23. RFC 8376：Low-Power Wide Area Network (LPWAN) Overview
RFC 8376：低功耗廣域網路（LPWAN）概述

網際網路工程任務組（IETF）
Request for Comments： 8376
分類: 資訊類
ISSN: 2070-1721

S. Farrell, Ed.
都柏林三一學院

2018 年 5 月

低功耗廣域網路（LPWAN）概述

摘要

低功耗廣域網路（LPWAN）是具有諸如大覆蓋區域，低頻寬，可能非常小的封包和應用層資料大小以及電池長壽命操作特性的無線技術。本文是對 IETF 中正在考慮的 LPWAN 技術集訊息概述，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。

本文的狀態

本文不是網際網路標準規範； 它發佈以提供資訊為目的。

本文是網際網路工程任務組（IETF）的產品。它代表 IETF 社群的共識。它已經過公眾審查，並已獲得網際網路工程指導小組（IESG）的批准發布。並非所有 IESG 批准的文件都適用於任何級別的網際網路標準； 請參閱 RFC 7841 的第 2 節。

有關本文當前狀態，任何勘誤以及如何提供反饋的信息，請參閱 https://www.rfc-editor.org/info/rfc8376。

版權聲明

制。從本文中提取的程式碼組件必須包含信任法律規定第 4.e 節中所述的簡化 BSD 許可文本，並且不提供簡化 BSD 許可中所述的保證。

目錄

1. 前言 3
2. LPWAN技術 4
2.1. LoRaWAN 4
2.2. 窄頻物聯網（NB-IoT） 12
2.3. Sigfox 17
2.4. Wi-SUN聯盟用戶端場域網路（FAN） 22
3. 通用術語 27
4. 間隙分析 29
4.1. IPv6的簡單應用 29
4.2. 6LoWPAN 29
4.3. 6lo 32
4.4. 6tisch 32
4.5. RoHC 33
4.6. ROLL 33
4.7. CoAP 33
4.8. 便攜性 34
4.9. DNS 及 LPWAN 34
5. 安全考量 34
6. IANA考量 35
7. 資訊參考 35
致謝 44
貢獻者 45
作者資訊 48

1. 前言

本文提供背景材料以及 IETF IPv6 低功耗廣域網路（LPWAN）工作小組（WG）中正在考慮的技術概述。它還提供這些技術的需求與當前可用的 IETF 規範之間的間隙分析。

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、低產出量的設備，因此即使是電池供電的設備也可以部署多年。 LPWAN 設備也傾向於限制其頻寬使用，例如，允許在有限的工作週期內使用有限的頻率（通常表示為允許設備傳輸的每小時的時間百分比）。顧名思義，大面積的覆蓋也是一

個共同的目標。因此，總的來說，不同的技術旨在在非常相似的情況下進行部署。

雖然所有受約束的網路必須平衡功耗/電池的壽命、成本及頻寬，但 LPWAN 通過在進行必要的權衡時接受嚴格頻寬和工作循環限制來優先考慮功率和成本優勢。這個優先順序是為了獲得 LPWAN 名稱中“廣域”所暗示的多公里無線電鏈路。

現有的引導部署顯示出巨大的潛力，並在這些技術中產生很多工業利息。在撰寫本文時，基本上沒有 LPWAN 終端設備（Wi-SUN 除外）具有 IP 功能。將 LPWAN 連接到網際網路將在可交互運作性、應用程式部署和管理（以及其他）方面為這些網際網路帶來顯著的好處。LPWAN WG 的目標是在必要時使 IETF 定義的協定、尋址方案和命名慣例適應這種特定的受約束環境。

本文主要是列出“貢獻者”中人員的工作。

2. LPWAN 技術

本節概述 LPWAN WG 正在考慮的一組 LPWAN 技術。每個文本都主要由每種技術的支援者提供。

請注意，本文無論在任何意義上都不是規範性的；它只是幫助讀者找到相關的第 2 層（L2）規範，並了解它們如何與 IETF 定義的技術整合。同樣，這裡也沒有試圖闡明相關技術的利弊。

2.1. LoRaWAN

2.1.1. 來源和文件

LoRaWAN 是一種基於工業、科學和醫療（ISM）的無線技術，用於 LoRa 聯盟開發的遠程低功耗低資料速率應用，LoRa 聯盟是一個會員聯盟<https://www.lora-alliance.org/>。 本文基於 LoRa 規範[LoRaSpec]的 1.0.2 版。該規範是公開的，已經在全球進行多次部署。

2.1.2. 特性

LoRaWAN 旨在支援單個電池上運行較長時間（例如，10 年或更長時間）的終端設備，
通過 155 dB 最大耦合損耗擴充覆蓋範圍，以及可靠有效的文件下載（根據遠端軟體/韌體升級的需要）。

LoRaWAN 網路通常以星形拓撲結構組織，其中閘道在終端設備和後端中央“網路伺服器”之間中繼訊息。閘道通過 IP 鏈路連接到網路伺服器，而終端設備使用可在一個或多個閘道接收的單一跳LoRaWAN通信。通信通常是雙向的；在整體頻寬可用性方面，從終端設備到網路伺服器的上行鏈路通信是有利的。

圖 1 顯示 LoRaWAN 網路中涉及的實體。

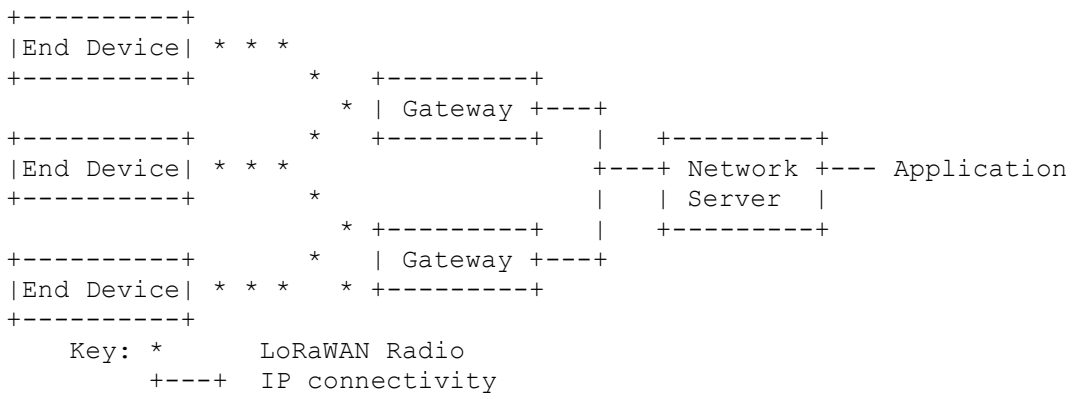

圖 1：LoRaWAN 架構

- End Device(終端設備)：LoRa 客戶端設備，有時稱為“mote ”。 與閘道通信。

- Gateway(閘道)：基礎設施方面的無線電，有時稱為“集中器”或“基地站”。 與終端設備通信，並通過 IP 與網路伺服器通信。

- Network Network(網路伺服器)：網路伺服器（NS）終止連接到網路的終端設備之 LoRaWAN 媒體存取控制（MAC）層。它是星形拓撲的中心。

- Join Server(加入伺服器)：加入伺服器（JS）是 NS 網路端的伺服器，用於處理來自終端設備的加入請求。

- Uplink message(上行鏈路訊息)：指通過一個或多個閘道從終端設備到網路伺服器或應用程式的通信。

- Downlink message(下行鏈路訊息)：指從網路伺服器或應用程式通過一個閘道到單個終端設備或一組終端設備的通信（考慮群播）。

- Application(應用程式)：指終端設備上的應用程式層程式碼，並在 NS 後面運行。對於 LoRaWAN，通常只有一個應用程式在大多數終端設備上運行。 這裡不再進一步描述 NS 與應用程式之間的介面。

在 LoRaWAN 網路中，可以在多個閘道處接收終端設備傳輸，因此，在標稱操作期間，網路伺服器可以從終端設備看到相同上行鏈路訊息的多個實例。

LoRaWAN 網路基礎設施通過自適應資料速率（ADR）方案單獨管理每個終端設備的資料速率和射頻（RF）輸出功率。終端設備可以隨時在本地監管允許的任何通道上進行傳輸。

LoRaWAN 無線電使用 ISM 頻段，例如歐盟內的 433 MHz 和 868 MHz 以及美洲的 915 MHz。

終端設備以每個傳輸的偽亂數方式改變通道，以幫助使系統對干擾更加堅固和/或符合當地法規。

圖 2 顯示在傳輸擴充槽之後，A 類設備接通其接收器，用於從傳輸窗口末端偏移的兩個短接收窗口。終端設備只能在相關接收窗口結束後發送後續上行鏈路框。當設備加入 LoRaWAN 網路時，該過程的某些部分會有類似的超時。

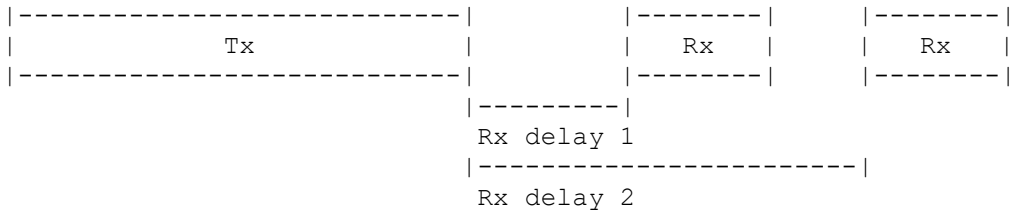

圖 2：LoRaWAN A 類發送和接收窗口

鑑於不同的區域要求，LoRaWAN 物理層（PHY）詳細規範（佔用規範的 30 多頁）在此不再複製。相反，主要是為了說明遇到的問題類型，表 1 列出一個 ISM 頻帶的一些預設設置（這裡沒有完全解釋）；表 2 描述那些定義在 LoRaWAN MAC 層上使用 IETF 協定方法所關注的一些參數之最大值和最小值。

