華亨科技 **ZigBee** 無線定位開發系統

IEEE 802.15.4 標準和 ZigBee 協定規範

首字母縮略詞及定義

ACL	Access Control List	存取控制列表
AES	Advanced Encryption Standard	高級加密標準
AF	Application Framework	應用框架
AIB	APS Information Base	APS 訊息庫
APDU	APS sub-layer PDU	應用支援子層協定資料單元
API	Application Programming Interface	應用編程介面
APL	Application Layer	應用層
APS	Application Support Sub-Layer	應用支援子層
APSDE	APS Data Entity	APS 資料實體
APSDE-SAP	APS Data Entity - Service Access Point	APS 資料實體-服務存取點
APSME	APS Management Entity	APS 管理實體
APSME-SAP	APS Management Entity - Service Access Point	APS 管理實體-服務存取點
ASDU	APS Service Datagram Unit	APS 服務資料單元
BE	Backoff Exponent	回退指數
BI	Beacon Interval	信標間隔
BO	Beacon Order	信標階數
BPSK	Binary Phase Shift Keying	二進位相移鍵控
BSN	Beacon Sequence Number	信標序號
BTR	Broadcast Transaction Record	廣播事務記錄
BTT	Broadcast Transaction Table	廣播事務表
CAP	Contention Access Period	競爭存取週期
CBC	Cipher Block Chaining	密碼防護鏈
CBC-MAC	Cipher Block Chaining Message Authentication Code	密碼防護鏈訊息驗證程式
CCA	Clear Channel Assessment	空閒通道評估
CCM	Encryption using CTR with CBC-MAC	計數器模式和密碼防護鏈訊息驗證程式
CD	Carrier Detect	載波檢測
CFP	Contention-Free Period	無競爭週期
CID	Cluster Identifier	簇標識
CLH	Cluster Head	簇頭
Coordinator	A full function device that accepts associations and transmits beacons	一個接受關聯並傳輸信標的全功能設備
CRC	Cyclic Redundancy Check	迴圈冗餘校驗
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance	避免衝突的載波偵聽多路存取
CW	Contention Window	競爭視窗（長度）

DSN	Data Sequence Number	資料序號
DSSS	Direct Sequence Spread Spectrum	直接序列擴頻
ED	Energy Detection	能量檢測
FCF	Frame Control Field	訊框(Frame)控制域
FCS	Frame Check Squence	訊框(Frame)校驗序列
FFD	Full Function Device	全功能設備
FH	Frequency Hopping	跳頻
FHSS	Frenquency Hopping Spread Spectrum	跳頻擴充頻譜
FIFO	First In First Out	先進先出
FLI	Frame Length Indicator	訊框(Frame)長度指示器
GTS	Guaranteed Time Slot	確保時隙
HCL	Home Control Lighting	家庭控制照明
IEEE	Institute of Electrical and Electronics Engineers	電氣和電子工程學會
IF	Intermediate Frequency	中頻
IFS	InterFrame Spacing	訊框(Frame)間隔
IB	Information Base	訊息庫
ISM	Industrial，Scientific and Medical	工業、科學和醫學
KVP	Key-Value Pair	鍵值對
LIFS	Long Interframe Spacing	長訊框(Frame)間隔
LLC	Logical Link Control	邏輯鏈路控制
LPDU	LLC Protocol Data Unit	LLC 協定資料單元
LQ	Link Quality	鏈路品質
LQI	Link Quality Indication	鏈路品質指示
LR-WPAN	Low-Rate Wireless Personal Area Network	低速無線個域網
LSB	Least Significant Bit/Byte	最低有效位元/位元組
MAC	Medium Access Control	媒體存取控制
MCPS	MAC Common Part Sublayer	MAC 公共部分子層
MCPS-SAP	MAC Common Part Sublayer - Service Access Point	MAC 公共部分子層-服務存取點
MFR	MAC Footer	MAC 訊框(Frame)尾
MHR	MAC Header	MAC 訊框(Frame)頭
MIC	Message integrity code	訊息完整性檢測碼
MLME	MAC Sublayer Management Entity(management interface)	MAC 子層管理實體（管理介面）
MLME-SAP	MAC Sublayer Management Entity - Service Access Point	MAC 子層管理實體-服務存取點
MPDU	MAC Protocol Data Unit	MAC 協定資料單元
MSG	Message Service Type	訊息服務類型
MSB	Most Significant Bit/Byte	最高有效位元/位元組
MSDU	MAC Service Data Unit	MAC 服務資料單元
NB	Number of Backoff(periods)	退避（週期）數
NBDT	Network Broadcast Delivery Time	網路廣播發送時間
NHLE	Next Higher Layer Entity	下一個更高層實體

