21. RFC 8180：Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration

RFC 8180：IEEE 802.15.4e（6TiSCH）配置的 TSCH 模式下的最簡 IPv6

網際網路工程任務組(IETF)
Request for Comments:8180
BCP: 10
分類: 當前最佳實踐
ISSN: 2070-1721

X. Vilajosana, Ed.
Universitat Oberta de Catalunya
K. Pister
University of California Berkeley
T. Watteyne
Analog Devices

May 2017

IEEE 802.15.4e（6TiSCH）配置的 TSCH 模式下的最簡 IPv6

摘要

該文描述了通過 IEEE 802.15.4e（6TiSCH）網路的 TSCH 模式的 IPv6 的最小操作模式。該最小操作模式指定了需要支援的基準協定集以及足以啟用 6TiSCH 功能網路的推薦配置和操作模式。6TiSCH 通過由 IEEE Std 802.15.4 TSCH 鏈路組成的時槽通道跳變（TSCH）網格提供 IPv6 連接。 此最小模式使用具有相應配置的協定集合，包括 IPv6 低功耗無線個人區域網路（6LoWPAN）框架，通過 IEEE Std 802.15.4 TSCH 實現可交交交互操作的 IPv6 連接。 這種最小配置為網路和安全引導提供了必要的頻寬，並定義了與 IEEE Std 802.15.4 TSCH 介面的 IETF 協定之間的正確鏈路。所有符合 6TiSCH 標準的設備都應實現這種最小操作模式。

本文的狀態

本備忘錄記錄了網際網路最好的實踐。

本文是網際網路工程任務組（IETF）的產品。 它代表了 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。 有關 BCP 的更多資訊，請參見 RFC 7841 的第 2 節。

有關本文的當前狀態，任何勘誤以及如何提供反饋的資訊，請訪問 http://www.rfc-editor.org/info/rfc8180。

版權聲明

目錄

1. 前言

6TiSCH 網路通過由 IEEE Std 802.15.4 TSCH 鏈路[IEEE.802.15.4]組成的時槽通道跳變（TSCH）網格[RFC7554]提供 IPv6 連接[RFC2460]。通過使用 6LoWPAN 框架（[RFC4944]，[RFC6282]，[RFC8025]，[RFC8138]和[RFC6775]），RPL [RFC6550]和 RPL 目標函數 0（OF0）[RFC6552]獲得 IPv6 連接]。

該規範定義了用於構建 6TiSCH 網路的最小操作模式的指令引數和過程。任何符合 6TiSCH 的設備都應該實現這種操作模式。此指令引數配置為節點引導網路提供必要的頻寬。引導過程包括初始網路配置和安全引導。 在本說明書中，未經修改地使用 802.15.4TSCH 模式，6LoWPAN 框架，RPL [RFC6550]和 RPL 目標函數 0（OF0）[RFC6552]。指定 TSCH 的參數和特定操作以保證 6TiSCH 網路中的節點之間的互通性。

在 6TiSCH 網路中，節點遵循根據 802.15.4 TSCH 的通信調度。節點在連接網路時學習通信時間表。遵循此規範時，所學習的計劃對於所有節點都是相同的，並且不會隨時間而變化。未來的規範可以定義用於動態管理通信調度的機制。動態調度解決方案超出了本文的範圍。

IPv6 尋址和壓縮由 6LoWPAN 框架實現。該框架包括[RFC4944]，[RFC6282]，[RFC8025]，用於尋址和標頭壓縮的 6LoWPAN 路由標頭分派[RFC8138]，以及用於重複地址檢測（DAD）和地址解析的[RFC6775]。

預計未來將進行更高級的工作，以此通過動態操作補充最小配置，這些操作可以使計劃在運行時適應流量需求。

2. 需求語言

關鍵詞"必須(MUST)"、"不得(MUST NOT)"，"必要(REQUIRED)"，"必須(SHALL)"，"不得(SHALL NOT)"，"應該(SHALL NOT)"，"不應該(SHOULD NOT)"，"建議(RECOMMENDED)"，"不建議(RECOMMENDED)"，"可以(MAY)"，"可選(OPTIONAL)"在本文中，只有當它們出現在所有大寫字母中時才會按照 BCP 14 [RFC2119] [RFC8174]中的描述進行解釋，如此處所示。

3. 術語

本文使用[TERMS-6TiSCH]中的術語。 本文中使用了以下概念：

802.15.4：我們將“ 802.15.4”用作“ IEEE 標準”的簡稱本文中的“ 802.15.4”。

SFD: Start of Frame Delimiter 訊號框首定界符

RX: Reception 接收

TX: Transmission 傳輸

IE: Information Element 資訊要素

EB: Enhanced Beacon 增強的信標

ASN: Absolute Slot Number 絕對槽數字

Join Metric: TSCH 同步 IE 中的欄位表示發送 EB 的節點與 PAN 協調器之間的拓撲距離。

PAN: Personal Area Network 個人區域網路

MLME: MAC Layer Management Entity MAC 層管理實體

4. IEEE Std 802.15.4 設定

符合本規範的實現必須在時槽通道跳頻(TSCH)模式下實現 IEEE Std 802.15.4 [IEEE.802.15.4]。

本節的其餘部分詳細介紹了推薦的 TSCH 設置，如圖 1 所示.EB 列中標記的任何屬性都在節點發送[IEEE.802.15.4]的EB中公佈，並由連接網路的人員學習。 更改其值意味著更改 EB 的內容。

如果本規範中的值與 IEEE Std 802.15.4 [IEEE.802.15.4]之間存在差異，則 IEEE 標準優先。

Property	Recommended Setting	EB*
Slotframe Size	Tunable. Trades off bandwidth against energy.	X
Number of scheduled cells** (active)	1 Timeslot 0x0000 Channel Offset 0x0000 Link Options = (TX Link = 1, RX Link = 1, Shared Link = 1, Timekeeping = 1)	X
Number of unscheduled cells (off)	All remaining cells in the slotframe.	X
Max Number MAC retransmissions	3 (4 transmission attempts)	
Timeslot template	IEEE Std 802.15.4 default (macTimeslotTemplateId=0)	X
Enhanced Beacon Period (EB_PERIOD)	Tunable. Trades off join time against energy.	
Number used frequencies (2.4 GHz O-QPSK PHY)	IEEE Std 802.15.4 default (16)	X
Channel Hopping sequence (2.4 GHz O-QPSK PHY)	IEEE Std 802.15.4 default (macHoppingSequenceID = 0)	X

