『推動 IPv4/IPv6 雙軌普行方案』

附錄十
『物聯網、5G 與 IPv6 國際技術標準及物聯網平台與應用之研析』
期末報告

108 年委託研究報告

『物聯網、5G 與 IPv6 國際技術標準及物聯網平台與應用之研析』
期末報告

計畫委託機關：台灣網路資訊中心

中華民國 108 年 10 月

108 年委託研究報告

物聯網、5G 與 IPv6 國際技術標準及物聯網平台與應用之研析

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

吳題羽、鍾奉原、江佳嬅、林育萱、

林昱廷、林姿岑、吳宜庭、蔡孟璇、

許翰薪、林辰昊、黃禹锜、鍾溥

研究期程：中華民國 108 年 4 月至 108 年 12 月

研究經費：新臺幣 78 萬元

本報告不必然代表台灣網路資訊中心意見

中華民國 108 **年** 10 **月**

目　　次

表　　次 …… III

圖　　次 …… VII

提　　要 …… XIV

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 3

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 8

一、　人力運用情形 8

二、　經費運用情形 9

第二章　成果說明 10

第一節　物聯網、5G 與 IPv6 之國際技術標準之研析 10

一、　物聯網、5G 與 IPv6 基本介紹 10

二、　物聯網、5G 與 IPv6 國際技術標準簡介 38

三、　物聯網、5G 與 IPv6 國際技術標準內容介紹 60

第二節　物聯網平台與應用 99

一、　物聯網基本介紹 99

二、　Amazon AWS 平台與應用 103

三、　Microsoft Azure 平台與應用 113

四、 Google IoT 平台與應用 122
五、 國內電信業者物聯網平台介紹 129
第三章 結論與建議 140
第一節 結論說明 140
第二節 建議事項 142
第四章 參考資料來源 143
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 8

表 4、合計總經費運用情形統計表 9

表 5、APNIC IPv6 使用調查-全球 14

表 6、APNIC IPv6 使用調查-亞洲 15

表 7、APNIC IPv6 排名 16

表 8、物聯網可能的安全議題和風險 24

表 9、TAICS 資安標準 28

表 10、5G 釋照與商轉時程 35

表 11、5G 商業活動 36

表 12、物聯網相關的工作小組列表 40

表 13、物聯網相關 RFC 列表 42

表 14、全文翻譯的 23 篇 RFC 列表 61

表 15、物聯網之可能應用 101

圖　次

圖 1: GOOGLE IPV6 調查(全球) 13

圖 2: GOOGLE IPV6 調查(國家) 13

圖 3: APNIC 調查台灣網路 IPV6 使用情形 15

圖 4: ETSI 物聯網架構 19

圖 5: 物聯網資安標章 28

圖 6: 行動通訊技術演進 29

圖 7: 5G 標準化時程 31

圖 8: 5G 的 3 大應用場景 34

圖 9: AWS IOT 運作方式 104

圖 10: AWS IOT 工業預防性維護參考架構 109

圖 11: LG 在 AWS 上的架構參考 111

圖 12: 英國威爾斯 NEWPORT 市在 AWS 上的架構參考 112

圖 13: AZURE IOT 技術和解決方案 114

圖 14: COSTA FARMS 使用 AZURE IOT 解決方案自動化控制 PH 值 . 119

圖 15: POWEL 使用 AZURE IOT 解決方案檢測漏水情況 120

圖 16: GOOGLE CLOUD PLATFORM 的 IOT 參考架構 125

圖 17: 中華電信 IoT 智慧聯網大平台 130

圖 18: AllSeen 使用中華電信 IoT 智慧聯網大平台 132

圖 19: Driving Insight 使用中華電信 IoT 智慧聯網大平台.....133

圖 20: 遠傳物聯網服務 135

提　要

關鍵詞：IPv6、物聯網、5G、標準、RFC、雲端平台

一、研究緣起

隨著新一代人工智慧不斷突破，加上雲端運算與大數據處理技術的成熟與普及，人工智慧物聯網 AIoT (AI + IoT) 在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。然而，全球 IPv4 位址已經用罄，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。同時，首個針對商用的 5G 標準 SA (Standalone)方案於西元 2018 年 6 月 13 日出爐。新一代的 5G 行動通訊能提供更優質網路服務。

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、5G 與 IPv6 等相關技術、及(2)物聯網平台與應用等兩個方面，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、5G 與 IPv6 相關技術、及分析物聯網平台與應用等兩方面，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 2 個分項：

分項一：物聯網、5G 與 IPv6 之國際技術標準之研析

1. IPv6 的發展現況與趨勢

2. 物聯網的基礎架構介紹

3. 5G 的基礎介紹

4. 物聯網、5G 與 IPv6 之國際技術標準

分項二：物聯網平台與應用

1. 物聯網的實體層介紹

2. 物聯網的應用介紹

3. 國際物聯網平台介紹

4. 國內電信業者物聯網平台介紹

三、重要發現

(一) 在與廠商訪談的過程中，物聯網應用廠商仍以閘道器(Gateway)作為裝置與網際網路(Internet)聯結的中介，加上大部份的應用並無傳輸延遲上的嚴峻考量，因此，在裝置端，主流仍是無 IP 連結或是使用 IPv4，且對是否支援或採用 IPv6 採取觀望的態度，特別是在沒有實際的市場需求下。

(二) 國際雲端三大平台 Amazon AWS, Microsoft Azure, 與 Google GCP，在部份產品支援 IPv6。其中，AWS IoT 支援 IPv6，而 Azure IoT 與 Google IoT 仍未支援 IPv6。此一

觀察，與之前廠商訪談的結果一致。

(三) IETF 從連結層、網路層、傳輸層到應用層幾個面向都有相關的 RFC 說明標準實施方向。在應用層有輕量級的 CoAP 系列 RFC 來替代 HTTP，用二進制的 CBOR 訊息來替代純文字的 JSON 訊息。在傳輸層與網路層，同樣有輕量級的 6LoWPAN 來替代完整的 IPv6 協定堆疊，並制定 RPL 相關路由協定來協助物聯網環境裡可能遇到的情形。同時，在低功耗有損網路 LLN 的概念下，針對不同的實體網路制定相關的協定，以協助受限制裝置在受限制網路裡完成資料傳輸。

(四) 在與廠商訪談的過程中了解到，是否實施 IETF 製定的物聯網相關 RFC 標準，目前並非廠商實作物聯網應用的主要考量。從三大國際雲端平台的物聯網服務 Amazon AWS IoT、Microsoft Azure IoT 與 Google Cloud Platform IoT 來看，最受支援的通訊協定仍是 MQTT 與 HTTPS，CoAP

則是需要透過第三方軟體的協助才能實現。

四、主要建議事項

(一) 雖然目前廠商在實作物聯網產品與應用時，IPv6 與 IETF 相關 RFC 並非最重要的考量，主因是市場的需求不明確，以及全球網路環境仍未全面開通 IPv6。就技術層面來說，由 IPv4 過渡 IPv6 的技術難度並不高，也是廠商沒有大動作開發/測試 IPv6 物聯網產品的原因之一。但廠商也表明了解未來會缺乏 IPv4 的事實，因此，適當的鼓勵廠商投入 IPv6 相關產品應是可行的。

(二) 在 IETF 相關物聯網標準(RFC)的實施上，國內廠商目前處於觀望的態度，相較於 CoAP，仍以 MQTT 為主。建議仍應參考 Amazon AWS IoT、Microsoft Azure IoT 與 Google Cloud Platform IoT 等三大國際雲端平台的投入來評估是否投入實作符合相關 RFC 標準的產品。

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

西元 2018 年 6 月 13 日，3GPP 會議在聖地牙哥召開，第 80 次 TSG RAN 會議正式發表了 5G NR 標準 SA (Standalone)方案，首個針對商用的 5G 標準出爐。與 4G 及其他前幾代行動通訊不同的是，5G 可以為各種業務的不同訴求，提供明確的個性化通訊服務，更高的頻寬、更快的速度、支援超高速移動等特性，為新型態的線上/線下整合服務提供更完善的網路環境。

同時，物聯網(IoT, Internet of Thing)應用也吸引全世界所有人的目光。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」。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。

另一方面，以 TCP/IP 為基礎的網際網路，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，目前已達 25%，估計今年(2019)可達 34%，這些數據顯示出基於 IPv6 之網際網路生態系也逐漸通行。

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、新商業模式的支援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、5G 與 IPv6 等相關技術、及(2)物聯網平台與應用等兩個方面，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，將快速改變人們的日常生活。

本計畫的目的為透過研析物聯網、5G 與 IPv6 相關技術、及分析物聯網平台與應用等兩方面，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 2 個分項：

分項一：物聯網、5G 與 IPv6 之國際技術標準之研析

分項二：物聯網平台與應用

三、工作架構與施行方法

兩個分項之架構如下：

分項一：物聯網、5G 與 IPv6 之國際技術標準之研析

1. IPv6 的發展現況與趨勢

2. 物聯網的基礎架構介紹

3. 5G 的基礎介紹

4. 物聯網、5G 與 IPv6 之國際技術標準

分項二：物聯網平台與應用

1. 物聯網的實體層介紹

2. 物聯網的應用介紹

3. 國際物聯網平台介紹

4. 國內電信業者物聯網平台介紹

四、**預期成果**

本計畫預計透過對物聯網、5G 與 IPv6 之國際技術標準之研析與物聯網平台與應用之研析，充份了解相關技術的發展、標準化的現況、國內外廠商的支援、創新服務應用的機會與風險。

分項一：物聯網、5G 與 IPv6 之國際技術標準之研析

本計畫預計就(1) IPv6 的發展現況與趨勢、(2) 物聯網的基礎架構介紹、(3) 5G 的基礎介紹、(4) 物聯網、5G 與 IPv6 之國際技術標準等四個方向，研析國內外之學術論文、技術報告、標準發展、產業

分析等資料。並透過專家訪談、問卷調查等多種方式了解國內相關產業的發展現況。

分項二：物聯網平台與應用之研析

5G、物聯網(IoT，Internet-of-Things)等新技術的發展，持續朝向萬物聯網的方向推進，未來將有更多的設備連上網路，因此也對 IP 位址之需求持續增加。IETF 已達成未來之新標準(RFC)皆以 IPv6 為適用平臺之共識，IPv6 已成未來技術主流暨網路的根基。

除了 IPv6 連網環境的基礎網路推動計畫外，如何創新為下一代的網路新產業鋪路，對國家未來經濟發展至關重要，為蓄積技術能量加強創新產業連結，及對新技術暨應用的瞭解及掌握，持續對物聯網和 IPv6 相關技術有更深入的了解，政府應扮演國內 物聯網和 IPv6 產業之統合協調與推動的角色，引領國內產業的發展，以創新產業發展，創造對 IPv6 新一代網路的需求，同時創造出 IPv6 的產業價值鏈，提昇業者進行網路升級 IPv6 之動能，協助國內突破 IPv6 推動的困境。為對物聯網和 IPv6 相關技術及平台暨應用有更深入的了解，並掌握技術的發展動向，透過收集及研析相關 RFC 和參與相關技術暨應用會議及展覽，以強化技術能量，充分掌握技術及產業發展的脈動。

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 2 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、5G 與 IPv6 之國際技術標準之研析											
IPv6 的發展現況與趨勢											100 %
物聯網的基礎架構介紹											100 %
5G 的基礎介紹											100 %
物聯網、5G 與 IPv6 之國際技術標準											100 %
物聯網平台與應用											
物聯網的實體層介紹											100 %
物聯網的應用介紹											100 %
國際物聯網平台介紹											100 %

國內電信業者物聯網平台介紹			[redacted]								100 %

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、5G 與 IPv6 之國際技術標準之研析	IPv6 的發展現況與趨勢		✓		
	物聯網的基礎架構介紹		✓		
	5G 的基礎介紹		✓		
	物聯網、5G 與 IPv6 之國際技術標準		✓		
物聯網平台與應用	物聯網的實體層介紹		✓		
	物聯網的應用介紹		✓		
	國際物聯網平台介紹		✓		
	國內電信業者物聯網平台介紹		✓		

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 13 人，除主持人 1 人外，碩士班兼任研究助理 3 人，大學部兼任研究助理 9 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
兼任研究助理	吳題羽		碩士研究生	雲端平台資料蒐集
兼任研究助理	鍾奉原		碩士研究生	5G 資料蒐集、物聯網資料蒐集
兼任研究助理	江佳嬅		碩士研究生	5G 資料蒐集、物聯網資料蒐集
兼任研究助理	林育萱		大學生	RFC 整理、翻譯
兼任研究助理	林昱廷		大學生	RFC 整理、翻譯
兼任研究助理	林姿岑		大學生	RFC 整理、翻譯
兼任研究助理	吳宜庭		大學生	RFC 整理、翻譯
兼任研究助理	蔡孟璇		大學生	RFC 整理、翻譯

兼任研究助理	許翰薪		大學生	RFC 整理、翻譯
兼任研究助理	林辰昊		大學生	RFC 整理、翻譯
兼任研究助理	黃禹鋐		大學生	RFC 整理、翻譯
兼任研究助理	鍾溥		大學生	雲端平台資料蒐集

二、經費運用情形

到 108 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	512,732	252,000	49%	
業務費	77,268	38,000	49%	
差旅費	120,000	90,000	75%	
行政管理費	70,000	70,000	100%	
合　計	780,000	450,000	58%	

第二章　成果說明

第一節　　物聯網、5G 與 IPv6 之國際技術標準之研析

一、物聯網、5G 與 IPv6 基本介紹

(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%。

從西元 1990 年開始，網際網路網路工程工作小組(IETF，Internet Engineering Task Force)即開始規劃 IPv4 的下一代協定，以解決 IP 位址短缺的問題，此外，更希望能將 TCP/IP 早期發展時沒有包含在內的許多新一代網路的功能納入，容許更多的擴充功能，並改善連網環境。IETF 小組創建 IPng，推動 IPv6 標準化工作。1994 年，在加拿大多倫多舉辦的 IETF 會議中，正式提議 IPv6 發展計劃，並於同年的 11 月 17 日得到認可，於 1996 年 8 月 10 日成為 IETF 的草案標準，

最終 IPv6 在 1998 年 12 月由網路工程工作小組以網際網路標準規範(RFC 2460)正式公布。

IPv6 具有以下的多個優勢：

1、 非常大的位址空間:128 位元的 IPv6 位址,未來不只是電腦，個人身上的手機、手錶、手環、家裡的電視、電冰箱、冷氣機、門鎖、路上的汽車、機車、路燈、路口監視器等各式各樣的裝置，都可以有一個獨一無二的 IPv6 位址。

2、 整合的認證及安全機制：IPv6 設計時，已考量網路安全，內建點對點安全保護能力，搭配使用 IPSec，可提供網際網路更安全的資料交換。

3、 支援行動網路：IPv6 在設計上加入支援 Mobile IP 的機制，以利未來支援行動網際網路。

4、 自動設定：IPv6 網路上的主機可自動取得 IPv6 位址，不需透過手動設定，將使行動通訊中之路由機制獲得最佳化。

5、 較佳的路由效率及最佳化：IPv6 位址空間使用階層式規劃，使得路由資訊的交換變得非常精簡，產生更有效率的路由。IPv6 也支援 anycast 的功能，可加快服務回應時間，並可有效的將流量負載分散。

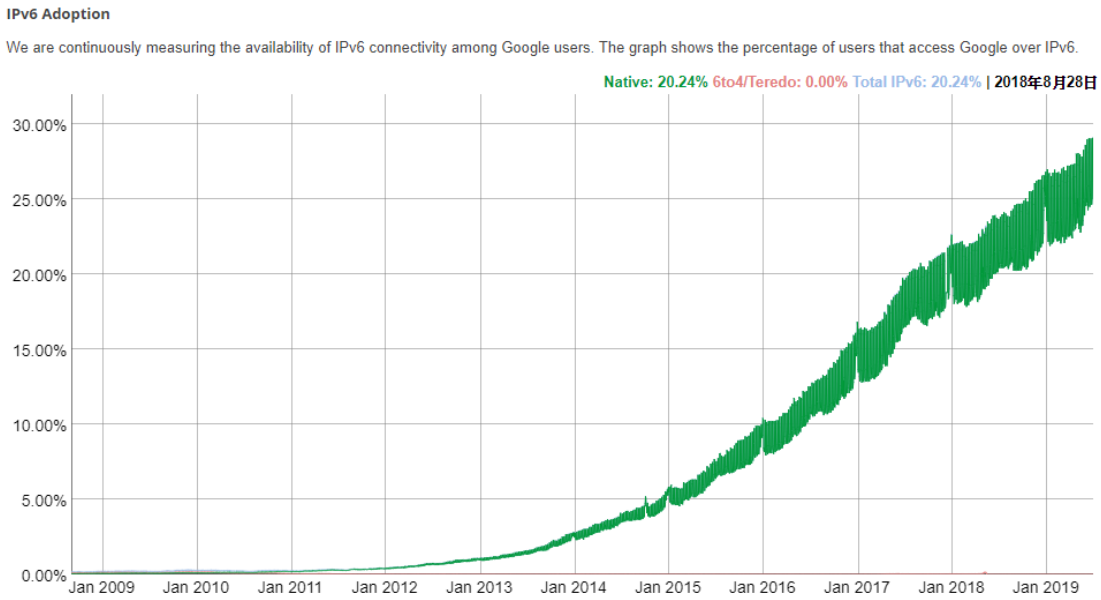
6、 服務品質的保證:IPv6 的標頭有兩項參數,資料流種類(traffic class)與資料流標記(flow label)，有助於服務品質控制機制的設計。

7、 更有效率的封包標頭處理:IPv6 簡化原先 IPv4 的標頭設計，雖然 IP 位址從原來的 32 位元變成 128 位元，但標頭長度僅成長兩倍且長度固定，這使得網路堆疊在處理封包標頭時可以更有效率。

8、 可擴充性：IPv6 設計時，以「下一標頭(Next Header)」的方式來增加標頭的可擴充性。使用者可以透過「下一標頭(Next Header)」的方式，在標頭中指示下一個標頭的內容，以利網路端或是接收端完成特定的工作,這樣的設計使得 IPv6 標頭具有更高的擴充性。

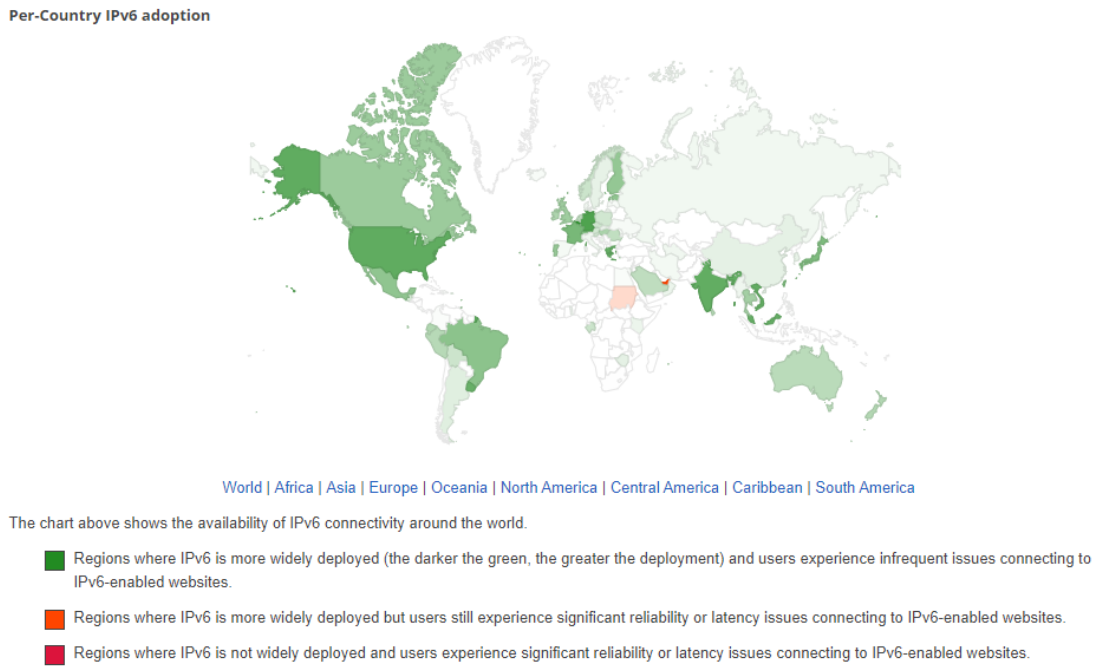
自 1998 年以來，IPv6 的發展已經歷經 20 個年頭，但在 2011 年前，全球 IPv6 的使用率幾乎毫無進展，直到 2011 年 6 月 8 日(世界 IPv6 日，World IPv6 Day)，由 Facebook、Google、Yahoo、Akamai 和 Limelight Networks 五家公司宣布了世界 IPv6 日,超過 400 家公司參與此活動，全球 IPv6 的佈建及使用狀況才漸漸露出曙光。即使如此，IPv6 的發展仍然相當緩慢。2015 年底，Google 統計的全球 IPv6

使用率才超過 5%，但之後每年成長率增加越來越快，預估 2019 年底可達 34%，由此可見 IPv6 已漸為主流趨勢。



資料來源：https://www.google.com/intl/en/IPv6/statistics.html

圖 1: Google IPv6 調查(全球)



資料來源：https://www.google.com/intl/en/IPv6/statistics.html

圖 2: Google IPv6 調查(國家)

圖 1 與圖 2 顯示 Google 最近的 IPv6 使用率的統計，圖 1 為全球趨勢，圖 2 則為各國 IPv6 的普及率。

由圖 2 可以看出台灣為深綠色，顯示在 Google 的調查裡，台灣 IPv6 的支援是較好的。

APNIC IPv6 量測網站(https://stats.labs.apnic.net/IPv6/)指出，2019 年 9 月，全球的 IPv6 Capable 的平均值約為 24%。美洲與亞洲均高於平均值，分別有 31%和 27%，歐洲和大洋洲低於平均值，分別為 17%和 18%，非洲則只有 2%，其他區域約 11%，如表 5 所示。亞洲來說，南亞最高，有 56%，東亞 18%，東南亞為 14%，如表 6 所示。

表 5、APNIC IPv6 使用調查-全球

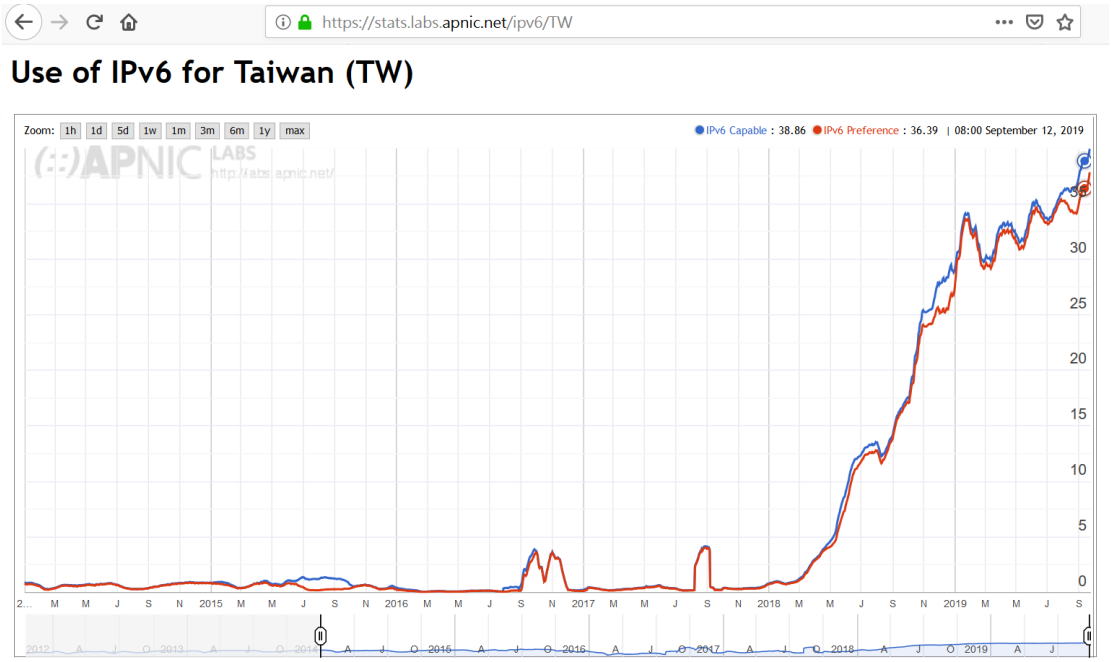
Region	IPv6 Capable	IPv6 Preferred
全球	24.29%	23.47%
美洲	31.06%	30.48%
歐洲	17.95%	17.61%
亞洲	27.70%	26.55%
大洋洲	18.71%	17.63%
非洲	2.00%	1.93%
其他	11.83%	11.82%

