動報告 349

第一節 參加 2020 AWS 臺北高峰會 349

一、 會議簡介 349

二、 心得 358

第二節 2020 台灣創新技術博覽會 362

一、 會議簡介 362

二、 心得 366

第六章 結論與建議 373

第一節 結論說明 373

第二節 建議事項 377

第七章 參考資料來源 378

中英專有名詞對照

表　　次

表 1、各項工作執行進度 6
表 2、各項查核進度表 7
表 3、執行人力表 9
表 4、合計總經費運用情形統計表 10
表 5、傳統與新型智慧動態心電圖監測比較 55
表 6、IPv4 與 IPv6 主要差異 120
表 7、IETF IPv6 相關領域的工作組概況 137
表 8、IETF IPv6 相關重點工作組簡介 138
表 9、DNS 封包格式 189
表 10、HEADER FLAGS FORMAT 189
表 11、QUESTION SECTION 格式 191
表 12、ANSWER SECTION 格式 192
表 13、常見的資源紀錄類型 193
表 14、DNSSEC 資源記錄 257
表 15、DNSKEY 演算法 259
表 16、DS 和 CDS 演算法 263

表 17、各對話控制通訊協定比較 302

表 18、SIP 標頭欄位的簡稱 313

圖　　次

圖 1、ETSI 物聯網架構 12
圖 2、GOOGLE IPV6 調查(全球)..... 16
圖 3、APNIC 調查台灣網路 IPV6 使用情形..... 16
圖 4、ISP 服務架構示意圖 17
圖 5、全球食物損耗統計 18
圖 6、全程冷鏈不斷鏈解決方案 20
圖 7、冷鏈解決方案系統架構..... 21
圖 8、裝置傳輸架構..... 22
圖 9、TREK-120 LORA 溫溼度感測器 23
圖 10、PWS-472 紅外線感測器 24
圖 11、TREK-530 車載電腦 25
圖 12、PWS-472 ANDROID APP 26
圖 13、研華科技 WISE-PAAS 雲服務..... 27
圖 14、通訊傳輸比較..... 28
圖 15、裝置應用在運送車輛的示意圖..... 30
圖 16、裝置應用在賣場的示意圖 31

圖 17、倉儲配送中心 32
圖 18、醫療院所 32
圖 19、零售門市 33
圖 20、2017 台灣智慧冷鏈創新論壇 34
圖 21、2019 台灣教育科技展 34
圖 22、未來三年產品路線 39
圖 23、監測流程中各硬體的作用 42
圖 24、LINCGO 運行架構 42
圖 25、三種雲端開發技術 44
圖 26、建立並監控低功耗藍牙無線網路之方法 46
圖 27、遠端藍牙裝置通訊系統 47
圖 28、遠距藍牙連線系統 48
圖 29、PAAS 雲端即服務分層框架需求 49
圖 30、策略合作商業模式 50
圖 31、24 小時心電圖監測應用場景 51
圖 32、醫院內心電圖檢查應用場景 52
圖 33、遠端醫療與預防醫療應用場景 53
圖 34、雙贏的解決方案 55

圖 35、WIPATCH LINCTRONIX 與他牌比較 56
圖 36、綁定裝置 57
圖 37、下載 APP 並啟用感測器 57
圖 38、顯示資訊並監測 58
圖 39、下載感測器數據 58
圖 40、檢查雲端同步 59
圖 41、下載報告結果 59
圖 42、第十六屆國家新創獎 60
圖 43、雲端智慧綠能管理系統(IGEMS)系統特點 63
圖 44、整體系統架構 64
圖 45、WPM-100 無線數位電錶與電能感測器 65
圖 46、雲端智慧綠能管理系統平台介面 66
圖 47、電能資料收集服務 69
圖 48、電能資料監控服務與電能資料分析服務 70
圖 49、溫溼度感測器 71
圖 50、安裝在機房的智慧電錶 71
圖 51、科技部工程司度電子資通領域應用型產學計畫「產學傑出獎」 72

圖 52、TANET 2015 綠能通訊與綠能機房類最佳論文獎... 72
圖 53、雲端計算與大數據會議 CCBDA 2016 榮獲最佳論文獎 73
圖 54、105 年第二屆台中市低碳城市榮獲傑出貢獻獎 73
圖 55：科技部工程司產學計畫優良成果專刊 148 期與專文報導 74
圖 56、智慧停車場物聯網架構 77
圖 57、地磁感測器 78
圖 58、智慧看板 79
圖 59、智慧停車管理平台 79
圖 60、停車場中裝置間的連接 80
圖 61、物聯網網路應用 82
圖 62、CMP 管理平台應用案例 83
圖 63、智慧停車示意圖 84
圖 64 東山服務區智慧停車看板 85
圖 65 東山服務區智慧尋車系統 85
圖 66、宜蘭縣停車資訊服務 86
圖 67、自動化模擬工廠 90

圖 68、顏色分類與檢測生產線 91
圖 69、真空吸物機械手臂 92
圖 70、自動化高架倉儲系統 93
圖 71、IoT 實驗模組 93
圖 72、3 軸機械手臂 94
圖 73、傳送帶 94
圖 74、TXT 雙核心控制器 96
圖 75、FISCHERTECHNIK-CLOUD 97
圖 76、各裝置間的連接 99
圖 77、元智大學工管系工業 4.0 教學 101
圖 78、健行科技大學實習(驗)室 101
圖 79、模擬生產線 102
圖 80、台灣教育科技展官網 103
圖 81、出國觀光旅遊採用之方式 104
圖 82、自助旅行困擾之處 105
圖 83、團體旅行困擾之處 106
圖 84、蹦世界網站線上導覽 111
圖 85、自動介紹與定位導航 112

圖 86、多國語言與及時通知.....113
圖 87、電子集章與 AR 擴增實境 114
圖 88、蹦世界實境解謎 115
圖 89、AR 拍照活動 116
圖 90、室內地圖導航.....116
圖 91、集章活動換福袋 117
圖 92、IP 的規格演進(引用自維基百科).....119
圖 93、IPv4 與 IPv6 表頭結構..... 121
圖 94、IPv4 與 IPv6 表頭結構 127
圖 95、DHCPv6 的運作過程 132
圖 96、命名空間示例..... 173
圖 97、DNS 查詢的流程 179
圖 98、遞迴查詢過程..... 184
圖 99、迭代查詢過程..... 185
圖 100、VIEW OF EXTERIOR AND INTERIOR ROUTING PROTOCOLS 203
圖 101、IBGP 與 EBGP..... 205
圖 102、BGP 相關 RFC 標準..... 213

圖 103、BGP 訊息格式 218
圖 104、BGP OPEN 訊息 219
圖 105、UPDATE 訊息 220
圖 106、BGP 路由選擇 225
圖 107、iBGP ROUTE REFLECTOR..... 229
圖 108、BGP CONFEDERATION..... 229
圖 109、RFC LIST..... 233
圖 110、RPKI 憑證頒發機構層級..... 235
圖 111、PKI 實體..... 237
圖 112、IPv4 ROA 內容..... 239
圖 113、IPv6 ROA 內容..... 239
圖 114、RPKI VALIDATOR 資料同步架構 247
圖 115、DNSSEC 運作流程 264
圖 116、CHAIN OF TRUST 示意圖 273
圖 117、ZSK 驗證流程 276
圖 118、KSK 驗證流程 276
圖 119、SIP RFC 重要歷程 299
圖 120、MGCP 拓樸 301

圖 121、SIP 的基礎架構 303
圖 122、SIP 相關的協定堆疊 308
圖 123、SIP 註冊流程 314
圖 124、SIP 對話建立及消滅流程 317
圖 125、SIP 重導向的流程 332
圖 126、SIP 的重新邀請流程 334
圖 127、SIP BRIDGING 架構 337
圖 128、SIP BRIDGING 通訊流程 338
圖 129、PSTN ORIGINATION 架構 338
圖 130、PSTN ORIGINATION 通訊流程 339
圖 131、IP ORIGINATION 架構 340
圖 132、IP ORIGINATION 通訊流程 340
圖 133、IMS 架構圖 343
圖 134、VOLTE / VO5G 架構 344
圖 135、物聯網應用情境 359
圖 136、AWS IOT 服務應用 360
圖 137、AWS IOT 的架構 361
圖 138、台灣創新博覽會平面配置圖 363

圖 139、光禾科技模擬球場展示 367

圖 140、智慧球場提供相關功能 367

圖 141、智慧球場提供相關功能 368

圖 142、蹦世界線上導覽展示 369

圖 143、用於智慧電表系統的單相三線式智慧電表 370

圖 144、光學式 PM2.5 感測模組 370

圖 145、微型數位式氣體感測器 371

圖 146、即時羽球訓練輔助裝置與動作分析系統 371

圖 147、5D 智慧城市—SMARTES 平台 372

提　要

關鍵詞：物聯網、網際網路標準、RFC、IP、DN、BGP、RPKI、DNSSEC、SIP、ISP、資訊安全

一、研究緣起

隨著以深度學習為代表的新一代人工智慧(AI, Artificial Intelligence)逐漸成熟，加上雲端運算(Cloud Computing)與大數據(Big Data)處理技術等關鍵基礎建設愈來愈普及，AIoT (AI＋IoT)在智慧製造、智慧醫療、車聯網、行動商務、社群媒體等諸多領域產生許多創新，新應用、服務與商業模式也隨之展開。

同時，隨著越來越多國家/區域開始商轉第五代行動電話(5G)業務，在既有的有線/無線區域網路+廣網網路的基礎建設上，將可為新型態的線上/線下整合服務提供更完善的網路環境，十分有利於物聯網應用的佈署。

因應未來各項通訊傳播網路匯流科技發展之趨勢，本計畫的目的為透過研析(1)物聯網服務與應用研析、(2)網際網路技術標準研析、及(3) ISP 之 IPv6 網路安全防護準則研析等三個方面，期能更了解新一代網路技術與應用的發展方向及市場脈動，期許台灣在國際資通訊科技競爭局勢中繼續領先之優勢。

二、研究方法及過程

本計畫的目的為透過研析物聯網服務與應用及網際網路技術標準等兩方面，以期能更了解新一代網路技術與應用的發展方向及市場脈動。

本計畫架構將包含以下 3 個分項：

分項一：物聯網服務與應用研析

1. 物聯網的基礎架構
2. 物聯網的應用

分項二：主題式網際網路技術標準研析

1. IETF 系列標準

分項三：ISP 之 IPv6 網路安全防護準則

1. IPv6 的發展現況與趨勢
2. ISP 服務架構

三、重要發現

計畫進行中，尚無具體重要發現。

四、主要建議事項

計畫進行中，尚無具體建議事項。

第一章　計畫執行狀況與檢討

第一節　計畫執行內容說明

一、背景分析

台積電董事長張忠謀口中的「next big thing」，聯發科董事長蔡明介倡言「讓台灣科技產業重新洗牌」的關鍵，鴻海集團董事長郭台銘強調的「代工廠一定要搭上的趨勢」，2020 年，物聯網(IoT, Internet of Thing)越來越引人注目。隨著以深度學習為代表的新一代人工智慧(AI, Artificial Intelligence)逐漸成熟，加上雲端運算(Cloud Computing)與大數據(Big Data)處理技術等關鍵基礎建設愈來愈普及，AIoT (AI + IoT)在智慧製造、智慧醫療、車聯網、行動商務、社群媒體等諸多領域產生許多創新，新應用、服務與商業模式也隨之展開。

同時，隨著越來越多國家/區域開始商轉第五代行動電話(5G)業務，具有更高的頻寬、更快的速度、支持超高速移動等特性，能夠提供明確的個性化通訊服務，可以為各種業務的不同訴求，在既有的有線/無線區域網路+廣網網路的基礎建設上，將可為新型態的線上/線下整合服務提供更完善的網路環境，十分有利於物聯網應用的佈署。

另一方面，以 TCP/IP 為基礎的 Internet，正面臨最重要的改變來臨之際。全球 IPv4 位址已經用罄，新的 IPv4 位址難以取得，IPv6 的

推動已經刻不容緩。從 Google 的報告顯示，以 IPv6 位址連線 Google 網站之用戶，目前已超過 30%，這些數據顯示出基於 IPv6 之 Internet 生態系也逐漸通行。

數位經濟為我國目前政策發展之關鍵重點，因應數位創新帶來之超寬頻基礎建設與資通訊科技發展，行政院公布的「數位國家 • 創新經濟發展方案」政策，為有效推動我國數位經濟政策發展，為新型態數位經濟之崛起從國家策略角度預作規劃與整備。其中一個發展重點為推動我國數位基磐建設發展，一方面提昇寬頻基礎建設，同時，研析前瞻創新應用規劃。其中，推動 IPv4/IPv6 雙軌普行使用是當前數位時代基礎建設中之非常重要的一環。基於新一代的 5G 行動通訊所能提供的更優質網路服務，同時，整體國家政策對於新服務、新商業模式的支持更將是新型態數位經濟是否能夠成功的關鍵。

因應未來各項通訊傳播網路匯流科技發展之趨勢，本計畫的目的為透過研析(1)物聯網服務與應用研析、(2)網際網路技術標準研析、及(3) ISP 之 IPv6 網路安全防護準則研析等三個方面，期能更了解新一代網路技術與應用的發展方向及市場脈動，期許台灣在國際資通訊科技競爭局勢中繼續領先之優勢。

二、計畫動機與主題

隨著行動通訊的普及，物聯網、人工智慧的興起，數位轉型的已

經不再是口號。相較於十年前、二十年前，今天人民的生活型態已有很大的不同。網際網路(Internet)加上行動通訊，今日網路基礎建設與其上的應用已讓很多人無法離開網路，從手機通訊、社群媒體、影音娛樂、知識與新聞的取得等等。而自駕車、無人飛機送貨、無人商店、行動商務、數位貨幣等等新應用的出現，更將加進改變人們的日常生活。

本計畫的目的為透過物聯網相關技術與應用的研析，以期能更了解新一代網路技術與應用的發展方向及市場脈動。

本計畫架構將包含以下三個分項：

分項一：物聯網服務與應用研析

分項二：主題式網際網路技術標準研析

分項三：ISP 之 IPv6 網路安全防護準則

三、工作架構與施行方法

三個分項之架構如下：

分項一：物聯網服務與應用研析

1. 物聯網的基礎架構
2. 物聯網的應用

分項二：主題式網際網路技術標準研析

1. IETF 系列標準

分項三：ISP 之 IPv6 網路安全防護準則

1. IPv6 的發展現況與趨勢

2. ISP 服務架構

四、預期成果

本計畫預計透過對物聯網服務應用與網際網路技術標準之研析，充份了解相關技術的發展、標準化的現況、國內外廠商的支持、創新服務應用的機會與風險。同持，對於 IPv6 未來普及，針對 ISP 之 IPv6 網路安全之進行分析，蒐集並整理網路安全防護準則。

分項一：物聯網服務與應用研析

本計畫分項預計就食、醫、住、行、育、樂各分類蒐集國內外物聯網服務實際應用案例，研析國內外相關之學術論文、技術報告、標準發展、產業分析等資料，透過訪談等多種方式，了解國內外物聯網相關產業的發展現況。

分項二：主題式網際網路技術標準研析

這個分項預計透過研讀 Internet 相關的技術標準，包含 IP、DN、

BGP、RPKI、DNSSEC 與 SIP 的 6 個主題的相關 RFC，進行深度分析，了解相關技術標準的發展與應用，並探討該系列標準在 IETF 最新的發展方向。

分項三：ISP 之 IPv6 網路安全防護準則

這個分項預計從資訊安全的角度,研讀相關的標準與案例,就 ISP 所提供的 IPv6 網路連線服務，提出防護準則。包含 ISP 的 IPv6 網路安全基本防護要項與針對固接網路、行動網路與公眾無線網路的安全防護建議。

第二節　與計畫符合情形

一、目標達成狀況

依照計畫內容將工作項目分為 3 大項，各項工作執行進度如下表所示：

表 1、各項工作執行進度

工作項目	四月	五月	六月	七月	八月	九月	十月	十一月	十二月		已完成進度
物聯網服務與應用研析											
食											100%
醫											100%
住											100%
行											100%
育											100%
樂											100%
主題式網際網路技術標準研析											
IP											100%
DN											100%
BGP											100%
RPKI											100%

DNSSEC											100%
SIP											100%
ISP 之 IPv6 網路安全防護準則											
網路安全基本防護要項											80%
安全防護建議-固接網路											0%
安全防護建議-行動網路											0%
安全防護建議-公眾無線網路											0%

二、進度符合情形

各項工作的查核點進度，符合原計畫申請書之規劃，完成預定應完成項目比例，詳細細目及工作進度，如下表所示：

表 2、各項查核進度表

分類	工作項目	執行進度			原因說明
		超前	符合	落後	
物聯網服務與應用研析	食		✓		
	醫		✓		
	住		✓		
	行		✓		
	育		✓		

	樂		✓		
主題式網際網路技術標準研析	IP		✓		
	DN		✓		
	BGP		✓		
	RPKI		✓		
	DNSSEC		✓		
	SIP		✓		
ISP 之 IPv6 網路安全防護準則	網路安全基本防護要項		✓		
	安全防護建議-固接網路		✓		
	安全防護建議-行動網路		✓		
	安全防護建議-公眾無線網路		✓		

第三節　資源運用檢討

一、人力運用情形

到 108 年 10 月為止，本研究計畫共投入總執行人力 15 人，除主持人 1 人外，共同主持人 2 人，專任助理 1 人，碩士班兼任研究助理 3 人，大學部兼任研究助理 8 人，各人力擔任之工作如下表所示：

表 3、執行人力表

類別	姓名	職位	最高學歷	在本計畫中擔任之工作
主持人	林正偉	副教授	博士	計畫管理與執行
共同主持人	蘇暉凱	副教授	博士	計畫執行
共同主持人	余心淳	助理教授	博士	計畫執行
專任研究助理	吳宜庭		學士	物聯網資料蒐集、資料統整、報告撰寫
兼任研究助理	賴囿嘉		碩士研究生	ISP 之 IPv6 網路資料整理
兼任研究助理	陳晏羚		碩士研究生	ISP 之 IPv6 網路資料整理
兼任研究助理	陳示珮		碩士研究生	RFC 資料整理
兼任研究助理	胡詠翔		大學生	RFC 資料整理
兼任研究助理	古庭瑋		大學生	RFC 資料整理
兼任研究助理	彭鍾碩		大學生	RFC 資料整理
兼任研究助理	張巧宜		大學生	RFC 資料整理

兼任研究助理	陳臻		大學生	RFC 資料整理
兼任研究助理	吳光軒		大學生	RFC 資料整理
兼任研究助理	許桓禎		大學生	RFC 資料整理
兼任研究助理	王品力		大學生	RFC 資料整理

二、經費運用情形

到 109 年 10 月為止，各項經費使用如下表所示：

表 4、合計總經費運用情形統計表

項　目	預算金額	使用金額	使用率	備　註
人事費用	480,000	192767	40.16%	因起聘期較晚，計畫主持人費尚未開始支用，預計於計畫結束時使用完畢。
業務費	117,000	93600	80.00%	預計於計畫結束時使用完畢。
差旅費	40,000	32000	80.00%	預計於計畫結束時使用完畢。
行政管理費	63,000	63000	100%	
合　計	700,000	107180	15.31%	

第二章　　成果說明

第一節　　物聯網服務與應用研析

一、物聯網的基礎架構

國際電信聯盟(ITU，International Telecommunication Union)在2005 年發表了對物聯網(IoT，Internet of Things)的第一個報告《ITU網際網路報告 2005：IoT》正式提出物聯網概念，闡述關於 IoT 技術、機會、挑戰和可能的影響。從 2006 年至 2008 年間，IoT 開始獲得歐盟認可，並舉辦了第一屆歐洲物聯網會議。之後，物聯網引起越來越多人的注意。

在物聯網應用裡，能行使獨立功能的裝置，透過網際網路實現相互連結的功能，採用有線或無線網路連結的方式。通過 IoT，中心電腦或雲端平台對機器、裝置、人員進行集中管理、控制，進行自動化操控系統，實現物和物相聯。同時透過收集不同物件的資料，最後可以聚集整合巨量資料，進行加值處理與應用。比如說，重新設計道路以減少車禍、災害預測與犯罪防治、流行病控制等等，對未來的社會將產生許多重大的改變。

一般物聯網的基礎架構可以用三層來說明，如圖 1 所示。

（1） 感知層

感知層是物聯網發展的基礎。將各種具有感測或辨識能力的元件嵌入具有網路連結的各種裝置，能夠對環境進行監控與感知。其中，日常生活中常被用來嵌入物體的感測元件，包括紅外線、溫度、濕度、光度、音量、壓力、三軸加速度等感測器，使裝置具有感測環境變化或物體移動的能力。常見的辨識技術包含無線射頻辨識(RFID，Radio Frequency Identification)、Bar Code、二維條碼、QR-Code、影像辨識技術等等。如將 RFID 的標籤嵌入於物件，便可讓周遭設備得知物件的身分或狀態。

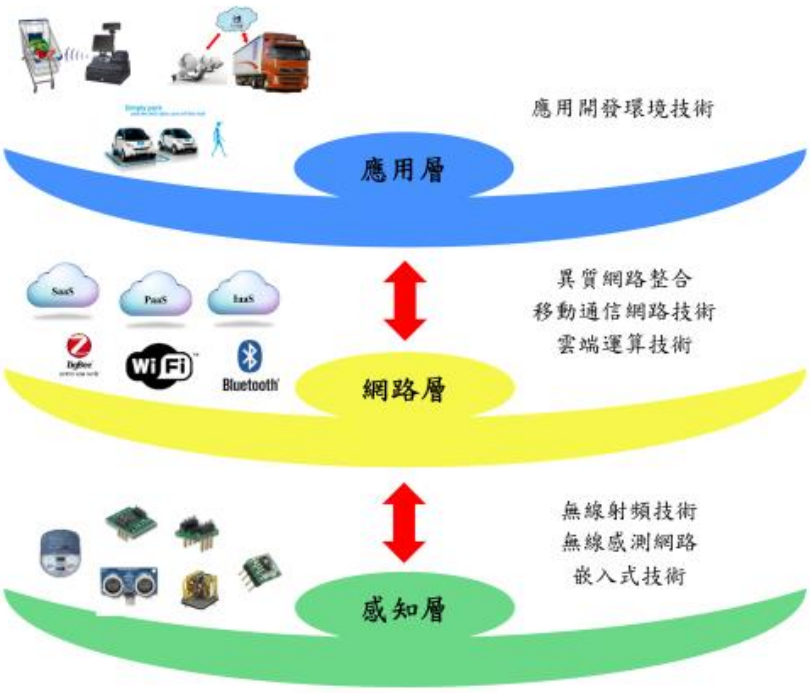


圖 1、ETSI 物聯網架構

（2） 網路層

網路層有如人體結構中的神經，使智慧裝置具有連網能力，能夠將感測到資料傳送至網際網路，除了分享這些即時且重要的資料給適當的使用者外，亦能提供遠端互動。智慧裝置透過無線或有線的方式連結至網際網路，常見的無線通訊技術包括 Zigbee、藍牙、Wi-Fi、LoRaWAN、3G/4G/5G 等。

網路層可看作為感知層與應用層之間的溝通橋樑，用以將智慧裝置所收集到的資料，透過網路傳送至雲端平台，進行儲存及有效地管理與運算。同時，應用層依據感知層蒐集到的資料進行加值運算後所產生的決策，必須透過網路層傳送給指定的智慧裝置或相關服務，使其能進行適當且即時的回饋與反應。

（3） 應用層

應用層是物聯網與各領域產業間進行的專業技術融合，並依照各行業或是用戶的需求對網路層中的感知數據進行分析處理，以提供特定的服務。其應用範圍遍及交通、環境保護、政府工作、公共安全、家居安全、消防、工業監測、老人護理、個人健康、綠能產業等多個領域，改善我們的生活品質。

由於物聯網感測器所收集的資料不僅量大，且通常需要即時分析，

因此，大數據的分析技術將扮演很重要的角色，以進一步的進行資料整合與資料分析。

二、物聯網的應用

物聯網的發展促使了生活模式的創新與轉型，除了為人類的生活帶來全新的體驗外，物聯網的應用也得以有效率的方式解決目前生活上或社會上所帶來的問題，其應用的範圍與種類相當的廣泛，包括智慧運輸、智慧節能、智慧運輸、智慧生活等各種面向。

我們透過蒐集並分析具有代表性的物聯網服務與應用案例，了解國內外物聯網技術的發展。從食、醫、住、行、育、樂等面向蒐集國內外物聯網服務實際應用案例至少各 1 項，共 6 項案例。

此 6 項案例將在第三章中詳細說明。

第二節　**主題式網際網路技術標準研析**

一、IETF 系列標準

透過探討 IETF 不同主題之技術標準，從特定主題的主要概念、技術特徵、標準文件列表、技術演進更迭、實現指引，到 IETF 會議中是否有新的發展等多個面相，完全兼具廣度與深度的技術報告，以供各界深入了解相關特定主題。

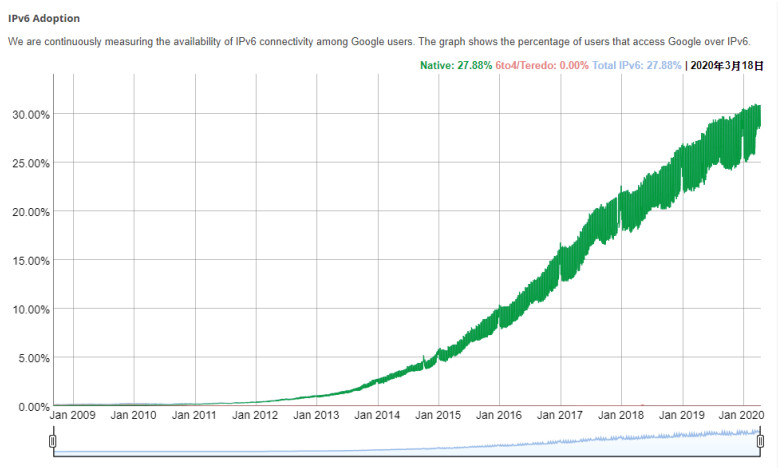
本計畫選定的主題包含：IP、DN、BGP、RPKI、DNSSEC、SIP 等 6 個主題。

此 6 個主題將在第四章中詳細提及。

第三節　ISP 之 IPv6 網路安全防護準則

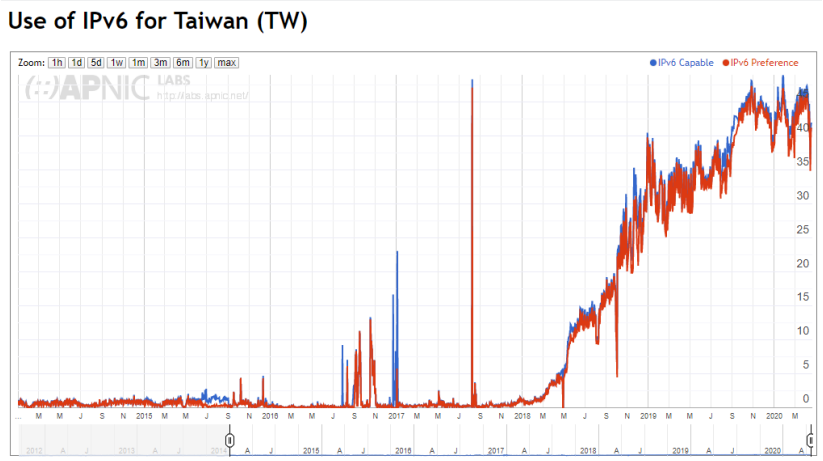
一、IPv6 的發展現況與趨勢

現今的網際網路發展蓬勃，截至 2018 年 1 月，全球上網人數已達 40.21 億，IPv4 僅能提供約 42.9 億個 IP 位置。用 IPv6 來取代 IPv4 主要是為了解決 IPv4 位址枯竭問題，不過它也在其他很多方面對 IPv4 有所改進。然而長期以來 IPv4 在網際網路流量中仍占據主要地位，IPv6 的使用增長緩慢。在 2017 年 7 月，通過 IPv6 使用 Google 服務的用戶百分率首次超過 20%。2020 年 3 月，IPv6 的使用率大約在 30% 左右，如圖 2 所示。隨著行動電話的普及，國內各大行動電話業者逐步啟用 IPv6，IPv6 連網能力快速提升，如圖 3 所示，在 APNIC 的調查中，台灣 IPv6 Capable 的比例已上昇到 45%左右。



資料來源：https://www.google.com/intl/en/ipv6/statistics.html

圖 2、Google IPv6 調查(全球)



資料來源：https://stats.labs.apnic.net/IPv6/TW

圖 3、APNIC 調查台灣網路 IPv6 使用情形

二、ISP 服務架構

一般網際網路服務提供者(ISP; Internet Service Provider)服務架構如圖 4 所示，包含網際網路存取服務(Internet Access Service)、網際網路互連(Internet Internetworking)連結網際網路與網際網路應用服務(Internet Service)三大類，且網際網路應用服務是 ISP 提供用戶使用網際網路相關之應用服務，例如：DNS、Email、Web 等等。因此本計畫將從這三方面，提供 ISP 之 IPv6 網路安全防護準則建議。

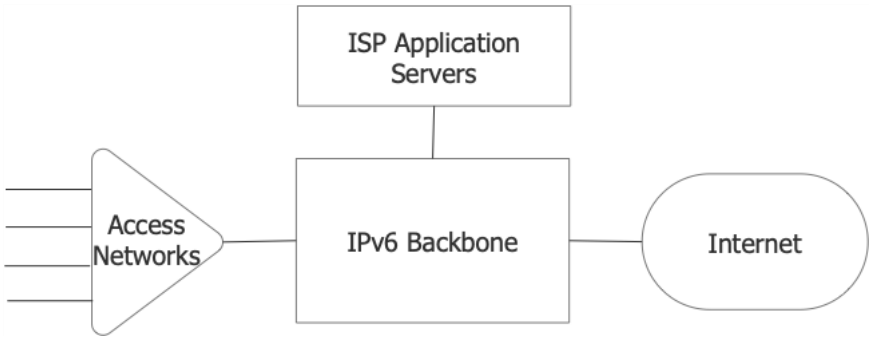


圖 4、ISP 服務架構示意圖

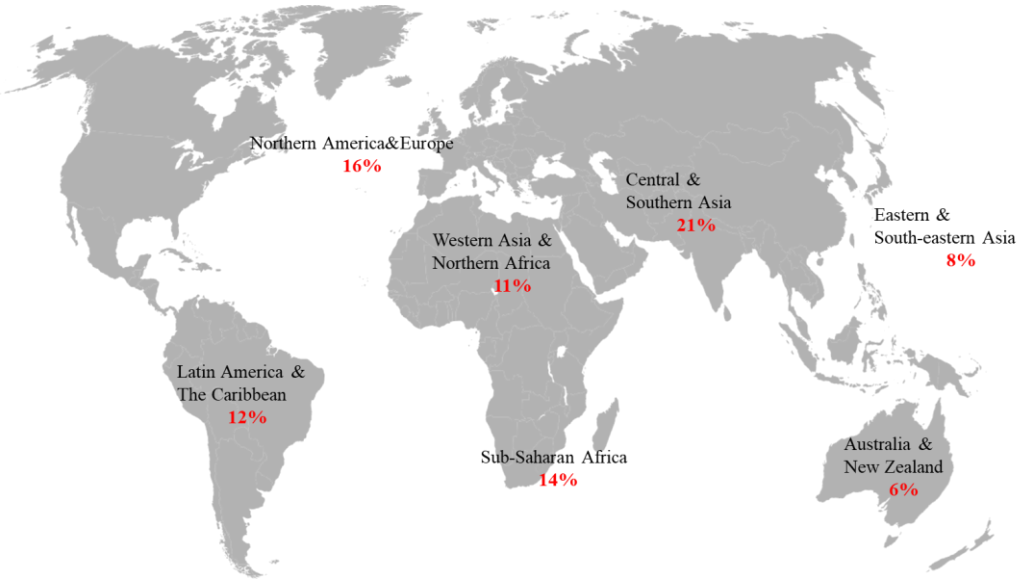
本報告的第二部分會詳述 ISP 資訊安全防護的建議。

第三章　物聯網的應用

第一節　食的物聯網 – 全程冷鏈不斷鏈管理

一、現況與挑戰

2019 年聯合國農糧組織（FAO）公布報告指出，全球每年食物採集後到零售前的全球食物損耗統計占糧食總產量的 14%，尤以中亞、東南亞、北美及歐洲的占比最高(如圖 5)。



資料來源：FAO “The state of food and agriculture,” 2019

圖 5、全球食物損耗統計

近期食品安全問題層出不窮，如從運輸中的溫度失溫、多數加工中心的有線感測器雜亂、加上一些非即時的數據等等，使人們無從得知食品的新鮮度與安全性；農產品、冰品、肉品、生鮮、藥品等在運輸過程中，需在全程低溫環境維持品質；而政府、食品業者與消費者，也日漸重視食品的生產源頭與運輸過程，以及能否以即時溫度控管避

免食品腐敗變質。

而以往的賣場食品安全管理為人工作業，賣場人員隨機抽選一批冷藏冷凍商品，使用感應式溫度計掃描商品溫度後，再手寫在紙上，之後回到辦公室輸入至系統中，用此作業方式有二個缺點，一是人工紀錄難免會有失誤，二為紙本紀錄容易遺失，故妥善保管資料就形成食安管理作業上的困擾。

然而也發生賣場客人從冷藏冷凍櫃拿取商品後就忘了關門或沒有關緊，而賣場工作人員往往又無法立即發現，導致冰櫃溫度上升，間接影響到食品品質，甚至造成商品損耗與電費支出。

二、願景

為上述的問題提出了「農場到餐桌，驅動全程溫度履歷需求提升食品安全」，研華科技提出完整的冷鏈物流解決方案，從生產製造、倉儲、配送到門店零售，其貨物的環境溫濕度將全程監控，確保運送全程冷鏈物流不斷鏈（如圖 6）。

資料來源：研華科技提供

圖 6、全程冷鏈不斷鏈解決方案

(一) 質化或量化目標

採用物聯網技術，以低功耗通訊技術做為無線感測器傳輸資料的基礎，食品從工廠到門市的運輸過程中，透過 GPS 與感測器全程即時監控並紀錄貨品位置、溫度狀態，再以藍牙傳送資訊至車載電腦上，同時也上傳至雲端平台。若食品在運輸過程中，車廂溫度異常時會發送即時警訊，司機從車載電腦搭配的螢幕得知異常，馬上下車察看狀況，同時傳送警訊至中控後台，有效紀錄運輸狀況、改善配送流程、降低損耗並提供零售商完整生產與物流配送履歷資料。

而在門市中則是當感測器感測到冷櫃溫度出現異常時，系統會在第一時間通知管理者，讓工作人員即時前去查看，進而避免不必要的

損耗與浪費。

三、服務架構

研華即時冷鏈物流，使用車載機、無線感測器，及感測器的 Android APP 和後端管理平台，在食品出廠前，業者可以根據食品所需要的環境溫度，事先設定與調整感測器參數；在食品運送途中，可同時監控食品與車輛狀態，將過程傳回後端管理平台；當食品運送到消費者或商店手上，後端管理平台也會紀錄並即時更新資料(如圖 7，圖 8)，進而確認食品運送過程中是否有缺口。

資料來源：https://www.advantech.tw/srp/cold-chain-management-solutions

圖 7、冷鏈解決方案系統架構

資料來源：http://www.twcloud.org.tw/files/file_pool/1/0i2273535745244066 09/6.pdf

圖 8、裝置傳輸架構

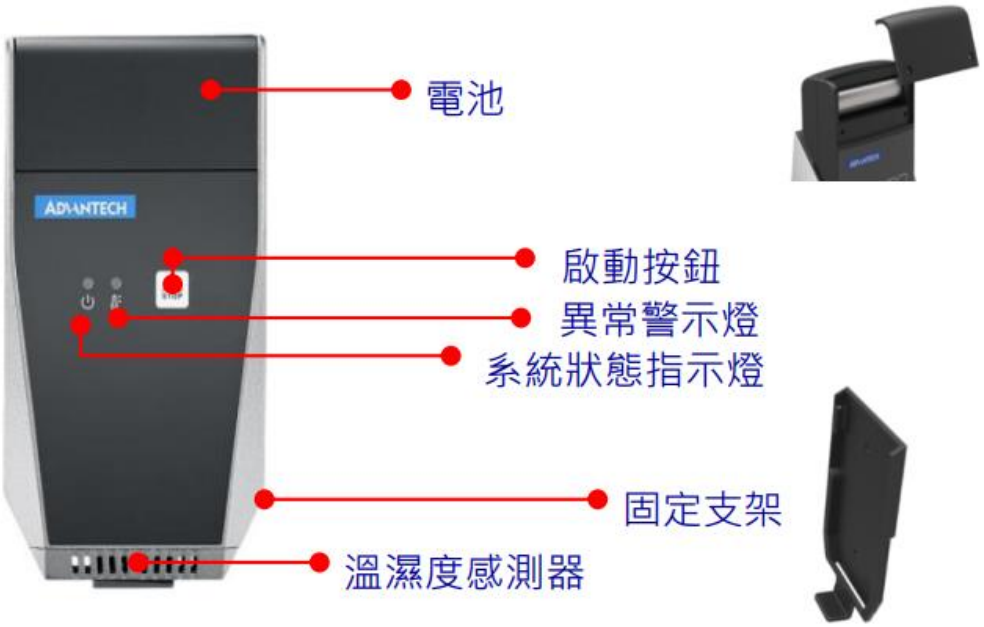
(一) 硬體

1. TREK-120 LoRa 溫溼度感測器

TREK-120 LoRa 溫溼度感測器(如圖 9)搭載 NFC 功能，亦使用 LoRa 技術搭配 gateway 可即時監控，有中央管理服務雲，易控管資料。

為了在各種使用環境中運行，TREK-12 感測器可以與 LoRa 閘道器或 NFC 讀取器配對，NFC 讀取器和 LoRa 閘道器集成在一起，以進行無線數據收集和傳輸。TREK-120 可以感測環境中的溫度、濕度和衝擊力。然後，可以使用 NFC 讀取器（或具有 NFC 功能的任何手持設備）下載收集的數據，或通過 LoRa 閘道器將其無線傳輸到雲中

以進行實時監控。



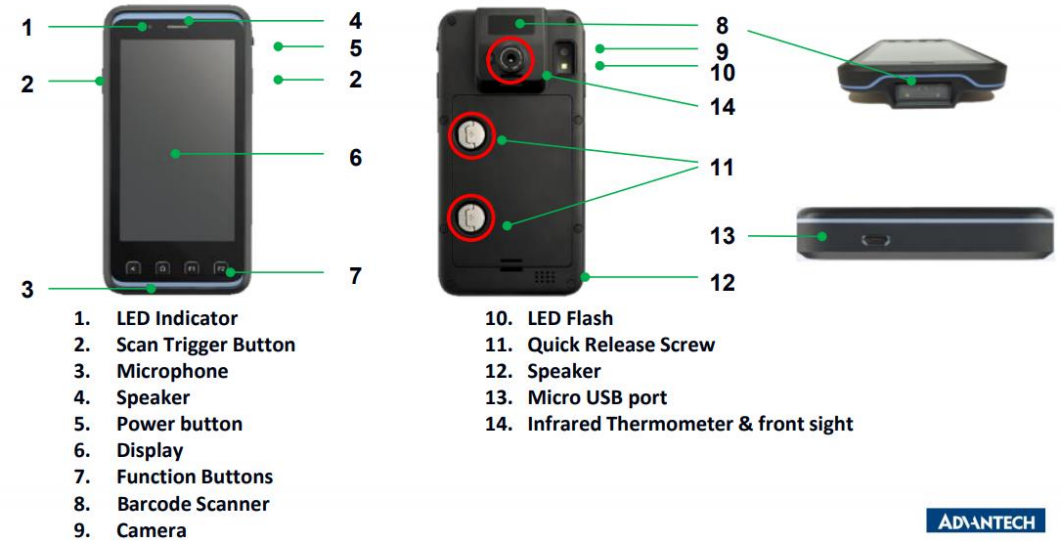
資料來源：https://advdownload.advantech.com/productfile/PIS/TREK-120/file/TREK-120_DS(040820)20200413120129.pdf

圖 9、TREK-120 LoRa 溫溼度感測器

2. PWS-472 紅外線感測器

PWS-472(如圖 10)是基於 Android 系統開發的，具有四核處理器和 5 吋的電容式多點觸控螢幕及綜合的紅外線測溫儀。支援多種無線傳輸，NFC 和選配 RFID Reader，內建 1D / 2D 條碼掃描功能，1300 萬畫素的相機。

通過採用工業設計，PWS-472 具有 IP65 防護，防水，防塵，防跌落功能，以及具有超過 12 小時電池壽命的大容量電池。



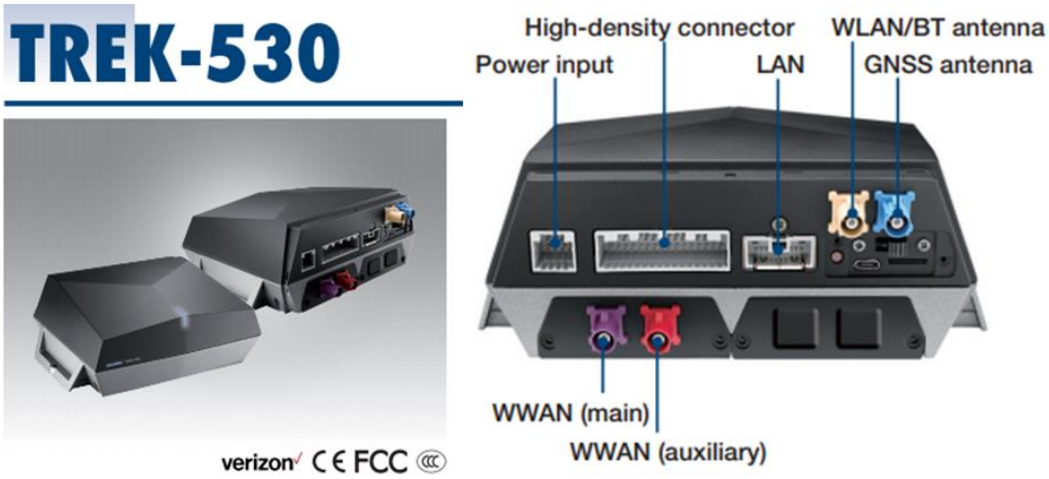
資料來源：https://advdownload.advantech.com/productfile/PIS/PWS-472%20INFRARED%20THERMOMETER/file/PWS-472-with-Infrared-Thermometer_DS(111119)20191119141312.pdf

圖 10、PWS-472 紅外線感測器

3. TREK-530 車載電腦

TREK-530(如圖 11)是基於 RISC 的緊湊型車載電腦，配備了 Qualcomm®Snapdragon™212 四核 ARM®Cortex™-A7 SoC，隔離式 DI / O 和兩個擴展插槽，可根據應用要求進行擴展。內置的 WLAN，藍牙和 GNSS 模塊提供增強的連接性，而定期性的，數據輸入和 WWAN 暫停/恢復功能則支持遠程監控，使 TREK-530 非常適合物流和車隊管理。 此外，該系統的寬工作溫度範圍（-20～65°C），支持 12 / 24V 車輛電源，並符合 MIL-STD-810G 和 5M3 衝擊/振動標準，從而確保 TREK-530 能夠承受惡劣環境下的操作。

TREK-530 負責搜集車上感測器資訊、GPS 定位記錄並傳輸上雲端。



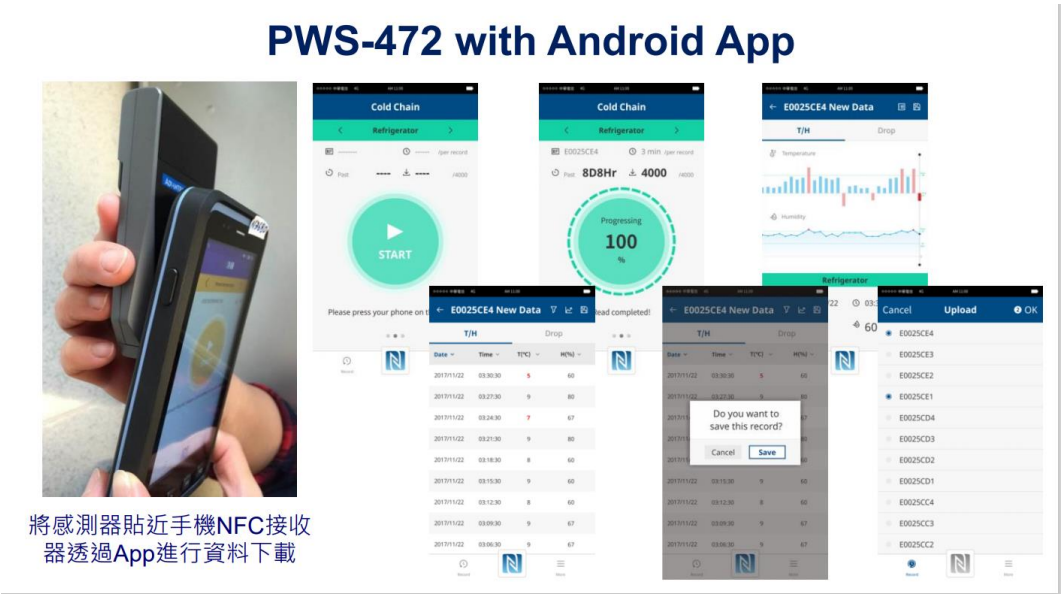
資料來源：https://advdownload.blob.core.windows.net/productfile/PIS/TREK-530/file/TREK-530_DS(060220)20200610125404.pdf

圖 11、TREK-530 車載電腦

(二) 軟體

1. PWS-472 with android app

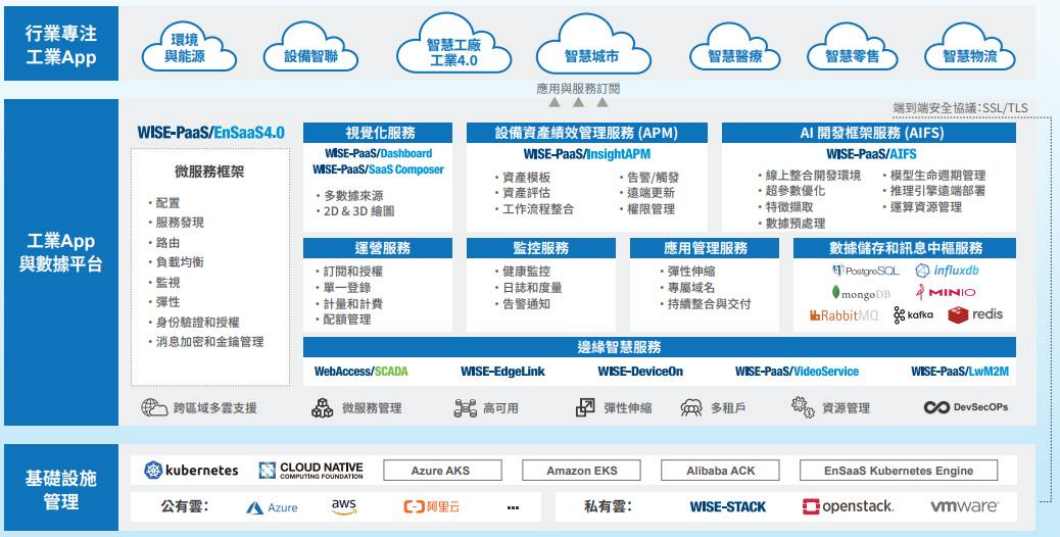
為了冷鏈管理，在 PWS-472 中的應用程式(如圖 12)，利用 NFC 的方式將資料傳輸至 PWS-472 中，以便查看存在感測器中的資訊。



資料來源：研華科技提供

圖 12、PWS-472 Android App

2. 研華科技的 WISE-PaaS 雲服務(如圖 13)為主要核心，和奇雲國際的 Fleetivity 主動式安全行車管理平台，共創智慧車隊管理 SRP（Solution Ready Package），而在此案例中所使用的車載裝置中的數據會連接上雲端，同步上傳研華 Azure 雲端平台。



資料來源：http://advcloudfiles.advantech.com/ecatalog/2018/02080902.pdf

圖 13、研華科技 WISE-PaaS 雲服務

(三) 網路連結

1、 各裝置的網路連接

(1) TREK-120 LoRa 溫溼度感測器：

NFC	13.56MHz
LoRa	860-930MHz for Taiwan/USA/Japan/South Korea 868MHz for Europe 470.3-489.3MHz for China

(2) PWS-472 紅外線感測器：

WLAN/Bluetooth	IEEE 802.11 a/b/g/n Bluetooth V4.1 BLE
NFC	Compatible with ISO 15693, ISO 14443A/B, MIFARE®
WWAN (Optional)*	LTE: B1, B3,B38, B39, B40, B41

(3) TREK-530 車載電腦：

WLAN/Bluetooth	IEEE 802.11 a/b/g/n dual band (2.4/5 GHz) and Bluetooth V4.1 Class 1 (with external antenna via FAKRA connector)

2、 網路協定

物聯網的通訊技術有很多種，如 Sigfox、LoRa、NB-IoT(如圖 14)，而研華科技在全程冷鏈不斷鏈管理中，使用了 LoRa 技術。

資料來源：研華科技提供

圖 14、通訊傳輸比較

因為 LoRa 技術有著無須額外頻段授權費，法規限制單純易於全球布建，且低功耗，可用電池供電，系統可以長時間運作。

由於操作頻率與展頻調變技術，使得訊號的抗干擾力與穿透性強，訊號的傳輸距離長，涵蓋範圍廣，由感應端，中繼端到雲端，具備高度彈性，可依據應用需求做設計。

而與 LoRa 較相關的網路協議為低功耗廣域網路（LPWAN），其 RFC 8376:Low-Power Wide Area Network (LPWAN) Overview 為 LPWAN 的概述，講述著低功耗廣域網路(LPWAN)為一種無線技術，具有覆蓋範圍大，低頻寬，封包和應用層數據大小可能非常小以及電池壽命長等特點。 此篇 RFC 是 IETF 正在考慮的一系列 LPWAN 技術以及這些技術的需求與在 LPWAN 中運行 IP 的目標之間存在的差

距的信息性概述。

在文件當中也有提及 LoRaWAN 技術，講述它的來源與特性及其使用時所需要的參數與整體架構。

3、 網路安全的考量

傳統感測器使用 Wi-Fi 或藍牙傳輸資料，但其缺點在於耗電量大，用戶須經常為其充電或更換電池，否則易造成資料遺失，即使後來的低功耗藍牙技術問市，但因容易受到外界干擾，故不適合使用在冷鏈食品安全監測。

而 LoRa 技術不只穿透率高、傳輸距離更遠勝於以往傳輸方式，使得商家只要在賣場內安裝一至兩個閘道器（Gateway）就足夠，降低系統架設的成本，再者 LoRa 基地台易架設，只要安裝特殊軟體與 Dongle 後，任何一個 IT 裝置都能變成基地台，確保通信服務的穩定度與可靠度。

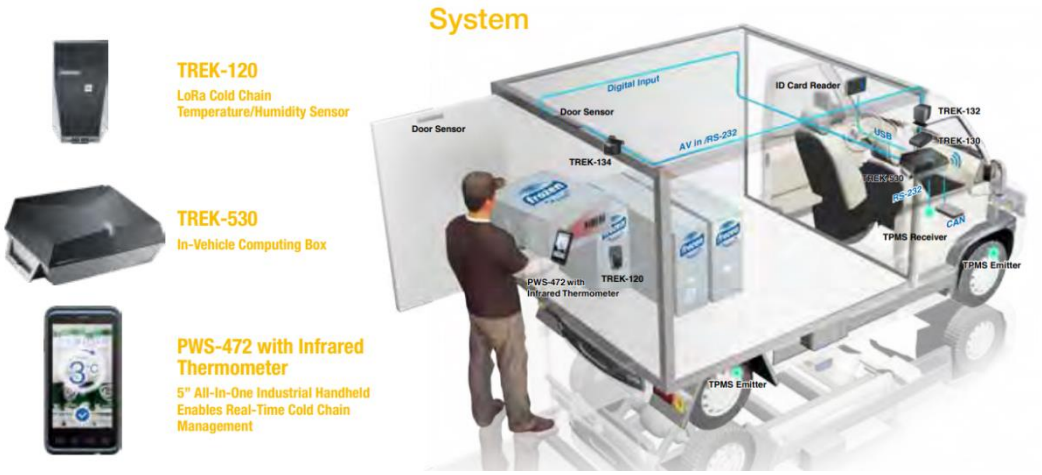
但能須注意，LoRa 主要運行在全球免費頻段，故容易與零售通路業者的無線對講機頻段重疊，造成訊號相互干擾，而研華工程師協助調整 LoRa 運行頻段，同時增設指令，讓感測器在傳輸資料前，先詢問空氣中是否有訊號占住通道，確保資料傳輸的品質與正確性。

4、 如何使用服務

全程冷鏈管理，從而實現了實時溫度/濕度/跌落感應和車門鎖監

控。配備 LoRa 技術的研華 TREK-530 車載電腦與 TREK-120 感測器組合在一起(如圖 15)，可以將實時數據傳輸到後端中心，為冷鏈管理提供了可靠而經濟的解決方案。此外，驅動程式還可以通過帶有紅外線溫度計的 PWS-472 實施行動管理，從而使它們成為不再需要拆開產品包裝進行檢查的冷鏈人員的理想行動監視解決方案。

在零售門市或賣場中也使用了 LoRa 無線冷鏈感測器(如圖 16)，隨時監測冰櫃溫度，另外，針對特定生鮮食品、溫度一有變化品質就會受影響的商品，以及供應商透過自有車輛運送的商品，業者會事先把 LoRa 無線冷鏈感測器交給供應商，請供應商放在貨箱裡一起運送過來，以便隨時監控商品在運輸過程中的環境溫度，確保冷凍冷藏商品沒有變質的風險。



資料來源：http://advcloudfiles.advantech.com/ecatalog/2019/01091800.pdf

圖 15、裝置應用在運送車輛的示意圖

資料來源：https://advcloudfiles.advantech.com/cms/ce9f64f1-2bc2-43cf-98d2-df4cdff74765/Content/content-image-1550039864516.jpg

圖 16、裝置應用在賣場的示意圖

四、應用與展示

針對全程冷鏈不斷鏈的案例有各種場域的應用，如倉儲配送中心(圖 17)、醫療院所(圖 18)、零售門市(圖 19)等等。

資料來源：研華科技提供

圖 17、倉儲配送中心

資料來源：研華科技提供

圖 18、醫療院所

資料來源：研華科技提供

圖 19、零售門市

五、參展紀錄

1. 研華科技與台灣冷鏈協會（Taiwan Cold Chain Association, TCCA），在研華物聯網智慧園區舉辦「2017 台灣智慧冷鏈創新論壇」，會中邀請研銳俌科技、邰利與 Thermo King（冷王）等業者共襄盛舉，就「台灣智慧冷鏈全程監控的挑戰與因應」討論。

資料來源：http://www.flutai.com.tw/news-detail.php?id=25

圖 20、2017 台灣智慧冷鏈創新論壇

2. 於 2019 年在台灣教育科技展上設有攤位展出

資料來源：https://www.youtube.com/watch?v=O4cwpWzA5Rk

圖 21、2019 台灣教育科技展

六、致謝

非常感謝研華科技提供多數內容與圖片，讓我們能為此物聯網案例的撰寫能順利完成，也更進一步的瞭解此產品的用途與技術的應用。

第二節　醫的物聯網 - LincGO 服務架構與技術

一、現況與挑戰

現有的心電監測器笨重昂貴，24 小時的裝配總讓使用者行動不便，且偵測完還需回到醫院歸還儀器才能讀取數值。另外由於監測裝置在使用上較為複雜，必須由專業的醫事人員協助，因此不論穿戴或移除，皆需要在醫療院所才能完成，若對於行動較不方便或剛接受完心臟相關手術後的受測者，便可能需住院幾天而無法在家舒適的休息。

長遠來看，除了儀器設備的限制外，隨著世界人口的增加與老化，醫療資源如何保持乘載運作甚至提升品質，都是未來的醫療趨勢，也是必須面對的醫療困境，以下便列出幾項現存的實質挑戰。

(一)　世界人口高齡化

人口高齡化是指因出生率降低和預期壽命延長導致年齡中位數增加的現象。大多數已開發國家人口長壽，高齡人群變多；但開發中國家目前也出現類似趨勢。

人口高齡化的衝擊將表現於社會與經濟上，尤其是對醫療體系的影響。雖然人的壽命延長，但罹患各種慢性病如關節炎、心臟血管疾病、癡呆症、巴金森氏症、腦血管疾病、糖尿病等的機會也隨著增加。據統計，50 歲以上罹患慢性疾病的機率每 5~7 年會增加 2 倍。而根據美國疾病管制局的報告，美國 65 歲以上的人口有超過七成至少有

一種慢性病，而治療慢性疾病患者的支出占美國醫療費用的 86%。

(二)　從預防醫療到遠距醫療

對慢性疾病的治療和老年人的照護將成為世界醫療保健的首要問題。按照現有的醫療模式，未來的醫療費用會是天文數字，多數政府都難以支持如此龐大的醫療開支。解決此難題的一個可行方案是實施預防醫療(Preventive Medicine)，亦即在疾病癥狀顯露之前，早期發現並介入處理疾病。由於疾病在早期階段往往是可逆的，因此可以顯著降低長期照護與治療成本。

另外，遠距醫療是預防醫療重要的一環，讓健康照護服務從傳統醫院的床邊服務，轉而以慢性病的居家照護與生活服務為主軸，讓民眾在熟悉的社區與居家環境中獲得健康照護與預防保健服務，這不僅是世界各國醫療科技與服務產業的發展趨勢，也是政府力推的政策。透過科技的介入，讓未來的慢性病照顧系統得以達到連續性、完整性。

(三)　心血管疾病與心電監測器

心血管疾病是全球最常見的死因之一。1970 年代起，在開發中國家裡不管哪個年齡層因心血管疾病的死亡率都在上升，2013 年心血管疾病共奪走了全球 1,730 萬條生命（占總死亡數的 31%），因此解決心血管疾病發病率增加的問題已成為醫學界關注的焦點。

在心血管疾病預防醫療中，偵測與診斷方法扮演了重要的角色。

心電圖(ECG)是心臟搏動相關的電位變化圖，由於心電圖各波形之形狀及其間隔皆與心臟之電氣特性有直接的關係，所以醫師可以藉著認出心臟電氣活動中的異常，而診斷出許多不同的心臟疾病，進而可用來監測病人安危、評估病情進展和治療成效等。

雖然心律失常為常見之疾病，但是檢測起來卻並不容易。院內所使用之單次檢測很難準確發現症狀，需要對患者長時間的連續監測才能蒐集有效數據。因此，醫院通常採用動態心電監測方式來檢測心律失常，又稱為 24 小時心電圖。長年來，醫院皆是使用 12 導程心電監測器來進行 24 小時動態心電監測。

(四)　心電監測器現存問題

對於使用者而言，裝配 12 導程心電監測器在身上時，需將拳頭大小的監測器主機貼在胸口或是背掛在腰間，接著分別牽引 4~10 條感測線端貼在身體上，分別貼附在鎖骨到腹部之間。由於導線複雜，身體動作容易牽扯到線路，導致使用者行動不便、戰戰兢兢；此外，監測器主機至少 300 克重，從衣物內突出的主機也不雅觀。因此進行 24 小時心電監測的使用者，大多選擇待在家裡而不會上班上課，遑論室外活動運動。並且，傳統心電監測器在實務上都是回收再重複使用，使用者心中難免有衛生上的疑慮。

另一方面，醫事人員在協助使用者配戴心電監測器時，需花

10~30 分鐘的時間為使用者衛教與裝設；在回收心電監測器時，需檢查電力、完整、故障情形，接著清潔監測器，此也造成人力成本的消耗。

在無法管理使用者行為的狀況下，所回收的心電監測器通常會具有高損壞率(10~20%)。由於心電監測器持續不間斷地給多個使用者配戴，難以追究使用者之使用責任，須由院方自行吸收，導致不論是維修或是重新添購心電監測器都是醫院另一筆難以精算及避免的成本消耗。

二、願景

LincGO 第一代是 72 小時一次使用心電監測貼片，未來第二代希望升級其使用時間至 120 小時，及增加呼吸率和心音等功能，第三代目標則能銷往一般通路藥局(圖 22)。

圖 22、未來三年產品路線

LincGO 與服務的首要市場是泰國與印度，第二階段將擴大至全

東協地區，最終目標以行銷國際為目標。因本產品涉及醫療器材，將受到各國的醫療衛生法規的限制。目前此計畫產品第一代「心電監測貼片」24 小時及演算報告已經於 2018 年六月獲得美國 FDA 核准上市，台灣的 TFDA 二類正在申請中，未來第二代「心電監測貼片」72 小時和傳輸演算整合這部分，預計於 2019 年下半年申請美國 FDA 認證(圖 43)。此外，印度的法規登記及泰國的東協醫療器材法規，也將會陸續申請。

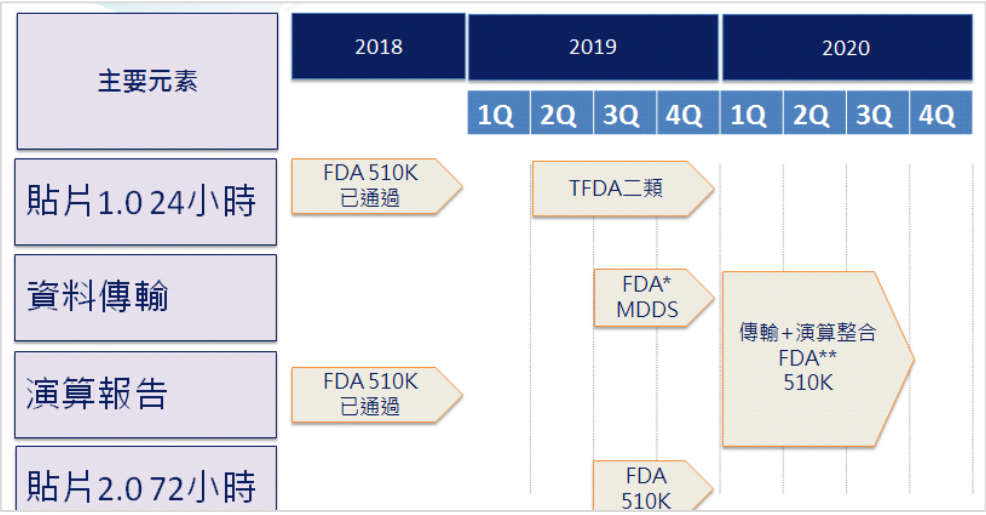


圖 43、FDA 申請時程表

(一) 產品目標

配戴活動輕便化	LincGO 系統平台的心電圖監測貼片重量不到 50 克，總體積小於 100 立方公分，不含有額外導線，從外表上不易察覺貼片的存在，醫事人員 10 分鐘內可以完成裝配與解釋。
監測設備耗材化	LincGO 系統平台的心電圖監測貼片價錢為 50 美元，內含的電池可支持 48~72 小時的偵測時間。使用後的監測貼片不需要交回醫院，直接作為垃圾處理即可。由於購置成本低，地區

	性的小型醫院診所皆有能力負擔。
資料傳輸網路化	透過閘道器與雲端平台，在偵測結束後心電監測器可經由網路傳送心電圖資料到醫院，不須使用者本人回到醫院歸還監測器，省下了使用者的時間成本，提高配戴意願性，並且雲端平台還可進一步提供心電圖初步解析。
醫事研究便捷化	雲端蒐集並儲存原始數據。除了提供給醫院心電圖室的醫事人員，也可成為大數據的寶庫，結合健保資料庫，作為醫事研究的便利途徑。
醫療資源普及化	心電圖監測貼片成本較低，全新品存量可以相當充足，有需要進行檢查的就診者不須漫長等待。若還能獲得健保補助，估計能有超過九成民眾能適時進行心電監測檢查，使得心電監測的醫療資源不再 M 型化，每位民眾都能受到保障。
預防醫療與 遠距醫療落實化	完整的遠端心電監測解決方案讓醫療機構更有意願導入此系統與服務。LincGO 系統平台之心電圖監測貼片的應用，除了就診後醫師指示的 24 小時心電圖監測需求，就診者平日更有意願做預防性的監測，當越來越多的醫療機構願意投入預防醫療與遠距醫療，自然有助於國家醫療的健全化。 同時 LincGO 系統平台之平台進一步協助建立遠距醫療的範本，也提供各種生理檢測平台的途徑，未來可應用在其他種慢性病上，例如糖尿病的血糖偵測等。

三、服務架構

(一) 硬體

使用者貼上心電圖偵測貼片後，即可開始進行心電監測，記錄下的數據會先暫存在貼片中，待監測完畢後再將資料傳送給閘道器，閘道器有很多形式，可以透過插座式閘道器軟體或手機裡的 APP 傳輸

數值到雲端，接著再傳輸資訊到醫院端(圖 23、圖 24)。

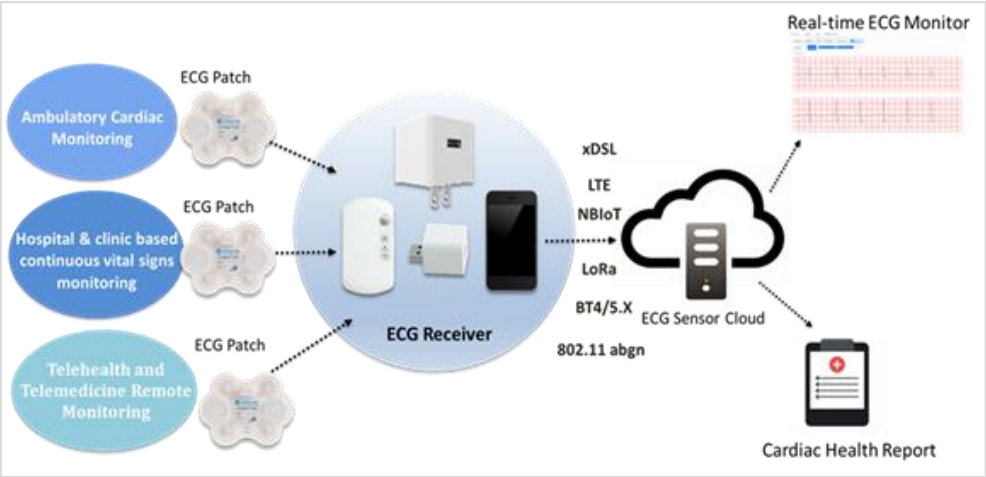


圖 23、監測流程中各硬體的作用

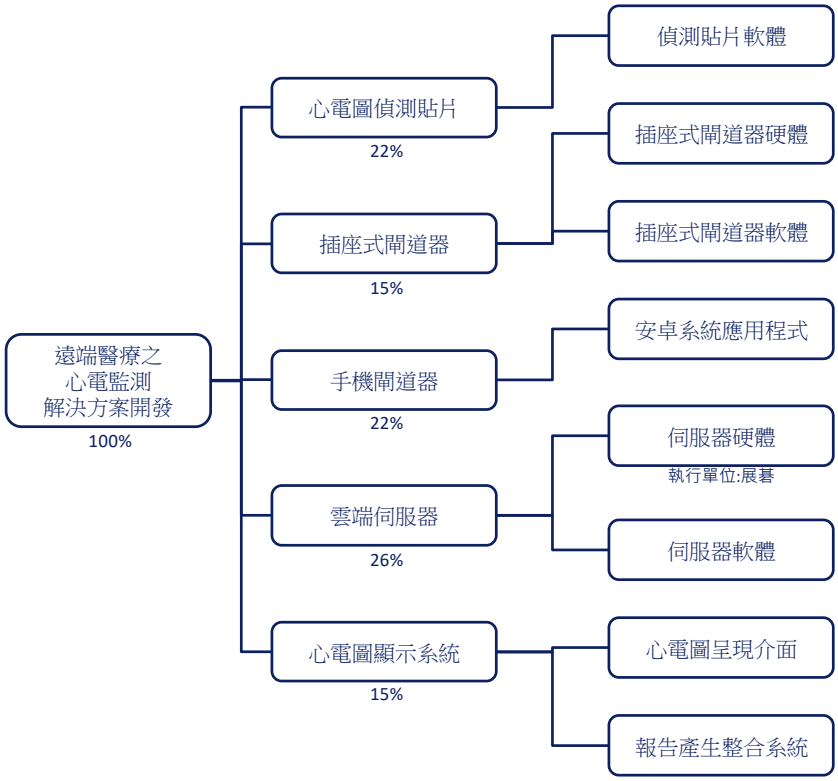


圖 24、LincGO 運行架構

(二) 軟體

LincGO 系統平台須配合硬體模組體積微縮化，致使中央處理器

與記憶體的體積也縮小。為各種因素考量，不使用高功率、高效能與容量最大的硬體元件，而是從軟體的編譯下手。系統平台的軟體須符合各種生理資訊的傳輸，但程式碼必需要精簡以減少硬體負擔，所以在程式碼的編譯設計上，必須反覆檢驗、精煉、優化。