*此欄中的“X”表示此屬性的值已在 EB 中宣佈； 因此，新節點在加入時會學習它。

**此單元格連接類型設置為 ADVERTISING。

圖 1：推薦的 IEEE Std 802.15.4 TSCH 設置

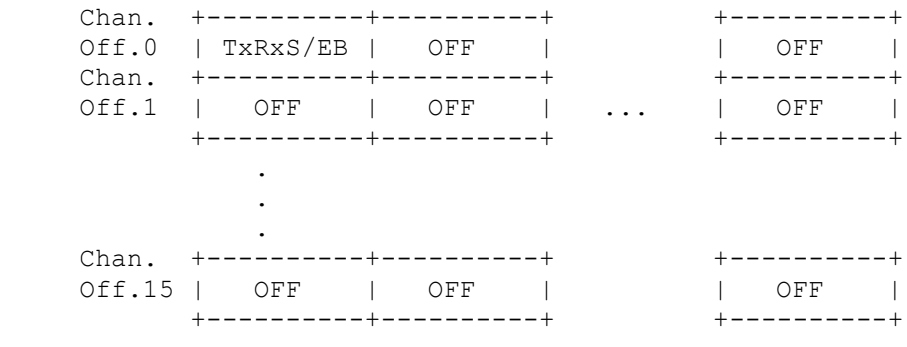
4.1. TSCH 時間表

這種最小運行模式使用單個槽框（slotframe）。 TSCH 槽框由可調數量的時槽組成。槽框大小（即它包含的時槽數量）換掉能量消耗的頻寬。 需要調整槽框大小; 調整它的方式超出了本規範的範圍。 槽框的尺寸在 EB 中公佈。

槽框控制碼（macSlotframeHandle）的推薦值為 0x00。 實現可以選擇使用不同的槽框控制碼，例如，添加具有更高優先級的其他槽框。 其他槽框的使用超出了本文的範圍。

在槽框中只有一個預定的單元。 可以在槽框內的任何 slotOffset / channelOffset 上調度該單元。 EB 中公佈了該單元格在計劃中的位置。調度單元的連接類型（LinkType）是廣告（ADVERTISING），以允許在其上發送 EB。

圖 2 示出了長度為 101 個時槽的槽框的範例，導致無線電佔空比低於 0.99％。



EB：Enhanced Beacon 增強型信標
Tx：Transmit 傳送
接收：Receive 接收
S：Shared 共用
OFF：Unscheduled by this specification 此規範未安排

圖 2：長度為 101 個槽框的範例時槽

節點可以使用調度的單位來發送/接收所有類型的鏈路層訊號框。 EB 被發送到鏈路層廣播地址並且不被確認。 資料訊號框是單播發送的，並由接收鄰居確認。

槽框中的所有剩餘單元都是未調度的。可以在將來定義動態調度解決方案來調度這些單位。 一個例子是 6top Protocol（6P）[PROTO-6P]。 動態調度解決方案超出了本文的範圍。

應使用 TSCH 時槽範本的默認值（在[IEEE.802.15.4]的第 8.4.2.2.3 節中定義）和通道跳躍序列（在[IEEE.802.15.4]的第 6.2.10 節中定義）。 節點可以通過在其 EB 中正確地宣佈它們來使用不同的值。

4.2. 單位選項

在調度的單位中，如果存在要發送的封包，則發送節點，否則就監聽（“TX”和“RX”位都被設置）。 當節點發送請求每[IEEE.802.15.4]的鏈路層確認並且沒有接收到所請求的確認時，它使用退避機制來解決可能的衝突（設置“共用”位）。連接網路的節點使用該單位維持與其初始時間源鄰居的時間同步(設置“計時”位）。

這將轉換為該單元的鏈接選項：

b0 = TX Link = 1 (set)
b1 = RX Link = 1 (set)
b2 = Shared Link = 1 (set)
b3 = Timekeeping = 1 (set)
b4 = Priority = 0 (clear)
b5-b7 = Reserved = 0 (clear)

4.3. 重傳

根據圖 1，RECOMMENDED 最大鍊路層重傳次數為 3，這意味著，對於需要確認的資料封包，如果在總共 4 次嘗試之後沒有接收到，則認為傳輸失敗並且鏈路層必須通知上層。 不重傳不需要確認的資料封包（包括 EB）。

4.4. 時槽時序

根據圖 1，RECOMMENDED 時槽範本是[IEEE.802.15.4]中定義的默認範本（macTimeslotTemplateId = 0）。

4.5. 訊號框的內容

[IEEE.802.15.4] 定義了訊號框的格式。 通過一組標誌，[IEEE.802.15.4]允許存在（或不存在）多個欄位，具有不同的長度，並具有不同的值。 本規範詳細介紹了 802.15.4 訊號框的推薦內容，同時嚴格遵守[IEEE.802.15.4]。

4.5.1. IEEE Std 802.15.4 Header

訊號框版本欄位必須設置為 0b10（訊號框版本 2）。 序列號欄位可以省略。

EB 目標地址欄位必須設置為 0xFFFF(短廣播地址)。如果支援，則應將 EB 源位址欄位設置為節點的短地址。 否則，必須使用長位址。

PAN ID 壓縮位應該指示源 PAN ID 是“不存在”而目標 PAN ID 是“存在”。 PAN ID 壓縮位的值在 IEEE Std 802.15.4-2015 規範的表 7-2 中規定，並且取決於目的地和源鏈路層地址的類型（例如，短，擴充，不存在）。

根據[IEEE.802.15.4]的第 6.7.2 節，節點遵循接收和拒絕規則。

根據[IEEE.802.15.4]格式化隨機數。 在 IEEE 標準 802.15.4 規範[IEEE.802.15.4]中，第 9.3.2.2 節描述了隨機數生成，第 9.3.1 節，附錄 B.2 和附錄 B.2.2 中描述了位元组排序。