Parameters	Default Value
Rx delay 1	1 s
Rx delay 2	2 s (must be RECEIVE_DELAY1 + 1 s)
join delay 1	5 s
join delay 2	6 s
868MHz Default channels	3 (868.1,868.2,868.3), data rate: 0.3-50 kbit/s

表 1：EU 868 MHz 頻段的默認設置

Parameter/Notes	Min	Max
Duty Cycle: some but not all ISM bands impose a limit in terms of how often an end device can transmit. In some cases, LoRaWAN is more restrictive in an attempt to avoid congestion.	1%	no limit
EU 868 MHz band data rate/frame size	250 bits/s : 59 octets	50000 bits/s : 250 octets
US 915 MHz band data rate/frame size	980 bits/s : 19 octets	21900 bits/s : 250 octets

表 2：各種 LoRaWAN 參數的最小值和最大值

注意，在最小訊號框大小（19 個八位元組）的情況下，LoRa MAC 層標頭需要 8 個八位元組，負載僅包括 11 個八位元組（包括 MAC 層選項）。但是，這些設置不適用於連接過程 - 終端設備需要使用可以為連接過程發送 23 位元組 Join-Request 訊息的通道和資料速率。

上行鏈路和下行鏈路高層資料在 MACPayload 中承載。有一個“埠口”（一個可選 8 位元值）的概念來處理終端設備上的不同應用程式。埠口 0 保留用於特定於 LoRaWAN 的訊息傳遞，例如

終端設備的網路參數配置（可用通道、資料速率、ADR 參數、Rx 延遲 1 和 2 等）。

除了承載更高層 PDU 之外，還存在用於處理網路訪問的 Join-Request 和 Join-Response（也稱為 Join-Accept）訊息。所謂的“MAC 命令”（見下文）長達 15 個位元組，可以在選項欄位中揹負（“FOpts”）。

有許多 MAC 命令用於鏈接和設備狀態檢查，ADR 和工作週期協商，以及管理 RX 窗口和無線電通道設置。例如，鏈路檢查回應訊息允許 NS（回應來自終端設備的請求）通知終端設備最近在閘道處看到的訊號衰減，並告知終端設備有多少閘道接收到對應的鏈路。請求 MAC 命令。

某些 MAC 命令由網路伺服器啟動。例如，一個命令允許網路伺服器要求終端設備將其工作週期減少到僅使用區域中允許的最大比例。另一個允許網路伺服器利用來自終端設備的回應來查詢終端設備的電源狀態，該回應指定它是否具有外部電源或是電池供電（在這種情況下，相對電池電量也被發送到網路伺服器）。

為了在 LoRaWAN 網路上名義地運行，設備需要 32 位元設備位址，該設備位址在設備“加入”網路時（參見下面的連接過程）或預先設置到設備中時分配。在漫遊設備的情況下，基於由 LoRa 聯盟分配給網路的 24 位元網路識別符(NetID)來分配設備位址。可以通過網路為非漫遊設備分配設備位址，而不依賴於 LoRa 聯盟分配的 NetID。

假設終端設備與一個或相當有限數量的應用程式一起工作，由 64 位元 AppEUI 識別，假定它是註冊 IEEE EUI64 值[EUI64]。此外，設備需要具有兩個對稱交談密鑰，一個用於保護網路組件（埠口 = 0），為 NwkSKey，另一個用於保護應用層流量，即 AppSKey。兩個密鑰都用於 128 位元 AES 加密操作。 因此，一種選擇是終端設備以某種方式（預先）提供所有上述加上通道訊息；在這種情況下，終端設備可以簡單地開始發送。考慮到 LoRaWAN 網路的性質，這在很多情況下可以透過帶外方式實現。 表 3 總結這些值。

Value	Description
DevAddr	DevAddr (32 bits) = device-specific network address generated from the NetID
AppEUI	IEEE EUI64 value corresponding to the join server for an application
NwkSKey	128-bit network session key used with AES-CMAC
AppSKey	128-bit application session key used with AES-CTR
AppKey	128-bit application session key used with AES-ECB

表 3：標稱操作所需的值

作為替代方案，終端設備可以使用 LoRaWAN 連接程序與 NS 後面的連接伺服器，以便設置其中一些值並動態獲得對網路的存取。要使用連接程序，終端設備仍必須知道 AppEUI 和綁定到 AppEUI 中不同（長期）對稱密鑰（這是應用程式密鑰（AppKey），並且它與應用程式交談密鑰不同（AppSKey））。 AppKey 需要特定於設備； 也就是說，每個終端設備應具有不同的 AppKey 值。最後，終端設備還需要一個自身的長期識別符，在語法上也是 EUI-64，稱為設備 EUI 或 DevEUI。 表 4 總結這些值。

Value	Description
DevEUI	IEEE EUI64 naming the device
AppEUI	IEEE EUI64 naming the application
AppKey	128-bit long-term application key for use with AES

表 4：加入過程所需的值

連接程序涉及一種特殊的交換，其中終端設備在 Join-Request 上行鏈路訊息中判斷提示 AppEUI 和 DevEUI（使用長期 AppKey 保護，但未加密）。 然後將其發送到網路伺服器，該網路伺服器與已知的 AppKey 以驗證 Join-Request 之實體進行交互作用。 如果一切順利，則從網路伺服器向終端設備返回 Join-Accept 下行鏈路訊息。該訊息指定 24 位元 NetID、32 位元 DevAddr 和通道訊息，並且可以基於 AppKey 的知識從中導引出 AppSKey 和 NwkSKey。
這為終端設備提供表 3 中列出的所有值。

所有有效負載都經過加密並具有資料完整性。 因此，當作有效負載（埠口零）發送時，MAC 命令受到保護。但是，隨著訊號框選項（ “FOpts”）被明確發送，MAC 命令被揹負。作為訊號框選項而不僅作為有效負載發送的任何 MAC 命令對被動攻擊者而言都是可見的，但由於使用下面描述的訊息完整性檢查（MIC），它們對於主動攻擊者而言不具有可擴充性。

對於 LoRaWAN 版本 1.0.x，NwkSKey 交談密鑰用於終端設備和網路伺服器之間提供資料完整性。AppSKey 用於終端設備和網路伺服器之間提供資料機密性，或者在網路伺服器“後面”的應用程式之間提供資料機密性，具體取決於網路的應用。

所有 MAC 層訊息都具有使用 AES-CMAC 計算的外部 32 位元 MIC，其輸入是密文負載和其他標頭，並使用 NwkSkey。 使用 AES-128 加密負載，使用 AppSKey 從[IEEE.802.15.4]導引出計數器模式。預計閘道不會提供 AppSKey 或 NwkSKey，所有基礎設施端加密都發生在網路伺服器中（或“後面”）。當作為連接過

程的結果從 AppKey 導引出交談密鑰時，特別處理 Join-Accept 訊息負載。

長期 AppKey 直接用於保護 Join-Accept 訊息內容，但所使用的功能不是 AES 加密操作，而是 AES 解密操作。這意味著終端設備只需要實現 AES 加密操作。（用於負載解密的計數器模式變體代表著終端設備不需要 AES 解密基元。）

Join-Accept 明文的長度始終小於 16 個位元組，因此電子碼簿（ECB）模式用於保護 Join-Accept 訊息。Join-Accept 訊息包含使用 AES 加密操作在終端設備上與其他 Join-Accept 內容（例如，DevAddr）一起恢復的 AppNonce（24 位元）。一旦 Join-Accept 負載可用於終端設備，交談密鑰從 AppKey、AppNonce 和其他值導出，再次使用 ECB 模式 AES 加密操作，明文輸入最多為 16 個八位元組。

2.2. 窄頻物聯網（NB-IoT）

2.2.1. 來源和文件

窄頻物聯網（NB-IoT）已由 3GPP 開發和標準化。NB-IoT 的標準化在 2016 年 6 月通過 3GPP 版本 13 最終確定，並且 NB-IoT 的進一步增強在 2017 年版本 14 中指定(例如，以群播支援的形式)。以下版本將開發更多功能和改進，但自 2016 年以來，NB-IoT 已準備好部署；部署起來相當簡單，特別是在操作員基地台中進行軟體升級的現有 LTE 網路中。有關 NB-IoT 指定內容的更多訊息，3GPP 規範 36.300 [TGPP36300]提供演進的通用陸面無線接入網路（E-UTRAN）無線電介面協定架構的概述和整體描述，而規範 36.321 [TGPP36321]、36.322 [TGPP36322]、36.323[TGPP36323]和 36.331 [TGPP36331]分別給出 MAC、無線電鏈路控制(RLC)、封包資料收斂協定（PDCP）和無線電資源控制（RRC）協定層的更詳細描述。注意，下面的描述假設熟悉許多 3GPP 術語。

有關 NB-IoT 的一般概述，請參閱[nbiot-ov]。

2.2.2. 特性

NB-IoT 的具體目標包括：模塊成本低於 5 美元，擴充覆蓋範圍為 164 dB 最大耦合損耗，電池壽命超過 10 年，每個單元約 55000 個設備，上行鏈路回報延遲小於 10 秒。

下行鏈路峰值速率為 30 kbit / s，最大傳輸單元（MTU）大小為 1600 位元組，受 PDCP 層限制（參見圖 4 中的協定結構），這是用戶平面中的最高層，如後面所述。直到所述 MTU 大小的任何封包大小可以從較高層傳遞到 NB-IoT 堆疊，封包的分段在 RLC 層中執行，RLC 層可以將資料分段為具有小到 16 位元大小的傳輸區塊。顧名思義，NB-IoT 在下行鏈路和上行鏈路中都使用頻寬為 180 kHz 的窄頻。在下行鏈路中使用的多址方案是具有 15kHz 子載波間隔的正交頻分複用（OFDMA）。在上行鏈路中，使用具有 15kHz 或 3.75kHz 音調間隔的子載波頻分複用（SC-FDMA）單音，或者可選地使用具有 15kHz 音調間隔的多音 SC-FDMA。