就如上節產品目標曾言，LincGO 系統平台的應用場域除了醫院內部，更需要支持遠距醫療。受限於藍牙標準協定的傳輸距離與協議架構，藍牙技術的網路規模與傳輸距離較小，其應用範圍大多落於短距傳輸。本系統平台須利用藍牙技術高安全性與匹配性等優勢，再結合遠距傳輸的需求才能完成。本公司需藉由多種閘道器還有藍牙傳輸協議的設計，使藍牙遠距傳輸得以實現。尤其本公司需開發至少三種閘道器的韌體與軟體，才得以利用藍牙和 Wi-Fi 手段協助傳輸至網際網路，當中必然存在許多困難。

接著談到雲端開發，其領域包括公有雲、私有雲以及混和雲的雲端技術，相似的技術可重新建構成 LincGO 系統平台中的心電圖雲端平台，當然由於醫療數據涉及使用者的隱私與機密，因此必將以私有雲作為主要開發技術(圖 25)。

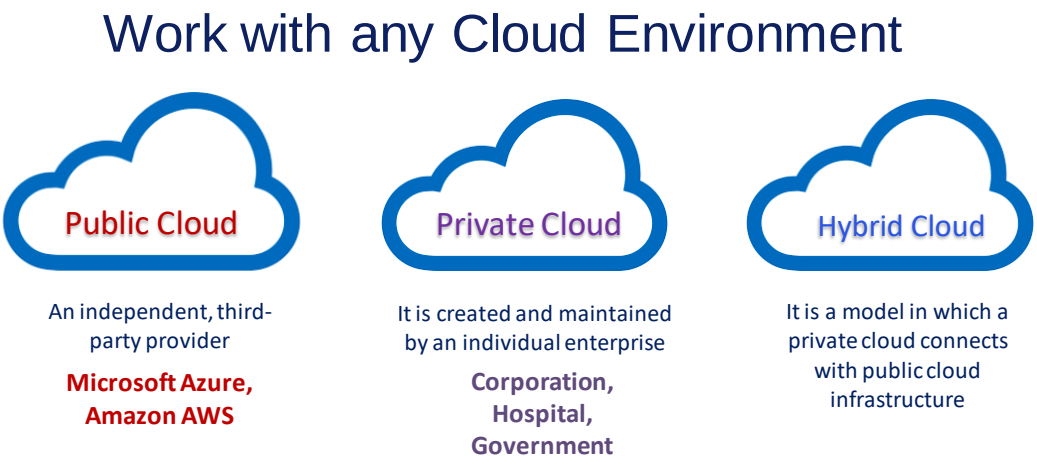


圖 25、三種雲端開發技術

LincGO 系統平台的服務模式中，雲端伺服器接收來自使用者的心電圖資訊，因此實務上網路服務必須穩定不能斷線。這當中也牽涉到網路架構、雲端架構的設計以及備用系統的執行，以建構高信賴度、高安全性的網路服務。進一步還要可以支援千萬人口的網路傳輸規模。這當中除了初期的編程與開發，還需要不斷地驗證與測試伺服器的功能，才可以將伺服器正式上線。

(三) 網路

1、 網路連結方式

現今低功耗藍牙無線裝置的普及，其普遍使用方式仍局限於點對點連結的個人區域性通訊，例如：穿戴式裝置與個人手持式裝置的連結，或是居家中影音裝置與無線閘道器的連結，各裝置間無法直接通訊並交換資料，裝置間形成的網路型態屬於星狀結構，僅能透過中央的閘道器或集線裝置，例如手持式裝置或個人電腦，與裝置溝通。另

外，網路中裝置之間的連結因為局限於低功耗藍牙的傳輸距離、低功耗藍牙裝置低耗電需求以及需要搭配閘道器以及電力線的建置來增加網路的規模以及涵蓋的範圍，導致無法簡易以及有效地將網路規模放大。

立創智能提出建立並監控低功耗藍牙無線網路之技術方法，以幫助複數個低功耗藍牙無線裝置建立複數個低功耗藍牙無線網路。該方法包含下列步驟：控制低功耗藍牙無線裝置中之第一藍牙無線裝置由廣播狀態進入偵查狀態。於偵查狀態中，第一藍牙無線裝置接收低功耗藍牙無線裝置中之第二藍牙無線裝置所發送之第一連線要求廣播訊號，第一連線要求廣播訊號包含對應於第二藍牙無線裝置之第一裝置識別碼。待第一藍牙無線裝置由偵查狀態進入建立連線狀態。於建立連線狀態中，第一藍牙無線裝置根據第一連線要求廣播訊號以及第一裝置識別碼與第二藍牙無線裝置建立第一藍牙連線。以及第一藍牙無線裝置透過第一藍牙連線傳送一觸發指令至第二藍牙無線裝置以控制第二藍牙無線裝置由待命狀態進入偵查狀態(圖 26)。

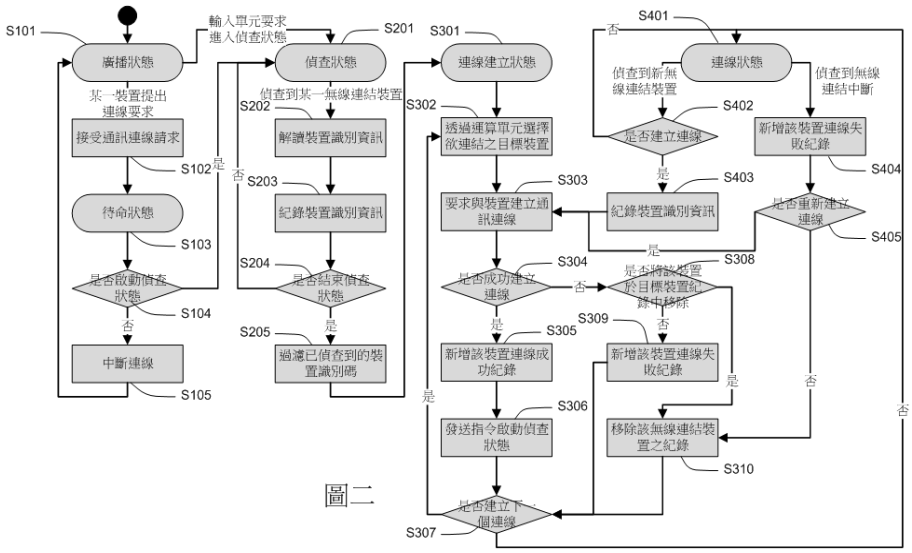


圖 26、建立並監控低功耗藍牙無線網路之方法

雖然使用藍牙無線傳輸技術有著許多優點，但傳輸距離的問題卻一直是藍牙技術廣泛被使用的最大阻礙，雖然藍牙 4.0 版本的藍牙裝置間傳輸距離已從傳統藍牙協定的 2~10 公尺提高為 60~100 公尺，但若使用於戶外空間或有建築物遮蔽的空間中，該通訊距離會受影響而縮減，致使不敷使用。

因應前述問題，立創智能也提出一種遠端藍牙裝置通訊系統，包含管理裝置、藍牙代理裝置以及藍牙終端裝置。管理裝置透過網際網路發送網際網路封包訊息至藍牙代理裝置。藍牙代理裝置接收到此網際網路封包訊息後，將網際網路封包訊息轉譯成標準藍牙通訊封包訊息並透過藍牙傳輸發送至藍牙終端裝置。藍牙終端裝置接收到標準藍牙通訊封包訊息後，執行標準藍牙通訊封包訊息所包含的資訊內容及命令設定之動作。相較於現有技術，此遠端藍牙裝置通訊系統透過藍

牙代理裝置將藍牙通訊封包訊息及網際網路封包訊息進行轉譯，利用網際網路傳輸達到遠距離控制藍牙終端裝置的目的，克服了藍牙無線傳輸距離限制的問題(圖 27)。

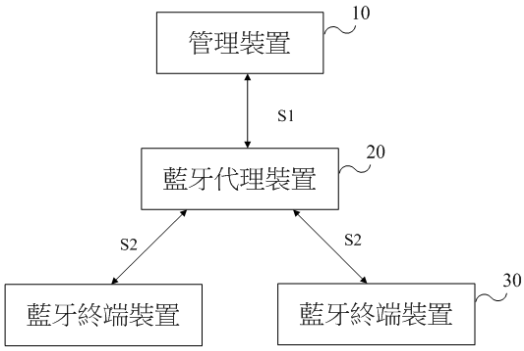


圖 27、遠端藍牙裝置通訊系統

2、 克服不同裝置的網路協議

在使用上，不同用途的藍牙裝置所需藍牙應用層通訊協定並不相同，所以各種藍牙裝置分別支援有不同組合的通訊協定，也衍生出各自對應的 APP。立創智能透過雲端的虛擬裝置，模擬手機執行供應商提供的 APP 來解決這個不便的問題。

本公司開發出一種遠距藍牙連線系統，包含有藍牙閘道器、藍牙設備、雲端虛擬裝置以及藍牙應用程式。藍牙設備設置於藍牙閘道器之服務範圍內。雲端虛擬裝置進一步包含有藍牙虛擬層模組以及通訊模組。藍牙虛擬層模組提供藍牙程式介面。通訊模組用以建立網路連線至藍牙閘道器。藍牙應用程式執行於雲端虛擬裝置，用以透過藍牙程式介面經由藍牙虛擬層模組建立網路通訊控制藍牙閘道器之服務

範圍內之藍牙設備或讀取藍牙閘道器之服務範圍內之藍牙設備所量測之數值，該網路通訊方式可為藍牙、有線網路、無線區域網路或行動通訊網路(圖 28)。

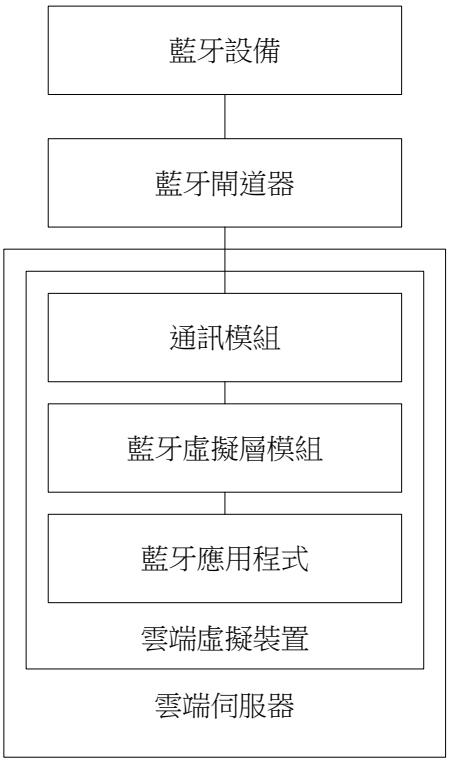


圖 28、遠距藍牙連線系統

遠距藍牙連線系統透過雲端虛擬裝置模擬手機安裝並執行藍牙應用程式。因此可解決手機安裝執行應用程式時耗費流量、記憶體以及處理器資源的問題。藉由藍牙虛擬層模組提供藍牙閘道器與藍牙設備連線所需之指令集。接著透過藍牙閘道器轉換，實現雲端虛擬裝置對藍牙設備的遠端操作。尤其執行於雲端伺服器的雲端虛擬裝置可以被設定自動的與藍牙設備溝通，無須人為的操作。甚至可以讓多位使用者分別用不同的智慧終端登入雲端伺服器，以相同的藍牙應用程式

操作藍牙設備。

藉由此技術，可以解決部分應用情境中監測貼片讀取到的數據需要即時傳輸出去的問題。這樣的應用下不須有終端裝置隨時與監測貼片連線準備接收數據，而是透過閘道器到雲端伺服器接收儲存數據，此外也不需要長時間開啟智慧終端以操作監測貼片，減少麻煩，提升待監測者的使用意願。

3、 網路安全的考量

雲端伺服器是能執行應用程式和資訊處理儲存的強大實體或虛擬基礎架構，當科技分工越來越細，租賃雲端伺服器便成為一種新的商業模式。欲租賃的公司依據所需要的伺服器等級、容量、時間來付費，並且不用負擔伺服器硬體的購置與維護費用。然而在開發性的網路中建立資料中樞，也提升了隱私安全性的風險(圖 29)。

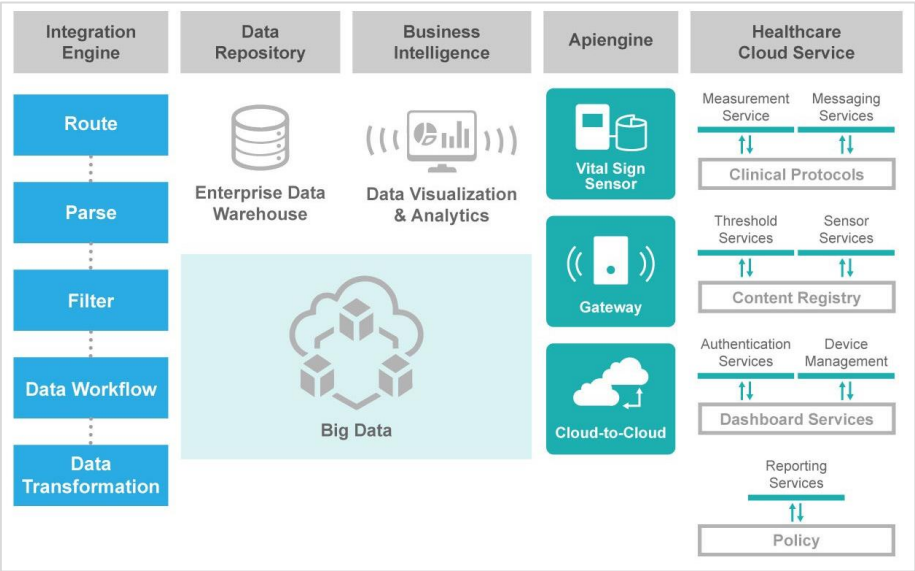


圖 29、PaaS 雲端即服務分層框架需求

實務上 LincGO 系統平台的網路服務必須穩定不能斷線，因此必須要設計良好的網路架構、雲端架構以及備用系統，以建構高信賴度的網路服務。此外還需要設計良好的防駭架構與權限設定，才能維護患者的病情隱私，又方便醫院管理。再進一步還要可以支援上千萬人口的網路傳輸規模，這當中除了初期的編程與開發，還需要不斷地驗證與測試伺服器的功能，才可以將伺服器正式上線。

4、 使用模式

國內合作模式以 B2B 為主，精準定位醫療院所，其醫療院所引進護理站設備與人員即時管理系統，未來可望從其推廣而入。海外部分，則主要以海外合資企業為核心的發展策略，初期先建構團隊，接下來試營運取得當地食藥局法規核准後，再導入示範進入大型醫院和健檢系統，最後擴大在當地的市場，並啟動上市(圖 30)。

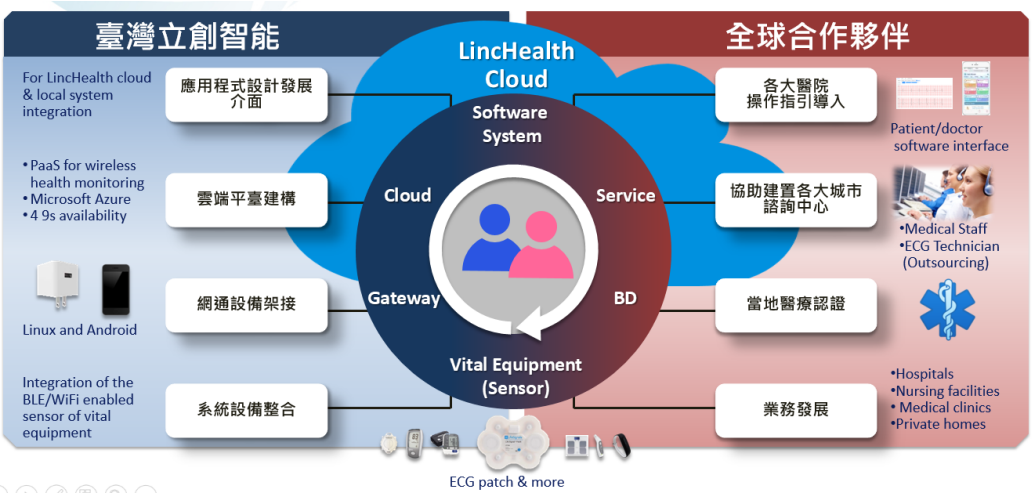


圖 30、策略合作商業模式

四、應用與展示

(一)　應用價值

1、 應用範圍

本服務與產品應用於心血管疾病的患者、心臟內外科的就診者、健康中心的定期檢查者、或是自覺心臟不適的未確診民眾。應用的檢查方式可以是運動心電圖、靜態心電圖或是 24 小時心電圖檢查。使用場域適用於家庭、療養院、醫療機構一般病房或重症病房。LincGO 系統平台的最主要的應用為:就診者受醫師指示進行 24 小時心電圖監測，即刻在醫院安裝監測貼片後返家。24 小時之後監測結束，就診者透過住家的閘道器或是安裝對應軟體的手機上傳心電圖數據到雲端。最後再從雲端伺服器傳輸資料到醫院的資料中心。可利用對應的貼片編號或是手機設定以讓醫院資料中心將心電圖資料歸檔至該就診者。在此案例中，監測貼片由醫院提供，監測結束後貼片可丟棄(圖 31)。

圖 31、24 小時心電圖監測應用場景

2、 實用價值性

(1) LincGO 系統平台在不同的商業合作模式之下，可以應用於心血管疾病病患住在醫院病房，或是就診者在心電圖室進行靜態心電圖檢測或運動心電圖檢測時使用。住院病房和心電圖室有預先設定好的院內閘道器，檢測完成後，透過院內閘道器將資料傳輸到雲端伺服器。最後再從雲端伺服器傳輸資料到醫院的資料中心。在此案例中，監測貼片與閘道器皆是由醫院提供，在醫院檢測結束後也方便回收貼片。回收的貼片可以送回工廠拆解外殼、電池等零件，重置系統後還可回收利用(圖 32)。

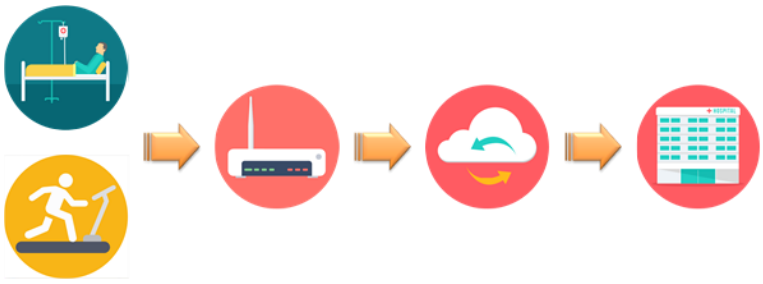


圖 32、醫院內心電圖檢查應用場景

(2) LincGO 系統平台可以延伸的第二種服務應用於預防醫療與遠端醫療。當使用者自覺有心血管症狀，或是欲進行定期檢測。此時使用者不須到醫院掛號進行診斷，僅需直接至藥局或相關合法機構購買監測貼片。使用者透過安裝對應軟體的手機或閘道器操作，可設定貼片的檢查項目係為靜態心電圖、運動心電圖或 24 小時心電圖。閘道器接收心電圖資料並且

附加上使用者輸入的其他資訊，再傳輸上述資訊至雲端伺服器。依據使用者設定，雲端伺服器可以傳送最終資訊給醫院、相關醫療人士或親友、或是使用者的手機當中。更佳的狀況是傳送至醫事人員將心電圖資料做初步評估後，傳送到使用者的手機當中。這樣的服務模式最為彈性，使用者不須親自前往醫院即可完成一系列的檢測。由於沒有指定的就診醫院，資料也可由專門的心電圖判讀機構進行分析，減輕醫院負擔。此種服務最能落實預防醫療與遠端醫療(圖 33)。

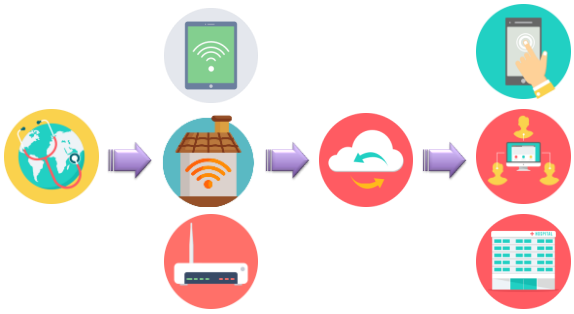


圖 33、遠端醫療與預防醫療應用場景

(3) 遠端醫療心電圖檢查或監測應用場景第三種加值應用需更多種終端監測器，例如血糖監測器、血壓監測器、血氧監測器等。此些監測器可與心電圖監測貼片共用同樣的閘道器與雲端系統。從這些監測器上得到的數據與心電圖監測貼片的數據合併後，更有助於醫事人員的病情掌握與診療判斷。提供更多檢測種類的服務，對於本服務的客戶黏著度也會提高。

(4) 第四種應用需要在雲端伺服器中建立人工智慧判斷系統，並在雲端伺服器中將心電圖數據透過智能分析判斷來產生初步的可用資訊。此服務可應用在心電圖室中，人工智慧產生該使用者的心電圖報告，包含異常狀態時間、異常波形間期等資訊彙整。心電圖室的醫檢人員不須再從頭製作報告，僅需具名確認報告正確性即可。

(5) 第五種服務應用也是在雲端伺服器中建立人工智慧判斷系統，但此人工智慧重點在即時(real-time)監測。應用在加護病房或重點觀察的病患當中，當病患心電活動發生異常狀態，雲端的人工智慧發現數據中產生離群值，即可立即通知相關醫護人員對病患進行關切。

(二) 產品優勢

LincGO 系統平台的產品與服務提供醫療單位整套的解決方案。無須拉導線裝配於身體，僅需簡單貼附於胸口。商業模式主打拋棄式監測貼片，可透過閘道器直接上傳數據到雲端，而不須回醫院拆卸或是郵寄回監測器。本平台不但可以雲端接收數據，無須消耗護理人員的安裝或拆卸時間，還可以在雲端中替醫療機構整理檔案，甚至協助初步分析數據成為報告。由於可以減輕醫療單位的許多負擔與時間成本，醫療單位將樂於引進此解決方案，成為 LincGO 系統平台服務切

入市場的第一個優勢，而對消費者而言，售價便宜則是第二個優勢。提供給使用者及醫療機構雙贏的解決方案(圖 34)。

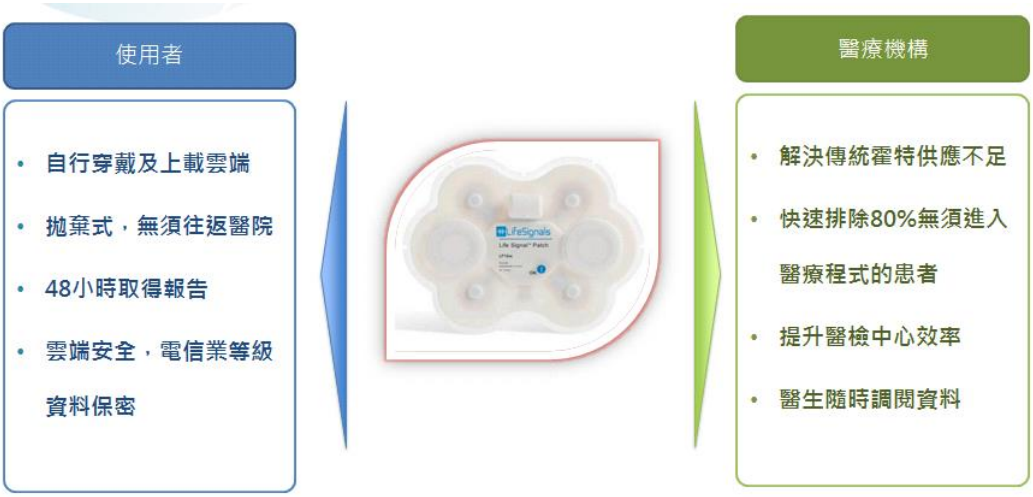


圖 34、雙贏的解決方案

表 5、傳統與新型智慧動態心電圖監測比較

	LincGO	傳統 ECG
金額價格	一次性裝置 產品價格較可負擔	非拋棄式 裝置成本與檢查費用較高
舒適度	較佳，重量輕，體積小	較差
資料傳輸	ECG 數據可在 醫療院所與住處間傳輸	ECG 數據需在醫療院所 讀取與分析
其他優勢	可協助術後心臟分析 與心臟健康檢查	

儘管近年來如 Apple、Nokia、華碩等科技公司陸續推出搭載有 ECG 功能的智慧手錶以搶佔醫療市場。然而，本產品為 3 導層式，智慧手錶的心電圖僅為單導層式(1-Lead)。多導層心電偵測器可以觀察

到心臟更多的訊息和特徵，且不易受到單一訊號干擾。因此在功能性以及精準度上，LincGO 系統平台遠優於市面上的穿戴式裝置或手錶。

再者，智能手錶和 LincGO 系統平台產品都可以通過手機作為中間閘道器傳輸資料出去。然而，智能手錶儲存功能有限，僅能擷取並發送片段的 ECG 圖；LincGO 平台中規畫有專業專用的雲端伺服資料庫，可以讓醫事人員看到更完整的 ECG 時間軸。

	WiPatch Linctronix(TW)	VitalPatch Vital Connect(US)	Spyder Web Biotech(SG)	ZIO XT iRhythm(US)	SEEQ MCT Medtronic(US)	myPatch CardioScan(AU)
Capacity	5 days	3 days real time 10 hours storage	Real time no data storage	14 days	7.5 days	7-14 Days (Lithium-ion battery)
Leads	Up to 3	1	2	1	1	2
SR (Hz)	244	240	150	200	200	100
Data	WiFi	Blue tooth 4.0	Blue tooth 2.0	Blue tooth 4.0	Blue tooth 4.0	No wireless
Weight (g)	12	13	48	21	50	25
Size(mm)	110 X 80 X 2	120 X 95 X 40	60 X 55 X 18	123 x 53 x 10.7	160 x 60 x 15	120x 44 x50
User cost	<US$150	US$400	US$ 230~380	US$329~500	US$300~718	US$230~380
Key advantage	High CP all in one Holter & Real Time & Event recorder	Multi vital sign detection device	Null	Mature business model	Famous worldwide brand	Easy wear
Key weakness	1st Generation product	None binding of clinician ECG report	Restriction disconnect BT 2.0 power consumption high	Holter only, easily drop when wearing	Specific receiver required, heavy and oversize for wearing	Holter only Lithium-ion battery risk of exposure not safety

圖 35、WiPatch Linctronix 與他牌比較

(三) 產品標準使用流程

受測者在雲端平台輸入感測器 ID 來綁定裝置，完成後可在雲端平台上檢查是否綁定成功。

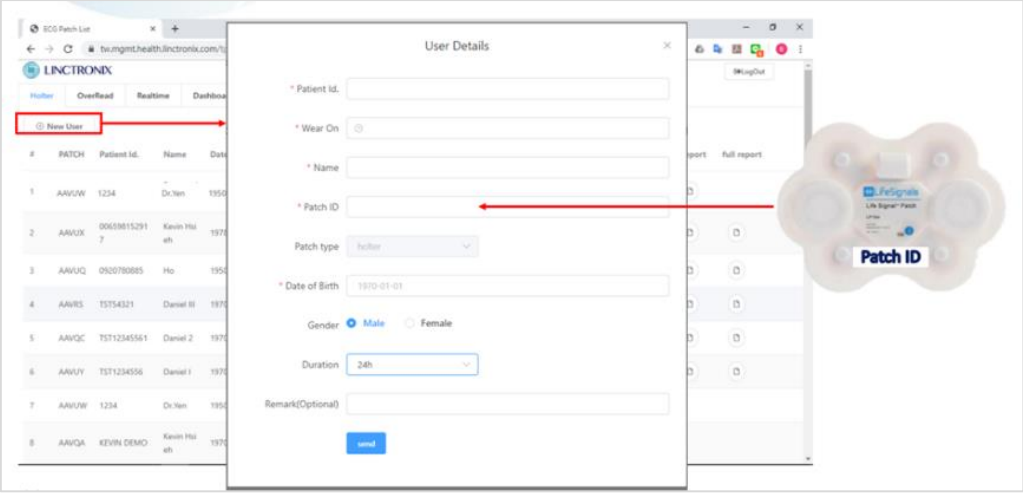


圖 36、綁定裝置

在移動裝置(手機、平板)下載專屬 App 並啟用感測器。

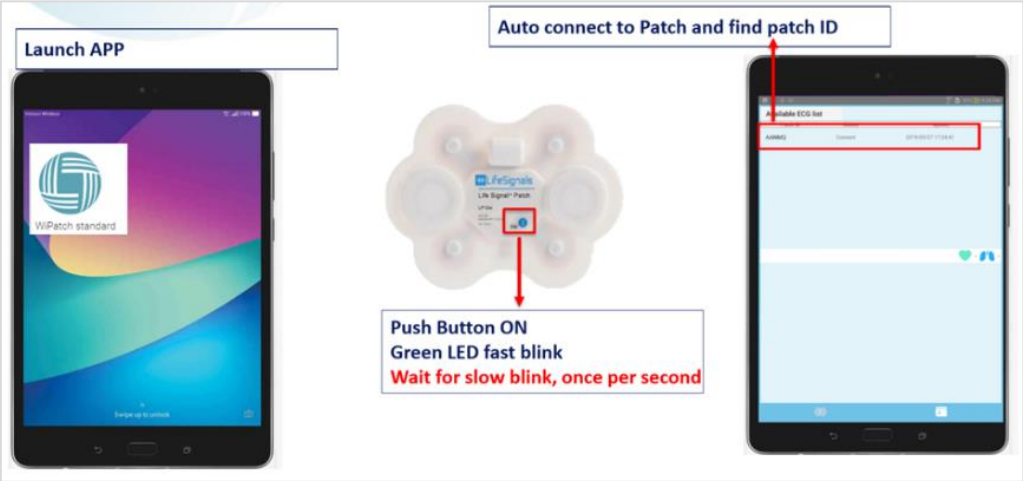


圖 37、下載 APP 並啟用感測器

移動裝置開啟 Wi-fi 並連上感測器後會在 App 內顯示感測器資訊，接著在 App 中切換至 24 小時錄製模式後即開始監測。

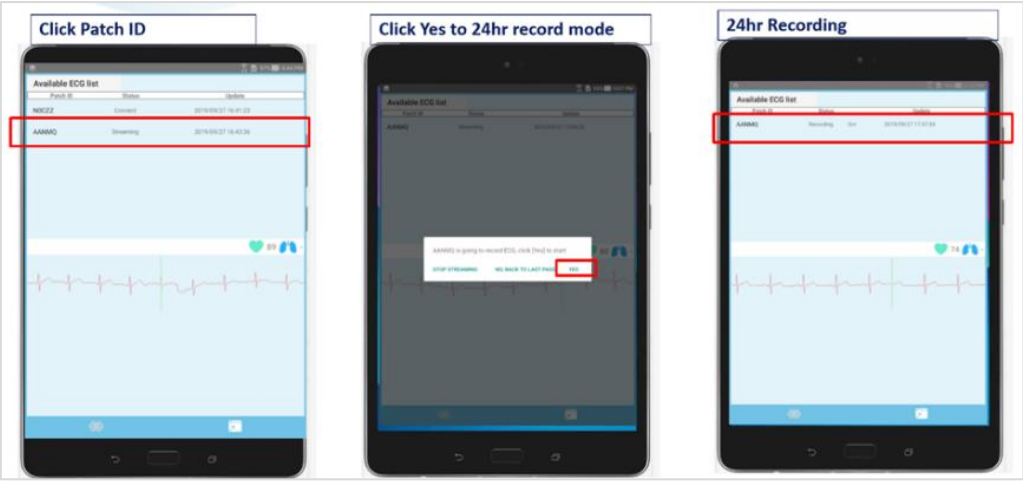


圖 38、顯示資訊並監測

監測完後將感測器數據下載至移動裝置中的 App。(20-30 分鐘)

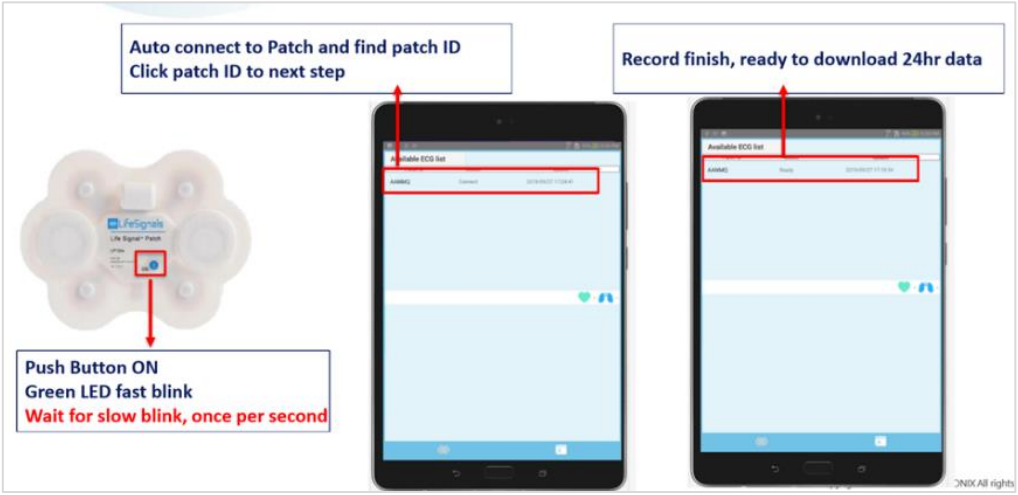


圖 39、下載感測器數據

至雲端平台檢查數據是否已同步上傳成功。

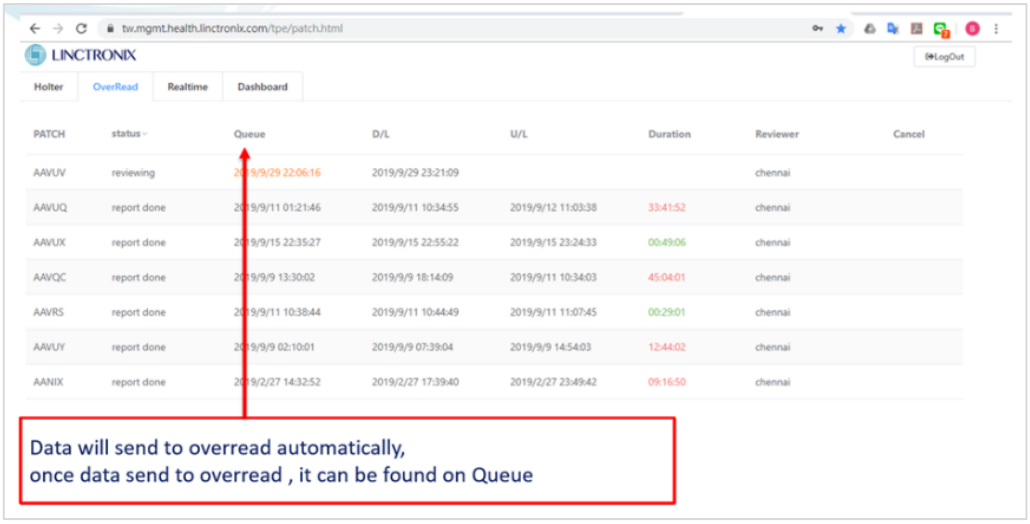


圖 40、檢查雲端同步

12 小時內可在雲端平台下載報告結果。

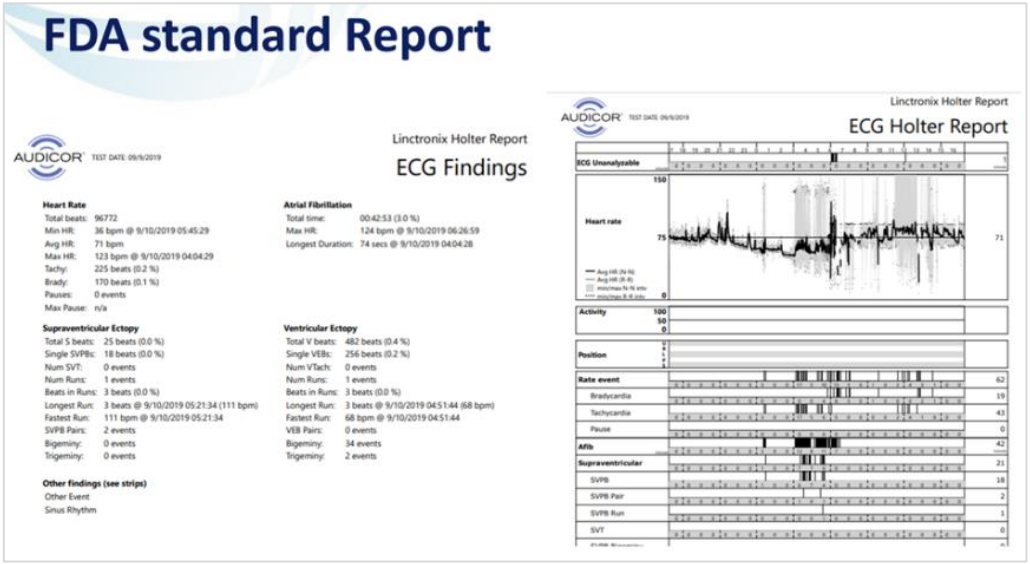


圖 41、下載報告結果

五、得獎紀錄

LincGO 遠距心電圖平台利用雲端技術，提供全世界各地居家之心血管疾病用戶之監控。以一次性的心電圖貼片取代原先高成本的傳統心電監測器，降低醫院成本支出，利用 LincGO 平台可做遠端即時

監控以及 72 小時心電圖，即時透過 AI 演算法篩選出高風險以及有問題之心電圖，再交由印度具有美國心臟協會認證之醫檢師進行判讀以確保結果並符合 FDA 之要求。

LincGO 系統擴大低功耗藍芽的網路規模，並延長藍芽技術的傳輸距離，且可因應貼身微型醫材之程式碼進行編譯，具創新特色。此外，較市面既有產品便利低價，市場接受度高，有利於產品導入，因此獲頒「第十六屆國家新創獎」。

圖 42、第十六屆國家新創獎

第三節　**住的物聯網 – 雲端智慧綠能管理系統(iGEMS)**

一、現況與挑戰

現今地球暖化，能源的消耗逐漸稱加，在舊式的傳統電表中只能單純的看到轉軸與數字的轉動，且需要人工的抄寫，相當的耗時耗力，以現在科技發達的生活相比較不便利。現今對於智慧型用電應用的需求日益增加，但為了與自然環境和諧共存，節能減碳程為了大家須共同努力的目標，若以傳統的方式來看用電情況則較難隨時監控電能的耗損，降低電能使用不僅僅只限於家庭；對於企業來說，尤其是製造相關的產業，由於現在製造業以普遍高度自動化，運用了許多的自動化的製造機台，但製造機台普遍耗能，電費對於製造產業的支出成本占了不小的比例。若要能控管用電的成本就必須清楚且詳細的了解用電量，故電能監控是一個很重要的議題。

二、願景

對於智慧型用電中基本的電能監控更是基本訴求，為求達到省電與節能的效用需藉助綠能管理平台取得相關的消耗資訊，必須考量到各伺服器的使用狀況、電錶和環境感測器所產生資料的大小及分析資料所需的運算資源，因此近年來相當熱門的雲端計算與巨量資料處理等技術，也逐漸被應用於節能的領域中。隨著巨量資料的應用越來越廣泛，全球各產業龍頭相繼投入大量資金與研究，都想透過巨量資料

的處理與分析技術，解決以往人工無法處理的大量且雜亂的資料，並透過資料探勘來得到有價值的資訊，期望以此來改善所面臨的困境。

(一) 質化或量化目標

電力的監測基本上是透過許多電錶來收集及傳送，要收集的資訊包含：電壓、電流、功率因數等等，為了即時監測，則必須要進行頻繁的資料收集，雖然單一電錶的用電資料並不大，但隨著時間增長及場域的擴大，資料量會快速成長，所以在系統設計上就須加入巨量資料處理架構，提升系統儲存與計算能力，提供一個具有巨量資料處理能力的電力分析與監測服務系統。

三、服務架構

東海大學電子計算中心為其數據機房建置一套雲端綠能管理系統，以降低數據訊息中心的 PUE（Power usage effectiveness）與整體用電量為目標，此系統以數據電表對用電設備進行資料收集，並搭配環境溫溼度與 CO2 資訊，提供使用者以圖形化介面呈現以利資料分析。運用巨量資料處理與分析架構為基礎，建置一個資料中心綠能管理平台。透過系統紀錄與用電分析可隨時隨地以行動裝置對用電設備進行查看。此系統具備有「視覺化的資料呈現」、「巨量化的資料處理」、「客製的延展擴充」、「完整的數據統計」與「智慧化的物聯控制」，如圖 43 所示。

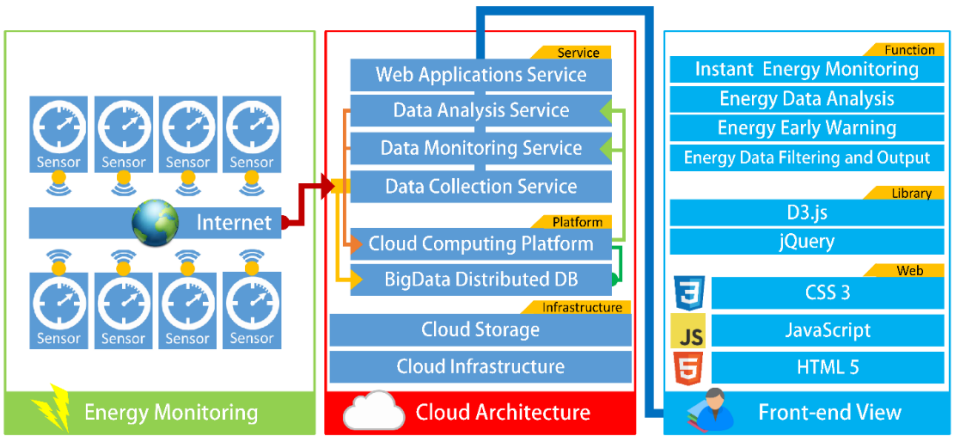
資料來源：東海大學電子計算中心與資訊工程學系

圖 43、雲端智慧綠能管理系統(iGEMS)系統特點

此系統分為三個子架構(如圖 44)，使用者介面(User Interface)、雲端系統(Cloud System)以及電能監控(Energy Monitoring)。使用者介面主要以網頁方式呈現，為方便使用者查看，將各種數據使用圖表式的呈現，並作成符合 RWD 的網頁設計，不論使用手機、平板或是電腦都能輕易觀看。

就系統長遠來看，資料會隨著時間以及感測器的擴增而大量增加，故將此系統導入雲端的架構，雲端架構對於未來系統資料擴增，運算需求增加甚至系統功能的擴增擁有很高的彈性，並且搭配巨量資料處

理的概念針對資料作處理及分析。



資料來源：東海大學電子計算中心與資訊工程學系

圖 44、整體系統架構

(一) 硬體

1. WPM-100 無線數位電錶(圖 45)：

用來接收電能資料，無線傳輸施工簡便迅速，並採活電作業安裝電錶, 降低設備/機台停機影響。智慧電表每秒進行讀數取樣讀數值 (Voltage, Current, PF, Power Energy, Frequency, THDi, THDv)，精準度為 0.5S (含夾式或軟式比流器)，此外，多個數位電錶之讀數可同步取樣。其中的感測器提供的數據收集包括：電壓、電流、功率、功率因數、頻率等等，能透過無線的方式傳輸感測的資料，這些資訊收集後將即時傳回雲端的收集平台。

資料來源：東海大學電子計算中心與資訊工程學系

圖 45、WPM-100 無線數位電錶與電能感測器

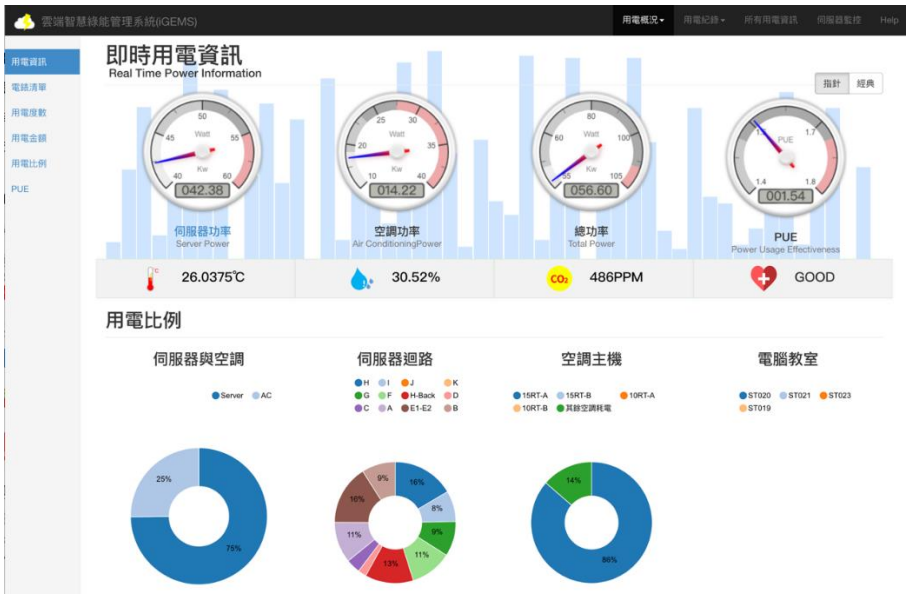
(二) 軟體

1. Apache Hadoop：是一款支援數據密集型分布式應用程式並以 Apache 2.0 許可協定發布的開源軟體框架。為此系統用來實作整體運算及電能資料的儲存。

2. Apache Hbase：從感測器上收集的資料將逐筆儲存至 HBase 資料庫中，但為提高資料處理效能，會在從 HBase 上將資料儲存在 Hadoop 提供的分散式檔案系統 HDFS 來儲存，利用 Hadoop MapReduce 的運算架構，透過分散式的運算方式來存取 HBase，來達到快速的資料分析及處理。

3. 雲端智慧綠能管理系統平台(iGEMS)：透過 HTML5, JavaScript, 以及 CSS3 為基礎，符合 RWD 網頁設計，並且透過 Bootstrap 框架來實作介面的部分。透過此平台，將資料蒐集、資

料監控和資料分析將電力資料加以處理後變成有意義的資訊，且提供報表或是圖像式的資訊(圖 46)。



資料來源：http://igems.thu.edu.tw/

圖 46、雲端智慧綠能管理系統平台介面

(三) 網路連結

1、 各裝置的網路連接

在數位電表中的感測器使用低功率 IEEE 802.15.4 2.4GHz (16 個頻段)無線傳輸，將資料傳輸上雲端後，雲端平台則是藉由 HTTP 的 POST 或 GET 請求來相互傳遞資料。

2、 網路協定

(1) IEEE 802.15.4：一項技術標準，定義了無線個人區域網路（low-rate wireless personal area networks , LR-WPANs）的操

作，旨在提供一種無線個人區域網路（WPAN）的基本底層網路層，該網路側重於設備之間的低成本，低速無處不在的通訊,也是是許多物聯網協議(例如 ZigBee 和 WirelessHART）使用的實體(Physical)層和媒體存取控制(Media Access Control, MAC)子層。

其相關 RFC 文件有 RFC 4919, RFC 4944：

i RFC 8137，在 RFC4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) : Overview, Assumptions, Problem Statement, and Goals 中提及，低功率無線個人區域網路（LoWPAN）包含符合 IEEE [IEEE802.15.4] 的 IEEE 802.15.4-2003 標準的設備。IEEE 802.15.4 設備具有短距離，低位元速率，低功耗和低成本的特點。使用 IEEE 802.15.4 協定的許多設備對於計算能力，記憶體或電力的可用性將受到限制。

ii RFC4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks 中提及，IPv6 封包傳輸的訊框格式以及在 IEEE 802.15.4 網路上形成 IPv6 鏈路本地地址和無狀態自動配置位址的方法。 其他規範包括使用共享上下文的簡單標頭壓縮機制以及 IEEE 802.15.4 網格中封包傳遞的規定。

iii RFC 8137: IEEE 802.15.4 Information Element for the IETF 中提及， IEEE Std 802.15.4 [IEEE802.15.4] 是 RFC 4944 [RFC4944]和其他文檔所引用的標準，它支持非常低成本和低功耗的通訊。該標準通過簡單有效的媒體存取控制層（MAC）定義了在許多不同頻寬中運行的眾多可選物理層（PHY）。

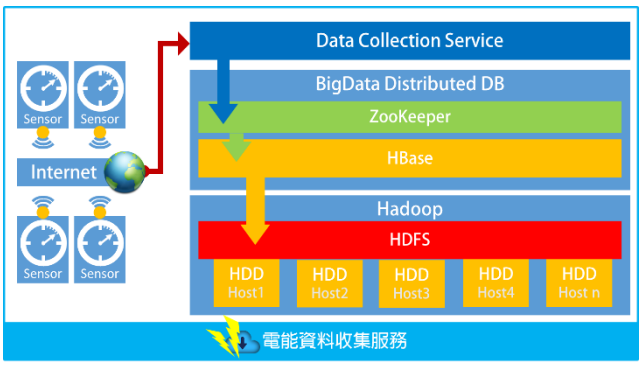
IEEE Std 802.15.4 定義了可用於以可交互運作的方式擴展 802.15.4 的資訊元素（IEs）。IEEE 802.15 分配號碼授權機構（Assigned Numbers Authority, ANA）管理資訊元素的註冊表。此文件提出了 ANA 的請求，以從該註冊表為 IETF 分配編號，並描述 IEs 如何格式化的設置以提供子類型。

(四) 如何使用服務

此系統以無線數位電錶與 PDU 對數據中心的設備進行用電資料收集，並搭配溫濕度與 CO2 環境資訊。將收集完的資料藉由無線傳輸的方式，上傳至雲端以利資料的監控、分析、與其他處理。

此系統的電能資料收集服務是一個 Java 的 Web Service，透過 Java 接收由網際網路傳送來的資料，並且將檢查感測器的 ID 是否為註冊於本系統的 ID，如果檢查結果為是才將資料收集暫存於記憶體中，這時程式將透過 ZooKeeper 與 HBase 做連線，透過 ZooKeeper 將暫

存於記憶體中的資料放進 HBase 相對應的資料表以及欄位中。以 HBase 來說收到要儲存的資料後，會將資料儲存於 HDFS 中，再由 HDFS 將檔案分散儲存於雲端叢集中的主機中，以備未來資料查詢及分析之用(如圖 47)。



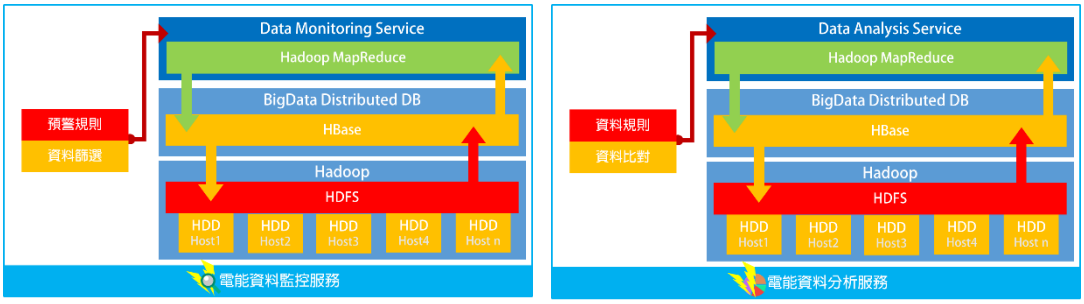
資料來源：東海大學電子計算中心與資訊工程學系

圖 47、電能資料收集服務

而監控部分，依照使用者的設定的監控頻率不斷掃描系統資料，本服務透過 Java 來運作，為了不對系統資源有太大的佔用，此服務在常駐監控時通常只會掃描近期或指定的少量資料，在使用者開啟監控頁面後，為了能快速收集篩選資料，本服務將透過 Hadoop MapReduce 做資料的篩選以及收集統計，透過 Hadoop MapReduce 的分散式運算存取 HBase，同時可由多部主機收集及統計資料，能大幅降低資料收集以及統計的時間，資料收集完成後將會透過網路應用程式回傳至前端使用者顯示(如圖 48 左)。

分析資料的部分因需要耗用相當大的系統資源，所以在接收到使

用者的規則後，透過演算法實現使用者的分析邏輯後，將會使用 Java 程式配發給 Hadoop MapReduce，透過 Hadoop MapReduce 的分散式運算存取儲存於 HBase 中的資料，在 Map 中針對資料做篩選以及基本的運算，並透過 Reduce 做資料的收集以及比對，完成後將會將資料送回網路應用程式端顯示於前端使用者。透過 Hadoop MapReduce 的分散式運算，將運算分散至雲端叢集中的主機，可以加速存取分析以及運算的速度，這在分析巨量資料時具有很大的優勢(如圖 48 右)。



資料來源：東海大學電子計算中心與資訊工程學系

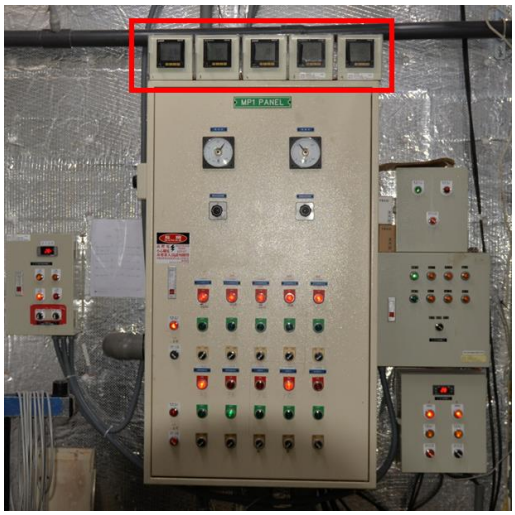
圖 48、電能資料監控服務與電能資料分析服務

四、應用與展示

以東海大學電算中心的機房為實驗場域，裝設各類感測器(如圖 49，圖 50)，實際搜集機房的溫度、用電、二氧化碳、電力使用效能等數據，當一行人進入機房時，電腦系統上顯示機房內的二氧化碳濃度數據明顯上升，從圖表也可看出因冷氣的開啟導致濕度的升高。在每日的用電數據中，看得出辦公室何時有人進入開啟冷氣，何時冷氣

關閉，以及當學校放假時電力消耗接近停止的情形。

圖 49、溫溼度感測器



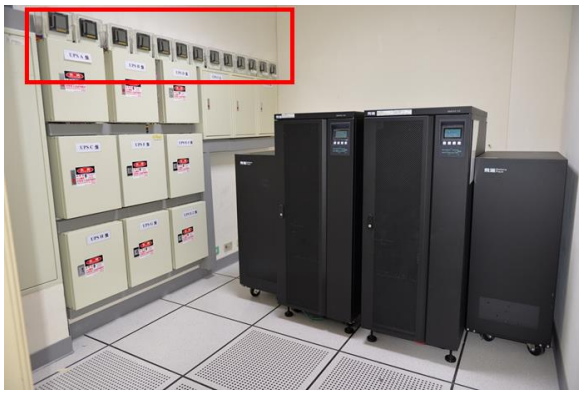


圖 50、安裝在機房的智慧電錶

五、得獎記錄

此系統於 103 及 104 年連續二年榮獲科技部工程司度電子資通領域應用型產學計畫「產學傑出獎」(圖 51)，在 TANet 2015 綠能通訊與綠能機房類榮獲最佳論文獎(圖 52)，雲端計算與大數據會議 CCBDA 2016 榮獲最佳論文獎(圖 53)， 105 年第二屆台中市低碳城

市榮獲傑出貢獻獎(圖 54)，且於科技部工程司產學計畫優良成果專刊上刊登過專文報導(圖 55)。

圖 51、科技部工程司度電子資通領域應用型產學計畫「產學傑出獎」

圖 52、TANet 2015 綠能通訊與綠能機房類最佳論文獎

圖 53、雲端計算與大數據會議 CCBDA 2016 榮獲最佳論文獎

圖 54、105 年第二屆台中市低碳城市榮獲傑出貢獻獎

工程科技通訊 Engineering Science & Technology Bulletin

雲端智慧綠能管理與服務系統

楊朝棟教授團隊、華楷光電、東海大學電算中心的合作

文/張萬珍

圖/張萬珍、沈宇權、計畫團隊

計畫團隊合影。（由左至右）顏尹婧同學、黃應沼副總、楊朝棟教授、陳昆良組長、沈宇權同學。

現代人的生活離不開網路，東海大學電算中心服務全校近兩萬名師生，任務繁重，網路組陳昆良組長形容，每天的日子「都好像在打仗」。

電算中心的機房支持全校師生的資訊系統和雲端應用服務。伺服器全天運作，節能和冷卻是管理者的任務和挑戰。

東海大學資工系楊朝棟教授兼任電算

42 2015年10月NO.148

eTop 工程科技推展平台 登入

工程科技推展中心

第 期電子報

搜尋 研討會補助申請 學門網站 專案網站 電子報 媒合平台 虛擬展場 留言板

新春開工，看這篇就對了~雲端用電資訊分析之巨量資料儲存與處理平台建置

返回

分類：產學快訊

發行期別：

發佈日期：2016-02-16

附件：

雲端用電資訊分析之巨量資料儲存與處理平台建置

文/計畫團隊、張萬珍 圖/計畫團隊

博雅雲展示會智慧綠能機房啓用儀式

圖 55：科技部工程司產學計畫優良成果專刊 148 期與專文報導

第四節　行的物聯網 – 中華電信智慧停車物聯網

一、現況與挑戰

台灣為地狹人稠的地方，在都會地區，民眾停車位常常一位難求，可能繞了老半天還找不到，經常造成駕駛人虛耗時間且增加油耗的尋找空位，間接提升空汙嚴重程度。而道路上也因停車場的滿位或是柵欄，繳費機的故障，等待的車輛造成了交通阻塞。

在觀光地區，也因停車場車位少之又少，使簡易的礫石地畫了格子因而成為了私有停車場，缺乏管理的簡約配置引來駕駛人的擦撞怒罵或大排長龍。

國道服務區每逢假日車流量大，停車問題常是很多用路人的困擾，提供足夠、甚至免費的停車位雖是讓城市順暢運轉不可或缺的一環，但這些停車場還存在最根本的效率問題：大部分的停車場其實根本沒有被充分利用。

早期在 2011 年時，停管處便提供路外（馬路以外）的停車位動態資訊，如學校公有地下停車場的剩餘車位，但臺北市停車管理處機電科長李世芬表示，民眾停車的習慣，還是偏好優先尋找路邊停車位，因此如何即時提供路邊停車位動態資訊成為挑戰。

二、願景

傳統的停車場管理依賴大量的人力，開單員定期的巡場，使用

PDA 開單，在開單的同時也以人工的方式確認停車場的使用狀況，台北市政府先前已開發了「北市好停車」的 APP 用來知道哪裡有停車空位，但因還是以傳統人力方式巡場，所以以這種方式來做路邊停車的車位動態來說，相對不夠即時，特別是在相對熱鬧的地區，車輛的流動率大，駕駛也難以掌握特定路段是否有空位。

而現在因網路技術相當發達，台灣中華電信積極布局 5G 各種智慧化應用，與交通部高速公路局聯手，在國道服務區建立「智慧停車資訊服務系統」，也有與城鄉共同合作，將主要旅遊區導入智慧停車方案，將人、路、車三者透過 5G 物聯網技術進行無縫銜接，提供即時交通資訊。

(一)　量化或質化目標

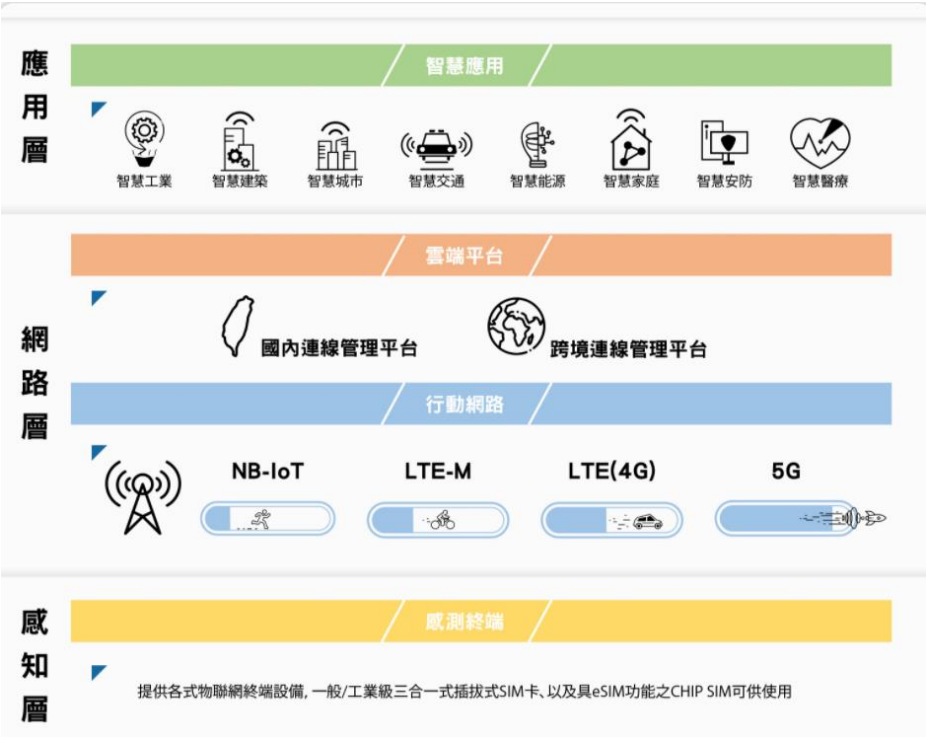
中華電信 ITS(Intelligent Transportation Systems)智慧運輸服務團隊，整合通訊、電子、導航、資訊、電腦及控制等先進科技技術，為降低用路人因尋找路邊停車位所造成交通衝擊，各縣市路邊停車資訊服務整合物聯網技術、地磁感應、行動通訊、CMS(資訊可變標誌 Changeable Message Sign)等技術，提供即時路邊停車位及路外停車場空位狀況，降低用路人虛耗時間、車輛油耗等問題，提高停車方便性。

三、服務架構

以物聯網架構來說，在感知層部分設置各感測設備如：地磁感測

或攝影鏡頭，而在網路層部分則使用 NB-IoT 技術並連接雲端平台，到了應用層則應用到智慧停車場部分。

在民眾使用部分則是可透過手機或電腦的方式至網頁上查詢資料，或是使用手機在 APP 上得知想要的資訊。



資料來源：https://www.cht.com.tw/home/Campaign/M-IoT/index.html?utm_source=google&utm_medium=cpc&utm_campaign=eb_iot&gclid=CjwKCAjwrcH3BRApEiwAxjdPTWgfpofJJ52IvLxONpF70jyO-nHrbFbMRaLT3XKlhFqrUs3c8df2zhoCTyQQAvD_BwE

圖 56、智慧停車場物聯網架構

(一) 硬體

- 地磁感測器：當車輛停放至停車格時，將產生磁場變化，地磁藉此感測車位是否被占據。

資料來源：

https://www.cht.com.tw/home/campaign/smartcitycase/SmartTraffic/index.html

圖 57、地磁感測器

- 柵欄機：可以透過紅外線或者是利用車牌辨識，使機器感應到車輛後，讓柵欄自動升降。
- 智慧看版：透過「智慧資訊可變標誌」（CMS）呈現停車格數量。

資料來源：

https://www.cht.com.tw/home/campaign/smartcitycase/SmartTraffic/index.html

圖 58、智慧看板

(二) 軟體

1. CMP 連線管理平台：提供物聯網連線管理服務，降低通信管理維運成本，讓客戶快速取得連線狀態、流量、門號啓停、帳務查詢及障礙告警等功能。

2. 智慧停車管理平台：提供各式模組化功能，如即時停車資料查詢、數據報表智慧分析、車位／設備／帳號管理、API 串接…等應用服務。

圖 59、智慧停車管理平台

(三) 網路連結

1、 各裝置的網路連接

透過安裝於每格停車位的智慧感測器進行偵測(地磁在席偵測技術)，當因車輛進出而造成磁場變化時，即透過 NB-IoT 通訊網路傳送至雲端計算，將停車位地磁感測設備 所收集到的即時資訊傳遞至智慧停車管理平台，使管理單位可發佈車位資訊至道路兩旁建置的數位電子看板和停車資料查詢網頁，提供民眾用最簡易的方式快速取得即時路況、交通宣導或相關訊息等。

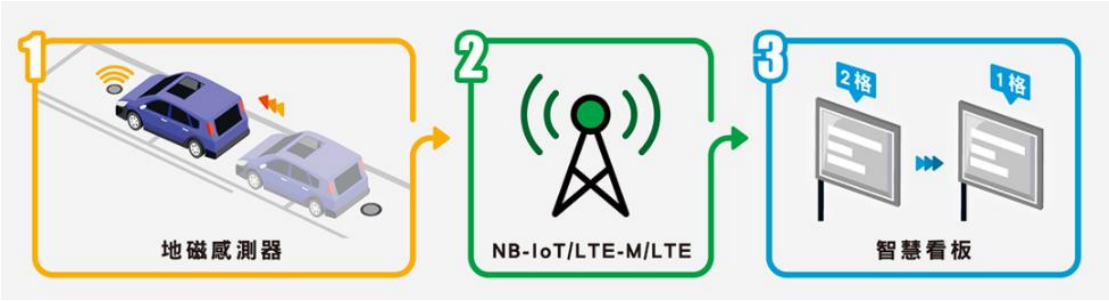


圖 60、停車場中裝置間的連接

若是要從平台上觀看任何即時資訊或是分析資訊，則藉由行動裝置連上 4G LTE 使用 APP 或是網頁或是一般電腦藉由有線網路連接上網至網頁操作。

2、 網路協定

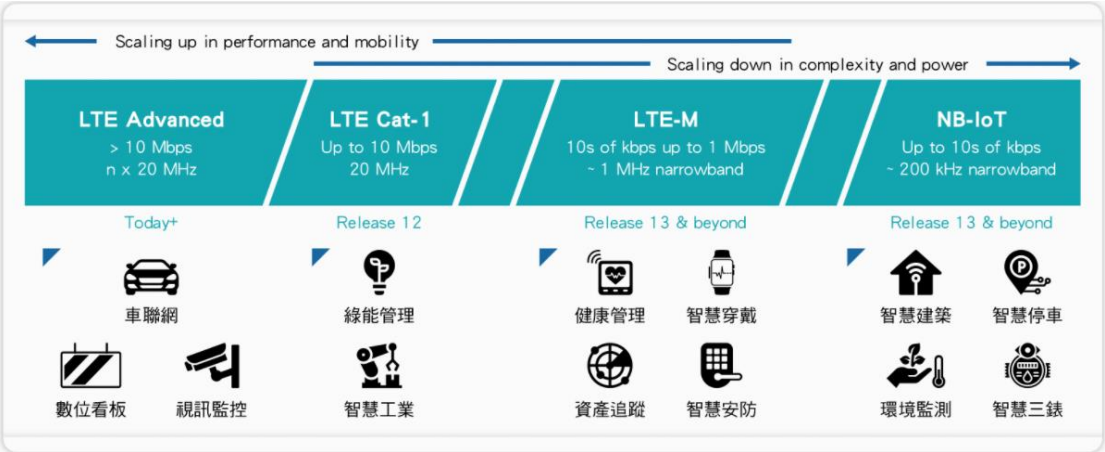
智慧停車的管理平台中，欲從手機 APP 觀看或是電腦操作網頁觀看資訊的話，皆由有線或無線網路的方式，網頁藉由 HTTPS 的方式傳輸。

而在底層，則使用 NB-IoT 技術，現今行動物聯網無線技術除了

有 4G LTE 外，3GPP 組織依據不同裝置的需求，發展出低功耗、低成本、廣域覆蓋及大量終端設備連結等特性的窄頻物聯網通訊協定(Narrow Band Internet of Things,NB-IoT)，使現有 LTE 頻段技術中，直接共享 4G 頻段網路，透過已建置的 4G 基地台，直接升級韌體版本為 NB-IoT/Cat-M1，藉此達到信號全台覆蓋。依據優勢，NB-IoT 較適合在少量封包傳輸設備、非即時資料傳輸應用，反之，Cat-M1 因可維持基站交握，對即時性資料傳遞與中量封包傳輸，更可適用在移動物件追蹤等特色產品。NB-IoT 適合在少量封包傳輸設備、非即時的資料傳輸應用。