4.5.2. 增強的信標訊號框

引導後，TSCH 節點以非同步，未連接狀態啟動。 通過監聽 EB 來實現初始同步。 可以監聽到來自多個網路的 EB。 存在許多用於區分網路的機制，其細節超出範圍。

IEEE Std 802.15.4 規範沒有定義發送 EB 的頻率，也沒有定義其內容 [IEEE.802.15.4]。 在最小 TSCH 配置中，節點應該每 EB_PERIOD 發送一個 EB。 調整 EB_PERIOD 允許在連接時間和能量消耗之間進行權衡。

應使用 EB 來獲取有關本地網路的資訊，並同步 ASN 和節點決定連接的特定網路的時間偏移。 一旦連接特定網路，節點可以選擇繼續監聽 EB，以收集有關其他網路的更多資訊。在連接過程中，在創建與時間父項的安全連接之前，節點可以使用 EB 保持同步。[RFC7554]討論了不同的時間同步方法。

IEEE Std 802.15.4 規範要求發送 EB 以使節點能夠連接網路。 EB 應該帶有下面列出的資訊元素（IE）[IEEE.802.15.4]。

TSCH 同步 IE：包含 ASN 和 Join Metric 等同步資訊。 Join Metric 欄位的值在 6.1 節中討論。

TSCH 時槽 IE：包含時槽範本識別符。 該範本用於指定時槽的內部時序。 此規範建議使用默認時槽範本。

通道跳躍 IE：包含通道跳躍序列識別符。該規範建議默認的通道跳躍序列。

TSCH Slotframe 和 Link IE：允許連接節點瞭解在連接網路時使用的初始計劃。 本檔建議使用單個單位。

如果節點嚴格遵循圖 1 中的建議設置，則它發送的 EB 具有與連接時接收的 EB 完全相同的內容，但 TSCH 同步 IE 中的連接度量欄位除外。

當節點已經與EB發送器同步的網路連接(即,它已經接收到EB）並按照此規範配置其調度時，節點應該忽略嘗試更改配置參數的後續 EB。 這並不排除從其他網路監聽 EB。

4.5.3. 確認訊號框

根據[IEEE.802.15.4]，每個確認（acknowledgment）包含 ACK / NACK 時間校正 IE。

4.6. 數據連接層

在保護鏈路層訊號框時，必須通過 IEEE Std 802.15.4 [IEEE.802.15.4]中定義的鏈路層安全機制來保護鏈路層訊號框。鏈路層認證必須應用於整個訊號框，包括 802.15.4 標頭。鏈路層加密可以應用於 802.15.4 有效載荷 IE 和 802.15.4 有效載荷。

本規範假定存在兩個加密密鑰：

密鑰 K1 用於驗證 EB。 EB 必須只進行身份驗證（不加密）；它們的內容在 4.5.2 節中定義。

密鑰 K2 用於驗證和加密 DATA 和 ACKNOWLEDGMENT 訊號框。

可以在密鑰分發階段預先配置或學習這些密鑰。 例如，在[SEC-6TISCH]和[SEC-JOIN-6TISCH]中定義了密鑰分發機制。密鑰分發超出了本文的範圍。

連接節點（JN）的行為根據預先配置的密鑰而不同：

如果密鑰 K1 和 K2 都是預先配置的，則 JN 不依賴於密鑰分發階段來學習 K1 或 K2。

如果密鑰 K1 是預先配置的而不是密鑰 K2，則 JN 使用 K1 對 EB 進行認證，並依賴於密鑰分發階段來學習 K2。

如果密鑰 K1 和密鑰 K2 都沒有預先配置，則 JN 接受 IEEE 標準 802.15.4 [IEEE.802.15.4]第 6.3.1.2 節中定義的 EB，即，如果狀態為“ 不安全的過程表明錯誤“。 然後 JN 運行密鑰分發階段以學習 K1 和 K2。 在此過程中，JN 正在與之通信的節點使用 secExempt 機制（參見[IEEE.802.15.4]的第 9.2.4 節）來處理來自 JN 的訊號框。 完成密鑰分發階段後，已為 JN 安裝 secExempts 的節點必須清除已安裝的異常規則。

在網路重置的情況下，新網路必須使用新的加密密鑰或確保 ASN 保持單調增加。

5. RPL 設定

在多跳拓撲中，可以使用 RPL 路由協定[RFC6550]。

5.1. 客觀功能

如果使用 RPL，節點必須實現 RPL 目標函數零（OF0）[RFC6552]。

5.1.1. 排序計算

排序計算在[RFC6552]的 4.1 節中描述。 節點的排序（參見圖 4）通過以下等式計算：

R(N) = R(P) + rank_increment
rank_increment = (Rf*Sp + Sr) * MinHopRankIncrease

圖 3 列出了使用 RPL 時必須使用的 OF0 參數值。

OF0 Parameters	Value
Rf	1
Sp	(3*ETX)-2
Sr	0
MinHopRankIncrease	DEFAULT_MIN_HOP_RANK_INCREASE (256)
MINIMUM_STEP_OF_RANK	1
MAXIMUM_STEP_OF_RANK	9
ETX limit to select a parent	3

圖 3：OF0 參數

step_of_rank（Sp）使用預期傳輸計數（ETX）[RFC6551]。

實現必須遵循 OF0 的規範化指導，如[RFC6552]的第 1 節和第 4.1 節中所討論的。 Sp 應該計算為（3 * ETX）-2。 Sp（MINIMUM_STEP_OF_RANK）的最小值表示質量良好的鏈接。 Sp（MAXIMUM_STEP_OF_RANK）的最大值表示鏈接質量差。 Sp 的默認值（DEFAULT_STEP_OF_RANK）表示平均質量鏈接。 ETX 大於 3 的候選父選項不應被選中。這樣可以避免在使用的鏈路上使用大於最大允許傳輸嘗試次數的 ETX 值。