NIB	Network layer Information Base	網路層資訊庫
NLDE	Network Layer Data Entity	網路層資料實體
NLDE-SAP	Network Layer Data Entity - Service Access Point	網路層資料實體-服務存取點
NLME	Network Layer Management Entity	網路層管理實體
NLME-SAP	Network Layer Management Entity - Service Access Point	網路層管理實體-服務存取點
NPDU	Network Layer Protocol Data Unit	網路層協定資料單元
NSDU	Network Layer Service Data Unit	網路層服務資料單元
NWK	Network	網路
OFB	Output Feedback(encryption)	輸出回饋（加密）
O-QPSK	Offset-Quadrature Phase Shift Keying	偏移正交相移鍵控
OSI	Open Systems Interconnection	開放系統互連
PAN	Personal Area Network	個域網
PD-SAP	PHY layer Data - Service Access Point	物理層資料-服務存取點
PDU	Protocol Data Unit	協定資料單元
PER	Packet Error Rate	包差錯率/誤訊框(Frame)率
PAN Coordinator	A coordinator that is the principal coordinator of a PAN	一個協調器，它是一個 PAN 的主要協調器
PHY	Physical layer	物理層
PIB	PAN Information Base	PAN 訊息庫
PLME	Physical layer Management Entity	物理層管理實體
PLME-SAP	Physical layer Management Entity - Service Access Point	物理層管理實體-服務存取點
POS	Personal Operating Space	個人工作空間
PPDU	PHY Protocol Data Unit	物理層協定資料單元
PSDU	PHY Service Data Unit	物理層服務資料單元
PSK	Phase Shift Keying	相位鍵控
PTI	Packet Trace Interface	包跟蹤介面
QoS	Quality of Service	服務品質
RF	Radio Frequency	無線射頻
RFD	Reduced Function Device	簡化功能設備
RN	Routing Node	路由節點
RREP	Route Reply	路由應答
RREQ	Route Request	路由請求
RSSI	Received Signal Strength Indicator	接收信號強度指示
SAP	Service Access Point	服務存取點
SD	Superframe Duration	超訊框(Frame)週期
SDU	Service Data Unit	服務資料單元
SFD	Start of Frame Delimiter	訊框(Frame)開始定界符
SHR	Synchronization Header	同步頭
SFS	Short InterFrame Spacing	短訊框(Frame)間隔
SKG	Secret Key Generation	密鑰產生
SKKE	Symmetrck-Key Key Establishment	對稱密鑰建立

SO	Superframe Order	超訊框(Frame)階數
SPDU	SSCS Protocol Data Unit	SSCS 協定資料單元
SSCS	Service Specific Convergence Sublayer	特定服務彙聚子層
SSS	Security Services Specification	安全服務規範
WLAN	Wireless Local Area Network	無線局域網
WPAN	Wireless Personal Area Network	無線個域網
ZDO	ZigBee Device Object	ZigBee 設備物件

目 錄

第一部分 IEEE 802.15.4 標準

1. 概述

ZigBee協定堆疊的物理、MAC層即是IEEE 802.15.4協定。爲此，本文件對其物理層和MAC層進行了細緻描述。物理層規範，主要從物理層的服務規範、資料格式、常量和屬性、物理層技術和通用射頻規範等方面進行了介紹。MAC層規範，主要從MAC層的服務規範、訊框(Frame)格式、命令訊框(Frame)、功能描述、安全規範和MAC — PHY資訊交互流程等方面進行了介紹。

2. 物理層規範

2.1 物理層概述

IEEE 802.15.4物理層主要完成以下幾項任務：開啓和關閉無線收發信機、能量檢測（ED）、鏈路品質指示（LQI）、空閒通道評估（CCA）、通道選擇、資料發送和接收。