NB-IoT 可以通過三種方式部署。帶內部署意味著窄頻部署在 LTE 頻帶內，無線電資源在 NB-IoT 和普通 LTE 載波之間靈活共享。在護帶部署中，窄頻使用兩個相鄰 LTE 載波之間的未使用資源區塊。還支援獨立部署，其中窄頻可以單獨位於專用頻譜中，這使得可以為 850/900 MHz 重新構建用於 NB-IoT 的 GSM 載波。所有三種部署模式都用於許可頻段。 對於上行鏈路傳輸，最大傳輸功率為 20 或 23dBm，而對於下行鏈路傳輸，eNodeB 可以使用更高的傳輸功率，取決於部署，高達 46dBm。

由 3GPP 定義的 NB-IoT 覆蓋增強其最大耦合損耗（MCL）目標是 164dB。使用此 MCL，NB-IoT 在下行鏈路中的性能在 200 bps 和 2-3 kbit/s 之間變化，具體取決於部署模式。獨立操作可以實現最高資料速率，高達些許 kbit/s，而帶內和保護頻帶操作可能達到幾百 bps。NB-IoT 甚至可以使用高於 170 dB 的 MCL 以及非常低的位元率運行。

對於信號優化，除了傳統的 LTE RRC 連接設置之外，還引入兩個選項；強制 Data-over-NAS（控制平面優化，[TGPP23720]中的解決方案 2）和可選的 RRC 暫停/恢復（用戶平面優化，[TGPP23720]中的解決方案 18）。在控制平面優化中，資料通過非接入層（NAS）直接發送到核心網路中的移動管理實體（MME）（參見圖 3 中的網路架構）到用戶設備（UE），沒有來自基地站的交互作用。 這

意味著 eNodeB 中的 PDCP 層不提供存取層安全性或標頭壓縮，因為繞過存取層，且僅限制 RRC 程序。基於堅固標頭壓縮（RoHC）的標頭壓縮仍然可選地在 MME 中提供和終止。

與傳統 LTE 操作相比，RRC 暫停/恢復程序減少 UE 狀態從 RRC 閒置轉換到 RRC 連接模式所需的訊號開銷，以便更快地與網路進行用戶平面交易並返回到 RRC 閒置模式。

為了延長設備電池壽命，NB-IoT 可以使用省電模式（PSM）和擴充 DRX（eDRX）。 使用 eDRX、RRC 連接模式 DRX 週期最長可達 10.24 秒； 在 RRC 閒置時，eDRX 週期最長可達 3 小時。 在 PSM 中，設備處於深度睡眠狀態，僅在上行鏈路回報時喚醒。 在回報之後，存在窗口（由網路配置），在該窗口期間，設備接收器打開用於下行鏈路連接或用於週期性“保活”訊號（PSM 使用具有用於下行鏈路可達性的附加接收窗口的周期性 TAU 訊號）。

由於 NB-IoT 在許可頻譜中運行，因此它沒有通道存取限制，允許高達 100％的工作週期。

3GPP 存取安全性在[TGPP33203]中規定。

```
+--+
|UE| \                  +-------+       +-------+
+--+  \                 | MME   |------| HSS   |
       \              / +-------+       +-------+
+--+    \+--------+ /       |
|UE| ----| eNodeB |-        |
+--+    /+--------+ \       |
       /              \ +--------+
      /                \|        |    +-------+    Service Packet
+--+ /                  |  S-GW  |----| P-GW |---- Data Network (PDN)
|UE|                    |        |    +-------+    e.g., Internet
+--+                    +--------+
```

圖 3：3GPP 網路架構

圖 3 顯示適用於 NB-IoT 的 3GPP 網路架構。MME 負責處理 UE 的移動性。MME 任務包括追蹤和調頁 UE、交談管理，在初始附接期間為 UE 選擇伺服閘道以及驗證用戶。在 MME 中，終止來自 UE 的 NAS 訊號。

伺服閘道（S-GW）通過存取網路發送和轉發用戶資料封包，且在稱為 eNodeB 基地台之間的切換期間以及在 NB-IoT 與其他 3GPP 技術之間的切換期間充當 UE 的移動性鏈結錨。

封包資料網路閘道（P-GW）用作 3GPP 網路和外部網路之間的介面。

本定用戶伺服器（HSS）包含用戶相關和訂閱相關的訊息。它是一個執行移動性管理、交談建立支援、用戶身份驗證和存取授權的資料庫。

E-UTRAN 由單一類型的組件 eNodeB 組成。eNodeB 是控制一個或多個單元的 UE 基地台。

3GPP 無線電協定架構如圖 4 所示。

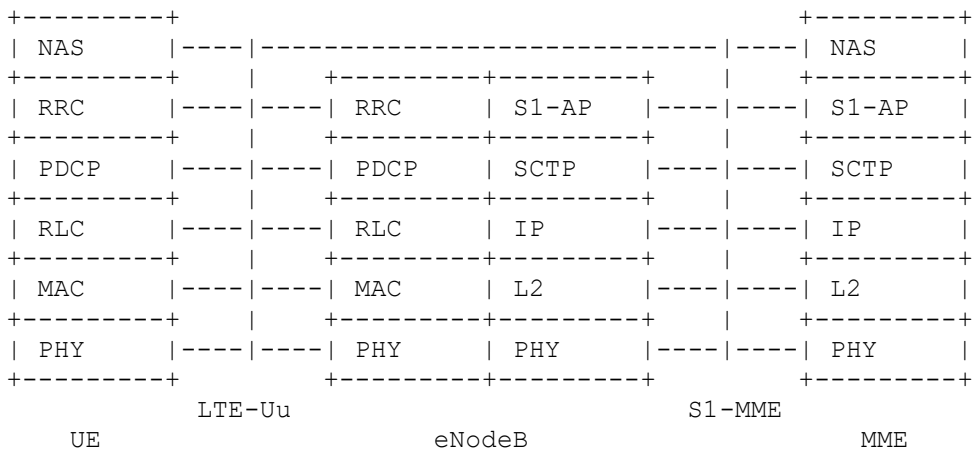

圖 4：用於控制平面的 3GPP 無線電協定架構

NB-IoT(和 LTE)的無線電協定架構被分成控制平面和用戶平面。控制平面由控制無線電存取支架的協定和 UE 與網路之間的連接組成。控制平面的最高層稱為非存取層（NAS），其傳送 UE 與演進封包核心（EPC）之間的無線電訊號，透明地通過無線電網路。NAS 負責身份驗證、安全控制、移動性管理和支架管理。

存取層（AS）是 NAS 下面的功能層；在控制平面中，它由無線電資源控制（RRC）協定[TGPP36331]組成，其處置連接建立和釋放功能，系統訊息的廣播，無線電支架建立，重新配置和釋放。RRC 根據網路狀態配置用戶和控制平面。存在兩個 RRC 狀態，RRC_Idle 或 RRC_Connected，並且 RRC 實體控制這些狀態之間的切換。在 RRC_Idle 中，網路知道 UE 存在於網路中，並且在呼叫/下行鏈路資料的情況下可以到達 UE。在這種狀態下，UE 監督調頁，執行單元測量和單元選擇，並獲取系統資訊。此外，UE 可以接收廣播和群播資料，但是不期望發送或接收單播資料。在 RRC_Connected 狀態中，UE 具有到 eNodeB 的連接，網路知道單元級別上的 UE 位置，並且 UE 可以接收和發送單播資料。當期望 UE 在網路中活動以發送或接收資料時，建立 RRC 連接。當沒有更多流量時，釋放 RRC 連接，切換回 RRC_Idle；這是為了保持 UE 電池壽命和無線電資源。

但是，如前所述，為 NB-IoT 引入一項新功能，允許資料從 MME 直接傳輸到 UE，然後透明地傳輸到 eNodeB，從而繞過 AS 功能。

PDCP 在控制平面中的[TGPP36322]主要服務是控制平面資料的傳輸，加密和完整性保護。

RLC 協定[TGPP36322]執行上層 PDU 的傳輸，並且可選地，利用 RLC 服務資料單元（SDU）的自動重複請求（ARQ）、序連連接、分段和重組來執行錯誤校正，按順序遞送上層 PDU、重複檢測、RLC SDU 丟棄、RLC 重建以及協助錯誤檢測和恢復。

MAC 協定[TGPP36321]提供邏輯通道和傳輸通道之間的映射、MAC SDU 的複用，排程資訊報告，具有混合 ARQ（HARQ）的糾錯、優先級處理和傳輸格式選擇。

PHY [TGPP36201]為更高層提供資料傳輸服務。這些包括錯誤檢測和更高層的指示，正向錯誤校正（FEC）編碼，HARQ 軟組合，速率匹配，傳輸通道至物理通道的映射，物理通道的功率加權和調制，頻率和時間同步，及無線電特性測量。

用戶平面負責透過存取層傳輸用戶資料。它與 IP 介面，用戶平面的最高層是 PDCP，PDCP 在用戶平面中使用 RoHC 執行標頭壓縮，在 eNodeB 和 UE 之間傳輸用戶平面資料，加密和完整性保護。與控制平面類似，用戶平面中的較低層包括 RLC、MAC，及 PHY 執行與它們在控制平面中相同的任務。

2.3. Sigfox

2.3.1. 來源和文件

Sigfox LPWAN 符合 ETSI [etsi_unb]定義的術語和規範。截至今日，Sigfox 的網路已在 12 個國家全面部署，並在其他 26 個國家進行部署中，總面積達 200 萬平方公里，包含 5.12 億人口。

2.3.2. 特性

Sigfox LPWAN 自動電池供電設備原則上每天、每週或每月僅發送幾個位元組，允許它們在單個電池上保留長達 10 - 15 年。 因此，該系統被設計為允許設備持續數年，有時甚至埋在地下。