LTE-M 可讓移動的設備持續與不同基地台的訊號做連接，在即時性資料傳遞與中量封包傳輸可以提供最佳的通信品質，適合在移動物件追蹤等應用(圖 61)。

而 M-IoT 的優勢為長效電池時間、低成本中短、低成本佈建、全面覆蓋及海量終端支援。



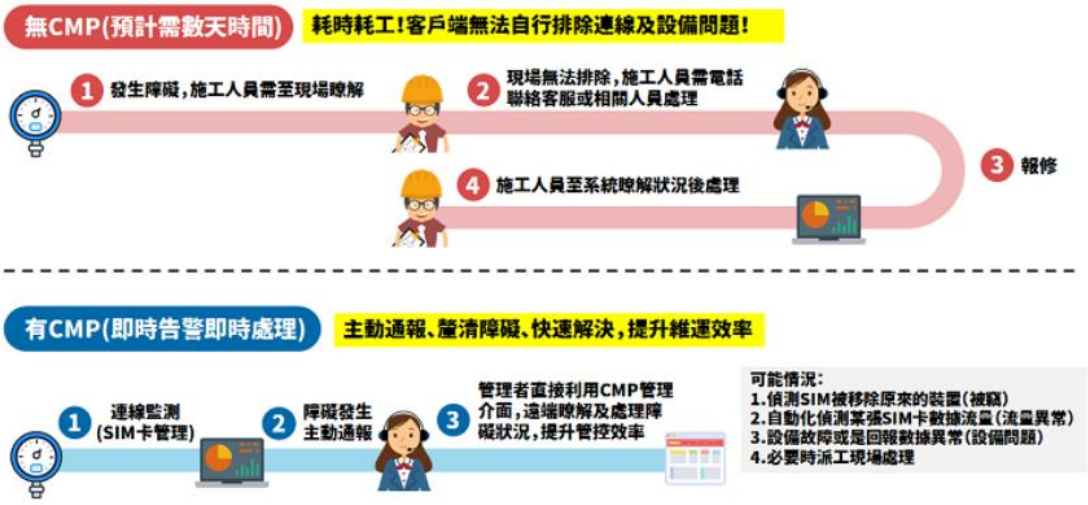
資料來源：https://www.emome.net/channel?chid=723

圖 61、物聯網網路應用

而在 RFC 文件當中與 NB-IoT 較相關之文件為 RFC 8376：Low-Power Wide Area Network (LPWAN) Overview，此為低功耗廣域網路(LPWAN)概述，文件當中提及幾項 LPWAN 技術，而 NB-IoT 就在其中，當中提及 NB-IoT 的概述，如具體目標、其傳送資料格式、傳送方式與限制、然後該如何部屬…等。

3、 網路安全的考量

因為過去物聯網服務曾遭遇設備連線異常、成本控管、安全漏洞及營運成本問題，故中華電信為協助企業客戶隨時掌握 IoT 設備的連線狀態，確保物聯網服務的運作，中華電信自主研發推出具電信資安等級的物聯網連線管理平台(Connectivity Management Platform, 簡稱 CMP)，CMP 支援客戶 IoT 設備之網路連線自主管理功能，如連線狀態、異常通棒、服務內容調整…等以提升客戶為運效率，然後也提供 IoT 設備連線狀況自主管理，簡化為運流程、提升設備、降低成本。

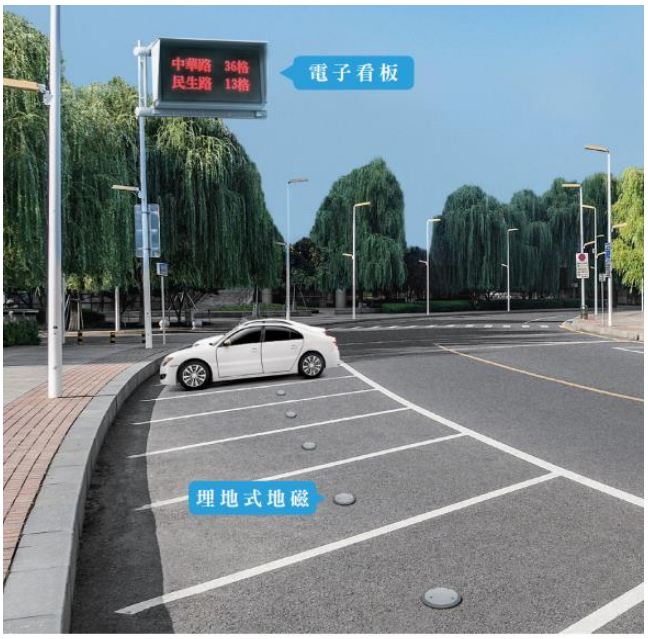


資料來源：https://www.emome.net/channel?chid=723

圖 62、CMP 管理平台應用案例

(四) 如何使用服務

在停車格佈建「地磁式車輛偵測感應器」，每當車輛停放時，將產生磁場變化，地磁藉此感測車位是否被占據，之後透過 NB-IoT 通訊網路將車位停車狀態傳送至管理平台，紀錄車位狀態與各車道剩餘車輛資訊，即時傳送至道路旁的 LED 指示看板。



資料來源：https://www.cht.com.tw/home/cht/-/media/Web/PDF/BusinessArea/6IOTparking.pdf

圖 63、智慧停車示意圖

四、應用與展示

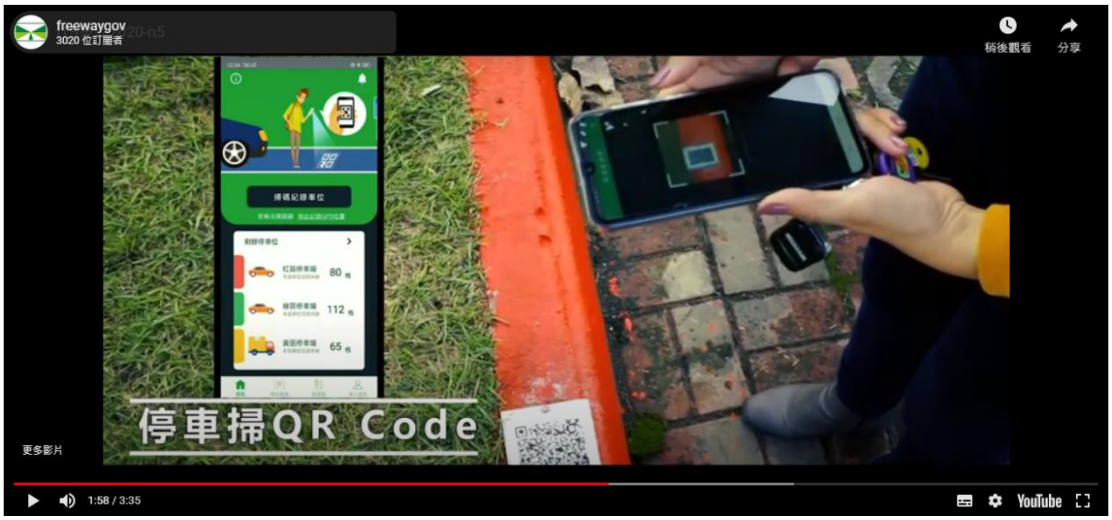
- 國道服務區：主要透過地磁式車輛感測器(透過物聯網 NB-IoT 通訊技術)、電子標籤偵測器、自動車牌辨識系統與事件自動偵測系統等偵測設施，搭配平台系統之資料分析，提供適時的導引，將建議停車資訊透過大型看板顯示於服務區入口處與各停車分區入口，同時在停車分區內提供車席導引數位顯示供用路人參考，藉以協助用路人迅速找尋停車位，減少因停車資訊不明確，造成之車輛繞駛、交織行為，進而影響服務區內之交通順暢與安全，甚至因服務區內湧入過多車

輛而影響至主線車流，開發智慧尋車系統，使用 APP 加上 GPS 定位紀錄車輛位置，解決忘記車輛停放處知困擾，結合服務區既有服務創新加值，提升服務區的服務效率與品質。

東山服務區

資料來源：https://transport-curation.nat.gov.tw/museum-ITS2020/result_5.html

圖 64 東山服務區智慧停車看板



資料來源：https://transport-curation.nat.gov.tw/museum-ITS2020/result_5.html

圖 65 東山服務區智慧尋車系統

- 縣市政府：中華電信和宜蘭縣政府合作的「宜蘭縣路邊停車

資訊服務」，運用 NB-IoT 通訊技術，在宜蘭市、羅東鎮、礁溪鄉與頭城鎮，埋設 9 百多個地磁感應器，讓停車數據可以即時回傳宜蘭停車資訊平台，再以手機或重要路口的 CMS（Changeable Message Sign）智慧型顯示看板，即時提供駕駛人最新的停車資訊。智慧停車系統可在不同停車地段預設告警值，例如車位快滿時，就會以 LBS（Location-Based Service）訊息適時通知民眾停車格滿載狀況，提早改道，減少民眾尋找車位的時間。民眾一旦收到 LBS 訊息後，可以透過手機上網連結上智慧停車系統，電子地圖上會把車主周邊的停車資訊清楚顯示，將找車位的時間縮短。

資料來源：https://www.wealth.com.tw/home/articles/22956

圖 66、宜蘭縣停車資訊服務

- 開單業者：降低開單人力成本/機動調度集績效管理、提升人

員開單效益及管理範圍。

- 大型戶外停車場：改善停車動線不明缺點，加快車輛出/入場速度，優話訪客停車體驗，提高車位轉換率。

第五節　育的物聯網 – 工業 4.0 模擬研發實驗室

一、現況與挑戰

當今全球兩大主題是「雙 E」，那就是教育(Education)和經濟(Economics)。德國官方認為 2030 年將完全進入「工業 4.0」的時代，也就是“智慧製造”將徹底實踐。台灣長期重理論輕實踐，導致國人科學素養普遍低落，反觀，德國重視早期性向確認及技職教育規劃，許多跡象顯現，教育品質影響經濟發展甚鉅。

在台灣面臨到的教育挑戰是，沒時間讓孩子做興趣的自我探索，因為現今社會的發展導致家長覺得讓孩子上好學校，畢業後可以找份好工作就不會有太多問題，但過於古板制式化的教育並無法激起學生的熱情，也無法讓學生在人生最有活力、好奇心最旺盛時，找到屬於自己的興趣。

二、願景

現今的教育與社會強調「國際化」、「整合化」之類的形容詞，而在美國，教育界最熱門的關鍵詞為「STEM」，四個英文字的縮寫分別代表科學(Science)、科技(Technology)、工程(Engineering)及數學(Mathematics)。而 STEM 教育熱門的原因在於在未來越來越複雜的社會上，知識已不再有價值，因此教育推動的目的為，必須從單純的「知識傳遞」，更進化為讓學生「學以致用」。

(一)　質化或量化目標

STEAM 5 大精神包含：跨領域、動手做、生活應用、解決問題、五感學習。教育部在 12 年國民基本教育課程綱要總綱的「核心素養」中表示：素養指人在適應現在生活和面對未來挑戰時，所應具備的知識、能力和態度。與 STEAM 所倡導的學習精神符合。

而在台灣某幾間大學也跟進了 STEM 教育，使用了慧魚工程積木組，建立實驗室及開設課程，針對工業 4.0 這個題目來「從中學，學中做」，德國工業 4.0 科學研究聯盟指出（Industry-Science Research Alliance）：「要實踐工業 4.0，首重工業模擬平台。」

在日常生活中不可能隨時都有辦法接觸到整個工廠的架構，就算可以接觸到也較難從大型機器中，學習到整體流程的概念與操作，所以可以從小小的模組透過教學認識從下單、製造與傳輸，也模擬工業數位化的過程。

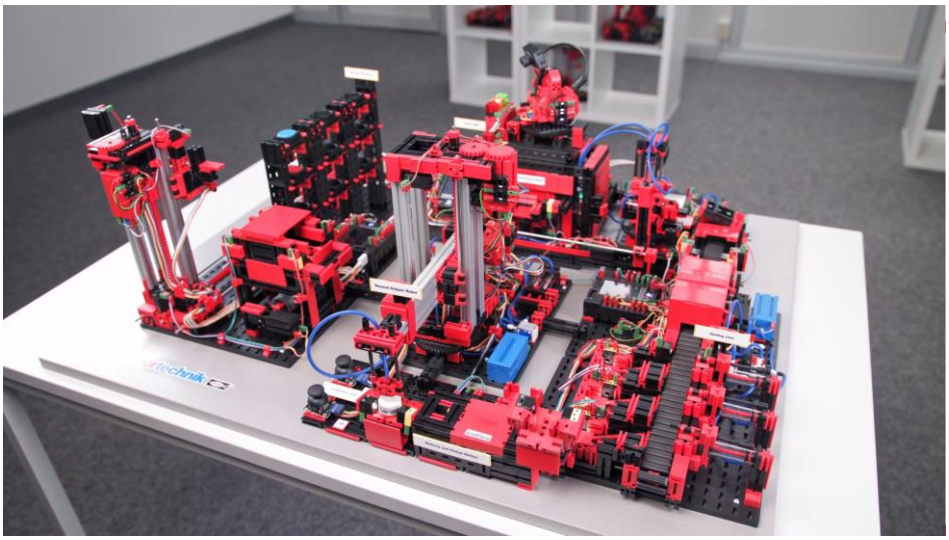
與慧魚工程模組進行工程與生產線模擬與開發的企業有數多家如：Siemens, Audi, BMW, 台灣漢翔航太等。而在台灣則是由柯達科技作為總代理商，柯達科技執行長宋德震先生也以投身機器人教育 20 年為例指出，如何培養孩子的跨領域素養，是件值得思考的課題。

三、服務架構

此為一套自動化模擬工廠(圖 67)，其中包含各種模組如：顏色分

類，複合式熱爐，高架倉儲，真空機械手臂等，充分展現工廠生產流程、端與端的溝通、生產數據蒐集與分析。

柯達科技和德國工業巨人西門子(Siemens)合作，把產線縮小，且做到「感測－整合－智能判斷－回應」，所占空間極小，能模擬多個工作站，並有 IoT 的功能。雲端只是一個設備，重要是底層的的機械平台要能互連，提供了一個跨平台學習，及進入工業 4.0 的最佳入門。



資料來源：柯達科技實業有限公司 產品型錄

圖 67、自動化模擬工廠

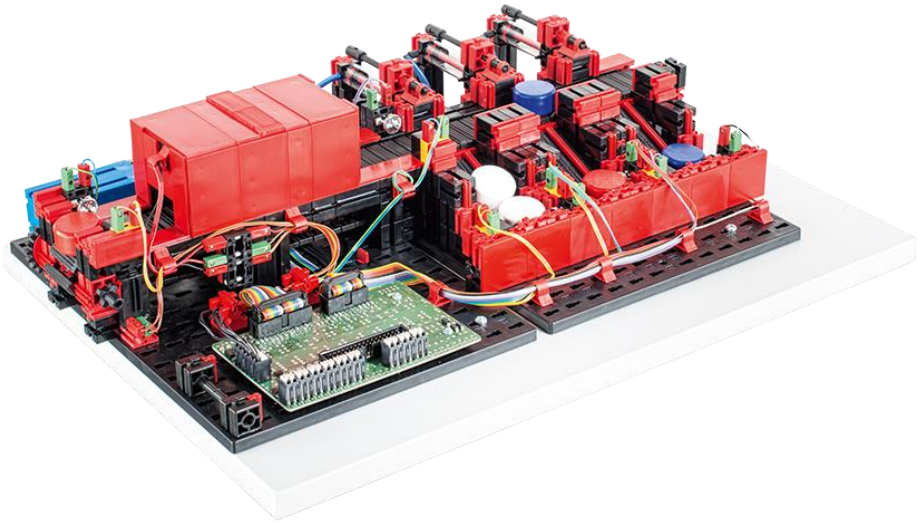
(一) 硬體

其中提出幾項硬體設備來做為介紹：

1. 顏色分類與檢測生產線(圖 68)

當物體放到輸送帶上時，經過光閘判定是否有物體在輸送帶上，若有物體，則輸送帶開始運送物件，當顏色感測器測到輸送帶上

的物件時，會依物件顏色的不同，氣缸會作動，把不同顏色的物件推到專屬的位置。

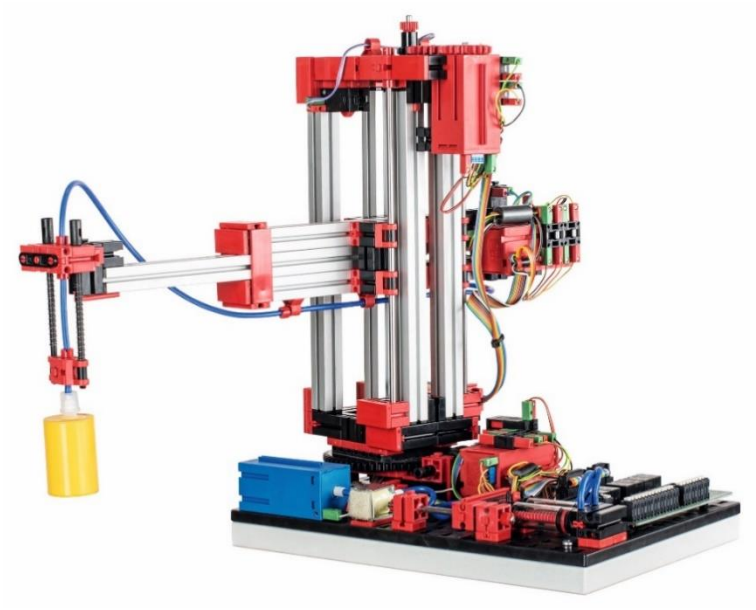


資料來源：柯達科技實業有限公司 產品型錄

圖 68、顏色分類與檢測生產線

2. 真空吸物機械手臂(圖 69)

機器透過限位開關來決定是否啟用，使用步進馬達來作移動幅度的計算，可以快速及精準的動作，把物件放置在 3D 的環境中，常與其他工作站同時使用。

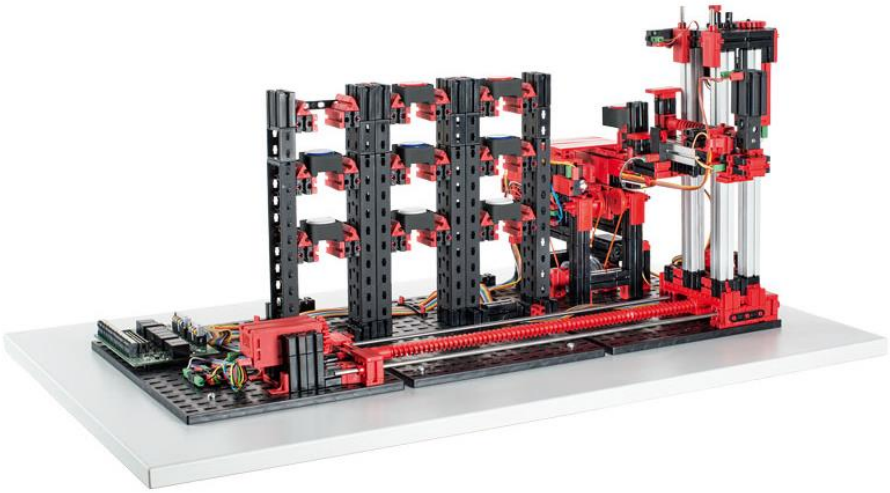


資料來源：柯達科技實業有限公司 產品型錄

圖 69、真空吸物機械手臂

3. 自動化高架倉儲系統(圖 70)

此模組通過限位開關來控制機器的啟動，並利用步進馬達來計算移動的幅度，利用傳動機構、各感應器的偵測及程式的控制，把物件存取在九格貨架框上。

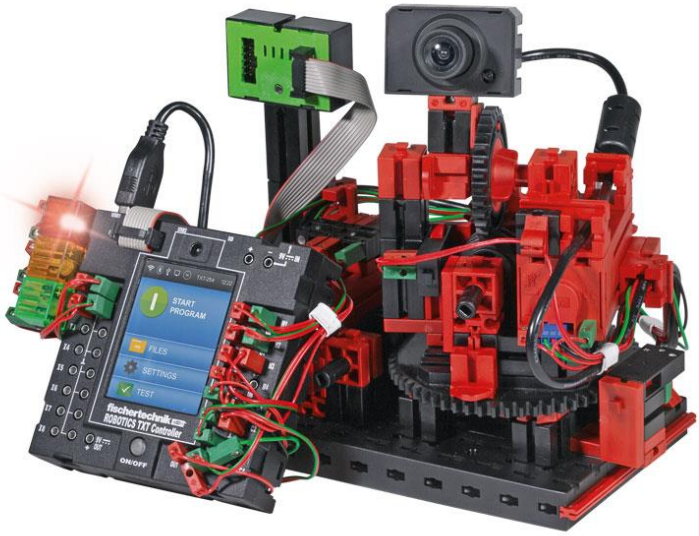


資料來源：柯達科技實業有限公司 產品型錄

圖 70、自動化高架倉儲系統

4. IoT 實驗模組(圖 71)

此模組有一個可轉動的攝影鏡頭、環境感測和其他感應器，可測量溫度、濕度、氣壓、空氣品質、音量及環境光源亮度等。主要功能為模擬工廠監控設備，隨時注意廠內狀況。



資料來源：柯達科技實業有限公司 產品型錄

圖 71、IoT 實驗模組

5. 3 軸機械手臂(圖 72)

利用限位開關控制啟動，能精確且快速的動作，並將物件放置或夾取於 3D 環境中，其活動範圍從軸 1 可 180 度旋轉、軸 2 可前/後運動距離 90mm，軸 3 可上/下運動距離 150mm，此機器可透過脈衝感測器來對力量的脈衝作出及時反應。

資料來源：柯達科技實業有限公司 產品型錄

圖 72、3 軸機械手臂

6. 傳送帶(圖 73)

模型長度 275mm，輸送帶可以自由拼接成任何想要的長度，其中模擬物件(長 29mm、高 25mm)可在傳送帶上被來回傳送。

資料來源：柯達科技實業有限公司 產品型錄

圖 73、傳送帶

7. TXT 雙核心控制器(圖 74)

由德國原廠開發的 RoboPro 流程圖軟體，是標準工業程式語言之一，符合人的直觀邏輯，簡單易懂的介面讓學習者更容易完成程式設計。此控制器可經由 Micro SD 卡擴充，且有彩色觸碰螢幕、無線裝置、紅外線二極管針對慧魚控制設置發射器，設有 USB 端口、攝影機插槽、控制器擴充。

其開發系統是基於 Linux 的開源操作系統，作業軟體有 ROBO Pro、C-Compiler、PC-Library、Scratach and many others，資料傳輸可透過 USB、藍芽或 WLAN 連接到智慧手機、電腦或平板。

TXT 控制器可搭配原廠出廠之各類感測器或從電子材料行取得，TXT 控制器也可以連接到雲端伺服器，在那裡被感應器搜集的數據不僅會被保存，還可以被檢索。因此，透過面板顯示可監控各種傳感器數據，並且可以控制攝影機的動作，如果環境中的訊息超過設定值，控制器的液晶螢幕會顯示異常，或發出警示訊號。

資料來源：柯達科技實業有限公司 產品型錄

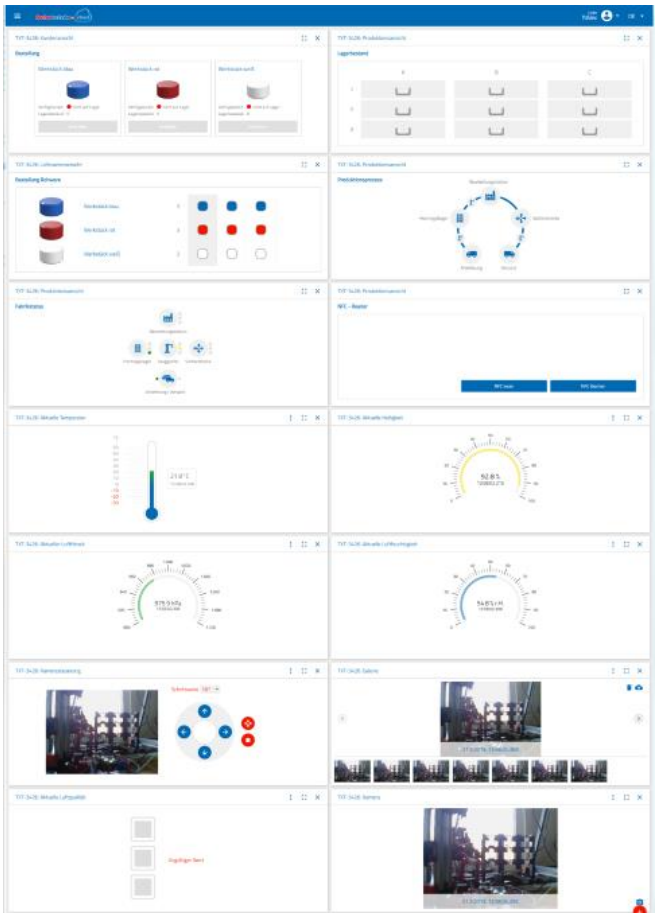
圖 74、TXT 雙核心控制器

(二) 軟體

1. fischertechnik-cloud

慧魚訓練與模擬工業 4.0 智慧工廠，能透過 WIFI 路由器與慧魚雲端(圖 75)連結，使用雲端前需至 www.fischertechnik-cloud.com 建立個人帳號並登入。慧魚雲端伺服器架構於德國，並嚴格諄手歐盟資訊儲存相關條例，使用業界標準”OAuth2”密碼驗證技術，保護個人資料存取。此系統的介面提供三個觀點：客戶端觀點，供應端觀點及製造端觀點，透過介面可以顯示生產區域的環境參數如:空氣品質、溫濕度、氣壓等。介面主要內容包含：網路商店與購物車，用戶可藉由此介面模擬下單訂購，並追蹤目前購物狀況，供應端介面主要顯示下單狀況與出貨進度，但也可操作生產

線上的監控攝影機，製造端介面則為：工廠狀況、出產進程、倉庫狀況，NFC/RFID 感應數據查詢。



資料來源：https://www.fischertechnik.biz/fischertechnik-Education/fischertechnik-training-factory-industry-4-0.html

圖 75、fischertechnik-cloud

2. TXT 控制器上的控制面板

在模擬工廠上所使用的 TXT 控制器連接在工廠的各個模組上，透過 MQTT(MQTT:Message-訊息、Queuing-順序、Telemetry-遙測、Transport-運送)達到彼此間的互動。

TXT 控制器的軟體是 C/C++ API 程式介面，並已就緒啟動狀態下

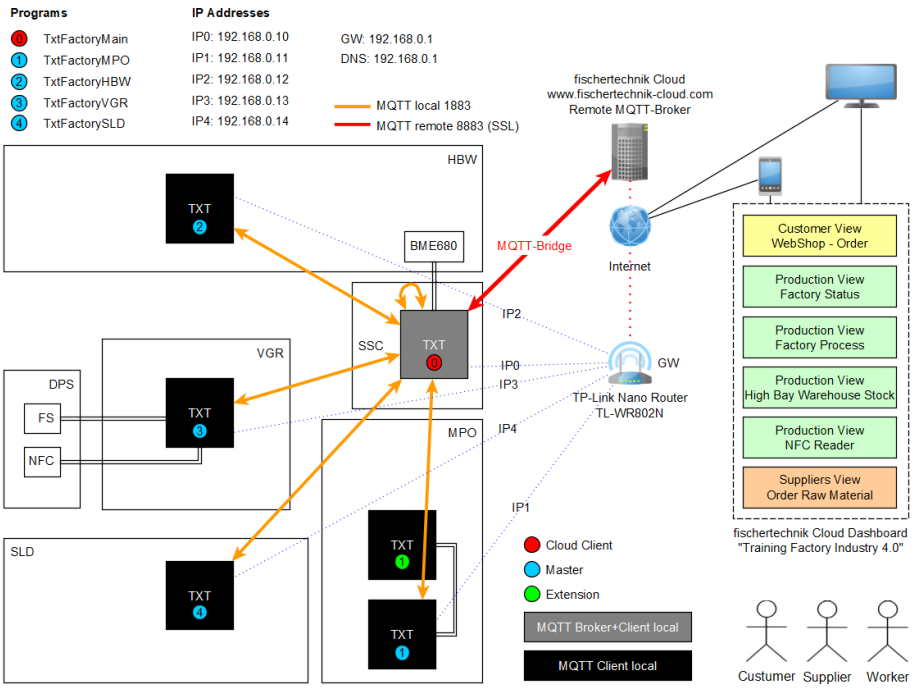
載到控制器上，Github 上提供相應的 C/C++和 API。

(三)　網路連結

1、 各裝置的網路連接

當一個模擬工廠組合好後，以下圖為案例說明，各個站區皆配有一台 TXT 控制器，TXT 控制器具有 Bluetooth/WiFi RF module: BT 2.1 EDR+ 4.0, WLAN 802.11 b/g/n，其資料傳輸可透過 USB、藍芽或 WLAN 連接，而控制器與控制器間使用 MQTT 的協定進行傳輸，而在這當中站區分別有 SSC：帶攝影機的感測器區域、HBW：高架倉儲、VGR：真空吸物機械手臂、DPS：派送站、MPO：複合式熱爐生產線及 SLD：顏色分類與檢測站。

其中以 SSC 為 MQTT Broker(代理人)作為一伺服器軟體可藉由 MQTT 協定接收其他本地用戶端的資料並將兼作雲端用戶將資料也藉由 MQTT 的協定傳輸傳送到遠端 MQTT Broker(代理人)上，而此遠端伺服器軟體即為 fischertechnik-cloud，可藉由網際網路傳送資訊到手機或平板上；而其他本地用戶端也可透過無線傳輸的方式經由閘道器透過網際網路直接將資料傳送至手機或平板上進行查看。



資料來源：https://github.com/fischertechnik/txt_training_factory

圖 76、各裝置間的連接

2、 網路協定

MQTT(Message Queuing Telemetry Transport) 訊息佇列遙測傳輸：於 1999 年由 IBM 發明，物解決在狹窄的網路頻寬與微小電力耗損的前提下，提供一個輕量、可靠的二進制通訊協定。於 2014 年正式成為開放的 OASIS 國際標準。適用於 M2M 和 IoT 環境。

MQTT 控制訊息最小只有 2 位元組的資料。最多可以承載 256 Mb 的資料。有 14 種預定義的訊息類型用於：連接客戶端與代理、斷開連接、發布資料、確認資料接收、監督客戶端與代理的連接。在資料傳輸上基於 TCP 協定，而變體 MQTT-SN 則基於 UDP，用在

藍牙傳輸。

3、 網路安全的考量

MQTT 預設埠為 1883，加密的埠為 8883。所以通過雲端連接的資料傳輸會經由 8883 埠加密傳送，而藉由閘道器連接至網際網路的皆通過 HTTPS 的方式利用 SSL/TLS 來加密封包在送出。

(四) 如何使用服務

此案例透過慧魚工業模組，先將模擬工廠架設好後，即可使用，在教學過程中，可先透過慧魚雲端，使學生體驗客戶下單，及工廠接到訂單後應該如何開始作業，在工廠作業過程中，使用自動化的流程，故需事先在 TXT 操作器中寫好每個站點所需的操作，然後在工廠中的各種情況可透過攝影機來做監控，在架設攝影機的模組處也設有環境感測器，整個模擬工廠中感測器所接收到的資料可經由 TXT 操作器藉由無線傳輸的方式傳上雲端。而在雲端平台上，將所接收到的資料經由分析，可在平板、電腦或手機上有圖表式的呈現。

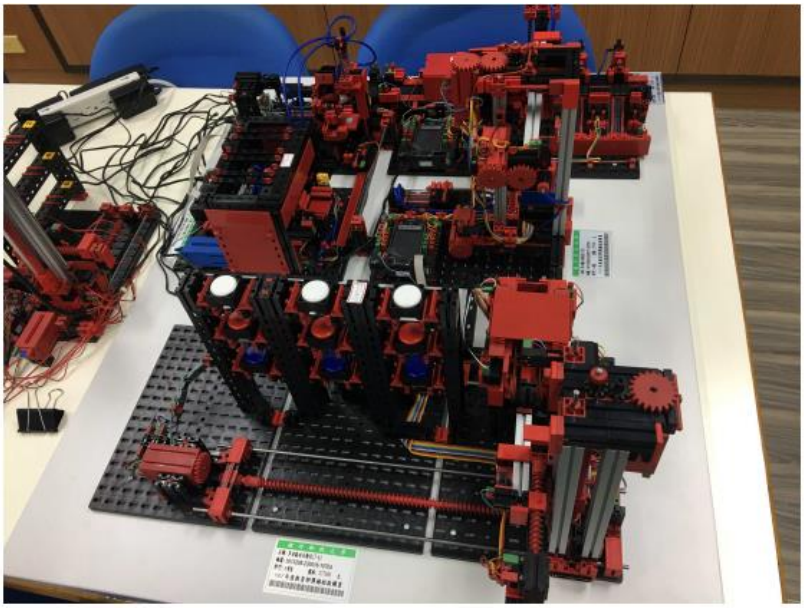
四、應用與展示

1. 元智大學工管系為提升學生在「工業 4.0」時代來臨時，所欠缺的基本知識與對應能力，因此購置了德國慧魚專業模組，藉由教學與互動來達到了解整個工廠系統的操作與基本的架構了解。

資料來源：http://www.iem.yzu.edu.tw/chinese/newsletter/035/#active2

圖 77、元智大學工管系工業 4.0 教學

2. 健行科技大學工業管理系為因應工業 4.0 之未來發展，設置了一實驗室旨在培養新一代工業管理相關人才，教導學生智能管理的觀念及相關技能。

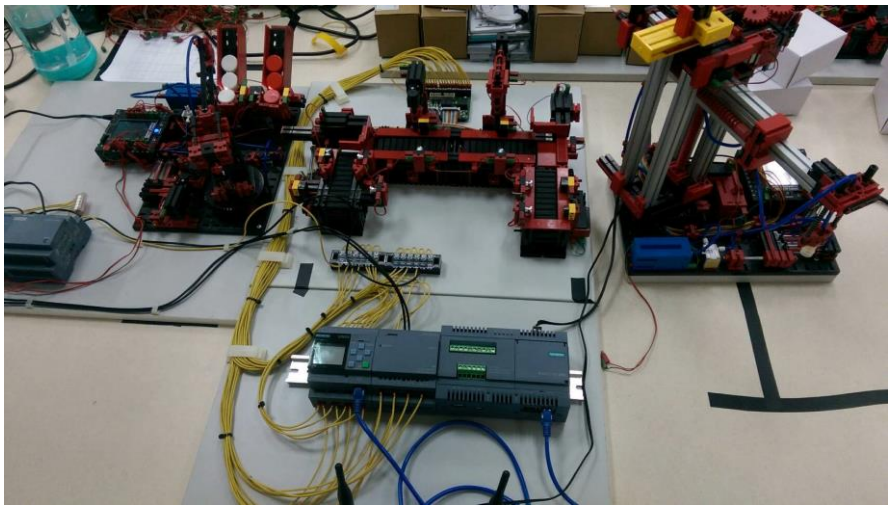


資料來源：

http://aps2.uch.edu.tw/asp_work/techcoop/tech/1004/upload/mresult/1397/C502 智能管理實驗室-106 學年度成果報告_1070827_.pdf

圖 78、健行科技大學實習(驗)室

3. 2017 年 11/3 到 11/5 在華山藝文中心展開 Maker Faire，主展題由柯達科技和西門子共同合作，使用最小的空間，做出一個生產流水線(圖)，並結合 IoT 搜集所有生產資訊。



資料來源：https://www.facebook.com/kotecstem/

圖 79、模擬生產線

五、參展紀錄

此教育模組放置在台灣教育科技展官網上，有簡短的產品亮點與產品簡介。

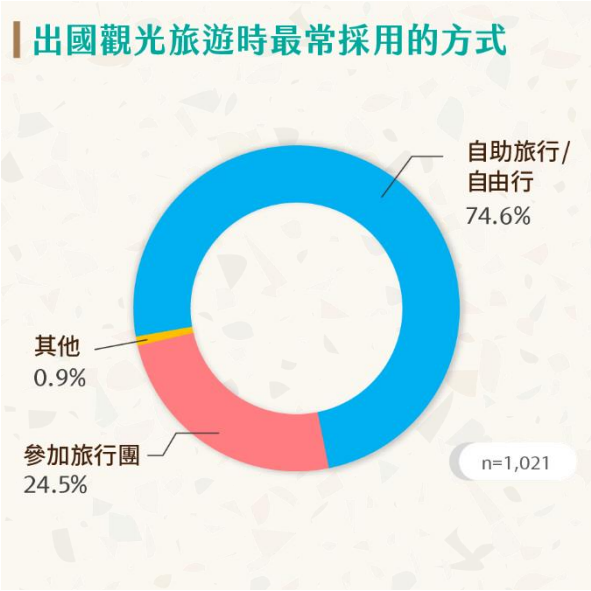
資料來源：https://www.itmonth.org.tw/edTech/product-detail/168?PHPSESSID=1ves9co6al22hnatmp2vipokv1

圖 80、台灣教育科技展官網

第六節　樂的物聯網 - 智慧導覽與實境遊戲平台

一、現況與挑戰

近年來旅遊市場的規模不斷擴大，隨著人們生活水準的不斷提高，旅遊不再是一件奢侈的事情，近幾年來，曾有觀光旅遊的民眾當中，有近 75%的民眾會採取自助旅行的方式進行國外觀光(圖 81)，隨著廉價航空的擴大、線上旅行社與旅遊產品比價平台的興盛，及行動應用服務的發展成熟，大幅降低自助旅行的門檻，而參加團體旅行的民眾，也可能因旅遊導遊人力資源有限，成本相對高，而服務品質也參差不齊，故使得自助旅行的比例逐年上升。

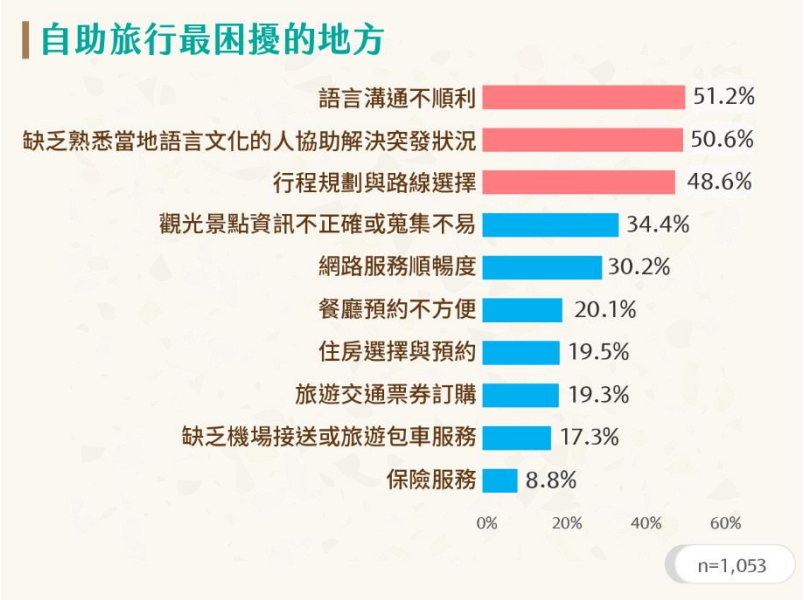


資料來源：http://www.twtrend.com/share_cont.php?id=68

圖 81、出國觀光旅遊採用之方式

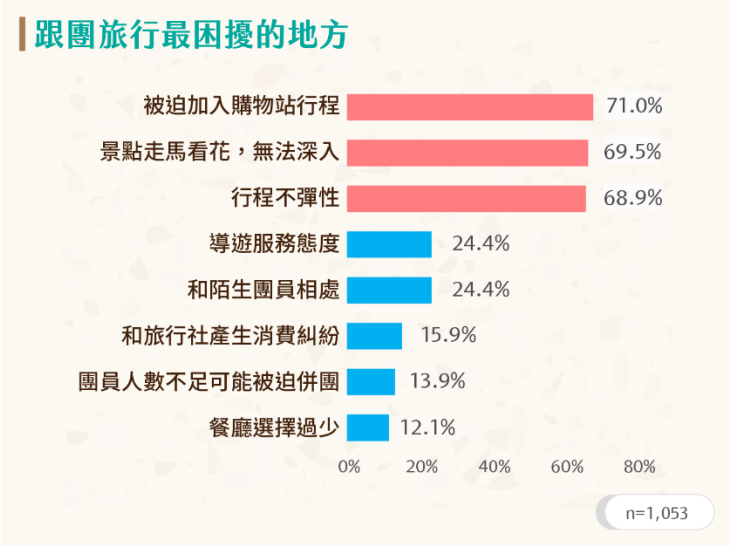
但在自助旅行的過程中，語言溝通困難，不熟悉當地語言文化或

是路線規畫都會造成自助旅行者的困擾(圖 82)；但另一方面，若是跟隨平價的旅遊團大多都會安排特定商店的購物行程，也因需跟隨團體行動，所以行程較不彈性，且因時間限制所以大多都是走馬看花，無法深度旅遊(圖 83)。



資料來源：http://www.twtrend.com/share_cont.php?id=68

圖 82、自助旅行困擾之處



資料來源：http://www.twtrend.com/share_cont.php?id=68

圖 83、團體旅行困擾之處

且隨著當今遊客消費逐漸趨向個性與自由，對旅遊品質也有了更高的追求，所以越來越多自由行旅客不再滿足於走馬看花式的旅行，反而想更深入了解當地景點的歷史背景和文化內涵，從而帶動了專業導覽需求的不斷提高，而現今物聯網的發展相當快速，各個產業都積極的與物聯網做結合，觀光產業亦是如此。

二、願景

導覽服務對於博物館、美術館等單位是一種剛性需求，人員口說或租借導覽機是常見的服務。然而導覽志工、人員的培訓需要時間，導覽機的存放需要空間，內容的更新甚至可能需要付出高額的費用。

隨著網路科技技術的不斷更新，傳統的導覽方式已轉變，現今當下，人手一支手機，利用 APP 或網頁，隨時連接網路或是只要能事先將資訊下載好，即可馬上體會舒適的導覽體驗。

台灣企業蹦世界的創辦人黃勝宏先生曾在某一專訪提到，許多外國朋友來台灣玩，但都走馬看花，那使用他們的技術能不能做導覽呢？

蹦世界在 2013 年時，台灣創新風氣爆發，做出全台首創結合 LBS 定位技術衍生的服務和 AR 擴增實境的冒險遊戲，也因為有此成績，後來蹦世界決定往旅遊的市場開發。

(一) 量化或質化目標

蹦世界首先鎖定博物館、園區等，讓人一抵達該地，就能收到資訊與館內導航，比傳統導覽機便捷、低成本，甚至內容都能作為數位商品銷售。

而透過手機提供了服務後，若想讓遊客與旅遊地點有更多的互動則可以藉由當地的一些資訊或園區的設計提供一些互動小遊戲或者設計解謎，增添趣味並更了解當地的特色與知識。除了利於遊客外，在業者部分也可無負擔的隨時更新內容，提供導覽服務，且可蒐集相關資訊，如訪客停留次數、時間、路線等，便於分析及規劃未來展區目標。

三、服務架構

(一) 硬體

1. 場域端：利用 Beacon 與 GPS 做定位，將 Beacon 裝置佈在博物館或美術館等園區的各個角落，使遊客到達園區時，可藉由行動裝置得知自身所在地點與園區內的可行走路線，在室外有 GPS 定位，而在室內透過 Beacon 裝置，這種小而價廉的低功耗藍芽，精準度可至 1 公尺，彌補 Google Map 未觸及的室內應用。
2. 客戶端：蹦世界為博物館及園區設計了智慧導覽，可使用行動裝置的相機掃描展品旁之 QRcode 獲取展品相關資訊，若是智

慧解謎遊戲的部分，在找尋線索時，可透過行動裝置的相機，對周圍環境感測後，對應到相對的場景時，及觸發 AR 虛擬實境的小動畫。

(二) 軟體

1、 平台：蹦世界使用 AWS 伺服器架設一平台，提供後臺管理系統域雲端伺服器建置服務，提供管理員編輯內容及查看使用者大數據；數據的儲存、交換與運算。

2、 蹦世界 APP：所有建置之遊戲及導覽 APP 集中在蹦世界的 APP 中。園區導覽雖然可從網頁上可得到室內導覽地圖，但如需更多的功能則要使用 APP 開啟服務。

3、 網頁：使用 RWD 的設計，供使用者使用任何裝置都可方便查看。

(三) 網路連結

1、 各裝置的網路連接

- 場域端：在場地中放置 Beacon，利用藍芽方式，當手機進入到藍芽可偵測範圍，即可使系統得知自己的位置。
- 客戶端：用戶的行動裝置利用 Wi-Fi 或 4G-LTE 先從 APP 當中下載導覽或者遊戲所需的資料。且可透過藍芽或 GPS 定位，到達展覽品附近時即可偵測，並跳出所設定之功能供客

戶使用及體驗。

- 後台系統：使用 Wi-Fi、4G-LTE 或有線網路連接到後台系統上，供使用者查詢或分析系統所蒐集之資料。

2、 網路協定

在此案例中使用到了 Wi-Fi，4G-LTE 與藍牙 Beacon 室內定位。

Wi-Fi：Wi-Fi 之網路協定是基於 IEEE802.11 標準的無線區域網路技術，利用 Wi-Fi 可從範圍內的無線網路連接到網路，2010 年，Wi-Fi 保護存取加密(WPA2)被認定安全，能讓用戶使用強大的密碼。新協定的 Wi-Fi Multimedia（WMM）說明 Wi-Fi 更適合於延遲敏感型應用（如語音和影片），此外，WMM 的省電機制能提高電池效率。

4G-LTE：4G 是行動通訊標準，而 LTE 為電信中用於手機及數據中端的高速無線通訊標準為高速下行封包接入(HSDPA)過渡到 4G 的版本，LTE 的遠期目標是簡化和重新設計網路體系結構，使其成為 IP 話網路，這有助於減少 3G 轉換中的潛在不良因素，因 LTE 的介面與 2G、3G 網路互不相容，所以 LTE 需同原有網路分頻段營運。LTE 可提供高速移動中的通訊需求，支援多播和廣播流。LTE 頻段擴充度好，支援 1.4MHz 至 20MHz 的頻雙分工和時雙分工頻段。全 IP 基礎網路結構，也被稱作核心封包網演進，將替代原先的 GPRS 核心封包網，可向原先較舊的網路如 GSM、UMTS 和 CDMA2000 提供語音資料的

無縫切換。

Beacon：Beacon 是一種短距離、低功耗的無線傳輸技術，會以一個固定頻率，廣播一個特定的 ID(Identification)，而行動裝置一旦進入訊號區域，並透過雲端做識別後訊息則會透過專屬的 APP 傳送出去，而依 Beacon 偵測到的距離範圍，透過藍芽的訊號強弱(RSSI 值)，可用來判斷使用者的距離，進而觸發相關事件與使用者互動。

3、 網路安全的考量

因此案例大多使用 APP 與網頁，而在網路連接的方式是使用 HTTPS，在過去大多的網頁都是使用 HTTP 的資料傳輸方式，但用此方式它的內容紙規範了客戶端請求與伺服器回應的標準，實際上是使用 TCP 作為資料的傳輸方式。但在傳輸過程中，資料都是明文傳送，若是有惡意的竊聽者，資料將有機會被窺探、盜用。

所以現今大多改為 HTTPS 的方式，一樣透過 HTTP 進行通訊，但在通訊過程中使用 SSL/TLS 進行加密，由於非對稱加密的運算量較高，傳遞回應較慢；實際的架構上，會透過公開金鑰加密傳遞出共用的金鑰，再透過共用金鑰加密進行後續的傳遞，兼顧了安全性及傳遞速度。

(四) 如何使用服務

1、 網頁：若以網頁瀏覽的話，只能使用導覽的功能，然後可見平面地圖，在地圖上有提供一些地點資訊或是園區介紹，點下詳細介紹後，除了直接觀看也可撥放語音導覽的功能。

資料來源：https://popworld.cc/guide/1321/webView

圖 84、蹦世界網站線上導覽

2、 蹦世界 APP：若是使用 APP 操作的話，會比網頁瀏覽多了許多功能及與遊客增加互動。以下為各功能作介紹：

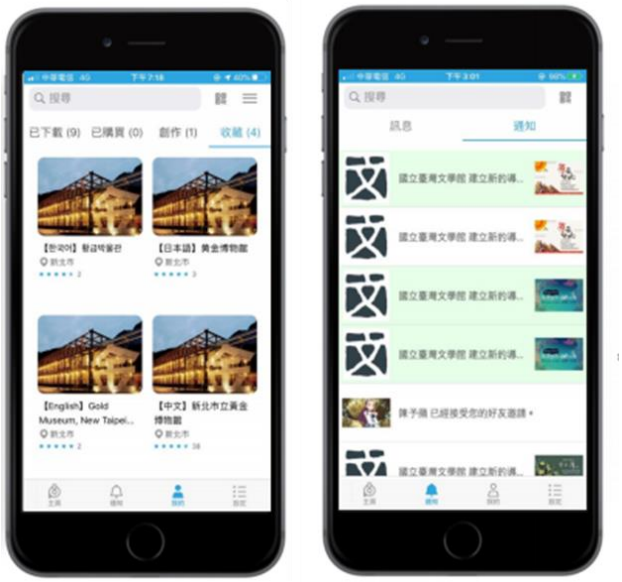
- 多元族群：視障人士若到達地點自動產生口述影像語音、藉由語音引導行進方向；錄製手語影片供聽障人士觀賞；行動不便者可透過電腦、平板或手機即使不到現場也可以觀賞，到了現場不需排隊租借導覽機。

- 自動介紹(圖 85 左)：運用 Beacon、GPS，遊客只需接近展覽品，語音、文字、圖片資訊即會自動跳出。
- 定位導航(圖 85 右)：利用蹦世界的 LBS 服務，在園區內不管室內室外即可藉由 APP 地圖為自己導航。

資料來源：蹦世界數位創意股份有限公司

圖 85、自動介紹與定位導航

- 多國語言(圖 86 左)：提供多國語言的翻譯錄音，製作其他語言導覽方便快速又輕鬆，再也不用擔心外國 人聽不懂。
- 即時通知(圖 86 右)：發出訊息通知遊客最新的消息，增加遊客 回訪的頻率。



資料來源：蹦世界數位創意股份有限公司

圖 86、多國語言與及時通知

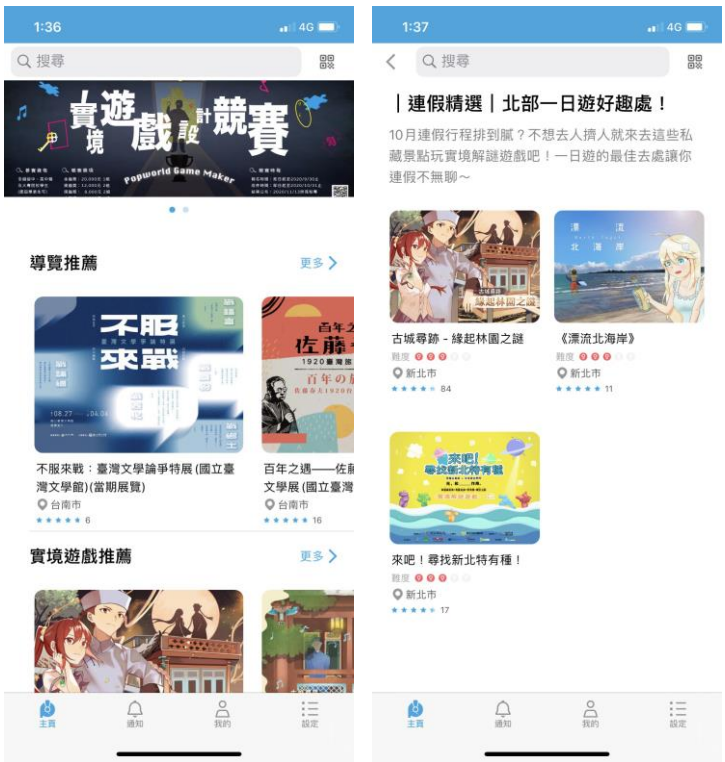
- 電子集章(圖 87 左)：利用室內外定位技術，讓遊客走到哪集到哪，不需要印章，直接使用手機集章換獎品。
- AR 擴增實境(圖 87 右)：使用擴增實境技術，結合科技與展覽， 除了讓遊客與吉祥物合照之外，也可以製造還原歷史現場的效果！

資料來源：蹦世界數位創意股份有限公司

圖 87、電子集章與 AR 擴增實境

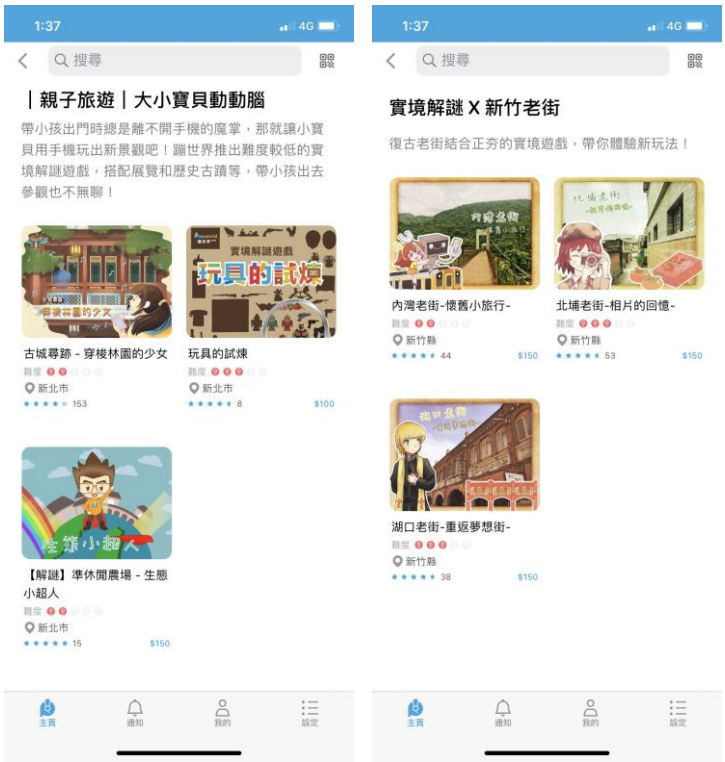
四、應用與展示

1. 蹦世界實境解謎與旅遊導覽平台：



資料來源：蹦世界數位創意股份有限公司

圖、蹦世界旅遊導覽



資料來源：蹦世界數位創意股份有限公司

圖 88、蹦世界實境解謎

五、參展紀錄

1. 2015、2016、2017 年台北國際旅展使用蹦世界 APP 可用來世貿室內地圖導航、集章活動換福袋、AR 拍照活動。

資料來源：蹦世界數位創意股份有限公司

圖 89、AR 拍照活動

資料來源：蹦世界數位創意股份有限公司

圖 90、室內地圖導航

資料來源：蹦世界數位創意股份有限公司

圖 91、集章活動換福袋

第四章　IETF 系列標準

第一節　IP (Internet Protocol)

一、IPv6 基本介紹

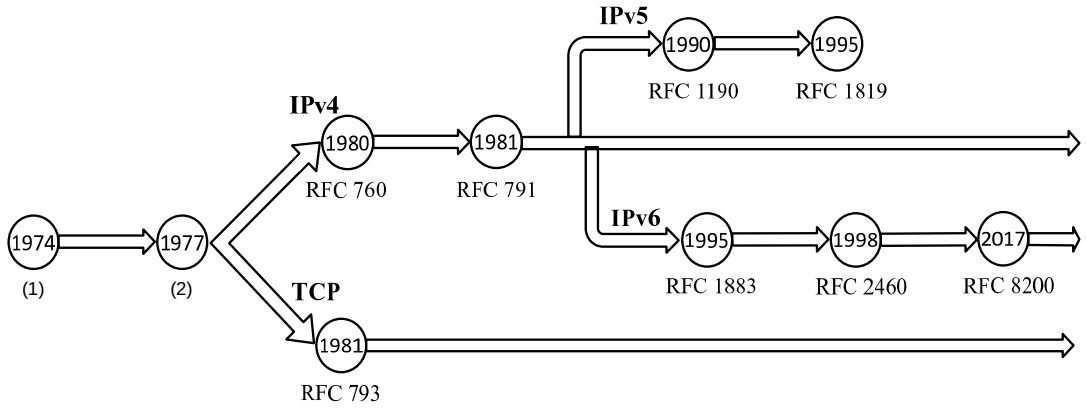
(一)　IP 的發展演進

網際網路(Internet)主要是指網路層透過網際網路協定(Internet Protocol, IP)連接全球數十億部裝置的數位資料傳輸系統。1960 年代冷戰時期，美國國防部高等研究計劃署（ARPA）為了能夠分時共用超級電腦，投入建立以封包交換為基礎的 ARPANET，並於 1969 年 10 月首次成功在兩節點間傳送輸入的文字，開啟了現今網際網路發展的新紀元。

1990 年 3 月歐洲的 CERN 網路利用 T1(1.5Mbit/s)線路與美國 NSFNet 相連，同年 Timothy John Berners-Lee 開發了首套 World-Wide Web 的瀏覽器。1991 年提供商用網路流量交換的 Commercial Internet eXchange 公司(CIX)成立，美國國家科學委員會(NSF)也允許非營利公司 Advanced Network and Services (ANS)的 ANSNet 與 NSFNet 同用實體主幹。台灣 TANet 則於 1991 年 12 月 3 日以 64Kbps 經美國東岸 Princeton University 連上 NSFNet。自 1990 年代起，網際網路開始從軍事、學術用途擴大為商用及民用，對網路接取及頻寬的需求也愈來

愈迫切。至 2020 年 1 月，全球估計上網人口已達 45 億人。

1974 年時 Vint Cerf 和 Bob Kahn 出版了一篇名為「Protocol for Packet Network Intercommunication」的論文，奠定了整個網際網路架構的基礎，後來該架構分為兩個模組分別進行發展，分別為傳輸層的 TCP 及網路層的 IP，亦即我們熟知的 TCP/IP 架構。第一版正式公開運作的 IP 是 IPv4，內建於當時的工作站及商用電腦。但是自 1990 年代起，考量到 IPv4 的位址空間可能無法負擔未來網路上的裝置數量，因此 IETF 在 1995 年制定了第一版 IPv6 規格以做為 IPv4 的繼任者，整個 IP 的規格發展如圖 92 所示。



(1). V. Cerf and R. Khan, "A Protocol for Packet Network Interconnection," *IEEE Transactions on Communications*, 22 (5), 1974
(2). IEN 2, Internet Experiment Note 2 (Comments on Internet Protocol and TCP), 1977

圖 92、IP 的規格演進(引用自維基百科)

(二) IPv6 和 IPv4 的主要差異

IPv6 (RFC 8200)是網際網路協定的最新版本，主要是為了解決 IPv4 (RFC 791)位址枯竭的問題，兩者的主要差別可以分為以下幾類，

其比較如表 6 所示。

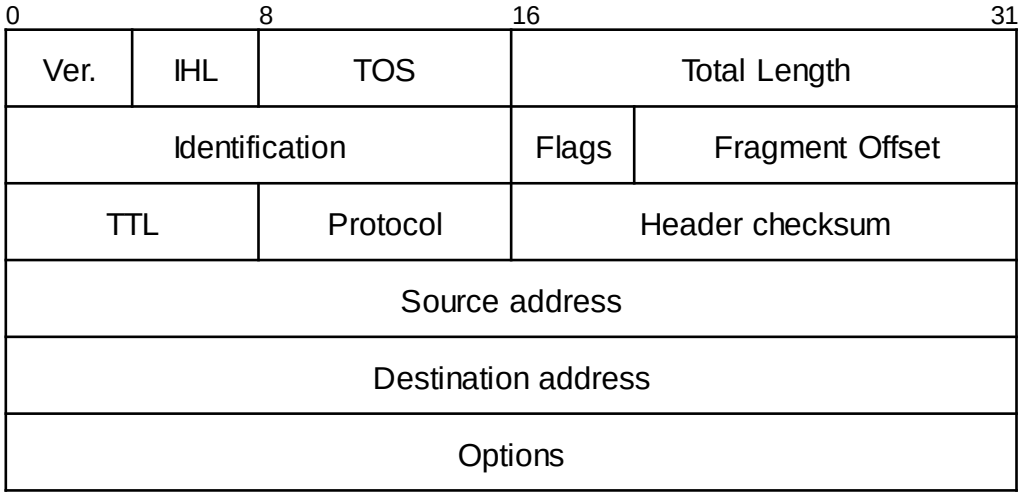
表 6、IPv4 與 IPv6 主要差異

	IPv4	IPv6
位址空間	32 位元 (4 Bytes)	128 位元 (16 Bytes)
位址類型	Unicast / Multicast / Broadcast	Unicast / Multicast / Anycast
表頭結構	可變長度 20-60Bytes，取決於使用的 IP 選項	固定 40Bytes，沒有 IP 表頭選項(比照傳輸層利用擴充標頭)
最大傳輸單元 MTU 的最小值	典型最小值為 576 Bytes	最小值為 1280 Bytes
位址解析	使用 ARP 來尋找與 IPv4 位址相關的實體位址	利用 NDP 或 SLAAC 將實體位址內含於 IP 進行芳鄰偵測和自動配置
封包分段	標準表頭佔有支援分段的欄位，來源節點或路由器皆可將封包分段	利用選擇性的分段擴充標頭，只能在來源節點執行分段且在目的地節點執行重組
QoS 品保支援	選項擴充 6 位元 DSCP 及 2 位元 ECN	預含包括 8 位元 Traffic Class 及 20 位元 Flow Label

每一台主機的每一個連線介面卡，均會自動取得或被設定一個全球或區網內部唯一的網路 IP 位址(IP Address)。發送端主機在送出的網路封包中，會在傳送的表頭內容(Header)表明自己的來源 IP 位址(Source Address)，並指名擬傳送對象的目的 IP 位址(Destination

Address)，表頭結構如圖 93 所示。IP 位址在 IPv4 為 32 位元，在 IPv6 為 128 位元。

IPv4



IPv6

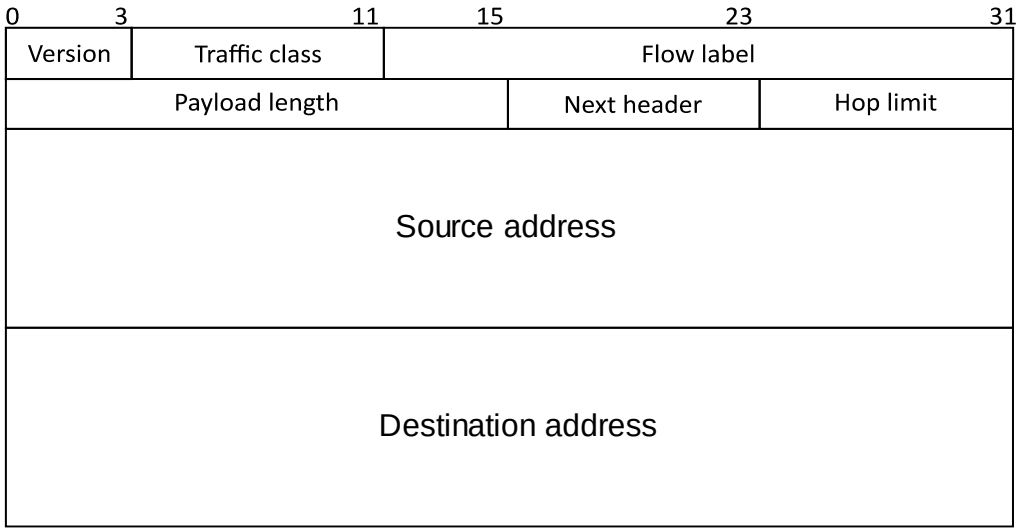


圖 93、IPv4 與 IPv6 表頭結構

傳統的網路通訊系統基本上都會提供一對一的單播(Unicast)、一對多的群播(Multicast)，或全體廣播(Broadcast)。網路群播已被廣泛應用在視訊、網路校時、內容散佈、mDNS、路由資訊交換、網路連線

遊戲等服務。IPv4 與 IPv6 也都支援群播(Multicast)，一般常見的 IP 網路層群播服務模式有支援多對多的 Any-Source Multicast (ASM)及以一對多為主的 Source-Specific Multicast (SSM)，兩者皆以一個識別用的群播位址來代表一個群播群組，擬接收群播封包的主機，必須先加入或取得該群組的群播位址，經由路由器的幫忙，後續才可以收到送往該群播位址的封包。

IPv4 的 Internet Group Management Protocol (IGMP)及 IPv6 的 Multicast Listener Discovery (MLD)，即是被提出來支援主機加入、離開群組，以及群組一致性的維護等。群播一直是非常熱門的研究議題，很多文獻都注重在探討各種網路環境及使用情境下，如何有效建立群播路由(Multicast Routing)或群播樹(Multicast Tree)，以降低需要重複傳送的封包量。

除了群播外，IPv6 支援任播(Anycast)，針對一個 Anycast 位址內的一群主機，只有一個主機會收到送往該 Anycast 位址的封包。一個 Anycast 位址對應一群接收端，但是對任一個發送端，藉由路由器的判斷與協助，只有其中一個最近或最好的接收端會接收到該發送端所傳送出的封包。現有的群播方法中，傳統的 Multicast 群播是讓已加入群組的所有成員均會收到群播封包，Anycast 則只有一個成員會收到封包。

IPv6 具有以下的多個優勢：

1、 擴增的位址空間：IPv6 將 IP 地址的大小從 32 位增加到 128 位，以支援更多級別的尋址層次結構、更多數量的可尋址節點以及更簡單的地址自動配置。在多播地址上加入作用域(Scope)區段，可以改善多播路由的可伸縮性。IPv6 還定義了一種新型的地址，稱為「任播地址(Anycast Address)」，用於將封包發送到一組節點中的任何一個。

2、 簡化表頭結構：某些 IPv4 表頭欄位已被棄用或成為選用欄位，以減少處理絕大多數封包的成本並限制 IPv6 表頭的頻寬成本。

3、 改進擴增和選項支援度：IP 表頭選項編碼方式的更動使得轉發更有效率、更少的選項長度限制以及提高將來引入新選項的靈活性。

4、 流量標記能力：IPv6 增加了一項可以標記發送端請求封包序列的功能，發送端請求的封包序列在網絡中被視為單一個流量。

5、 身份驗證和隱私功能：IPv6 中的擴增支援了身份驗證、資料完整性和資料機密性(選項)的功能。

(三) IPv6 和 IPv4 對物聯網的差異

相較於 IPv4，IPv6 擁有大量位址空間以及不需透過網路位址轉換(NAT)連接的特性，使其對物聯網的相關應用極為友善。事實上，有關 IPv6 與物聯網的相關標準為 IETF 目前的重點之一，如已經結束的 6LoWPAN，目前仍在運作的 6Lo、lpwan 及 lwig 等都是與物聯網及資源限制裝置上的 IPv6 連接標準相關的工作組。

IPv6 的一大特點為其對低功耗無線個人區域網路(LoWPAN)及低功耗廣域網路(LPWAN)中的鏈路支援，這是 IPv4 中所沒有的特性。能達成這個特性的主要原因為 IPv6 針對不同種類的 LoWPAN 鏈路或是 LPWAN 鏈路制定了不同的轉換層。如 6LoWPAN 工作組制定了 IPv6 與 IEEE 802.15.4 間的轉換層。6Lo 工作組將 6LoWPAN 的成果進一步推廣，制定了 IPv6 到常見的 LoWPAN 鏈路協定(如 BLE、ITU-T G.9959、NFC、IEEE 802.11ah)的轉換層。而 lpwan 則制定了 IPv6 到如 SigFox、LoRa、Wi-SUM、NB-IoT 等 LPWAN 的轉換層。

由於 LoWPAN 和 LPWAN 的鏈路拓樸、MTU 與上下行鏈路模型皆與以大頻寬、高效能為訴求的 Ethernet 或是 WLAN 技術不同，因此上述這些轉換層的目的皆為將標準 IPv6 轉換至適合 LoWPAN 及 LPWAN 鏈路的大小與格式，其功能主要可以分為表頭壓縮、分段、群播轉換及鄰居發現。