IEEE 802.15.4物理層定義了868MHz、915MHz和2.4GHz三個頻段。這些頻段上所採用的調製和擴充技術參數可歸納爲表1。

表1 IEEE 802.15.4的頻寬和資料速度

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

IEEE 802.15.4物理層在三個頻段上共劃分了27個通道，通道編號k爲0～26。2450MHz頻段上劃分了16個通道，915MHz頻段有10個通道，868MHz頻段只有1個通道。27個通道的中心頻率和對應的通道編號定義如下：

f_c=868.3MHz　　k=0

f_c=[906+2(k-1)]MHz　　k=1,2,…，10

f_c=[2405+5(k-11)]MHz　　k=11,12,…，26

2.2 物理層服務規範

物理層透過射頻硬體和硬體提供MAC層與物理無線通道之間的介面。從概念上說，物理層還應包括物理層管理實體（PLME），以提供調用物理層管理功能的管理服務介面；同時PLME還負責維護物理層PAN資訊庫（PHY PIB）。IEEE 802.15.4物理層的參考模型如圖1所示。物理層透過物理層資料服務存取點（PD-SAP）提供物理層資料服務；透過物理層管理實體服務存取點（PLME-SAP）提供物理層管理服務。

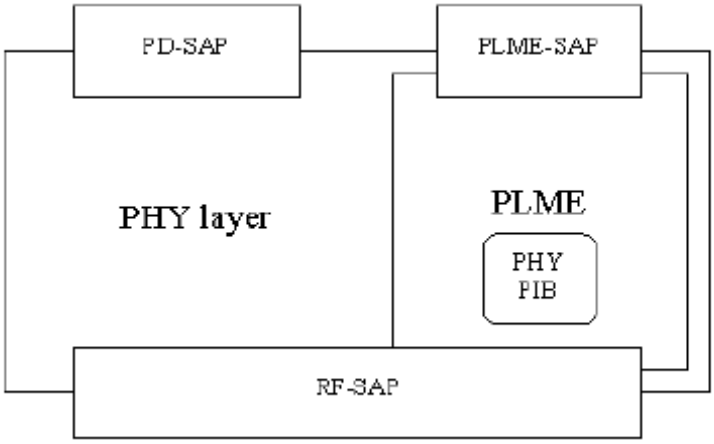


圖1 物理層參考模型

2.2.1 物理層資料服務

PD-SAP支援在兩個對等的MAC層實體之間傳輸MAC協定資料單元（MPDU）。PD-SAP支持的原語有三種：PD-DATA.request、PD-DATA.confirm和PD-DATA.indication。

PD-DATA.request原語由MAC層發送給本地物理層，請求發送MPDU（即物理層服務資料單元PSDU）。它的語法如下：

PD-DATA.request （psduLength，psdu）

其中：參數psdu是MAC層請求物理層發送的實際資料；參數psduLength是一個無符號整數，表示psdu的長度，單位是位元組。物理層收到PD-DATA.request原語時，如果設備處於發射致能狀態（TX_ON），則物理層先把請求原語提供的PSDU封裝成物理層協定資料單元（PPDU），然後開始發送。資料發送成功後，物理層就向MAC發出狀態爲SUCCESS的證實原語PD-DATA.confirm。如果設備處於接收致能狀態（RX_ON）或者處於收發都關閉狀態（TRX_OFF），則物理層向MAC層發送狀態爲RX_ON或TRX_OFF的PD-DATA.confirm原語。

PD-DATA.confirm原語由物理層實體發送給MAC層實體，作爲對PD-DATA.request原語的回應。證實原語的語法如下：

PD-DATA.confirm（status）

其唯一參數status表示MAC層請求發送資料的結果，它是取值爲SUCCESS、RX_ON或TRX_OFF的枚舉型變數。MAC子層實體從收到的PD-DATA.confirm原語中獲知此前資料發

送請求的結果。如果資料發送請求成功，則狀態參數status的值爲SUCCESS；如果資料發送請求失敗，則狀態參數指示資料發送失敗的原因（RX_ON或TRX_OFF）。

PD-DATA.indication原語指示一個MPDU（也即PSDU）從物理層傳送到本地MAC層實體。其語法如下：

PD-DATA.indication（psduLength，psdu，ppduLinkQuality）

其中參數ppduLinkQuality表示根據接收PPDU測得的鏈路品質（LQ），其取值爲整數0x00～0xFF。PD-DATA.indication原語由物理層產生併發送給MAC層以提交接收到的PSDU。如果接收到的psduLength欄位爲0或大於內部常數aMaxPHYPacketSize，則物理層不產生服務原語。