由於無線電協定是無連接的並且針對上行鏈路通訊進行優化，因此 Sigfox 基地台的容量取決於設備生成的訊息數量，而不取決於設備的實際數量。 同樣，設備的電池壽命取決於設備生成的訊息數量。 根據使用情況，設備可以從每台設備每天發送少於一條訊息到每台設備每天發送數十封訊息。

單元的覆蓋範圍取決於連線預算表和部署類型（城市，農村等）。 無線電介面符合以下規定：

美國的頻譜分配[fcc_ref]

歐洲的頻譜分配[etsi_ref1][etsi_ref2]

日本的頻譜分配[arib_ref]

Sigfox 無線電介面還符合以下國家/地區的當地法規：澳大利亞、巴西、加拿大、肯尼亞、
黎巴嫩、毛里求斯、墨西哥、新西蘭、阿曼、秘魯、新加坡、南非、韓國和泰國。

無線電介面基於超窄頻（UNB）通訊，透過在設備上消耗有限的能量來增加傳輸範圍。此外，UNB 允許大量設備在給定單元中共存而不會顯著增加頻譜干擾。

雖然系統針對上行鏈路通訊進行優化，但仍支援上行鏈路和下行鏈路。由於頻譜優化，需要不同的上行鏈路和下行鏈路訊號框以及時間同步方法。

UNB 上行鏈路傳輸的主要無線電特性是：

- 通道化遮罩：100 Hz / 600 Hz（取決於地區）
- 上行鮑率：100 鮑/ 600 鮑（取決於地區）
- 調制方案：DBPSK
- 上行傳輸功率：符合當地法規
- 連線預算：155 dB（或更高）

- 中心頻率準確度：不相關，前提是上行鏈路封包傳輸中沒有明顯的頻率漂移

例如，在歐洲，UNB 上行鏈路頻帶限制為 868.00 至 868.60 MHz，最大輸出功率為 25 mW，工作週期為 1%。

上行鏈路訊號框的格式如下：

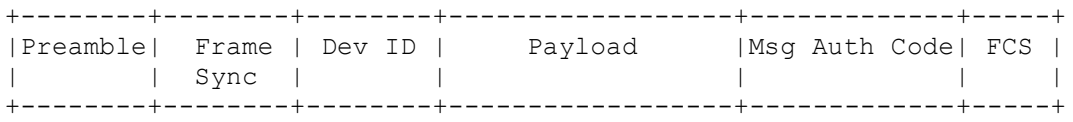

圖 5：上行訊號框格式

上行鏈路訊號框由以下欄位組成：

- Preamble(前文)：19 位元
- Frame sync and header(訊號框同步及標頭)：29 位元
- Device ID(設備 ID)：32 位元
- Payload(負載)：0-96 位元
- Authentication(身份驗證)：16-40 位元
- Frame check sequence(訊號框檢查順序)：16 位元（循環冗餘檢查（CRC））

UNB 下行鏈路傳輸的主要無線電特性是：

- 通道化遮罩：1.5 kHz
- 下行鏈路鮑率：600 鮑
- 調制方案：GFSK
- 下行鏈路傳輸功率：500 mW / 4W（取決於地區）
- 連線預算：153 dB（或更高）

- 中心頻率準確度：下行傳輸的中心頻率由網路根據相應的上行傳輸設置。

例如，在歐洲，UNB 下行鏈路頻段限制為 869.40 至 869.65 MHz，最大輸出功率為 500 mW，工作週期為 10%。

下行鏈路訊號框的格式如下：

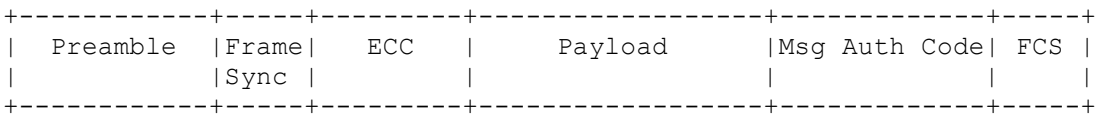

圖 6：下行訊號框格式

下行鏈路訊號框由以下欄位組成：

- Preamble(前文)：91 位元
- Frame sync and header(訊號框同步及標頭)：13 位元
- Error Correcting Code(糾錯碼)（ECC）：32 位元
- Payload(負載)：0-64 位元
- Authentication(身份驗證)：16 位元
- Frame check sequence(訊號框檢查順序)：16 位元（CRC）

無線電介面針對異步的上行鏈路傳輸進行優化。透過向網路查詢可用資料的設備實現下行鏈路通訊。

願意接收下行鏈路訊息的設備在發送上行鏈路傳輸之後打開用於接收的固定窗口。此窗口的延遲和持續時間具有固定值。網路在接收窗口期間發送給定設備的下行鏈路訊息，且網路還選擇 BS 用於發送相應的下行鏈路訊息。

由於 ISM 頻段的監管限制，上行鏈路和下行鏈路傳輸不平衡。根據最嚴格的規定，系統每天每台設備最多允許 140 則上行鏈路訊

息和 4 則下行鏈路訊息。根據系統條件和特定的操作監管領域，這些限制可以略微放寬。

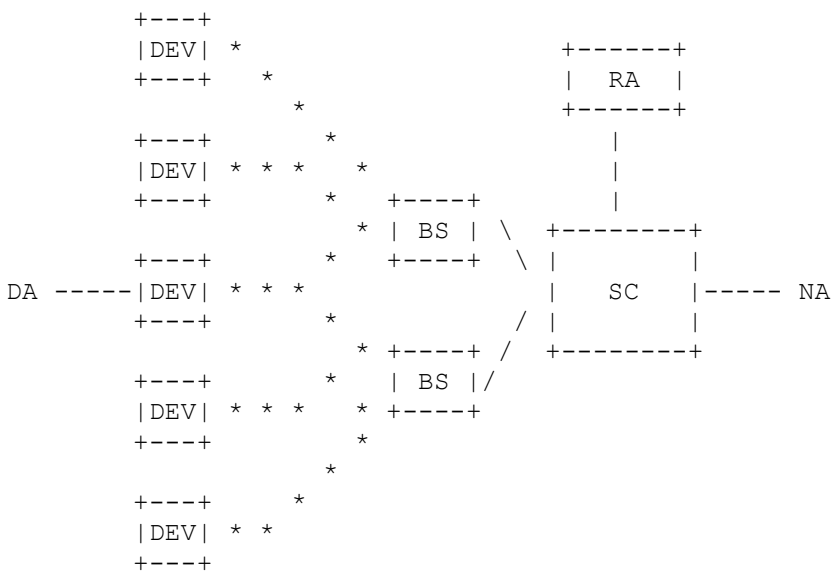

圖 7：Sigfox 網路架構

圖 7 描繪 Sigfox 網路架構的不同元素。

Sigfox 擁有“單一合約 單網路”模式，允許設備在任何國家/地區進行連接，無需漫遊或移交任何需求或概念。

該架構由單個基於雲端的核心網路組成，該網路允許全球連接，對終端設備和無線存取網路的影響最小。核心網路元素是伺服中心（SC）和註冊機構（RA）。 SC 負責 BS 和網際網路之間的資料連接，以及 BS 和端點（EP）的控制和管理。RA 負責 EP 網路訪問授權。

無線電存取網路由直接連接到 SC 的幾個 BS 組成。每個 BS 執行複雜的 L1 / L2 功能，
為 SC 留下一些 L2 和 L3 功能。

設備（DEV）或 EP 是在本地設備應用程式（DA）和網路應用程式（NA）之間傳遞應用程式資料的物件。

設備（或 EP）可以是靜態的或游牧的，因為它們與 SC 相關聯並且它們不附著到任何特定的 BS。
因此，他們可以通過一個或多個 BS 與 SC 通訊。

由於設備複雜性的限制，假設設備僅託管一個或極少數設備應用程式，其中大多數時間一次將每個設備應用程式通訊到單個網路應用程式。

無線電協定驗證並確保每則訊息的完整性。這是透過使用唯一的設備 ID 和基於 AES-128 的訊息驗證編碼來實現的，確保訊息已由設備生成並使用訊息中聲明的 ID 發送。應用程式資料可以在應用程式級別進行加密，具體取決於實例的重要性，以便在成本和工作量與風險之間取得平衡。計數器模式下的 AES-128 用於加密。 加密密鑰對每個設備都是獨立的。 這些密鑰與設備 ID 相關聯，並且預先配置單獨的完整性和機密性密鑰。 如果要使用機密性，則僅提供機密性密鑰。在撰寫本文時，尚未公佈演算法和鍵控細節。

2.4. Wi-SUN 聯盟用戶端場域網路（FAN）

這裡的文字內容來自 Bob Heile（bheile@ieee.org）的個人通訊，由 Bob 和 Sum Chin Sean 撰寫。Paul Duffy（paduffy@cisco.com）也在此部分提供其他意見/建議。

2.4.1. 來源和文件

Wi-SUN 聯盟<https://www.wi-sun.org/>是智慧城市、智慧電網，智慧公用程式
和一系列通用物聯網應用的行業聯盟。 Wi-SUN 聯盟用戶端場域網路（FAN）配置文件基於開放標準（主要基於 IETF 和 IEEE 802 標準），旨在滿足智慧城市/城市基礎設施監控和管理、電動汽車（EV）基礎設施、高級等應用的需求、計量基礎設施（AMI）、配電自動化（DA）、監控和資料採集（SCADA）保護/管理、分佈式發電監控和管理，以及更多物聯網應用。 此外，該聯盟還創建一個認證計劃，以促進全球多廠商可交互運作性。

FAN 配置文件在 ANSI / TIA 中指定，作為先前在智慧公用程式網路[ANSI-4957-000]上完成的工作擴充。
打算在2017年發布的那些規範更新將包含FAN配置文件的詳細訊息。在[wisun-pressie1]和[wisun-pressie2]中介紹生成該配置文件的工作當前快照。