IPv6 對物聯網有以下優勢：

1、 表頭壓縮降低成本：

若在 LoWPAN 及 LPWAN 的鏈路中使用標準 IPv6 40Bytes 的表頭，將會在鏈路訊框上消耗大量的空間，使得載酬的空間受到壓縮而降低傳輸效率，同時也會浪費多餘的能源與頻寬在傳輸 IPv6 的表頭。有鑑於此，IPv6 到 LoWPAN 或是 IPv6 到 LPWAN 的轉換層會執行表頭壓縮，表頭壓縮可以分為無狀態及有狀態兩種壓縮方式。無狀態表頭壓縮會透過鏈路層的表頭來推導出部分 IPv6 的表頭(如來源位址、Datagram 長度等)，或者透過將 IPv6 表頭的特定欄位設為一典型值來進行 IPv6 的表頭壓縮，如由 6LoWPAN 工作組所提出的 6LoWPAN-HC 其中的一種運作模式即為此方式。另一方面，有狀態表頭壓縮則透過雙方共享如位址前綴等語境的方式來使得可以在鏈路訊框中使用較短的識別碼即可還原出原 IPv6 的表頭，由 lpwan 工作組所提出靜態語境表頭壓縮(SCHC)即為此種壓縮方式，而 IPv4 僅能使用如 Robust Header Compression (ROHC)等編碼方式來實現表頭壓縮。

2、 取消分段並簡化錯誤檢查提升效率：

許多 LoWPAN 與 LPWAN 的 PHY/MAC 層技術為了簡化錯誤檢查機制、降低系統記憶體和處理器的需求以及達到較低的耗電量，僅會在鏈路層提供數十到數百 Bytes 的 MTU，這與 Ethernet 動輒 1500 Bytes 起跳的 MTU 差距甚大。此外，標準 IPv6 所要求的最小 MTU

為 1280 Bytes，顯然 LoWPAN 與 LPWAN 的部分鏈路無法滿足此一要求。因此，若 LoWPAN 與 LPWAN 的鏈路層沒有提供分段與重組功能的話,轉換層就必須負擔起將標準 IPv6 封包分段及重組的工作。此外，IPv6 並不允許中間節點進行封包的分段，這與 IPv4 相比大幅降低了節點的複雜度。

3、 可省略群播降低複雜度：

LoWPAN 與 LPWAN 的底層鏈路中通常只有單播或是廣播，只有如 IEEE 802.11ah 等少量的鏈路提供群播的功能，因此轉換層需透過直接將群播映射到廣播或是透過多次的單播來實現群播的轉換。相較之下 IPv4 並無此功能。

4、 優化鄰居發現：

鄰居發現是 IPv6 中一個優良的特性，該特性提供了物聯網自動設定位址及其他資訊的可能性，但是 LoWPAN 與 LPWAN 中的節點常常會進行休眠，其鏈路也為週期性可用，這些鏈路特性使得標準 IPv6 中的鄰居發現難以適用於 LoWPAN 與 LPWAN 的網路中。因此轉換層中需透過如 6LoWPAN ND 中節點主動和路由器溝通的方式進行鄰居發現。相較之下 IPv4 仍須透過如 ARP 等通訊協定來進行鄰居發現。

(四) IPv6 主要通訊協定

IPv6 正常運作需有許多協議參與其中，最主要的幾個協議為 NDP、SLAAC、DAD、ICMPv6、MLDv2 及 DHCPv6，這些協定運作時的架構如圖 94 所示，以下將針對上述幾個通訊協定進行簡介。

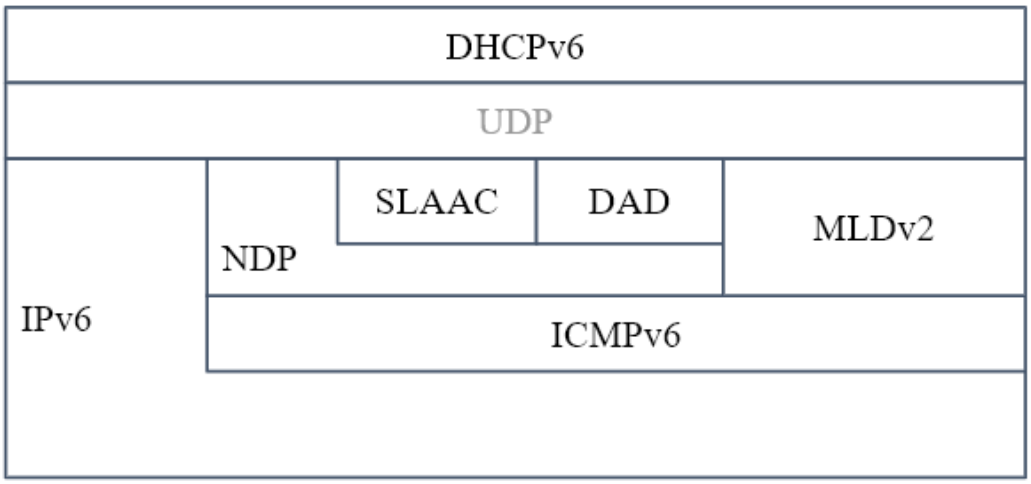


圖 94、IPv4 與 IPv6 表頭結構

1、 NDP (Neighbor Discovery Protocol, RFC 4861)

鄰居發現協議(Neighbor Discovery Protocol, NDP)是 IPv6 架構中一個極為重要的通訊協議，同一個鏈路中的 IPv6 節點透過鄰居發現協議尋找鏈路上其他節點的鏈路位址、尋找可以代替轉送封包的路由器並持續追蹤鄰居是否可達及其鏈路位址。

NDP 的定義主要是靠解決兩個在相同鏈路的節點進行資訊交換時所發生的問題來給出，其主要問題如下：

(1) 路由器發現：主機該如何在已銜接的鏈路上找到路由器。

(2) 前綴發現：主機該如何找到已銜接鏈路上的位址前綴集合。

(3) 參數發現：主機該如何知道鏈路的參數(如鏈路的MTU等)及網路層的參數(如節點跳躍數量限制等)。

(4) 位址自動設定：節點須進行如 RFC 4862 內提到的無狀態位址自動設定。

(5) 位址解析：節點如何從 IP 位址得出目標節點的鏈路位址。

(6) 決定 Next-Hop：如何從 IP 位址決定該將流量送給哪個鄰居。

(7) 鄰居不可達偵測：節點該如何知道某個鄰居已經不可達。若該鄰居是路由器的話，節點將會嘗試替代的預設路由器。

(8) 重複位址偵測：節點該如何知道欲使用的位址已經被其他節點使用。

(9) 重導向：路由器該如何告知主機有更佳的 First-Hop 通往特定的目的地。

2、 SLAAC (Stateless Address Autoconfiguration, RFC 4862)

自動位址設定的過程包含產生一個本地鏈路位址、透過無狀態位址自動設定產生全域位址並透過重複位址偵測的機制判斷欲使用的位址是否已被使用。IPv6 無狀態位址設定顧名思義主機不需要任何額外的手動位址設定，對於路由器也僅須少量的設定且無須額外的伺服器輔助。

位址自動設定透過結合本地資訊與路由器建議的資訊來產生全域位址。路由器建議鏈路上的前綴及子網路識別碼，而主機則會針對每個介面產生一個獨一無二的「介面識別碼」，兩者結合即為一個 IPv6 的地址。若沒有路由器的參與，則主機只能產生本地鏈路位址來和同一個鏈路下的其他節點通訊。

如果不在意主機所使用的確切位址，只在意位址是唯一且可正確被路由，則可使用無狀態的方法。另一方面，如果需要更強烈的位址分配控制則可使用 RFC 8415 所提到的動態主機設定協定(Dynamic Host Configuration Protocol for IPv6, DHCPv6)，無狀態位址自動設定可以和 DHCPv6 同時共存。

3、 DAD (Enhanced Duplicate Address Detection, RFC 7527)

此文件介紹了一種藉由偵測回送 IPv6 ND 訊息方式所實現的重複位址偵測(Duplicate Address Detection, DAD)演算法，此外此文件還探討了在某些特殊接取網路中的重複位址偵測。

在 RFC 4862 的附錄 A 中討論了 IPv6 回送抑制(Loopback Suppression)和重複地址檢測（Duplicate Address Detection, DAD）。該文件提到了一種硬體輔助機制來檢測回送的 DAD 消息。如果硬體無法抑制回送的 DAD 消息，則需要軟體解決方案。DAD 所使用的特別 NDP 訊息類型是在 RFC 4861 中所說明的鄰居請求（Neighbor

Solicitation, NS）。 NS 由 DAD 的 IPv6 節點的網介面產生。

DAD 中所涉及的另一個消息是鄰居建議(Neighbor Advertisement, NA)。此文件中的增強型 DAD 算法重點在於在 DAD 操作期間檢測回送的 NS。 檢測回送的 NA 不能解決回送的 DAD 問題。在 DAD 操作期間檢測到任何其他回送 ND 訊息不在此文檔的範圍之內。此文檔還包括有關一節的章節,討論了可用於緩解 DAD 回送問題的方法。

4、 PMTU (Path MTU Discovery for IPv6, RFC 8201)

當一個 IPv6 節點有大量資料要發送到另一個節點時，該資料將以一系列 IPv6 封包進行傳輸。這些封包的大小可以小於或等於路徑 MTU(Path MTU, PMTU)。或者是封包會被分成一系列片段，每個片段的大小小於或等於 PMTU。

通常最好的封包大小為從起始節點到目標節點的路徑中的最小鏈路 MTU，這讓封包可以順利從起始節點傳送至目標節點從而無需 IPv6 分段，這個封包大小稱為路徑 MTU(Path MTU, PMTU)。此文件定義了一種用於節點發現任意路徑的 PMTU 的標準機制。

IPv6 節點應實作路徑 MTU 發現，以便發現並利用 PMTU 大於 IPv6 最小鏈路 MTU 的路徑。最小的 IPv6 實現（例如在開機 ROM 中）可以選擇省略路徑 MTU 發現的實作。

未實作路徑 MTU 發現的節點必須使用 RFC 8200 中定義的 IPv6

最小鏈路 MTU 作為最大封包大小。在大多數情況下，這將導致使用較小的封包大小，因為大多數路徑的 PMTU 均大於 IPv6 最小鏈路 MTU。發送比路徑 MTU 所允許的封包大小還要小得多的封包的節點正在浪費網絡資源，並可能導致吞吐量不足。

如果阻止或不發送 ICMPv6 訊息，則實現路徑 MTU 發現並發送大於 IPv6 最小鏈路 MTU 的數據包的節點容易出現連接問題。例如，這將導致連接正確完成 TCP 三向握手，但是在傳輸數據時掛起，此狀態稱為黑洞連接(RFC2923)。路徑 MTU 發現依靠 ICMPv6 封包太大（Packet Too Big, PTB）來確定路徑的 MTU。

在 RFC4821 中可以找到路徑 MTU 發現的擴展。 RFC 4821 定義了一種用於打包層路徑 MTU 發現（Packetization Layer Path MTU Discovery, PLPMTUD）的方法，該方法設計用於無法確保向主機傳遞 ICMPv6 訊息的路徑上。

5、 DHCPv6 (Dynamic Host Configuration Protocol for IPv6 (RFC 8415)

DHCPv6 是一種用於自動配置網絡配置參數的可擴展機制，如自動配置節點的 IP 位址和前綴。網路參數可以以無狀態的方式提供，也可以結合一個或多個 IPv6 地址或 IPv6 前綴來進行有狀態分配參數提供。 DHCPv6 可以代替無狀態地址自動配置（SLAAC）或與其並

存。其運作過程如圖 95 所示，客戶端使用 DHCP_Relay_Agents_and_Servers multicast address (FF02::1:2) 和 DHCP 伺服器溝通，因此 DHCP 伺服器不須額外配置一個位址。

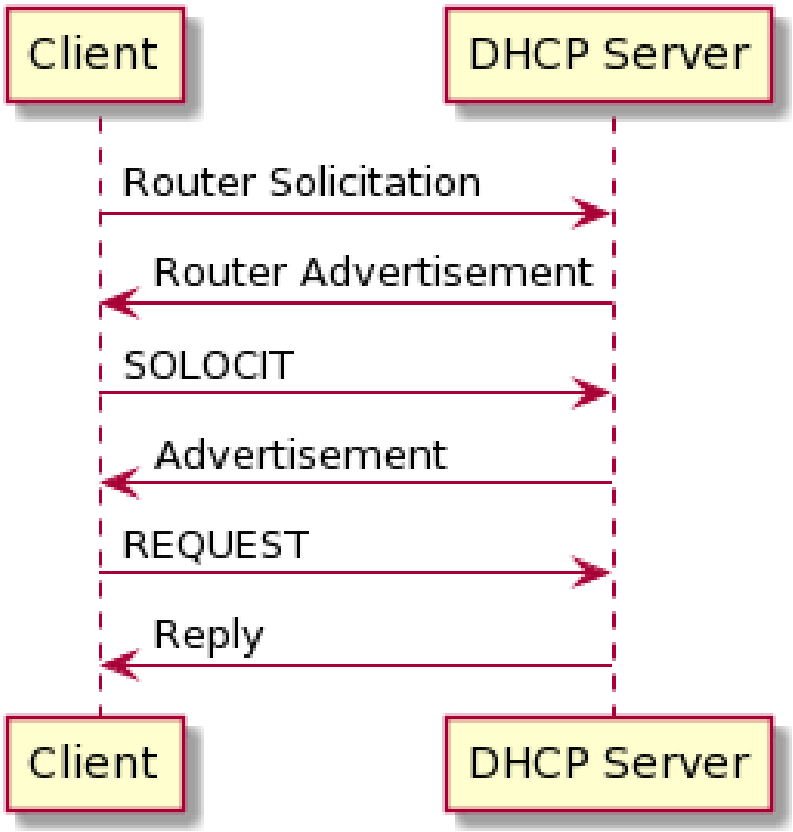


圖 95、DHCPv6 的運作過程

6、 ICMPv6 (Internet Control Message Protocol, RFC 4443)

IPv6 透過 ICMPv6 來傳遞控制訊息，如進行 Path MTU Discovery 及 NDP 等，ICMPv6 的 IPv6 Next Header 值為 58。

7、 MLDv2 (Multicast Listener Discovery Version 2 for IPv6, RFC 3810)

IPv6 路由器使用群播監聽器發現協議（MLD）來發現在其直接連接的鏈路上且希望接收群播封包的節點，並發現鄰居所感興趣的特定群播地址。群播路由器本身可以是一個或多個群播地址的監聽器。在這種情況下，它既執行 MLDv2 的“群播路由器部分”，負責收集其群播路由協議所需的群播監聽器訊息。另一方面又執行“群播地址偵聽器部分”通知自身和其他相鄰的多播路由器它的收聽狀態。

二、IETF IPv6 標準制定現況

(一) IPv6 相關領域分析

Internet Engineering Steering Group (IESG) 將 Internet Engineering Task Force (IETF) 的工作組 (Working Group, WG) 劃分為七個領域，分別是應用及即時通訊領域 (Applications and Real-Time Area, ART)、傳輸領域 (Transport Area, TSV)、路由領域 (Routing Area, RTG)、網際網路領域 (Internet Area, INT)、維護及管理領域 (Operations and Management Area, OPS)、資訊安全領域 (Security Area, SEC) 和一般事務領域 (General Area, GEN)。

其中，INT、OPS 及 SEC 為三個和 IPv6 較為相關的領域，INT 領域中因工作組眾多，故可再依據技術領域將工作組分類為專注在 IP 核心通訊協定的核心技術領域 (Core)、專注在資源限制較為嚴格節點上的低功耗網路技術領域 (Low Power) 、專注在移動性及備援

容錯機制的移動性和多址傳送技術領域(Mobility and Multihoming)及專注在時間相關通訊協定的時間技術領域 (Time) 等，各技術領域內相關的工作組及各工作組的目前階段如表 6 所示，其中各領域都另有同名、持續進行中的工作組未另外列出。

核心技術領域中共有七個工作組，分別是 Adaptive DNS Discovery (add)、Extensions for Scalable DNS Service Discovery (dnssd)、DNS PRIVate Exchange (dprive)、IPv6 Maintenance (6man)、Internet Area Working Group (intarea)、Home Networking (homenet) 和 Dynamic Host Configuration (dhc)。 add 負責進行自適應 DNS 解析器發現協定制定，其內容包括定義一種適用於公開或私有網路並支援加密的 DNS 解析器發現機制、制定客戶端和 DNS 解析器通訊的機制，使 DNS 解析器能提供一些訊息作為客戶端決策的依據。 dnssd 負責將原本僅限於本地鏈路連接 DNS 服務發現協定擴充成可以跨多個鏈路的協定，以方便無組態網路設定進行。 dprive 則負責提供 DNS 解析器和權威域名伺服器之間訊息交換的機密性，以避免使用者的個人訊息透過 DNS 洩漏。 6man 工作組的主要的工作為維護、修復和改進 IPv6 的協定及位址結構。 homenet 負責利用 IPv6 制定多路由器的家庭網路的架構及。dhc 則負責如 DHCPv6 等自動網路組態設定協定之制定。

低功耗網路技術領域內有四個工作組 IPv6 over Low Power Wide-Area Networks (lpwan)、IPv6 over Networks of Resource-constrained Nodes (6lo)、Light-Weight Implementation Guidance (lwig) 和 IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch)。 lpwan 提出了可以在低功耗廣域網路壓縮標頭及分段標頭的靜態語境標頭壓縮與分段 (Static Context Header Compression and Fragmentation, SCHC) 標準，該工作組將繼續維護 SCHC 及提出將 SCHC IPv6/UDP 應用於目前技術的標準。 6lo 關注資源限制網路節點的連線，負責制定 IPv6 及由 6LoWPAN 所定的鍊結層技術間的轉換層標準及低複雜度標頭壓縮等通用標準。 lwig 負責制定在資源限制網路節點相容於目前標準且精簡的通訊標準。 即將進入收尾階段的 6tisch 則負責制定基於 IEEE802.15.4 時槽跳頻技術的 IPv6 協定。

移動性和多址傳送技術領域內有 IP Wireless Access in Vehicular Environments (ipwave) 、 Distributed Mobility Management (dmm) 和 Host Identity Protocol (hip) 三個工作組。 ipwave 負責車對基礎設施通訊 (Vehicle-to-Infrastructure Communication, V2I) 及車對車通訊 (Vehicle-to-Vehicle Communications, V2V) 等車連網相關的網路通訊協定制定。 dmm 負責制定分散式移動設備管理及增強型移動性錨點的標準，以利無線網路中的移動性設備在移動時維持可用網路。 hip

提供了將終端節點識別與 IP 位址分開的方法，在該方法中終端節點使用公開金鑰來識別身份而非 IP 位址。

時間技術領域內有 Network Time Protocol (ntp) 及 Timing over IP Connection and Transfer of Clock(tictoc) 兩個工作組。ntp 負責制定第四版網路時間通訊協定 (NTPv4)的標準。 而 tictoc 則專注於提供高精準度的網路時鐘同步。

剩下的 IETF 研究領域中，OPS 及 SEC 都有和 IPv6 相關的工作組，以下將介紹所有有關的工作組。OPS 內的 IPv6 Operations (v6ops) 負責蒐集 IPv6 營運商和使用者所產生的問題及解決方案，以解決 IPv6 的營運問題。SEC 內的 IP Security Maintenance and Extensions (ipsecme)負責維護及擴充前代 IPsec 工作組所制定的 IPsec 協議套件，如 IKEv1、IKEv2 等，各工作組的目前階段如表 7 所示。

本報告將在上述工作組中挑出和 IPv6 相關的工作組，從中挑出和 IPv6 較為相關的 Standard Track RFC 和 Internet Draft，並進行更進一步的報告。Internet Area 的核心技術領域內總共挑出 6man 和 dhc 等和 IPv6 較為相關的工作組，低功耗網路內總共挑選了 6lo、lpwan、lwig 及 6tisch 等工作組，負責車連網相關標準制定的 ipwave 也在本報告的範圍內。最後，本報告從 Security Area 及 Operations and Management Area 內挑出 ipsecme 及 v6ops 等與 IPv6 的資訊安全

及維護有關的工作組進行報告，欲報告工作組如表 8 所列。

表 7、IETF IPv6 相關領域的工作組概況

領域	技術範籌	啟動階段	穩定運作	收尾階段
Internet Area (共 17WGs)	核心(Core)	add, dprive	dnssd, **dhc**, **6man**	homenet
	低功耗網路(Low Power)		**lpwan**, **6lo**	**lwig**, **6tisch**
	移動性和多址傳送 (Mobility and Multihoming)	drip	dmm	**ipwave**, hip
	時間(Time)		ntp, tictoc	
Operations and Management Area (共 14WGs)	網際網路維護(Internet)	mops	mboned, opsec, bmwg	**v6ops**
	路由和域名系統維護 (Routing & DNS)		grow, sidrops, dnsop	
	自動網路配置維護 (Automatic Network Configuration)	anima	netmod	netconf
	認證維護 (Authentication)	radext	dime	
Security Area (共 23WGs)	驗證和授權 (Authentication & Authorization)	emu, lake	oauth, kitten	ace
	憑證和身份 (Certificate & Identity)	rats	acme, sacm	
	簽章、加密和密碼學 (Signing, Encryption & Cryptography)	cose. lamps	trans, curdle	
	網路安全 (Network Security)	mls	tls, **ipsecme**, i2nfs	dots

	應用安全 (Application Security)		secevent, teep, tokbind, suit, mile	

表 8、IETF IPv6 相關重點工作組簡介

工作組名稱	工作組全名	領域	工作組介紹
6lo （8 Active Drafts, 11 RFCs）	IPv6 over Networks of Resource-constrained Nodes	Internet Area	關注資源限制網路節點的連線。
lpwan （5 Active Drafts, 2 RFCs）	IPv6 over Low Power Wide-Area Networks	Internet Area	負責提出適用於低功耗廣域網路的表頭壓縮，並將其套用在不同的實體層協定上。
lwig （5 Active Drafts, 4 RFCs）	Light-Weight Implementation Guidance	Internet Area	負責制定在資源限制網路節點相容於目前標準且精簡的通訊標準。
6tisch （4 Active Drafts, 3 RFCs）	IPv6 over the TSCH mode of IEEE 802.15.4e	Internet Area	負責制定基於 IEEE802.15.4 時槽跳頻技術的 IPv6 協定
ipwave （1 Active Drafts, 1 RFCs）	IP Wireless Access in Vehicular Environments	Internet Area	負責車連網相關的通訊協定制定。
6man （6 Active Drafts, 49 RFCs）	IPv6 Maintenance	Internet Area	維護和改進 IPv6 協定及位址結構。
dhc （5 Active Drafts, 100 RFCs）	Dynamic Host Configuration	Internet Area	負責如 DHCPv6 等自動網路組態設定協定之制定。
v6ops （4 Active Drafts, 78 RFCs）	IPv6 Operations	Operations and Management Area	負責蒐集 IPv6 營運商和使用者所產生的問題及解決方案。

ipsecme （6 Active Drafts, 28 RFCs）	IP Security Maintenance and Extensions	Security Area	負責維護及擴充前代 IPsec 工作組所制定的 IPsec 協議套件，如 IKEv2。

(二) IPv6 活躍工作組分析

1、 6lo - 負責 IPv6 在低功耗網路節點上的標準制定

(1) 工作組說明

6lo 致力於促進資源受限節點網絡上的 IPv6 連接的工作，這些節點的特點是：

- 有限的電源，記憶體和處理器資源
- 嚴格限制的狀態、程式碼空間及處理週期
- 最佳化的能源和網路頻寬使用
- 缺乏某些鏈路層服務，例如完整的設備連接和廣播/群播

具體來說，6lo 將在以下方面工作：

- 適用於資源受限節點的 IPv6-over-foo 的轉換層規範，使用 6LoWPAN 技術（RFC4944，RFC6282，RFC6775）作為鏈路層技術
- 上述轉換層用於基本監控和故障排除的訊息和資料模型（例如 MIB 模組）。
- 適用於多個轉換層規範的規範，例如低複雜度表頭壓縮

(2) 相關 RFCs

i RFC 4944 (Transmission of IPv6 Packets over IEEE 802.15.4 Networks, Proposed Standard RFC)：介紹了 IPv6 封包傳輸的幀格式以及在 IEEE 802.15.4 網絡上形成 IPv6 鏈路本地地址和無狀態自動配置地址的方法。此文件提到的其他規範包括使用共享上下文的簡單標頭壓縮方案以及 IEEE 802.15.4 網格中的封包傳遞規定。

ii RFC 6282 (Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, Proposed Standard RFC)：此文件為 6LoWPAN 中的 IPv6 封包傳遞指定了 IPv6 表頭壓縮格式。壓縮格式依靠共享上下文來允許壓縮任意前綴。 如何在共享上下文中維護信息不在此文件的範圍。此文件指定了多播地址的壓縮和用於壓縮下一個標頭的框架。UDP 標頭壓縮是在此框架中指定的。

iii RFC 6775 (Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), Proposed Standard RFC)：介紹了針對 6LoWPAN 和類似網絡的 IPv6 鄰居發現的簡單優化、尋址機制以及重複地址檢測。

iv RFC 7388 (Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), Proposed Standard RFC)：定義了一個管理資訊庫(Management Information Base, MIB)上的物件，用來管理在無線個人區域網路上的 IPv6。

v RFC 7400 (6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), Proposed Standard RFC)：擴充了 RFC 6282 所定義之 6LoWPAN 中的表頭壓縮，使其能支援通用表頭(generic headers) 及表頭狀載酬(header-like payloads)之壓縮，從而避免為了上述兩種資料重新定義資料壓縮格式。

vi RFC 7428 (Transmission of IPv6 Packets over ITU-T G.9959 Networks, Proposed Standard RFC)：描述了在 ITU-T G.9959 網路上進行 IPv6 傳輸時的訊框(frame)格式、本地鏈路位址(link-local address)及無狀態自動位址設定的方法。

vii RFC 7668 (IPv6 over BLUETOOTH(R) Low Energy, Proposed Standard RFC)：介紹了如何在藍芽低功耗網路上進行 IPv6 的傳輸，包括鏈路模型(Link Model)、無狀態位址自動設定及鄰居發現等等。

viii RFC 7973 (Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation, Informational RFC)：描述了使用 LoWPAN 的 IPv6 的 datagram 若被 Ethernet 封裝時，其訊框之 EtherType 應為 0xA0ED 。EtherType 列表可以參考 http://standards-oui.ieee.org/ethertype/eth.txt。

ix RFC 8025 (IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch, Proposed Standard RFC)：補充 RFC4944，介紹了一種適用於 6LoWPAN 表頭壓縮的 contex-switch 機制，該機制以分頁表示，並以新的機制調度分頁。

x RFC 8065 (Privacy Considerations for IPv6 Adaptation-Layer Mechanisms, Informational RFC)：討論了當 IPv6 設計跨越了多種 link-layer 時會發生的幾種隱私威脅，並提供如何識別那些威脅的方法。

xi RFC 8066 (IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines, Proposed Standard RFC)：補充了 RFC 4944 中所提到的 ESC

dispatch type，該 dispatch type 可以讓 6LoWPAN 的 header 調度多個位元組。

xii RFC 8105 (Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE), Proposed Standard RFC)：超低功耗數位增強無線電話 (DECT ULE) 是一個由 DECT 論壇所推出並由 ETSI 制定規格的低功耗空中介面技術。該文件描述了當使用 DECT ULE 進行 IPv6 傳輸時的通訊協議堆疊及鏈路模型。

xiii RFC 8163 (Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks, Proposed Standard RFC)：MS/TP 是一個 RS-485 的媒體存取控制方法，該文件定義了在 MS/TP 網路上傳輸 IPv6 封包時的訊框格式、鏈路形成的方法及無狀態自動位址設定的方法。

xiv RFC 8505 (Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery, Proposed Standard RFC)：簡化了 RFC 6775 6LoWPAN 鄰居發現協議的註冊過程，以增進註冊的容量及不同網路拓樸間移動的偵測。

(3) 進行中的 Internet Drafts

i Address Protected Neighbor Discovery for Low-power and Lossy Networks (draft-ietf-6lo-ap-nd-23, Date: 2020-04-30)：提出了一種在 6LoWPAN 上可以防止位置被竊盜的鄰居發現協定擴充。在該方法中，節點須先以密碼識別號碼(Crypto-ID) 註冊位址並證明持有該 Crypto-ID，使用 Crypto-ID 可以防止已註冊的位址在低功耗易遺失網路上(Low-power and Lossy Network, LLN)被竊盜。

ii IPv6 Backbone Router (draft-ietf-6lo-backbone-router-20, Date: 2020-03-23)：該文件擴充了 RFC 6775 以使用骨架路由器(Backbone Router)代理居發現協定的服務，骨架路由器被放置於骨幹網路的邊緣，以整合多個無線鍊路形成一個子網路。

iii IPv6 Mesh over BLUETOOTH(R) Low Energy using IPSP (draft-ietf-6lo-blemesh-07, Date: 2019-12-14)：該文件將 IPv6 over BLE (RFC 7668) 的拓樸由星狀網路改為網狀網路，並敘述建立鍊路的機制，該文件並不包含在 BLE Mesh 上進行路由的部份。

iv Packet Delivery Deadline time in 6LoWPAN Routing Header (draft-ietf-6lo-deadline-time-05, 2019-07-08)：定義了一個新的 6LoWPAN 路由類型，該路由類型還有一個截止時限，使得

在具有時間同步網路內的路由排程器可以決定時間緊迫的機器對機器溝通(M2M) 之路由順序。

v 6LoWPAN Selective Fragment Recovery (draft-ietf-6lo-fragment-recovery-21, Date: 2020-03-23)：提出了一種可以單獨傳送個別分段(fragment)到終端且具有壅塞控制的通訊協定，使得大資料傳輸失敗時只須重傳失敗的部份就好，不須重傳整段資料。

vi On Forwarding 6LoWPAN Fragments over a Multihop IPv6 Network (draft-ietf-6lo-minimal-fragment-15 , Date: 2020-03-23)：提供了一個泛化的規則讓 6LoWPAN 的 fragment 可以被轉送到 route-over network，如此的轉送可以降低延遲、提昇可靠度並降低中間節點的緩衝區需求。

vii Transmission of IPv6 Packets over Near Field Communication (draft-ietf-6lo-nfc-15, Date: 2019-07-08)：敘述如何在近場通訊(NFC)上進行 IPv6 的傳輸，包括協定堆疊、鏈路模型、無狀態自動位址設定、本地鏈路位址、鄰居發現、表頭壓縮等。

viii Transmission of IPv6 Packets over PLC Networks (draft-ietf-6lo-plc-03, Date: 2020-04-29)：敘述如何在如 ITU-T G.9903, IEEE 1901.1 和 IEEE 1901.2 等電力線通訊(PLC)上進行 IPv6 的

傳輸，包括協定堆疊、無狀態自動位址設定、本地鍊路位址、鄰居發現、表頭壓縮等。

2、 lpwan - 負責 IPv6 在低功耗廣域網路上的標準制定

(1) 工作組說明

SIGFOX，LoRa，WI-SUN 和 NB-IOT 等低功耗廣域網路(LPWAN)的技術出現帶給物連網領域不小的衝擊。這些技術都有一些共同的特徵，如最佳化的無線電調製、星形拓撲、以超低速每天傳輸幾十個位元組、有時可變的 MTU 且大部分是上行傳輸模式，這些特性使得設備可以將大部分時間花費在低能耗深度睡眠模式下，以節約耗電量並延長電池壽命。

然而這些好處是有代價的，低功耗廣域網路的鏈路層幀格式已針對每種技術進行了優化和特化。由於沒有網路層，所以應用程式通常直接連接到鏈路層。這導致不同技術間的部署及管理必須單獨進行且從一種 LPWAN 技術遷移到另一種 LPWAN 技術意味著要重新建構整個通訊鏈。因此需引入網路層的 IPv6 來提供一個統一的介面讓不同技術間互相溝通。

LPWAN 的特徵為稀疏且廣泛的不平衡空中傳輸，且幾乎沒有辦法透過改變幀格式引入 IPv6，這使得現有的 IETF 工作（6lo）無法被簡單地應用。因此 lpwan 工作組將：

- 維護 SCHC，包括為上層協議啟用 SCHC 機制。
- 產出在現有技術上應使用 SCHC IPv6 / UDP 的標準文件。
- 生成一份標準文件，以定義通用資料模型，用以正式化 LPWAN 的壓縮和分段上下文。
- 產出一份對 LPWAN 設備的操作，管理和維護（OAM）的標準文件，包括對延遲或代理存活性驗證（Ping）的支援。

(2) 相關 RFCs

i RFC 8376 (Low-Power Wide Area Network (LPWAN) Overview, Informational RFC)：低功耗廣域網路(Low-Power Wide Area Network, LPWAN) 是一種涵蓋範圍很廣的無線技術，該網路的頻寬低、封包大小可能很小 、 裝置電池壽命長。本文件涵蓋了多種被 IETF 所考慮進來的 LPWAN 技術介紹，包括 LoRaWAN、NB-IoT、Sigfox 及 Wi-SUN Alliance Field Area Network (FAN)，同時也介紹目前技術和 LPWAN WG 目標間的差異。

ii RFC 8724 (SCHC: Generic Framework for Static Context Header Compression and Fragmentation, Proposed Standard RFC)：定義了靜態語境表頭壓縮及分段(Static Context Header Compression and fragmentation, SCHC)的框架，該框架提供了

表頭壓縮和一個最佳化的分段機制。SCHC 的壓縮是基於儲存在 LPWAN 裝置和網路基礎建設內的共同靜態語境 (Common Static Context) ，此文件定義了一個泛化的表頭壓縮機制和其在 IPv6/UDP 表頭壓縮上的應用。

3、 lwig - 負責制定在資源限制網路節點相容於目前標準且精簡的通訊標準

(1) 工作組說明

通信技術已嵌入到我們的環境中，我們的建築物，車輛，設備和其他物體中的不同類型的設備需要進行通信，並且可以預期大多數設備將採用 IPv6 進行通信。但是，不同類型的設備之間的功能差異很大，並且嵌入所有必需的功能並不是那麼容易。

輕量級實施指南（Light-Weight Implementation Guidance, LWIG）工作組致力於幫助最小裝置上的實作。目標是能夠為最受限制的環境構建最小但具有可交互操作 IP 功能的設備。

(2) 相關 RFCs

i RFC 7228 (Terminology for Constrained-Node Networks, Informational RFC)：該文件敘述了如 Constrained Nodes、Constrained Networks 、 Challenged Networks 、 LLN 和 LoWPAN 的解釋。

ii RFC 7815 (Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation, Informational RFC)：介紹了 IPsec 中用來進行驗證的 IKEv2 通訊協定之最小實作版本，以利資源限制網路節點使用。IKEv2 中有幾個選項特色在此文件的實作中被認為是不需要的特色而被移除，此文件只保留 IKEv2 能正常使用且相容於原版 IKEv2 的實作。

iii RFC 8352 (Energy-Efficient Features of Internet of Things Protocols, Informational RFC)：介紹了具能源效率之通訊協定的挑戰以及現今如何跨越這些挑戰，並總結出鍊路層進行俱能源效率之通訊協定設計時的技巧。本文件同時也提供了不同層在制定俱能源效率之通訊協定時的技巧概覽。

iv RFC 8387 (Practical Considerations and Implementation Experiences in Securing Smart Object Networks, Informational RFC)：敘述了設計安全且資源受限之智能物件的挑戰，並提出一個可以被該種物件使用的部屬模型。該文件也討論了現行密碼程式庫在資源受限裝置上的可用性，並實驗在資源受限裝置上進行數位簽章的效能。最後，該文件探討了不同逼近安全方法的優缺點。

(3) 進行中的 Internet Drafts

i Virtual reassembly buffers in 6LoWPAN (draft-ietf-lwig-6lowpan-virtual-reassembly-02, Date: 2020-03-09)：敘述 6LoWPAN 在進行分段時可能會產生的問題，並提出了方法解決該分段問題。

ii Building Power-Efficient CoAP Devices for Cellular Networks (draft-ietf-lwig-cellular-06, Date: 2016-01-04)：討論了受限應用通訊協定(Constrained Application Protocol, CoAP) 在透過蜂窩網路連接的感測網上的使用。該文件聚焦在如何降低使用功率。

iii Alternative Elliptic Curve Representations (draft-ietf-lwig-curve-representations-10, Date: 2020-04-23)：敘述了如何將 Montgomery curves 和 (twisted) Edwards curves 等橢圓曲線用 short-Weierstrass form 表達，並展示如何使用這個格式實作如 ECDSA 及 ECDH 等橢圓曲線密碼學。

iv TCP Usage Guidance in the Internet of Things (IoT) (draft-ietf-lwig-tcp-constrained-node-networks-09, Date: 2019-11-04)：提供了如何在資源受限裝置上實作輕量化的 TCP 協定的引導。基於 IP 的 IoT 中目前主要的傳輸層協議是 UDP 和 TCP。但是，TCP 通常被不公平的批評為不適用於 IoT 協定。事實上

某些 TCP 功能對於物聯網應用情境不是最佳的，例如相對較長的表頭大小、不適合多播以及始終確認的資料傳遞。但是關於 TCP 不適合物聯網的許多典型主張（例如，高複雜性，連接導向的方法與無線電佔空比的不相容以及無線鏈路中的虛假擁塞控制）是無效的且可以解決的。或者也可以找到公認的物聯網節點到節點可靠性機制。在應用層，CoAP 是使用 UDP (RFC7252)開發的。但是某些 CoAP 部署與現有基礎架構的集成正受到中間節點（如防火牆）的挑戰，這可能會限制甚至阻止基於 UDP 的通訊。這是開發基於 TCP 的 CoAP 規範(RFC8323)的主要原因。

v Terminology for Constrained-Node Networks (draft-bormann-lwig-7228bis-06, Date: 2020-03-09)：敘述了如 Constrained Nodes、Constrained Networks、Challenged Networks、LLN 和 LoWPAN 的解釋，這份文件可能會更新 RFC 7228。

vi Security Classes for IoT devices (draft-urien-lwig-security-classes-03, Date: 2020-05-24)：定義了資源受限裝置的安全分類，使用五個布林指標進行分類：一次性可程式記憶體(one time programmable memory, OTP)、韌體載入器(firmware loader, FLD)、安全韌體載入器(secure firmware loader, FLD-

SEC)、抗竄改密鑰(tamper resistant key, TRT-KEY) 及多元化密鑰(diversified key, DIV-KEY)。

4、 6tisch - IPv6 在 IEEE 802.15.4e 的 TSCH 模式下的規範制定

(1) 工作組說明

低功率有損網路（LLN）可能連接了大量的資源受限節點，以形成無線網狀網絡。 6LoWPAN，ROLL 和 CoRE IETF 工作組在協議堆疊的各個層上定義了協定，包括 IPv6 轉換層，路由協定和 Web 傳輸協定。該協議堆疊已使用在 IEEE802.15.4 低功耗無線電上。

時槽跳頻（TSCH）模式於 2012 年引入，是對 IEEE802.15.4 標準的媒體訪問控制（MAC）部分的修正。 TSCH 是工業自動化和過程控制 LLN 的新興標準，直接繼承自 WirelessHART 和 ISA100.11a。6TiSCH 通過 TSCH 定義了 IPv6，為在工業標準中進一步採用 IPv6 以及將運營技術（OT）與信息技術（IT）融合的關鍵。

6tisch 將致力於通過 IEEE802.15.4 標準的 TSCH 模式啟用 IPv6。其工作組的問題範圍是一個或多個 LLN，可能通過一個或多個 LLN 邊界路由器（LLN Border Router, LBR）透過公共主幹鏈路結合。6tisch 將依賴於現有的 LBR 認證機制，並在必要時進行擴展。

(2) 相關 RFCs

i RFC 8180 (Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration, Best Current Practice RFC)：敘述了 IPv6 over TSCH mode of IEEE 802.15.4e 的最小設定，並定義了連接其他 IETF 通訊協定的介面，該設定應該被所有與 6TiSCH 相容的裝置實作。

ii RFC 8480 (6TiSCH Operation Sublayer (6top) Protocol (6P), Proposed Standard RFC)：敘述了 6TiSCH 的作業子層(Operation Sublayer)的協定，該子層可以使 6TiSCH 網路具有分散式排程的功能。6TiSCH 網路中的所有通信均按排程表進行安排。 排程表由單元格組成，每個單元格均有（slotOffset，channelOffset）標識。 此規範接手定義了尚未被6top工作組定義完成的6TiSCH操作子層(6top)協議(6P)。6P 允許節點與鄰居節點通信，以相互添加/刪除時槽跳頻（TSCH）單元。 這讓節點得以在 6TiSCH 網路中進行分散式排程管理。 6top 由一個或多個調度功能（SF）和此文件中定義的 6top 協議組成。

(3) 進行中的 Internet Drafts

i Constrained Join Protocol (CoJP) for 6TiSCH (draft-ietf-6tisch-minimal-security-15, Date: 2019-12-10)：敘述了新裝置安全加

入 6TiSCH 網路的最小框架，該框架要求新加入的節點和 JRC (join registrar/coordinator, a central entity) 共享一把對稱金鑰，並透過 CoAP 傳送請求的方式取得網路參數並加入 6TiSCH 的網路。

ii 6TiSCH Minimal Scheduling Function (MSF) (draft-ietf-6tisch-msf-16, Date: 2020-04-02)：敘述了 6TiSCH 的最小排程函數 (MSF)，排程函數決定了一個新節點加入網路時的行為及節點間的通訊如何排程。

5、 ipwave - 負責車連網相關的網路通訊協定制定

(1) 工作組說明

越來越多的汽車和車輛連接到網際網路。2020 年左右汽車有望在道路上使用如增強舒適性的娛樂應用、使用雙向資料流的道路安全應用以及聯網的自動駕駛的一些新功能。

如今有幾種已部署的車輛到網際網路技術（V2Internet），它們利用嵌入式網際網路模組或乘客的智慧手機，如 mirrorlink，carplay，android auto。車輛到基礎設施（Vehicle-to-Infrastructure, V2I）通信用於車輛和道路基礎設施之間無線交換重要的安全性和運作資料，主要目的是避免汽車碰撞。車輛到車輛通信（Vehicle-to-Vehicle Communications, V2V）用於車輛之間的短距離通信，以交換車輛信息，

例如車輛速度、前進方向和製動狀態。

ipwave 將研究非常適合以 IP 作為網絡技術的 V2V 和 V2I 使用案例，並將開發基於 IPv6 的解決方案，以在車輛與其他車輛或固定系統之間建立直接和安全的連接。這些車連網的特徵在於動態改變網絡拓撲和連接性。

(2) 相關 RFCs

i. RFC 8691 (Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11, Proposed Standard RFC)：描述了如何使用 IPv6 連接兩個以單一 IEEE 802.11-OCB 鍊路連接在一起的節點。並討論了該方法的相關缺點，此文件並沒有描述最佳化方法及複雜的 IPv6 使用情境，這些議題將在未來的文件被討論。

(3) 進行中的 Internet Drafts

i IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases (draft-ietf-ipwave-vehicular-networking-14, Date: 2020-3-9)：該文件敘述了在車連網使用 IPv6 時的問題描述及使用案例。該文件也描述了車對車(vehicle-to-vehicle, V2V)、車對基設施(vehicle-to-infrastructure, V2I)及車對任何物品(vehicle-to-everything, V2X)的主要情境。

這份文件同時也構成了以 IPv6 為基底的車連網的需求，如鄰居發現、移動性管理、資訊安全及隱私等。

ii Context-Aware Navigator Protocol for IP-Based Vehicular Networks (draft-jeong-ipwave-context-aware-navigator-01, Date: 2020-05-07)：提出了一種語境敏感之導航通訊協定(Context-Aware Navigator Protocol, CAN)，其目標為透過輕量化的資訊共享增進 IP 車連網的駕駛安全性。CAN 使用 IPv6 的鄰居發現協定中的選填欄位傳遞駕駛資訊，如車輛位置、行車速度、加速減速狀態、行使方向及駕駛人的操作。

iii DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks (draft-jeong-ipwave-iot-dns-autoconf-08, Date: 2020-05-07)：描述了一種適用於 IP 車連網的自動網路設定、裝置發現及服務發現方案。此方案中，IoT 裝置的 DNS 名稱可以被自動設定。使用者或是其他 IoT 裝置可以透過 DNS 名稱來識別該裝置。

iv Basic Support for Security and Privacy in IP-Based Vehicular Networks (draft-jeong-ipwave-security-privacy-01, Date: 2020-05-07)：聚焦在 IP 車連網可能的安全及隱私問題，並對這些問題提出對策。可能的攻擊方式有假訊息攻擊、身份偽造攻

擊、服務阻斷攻擊、訊息擱置攻擊、竄改攻擊及追蹤的可能性。

v Vehicular Mobility Management for IP-Based Vehicular Networks (draft-jeong-ipwave-vehicular-mobility-management-03, Date: 2020-05-07)：定義了載具移動管理(Vehicular Mobility Management , VMM) 的方案。此方案為基於多鍊路子網(multi-link subnet)的車連網模型，車輛可在移動時透過該方案傳遞自身的位置及速度資料。

vi Vehicular Neighbor Discovery for IP-Based Vehicular Networks (draft-jeong-ipwave-vehicular-neighbor-discovery-09, Date: 2020-05-07)：定義了 IPv6 鄰居發現協定的擴充—載具鄰居發現協定(Vehicular Neighbor Discovery, VND)。該方法使用了最佳化的地址註冊(Address Registration)及多跳重複位址發現機制(Duplicate Address Detection, DAD)。

vii Considerations for ID/Location Separation Protocols in IPv6-based Vehicular Networks (draft-kjsun-ipwave-id-loc-separation-02, Date: 2020-03-09)：為了達到可擴展的路由、加強移動性及增進隱私，ID/位置分離協定在 IP 車連網中被提出。此文

件分析了要如何將 ID/位置分離協定導入 IP 車連網及提出有效的 ID/位置分離協定建議。

viii Data Aggregation in IPv6-based Vehicular Networks (draft-yan-ipwave-aggregation-01, Date: 2020-05-17)：由於在 IP 車連網中所交換的通常是小且多的訊息，所以為了更有效的交換資料，這份文件描繪了基於訊息中心網路(Information-centric networking, ICN) 的資料聚合的需求，以提昇 IP 車連網中的訊息交換效率。

ix Service and Neighbor Vehicle Discovery in IPv6-Based Vehicular Network (draft-yan-ipwave-nd-06, Date: 2020-05-17)：使用了 DNS-SD/mDNS 去實作 IP 車連網中的鄰居發現及載具的鍊路層位址發現，其目標為協同自適應巡航控制(Cooperative Adaptive Cruise Control, C-ACC)。

6、 6man - 負責 IPv6 的維護、演化、進場以及 IPv4 的退場

(1) 工作組說明

6man 工作組負責 IPv6 協議規範和定址體系結構的維護，維護和改進，並不會對 IPv6 規范進行重大更改或添加。6man 將解決在部署和操作過程中發現的協議限制、問題，同時也是在 IETF 中討論及處理 IPv6 相關問題的適當場所。

6man 是對 IPv6 協定進行擴展和修改的設計機構。6man 可以自行決定審查在另一個工作組中擴展或修改 IPv6 協定的任何文件、進行兩個工作組的 AD 協商並可以向 IESG 建議在這些文件中的任何一個出版前都須和 6man 工作組達成共識。

(2) 相關 RFCs

i RFC 6437 (IPv6 Flow Label Specification, Proposed Standard RFC)：流量標籤為 IPv6 的一大特色，流量標籤使得 IPv6 僅須檢查表頭的固定欄位即可分類流量，提高了分類的效率。此文件為 IPv6 流量標籤的規格書，其中敘述了流量標籤的欄位、IPv6 節點對流量最標籤時的最低要求及流量狀態建立的方式。以網路層的觀點來看，流量是指從同一個來源透過單播、群播、任播的方式送給同一個或是同一群目的地的一連串封包。傳統僅能透過一個五元組(5-tuple)去區分不同的流量，這五個欄位分別是來源位址、來源連接阜、目的位址、目的連接阜及傳輸層類型，但是，這其中有些欄位常常因為分段或是加密的原因使得他們讀會同時出現在同一個封包，因此 IPv6 採用以流量標籤、來源位址及目的位址所構成的三元組來區分各個流量，如此便能更有效率的進行流量的分類。

ii RFC 6438 (Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels, Proposed Standard RFC)：流量標籤使用上固然方便，但是其有一些使用限制。此文件便在描述流量標籤在使用多氣徑路由進行負載平衡並面對相同路徑成本的多條路徑時的使用限制。

iii RFC 6553 (The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, Proposed Standard RFC)：描述低功耗且易遺失路由協定(Routing Protocol for Low-Power and Lossy Networks, RPL) 的選項欄位，該選項欄位能儲存如路由訊息等資訊。

iv RFC 6554 (An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL), Proposed Standard RFC)：低功耗且易遺失路由協定(Routing Protocol for Low-Power and Lossy Networks, RPL) 為低功耗且易遺失網路上的一種重要的路由協定，通常運作在記憶體受限制的網路節點上。為此，本文件制定了一個新的 IPv6 路由表頭選項，使得可以 IPv6 節點可以使用 RPL 進行路由。

v RFC 6935 (IPv6 and UDP Checksums for Tunneled Packets, Proposed Standard RFC)：為了增進 UDP datagram 使用 IPv6

隧道進行傳輸時的效率，本文件描述了一種透過放寬 IPv6 UDP 校驗和的需求來增進效能的方式。

vi RFC 6946 (Processing of IPv6 "Atomic" Fragments, Proposed Standard RFC)：IPv6 的規格內允許封包含有分段表頭但是該封包卻不會分段，這種封包稱為原子分段(Atomic Fragments)。這種封包通常是被那些收到 ICMPv6 “Packet Too Big”錯誤訊息的節點所發出，用來建議 Next-Hop MTU 設定為小於 1280 bytes 並開始傳送分段流量。此文件在討論原子分段的產生以及相關的資訊安全議題。

vii RFC 6980 (Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery, Proposed Standard RFC)：分析使用了 IPv6 分段的鄰居發現之安全議題，並討論了使用 IPv6 分段和安全鄰居發現 (SEcure Neighbor Discovery, SEND) 如何減輕上述問題。

viii RFC 7048 (Neighbor Unreachability Detection Is Too Impatient, Proposed Standard RFC)：敘述了一個潛藏在 IPv6 鄰居發現協定裡的一個會造成效能下降的問題—鄰居不可達偵測(Neighbor Unreachability Detection)，發生問題的是其預設等待時間為三秒。對於沒有替代鄰居(alternative neighbors)的情

境下，預設等待時間顯的有點冗長。因此此文件提出一套相對寬鬆的鄰居發現規則以改善上述問題。

ix RFC 7217 (A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC), Proposed Standard RFC)：當使用者改變其通訊介面時，舊有的方法會根據新的 MAC Address 產生新的介面識別碼(Interface Identifier, IID)，造成使用者使用無狀態位址自動設定(Stateless Address Autoconfiguration, SLAAC) 時會在網路上遷移。此文件提出了一種新的介面識別碼產失機制，該方法在使用者切換通訊介面時並不會改變通訊介面識別碼，進而不會影響到無狀態位址自動設定及使用者在網路上的位置，其最大優點是可以在不犧牲使用者隱私權的前提下讓使用者在網路上的位置可以固定。

x RFC 8781 (Discovering PREF64 in Router Advertisements, Proposed Standard RFC)：具有 DNS 擴展的 NAT64（RFC6146）網路地址轉換（DNS64）（RFC6147），是一種廣泛部署的機制，用於在純 IPv6 的網路上提供 IPv4 存取。 在各種情況下，主機必須知道網路正在使用的 NAT64 前綴。 此文件指

定在路由器建議（Router Advertisements, RA）中使用的鄰居發現（RFC4861）選項將 NAT64 前綴傳達給主機。

(3) 進行中的 Internet Drafts

i Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers (draft-ietf-6man-grand-00, Date: 2020-03-09)：IPv6 使用鄰居發現來決定和鄰居節點的鏈路位址，該文件敘述了當新的 IPv6 位址被分配到新節點上時，路由器可以主動建立鄰居的快取紀錄(Neighbor Cache entry)以降低和新節點建立連線時因鏈路尚未初始化所造成的封包遺失。

ii IPv6 Neighbor Discovery on Wireless Networks (draft-thubert-6man-ipv6-over-wireless-05, Date: 2020-03-31)：介紹了在無線網路的環境下如何進行無線鄰居發現(Wireless Neighbor Discovery, WiND)。WiND 透過將鄰居發現封包透過 Host Router 轉送來避免用無線廣播來建立連居。

iii IPv6 Source Routing for ultralow Latency (draft-foglar-ipv6-ull-routing-06, Date: 2020-01-2)：介紹了 IPv6 的階層式的定址方案，透過盡量簡化的架構加速 Source Routing 的速度。

7、 dhc - 負責如 DHCPv6 等自動網路組態設定協定之制定

(1) 工作組說明

動態主機配置工作組（Dynamic Host Configuration Working Group, DHC WG）開發了 DHCP，用於自動分配、配置和管理 IP 地址、IPv6 前綴、IP 協定堆疊和其他參數。 DHCPv4 目前是草案標準，並在 RFC 2131 和 RFC 2132 中進行了記錄。DHCPv6 目前是提議的標準，正在更新中。 dhc 計劃將 DHCPv6 協定提升到網際網路標準。

(2) 相關 RFCs

i RFC 7341 (DHCPv4-over-DHCPv6 (DHCP 4o6) Transport, Proposed Standard RFC)：描述了如何在 IPv6 的網路中動態獲取 IPv4 的設定。該方法是將 DHCPv4 的封包訊息透過 DHCPv6 傳輸，為此 dhc 制定了兩種新的 DHCPv6 訊息及兩個新的選項。

ii RFC 7653 (DHCPv6 Active Leasequery, Proposed Standard RFC)：描述了 DHCPv6 的租賃查詢，此機制可以請求者對 DHCP 伺服器發出配對資料的請求。同時 DHCPv6 也支援使用 TCP 進行連續的查詢。

iii RFC 8156 (DHCPv6 Failover Protocol, Proposed Standard RFC)：描述了 DHCPv6 的降級通訊協定。該文件也提到在同一個

broadcast domain 有兩台不同版本的 DHCP Server 可能會造成伺服器錯誤或是網路分割。

iv RFC 8415 (Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Proposed Standard RFC)：介紹了用於 IPv6 的動態主機配置協議(DHCPv6)：一種用於使用網路配置參數、IP 地址和前綴配置節點的可擴展機制。可以無狀態提供參數，也可以結合一個或多個 IPv6 地址和/或 IPv6 前綴的有狀態分配來提供參數。DHCPv6 可以代替無狀態地址自動配置(SLAAC)或在其之外運行。此文件描述了 DHCPv6 的詳細規格，包含 Operational Models、Message Format, Rely, Agents...等。

v RFC 8539 (Softwire Provisioning Using DHCPv4 over DHCPv6, Proposed Standard RFC)：基於 DHCPv6 的 DHCPv4(RFC 7341)是一種動態配置 IPv4 的機制，以在純 IPv6 網路中用作上層服務。Softwire 就是這種服務的一個例子。為了使 DHCPv4 over DHCPv6（DHCP 4o6）與某些 IPv4 over IPv6 Softwire 機制和部署方案（例如 RFC 7596 或 RFC 7597）一起工作，運營商需要知道客戶端將用作 IP 地址來源的 IPv6 地址。IPv4-in-IPv6 Softwire 隧道。該地址與客戶端的 IPv4 地址以及(在某些部署中)連接阜集 ID 一起用於在運營商的 Softwire

隧道集中器中建立綁定表條目。此文件定義了一個 DHCPv6 選項，以傳達用於建立 Softwire 隧道的 IPv6 參數，以及一個 DHCPv4 選項（僅與 DHCP 4o6 一起使用），以在 DHCP 4o6 客戶端和伺服器之間傳遞來源隧道 IPv6 地址。 它旨在與 IPv4 地址分配過程結合使用。

8、 v6ops - 蒐集 IPv6 營運商和使用者所產生的問題及解決方案

(1) 工作組說明

IPv6 的全球部署正在進行中，這創造了一個由單純 IPv4、單純 IPv6、IPv4-IPv6 Dual Stack 以及 IPv6 +轉換網路的節點組成的網際網路。 必須正確處理此部署，以避免將網際網路劃分為單獨的 IPv4 和 IPv6 網絡，從而確保所有 IPv4 和 IPv6 節點的定址和連接性。IPv6 運營工作組（IPv6 Operations, 6ops）為新的和現有的 IPv6 網路部署和運營製定了指南。

(2) 相關 RFCs

i RFC 7526 (Deprecating the Anycast Prefix for 6to4 Relay Routers, Best Current Practice RFC)：經過實驗證實，RFC 3056 所提出的 6to4 的機制並不適合大量部屬且不適合網際網路的任播路由拓樸。因此，此文件要求 RFC 3068 及 RFC 6732 應該被設置為過期的狀態。

ii RFC 8215 (Local-Use IPv4/IPv6 Translation Prefix, Proposed Standard RFC)：說明 IPv6 中的前綴 64:ff9b:1::/48 應該被保留給本地的 IPv4/IPv6 轉譯使用。

iii RFC 8305 (Happy Eyeballs Version 2: Better Connectivity Using Concurrency, Proposed Standard RFC)：在現代網際網路上運作的許多通訊協定都使用主機名稱。 這些主機名稱通常解析為多個 IP 地址，每個 IP 地址可能具有不同的性能和連接特性。 由於特定的地址或地址族（IPv4 或 IPv6）在網路上可能被阻止、破壞或不理想，因此嘗試並行進行多個連接的客戶端可以更快地建立連接。 此文件指定了減少該用戶建立連線延遲的演算法要求，並提供了番理演算法，稱為「Happy Eyeballs」。

(3) 進行中的 Internet Drafts

i Neighbor Cache Entries on First-Hop Routers: Operational Considerations (draft-ietf-v6ops-nd-cache-init-01, Date: 2019-12-10)：這份文件在探討當使用鄰居快取(Neighbor Cache Entries)並且一個新的 IPv6 位址被使用時，first-hop router 上的狀態機會出問題。

9、 ipsecme - 維護及擴充前代 IPsec 工作組所制定的 IPsec 協議

(1) 工作組說明

IPsec 協議套件包括 IKEv1（RFC 2409，現已淘汰），IKEv2（RFC 7296）和 IPsec 安全體系結構（RFC 4301）。 IPsec 廣泛部署在閘道器及 VPN 遠端存取客戶端中，並作為主機到主機、主機到網路和網路到網路安全性的基礎。

IPsec 維護和擴展工作組(IPsec Maintenance and Extensions, ipsecme)繼續了 2005 年結束的早期 IPsec 工作組的工作。其目的是維護 IPsec 標準並促進對 IPsec（主要是 ESP 和 IKEv2）的澄清，改進和擴展的討論。 該工作組還作為其他在其自己的協議中使用 IPsec 的 IETF 工作組的焦點。

(2) 進行中的 Internet Drafts

i IP Traffic Flow Security (draft-ietf-ipsecme-iptfs-01, Date: 2020-03-02)：介紹了一種增進 IPsec 流量安全的機制，運作原理為使用固定大小的流量和頻率來增加流量機密性。流量分析是提取有關通過網路發送資料的信息的操作。儘管可能會通過使用加密(RFC4303)直接遮蓋資料，但流量模式本身會由於其形狀和時間的變化而暴露信息。隱藏流量的大小和頻率根據(RFC4303)被稱為流量流機密性(Traffic Flow Confidentiality, TFC)。RFC4303 透過將填充添加到加密的 IP

封包並允許傳輸所有填充封包（使用協議 59 表示）來提供 TFC。這種方法的主要局限性在於它可能會嚴重利用可用頻寬。IP-TFS 解決方案提供了完整的 TFC，而沒有上述頻寬限制。為此，我們使用具有固定大小的封裝封包的恆定發送速率 IPsec (RFC4303)隧道。但是，這些固定大小的封包可以包含部分、整個或多個 IP 數據包，以最大化隧道的頻寬。另外，IP-TFS 提供了處理網絡擁塞的功能(RFC2914)。當 IP-TFS 使用者無法完全控制 IP-TFS 隧道路徑流經的網路領域時，這非常重要。

第二節　DN (Domain Name)

一、DNS 歷史

DNS 是因為網路的增長而發展，在 20 世紀 70 年代的時候，ARPAnet 是一個只有幾百台主機的小型社區，原來的主機名稱到位址的映射存在網路介面控制器 NIC(Network Information Center)所維護的 HOSTS.TXT 文件中，而每個主機都是由 FTP 將其傳輸，隨著網路的發展，這種傳輸方式對 NIC 的主機造成很大的負擔。網路性質不斷的在做改變，區域組織能夠管理自己的名稱與地址，但需要等到 NIC 將 HOSTS.TXT 修改才能有所改變，因此他們希望能有自己的命名空間結構。在網路應用越來越複雜之下，需要一個普遍的管理方式，因

此採用階層式的命名空間，以“ . ”分隔不同的階層。而以下幾點為 DNS 的設計目標:

1. 最主要的目標為要有一致的命名空間，為了避免臨時的編碼引起的問題，名稱中不需包含網路標示符、地址、路由等訊息。
2. 數據庫龐大的規模與更新頻率、創建與刪除名稱的機制，都須以分佈式的方式維護。
3. 要在獲取數據的成本、更新速度和緩存的準確性之間達到平衡。
4. 應用應相當普遍，能從名稱找回地址、信箱數據和其他尚未確定的訊息，且將與名稱有關聯的數據都歸類成一個類別，在查詢時能限制單一類別做查詢。
5. 能因應不同類型的網路和應用，提供不同協議或地址格式類型的服務。
6. 期望名稱服務器獨立承載通訊系統，其他服務僅需提供虛擬電路即可使用。
7. 系統能廣泛使用於不同類型的主機。

二、DNS 結構

(一) 域名空間

域名空間由樹狀結構組成。樹中的每個節點或葉子都有一個標籤和零個或多個資源記錄（RR），其中包含與域名關聯的訊息。域名本身由標籤組成，該標籤與其右邊的父節點名稱連接在一起，並用點分隔。

該樹為從根區域開始的區域。一個 DNS 區域可以由只有一個域，或者由多個域和子域，這取決於區域經理的管理選擇。還可以根據類對 DNS 進行分區，其中可以將單獨的類視為並行的名稱空間樹。

可以通過創建其他區域來劃分對任何區域的管理責任。當新區域的授權被委派給指定的名稱服務器。父區域不再對新區域具有權威性。

1、 域名語法

域名由一個或多個部分，每個部分稱為標籤，當用戶需要輸入網域名稱時，將省略每個標籤的長度，並且標籤之間使用“.”作為分隔。例如：example.com，而 example 與 com 都是一個標籤。

網域名稱的標籤由左至右讀取，表示最遠離根到最接近根。左側的每個標籤都指定右側域的細分或子域。例如：標籤示例指定 com 域的子域，而 www 是 example.com 的子域。此細分樹最多可包含 127

個級別，最右邊的標籤為頂級域名，例如：域名 www.example.com 中的 com 屬於頂級域名。

每個標籤可以包含 0 到 63 個字符。長度為零的空標籤保留給根區域，而完整域名的文字表示形式不得超過 253 個字符。在 DNS 的內部二進制表示中，最大長度需要 255 個八位元組的存儲，因為它還存儲名稱的長度。儘管不存在使用八位字節表示的域名標籤中使用任何字符的技術限制，但主機名使用首選格式和字符集。標籤中允許使用的字符是 ASCII 字符集的子集，由 ASCII 字符 a 到 z，A 到 Z，數字 0 到 9 和連字符號組成，此規則稱為 LDH（Letters-Digits-Hyphen）規則（字母、數字、連字符）。雖然英文的大小寫都可以使用，但是網域名稱是不區分英文字母大小寫。標籤不能以連字符號開頭或結尾。附加規則為頂級域名不應為全數字。

DNS 中允許的一組有限的 ASCII 字符阻止了許多語言的名稱和單詞用其本機字母或腳本表示。為此，ICANN 批准了應用程序國際化域名（IDNA）系統，通過該系統，用戶應用程序（例如 Web 瀏覽器）可以使用 Punycode 將 Unicode 字符串映射到有效的 DNS 字符集中。ICANN 在 2009 年批准了國際化域名國家/地區代碼頂級域名（ccTLD）的安裝。圖 96 為命名空間示例，在此示例中，根網域具有三個直接子網域：MIL、EDU 和 ARPA。LCS.MIT.EDU 網域具有

一個名為 XX.LCS.MIT.EDU 的直接子網域。而所有的葉子也都是網域。

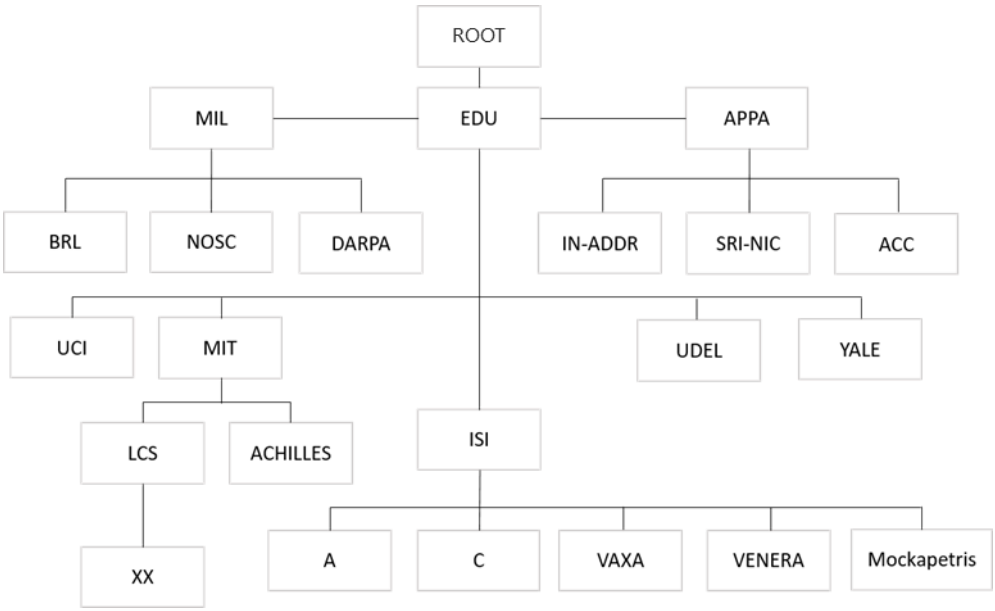


圖 96、命名空間示例

(1) IDNA(Internationalizing Domain Names in Applications)

國際化域名（Internationalized Domain Name，IDN）的發展一直是全球關心的議題之一。由於全球 80%以上的使用者來自非英語系的國家，多年來 IDN 標準的差異，造成上百萬個 IDN 網址存在著許多互通性與相容性的問題，而長期致力於 IDN 標準的發展與研究的 IETF 於 2003 年發布了國際化域名技術標準相關的 RFCs，分別為 RFC 3490、3491 和 3492，這些標準為 IDN 提供了技術指導，而 IDN 是一種以標準方式處理域名中非 ASCII 字符的機制，它通過將具有非 ASCII 字符的名稱轉換為域名系統可以理解的 ASCII 標籤來作業。隨

後，在 2010 年發布了 6 篇與 IDNA 相關的 RFC，分別為 RFC 5890、5891、5892、5893、5894 與 5895，其中 RFC 5890 廢除了 RFC 3490，並描述了國際化應用程序域名修訂版的協議和使用環境，而 RFC 5891 則是廢除 RFC 3491，內容則為國際化域名（IDNs）的修訂協議定義。

國際化域名又稱特殊字元域名，是指部分或完全使用特殊的文字或字母組成的網際網路域名，包括法語、阿拉伯語、中文、斯拉夫語、泰米爾語、希伯來語或拉丁字母等非英文字母，這些文字經多位元組萬國碼編譯而成。在域名系統中，國際化域名使用 Punycode 轉寫以 ASCII 字符串格式儲存。

域名系統的建立是為了將網路搜尋用語變成更加通俗易懂的語言，但由於技術限制和長久實踐，域名使用美國資訊交換標準代碼字元已成為慣用標準。國際化域名通過將各種非英語字元轉化成與現有域名系統相容的 ASCII 字串，並儲存在域名系統中，使得世界各地的用戶可以直接使用他們的母語輸入域名。並且這種技術並不需要對網際網路結構做任何改變。

對於支持 IDNA 的應用程序，有效標籤的兩種類型為 A 標籤、U 標籤，以下分別定義。

A-label 是 IDNA 有效字符串的 ASCII 兼容編碼（ACE）。它必須

是完整的標籤，IDNA 是為標籤定義的，而不是標籤的一部分，也不是完整的域名。根據定義，這意味著每個 A 標籤都將以 IDNA ACE 前綴“ xn-”開頭，後跟一個字符串，該字符串是 Punycode 算法的有效輸出，因此最多 59 個 ASCII 字符的長度。前綴和字符串必須一起滿足可存儲在 DNS 中的標籤的所有要求。當且僅當滿足以上要求的字符串可以解碼為 U 標籤時，它才是 A 標籤。

U-label 是 IDNA 有效的 Unicode 字符串，以規範化形式 C（NFC）且包括至少一個非 ASCII 字符，以標準 Unicode 編碼形式（例如 UTF-8）表示。U 標籤和 A 標籤之間的轉換是根據 Punycode 規範執行的，根據需要添加或刪除 ACE 前綴。