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

表 6、APNIC IPv6 使用調查-亞洲

SubRegion	IPv6 Capable	IPv6 Preferred
亞洲	27.70%	26.55%
南亞	55.92%	55.69%
東亞	17.87%	15.46%
東南亞	14.02%	13.77%
西亞	3.08%	3.02%
中亞	0.01%	0.00%

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



來源網址：https://stats.labs.apnic.net/IPv6/TW

圖 3: APNIC 調查台灣網路 IPv6 使用情形

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。今年 9 月，台灣 IPv6 Capable 的比例已上昇到 41%左右，IPv6 Preference 為 37%，全球排名第 7 名，前十名如表 7 所示。

表 7、APNIC IPv6 排名

	Country Code	Country	IPv6 Capable	IPv6 Preferred
1	IN	印度	69.63%	69.34%
2	BE	比利時	56.76%	56.23%
3	US	美國	55.01%	54.27%
4	YT	馬約特	52.65%	52.11%
5	DE	德國	41.44%	40.92%
6	MY	馬來西亞	41.15%	40.90%
7	TW	臺灣	41.01%	39.01%
8	VN	越南	39.75%	38.75%
9	GR	希臘	39.12%	38.91%
10	BL	聖巴泰勒米	37.06%	36.47%

(二) 物聯網的基礎架構介紹

1、 物聯網簡介

物聯網(IoT，Internet of Things)是網際網路、傳統電信網等資訊承載體，讓所有能行使獨立功能的普通物體實作互聯互通的網路。換句話說，物聯網就是將物體植入各種微型感應晶片，來賦予物體智慧化，並藉助無線網路，實現人與物、人與人、物與物之間的交流，使生活中任何物體都可以變得更有智慧，能夠自動回報狀態、自動與物溝通、自動與人溝通、更容易與人類互動以及更聰明地被人類使用，這種將各個智慧化物體連接起來的網路，就是物聯網。

隨著行動雲端、巨量資料與無線技術快速演進，促使智慧聯網應用的快速發展，物聯網的興起，結合大數據(Big Data)的分析為產業帶來了創新的變革與發展契機，可視為當代網路技術重要里程碑與未來潮流趨勢。

2、 物聯網的發展歷程

物聯網一詞是由 Auto-ID 實驗室的執行董事 Kevin Ashton 所創。Auto-ID 實驗室成立於 1999 年，除此之外，也是在物聯網領域領先全球研究網路的學術實驗室。有 GS1 作為他們主要的研究夥伴，他們協助發展了 EPC (產品電子碼，Electronic Product Code)，是以全球性 RFID (無線射頻辨識，Radio Frequency IDentification)為基礎的物品識別系統，目的是取代 UPC (通用商品碼，Universal Product Code)條碼。

在 2005 年，國際電信聯盟(ITU，International Telecommunication

Union)發表了對其專題的第一個報告《ITU 網際網路報告 2005：IoT》正式提出物聯網概念。該報告在細節裡詳盡的闡述關於 IoT 技術、市場機會、挑戰和顯示出的影響。

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。這個會議在蘇黎士召開，並且是第一個擁有一流的研究人員以及來自學術界和工業界的專家一起分享相關應用、研究結果和知識。

3、 物聯網架構

根據歐洲電信標準協會(ETSI，European Telecommunications Standards Institute)之定義，物聯網可依照不同的工作內容劃分為感知層、網路層及應用層。

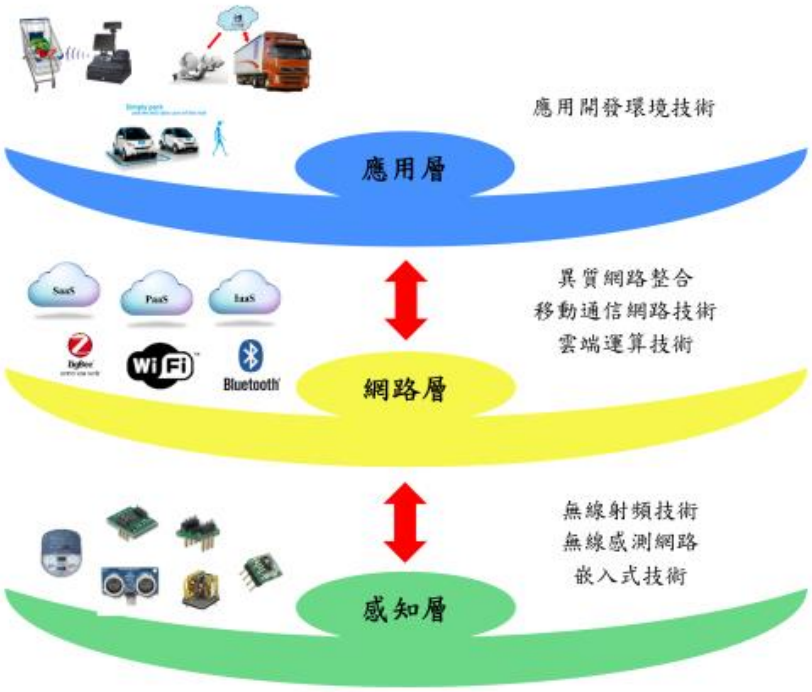


圖 4: ETSI 物聯網架構

(1) 感知層

感知層是物聯網發展的基礎，將各種具感測或辨識能力的元件，嵌入準備連結上網的各種真實物體，使其實體物件智慧化，進而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，使智慧物件具有感測環境變化或物體移動的能力。除了感測器外，針對實體物件嵌入具辨識能力的技術而言，最常見的是 RFID 技術，將 RFID 的標籤嵌入於物體，便可讓周遭設備得知自己的身分或狀態。其餘常見的辨識技術分別有條碼辨識技術 Bar Code、影像辨識技術 VID (Video Image Detection)、二維條碼辨識技術 QR Code 等等。

(2) 網路層

網路層有如人體結構中的神經，使智慧物件具有聯網能力，能夠將感測資訊傳遞至網際網路，除了分享這些即時且重要的資訊給適當的使用者外，亦能提供使用者遠端互動的功能。為達到此目的，通常會將無線通訊的能力嵌入智慧物件中，使其具有聯網能力，常見的無線通訊技術包括 Zigbee、藍牙、Wi-Fi、3G/4G 等，智慧物件透過無

線或有線的方式連結至網際網路，使人們可隨時掌握該物體的狀態或對該物體進行遠端操控，網路層可看作為感知層與應用層之間的溝通橋樑，用以將智慧物件所收集到的數據資料，透過網路傳送至雲端並進一步的進行儲存及有效地管理與運算，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，以更進一步的進行資料分析、資料探勘與資料整合。

(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。

4、 物聯網與 IPv6

當萬物連網的時代來臨，要能實際掌握裝置的狀況，裝置對 IP 的需求成為無可避免。可以從三個角度來討論物聯網和 IPv6 的關係。

(1) 安全性(Security)：當所有設備都連上網路，安全性成為物聯網應用需考慮的一大要務，面對駭客無所不用其極的威脅及

攻擊，在物聯網應用上將帶來更高複雜度的安全疑慮。IPv6 提供了比 IPv4 更好的安全解決方案，特別是 IPSec 的採用。

(2) 可擴充性(Scalability)：根據 Gartner 發布的一份報告，2015 年有 49 億台設備連接到網際網路，2020 年將成長到有 250 億設備，可以預見未來物聯網裝置的成長將難以估計。因為物聯網產品需要大量 IP，IPv6 相對 IPv4 是為更佳的選擇。

(3) 連結性(Connectability)：當數十億的設備連上物聯網後，如何允許網路設備相互連結就相當的重要。對於 IPv4，網路地址轉換(NAT，Network Address Translation)的使用就是一個阻礙網路設備互連的瓶頸。IPv6 顯然就比 IPv4 有優勢。

從 IP 的角度來看，目前的物聯網產品，主要有兩類：

- 裝置不使用 IP，使用私有的通訊協定連結到閘道器。
- 裝置使用 Private IP，透過 NAT，連結閘道器。

具體來說，雖然 IPv6 可以提供遠較 IPv4 更多的 IP 位址，且不需使用 NAT 來進行位址轉換。然而，物聯網生態系未完整，網路 IPv6 支援未完整，使用者需求不明顯的情形下，物聯網廠商實作支援 IPv6 的物聯網產品的意願不強。

從生態系來說，在大量佈署的考量下，裝置端的成本是一個不可忽略的因素，這些成本包含開發、認證、佈署、測試等等。因此，物聯網廠商選擇硬體(包含感測器和通訊晶片)時，IPv6 的支援並非主要的考量。同樣的，作業系統是否支援 IPv6，也非主要考量。許多情境裡，裝置端僅是簡單的上傳感測到的資料，或是具有一些簡單的設定功能，此時，裝置端是否擁有 IP，可否直接連上網際網路，並非首要考量。從而，物聯網廠商可以選擇讓裝置端不具備 IP 連網能力，而是透過閘道器作為中介，以私有通訊協定，來實現產品所需之功能。

即使較為高端的裝置具有使用 IP 連網的能力，當裝置端使用私有 IPv4 位址透過閘道器上的 NAT 轉換來完成網際網路的連線時，也通常能滿足許多物聯網的情境。目前，NAT 相關技術已經非常的成熟，結合其他 IPv4 相關的網際網路技術，可以提供包含虛擬網路、防火牆、負載平衡等多種功能。由於僅閘道器等少數設備需要 public IP 位址，在這樣的情境下，大多數的物聯網情境，並沒有一定要使用 IPv6 的必要性。

對物聯網廠商而言，當產品宣稱支援 IPv6 時，需要通過的認證項目也增加。同時，物聯網廠商在人才招募/培訓上，熟悉 IPv6 的人材也較難招募。即使產品具有 IPv6 連網能力，客戶所在的環境，其網路基礎建置上也不見得支援 IPv6。在佈署時，除非客戶特別指定需

要 IPv6，或是當時無法取得閘道器等相關設備所需的 IPv4 位址，IPv6 才是必須的。由前面章節裡所述的 IPv6 使用情形的調查來說，雖然許多區域已經大幅提高了網路基礎建設的 IPv6 支援能力，但還有許多區域，IPv6 的支援相對低落。在佈署時，這也會增加測試的困難度，對物聯網廠商與客戶而言，這並非是一個必要承擔的風險。

同樣的，由於 NAT 技術的成熟，這也使得客戶取得 public IPv4 的可能性提高。特別是早期已經取得不少 IPv4 位址的公司，藉由 NAT、雲端技術、網路虛擬化技術等等，過去許多主機佔用的 public IPv4 位址可以被釋放出來，加以重新利用。或者是建議使用公有雲，在之後的章節裡，我們可以看到，使用 Amazon AWS，Microsoft Azure 或 Google Cloud Platform IoT 時，可以使用非常少數的 public IPv4 位址來實作物聯網應用。

從以上分析來看，就已經擁有 IPv4 物聯網產品的廠商而言，開發支援 IPv6 的物聯網產品並非特別的困難。主要的問題在於客戶是否有明確的需求，以及實際佈署時，是否能夠取得足夠的 IPv4 位址。

在物聯網的應用情境裡，若裝置端有大量直接上網的需求，大量 public IPv4 位址取得不易時，問題才會突顯。此時，使用 IPv6 的急迫性就會出現。舉例來說，當物聯網產品與應用更加成熟時，跨公司/地域/領域的物聯網產品需要進一步的整合時，使用互通的通訊協定

是必要的，裝置之間可以直接互連是需要的，IPv6 的優勢可以突顯，物聯網廠商推出 IPv6 的物聯網產品趨勢會更加明顯。

5、 物聯網資訊安全考量

隨著物聯網的發展，相關的資訊安全問題也越來越被注意。在趨勢科技於 2019 公佈的資料說明，許多物聯網應用在設計之初，就沒有把資訊安全的考慮放進來，加上為了讓產品容易被一般客戶能夠輕易的使用，在相關的產品使用設定和安全設定上面也十分的簡略，這使得物聯網產品十分容易受到攻擊。

駭客可以從很多面向發動攻擊。如在硬體層，他們可以利用主機板上的一些除錯功能(如 JTAG UART、I2C 和 SPI)等方式進行入侵，或比如可以掃描燒在軔體上面的密碼、後門和弱點。可以從物聯網裝置使用的內嵌式作業系統、網路堆疊的漏洞入侵系統。許多物聯網產品可能使用的網路堆疊實作可能是私有的或是不常見的，其安全並沒有保證。而一般來說，要對已經佈署在場域裡的物聯網裝置進行更新作業是有一定的困難，而使用這些物聯網產品的客戶也可能沒有相關的資安意識或能力進行系統更新。駭客也可以利用物聯網應用伺服器(如 Web 伺服器)，使用如 SQL Injection 等技術入侵。

表 8、物聯網可能的安全議題和風險

攻擊點	安全議題	風險
硬體	容易被拆解和檢視 除錯埠	駭客使用這些除錯埠(JTAG UART)等侵入系統
韌體	機密資料 後門 未更新 Buffer Overflow 攻擊 權限升級	韌體可能燒入相關的憑證資料、預設密碼、除錯用的後門 駭客可以掃描上述機密、後門，進而輕易侵入系統
作業系統與應用軟體	Buffer Overflow 攻擊 權限升級 未更新 中間人攻擊	裝置更新系統困難，駭客可利用作業系統漏洞入侵，取得系統權限
Web 介面	SQL Injection Directory Traversal Buffer Overflow 攻擊 Cross-site Scripting Corss-site Request forgery 預設或樣本頁面 權限升級 其他 OWASP issues	駭客可以不需密碼取得系統控制權 駭客可以取得系統資訊，如內部系統架構(IP 使用)、目錄架構、資料庫架構與內容
網路協定堆疊	DoS or DDoS Session hijacking	駭客可以讓裝置或系統失效 駭客可以攔截網路會

	Authentication bypass MAC spoofing attacks PIN cracking attacks 中間人攻擊 Hard-coded key attacks Replay attacks	話並傳送假造的資料 駭客可以偷取資料或機密
政策	錯誤的設定政策 政策未被遵守	駭客可以取得敏感資料 駭客可以無限制的使用系統 在無意間洩漏敏感資料

6、 台灣物聯網資安標章

我國為面對各種物聯網資安挑戰，協助物聯網產業發展，在行政院科技會報暨行政院資通安全處指導下，推動建立國內物聯網廠商遵循之安全檢驗標準，以提高產品安全與消費者信心。由經濟部負責具有線介面之物聯網終端產品資安檢測，由國家通訊傳播委員會主責具無線介面或電信/傳播終端設備介面者。相互合作，制訂物聯網設備資安測試標準、檢測環境及輔導廠商產品進行資安檢測等業務，以建置產品淬煉場域，協助產業進軍國際。

台灣物聯網資安標章制度目的如下：

(1) 落實各類型物聯網資安測試規範，推動物聯網產品與設備商落實資安檢測。

(2) 推動物聯網資安驗證制度，強化物聯網安全。

(3) 建立物聯網資安標章制度，使消費者易於識別通過本資安驗證制度檢測之物聯網設備。

物聯網資安標章驗證制度為行政院科技會報與行政院資通安全處的指導下，由國家通訊傳播委員會與經濟部合作建立。標章安全等級依據(1)資安風險高低、(2)資安技術防護複雜度，分為 1 級、2 級、3 級，標章設計為提供物聯網產品與服務如堡壘般的安全防護機制。通過驗證取得標章的產品，能在國內成為公部門優先採購的安全產品。

	初階1星	中階2星	高階3星
圖示			
安全等級	1級	2級	3級
說明	適合一般家庭使用	適合商業用途使用	最高防護強度

資料來源：http://www.ifantech.net/taics/Validation01.aspx?validateType_id=2#Validation

圖 5: 物聯網資安標章

目前，有 8 個影像監控系統相關的資安標準，3 個無線/混合型網路攝影機相關的資安標準，列舉如下。

表 9、TAICS 資安標準

認驗證制度規章	
1	物聯網資安認驗證制度—影像監控系統 V1.0
影像監控系統資安標準	
1	TAICS TS 0014-1 v1.0-影像監控系統資安標準-第一部:一般要求
2	TAICS TS 0014-2 v2.0-影像監控系統資安標準-第二部:網路攝影機
3	TAICS TS 0014-3 v1.0-影像監控系統資安標準-第三部:影像錄影機
4	TAICS TS 0014-4 v1.0-影像監控系統資安標準-第四部:網路儲存裝置
5	TAICS TS-0015-1 v1.0-影像監控系統資安標準測試規範-第一部:一般要求
6	TAICS TS-0015-2 v2.0-影像監控系統資安標準測試規範-第二部:網路攝影機-01
7	TAICS TS-0015-3 v1.0-影像監控系統資安標準測試規範-第三部:影像錄影機
8	TAICS TS-0015-4 v1.0-影像監控系統資安標準測試規範-第四部:網路儲存裝置
無線/混合型網路攝影機	
1	無線網路攝影機資通安全檢測技術指引
2	具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引
3	具網際網路連線功能之固定通信多媒體內容傳輸平臺及有線廣播電視機上盒資通安全檢測技術指引_總說明及逐點說明

(三) 5G 的基礎介紹

第五代行動通訊技術(5th generation mobile networks，5G)是最新一代蜂窩行動通訊技術，是 4G (LTE-A、WiMax)、3G (UMTS、LTE) 和 2G (GSM)系統後的延伸。

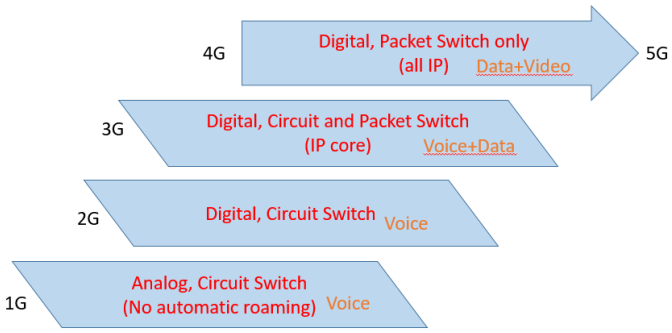


圖 6: 行動通訊技術演進

5G 的效能目標是高資料速率、減少延遲、節省能源、降低成本、提高系統容量和大規模裝置連接。

1、 5G 定義

下一代行動網路聯盟（Next Generation Mobile Networks Alliance）定義了 5G 網路的以下要求：

(1) 以 10Gbps 的資料傳輸速率支援數萬用戶

(2) 以 1Gbps 的資料傳輸速率同時提供給在同一樓辦公的許多人

(3) 支援數十萬並發連接以用於支援大規模傳感器網路的部署

(4) 頻譜效率應當相比 4G 被顯著增強；

(5) 覆蓋率比 4G 有所提高；

(6) 信號效率應得到加強；

(7) 延遲應顯著低於 LTE。

3GPP 工作組分為 RAN (Radio Access Networks)、SA (Servuce abd System Aspects)以及 CT (Core Network & Terminals)三大領域，RAN 主要負責無線接入網路相關的內容，SA 主要負責業務和系統概念等相關的內容，CT 負責核心網和裝置等相關的內容。

Release-15 (簡稱 R15)標準是第一階段全功能版本。R15 中的 5G 規範的第一階段是為了適應早期的商業部署。Release-16 的第二階段將於 2020 年 4 月完成，作為 IMT-2020 技術的候選提交給國際電信聯盟。

R15 標準包括 NSA (Non-Standalone)和 SA (Standalone)兩種標準，NSA 於 2017 年 12 月完成，2018 年 3 月凍結。NSA 是 SA 標準的過渡。NSA 有利於保護營運商目前的投資，以現有的 4G 接入網以及核心網涵蓋為錨點，新增 5G 無線組網接入標準。NSA 這樣做沒有獨立信號(Signaling)，主要目的是為了提升特定區域頻寬。

R15 是 5G 第一版成型的商業化標準，與後續推進的 R16 標準也有一定協同性。

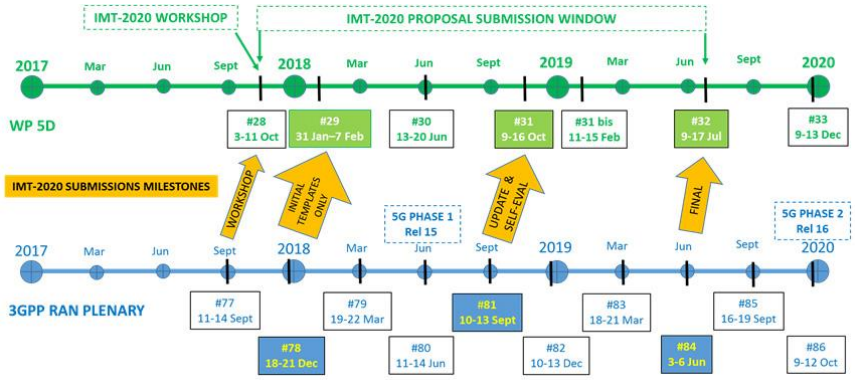


圖 7: 5G 標準化時程

5G 網路的主要優勢在於，資料傳輸速率遠遠高於以前的蜂巢式網路，最高可達 10 Gbit/s，比目前的有線網際網路要快，比先前的 4G LTE 蜂巢式網路快 100 倍。另一個優點是較低的網路延遲(更快的回應時間)，低於 1 毫秒，而 4G 為 30-70 毫秒。

5G 與 4G 相比的技術創新如下：

(1) 5G 採用 512-QAM 或 1024-QAM 或更高的資料壓縮密度調變/解調變器，頻譜效率更高，提高更多傳輸速率。目前 4G 使用 256-QAM 或 64-QAM 的調變以壓縮傳輸資料。

(2) 5G 將採用 28GHz 毫米波通訊。目前 4G 使用 700MHz、900MHz、1800Mhz、2600Mhz 等頻段，雖然電波繞射能力比較高但是在低頻上頻譜資源卻相當有限。高頻的毫米波大

多是軍用戰鬥機雷達或測速照相等少數裝置，頻譜寬度更高，更容易找到連續頻譜，空白頻譜容易取得。

(3) 波束指向配合多輸入多輸出(Multi-input Multi-output，MIMO)相控陣列天線。MIMO 多輸入多輸出利用電磁波的空間多工和路徑不同多天線系統提高傳輸速率，類似在軍用領域的技術將延伸出的商用技術版本。

(4) 波束自適應和波束成形，能夠提高特定方向的波辦優化傳輸距離。

(5) 新材料將使用 GaN 氮化鎵或是 GaAs 砷化鎵材料的 RF 射頻天線和功率放大器，此材料的 RF 射頻天線能在更高的頻段有更高的能源效率，裝置會比較省電。

(6) 為了適應工業物聯網、無人駕駛汽車、商用無人機等新技術的應用，網路延遲時間將降低到 1 毫秒以下。

2、 5G 核心技術

為了強化行動裝置的訊號強度，NR (New Radio)運用結合類比與數位波束賦形的技術。由於今日的 LTE 網路廣泛運用數位波束賦形技術，因此在行動通訊領域，這項技術並非全新概念。然而在 5G 應用上，為了達到訊號傳播目的並將天線體積縮小，業界開始使用廣泛