2.4.2. 特性

FAN 配置文件是 IPv6 無線網狀網路，支援企業級安全性。跳頻無線網狀拓撲旨在提供卓越的網路穩定性，因為高冗餘而具有可靠性、靈活的網狀配置而具有良好的可擴充性，以及良好的干擾恢復能力。正在開發的極低功耗模式允許網路節點的電池長期操作。

以下列表包含與 LPWAN 應用程式相關的 Wi-SUN 總體特徵。

- 覆蓋範圍：Wi-SUN FAN 的範圍通常為 2-3 公里，符合鄰近區域網路、校園網路或企業區域網路的需求。該範圍還可以通過多個跳網路進行擴充。

- 高頻寬，低鏈路潛伏：Wi-SUN 支援相對較高的頻寬，即高達 300 kbit/s [FANOV]，可實現設備的遠端更新及升級，從而可以處理新應用，延長其工作壽命。Wi-SUN 通過提供低鏈路潛伏（0.02 s）和雙向通訊，支援按需求控制的 LPWAN IoT 應用。

- 低功耗：FAN設備休息時的功耗小於2 uA，收聽時僅為8 mA。這種設備即使經常收聽也能保持較長的使用壽命。例如，假設設備每 10 秒發送一次 10ms 的資料；從理論上而言，1000 mAh 的電池可以使用 10 年以上。

- 可擴充性：數千萬台 Wi-SUN 風扇設備已部署在城市、郊區和鄉村環境中，包括部署超過 100 萬台設備。

FAN 包含一個或多個網路。在網路中，節點承擔三個操作角色之一。 首先，每個網路都包含一個邊界路由器，為網路提供 WAN 連接。 邊界路由器維護其網路中所有節點的來源路由表，提供節

點認證和密鑰管理服務，並傳播網路範圍的訊息，如廣播時程表。第二，路由器節點，提供向上和向下的封包轉發（在網路內）。路由器還提供用於中繼安全性和位址管理協定的服務。最後，葉節點提供最低限度的功能：發現和加入網路，發送/接收 IPv6 封包等。
低功耗網路可能包含網狀拓撲，邊界處的路由器構建具有葉節點的星形拓撲。

FAN 配置文件基於 IETF 開發的各種開放標準（包括[RFC768]、[RFC2460]、[RFC4443]和[RFC6282]。相關的 IEEE 802 標準包括[IEEE.802.15.4]和[IEEE.802.15.9]。對於低功耗和有損網路（LLN），請參見 ANSI / TIA [ANSI-4957-210]。

FAN配置文件規範提供獨立於應用程式基於IPv6的傳輸服務。建立 IPv6 封包路由有兩種可能的方法：網路層的低功耗和有損網路路由協定（RPL）是強制性的，資料鏈路層的多跳傳送服務（MHDS）是可選的。圖 8 提供 FAN 網路堆疊的概述。

傳輸服務基於 UDP（在[RFC768]中定義）或 TCP（在[RFC793]中定義）。

網路服務由[RFC2460]中定義的 IPv6 提供，其具有[RFC4944]和[RFC6282]中定義的 IPv6 低功耗無線個人區域網路（6LoWPAN）適配。 如[RFC4443]中所定義的 ICMPv6 在訊息交換期間用於控制平面。

資料鏈路服務向網路層提供 PHY 和資料傳輸/管理服務的控制/管理。這些服務分為 MAC 和邏輯鏈路控制（LLC）子層。 LLC 子層提供支援 6LoWPAN 和可選 MAC 子層網格服務的協定調度服務。 使用[IEEE.802.15.4]中定義的資料結構構造 MAC 子層。定義多種跳頻模式。 整個 MAC 負載封裝在[IEEE.802.15.9]訊息元素中，以實現上層 6LoWPAN 處理和 MAC 子層網格處理等之間的 LLC 協定調度。
這些區域完成擴充一次[IEEE.802.15.12] 。

PHY 服務源自[IEEE.802.15.4]中 SUN FSK 規範的子集。2-FSK 調制方案的通道間隔範圍為 200 至 600 kHz，定義為 50 至 300 kbit/s

的資料速率，FEC 作為可選功能。 為實現超低功耗應用，PHY 層設計還可擴充到低能耗和關鍵基礎設施監控網路。

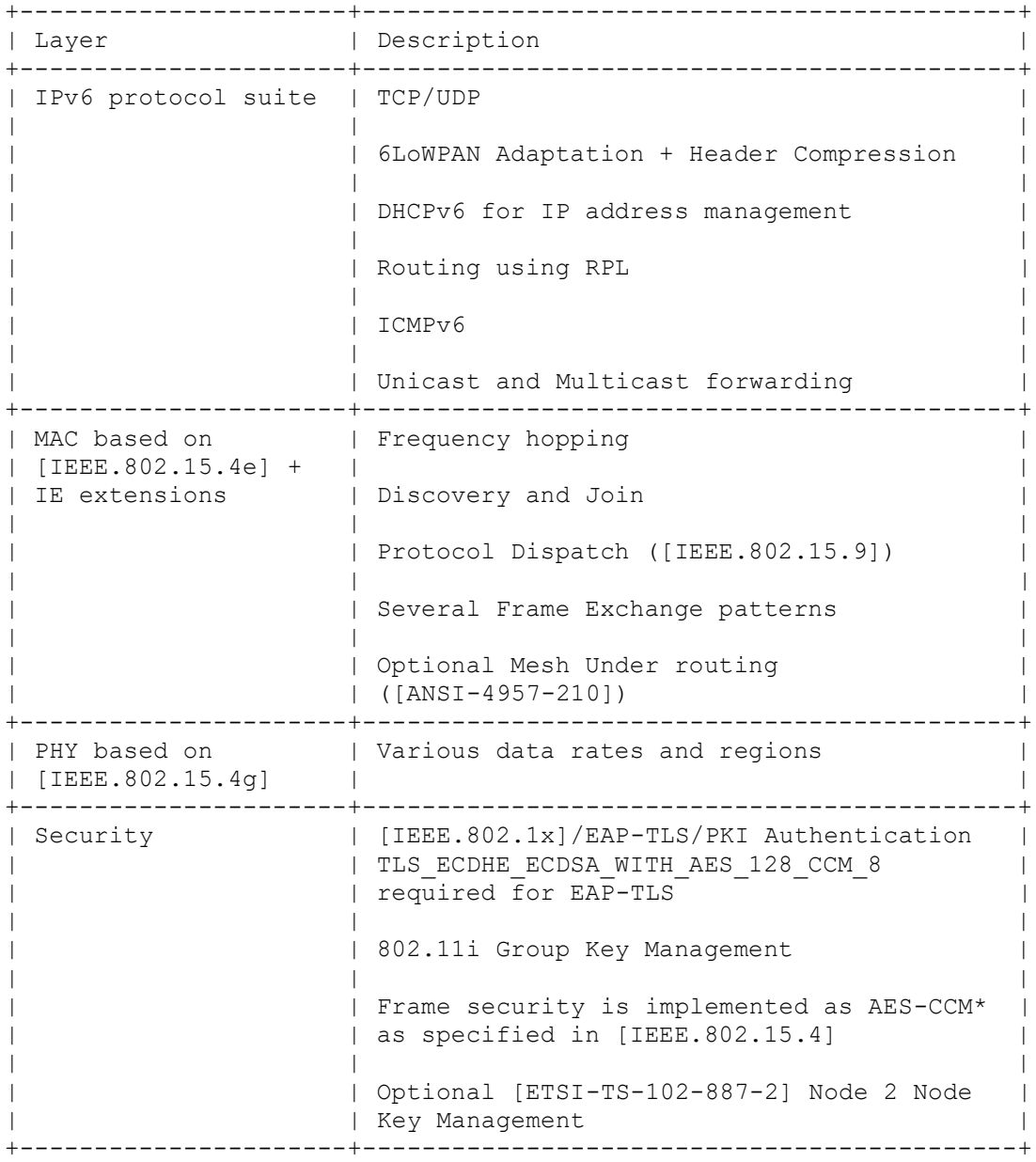

圖 8：Wi-SUN 堆疊概述

FAN 安全性支援資料鏈路層網路存取控制、相互認證以及在 FAN 節點與其邊界路由器之間建立安全成對鏈路，該節點通過[IEEE.802.1x]和 EAP-TLS 的改編實現，如 [RFC5216]使用[IEEE.802.1AR]中描述的安全設備識別。憑證格式基於[RFC5280]。使用[IEEE.802.11]四次握手的改編建立邊界路由器和一組 FAN 節點之間的安全群組鏈路。在網路內維護一集合的四個群組密鑰，其中一個是當前的發送密鑰。使用[ETSI-TS-102-887-2]的自適應，

在單一跳 FAN 鄰居之間支援安全的節點到節點鏈路。FAN 節點實現[IEEE.802.15.4]中規定的訊號框安全性。

3. 通用術語

LPWAN 技術，例如上面討論的那些，具有相似的架構但是術語不同。我們可以在典型的 LPWAN 網路中識別不同類型的實體：

- 終端設備是設備或“東西”（例如，感測器，致動器等）；它們在每種技術（終端設備，用戶設備或 EP）中的命名方式不同。 每個無線電網路可以有高密度的終端設備。

- 無線電閘道，是受約束鏈路的 EP。 它被稱為：閘道，演進節點 B 或基地站。

- 網路閘道或路由器是無線電閘道和網際網路之間的互連節點。它被稱為網路伺服器、伺服 GW 或伺服中心。

- LPWAN-AAA 伺服器，用於控制用戶身份驗證。 它被稱為 Join-Server、Home Subscriber Server 或 Registration Authority。（我們使用術語 LPWAN-AAA 伺服器，因為我們不假設這個實體像許多/大多數 AAA 伺服器那樣稱 RADIUS 或 Diameter；但是，同樣地，我們不想排除這一點，因為功能類似。）