2.2.2 物理層管理服務

PLME-SAP允許在MLME和PLME之間傳送管理命令。PLME-SAP支持的原語有PLME-CCA、PLME-ED、PLME-GET、PLME-SET-TRX-STATE和PLME-SET。

1. PLME-CCA.request原語請求PLME執行空閒通道評估（CCA）。這是一個無參數的請求原語，其語法如下：

PLME-CCA.request（）

每當MAC層的CSMA-CA演算法要求進行物理通道評估時，MLME就產生PLME-CCA.request原語併發送給PLME。收到PLME-CCA.request請求原語時，如果設備處於接收致能狀態，PLME就指示物理層進行通道評估。物理層完成CCA後，PLME就向MLME發送PLME-CCA.confirm原語，根據CCA結果提供通道狀態資訊繁忙（BUSY）或空閒（IDLE）。如果PLME收到PLME-CCA.request原語時，設備處於收發關閉狀態（TRX_OFF）或處於發送致能狀態（TX_ON），則無法進行通道評估。此時PLME向MLME發送PLME-CCA.confirm原語的狀態參數將指示CCA失敗的原因（TRX_OFF或TX_ON）。PLME-CCA.confirm原語的語法如下：

PLME-CCA.confirm（status）

它是PLME向MLME報告CCA結果的證實原語。status參數的取值爲TRX_OFF、TX_ON、BUSY或IDLE。

2. PLME-ED.request原語由MLME產生，請求PLME執行能量檢測（ED）。這也是一個無參數的請求原語，其語法如下：

PLME-ED.request （）

收到PLME-ED.request原語時，如果設備處於接收致能狀態，PLME就指示物理層執行ED。完成ED後，PLME向MLME發送PLME-ED.confirm原語，報告能量檢測成功（SUCCESS）和測得的通道能量等級。PLME-ED.confirm的語法如下：

PLME-ED.confirm （status，EnergyLevel）

其中參數EnergyLevel表示測得的當前通道能量等級，其取值範圍爲整數0x00～0xFF。PLME收到PLME-ED.request原語時，如果設備處於收發關閉狀態（TRX_OFF）或發送致能狀態（TX_ON），則無法進行能量檢測。此時PLME向MLME發送的PLME-ED.confirm原語狀態

參數將指示能量檢測失敗的原因（TRX_OFF或TX_ON）。

3. PLME-GET.request原語由MLME產生，向PLME請求物理層PIB中相關屬性的值。

其語法如下：

PLME-GET.request （PIBAttribute）

參數PIBAttibute是PIB屬性的標識。收到PLME-GET.request原語後，PLME就到資料庫中檢索該屬性。如果資料庫中找不到請求的PIB屬性標識，則PLME向MLME發送PLME-GET.confirm原語，狀態爲“不支援的屬性”（UNSUPPORT_ATTRIBUTE）。如果從資料庫中找到了PLME-GET.request請求的屬性，則PLME-GET.confirm原語中的狀態參數值爲SUCCESS，並返回屬性值。PLME-GET.confirm原語的語法如下：

PLME-GET.confirm （Status，PIBAttribute，PIBAttributeValue）

其中參數PIBAttributeValue攜帶的是PIB屬性的值。

4. PLME-SET-TRX-STATE.request原語由MLME產生，向PLME請求改變收發信機的內部工作狀態。其語法如下：

PLME-SET-TRX-STATE.request （state）

其唯一參數state的取值爲RX_ON、TRX_OFF、FORCE_TRX_OFF或TX_ON。PLME-SET-TRX-STATE.confirm原語由PLME產生，向MLME報告PLME-SET-TRX-STATE.request請求的結果，其語法如下：

PLME-SET-TRX-STATE.confirm （status）

其唯一參數status的取值爲SUCCESS、RX_ON、TRX_OFF、TX_ON、BUSY_RX或BUSY_TX。收到PLME-SET-TRX-STATE.request原語後，PLME指令物理層改變到請求的工作狀態。如改變收發信機工作狀態的請求被接受，則PLME-SET-TRX-STATE.confirm的狀態爲SUCCESS。如果設備當前的收發狀態就是請求原語請求的工作狀態，則證實原語參數status的值爲收發信機當前狀態（RX_ON、TRX_OFF或TX_ON）。如果請求原語請求改變到狀態RX_ON或TRX_OFF，而此時物理層正在發送一個PPDU，則證實原語的status參數值爲BUSY_TX，並在發送結束後改變到請求的收發信機工作狀態。如果請求原語請求改變到狀態TX_ON或TRX_OFF，而此時設備處於RX_ON狀態並且已經接收到有效的訊框(Frame)開始符（FSD），則證實原語的status參數值爲BUSY_RX，並在接收資料結束後改變到請求的收發信機工作狀態。如果PLME-SET-TRX-STATE.request原語的狀態爲FORCE_TRX_OFF，則不管物理層當前處於什麼狀態，收發信機將被強制改變到TRX_OFF（收發都關閉）狀態。