的類比波束賦形技術。在 24 GHz 以上的頻譜，採用類比波束賦形技術的較窄波束寬度，能讓 5G 基地台更有效率地引導下鏈訊號。這項程序首先必須掃描波束，讓基地台得以針對特定行動裝置的需要，找出最有效的波束位置。透過這項方式，下鏈傳輸訊號的接收方可獲得更高的訊號強度；對透過更高階調變機制進行傳輸的接收方來說，這項效益尤其明顯。然而，波束賦形技術最終還是帶來了重大的測試挑戰；每一個波束不只需要進行特性參數描述並經過測試，更需要透過空中傳輸量測來驗證無線電效能。

5G 第一階段仍將採用 OFDM 波形，5G 有許多候選波形，但是 NR 的第一階段仍將使用正交分頻多工(OFDM)版本。用於 5G NR 下鏈的特定 OFDM 版本，是循環式前置區段；而 OFDM 也是 LTE 用於下鏈訊號的相同波形。然而，與 LTE 不同的是，5G NR 在上鏈中使用基於 CP-OFDM 與 DFT-S-OFDM 的波形。另一個與 LTE 不同的地方是 5G NR 允許變化極大的子載波間距。LTE 子載波間距幾乎都落在 15 kHz，但 5G NR 卻能給予較多彈性，讓子載波間距訂為 15 kHz x 2n。在 5G NR，可允許的最大子載波間距為 240 kHz，並保留給使用 400 MHz 載波頻寬的情況使用。

3、 5G 應用

5G 支援三大應用場景：(1)增強型行動寬頻(eMBB)、(2)超可靠低延遲(URLLC)、和(3)大量機器類通訊(mMTC)。車聯網、行動醫療、工業 4.0 等以往存在於概念或者只是初步智慧化的場景應用，有 5G 做為支撐才有可能發揮出最大的潛力。例如，道路上車輛中的電腦可以通過 5G 連續不斷地相互通訊，也可以連續不斷地與道路通訊。

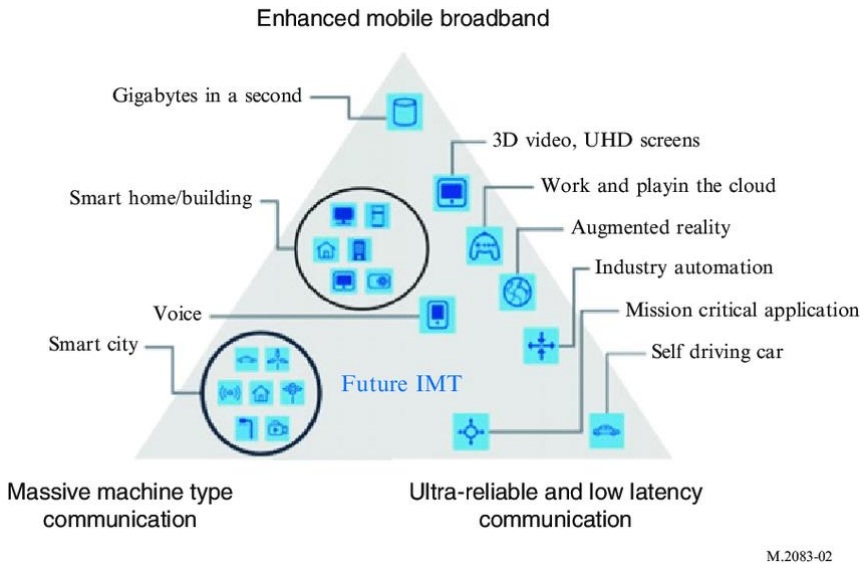


圖 8: 5G 的 3 大應用場景

未來 5G 以更多的高速率、低延遲、超大連接的解決方案為主要應用。目前，比較重要的方向在下面幾個。

(1) 高解析度影像直播：在智慧交通、災難探勘、災難救援、場域影像監控等情境下，高解析度影像直播有實質上的意義。行動網路的上傳頻寬在一般情形下並不高，5G 網路的高頻寬、低延遲特性較 4G 網路容易完成高速的影像上傳。無法

排除超高速下載高解析度影片的潛在需求，但一般情境(如下載電影)的需求量是否達到一定水準則仍有待未來商業運轉後驗證。

(2) AR/VR 沈浸式體驗：在遠距醫療、遠距維修、遠距教學等應用中，比如透過 AR/VR 教導遠方的工程師完成特定的維修任務，5G 網路的高頻寬、低延遲特性更容易完成這些應用。

(3) 廣域監控，如農業、森林、河川、海洋等應用裡，5G 網路可以更容易的透過網路功能虛擬化來支援。

4、 5G 商業運轉

目前，以 R15 標準 NSA (Non-Standardalone，使用 4G 核心網路)為基礎，全球主要先進國家紛紛展開測試，部份行動服務業者在選定區域也開始商業運轉。表 10 列出部份國家 5G 釋照與商轉時程，表 11 列出部分國家 5G 商業活動。

表 10、5G 釋照與商轉時程

國家/地區	**5G 釋照與商轉時程**
卡達	2018 年 5 月
愛沙尼亞	2018 年 6 月

芬蘭	2018 年 6 月
美國	2018 年 10 月
韓國	2018 年 12 月
澳洲	2018 年 12 月
英國	2019 年 5 月底
日本	2019 年 4 月釋出 5G 頻譜
中國	2019 年 6 月初釋出商業執照
台灣	預計 2019 年底到 2020 年 1 月釋出頻譜

表 11、5G 商業活動

國家	**商業活動**
美國	2018 年 1 月，AT&T 宣佈其計畫在美國 12 個城市部署 5G 網路。 2018 年 9 月，AT&T 宣佈將在 2018 年底之前在另外 5 個城市部署 5G 網路，5G 行動服務。 2018 年 6 月，AT&T 公佈了一項位於印第安那州南本德的固定無線 5G 試驗，利用該公司的全光纖寬頻網路和毫米波（mmWave）頻譜。

	2018 年 4 月，AT&T 和 Crown Castle 簽署了一項新協定，簡化和擴充其無線網路基礎設施的長期租賃協議。
中國	2018 年 11 月，中國移動和華為實現了首例基於 5G 的 8k VR 直播。 2018 年，英特爾與百度、中國移動、中國電信、中國聯通、華為等合作開發 5G 系統。 2016 年，三星成功與中國移動進行了 5G 樣機試驗。
韓國	2018 年 4 月，印度在與韓國討論共同建立 5G 測試實驗室。 2018 年 10 月，三星和高通宣佈在 5G 小型基地站開發方面建立合作夥伴關係。 2018 年 10 月，三星和 NEC 公司宣佈了 5G 合作夥伴關係。將為行動營運商提供靈活的 5G 解決方案，提供客製化服務以有效滿足行動通訊服務商的需求。 2018 年 2 月，愛立信和韓國電信與英特爾一起進行了 5G 試驗，將汽車與現場的 5G 網路連接起來。試驗位置在首爾市中心，將愛立信的 5G 無線電試驗系統與英特 5G 汽車試驗平臺結合使用。
日本	富士通和愛立信正在合作開發和製造 5G 基地站。

	三星和 NEC 正在合作開發和製造 5G 基地站。
歐洲	2017 年 9 月，英特爾在歐洲開展了首個展示產業應用案例的公共 5G 網路的測試，其中第一個將是乘客在游輪上的高速連接。 2018 年 2 月，Orange、三星電子和思科宣佈將在 2018 年下半年開始在羅馬尼亞的多個家庭合作進行 5G 毫米波試驗。 2018 年 6 月，諾基亞與 Orange 合作在波蘭完成了現場網路測試，以驗證雲端優化無線接入網路對於順利演進到下一代 5G 技術的好處。
台灣	聯發科技正在研發 5G 無線數據機”Helio M70”，產品將於 2019 年進行商用部署。 中華電信與愛立信和諾基亞就 5G 項目簽署了諒解備忘錄（MoU）。 臺灣已與歐盟達成協議，以協助開發 5G 無線系統。 遠傳電信以及鴻海精密工業公司的附屬公司亞太電信正計畫建立單獨的 5G 聯盟。

二、物聯網、5G 與 IPv6 國際技術標準簡介

IPv6 已經成為 5G、IoT、SDN (Software-Defined Network)/NFV

(Network Functions Virtualization)、雲端計算以及邊緣計算等新興技術的基礎。大量的終端設備連網產生了大量的地址需求，使用傳統 NAT 的方式無法有效支援新的 5G 及物聯網應用。

有關 IPv6 的網際網路標準協定，因應產業環境不斷的變化，因此不斷有新的草案的討論及標準協定的修正版本在進行。目前，IETF 有 General Area (gen, 3 WG)、Applications and Real-Time Area (art, 30 WG)、Internet Area (int, 16 WG)、Operations and Management Area (ops, 13 WG)、Routing Area (rtg, 23 WG)、Security Area (sec, 22 WG)、Transport Area (tsv, 11 WG)共 7 個領域，超過 100 個活躍工作小組。IETF 的每一個工作小組，同時會有數個草案同時在進行討論。

本計畫將持續蒐集與研析物聯網與 IPv6 相關技術的國際標準協定(RFC)，內容解析，以期對技術有更深入的了解，並掌握重點技術的發展動向，強化技術能量。

(一) IETF 物聯網相關工作小組

因應物聯網的發展，就網際網路相關的協定的需求，IETF 也成立了相關的工作小組，對物聯網在網路連網環境相關議題進行討論，且已經公布了第一波所制定的標準。除此之外，際網路研究工作小組(IRTF，Internet Research Task Force)於 2015 年成立了物聯網專門研究

小組(T2TRG，Thing-to-Thing)，以調查物聯網的開放性研究問題。

物聯網相關的工作小組資料，如下表所列。

表 12、物聯網相關的工作小組列表

Working Group	Name	Area	Status
6lo/ 6LoWPAN	IPv6 over Networks of Resource-constrained Nodes ● 使用 6LoWPAN 的 IPv6-over-foo 適配層規範鏈路層技術，適用於受限制網路與節點的規範。	Internet	Active
6tisch	IPv6 over the TSCH mode of IEEE 802.15.4e ● 專注於通過 TSCH 模式啟用 IPv6。	Internet	Active
ipwave	IP Wireless Access in Vehicular Environments ● 致力於 V2V (Vehicle-to-vehicle)和 V2I (Vehicle-to-Internet)的網路使用情境，並將開發基於 IPv6 的直接和安全網路連接，以解決車輛與其他車輛或固定系統之間的網路連接問題。這些車載網路的特點是動態變化的網路拓撲和連通性。	Internet	Active
lpwan	IPv6 over Low Power Wide-Area Networks ● 製作一份介紹性文件，描述和關聯一些精選的 LPWAN 低功耗廣域網路技術 ● 生成標準以啟用壓縮和 LPWAN 網路上的 CoAP / UDP / IPv6 資料封包。	Internet	Active
lwig	Light-Weight Implementation Guidance ● 收集受限制設備中 IP protocal stack 的實現經驗。僅專注於實際使用的技術實施，並且不影響與其他設備的互操作性。	Internet	Active
homenet	Home Networking ● 該小組的任務是產生一個架構文件，概述如何建構涉及多個路由器的家庭網路，以及子網。	Internet	Active
roll	Routing Over Low power and Lossy networks	Routing	Active

	● 致力於家庭、建築物、都會網路中感測裝置的路由問題。這些裝置的能源、記憶體和計算資源都相當的受限，使用不同的實體網路技術。		
ace	Authentication and Authorization for Constrained Environments ● 目標在產生標準的認證與授權方法，可以在受限制網路中存取一個由 URI 指定的資源。伺服器與客戶端都可能是受限制的，預設使用 CoAP 與 DTLS。	Security	Active
cose	CBOR Object Signing and Encryption ● COSE (RFC 8152)描述如何將 CBOR (RFC 7049)物件進行簽章與加密。	Security	Active
suit	Software Updates for Internet of Things ● 專注於 IoT 裝置中如何安全的進行韌體更新的解決方案。	Security	Active
dice	DTLS In Constrained Environments ● 致力於在受限制環境中支援 DTLS Transport-Layer Security 的解決方案，以支援 CoAP。	Security	Concluded
cbor	Concise Binary Object Representation Maintenance and Extensions ● Concise Binary Object Representation (COBR)延伸 JavaScript Object Notation (JSON)資料交換格式，以支援可擴充的二進制資料表示格式。	Applications and Real-Time	Active
core	Constrained RESTful Environments ● 建立一個能在受限制環境中執行的資源導向應用軟體框架 CoAP。	Applications and Real-time	Active
Research Group	**Name**		**Status**
t2trg	Thing-to-Thing research group ● 探索開放的研究議題，以期能真正的實現物聯網，特別是讓資源受限的受限制節點可以彼此互連或與 Internet 相連。		Active

(二) IETF 物聯網相關 RFC

在這個研中中，我們從相關的小組中，整理 IETF 物聯網相關 RFC 共 81 篇，列表如下。

表 13、物聯網相關 RFC 列表

編號	RFC	名稱	狀態	時間	Working Group
1	4919	IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals	Informational	2007/04	6lo 6LoWPAN
2	4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks	Standards Track Updates by RFC 6282, 6775, 8025, 8066	2007/09	6lo 6LoWPAN
3	5548	Routing Requirements for Urban Low-Power and Lossy Networks	Informational	2009/05	roll
4	5673	Industrial Routing Requirements in Low-Power and Lossy Networks	Informational	2009/10	roll
5	5826	Home Automation Routing Requirements in Low-Power and Lossy Networks	Informational	2010/04	roll
6	5867	Building Automation Routing Requirements in Low-Power and Lossy Networks	Informational	2010/06	roll
7	6206	The Trickle Algorithm	Informational	2011/03	roll
8	6282	Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks	Standards Track Updates RFC 4944	2011/09	6lo 6LoWPAN
9	6550	RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks	Standards Track	2012/03	roll
10	6551	Routing Metrics Used for Path Calculation	Standards Track	2012/	roll

		in Low-Power and Lossy Networks		03	
11	6552	Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)	Standards Track	2012/03	roll
12	6553	The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams	Standards Track	2012/03	roll
13	6554	An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)	Standards Track	2012/03	roll
14	6568	Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	Informational	2012/04	6lo 6LoWPAN
15	6574	Report from the Smart Object Workshop	Informational	2012/04	iab
16	6606	Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing	Informational	2012/05	6lo 6LoWPAN
17	6687	Performance Evaluation of the Routing Protocol for Low-Power and Lossy Networks (RPL)	Informational	2012/10	roll
18	6690	Constrained RESTful Environments (CoRE) Link Format	Standards Track	2012/08	core
19	6719	The Minimum Rank with Hysteresis Objective Function	Standards Track	2012/09	roll
20	6775	Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	Standards Track Update 4944	2012/11	6lo 6LoWPAN
21	6997	Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks	Experimental	2013/08	roll
22	6998	A Mechanism to Measure the Routing Metrics along a Point-to-Point Route in a Low-Power and Lossy Network	Experimental	2013/08	roll
23	7049	Concise Binary Object Representation (CBOR)	Standards Track	2013/10	cbor
24	7102	Terms Used in Routing for Low-Power and Lossy Networks	Informational	2014/01	roll

25	7228	Terminology for Constrained-Node Networks	Informational	2014/05	lwig
26	7252	The Constrained Application Protocol (CoAP)	Standards Track	2014/06	core
27	7368	IPv6 Home Networking Architecture Principles	Informational	2014/10	homenet
28	7388	Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	Standards Track	2012/07	6lo
29	7390	Group Communication for the Constrained Application Protocol (CoAP)	Experimental	2014/10	core
30	7397	Report from the Smart Object Security Workshop	Informational	2014/12	iab
31	7400	6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	Standards Track	2014/12	6lo
32	7416	A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)	Informational	2015/01	roll
33	7428	Transmission of IPv6 Packets over ITU-T G.9959 Networks	Standards Track	2015/02	6lo
34	7452	Architectural Considerations in Smart Object Networking	Informational	2015/03	iab
35	7547	Management of Networks with Constrained Devices: Problem Statement and Requirements	Informational	2015/05	opsawg
36	7548	Management of Networks with Constrained Devices: Use Cases	Informational	2015/05	opsawg
37	7554	Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement	Informational	2015/09	6tisch
38	7641	Observing Resources in the Constrained Application Protocol (CoAP)	Standards Track	2015/09	core
39	7650	A Constrained Application Protocol (CoAP) Usage for REsource LOcation And Discovery (RELOAD)	Standards Track	2015/09	core

40	7668	IPv6 over BLUETOOTH(R) Low Energy	Standards Track	2015/10	6lo
41	7695	Distributed Prefix Assignment Algorithm	Standards Track	2015/11	homenet
42	7731	Multicast Protocol for Low-Power and Lossy Networks (MPL)	Standards Track	2016/02	roll
43	7732	Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL)	Informational	2016/02	roll
44	7733	Applicability Statement: The Use of the Routing Protocol for Low-Power and Lossy Networks (RPL) Protocol Suite in Home Automation and Building Control	Standards Track	2016/02	roll
45	7744	Use Cases for Authentication and Authorization in Constrained Environments	Informational	2016/01	ace
46	7774	Multicast Protocol for Low-Power and Lossy Networks (MPL) Parameter Configuration Option for DHCPv6	Standards Track	2016/03	roll
47	7787	Distributed Node Consensus Protocol	Standards Track	2016/04	homenet
48	7788	Home Networking Control Protocol	Standards Track	2016/04	homenet
49	7815	Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation	Informational	2016/03	lwig
50	7925	Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things	Standards Track	2016/07	dice
51	7959	Block-Wise Transfers in the Constrained Application Protocol (CoAP)	Standards Track Updates 7252	2016/08	core
52	7967	Constrained Application Protocol (CoAP) Option for No Server Response	Informational	2016/08	core
53	7973	Assignment of an Ethertype for IPv6 with Low-Power Wireless Personal Area Network (LoWPAN) Encapsulation	Informational	2016/11	6lo
54	8025	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging	Standards Track Update RFC	2016/11	6lo

		Dispatch	4944		
55	8036	Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks	Standards Track	2017/01	roll
56	8065	Privacy Considerations for IPv6 Adaptation-Layer Mechanisms	Informational	2017/02	6lo
57	8066	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines	Standards Track Updates RFC 4944, RFC 6282	2017/02	6lo
58	8075	Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP)	Standards Track	2017/02	core
59	8105	Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)	Standards Track	2017/05	6lo
60	8132	PATCH and FETCH Methods for the Constrained Application Protocol (CoAP)	Standards Track	2017/04	core
61	8138	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header	Standards Track	2017/04	roll
62	8148	Next-Generation Vehicle-Initiated Emergency Calls	Standards Track	2017/05	ecrit
63	8152	CBOR Object Signing and Encryption (COSE)	Standards Track Possible Obsolete soon	2017/07	cose
64	8163	Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks	Standards Track	2017/05	6lo
65	8180	Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration	Best Current Practice BCP 210	2017/05	6tisch
66	8230	Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages	Standards Track	2017/09	cose
67	8240	Report from the Internet of Things Software Update (IoTSU) Workshop 2016	Informational	2017/09	IoTSU
68	8272	TinyIPFIX for Smart Meters in Constrained	Informational	2017/	6lo

		Networks		11	6LoWPAN ipfix
69	8323	CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets	Standards Track Updates RFC 7641, RFC 7959	2018/02	core
70	8352	Energy-Efficient Features of Internet of Things Protocols	Informational	2018/04	lwig
71	8375	Special-Use Domain 'home.arpa.'	Standards Track	2018/05	homenet
72	8376	Low-Power Wide Area Network (LPWAN) Overview	Informational	2018/05	lpwan
73	8387	Practical Considerations and Implementation Experiences in Securing Smart Object Networks	Informational	2018/05	lwig
74	8392	CBOR Web Token (CWT)	Standards Track	2018/05	ace
75	8428	Sensor Measurement Lists (SenML)	Standards Track	2018/08	core
76	8477	Report from the Internet of Things (IoT) Semantic Interoperability (IOTSI) Workshop 2016	Informational	2018/10	IoTSU
77	8480	6TiSCH Operation Sublayer (6top) Protocol (6P)	Standards Track	2018/11	6tisch
78	8505	Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery	Standards Track Updates RFC 6775	2018/09	6lo
79	8539	Softwire Provisioning Using DHCPv4 over DHCPv6	Proposed Standard	2019/03	dhc
80	8576	Internet of Things (IoT) Security: State of the Art and Challenges	Informational	2019/04	IRTF
81	8585	Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service	Informational	2019/05	v6ops

以下，將這 81 篇 RFC 分為下列 5 個類別，研討會概述(4 篇)、

概念型(17 篇)、應用層(14 篇)、資訊安全(9 篇)、網路層與傳輸層(37 篇)。

1、 研討會概述 (4 篇)

(1) RFC 6574：概述網際網路架構委員會(IAB)舉辦的關於將智慧對象與網際網路連接研討會的結論和建議。

(2) RFC 7397：總結 2012 年 3 月 23 日在巴黎舉行的智慧對象安全研討會的討論情況，並列出了網際網路工程任務組(IETF)社群的結論和建議。

(3) RFC 8240：概述 2016 年 6 月 13 日和 14 日在愛爾蘭都柏林聖三一學院舉辦的物聯網軟體更新(IoTSU)研討會。研討會的主要目標是促進對需求的討論，挑戰以及為物聯網設備帶來軟體和韌體更新的解決方案。

(4) RFC 8477：概述了物聯網(IoT)語義互操作性(IOTSI)研討會，研討會的主要目標是促進討論公司和標準開發組織(SDO)用於在應用層實現互操作性的不同方法。

2、 概念型 RFC (17 篇)

(1) RFC 4919：詳述了在 IEEE 802.15.4 網路上傳輸 IP 的假設，問題陳述和目標。本文列舉的目標集僅屬於初始集。

(2) RFC 5548：設定一組 IPv6 路由需求，以反映和其他都會低功耗有損網路(U-LLN)的特定特徵。

(3) RFC 5673：分析工業用低功耗有損網路(LLN)場域設備使用的路由協定的功能需求。如廣泛部署的低成本無線設備將顯著提高工業設備的生產和安全性。

(4) RFC 5867：根據低功耗有損網路(LLN)的路由解決方案，定義大樓自動化的 IPv6 路由要求。

(5) RFC 5826：介紹低功耗有損網路路由(ROLL)於家庭控制和自動化應用的特定需求。

(6) RFC 6568：研究低功耗無線個人網路(LoWPAN)的潛在應用場景和案例。

(7) RFC 7102：LLN 通常由許多嵌入式設備組成，這些嵌入式設備具有通過各種連結互連的有限功率、記憶體和處理資源，本文提供路由要求和術語解決方案中使用的術語表。

(8) RFC 7228：針對受限制節點和受限制網路進行各種術語的定義與說明，包含 LLN 與(6)LoWPAN，用以協助標準化。也說明了受限制裝置的分級，電力術語，能源限制分級，電力策略等。

(9) RFC 7548：討論涉及受限制設備的網路管理的案例。

(10) RFC 7368：定義基於 IPv6 的家庭網路的通用架構，描述相關的原則，注意事項和要求。

(11) RFC 7788：介紹了家庭網路控制協定（HNCP），可擴充的配置協定以及對家庭網路設備的一組要求。

(12) RFC 7388：定義管理資訊庫(MIB)的一部分，用於網際網路社群中的網路管理協定。

(13) RFC 7452：提供工程師設計連接網際網路的智慧對象指導原則。

(14) RFC 7547：提供了問題說明，部署和管理拓撲選項，以及針對涉及受限制設備的網路管理的不同使用案例的要求。

(15) RFC 8376：概述 LPWAN 技術集訊息, 這些技術的需求與在 LPWAN 中運行 IP 的目標之間存在的差異。介紹 LPWAN 技術(LoRaWAN、NB-IoT、Sigfox、Wi-SUN)。

(16) RFC 8352：總結用於節能網路的主要連結層技術，並強調這些技術對上層協定的影響，以便能夠共同實現節能行為。

(17) RFC 7733：為選擇和使用低功耗有損網路路由協定(RPL)套件中的協定提供指導原則，以實現建築和家庭環境中控制所需的功能。

3、 應用層 RFC (14 篇)