- 最後，我們有了應用程式伺服器，也稱為封包資料節點閘道或網路應用程式。

Function/ Technology	LoRaWAN	NB-IoT	Sigfox	Wi-SUN	IETF
Sensor, Actuator, device, object	End Device	User Equipment	End Point	Leaf Node	Device (DEV)
Transceiver Antenna	Gateway	Evolved Node B	Base Station	Router Node	Radio Gateway
Server	Network Server	PDN GW/ SCEF*	Service Center	Border Router	Network Gateway (NGW)
Security Server	Join Server	Home Subscriber Server	Registration Authority	Authent. Server	LPWAN-AAA Server
Application	Application Server	Application Server	Network Application	Appli-cation	Application (App)

* SCEF = Service Capability Exposure Function

圖 9：LPWAN 結構術語

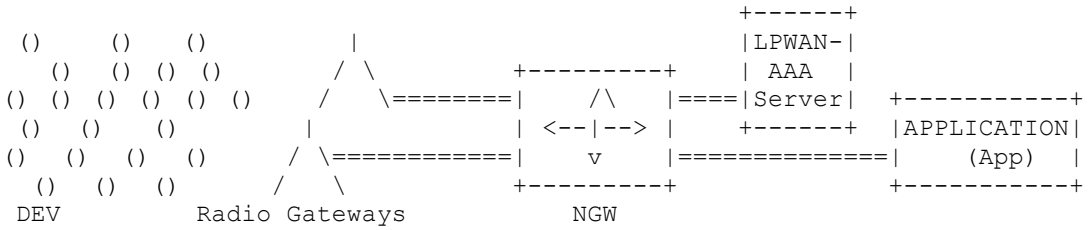

圖 10：LPWAN 結構

除了實體名稱之外，LPWAN 還可能受到區域頻段規定的約束。這些可能包括對工作週期的限制，例如，要求主機僅傳輸每小時的特定百分比。

4. 間隙分析

本節考慮當前LPWAN技術與LPWAN WG目標之間的一些間隙。[RFC7452]中描述的許多通用考慮因素也適用於LPWAN，因為終端設備也可以被認為是（所謂的）“智慧物件”的子類。此外，LPWAN 設備實施者還需要考慮[RFC8240]中描述與韌體更新有關的問題。

4.1. IPv6 的簡單應用

IPv6 [RFC8200]旨在為連接到網際網路的所有節點分配位址。 然而，協定引入的至少 40 位元組的標頭附加與 LPWAN 約束不兼容。如果使用沒有進一步優化的 IPv6，則可能只需要幾個 LPWAN 訊號框來承載 IP 標頭。另一個問題來自 IPv6 MTU 要求，要求下面的層支援至少 1280 位元組的封包[RFC2460]。

IPv6 具有配置協定：鄰居發現協定（NDP）[RFC4861]。對於節點學習網路參數，
NDP 生成具有相對較大的訊息大小常規流量，該流量不符合 LPWAN 約束。

在某些 LPWAN 技術中，不支援 L2 群播。在這種情況下，如果網路拓撲是星形，則可以應用[RFC7668]的第 3.2.5 節中的解決方案和注意事項。

其他關鍵協定（例如 DHCPv6 [RFC3315]、IPsec [RFC4301]和 TLS [RFC5246]）在此上下文中具有類似的問題屬性。每個協定都要求主機與網路上的其他主機之間進行相對頻繁的往返。在加密協定（例如 IPsec 和 TLS）的情況下，除了安全交談建立所需的往返之外，加密操作可能需要填充和添加在考慮 LPWAN 較低層時有問題的驗證器。請注意，主電源供電的 Wi-SUN 網狀路由器節點通常比所討論的其他 LPWAN 技術更具資源能力。這可以為 Wi-SUN 的某些方面使用更多“chatty”協定。

4.2. 6LoWPAN

在各種維度上表現出顯著限制的幾種技術已經利用 6LoWPAN 規範套件（[RFC4944]、[RFC6282]和[RFC6775]）來支援 IPv6 [USES-6LO]。然而，LPWAN 的約束通常比具有（重新）使用 6LoWPAN 的技術的典型情況更為極端，這對 6LoWPAN 套件構成挑戰，以便通過 LPWAN 啟用 IPv6。LPWAN 的特徵在於設備約束（於處理能力、內存和能量可用性方面），尤其是鏈路約束，例如：

- 微小的 L2 負載大小（從 ~10 到 ~100 字元），
- 非常低的位元率（從~10 bit/s 到 ~100 kbit/s），以及
- 在某些特定技術中，進一步的訊息速率限制（例如，在~0.1 訊息/分鐘 和 ~1 訊息/分鐘 之間）由於限制工作週期的地區法規。

4.2.1. 標頭壓縮

6LoWPAN 標頭壓縮通過在可以從鏈路層導出標頭欄位時並通過假設某些標頭欄位將頻繁攜帶期望值來減少 IPv6（和 UDP）標頭負擔。6LoWPAN 提供無狀態和有狀態標頭壓縮。在後者中，假設 6LoWPAN 的所有節點共享壓縮上下文。在最好的情況下，鏈路本地通訊的 IPv6 標頭可以減少到只有 2 個位元組。對於全局通訊，在最極端的情況下，IPv6 標頭可以被壓縮到 3 個位元組。但是，在更實際的情況下，最小的 IPv6 標頭大小可以是 11 個位元組（一個壓縮的位址前綴）或 19 個位元組（壓縮的來源和目的地前綴）。考慮到 LPWAN 技術的鏈路層負載大小，這些標頭很大，並且在某些情況下甚至比 LPWAN PDU 更大。6LoWPAN 最初設計用於[IEEE.802.15.4]網路，訊號框大小高達 127 位元組，通量高達 250 kbit/s，可能會或可能不會被工作循環。

4.2.2. 位址自動配置

傳統上，介面識別符（IID）是從鏈路層識別符[RFC4944]導引出的。這允許優化，例如標頭壓縮。儘管如此，最近的導引已就以下事實提出建議：由於隱私問題，6LoWPAN 設備不應配置為默認情況下將其鏈路層位址嵌入 IID 中。[RFC8065]提供有關生成 IID 的更好方法的導引。

4.2.3. 片段儲存

如上所述，IPv6 要求下面的層支援 1280 位元組的 MTU [RFC8200]。因此，考慮到 LPWAN 技術的最大負載大小，需要分段。

如果 LPWAN 技術的一層支援分段，則必須進行適當的分析以確定是否應該使用由較低層提供的分段功能或在適配層處使用分段。否則，應在適應層使用分段功能。

6LoWPAN 定義一個分段機制和一個分段標頭，以支援通過 IEEE.802.15.4 網路傳輸 IPv6 封包[RFC4944]。雖然 6LoWPAN 分段標頭適用於 2003 版[IEEE.802.15.4]（訊號框負載大小為 81-102 字位元組），但它不適用於多種 LPWAN 技術，其中許多技術具有最大負載大小比 2003 版[IEEE.802.15.4]低一個數量級。考慮到 LPWAN 技術的負載大小減小，以及使用這些技術的設備的有限能量可用性，6LoWPAN 分段標頭的負擔很高。此外，其資料報偏移欄位以八個八位元組的增量表示。在一些 LPWAN 技術中，6LoWPAN 分段標頭加上原始資料報中的八個八位元組超過第二層負載中的可用空間。此外，LPWAN 網路中的 MTU 可以是可變的，這意味著可變的分段解決方案。

4.2.4. 鄰居發現

6LoWPAN 鄰居發現[RFC6775]定義對 IPv6 ND [RFC4861]的優化，以便使後者的功能適用於使用[IEEE.802.15.4]或類似技術的設備網路。優化包括允許睡眠主機的主機發起交互作用，通過位址註冊機制替換主機基於組播的位址解析，用於前綴分發的多跳躍擴

充和重複位址檢測（注意星形拓撲網路中不需要這些），並支援 6LoWPAN 標頭壓縮。

6LoWPAN ND 可用於不那麼嚴格約束的 LPWAN 網路。產生的相對附加將取決於所使用的 LPWAN 技術（如果合適，還取決於其配置）。在某些 LPWAN 設置中（最大負載大小大於約 60 位元組並且無工作週期或等效操作），RS / RA / NS / NA 交換可以在幾秒鐘內完成，而不會引起封包碎片。

在其他 LPWAN 中（最大負載大小為~10 位元，訊息速率為~0.1 訊息/分鐘），相同的交換可能需要數小時甚至數天，導致嚴重的碎片並消耗大量可用的網路資源。 6LoWPAN ND 行為可以通過使用預設路由器生命週期的適當值，PIO 中的有效生命週期和 6LoWPAN 上下文選項（6CO）中的有效生命週期以及位址註冊生命週期來調整。然而，對於以上提到後面的 LPWAN，6LoWPAN ND 是不合適的。

4.3. 6lo

6lo WG 一直在重用和調整 6LoWPAN，以支援藍芽低功耗（BTLE）、ITU-T G.9959 [G9959]、數位增強無線通訊（DECT）超低功耗（ULE）等鏈路層技術的 IPv6 支援 ，MS / TP-RS485，近距離無線通訊（NFC）IEEE 802.11ah。 （有關 6lo WG 的詳細信息，請參見 <https://datatracker.ietf.org/wg/6lo/>。）這些技術在幾個方面類似於[IEEE.802.15.4]，這是最初的 6LoWPAN 目標技術。

6lo 主要使用最適合每種低層技術的 6LoWPAN 技術子集，並為使用星形拓撲的技術（如 BTLE 或 DECT-ULE）提供額外的優化。

這些網路的主要限制來自設備的性質（受限制設備）；然而，在 LPWAN 中，網路本身施加最嚴格的限制。

4.4. 6tisch

基於 IEEE 802.15.4e（6tisch）解決方案的 TSCH 模式的 IPv6 專用於使用具有確定性時隙通道的[IEEE.802.15.4e] MAC 操作的網狀網路。時隙通道跳頻（TSCH）可以幫助減少衝突並實現更好的