5. PLME-SET.request原語由MLME產生，向PLME請求設置或改變PIB屬性的值。其語法如下：

PLME-SET.request （PIBAttribute，PIBAttributeValue）

對應的PLME-SET.confirm原語由PLME產生，向MLME報告請求設置PIB屬性值的結果。其語法如下：

PLME-SET.confirm（status，PIBAttribute）

其中參數status的取值爲SUCCESS、UNSUPPORTED_ATTRIBUTE或INVALID_PARAMETER。如果在資料庫中找不到PLME-SET.request請求原語中的PIB屬性，則PLME-SET.confirm原語中的狀態值爲UNSUPPORTED_ATTRIBUTE。如果

PLME-SET.request原語中要設置的PIB屬性值超出有效範圍，則PLME-SET.confirm原語中的狀態值爲INVALID_PARAMETER。如果成功設置了PIB屬性值，則PLME-SET.confirm原語中的狀態值爲SUCCESS。

2.3 物理層資料格式

物理層協定資料單元（PPDU）由三部分構成：同步頭（SHR）允許接收設備同步並鎖定位元流；物理層訊框(Frame)頭（PHR）包含的是訊框(Frame)長資訊；有效載荷部分是PSDU。PPDU的格式如下：

<table>
<tr><td>位元組數：4</td><td>1</td><td colspan="2">1</td><td>可變長度</td></tr>
<tr><td>引導序列</td><td>訊框(Frame)開始符</td><td>訊框(Frame)長（7位）</td><td>預留（1位）</td><td>物理層服務資料單元（PSDU）</td></tr>
<tr><td colspan="2">同步頭（SHR）</td><td colspan="2">物理層訊框(Frame)頭（PHR）</td><td>物理層有效載荷</td></tr>
</table>

引導序列欄位：收發信機用來獲得碼片和符號同步，它是32位長度的全0序列。

訊框(Frame)開始符（SFD）欄位：表示引導序列的結束和資料訊框(Frame)的開始，它是8位元的二進位序列11100101。

訊框(Frame)長欄位：它用7位元表示物理層有效載荷PSDU的長度，取值範圍是0到aMaxPHYPacketSize之間的整數。

PSDU欄位：可變長度的欄位，它是物理層要發送的資料包，即MPDU。

2.4 物理層的常量和屬性

物理層常量是依賴硬體的，並且在設備工作期間是不能更改的，它表徵了物理層的某些特徵。IEEE 802.15.4的兩個物理層常量如表2所列。

表2 物理層常量

常　量	描　述	取　值
aMaxPHYPacketSize	物理層所能接收的PSDU的最大長度（用位元組數表示）	127
aTurnaroundTime	RX-to-TX或TX-to-RX的最大切換時間	12個符號週期

物理層的屬性是儲存在物理層PIB中的，用於設備物理層的管理，可以用PLME-GET和PLME-SET原語對其進行讀寫操作。PIB中包含的物理層屬性如表3所列。

表3 物理層PIB屬性

屬性	標識碼	類型	取值範圍	描述
PhyCurrentChannel	0x00	整數	0～26	收發信使用的射頻通道
phyChannelSupported	0x01	點陣圖	0x00000000 ～0x07FFFFF	32位中的5個高有效位（b_{27}，…，b_{31}）預留，設爲0；27個低有效位（b_0，…，b_{26}）分別表示27個有效通道的狀態（b_k=1，通道k可用；b_k=0，通道k不可用）
PhyTransmitPower	0x02	點陣圖	0x00～0xBF	高2位表示發射功率誤差的容忍度：00=±1dB；01=±3dB；10=±6dB。低6位元是帶符號整數，表示發射功率標稱值（dBm）
PhyCCAMode	0x03	整數	1~3	表示CCA的3種模式