(2) 名稱服務器

名稱服務器是構成網域資料庫的資訊儲存庫。資料庫被劃分稱為區域，這些區域分佈在名稱服務器之間。雖然名稱服務器可以具有多個選擇性功能和資料來源，但名稱服務器的基本任務是使用其區域中的數據回答查詢。根據設計，名稱服務器可以以簡單的方式回答查詢；回覆始終可以僅使用本地數據生成，並且包含對問題的答案或引用其他具有更接近所需資訊的名稱服務器。儘管主機或通訊鏈路出現故障，以確保其可用性給定區域將從多個名稱服務器獲得。根據管理法，我們要求每個區域至少可在兩台服務器上使用，而且許多區域具有更多

的冗餘。給定的名稱服務器通常支持一個或多個區域，但這只為提供有關網域樹的一小部分的權威資訊，它可能還緩存了一些關於樹其他部分的非權威數據。名稱服務器標記其對查詢的回覆，以便請求者能夠判斷回覆是否來自權威數據。

名稱服務器的主要功能是回答標準查詢，查詢及其回覆都以標準訊息格式進行。查詢包含 QTYPE、QCLASS 和 QNAME，用於描述所需資訊的類型和類別以及感興趣的名稱。

名稱服務器回答查詢的方式取決於它是否在遞迴模式下運行：

- 服務器最簡單的模式是非遞迴模式，因為它只能使用本地資訊應答查詢，回覆包含錯誤、答案或引用到某些其他更接近答案的服務器。所有名稱服務器都必須實現非遞迴查詢。
- 用戶端最簡單的模式是遞迴模式，因為在此模式下，名稱服務器充當解析器的角色，並返回錯誤或答案，但從不引用。此服務在名稱服務器中是可選擇的，名稱服務器也可以選擇使用遞迴模式的用戶端。

i　根名稱服務器

每個遞歸解析器都知道 13 個 DNS 根名稱服務器，它們是遞歸解析器對 DNS 記錄的搜尋的第一站。根服務器接受包含域名的遞歸解

析器的查詢，根名稱服務器根據該域的擴展名（.com，.net，.org 等），通過將遞歸解析器定向到 TLD 域名服務器進行回覆。根名稱服務器由一家名為 Internet for Assigned Names and Numbers（ICANN）的非營利組織監督。

請注意，儘管有 13 個根名稱服務器，但這並不意味著根名稱服務器系統中只有 13 台計算機。根名稱服務器有 13 種類型，但是在世界範圍內每種都有多個副本，它們使用 Anycast 路由提供快速回覆。

ii TLD(Top-Level Domain)名稱服務器

TLD 名稱服務器維護所有共享通用域擴展名的域名的訊息，例如.com，.net 或 url 中最後一個點之後的任何內容。例如.com TLD 名稱服務器包含以'.com'結尾的每個網站的信息。如果用戶正在搜索 google.com，則在收到根域名服務器的回覆後，遞歸解析器將向.com TLD 名稱服務器發送查詢，該查詢將通過指向該域的權威名稱服務器進行回覆。

TLD 名稱服務器的管理由互聯網名稱與數字地址分配機構（IANA）處理，該機構是 ICANN 的一個分支機構。IANA 將 TLD 服務器分為兩種：

- 通用頂級域名：這些不是特定國家或地區的域名，以下是一些最知名的通用 TLD

.com　商業組織

.org　非營利組織和其他

.net　主要網絡支持中心

.edu　教育機構

.gov　政府機構

.int　國際組織

.mil　軍事團體

- 國家/地區代碼頂級域: 這些域包括特定於某個國家或州的任何域。例如: .uk、.us、.ru 和.jp。

iii　權威名稱服務器

當遞歸解析器從 TLD 名稱服務器收到回覆時，該回覆會將解析器定向到權威名稱服務器。權威的名稱服務器通常是解析器在 IP 地址過程中的最後一步。權威名稱服務器包含特定於它所服務的域名的信息（例如 google.com），它可以為遞歸解析器提供在 DNS A 記錄中找到的服務器的 IP 地址，或者該域具有 CNAME 記錄（別名）它將為遞歸解析器提供一個別名域，此時遞歸解析器將必須執行一個全新的 DNS 查找，以從權威名稱服務器中獲取一條記錄（通常是一個包含 IP 地址的 A 記錄）。

三、運作方式

圖 97 為 DNS 查詢的流程：

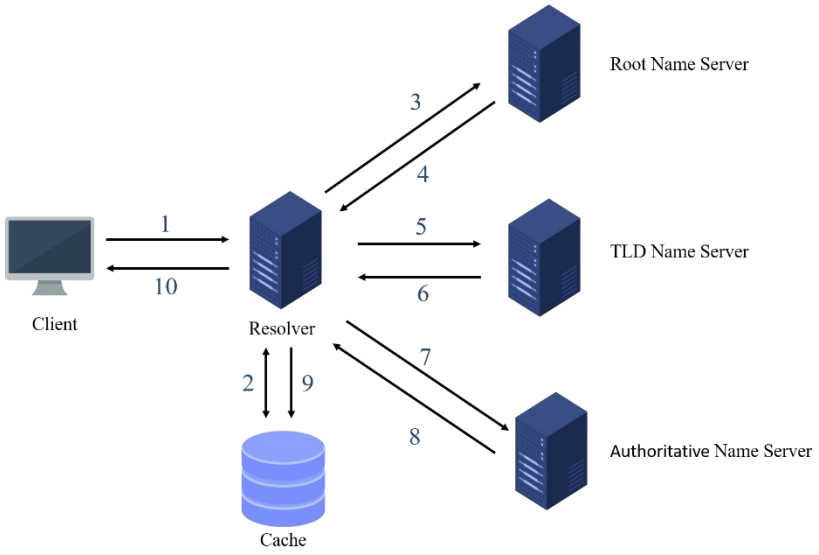


圖 97、DNS 查詢的流程

假設用戶在瀏覽器中查詢“example.com”，查詢步驟如下:

1. 查詢進入網路中，並由 DNS 解析器接收
2. 解析器檢查緩存是否已經具有該名稱的地址，如果存在，將會傳回地址至瀏覽器。在此假設不存在
3. 解析程序查詢 DNS 根名稱服務器
4. 根名稱服務器返回 .com 域的名稱服務器的名稱和地址
5. 解析程序向.com TLD 名稱服務器發出請求
6. TLD 名稱服務器返回 example.com 域的名稱服務器的名稱和地址
7. 遞歸解析器將查詢發送到 DNS 權威名稱服務器
8. example.com 的 IP 地址從名稱服務器返回到解析器

9. 解析器緩存訊息

10. 解析器將地址提供至瀏覽器讓使用者使用。

(一) 解析器

解析器是將用戶程序連接到網域名稱服務器的程序。在最簡單的情況下，解析器以子程序呼叫、系統調用等形式從用戶程序（例如：郵件程序、TELNET、FTP）接收請求，並返回與本地主機資料格式相容的資訊。解析器與請求解析程序服務的程序位於同一台電腦上。但解析器可能需要查詢多個名稱服務器，或者可能在本地緩存中擁有請求的訊息，所以解析程序完成所需的時間可能會有所不同，從毫秒到幾秒鐘。解析器的一個重要目標是通過從先前結果的緩存中應答這些請求來消除網路延遲和名稱服務器負載。因此，由多個進程、使用者、計算機等共用的緩存比非共用緩存更有效。而解析器分為兩種，分別為存根解析器與遞歸解析器

1、 存根(Stub)解析器

假設在瀏覽器上輸入 www.google.com 時，瀏覽器會向操作系統詢問 IP 地址。該操作系統具有所謂的存根解析器，這是一個簡單的解析器，用於處理該操作系統的所有 DNS 查找。解析程序將 DNS 查詢發送到指定的遞歸解析程序（名稱服務器），並根據其 TTL 將記錄存儲在其緩存中。當存根解析器從應用程序獲取請求時，它首先在其

緩存中查找，如果有記錄，它將信息提供給應用程序。如果沒有，它將向遞歸解析器發送 DNS 查詢。

2、 遞歸解析器

遞歸解析器充當客戶端和 DNS 名稱服務器之間的中間人。從客戶端收到 DNS 查詢後，遞歸解析器將以緩存的數據作為回覆，或者將請求發送到根名稱服務器，然後將另一個請求發送到 TLD 名稱服務器，再將最後一個請求發送到權威名稱服務器。收到包含請求的 IP 地址的權威名稱服務器的回覆後，遞歸解析器將回覆發送給客戶端。在此過程中，遞歸解析器將緩存從權威名稱服務器接收的訊息。當一個客戶端請求另一個客戶端最近請求的域名的 IP 地址時，解析程序可以繞過與名稱服務器通信的過程，而只是從客戶端的緩存中傳遞所請求的記錄。

(二) 記錄緩存

在應用程序中實現名稱解析的標準做法是通過在本地或解析器主機中緩存結果來減少域名系統服務器上的負載。從 DNS 請求獲得的結果始終與生存時間（TTL）相關聯，當生存時間為過期時間，就必須丟棄或刷新結果。TTL 由權威 DNS 服務器的管理員設置。有效期可能從幾秒鐘到幾天甚至幾週不等。

由於採用了這種分佈式緩存體系結構，對 DNS 記錄的更改不會

立即在整個網絡中傳播，而是要求所有緩存在 TTL 之後過期並進行刷新。RFC 1912 傳達了確定適當 TTL 值的基本規則。

一些解析器可能會覆蓋 TTL 值，因為該協議支持長達 68 年的緩存或根本不支援緩存。負緩存，即記錄不存在的事實的緩存，由區域內具有權威性名稱服務器確定，當報告不存在所請求類型的數據時，該區域必須包括授權開始（SOA）記錄。SOA 記錄的最小字段的值和 SOA 本身的 TTL 用於建立否定答案的 TTL。

而 RFC 2308 取代了 RFC1034 第 4.3.4 節中有關負緩存的描述，將一個根本性的缺陷，也就是不允許名稱服務器將那些緩存的回覆分發給其他解析器，從而大大降低了緩存效果的問題，依據經驗解決了問題。

(三)　查詢

查詢就是向名稱服務器要求回覆的一個請求。在網路中，查詢以 UDP 或 TCP 傳輸。名稱服務器的回覆可能回答查詢中提出的問題，也可能將請求者引用到另一組名稱服務器，或發出一些錯誤條件的訊號。

通常用戶不會直接查詢，而是會向解析器發出請求，而解析器又會將一個或多個查詢發送到名稱服務器，並處理可能導致的錯誤條件和引用。查詢中所提出的問題會影響解析器可以提供的服務類型。

訊息格式具有一個標頭，其中包含許多始終存在的固定欄位，以及包含查詢參數和 RR 的四個部分。標頭中最重要的欄位是一個稱為操作碼的四位欄位，用於分隔不同的查詢。

1、 標準查詢

標準查詢指定目標網域名稱（QNAME）、查詢類型（QTYPE）和查詢類（QCLASS），並請求匹配的 RRs。這種查詢構成了絕大多數的 DNS 查詢，而此查詢分為兩種，分別為遞迴查詢與迭代查詢。

遞迴查詢(Recursive DNS Query): DNS 用戶端向 DNS 伺服器發出查詢請求，如果 DNS 伺服器裡面沒有所需要的資料，則 DNS 伺服器會代替用戶端向其他的 DNS 伺服器進行查詢，其他的 DNS 伺服器如果也沒有所需要的資料，則再向它的 DNS 作業系統請求，如果這個時候 DNS 伺服器有相關對應資料，則會先回饋給之前的 DNS 伺服器，再依次回饋到最開始的 DNS 伺服器，直到 DNS 的用戶端得到資料。這種傳遞方式，DNS 伺服器必須向用戶端做出回答，一般由 DNS 用戶端提出的查詢都是遞迴查詢。而圖 98 為遞迴查詢過程的示意圖。

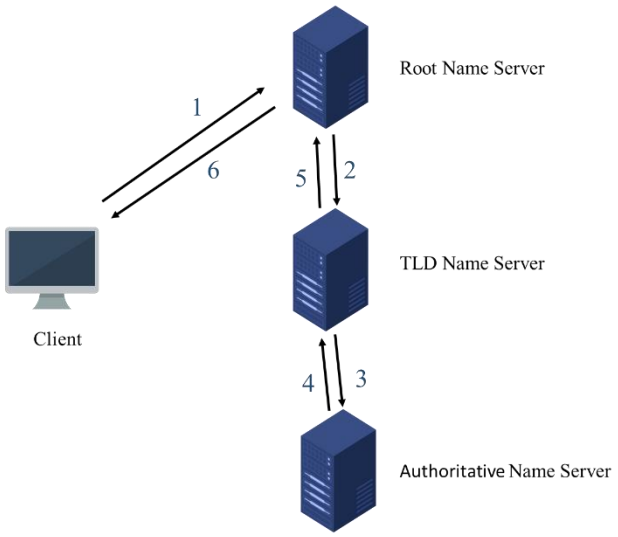


圖 98、遞迴查詢過程

迭代查詢(Iterative DNS Query)：DNS 用戶端向 DNS 伺服器發出查詢請求，如果 DNS 伺服器裡面沒有所需要的資料，則第一台 DNS 伺服器會告訴用戶端它的 DNS 伺服器的 IP 位址，由 DNS 用戶端直接和第一台 DNS 伺服器提出查詢請求，如果第一台 DNS 伺服器也沒有資料，則第一台 DNS 伺服器會告訴用戶端它的 DNS 伺服器，即第二台 DNS 伺服器，用戶端直接和第二台伺服器提出請求，直到找到資料為止。讓 DNS 用戶端利用自己的 IP 位址查詢它的主機名稱。而圖 99 為迭代查詢過程的示意圖。

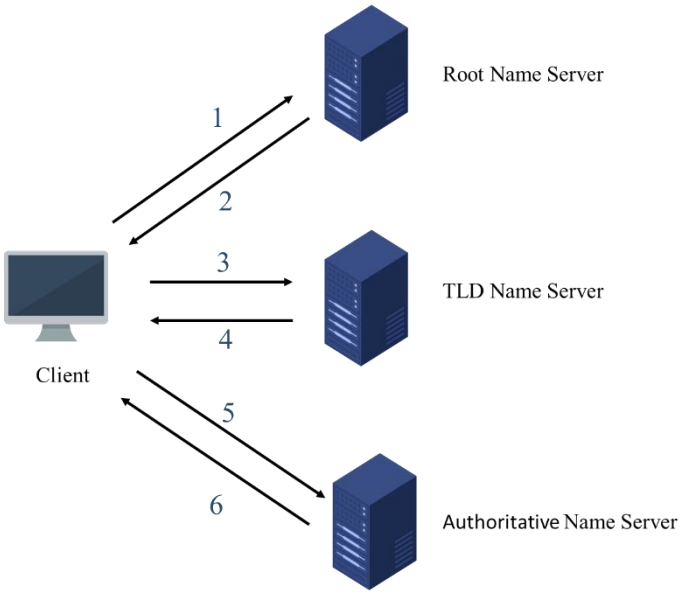


圖 99、迭代查詢過程

而遞迴查詢與迭代查詢的差異在於，在遞歸查詢中，客戶端僅需將查詢發送到第一台服務器，然而服務器將請求發送到下一個服務器，直到查詢被解決。迭代查詢則是客戶端需負責將查詢發送到不同的服務器，直到查詢被解決。

2、 反向查詢

反向查詢是依據 DNS 用戶端提供的 IP 位址來查詢它主機名稱，由於 DNS 名字空間中功能變數名稱與 IP 位址之間無法建立直接對應關係，所以必須在 DNS 伺服器內創建一個反向查詢區域。DNS 以域名形式將 IP 地址存儲為基礎結構頂級域 arpa 中的指針（PTR）記錄中的特殊格式名稱。對於 IPv4，該域為 in-addr.arpa。對於 IPv6，反向查詢域是 ip6.arpa。

名稱服務器可能支援網域名稱或將特定資源映射到具有該資源網域名稱的反向查詢。例如雖然標準查詢可能會將網域名稱映射到 SOA RR，但相應的反向查詢可能會將

映射回網域名稱。

此服務在名稱服務器中是可以選擇的，但所有名稱服務器至少必須能夠理解反向查詢訊息並返回未實現的錯誤回覆。網域系統無法保證反向查詢的完整性或唯一性，因為網域系統是按照網域名稱而不是主機位址或任何其他資源類型而組成。反向查詢主要用於錯誤偵測和資料庫維護。

反向查詢可能不會返回正確的 TTL，也不會指出標識的 RR 是集合之一，例如具有多個位址的主機位址。因此，絕不應緩存反向查詢中返回的 RR。

反向查詢不是將主機位址映射到主機名的可接受方法。

(四) DNS 的傳輸

因 UDP 的傳送方式能讓 DNS 伺服器負載更低且回應得更快速，因此大多數 DNS 事務都通過 UDP 進行，雖然 UDP 封包的最大長度為 512 位元組，但用戶端向 DNS 伺服器查詢域名時，一般返回的內容都不超過 512 位元組。

TCP 則用於區域傳輸（zone transfer），區域傳輸就是當輔助 DNS 伺服器啟動，需要與主 DNS 伺服器通訊，並載入資料資訊時就是所謂的區域傳輸，而 TCP 通常用於大小超過 DNS 協議原始 512 字節限制的郵件。DNS 安全性和 IPv6 的不斷增長的部署增加了回覆大小，因此增加了 TCP 的使用。它提供了防止對地址欺騙 DNS 的反射/放大攻擊的保護，也推動了對 TCP 使用量的增長的需求。現在，它已廣泛用於回覆速率限制。另外，DNS 隱私解決方案（例如基於 TLS 的 DNS）上的工作是重新審視基於 TCP 的 DNS 要求的另一個動機。而以下幾點為 TCP 的特性:

- 持久連接：TCP 連接在發送第一個回覆後不會被服務器關閉，在收到第一個回覆後也不會被客戶端關閉。
- 連接重用：通過單個 TCP 連接發送多個查詢和回覆。
- 閒置 DNS-over-TCP 期間：客戶端和服務器以不同的方式查看應用程序級的空閒狀態。當沒有任何待發送的查詢要發送且沒有未完成的回覆時，DNS 客戶端會認為已建立的 TCP 上 DNS 會話處於空閒狀態。當 DNS 服務器已發送對在該連接上收到的所有查詢的回覆時，則認為已建立的 TCP 上 DNS 會話處於空閒狀態。

- 管線：通過單個 TCP 連接發送多個查詢和回覆，但在發送另一個查詢之前不等待任何未完成的答覆。
- 亂序處理：同時處理查詢，並在可能的情況下盡快將單個回覆返回。 這很可能發生在遞歸服務器中。然而，也有可能在權威服務器，例如:具有不同的後端數據存儲。

(五) IPv6

由於應用程序假定地址查詢僅返回 32 位 IPv4 地址，因此 IPv6 地址對域名系統中 Internet 地址存儲無法輕易地擴展。為了支持 IPv6 地址在 DNS 中的存儲，定義了以下擴展，讓 DNS 能支援 IPv6 地址：

- 定義了資源記錄類型以將域名映射到 IPv6 地址。
- 定義了一個域以支持基於地址的查詢。
- 重新定義了執行附加處理以定位 IPv4 地址的現有查詢，以對 IPv4 和 IPv6 地址執行附加處理。

這些更改是為了與現有軟體兼容。保留了對 IPv4 地址的現有支持。而在 RFC 2893 中討論了與 DNS 中 IPv4 和 IPv6 地址的共存相關的轉換問題。

四、訊息格式

DNS 協議使用兩種類型的 DNS 訊息：查詢與回覆，而兩者使用

相同的標準訊息格式，如表 9 所示。每條訊息均由標頭(header)和四個部分組成，而這四個部分分別為問題(Question)、答案(Answer)、權限(Authority)與附加的資訊(Additional)，標誌字段(Flags)則負責控制這四個部分的內容，而其長度固定為 12 Bytes。標頭包括以下字段：識別代碼、標誌、問題數目、答案數目、權威資源記錄的數量以及額外的 RRs 數。

表 9、DNS 封包格式

Identification(識別代碼)	Flags(標誌)	Header
Number of questions(問題數目)	Number of answers(答案數目)	
Number of authority RRs (權威 RRs 的數量)	Number of additional RRs (額外的 RRs 數)	
Question Section		
Answer Section		
Authority Section		
Additional Section		

標誌(Flags)字段由以下字段組成：

表 10、Header flags format

Field	Description	Length (bits)
QR	查詢／回覆，1 為回覆，0 為查詢	1
OPCODE	類型可以是 QUERY（標準查詢，0），IQUERY（反	4

	向查詢，1）或 STATUS（服務器請求狀態，2）	
AA	Authoritative Answer，指 DNS 服務器對於所查詢的主機名是否具有權威性	1
TC	TrunCation，指此訊息因長度過長而被截斷	1
RD	Recursion Desired，指客戶端是否意味著遞歸查詢	1
RA	Recursion Available，指正在回覆的 DNS 服務器是否支持遞歸	1
Z	Zero，全 0 保留欄位以備將來使用	3
RCODE	Response Code，以下 4 種作為舉例: NOERROR（0，查詢成功完成） FORMERR（1，格式錯誤） SERVFAIL（2，查詢失敗，因為無法給出答案） NXDOMAIN（3，查詢失敗，因為查詢的域名不存在）	4

問題區段(Question Section) 是客戶端（或伺服器）向名稱伺服器查詢時，所攜帶完整網域名稱所儲存的位置。一般來講，客戶端每次向名稱伺服器查詢一個完整網域名稱（Question Count = 1），然而客戶端並非每次都只查詢一筆資料，如需要詢問多筆資料時，則會在問題計數欄位中指明後面緊接著有幾個問題區段。

問題區段的功能如表 11：

表 11、Question Section 格式

Field	Description	Length (octets)
QNAME	此欄位存放所要查詢的完全網域名稱，它是一個或多個標識符的序列。每個標識符以首字節的值表示為該名稱的長度，每個名稱最後以 0 表示結束，長度為 0 的標識符為根標識符	Variable
QTYPE	表示為要查詢的資源紀錄類型，這個類型表明需要進行的服務類型，常用之紀錄型態如下： 1 A 查詢 IP 位址 2 NS 查詢名稱伺服器 5 CNAME 查詢主機別名 12 PTR 反向查詢網域名稱 13 NINFO 查詢主機訊息 15 MX 查詢郵件交換紀錄	2
QCLASS	此欄位表示要在哪一類的網路上做查詢，通常都為 1（IN），表示 Internet 通訊協定的位址，如果不是 1，則表示其他網路型態（非 IP 位址格式）。	2

答案區段(Answer Section) 裡所存放的是被查詢之名稱伺服器所回應的資料，一般查詢都只是一筆資料（Answer RR Count = 1），如

有多筆資料回應,則會在答案計數欄位中指明有幾筆資源紀錄(RR)。

答案區段中各欄位功能如表 12：

表 12、Answer Section 格式

欄位	描述
名稱(Name)	擁有者名稱，即此資源記錄所屬的節點的名稱。
類型(Type)	是編碼的 16 位元值，用於指定此資源記錄中資源的類型。類型是指抽象資源。
類別(Class)	是編碼的 16 位值，用於標識協議族或協議實例。 IN Internet 系統 CH 混淆(Chaos)系統 HS Hesiod
存活時間(TTL)	此欄位是以秒為單位，長度為 32 位元整數，表示該筆資源紀錄可以存活的時間（也就是可儲存於 Cache 的時間），主要由解析器緩存 RR 時使用。如超過時間（一般都是 2 天），則表示該筆資料已失去時效，必須將其刪除。如果 TTL＝0，表示該筆記錄為變動性，而接收端（客戶端或伺服器）不必再儲存於快取伺服器（或快取資料庫）上。。
資源資料長度(RDLENGTH)	長度為 16 位元整數，表示後面資源資料的長度，以位元組計算
資源資料(RDATA)	長度不一定。表示所回應的資源紀錄的答案，例如: RR＝A(詢問主機位址),則資料資料欄位回應該主機的 IP

	位址。

五、資源紀錄

域名系統指定網路資源訊息元素的數據庫。訊息元素的類型通過 DNS 記錄類型，也就是資源記錄列表進行分類和組織。每個記錄都有一個類型（名稱和編號），一個到期時間（生存時間），與一個類以及特定於類型的數據。而網域名稱標識一個節點。每個節點都有一組資源資訊，該資訊可以為空。相同類型的資源記錄被組成為資源記錄集（RRset），一組中的 RR 順序並不重要，並且不需要由名稱服務器、解析器或 DNS 的其他部分保留。表 13 為常見的資源紀錄類型。

表 13、常見的資源紀錄類型

欄位值	RR Type	描述
1	A	主機位址（Address, A），紀錄網域名稱到 IP 位址（32 位元）之間的轉換，此為 DNS 資料庫最常見的 RR。
2	NS	網域的權威名稱服務器
5	CNAME	主機別名（Canonical NAME, CNAME）是提供主機設定另一個別名。CNAME 是非常重要的資源紀錄，提供不同的網域名稱轉譯到同一個 IP 位址，較常用的是將 www、ftp、mail 名稱轉譯到同一主機位址，例如：www.cu.edu.tw、ftp.cu.edu.tw、mail.cu.edu.tw 都是 linux-

		2.cu.edu.tw 的別名，都表示為同一主機位址。設定時每一主機只能設定一個 A 紀錄，而其它 CNAME 便設定到此 A 紀錄的主機上，同一主機可以設定多個 CNAME 紀錄。
6	SOA	授權啟動（Start Of Authority, SOA）是在任何網域區域設定中的第一項紀錄，用來指定 DNS 伺服器或是目前區域上的主要伺服器名稱，以及有關伺服器的設定內容。在 SOA 紀錄上所設定的內容主要是伺服器版本和到期日期，以及區域授權伺服器之間（主要和次要伺服器之間）的區域傳送頻率。
12	PTR	指標（Pointer, PTR）是用來登錄由 IP 位址轉譯成網域名稱，其功能剛好和 A 紀錄相反。也就是使用 PTR 來反向查詢網域名稱。
13	HINFO	主機資訊（Host Information, HINFO）是登錄主機使用的硬體和作業系統訊息，以供查詢使用。
15	MX	郵件交換器(Mail Exchanger, MX)，用於將 DNS 域名映射到郵件服務器。電子郵件應用程序使用 MX 記錄根據目標電子郵件地址查找 DNS 域的郵件服務器。MX 記錄存儲特定域的郵件服務器訊息。
16	TXT	文字（Text, TXT）紀錄是提供一些文字說明，用來說明主機或網環境的設定。
28	AAAA	AAAA 資源紀錄是將 DNS 網域名稱對應到 IPv6 的 128 位元位址。
33	SRV	服務位置記錄(Service Record, SRV)，用於指定伺服器提供服務的位置（如主機名和埠）數據。

(一)　萬用字元 DNS 記錄(Wildcard DNS record)

萬用字元 DNS 記錄是 DNS 區域中的一條記錄，該記錄將匹配對不存在域名的請求，DNS 中的萬用字元比其他計算機系統中使用的其他通配符更受限制。萬用字元 DNS 記錄的最左側 DNS 標籤帶有單個“ * ”（星號），例如: * .example.com。 域中其他位置的星號不能當作是通配符，因此* abc.example.com 和 abc.*.example.com 都不能當作是通配符 DNS 記錄。此外，僅當域不存在時才匹配通配符，而不僅僅是在沒有查詢類型的匹配記錄時才匹配。

DNS 通配符的原始定義在 RFC 1034 第 4.3.2 和 4.3.3 節中指定，但只能通過搜索算法中的某些步驟間接地確認，因此規則既不直觀也不明確。而在 20 年後，發表了 RFC 4592“通配符在域名系統中的作用”以幫助闡明規則。

六、協議擴展

DNS 的擴展機制（EDNS）是用於擴展域名系統協議的幾個參數大小的規範，而第一組規範由網際網路工程任務組(IETF)於 1999 年發布於 RFC 2671。2013 年則由 RFC 6891 更新並廢除 RFC 2671。

傳統 DNS 傳輸是透過 UDP port 53 的封包，UDP 封包本身的限制大小是 512 bytes，在傳統的 DNS 是足夠使用的。DNSSEC 因

為納入了數位簽章的功能，變成原本 UDP 的封包要包含數位簽章的資料，不敷使用。能夠解決此問題最好的方法就是使用 EDNS0，它可以將 UDP 封包擴展到 4096 bytes 的大小，這樣的大小才能容納 DNSSEC 的資料傳輸。

EDNS0 的流程是由 DNS 用戶端發起的，當解析器可以接受 EDNS0 的封包時，就會在封包的 Additional 區段放入一個“ opt ”資訊傳遞給 Server，表示自己支援 EDNS0，而 DNS Server 收到 DNS 封包後看到 Additional 區段有『opt』 資訊，就會知道用戶端有支援 EDNS0 封包，在 Server 產生回覆封包後也會在 Additional 區段加入“ opt ”資訊表示這是 EDNS0 封包，所以如果你有觀察 DNSSEC 的 Additional 區段，你發現回覆數目會加一，這表示是 EDNS0 封包，雖然是 EDNS0 封包，可是不代表這是 DNSSEC 封包，在 EDNS0 中有一個 bit: DO 被設定為 1 的時候，才代表這是 DNSSEC 封包。

七、動態更新

動態 DNS（Dynamic DNS，DDNS）是域名系統中的一種自動更新名稱伺服器內容的技術。根據網際網路的域名訂立規則，域名必須跟從固定的 IP 位址。但動態 DNS 系統為動態網域提供一個固定的名稱伺服器，透過即時更新，使外界用戶能夠連上動態用戶的網址。

在網路（ARPANET）的初始階段，網絡上主機的尋址是通過將主機名映射到 IP 地址的靜態轉換所完成。這些表以主機文件的形式手動維護。域名系統提供了一種通過遞歸查詢將在線的相同地址信息自動分發到為每個網路或網域配置的遠程數據庫的方法。即使該 DNS 設施仍在每個節點上使用靜態查找，IP 地址一但分配給特定主機就很少更改。隨著網路的快速增長以及工作場所和家庭中個人計算機的普及給管理員帶來了很大的負擔，使他們不得不跟踪分配的 IP 地址並管理其地址空間。

動態主機配置協議（DHCP）允許企業和網際網路服務供應商（ISP）在開機時自動為計算機分配地址。這也有助於節省可用的地址空間，因為並非所有設備都可以一直處於活動狀態，並且可以根據所需分配地址。此功能讓 DNS 服務器也自動保持最新狀態。動態 DNS 的第一個實現此目的：主機獲得了來自 DHCP 服務器或通過自配置收到的地址通知其各自的 DNS 服務器的功能。這種基於協議的 DNS 更新方法在 1997 年 IETF 出版 RFC 2136 中進行了記錄和標準化，並已成為 DNS 協議的標準部分。

這個術語被用來描述兩種不同的概念。在網際網路的管理層面來說，動態 DNS 更新是指建立一個 DNS 系統，能夠自動更新傳統的 DNS 記錄，而不需要手動編輯。這個機制在 RFC 2136 中被解釋，利

用 TSIG 機制來提供安全性。

在用戶端來說，動態 DNS 提供了一個輕量化機制，讓本地 DNS 資料庫可以即時的更新。它能把網際網路域名指往一個可能經常改變的 IP 位址，讓經常改變位置及組態的裝置，能夠持續性的更新 IP 位址。令網際網路上的外界用戶可以透過一個大家知道的域名，連接到一個可能經常動態改變 IP 位址的機器。其中一個常用的用途是在使用動態 IP 位址連線（例如在每次接通連線就會被分配一個新的 IP 位址的撥號連線等）的電腦上運行伺服器軟體。

若要實現動態 DNS，就需要將網域的「最大快取時間」設定在一個非常短的時間（一般為數分鐘）。此舉可避免外界用戶在快取中保留了舊的 IP 位址，並且使每個新連線被建立時都會經過名稱伺服器取得該機器的新位址。

各種機構都有大規模地提供動態 DNS 的服務。他們會利用資料庫儲存使用者當前的 IP 位址，並會對使用者提供更新當前 IP 位址的方法。當一些客戶程式被安裝了之後，會在後台執行並每隔數分鐘檢查電腦的 IP 位址。當發現其 IP 位址有所變更，程式便會送出一個更新 IP 位址的請求至動態 DNS 的伺服器。有很多路由器和其他網路裝置也在其韌體中包含了上述的功能。

八、安全問題

最初，安全問題不是 DNS 或任何在早期網路上部署軟體的主要設計考量，因為該網絡不開放給公眾參與。但在 1990 年代，互聯網向商業領域的擴展改變了對保護數據完整性和用戶身份驗證的安全措施的要求。

惡意用戶發現並利用了幾個漏洞問題。DNS 緩存中毒就是一個問題，在這種情況下，數據以偽裝成權威的原始服務器的形式分發到緩存解析器，從而以潛在的虛假信息和較長的有效期（生存時間）污染了數據存儲。隨後，合法的應用程序請求可能會重定向到出於惡意目的運行的網絡主機。

某些域名可能被用來實現欺騙效果。例如，paypal.com 和 paypa1.com 是不同的名稱，但是根據用戶選擇的字體，用戶可能無法在圖形用戶界面中區分它們。在許多字體中，字母 l 和數字 1 看起來非常相似甚至相同。在支持國際化域名的系統中，這個問題非常嚴重，因為在典型的計算機屏幕上，ISO 10646 中的許多字符代碼可能看起來相同。網絡釣魚有時會利用此漏洞。如果不注意 DNS 的配置，DNS 也可能從其他安全或私有連接中“洩漏”，並且由於經常被視為無害的，DNS 有時已被惡意人員用來繞過防火牆並洩露數據。

(一) DNSSEC

域名系統的原始設計未包含任何安全性詳細信息。而它被設計為

可伸縮的分佈式系統。域名系統安全擴展（DNSSEC）嘗試增加安全性，向 DNS 添加身份驗證和數據完整性檢查，同時保持向後兼容性。

DNSSEC 的目的是在保護應用程序(以及為這些應用程序提供緩存的解析程序）免於使用偽造或操縱的 DNS 數據，例如由 DNS 緩存中毒所產生的數據。來自 DNSSEC 保護區的所有答案均經過數位簽章。通過檢查數位簽章，DNS 解析器可以檢查該訊息是否與區域所有者發布並提供給權威 DNS 服務器的信息相同（即未修改且完整)。雖然保護 IP 地址是許多用戶的緊迫問題，但 DNSSEC 可以保護 DNS 中發布的任何數據，包括文本記錄（TXT）和郵件交換記錄（MX)，並可以用於引導其他安全系統

九、隱私問題

(一) DNS-over- TLS

DNS-over- TLS(傳輸層安全性）或“ DoT”是一種 IETF 標準，可在 DNS 客戶端和 DNS 服務器之間提供全流加密。傳統上，DNS 遭受安全問題的困擾，DNS 客戶端與 DNS 服務器之間的通信幾乎始終未加密，因此容易受到欺騙，攔截等情況。

DoT 是加密 DNS 查詢以確保其安全和隱密性的標準。DoT 使用與 HTTPS 網站用來加密和認證通信的相同安全協議 TLS（也稱為“ SSL”)。DoT 在用於 DNS 查詢的用戶數據報協議（UDP）之上

添加 TLS 加密。此外，它確保 DNS 請求和回覆不會被中間人攻擊篡改或偽造。

(二) DNS-over-HTTPS

DNS-over-HTTPS 或“ DoH”是第二種 IETF 安全協議，是 DoT 的替代方法，用於解決 DNC 客戶端和 DNS 服務器通信的安全性，使用 DoH 來讓 DNS 查詢和回覆被加密，但是它們是通過 HTTP 或 HTTP / 2 協議而不是直接通過 UDP 發送的。DoH 在 IETF RFC 8484 中進行了記錄。TLS 上的 DNS 和 HTTPS 上的 DNS 都提供了 DNS 客戶端和 DNS 服務器之間的加密，從而實現了數據保密性和完整性。但是，DoH 使用與其他 HTTPS 流量相同的 TCP 端口，即端口 443。因此，很難從其他 HTTPS 流量中識別 DoH，由於 DoT 具有專用端口，因此即使請求和回覆本身都是加密的，具有網絡可見性的任何人都可以看到 DoT 通信的來來去去。相比之下，使用 DoH，DNS 查詢和回覆在其他 HTTPS 流量中會有所掩飾，因為它們都來自同一端口。

第三節　BGP (Border Gateway Protocol)

一、前言

網際網路(Internet)是由許多大大小小、不同型態的網路彼此互相連網構成的。在網際網路上面傳送的訊息經由多層的網路堆疊處理後，被切割並封裝成一個又一個網路封包(packet)，由底層實體網路傳送。當封包在不同的網路之間傳送時，必須通過路由器(router)的協助將封包轉發(relay)到下一個網路。在不同的網路間，路由器透過查詢路由表(route table)來決定封包轉發的下一個網路。

在小型網路裡面，透過人工的方式來指定每一個路由器的路由表仍是可行的。但在大型網路裡面，網路拓樸(network topology)可能因為很多狀況而隨時發生改變，如果還是採用人工的方式來維護每一個路由器的路由表，會給網路管理人員帶來巨大的負擔。透過路由協定(routing protocol)，路由器可以和網路上的其他路由器或網路設備交換訊息，從而讓路由器可以動態發現網路狀況改變，學習新的路由，並更新路由表。

網際網路上常見的路由協定可以分成兩類，一類稱為內部閘道協定(interior gateway protocol，簡稱 IGP)，適合使用在單一一個自治系統(Autonomous System，簡稱 AS)內，這個自治系統的網路共用一個 AS Number (簡稱 ASN)，如 RIP (Routing Information Protocol)、IGRP

(Interior Gateway Routing Protocol)、EIGRP (Enhanced Interior Gateway Routing Protocol)、OSPF (Open Shortest Path First)、IS-IS (Intermediate system to intermediate system)等等，這些路由協定所維護的路由資訊通常屬於 OSI 網路模型中的網路層，比如 Internet Protocol (簡稱 IP)。

另一類路由協定為外部閘道協定(exterior gateway protocol)，在由多個自治系統構成的複雜網路中使用，如早期使用的 EGP (Exterior Gateway Protocol，RFC 904，已作廢)，以及本文要介紹的邊界閘道器協定(Border Gateway Protocol，簡稱 BGP)。外部閘道協定用來確定在不同的自治系統間網路的可達性，並通過內部閘道協定來解析某個自治系統內部的路由，如圖 100 所示。

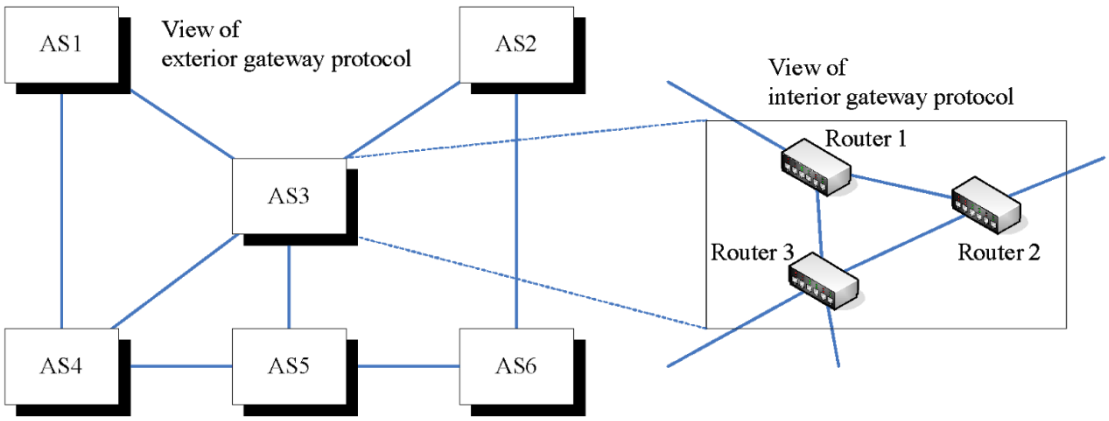


圖 100、View of exterior and interior routing protocols

BGP 是網際網路最重要的協定之一。大多數網際網路服務提供者(Internet Service Provider，簡稱 ISP)使用 BGP 來與其他 ISP 建立路由連接，彼此之間互稱為通信對端或對等實體(peer)，可為單個或多

個 ISP 網路提供更好的冗餘網路(RFC 1998)。BGP 取代了早期的 EGP，並透過使用 CIDR (Classless Inter-Domain Routing)和路由聚合(route aggregation)來降低路由表的大小。

BGP 允許網路管理者自定 BGP 路由器(又可稱為 BGP Speaker)的路由政策(routing policy)，並給予較高的優先權，手動選擇最佳路徑、次佳路徑等等，這些作法增加了 BGP 的彈性。然而，自定的路由資訊沒有受到監管，並可能在 BGP 廣播時被其他 AS 信任，使得 BGP 路由器收到錯誤或虛假路由資訊，導致路由意外，甚至如路由外洩、路由劫持等惡意事件的發生。

規模較小的單一自治系統，一般可使用內部閘道協定，如 RIP 或 OSBF。大型複雜的單一自治系統，也可採用 BGP，以面對使用 RIP 或 OSPF 可能存在的效能瓶頸。iBGP (Interior/Internal BGP)指在單一自治網路中使用 BGP，所有的 iBGP 對等實體(peer)之間需要全連接。而在不同的自治網路使用的 BGP 則稱為 eBGP (Exterior BGP)。如圖 101 所示。

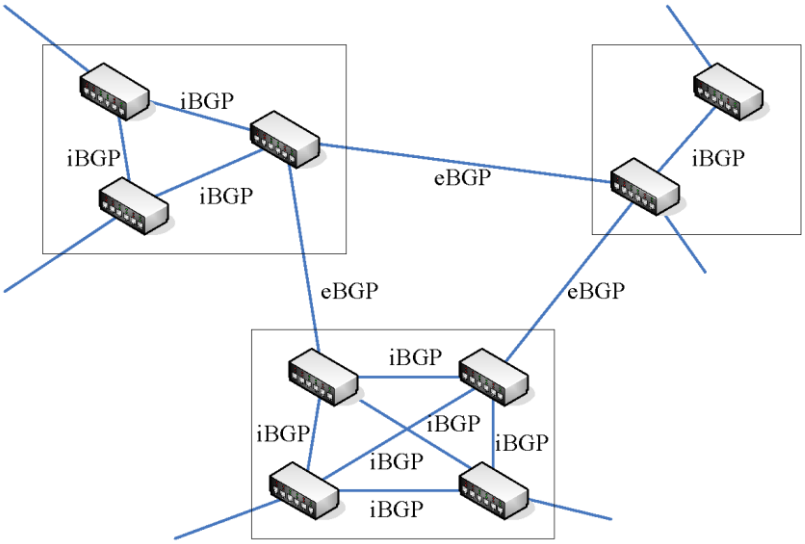


圖 101、iBGP 與 eBGP

二、RFC List

BGP 為目前最常用的路由協定之一，特別是在 ISP 之間使用。IETF 相關的 RFC 標準眾多。本研究列出下列 69 個 BGP 相關的 RFC 標準，如下：

(一) 初期

1. RFC 1105, 1989 (作廢) Border Gateway Protocol (BGP),
2. RFC 1163, 1990 (作廢) Border Gateway Protocol (BGP)
3. RFC 1164, 1990 (作廢) Application of the Border Gateway Protocol in the Internet

(二) BGP3

4. RFC 1267, 1991 Border Gateway Protocol 3 (BGP-3)
5. RFC 1268, 1991 (作廢) Application of the Border Gateway

Protocol in the Internet

6. RFC 1269, 1991 (作廢) Definitions of Managed Objects for the Border Gateway Protocol: Version 3

(三) BGP4

7. RFC 1654, 1994 (作廢) A Border Gateway Protocol 4 (BGP-4)
8. RFC 1655, 1994 (作廢) Application of the Border Gateway Protocol in the Internet
9. RFC 1656, 1994 (作廢) BGP-4 Protocol Document Roadmap and Implementation Experience
10. RFC 1657, 1994 (作廢) Definitions of Managed Objects for the Fourth Version of the Border Gateway
11. RFC 1771, 1995 (作廢) A Border Gateway Protocol 4 (BGP-4)
12. RFC 1772, 1995 Application of the Border Gateway Protocol in the Internet Protocol (BGP-4) using SMIv2
13. RFC 1773, 1995 Experience with the BGP-4 protocol
14. RFC 1774, 1995 BGP-4 Protocol Analysis
15. RFC 4271, 2006 A Border Gateway Protocol 4 (BGP-4)
16. RFC 4272, 2006 BGP Security Vulnerabilities Analysis
17. RFC 4273, 2006 Definitions of Managed Objects for BGP-4

18.RFC 4274, 2006 BGP-4 Protocol Analysis

19.RFC 4275, 2006 BGP-4 MIB Implementation Survey

20.RFC 4276, 2006 BGP-4 Implementation Report

21.RFC 4277, 2006 Experience with the BGP-4 Protocol

22.RFC 4278, 2006 Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification

(四) 延伸

23.RFC 2283, 1998 (作廢) Multiprotocol Extensions for BGP-4

24.RFC 2858, 2000 (作廢) Multiprotocol Extensions for BGP-4

25.RFC 4760, 2007 Multiprotocol Extensions for BGP-4

26.RFC 8654, 2019 Extended Message Support for BGP

(五) 輔助

27.RFC 2280, 1998 (作廢) Routing Policy Specification Language (RPSL)

28.RFC 2622, 1999 Routing Policy Specification Language (RPSL)

29.RFC 2725, 1999 Routing Policy System Security

30.RFC 4012, 2005 Routing Policy Specification Language next

generation (RPSLng)

31. RFC 7909, 2016 Securing Routing Policy Specification Language (RPSL) Objects with Resource Public Key Infrastructure (RPKI) Signatures

32. RFC 2842, 2000 (作廢) Capabilities Advertisement with BGP-4

33. RFC 3392, 2002 (作廢) Capabilities Advertisement with BGP-4

34. RFC 5492, 2009 Capabilities Advertisement with BGP-4

35. RFC 8810, 2020 Revision to Capability Codes Registration Procedures

36. RFC 2918, 2000 Route Refresh Capability for BGP-4

37. RFC 7313, 2014 Enhanced Route Refresh Capability for BGP-4

38. RFC 1966, 1996 (作廢) BGP Route Reflection An alternative to full mesh IBGP

39. RFC 2796, 2000 (作廢) BGP Route Reflection – An Alternative to Full Mesh iBGP

40. RFC 4456, 2006 BGP Route Reflection – An Alternative to

Full Mesh Internal BGP (iBGP)

41. RFC 6608, 2012 Subcodes for BGP Finite State Machine Error

42. RFC 7606, 2015 Revised Error Handling for BGP UPDATE Messages

43. RFC 7911, 2016 Advertisement of Multiple Paths in BGP

(六) 自治系統

44. RFC 1930, 1996 Guidelines for creation, selection, and registration of an Autonomous System (AS)

45. RFC 6996, 2013 Autonomous System (AS) Reservation for Private Use

46. RFC 7300, 2014 Reservation of Last Autonomous System (AS) Numbers

47. RFC 1965, 1996 (作廢) Autonomous System Confederations for BGP

48. RFC 3065, 2001 (作廢) Autonomous System Confederations for BGP

49. RFC 5065, 2007 Autonomous System Confederations for BGP

50. RFC 4893, 2007 (作廢) BGP Support for Four-octet AS

Number Space

51. RFC 6793, 2012 BGP Support for Four-Octet Autonomous System (AS) Number Space

52. RFC 6286, 2011 Autonomous-System-Wide Unique BGP Identifier for BGP-4

53. RFC 7607, 2015 Codification of AS 0 Processing

54. RFC 7705, 2015 Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute

(七) 其他

55. RFC 4724, 2007 Graceful Restart Mechanism for BGP

56. RFC 8538, 2019 Notification Message Support for BGP Graceful Restart

57. RFC 1997, 1996 BGP Communities Attribute

58. RFC 4360, 2006 BGP Extended Communities Attribute

59. RFC 5543, 2009 BGP Traffic Engineering Attribute

60. RFC 5701, 2009 IPv6 Address Specific BGP Extended Community Attribute

61. RFC 7153, 2014 IANA Registries for BGP Extended Communities

62. RFC 8642, 2019 Policy Behavior for Well-Known BGP Communities
63. RFC 6368, 2011 Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
64. RFC 8212, 2017 Default External BGP (EBGP) Route Propagation Behavior without Policies
65. RFC 2439, 1998 BGP Route Flap Damping
66. RFC 3765, 2004 NOPEER Community for Border Gateway Protocol (BGP) Route Scope Control
67. RFC 5575, 2009 Dissemination of Flow Specification Rules
68. RFC 7674, 2015 Clarification of the Flowspec Redirect Extended Community
69. RFC 7752, 2016 North-Bound Distribution of Link-State and Traffic Engineering Information Using BGP

圖 102 顯示了這 69 個 RFC 之間的關係。

1989 年，最早的 BGP (已廢除)出爐，經過陸續討論與修正後，1994 年公告了最原始的 BGP 第 4 版(BGPv4)，1995 年的 RFC 1771 進行了一次修正，同年的 RFC 1883 定義了 IPv6 BGP，並在隨後 1998 年 RFC 2208 中修正，使得 BGPv4 能夠支援諸如 IPv4、IPv6 等系列

位址，也因此被稱為 Multiprotocol BGP。

之後，相關的 RFC 標準陸續發表，包含 BGP 對於自治系統的考量、路由政策的規範、實施的經驗與分析等。經過約 10 年的實施後，於 2006 年發表最新的 BGP 標準 RFC 4271，和相關伴隨文件(RFC 4272~4278)，如經驗與分析。之後，也陸續更新既有的 RFC，和發表新功能(如 Graceful Restart)的標準文件。

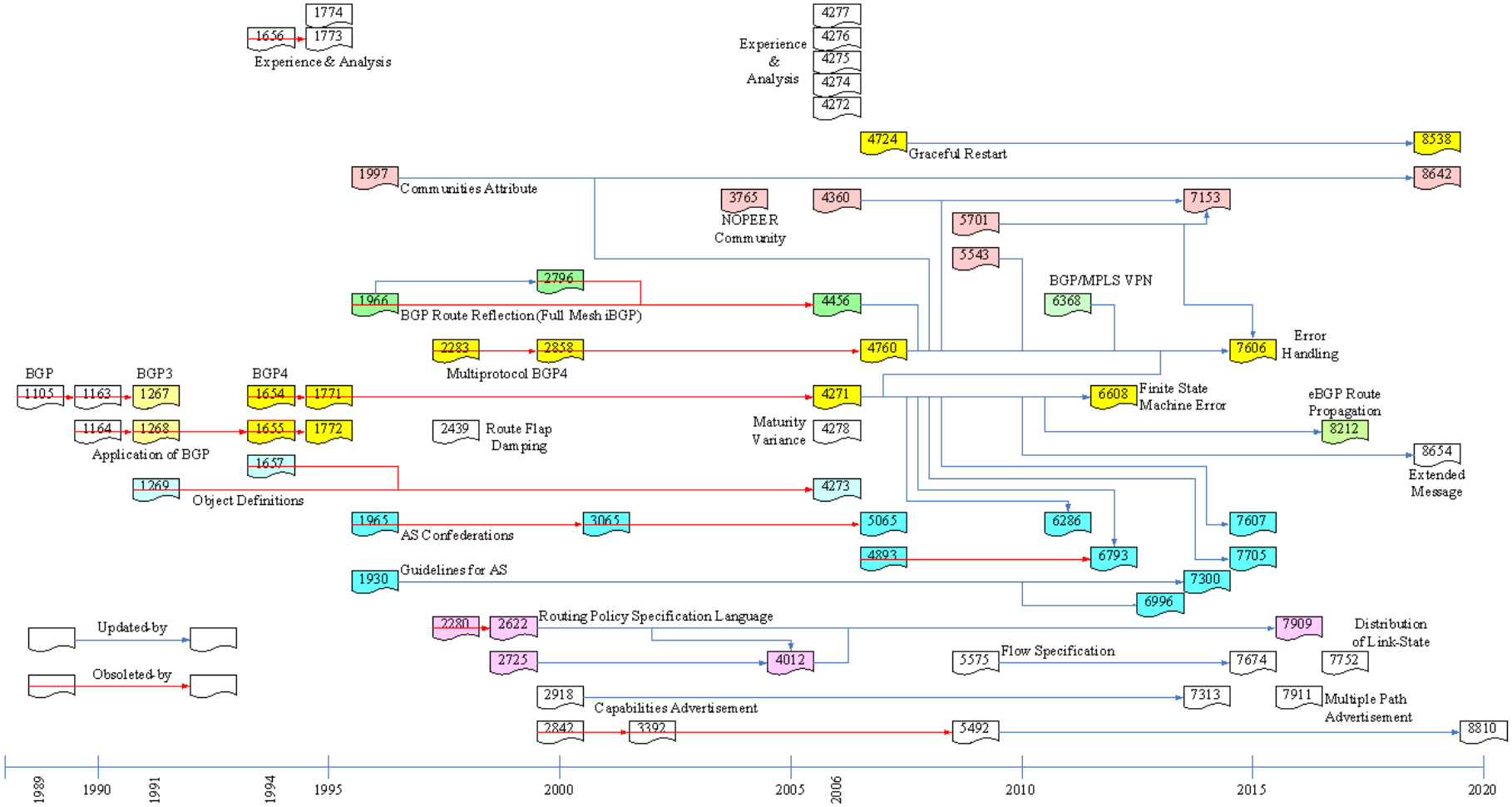


圖 102、BGP 相關 RFC 標準

三、相關知識

(一) 自治系統(Autonomous System，AS)

一個自治系統(Autonomous System，簡稱 AS)是一個由彼此互連的網路所構成的集合，其中的每個網路以一個 IP 路由前綴(routing prefix)為代表。一個 AS 被視為一個單一的管理實體(或域)，具有共同而且明確的路由策略。每個 AS 會被分配給唯一的 ASN (AS number)。對 BGP 來說，ASN 是區別整個 Internet 中的各個網路的唯一標識。

一開始的時候，一個 AS 只能被一個實體控制，通常是一個 ISP 或是具有多個網路連接的大型組織(RFC 1771)。現在，一個 AS 可以由一個或多個網路營運商共同控制(RFC 1930)。

2007 年以前，ASN 是 16 位元的，從 1 到 64,511 的 ASN 是公開，從 64,512 到 65,535 的 ASN 是私有的，私有 ASN 只能在一個組織內部的網路中使用。RFC 4893 定義了 32 位元的 ASN，並可用『高 16 位元的 10 進位.低 16 位元的 10 進位』的形式來表達(RFC 5396)，舉例來說，16 進位為 1000800016 的 ASN 可以表達為 4096.32768。從 4,200,000,000 to 4,294,967,294 的 32 位元 ASN 是私有的(RFC 6996)。

網際網路位址分派機構(Internet Assigned Numbers Authority，簡稱 IANA)將一個一個的 ASN 區塊分配給區域網際網路註冊管理機構(Regional Internet Registry，簡稱 RIR)，各地區的 RIR 再進一步從 ASN

區塊中挑選一個 ASN 分配給一個管理實體(RFC 6793)。每個管理實體必須按其所屬地區的 RIR 的規定申請，得到批准後才會分配到一個 ASN。所有 ASN 的分配情況可以在 IANA 的網站找到。截至 2019 年 8 月，已分配的 ASN 數量已超過 92,000。

根據連接性和操作策略，AS 可以分為下列四類。

1. Transit (中轉/過境) AS

末端 AS 只與一個 AS 相連。一般而言，末端 AS 只透過一條網路連線連接到其他的 AS，這種網路是資料流的起點或終點。末端 AS 的路由策略可能其上游 ISP 的路由策略完全相同，這種情形下，末端 AS 其實浪費了一個 ASN。

2. Stub (末端) AS

末端 AS 只與一個 AS 相連。一般而言，末端 AS 只透過一條網路連線連接到其他的 AS，這種網路是資料流的起點或終點。末端 AS 的路由策略可能其上游 ISP 的路由策略完全相同，這種情形下，末端 AS 其實浪費了一個 ASN。

3. Multihomed AS

一種與多個其他 AS 保持連接的 AS。即使其中一個連接完全失效，Multihomed AS 仍可保持與 Internet 連接。與中傳 AS 不同，這種類型的 AS 通常不允許來自其他 AS 的流量通過自身傳遞到另一個

AS。舉例來說，一個 Multihomed AS 網路 A 有二條對外連線連接到兩個不同的 ISP，分別為 ISP B 與 ISP C，以保證網路 A 的可靠性，但不允許 ISP B 到 ISP C 的資料流經過網路 A，反向流量(ISP C 到 ISP B)也是。

4. Internet Exchange Point (IX 或 IXP)

一種可以讓 ISP 或內容傳遞網絡(Content Delivery Networks，簡稱 CDN)之間進行資料交換的實體網路基礎建設。對於一般的網路而言，IXP 通常是透明的。

(二) 路由協定的技術

內部閘道協定可以細分為三類。

1、 Distance-vector routing protocol

包含 RIP、RIPv2、RIPng、IGRP 等。使用這類型路由協定時，路由器通常沒有完整的網路拓樸訊息。每一個路由器在路由表中維護到其他路由器的距離(如 hop count)，並週期性地公告給其他路由器，彼此交換，同時，使用 Bellman-Ford 演算法尋找最短路徑。這類型路由協定的缺點是需要較長的時間收斂，因此，比較適合使用在簡單的小型網路。

2、 Link state routing protocol

包含 OSFP、IS-IS 等。使用這類型路由協定時，路由器知道整個

網路的拓撲訊息，因此，可以獨立的計算目的地址的最佳下一站。路由器之間，僅傳送構造整個網路連通所需要的資訊，收斂較快，但路由器需要較多的記憶體與計算能力來維護網路拓樸與進行路由運算與選擇。

3、 Advanced distance vector routing protocol

如 EIGRP，藉由混合上述兩種技術，來達到較好的效能。

相對於內部閘道協定，BGP 可稱為 path vector (或 distance-path) routing protocol，既不像 link-state routing protocol 那樣去追蹤完整的網路拓樸，也不滿足於像 distance-vector routing protocol 僅僅計算 hop count。在 BGP 中，一條路徑(path)將包含到達目的位址的所有自治系統，並基於路徑及網管人員設定的網路策略和規則集來決定路由。

四、BGP 運行

BGP 一個完全分散的路由系統。在 BGP 裡，對等實體之間的鄰居關係是通過人工組態實現的，並通過 TCP 建立會話並交換資料，預設埠(port)是 179。在各種路由協定中，只有 BGP 使用 TCP 作為傳輸層協定。在 AS 網路邊界上與其他 AS 網路交換路由資訊的路由器稱為邊界路由器(border/edge router)，或者簡稱為 eBGP 對等實體。對等實體之間通常直接連接。iBGP 和 eBGP 的主要區別在於轉發路由資訊的行為。例如，從 eBGP 對等實體獲得的路由資訊會分發給所有

iBGP 對等實體和 eBGP 對等實體，但從 iBGP 對等實體獲得的路由資訊通常僅會分發給所有 eBGP 對等實體。這使得在同一個 AS 網路中的 iBGP 對等實體必須是全連接(full-mesh)的。使用 BGP Route Reflector 可以在某種程度上避免 iBGP 對等實體全連接的要求。

BGP 路由器在啟動的時候，會計算本地路由，並發佈給與之相連的 BGP 對等實體。這個過程結束之後，BGP 路由器就是斷斷續續的接收一些更新事件，再將路由重新發佈給它的 BGP 對等實體。BGP 路由器啟動之後，過程可以分為兩個部分，一個是初始化路由並發佈，接下來就是正常工作時的路由發佈。

(一) BGP 訊息

BGP 訊息通過 TCP 傳送，只在完整接收後才能進行處理。最大訊息的長度是 4096 個字節(octet，8 位元)，最小訊息只有 19 個字節，僅有 BGP 表頭(header)。

BGP 表頭包含 16 字節的 Marker，儲存同步訊息和加密訊息，2 字節的 Length，指定包含表頭在內的訊息長度，和 1 字節的 Type，表示當前 BGP 訊息的類型。BGP 表頭如圖 103 所示。

Marker (32 bits)	
Length (16 bits)	Type (8 bits)

圖 103、BGP 訊息格式

BGP 使用 5 種訊息，分別是 Open (Type = 1)、Update (Type = 2)、Notification (Type = 3)、Keep-alive (Type = 4)與 Route-Refresh (Type = 5) (RFC 2918)。

1、 Open 訊息

在建立 TCP 連線後，每個 BGP 對等實體第一個送出的訊息就是 Open 訊息，接受 Open 訊息後則將回送一個 Keep-alive 訊息作為確認。Open 訊息的格式如圖 104 所示，其中用以表示 BGP 訊息傳送者的一組 32 位元的無號整數，可以是該 BGP 對等實體的 IPv4 位址。

<table>
<tr><td colspan="3">Marker (32 bits)</td></tr>
<tr><td>Length (16 bits)</td><td>Type (8 bits)</td><td>Version (8 bits)</td></tr>
<tr><td>My ASN (16 bits)</td><td colspan="2">Hold Time (16 bits)</td></tr>
<tr><td colspan="3">BGP Identifier (32 bits)</td></tr>
<tr><td>Optional Parameter Length (8 bits)</td><td colspan="2" rowspan="2">Optional Parameter (variable-length)</td></tr>
<tr><td colspan="3"></td></tr>
</table>

圖 104、BGP Open 訊息

2、 Update 訊息

確認 Open 訊息後，BGP 連接後的首次 Update 訊息會交換整個 BGP 路由表，之後的 Update 訊息只會發送有變化的路由信息。

不包含表頭的 Update 訊息格式如圖 105 所示。

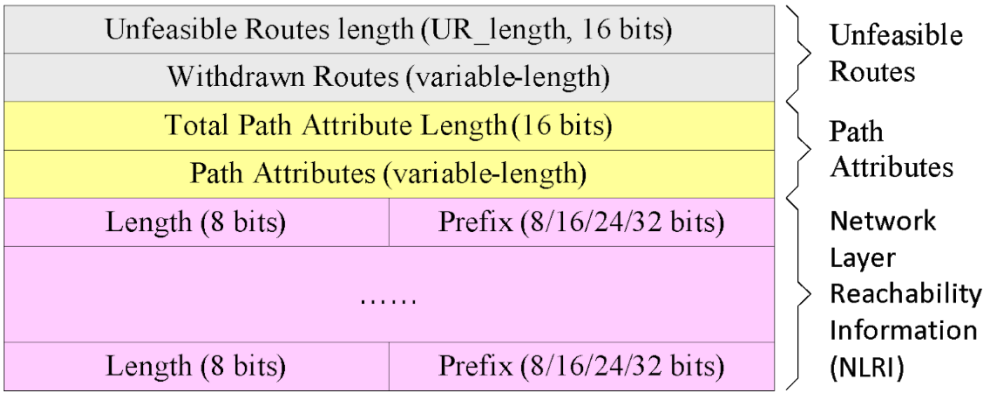


圖 105、Update 訊息

Update 訊息包含撤回和新增的路由，兩者可以同時進行。

每個被撤回的路由都包含一個長度欄位和一個路由前綴欄位。

一個 Update 訊息裡面只會包含一條路徑(path)的路由訊息，因此只有一組路徑屬性(Path Attribute，簡稱 PA)，但是可以包含多條路由，記錄在 Network Layer Reachability Information (簡稱 NLRI)。具體的說，一個 BGP 路由器可能連接了多個 BGP 對等實體路由器，它在發送 BGP Update 訊息時，一次只會發送其中一個 BGP 對等實體路由器的信息。

所有的路徑屬性都包含一個路徑屬性旗標欄位、一個路徑屬性型態欄位，這兩個欄位決定第三個欄位路徑屬性的長度與值。路徑屬性旗標說明路徑是否 well-known、transitive、optional。BGP 路由器必須認得所有的 well-known 路徑屬性。路徑屬性型態有 Origin、AS path、

Next hop、Multi Exit Discriminator、Local Preference、Atomic Aggregate 和 Aggregator。

下面介紹幾種常用的 BGP 路徑屬性：

1. Origin 屬性：用來定義路徑訊息的來源，有以下 IGP、EBP 和 Incomplete 等 3 種類型。IGP 具有最高的優先級，如通過命令列進入到 BGP 路由表的路由，Origin 屬性為 IGP。EGP 優先級次之。Incomplete 優先級最低，通過其他方式學習到的路由信息，其 Origin 屬性為 Incomplete。
2. AS_Path 屬性：按順序記錄了某條路由從本地到達目的地址經過的所有 ASN。
3. Next_Hop 屬性：記錄了路由的下一跳信息。BGP 路由器向 eBGP 對等實體發佈某條路由時，該路由訊息的 Next_Hop 屬性將設為一個本地垃址，BGP 路由器用該位址與 eBGP 對等實體建立 BGP 鄰居關係。iBGP 的情形類似。向 IBGP 對等實體發佈從 eBGP 對等實體學來的路由時，不改變該路由信息的 Next_Hop 屬性。
4. Local_Pref 屬性：表明本地路由的優先屬性，用於判斷流量離開 AS 時的最佳路由。當 BGP 通過不同的 iBGP 對等實體得到目的地址相同但下一跳不同的多條路由時，將優先選擇

Local_Pref 屬性值較高的路由。Local_Pref 屬性僅在 iBGP 對等實體之間有效，不會通告給其他 AS。Local_Pref 屬性可以手動配置。

5. MED 屬性：用於判斷流量進入 AS 時的最佳路由。當 BGP 發現從不同的 eBGP 對等實體學習得到的目的地址相同但下一跳位址不同的多條路由時，在其它條件相同的情況下，將優先選擇 MED 值較小者作為最佳路由。MED 屬性僅在相鄰兩個 AS 之間傳遞，收到這個屬性的 AS 不會再將其通告給任何其他第三方 AS。MED 屬性可以手動配置。

6. 社區(Community)屬性：用於標識具有相同特徵的 BGP 路由，使路由策略的應用更加靈活，同時降低了維護管理的難度。

路由資訊儲存於路由資訊庫(Routing Information Base，簡稱 RIB)。RIB 可說是路由表的同義詞，儲存至少以下三種資訊：目標位址、子網路遮罩和下一跳位址。BGP 使用三種 RIB：Adj-RIBs-In、Loc-RIB 和 Adj-RIBs-Out。

3、 Notification

當偵測到錯誤狀況時，BGP 路由器會送出一個 Notification 訊息，並在送出訊息後立刻中止連線。Notification 訊息包含了一個字節的錯誤碼、一個字節的次錯誤碼和其他相關資料。

4、 Keep-alive

BGP 路由器會周期地傳送 Keep-alive 訊息來維護連接，預設周期為 60 秒。Keep-alive 訊息只有表頭，沒有資料，因此，只有 19 字節，是最小的 BGP 訊息。

5、 Route-Refresh

當 BGP 路由器發現某個路由資訊已經失效，它有三種機制通知鄰居。

1. 發送 Update 訊息，將失效路由的位址前綴寫入 Withdrawn Routes 欄位。
2. 發送 Update 訊息，在 NLRI 中發佈該位址前綴新的路由資訊，取代舊的路由資訊。
3. 關閉連線，來自對方的路由資訊就會自動被刪除。

(二) Multiprotocol BGP

在 BGP 路由器之間建立對話的握手(handshake)期間，交換 Open 訊息時，BGP 路由器彼此可以協商是否使用 BGP 可選功能，包括多協定擴展(multiprotocol extensions，或稱為 Multiprotocol BGP)和各種恢復模式。如果在創建時就決定使用 Multiprotocol BGP，則 BGP 路由器可以為其發布的 NLRI 路由資訊加上位址家族前綴，這些系列包括 IPv4(默認)、IPv6、IPv4/IPv6 VPN 和 Multicast BGP。

(三) BGP 路由器的狀態

BGP 對等實體使用一個簡單的有限狀態機(Finite State Machine，FSM)，它包含六個狀態：Idle、Connect、Active、OpenSent、OpenConfirm 與 Established。BGP 定義了每個對等實體在某個狀態下應與對方交換的消息，以便將會話從一種狀態更改為另一種狀態。

BGP 路由器的初始狀態是 Idle 狀態。在 Idle 狀態下，BGP 路由器初始化所有資源，拒絕所有從外界來的 BGP 連接嘗試，啟動與對方的 TCP 連接，進入 Connect 狀態。在 Connect 狀態下，BGP 路由器等待 TCP 連接完成，如果成功，則送出 Open 訊息，並進入到第三種狀態 OpenSent。如果不成功，它將啟動 ConnectRetry 計時器，並在時間到時進入為 Active 狀態。在 Active 狀態下，路由器將 ConnectRetry 計時器重置為零，並返回到 Connect 狀態。在 OpenSent 狀態下，路由器已經發送一個 Open 訊息，正在等待 Keep-alive 訊息確認，以便進入 OpenConfirm 狀態。彼此完成交換 Keep-alive 訊息，並在成功接收後，路由器進入 Established 狀態。在 Established 狀態下，路由器可以發送/接收 Keep-alive、Update 與 Notification 訊息。