通道平衡。 它通過避免返回通道的空閒收聽時間來改善電池壽命。

6tisch 的一個關鍵要素是使用同步來啟用確定性。TSCH 和 6tisch 可以提供標準調度功能。LPWAN 網路可能不支援 6tisch 中使用的同步。

4.5. RoHC

RoHC 是針對點對點通道中的多媒體流而開發的標頭壓縮機制 [RFC3095]。 RoHC 使用三級壓縮，每個級別都有自己的標頭格式。在第一級，RoHC 發送 52 個位元組的標頭；在第二級，標頭可以是 34 到 15 個位元組；在第三級，標頭大小可以是 7 到 2 個位元組。壓縮級別由序列號（SN）管理，序列號（SN）在最小壓縮中的大小從 2 位元組變化到 4 位元。使用稱為窗口最低有效位元（W-LSB）的演算法完成 SN 壓縮。該窗口具有 4 位元大小，表示 15 個封包，因此每 15 個封包，RoHC 需要滑動窗口以便接收正確的 SN，並且滑動窗口意味著降低壓縮級別。當封包丟失或出錯時，解壓縮程序丟失上下文並丟棄封包，直到發送更大的標頭並提供更完整的訊息。為了估計 RoHC 的性能，使用平均標頭大小。該平均值取決於傳輸條件，但大多數時間在 3 到 4 個位元組之間。

RoHC 還沒有專門針對 LPWAN 的受限主機和網路進行調整：它沒有考慮能量限制和傳輸速率。另外，RoHC 上下文在傳輸期間是同步的，這不允許更好的壓縮。

4.6. ROLL

LPWAN WG 考慮的大多數技術都基於星型拓撲，無需在該層進行路由。未來的工作可能會解決需要調整現有路由協定或新路由協定定義的其他實例。截至編寫本報告時，類似於低功耗和有損網路路由（ROLL）WG 和其他路由協定所做的工作超出 LPWAN WG 的範圍。

4.7. CoAP

約束應用程式協定（CoAP）[RFC7252]為旨在在受約束的 IP 網路上運行的應用程式提供 RESTful 框架。可能有必要調整 CoAP 或相關協定以考慮極端工作週期和 LPWAN 潛在的非常有限通量。

例如，CoAP 中的某些計時器可能需要重新定義。考慮到 CoAP 應答可能允許減少 L2 應答。另一方面，當前在 CoRE WG 中正在進行的工作中，約束管理介面（COMI）/ 約束物件語言（CoOL）網路管理介面使用結構化識別符（SID）來減少 CoAP 上的負載大小可能證明是 LPWAN 技術的良好解決方案。通過添加將 URI 與小識別符匹配的字典以及將 YANG 資料模型緊湊映射到簡明二進制物件表示（CBOR）中來減少負擔。

4.8. 便攜性

LPWAN 節點可以是移動的。 但是，LPWAN 移動性與為移動 IP 指定的移動性不同。LPWAN 意味著零星的流量，很少用於高頻、即時通訊。 應用程序式不生成流程； 他們需要節省能源，而且大多數時候節點都會耗盡。

此外，LPWAN 移動性可能主要適用於代表網路的設備組； 在這種情況下，移動性比閘道更關注閘道。網路移動性（NEMO）[RFC3963]或其他移動閘道解決方案（例如具有 LTE 上行鏈路的閘道）可以用於屬於同一網路閘道的一些終端設備從一個點移動到另一個點以使得它們不會意識到移動。

4.9. DNS 及 LPWAN

域名系統（DNS）[RFC1035]使應用程式能夠使用全局可解析的名稱來命名。許多協定使用 DNS 來識別主機，例如，使用 CoAP 的應用程式。

DNS 查詢/回覆協定作為 DNS 應答的生存時間（TTL）內其他通訊的前標，在 LPWAN 中顯然存在問題，例如，每小時只能使用一次往返，並且使用 TTL 不到 3600 秒。目前尚不清楚 LPWAN 中是否以及如何提供類似 DNS 的功能。

5. 安全考量

大多數 LPWAN 技術集成在 IETF 之外定義的一些身份驗證或加密機制。LPWAN 工作小組可能需要開展工作來整合這些機制以統一管理。標準化的認證、授權和計費(AAA)基礎設施[RFC2904]可以為 LPWAN 的一些安全和管理問題提供可擴充的解決方案。AAA 提供可能在 LPWAN 中使用的集中管理，例如[LoRaWAN-AUTH]和[LoRaWAN-RADIUS]為 LoRaWAN 網路建議可能的安全過程。類似的機制可能有助於探索其他 LPWAN 技術。

使用 LPWAN 的一些應用程式可能會引起很少或沒有隱私考慮。例如,大型辦公樓中的溫度感測器可能不會引起隱私問題。但是，相同的感測器，如果部署在家庭環境中，特別是如果由於人的存在而被觸發，則會引起嚴重的隱私問題：如果終端設備每次有人進入家中的房間時發出（加密）封包，那麼流量對隱私敏感。並且網路實體可以看到該流量的存在越多，就會產生越多的隱私敏感性。此時，尚不清楚這樣的問題是否有可行的緩解措施。在更典型的網路中，可以考慮定義填充機制並允許覆蓋流量。在一些 LPWAN 中，這些機制可能不可行。儘管如此，隱私挑戰確實存在並且可能是真實的；因此，需要一些解決方案。注意，該空間中的解決方案的許多方面可能在 IETF 規範中不可見，但可以是例如特定於實現或部署。

LPWAN 的另一個挑戰將是如何處理密鑰管理和相關協定。在更傳統的網路（例如，Web）中，伺服器可以“裝訂”線上憑證狀態協定（OCSP）回應，以允許瀏覽器檢查所呈現的憑證撤銷狀態[RFC6961]。雖然裝訂方法可能對 LPWAN 有幫助，但由於它避免 RTT、憑證和 OCSP 回應是龐大的項目，並且在具有有限頻寬的 LPWAN 中處理將具有挑戰性。

6. IANA 考量

本文沒有 IANA 指令。

7. 資訊參考

[ANSI-4957-000]
ANSI/TIA, "Architecture Overview for the SmartUtility Network", ANSI/TIA-4957.0000 , May 2013.

[ANSI-4957-210]
ANSI/TIA, "Multi-Hop Delivery Specification of a DataLink Sub-Layer", ANSI/TIA-4957.210 , May 2013.

[arib_ref] ARIB, "920MHz-Band Telemeter, Telecontrol and Data Transmission Radio Equipment", ARIB STD-T108 Version1.0, February 2012.

[ETSI-TS-102-887-2]
ETSI, "Electromagnetic compatibility and Radio spectrum Matters (ERM)； Short Range Devices； Smart Metering Wireless Access Protocol； Part 2: Data Link Layer (MAC Sub-layer)", ETSI TS 102 887-2, Version V1.1.1,September 2013.

[etsi_ref1]
ETSI, "Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz； Part 1: Technical characteristics and methods of measurement", DraftETSI EN 300-220-1, Version V3.1.0, May 2016.

[etsi_ref2]
ETSI, "Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz； Part 2: Harmonised Standard covering the essential requirements ofarticle
3.2 of Directive 2014/53/EU for non specific radio equipment", Final draft ETSI EN 300-220-2P300-220-2, Version V3.1.1, November 2016.

[etsi_unb] ETSI ERM, "System Reference document (SRdoc)； ShortRange Devices (SRD)； Technical characteristics for UltraNarrow Band (UNB) SRDs operating in the UHF spectrum below 1 GHz", ETSI TR 103 435, Version V1.1.1, February2017.

[EUI64] IEEE, "Guidelines for 64-bit Global Identifier

(EUI),Organizationally Unique Identifier (OUI), and Company ID (CID)", August 2017, <http://standards.ieee.org/develop/regauth/tut/eui.pdf>.

[FANOV] IETF, "Wi-SUN Alliance Field Area Network (FAN)Overview", IETF 97, November 2016, <https://www.ietf.org/proceedings/97/slides/slides-97-lpwan-35-wi-sun-presentation-00.pdf>.

[fcc_ref] "Telecommunication Radio Frequency Devices - Operation within the bands 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz.", FCC CFR 47 15.247, June 2016.

[G9959] ITU-T, "Short range narrow-band digital radiocommunication transceivers - PHY, MAC, SAR and LLC layer specifications", ITU-T Recommendation G.9959, January 2015, <http://www.itu.int/rec/T-REC-G.9959>.

[IEEE.802.11]
IEEE, "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium AccessControl (MAC) and Physical Layer (PHY) Specifications",IEEE 802.11.

[IEEE.802.15.12]
IEEE, "Upper Layer Interface (ULI) for IEEE 802.15.4Low- Rate Wireless Networks", IEEE 802.15.12.

[IEEE.802.15.4]
IEEE, "IEEE Standard for Low-Rate WirelessNetworks", IEEE 802.15.4, <https://standards.ieee.org/findstds/standard/802.15.4-2015.html>.

[IEEE.802.15.4e]
IEEE, "IEEE Standard for Local and metropolitanarea networks--Part 15.4: Low-Rate Wireless

PersonalArea Networks (LR-WPANs)
Amendment 1: MAC sublayer",
IEEE 802.15.4e.

[IEEE.802.15.4g]
IEEE, "IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, SmartMetering Utility Networks", IEEE 802.15.4g.

[IEEE.802.15.9]
IEEE, "IEEE Recommended Practice for Transport ofKey Management Protocol (KMP) Datagrams", IEEE Standard 802.15.9, 2016, <https://standards.ieee.org/findstds/standard/802.15.9-2016.html>.

[IEEE.802.1AR]
ANSI/IEEE, "IEEE Standard for Local and metropolitanarea networks - Secure Device Identity", IEEE 802.1AR.