(1) RFC 7049：許多物聯網應用 JSON 來傳輸資料，CBOR 定義如何將 JSON 這種純文字的資料轉為二進制的方式來儲存。

(2) RFC 7252：CoAP 是一種專門的 web 傳輸協定，用於受限制節點和受限制網路, 包含應用模型(訊息傳遞、請求/響應等)、訊息格式，資料傳輸(可靠、不可靠等等)。

(3) RFC 7641：規定了 CoAP 的簡單協定擴充，使 CoAP 客戶端能夠“觀察”資源，即檢索資源的表示並在一段時間內保持服務器更新該表示。

(4) RFC 7959：此規範更新了 RFC 7252。不支援這些選項的 CoAP 實現通常受限於可交換的表示的大小，因此期望塊選項將在 CoAP 實現中廣泛使用。

(5) RFC 7967:該規範引入了一個名為“無響應”的 CoAP 選項。本文還討論了一些受益於此選項的應用程序範例。

(6) RFC 8132：該規範定義了新的 CoAP 方法，FETCH，PATCH 和 iPATCH，用於訪問和更新資源的一部分。

(7) RFC 8323:概述在 TCP、TLS 和 WebSockets 傳輸上使用 CoAP 所需的更改。且更新了 RFC 7641 以使用這些傳輸，和 RFC7959，以便在可靠傳輸上能使用的更長訊息。

(8) RFC 8075：提供了實現跨協定網路代理的參考資訊，該代理執行從 HTTP 協定到受限制應用協定(CoAP)的轉換。

(9) RFC 7390：詳述了在 IP 群播上使用 CoAP 的方法。另外也提供了多種案例和對應的協定流程來說明重要概念，以及在各種網路拓撲中部署的指導原則。

(10) RFC 7650：定義 REsource LOcation And Discovery(RELOAD)的限制應用程序協定(CoAP)用法。

(11) RFC 6690：基於 RFC 5988 中定義的 HTTP 鏈接標頭字段，限制 RESTful 環境(CoRE)鏈接格式作為有效負載攜帶，並被分配網際網路媒體類型。

(12) RFC 7744：討論受限制的設備是具有有限處理能力，存儲空間和傳輸容量的節點。在許多情況下，這些設備不提供用戶界面，並且通常用於在沒有人為干預的情況下進行訊息交互作用。

(13) RFC 8148：描述了如何使用基於 IP 的緊急服務機制來支援車輛發出的下一代緊急呼叫。

(14) RFC 8428：定義一種格式，用於表示傳感器測量列表(SenML)中的簡單傳感器測量和設備參數。

4、 資訊安全 (9 篇)

(1) RFC 8065：討論了許多隱私威脅如何應用於各種 IPv6 連結層協定，並為協定設計者提供了有關如何通過此類連結解決 IPv6 適配層規範中的此類威脅的建議。

(2) RFC 8387：關於資源受限制智慧物件上的安全挑戰，描述可能的佈署模式，資源受限制對訊息物件簽章，討論加密函數庫的可用性，和展示前導實驗。

(3) RFC 8576：討論事物生命週期中的各個階段，並記錄事物的安全威脅以及人們可能面臨防範這些威脅的挑戰。最後討論促進安全物聯網系統部署所需的後續步驟。

(4) RFC 7416：針對低功耗有損網路(RPL)的路由協定的安全威脅分析。

(5) RFC 7925：針對既有的安全性協定 Transport Layer Security (TLS) 與 Datagram Transport Layer Security (DTLS)的進行修正，以滿足物聯網的特性。

(6) RFC 8152：將用 RFC 7049 (CBOR)產生的 JSON 資料進行加密和簽章。

(7) RFC 8230：補充 COSE 物件進行加密和簽章時，可以使用 RSA 演算法，及相關的參數。

(8) RFC 8392：討論在一個 CWT 中的宣言，使用 CBOR 編碼，CBOR 物件簽章與加密(COSE)用於增加應用層的安全保護。

(9) RFC 7815：描述在一個受限制節點上，最小的網際網路金鑰交換協定(IKEv2)。IKEv2 歸屬於 IPsec 協定之下，用於身份驗證以及建立與維持安全關聯(Security Associations，SAs)。

5、 網路層與傳輸層 (37 篇)

(1) RFC 4944：詳述在 IEEE 802.15.4 網路上傳輸 IPv6 封包的訊號框格式，以及形成 IPv6 本地連結位址和無狀態自動配置地址的方法。並說明一種標頭壓縮方法。

(2) RFC 6282：更新 RFC 4944。規範了在 6LoWPAN 上傳遞 IPv6 封包時的 IPv6 標頭壓縮格式。同時使用這個框架規範 UDP 的標頭壓縮。

(3) RFC 7400：規定了一種簡單的附加，它能夠壓縮通用標頭和類似標頭的有效載荷，而無需為每個新標頭或類似標頭的有效負載定義新的標頭壓縮方案。

(4) RFC 7973：當通過以太網等第 2 層技術承載時，必須識別使用 RFC 4944 中定義的低功耗無線個人網路(LoWPAN)封裝的 IPv6 封包，以便接收器能夠正確解釋編碼的 IPv6 封包。

(5) RFC 8025：更新 RFC4944。引入新的文本切換機制，以支援 6LoWPAN 壓縮。以頁(Page)的型式，並通過 Paging Dispatch 來指派。

(6) RFC 8066：更新 RFC 4944 和 RFC 6282，定義 ESC 擴充碼的碼點和列舉已知使用案例的註冊條目。

(7) RFC 6606：6LoWPAN 由與 IEEE 802.15.4 標準兼容的設備構成，但是 IEEE 802.15.4 標準和 6LoWPAN 格式規範都沒有定義如何獲得網狀拓撲，本文提供了 6LoWPAN 路由的問題陳述和設計空間。

(8) RFC 6550：詳述低功耗有損網路(Low-Power and Lossy Network，LLN)上的 IPv6 路由協定(RPL)。

(9) RFC 6551：規定一組連結和節點路由度量和限制，適用於低功耗有損網路路由協定(RPL)使用的 LLN。

(10) RFC 6687：介紹了低功耗有損網路路由協定(RPL)的性能評估，用於小型室外部署傳感器節點和大規模智慧電錶網路。

(11) RFC 6552：設定一個基本的目標函數，該函數僅依賴於低功耗有損網路路由協定(RPL)中定義的對象，並且不使用任何協定擴充。

(12) RFC 6553：詳述 RPL 路由器中使用的 RPL 選項，以包括此類路由資訊。

(13) RFC 6554：指定了一種新的 IPv6 路由標頭類型，用於在 RPL 路由域內傳遞資料封包。

(14) RFC 8585：規定 IPv6 客戶邊緣(CE)路由器的 IPv4 服務連續性要求，這些要求由服務供應者或透過零售市場銷售的供應商提供。

(15) RFC 6719：描述具有最小秩遲滯目標函數(Minimum Rank with Hysteresis Objective Function, MRHOF)，該目標函數選擇最小化度量的路由，同時使用滯後來減少度量變化的流失。

(16) RFC 6997：規定一種點對點路由發現機制，是對低功耗有損網路路由協定(RPL)核心功能的補充。

(17) RFC 6998：規定了一種機制，得以讓低功耗有損網路路由協定(RPL)路由器可以延著已經存在的一條到另外一個 RPL 路

由器的路由測量指定度量的聚合值，從而讓該路由器決定是否要啟動路由發現機制去尋找一條更好的路由。

(18) RFC 8036：討論低功耗有損網路(RPL)路由協定在高級計量基礎設施(AMI)網路中的適用性。

(19) RFC 6206：詳述了 Trickle 演算法及其使用的注意事項。Trickle 演算法允許有損共享媒體(例如：低功耗有損網路)中的節點能以高強度，節能，簡單和可擴充的方式交換資訊。

(20) RFC 7787：描述分佈式節點共識協定(DNCP)，這是一種使用 Trickle 演算法和雜湊樹的通用狀態同步協定。

(21) RFC 8138：引入一種用於 6LoWPAN 路由的新調度類型，涵蓋了低功耗有損網路路由協定(RPL)的需求。

(22) RFC 6775：描述一個對於 6LoWPAN 的 IPv6 鄰居發現機制的簡單優化，定址機制，重覆位址偵測。

(23) RFC 8505：更新 RFC 6775 低功耗無線個人網路(6LoWPAN)鄰居發現規範，以闡明協定作為註冊技術的作用，簡化 6LoWPAN 路由器中的註冊操作，同時提供增強功能。

(24) RFC 7428：詳述在 ITU-T G.9959 網路上傳輸 IPv6 封包的訊號框格式，以及形成 IPv6 本地連結位址和無狀態自動配置地址的方法。

(25) RFC 7554：描述在低功耗有損網路(Low-Power and Lossy Network，LLN)的情境下，使用 IEEE 802.15.4e TSCH 媒體存取控制(MAC)協定的環境、問題陳述、與目的。

(26) RFC 8180：描述在 IEEE 802.15.4e TSCH 上支援 IPv6 的最小操作模式。

(27) RFC 8480：描述 IEEE 802.15.4e TSCH 操作子層協定(6P)。是 6TiSCH 操作子層(6top)的一部份，允許在 6TiSCH 網路上啟用分散式排程。

(28) RFC 7668：詳述如何通過低功耗無線個人網路 (6LoWPAN) 技術在低功耗藍牙上傳輸 IPv6 封包。

(29) RFC 8105：描述如何通過低功耗無線個人網路 (6LoWPAN) 技術在 DECT ULE 上傳輸 IPv6 封包。

(30) RFC 8163：本規範通過最大程度地利用現有標準，直接在建築自動化和控制網路中的有線終端設備上啟用 IPv6，並與傳統的 MS/TP 實現共存。MS/TP 設備通常類似於 6LoWPAN 網路中面臨的限制

(31) RFC 8272：規定 TinyIPFIX 協定，如何在限制網路(如 6LoWPAN)中傳輸 TinyIPFIX 資料和模板記錄，以及如何將 TinyIPFIX 資料轉換為代理設備中不是 TinyIPFIX 的資料。

(32) RFC 8375：指定了域名系統對於以“.home.arpa”結尾的名稱的 DNS 查詢所期望的行為。

(33) RFC 7695：指定了一種分佈式演算法，用於以允許自動分配唯一且不重疊的子前綴的方式劃分一組前綴。

(34) RFC 8539：定義一個 DHCPv6 選項，用於傳達建立 Softwires 通道的 IPv6 參數和一個 DHCPv4 選項(僅用於 DHCP 4o6)，以在 DHCP 4o6 客戶端和伺服器之間傳送資源通道的 IPv6 位址。

(35) RFC 7731：描述在低功率有損耗網路上群播協定，提供在受限制網路上 IPv6 群播轉送。

(36) RFC 7774：定義了一種通過 DHCPv6 選項為 MPL(低功耗有損網路的群播協定)配置參數集的方法。

(37) RFC 7732：描述了用於低功耗有損網路多播協定(Multicast Protocol for Low-Power and Lossy Networks，MPL) (RFC 7731)的自動化策略

大致上，我們可以看到 IETF 從連結層、網路層、傳輸層到應用層幾個面個都有相關的 RFC 說明標準實施方向。在應用層，有輕量級的 CoAP 系列 RFC 來替代 HTTP，用二進制的 CBOR 訊息來替代

純文字的 JSON 訊息，CBOR 訊息的加密與簽章來確保訊息的安全。在傳輸層與網路層，同樣有輕量級的 6LoWPAN 來替代完整的 IPv6 協定堆疊，並制 RPL 相關路由協定來協助物聯網環境裡可能遇到的情形。同時，在低功耗有損網路 LLN 的概念下，針對不同的實體網路制定相關的協定，以協助受限制裝置在受限制網路裡完成資料傳輸。

另一方面，在與廠商訪談的過程中，IETF 製定的物聯網相關 RFC 系列卻非廠商實作物聯網應用的主要考量。從三大國際雲端平台的物聯網服務 Amazon AWS IoT、Microsoft Azure IoT 與 Google Cloud Platform IoT 來看，三個平台都支援的通訊協定仍是 MQTT 與 HTTPS，CoAP 則是需要透過第三方軟體的協助才能實現。如之前在物聯網小節的分析中所述，市場需求仍是廠商開發產品的第一個考量。

三、物聯網、5G 與 IPv6 國際技術標準內容介紹

從上述 81 篇 RFC 中，我們選出 23 篇相對重要的 RFC 進行全文翻譯，包含 3 篇概念型(RFC 7228、7368 與 8376)，2 篇屬於應用層(RFC 7252 與 7049)，4 篇關於資訊安全(RFC 7925、7815、8152 與 8230)，14 篇為網路層與傳輸層相關(RFC 4944、6282、8025、8066、6550、8138、7732、6775、7428、7668、8105、8163、7554 與 8180)，列表

如下。

表 14、全文翻譯的 23 篇 RFC 列表

	RFC編號	RFC篇名	分類
1	RFC4944	Transmission of IPv6 Packets over IEEE 802.15.4 Networks	網路層與傳輸層
2	RFC6282	Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks	網路層與傳輸層
3	RFC6550	RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks	網路層與傳輸層
4	RFC6775	Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	網路層與傳輸層
5	RFC7049	Concise Binary Object Representation (CBOR)	應用層
6	RFC7228	Terminology for Constrained-Node Networks	概念型
7	RFC7252	The Constrained Application Protocol (CoAP)	應用層
8	RFC7368	IPv6 Home Networking Architecture Principles	概念型
9	RFC7428	Transmission of IPv6 Packets over ITU-T G.9959 Networks	網路層與傳輸層
10	RFC7554	Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement	網路層與傳輸層
11	RFC7668	IPv6 over BLUETOOTH(R) Low Energy	網路層與傳輸層
12	RFC7732	Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL)	網路層與傳輸層
13	RFC7815	Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation	資訊安全
14	RFC7925	Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things	資訊安全
15	RFC8025	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch	網路層與傳輸層

16	RFC8066	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines	網路層與傳輸層
17	RFC8105	Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)	網路層與傳輸層
18	RFC8138	IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header	網路層與傳輸層
19	RFC8152	CBOR Object Signing and Encryption (COSE)	資訊安全
20	RFC8163	Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks	網路層與傳輸層
21	RFC8180	Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration	網路層與傳輸層
22	RFC8230	Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages	資訊安全
23	RFC8376	Low-Power Wide Area Network (LPWAN) Overview	概念型

以下列出這 23 篇 RFC 的重點整理。

1. RFC4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks

IPv6 封包並非先天適合 IEEE 802.15.4 網路。由於低吞吐量、緩衝有限、封包只有 IPv6 MTU 下限的十分之一，故必須壓縮標頭，進行資料分割，其次，由於 IEEE 802.15.4 特點為低功率、低吞吐量、使用射頻為媒介，較容易出現雜訊干擾、連結故障、不對稱連結(A 能聽見 B，但 B 無法聽見 A)，因此網路層必須具備彈性及迅速反應，同時維持低功率與高效能，本篇文章的目標為解決以上問題。

本文主要針對低功率無線個人區域網路。定義了 IPv6 [RFC2460] 封包傳輸的訊號框格式，以及在 IEEE 802.15.4 網路之上形成 IPv6 連結本地位址和無狀態自動配置地址。由於 IPv6 需要支援比 IEEE 802.15.4 最大訊號框大小大得多的封包，因此定義了適應層，透過適應層以符合最低 MTU 的 IPv6 要求。本文也定義了使用 IPv6 在 IEEE 802.15.4 網路上實用所需的標頭壓縮機制，以及 IEEE 802.15.4 網格中封包傳送所需的規定。

為了讓不同設備製造商的設備之間能夠互連，需要製定統一的網路層標準。早期的無線感測網路缺乏一個共通的通訊協定標準，為了讓這些不同的感測網路裝置能夠互通，IPv6 over LR-WPAN (簡稱

6LoWPAN) 工作組，制定專屬於這些低功率、低可靠度、網路規模，極大網路裝置的互連通訊協定，即 IPv6 over IEEE802.15.4。因為 IP 對內存和頻寬要求較高，要降低它的運行環境要求以適應微控制器及低功率無線連接是比較難的。而 6LoWPAN 協定的制定提供了可能性。

2. RFC6282: Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks

這份文件指定了一個 IPv6 標頭壓縮格式，使得在低功耗個人區域網路路(6LoWPANs)中遞送 IPv6 封包。這種壓縮格式依賴於共享上下文，以允許壓縮任意前綴。而如何在共享上下文中保持訊息的完整性，超出本文範圍。這份文件指定了群播地址的壓縮方式，以及壓縮後續標頭的框架。在這個框架中也指定了 UDP 標頭的壓縮。

IEEE802.15.4 標準規定了 127 位元組的最大傳輸單元，在鏈路吞吐量為 250 kbps 或更低的無線鏈路上，在啟用安全性的情況下產生大約 80 個八位元組的實際媒體訪問控制（MAC）有效載荷。6LoWPAN 適應格式被指定用於在這種受約束的鏈路上承載 IPv6 資料封包，同時考慮到在無線傳感器網路的應用中預期的有限頻寬，儲存器或能量資源。RFC4944 定義了一個支援子 IP 轉發的網格尋址標頭，一個支援 IPv6 最小 MTU 需求的碎片標頭，以及針對 IPv6 數據(LOWPAN_HC1 和 LOWPAN_HC2)的無狀態標頭壓縮，以將相對較大的 IPv6 和 UDP 標頭減少(在最佳情況下)幾個位元組。

對於 6LoWPANs 中 IPv6 的大多數實際應用來說，LOWPAN_HC1 和 LOWPAN_HC2 是不夠的。本文定義了一種編碼格式，即

LOWPAN_IPHC，用於根據上下文中的共享狀態，有效壓縮唯一的本地、全局和群播 IPv6 地址。此外，本文還介紹了對 RFC4944 中定義的標頭壓縮格式的一些額外的改進。

本文還定義了 LOWPAN_HC1，一種任意後續標頭的編碼格式。LOWPAN_IPHC 指示是否使用 LOWPAN_IPHC 對以下標頭進行編碼。本文使用 LOWPAN_NHC 來定義了 UDP 的壓縮機制。雖然 RFC4944 為 UDP 定義了一種壓縮機制，但如果上層機制提供了可能性，如上層訊息完整性檢查(MIC)，則該機制不會啟動校驗和壓縮。此規範添加了在 6LoWPAN 上刪除 UDP 校驗總和的功能，從而可以保存另外兩個八字位元組。

此外，在使用 LOWPAN_NHC 時，本文定義了 IPv6-in-IPv6 封裝以及 IPv6 擴充標頭的編碼格式。

3. RFC6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks

本文規定了 IPv6 的 LLN 路由協定,詳述了低功耗有損網路(RPL)的 IPv6 路由協定。

網路可以同時運行多個 RPL 實例，而本文定義了單個實例的運行方式。RPL 實例可以提供路由給已訂定的前綴目的地，能通過 DODAG 根或 DODAG 中的備用路徑到達。這些根為獨立運作，可通過網路進行協調，不像 LLN 一樣受限。RPL 實例有兩種類型：本地和全局，且任何給定的 RPL 實例都是儲存或非儲存模式。本文介紹了可能形成的基本 RPL 拓撲，以及構建、識別、維護這些拓撲結構的規則及方法。也提到了 RPL 發現和上/下行路由的維護、目的地公告及安全機制。上行路由使用 DIS 用於引發傳送 DIO 訊息以進行發現及維護；下行路由以 RPL 通過目的地公告對象（DAO）訊息來構造和維護，主要分為兩種模式：儲存模式和非儲存模式。由目標函數（OF）定義了 RPL 節點如何選擇和優化路由。RPL 支援訊息的機密性和完整性,有三種自己的基本安全模式:不安全、欲安裝、已鑑別。而最後則是相關資訊的新註冊表內容。

低功耗有損網路(LLN)由幾十個到幾千個路由器(受限節點)組成，

是一種路由及互連都受到約束的網路。LLN 路由器通常在處理能力，記憶體和能量(電池電量)端面受到限制。它們的互連具有高損耗率，低數據速率和不穩定性的特點。支援包括點對點、點對多點，以及多點對點的通信流。

目的：

- 最小化能量
- 最小化延遲
- 滿足約束目標
- 最小化路徑(路由)
- 最小化監控未使用的連接成本
- 上/下行路由的維護

4. RFC6775: Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)

IETF 在低功耗無線個人區域網上的 IPv6 工作（6LoWPAN）定義了 6LoWPANs，如 IEEE 802.15.4。這個和其他類似的連結科技限制或不使用多播節能訊號。此外，無線網路可能不嚴格遵循傳統的 IP 子網概念和 IP 連結。

IPv6 鄰居發現不是為非傳遞無線鏈結所設計，因為其依賴於傳統的 IPv6 鏈結理念，並且大量的使用了多播，這使得其在低功耗有損網路中效率低並且有時候不切實際。因此,本文更新了 RFC4944,以便規範定義在這裡的優化的使用。

考慮低功耗網路的特點，以及 IPv6 鄰居發現[RFC 4861]協定設計，一些對鄰居發現的優化和擴充對於在低功耗有損網路（例如：個人區域無限網路標準和其他同類低功耗網路）上廣泛部署 IPv6 非常有用）。

鄰居發現是一種專用於 IPv6 的新協定，由於 6LoWPAN 網路應用的特點，鄰居發現協定必須優化。為了更好地降低功耗，提出了限制多播路由請求和路由公告，避免重複位址檢測、多播鄰居請求和鄰居不可達檢測資訊等一系列 6LoWPAN 鄰居發現優化策略。

本規範介紹了針對低功耗有損網路如（底層網路）的 IPv6 鄰居發現[RFC4861]的以下優化：

- 主機啟動的互動允許休眠主機。
- 消除主機基於多播的位址解析。
- 在單播鄰居請求（NS）和鄰居公告（NA）訊息中使用新選項的主機位址註冊功能。
- 一個新的鄰居發現選項，用於將低速無限個人網路標準標頭壓縮上下文分發給主機。
- 首碼和低速無限個人網路標準標頭壓縮上下文的多跳分佈。
- 多跳重複位址檢測（DAD），它使用兩種新的 ICMPv6 訊息類型。

5. RFC7049: Concise Binary Object Representation (CBOR)

簡明二進制對象表示（CBOR）是一種數據格式，其設計目標包括極小的代碼大小,相當小的訊息大小和可擴充性,而無需版本協商。這些設計目標使它不同於早期的二進位序列化，如 ASN.1 和 MessagePack

CBOR 的目標為：

- 這種表示必須能夠明確地編碼網際網路標準中使用的最常見的資料格式。它必須使用二進位編碼表示一組合理的基底資料型別和結構。這裡的“合理”，在很大程度上受 JSON 功能的影響，主要是二進位位元組字串的添加。所支援的結構僅限於陣列和樹；循環圖表和點陣圖不被移植。沒有要求所有資料格式都是唯一編碼的；也就是說，用多種不同的方式編碼數字“7”是可以接受的。
- 編碼器或解碼器的代碼必須緊湊，以支援記憶體、處理器電源和指令集非常有限的系統。編碼器和解碼器需要在非常少量的代碼中實現。該格式應使用現代機器表示的資料（例如，不需要二進位到十進位轉換）。
- 資料必須能夠在沒有模式描述的情況下解碼。與 JSON 類

似，編碼資料應該是自描述的，這樣就可以編寫通用的解碼器。

- 序列化必須合理地緊湊。這裡的“合理”是指與 JSON 比較，實現序列化的複雜度來限定的。使用一般的壓縮方案或大量的位元處理都會違反複雜度目標。
- 該格式必須同時適用於受約束的節點和大容量應用程式。這意味著在編碼和解碼方面，CPU 的使用必須相當節儉。這既適用於受約束的節點，也適用於資料量非常大的應用程式中的潛在用途。
- 該格式必須支援所有 JSON 資料類型，以便在 JSON 之間進行轉換。只要表示的資料在 JSON 的能力範圍內，它就必須支援合理的轉換級別。必須能夠為所有類型的資料定義指向 JSON 的單向映射。
- 格式必須是可擴充的，並且擴充資料必須可以被早期的解碼器解碼。這種格式是為幾十年的使用而設計的。格式必須支援一種允許回退的擴充形式，以便不理解擴充的解碼器仍然可以對訊息進行解碼。