(四) BGP Route Processing

概念上，一個 BGP 路由器可以接受來自多個鄰居的 Update 訊息，並將 Update 訊息中的 NLRI 通告給相同或不同組的鄰居。

BGP 使用三種 RIB：Adj-RIBs-In、Loc-RIB 和 Adj-RIBs-Out。BGP 並不強制要求 BGP 路由器維護 3 份獨立的資訊，也可以是 1 個指標。

1. Adj-RIBs-In：本地 BGP 路由器從其他 BGP 路由器收到的路由訊息。
2. Loc-RIB：儲存在 Adj-RIBs-In 中未經處理過的路由訊息，經過本地 BGP 路由器的決定程序，依據本地政策所選出的路由資訊。Loc-RIB 記載的每個路由資訊的下一跳都必須是本地 BGP 路由器的路由表可以分辨的。
3. Adj-RIBs-Out：透過本地 BGP 路由器發送的 Update 訊息通告給特定鄰居的路由資訊。

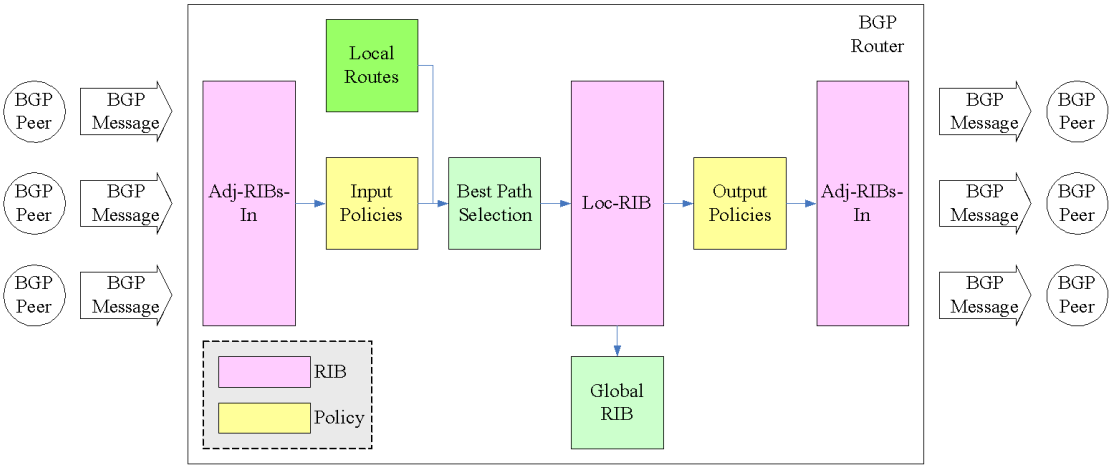


圖 106、BGP 路由選擇

BGP 使用路徑屬性來衡量每一條路徑的成本。BGP 指定了許多決策因素來從 Adj-RIBs-In 中選擇合適的路由進入 Loc-RIB，包含許多一般路由決策過程沒有使用的因素。

評估 Update 訊息中 NLRI 路由是否合適的第一個決策點是其下一跳屬性必須是可到達的或可解析的。接下來，對於每個鄰居，BGP 可以採用不同的標準和實作相關的條件來決定哪些路由可以加入該鄰居對應的 Adj-RIB-in。鄰居可以在 NLRI 中記錄到達某個目的地的多個可能的路由，但在 Adj-RIB-In 中，每個目的地應僅安裝一條路由。在這個過程裡，所有被鄰居撤回的路由也將從 Adj-RIB-In 中刪除。

每當 Adj-RIB-In 發生更改時，BGP 會確定鄰居的任何新路由是否比 Loc-RIB 中已經存在的路由更佳。如果是這樣，它將替換它們。如果給定的路由被鄰居撤回，並且沒有其他路由到達該目的地，則該路由將從 Loc-RIB 中刪除，並且不再由 BGP 發送給主路由表管理器。

驗證下一跳是否可達後，如果路由來自內部(即 iBGP)，則要應用的第一個規則是檢查 LOCAL_PREFERENCE 屬性。如果有來自鄰居的多個 iBGP 路由，選擇 LOCAL_PREFERENCE 最高的路由。若有多個路由擁有相同的最高 LOCAL_PREFERENCE，此時，思科(Cisco)和其他幾家供應商的 BGP 路由器首先會考慮一個稱為 WEIGHT 的決策因素，該因素對於路由器而言是本地的，選擇具有最高 WEIGHT 的路由。LOCAL_PREFERENCE，WEIGHT 和其他條件通常可以通過本地配置和軟件功能進行操作。雖然這種操作超出了 BGP 標準的範圍，

但是很常用，比如使用 COMMUNITY 屬性。其他可能的因素，包含：優先選擇 AS_PATH 最短的路由、優先選擇 ORIGIN 屬性值最低的路由、優先選擇具有最低 MULTI_EXIT_DISC (MED)值的路由等等。

其中，AS_PATH 屬性記錄了某條路由從本地到目的地址經過的所有 ASN。

(五) BGP communities

BGP communities 在概念上可以視為屬性標籤(attribute tags)，可將其應用於(進入或傳出的)位址前綴，以實現某些共同路由目標(RFC 1997)。舉例來說，BGP 允許管理員設置 ISP 如何處理位址前綴的策略，但在實務上，這通常是有困難的或不可能的。例如，BGP 並沒有這樣的一個概念，允許一個 AS 告訴另一個 AS，限制某個位址前綴的廣告(advertisement)僅發送給某個區域的對等實體。然而，ISP 可以發佈一個列表，上面列出公開或專有社區，並為每個社區提供描述。RFC 1997 定義了三個具有全球意義的知名社區：NO_EXPORT 社區、NO_ADVERTISE 社區和 NO_EXPORT_SUBCONFED 社區。RFC 7611 定義了 ACCEPT_OWN 社區。常見的社區範例包括對於本地偏愛調整、地理限制或對等實體類型限制，DoS (Denial of Service)避免(黑洞)和 AS 優先選項。

2006 年擴展了 Extended Community Attribute，目的是擴展屬性的

範圍，RFC 4360 中記錄了此 Extended Community Attribute 的定義。IANA 管理 BGP Extended Communities Types。

(六) BGP Route Reflector

大型 AS 網路內，也可以選擇使用 iBGP。比如說，由於 BGP 使用 TCP 傳送路由訊息，當網路規模足夠大的時候，iBGP 比 OSPF 能更加穩定可靠的傳輸路由訊息。對於路由器來說，eBGP 和 iBGP 只是對應的參數不一樣，但都是通過同一個 BGP 行程(process)來運行，不會增加路由器的負擔。此時，只需要建立好 eBGP 和 iBGP 之間的連接，相應的路由就可以會通過 BGP 傳送。同時，AS 內部的中介路由器(intermediate router)的路由表可以比較小，因為它們並不需要關心 AS 以外的路由信息。

從 iBGP 對等實體獲得的路由資訊通常僅會分發給所有 eBGP 對等實體，不會傳遞給其他的 iBGP 對等實體，這是為了防止產生循環(loop)。不像 eBGP 對等實體通過可以通過 BGP 裡面的 AS_PATH 和其他元素過濾一個來自於自身 AS 的路由，但是 iBGP 運行在一個 AS 內部，沒有 AS_PATH。這也要求，同一個 AS 網路中的 iBGP 對等實體必須形成一個全連接(full-mesh)網路。這會使得 iBGP 對等實體之間的連接數隨著節點數量成二次方成長，對大型複雜的 AS 網路來說，是一個配置與管理上的困難。

BGP Route Reflector (RFC 4456)是一種特殊的 iBGP 路由器，它會將學習到的 iBGP 路由，傳遞給所有連接的 BGP Route Reflector 客戶端，可以避免 iBGP 對等實體全連接的要求，如圖 107 所示。

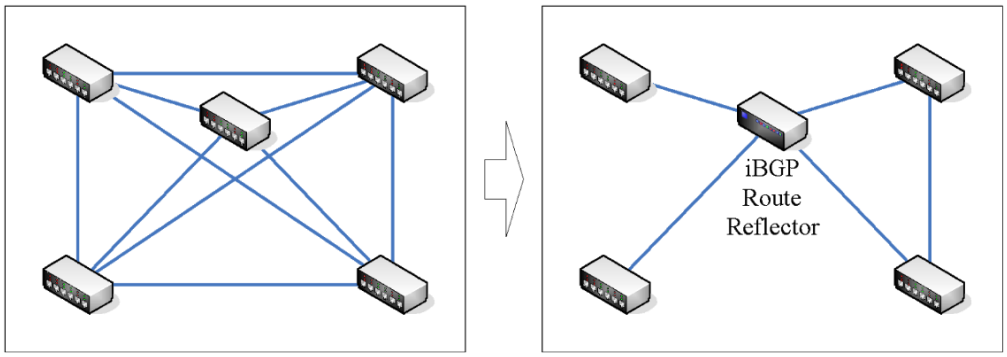


圖 107、iBGP Route Reflector

BGP Confederation (RFC 5065)是另一種處理方式，如將一個大型的 AS 裡面的 iBGP router，劃分到多個小的 Sub-AS，如圖 108 所示。

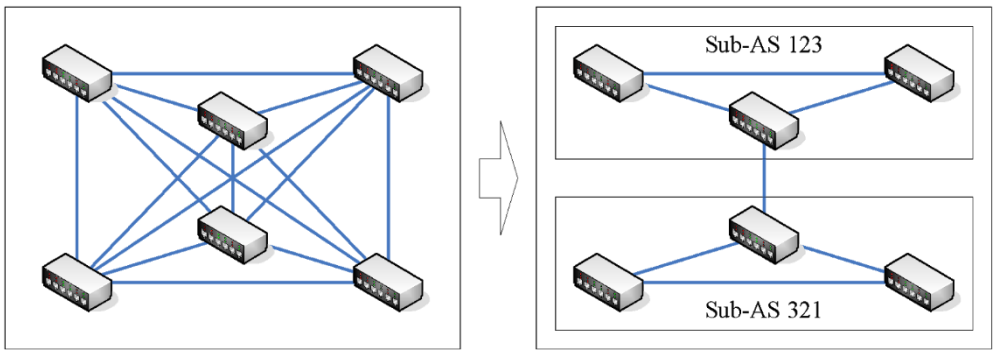


圖 108、BGP Confederation

(七) Graceful Restart

當一個 BGP 路由器與一個對等實體的連接中斷時，它會認為這個對等實體已經不能工作，它會刪除之前從這個對等實體學習到的路由訊息，並希望能以最快的速度收斂到整個網路最新的狀態。但與對

等實體連接中斷並不一定代表對路由無法進行了，可能只是與對等實體之間的 TCP 連接有問題，或是 Keep-alive 訊息丟失了。對等實體的路由功能仍有可能是正常的，具備正常封包轉發的能力。也有可能因為某些因素，這個對等實體正在重新啟動中，很快就能恢復到原來的狀態。這些狀況將造成該 BGP 路由器必須重新學習在之前一段相對短的時間內才剛剛被刪除掉的路由訊息。

如果對等實體之間的連接才剛剛斷開，BGP 路由器就開始刪除相關的路由，一會之後又很快地重新建立連接、新增路由，可能會造成 BGP 路由器上路由反轉，產生短時間內的路由環路或者路由黑洞。這樣的路由反轉甚至可能會傳遞到整個數據中心，不僅消耗了路由器控制平面的計算能力，甚至會引起整個網路的抖動。特別是現在許多 BGP 路由器是採取軟體實現的方式，軟體的維護與更新經常需要重新啟動 BGP 路由器。

RFC 4724 為 BGPv4 和 Multiprotocol BGP 新增了 Graceful Restart。使用 Graceful Restart，在 BGP 對等實體之間發生連接中斷的時候，BGP 路由器不會在很短時間內就刪除相對的路由信息，從而確保網路的穩定性。

第四節　RPKI (Resource Public Key Infrastructure)

一、前言

隨著網際網路的蓬勃發展，網路的用戶也日漸遞增，網路使用邊界閘道協定 (Border Gateway Protocol, BGP)進行路由資訊交換，達成各網際網路服務供應商(Internet Service Provider，ISP)之間的互相溝通。

但由於 BGP 協定的運作屬於信任制，近年來發生了許多駭客散布錯誤路由的資訊或是網路管理者宣布錯誤路由，造成全球網路骨幹流量異常流動與網路無法連線的現象，為解決這個問題全球網路註冊管理機構開始推動資源公鑰基礎建設(Resource Public Key Infrastructure，RPKI)。

資源公鑰基礎建設是一個基於公共密鑰基礎建設(Public Key Infrastructure，KPI)框架，讓各 ISP 在交換路由時驗證來源的合法性，確保路由安全。特別是在邊界閘道器協定（Border Gateway Protocol，BGP）上，RPKI 提供了將網際網路號碼資源資訊（如 IP 地址）連結到信任錨（Trust Anchor）的方法。使用 RPKI，號碼資源的合法持有者能夠掌握網際網路路由協定的運作，以防止路由劫持和其他攻擊。

由於路由協定存在可能會損害個人用戶或整體網路操作的攻擊風險，由網際網路工程任務組（Internet Engineering Task Force，IETF）訂定的 RPKI 標準提供了一種安全的方法來認證網際網路號碼資源的

分配，以作為確保路由安全的一個步驟。IETF 的網際網路架構委員會(Internet Architecture Board，IAB)認為，合理設計及實現 RPKI 絕對是全球路由系統安全的先決條件，而這也是建立全球網際網路可靠性的先決條件。

RPKI 將 IP 位址以及自製網路號碼(Autonomous System Number，ASN)利用公鑰基礎建設對所有權進行驗證，透過最初由網際網路號碼分配局(Internet Assigned Numbers Authority，IANA)分配到區域網際網路註冊管理機構(Regional Internet Registry，RIR)，再由 RIR 分配給本地網路註冊管理機構(Local Internet Registry，LIR)，最後由 LIR 分配給使用者的這些網路號碼資源進行認證，以此提高網路資料傳輸的安全性。

二、RFC List

圖 109 將此文件所提相關 RFC 列出，並以實線作為取代過程、虛線作為更新過程，當中藍色、綠色、黃色及紅色作為區別，分別為 X.509、ROAs、RPKI 及安全鄰居發現協定(Secure Neighbor Discovery，SEND)。

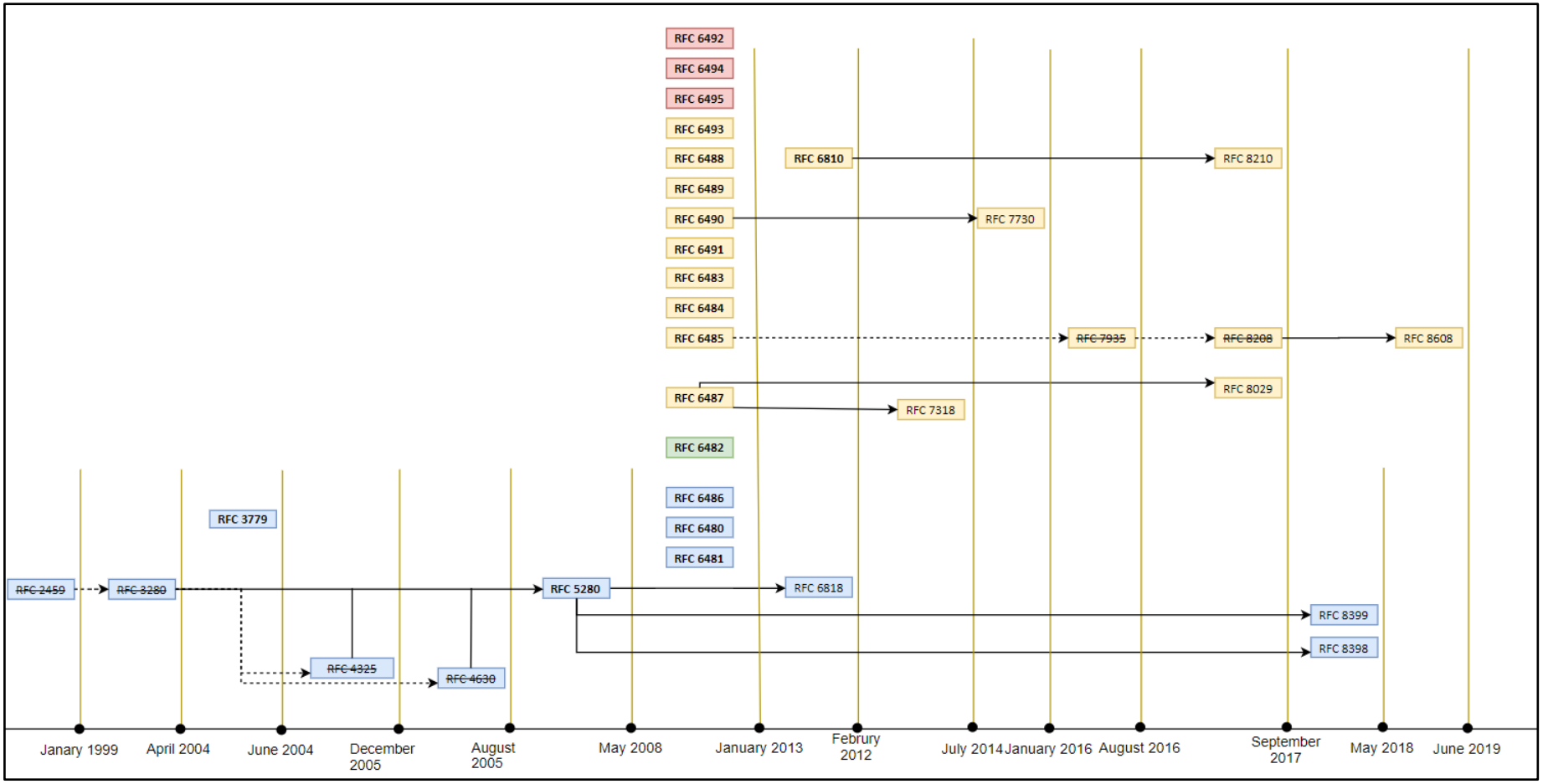


圖 109、RFC List

三、資源憑證與子物件

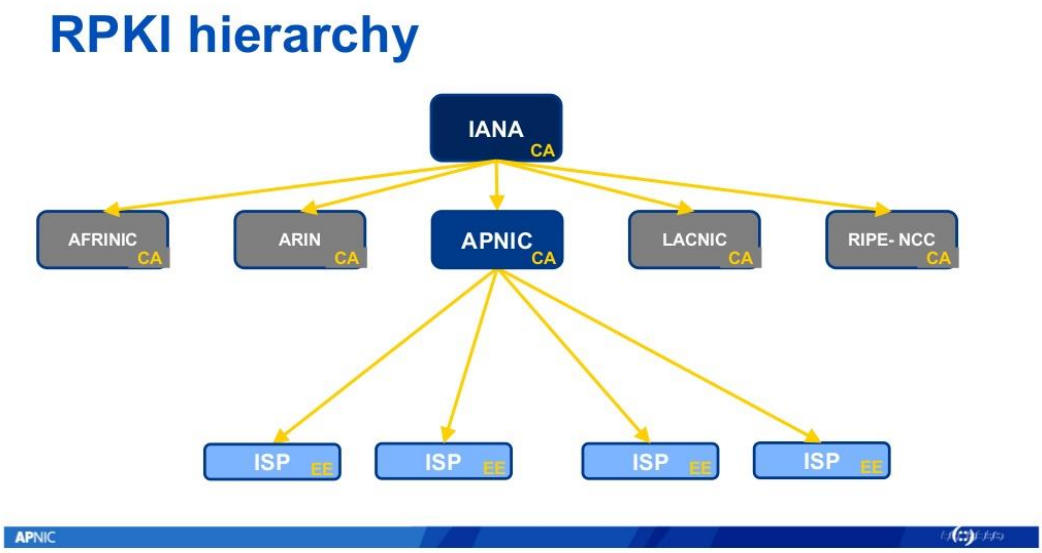
資源公鑰基礎設施(RPKI)使用了帶有 IP 位址和 AS 識別碼（RFC 3779）擴展名的 X.509 PKI 證書。它允許了區域網際網路註冊管理機構的成員，亦即本地網際網路序號產生器取得一個資源的憑證，並列出它所持有的網際網路號碼分配局(IANA)的資源。這為了它的持有提供了有效的證據，但要注意的是該憑證並不含任何身分資訊。透過使用了這個資源憑證，本地的機構可為其所持有的字首執行路由宣告建立密碼學證明。以上那些證明被稱為路由起源授權(Route Origin Authorization，ROA)。

(一) 憑證頒發機構

RPKI 使用 RFC3779 定義的 X.509 授權憑證格式，將 IP 位址以及 ASN 的組合進行簽署，憑證的結構依據網際網路資源的分發方式，每一個網際網路號碼資源的註冊單位都是憑證授權中心，在註冊單位將 IP 位址以及 ASN 配發給下級單位時，同時會簽署一張資源憑證給該單位，以確認這個資源的所有權。

所有網路號碼資源由 IANA 統一分發,所以 IANA 具有所有號碼資源的憑證，當 IANA 將號碼資源分配給五個區域網路註冊管理機構(Regional InternetRegistries，RIRs)時，也會同時簽署資源憑證給這些 RIRs，當 RIRs(例如 APNIC)再將其資源向下分配給國家網路註冊管

理機構(National InternetRegistries，NIRs)時，也會同時簽署資源憑證給 NIRs，RIRs 及 NIRs 需扮演憑證授權中心的角色。



資料來源：https://www.slideshare.net/apnic/31st-twnc-ip-opm-and-twnog-rdap-and-rpki

圖 110、RPKI 憑證頒發機構層級

(二) X.509

X.509 是密碼學裡「公開金鑰認證」(Public key certificate，PKI)的一種格式標準。X.509 憑證已應用在包括傳輸層安全性協定(Transport Layer Security，TLS)以及其前身的安全通訊協定協定(Secure Sockets Layer，SSL)內的許多網路協定中，同時它也使用在很多非線上的應用服務，例如:電子簽章服務等。X.509 憑證內容裡含有

公鑰、身分資訊（網路主機名、組織名稱或個體名稱等）和簽章資訊（可以是憑證授權中心(Certificate Authority，CA)的簽章，或是是自簽章）。對於經由可信度高的憑證簽發機構簽章或是其它方式驗證的憑證，憑證擁有者就可以用憑證與相應的私鑰來建立安全通信，對文件進行數位簽章或加密。

除了憑證本身功能之外，X.509 還附帶了憑證吊銷列表(Certificate Revocation List，CRL)和憑證合法性驗證演算法。

1、 X.509 歷史及使用情況

X.509 最早與 X.500 一起發布於 1988 年。它是假設有一套嚴格的層次化憑證授權中心。X.500 僅由主權國家實施，以達成國家身分資訊共享條約的實施目的；而 IETF 的公鑰基礎設施（X.509）簡稱 PKIX 工作群組將該標準制定成更靈活適用於網際網路組織。

事實上 X.509 認證指的是 RFC5280 里定義的 X.509 v3 ，包括對 IETF 的 PKIX 憑證和憑證吊銷列表(Certificate Revocation List，CRL) ，通常也稱為公開金鑰基礎建設（Public Key Infrastructure，PKI）。

2、 X.509（PKIX）規範的公鑰基礎結構

下圖 111 是 PKIX 規範假定的體系結構模型的簡化視圖：

```
+---+
| C |                        +------------+
| e | <--------------------->| End entity |
| r |       Operational      +------------+
| t |       transactions           ^
|   |      and management          |  Management
| / |       transactions           |  transactions
|   |                              |                PKI users
| C |                              v
| R |       -------------------+--+-----------+----------------
| L |                          ^              ^
|   |                          |              |  PKI management
|   |                          v              |      entities
| R |                        +------+         |
| e | <--------------------- | RA   | <---+   |
| p |  Publish certificate   +------+     |   |
| o |                                     |   |
| s |                                     |   |
| I |                                     v   v
| t |                              +------------+
| o | <----------------------------|     CA     |
| r |   Publish certificate        +------------+
| y |   Publish CRL                       ^
|   |                                     |
+---+                        Management   |
                             transactions |
                                          v
                                     +------+
                                     |  CA  |
                                     +------+
```

資料來源：RFC 2459 Internet X.509 Public Key Infrastructure

圖 111、PKI 實體

End entity：PKI 證書的使用者和/或使用者系統(證書的主題)

CA：證書授權機構

RA：證書吊銷機構，可選

CRL issuer：生成並簽名 CRL 的系統

repository：儲存證書和 CRL 的單個系統或分散式系統，同時用於分發證書和 CRLs 到 End entities

CA 負責指明其頒發的證書的吊銷狀態，可以通過 Online

Certificate Status Protocol (OCSP)[RFC2560]，CRLs 或其他機制獲得證書的吊銷狀態。通常情況下，當吊銷狀態由 CRLs 提供時，CA 同時也是 CRL issuer。然而 CA 可能負責頒發 CRLs 到不同的實體(entity)。

注意一個 Attribute Authority (AA)同時選擇為 CRL issuer 頒發 CRLs。

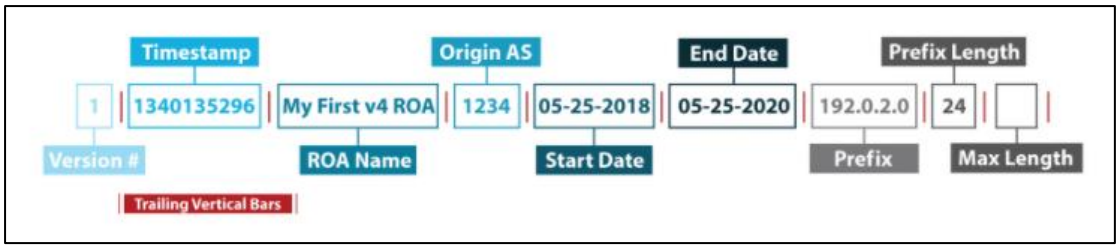
(三) 路由源授權(Route Origin Authorization，ROA)

路由來源授權（Route Origin Authorization，ROA）是用來證明 IP 位址和 AS 號碼在 BGP 路由表資訊中是正確的組合。ROA 可以用多個前綴來描述，它提供路由器來驗證從網路上公佈的 BGP 路由是否正確。ROA 除了記錄 IP 位址前綴和起源 AS 之外，有一個“maxlen（最大前綴長度）”的概念，即記錄允許的最大前綴長度，使得 ROA 能夠描述若有更長的前綴。

一個 ROA 是一個加密簽章的物件，指出其自治系統 AS 號碼被授權於某個來源前綴，這意味著 ROA 說明您的地址空間完成 BGP 公告。

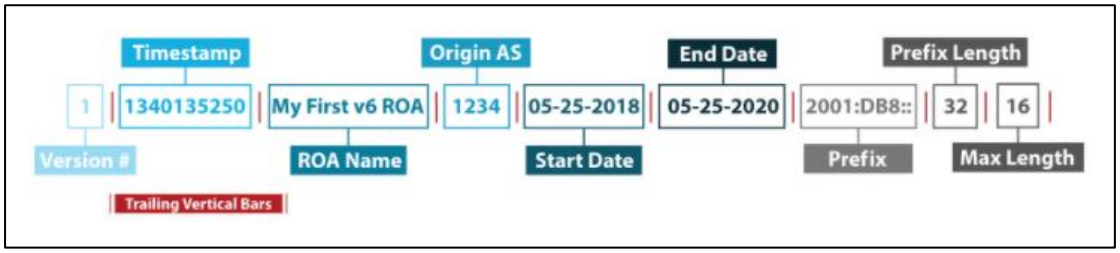
路由來源授權（ROA）中包含的內容

- 您授權的 AS 號碼。
- 正在從它發起的 IP 位址前綴。
- AS 可能宣布的最特有的 IP 位址前綴（最大長度）。



資料來源：https://www.arin.net/resources/manage/rpki/roa_request/

圖 112、IPv4 ROA 內容



資料來源：https://www.arin.net/resources/manage/rpki/roa_request/

圖 113、IPv6 ROA 內容

ROA 可能看起來像下列顯示，例如：“ISP 4 允許 AS 65000 發起前綴為 192.2.200.0/24 的路由”

建立路由來源授權（ROA）的好處

- 驗證某個 AS 是否有權發布特定的 IP 位址前綴。
- 盡量減少常見的路由錯誤。
- 防止大多數的意外劫持。

任何其他的前綴公告將被視為未經授權。這是通過發布具體的前綴來強制聚合和防止劫持的一種方法。

ROA 使用 RPKI 數位簽章物件的模板[RFC6488]，該模板為 ROA

內容定義了加密郵件語法（Cryptographic Message Syntax，CMS）[RFC5652]包裝程序，並為 RPKI 簽章物件定義了通用驗證過程。 因此，為了完成 ROA 的規範（請參閱[RFC6488]的第 4 部分）：

1. 將已簽章物件標識為 ROA 的 OID。（此 OID 出現在 encapContentInfo 物件的 eContentType 以及 signerInfo 物件的 content-typesigned 屬性內）。
2. ROA eContent 的 ASN.1 語法。（這是有效負載，用於指定被授權發起路由的 AS 以及該 AS 可以向其發起路由的前綴。）ROA eContent 是使用專有編碼規則（DER）[X.690]進行 ASN.1 編碼的。

驗證 ROA 所需的其他步驟（除了[RFC6488]中指定的驗證步驟之外）。

(四) 自治系統(Autonomous System，AS)

自治系統或自治域（Autonomous System，AS）是指在網際網路中，一個或多個實體管轄下的所有 IP 網路和路由器的組合，它們對網際網路執行共同的路由策略。

最初自治系統（Autonomous System，AS）要求由單一實體管轄，通常是一個網際網路服務提供者或一個擁有多個網路獨立連接的大型組織，其遵循單一且明確的路由策略，參看 RFC 1771 和邊界閘道

器協定的初始定義（現在已經廢除）。由於多個組織可使用各自的自治系統編號與將它們連接到網際網路的網際網路服務供應商之間執行「BGP 協定」，因此得到較多應用的是 RFC 1930 中較新的定義。儘管 ISP 支援了這些自治系統，但對網際網路來說只能看到該 ISP 的路由策略。所以 ISP 必須具有一個公開且正式登記的自治系統編號（Autonomous System Number，ASN）。

用於 BGP 路由中的每個自治系統都被分配一個唯一的自治系統編號（ASN）。對 BGP 來說，因為 ASN 是區別整個網路中的各個網路的唯一標識，所以這個自治系統編號非常重要。網際網路號碼分配局將 64512 到 65535 的 ASN 編號保留給（私有）專用網路使用。

(五) 信任錨(Trust Anchors，TAs)

在任何 PKI，每個依賴方（relying party，RP）都會選擇自己的一組信任錨（TAS）。PKI 的一般屬性也適用於此。現有的 IP 地址空間和 AS 號碼分配的層次結構，因此 IANA 和/或五個 RIR 顯然是此處預設的信任錨。儘管如此，每個 RP 最終選擇了一套將用於證書驗證信任錨。

(六) 儲存庫

為了驗證在資源公鑰基礎結構(RPKI)[RFC6480]中進行的證明，依賴方（RP）需要訪問所有 X.509 / PKIX 資源證書，證書吊銷列表

（CRL）和共同定義 RPKI 的已簽章物件。

每個證書的頒發者，CRL 或已簽章的物件，可以通過在 RPKI 儲存庫中發布物件來將其下載到 RPs。

儲存庫系統是所有 RPs 必須全局訪問的所有已簽章物件。創建證書，CRL 和簽章物件資源庫發佈點，從那裡可以下載它們供 RPs 使用。

儲存庫物件（或物件）：

這是指儲存庫發佈點中的終端物件。終端物件通常被實現為可公開訪問的目錄中的文件，其中該文件不是目錄本身，儘管該項包括具有與文件相似的公共樣子的另一種形式的物件。

儲存庫發佈點：

這是指在公共發佈點發布的儲存庫物件的集合。常規上，這被實現為由 URI [RFC3986]標識的可公開訪問的文件系統中的目錄，儘管此術語也包含另一種形式的本地儲存，其外觀類似於文件的簡單目錄。

儲存庫範例：

這是指共享一個公共發布範例的一個或多個儲存庫發佈點的集合。通常，這是作為共享公用 URI 前綴的文件系統目錄的集合來實現的，其中每個目錄也可以通過其自己的唯一 URI 進行標識。

四、管理

利用 GitHub 開源工具將頁面存檔備份，並存於網際網路檔案館(Internet Archive)可用於執行憑證頒發機構和管理資源憑證以及子物件（例如 ROA）且不會因時間的延續而使資料消失。此外，在區域機構鍾其中的成員設有代管的 RPKI 平台。本地機構可以選擇依賴於一個代管的系統，或執行自己的軟體。

五、發布

資源持有單位如 ISP，欲發布的資料儲存庫與一個或多個 RPKI 憑證點相關聯。在實踐中與 CA 互動與執行時，單位可以選擇自己發布所有加密資料，也可以依賴第三方發布。且可利用註冊單位簽署過的 IP 位址終端憑證以及 ASN 終端憑證進行 ROA 的建立，讓 IP 位址前綴與 ASN 的關係連結起來，以下為與 CA 的其中一種互動。

- CA-證書頒發

客戶端使用此查詢來請求伺服器的CA為已分配或分配給客戶端的資源頒發資源證書。如果可以成功處理該請求，則伺服器的回應將包含頒發的證書。

此請求的訊息“類型”元素的值為：

type = "issue"

以下為證書的發放請求格式：

Payload:

```
<request
        class_name="class name"
        req_resource_set_as="as resource set"
        req_resource_set_ipv4="ipv4 resource set"
        req_resource_set_ipv6="ipv6 resource set">
        [Certificate request]
</request>
```

客戶端必須為每個不同的資源類使用不同的密鑰配對。req_resource_set 屬性在請求中是可選的。如果未指定任何 req_resource_set 屬性，則該請求表示與客戶端當前資源匹配的所有資源包含在已頒發的證書中。如果任何包含的 req_resource_set 屬性的值為空值(“”)，則表明已頒發的證書中不包含該資源類型的資源。

發出者針對資源類和客戶的公鑰將請求的資源集合的值保存為本地記錄。任何後續的指定相同資源類別和相同客戶端公共金鑰的證書頒發請求都將（重新）將請求者資源集合的頒發者本地記錄設置為最近指定的值。

class_name：其值是資源類的伺服器識別。

req_resource_set_as(可選)：定義 AS 編號集合的最大限度，其格式按照資源類列表回應的 resource_set_as 屬性設置。

req_resource_set_ipv4(可選)：定義 IPv4 地址集合的最大限度，其格式按照資源類列表回應的 resource_set_ipv4 屬性設置。

req_resource_set_ipv6(可選)：定義 IPv6 地址集合的最大限度，其格式按照資源類列表回應的 resource_set_ipv6 屬性設置。

[證書要求]

值是證書請求。這是使用 PKCS＃10 [RFC2986]格式化的請求的 Base64 編碼 DER 版本。使用密鑰對的私鑰部分對證書請求進行簽章，該密鑰對的私鑰部分是認證請求中的 subject 密鑰值。簽章演算法在[RFC6485]中指定。(此簽章組件旨在證明擁有私鑰的證據。)

如果可以線上處理請求，則此請求的回應為證書頒發回應。如果不能立即執行請求，則伺服器必須使用適當的錯誤代碼回應“請求未執行”訊息：

請求未執行的訊息“類型”元素的值為：

type = " error_response"

Payload:

<status>[Code]</status>

<description xml:lang="en-US">[Readable text]</description>

由於檢測到的錯誤或請求內容中的不一致或阻止執行請求的伺

服器端狀態而導致生成錯誤回應的所有狀態都會生成請求未執行的回應。

代碼值說明:

1101 已處理請求

1102 版本號錯誤

1103 無法識別的請求類型

1104 已安排處理

1201 伺服器未定義資源類別

1202 客戶端在定義的資源類中不擁有任何資源

1203 格式錯誤的證書請求

1204 客戶端試圖對多個資源類使用相同的密鑰配對

1301 已使用的密鑰被撤消

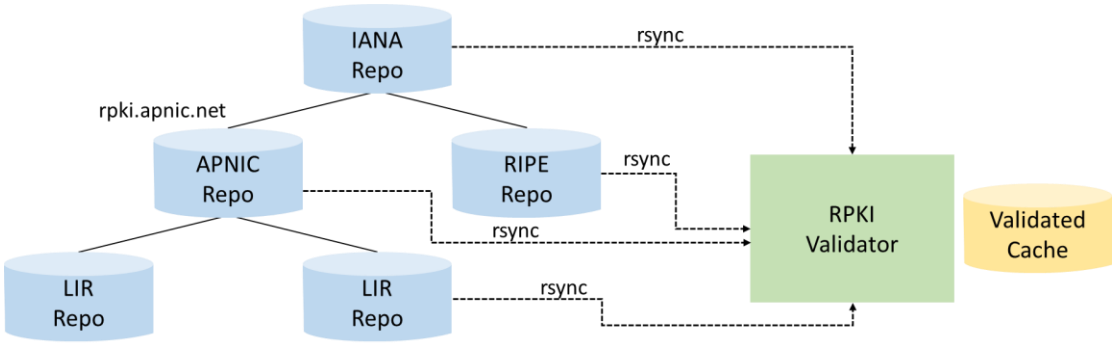
1302 無此密鑰

2001 內部伺服器錯誤

六、驗證

當為特定源AS和字首建立一個ROA時,註冊管理機構會將ROA紀錄逐筆儲存在本地資料庫中，ROA 是由多個分散的資料庫所儲存的,RPKI Validator 則是會利用 rsync 週期性的同步下載這些建立好的加密 ROA 元件，並儲存一份本地驗證的快取。若網路路由設備啟用

RPKI 技術，則可將網路路由設備與 RPKI Validator 建立連結，將 ROA 元件的資料下載網路路由設備中，供設備進行 BGP 路由策略使用，RPKI Validator 資料同步架構如下圖所示。



資料來源：https://www.slideshare.net/apnic/peering-asia-20-rpki-for-peering

圖 114、RPKI Validator 資料同步架構

當網路路由設備同步完成本地驗證的快取後，即可比對路由表中的每筆 IP 位址前綴，作為路由表中 IP 網路位址來源有效性驗證使用，每一筆 IP 網路位址比對來源宣告後有以下三種結果：

有效(Valid)：代表該筆 IP 網路位址包含在一個 ROA 元件中，且自治系統號碼一致，是來源合法的 IP 網路位址宣告。

無效(Invalid)：代表該筆 IP 網路位址包含在一 個 ROA 元件中，且自治系統號碼不一致，示該筆 IP 網路位址的來源位址是沒有獲得授權的，或者是該筆 IP 網路位址宣告的長度超過 ROA 中設定的最大長度。

未知(Not found/Unknown)：代表該筆 IP 位置並未包含於現有的

ROA 紀錄當中，因無 ROA 紀錄可供比對，無法確定其來源宣告的合法性。

錄當中，因無 ROA 紀錄可供比對，無法確定其來源宣告的合法性。

(一) BGP 來源認證

邊界閘道協定(Border Gateway Protocol, BGP)，是網際網路上一個核心的去中心化自治路由協定。它通過維護 IP 路由表或「字首」表來實現自治系統（AS）之間的可達性，屬於向量路由協定。

BGP 來源驗證有助於防止無意間通告路由。當網絡管理員錯誤地向未控制的網絡通告路由時，可以通過配置來源驗證來解決此安全問題。BGP 來源驗證是一種機制，其路由通告可通過來自預期自治系統（AS）的認證。BGP 來源驗證使用一個或多個資源公鑰基礎結構（RPKI）緩存伺服器對指定的 BGP 前綴執行身份驗證。要對前綴進行身份驗證，路由器（BGP 發言者）會查詢已驗證的前綴到 AS 對應的數據庫（從緩存伺服器下載），並確保前綴源自預期 AS。

(二) ROA 驗證

在依賴方可以使用 ROA 驗證路由公告之前，依賴方必須首先驗證 ROA。 為了驗證 ROA，依賴方必須執行[RFC6488]中指定的所有驗證檢查以及以下其他特定於 ROA 的驗證步驟。

- IP 地址委託擴展名[RFC3779]存在於最終實體（End entity，EE）證書中（包含在 ROA 中），並且 ROA 中的每個 IP 地址前綴都包含在 EE 指定的一組 IP 地址中證書的 IP 地址委託擴展。

七、路由決策

在經過 ROA 驗證後的證明可以與 BGP 路由一同協助網路業者的決策過程。這項決策過程可以以手動方式去完成，但已驗證字首的原始資料也可以使用 RPKI to Router Protocol (RFC 6810)將 Notify 消息傳送到支援的路由器，關於 RPKI to Router Protocol 運作原理大致如下：當路由器從快取（cache）中接收到所有數據記錄時，它將其當前序列號設置為數據 PDU(Power Distribution Unit)末尾中的序列號。當快取更新其數據庫時，它將向每個當前連接的路由器發送一條 Notify 消息。此舉將提示路由器現在是調查新版的好時機，但這僅是提示。該協議要求路由器在任何情況下都定期調查更新（詳細原理請參考 RFC 6810 第 4 節）。而相關技術也有多家廠商進行實作，包括思科 Cisco 網路使用 IOS-XR 及 IOS-XE 之作業系統的路由設備，版本在 XR4.3.2 及 XE3.5 版之後，即有支援 RPKI 之技術。其他像是 Quagga 的網路路由設備,也利用 BGP Secure Routing Extensions(BGP-SRx)技術或以 RTRlib 為基礎的一個 RFC-compliant 實現 RPKI 而獲

得此功能。

RFC 6494 更新了鄰居發現協定（ND）的安全機制（即安全鄰居發現協定，SEND）的憑證驗證方法，以便在 IPv6 中使用 RPKI。它使用修改的 RFC 6487 RPKI 憑證組態定義了 SEND 憑證組態，其中包含一個 RFC 3779 IP 位址委派擴充。也就是說，在 SEND 中使用的證書(由路由器，代理或地址所有者使用)必須符合此證書配置文件，並且可以符合[RFC3971]中的原始配置文件。

第五節　DNSSEC (DNS Security Extensions)

一、RFC List

RFC 2065: Domain Name System Security Extensions, D. Eastlake, 3rd, Proposed Standard

RFC 2535: Domain Name System Security Extensions, D. Eastlake, Proposed Standard

RFC 3225: Indicating Resolver Support of DNSSEC, D. Conrad, Proposed Standard

RFC 3226: DNSSEC and IPv6 A6 aware server/resolver message size requirements, O. Gudmundsson, Proposed Standard

RFC 4033: DNS Security Introduction and Requirements, R. Arends, Proposed Standard

RFC 4034: Resource Records for the DNS Security Extensions, R. Arends, Proposed Standard

RFC 4035: Protocol Modifications for the DNS Security Extensions, R. Arends, Proposed Standard

RFC 4310: Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP), S. Hollenbeck, Proposed Standard

RFC 4470: Minimally Covering NSEC Records and DNSSEC On-line Signing, S. Weiler, Proposed Standard

RFC 4509: Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records, W. Hardaker, Proposed Standard

RFC 5011: Automated Updates of DNS Security (DNSSEC) Trust Anchors, M. StJohns, Internet Standard

RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence, B. Laurie, Proposed Standard

RFC 5702: Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC, J. Jansen, Proposed Standard

RFC 5910: Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP), J. Gould,

Proposed Standard

RFC 5933: Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC, V. Dolmatov, Ed., Proposed Standard

RFC 6014: Cryptographic Algorithm Identifier Allocation for DNSSEC, P. Hoffman, Proposed Standard

RFC 6605: Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC, P. Hoffman, Proposed Standard

RFC 6944: Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status, S. Rose, Proposed Standard

RFC 7344: Automating DNSSEC Delegation Trust Maintenance, W. Kumari, Proposed Standard

RFC 7646: Definition and Use of DNSSEC Negative Trust Anchors, P. Ebersman, Informational

RFC 8080: Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC, O. Sury, Proposed Standard

RFC 8624: Algorithm Implementation Requirements and Usage Guidance for DNSSEC, P. Wouters, Proposed Standard

二、簡介

若要通過網際網路聯繫他人，就必須在電腦中輸入一個位址（以名稱或數位表示）。該位址必須是唯一的，這樣電腦才能確定彼此的位置。網際網路名稱與數字位址分配機構(Internet Corporation for Assigned Names and Numbers，ICANN)負責在全球範圍內協調此類唯一識別碼。如果沒有這種協調，我們就不會擁有統一的全球網際網路。在輸入名稱時，必須首先由某個系統將該名稱轉換為數位，然後才能建立連接。該系統稱為網域名稱系統 (Domain Name System， DNS)，

它將名稱轉換為數位，這些數位稱為網際網路協定 (Internet Protocol，IP) 地址。ICANN 對定址系統進行協調，以確保所有位址都是唯一的。

最近，人們在 DNS 中發現了一些漏洞，攻擊者可以利用這些漏洞劫持這一使用名稱在網際網路上搜尋某個人或某個網站的過程。這種攻擊的目的是取得對會話的控制以實施某種操作，例如使用者進入劫持者自己設立的欺騙性網站，以便收集使用者的帳戶和密碼。

由於這些漏洞的存在，人們開始希望引入一種稱為 DNS 安全擴展 (DNS Security Extensions， DNSSEC) 的技術，以保護網際網路的基礎設施。

三、歷史

DNS 是一項重要的基礎網際網路服務，但在 1990 年 Steve Bellovin 發現了其中嚴重的安全漏洞，他的論文於 1995 年公開發表的同時保護 DNS 的研究也開始了。IETF 在 1997 年發布了 RFC 2065，最初嘗試實施該規範，因此在 1999 年修訂了被認為是完全可行的規範，即 IETF RFC 2535，並計畫部屬基於 RFC 2535 的 DNSSEC。

不幸的是，IETF RFC 2535 規範在擴展到整個網際網路時存在很大的問題。到 2001 年，很明顯的該規範不適用於大型網路。在正常操作中 DNS 伺服器通常會與其父伺服器不同步。通常這不是個問題，

但是啟用 DNSSEC 時，這種不同步的數據可能會導致嚴重的自行創建的拒絕服務。原始 DNSSEC 需要復雜的六消息協議和大量數據傳輸才能為子級執行密鑰更改（DNS 子區域必須將其所有數據發送給父級，讓父級對每個記錄簽章，然後將其發送簽章返回給子級，以便子級將其儲存在 SIG 記錄中）。而且公鑰更改可能會產生荒唐的效果，例如，如果“ .com”區域更改了其公開金鑰，則它必須發送 2200 萬條記錄（因為它將需要更新其所有子項中的所有簽章）。因此，RFC 2535 中定義的 DNSSEC 無法擴展到網際網路。

IETF 從根本上修改了 DNSSEC，必要時將其稱為 DNSSEC bis，以區別於 RFC 2535 的原始 DNSSEC 方法。此新版本使用“委託簽署者（Delegation Signer，DS）資源記錄”在代理之間的委託點上提供附加級別的間接訪問。父子區域。在新方法中，當子級的主公鑰發生更改時，與其在每個子級的記錄中沒有六條消息，不如說一條消息：子級將新的公鑰發送給其父級。父級只需為每個子級儲存一個主公鑰即可。這更加的實用，也意味著將少量數據推送到父級，而不是在父級和子級之間交換大量數據。這確實意味著客戶端在驗證密鑰時必須做更多的工作。更具體地說，驗證 DNS 區域的密鑰資源紀錄集 (Resource Record set，RRset) 需要兩次簽章驗證操作，而不是 RFC 2535 要求的操作（對其他類型的 RRset 驗證的簽章數量沒有影響）。大多

數人認為這是一個很小的代價，因為它使 DNSSEC 部署更加實用。

四、DNS 常見攻擊

由於 DNS 潛在一些漏洞，且 DNS 是大多數網際網路請求組成的部分，這使 DNS 成為惡意攻擊的主要目標。攻擊者發現了多種針對和利用 DNS 伺服器的方法，以下是一些最常見的方法：

DNS 詐騙/快取記憶體中毒：這種攻擊會將偽造的 DNS 資料引入 DNS 解析程式的快取記憶體中，造成解析程式傳回不正確的網域 IP 位址。流量可能會被轉移到惡意電腦或攻擊者想要的其他任何位置，而不是前往正確網站；通常，這將是用於惡意目的地原始網站副本，例如分發惡意程式碼或收集登入資訊。

DNS 通道建立：此攻擊使用其他通訊協定，透過 DNS 查詢和回應建立通道。攻擊者可以使用 SSH、TCP 或 HTTP 以將惡意程式碼或竊取的資訊傳遞至 DNS 查詢中，並且不會被大部分的防火牆偵測到。

DNS 劫持：在 DNS 劫持中，攻擊者將查詢重新導向至不同的網域名稱伺服器。這可以透過惡意程式碼或未獲授權的 DNS 伺服器

修改來進行。儘管其結果與 DNS 詐騙的結果相似，但這是一種截然不同的攻擊，因為其目標是名稱伺服器上網站的 DNS 記錄，而不是解析程式的快取記憶體。

NXDOMAIN 攻擊：這是一種 DNS 洪水攻擊，攻擊者會要求不存在的記錄，藉由這樣的請求讓 DNS 伺服器應接不暇，企圖造成合法流量的阻斷服務。這可以使用純熟的攻擊工具來達成，這些工具可以對每個請求自動產生唯一的子網域。NXDOMAIN 攻擊也能以遞迴解析程式為目標，目的是使用垃圾請求填充解析程式的快取記憶體。

幻影網域攻擊：幻影網域攻擊的結果與 DNS 解析程式的 NXDOMAIN 攻擊相似。攻擊者設定一串「幻影」網域伺服器這會以非常緩慢的速度回應請求，或完全不回應請求。然後解析程式會因為對這些網域洪水般的請求而遭受攻擊，解析程式被困在等待回應的過程中，導致效能緩慢和阻斷服務。

隨機網域攻擊：在此情況下，攻擊者對某個合法網站的數個不存在的隨機子網域傳送 DNS 查詢。目標是對網域的權威名稱伺服器建立阻斷服務，使之無法從名稱伺服器查閱網站。副作用是，為攻擊者

服務的網際網路服務供應商(Internet Service Provider，ISP)也可能會受到影響，因為他們的遞迴解析程式快取記憶體將會載入不良請求。

網域鎖定攻擊：策畫此形式的攻擊時，會設定特殊網域和解析程式，用來建立與其他合法解析程式的 TCP 連線。當目標解析程式傳送請求時，這些網域會傳回緩慢的隨機封包串流，纏住解析程式的資源。

殭屍網路式 CPE 攻擊：這些攻擊使用 CPE 裝置（使用者終端裝置，這是服務提供者提供的供客戶使用的硬體，例如資料機、路由器、機上盒等）進行。攻擊者入侵 CPE，而裝置就成為殭屍網路的一部分，用來針對某個網站或網域執行隨機子網域攻擊。

五、資源紀錄

DNS 通過使用幾個資源記錄來實現。為了實現 DNSSEC，創建了幾種新的 DNS 記錄類型或將其修改為與 DNSSEC 一起使用。

表 14、DNSSEC 資源記錄

RR Type	描述
RRSIG	資源記錄簽章(resource record signature)，包含一個記錄集的 DNSSEC 簽章。DNS 解析器使用儲存在一個 DNSKEY

	記錄中的公開金鑰驗證簽章。
DNSKEY	包含用來驗證 RRSIG 記錄中 DNSSEC 簽章的 DNS 解析器的公開金鑰。
DS	委託簽署者(delegation signer)，存放委託區域的名稱。在子授權區域中引用 DNSKEY 記錄，DS 記錄與委派的 NS 記錄一起放在父區域中。
NSEC	下一個安全記錄(next secure record)，包含指向該區域中下一個記錄名稱的鏈接，並列出該記錄名稱存在的記錄類型。DNS 解析器使用 NSEC 記錄來驗證記錄名稱和類型的不存在，作為 DNSSEC 驗證的一部分。
NSEC3	下一個安全記錄版本 3 (next secure record version 3)，包含指向該區域中下一個記錄名稱的鏈接（按雜湊名稱排序順序），並在 NSEC3 記錄自己名稱的第一個標籤中列出雜湊值所覆蓋的名稱所存在的記錄類型。解析程序可以使用這些記錄來驗證記錄名稱和類型的不存在，作為 DNSSEC 驗證的一部分。NSEC3 記錄與 NSEC 記錄相似，但是 NSEC3 使用加密雜湊記錄名稱，以避免列舉區域中的記錄名稱
NSEC3PARAM	下一個安全記錄版本 3 參數(next secure record version 3 parameters)，權威 DNS 伺服器使用此記錄來計算和確定要對不存在的名稱/類型的 DNSSEC 請求進行回應的 NSEC3 記錄。

六、演算法

DNSSEC 被設計為可擴展的，因此當發現針對現有算法的攻擊時，可以以向後兼容的方式引入新演算法。下表列出了 DNSKEY 演算法

的實施建議。

表 15、DNSKEY 演算法

Number	Mnemonics	DNSSEC Signing	DNSSEC Validation
1	RSA / MD5	MUST NOT	MUST NOT
3	DSA	MUST NOT	MUST NOT
5	RSA / SHA-1	NOT RECOMMENDED	MUST
6	DSA-NSEC3-SHA1	MUST NOT	MUST NOT
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	MUST
8	RSA / SHA-256	MUST	MUST
10	RSA / SHA-512	NOT RECOMMENDED	MUST
12	ECC-GOST	MUST NOT	MAY
13	ECDSA P-256 / SHA-256	MUST	MUST
14	ECDSA P-384 / SHA-384	MAY	RECOMMENDED
15	ED25519	RECOMMENDED	RECOMMENDED
16	ED448	MAY	RECOMMENDED

- RSA / MD5 並未得到廣泛部署，且業界普遍傾向於不支援 MD5 的使用。

- RSA / SHA-1 和 RSASHA1-NSEC3-SHA1 已被廣泛部署，但由於整個行業都傾向於使用橢圓曲線密碼學，因此建議將部署它的區域切換到 ECDSA P-256 / SHA256。RSA / SHA-1 不支持 NSEC3。RSA SHA1-NSEC3-SHA1 可以與 NSEC3 一起使用，也可以不與 NSEC3 一起使用。

- DSA 和 DSA-NSEC3-SHA1 未被廣泛部署，當使用一個弱的或被破壞的亂數產生器生成簽章時，它們很容易受到私鑰洩露的攻擊。

- RSA / SHA-256 被廣泛使用並且被認為是強大的。多年來，它一直是預設演算法，現在正慢慢被 ECDSA P-256 / SHA-256 所取代，因為它的金鑰和簽章更短，使 DNS 封包更小。

- 不建議將 RSA / SHA-512 用於 DNSSEC 簽章，因為它尚未廣泛部署，但是有一些部署。因此，DNSSEC 驗證必須實現 RSA / SHA-512 以確保互操作性。RSA / SHA-512 和 RSA / SHA-256 之間的加密強度沒有顯著差異。因此，不建

議使用 RSA / SHA-512，因為這只會使舊演算法更難棄用。希望使用密碼學上更強的演算法的人應該切換到橢圓曲線加密演算法。

- ECC-GOST（GOST R 34.10-2001）已由 RFC 7091 中的 GOST R 34.10-2012 取代。GOST R 34.10-2012 尚未標準化用於 DNSSEC。

- 與 RSA / SHA-256 或 RSA / SHA-512 相比，ECDSA P-256 / SHA-256 以較短的簽章長度提供了更高的加密強度。ECDSA P-256 / SHA-256 已被廣泛部署。因此，現在對於驗證和簽章都是必須的。在實現 ECDSA P-256 / SHA-256 和 ECDSA P-384 / SHA-384 時，建議使用 RFC 6979 中指定的橢圓曲線數位簽章演算法（ECDSA）的確定性數字簽章生成過程。

- ECDSA P-384 / SHA-384 與 ECDSA P-256 / SHA-256 共享相同的屬性，但與 ECDSA P-256 / SHA-256 相比，具有適度的安全優勢（192 位元的強度與 128 位元的強度）。對於大

多數 DNSSEC 應用程式，ECDSA P-256 / SHA-256 在可預見的未來應該是令人滿意且強大的，因此建議進行簽章。雖然不太可能出現需要 192 位元安全強度的 DNSSEC 用例，但為此類應用程式提供了 ECDSA P-384 / SHA-384，並且可以在這些情況下將其用於簽章。

- ED25519 和 ED448 使用愛德華茲曲線數位簽章演算法（EdDSA）。EdDSA 具有三個主要優點：它不需要為每個簽章使用唯一的隨機數；與 ECDSA 一樣，不存在填充或截斷問題；它對側通道攻擊更具彈性。此外，EdDSA 加密不太容易出現實現錯誤（RFC8032，RFC8080）。一旦已部署的 DNSSEC 驗證程序中對該算法有足夠的支持，ED25519 則有望成為未來的推薦的默認演算法。

由於業界普遍傾向於橢圓曲線密碼學，新的 DNSSEC 部署推薦使用 ECDSA P-256 / SHA256 作為 DNSKEY 演算法，基於 RSA 演算法的使用者應該升級到 ECDSA P-256 / SHA256。

下表列出了有關委託簽署者摘要算法[DS-IANA]的建議。這些建議還適用於[RFC7344]中指定的 Child DS（CDS）RRTYPE。

表 16、DS 和 CDS 演算法

Number	Mnemonics	DNSSEC Delegation	DNSSEC Validation
0	NULL(CDS only)	MUST NOT [*]	MUST NOT [*]
1	SHA-1	MUST NOT	MUST
2	SHA-256	MUST	MUST
3	GOST R 34.11-94	MUST NOT	MAY
4	SHA-384	MAY	RECOMMENDED

[*]-這是一種特殊類型的 CDS 記錄，用信號表示在[RFC8078]中刪除了父級的 DS。

- NULL 是一種特殊情況；參見[RFC8078]。
- SHA-1 仍廣泛用於委託簽署者（DS）記錄，因此驗證器必須實施驗證，但絕不能用於生成新的 DS 和 CDS 記錄。
- SHA-256 被廣泛使用並且被認為是強大的。
- GOST R 34.11-94 已在[RFC6986]中被 GOST R 34.11-2012 取代。GOST R 34.11-2012 尚未標準化用於 DNSSEC。
- SHA-384 與 SHA-256 共享相同的屬性，但與 SHA-256 相比具有適度的安全優勢（384 位元的強度與 256 位元的強

度）。對於 DNSSEC 的大多數應用，SHA-256 在可預見的將來應該是令人滿意且強大的，因此建議將其用於 DS 和 CDS 記錄。雖然不太可能需要 384 位元安全強度的 DNSSEC 使用案例出現，但為此類應用程式提供了 SHA 384，並且在這些情況下可以將其用於生成 DS 和 CDS 記錄。

七、尋找過程

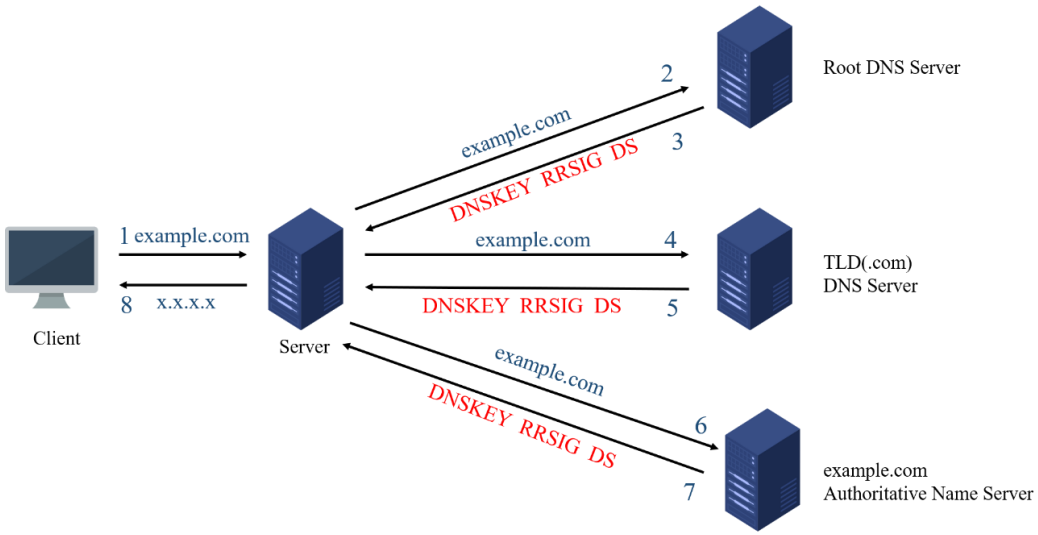


圖 115、DNSSEC 運作流程

DNSSEC 運作流程如下:

1. 使用者向 DNS 伺服器要求解析 example.com 的網址
2. 伺服器向 Root 伺服器詢問
3. Root 伺服器回應自己的 DNSKEY、RRSIG 和下層伺服器的 DS 金鑰

4. 向 com 層級 DNS 伺服器詢問

5. com 層級 DNS 伺服器回應自己的 DNSKEY、RRSIG 和下層伺服器的 DS 金鑰，伺服器利用從 Root 伺服器取得的 DS 金鑰比對和.com 所提供的是否一致

6. 向 example.com 所在的 DNS 伺服器詢問

7. example.com 所在的 DNS 伺服器回應自己的 DNSKEY、RRSIG，伺服器利用從.com 取得的 DS 金鑰比對和 example.com 所提供的是否一致

8. 回應 x.x.x.x 的 IP 位置給使用者

根據 DNS 查找的結果，具有安全意識的 DNS 解析器可以確定所查詢域的權威名稱伺服器是否支持 DNSSEC，其收到的答案是否安全以及是否存在某種錯誤。對於遞迴名稱伺服器和存根解析器，查找過程有所不同。Microsoft Windows 使用存根解析器，而 Windows Server 2008 R2 和 Windows 7 特別使用非驗證但可識別 DNSSEC 的存根解析器。

(一) 遞迴名稱服務器

使用信任鏈模型，父系網域中的委託簽章者(DS)記錄可以用來驗證子域中的 DNSKEY 記錄，然後子域可以包含其他 DS 記錄來驗證

進一步的子域。假設遞迴解析器(比如 ISP 名稱伺服器)想要獲得功能變數名稱“www.example.com”的 IP 位址(一個記錄和/或 AAAA 記錄)。

1、 當安全意識解析器在 DNS 查詢中設置“DO”(DNSSEC OK）標誌位時，該過程開始。由於 DO 位在 EDNS 定義的擴展標誌位中，因此所有 DNSSEC 事務都必須支持 EDNS。EDNS 支持還需要允許 DNSSEC 事務所需更大的數據包大小。

2、 當解析器通過正常的 DNS 查找過程收到答案時，它將進行檢查以確保答案正確。理想情況下，安全意識解析器將從驗證 DNS 根目錄處 DS 和 DNSKEY 記錄開始。然後，它將使用在根目錄中找到的“ com” 頂級域的 DS 記錄來驗證“com”區域中的 DNSKEY 記錄。而它將看到在“com”區域中是否存在“example.com”子域的 DS 記錄，如果有，那麼它將使用 DS 記錄來驗證在“example.com”中找到的 DNSKEY 記錄。最後，它將驗證在“www.example.com”A 記錄的答案中找到的 RRSIG 記錄。

上面的範例有幾個例外。首先，如果“example.com”不支持 DNSSEC，則答案中將沒有 RRSIG 記錄，並且“com”區域中沒有

“ example.com”的 DS 記錄。如果存在“example.com”的 DS 記錄，但答覆中沒有 RRSIG 記錄，則是出了問題，可能是中級人員在繼續攻擊，剝離 DNSSEC 信息並修改 A 記錄。或者，它可能是一台損壞的安全性名稱伺服器，從查詢中刪除了 DO 標誌位或從答案中刪除了 RRSIG 記錄，也可能是配置的錯誤。

接下來，可能是沒有域名“www.example.com”，在這種情況下，不是返回答案中的 RRSIG 記錄，而是一個 NSEC 記錄或 NSEC3 記錄。這些是“下一個安全”記錄，可讓解析器證明域名不存在。NSEC / NSEC3 記錄具有 RRSIG 記錄，可以如上所述進行驗證。

最後，可能是“example.com”區域實現了 DNSSEC，但是“com”區域或根區域都沒有，從而創建了一個“安全島”，需要以其他方式進行驗證。截至 2010 年 7 月 15 日，DNSSEC 到根的部署已完成。.com 域已使用有效的安全密鑰簽章，並且安全委派已於 2011 年 4 月 1 日添加到根區域。

(二) 存根解析器

存根解析器是使用遞迴查詢模式將大部分 DNS 解析工作分流到遞迴名稱伺服器的最小 DNS 解析器。存根解析器將簡單地將請求轉發到遞迴名稱伺服器，並將回應中的 Authenticated Data（AD）位用作提示，以查明遞迴名稱伺服器是否能夠驗證所有遞迴名稱伺服器回

應的答案和權限部分中所有數據的簽章。Microsoft Windows 使用存根解析器，而 Windows Server 2008 R2 和 Windows 7 特別使用了非驗證但可識別 AD 位的存根解析器。

一個驗證存根解析器可能還可以通過其查詢消息設置 Checking Disabled（CD）位執行自己的簽章驗證。驗證存根解析器使用 CD 位執行自己的遞迴身份驗證。使用這樣的驗證存根解析器可以為實現 DNSSEC 的域提供客戶端端到端 DNS 安全性，即使網際網路服務提供商或與它們的連接不受信任也是如此。

為了使非驗證存根解析器真正依賴 DNSSEC 服務，存根解析器必須同時信任有問題的遞迴名稱伺服器（通常由網際網路服務提供商控制）以及其與這些名稱伺服器之間的通訊通道，使用方法如 IPsec、SIG（0）或 TSIG 之類的方法。但 IPsec 的使用並不廣泛。

八、信任錨(Trust anchors)

要證明 DNS 答案是正確的，需要從 DNS 以外的來源知道至少一個正確的金鑰或 DS 記錄。這些起點稱為信任錨點，通常驗證解析器必須通過 DNS 協議之外的某些安全或可信源來獲取其信任錨的初始值。最初設計 DNSSEC 時，人們認為唯一需要的信任錨點是 DNS 根伺服器。根錨首次發佈於 2010 年 7 月 15 日。信任錨是放置在驗證解析器中的密鑰，以便驗證器可以將給定請求的結果驗證返回已知或信

任的公開金鑰（信任錨）。驗證解析器必須至少安裝一個信任錨才能執行 DNSSEC 驗證。

(一) 否定信任錨(Negative Trust Anchors, NTA)

DNS 遞迴解析器的運營商，例如 ISP 偶爾會發現域錯誤地管理與 DNSSEC 相關的資源記錄。這種管理不當會觸發 DNSSEC 驗證失敗，導致大量最終用戶無法訪問域。許多最終用戶傾向於將其解釋為 ISP 或解析器運營商的失敗，他們可能會切換到非驗證解析器或聯繫其 ISP 進行投訴，而不是將其視為他們想要到達的域的部分失敗。這種壓力可能會導致解析程序操作員禁用或根本不部署 DNSSEC 驗證。

否定信任錨（NTA），可在向普遍存在的 DNSSEC 部署過渡期間使用。NTA 在驗證 DNS 遞迴解析器上本地配置，以保護最終用戶免受 DNSSEC 相關的權威名稱伺服器操作錯誤的影響。NTA 是臨時的，僅由需要 NTA 的組織實施，而不是由管理邊界之外的任何組織分發。

使用 NTA 臨時禁用特定配置錯誤域名的 DNSSEC 驗證會立即恢復最終用戶的訪問權限。這使域的管理員可以解決他們的錯誤配置，同時還允許使用 NTA 的組織保持啟用 DNSSEC 驗證的狀態，並且仍然可以訪問錯誤配置的域。以下為否定信任錨能夠改善的三種情況：

1、 緩解域驗證失敗

域名驗證失敗的原因有兩個：一般的安全性失敗（例如，由於某

種攻擊或破壞）或區域管理員配置錯誤。當域過渡到 DNSSEC 時，驗證失敗的最常見原因是配置錯誤。

由於不同軟件開發人員對 DNSSEC 標準的解釋方式或這些開發人員選擇實現對DNSSEC支持的方式不同，也可能導致某些DNSSEC驗證失敗。例如，可以想像一個域可能是經過 DNSSEC 正確簽章的，一個供應商的 DNS 遞迴解析程序將驗證該域，而其他供應商的軟件可能無法驗證該域。