5.1.2. 排序計算範例

本節說明瞭 OF0 的使用（參見圖 4）。 我們有：

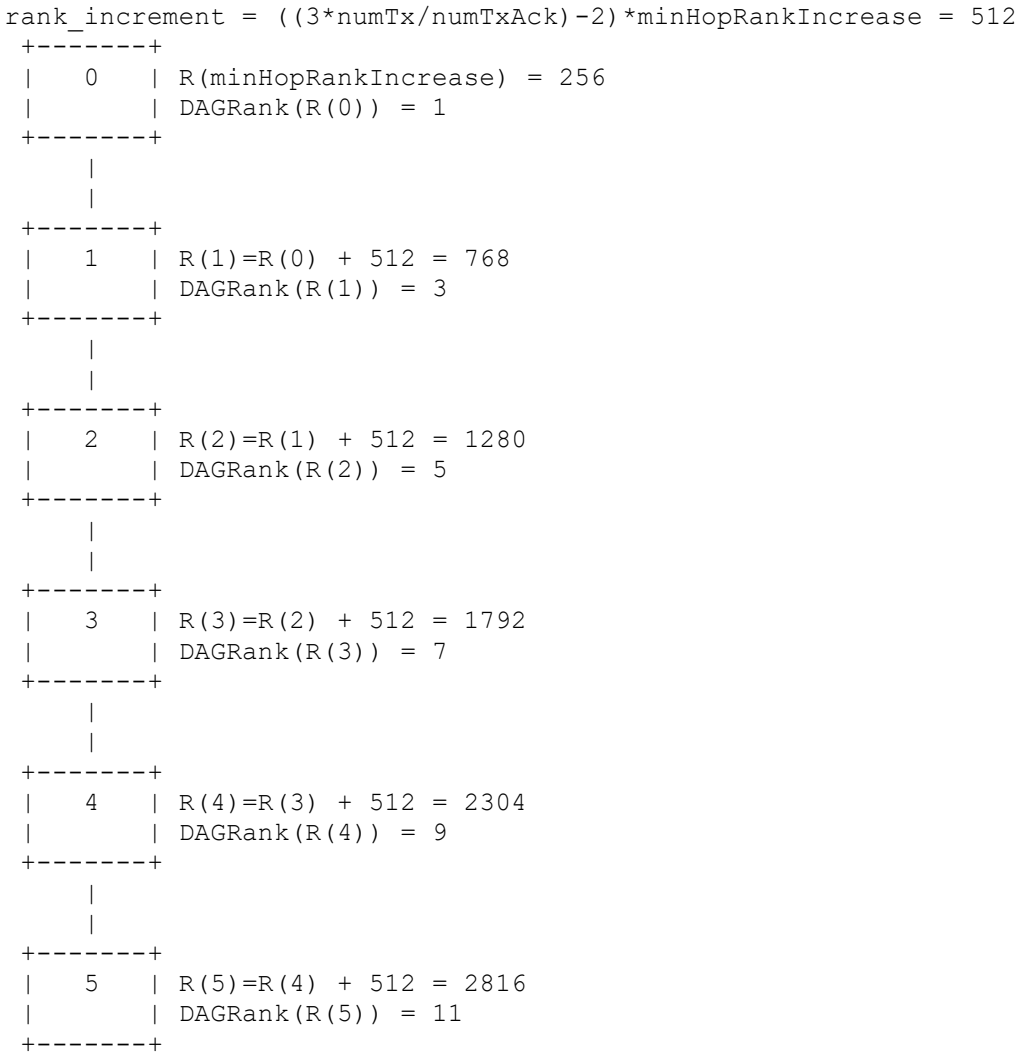


圖 4：5-hop 網路的排名計算範例，其中所有鏈接的 numTx = 100 和 numTxAck = 75。

5.2. 運行的模式

當使用 RPL 時，節點必須實現非存儲操作模式（參見[RFC6550]的第 9.7 節）。 存儲操作模式（參見[RFC6550]的第 9.8 節）應該

由具有足夠功能的節點實現。 未實現 RPL 的節點必須作為葉節點連接。

5.3. Trickle 計時器

使用 Trickle 演算法發送諸如 DODAG 資訊對象（DIO）之類的 RPL 信號消息（參見[RFC6550]的第 8.3.1 節和[RFC6206]的第 4.2 節）。 對於此規範，Trickle 定時器必須與 RPL 定義的默認值一起使用（參見[RFC6550]的第 8.3.1 節）。

5.4. 封包內容

RPL 資訊和逐跳擴充標頭必須遵循[RFC6553]和[RFC6554]。對於在低功耗和有損網路（LLN）上形成的資料封包需要穿過中間路由器的情況，這些必須遵循[RFC6282]和[RFC2460]規定的 IP-in-IP 封裝要求。 路由擴充標頭，例如 RPL 包資訊（RPI）[RFC6550]和源路由標頭（SRH）[RFC6554]，以及封裝時的外部 IP 標頭，必鬚根據[RFC8138]和[RFC8025]進行壓縮。

6. 網路形成和生命週期

6.1. 連接度量欄位的值

EB 中的 TSCH 同步 IE 的連接度量必須基於節點的路由度量來計算，歸一化為 0 到 255 之間的值。連接度量的較低值表示發送 EB 的節點在拓撲上“更接近”到網路的根源。 因此，連接度量的較低值表示連接節點與該鄰居同步的較高偏好。

如果網路使用 RPL，任何節點（包括有向無環圖（DAG）根）的連接度量必須設置為 DAGRank（rank）-1。 根據第 5.1.1 節，DAGRank（rank（0））= 1.DAGRank（rank（0））- 1 = 0 符合 802.15.4 要求 root 用戶 Join Metric = 0。

如果網路不使用 RPL，則 Join Metric 值必須遵循[IEEE.802.15.4]規定的規則。

6.2. 時間來源鄰居選擇

當節點連接網路時，它可能會監聽到網路中已有的不同節點發送的 EB。決定哪個鄰居同步（例如，哪個鄰居成為節點的初始時間源鄰居）是特定於實現的。例如，在收到第一個 EB 之後，節點可以監聽最多 MAX_EB_DELAY 秒，直到它收到來自 NUM_NEIGHBOURS_TO_WAIT 個不同鄰居的 EB。MAX_EB_DELAY 和 NUM_NEIGHBOURS_TO_WAIT 的推薦值在圖 5 中定義。當從不同的鄰居接收 EB 時，節點可以使用每個 EB 中的 Join Metric 欄位來選擇初始時間源鄰居，如 IEEE Std 802.15.4 [IEEE.802.15.4]。的第 6.3.6 節所述。