2.5 2.4GHz 頻段的物理層技術

IEEE 802.15.4標準2.4GHz頻段物理層支援250kbps的資料速率，採用十六進位准正交調製技術。在每個符號週期內，4個資訊位元映射爲一個32位的准正交僞隨機序列，所以其符號速率爲62.5ksymbol/s，碼片速率爲2000kchip/s。所有符號的僞隨機序列級聯後得到的碼片序列再用O-QPSK調製到載波上，其調製原理如圖2所示。

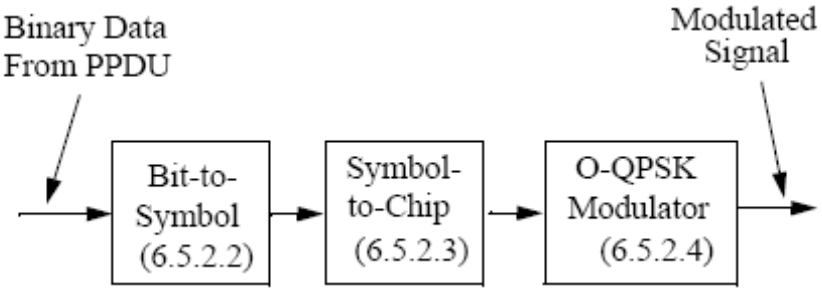


圖2 2.4GHz物理層調製方案

從PPDU引導序列的第一個位元組開始，每個位元組的低4位元（b_0，b_1，b_2，b_3）和高4位（b_4，b_5，b_6，b_7）分別映射爲一個符號，低位元在前高位在後。每個符號再映射爲一個32位長度的PN序列。IEEE 802.15.4標準2.4GHz頻段調製的映射關係如表4所列。

表4 Bit-Symbol-Chip映射

二進位序列	十進位符號	碼片序列（c_0，c_1，…，c_{30}，c_{31}）
0 0 0 0	0	1 1 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1 0 0 0	1	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
0 1 0 0	2	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
1 1 0 0	3	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
0 0 1 0	4	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
1 0 1 0	5	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0

0 1 1 0	6	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
1 1 1 0	7	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
0 0 0 1	8	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
1 0 0 1	9	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1
0 1 0 1	10	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1
1 1 0 1	11	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
0 0 1 1	12	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
1 0 1 1	13	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
0 1 1 1	14	1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
1 1 1 1	15	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

碼片序列採用半正弦脈衝成形的O-QPSK載波調製，偶數位元的碼片調製到同相載波I上，奇數位元的碼片調製到正交載波Q上，正交碼片序列延遲一個碼片週期T_c，形成了圖3所示的偏移關係。

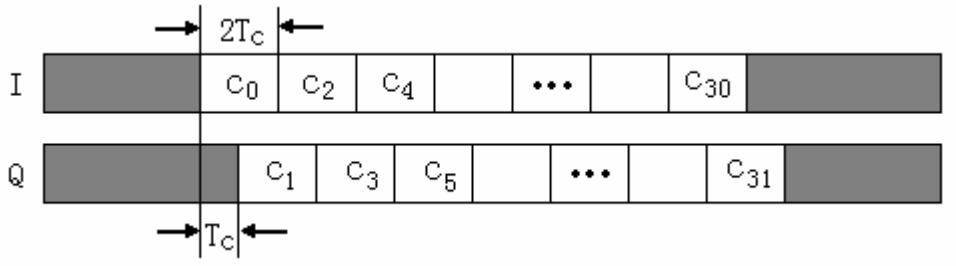


圖3 O-QPSK偏移關係

以半正弦脈衝p（t）表示基帶碼片，則O-QPSK的基帶碼片序列如圖4所示。

$$p(t)=\begin{cases}\sin(\pi\dfrac{t}{2T_c}) & 0\le t\le 2T_c\\ 0 & \text{其他}\end{cases}$$