6. RFC7228: Terminology for Constrained-Node Networks

擁有受到限制的 CPU，記憶體，以及能源的小型設備被稱為“受限制性設備”的裝置數量正在日益增加，而這些“受限制設備”可以構成“受限制網路”，可以在物聯網中產生作用，為了應對未來可能會遇到大面積使用此類設備與網路的狀況，該文對這類文件進行了規範化處理，設定了一些規範來定義，規劃此類設備與網路。

對此類設備依照處理能力，功耗等各個方面來進行劃分等級，對其進行分類。設備的受限制等級（如其運算能力，功耗等）分為 0 類，1 類，2 類三種。

按照設備的可用能源的限制來劃分，不受限制的為 E9，一次性電池耗盡時被丟棄的設備為 E1，可充電的設備可以劃為 E2，可能存在可用於特定事件的有限量的能量，例如，用於能量收集燈開關中的按鈕按壓; 這些設備被歸類為 E0。

7. RFC7252: The Constrained Application Protocol (CoAP)

受限制的應用協定(CoAP)是一種專門的 web 傳輸協定，用於受限節點和受限制的網路。節點通常具有 8 位元的微控制器，具有少量 ROM 和 RAM，而低功耗無線的 IPv6 等則受限制網路個人區域網路(6LoWPAN)常常有高封包錯誤率和典型的 10 kbit/s 的網路輸送量。該協定專為機器對機器(M2M)應用而設計，如智慧能源和建築自動化。

特點如下：

- Web 協定在受限環境中可滿足 M2M 需求
- 基於 UDP，擁有可選的可靠性保障，支援單播和多播請求
- 非同步訊息交換
- 低標頭 overhead 且解析複雜度
- 支援 URI 與 HTTP 內容類型
- 簡單的代理和緩衝區功能
- 無狀態 HTTP 映射時，允許構建代理，以統一的方式通過 HTTP 訪問 CoAP 資源，或者通過 CoAP 實現 HTTP 的簡單介面

- 安全綁定到 DTLS 資料封包傳輸層安全(DTLS)

訊息傳輸特點：

- 對於可確認的訊息，具有指數級回退的簡單停等重傳可靠性。
- 確認和非確認訊息的重複檢測。

8. RFC7368: IPv6 Home Networking Architecture Principles

本文描述了住宅家庭網路中不斷發展的網路技術，其中設備數量越來越多，內部路由越來越多。本文的目標是定義基於 IPv6 的家庭網路的通用架構，描述相關的原則，注意事項和要求。本文簡要強調了 IPv6 引入家庭網路的具體含義，討論了該架構的各個要素，並建議如何在家庭網路中採用標準的 IPv6 機制和定址。該體系結構描述了對特定附加功能的特定協定擴充的需求。假設 IPv6 家庭網路不是主動管理的，並且作為僅 IPv6 或 IPv4/IPv6 雙堆疊網路運行。本文中沒有針對 IPv4 部分的建議。

本文中主要關注於在引入 IPv6 時要解決的問題，著眼於比今天使用 IPv4 更好的結果，以及提供更一致的解決方案，以盡可能滿足已確定的要求。本文旨在為家庭網路中如何使用標準 IPv6 機制和定址提供基礎和指導原則，同時與現有的 IPv4 機制共存。在新興的雙堆疊家庭網路中，引入 IPv6 對 IPv4 操作沒有不利影響至關重要。我們假設家庭網路中的 IPv4 網路架構就是這樣，並且不能通過新建議進行修改。本文未討論 IPv4 家庭網路如何提供對多個子網的支援。不應該假設任何未來使用 IPv6 創建的新功能將向後相容，以支援 IPv4。

此外，未來的部署或在其他 IPv4/IPv6 雙堆疊家庭網路內的特定子網可能僅是純 IPv6 環境，在這種情況下，考慮 IPv4 的影響將不適用。

本文提出了一種基本家庭網路體系結構，盡可能使用經過驗證和可靠的協定和實現。本文的範圍主要是網路層技術，提供了實現定址、連接、路由、命名和服務發現的基本功能。

例如，雖然家庭網路組件應該易於部署和使用，但本文不討論特定的用戶界面，也不討論特定的物理、無線或數據鏈路層考慮因素。同樣，也沒有從上到下指定整個家庭網路路由器的設計; 相反，專注於第 3 層方面。這表示第 2 層在很大程度上超出了本文範圍。假設存在支援 IPv6 的資料鏈路層，並且會做出相應的反應。

9. RFC7428: Transmission of IPv6 Packets over ITU-T G.9959 Networks

本文描述了用於傳輸 IPv6 封包裡的乙太網路訊號框以及在 ITU-T G.9959 網路上形成 IPv6 鏈路本地地址和無狀態自動配置的 IPv6 地址的方法。

本文定義了 IPv6 資料封包傳輸的乙太網路訊號框，以及在 G.9959 網路上形成 IPv6 鏈路本地地址和無狀態自動配置的 IPv6 地址。一般方法是使 RFC4944 的元素適應 G.9959 網路。G.9959 提供分段和重組（SAR）層，用於傳輸大於 G.9959 媒體訪問控制協定數據單元（MAC PDU）的資料封包。RFC 6775 通過為 IPv6 鄰居搜索（ND）（最初由 RFC 4861 定義）的低功耗無線個人區域網路（6LoWPAN）優化指定 IPv6 來更新 RFC 4944。本文限制使用 RFC 6775 前綴和上下文頁面分配。介面標識符（IID）可以由 G.9959 鏈路層地址構成，從而產生“鏈路層導出的 IPv6 地址”。使用該方法，則不需要重複地址檢測（DAD）。可以透過 DHCP 集中分配 IPv6 地址，從而產生“非鏈路層導出的 IPv6 地址”。僅在某些情況下才需要地址註冊。除了 IPv6 應用程序通信之外，本文中定義的訊號框可以由 IPv6 路由協定使用，例如低功耗有損網路路由協定（RPL）[RFC6550]或點對

點路由的反向發現。低功耗有損網路（P2P-RPL）[RFC6997]通過 G.9959 網路實現 IPv6 路由。由本文定義的封裝框架可以選擇透過 6LoWPAN 層下方的網格佈線來傳輸。網狀網路和其路由協定規範超出本文的範圍。

概述了適用於 G.9959 的 PHY 和 MAC 層的屬性以及如何將這些屬性用於 IPv6 傳輸。G.9959 定義了網路控制器如何分配唯一的 32 位 HomeID 網路標識符以及如何為每個節點分配 8 位 NodeID 主機標識符。 NodeID 在 HomeID 標識的網路中是唯一的。 G.9959 HomeID 表示由一個或多個 IPv6 前綴標識的 IPv6 子網。

10. RFC7554: Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement

本文描述了在低功耗有損網路(LLN)環境中使用 IEEE 802.14.4e 的時隙通道跳頻（TSCH）媒體存取控制（MAC）協定的環境，問題陳述和目標。

本文描述了在 LLN 背景下採用 TSCH 所產生的主要問題。附錄 A 進一步概述了 IEEE 802.15.4e 的 TSCH 修正案的主要特徵。TSCH 旨在使 IEEE 802.15.4 設備能夠支援廣泛的應用，包括但不限於工業應用。其核心是一種媒體存取技術，它使用時間同步來實現低功耗操作和通道跳躍，以實現高可靠性。同步精度會影響功耗，並且可能會在幾微秒到幾毫秒之間變化，具體取決於解決方案。這與傳統的 IEEE 802.15.4 MAC 協定非常不同，可說是重新設計。TSCH 不修改物理層，可以在符合 IEEE 802.15.4 的任何硬體上操作。

IEEE 802.15.4e 是針對 LLN 的最新一代超低功耗和可靠的網路解決方案。RFC 5673 討論了工業應用，並強調了 LLN 在工業環境中運行的操作條件以及可靠性，可用性和安全性要求。在這些環境中，具有大型（金屬）設備的大量部署環境會導致多徑衰落和干擾，從而阻礙單通道解決方案的嘗試；TSCH 的通道靈活性是其超高可靠性的

關鍵。商用網路解決方案現已上市，其中節點平均消耗 10 個微安，端到端資料封包傳輸率超過 99.999%。

TSCH 僅關注 MAC 層。這種乾淨的分層允許 TSCH 適合支援 IPv6 的 LLN 協定，通過低功耗無線個人區域網路（6LoWPAN）運行 IPv6 [RFC6282]，低功耗有損網路的 IPv6 路由協定（RPL） [RFC6550] 和約束應用協定（CoAP）[RFC7252]。缺少的是負責調度要發送的訊號框的 TSCH 時隙的功能實體。在本文中，將此實體稱為“邏輯鏈路控制”（LLC），該實體的實現可以是不同類型的，包括分佈式協定或負責調度的集中式服務器。

雖然 IEEE.802.15.4e 定義了 TSCH 節點進行通信的機制，但它沒有定義構建和維護通信調度的策略，將該調度與 RPL 維護的多跳路徑相匹配，調整之間分配的資源。鄰居節點到數據業務流，對應用層生成的數據實施差異化處理，並對 6LoWPAN 和 RPL 發現鄰居，對拓撲變化作出反應，自行配置 IP 地址或管理密鑰資料所需的信號訊息進行處理。

11. RFC7668: IPv6 over BLUETOOTH(R) Low Energy

本文描述如何使用 IPv6 通過低功耗無線個人區域網路（6LoWPAN）技術使用低功耗藍牙傳輸 IPv6 訊息。

藍牙智慧型是藍牙技術聯盟定義的藍牙規範中藍牙低功耗特性（以下稱為“低功耗藍牙”）的品牌名稱。低功耗藍牙是一種無線電技術，適用於使用極低容量（例如鈕扣電池）電池或簡約電源工作的設備，低功耗藍牙設計用於以適度的數據速率不頻繁地傳輸少量數據，每位元的能量消耗非常小。這意味著低功耗、少量數據的特點非常適合於物聯網的使用。而物聯網的大量傳感設備也就需要非常大量的地址空間，所以才引入使用 IPv6。

考慮到傳感器和網際網路連接設備數量呈指數增長的可能性，IPv6 用於與這些設備進行通信是一種理想的協定，因為它提供了較大的地址空間。此外，IPv6 還提供了無狀態地址自動配置工具，尤其適用於處理能力非常有限或缺乏完整操作系統或用戶界面的傳感器網路應用和節點。藍牙技術聯盟還發布了網際網路協定支援配置文件（IPSP），其中包括網際網路協定支援服務。IPSP 允許發現啟用 IP 的設備並建立用於傳輸 IPv6 資料封包的鏈路層連接。

為了描述如何使用 IPv6 通過低功耗藍牙傳輸訊息，本文首先講

述了低功耗藍牙的原理與特性。包括堆疊與拓撲，每個低功耗藍牙設備都有一個 48 位元設備地址。通過低功耗藍牙為 L2CAP 固定通道定義的最佳 MTU 是 27 個位元組，包括 4 個八位元組的 L2CAP 標頭。之後講述了 IPv6 在低功耗藍牙上的工作原理，說明 IPv6 堆疊如何與低功耗藍牙 L2CAP 層之上的 GATT 堆疊並行工作。

低功耗藍牙協定（如 L2CAP）使用小端位元組排序，但 IPv6 資料封包必須以大端順序（網路位元組順序）傳輸。後面帶出了 IPv6 的標頭壓縮。

12. RFC7732: Forwarder Policy for Multicast with Admin-Local Scope in the Multicast Protocol for Low-Power and Lossy Networks (MPL)

本文用於完善其他文件的定義。本文描述了用於低功耗有損網路多播協定（MPL Multicast Protocol for Low-Power and Lossy Networks）[RFC7731]的自動化策略（automated policy automated policy），該策略在位於運行 MPL 的網路和其他網路之間的邊界路由器內使用 Admin-Local 範圍轉發多播訊息。

MPL 的自動化策略需要通過 Admin-Local 範圍來配置。多播範圍在 RFC 4291 中被定義。RFC 7346 使用以下文本擴充定義範圍：Interface-Local，Link-Local 和 Realm-Local 範圍邊界，自動從物理連接或其他非多播相關配置派生。全域範圍（Global Scope）是沒有邊界的。Admin-Local 或更大的所有其他非保留範圍的邊界，由管理方式配置。

該文設定了相關的 MPL4 術語，界面參數等等。MPL4 路由器擁有相關的演算法用來確定 MPL 訊息可以傳播的網路層。該文定義了什麼是合法的多播訊息與 MPL 選項，以及 MPL 訊息在介面上的轉發方式等等。

13. RFC7815: Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation

這份文件描述在一個受限制節點上，最小及初始版本的網際網路金鑰交換協定(IKEv2)。IKEv2 歸屬於 IPsec 協定之下，用於身份驗證以及建立與維持安全關聯(Security Associations，SAs)的運作。IKEv2 包含數個可選功能，在最小限度運行的要求中是不需要的。本文描述了對最小限度運行的要求，以及多種可被運行的最佳化成果。此處描述的協定可與使用共享密鑰身份驗證的完整 IKEv2 方法相互操作(IKEv2 無需使用身份驗證)。這個最小的啟動器只能與扮演回應者的完整 IKEv2 進行溝通。因此，兩個最小的啟動器無法彼此通信。

此文件並非一個網路標準的規範，只是用於提供訊息。

網際網路協定越來越多地用於對電源、內存和處理資源有嚴格限制的小型設備上。本文描述了最小的 IKEv2 運行，設計用於可與網際網路密鑰交換協定版本 2（IKEv2）相互操作的受限制節點。主要描述如何在 IKEv2 中使用共享密鑰進行身份驗證，因為它最容易運行，也描述了如何使用原始公鑰而不是共享密鑰身份驗證。

14. RFC7925: Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things

物聯網（IoT）部署中的常見設計模式是使用受限制設備，該設備通過傳感器收集數據，以用於家庭自動化，工業控制系統，智慧城市和其他物聯網部署。

本文定義了傳輸層安全協定（TLS）和資料封包傳輸層安全協定（DTLS）配置文件，為數據交換提供安全，以防止竊聽，篡改和訊息偽造。缺乏安全是物聯網產品中的常見漏洞，可以通過使用這些經過充分研究和廣泛部署的網際網路安全協定解決。

IoT 設備能夠交換數據通常需要對兩個端點進行身份驗證，並且能夠為交換的數據提供完整性和機密性保護。雖然可以在協定堆疊的不同層提供這些安全服務，但是使用傳輸層安全協定（TLS）/資料封包傳輸層安全協定（DTLS）已經受到許多應用程序協定的歡迎，對物聯網很有用。

將網際網路協定安裝到受限制設備中可能很困難，但由於標準化工作，可以使用新的配置文件和協定，例如受限制的應用協定（CoAP）[RFC7252]。CoAP 訊息主要通過 UDP/DTLS 傳輸，但也可以使用其他傳輸，例如 SMS（如附錄 A 中所述）或 TCP（由[COAP-TCP-TLS]

提出）。

本文的主要目的是使用 DTLS 1.2 [RFC6347]保護 CoAP 訊息，但各節中包含的訊息不僅限於 CoAP，也不限於 DTLS 本身。

本文定義了 DTLS 1.2 [RFC6347]和 TLS 1.2 [RFC5246]的配置文件，為物聯網應用程序提供通信安全服務，並且可在許多受限制設備上實現。因此，配置文件意味著利用可用的配置選項和協定來擴充以支援 IoT 環境。本文不會改變 TLS/DTLS 規範，也不會引入任何新的 TLS/DTLS 擴充。

本文的主要目標讀者是配置和使用 TLS/DTLS 堆疊的嵌入式系統開發人員。但是，該文也可以幫助那些為物聯網產品開發或選擇合適的 TLS/DTLS 堆疊的人。

15. RFC8025: IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch

低功耗有損網路（LLN）的設計通常側重於節約能源，這通常是一種非常受限制的資源。

控制資料傳輸量是節約能源的一種可能的方法。在許多 LLN 標準中，訊號框大小被限制為比 1280 位元組的 IPv6 最大傳輸單元（MTU）小得多的值。比較特別的是，依賴於 IEEE 802.15.4 實體層（PHY）的 LLN 會被限制在每個訊號框為 127 位元組。對於 IEEE 802.15.4 壓縮 IPv6 封包的需求促成了 6LoWPAN 標頭壓縮（6LoWPAN-HC）[RFC6282]的工作。

為了減少在 IPV6 上傳遞訊息時相關的資源耗損，可以使用標頭壓縮的方法來減少工作量。該文建立在 RFC4944 的基礎上。

RFC4944 在 6LoWPAN 解析器中引入“解析上下文”的概念來適應 6LoWPAN，同時透過 IEEE 802.15.4 [RFC4944]保持與 IPv6 的向後相容性，該解析上下文由頁面標識。該規範定義了 16 個頁面。頁面在 6LoWPAN 資料封包中透過 Paging Dispatch 值分隔，該值指示下一個當前頁面。

16. RFC8066: IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines

RFC 4944 的 5.1 節定義了調度(Dispatch)標頭和類型。ESC 類型被定義為在 6LoWPAN 標頭中使用附加的調度位元組。RFC 6282 修改了 ESC 調度類型的值，該值記錄在 IANA 註冊表中。但是，ESC 調度類型之後的位元組和用法未在 RFC 4944 或 RFC 6282 中定義。近年來，6LoWPAN 的部署、實施和標準組織已開始使用 ESC 擴充位元組。這顯示了更新 IANA 註冊政策的必要性。

本文定義了新的 ESC 擴充類型註冊表和 ESC 擴充位元組，以供將來的應用程式使用。此外，將 ITU-T 規範的 ESC 調度位元組碼點記錄為已知。

預期 RFC 4944 的現有措施不能處理本文中定義的 ESC 擴充資料位元組。為了互操作性，新的調度類型（EET）絕不能修改現有調度類型的行為。

17. RFC8105: Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)

本文描述如何使用通過低功耗無線個人區域網路（6LoWPAN）技術在 DECT ULE 上傳輸 IPv6。

DECT 技術已在全球通信設備中使用了 20 多年。主要用於承載無線電話語音，但也用於以數據為中心的服務。DECT ULE 是 DECT 介面的最新成員，主要用於低頻寬，低功耗應用，如傳感器設備，智慧電錶，家庭自動化等。由於 DECT ULE 介面繼承了 DECT 的許多功能，因此受益於具有遠程和無干擾的全球保留頻段，低價格和成熟的操作。DECT ULE 的 IPv6 通信能力具有附加價值，例如物聯網應用程序。

DECT 是 ETSI 規定的標準系列，CAT-iq 是一套產品認證和互操作性配置文件，由 DECT 論壇定義。DECT ULE 是一種無線介面技術，建立在傳統 DECT/CAT-iq 的關鍵基礎之上，以犧牲資料流量為代價來降低功耗。

本文描述如何在 DECT ULE 鏈路上使用 IPv6 來優化功率，同時保持 IPv6 傳輸的多項優勢。RFC 4944，RFC 6282 和 RFC 6775 指定透過 IEEE 802.15.4 傳輸 IPv6。DECT ULE 具有許多類似於 IEEE

802.15.4 的特性，但也有差異。定義透過 IEEE 802.15.4 傳輸 IPv6 的機制子集，於 DECT ULE 鏈路上傳輸 IPv6。

18. RFC8138: IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header

本文引入一種新的 IPv6 低功率無線個人區域網路（6LoWPAN）調度類型，用於 6LoWPAN 路由拓撲，最初涵蓋了低功耗有損網路（RPL）封包壓縮路由協定的需求。使用此調度類型，此規範定義了一種壓縮 RPL 選項和路由標頭類型 3 的方法，是一種高效的 IP-in-IP 技術，並且可擴充用於更多應用程序。

低功耗有損網路（LLNs）的設計通常以節約能源為主要考量，在大多數情況下，能源是非常有限的資源。其他限制，包含有損網路設備的儲存器容量和工作環境。

控制數據傳輸量是節省能源的一個可能方法。在許多有損網路標準中，訊號框大小被限制比 IPv6 最大傳輸單元（MTU）1280 位元組小得多。特別是依賴於 IEEE 802.15.4 物理層（PHY）的有損網路，限制每個訊號框最大為 127 位元組。透過 IEEE 802.15.4 壓縮 IPv6 資料封包的需求促成了基於 IEEE 802.15.4 網路上的 IPv6 封包壓縮格式。

出於安全性和將 ICMPv6 錯誤訊息發送回源頭的原因，原始封包不得被篡改，在 IPv6 封包中插入或刪除的任何訊息都必須放在額外

的 IP-in-IP 封裝中。

使用頁面調度。該規範引入了一個新的 6LoWPAN 路由標頭（6LoRH）來承載 IPv6 路由訊息。6LoRH 可以包含來源路由訊息，例如 SRH 的壓縮形式，以及其他種類的路由訊息，例如 RPI 和 IP-in-IP 封裝。

19. RFC8152: CBOR Object Signing and Encryption (COSE)

本文定義了 CBOR 物件簽章和加密（COSE）協定。簽章方面，它支援兩種不同的結構，及不同的情況下的參數。本文定義了如何計算簽章和驗證簽章的步驟，描述如何使用 CBOR 序列化來建立和處理簽章，訊息鑑別碼和加密。文件中提到加密物件內容密鑰的分配方法，和如何進行加密與解密，MAC 物件的內容如何計算及驗證。

文中介紹兩種簽章演算法，ECDSA 和 Edwards 曲線數位簽章演算法，訊息鑑別碼演算法可使用雜湊訊息鑑別碼和 AES 訊息驗證碼，內容加密演算法有 AES GCM, AES CCM, ChaCha20 和 Poly1305，及密鑰函數及密鑰分配方法，附錄中並提列數個 CBOR 編碼的範例。

在正常情況下，資料可以使用 JSON 格式去做傳輸，而物聯網（IoT）小型受限制設備會有傳輸上的限制。簡明二進制物件表示法（CBOR）是一種專為小程式和小訊息設計的數據格式。為提供 IoT 訊息安全服務，本文為 CBOR 格式定義基本安全服務，進行簽章及加密的動作。

20. RFC8163: Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks

MS/TP 設備通常為具有有限處理能力和記憶體的低成本微控制器。這些限制以及低資料速率和小 MAC 位址空間，類似於 6LoWPAN 網路中面臨的限制。

該規範的主要目標是：(1)透過最大程度地利用現有標準，直接在建築自動化和控制網路中的有線終端設備上啟用 IPv6，以及(2)與傳統的 MS/TP 共存。共存允許 MS/TP 網路逐步升級以支援 IPv6。

為了與傳統設備共存，不允許對 BACnet 標準中規定的 MS/TP 定址模式，訊號框標頭格式，控制訊號框或主節點狀態進行任何更改。

21. RFC8180: Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration

本文描述 6TiSCH (IEEE 802.15.4e 網路 TSCH 模式 IPv6)的最小操作模式。這個最小操作模式指定了必需支援的協定基準集合，以及足以啟用 6TiSCH 功能網路的設定和操作模式的推薦。

在 IEEE 802.15.4 TSCH (Time-Slotted Channel Hopping)網路連結組成的 TSCH 網格之上，6TiSCH 提供 IPv6 連接能力。此最小模式使用具有相應配置的協定集合，包括 IPv6 6LoWPAN 框架，通過 IEEE 802.15.4 TSCH 實現可相互合作的 IPv6 連接。此最小配置提供了網路必要頻寬和安全導引，並為 IETF 協定與 IEEE 802.15.4 TSCH 之間的介面定義了適當的連結。所有符合 6TiSCH 標準的設備都應實現這個最小操作模式。

22. Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages

CBOR 是使用二進位來表示 JSON 字符資料的方法，目的在於減少傳輸的資料量，適合於物聯網應用中使用。COSE 對 CBOR 物件提供簽章與加密的方法，以提昇物聯網資料傳輸的安全性。由於 RSA 演算法本身不適用於 COSE，需要用一種新的方法來對 COSE 訊息進行加密。本文對 RSA 演算法進行了適當的設計，使其產生一種可以用於 COSE 環境的加密演算法。