任何時候，節點必須保持與至少一個時間源鄰居的同步。當使用 RPL 時，必須在其 RPL 路由父集中的鄰居中選擇節點的時間源鄰居。在節點不能保持與至少一個時間源鄰居的連接的情況下，該節點失去同步並且需要再次連接網路。

6.3. 何時開始發送 EB

當 RPL 節點連接網路時，它必須在獲取 RPL Rank 之前不發送 EB 以避免時間同步結構中的不一致。這適用於具有相應路由度量的其他路由式通訊協定。一旦節點獲取路由資訊（例如，RPL 秩，參見 5.1.1 節），它就應該開始發送 EB。

6.4. 滯後

根據 [RFC6552] 和 [RFC6719]，規範建議使用邊界值（PARENT_SWITCH_THRESHOLD）以避免在比較等級時父節點的不斷變化。當評估屬於比當前最小路徑更小的路徑成本的父級時，僅當新路徑和當前路徑之間的差異大於定義的 PARENT_SWITCH_THRESHOLD 時，才選擇候選節點作為新父級。否則，節點可以繼續使用當前首選父節點。根據[RFC6719]，當使用 ETX 度量時，PARENT_SWITCH_THRESHOLD 應該設置為 192（格式為 128 * ETX）; 如果使用的度量是（（3 * ETX）-2）

* minHopRankIncrease 或比例值，則本文的建議是使用 PARENT_SWITCH_THRESHOLD 等於 640。 這涉及路由父和時間源鄰居選擇的滯後。

7. 實施推薦

7.1. 鄰居表

鄰居表的確切格式是特定於實現的。推薦的每個鄰居資訊（取自[openwsn]實現）：

identifier: 鄰居的識別符（例如，EUI-64）。

numTx: 到該鄰居的鏈路層傳輸嘗試次數。

numTxAck: 已經由該鄰居確認鏈路層的傳輸鏈路層訊號框數。

numRx: 從該鄰居收到的鏈路層訊號框數。

timestamp: 當從該鄰居收到最後一個訊號框時。 這可以基於 ASN 計數器或任何其他時基。 它可用於觸發保持活動的消息。

routing metric: 例如，該鄰居的 RPL 排名。

time-source neighbor: 指示此鄰居是否是時間源鄰居的標誌。

7.2. 隊列和優先級

IEEE Std 802.15.4 規範[IEEE.802.15.4]沒有定義使用佇列來處理上層資料（來自上層的應用程式或控制資料）。推薦以下規則：

節點配置為在佇列中保留每個鏈路可配置數量的上層資料封包（預設值為 NUM_UPPERLAYER_PACKETS）一段時間，該時間應覆蓋連接進程（默認為 MAX_JOIN_TIME）。

由 802.15.4 層（包括 EB）生成的訊號框排隊的優先順序高於來自更高層的訊號框。

訊號框類型 BEACON 的排隊優先順序高於框架類型 DATA。

7.3. 推薦設置

圖 5 列出了本規範中討論的設置的推薦值。

Parameter	RECOMMENDED Value
MAX_EB_DELAY	180
NUM_NEIGHBOURS_TO_WAIT	2
PARENT_SWITCH_THRESHOLD	640
NUM_UPPERLAYER_PACKETS	1
MAX_JOIN_TIME	300

Figure 5: 推薦設置

8. 安全注意事項

本文僅涉及鏈路層安全性。

就其本質而言，許多物聯網（IoT）網路在物理上易受攻擊的位置上有著節點。 我們應該假設節點將會受到物理攻擊，檢查其記憶體並提取其密鑰。 固定的密碼無法保密。 這會影響節點連接過程。 為網路配置固定鏈路金鑰 K2 並不安全。 對於大多數應用程式，這意味著會存在連接階段，在該階段期間將允許對未經過身份驗證的節點進行某種級別的授權。 這些細節超出了範圍，但連結層必須在這裡提供一些靈活性。

如果攻擊者獲得了 K1，則可以通過發送經過身份驗證的 EB 來生成偽 EB 以攻擊整個網路。 攻擊者可以使連接節點啟動攻擊者的連接進程。 在連接進程包括 K2 的認證和分發的情況下，連接進程將失敗並且 JN 將注意到攻擊。 如果 K2 也遭到入侵，JN 將不會注意到攻擊並且網路將受到損害。
即使攻擊者不知道 K1 和 K2 的值（第 4.6 節），它仍然可以生成使用任意金鑰驗證的偽 EB 訊號框。在這裡，我們討論這些假 EB 可能產生的影響，具體取決於預先配置的金鑰。

如果 K1 和 K2 都預先配置好; 連接節點可以區分合法 EB 和假 EB，並連接合法網路。 假 EB 不會有影響。

如果 K1 是預先配置但不是 K2，則同樣成立。

如果 K1 和 K2 都沒有預先配置，則連接節點可能會將偽 EB 誤認為是合法的 EB 並啟動對攻擊者的連接進程。 連接進程將失敗，因為連接節點將無法在安全握手期間對攻擊者進行身份驗證。這將強制連接節點重新開始監聽 EB。 因此，雖然連接節點從不會連接攻擊者，但這會花費連接節點的時間和能源，並且這也會是攻擊的載體。

選擇預先提供的金鑰需要平衡上述不同的討論。

連接進程結束後，已連接的節點可以驗證 EB（它知道 K1）。 這意味著它可以處理其內容並使用 EB 進行同步。

ASN 為插槽中的安全運行提供亂數。使用給定金鑰重新使用 ASN 會暴露有關加密資料封包內容的資訊，並存在重放攻擊的風險。防止重放攻擊是因為，當網路重置時，新網路使用新的加密金鑰或確保 ASN 單調增加（第 4.6 節）。

保持準確的時間同步對網路運行至關重要。在正常的網路運行期間，必須避免接受來自不安全源的定時資訊，如第 4.5.2 節所述。在連接期間，節點可能在學習金鑰 K1 和 K2 之前易受定時攻擊的影響。 在網路運行期間，節點可以維護來自鄰居的時間更新的統計資訊並監視異常。