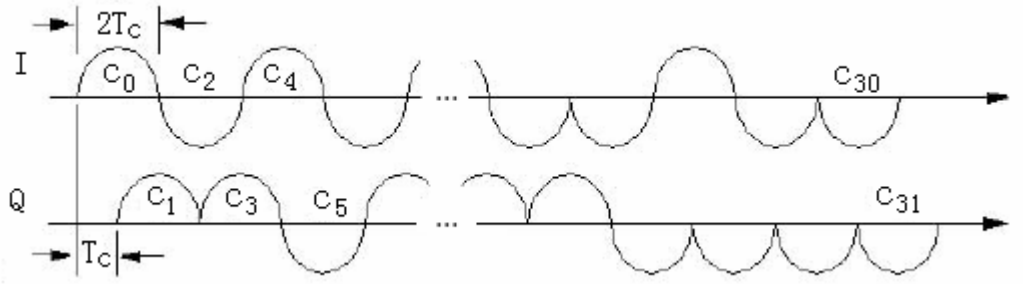


圖4 半正弦脈衝成形的O-QPSK

2.6 868/915MHz 頻段的物理層技術

IEEE 802.15.4標準868MHz頻段物理層支援20kbps的資料速率，915MHz頻段支援40kbps資料數率。868/915MHz物理層採用圖5所示的直接序列擴頻（DSSS）結合差分編碼和BPSK調製的傳輸方案。

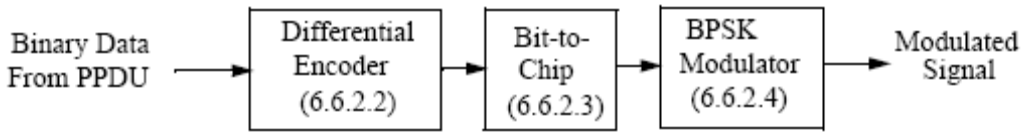


圖5 868/915MHz物理層調製方案

從PPDU引導序列的第一個位元組開始，低有效位元在前，高有效位在後，逐位元進行差分編碼；差分編碼得到的每一個位映射爲一個15位長度的PN序列，然後對每個碼片用BPSK調製。所以868/915MHz物理層的碼片序列分別是300kchip/s和600kchip/s。

位元差分編碼透過模2加法實現：如果R_n表示差分編碼器輸入，E_n表示差分編碼的輸出，E_{n-1}表示前一時刻的差分編碼，則有$E_n=R_n \oplus E_{n-1}$。類似的，差分解碼的模2加法實現爲$R_n=E_n \oplus E_{n-1}$。透過DSSS，差分編碼輸出0映射爲序列（111101011001000），1映射爲序列（000010100110111）。碼片序列用BPSK調製到載波上，成形脈衝爲升余弦p(t)：

$$p(t)=\frac{\sin(\pi t/T_c)}{\pi t/T_c}\frac{\cos(\pi t/T_c)}{1-(4t^2/T_c^2)}$$

2.7 通用射頻規範

IEEE 802.15.4物理層通用規範同時適用於2.4GHz和868/915MHz物理層，包括能量檢測（ED）、鏈路品質指示（LQI）、空閒通道評估（CCA）等。

接收機能量檢測是在8個符號週期內對IEEE 802.15.4通道帶寬內的接收信號功率進行估計，用於網路層的通道選擇演算法。ED結果的取值範圍是0x00～0xFF，透過PLME-ED.comfirm原語報告給MLME。ED結果的最小值“0”表示接收功率不超過接收靈敏度10dB，要求ED指示的功率至少達40dB，所以ED結果和接收功率的映射精度可達6dB。

LQI用於指示接收資料包的品質，它透過接收機ED、信噪比估計來測量，或者由這些方法聯合實現。物理層對每個接收資料包都執行LQI，並透過PD-DATA.indication原語連同資料訊框(Frame)一起報告給MAC層，以用於網路層或應用層。LQI結果取值爲0x00～0xFF，最小值0x00和最大值0xFF分別表示接收機可檢測信號的最差品質和最好品質。

IEEE 802.15.4物理層至少要支援下面3種CCA模式之一：

- CCA模式1—能量門限檢測。如果檢測到的信號能量超過設定的ED門限，則表示通道忙（被佔用）。

- CCA模式2—載波偵聽。如果檢測到符合IEEE 802.15.4調製和擴頻特徵的信號，則表示通道忙，信號的強度可能高於或低於ED門限。
- CCA模式3—載波偵聽聯合能量檢測。如果檢測到的符合IEEE 802.15.4調製和擴頻特徵的信號強度超過ED門限，則表示通道忙。

一個設備所採用的CCA模式由物理層PIB屬性phyCCAMode決定，標準規定CCA中ED門限不得超過接收靈敏度10dB，CCA檢測時間爲8個符號週期。

3. MAC 層規範

IEEE 802.15.4標準MAC子層主要負責以下幾項任務：協調器產生網路信標；信標同步；支持PAN關聯和解關聯；CSMA-CA通道存取機制；處理和維護保證時隙（GTS）機制；在兩個對等MAC實體間提供可靠鏈路。