[IEEE.802.1x]
IEEE, "Port Based Network Access Control", IEEE 802.1x.

[LoRaSpec] LoRa Alliance, "LoRaWAN Specification Version V1.0.2", July 2016, <https://lora-alliance.org/sites/default/files/2018-05/lorawan1_0_2-20161012_1398_1.pdf>.

[LoRaWAN] Farrell, S. and A. Yegin, "LoRaWAN Overview", Work in Progress, draft-farrell-lpwan-lora-overview-01,October 2016.

[LoRaWAN-AUTH]
Garcia, D., Marin, R., Kandasamy, A., and A. Pelov, "LoRaWAN

Authentication in Diameter", Work inProgress, draft-garcia-dime-diameter-lorawan-00, May 2016.

[LoRaWAN-RADIUS]
Garcia, D., Lopez, R., Kandasamy, A., and A. Pelov, "LoRaWAN Authentication in RADIUS", Work inProgress, draft-garcia-radext-radius-lorawan-03, May 2017.

[LPWAN-GAP]
Minaburo, A., Ed., Gomez, C., Ed., Toutain, L.,Paradells, J., and J. Crowcroft, "LPWAN Survey and GAP Analysis", Work in Progress, draft-minaburo-lpwan-gap-analysis-02, October 2016.

[NB-IoT] Ratilainen, A., "NB-IoT characteristics", Work in Progress, draft-ratilainen-lpwan-nb-iot-00, July2016.

[nbiot-ov] IEEE, "NB-IoT Technology Overview and Experience from Cloud-RAN Implementation", Volume 24, Issue 3 Pages26-32, DOI 10.1109/MWC.2017.1600418, June 2017.

[RFC768] Postel, J., "User Datagram Protocol", STD 6, RFC768, DOI 10.17487/RFC0768, August 1980, <https://www.rfc-editor.org/info/rfc768>.

[RFC793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol,

Version6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <https://www.rfc-editor.org/info/rfc2460>.

[RFC2904] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M.,and D. Spence, "AAA Authorization Framework", RFC2904, DOI 10.17487/RFC2904, August 2000, <https://www.rfc-editor.org/info/rfc2904>.

[RFC3095] Bormann, C., Burmeister, C., Degermark, M., Fukushima,H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP,UDP, ESP, and uncompressed", RFC 3095, DOI 10.17487/RFC3095, July 2001, <https://www.rfc-editor.org/info/rfc3095>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315,July 2003, <https://www.rfc-editor.org/info/rfc3315>.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic SupportProtocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <https://www.rfc-editor.org/info/rfc3963>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September2007, <https://www.rfc-editor.org/info/rfc4944>.

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, DOI10.17487/RFC5216, March 2008, <https://www.rfc-editor.org/info/rfc5216>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate RevocationList (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format forIPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/info/rfc6282>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[RFC6961] Pettersen, Y., "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", RFC6961, DOI 10.17487/RFC6961, June 2013, <https://www.rfc-editor.org/info/rfc6961>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7452] Tschofenig, H., Arkko, J., Thaler, D., and D. McPherson, "Architectural Considerations in Smart ObjectNetworking", RFC 7452, DOI 10.17487/RFC7452, March 2015, <https://www.rfc-editor.org/info/rfc7452>.

[RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", RFC 7668, DOI 10.17487/RFC7668, October2015, <https://www.rfc-editor.org/info/rfc7668>.

[RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation- Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <https://www.rfc-editor.org/info/rfc8065>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8240] Tschofenig, H. and S. Farrell, "Report from the Internet of Things Software Update (IoTSU) Workshop 2016", RFC 8240, DOI 10.17487/RFC8240, September 2017, <https://www.rfc-editor.org/info/rfc8240>.

[Sigfox] Zuniga, J. and B. PONSARD, "Sigfox System Description", Work in Progress, draft-zuniga-lpwan-sigfox-system-description-04,December 2017.

[TGPP23720]
3GPP, "Study on architecture enhancements forCellular Internet of Things", 3GPP TS 23.720 13.0.0, 2016.

[TGPP33203]
3GPP, "3G security； Access security forIP-based services", 3GPP TS 23.203 13.1.0, 2016.

[TGPP36201]
3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA)； LTE physical layer； General description",3GPP TS 36.201 13.2.0, 2016.

[TGPP36300]
3GPP, "Evolved Universal Terrestrial Radio Access(E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)； Overall description； Stage 2", 3GPP TS36.300 13.4.0, 2016, <http://www.3gpp.org/ftp/Specs/2016-09/Rel-14/36_series/>.

[TGPP36321]
3GPP, "Evolved Universal Terrestrial RadioAccess (E-UTRA)； Medium Access Control (MAC) protocol specification", 3GPP TS 36.321 13.2.0, 2016.

[TGPP36322]
3GPP, "Evolved Universal Terrestrial RadioAccess (E-UTRA)；

Radio Link Control (RLC) protocol specification", 3GPP TS 36.322 13.2.0, 2016.

[TGPP36323]
3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA)； Packet Data Convergence Protocol(PDCP) specification (Not yet available)", 3GPP TS 36.32313.2.0, 2016.

[TGPP36331]
3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA)； Radio Resource Control (RRC)； Protocol specification", 3GPP TS 36.331 13.2.0, 2016.

[USES-6LO] Hong, Y., Gomez, C., Choi, Y-H., and D-Y. Ko, "IPv6 over Constrained Node Networks(6lo) Applicability & Usecases", Work in Progress, draft-hong-6lo-use-cases-03, October 2016.

[wisun-pressie1]
Beecher, P., "Wi-SUN Alliance", March 2017, <http://indiasmartgrid.org/event2017/10-03-2017/4.%20Round table%20on%20Communication%20and%20Cyber%20Security/1.%20P hil%20Beecher.pdf>.

[wisun-pressie2]
Heile, B., "Wi-SUN Alliance Field Area Network (FAN)Overview", As presented at IETF 97, November2016, <https://www.ietf.org/proceedings/97/slides/ slides-97-lpwan-35-wi-sun-presentation-00.pdf>.

致謝

感謝貢獻者部分中列出的所有優秀文本。 處理錯誤只是編輯的錯。

除了貢獻者部分的內容之外，還要感謝（按字母順序排列）以下內容以供評論：

Abdussalam Baryun
Andy Malis
Arun (arun@acklio.com)
Behcet SariKaya
Dan Garcia Carrillo
Jiazi Yi
Mirja Kuhlewind
Paul Duffy
Russ Housley
Samita Chakrabarti
Thad Guidry
Warren Kumari

在撰寫本文時，Alexander Pelov 和 Pascal Thubert 是 LPWAN WG 主席。

這是愛爾蘭科學基金會的 CONNECT 中心國家物聯網網路 <https://connectcentre.ie/pervasive-nation/>。

貢獻者

如上所述，本文主要是由下列全部貢獻者開發的內容集合。 主要輸入文件及其作者：

- 第 2.1 節的文字由 Alper Yegin 和 Stephen Farrell 在[LoRaWAN]中提供。
- 第 2.2 節的文本由 Antti Ratilainen 在[NB-IoT]中提供。
- 第 2.3 節的文字由 Juan Carlos Zuniga 和 Benoit Ponsard 在[Sigfox]中提供。
- 第 2.4 節的文本是通過 Bob Heile 的個人通訊提供，由 Bob 和 Sum Chin Sean 撰寫。 在撰寫本文時，沒有網際網路草案。
- 第 4 節的文字由 Ana Minabiru、Carles Gomez、Laurent Toutain、Josep Paradells 和 Jon Crowcroft 在[LPWAN-GAP]中提供。 該文件的其他文本也在上文其他地方使用。

貢獻者的完整列表如下：

Jon Crowcroft
劍橋大學
JJ 湯姆森大道
劍橋，CB3 0FD
英國

電子郵件：jon.crowcroft@cl.cam.ac.uk

Carles Gomez
UPC / i2CAT
C / Esteve Terradas，7
Castelldefels 08860
西班牙

電子郵件：carlesgo@entel.upc.edu

Bob Heile
Wi-Sun 聯盟
11 Robert Toner Blvd，Suite 5-301
North Attleboro，MA 02763
美國

電話：+ 1-781-929-4832
電子郵件：bheile@ieee.org

Ana Minaburo
Acklio
2bis rue de la Chataigneraie
35510 Cesson-Sevigne Cedex
法國

電子郵件：ana@ackl.io

Josep PAradells
UPC / i2CAT
C / Jordi Girona，1-3
巴塞羅那 08034
西班牙

電子郵件：josep.paradells@entel.upc.edu

Charles E. Perkins
Futurewei
2330 中央高速公路
聖克拉拉，加州 95050
美國

電子郵件：charliep@computer.org

Benoit Ponsard
Sigfox
Jean Rostand 街 425 號
Labege 31670
法國

電子郵件：Benoit.Ponsard@sigfox.com
URI：http：//www.sigfox.com/

Antti Ratilainen
愛立信
Hirsalantie 11
Jorvas 02420
芬蘭

電子郵件：antti.ratilainen@ericsson.com

Chin-Sean SUM
Wi-Sun 聯盟

20，Science Park Rd 117674
新加坡

電話：+65 6771 1011
電子郵件：sum@wi-sun.org

Laurent Toutain
研究所 MINES TELECOM；電信布列塔尼
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
法國

電子郵件：Laurent.Toutain@telecom-bretagne.eu

Alper Yegin
Actility
巴黎
法國

電子郵件：alper.yegin@actility.com

Juan Carlos Zuniga
Sigfox
Jean Rostand 街 425 號
Labege 31670
法國

電子郵件：JuanCarlos.Zuniga@sigfox.com
URI：http：//www.sigfox.com/

作者資訊

Stephen Farrell（編輯）
都柏林聖三一學院
都柏林 2

愛爾蘭

電話：+ 353-1-896-2354
電子郵件：stephen.farrell@cs.tcd.ie