LLN 中媒體存取控制（MAC）層的拒絕服務（DoS）攻擊很容易通過射頻（RF）幹擾實現。 這是應該判斷更複雜的 DoS 攻擊的基本案例。 例如，發送假 EB 表示非常低的 Join Metric 可能會導致節點浪費時間和精力嘗試連接虛假網路，即使在監聽到合法的 EB 時也是如此。適當的連接安全性將阻止節點連接虛假假標誌，但到那時浪費的時間和精力。 但是，如果攻擊者只是在其監聽到的任何有效 EB 中間發送大量短資料封包，則攻擊者的能源成本會降低，並且加入節點的能源成本會更高。

由於通道條件的變化和無意或有意的幹擾，ACK 接收概率小於100%。 這將導致發送節點重新發送相同的資料封包，直到它被確認或達到重傳限制。 上層協定應考慮到這一點，可能使用序號來匹配重傳。

6TiSCH 層應該跟蹤異常事件並將其報告給更高級別的機構。 例如，如上所述，報告無法加入的網路的低加入度量標準的 EB 可能是攻擊的標誌。 另外，在正常網路操作中，具有有效迴圈冗餘校驗（CRC）的分組上的消息完整性檢查失敗將以每百萬分組一次的速率發生。與此速率的任何顯著偏差都可能是網路攻擊的跡象。 沿著相同的路線，ACK 或 EB 中與 MAC 層的時間感和其自身合理的時間誤差漂移率不一致的時間更新也可能是網路攻擊的結果。

9. IANA 注意事項

本檔不要求任何 IANA 行動。

10. 參考文獻

10.1. 規範性參考

[IEEE.802.15.4] IEEE, "IEEE Standard for Low-Rate Wireless Networks", IEEE 802.15.4, <http://ieeexplore.ieee.org/document/7460875/>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[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, September 2007, <http://www.rfc-editor.org/info/rfc4944>.

[RFC6206] Levis, P., Clausen, T., Hui, J., Gnawali, O., and J. Ko, "The Trickle Algorithm", RFC 6206, DOI 10.17487/RFC6206, March 2011, <http://www.rfc-editor.org/info/rfc6206>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <http://www.rfc-editor.org/info/rfc6282>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <http://www.rfc-editor.org/info/rfc6550>.

[RFC6551] Vasseur, JP., Ed., Kim, M., Ed., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", RFC 6551, DOI 10.17487/RFC6551, March 2012, <http://www.rfc-editor.org/info/rfc6551>.

[RFC6552] Thubert, P., Ed., "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6552, DOI 10.17487/RFC6552, March 2012, <http://www.rfc-editor.org/info/rfc6552>.

[RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, DOI 10.17487/RFC6553, March 2012,

<http://www.rfc-editor.org/info/rfc6553>.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, DOI 10.17487/RFC6554, March 2012, <http://www.rfc-editor.org/info/rfc6554>.

[RFC6719] Gnawali, O. and P. Levis, "The Minimum Rank with Hysteresis Objective Function", RFC 6719, DOI 10.17487/RFC6719, September 2012, <http://www.rfc-editor.org/info/rfc6719>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <http://www.rfc-editor.org/info/rfc6775>.

[RFC8025] Thubert, P., Ed. and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch", RFC 8025, DOI 10.17487/RFC8025, November 2016, <http://www.rfc-editor.org/info/rfc8025>.

[RFC8138] Thubert, P., Ed., Bormann, C., Toutain, L., and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header", RFC 8138, DOI 10.17487/RFC8138, April 2017, <http://www.rfc-editor.org/info/rfc8138>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <http://www.rfc-editor.org/info/rfc8174>.

10.2. 資訊參考

[openwsn] Watteyne, T., Vilajosana, X., Kerkez, B., Chraim, F., Weekly, K., Wang, Q., Glaser, S., and K. Pister, "OpenWSN: a standards-based low-power wireless development environment", Transactions on Emerging Telecommunications Technologies, Volume 23 Issue 5, pages 480-493, DOI 10.1002/ett.2558, August 2012.

[PROTO-6P] Wang, Q., Vilajosana, X., and T. Watteyne, "6top Protocol (6P)", Work in Progress, draft-ietf-6tisch-6top-protocol 05, May 2017.

[RFC7554] Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement", RFC 7554, DOI 10.17487/RFC7554, May 2015, <http://www.rfc-editor.org/info/rfc7554>.

[SEC-6TISCH] Vucinic, M., Simon, J., Pister, K., and M. Richardson, "Minimal Security Framework for 6TiSCH", Work in Progress, draft-ietf-6tisch-minimal-security-02, March 2017.

[SEC-JOIN-6TISCH] Richardson, M., "6tisch Secure Join protocol", Work in Progress, draft-ietf-6tisch-dtsecurity-secure-join-01, February 2017.

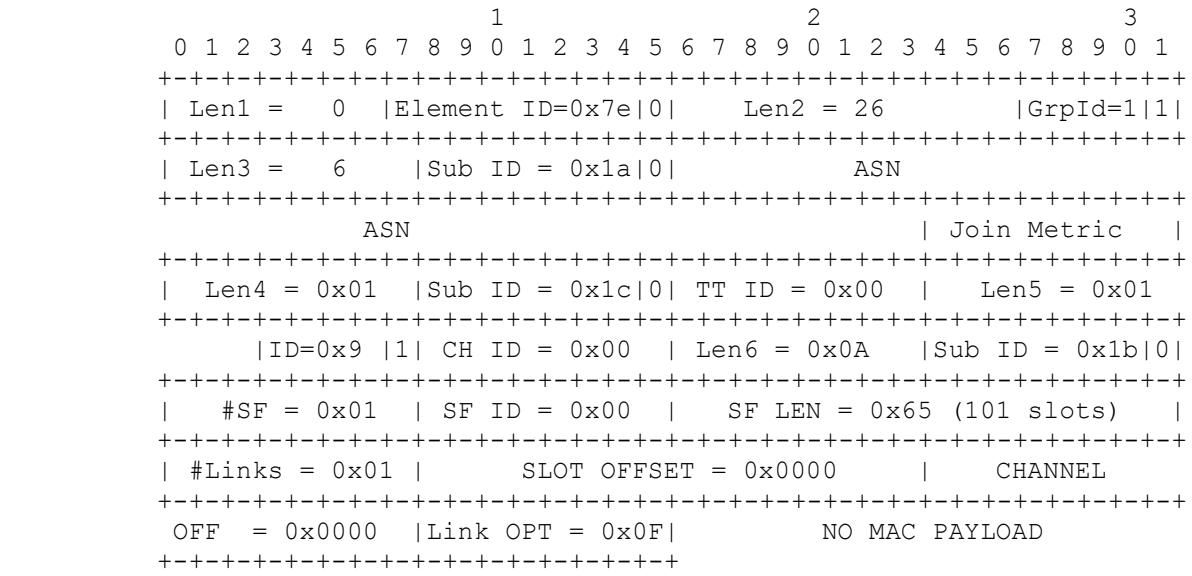
[TERMS-6TiSCH] Palattella, M., Thubert, P., Watteyne, T., and Q. Wang, "Terminology in IPv6 over the TSCH mode of IEEE 802.15.4e", Work in Progress, draft-ietf-6tisch terminology-08, December 2016