23. RFC8376: Low-Power Wide Area Network (LPWAN) Overview

低功率廣域網路（LPWAN）是具有諸如大覆蓋區域、低頻寬、可能非常小的封包以及使用電池等特性的無線技術。

本文提供 IETF IPv6 低功耗廣域網路工作小組正在考慮的技術概述和背景資料，以及這些技術需求與在 LPWAN 中運行時的差距。本文還提供了這些技術需求與當前可用的 IETF 規範之間的分析。

本文不是網際網路標準規範，以提供資訊為目的。

該領域的大多數技術旨在實現類似的目標，即以極低的功耗支援大量極低成本、低吞吐量的設備，具有長距離傳輸能力以覆蓋大面積，即使是電池供電的設備也可以部署多年。

本文介紹 LPWAN 技術：LoRaWAN、窄頻物聯網(NB-IoT)、Sigfox、Wi-SUN 聯盟用戶端場域網路(FAN)。

本文介紹使用 LPWAN 的一些應用可能會引起的隱私考慮。另一個挑戰是如何處理密鑰管理和相關協定。

第二節　　物聯網平台與應用

一、物聯網基本介紹

在物聯網的架構中，終端的實體設備會包含各種感測器，用以識別與感知數據，而這些數據將會以有線或無線的網際網路傳輸技術，傳遞至資料主機或雲端平台，使應用層能夠接受到最新的數據資料，並做最有效的應用。

(一) 關鍵的感知層技術

1、 感知技術

使實體物件具有感測物理世界中物理量、化學量、生物量變化的能力，如溫度、濕度、壓力、位移、速度等感測器，則是將感測到的物理量轉化為電腦可以處理的數位訊號。

2、 辨識技術

用以辨識物體的身分或狀態，最常見的辨識技術有 RFID 標籤、影像辨識、文字辨識、二維條碼標籤等等。

(二) 關鍵的網路層技術

1、 無線電信網路

無線電信網路是由「基地台」與「行動電話」等設備所組成，處

於基地台服務範圍內的手機可以用無線的方式與基地台進行傳輸。如3G/4G 行動通訊網路。

2、 無線數據網路

無線數據網路的應用在我們日常生活中已經非常普及，其依照通訊範圍的大小將會使用到不同的通訊技術。常見的無線數據網路技術有 WiMAX、Wi-Fi、Bluetooth、6LoWPAN。

3、 雲端運算

雲端運算是一種基於網際網路的運算方式，能夠依照使用者的需求，方便且快速的取用雲端服務商所提供各式各樣的應用服務。對於使用者而言，只要能夠連上網路，即可使用龐大的硬體設備與運算能力。

(三) 物聯網的應用介紹

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，表 15 列出一

些可能的物聯網應用，但物聯網應用不限於此表所列，未來仍有新的應用案例仍可能產生。

表 15、物聯網之可能應用

	物聯網應用案例
智慧製造	遠端監控機器運作狀況，以確保穩定生產流程、故障預警、機器運作之最佳化、RFID 感測器等推動自動化流程
車聯網	提供影音娛樂系統(infotainment)，包括多媒體、SNS、定位系統等、運用車載感測裝置(雷達、加速器等)、GPS 等提升車輛操控性(無人駕駛等)
醫療照護	利用穿戴式裝置搜集人體資訊(血壓、脈搏、活動量、睡眠時間等)、疾病與診斷，並搭配個人遺傳因子等資訊，可推動預防醫療等
金融保險	利用 NFC、行動電話進行支付、依車聯網之駕駛傾向，計算汽車保險等
零售	利用 RFID 進行銷售與庫存管理、利用銷售資訊，進行促銷活動、透過人流分析調整賣場動線與商品陳列
物流	利用各式的 sensors 追蹤配送狀態、及早預知收件與配送壅塞狀況，提升效率、運用車輛運行資訊與駕駛者開車傾向，預防事故與防止故障發生
能源	分散電源的電力供應調整、依據 demand-response 控制電力消費量、最佳化家庭、工廠、大樓的電力消費量
農畜牧業	根據氣象、土壤、農作物等收成有關的數據來預測與最適化種植監控、搜集家畜的體溫、活動等數據，掌握家畜的體適能與繁殖期等
智慧居家	照明、空調、音響等設備的遠端操控、確保高齡者與小孩的使用安全性來自動調理設備
公共設施(道路下水道等)	遠端監控道路、橋梁、隧道等，預防崩塌與異常檢點、遠端監控水管線路，檢測與防治漏水
智慧校園	監控校園與宿舍安全、了解教室與設備的使用情形
智慧交通	如火車、公車、捷運、高鐵的大眾運輸公具的即時監控、行車資訊、紅綠燈等號誌的自動控制、道路使用情形監控與事故偵測、行車流量的估計等

為了使物聯網的應用能夠擁有更多功能以及更快的運算能力，多種技術之間的連結整合是必須的，在這種趨勢之下，人工智慧與物聯網的結合成為了智慧物聯(AIoT)。在 AIoT 的帶動下，自駕車的發展成為了熱門的焦點，這讓原本具有感測能力的汽車能透過蒐集的資料來加以學習，來達到更精確的判斷與操控。

(四) 物聯網平台

雲端概念與物聯網是息息相關的，因為要運行物聯網，來自四面八方的龐大資料量將會非常驚人，成熟的雲端技術可以將這些資料完善儲存、處理以便供應至應用層。不僅如此，使用者還能依照自身需求來使用各種加值服務，透過雲端來對系統進行預防性維護、即時性更新，以及提升系統運作可靠度，不僅可以降低設備購置與維護系統等成本，還可以將省下的時間更專注於應用服務的開發。

國際三大雲端平台 Amazon AWS、Microsoft Azure 與 Google Cloud Platform 都有針對物聯網推出相關產品。物聯網服務商除了可以利用這些平台的 IaaS 虛擬機服務來建構物聯網服務，也可以使用相關的 PaaS 或 SaaS 服務。如 Amazon 的 AWS IoT Core 則能夠讓連接的裝置輕鬆的與雲端應用服務和其他裝置進行資訊傳遞，簡單實現可靠的遠端設備連接、控制與管理。而 AWS IoT Core 亦能透過 AWS Lambda、Amazon Kinesis、Amazon S3、Amazon SageMaker、Amazon

DynamoDB、Amazon CloudWatch、AWS CloudTrail 和 Amazon QuickSight 等 AWS 服務，直接將裝置所蒐集到的資料進行處理、存放與分析等操作，而無須管理任何基礎架構。

國內在物聯網裝置製造上，有長久以來的優勢。因此，也有不少業者推出物聯網平台服務。

以下，將分別介紹國際三大雲端平台上面的物聯網產品，以及國內電信業者物聯網平台。

二、Amazon AWS 平台與應用

(一) AWS IoT 平台

AWS IoT 可讓已與網際網路連線的 IoT 裝置連線至 AWS 雲端，並讓雲端中的 IoT 應用系統與其互動。IoT 應用系統收集並處理由來各自地 IoT 裝置的感測資料，必要時，也能遠端控制裝置。物件可以對不同的 MQTT 主題發佈訊息，以回報其狀態。每個 MQTT 主題都有一個階層式名稱，可識別正在更新狀態的裝置。當訊息以 MQTT 主題發佈時，此訊息會傳送至 AWS IoT MQTT 訊息中介裝置，再由訊息中介裝置將所有以 MQTT 主題發佈的訊息傳送至所有訂閱該主題的用戶端。

AWS IoT Core 能夠將裝置連接至 AWS 服務和其他裝置、保護資

料和互動安全、處理裝置資料並採取行動，以及即使離線也能讓應用程式與裝置互動的平台。讓裝置透過 MQTT、HTTP 或 WebSocket 協定，與 AWS IoT Core 進行連線、驗證和交換訊息。支援 C、JavaScript 和 Arduino，而且內含用戶端程式庫、開發人員指南和製造商的移植指南。

簡介 AWS IoT 如下。

AWS IoT 可在已與網際網路連線的裝置 (例如感測器、傳動器、嵌入式微控制器或智慧型設備) 和 AWS 雲端。AWS IoT 包含以下元件: 裝置閘道、訊息中介裝置、規則引擎、安全與身分服務、裝置影子、裝置佈建服務、任務服務。

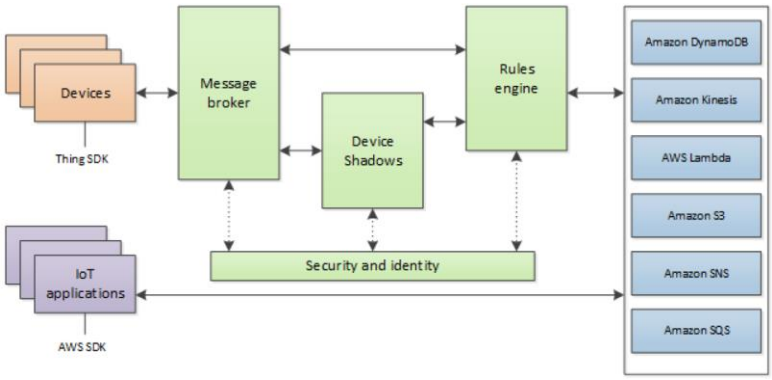


圖 9: AWS IoT 運作方式

資料來源： AWS-IoT 開發人員指南

AWS IoT 可讓已與網際網路連線的裝置連線至 AWS 雲端，並讓雲端中的應用程式與其互動。所有連線至 AWS IoT 的裝置，在登錄

檔中都要有一個項目。登錄檔會存放裝置與該裝置使用之憑證(如X.509)的相關資訊，以保護與 AWS IoT 之間的通訊。當裝置與 AWS IoT 通訊時，裝置會向 AWS IoT 提供憑證做為登入資料。

裝置以 JSON 格式對 MQTT 主題發佈訊息，用來回報其狀態。每個 MQTT 主題都有一個階層式名稱，可識別正在更新狀態的裝置。當訊息以 MQTT 主題發佈時，訊息會傳送至 AWS IoT MQTT 訊息中介裝置，再由訊息中介裝置將所有以 MQTT 主題發佈的訊息傳送至所有訂閱該主題的用戶端。

用戶端可以建立規則，定義根據訊息之內容執行的一個或多個動作。例如，插入、更新或查詢 DynamoDB 表格，或是呼叫 Lambda 函數。必要時，規則應包含 IAM 角色，授與 AWS IoT 權限使用相關的 AWS 資源。

每個裝置都有一個可存放及擷取狀態資訊的裝置影子。應用程式可以請求裝置目前狀態的資訊。裝置影子會回應請求，提供具有狀態資訊、中繼資料和版本編號的 JSON 文件。應用程式可要求變更裝置狀態，來控制裝置。裝置影子會接收狀態變更請求，更新其狀態資訊，並且傳送訊息指示狀態資訊已經更新。

相關 AWS IoT 包含以下元件描述如下。

1、 **裝置閘道**讓裝置以安全有效的方式與 AWS IoT 通訊。

2、 **訊息中介裝置**提供安全的機制，讓裝置和 AWS IoT 應用程式能夠互相發佈與接收訊息，可以直接使用 MQTT 通訊協定，或是經 WebSocket 的 MQTT 來發佈和訂閱，或是使用 HTTP REST 介面發佈。使用 MQTT 和 HPPTS 這兩種通訊協定均可透過 IPv4 及 IPv6 支援。

3、 **規則引擎**可處理訊息並與其他 AWS 服務整合。以 SQL 為基礎的語言選擇資料，處理資料，然後傳送至其他服務，例如 Amazon S3 (Object Storage)、Amazon DynamoDB (NoSQL 資料庫)和 AWS Lambda (無伺服器運算)，或是使用**訊息中介裝置**重新發佈訊息給其他訂閱者。

4、 **安全與身分服務**在 AWS 雲端對於雲端安全提供共同的責任。**訊息中介裝置**和**規則引擎**使用 AWS 安全功能，將資料安全傳送至裝置或其他 AWS 服務。**登錄**或**群組登錄**整理 AWS 雲端中與每項裝置相關聯的資源。**自訂身分驗證服務**可以定義自訂授權方，使用自訂身分驗證服務和 Lambda 函數，管理自己的身分驗證和授權策略。

5、 **裝置影子**用於存放及擷取裝置目前狀態資訊的 JSON 文件。**裝置影子服務**提供裝置在 AWS 雲端中不變的表示方式，可以對**裝置影子**發佈更新的資訊，裝置會在連線時同步其狀態，

裝置也可以對**裝置影子**發佈其目前的狀態，供應用程式或其他裝置使用。

6、 **裝置佈建服務**使用描述裝置所需資源的範本，來佈建裝置。

7、 **任務服務**定義一組遠端操作，這組操作會傳送到連接 AWS IoT 的一個或多個裝置並且執行。

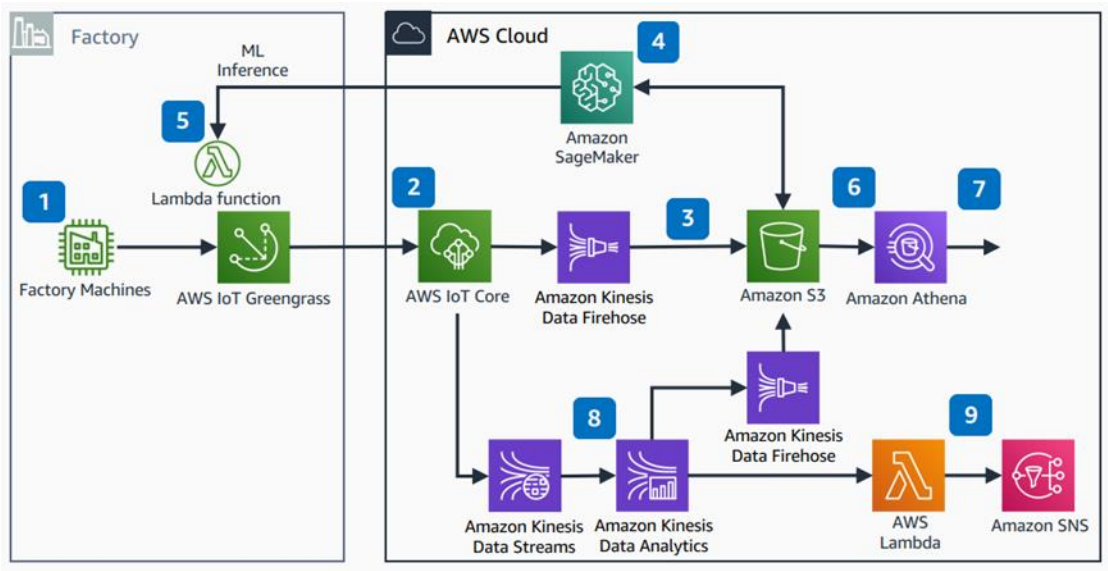
AWS IoT 整合了下列 AWS 服務: Amazon S3 (Simple Storage Service)，Amazon DynamoDB (NoSQL 資料庫)，Amazon Kinesis (大規模串流資料即時處理)，AWS Lambda (無伺服器運算)，Amazon SNS (Simple Notification Service)，Amazon SQS (Simple Queue Service)。AWS IoT API 使用 HTTP 或 HTTPS 請求來建置 IoT 應用程式。

在物聯網的情境中，裝置與 AWS 的網路連線基本上是以 AWS IoT Core 為進入點。在之後，則可以串接不同的服務，如 AWS IoT Analytics、Amazon QuickSight、AWS IoT Events、Amazon SNS、AWS Lambda 等等，這些後續的串接服務並不直接面向 IoT 裝置或一般使用者，屬於 management service，可以透過命令列工具(cli tool)或 web console 來管理或操作，不需要指定 domain name 或 IP address。

AWS 官網提供數個 IoT 的參考架構，根據 IoT 的應用情境，可以使用不同的 AWS 服務來建立許多不同類型的服務。裝置與 AWS

的網路連線基本上均是以 AWS IoT Core 為進入點，支援 IPv4 與 IPv6 兩種連接方式。

圖 10 展示一個工業預防性維護-機器學習建模與異常偵測的 AWS IoT 參考架構。在工廠端，使用了 AWS IoT Greengrass，提供邊緣運算服務，負責將 IoT 裝置感測到的資料進行預處理，並後送到 AWS IoT Core。AWS IoT Core 收集到資料後，分兩路進行處理，一路是使用 Amazon Kinesis Data Firehose 串流服務將資料放到 Amazon S3 (物件儲存服務)，提供後續的 Amazon Athena 進行資料視覺化 Amazon QuickSight，以及 Amazon SegaMaker 進行機器學習建模，工廠端的 AWS IoT Greengrass 可以下載這個模型進行異常事件偵測。另一路，則可以透過 Amazon Kinesis Data Streams、Amazon Kinesis Data Analytics，進行不同類型的處理，並透過 Amazon SNS 發送訊息給相關人事。



資料來源：https://aws.amazon.com/tw/architecture/

圖 10: AWS IoT 工業預防性維護參考架構

(二) AWS IoT 的 IPv6 支援

AWS IoT 目前在 IPv6 的支援上包含了 15 個區域，亞太地區僅包含東京、新加坡、首爾、雪梨、孟買等地，台灣還未納入。在連接設備數量相當龐大的狀況之下，IPv4 的位址已不敷使用，因此 IPv6 的支援不僅能免去網路位址轉譯(NAT)的需要，亦可滿足終端設備對於 IP 位址的需求，這顯示出 IPv6 已在物聯網當中扮演一個相當重要的角色。根據官網的說明，目前支援 IPv6 的 AWS 服務包括 Elastic Load Balancing、AWS Direct Connect、Amazon Route 53、Amazon CloudFront、AWS WAF、S3 Transfer Acceleration 與 EC2 instances in Virtual Private Clouds，以及 AWS IoT。AWS IoT 訊息中介裝置支援使用 MQTT 通

訊協定發佈與訂閱，也支援使用 HTTPS 發佈。使用這兩種通訊協定均可透過 IPv4 及 IPv6 支援。訊息中介裝置也支援透過 WebSocket 通訊協定的 MQTT。

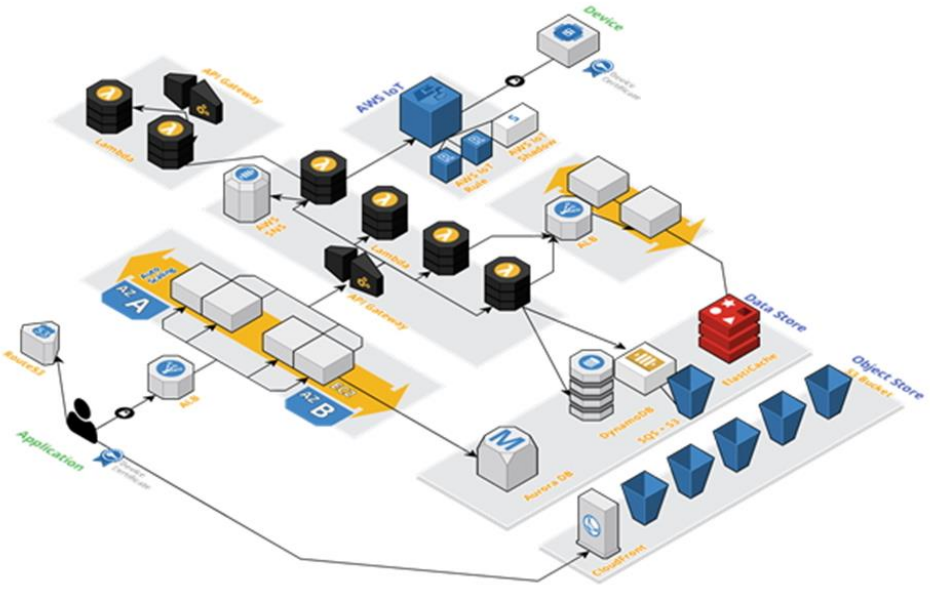
(三) AWS IoT 應用

以下簡介幾個基於 AWS IoT 的應用情境。

1、 LG ThinQ

2017 年，知名家電品牌 LG 已在全球銷售超過 7 千萬台的 Smart TV 和 5 百萬個 Home Applicans，為其內建 Wi-Fi 的 ThinQ 系列產品，LG 使用 AWS IoT 平台建立了自己的 IoT 平台，來聯結其 ThinQ 系列的 Smart 裝置與 LG 伺服器。LG 使用了 AWS IoT 與無服務器(serverless)架構，支援其空氣品質監控服務、客服機器人、和能源方案。

2016 年，LG 成功地將其家用電器的 IT 平台（包括 1,000 多個伺服器）從其數據中心遷移到了 Amazon Web Services（AWS）。該業務採用了 Amazon Elastic Compute Cloud（Amazon EC2）和 Amazon Simple Storage Service（Amazon S3），參考架構如圖 11。。



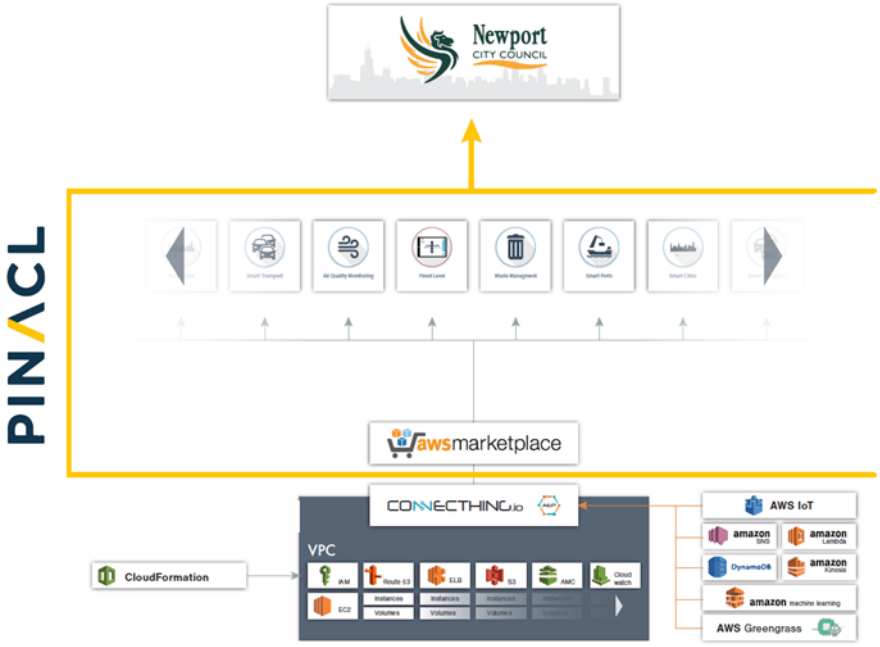
資料來源：https://aws.amazon.com/tw/solutions/case-studies/lg-electronics/

圖 11: LG 在 AWS 上的架構參考

2、 英國威爾斯 Newport 市

英國威爾斯 Newport 市在 AWS 上面實現了三個 Proof-of-Concept 的計畫，分別是空氣品質、洪水控制和垃圾管理，，參考架構如圖 12。

該市之前已經在市中心和主要公共建設上提供 Wi-Fi 上網服務。原本，該市只有 85 個空氣品質監測站，只有月平均值可以粗估空氣品質。在排水系統上，只能人工手動撿查，經常只有被洪水破壞後才能知道。而垃圾筒經常滿出來，造成污染和影響市容。



資料來源：https://aws.amazon.com/tw/solutions/case-studies/CityofNewport/

圖 12: 英國威爾斯 Newport 市在 AWS 上的架構參考

他們在許多地方佈置了空氣品質感應裝置、在排水系統上加裝水位監控裝置，在垃圾筒上放了感應器，透過 AWS IoT 與 AWS 的 Elastic (彈性)服務，可以少量的試點，再逐步擴大到更多的區域。如此，許多區域空氣品質可以得到即時的監控。排水系統的水位的即時監控，讓他們能更早發現問題，避免洪水造成災害，同時，對於清潔人員的安排，可以更有效的巡訪較多垃圾的區域，及早清運滿出來的垃圾筒，美化市容。