2、 改善最終用戶(End-User)體驗

最終用戶通常不知道或不了解導致連接發生的解析過程。這是設計使然：DNS 的目的是使用戶不必通過更友好的命名系統來記住 IP 地址。由此得出結論，最終用戶不應該也不應該知道 DNSSEC，驗證或任何種類的訊息。由於與 DNSSEC 相關的錯誤配置，最終用戶可能會誤解無法訪問域。他們可能錯誤地認為 ISP 故意阻止了對該域的訪問，或者這是 ISP 方面（尤其是 ISP 的 DNS 伺服器）性能故障。他們可能會聯繫 ISP 進行投訴，這將為其 ISP 產生費用。此外，他們可能會使用在線工具和網站來投訴此問題，例如通過網站論壇或社交媒體網站，這可能會導致其他最終用戶的不滿或對 ISP 或運營商的普遍批評 DNS 遞迴解析器。

隨著最終用戶公佈這些故障，其他人可能會建議他們從安全意識

較高的 DNS 解析器切換到不執行 DNSSEC 驗證的解析器。而 ISP 或其他 DNS 遞迴解析器操作員實際上在做他們應該解析的域名失敗時應做的事情；當無法再驗證域時，這是預期的結果，它可以保護最終用戶免受潛在的安全威脅。使用 NTA 將允許 ISP 特別糾正無法到達該域的故障，而不會影響其他站點的安全性。這將使最終用戶滿意，對 ISP 的影響最小，同時為正確維護的域維護 DNSSEC 的安全性。

3、 避免切換到非驗證解析器

有些人可能會考慮自己切換到其他未驗證的解析程序，或者可能建議其他人這樣做。但是，如果域未通過 DNSSEC 驗證並且不可訪問，則很可能是與安全相關的問題。為了盡可能地安全，最終用戶不應將 DNS 伺服器更改為不執行 DNSSEC 驗證的解決方法，人們也不應該建議其他人也這樣做。由於正當原因，相對於配置錯誤，使 DNSSEC 失敗的域可能受到駭客的控制，或者該域可能存在其他重大安全問題。

因此，不建議切換到非驗證解析器以恢復對 DNSSEC 驗證失敗的域的訪問，這對其他人是不好的建議，並且可能對最終用戶的安全有害。

九、信任鏈(Chain of trust)

在電腦安全性中，通過驗證軟體和硬體的每個組件來建立信任鏈。

主要目的在確保僅使用受信任的軟體和硬體，同時仍保持靈活性。簽章機構將僅對強制執行安全性的啟動程序進行簽章，例如僅運行本身已簽章的運行程序，或僅允許已簽章的代碼訪問電腦的某些功能。此過程可能會持續幾層。而這個過程產生了信任鏈。可以相信最終軟體具有某些屬性，因為如果對它進行了非法修改，則其簽章將無效，並且先前的軟體也不會執行它。以前的軟體是可以信任的，因為如果簽章無效，則不會加載該軟體。每一層的可信賴性由之前的一層（回到信任錨點）來保證。

在 DNSSEC 中，查詢名稱伺服器使用區域的公鑰來驗證區域中的簽章數據。而公開金鑰的有效性是由區域的父級別確定。例如，如果我們的簽章區域稱為 example.com，那麼為 example.com 區域的公開金鑰擔保的就是 com 區域。

在 example.com 區域簽章後，管理員會將其公開金鑰的副本以及確定他是 example.com 區域的正式授權管理員的所有必要訊息發送給 com 區域的管理員。一旦 com 區域的管理員對自己擁有 example.com 區域的合法公鑰感到滿意，便會將新記錄添加到 com 區域，稱為 DS 記錄。DS 記錄包含公開金鑰的指紋。然後，com 區域的管理員在 com 區域簽章，該區域添加了 RRSIG 記錄，以證明此新 DS 記錄是真實的。

當在 example.com 中解析域名的名稱伺服器查詢其中一個 com 名稱伺服器時，它將收到包含 DS 記錄的 example.com 名稱伺服器的引用。而在引用中的 NS 記錄和 DS 記錄都將被簽章。當查詢名稱伺服器查找 example.com DNSKEY 記錄以驗證已簽章的 example.com 記錄，它將首先從 DS 記錄中的指紋驗證 DNSKEY 記錄。

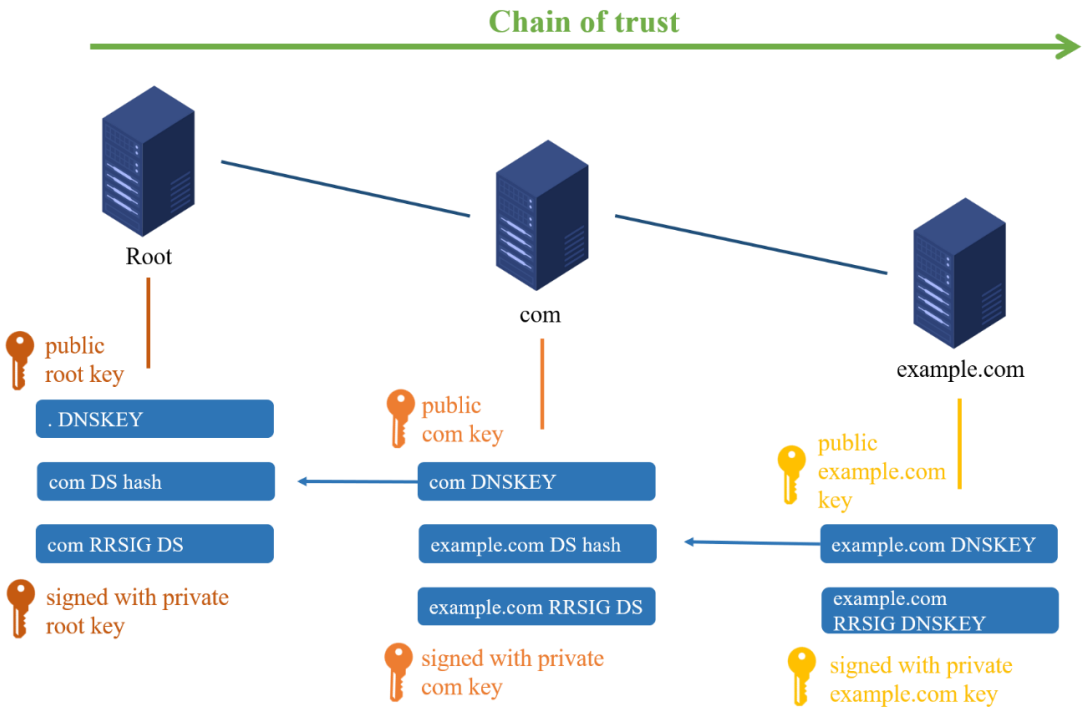


圖 116、Chain of trust 示意圖

十、簽名和區域簽名

為了限制重播攻擊，不僅存在用於緩存的常規 DNS TTL 值，而且在 RRSIG 記錄中還存在用於限制簽章有效性的額外時間戳記。與 TTL 值相對於記錄發送的時間不同，時間戳記是絕對的。這意味著所有具有安全意識的 DNS 解析器必須有相當緊密同步的時鐘，比如在

幾分鐘內。

這些時間戳記意味著必須定期重新簽署區域並將其重新分發到次要伺服器，否則簽章將被驗證解析器拒絕。

DNSSEC 引入了簽章區域的概念。簽章區域分別包括 DNS 公鑰（DNSKEY），資源記錄簽章（RRSIG），下一安全（NSEC）和委託簽章者（DS）記錄。而不包括這些記錄的區域屬於未簽章的區域。

十一、 密鑰管理

DNSSEC 涉及許多不同的密鑰，既儲存在 DNSKEY 記錄中，也儲存在其他來源中，以形成信任錨。為了允許替換密鑰，需要密鑰翻轉方案。通常除了現有的舊密鑰之外，這還涉及在新的 DNSKEY 記錄中首先推出的新密鑰。然後，當可以安全地認為生存時間值已導致舊鍵的緩存已通過時，可以使用這些新鍵。最後，當可以安全地假定使用舊密鑰的記錄緩存已過期時，可以刪除舊的 DNSKEY 記錄。對於諸如信任錨的密鑰之類的事情，此過程更加複雜，這可能需要更新操作系統。

DNSKEY 記錄中的金鑰可用於兩種不同的事物，通常每種金鑰都使用不同的 DNSKEY 記錄。分別有用於簽章其他 DNSKEY 記錄的 KSK，以及用於簽章其他記錄的 ZSK。以下為這兩種金鑰的介紹：

- Zone-Signing Keys (ZSK)

DNSSEC 中的每個區域都有一個區域簽章密鑰（ZSK）。密鑰的私有部分對區域中的每個 RRset 進行數字簽章，而公共部分則對簽章進行驗證。為了啟用 DNSSEC，區域運營商使用私有 ZSK 為每個 RRset 創建數位簽章，並將其作為 RRSIG 記錄儲存在其名稱伺服器中。但是，除非 DNS 解析程序具有驗證簽章的方法，否則這些 RRSIG 記錄將無用。區域運營商還需要通過將公共 ZSK 添加到 DNSKEY 記錄中的名稱伺服器來使其可以使用。當 DNSSEC 解析程序請求特定記錄類型（例如 AAAA）時，名稱伺服器也返回相應的 RRSIG。然後，解析程序可以從名稱伺服器中提取包含公用 ZSK 的 DNSKEY 記錄。RRset，RRSIG 和公共 ZSK 可以一起驗證回應。如果我們信任 DNSKEY 記錄中的區域簽章密鑰，則可以信任該區域中的所有記錄。但是，如果區域簽章密鑰被洩露，我們則需要另一種方法來驗證公開 ZSK。

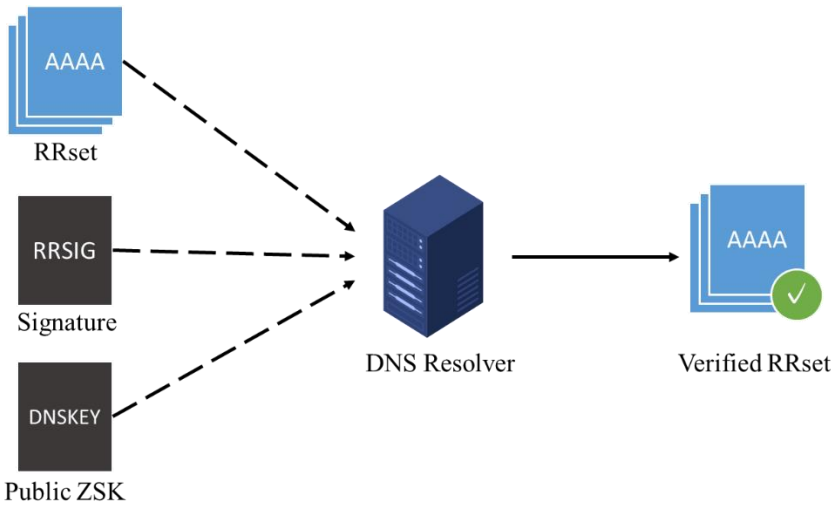


圖 117、ZSK 驗證流程

- Key-Signing Keys (KSK)

除了區域簽章密鑰外，DNSSEC 名稱伺服器還具有密鑰簽章密鑰（KSK）。KSK 驗證 DNSKEY 記錄的方式與 ZSK 保護其餘 RRset 的方式完全相同。它簽章公共 ZSK（儲存在 DNSKEY 記錄中），從而為 DNSKEY 創建 RRSIG。

就像公用 ZSK 一樣，名稱伺服器將公用 KSK 發佈到另一個 DNSKEY 記錄中，這給了 DNSKEY RRset。公共 KSK 和公共 ZSK 均由私有 KSK 簽章。然後，解析程序可以使用公共 KSK 來驗證公共 ZSK。

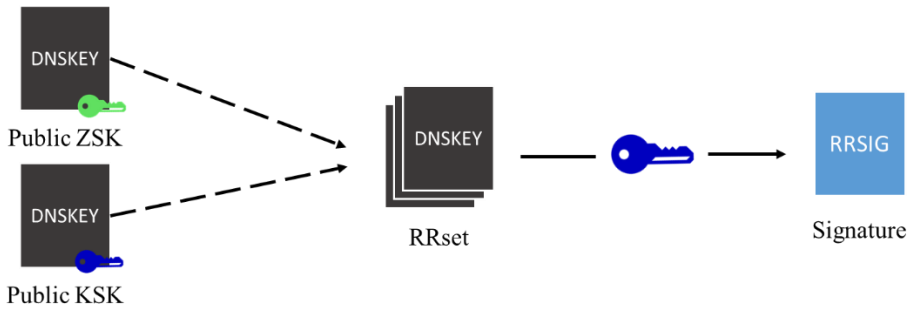


圖 118、KSK 驗證流程

由於 ZSK 受一個特定 DNS 區域的完全控制和使用，因此可以更輕鬆，更頻繁地進行切換。ZSK 可以比 KSK 短得多，並且仍可以提供相同級別的保護，同時減小 RRSIG / DNSKEY 記錄的大小。

創建新的 KSK 時，必須將 DS 記錄轉移到父區域並在那裡發布。

DS 記錄使用 KSK 的消息摘要而不是完整密鑰，以保持較小的記錄大小。這對於.com 域之類的區域非常有用。與要求 DNSKEY 記錄位於父區域中的早期 DNSSEC 版本相比，在父區域中更新 DS 密鑰的過程也更簡單。

十二、 部署

網際網路是至關重要的基礎架構，但其運行於不安全的 DNS。因此，有強烈的動機來保護 DNS，而部署 DNSSEC 通常被認為是這項工作的關鍵部分。例如，《美國國家安全網路空間戰略》明確指出了對 DNS 安全的需求。DNSSEC 的大規模部署還可以解決許多其他安全問題，例如電子郵件地址的安全密鑰分發。

在大型網路中部署 DNSSEC 也具有挑戰性。Ozment 和 Schechter 觀察到 DNSSEC 存在“引導問題”，用戶通常僅在獲得直接收益的情況下才部署技術，但是如果需要最低限度的部署才能使任何用戶獲得的收益大於其成本，會難以部署。DNSSEC 可以部署在 DNS 層次結構的任何級別，但是在許多其他人希望採用它之前，它必須在區域中廣泛可用。必須使用支持 DNSSEC 的軟體更新 DNS 伺服器，並且必須創建 DNSSEC 數據並將其添加到 DNS 區域數據中。使用 TCP / IP 的客戶端必須先更新其 DNS 解析器（客戶端），然後才能使用 DNSSEC 的功能。更重要的是，任何解析程序在開始使用 DNSSEC 之

前，必須擁有或擁有一種至少可以信任的公鑰的獲取方式。

DNSSEC 實施可能會造成某些 DNS 伺服器增加的負載。常見的 DNSSEC 簽章回應遠遠大於默認的 512 位元 UDP 大小。從理論上講，這可以通過多個 IP 片段來處理，但是該領域中的許多“中間盒”無法正確處理這些片段。這導致使用 TCP 代替。然而，許多當前的 TCP 實現為每個 TCP 連接儲存大量數據。重負載的伺服器可能會耗盡資源，只是試圖回應大量（可能是偽造的）DNSSEC 請求。已經開發了一些協議擴展（例如 TCP Cookie 事務）來減少此負擔。為了應對這些挑戰，由於網際網路對許多組織至關重要，因此正在大力部署 DNSSEC。

(一) 早期部署

早期使用 DNSSEC 作為其國家頂級域名代碼包括巴西（.br）、保加利亞（.bg）、捷克共和國（.cz）、納米比亞（.na）、波多黎各（.pr）和瑞典（.se）。RIPE NCC 已經簽署了所有從網際網路分配號碼授權機構（IANA）委派給它的反向查詢記錄（in-addr.arpa）。美國網際網路號碼註冊處(ARIN)也正在簽署其反向區域。在 2007 年 2 月丹麥電信公司 TDC 成為第一個開始向其客戶提供此功能的瑞典 ISP。

自 2007 年 6 月以來，IANA 公開測試了簽章的根範例。在根簽章生產之前的這段時間內，還存在多個替代的信任錨。IKS 耶拿在

2006 年 1 月 19 日推出了一個，網際網路系統聯盟(Internet Systems Consortium)在同年 3 月 27 日推出了另一個，而 ICANN 在 2009 年 2 月 17 日宣佈了第三個。

2009 年 6 月 2 日，公共利益註冊中心簽署了.org 區域。公共利益註冊機構也於 2008 年 9 月 26 日詳細說明，第一階段將涉及與朋友和家人有緊密工作關係的大型註冊服務商，最早將於 2009 年開始 。2010 年 6 月 23 日，列出了 13 個註冊商，它們為.ORG 域提供 DNSSEC 記錄。

威瑞信（VeriSign）運行了一個試點項目，允許.com 和.net 域進行自身註冊以進行 NSEC3 實驗。他們在 2009 年 2 月 24 日宣布，他們將在 24 個月內在所有頂級域（.com，.net 等）中部署 DNSSEC，並在同年 11 月 16 日說，.com 和.net 由於實施的技術方面的原因，這些域名將在 2011 年第一季度簽署。該目標已按計劃實現，Verisign 的 DNSSEC 副總裁 Matt Larson 因在推進 DNSSEC 方面的作用而獲得了 2011 年 InfoWorld 的技術領導獎。

(二) 在 DNS 根目錄下部署

DNSSEC 首次於 2010 年 7 月 15 日在根級別進行部署。由於根信任錨可用於驗證具有完整信任鏈的任何 DNSSEC 區域，因此有望大大簡化 DNSSEC 解析器的部署。由於必須將信任鏈追溯到受信任

的根而不中斷，以進行驗證，因此，如果安全地帶上方的任何區域都不安全，則仍必須為安全區域配置信任錨。例如，如果保護了“signed.example.org”區域，但沒有保護“example.org”區域，則即使對“.org”區域和根進行了簽章，也必須在其中部署信任錨來驗證區域。

關於簽署根源的問題一直是一個持續關注的問題，主要是關於一些中心問題：

- 其他國家擔心美國對網際網路的控制，因此可能會拒絕任何集中式密鑰輸入。
- 一些政府可能會嘗試禁止 DNSSEC 支持的加密密鑰分發。

1、 規劃

ICANN 和 VeriSign 在 2008 年 9 月分別發布了實施提案，而在 10 月，美國國家電信暨資訊管理局（NTIA）向公眾徵求意見。尚不清楚收到的評論是否影響了最終部署計劃的設計。

2009 年 6 月 3 日，美國國家標準暨技術研究院（NIST）宣布與 ICANN 的計劃，VeriSign 和 NTIA 一起在 2009 年底前簽署根協議。

2009 年 10 月 6 日，在第 59 屆 RIPE 大會上，ICANN 和 VeriSign 宣布了計劃在根區域內部署 DNSSEC 的部署時間表。在會議上宣布，它將從 2009 年 12 月 1 日開始每月遞增部署到一個根名稱伺服器，最

終的根名稱伺服器將在 2010 年 7 月 1 日為 DNSSEC 簽章區域提供服務，根區域將使用 RSA/SHA256 DNSKEY 簽章。在增量推出期間，根區域將用作使用虛擬密鑰的故意無法驗證的根區域（DURZ），最終的 DNSKEY 記錄要到 2010 年 7 月 1 日才分發。這意味著用於簽章區域使用的密鑰是故意不可驗證的。進行此部署的原因是監視由請求 DNSSEC 資源記錄的查詢的較大回應引起的流量模式變化。

.org 頂級域名已於 2010 年 6 月與 DNSSEC 簽署，隨後在 2010 年和 2011 年晚些時候與.com，.net 和.edu 簽署了協議。國家代碼頂級域名於 2010 年 5 月開始能夠儲存密鑰。截至 2011 年 11 月，超過 25% 的頂級域名已與 DNSSEC 簽署。

2、 實施

2010 年 1 月 25 日，L（ell）根伺服器開始為故意不可驗證的根區域（DURZ）提供服務。該區域使用 RFC 5702 中定義的使用 RSA 算法創建的 SHA-2（SHA-256）雜湊的簽章。截至 2010 年 5 月，所有十三台根伺服器都已開始為 DURZ 服務。2010 年 7 月 15 日，第一台根完整生產 DNSSEC 根區域已簽署，其 SOA 序列號為 2010071501。根信任錨可從 IANA 獲得。

3、 在 TLD 級別進行部署

在根目錄下，必須簽署一大套頂級域，以實現完整的 DNSSEC 部

署。網際網路頂級域列表提供了有關哪些現有頂級域已簽章並鏈接到根的詳細訊息。

4、 DNSSEC 後備驗證-歷史

在 2006 年 3 月，網際網路系統聯盟引入了 DNSSEC 後備驗證註冊表。DLV 旨在使 DNSSEC 在沒有根信任錨的情況下更易於部署。當時，人們想像驗證者可能必須維護與 DNS 的簽章子樹相對應的大量信任錨。DLV 的目的是允許驗證者將管理信任錨儲存庫的工作分擔給可信任的第三方。DLV 註冊中心維護信任錨的中央列表，而不是每個驗證器都重複維護自己的列表的工作。

要使用 DLV，需要支持它的驗證器，例如 BIND 或 Unbound，並為其配置了 DLV 區域的信任錨。該區域包含 DLV 記錄； 它們具有與 DS 記錄完全相同的格式，但是它們不是引用委託的子區域，而是引用 DNS 樹中其他地方的區域。當驗證器找不到要嘗試檢查的從根到 RRset 的信任鏈時，它將搜索 DLV 記錄以提供替代的信任鏈。

信任鏈中的空白（例如未簽章的頂級域或不支持 DNSSEC 委派的註冊商）意味著較低級別域的管理員可以使用 DLV 來允許已配置為使用 DLV 的解析器驗證其 DNS 數據 。這可能通過減輕註冊服務商和 TLD 註冊管理機構的壓力來適當支持 DNSSEC，從而阻礙了 DNSSEC 的部署。DLV 還通過為 DNSSEC 驗證添加更多參與者和代

碼路徑而增加了複雜性。

ISC 在 2017 年停用了其 DLV 註冊中心。BIND 9.12 中棄用了 DLV 支持，並已從 BIND 9.16 中完全刪除了該支持。未綁定版本 1.5.4（2015 年 7 月）在範例配置和手冊頁中將 DLV 標記為已停用。Knot Resolver 和 PowerDNS Recursor 從未實現 DLV。

2020 年 3 月，IETF 發布了 RFC 8749，將 DLV 取消為標準，並將 RFC 4432 和 RFC 5074 移至歷史狀態。

5、 美國聯邦政府的 DNSSEC 部署計劃

美國國土安全部（DHS）科學技術局贊助了“DNSSEC 部署計劃”。該計劃鼓勵所有部門自願採取安全措施，以提高網際網路命名基礎設施的安全性，這是涉及許多公共和私營部門的國家和組織的全球合作努力的一部分。國土安全部還為 DNSSEC 的完善工作提供資金，並將其部署在美國聯邦政府內部。

據報導，2007 年 3 月 30 日，美國國土安全部提議“擁有在美國政府手中牢固簽署 DNS 根區的密鑰”。但是會議室中沒有美國政府官員在場，引發這篇文章的言論是另一方提出的。國土安全部隨後評論了為什麼他們認為其他人會誤以為美國政府已經提出了這樣的提議：“美國國土安全部正在資助制定實施 DNSSEC 的技術計劃，去年 10 月分發了一份初步計劃草案。草案向一長串國際專家徵求意見。

草案為誰可以成為根區密鑰的持有者或“操作者”列出了一系列選擇方案，基本上是由政府機構或承包商負責。國土安全部網路安全研究和發展經理 Maughan 說: “在檔中我們沒有提出任何關於根金鑰操作員身份的建議。”

6、 在美國聯邦政府中部署 DNSSEC

美國國家標準技術研究院（NIST）在 2006 年 5 月 16 日發布了 NIST 特別出版物 800-81 安全域名系統（DNS）部署指南，並提供了有關如何部署 DNSSEC 的指南。NIST 打算參考此部署指南，在 NIST SP800-53-R1 中發布新的 DNSSEC 聯邦信息安全管理法（FISMA）要求。美國機構將在 NIST SP800-53-R1 最終發布之後一年後才能滿足這些新的 FISMA 要求，但是當時 NSEC3 尚未完成。NIST 已建議使用拆分域，該技術已知是可行的，但難以正確部署，並且存在上述安全漏洞。

2008 年 8 月 22 日，管理和預算辦公室（OMB）發布了一項備忘錄，要求美國聯邦機構在.gov 網站之間部署 DNSSEC；.gov 根目錄必須在 2009 年 1 月之前簽章，.gov 下的所有子域都必須在 2009 年 12 月之前簽章。雖然該備忘錄著重於.gov 網站，但美國國防信息系統局表示打算滿足該.OMB DNSSEC 要求。軍事（美軍）領域也是如此。NetworkWorld 的 Carolyn Duffy Marsan 表示，DNSSEC 尚未得到廣泛

部署，因為它遇到了典型的“雞與蛋”難題，而 OMB 要求它似乎在破裂。

7、 在解析器中部署

一些 ISP 已開始部署驗證 DNSSEC 的 DNS 遞迴解析器。康卡斯特（Comcast）成為美國第一個這樣做的主要 ISP，於 2010 年 10 月 18 日宣布了其意圖，並於 2012 年 1 月 11 日完成了部署。

根據 APNIC 的一項研究，到 2013 年 5 月，僅使用 DNS 解析器執行 DNSSEC 驗證的客戶比例上升到 8.3%。其中大約一半的客戶使用 Google 的公共 DNS 解析器。

2015 年 9 月，Verisign 宣布了免費的公共 DNS 解析器服務，儘管在新聞發布中未提及，但它還執行 DNSSEC 驗證。

到 2016 年初，APNIC 的監控顯示，僅使用執行 DNSSEC 驗證的 DNS 解析器的客戶端比例已增加到約 15%。

(1) 支援 DNSSEC

- Google Public DNS 是一項免費提供的公共 DNS 服務，完全支持 DNSSEC。
- 2013 年 5 月 6 日，Google 公共 DNS 默認啟用了 DNSSEC 驗證；這意味著除非客戶明確選擇退出，否則所有查詢都將得到驗證。

- 自 9.5 版起，BIND 是最流行的 DNS 管理軟體，默認情況下啟用 DNSSEC 支持。
- 默認情況下，Quad9 在其主伺服器上啟用 DNSSEC。但是，它們還提供了在不同 IP 地址上不使用 DNSSEC 的伺服器。

十三、 工具

DNSSEC 部署需要伺服器端和用戶端上的軟體。支持 DNSSEC 的一些工具包括：

- Windows 7 和 Windows Server 2008 R2 包括一個“安全感知”的存根解析器，它能夠通過遞迴名稱伺服器區分安全回應和不安全回應。Windows Server 2012 DNSSEC 相容主動目錄集成區域的安全動態更新，以及主動目錄複寫錨鍵到其他此類伺服器。
- BIND 是最流行的 DNS 名稱伺服器(包括 dig)，它合併了較新的 DNSSEC-bis (DS records)協定以及對 NSEC3 記錄的支援。
- Unbound 是一個根據 DNSSEC 概念從頭開始設計的 DNS 名稱伺服器。

- mysqlBind 用於 DNS asp 的 GPL DNS 管理軟體現在支援 DNSSEC。
- OpenDNSSEC 是一個指定的 DNSSEC 簽署者工具，使用 PKCS#11 與硬體安全模組介面。
- Knot DNS 在 1.4.0 版本中增加了對自動 DNSSEC 簽名的支持。
- 從 3.0 版本開始，PowerDNS 完全支持預簽名和即時簽名模式的 DNSSEC。

十四、 IoT 與 DNSSEC

物聯網(IoT)通過來自各種傳感器數據的不斷更新物理環境的表示形式，再通過執行器對現實世界進行操作來實現目的，而這些動作通常都不需要人工直接參與或意識。

物聯網設備上的應用程式通常是在廣泛的硬體，CPU 體系結構和操作系統上運行。而某些程序在具有小型電池供電傳感器且沒有用戶界面的 IoT 設備上運行，並通過中間節點連接到網際網路的低功率無線電，例如低功耗藍牙（BLE）或 Zigbee 進行通訊。其他具有更高交互功能(例如具有觸控界面的冰箱)，強大的處理和儲存功能，WiFi 連接以及內置 IP 協議棧的高端設備上運行，從而使它們可以直接連接使用網際網路上的服務。

現代具有 IP stack 的 IoT 設備通常與網際網路上的一個或多個遠程服務交換數據，並使用 DNS 定位這些服務。因為物聯網設備可以感知物理環境並在物理環境上起作用，因此具有 DNS 功能可以滿足部分安全性、穩定性和透明度要求。例如，連接的門鎖的控制軟體需要確保它與用戶向其發送解鎖指令的網際網路服務進行對話。如果 IoT 設備驗證了 DNSSEC 簽章，則它將能夠發現 DNSSEC 驗證錯誤，並決定不接受 DNS 告訴其連接服務的解鎖指令。DNSSEC 驗證錯誤通常是中間人攻擊的結果，例如，於 2018 年 4 月針對亞馬遜的路由劫持。如果沒有 DNSSEC，設備將不會注意到此類攻擊，並且會從惡意目的地發送或接收流量，這可能會危害用戶的安全和隱私。但廣泛地用於傳統網際網路應用程式的 DNSSEC 已經具有挑戰性，對於 IoT 而言則更為複雜，因為它需要許多不同的 IoT 操作系統（例如 OpenWRT，RIOT 和 Contiki）的支持，並且必須處理更多的硬體（例如，限制在低功耗硬件上實現密碼功能）。

(一) 使用 DNSSEC 檢測 IoT 設備的惡意重新導向

DNSSEC 能為 IoT 設備檢測惡意重新導向的問題， DNSSEC 在 DNS 中提供了訊息完整性，這表示解析程序能夠檢測對 DNS 訊息的內容進行更改的敵人（例如，通過將虛假訊息注入解析程序的緩存中）。這在物聯網中尤其重要，因為操縱的 DNS 訊息會將物聯網設備

重新定向到惡意服務，這會危害用戶的隱私和安全。另外，用戶可能不知道這樣的重新定向，因為設備可能是非交互式並且自主運行的設備（例如，沒有用戶界面的微小傳感器）。這不同於傳統的網際網路應用程式，在傳統情況下，用戶通常會與遠程內容或服務進行顯式交互（例如，使用瀏覽器或移動設備上的應用程式）。

DNSSEC 檢測一種特別的攻擊類型為 Border Gateway Protocol（BGP）劫持，該劫持通常在網際網路上發生。BGP 劫持不同於 DNS 緩存中毒攻擊，DNS 緩存中毒攻擊是直接針對解析器，而 DNSSEC 最初的設計就是為了防範這種攻擊。使用更好的端口隨機性的現代解析程序可以緩解部分 DNS 緩存中毒攻擊。路由劫持可能還會持續發生一段時間，因為用於防禦它們的解決方案正在部署（例如 RPKI），但尚未達到普遍部署的程度。

舉例來說，敵人通過路由劫持將設備（智慧手錶）重新定向到惡意服務。攻擊者通過向網際網路的路由系統中注入惡意公告來實現此目的，聲稱其擁有網路的 IP 地址範圍，從而導致網際網路將智慧手錶的 DNS 查詢以及所有其他流量路由到敵人的網路。為了在劫持之後從智慧手錶捕獲任何 DNS 查詢，敵人還設置了一個惡意名稱伺服器，該伺服器使用不是正確的 IP 地址回答對查詢，從而有效地毒化了緩存智慧手錶使用的解析程序的大小。在查詢時連接到惡意服務，

這使得惡意服務可以分析或解密智慧手錶的傳感器訊息，甚至將指令發送到門鎖，從而使其作用於用戶的物理環境。

DNSSEC 通過對 DNS 記錄進行數位簽章來工作，這使解析程序可以使用 DNSSEC 的信任鏈來驗證這些簽章。驗證錯誤表示權威名稱伺服器的回應可能已被篡改，例如，由於中間發生了路由劫持或人員入侵。在上面的範例中，啟用智慧手錶的 DNSSEC 解析器檢測到重新定向，因為它無法驗證從敵人的名稱伺服器接收到的 DNS 記錄，例如，因為它們未簽章或簽章無效。解析器向智慧手錶返回錯誤，以防止將智慧手錶的測量結果傳輸到惡意服務。

(二) DNS 協議以雙重檢查 IoT 服務的真實性

還存在幾種基於 DNS 的安全協議，這些協議為 IoT 設備提供了其他方法，以在 DNS 解析後檢查從服務接收到的證書的真實性。與保護 DNS 消息的完整性，這對於避免 IoT 設備與可能影響用戶隱私和安全的惡意服務進行通信非常重要。

其中一項是基於 DNS 的命名實體身份驗證（DNS-based Authentication of Named Entities， DANE），是 DNSSEC 的應用程式，需要 DNSSEC 驗證才能起作用。它使 IoT 設備和閘道器能夠驗證它們收到的傳輸層安全性（TLS）證書，例如當它們通過 HTTPS 連接到遠程服務時，如果設備使用 HTTPS 連接到 s1.sp1.example.，則可以在

DNS 中查找 s1.sp1.example.的證書，並檢查通過 HTTPS 連接收到的證書是否為有效證書，以及綁定到 s1.sp1.example.。

(三) DNS 與 IoT 面臨的挑戰

DNS 與 IoT 的結合面臨了許多挑戰，而其中幾項與 DNSSEC 相關。

第一個挑戰是開發和維護一個開源 DNS 安全庫，使 DNSSEC 驗證、DANE 和 DoH/DoT 等功能在 IoT 設備上可用。該庫需要包括對常規根 KSK 翻轉的透明支援，例如，自動更改密鑰並通知其中 KSK IoT 設備當前使用的 DNS。這與傳統解析器相比可能更具挑戰性，部分原因是可能無法遠端更新 IoT 設備，而且許多 IoT 裝置缺少儲存金鑰材料所需的非易失性儲存。

該庫需要使用最流行的 IoT 作業系統(例如 OpenWRT 和 RIOT)和 CPU 架構，以及更有限的 IoT 裝置資源(例如，電池功率有限、CPU 電源或執行加密操作的能力)。它還需要提供一個 API，使 IoT 設備工程師能夠輕鬆地包含和使用庫。開發 DNS 安全庫的潛在起點可能是丹麥文，使 HTTPS DANE 可在 OpenWRT 上可用或 DNSSEC 觸發器，它為筆記型電腦和手機提供 DNSSEC 簽章驗證。

另一個挑戰是為 IoT 和 DNS 專業人員提供關於 IoT 和 DNS 之間互動的多語言培訓。培訓還將討論 IoT 安全措施(例如 DNS 的

安全功能和其他安全協定)以及計算開發和維護這些措施成本的指導原則。將包括增加對設備和網路安全的瞭解，例如 DNSSEC 的工作原理。物聯網和 DNS 共同發展迅速，因此培訓也需要不斷的更新。

第六節　SIP (Session Initiation Protocol)

一、SIP 介紹

對話啟動協定 (Session Initiation Protocol, SIP) 為 IETF (Internet Engineering Task Force) 所制定之進行對話管理的應用層通訊協定。SIP 的設計目標之一是在 IP 網路上提供類似公用交換電話網 (Public Switched Telephone Network, PSTN) 中信令處理的功能，如撥號、振鈴、回鈴音或者忙音等日常電話操作。 SIP 的特點如下：

1. 簡單且易於擴充： SIP 的通訊模式與 HTTP 雷同，採用純文字的請求 (request) 與回應 (response)，SIP 提供數種請求方法 (method) 以及回應狀態代碼 (status code)，並使用夾帶在標頭的標頭欄位 (header fields) 訊息以及通訊內容 (content)，來完成對話控制。SIP 的協定格式以標準字元集編碼的純文字表達，而非二進制封包格式。 這使得 SIP 的封包具有下列優點，首先是由於內容為肉眼可辨識之字串，因此容易進行偵錯。再者因為增加額外的擴充訊息不需要大幅更動原有的解析程式，因此擴充性較佳。
2. 良好的移動性支援：SIP 制定之初就將移動性的支援納入考量，這使得 SIP 無論在對話建立階段或是對話進行過程中都可以藉由轉送或是重新邀請 (re-invite) 的方式來維持對話

的暢通。

3. 建構於傳輸層之上的協定：SIP 在位於傳輸層之上的對話層運作，可以根據需求選擇適當的傳輸層協議，例如在封包較容易遺失的網路環境中使用 TCP 作為傳輸層協議以獲得穩定的連線，而在連線品質較好的環境中可考慮使用 UDP 降低傳輸延遲。

SIP 在應用時通常會搭配 SDP 進行對話描述並且使用 RTP 、RTPC 等多媒體傳輸協定在網際網路上進行實時的影像或音訊傳播，亦即所謂的 VoIP 或是視訊，且 SIP 並沒有限制僅能維護一對一對話，故多人視訊或語音會議同樣可以利用 SIP 進行對話管理。

(一) RFC 列表

1、 核心標準

- RFC 3261: SIP: Session Initiation Protocol, July 2002.
- RFC 3262: Reliability of Provisional Responses in SIP, July 2002.
- RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers, July 2002.
- RFC 3264: An Offer/Answer Model with SDP, July 2002.

- RFC 5954: Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261, August 2010.
- RFC 6665: SIP-Specific Event Notification, July 2012.

2、 訊息處理

- RFC 5621: Message Body Handling in the SIP, September 2009.
- RFC 5626: Managing Client-Initiated Connections in the SIP, October 2009.
- RFC 5630: The Use of the SIPS URI Scheme in the SIP, October 2009.
- RFC 8217: Clarifications for When to Use the name-addr Production in SIP Messages, August 2017.

3、 請求及回覆

- RFC 3331: The SIP UPDATE Method, October 2002.
- RFC 3428: SIP Extension for Instant Messaging, December 2002.
- RFC 3515: The Session Initiation Protocol (SIP) Refer Method, April 2003.

- RFC 3903: SIP Extension for Event State Publication, November 2004.
- RFC 6026: Correct Transaction Handling for 2xx Responses to Session Initiation Protocol (SIP) INVITE Requests, September 2010.
- RFC 6086: SIP INFO Method and Package Framework, January 2011.
- RFC 7647: Clarifications for the Use of REFER with RFC 6665, September 2015.
- RFC 8591: SIP-Based Messaging with S/MIME, April 2019.

4、 SDP

- RFC 3264: An Offer/Answer Model with SDP, July 2002.
- RFC 4566: SDP: Session Description Protocol, July 2006.

5、 IPv6 及 SIP

- RFC 6157: IPv6 Transition in the SIP, April 2011.
- RFC 7984: Locating SIP Servers in a Dual-Stack IP Network, September 2016.

6、 應用

- RFC 3665: SIP Basic Call Flow Examples, January 2004.
- RFC 3666: SIP PSTN Call Flows, January 2004.
- RFC 4240: Basic Network Media Services with SIP, December 2005.
- RFC 4353: A Framework for Conferencing with the SIP, February 2006.

7、 資訊安全

- RFC 3329: Security Mechanism Agreement for the SIP, January 2003.
- RFC 3853: S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP), July 2004.
- RFC 4916: Connected Identity in the SIP, June 2007.
- RFC 5393: Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies, December 2008.
- RFC 5922: Domain Certificates in the SIP, June 2010.
- RFC 8225: PASSporT: Personal Assertion Token, February 2018.

- RFC 8760: The SIP Digest Access Authentication Scheme, March 2020.

(二) RFC 重要歷程

SIP 最先由美國哥倫比亞大學的 Henning Schulzrinne 和 Mark Handley 於 1996 年所設計，並在 1999 年 3 月由 IETF 的 MMUSIC (Multipart Multimedia Session Control) 工作組制定正式標準成為 RFC2543。

1999 年 9 月 IETF 成立新的工作組 SIP (Session Initiation Protocol) 負責新版 SIP 的制定工作，該工作組於 2000 年 7 月釋出初版 draft-ietf-sip-rfc2543bis ，並於 2002 年 7 月發佈了 RFC3261，RFC3261 的發佈表示著 SIP 的基礎已經成熟。SIP 工作組隨後又發佈了擴充可靠臨時訊息回覆的 RFC 3262、闡明如何使用 DNS 進行 SIP URI 解析的 RFC 3263 及擴充事件請求及通知的 RFC 3265 (已被 RFC 6665 推翻)，充份展現了 SIP 易於擴展的特性。 SIP 工作組於 2009 年 5 月結案，後續維護及發展交由 SIPCORE (Session Initiation Protocol Core) 工作組進行。

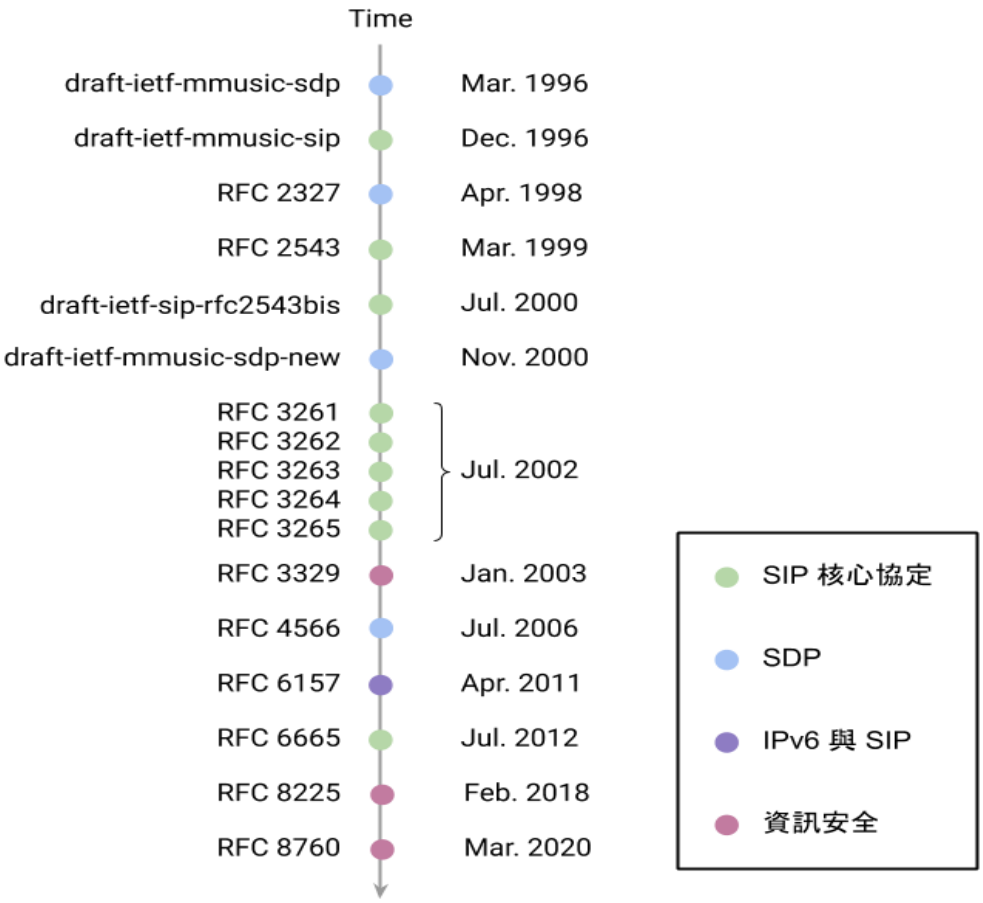


圖 119、SIP RFC 重要歷程

(三) 其他 VoIP 通訊協定

除了 SIP 以外尚有許多用來進行 VoIP 對話控制的通訊協定，如由國際電信聯盟電信標準化部門 (ITU Telecommunication Standardization Sector, ITU-T) 制定的 H.323 及由 IETF 所制定的多媒體閘道控制協定 (Media Gateway Control Protocol, MGCP) 等。 不同協定當初制定時的需求及目標都不盡相同，導致他們有各自的特色，以下將對 H.323 及 MGCP 進行簡單的介紹，並比較此二者和 SIP 的優劣。

1、 H.323

H.323 為 ITU-T 於 1996 年所制定的標準，原本目標是做為區域網路視訊會議的應用基礎，後來被用於網路電話。該標準的新版本陸續在進行，以因應新興的網路電話應用，最新規範版本於 2009 年 12 月提出。H.323 定義了如語音壓縮格式（G.711、G.729、G.723.1）、影像壓縮格式（H.261、H.263）、呼叫信令（H.225）、控制信令（H.245）、註冊與認證等(Registration ， Admission， Status； RAS）等一系列的規範，使得網路上遵循這些規範的終端設備得以順利進行溝通。 H.323 架構由 4 個元件所組成，包括終端設備（Terminal）、閘道器（Gateway）、閘道管理員（Gatekeeper）、多點控制單元（Multipoint Control Unit, MCU），這些元件使得 H.323 可進行一對一或一對多的通訊。

以 VoIP 的應用角度來看，H.323 的子協定相當多且複雜，且 H.232 被許多技術上的問題受限，使使其無法完全符合 VoIP 應用。因此 IETF(Internet Engineering Task Force) 分別在 1999 年 8 月提出 MGCP (Media Gateway Control Protocol) 協定與 1999 年 3 月提出 SIP (Session Initiation Protocol) ，以簡化 H.323 的複雜性並在語音傳遞的功能上提供較高的擴充性。

2、 Media Gateway Control Protocol (MGCP)

多媒體閘道控制協定 (Media Gateway Control Protocol, MGCP)，則是另一種不同於 H.323 和 SIP 的協定，不像 H.323 和 SIP 屬於 Peer-to-Peer Protocol，MGCP 是屬於 Master-slave Protocol，也就是完全由 MGCP Server 控制其 Gateway，MGCP 的網路拓樸如圖 120 所示。MGCP Call Agent 控制了 Signaling Gateway 及 Media Gateway，且 MGCP Call Agent 會接收用戶端的所有控制訊息，如拿起電話或是撥號，並決定這些訊息所代表的意義，以產生相對應的動作。相較於 H.323 或 SIP， MGCP Gateway 顯得簡單了許多，因其將所有的功能都由 Call Agent 控制，而相對而言 Call Agent 也比 H.323 SIP 的 Server 複雜了許多。

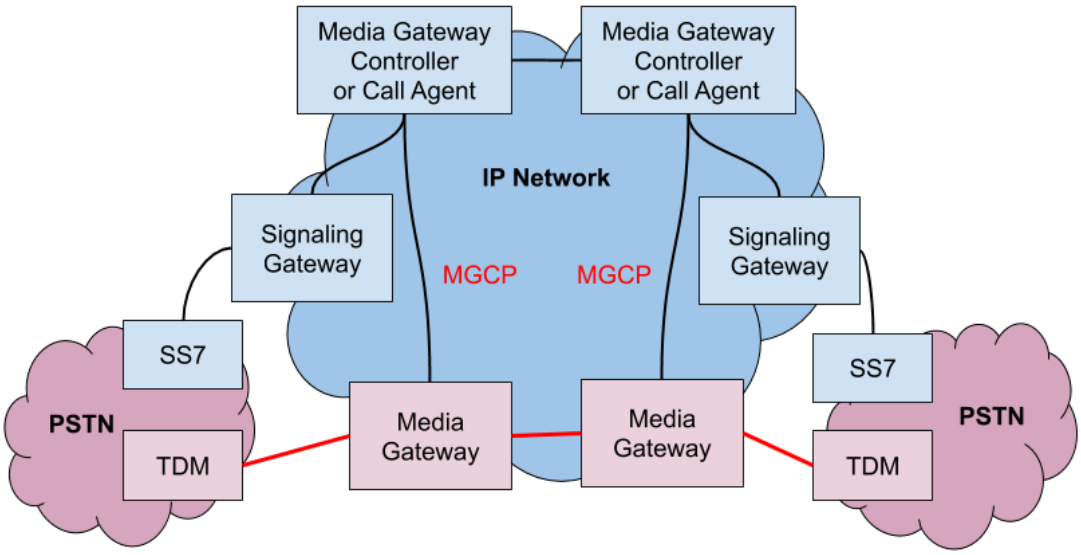


圖 120、MGCP 拓樸

3、 各通訊協定比較

上述各個通訊協定的比較如表 17 所示。

表 17、各對話控制通訊協定比較

項目	SIP	H.323	MGCP
通訊編碼	純文字 (ASCII)	二進位 (ASN.1 編碼)	純文字 (ASCII)
協定型態	Peer-to-Peer	Peer-to-Peer	Master-Slave
制定組織	IETF	ITU-T	IETF
用途	信令傳遞	信令傳遞	多媒體閘道控制

2000 年 11 月並 SIP 獲得 3GPP (Third Generation Partnership Project)、3GPP2 (Third Generation Partnership Project Number2) 等機構認可，成為未來 3G、4G 乃至於 5G 的標準並且為 IMS 體系結構的一個永久單元，這使得 H.323 和 MGCP 逐漸勢微。 IMS 系統設計的目標為讓使用者可以在以 SIP 為基底的環境中使用 VoIP 的服務，並且在使用者漫遊時系統會自動建立漫遊連線並繼續先前的通話。

二、協定架構

SIP 的基礎架構由 User Agent、Proxy Server、Redirect Server 及 Register Server 組成，其架構如圖 121 所示。 SIP 需要正常運作尚須其他通訊協定協同運作，如 SDP、MSRP、LDAP...等。

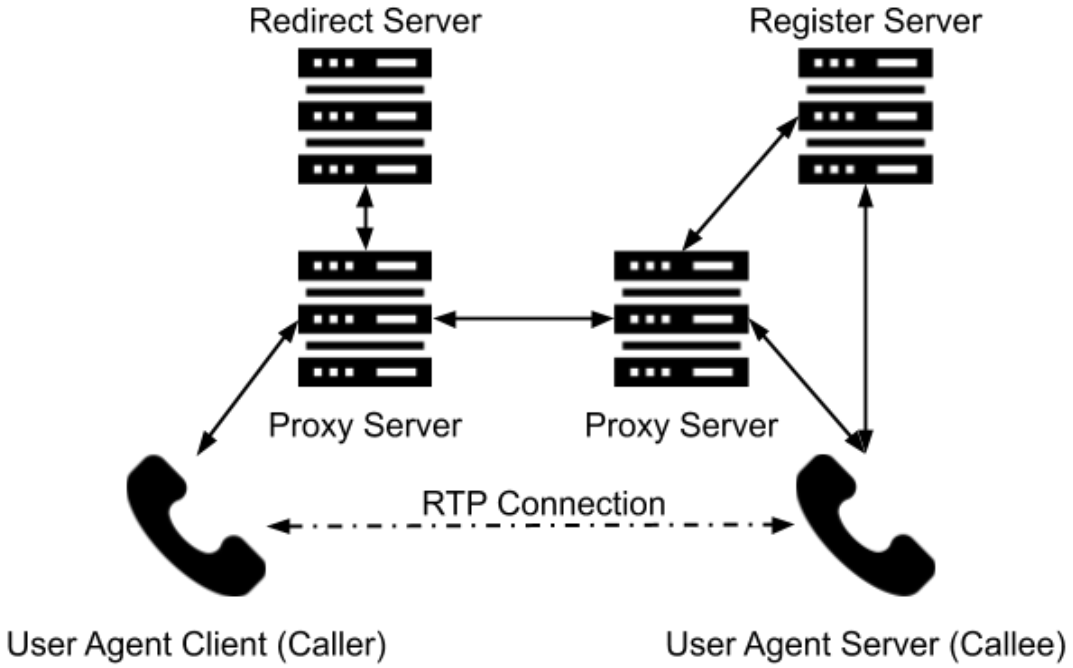


圖 121、SIP 的基礎架構

(一) 基礎元件

1、 User Agent

User Agent 負責為終端網路語音設備提供 SIP 的服務 ， 按照其角色可細分為負責提出請求的客戶端 User Agent Client(UAC) 和負責進行訊息回覆的伺服端 User Agent Server(UAS)。 每一個 SIP UA 都可以扮演 UAC 或 UAS 但同時只能選擇一個角色，呼叫者(Caller)的 UA 扮演 UAC 的角色，而被呼叫(Callee)的 UA 則扮演 UAS 的角色。

2、 Proxy Server

Proxy Server 是 SIP 運作時的核心，如同網路層的路由器般，

Proxy Server 會接受呼叫者的請求並將其轉送到另外一端，因此它同時會扮演 UAC 和 UAS 的角色。Proxy Server 同時提供一些如身份認證等功能供 UA 使用。

3、 Redirect Server

為了能在固定邏輯位址的情況下隨意變更實體位址，SIP 使用 Redirect Server 來將邏輯位址和實體位址分離，所謂邏輯地址即為 SIP URI， 每個使用者擁有一個固定不變的邏輯位址，而實體位址為 IP 位址等底層通訊協定的位址，實體位址可以隨意變動。 每當使用者移動時該使用者的 UA 必須負責向 SIP 網路中的其中一個 Redirect Server 註冊，因此其他人可以使用被呼叫者的邏輯位址詢問 Redirect Server 以獲得被呼叫者的實體位址，從而在固定邏輯位址的情況下隨意變更實體位址。 Redirect Server 同時可以用來實現如 Call Forward 等功能。 然而與 Proxy Server 不同，Redirect Server 不會轉送任何 SIP 訊息。

4、 Register Sever

Register Server 的目的為紀錄或更新使用者的邏輯位址以及使用者的目前狀態。當 User Agent 上線時，會先以 REGISTER 請求方法來更新目前 UA 的邏輯位址及狀態紀錄。若有呼叫者對目前的 UA 提出對話建立的請求時，SIP 網路內相關的其他元件就能透過 Register

Server 順利的找到被呼叫端。 UA 的註冊時都有一定的時效限制，若 UA 沒在相關紀錄過期前重新註冊的話相關的對話狀態就無法維護。Register Server 與 Redirect Server 的存在讓 SIP 具有支援移動性的能力。

(二) 相關協定

1、 Session Description Protocol (SDP)

SDP 為用來描述串流媒體對話初始化參數的通訊協定，被廣泛用於和 RTSP 以及 SIP 協同工作，此協定最初的時候是對話發布協定（Session Announcement Protocol, SAP）的一個元件。 SDP 於 1998 年 4 月由 IETF 推出第一版 RFC 2327，目前的最新版本為 RFC 4566，該版本更新了 ABNF 語法以及整合 IPv6 擴充。

2、 Message Session Relay Protocol (MSRP)

MSRP 是一基於 SIP 的即時訊息（Instant Messaging）協定，可以在 SIP 的對話中進行一對一或一對多的即時通訊、傳送檔案或圖片分享。

3、 Lightweight Directory Access Protocol (LDAP)

LDAP 是一個開放且中立的工業標準應用協定，通過 IP 協定提供存取控制和維護分散式資訊的目錄資訊。

目錄服務在開發內部網路和與網際網路程式共享用戶、系統、網

路、服務和應用的過程中占據了重要地位，例如目錄服務可能提供了組織的有序記錄集合，通常有層級結構，例如公司電子郵件目錄或包含了位址和電話號碼的電話簿。最新的 LDAP 由 IETF 的 RFC 4511 定義，使用了描述語言 ASN.1 來定義。

LDAP 在 SIP 協同運作中的用途主要是用來在內部網路註冊階段查詢使用者的密碼或是在建立對話階段查詢使用者的邏輯位置，可替換的技術還有 Name/Finger 及 DNS 等。

4、 Resource Reservation Protocol (RSVP)

RSVP 是一個通過網路進行資源預留的協定，是為實現綜合業務網而設計的，其具體定義於 RFC 2205。RSVP 要求接收者在連接建立之初進行資源預留。主機或者路由器可以使用 RSVP 滿足不同應用程式資料流所需的不同的服務品質(QoS)。 RSVP 定義應用程式如何進行資源預留並在預留的資源不用時如何進行預留資源的刪除， 同時也會使得路徑上每個節點都進行資源預留。

5、 Real-time Transport Protocol (RTP)

RTP 是一個建立在 UDP 協定上的多媒體傳輸協定，最新協定版本是 RFC 3550。RTP 協定詳細說明了在網際網路上傳遞音訊和視訊的標準封包格式。它一開始被設計為一個多播協定，但後來被用在許多單播應用中。RTP 也常常配合 H.323 或 SIP 用於視訊會議和一

鍵通（Push to Talk）系統，使它成為 IP 電話產業的技術基礎。 RTP 通常和 RTCP 伴隨使用，RTP 負責 Data Plane 而 RTCP 負責 Control Plane。

6、 Real-time Transport Control Protocol (RTCP)

RTCP 是 RTP 的一個姐妹協議，RTCP 和 RTP 一樣定義在 RFC 3550。RTCP 為 RTP 媒體串流提供信道外（out-of-band）控制。RTCP 本身並不傳輸數據，但和 RTP 一起協作將多媒體數據打包和發送。 RTCP 定期在多媒體串流對話參加者之間傳輸控制數據。RTCP 的主要功能是為 RTP 所提供的服務質量（Quality of Service）提供回饋。

RTCP 收集相關媒體連接的統計信息，例如：傳輸位元組數、傳輸分組數、丟失分組數、jitter 以及單向和雙向網絡延遲等等，網路應用程式即可利用 RTCP 的統計信息來控制傳輸的品質，比如網路頻寬高負載時限制訊息流量或改用壓縮比較小的編碼器。另外，RTCP 本身不提供數據加密或身份認證，若有相關需求可以使用 SRTCP 來達成。

7、 協定堆疊

上述各個與 SIP 協同運作的通訊協定之間的關係如圖 122 所示。協定主要可以分為 Data Plane 及 Control Plane，Data Plane 的主要

通訊協定為 RTP 及其控制協定 RTCP，此外為了加強安全性亦可以使用上述兩協定的安全版本 SRTC 及 SRTCP。Control Plane 則以 SIP 為主要通訊協定，搭配 SDP 及 MSRP 敘述該對話的詳細內容，使用 DNS 及 LDAP 查詢實用者的邏輯位置，並搭配 RSVP 進行網路資源的保留。此外，Control Plane 的安全性主要來自於 IP 層的 IPsec 及傳輸層的 TLS 安全協定。

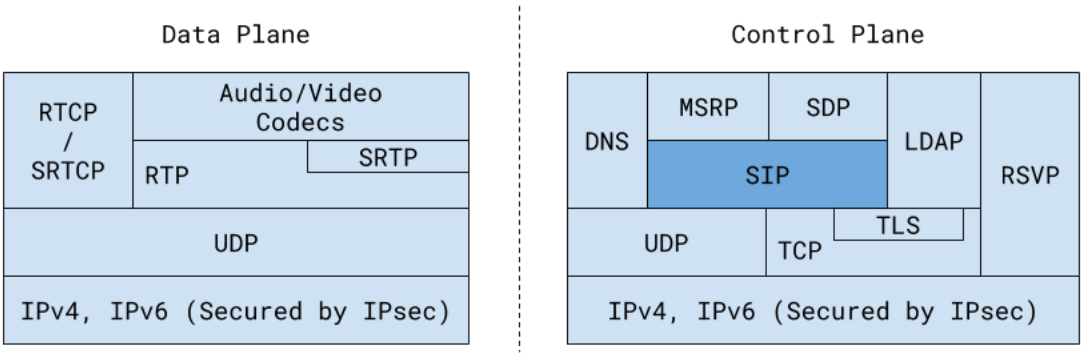


圖 122、SIP 相關的協定堆疊

三、通訊流程

SIP 的通訊協定內容和 HTTP 很類似，都是以純文字作為協定的內容，且都是一個請求對上一個回覆，由 UAC 發起請求並由 UAS 接受請求並回覆，以下將詳細介紹 SIP 的請求及回覆格式以及基礎的通訊流程。

(一) 請求格式

SIP 的請求主要有 REGISTER, INVITE, ACK, CANCEL, BYE, OPTION 六種，詳細敘述如下：

1. INVITE：邀請 UAS 加入對話。
2. ACK：當 UAC 發出 INVITE 請求和 UAS 建立對話且對方回傳最終請求時，UAC 必須利用 ACK 通知對方進行確認。
3. BYE：參與對話的雙方其中一方欲結束對話時所發送的請求。
4. CANCEL：取消之前所發出的 INVITE 請求。
5. REGISTERS：向 Register Server 註冊目前 UA 的相關資訊，以利其他 UA 尋找此 UA。
6. OPTIONS：用來詢問伺服器是否支援某些擴充功能。

(二) 回應格式

SIP 的回覆狀態碼和 HTTP 雷同，都是三個數字位數的狀態碼來表達回覆的各種狀態，詳細敘述如下：

1. 1XX—Informational Messages：資訊性消息。
2. 2XX—Successful Responses：請求成功。
3. 3XX—Redirection Responses：請 UAC 轉發新的連線請求到被 UAS 的其他位址。
4. 4XX—Request Failure Responses：請求失敗。
5. 5XX—Server Failure Responses：UAS 發生錯誤。

6. 6XX—Global Failure Responses：其他錯誤發生。

(三) 標頭欄位

本節將介紹 SIP 訊息中常見的標頭欄位，標頭欄位可依照其在 SIP 訊息中的作用分類為要求、回應、僅限要求、僅限回應及訊息主體欄位。 SIP 的標頭欄位主要定義在 RFC 3261，其擴充標頭由各相關 RFC 去定義。

SIP 的標頭欄位依循著和 HTTP 相同的標頭欄位規則，標頭欄位都以”欄位：值”的格式出現。其中欄位為區分大小寫的英文字串用以表示此欄位的名稱，而值同樣也是區分大小寫的英文字串，用以表此欄位的內容資訊。若沒有特別規範，則欄位及欄位間的順序通常沒有意義也不重要，標頭欄位的值可以為多行的字串，但是第二行以後的字串開頭至少須有一個以上的空白字元或是 tab，若為不合法的標頭欄位則可能會被 proxy server 忽略。許多 SIP 訊息中的標頭欄位有著一個小寫字母的欄位簡稱，其列表如表 18 所示，這些簡稱的目的是為了降低傳輸時的頻寬需求，以避免重複傳輸不必要的訊息。SIP 訊息的標頭欄位可以是端對端的欄位或是節點到節點的欄位，節點到節點的欄位為那些在傳輸過程中由 proxy server 新增或是更動的欄位，可能的欄位如 Via、Route、Record-Route...等。

SIP 透過 From 和 To 兩個欄位紀錄識別該對話的雙方位址 ，

此二欄位透 URI 來紀錄對話發起者及對話接收者的位址，欄位內除了 URI 外可能還會包含該使用者的顯示名稱或是標籤。顯示名稱並非 URI 的一部分也不具定位使用者的功效， 該數值僅僅用於顯示該使用者的別名而已。而標籤通常用來識別特定的呼叫，使用 ; 添加在原始的 URI 後方。

Via 為 SIP 紀錄請求一路上經過哪些 proxy server 及讓回覆沿著同樣路徑回來的標頭欄位，當 UAC 產生請求後會將自己的位址紀錄在 Via 欄位內並送交給 proxy server，每一個 proxy server 在轉送請求前會將自己的位址加入 Via 列表的最上面並將原始請求的 To、From 及 Call-ID 雜湊後的數值加在後方的 branch 標籤內。因此 Via 欄位會受到其擺放順序的影響造成不同的意思解讀，這和其他標頭欄位不相同。 當 proxy server 收到回覆後會檢查頂端的 Via 位址是否為自己的位址，若不是則該訊息可能被錯誤路由，因此應該將其丟棄，若頂端的 Via 位址為自身的位址，則 proxy server 會將頂端的 Via 欄位移除並轉送到下一個 Via 欄位所指定的主機。

Contact 欄位用以傳遞目前請求或回應的發起人 URI 為何，當 Contact 欄位出現在訊息中時，可以對該 URI 進行 cache 以加快後續可能的 SIP 訊息。Contact 欄位必須在 INVITE 請求及其對應的 200 OK 回覆中出現。若須將所有已註冊訊息從 register server 移除

的話 UA 可以對 register server 發送新的註冊要求並配合欄位 Contact: * 並配合 Expire: 0 的欄位。

Call-ID 為每一個 SIP 請求及回應都必須有的欄位，其作用為在兩個 user agent 之間識別唯一一個獨特的呼叫。除了註冊過程外，Call-ID 在整個呼叫的過程中必須保持一致且不能和其他呼叫重複，同一個 user agent 在註冊時所使用的 Call-ID 皆為同一個。 Call-ID 必須為密碼學安全的隨機識別碼以避免第三方攻擊者猜測 Call-ID 進而偽造不存在的請求或是回覆。

由於 SIP 的請求順序會影響所傳訊息的語意 ， 因此 SIP 在請求標頭使用命令順序 (Command Sequence, CSeq) 欄位來確保請求的順序。CSeq 欄位的數字每次請求都會往上加一，但是 ACK 和 CANCEL 時是沿用該請求所參照之 INVITE 請求的 CSeq 欄位數值。CSeq 被 UAS 用來區分是否為新請求，若 CSeq 欄位數值為新數值則為新請求，否則則是舊請求的重傳，另一方面 CSeq 被 UAC 用來配對所收到的回覆及所發出去的請求。不同 user agent 間的 CSeq 屬於不同的指令順序空間且互不影響。

表 18、SIP 標頭欄位的簡稱

原始欄位	欄位簡稱	原始欄位	欄位簡稱	原始欄位	欄位簡稱
Accept-Contact	a	Call-ID	i	Via	v
Reject-Contact	j	Refer-To	r	To	t
Content-Type	c	Referred-By	b	From	f
Content-Encoding	e	Subject	s	Contact	m
Content-Length	l	Allow-Event	u	Event	o

(四) 註冊

此範例展示 SIP 中 User Agent 如何向 Register Server 進行註冊。如圖 123 所示，在 F1 的請求中 Bob 送出自己的通訊錄給 Register Server，但是因為需要先使用 HTTP 摘要驗證進行身份確認，因此 Register Server 回覆 401 Unauthorized 並附加挑戰(challenge)訊息給 Bob。 Bob 收到訊息後再發送一次 REGISTER 請求並附加 HTTP 摘要認證，Register Server 確認 Bob 在其資料庫有資料後便發送 200 OK 回去給 Bob，完成一次註冊流程。此外，為了保障 HTTP 摘要認證的安全，所有通訊都必須在 TLS 之上進行以確保訊息不會被劫持甚至是偽造。

```
Bob                          SIP Server
 |                                |
 |          REGISTER F1           |
 |------------------------------->|
 |      401 Unauthorized F2       |
 |<-------------------------------|
 |          REGISTER F3           |
 |------------------------------->|
 |            200 OK F4           |
 |<-------------------------------|
 |                                |
```

圖 123、SIP 註冊流程

詳細訊息如下：

- F1 REGISTER Bob -> SIP Server

  REGISTER sips:ss2.biloxi.example.com SIP/2.0

  Via:SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashds7

  Max-Forwards: 70

  From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl

  To: Bob <sips:bob@biloxi.example.com>

  Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

  CSeq: 1 REGISTER

  Contact: <sips:bob@client.biloxi.example.com>

  Content-Length: 0

- F2 401 Unauthorized SIP Server -> Bob

  SIP/2.0 401 Unauthorized

  Via:SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashds7

  ;received=192.0.2.201

From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl

To: Bob <sips:bob@biloxi.example.com>;tag=1410948204

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 1 REGISTER

WWW-Authenticate: Digest realm="atlanta.example.com", qop="auth",

nonce="ea9c8e88df84f1cec4341ae6cbe5a359",

opaque="", stale=FALSE, algorithm=MD5

Content-Length: 0

- F3 REGISTER Bob -> SIP Server

REGISTER sips:ss2.biloxi.example.com SIP/2.0

Via:SIP/2.0/TLS

client.biloxi.example.com:5061;branch=z9hG4bKnashd92

Max-Forwards: 70

From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH

To: Bob <sips:bob@biloxi.example.com>

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 2 REGISTER

Contact: <sips:bob@client.biloxi.example.com>

Authorization: Digest username="bob", realm="atlanta.example.com"

nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",

uri="sips:ss2.biloxi.example.com",

response="dfe56131d1958046689d83306477ecc"

Content-Length: 0

- F4 200 OK SIP Server -> Bob

SIP/2.0 200 OK

Via:SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashd92

;received=192.0.2.201

From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH

To: Bob <sips:bob@biloxi.example.com>;tag=37GkEhwl6

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 2 REGISTER

Contact: <sips:bob@client.biloxi.example.com>;expires=3600

Content-Length: 0

(五) 對話建立/消滅

在下圖 124 中 Alice 透過兩個 Proxy Server 和 Bob 溝通，Proxy 1 被設定為 Alice 的預設 Proxy Server，因此在 F1 的 INVITE 請求的 Route 表頭欄位中含有 Proxy 1 的位址。但是因為 Alice 還沒有和 Proxy 1 進行身份確認，因此 Proxy 1 駁回 Alice 的請求。 Alice 順完成和 Proxy 1 的身份認證後 Proxy 1 便會開始幫 Alice 轉送請求到 Proxy 2，Proxy 2 再幫忙轉送到 Bob，其中兩個 Proxy 都會在轉送的封包表頭的 Record-Route 欄位中加入自身的位址以確保可以沿著原路徑送回去。整個對話的消滅僅須其中一方傳送 BYE 的請求並且對方回傳 200 OK 即可完成。

```
Alice           Proxy 1          Proxy 2            Bob
  |                |                |                |
  |   INVITE F1    |                |                |
  |--------------->|                |                |
  |     407 F2     |                |                |
  |<---------------|                |                |
  |     ACK F3     |                |                |
  |--------------->|                |                |
  |   INVITE F4    |                |                |
  |--------------->|   INVITE F5    |                |
  |     100  F6    |--------------->|   INVITE F7    |
  |<---------------|     100  F8    |--------------->|
  |                |<---------------|                |
  |                |                |     180 F9     |
  |                |    180 F10     |<---------------|
  |     180 F11    |<---------------|                |
  |<---------------|                |     200 F12    |
  |                |    200 F13     |<---------------|
  |     200 F14    |<---------------|                |
  |<---------------|                |                |
  |     ACK F15    |                |                |
  |--------------->|    ACK F16     |                |
  |                |--------------->|     ACK F17    |
  |                |                |--------------->|
  |                Both Way RTP Media                |
  |<==============================================>|
  |                |                |     BYE F18    |
  |                |    BYE F19     |<---------------|
  |     BYE F20    |<---------------|                |
  |<---------------|                |                |
  |     200 F21    |                |                |
  |--------------->|     200 F22    |                |
  |                |--------------->|     200 F23    |
  |                |                |--------------->|
  |                |                |                |
```