附錄 A.範例

本章節包含了幾個範例封包。每個封包包含了（1）適宜性的標頭圖（2）對應的字流節（3）形成封包的每一個 IE 的描述。封包格式特定用於[IEEE.802.15.4] 版本，可能與未來 IEEE 標準發佈的版本有所不同。如果本章節提供的封包內容與 IEEE 標準有不同之處，則應當以後者優先。

MAC 標頭欄位以特定順序描述。 本例中的所有欄位格式按從左到右的順序進行描述，其中最左邊的位元首先被發送。每個欄位內的位元從 0（最左和最不重要）到 k-1（最右和最重要）編號，其中欄位的長度是 k 位元。長度超過單個八位元組的欄位按從包含最低編號位元的八位元組到包含最高編號位元（小端）的八位元組的順序發送到 PHY。

A.1. 範例：具有默認時槽範本的 EB



位元組流:

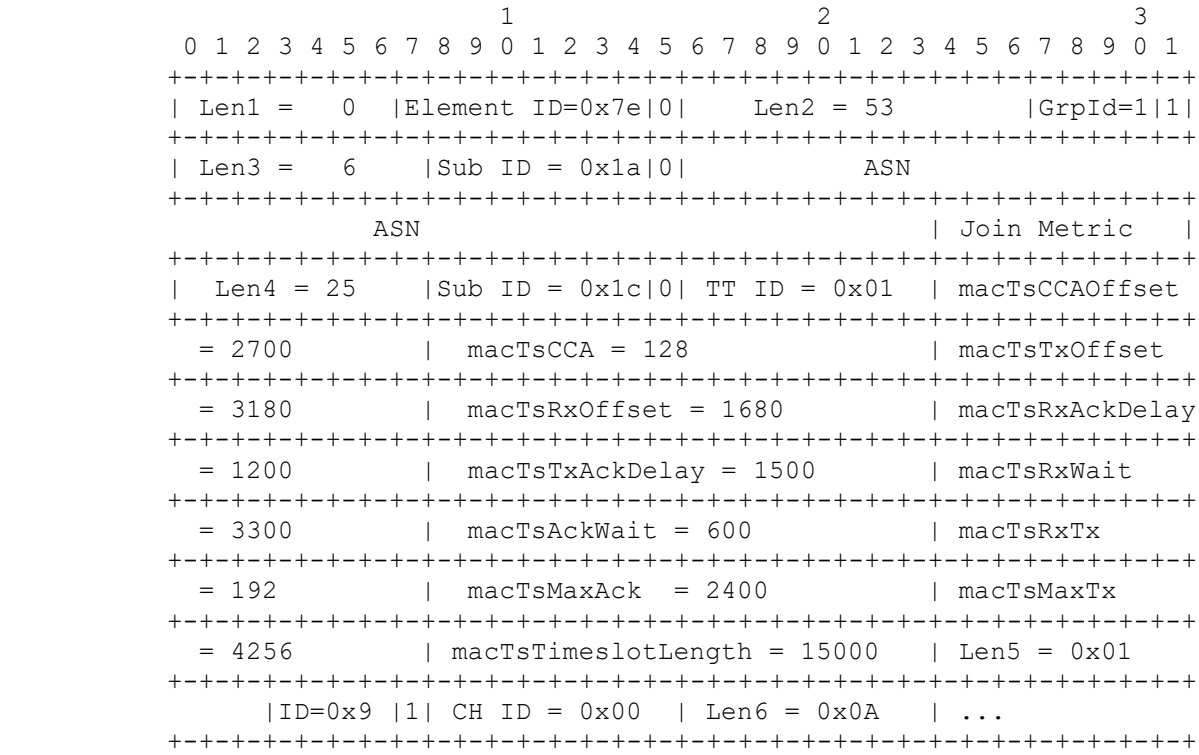
```
00 3F 1A 88 06 1A ASN#0 ASN#1 ASN#2 ASN#3 ASN#4 JP 01 1C 00
01 C8 00 0A 1B 01 00 65 00 01 00 00 00 00 0F
```

IEs 的描述:

```
#Header IE Header
    Len1 = Header IE Length (0)
    Element ID = 0x7e - termination IE indicating Payload IE
        coming next
    Type 0

#Payload IE Header (MLME)
    Len2 = Payload IE Len (26 bytes)
    Group ID = 1 MLME (Nested)
    Type = 1

#MLME-SubIE TSCH Synchronization
    Len3 = Length in bytes of the sub-IE payload (6 bytes)
    Sub-ID = 0x1a (MLME-SubIE TSCH Synchronization)
    Type = Short (0)
    ASN  = Absolute Sequence Number (5 bytes)
    Join Metric = 1 byte

#MLME-SubIE TSCH Timeslot
    Len4 = Length in bytes of the sub-IE payload (1 byte)
    Sub-ID = 0x1c (MLME-SubIE Timeslot)
    Type = Short (0)
    Timeslot template ID = 0x00 (default)

#MLME-SubIE Channel Hopping
    Len5 = Length in bytes of the sub-IE payload (1 byte)
    Sub-ID = 0x09 (MLME-SubIE Channel Hopping)
    Type = Long (1)
    Hopping Sequence ID = 0x00 (default)


#MLME-SubIE TSCH Slotframe and Link
    Len6 = Length in bytes of the sub-IE payload (10 bytes)
    Sub-ID = 0x1b (MLME-SubIE TSCH Slotframe and Link)
    Type = Short (0)
    Number of slotframes = 0x01
    Slotframe handle = 0x00
    Slotframe size = 101 slots (0x65)
    Number of Links (Cells) = 0x01
    Timeslot = 0x0000 (2B)
    Channel Offset = 0x0000 (2B)
    Link Options = 0x0F
    TX Link = 1, RX Link = 1, Shared Link = 1,
    Timekeeping = 1 )
```