3、 美國 Rachio

Rachio 是一家在美國 Colorado 生產製造灌溉用灑水控制器的廠商，採用 AWS IoT 做為其 Wi-Fi 智慧灑水控制器的管理平台。這些智慧灑水控制器可以透過網路查詢天氣(下雨)預報，配合使用者指示的灑水情境(時間長短、水量大小、灑水時間、灑水區域、植物種類、鹽份)來決定灑水排程。

三、**Microsoft Azure 平台與應用**

(一) Azure IoT 平台

Micorsoft Azure IoT 產品組合提供兩種途徑讓您建立自己的解決方案：

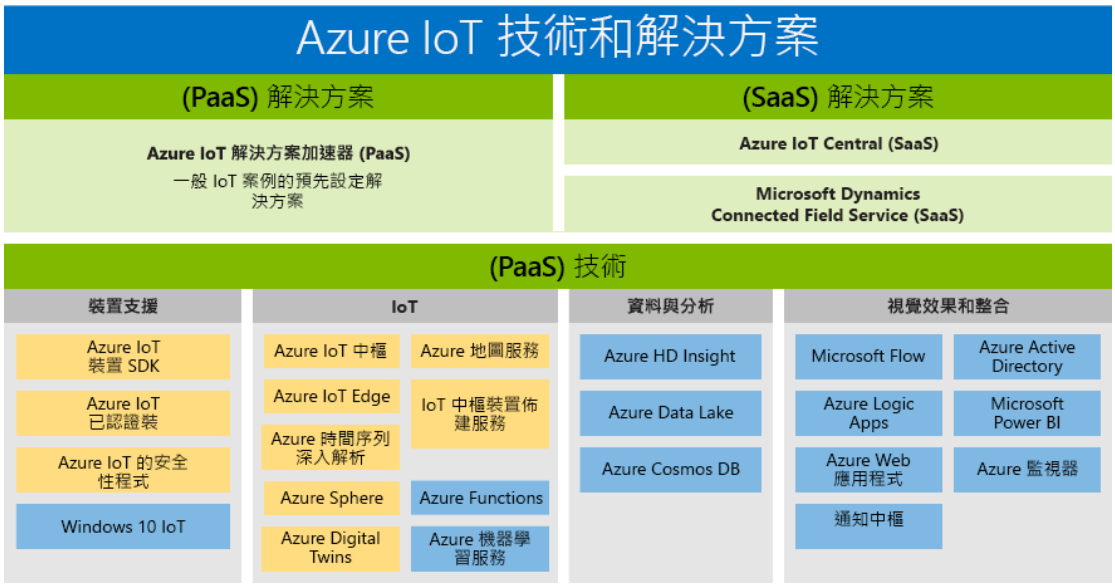
1、 平台即服務 (PaaS)：使用下列任何服務建置您的應用程式。

(1) Azure IoT 解決方案加速器：預先設定的企業級解決方案集合，可讓用戶加快自訂 IoT 解決方案的開發速度。

(2) Azure Digital Twins 服務，可讓用戶建立實體環境的模型，以使用空間智慧圖形和特定網域物件模型建立內容感知的 IoT 解決方案。

2、 軟體即服務 (SaaS)：可讓用戶快速開始使用 Azure IoT 中心這個 SaaS 解決方案，來開發 IoT 應用程式，而無須接觸到複雜的 IoT 解決方案。Azure IoT 中心是一種無程式碼的

IoT 解決方案，可以在數分鐘內建立裝置型號、儀表板和規則。



資料來源：

https://docs.microsoft.com/zh-tw/azure/iot-fundamentals/iot-services-and-technologies

圖 13: Azure IoT 技術和解決方案

Azure 中有數個與 IoT 相關的服務。列舉如下：

1、 IoT Central：這是 SaaS (Software as a Service) 解決方案，可協助連接、監視及管理 IoT 裝置。透過選取適用裝置類型的範本，然後建立及測試基本 IoT Central 應用程式，讓裝置操作員

佈建新的裝置、監視裝置。此一服務適用於簡單而不需要深入自訂的解決方案。

2、 IoT solution accelerators (解決方案加速器)：這是 PaaS 解決方案的集合，可用來加速開發 IoT 解決方案。從所提供的 IoT 解決方案著手，然後再根據需求來完整自訂此解決方案。需要 Java 或 .NET 技能來自訂後端，並需要 JavaScript 技能來自訂視覺效果。

3、 IoT Hub (中樞)：此服務可讓裝置連線到 IoT 中樞，並監視及控制數十億個 IoT 裝置。如果需要讓 IoT 裝置與後端進行雙向通訊，特別實用。這是 IoT Central 和 IoT 解決方案加速器的基礎服務。

4、 IoT Hub Device Provisioning Service (中樞裝置佈建服務)：這是 IoT 中樞的協助服務，可用來安全地將裝置佈建到 IoT 中樞。使用此服務，可以輕鬆且快速地佈建數百萬個裝置，而非一個一個逐一佈建。

5、 IoT Edge：建立在 IoT 中樞之上，此服務可用來分析 IoT 裝置上的資料，而並非雲端中的資料。藉由將部分工作負載移到邊緣裝置，可以減少傳送至雲端的訊息量。

6、 Azure Digital Twins：此服務可以讓用戶建立完整的實體環境模型。可以為人員、空間和裝置之間的關聯性和互動方式建立模型。例如，用戶可以預測工廠的維修需求、分析輸電網路的即時能源需求，或最佳化辦公室的可用空間。

7、 Time Series Insights (時間序列深入解析)：此服務可讓用戶儲存、視覺化及查詢 IoT 裝置所產生的大量時間序列資料。可以搭配 IoT 中樞來使用。

8、 Azure Maps (地圖服務)：此服務提供地理資訊給 Web 和行動應用程式。它有一組完整的 REST API 和 Web-based JavaScript 控制項，可用來建立有彈性的應用程式，並且適用於 Apple 和 Windows 裝置的桌面或行動應用程式。

有些服務，例如 IoT Central 和 IoT 解決方案加速器，會提供範本，以協助建立解決方案，快速上手。也可以使用其他可用服務來完整開發新的解決方案，取決於開發者需要多少協助和多大的控制權。

Azure IoT Hub 支援的通訊協定共有四種，分別是 HTTPS、AMQP、AMQP over WebSockets、MQTT。傳入的訊息目前支援 JSON 格式的字串。

(二) Azure IoT 的 IPv6 支援

目前 Azure preview 階段的 IPv6 支援是在 IaaS (infrastructure) level。因為 Azure IoT Hub 是屬於 PaaS (platform)服務架構。Azure 目前有積極在規劃 VNET 及 IPv6 支援，但時間還不確定。

官方的建議是，若是現在當下要設計 IPv6 架構，可以先用 IaaS 部分服務，或是先採用 IPv4 在 Azure IoT Hub 等參考架構上開發，待 Azure IoT 支援 IPv6 後，再將相關服務移植到支援 IPv6 的新服務上。

(三) Micorsoft Azure IoT 應用

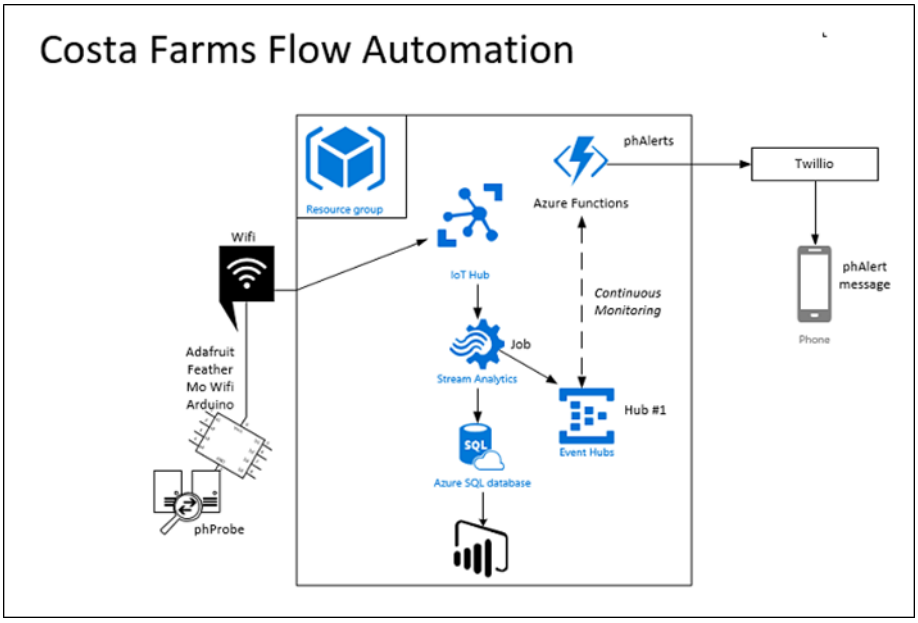
以下簡介幾個基於 Micorsoft Azure IoT 的應用情境。

1、 Costa Farms：使用 IoT 自動化控制 pH 值

(1) 客戶問題：Costa Farms 近年開始創新並引進了新的室內植物，出售給 Walmart、Home Depot 和 Lowe's 等大型商店。pH 值是植物健康的關鍵因素之一，為了提高養分吸收使植物健康，進而提高產量，需要更加密切地監測和即時調節水和流質肥料中的 pH 值。然而，對他們來說，在整個植物生命週期內不斷測量和調節 pH 值是耗時、沒效益且困難的。

(2) 解法方案：將帶有 pH 感測器設備連上 Azure IoT Hub，在水力系統上測量精確的 pH 值。這個方案使用了 Adafruit Feather

M0 Wi-Fi 和 pH 感測器，Microsoft Azure、Azure IoT Hub、Azure Stream Analytics、Azure Event Hubs、Azure Functions、Azure SQL 數據庫以及透過 Twilio 發送的訊息，以此構建了一個客戶可以在其解決方案中使用的概念驗證。其系統架構如圖 14 所示。包含①測量數據發送到 Azure IoT Hub，然後傳入 Azure SQL 數據庫，並儲存於 Power BI。②數據透過 AzureSQL 中的 Stream Analytics 發送，事件中心接收進入的數據。③事件中心配置為 pH 警報和 pH 數據，然後觸發 pH 警報發送。④使用 Azure Functions，通過 Twilio 發送訊息。⑤使用 Azure Functions，根據最小和最大 pH 值，向 Twilio 發送訊息。⑥最終將 pH 警報訊息發送到種植者的行動電話。



資料來源：https://microsoft.github.io/techcasestudies/iot/2016/11/03/CostaCorp.html

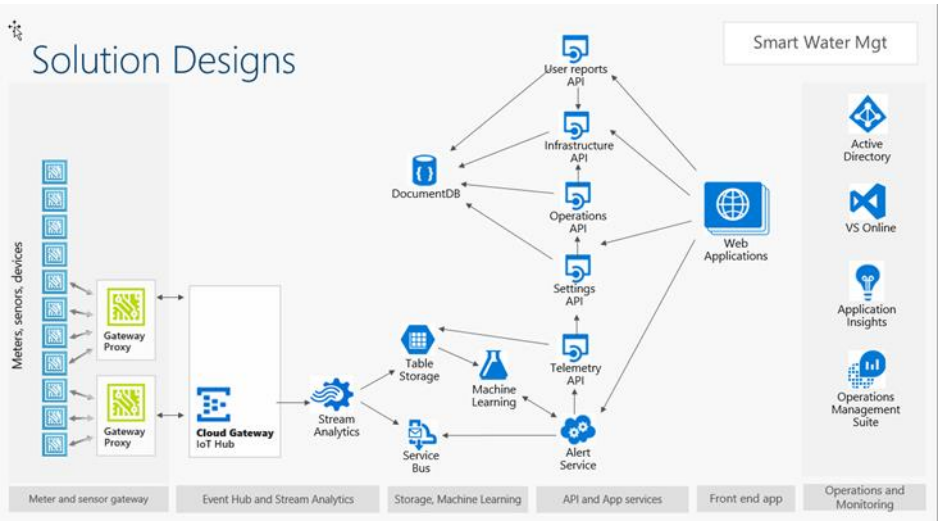
圖 14: Costa Farms 使用 Azure IoT 解決方案自動化控制 pH 值

2、 Powel：使用 IoT 檢測漏水情況

(1) 客戶問題：Powel 公司的配水系統面臨兩項挑戰，一是基礎設施中各種組件的使用年限，二是水壓的設定會保持一定的等級，因此若有破洞將增加流出的水量。在發生火災時，壓力會設定得更高，消防員需要為他們的水管施加額外的壓力。以下為 Powel 的目標：①尋找一種安全的，可擴充的方式來傳送和存儲遙測數據。②了解如何為機器學習準備遙測數據。③配置 Azure 機器學習以對數據執行異常檢測。④將異常檢測結果連接到 SmartWater application。

(2) 數據蒐集準備：定位漏水是個實質的問題，利用特殊的麥克風連接到水管，然後用聲波對洩水處的大致位置進行三角測量。另外，收集盡可能越多的數據並查看它們和不同方法之間的關聯，如交通狀況、天氣或其他外部數據來源是否可以幫助確定漏水情況，並找到相關的第三方數據來源。

(3) 解決方案：該解決方案的關鍵部分是使用 Azure 機器學習，SmartWater 會比較監測到的數值與學習模型的分析結果，若有異常，操作員將在其應用程式中看到警報，並立即採取適當的操作。目標是儘早阻止漏水，未來安裝更多感測器和智慧水錶時，該解決方案將有可能提供更多效益。



資料來源：https://microsoft.github.io/techcasestudies/iot/2016/11/29/Powel.html

圖 15: Powel 使用 Azure IoT 解決方案檢測漏水情況

3、 GCBA：使用 IoT 無人機解決方案清理河流

(1) 客戶問題：Matanza-Riachuelo 河被河邊眾多工廠產生的大量工業廢物污染，尤其是製革廠。最危險的污染物是重金屬（砷，鉻，銅，鋅和鉛）和盆地飽和層的廢水。例如，鉻在土壤中的平均值為 1,141 ppm，顯著高於建議的 220 ppm 標準。2013 年發表在 Salud Colectiva 上的一篇文章發現，從 Matanza-Riachuelo 河流域附近井中取出的水，80％因污染而不能安全飲用。

(2) 解決方案：①無人機將從同一個點降落並起飛，讀取感測器並將數據儲存在本身記憶體中。之後，設備將數據同步到 Azure IoT Hub和開發的後端。感測器將測量以下內容：GPS、GSM、pH 值、溫度、流向、氯、鈣、Iodes、硝酸鹽、亞硝酸鹽、溶氧量、混濁度、導電率。②無人機運行 Windows 10 IoT 的 Raspberry Pi 3。連接到 Raspberry Pi 3 的是感測器和 GSM 模塊，用於將數據發送到 Azure IoT Hub，再將感測器數據發送到 Azure Service Bus Queue，包含緯度，經度，設備 ID 和時間標記(Timestamp)。③ Azure Service Fabric 部署三位工作者，Worker1 將原始數據作為文件發送到 Azure Blob

儲存，然後將感測器數據發送到另一個佇列；Worker2 從佇列中獲取感測器數據，驗證其數據並將其發送到 Azure 表儲存，然後再將更新訊息發送到另一個佇列；更新訊息到達時會觸發 Worker3，在地圖上顯示的數據。

四、**Google IoT 平台與應用**

(一) GCP IoT 平台

Google Cloud Platform for IoT 的中心是 Cloud IoT Core。

Cloud IoT Core 是一套全代管的 IoT 服務，可讓客戶以簡便又安全的方式來連結及管理散佈在全球各地的數百萬部感測裝置，擷取、儲存、分析這些感測裝置中的資料。結合 GCP 平台上的其他服務，Cloud IoT Core 可以提供企業一應俱全的解決方案，方便即時收集、處理、分析並視覺化 IoT 資料，以利提高作業效率。

Cloud IoT Core 有兩項主要元件：裝置管理員和通訊協定橋接器。裝置管理員可讓客戶安全地設定及管理各個裝置。裝置管理員會建立裝置的身分，並且在連線時提供裝置驗證機制。此外，裝置管理員還會保存每個裝置的邏輯設定，並可用於從雲端控制裝置。針對所有裝置連線，通訊協定橋接器會採用自動負載平衡技術為通訊協定提供連

接端點。通訊協定橋接器支援透過業界標準通訊協定，如 MQTT 和 HTTP 建立安全連線。此外，通訊協定橋接器也會將所有裝置遙測事件發布至 Cloud Pub/Sub，以便下游分析系統接手處理。

Cloud IoT Core 是一個 GCP 中的一個無服務器元件，能夠支援任意數量的裝置連結到 Cloud IoT Core 裡，無需考量服務器的提供、設定、調校等等需要 IT 人員進行的管理作業。

Cloud IoT Edge 是一個基於 Linux 的裝置，結合一組軟體與服務，是供完整的 IoT 邊緣運算，可以在資料來源端執行與應用機器學習模型。在硬體架構上，Cloud IoT Edge 裝置可以配置一個或多個 Edeg TPU (Tensor Processing Unit)。Edeg TPU 是由 Google 為 TensorFlow 深度學習框架開發的小型 ASIC 硬體加速器。由 Google 開源的深度學習框架 TensorFlow 是一套知名的深度神經網路，在機器學習領域中有很大的成果，並已應用在許多的實際案例中。Cloud IoT Edge 包含 TensorFlow Lite 和 Edge IoT Core。TensorFlow Lite 是一個為了行動裝置和內嵌式裝置設計的 TensorFlow 框架實現，內建 Edge ML，可執行在 GCP 上面建立且優化過後的 TensorFlow 模型。Cloud ML Engine 是 GCP 裡的一個無服務器、全代管的元件，是 Google 機器學習的核心，提供 TensorFlow 深度學習服務，建立深度神經模型。

參考架構如圖 16 所示。

1、 場域中的感測裝置將感測資料傳送到 Cloud IoT Core。使用 MQTT 協定，無論感測裝置的來源位置為何，全球使用一個端點 mqtt.googleapis.com。這個設計讓 Cloud IoT Core 解決方案無需考慮 GCP 端的 region 位置，也無需考慮跨 regions 的 GCP 服務裡的設定。

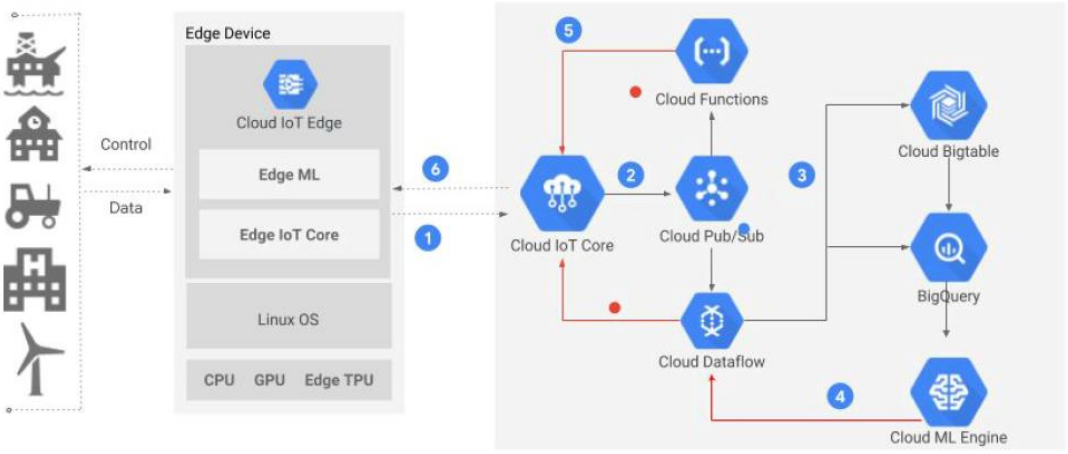
2、 Cloud IoT Core 收到資料後，後傳到 Cloud Pub/Sub 服務。Cloud Pub/Sub 是 GCP 中的一個無服務器、全代管的訊息佇列服務與事件轉發。Cloud Pub/Sub 會將資料以不同的通知主題送到佇列中。主題會被儲存 7 天，並可以被場景需要的其他後續服務立即存取。

3、 由 Cloud IoT Core 或 Cloud Pub/Sub 起，資料處理可以經過任意數量的不同路徑。比如，感測資料可以被 Cloud Dataflow 轉換，並儲存在 Google Cloud Storage、Google BigQuery 或 Google Bigtable 中。

4、 研究人員可以嚐試發展智慧系統，比如說，事件偵測與通知警告。他們可以使用儲存在 Google Cloud Storage 中的資料，透過 Cloud Machine Learning (ML) Engine 來訓練與修正模型。

5、 在這個參考架構中，使用 Cloud Functions 訂閱 Cloud Pub/Sub 轉發的不同主題資料。Cloud Functions 也是 GCP 中的一個無伺服器、全代管服務，它是一個執行環境可以運行單一目標的特定函數，用以響應事件。同時使用數個函數可以快速的評估真實的狀況。若滿足某些預先設定的臨界值，可以立即觸發警告通知。

6、 控制資料可以由 Cloud IoT Core 傳送回 IoT 裝置，必要時，可透過 Cloud IoT Edge 傳送。如，可將一個經 Cloud ML Engine 訓練好的深度神經網路模型下載到 Cloud IoT Edge，由 Edge TPU 在本地就近執行。



資料來源：Google Cloud Platform - IoT Partner Quickstart

圖 16: Google Cloud Platform 的 IoT 參考架構

(二) GCP IoT 的 IPv6 支援

GCP 目前支援的 IPv6 位址只限通用位址，且只適用於 HTTP(S)、SSL Proxy 和 TCP Proxy 負載平衡器。

(三) GCP IoT 應用

以下簡介幾個基於 GCP IoT 的應用情境。

1、 Smart Parking

(1) 關於 Smart Parking：在紐西蘭、澳大利亞和英國營運，為全球城市和企業提供點到點的智慧停車管理/智慧城市解決方案。

(2) 應用原理：核心產品是一個名為 Smart Park 的傳感器系統，包括①地面傳感器，該傳感器使用紅外線和電磁技術記錄車輛的停靠，並與停車場出入口進行通訊。這使管理員可以及時了解停車場的使用情況並管理容量。②提供自動導引和指示牌，告訴客戶在一個停車結構或城市街道區域的不同位置上有多少可用車位。③超時功能，使停車場管理員能夠識別在限時停車格的車輛是否已經超時。經營者可以通知檢查人員採取強制行動，例如發出超時通知。

(3) 應用範圍：可用於購物中心、商業停車場、機場、大學和市政街道等環境。Smart Parking 已在全球部署了 50,000 多個傳感器來支援停車系統。

2、 Oden Technologies

(1) 關於 Oden Technologies：將工業硬體，無線連接和大數據架構整合到一個雲端基礎的平台中，製造商可以透過他們選擇的任何設備來分析和優化其生產。

(2) 背景與目標：使用物聯網改進當今的工廠。透過網際網路相互連接的龐大的物(人)，減少浪費、提高效率與各行各業的安全性。透過無線連接，大數據和雲端計算相結合，引領製造業的物聯網創新。

使用數據來改善製造業實際上與製造業本身一樣古老。但是，製造業的電腦化已導致對數據收集和處理方式以及可用數據量的巨大而迅速的改變。Oden 的目標是幫助製造商利用這些數據快速趨勢分析，甚至警告機器故障。視覺化可以改善製造和維護流程的機會，從而減少浪費並提高利潤。