圖 124、SIP 對話建立及消滅流程

詳細訊息：

- F1 INVITE Alice -> Proxy 1

  INVITE sip:bob@biloxi.example.com SIP/2.0

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43

  Max-Forwards: 70

  Route: <sip:ss1.atlanta.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>

  Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 1 INVITE

Contact: <sip:alice@client.atlanta.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 151

v=0

o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F2 407 Proxy Authorization Required Proxy 1 -> Alice

SIP/2.0 407 Proxy Authorization Required

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43

;received=192.0.2.101

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=3fla112sf

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 1 INVITE

Proxy-Authenticate: Digest realm="atlanta.example.com", qop="auth",

nonce="f84f1cec41e6cbe5aea9c8e88d359",

opaque="", stale=FALSE, algorithm=MD5

Content-Length: 0

- F3 ACK Alice -> Proxy 1

ACK sip:bob@biloxi.example.com SIP/2.0

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43

Max-Forwards: 70

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=3flal12sf

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 1 ACK

Content-Length: 0

- F4 INVITE Alice -> Proxy 1

  INVITE sip:bob@biloxi.example.com SIP/2.0

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

  Max-Forwards: 70

  Route: <sip:ss1.atlanta.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 2 INVITE

  Contact: <sip:alice@client.atlanta.example.com;transport=tcp>

  Proxy-Authorization: Digest username="alice",

  realm="atlanta.example.com",

  nonce="wf84f1ceczx41ae6cbe5aea9c8e88d359", opaque="",

  uri="sip:bob@biloxi.example.com",

  response="42ce3cef44b22f50c6a6071bc8"

  Content-Type: application/sdp

  Content-Length: 151

v=0

o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F5 INVITE Proxy 1 -> Proxy 2

INVITE sip:bob@biloxi.example.com SIP/2.0

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

Max-Forwards: 69

Record-Route: <sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:alice@client.atlanta.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 151

v=0

o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F6 100 Trying Proxy 1 -> Alice

SIP/2.0 100 Trying

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Content-Length: 0

- F7 INVITE Proxy 2 -> Bob

INVITE sip:bob@client.biloxi.example.com SIP/2.0

Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

Via:SIP/2.0/TCP ss1.atlanta.exa

mple.com:5060;branch=z9hG4bK2d4790.1

;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

Max-Forwards: 68

Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:alice@client.atlanta.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 151

v=0

o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F8 100 Trying Proxy 2 -> Proxy 1

SIP/2.0 100 Trying

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Content-Length: 0

- F9 180 Ringing Bob -> Proxy 2

SIP/2.0 180 Ringing

Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

;received=192.0.2.222

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

CSeq: 2 INVITE

Content-Length: 0

- F10 180 Ringing Proxy 2 -> Proxy 1

SIP/2.0 180 Ringing

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 384827629822018851 1@atlanta.example.com

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

CSeq: 2 INVITE

Content-Length: 0

- F11 180 Ringing Proxy 1 -> Alice

  SIP/2.0 180 Ringing

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

  ;received=192.0.2.101

  Record-Route: <sip:ss2.biloxi.example.com;lr>,

  <sip:ss1.atlanta.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>;tag=314159

  Call-ID: 384827629822018851 1@atlanta.example.com

  Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

  CSeq: 2 INVITE

  Content-Length: 0

- F12 200 OK Bob -> Proxy 2

  SIP/2.0 200 OK

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  ;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 147

v=0

o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com

s=-

c=IN IP4 192.0.2.201

t=0 0

m=audio 3456 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F13 200 OK Proxy 2 -> Proxy 1

SIP/2.0 200 OK

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 147

v=0

o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com

s=-

c=IN IP4 192.0.2.201

t=0 0

m=audio 3456 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F14 200 OK Proxy 1 -> Alice

SIP/2.0 200 OK

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 147

v=0

o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com

s=-

c=IN IP4 192.0.2.201

t=0 0

m=audio 3456 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F15 ACK Alice -> Proxy 1

  ACK sip:bob@client.biloxi.example.com SIP/2.0

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b76

  Max-Forwards: 70

  Route: <sip:ss1.atlanta.example.com;lr>,

  <sip:ss2.biloxi.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>;tag=314159

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 2 ACK

  Content-Length: 0

- F16 ACK Proxy 1 -> Proxy 2

ACK sip:bob@client.biloxi.example.com SIP/2.0

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b76

;received=192.0.2.101

Max-Forwards: 69

Route: <sip:ss2.biloxi.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 384827629822018851 1@atlanta.example.com

CSeq: 2 ACK

Content-Length: 0

- F17 ACK Proxy 2 -> Bob

ACK sip:bob@client.biloxi.example.com SIP/2.0

Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b76

;received=192.0.2.101

Max-Forwards: 68

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 384827629822018851 1@atlanta.example.com

CSeq: 2 ACK

Content-Length: 0

/* 開始通話，RTP 串流建立 */

/* … */
/* Bob 掛 Alice 電話 */

- F18 BYE Bob -> Proxy 2

  BYE sip:alice@client.atlanta.example.com SIP/2.0

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  Max-Forwards: 70

  Route: <sip:ss2.biloxi.example.com;lr>,

  <sip:ss1.atlanta.example.com;lr>

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F19 BYE Proxy 2 -> Proxy 1

  BYE sip:alice@client.atlanta.example.com SIP/2.0

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.201

  Max-Forwards: 69

  Route: <sip:ss1.atlanta.example.com;lr>

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F20 BYE Proxy 1 -> Alice

  BYE sip:alice@client.atlanta.example.com SIP/2.0

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.201

  Max-Forwards: 68

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F21 200 OK Alice -> Proxy 1

  SIP/2.0 200 OK

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  ;received=192.0.2.111

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.201

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F22 200 OK Proxy 1 -> Proxy 2

  SIP/2.0 200 OK

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.101

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F23 200 OK Proxy 2 -> Bob

  SIP/2.0 200 OK

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.201

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

(六) 重導向

在圖 125 中 Alice 透過 Redirect Server 及 Proxy 3 和 Bob 溝通。首先 Alice 會先向 Redirect Server 傳送 INVITE 請求，由於 Bob 的邏輯位址或實體位置已經變更，因此 Redirect Server 回傳

302 Move Temporarily 並附加 Bob 的新位址。然後 Alice 再根據這個新位址透過 Proxy 3 對 Bob 發起 INVITE 請求。

```
Alice        Redirect Server     Proxy 3             Bob
  |                 |                |                 |
  |   INVITE F1     |                |                 |
  |---------------->|                |                 |
  |     302 F2      |                |                 |
  |<----------------|                |                 |
  |     ACK F3      |                |                 |
  |---------------->|                |                 |
  |     INVITE F4                    |                 |
  |--------------------------------->|    INVITE F5    |
  |             100  F6              |---------------->|
  |<---------------------------------|      180 F7     |
  |             180 F8               |<----------------|
  |<---------------------------------|                 |
  |                                  |     200 F9      |
  |             200 F10              |<----------------|
  |<---------------------------------|                 |
  |             ACK F11              |                 |
  |--------------------------------->|     ACK F12     |
  |                                  |---------------->|
  |                Both Way RTP Media                  |
  |<================================================>|
  |                                  |     BYE F13     |
  |             BYE F14              |<----------------|
  |<---------------------------------|                 |
  |             200 F15              |                 |
  |--------------------------------->|     200 F16     |
  |                                  |---------------->|
  |                                  |                 |
```

圖 125、SIP 重導向的流程

詳細訊息：

- F1 INVITE Alice -> Redirect Server
  INVITE sip:bob@biloxi.example.com SIP/2.0
  Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bKbf9f44
  Max-Forwards: 70
  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
  To: Bob <sip:bob@biloxi.example.com>
  Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
  CSeq: 1 INVITE
  Contact: <sip:alice@client.atlanta.example.com>
  Content-Length: 0

- F2 302 Moved Temporarily Redirect Proxy -> Alice

SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bKbf9f44
;received=192.0.2.101
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>;tag=53fHlqlQ2
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:bob@chicago.example.com;transport=tcp>
Content-Length: 0

- F3 ACK Alice -> Redirect Server
  ACK sip:bob@biloxi.example.com SIP/2.0
  Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bKbf9f44
  Max-Forwards: 70
  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
  To: Bob <sip:bob@biloxi.example.com>;tag=53fHlqlQ2
  Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
  CSeq: 1 ACK
  Content-Length: 0

- F4 INVITE Alice -> Proxy 3
  INVITE sip:bob@chicago.example.com SIP/2.0
  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
  Max-Forwards: 70
  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
  To: Bob <sip:bob@biloxi.example.com>
  Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
  CSeq: 2 INVITE
  Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
  Content-Length: 0

以下訊息同上一節，故省略

(七) 重新邀請

圖 126 說明了 SIP 重新邀請的流程，重新邀請用於對話建立後某一方的 IP 位址改變時維持對話使用。在此範例中 Bob 在對話建

立後改變了 IP，因此須重新發送 INVITE 請求給 Alice，請求中包含 Bob 的新通訊錄以及新的 SDP 資訊。

```
Alice                 Proxy 2                 Bob
   |   F1 INVITE         |                     |
   |------------------->|      F2 INVITE      |
   |   F3 100 Trying     |------------------->|
   |<-------------------|   F4 180 Ringing    |
   |   F5 180 Ringing    |<-------------------|
   |<-------------------|                     |
   |                     |    F6 200 OK        |
   |    F7 200 OK        |<-------------------|
   |<-------------------|                     |
   |                  F8  ACK                  |
   |---------------------------------------->|
   |      Both Way RTP Media Established      |
   |<=======================================>|
   |                                          |
   |           Bob changes IP address         |
   |                                          |
   |                  F9 INVITE               |
   |<----------------------------------------|
   |                 F10 200 OK               |
   |---------------------------------------->|
   |                  F11  ACK                |
   |<----------------------------------------|
   |         New RTP Media Stream             |
   |<=======================================>|
   |                  F12 BYE                 |
   |---------------------------------------->|
   |                F13 200 OK                |
   |<----------------------------------------|
   |                                          |
```

圖 126、SIP 的重新邀請流程

詳細訊息：

/* F1~F8 同前面章節內容，故省略。 */

/* Bob 和 Alice 已經建立對話，但 Bobe 在過程中改變了 IP 位址。 */

- F9 INVITE Bob -> Alice

  INVITE sip:alice@client.atlanta.example.com SIP/2.0

  Via: SIP/2.0/UDP client.chicago.example.com:5060;branch=z9hG4bKlkld5l

  Max-Forwards: 70

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com

  CSeq: 14 INVITE

  Contact: <sip:bob@client.chicago.example.com>

Content-Type: application/sdp
Content-Length: 149

v=0
o=bob 2890844527 2890844528 IN IP4 client.chicago.example.com
s=-
c=IN IP4 192.0.2.100
t=0 0
m=audio 47172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

- F10 200 OK Alice -> Bob
  SIP/2.0 200 OK
  Via: SIP/2.0/UDP client.chicago.example.com:5060;branch=z9hG4bKlkld5l
  ;received=192.0.2.100
  Max-Forwards: 70
  From: Bob <sip:bob@biloxi.example.com>;tag=314159
  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
  Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
  CSeq: 14 INVITE
  Contact: <sip:alice@client.atlanta.example.com>
  Content-Type: application/sdp
  Content-Length: 150

  v=0
  o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
  s=-
  c=IN IP4 192.0.2.101
  t=0 0
  m=audio 1000 RTP/AVP 0
  a=rtpmap:0 PCMU/8000

- F11 ACK Bob -> Alice
  ACK sip:alice@client.atlanta.example.com SIP/2.0
  Via: SIP/2.0/UDP client.chicago.example.com:5060;branch=z9hG4bKlkldcc
  Max-Forwards: 70
  From: Bob <sip:bob@biloxi.example.com>;tag=314159
  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

```
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 14 ACK
Content-Length: 0

/* 新 RTP 串流建立 */
/* 後面訊息同前面章節，故省略。 */
```

四、SIP 的應用

(一) SIP for Telephones (SIP-T)

VoIP 網路電話與現有公用交換電話網路(Public Switched Telephone Network, PSTN) 的互通性為推廣 VoIP 服務時一個重要的議題。作為 VoIP 裡主要信令通訊協定的 SIP 必須進行相對應的擴展，以整合 SIP 的信令網路與現有的信令網路。得益於 SIP 方便擴展的特性，定義於 RFC 3372 的 SIP-T (SIP for Telephone) 便應運而生。SIP-T 為 sipping 小組所制定的通訊協定，該小組和制定 SIP 協定為同一組人，因此對 SIP 的了解最深入，理當由他們來制定，且若在制定過程中發現 SIP 的協定有不足的地方時，該工作組還可以去修改並補足原來 SIP 協定不足的部分。

SIP-T 的主要目的為提供 PSTN 與 IP 網路之間訊號相互轉換與互相運作的一套機制，使得從 PSTN 或是從 IP 網路都能與對方連接或是 PSTN 可以透過 IP 網路互相連接。在 SIP-T 的協定中定義了三種連接的方式，分別為 SIP Bridging、PSTN origination，IP termination 及 IP origination，PSTN termination，其敘述分別如下:

1、 SIP Bridging：由 PSTN 的使用者發起，透過多媒體網關控制器(Media Gateway Controller, MGC)接入以 SIP 做信令協定的 IP 網路，再透過 MGC 轉到另一個 PSTN 網路接收，其架構及通訊流程如圖 127 及圖 128 所示。

```
                    ********************
                 ***                    ***
                *                        *
               *    -------               *
              *     |proxy|                *
             *      -------                 *
           |---|                           |---|
          /|MGC|       VoIP Network         |MGC|\
         /  ---                             ---  \
        /     *                             *     \
       /       *           -------           *      \
      /          *         |proxy|          *        \
   --------        *        -------         *     ---------
   | PSTN |         ***                   ***      | PSTN  |
   --------           ********************        ---------
```

圖 127、SIP Bridging 架構

```
PSTN             MGC#1   Proxy    MGC#2          PSTN
|-------IAM------>|       |        |               |
|                 |-----INVITE---->|               |
|                 |       |        |-----IAM----->|
|                 |<--100 TRYING---|               |
|                 |       |        |<----ACM------|
|                 |<-----18x-------|               |
|<------ACM-------|       |        |               |
|                 |       |        |<----ANM------|
|                 |<----200 OK-----|               |
|<------ANM-------|       |        |               |
|                 |------ACK------>|               |
|===================Conversation=================|
|-------REL------>|       |        |               |
|<------RLC-------|------BYE------>|               |
|                 |       |        |-----REL----->|
|                 |<----200 OK-----|               |
|                 |       |        |<----RLC------|
|                 |       |        |               |
```

圖 128、SIP Bridging 通訊流程

1、PSTN origination，IP termination: 由 PSTN 的使用者發起，透過 MGC 轉入 IP 網路後透過 SIP 的 proxy server 轉交 SIP 使用者接收，其架構及通訊流程如圖 129 及圖 130 所示。

```
                    ********************
                  ***                  ***
                 *                      *
                *                        *
               *                          *
              *                            *
           |----|                        |-----|
          /|MGC |       VoIP Network     |proxy|\
         /  ----                          -----  \
        /       *                           *     \
       /         *                          *       \
      /           *                         *         \
--------          *                       *     -------------
| PSTN |           **                    **      | SIP phone |
--------            ********************        -------------
```

圖 129、PSTN origination 架構

```
PSTN            MGC                   Proxy              SIP phone
  |----IAM----->|                     |                    |
  |             |--------INVITE------>|                    |
  |             |                     |-------INVITE------->|
  |             |<------100 TRYING----|                    |
  |             |                     |<-------18x----------|
  |             |<---------18x--------|                    |
  |<----ACM-----|                     |                    |
  |             |                     |<-------200 OK-------|
  |             |<-------200 OK-------|                    |
  |<----ANM-----|                     |                    |
  |             |---------ACK-------->|                    |
  |             |                     |---------ACK-------->|
  |=====================Conversation=======================|
  |-----REL---->|                     |                    |
  |             |----------BYE------->|                    |
  |<----RLC-----|                     |---------BYE-------->|
  |             |                     |<-------200 OK-------|
  |             |<-------200 OK-------|                    |
  |             |                     |                    |
```

圖 130、PSTN origination 通訊流程

2、 IP origination，PSTN termination: 由 IP 網路的 SIP 使用者發起，並透過連接於 IP 網路的 MGC 轉入 PSTN 網路並由 PSTN 的使用者接收，其架構及通訊流程如圖 131 及圖 132 所示。

```
                    ********************
                  ***                  ***
                 *                       *
                *                         *
               *                           *
              *                             *
          |-----|                         |----|
         /|proxy|       VoIP Network      |MGC |\
        /  -----                          ----  \
       /       *                           *     \
      /         *                         *       \
     /           *                       *         \
 ------------     *                     *     ---------
 |SIP phone |      **                  **      | PSTN  |
 ------------        ********************       ---------
```

圖 131、IP origination 架構

```
   SIP phone         Proxy                    MGC          PSTN
|-----INVITE----->|                      |             |
|                 |--------INVITE-------->|             |
|<---100 TRYING---|                      |-----IAM---->|
|                 |<------100 TRYING------|             |
|                 |                      |<----ACM-----|
|                 |<---------18x----------|             |
|<------18x-------|                      |             |
|                 |                      |<----ANM-----|
|                 |<--------200 OK--------|             |
|<-----200 OK-----|                      |             |
|-------ACK------>|                      |             |
|                 |----------ACK--------->|             |
|=======================Conversation==================|
|-------BYE------>|                      |             |
|                 |----------BYE--------->|             |
|                 |                      |-----REL---->|
|                 |<--------200 OK--------|             |
|<-----200 OK-----|                      |<----RLC-----|
```

圖 132、IP origination 通訊流程

上述的三種呼叫模型最主要的整合工作為 SIP 和 ISUP(ISDN

User Part)訊息的轉換及傳送。ISUP 為 PSTN 網路上負責通話控制的信令協定，其地位猶如 SIP 之於 IP 網路。除了 ISUP，SIP-T 也支援在 PBX(private branch exchanges)裡所使用的一種類比式的信令控制協定 QSIG。SIP-T 提出封裝(Encapsulating)與對應(Mapping)兩種方法以增加對 PSTN 各方面的應用支援及與 ISUP 的互通性，其分別定義於 RFC3204 與 RFC3398。

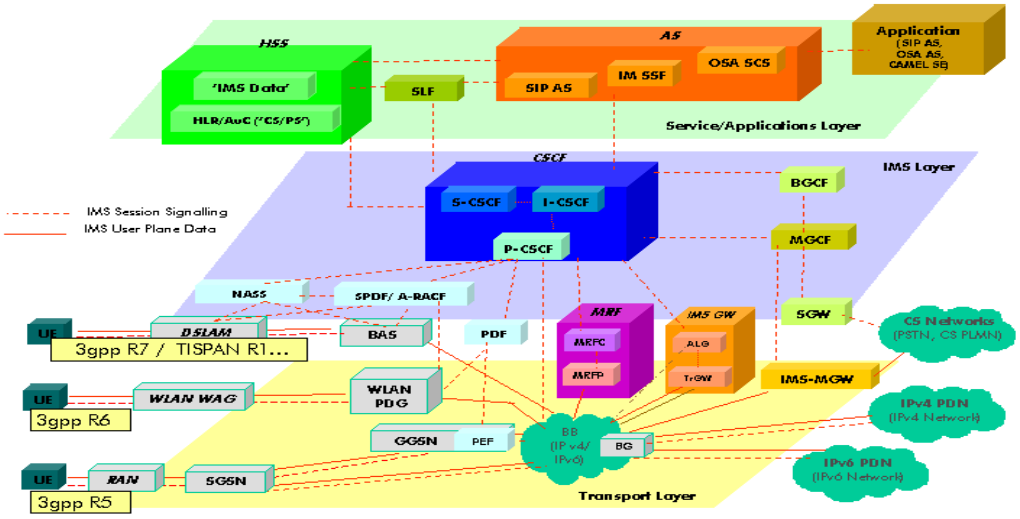
封裝即為在 ISUP 的訊息進入 MGC 時，將其完整的封裝起來，以確保所有與 ISUP 服務相關的資訊毫無遺漏的被複製進 SIP 網路。因為這些資訊需要以 ASN.1 的二進位碼方式儲存，而且其長度不固定，故 SIP-T 使用常見於 SMTP 與 HTTP 的 Multipurpose Internet Mail Extensions(MIME) Multipart 方式進行封裝。以 MIME 的方式進行編碼就可以確保二進位碼的資料可以在以純文字為主的 SIP 網路中傳送，而使用 Multipart 的方式則可以進行不定長度的資料封裝。

對應即為將 ISUP 所提供的一些服務定義出相對應的 SIP 訊息，以便讓使用 SIP 的 IP 網路可以支援使用對應的 SIP 功能來完成一些 PSTN 常用的呼叫服務，如無人回應、自動回覆、自動轉接及呼叫取消等功能。至於那些在 SIP 網路中找不到對應功能，只在 PSTN 網路有效的服務，則只能藉著前述的封裝技巧將訊息傳送到另一端的 PSTN 網路進行處理。

(二) 3GPP IMS

傳統的行動通訊使用電路交換來進行語音通訊而非 IP 網路的封包交換，IP 多媒體子統(IP Multimedia Subsystem, IMS) 即為 3GPP 這個組織所制定的一個以 SIP 為基礎來進行信令與對話管理的功能並建構在 IP 網路中的子系統。

IMS 的基本架構在 3GPP Relese5 之後便大致確立了，相關的需求及技術細節被可以在 3GPP TS 22.228 找到。IMS 裡定義了在 IP 網路裡進行及時語音多媒體傳輸服務會使用到的單元以及通訊協定，其中 SIP 被用來執行對話控制和對話管理的即時服務。在 IMS 架構中最重要的單元就是通話狀態控制功能 (Call State Control Function, CSCF)，按照不同任務，這些 CSCF 又可區分為三種： 負責處理 SIP 註冊的服務通話狀態控制功能 (Serving CSCF, S-CSCF)、作為 SIP proxy server 的代理通話狀態控制功能 (Proxy CSCF, P-CSCF) 及負責協助 S-CSCF 進行註冊的詢問通話狀態控制功能 (Interrogating CSCF, I-CSCF)。



資料來源：維基百科

圖 133、IMS 架構圖

(三) VoLTE / Vo5G

VoLTE（Voice over Long-Term Evolution）及 Vo5G 是一個手機和資料終端導向的高速無線通訊標準。它基於前面章節所提到的 IP 多媒體子系統（IMS），在 LTE 上使用為控制層面（Control plane）和語音服務的媒體層面（Media plane）特製的設定檔。

其目的為將語音服務作為資料流並在 LTE 資料承載網路中傳輸，而不再需維護和依賴傳統的電路交換語音網路。因為 VoLTE 封包標頭比未最佳化的 VoIP/LTE 還要更小更有效的利用頻寬，這使得 VoLTE 的語音和資料容量超過 3G UMTS 三倍以上，超過 2G GSM 六倍以上。

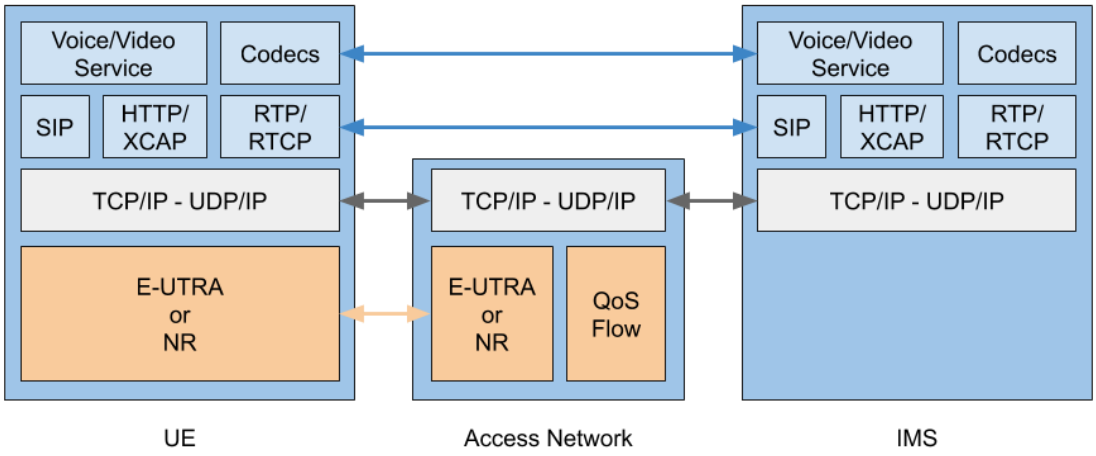


圖 134、VoLTE / Vo5G 架構

五、相關議題

(一) NAT 路由器

由於 SIP 在呼叫過程中需要 User Agent Server 的確切位址，因此位於 NAT 後方的 User Agent Server 若沒有經過特殊設定將無法接受來自 User Agent Client 的請求，可以靠著 SIP 搭配 STUN 來解決此問題。

STUN（Session Traversal Utilities for NAT）是一種網路協定，該協定在 RFC 5389 中被定義。STUN 允許位於 NAT（或多重 NAT）後的客戶端找出自己的公網位址，查出自己位於哪種類型的 NAT 之後以及 NAT 為某一個本地連接埠所繫結的網際網路端連接埠。 這些資訊被用來在兩個同時處於 NAT 路由器之後的主機之間建立 UDP 通訊。

一旦客戶端得知了網際網路端的 UDP 連接埠，通信便可開始。

如果 NAT 是完全圓錐型 (Full-cone) 的，那麼雙方中的任何一方都可以發起通信。如果 NAT 是受限圓錐型 (Restricted cone) 或埠受限圓錐型 (Restricted port)，雙方必須一起開始傳輸。

STUN 是一個 Client-Server 協定。一個 VoIP 電話或軟體包可能會包括一個 STUN 客戶端。這個客戶端會向 STUN 伺服器傳送請求，之後伺服器就會向 STUN 客戶端報告 NAT 路由器的公開 IP 位址以及 NAT 對外的對應連接阜。以上的回應同時還使得 STUN 客戶端能夠確定正在使用的 NAT 類型，因為不同 NAT 類型處理傳入 UDP 分組的方式不同。

(二) 資訊安全

相較於傳統的 Circuit-Switch Based Network，基於 IP 的 SIP 對話資訊容易從軟體方面透過封包捕捉來截獲，若對話資訊沒有進行加密的話則在對話資訊中的如電話號碼等敏感資料容易洩漏，因此 RFC 3329 中建議使用 TLS 或是 IPsec 等現存的安全機制來保障 SIP 的資料傳輸安全。

原始的 SIP 沒有進行傳送者身份的認證及資料完整性的確認，這導致駭客可以輕易的偽造或是變更 SIP 的訊息，可能會導致假冒身份傳送訊息等問題。因此同樣在 RFC 3329 中建議使用 HTTP Digest 進行使用者的身份認證及資料完整性的確認。不過考量到

RFC 2617 HTTP Digest 中所規範的 MD5 雜湊函數現在已經不安全，因此 SIPCORE 工作組於 2020 年三月提出了基於 SHA-256/512 的 RFC 8760 來替代 SIP 中的身份認證及資料完整性確認。

SIP 的第三個安全性問題是部份電信營運商的 IMS 沒有檢查傳送者電話號碼是否屬實，這造成了可以對來源電話號進行偽造 ，進而形成電話詐騙或是偽造公司電話等問題。 因此 IETF 的 STIR 工作組於 2018 年 2 月的 RFC 8225 中提出了一種基於密碼學且可以驗證 SIP 來源身份的 Token — PASSporT。

六、IETF 活躍中的 Working Groups

(一) Session Initiation Protocol Core (SIPCORE)

SIPCore 工作組的目的是維護和繼續 SIP 協定的開發，亦即目前已將 SIP 協定定義為標準的 RFC 3261、3262、3263、3264 和 6665。

SIPCore 工作組將專注於更新或替換上面提到的核心 SIP 規範以及與小型獨立 SIP 協議擴展有關的規範。 RFC5727 “Change Process for the Session Initiation Protocol (SIP)” 中記錄了新 SIP 擴展的過程和要求。

在整個工作中，該小組將努力維護 SIP 定義的基本模型和體系結構。特別是：

1、 盡可能以端到端的方式提供服務和功能。

2、 重用現有的 Internet 協議和體系結構以及與其他 Internet 應用整合。

3、 Standards-track 擴展和新功能必須通用，而不僅僅適用於特定的對話類型。

4、 應該使用較簡單的解決方案，而不是較複雜的解決方案。

(二) Secure Telephone Identity Revisited (STIR)

STIR 工作組將提出基於 Internet 的機制，該機制允許驗證呼叫機構使用特定電話號碼進行傳入呼叫的授權。 與電子郵件一樣，未經身份驗證的 SIP 請求的來源身份也不會得到驗證，使得未經授權使用該來源身份成為欺騙性和強制性活動的一部分。

由於提供不正確的來源電話號碼變得相當容易，因此在過去十年中出現了越來越多的問題，例如自動呼叫（大量未經請求的商業通信），誘捕（語音郵件駭客和冒充銀行） 以及打擊 （使呼叫者冒充緊急服務人員以刺激不必要的大規模執法部署）等。 另外，使用不正確的來源電話號碼會助長電匯欺詐，或導致以溢價率返回電話。

STIR 工作組的工作僅限於開發電話號碼解決方案。 使用 user @ domain 或其他名稱形式將授權機制擴展為身份超出範圍。此小組已經於 RFC 8225 提出一種用於個人身份驗證的密碼學 Token，名為 PASSporT。

(三) Automatic SIP trunking And Peering (ASAP)

在過去的幾年中，基於 SIP 的基礎建設在企業和服務提供商通信網絡中的部署已逐漸增加。因此，企業和服務提供商網路之間的直接 IP 對等取代了這些網絡之間的傳統連線建立方法，例如類比線路和基於時分複用（TDM）的數位電路。

目前發布的標準為實現直接 IP 對等提供了堅實的基礎。但是考慮到這些標準的數量眾多，通常不清楚企業網絡管理員應配置哪些行為子集、基準協議的擴展和操作原理，以確保與 SIP 服務提供商網絡的 IP 對等成功。 語境的缺乏經常導致企業和服務提供商 SIP 網路之間的互操作性問題。 導致企業網路管理員花費大量時間單獨或與企業設備製造商和服務提供商支持團隊一起對這些互操作性問題進行故障排除。 因此增加了在企業和服務提供商網路之間部署 SIP 中繼所花費的時間。

ASAP 工作組將定義一個描述性功能集，該功能集由 SIP 服務提供商填充，並在與企業網絡通信時封裝足夠的信息以與服務提供商網絡建立 SIP 中繼。 除了定義描述性功能集之外，ASAP 工作組還將定義功能集的數據模型，服務發現機制和功能集的傳輸機制。ASAP 工作組的上述交付成果統稱為 “SIP Auto Peer”。

第五章　參與技術活動報告

團隊參與 2 場國內會議， 2020 AWS 臺北高峰會與 2020 台灣創新技術博覽會。

相關會議內容如後所述。

第一節　參加 2020 AWS 臺北高峰會

一、會議簡介

2020 年 7 月 10 日，2020 AWS 臺北高峰會因受疫情影響採用線上舉行，參與者除了可以根據需求參與 42 場精彩的主題演講，還可以體驗帶領雲端初學者入門的 AWSome Day、旁觀或下場切磋一場 AWS DeepRacer League 線上 AI 賽車競賽，或是一探高手創意過招的 Hack for Good 線上黑客松，同時還有專家即時在線可以一對一解惑。

此次活動的主題演講包含 8 大主題，企業上雲策略(Strategy)、微型服務(Microservices)、人工智慧與機器學習(AI/ML)、數據分析(Data & Analytics)、資安與規範(Security & Compliance)、網路(Networking)、無伺服器 (Serverless) 服務、容器服務(Containers)，從大數據分析到時下正夯的網路資安議題，無論你對雲端科技是初次涉略或是小有研究，都可以在這次的 AWS 臺北雲端高峰會得到更多專業且實用的知識！

(一)　開幕致詞嘉賓

1、 王定愷 (Robert)

現任為 AWS 香港及台灣總經理，負責 AWS 在香港及台灣的策略規劃、業務發展和營運工作。在 2020AWS 臺北雲端高峰會分享數位轉型為企業帶來的正向改變，以及 5G 和科技政策在雲端加乘之下，將如何影響未來台灣的市場！

(二)　大會演講嘉賓

1、 Dr. Werner Vogels - Amazon.com 的 CTO

2、 Olivier Klein - AWS 方案架構部亞太區新興技術主管

作為 Amazon CTO，Dr. Werner Vogels 負責推動企業以客戶為中心的技術願景，在此活動中分享企業如何規劃、建構以及運用 AWS 最新技術並發揮至最大效益！Olivier 效力於亞太地區與歐洲的亞馬遜網路服務，協助客戶建立可復原、可擴展、安全和符合效益的應用，並創建創新的數據驅動商業模式。他針對人工智慧 (AI)、機器學習 (ML)、和物聯網 (IoT) 領域如何為生產助力、提升工作流程效率提出建議，也提供以終端消費者為目標的全面性營運分析及新通路應用，也積極協助客戶，幫助他們建立平台，並讓公司 IT 基礎架構支出符合收益模式，有效減少產品開發造成的浪費與破壞。

(三)　議程

1、 7 月 10 日 活動議程

時間(GMT+8)	大會議程
9:00am	平台開放登入
10:00am -10:15am (15mins)	講師: Robert Wang, Managing Director, AWS Taiwan & Hong Kong 開幕致詞
10:15am -11:00am (45mins)	講師: Dr. Werner Vogels, Chief Technology Officer, Amazon.com 大會主題演講 1 （英文搭配中文字幕)
11:00am -12:00pm (60mins)	Breakout Session 分堂議程 (Part 1): Business Track & Technical Track
12:00pm-12:50pm (50mins)	午休時間 歡迎瀏覽線上攤位
12:50pm -13:25pm (35mins)	講師: Olivier Klein, Lead Technologist Asia-Pacific, AWS 大會主題演講 2 （英文搭配中文字幕)
13:30pm -14:30pm (60mins)	Breakout Session 分堂議程 (Part 2): Business Track & Technical Track
14:30pm - 14:40pm (10mins)	茶歇時間 歡迎瀏覽線上攤位
14:40pm - 15:40pm (60mins)	Breakout Session 分堂議程 (Part 3): Business Track & Technical Track
15:40pm - 16:00pm	線上互動與交流

(20mins)	

其中分堂議程詳細內容如下，分別分為產業聚焦、數位轉型/企業應用、建構現代化應用、資訊安全、資料分析/人工智慧/機器學習：

分堂議程 / 時間 (GMT+8)	Level 100-200	
	Track1 產業聚焦	Track2 產業聚焦
11:00am - 11:30am (30mins)	製造	零售
	企業善用雲端來加速數位化及創新	保有地端投資加乘雲端，逆向高流量
11:30am - 12:00am (30mins)	製造	零售
	如何藉由雲端優勢推動製造及運籌數位轉型	電商平台的資安維運與成本管理
12:00pm – 12:50pm (50mins)	午休時間 歡迎瀏覽線上攤位	
13:30pm - 14:00pm (30mins)	高效能運算 HPC	媒體串流
	建構安全高效的電子設計自動化環境	日本電視直播技術革命串流平台不容忽視的技術創

		新
14:00pm - 14:30pm (30mins)	金融	媒體串流
	如何透過機器學習進行詐欺偵測	全民直播時代的多 CDN 架構監控與觀看體驗最佳化
14:30pm - 14:40pm (10mins)	茶歇時間 歡迎瀏覽線上攤位	
14:40pm - 15:10pm (30mins)	金融	行銷科技
	資本市場數位創新：市場資料雲端分析與應用	利用 SageMaker 深度學習容器化在廣告推播之應用
15:10pm - 15:40pm (30mins)	金融	遊戲產業
	建立安全高效的資料分析平台加速金融創新	利用 Amazon Personalize 個人化推薦提升玩家體驗
15:40pm - 16:00pm (20mins)	線上互動與交流	

分堂議程 / 時間 (GMT+8)	Level 300-400	
	Track3 數位轉型/企業應用	Track4 建構現代化應用
11:00am - 11:30am (30mins)	Amazon 文化	Serverless
	Amazon 的創新實踐	如何活用事件驅動架構快速擴展應用
11:30am - 12:00am (30mins)	架構策略	容器應用
	從傳統 legacy 邁向數位化與現代化架構	容器技術和 AWS Lambda 讓您專注「應用優先」
12:00pm – 12:50pm (50mins)	午休時間 歡迎瀏覽線上攤位	
13:30pm - 14:00pm (30mins)	雲端投資	Serverless
	如何妥善運用雲端優勢遷移上雲	利用 AWS Step Functions 建構穩健的業務處理流程
14:00pm - 14:30pm (30mins)	雲端搬遷	CI/CD
	企業工作負載遷移至 AWS 的最佳實踐	如何藉由 CI/CD 流程管理容器化和無伺服器應用

14:30pm - 14:40pm (10mins)	茶歇時間 歡迎瀏覽線上攤位	
14:40pm - 15:10pm (30mins)	Amazon EC2	Kubernetes
	使用 Amazon EC2 打造企業計算平台與成本和容量優化	架構即代碼-AWS CDK 與 CDK8S 聯手打造下一代 K8S 應用
15:10pm - 15:40pm (30mins)	資料庫	遊戲產業
	打造應用專屬資料庫(Purpose-built)與了解託管服務優勢	如何透過 AWS IOT 服務建構物聯網應用
15:40pm - 16:00pm (20mins)	線上互動與交流	

分堂議程 / 時間 (GMT+8)	Level 300-400	
	Track5 資訊安全	Track6 資料分析/人工智慧/機器學習
11:00am - 11:30am (30mins)	網頁安全	Data Engineering
	如何藉由多層次防禦	進入 AI 領域的第一步驟-資

	搭建網路應用安全	料平台的建置
11:30am - 12:00am (30mins)	安全與合規	Data Lake
	多重帳戶安全策略與方針	搭建現代化的資料數據湖
12:00pm – 12:50pm (50mins)	午休時間 歡迎瀏覽線上攤位	
13:30pm - 14:00pm (30mins)	DDoS	AI/ML
	迎戰 DDoS 攻擊的資安最佳實踐	如何藉由 AWS AI 和機器學習平台搭建多功能的 AI 解決方案
14:00pm - 14:30pm (30mins)	混合雲託管	Healhcare/ML
	透過 AWS Outpost 就地部屬(on-premises)雲端環境	AWS AI/ML 如何幫助醫療業
14:30pm - 14:40pm (10mins)	茶歇時間 歡迎瀏覽線上攤位	
14:40pm -	Storage	IoT/ML

<table>
<tr><td>15:10pm
(30mins)</td><td>AWS 檔案儲存服務概觀</td><td>如何藉由物聯網(IoT)與機器學習提高預測性維修與產品良率</td></tr>
<tr><td rowspan="2">15:10pm - 15:40pm
(30mins)</td><td>區塊鏈</td><td>Robotic</td></tr>
<tr><td>透過 Amazon Managed Blockchain 與 Amazon QLDB 打造區塊鏈應用</td><td>透過 AWS AI 服務模擬、部屬機器人於產業之應用</td></tr>
<tr><td>15:40pm - 16:00pm
(20mins)</td><td colspan="2">線上互動與交流</td></tr>
</table>

二、心得

此次參與線上舉辦的高峰會，除了觀看主題演講和產業/技術專題外，也利用大會安排的午休時間瀏覽了線上攤位。

在產業/技術專題中觀看了兩個與 IoT 有關的內容：

1. 如何透過 AWS IoT 服務建構物聯網應用：演講者為台灣 AWS Cloud Support Engineer，AWS IoT Core 領域專家 Ed Tsai (蔡勝全)，此演講提到物聯網上的應用情境有許多，例如：工業領域、能源產業、醫療領域、農業領域、倉儲管

理領域與智慧家庭等等...(如圖 135)，目前有許多產業使用 AWS IoT 來做轉型，透過 AWS IoT，讓企業安全地連接、管理，同時兼顧無縫地擴展、端對端安全、也能和 AWS 其他服務緊密結合。藉著一些實際案例，如：拜耳、SKF 的案例說明數位化轉型的流程，使團隊對物聯網應用能協助解決的能力更深入瞭解。

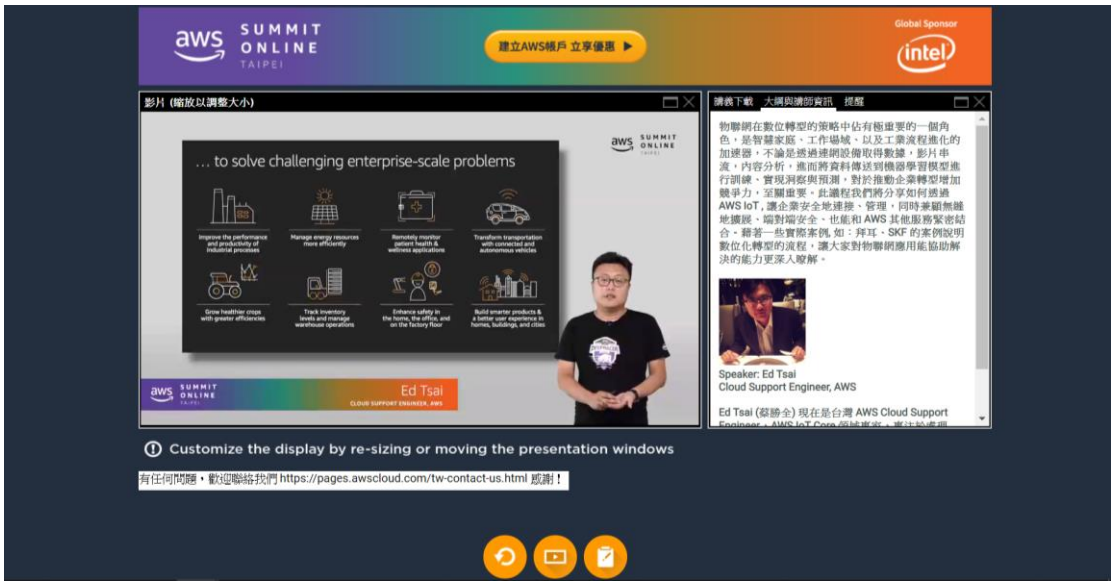


圖 135、物聯網應用情境

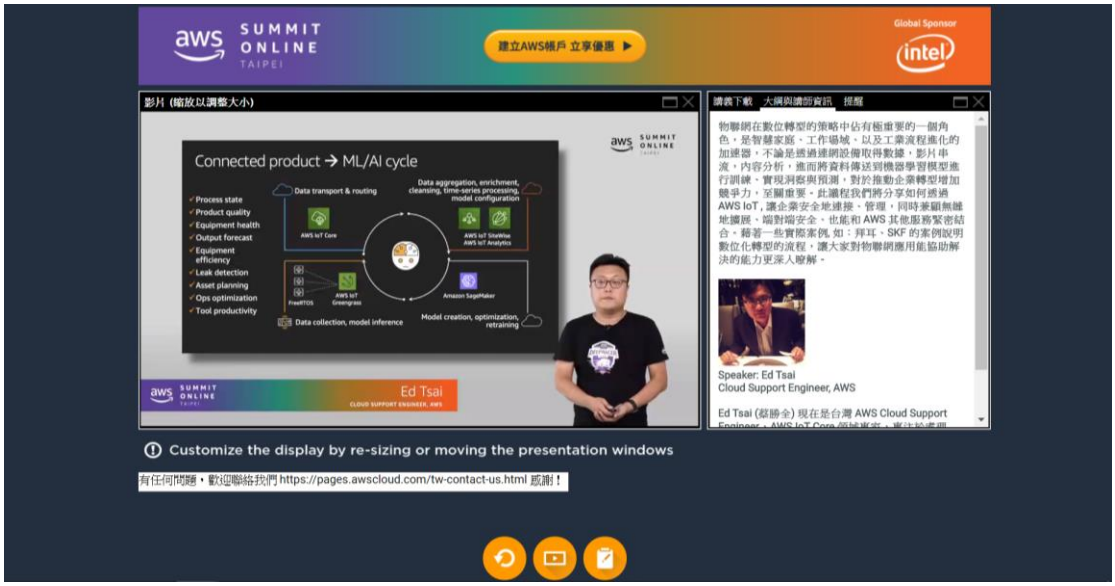


圖 136、AWS IoT 服務應用

2. 如何藉由物聯網 (IoT) 與機器學習提高預測性維修與產品良率(圖 137)：演講者為 Lucern Ma 是 AWS 在台灣的解決方案架構師團隊經理，此演講首先提到預測性維護的定義，監控、預測、提醒與通知，預測性維護一直是在自動化製造業整體生產中，很重要的一個環節。其中，提到一個空氣過濾器的案例，一開始是使用人工的方式，所以需花費許多人力成本與時間，藉由 AWS 的 IoT 和機器學習服務，加速物聯網應用之落實。在內容當中也分享如何訓練機器學習模型，加速預測問題發生的速度，使一些行程較彈性化，且妥善安排設備維護。

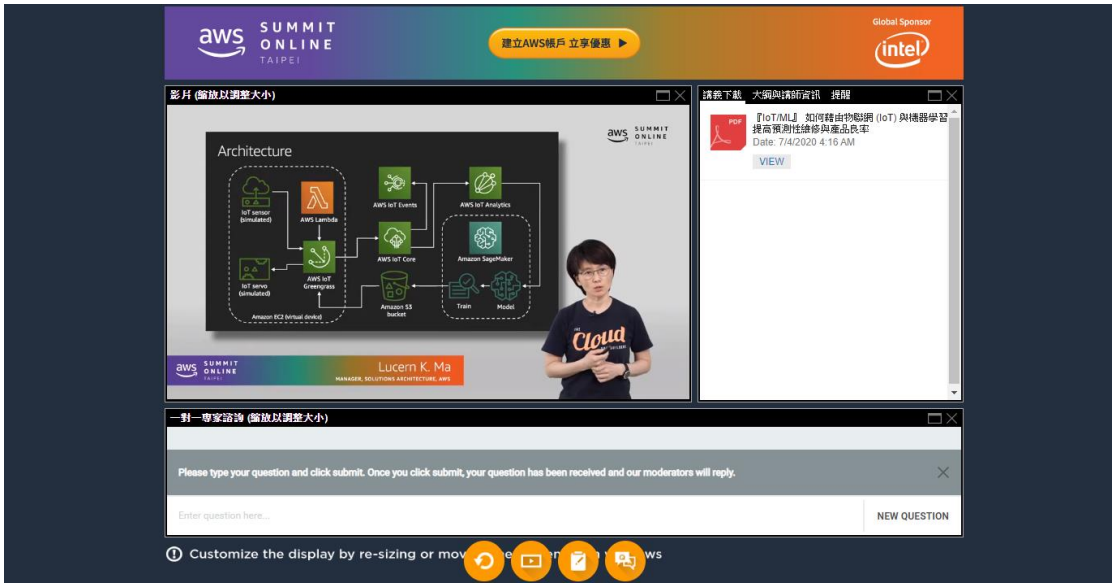


圖 137、AWS IOT 的架構

第二節　**2020 台灣創新技術博覽會**

一、會議簡介

2020 年 9 月 24 日至 26 日在台北世貿一館盛大舉行「2020 台灣創新技術博覽會」。大會以「韌性台灣 智慧未來」為主軸，除原有發明競賽區及傑出發明館外，亦結合政府 5+2 產業創新技術政策，規劃「未來科技館」、「永續發展館」及「創新領航館」等三大主題館匯集政府各部會能量，並特別企劃科技防疫、防災解決方案、數位服務、精準健康、綠色產業鏈等科技專區，預計展出超過上千件專利與技術的應用。另外在國際展區更集結歐、美、日及新南向等逾 40 家國際機構與企業參與，包括微軟、CISCO、西門子、康寧、羅技、泰國國家科技發展局(NSTDA)等，期望以豐富多元的交易樞紐平台，結合在地創新動能與區域優勢，對接新南向與歐、美、日等地區，以「國際研發交易樞紐平台(IP HUB)」角色，將台灣技術推廣至國際，持續展現台灣智慧價值。

展覽期間舉辦近 20 場次的產業趨勢研討會、技術發表與商機媒合會等活動，展期次日亦規劃「創新科技論壇」(Taiwan Innotech Forum)，以「無形資產的價值」、「技術合作與移轉」為主題，邀請國際級智財大師包括：Hitachi、Uber、HZO 等機構專家分享全球智財商業策略，期望透過跨越國界與全球交流，激盪產業新火花。

下圖為次博覽會之平面配置圖。

圖 138、台灣創新博覽會平面配置圖

(一) 展會活動資訊

今年展覽期間亦舉辦豐富的周邊活動，包含國際論壇、技術商討會、技術經驗交流分享會等，以下為各活動/商談會/研討會之時間表。

1、 2020 年 9 月 24 日

時間	活動名稱	地點
09:00-12:00	互動式科技復健研討會	世貿中心一館 2 樓第 2 會議室
09:00-12:00	鏈結融資保證與科技市場媒合會	世貿中心一館 2 樓第 3 會議室
09:30-12:00	乳牛場擠乳機器人研討會	世貿中心一館 2 樓第 4 會議室
12:30-16:10	高值化農產素材產業應用論壇	世貿中心一館 2 樓第 5 會議室
13:00-14:00	先進健康照護技術發表會(遠距)	世貿中心一館 1 樓 遠距展示區
13:00-16:00	塑膠創新與專利應用技術研討會	世貿中心一館 2 樓第 3 會議室
13:30-16:30	航向未來：台灣自駕船技術發展現況	世貿中心一館 2 樓第 2 會議室
14:00-16:30	乳質檢測儀器的國際趨勢研討會	世貿中心一館 2 樓第 4 會議室
15:30-16:30	機器人系統及氣體分析技術發表會(遠距)	世貿中心一館 1 樓 遠距展示區

2、 2020 年 9 月 25 日

時間	活動名稱	地點
09:00-11:50	環保設備與生質能應用推廣說明會	世貿中心一館 2 樓第 2 會議室
09:00-12:00	2020 台日創新技術媒合交流會	世貿中心一館 2 樓第 5 會議室

09:00-12:00	動物繁殖保育新科技應用方向研討會	世貿中心一館 2 樓第 4 會議室
10:00-16:00	創新科技論壇	世貿中心一館 2 樓第 5 會議室
10:00-12:00	省能空調及 AI 內視鏡技術發表會（遠距）	世貿中心一館 1 樓 C 區大會舞台區、線上論壇
10:30-11:45	創新領航館現場直播 ～ ＜路怡珍主播＞	世貿中心一館 1 樓 遠距展示區
13:00-17:00	AI 與智慧製造現況及解決方案	世貿中心一館 2 樓第 5 會議室
13:00-16:30	AIoT 智聯應用技術推廣媒合商談會	世貿中心一館 2 樓第 4 會議室
13:30-16:00	TAIP 台灣高階儀器研發技術分享展示會	世貿中心一館 2 樓第 2 會議室
14:00-16:00	國際創新技術推廣發表會	世貿中心一館 1 樓 遠距展示區

3、 2020 年 9 月 26 日

時間	活動名稱	地點
09:00-12:00	跨域智慧製造技術推廣媒合商談會	世貿中心一館 2 樓第 3 會議室
11:00-12:00	創新應用技術發表會	世貿中心一館 1 樓 遠距展示區
13:30-16:30	數位影像暨色彩技術跨域應用研討會	世貿中心一館 2 樓第 2 會議室

二、心得

在本次展覽中，因國發會亞洲·矽谷計畫執行中心已連續三年參加此博覽會，而亞洲·矽谷計畫主軸之一為推動物聯網產業創新研發，故此次率領 16 間國內廠商於「創新領航館」中以多元情境場域呈現「5G 智慧城市應用」，透過 AI、5G、雲端運算等技術結合物聯網多元技術應用樣貌，以「超自動」、「全物聯」、「跨虛實」即「新保健」四大主題區呈現貼近民眾之智慧應用解決方案。

以下介紹幾個在展場上展出的案例：

1、 在「創新領航館」中，OSENSE 光禾科技提出了「智慧球場解決方法」，結合 AI 與 IoT 技術，在智慧球場中針對不同球場的需求，以資訊、互動、消費三大核心，提供球迷互動式競賽體驗。亦為球團、球員提供各式整合情資。藉由辨別技術將環境數據化。或是以 AR 增加互動性及趣味性，可有效整合數位服務和實體空間，擴增 O2O 或 OMO 應用。圖 139 為現場展示的模擬球場，可在平板上利用 AR 的方式出現怪獸，增加與球迷間的互動。圖 140 與圖 141 皆為現場撥放與此方案有關之功能介紹。

圖 139、光禾科技模擬球場展示

圖 140、智慧球場提供相關功能

圖 141、智慧球場提供相關功能

2、 蹦世界在展場中展出「LBS 平台：智慧導覽、實境遊戲」，此公司主打只需透過 Beacon 與 GPS 定位，不論在室內或在戶外，只要接近展覽品或特定景點，手機就會自動蹦出語音、文字、圖片、AR 擴增實境等介紹內容。且為因應現代數位潮流，蹦世界更將博物館線上化，推出線上/數位博物館，並且讓使用者從網頁或 APP 皆可觀賞使用。

圖 142、蹦世界線上導覽展示

3、 台灣電力公司也在會場供展出了「用於智慧電表系統的單相三線式智慧電表」(圖 143)，在現今技術發達的時代，對於使用傳統機械式電表與電子式電表的用戶來說，若想得知前期電量使用度數，須等電費單寄到，即使想規劃節電方式，式不知從何改善的，故台電推出新一代電表，除了具有即時記錄總用電量外更加裝通訊系統，能將用電資訊傳輸到台電的電表資料管理中心，進行用電統計即分析。用戶可在台電設置的用戶入口服務網站中，清楚地得知與自己相關的用電數據、圖表。此方案一方面解決了傳統抄表所造成的人力與時間的耗費，減少數據的錯誤率，另一方面也可讓家庭用戶、企業用戶即時的得知目前的用電情況，並進而改善節能。

圖 143、用於智慧電表系統的單相三線式智慧電表

以下再以多張照片展示在本次展覽展出的物聯網應用。

圖 144、光學式 PM2.5 感測模組

圖 145、微型數位式氣體感測器

圖 146、即時羽球訓練輔助裝置與動作分析系統

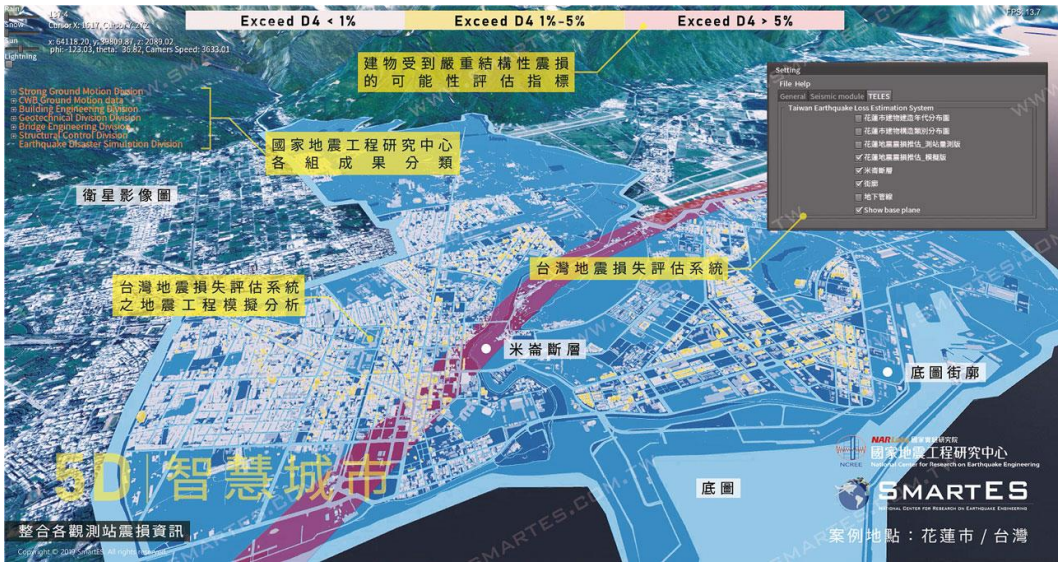


圖 147、5D 智慧城市—SmartES 平台

第六章　結論與建議

第一節　結論說明

我們在此計畫中針對食、醫、住、行、育、樂，做了六項物聯網應用的調查。然而也發現到了已有越來越多物聯網的應用出現在生活當中。例如：使用在車輛上、家庭中的電器用品、身上的穿戴式裝置或是工廠中的機器設備...等，以下對於我們的六項調查做個總結性的描述。

在食的部分，透過研華科技的冷鏈系統解決了食物從生產後到配送門市或工廠時，無法隨時確認食物在運輸工程中溫度是否異常的狀況，藉由溫濕度感測器加上資料即時回傳平台，在食物運送的過程中能保以隨時監控，降低食物損耗且減少不必要的浪費；在醫的部分，則是立創智能公司研發出的心電監測貼片解決了過往傳統心電監測器的困擾，且在貼片中記錄下的數據會先暫存在貼片中，待監測完畢後再將資料傳送給閘道器，利用插座式的閘道器或手機 APP 即可將資料上傳至雲端平台，接著在傳回至醫院；在住的部分，則是提及了東海大學計算機中心為了能即時監控機房的室內溫度，且做到節約電能的目的，透過無線數位電表，將電表所紀錄之資料儲存至資料庫，並為此做分析，以達到清楚的了解電能消耗進而做出對應方式；在行

的部分，藉由中華電信提出的智慧停車場案例，利用地磁感測器加上即時的資料回傳，使出遊之駕駛人可立即得知車位而減少許多時間尋找車位，且降低廢氣排放；在育的部分，透過德國慧魚工程積木組模擬出了工業 4.0 的小型實驗室，利用模組化的積木做出基本的產線組合，且架設攝影機可模擬工廠監控，工廠內的所有操作可藉由自動化的操作且將資料透過感測器儲存、傳送資料到雲端，所有工廠生產的流程細節不需到實際的工廠即可教導學生如何操作與管理；在樂的部分，藉由蹦世界的平台與技術，使用 Beacon 與 GPS 定位做到室內外定位，進而做到智慧導覽且可進而配合當地的文化風情與當地環境設計智慧解謎。

從上述的物聯網應用研析，我們了解基本上現有的物聯網應用發展多遵循第二章所述之架構(p11~p13)，由上到下分別是感知層、網路層與應用層，並應重視資訊安全防護。在個別領域裡，感知層可適用多種不同之感測設備收集環境等相關資料，如上段所述，不同應用之間所使用不同之感測器。在網路層，應根據應用情境考量實體網路之傳送距離、頻寬、訊息傳送頻率、上行下行資料之需求、電源供應，可選多種不同的實體網路配合來實現網路層訊息傳輸。在不同情境下，也可考慮是否使用邊緣計算架構來提升系統的穩定度與效能。

然後在 IETF 的技術標準中，針對了 IP、DN、BGP、RPKI、DNSSEC、

SIP 6 個主題做介紹，IP 部分主要還是提及 IP 的演進，從 IPv4 到 IPv6 因應現今 IP 位置越來越少，所以現在需往 IPv6 發展，所以訂制了 IPv6 標準以及談及 IPv6 與物聯網間的關係及使用 IPv6 的優勢；而 DN 部分講解了 DN 的發展與其運作方式，並描述訊息格式與提及安全問題；BGP 是網際網路最重要的協定之一。大多數網際網路服務提供者(Internet Service Provider，簡稱 ISP)使用 BGP 來與其他 ISP 建立路由連接，彼此之間互稱為通信對端或對等實體(peer)，可為單個或多個 ISP 網路提供更好的冗餘網路(RFC 1998)。內容中提及與路由協定相關之技術及 BGP 的運行方式；RPKI 講述許多駭客散步錯誤路由的資訊或是網路管理者宣布錯誤路由，造成全球網路骨幹流量異常流動與網路無法連線的現象，為解決這個問題全球網路註冊管理機構開始推動資源公鑰基礎建設(RPKI)，內容中也描述了 RPKI 所使用的資源憑證，該如何做管理發布與驗證；DNSSEC 為 DN 的延伸，DNSSEC 是為保護應用程式（以及服務這些應用程式的快取解析器）免受 DNS 所出現之漏洞所造成的影響，其中提到了幾個 DNS 的攻擊，然而為防範這些攻擊，進而需驗證多個項目，及做簽章、加密的處理；最後 SIP 則是為進行對話管理的應用層通訊協定，先前的敘述提及其協定架構與當中有和基礎元件並有哪些相關協定，並詳述了通訊的流程，介紹了其應用有哪些。

第二節　**建議事項**

感謝計畫經費的支持，團隊參訪了國內舉辦之物聯網展與進行廠商訪談，了解目前市場上 IPv6 的物聯網應用仍未普及，但廠商表明了解 IPv6 對於物聯網應用的未來發展是很關鍵的，建議政府及相關單位可以加強 IPv6 基礎建設的普及，並鼓勵國內廠商投入相關之研發。

在物聯網的資訊安全，目前並沒有統一的標準與最佳的實施方式，建議政府與相關單位著手開始引導相關廠商投入物聯網資安標準之制定。

第七章　參考資料來源

[1] IP。https://en.wikipedia.org/wiki/IP

[2] Domain name。https://en.wikipedia.org/wiki/Domain_name

[3] Border Gateway Protocol。
https://en.wikipedia.org/wiki/Border_Gateway_Protocol

[4] Resource Public Key Infrastructure。
https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure

[5] Domain Name System Security Extensions。
https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

[6] Session Initiation Protocol。
https://en.wikipedia.org/wiki/Session_Initiation_Protocol

[7] IETF Working Groups. https://www.ietf.org/how/wgs/

[8] 張志勇、石貴平、翁仲銘、廖文華(2016)。TQC 物聯網智慧應用及技術特訓教材。碁峯資訊。

[9] 周立德、曾家偉(2017)。物聯網與大數據。台網中心電子報。

[10] 周碩彥(2015)。物聯網發展趨勢展示內容研究報告。國立科學工藝博物館。

[11] 王文娟(2016)。物聯網概念及應用。中華經濟研究院 經濟前瞻。

[12] 陳榮貴(2018)。物聯網發展與應用。第 27 屆近代工程技術討論會。

[13] Ziv Chang (2019)。IoT Device Security – Locking Out Risks and Threats to Smart Homes。趨勢科技。

[14] E. Vyncke, Ed., K. Chittimaneni, M. Kaeo, E. Rey, "Operational Security Considerations for IPv6 Networks," IETF Internet-Draft, draft-ietf-opsec-v6-21, November 3, 2019.

[15] E. Davies, S. Krishnan, P. Savola, "IPv6 Transition/Coexistence Security Considerations," RFC 4942, September 2007.

[16] S. Asadullah, A. Ahmed, C. Popoviciu, P. Savola, J. Palet, "ISP IPv6 Deployment Scenarios in Broadband Access Networks", RFC 4779, January 2007.

[17] G. Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, "Local Network Protection for IPv6," RFC 4864, May 2007.

[18] J. Woodyatt, Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.

[19] B. Carpenter, S. Jiang, "IPv6 Guidance for Internet Content Providers and Application Service Providers," RFC 6883, March 2013.

[20]

中英專有名詞對照

3G 第三代行動電話(3rd-Generation, 3G)

4G 第三代行動電話(4rd-Generation, 4G

A

ADSL 非對稱式數位用戶迴路(Asymmetric digital subscriber line, ADSL)

Akamai 阿卡邁 (Akamai Technologies)

AP 無線接入點(Access Point, AP)

APNIC 亞太網路資訊中心(Asia-Pacific Network Information Centre, APNIC)

C

CERNET 中國教育和科研計算機網(China Education and Research Network, CERNET)

DHCP 動態主機組態協定(Dynamic Host Configuration Protocol)

DNS 網域名稱伺服器(Domain Name System, DNS)

Dual Stack IPv4/ IPv6 雙協定(Dual Stack)

E

Email 電子郵件(Electronic mail, Email)

EPC 產品電子碼(Electronic Product Code)

F

FTTx 光世代網(Fiber To The x, FTTx)

Firmware 韌體(Firmware)

G

Gateway 閘道器(Gateway)

GOLD Logo 金質標章(GOLD Logo)

Google 谷歌(Google)

GRB 政府研究資訊系統(Government Research Bulletin, GRB)

GSN 政府網際服務網(Government Service Network , GSN)

H

Hot Spot 熱點(Hot Spot)

I

IAB 網際網路架構委員會(Internet Architecture Board, IAB)

IANA 國際網路位址分配機構(Internet Assigned Numbers Authority, IANA)

ICANN 網際網路名稱與號碼指配機構(Internet Corporation for Assigned Names and Numbers, ICANN)

ICP 網際網路內容提供者(Internet Content Provider, ICP)

IDC 資訊機房(Internet Data Center, IDC)

IETF 網際網路工程任務小組(Internet Engineering Task Force, IETF)

Information Security 資訊安全 (Information Security)

Internet APN 網際網路接入點名稱 (Internet Access Point Name)

IoT 物聯網(Internet of Things, IoT)

IP 網際網路協定(Internet Protocol, IP)

IPsec 網際網路安全機制(Internet Protocol Security, IPsec)

IPSecv6 IPv6 網際網路安全機制 (Internet Protocol Security of IPv6, IPSecv6)

IPSO IP 智慧物件(Internet Protocol Smart Objects, IPSO)

IPv4 網際網路通訊協定第四版 (Internet Protocol version 4, IPv4)

IPv6 網際網路通訊協定第六版 (Internet Protocol version 6, IPv6)

IPv6 Day IPv6 日(IPv6 Day)

IPv4/v6 Dual Stack 網際網路通訊協定第四版及第六版雙軌並行(IPv4/v6 Dual Stack)

IPv6 Ready Logo 網際網路通訊協定第六版認證獎章(IPv6 Ready Logo)

ISOC 網際網路協會(Internet Society, ISOC)

ISP 網際網路服務提供者(Internet Service Provider ,ISP)

IASP 網際網路服務提供者(Internet Access Service Provider ,ISP)

IT 資訊技術(Information Technology)

K

KISA 韓國網路振興院（Korea Internet Security Agency

L

L3 Switch 第三層交換器(Layer 3 Switch)

M

Mobile Internet 行動上網(Mobile Internet)

N

NAT 網路位址轉譯(Network Address Translation, NAT)

NCC 國家通訊傳播委員會(National Communications Commission)

Network Layer 網路層(Network Layer)

NRO 號碼資源組織(Number Resource Organization, NRO)

P

P2P 點對點對等網路架構(Point to Point , P2P)

PAD 平板電腦(PAD)

PHONE 手機(Phone)

PPPoE 網路對等協定(Point-to-Point Protocol Over Ethernet)

Profile 設定檔(Profile)

PWLAN 公用無線區域網路(Public Wireless Local Area Networks)

R

RFID 無線射頻辨識，Radio Frequency IDentification)

RIR 區域網路註冊管理機構(Regional Internet registry, RIR)

Router 路由器(Router)

S

Smarter Meter 智慧量表(Smarter Meter)

T

TABLET 平板電腦(Tablet)

TANet 臺灣學術網路(Taiwan Academic Network, TANet)

Tunnel Broker 通道代理伺服器(Tunnel Broker)

TWNIC 財團法人台灣網路資訊中心(Taiwan Network Information Center, TWNIC)

U

UPC 通用商品碼(Universal Product Code)

USGv6 美國聯邦政府 IPv6 網通設備支援標準(United States Government IPv6 Profile, USGv6)

W

Wiki 維基百科(Wikipedia, WiKi)

WWW 全球資訊網(World Wide Web, WWW)

WiFi AP 無線基地台(WiFi AP)

WiFi Adaptor 無線網路卡(WiFi Adaptor)

WiFi Router 寬頻分享器(WiFi Router)