A.2. 範例：具有自定義時槽範本的 EB

在 EB 中使用自訂時間段範本：將時間段長度設置為 15 毫秒。



位元組流:

```
00 3F 1A 88 06 1A ASN#0 ASN#1 ASN#2 ASN#3 ASN#4 JP 19 1C 01 8C 0A 80
00 6C 0C 90 06 B0 04 DC 05 E4 0C 58 02 C0 00 60 09 A0 10 98 3A 01 C8
00 0A ...
```

IEs 的描述:

```
 #Header IE Header
     Len1 = Header IE Length (none)
     Element ID = 0x7e - termination IE indicating Payload IE
         coming next
     Type 0

   #Payload IE Header (MLME)
       Len2 = Payload IE Len (53 bytes)
       Group ID = 1 MLME (Nested)
       Type = 1

   #MLME-SubIE TSCH Synchronization
       Len3 = Length in bytes of the sub-IE payload (6 bytes)
       Sub-ID = 0x1a (MLME-SubIE TSCH Synchronization)
       Type = Short (0)
       ASN  = Absolute Sequence Number (5 bytes)
       Join Metric = 1 byte

   #MLME-SubIE TSCH Timeslot
       Len4 = Length in bytes of the sub-IE payload (25 bytes)
       Sub-ID = 0x1c (MLME-SubIE Timeslot)
       Type = Short (0)
       Timeslot template ID = 0x01 (non-default)
```

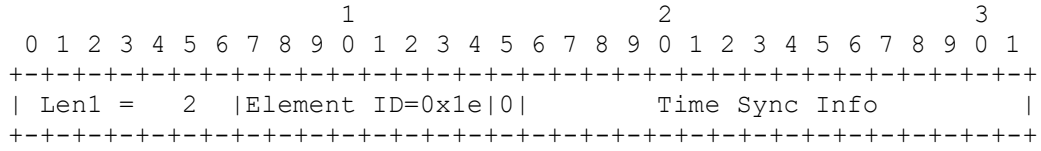
15 ms 時槽宣告：

```
+--------------------------------+------------+
| IEEE 802.15.4 TSCH parameter   | Value (us) |
+--------------------------------+------------+
| macTsCCAOffset                 |       2700 |
+--------------------------------+------------+
| macTsCCA                       |        128 |
+--------------------------------+------------+
| macTsTxOffset                  |       3180 |
+--------------------------------+------------+
| macTsRxOffset                  |       1680 |
+--------------------------------+------------+
| macTsRxAckDelay                |       1200 |
+--------------------------------+------------+
| macTsTxAckDelay                |       1500 |
+--------------------------------+------------+
| macTsRxWait                    |       3300 |
+--------------------------------+------------+
| macTsAckWait                   |        600 |
+--------------------------------+------------+
| macTsRxTx                      |        192 |
+--------------------------------+------------+
| macTsMaxAck                    |       2400 |
+--------------------------------+------------+
| macTsMaxTx                     |       4256 |
+--------------------------------+------------+
| macTsTimeslotLength            |      15000 |
+--------------------------------+------------+
```

```
#MLME-SubIE Channel Hopping
    Len5 = Length in bytes of the sub-IE payload. (1 byte)
    Sub-ID = 0x09 (MLME-SubIE Channel Hopping)
    Type = Long (1)
    Hopping Sequence ID = 0x00 (default)
```

A.3. 範例：鏈路層確認

增強型確認資料封包攜帶時間校正 IE（標頭 IE）。



位元組流

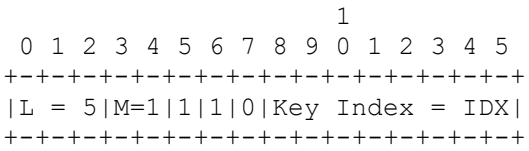
```
02 0F TS#0 TS#1
```

IEs 的描述:

```
#Header IE Header
    Len1 = Header IE Length (2 bytes)
    Element ID = 0x1e - ACK/NACK Time Correction IE
    Type 0
```

A.4. 範例：輔助安全標頭

802.15.4 輔助安全標頭，其安全級別設置為 ENC-MIC-32。



位元組流

```
    6D IDX#0
Security Auxiliary Header fields in the example:

    #Security Control (1 byte)
        L = Security Level ENC-MIC-32 (5)
        M = Key Identifier Mode (0x01)

    Frame Counter Suppression = 1 (omitting Frame Counter field)
    ASN in Nonce = 1 (construct Nonce from 5 byte ASN)
    Reserved = 0

#Key Identifier (1 byte)
    Key Index = IDX (deployment-specific KeyIndex parameter that
                identifies the cryptographic key)
```

致謝

作者感謝 Rene Struik，Pat Kinney，Michael Richardson，Tero Kivinen，Nicola Accettura，Malisa Vucinic 和 Jonathan Simon 的指導和意見。感謝 Charles Perkins，Brian E. Carpenter，Ralph Droms，Warren Kumari，Mirja Kuehlewind，Ben Campbell，Benoit Claise 和 Suresh Krishnan 所作的詳盡詳盡的評論。 感謝 Simon Duquennoy，Guillaume Gaillard，Tengfei Chang 和 Jonathan Munoz 對範例部分的詳細介紹。 感謝 6TiSCH 聯合主席 Pascal Thubert 的指導和建議。

作者資訊

Xavier Vilajosana (editor)
Universitat Oberta de Catalunya
156 Rambla Poblenou
Barcelona, Catalonia 08018
Spain

Email: xvilajosana@uoc.edu

Kris Pister
University of California Berkeley
512 Cory Hall
Berkeley, California 94720
United States of America

Email: pister@eecs.berkeley.edu

Thomas Watteyne
Analog Devices
32990 Alvarado-Niles Road, Suite 910
Union City, CA 94587
United States of America

Email: twatteyne@linear.com