(3) 解決方案：①Oden 設計並開發了數據收集設備，該設備可以插入任何類型的機器中，並且可以以最小的複雜性和設置時

間來進行無線傳輸數據。設備安裝後，Oden 技術平台將處理數據，以為製造商提供易於理解的分析。該平台產生的分析為工廠工程師提供了數據，例如詳細的根本原因分析，及時工廠範圍內的性能以及趨勢分析。② Oden 運行 GCP，包括 Google Compute Engine、Google Cloud Pub/Sub、Google Cloud Bigtable、Google Stackdriver，和 Google Kubernetes Engine。從廠房，Oden 無線設備獲取數據。然後，Google Cloud Pub/Sub 及時將數據發送到 Google Cloud Bigtable，在其中使用 Oden 專有的分析工具處理數據。Google Stackdriver 支援 Google Cloud Platform 監視，日誌記錄和診斷，有助於 Oden 交付其雲端平台。Oden 建立了由 Kubernetes Engine 驅動的儀表板，該儀表板從 Google Cloud Bigtable 中提取了分析數據，為客戶提供其生產線的及時可見性。③ Oden 可以幫助每間工廠平均每天在一條生產線上獲取並存儲大約 1000 萬個指標性資料。度量標準可能包含極其詳細的細節，例如機器的電量、消耗的原材料量以及生產的物料量。傳感器還可以獲取並傳輸環境訊息，例如溫度和濕度，以便製造商可以識別與天氣有關的季節變化和季節性影響。

3、 Vagabond

(1) 關於 Vagabond：Vagabond 是自動售貨行業的技術平台，將即時商務智慧傳遞到操作員的手掌上。

(2) 背景與目標：該公司啟動了一個物聯網網路，將操作員即時連接到他們的每台自動售貨機，使他們可以從辦公室或道路上獲取有關每台機器的營運和銷售數據。為了補強其 Mobile Web 和 ERP 工具，該公司需要一個映射平台，使操作員能夠獲得機器的精確位置並有效地擬定運輸路線。

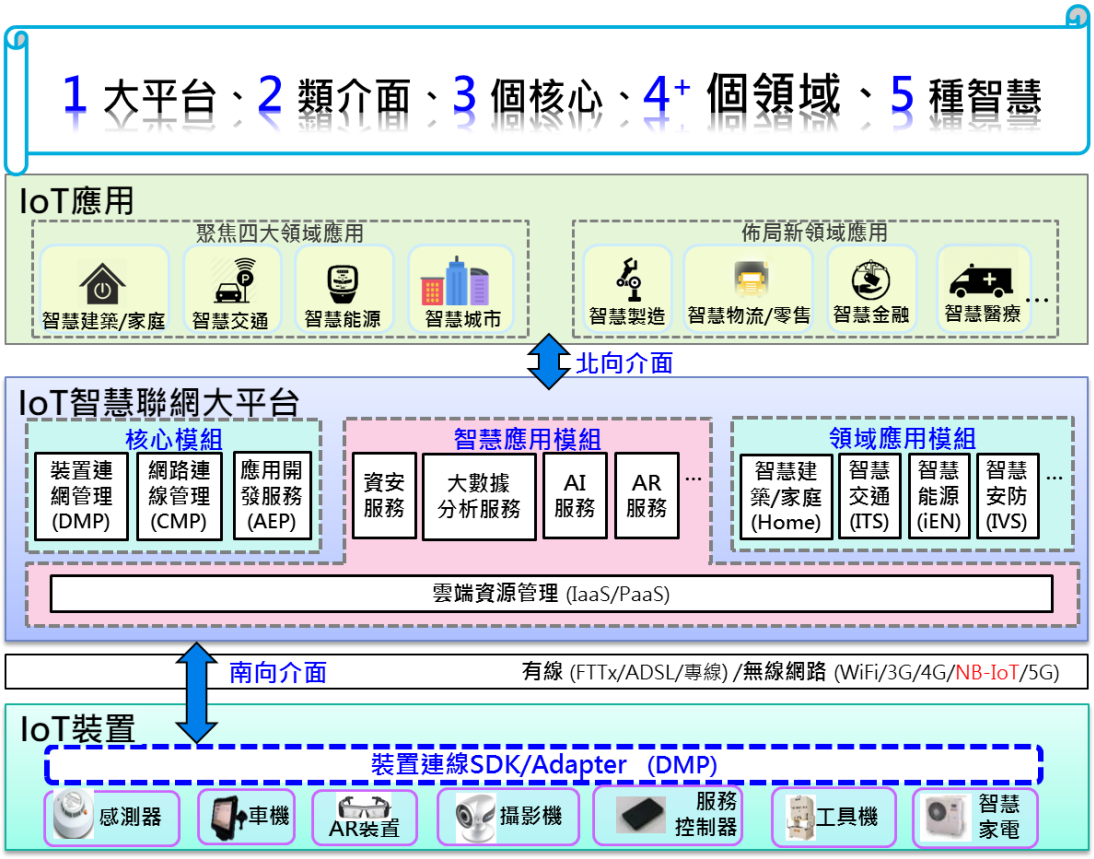
(3) 解決方法：①使用 Maps JavaScript API 構建了一個 Web 應用程式，將每位操作員的自動售貨機的位置顯示在地圖上。有關機器的重要訊息(例如庫存水準和收取的現金量)會覆蓋在地圖上，以便系統可以根據每台機器的需求和地理位置進行過濾。操作員使用此訊息來確定何時需要補充庫存，並建立有效的運輸路線。②安裝機器後，操作員使用部署了 Places API 和 Geocoding API 的行動應用程式來確定其在建築物中的位置。

五、國內電信業者物聯網平台介紹

(一) 中華電信

中華電信推出的 IoT 智慧聯網大平台，藉由提供感測資料之收集、處理、儲存、供應及管理等，來建構出高可用性、高可靠性、高處理量的智慧感測資料中心。主要的功能包含網路管理、裝置連線管理、應用開發服務、大數據分析以及資安機制，可使開發者在安全環境下更快速導入應用功能。

中華電信 IoT 智慧聯網大平台，包含 1 個平台架構、2 類介面、3 個核心、4+個領域、5 種智慧，建構 IoT 產業生態系。平台支援三種傳輸協定: (1)RESTful、(2) MQTT、(3) WebSocket。



資料來源：https://iot.cht.com.tw/iot/developer/introduction

圖 17: 中華電信 IoT 智慧聯網大平台

3 核心服務包含：裝置連網管理、網路連線管理、與應用開發服務，支援 IoT 產業標準(OCF)、NB-IoT 裝置連網、裝置 PnP 等，提供多版本裝置連線 SDK/Adapter/範例程式、Android/iOS/Cordova 版 IoT APP 框架，企業用戶可透過單一介面(WEB)或 API 自主網路連線管理與監測。

4+領域應用服務包含智慧建築/家庭、智慧交通、智慧能源、智慧安防，支援智慧家電業界通訊標準(TaiSEIA 101)、TTIA 營業大客車車載標準(台灣車載資通訊產業協會)、Modbus、BACNet、OPC Server 等通訊協定、提供能源效能指標 API、電費計算、最佳契約容量分析等用電分析 API、支援 ONVIF 通訊協定，提供市面上約 5,000 種 IP CAM 設備連線納管等等。

5 種智慧應用服務，人工智慧(AI)提供深度學習運算環境、擴增實境(AR)服務提供即時雙向影音協作、智慧型眼鏡 AR 文字/繪圖資訊顯示、區塊鏈(Blockchain)服務提供不可否認之區塊鏈智慧存證服務、大數據服務提供親和性介面、完整的大數據分析工具，與資安服務支援 PKI 憑證雙向認證、TLS 資訊加密、通訊風險偵測機制。

而智慧聯網大平台也擴及到各領域的應用，包含交通、能源管理、健康醫療、政府等方面，如與台電合作的智慧讀表、中華電健康照護

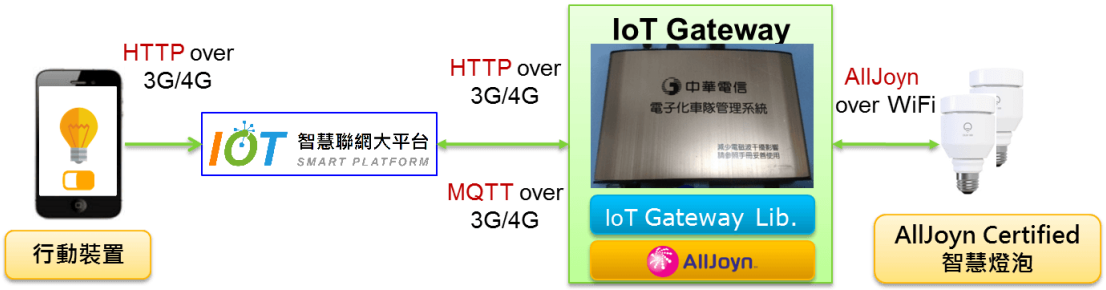
雲等等，提升物聯網在台的發展與可能性。

以下簡介幾個基於中華電信 IoT 智慧聯網大平台的案例。

1、 AllSeen

以開放原始碼專案 AllJoyn 為基礎所發展成的聯盟，其目的是要建立一個共通的物聯網標準，讓各種行動裝置、家電產品及汽車之間進行連結。

圖 18 展示透過行動裝置遠端控制通過 AllJoyn 認證的 LIFX 智慧燈泡。在這個架構裡，使用者的行動裝置安裝 IoT Mobile APP，透過 IoT RESTful APIs 存取燈泡設備資訊與狀態。IoT Gateway 實作 IoT Gateway Lib 和 AllJoyn 協定，以連結 IoT 智慧聯網大平台與 AllSeen 認證的產品，即這個案例裡的燈泡。

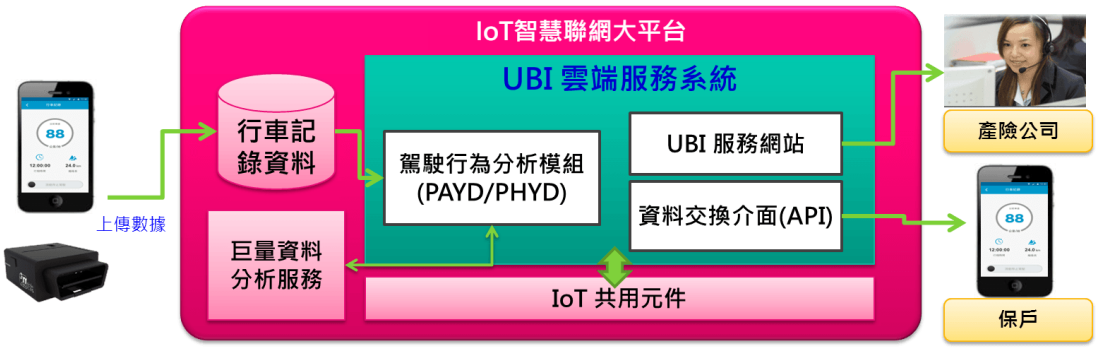


資料來源：https://iot.cht.com.tw/iot/developer/case

圖 18: AllSeen 使用中華電信 IoT 智慧聯網大平台

2、 Driving Insight

駕駛行為計費服務系統可了解使用者平日開車習慣。採用 UBI Dongle 設備與 IoT 服務平台連結，透過 RESTful API 儲存感測資料於 IoT 智慧聯網大平台，使用巨量資料分析服務進行駕駛行為風險分析，為了開創國內新世代車險的服務商機。



資料來源：https://iot.cht.com.tw/iot/developer/case

圖 19: Driving Insight 使用中華電信 IoT 智慧聯網大平台

(二) 遠傳電信

遠傳電信積極整合生態圈資源，與雲端物聯網產業協會共同發行「物聯網生態圈手冊」，推動產業結盟。以電信級網路提供通訊服務，積極布局物聯網與 5G，輔以連線管理平台，協助企業有效掌握 SIM 卡流量與狀態。

在網路層，遠傳物聯網目前支援 4 種連線方式，NB-IoT、LTE-M、CAT-1 與 IoT 4G。其中，NB-IoT 與 LTE-M 適合低速率、高時延的情

境，CAT-1 適合低速率、低時延的情境，而 IoT 4G 適合高速率、低時延的情境。

遠傳物聯網平台服務提供 4 種服務，CMP 連線管理平台、DCP 設備連接管理平台、eSim 全球管理平台、CAT (AEP)物聯網平台。

1、 CMP連線管理平台:可將已裝有SIM卡的終端裝置(如路燈、機車、感測設備等)，以及企業自身的系統進行串連。每張SIM卡的資料以圖表化的方式呈現在平台上。當流量超出或SIM卡發生異常狀態時，客戶會收到告警通知，方便即時排除異常狀況。

2、 DCP 設備連接管理平台：與全球超過 400 家電信夥伴合作，企業不需逐一與各國電信商洽談。產品在本國組裝後直接出口，不需在他國進行二次加工，除大幅降低企業成本，也能夠確保產品品質。

3、 eSim 全球管理平台：設備製造廠可以透過平台，自由切換跨國電信業者的 SIM 卡資訊，單一 SIM 卡、單一平台，全球同步管理 SIM 卡裝置。過往，設備出口至不同國家時，企業必須取得各國電信業者的 SIM 卡，以及簽訂不同漫遊資費合約，同時設備在製造地生產後，又需進行拆卸設備進行 SIM 卡置入的二次加工繁瑣流程。

4、 CAT (AEP)物聯網平台：垂直應用的物聯網平台服務，具有租戶管理、裝置管理、場域抽象設計、框架式的規則引擎，建置彈性，可快速反應市場變化等。具有擁有可擴充與可程式化的規則撰寫，可以滿足不同領域建置的彈性需求。

資料來源：https://www.fetnet.net/enterprise/campaign/iot/intro.html

圖 20: 遠傳物聯網服務

遠傳提供多元應用解決方案,如智慧車聯、智慧路燈、智慧大樓、能源管理、智慧停車、智慧偵測、資產追蹤、智慧門鎖、Health 健康

等等。

1、 智慧大樓：將感測裝置(如偵測空氣品質、溫度、濕度、電量資訊等等設備)放置於大樓空間。透過 NB-IoT 網路服務，將感測資料傳回遠端機房，進而得知該空間的網路狀態。

2、 智慧車聯：將感測裝置安裝於汽機車上，透過 NB-IoT 網路服務，將資料傳回遠傳機房。客戶與使用者可以透過平台即時監控汽機車位置及行駛路徑狀態。

3、 智慧偵測：提供智慧偵測解決方案，透過感測器外接功能，快速達到農林漁牧業之服務推廣。如結構安全監測、水位監測、雨量監測、空汙監測。

4、 資產追蹤：透過遠端監控資產動向與狀態，可快速標記任何裝置的即時位置，支援全球漫遊。

5、 能源管理：提供完整的能源管理系統，搭配電表、環境感測器，產生用電分析並給予節電建議。優化日常營運、即時參數建議、預知設備狀態、彈性動態調控。

(三) 台灣大哥大

台灣大哥大物聯網服務(M2M 或 IoT)提供物聯網數據服務，主要應用場景為企業用途與消費者用途兩種市場。

企業物聯網包含公用事業(水、電、瓦斯表、垃圾桶、環境監控等)、物流事業(資產追蹤、供應鏈管理、智慧物流等)、智慧城市(智慧路燈、智慧停車、智慧交通等)與其他(智慧農業、智慧零售等)。

消費者物聯網則包含智慧生活(智慧穿戴、醫療監控、車輛 UBI 等)與智慧家庭(煙霧偵測、門禁管理、居家監控、機器人等)。

台灣大哥大提供三個方向的解決方案與服務。

1、 SIM 管理平台：幫助企業快速自主的訂購 SIM 卡、查詢 SIM 卡的狀態、開通或停用 SIM 卡、動態管理資費。

2、 eSIM (embedded SIM)與 Profile 管理平台：採用 eSIM，並透過 Profile 管理平台來管理在不同國家可以切換不同的電信業者，享受最低上網資費。

3、 NB-IoT 的新應用開發：GSMA 推動 NB-IoT 技術規格，訴求長距離、低成本、低功耗的物聯網應用情境。

(四) 亞太電信

亞太電信提供 GT 智慧生活一站式(One-Stop-Shop)完整解決方案的物聯網服務，提供模組與晶片、終端設備、網路連接、應用平台、系統整合、客製服務到 B2B 電商媒合。

目前，亞太電信正在積極建立一個涵蓋全台灣的物聯網實驗網，

從智慧測量設備做起，包括智慧電錶、智慧水錶、智慧瓦斯錶等設備，利用集團強大的業務網路，加速物聯網生態系統的發展，整合物聯網解決方案，加速在亞太地區實現智慧城市。

透過母公司鴻海集團策略性投資，加強硬體的生產製造和軟體服務，在網路層應用 LoRaWAN 技術與物聯網平台連結，提供解決方案至台灣、中國及亞洲其他地區。

1、 跨境物聯服務：從物聯網服務供應商來說，傳統上，全球物聯網服務必須面對世界各地的電信商，包含洽談資費服務、不同 SIM 卡的安裝與管理，漫遊資費成本高，受各國法規影響，設備連線狀況難以掌握。

亞太電信提供單一連線管理平台，可以即時掌握出口各國的設備連線狀況，還有 35 個國家在地資費。企業主不需再花費時間、精力與各出口國當地電信商協商資費方案。

2、 連線管理平台(CMP)：協助物聯網服務供應商及設備製造商管理設備連線狀態，即時查詢傳輸流量。

(五) 台灣之星

台灣之星物聯網以「最務實的物聯網傳輸夥伴」為定位，相信物聯網服務的關鍵是傳輸，專注發展現階段技術成熟、穩定且擴充彈性

大的 4G LTE。提供總量計費型資費的其特色之一，不必一個門號一個門號付月租費。提供免費的連網管理平台，可以自主管理傳輸服務，提升商轉營運效率。

連網管理平台特色如下：

1、 連網設定：SIM 卡狀態及功能即時調整與彈性管理。

2、 資訊管理：傳輸量、帳單即時查詢，隨時掌握使用狀況。

3、 異常告警：監控傳輸，異常自動警示。

4、 介面友善：簡單直覺，快速上手。

應用實例包括：

1、 智慧自動販賣機：首家加入「第三方支付」開發商，實現自動販賣機的智慧零售應用。可以多元的即時線上支付，即時提供正確的補貨資訊，進行多媒體影音廣告推播。

2、 整合影像車隊管理系統：系統掌控行車狀況、駕駛行為、勤務作業。智慧車機整合多路攝錄鏡頭，回傳長程移動時的沿途影像，連線行車管控中心進行即時監控。

3、 太陽能發電控管系統：協助太陽能光電能源科技業者，進行資料採集及傳輸，包含太陽能工作場域暨設備影像監控，透過雲端聯網智慧監控系統，進行即時監控。

第三章　結論與建議

第一節　結論說明

在與廠商訪談的過程中，物聯網應用廠商仍以閘道器(Gateway)作為裝置與網際網路(Internet)聯結的中介，加上大部份的應用並無傳輸延遲上的嚴峻考量，因此，主流仍是無 IP 或使用 IPv4 的組態，且對是否支援或採用 IPv6 採取觀望的態度，主因為市場上的需求仍不明顯。

國際雲端三大平台 Amazon AWS, Microsoft Azure, 與 Google GCP，在部份產品支援 IPv6。其中，AWS IoT 支援 IPv6，而 Azure IoT 與 Google IoT 而仍未支援 IPv6。此一觀察，與之前廠商訪談的結果一致。

IETF 從連結層、網路層、傳輸層到應用層幾個面個都有相關的 RFC 說明標準實施方向。在應用層有輕量級的 CoAP 系列 RFC 來替代 HTTP，用二進制的 CBOR 訊息來取代純文字的 JSON 訊息。在傳輸層與網路層，同樣有輕量級的 6LoWPAN 來替代完整的 IPv6 協定堆疊，並制定 RPL 相關路由協定來協助物聯網環境裡可能遇到的情形。同時，在低功耗有損網路 LLN 的概念下，針對不同的實體網路制定相關的協定，以協助受限制裝置在受限制網路裡完成資料傳輸。

另一方面，在與廠商訪談的過程中了解到，IETF 製定的物聯網相關 RFC 卻非廠商實作物聯網應用的主要考量。從三大國際雲端平台的物聯網服務 Amazon AWS IoT、Microsoft Azure IoT 與 Google Cloud Platform IoT 來看，最受支援的通訊協定仍是 MQTT 與 HTTPS，CoAP 則是需要透過第三方軟體的協助才能實現。市場需求仍是廠商開發產品的第一個考量。

第二節　　建議事項

雖然目前廠商在實作物聯網產品與應用時，IPv6 與 IETF 相關 RFC 並非最重要的考量，主因是市場的需求不明確，以及網路環境仍未全面開通 IPv6。就技術層面來說，由 IPv4 過渡 IPv6 的技術難度並不高，也是廠商沒有大動作開發/測試 IPv6 物聯網產品的原因之一。但廠商也表明了解 IPv4 缺乏的困難，因此，適當的鼓勵廠商投入 IPv6 相關產品應是有效的。

在 IETF 相關物聯網標準(RFC)的實施上，國內廠商目前處於觀望的態度，相較於 CoAP，仍以 MQTT 為主。建議仍應參考 Amazon AWS IoT、Microsoft Azure IoT 與 Google Cloud Platform IoT 等三大國際雲端平台的投入來評估是否投入實作符合相關 RFC 標準的產品。

第四章　參考資料來源

[1] IETF Working Groups. https://www.ietf.org/how/wgs/

[2] Mobile Technolgies - 5G. European Telecommunications Standards Institute. https://www.etsi.org/technologies/5g

[3] Colin BLACKMAN and Simon FORGE (2019). 5G Deployment-State of Play in Europe, USA and Asia. https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/631060/IPOL_IDA(2019)631060_EN.pdf

[4] 科睿唯安(2018)。5G 技術全景報告。經濟部智慧財產局。https://pcm.tipo.gov.tw/PCM2010/PCM/resources/patentreport/5G.pdf

[5] 科技產業資訊室(2019)。南韓及美國正式 5G 商轉及手機實測。科技政策研究與資訊中心, 國家實驗研究院。https://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=15445

[6] 陳梅鈴 (2015)。全球 5G 市場發展趨勢。電腦與通訊。工業技術研究院。https://ictjournal.itri.org.tw/Content/Messagess/contents.aspx?&MmmID=654304432070702333&CatID=654313611270316241&MSID=654526036164003536

[7] 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。

[8] 周立德、曾家偉(2017)。物聯網與大數據。台網中心電子報。

[9] 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。

[10] 王文娟(2016)。物聯網概念及應用。中華經濟研究院 經濟前瞻。

[11] 魏茂國(2019)。AIoT 實現自駕車多元應用。工業技術與資訊月刊。

[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] 物聯網資安標章說明。台灣資通產業標準協會。https://www.taics.org.tw

[15] AWS IoT-開發人員指南- AWS IoT 的訊息中介裝置-通訊協定. https://docs.aws.amazon.com/iot/latest/developerguide/protocols.html

[16] Jeff Barr, “AWS IPv6 Update – Global Support Spanning 15 Regions & Multiple AWS Services,” AWS News Blog, 2017/1/25. https://aws.amazon.com/tw/blogs/aws/aws-IPv6-update-global-support-spanning-15-regions-multiple-aws-services/

[17] Azure 物聯網(IoT)簡介。 https://docs.microsoft.com/zh-tw/azure/iot-fundamentals/iot-introduction

[18] Azure 虛擬網路的 IPv6 總覽(預覽)。 https://docs.microsoft.com/zh-tw/azure/virtual-network/IPv6-overview

[19] Microsoft Technical Case Studies。 https://microsoft.github.io/techcasestudies/#technology=IoT&sortBy=featured

[20] Google Cloud Platform (GCP) IoT Quickstart 1.0.

[21] GCP Cloud IoT Core Quickstart。https://cloud.google.com/iot/docs/quickstart

[22] GCP 保留靜態外部 IP 位址。 https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address?hl=zh-tw

[23] 中華電信 IoT 智慧聯網大平台。https://iot.cht.com.tw/iot/developer/introduction

[24] 台灣大哥大-物聯網服務。https://iot.taiwanmobile.com/iot/portal/index

[25] 遠傳物聯網。https://www.fetnet.net/enterprise/campaign/iot/intro.html

[26] 亞太電信-GT 智慧生活。http://topic.aptg.com.tw/IoT/

[27] 台灣之星-物聯網。https://www.tstartel.com/CWS/IOT.php

[28] 陳俊賢(2018)。中華電信 IoT 物聯網平台應用分享。

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)