3.1 MAC 層服務規範

MAC提供了特定服務會聚子層（SSCS）和物理層之間的介面。從概念上說，MAC層還包括MAC層管理實體（MLME），以提供調用MAC層管理功能的管理服務介面；同時，MLME還負責維護MAC PAN資訊庫（MAC PIB）。MAC層的參考模型如圖6所示。MAC層透過MAC公共部分子層（MCPS）的資料SAP（MCPS-SAP）提供MAC管理服務。這兩種服務透過物理層PD-SAP和PLME-SAP提供了SSCS和PHY之間的介面。除了這些外部介面外，MCPS和MLME之間還隱含了一個內部介面，用於MLME調用MAC資料服務。

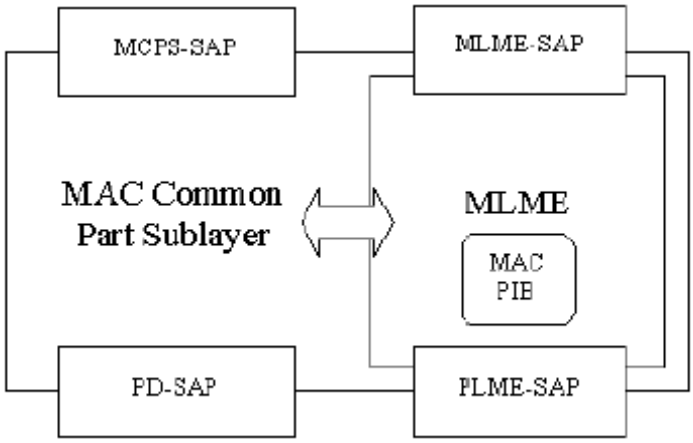


圖6 MAC層參考模型

3.1.1 MAC 層資料服務

MCPS-SAP支援兩個對等的SSCS實體之間SSCS協定資料單元（SPDU）的傳輸。MAC資料服務是透過兩類服務原語MCPS-DATA和MCPS-PURGE實現的。其中MCPS-PURGE原

語在簡化功能設備（RFD）中是可選的，不必強制支持。

MCPS-DATA.request原語請求從本地SSCS實體向一個對等的SSCS實體發送SPDU（即MAC服務資料單元MSDU）。當SSCS層有資料需要發送時，就產生該原語並透過MCPS-SAP傳遞給MAC層。MCPS-DATA.request的語法如下：

MCPS-DATA.request（SrcAddrMode，SrcPANId，SrcAddr，DstAddrMode，DstPANId，DstAddr，msduLength，msdu，msduHandle，TxOptions）

MCPS-DATA.request的參數定義如表5所列。

表5 MCPS-DATA.request的參數

參數	類型	有效範圍	描述
SrcAddrMode	整數	0x00～0x03	原語及其MPDU的源位址模式：0x00表示無位址，位址欄位省略；0x01預留；0x02表示16位短位址；0x03表示64位擴充位址
SrcPANId	整數	0x0000～0xFFFF	發送MSDU的源設備PAN標識碼
SrcAddr	設備位址	由SrcAddrMode參數決定	來源位址
DstAddr	設備位址	由DstAddrMode參數決定	目的位址
DstAddrMode	整數	0x00～0x03	原語及其MPDU的目的位址模式：0x00表示無位址，位址欄位省略；0x01預留；0x02表示16位短位址；0x03表示64位元擴充位址
DstPANId	整數	0x0000～0xFFFF	接收MSDU的目的設備PAN標識碼
msduLength	整數	<=aMaxMACFrameSize	MSDU的長度（用位元組數表示）
msdu			請求發送的MSDU內容
msduHandle	整數	0x00～0xFF	MSDU控制碼
TxOptions	點陣圖	0000XXXX（X爲0或1）	發送MSDU的選項，它是下面四項中若干項的位相“或”：0x01（要求確認的發送）、0x02（GTS發送）、0x03（間接發送）、0x04（使用安全機制發送）

MCPS-DATA.confirm原語是對MCPS-DATA.request的回應，由MAC層產生向SSCS報告請求發送MSDU的結構。它的語法如下：

MCPS-DATA.confirm（msduHandle，status）

其中：參數msduHandle是待證實的MSDU的控制碼；status指示資料發送請求的結果。

如果MCPS-DATA.request的參數TxOptions指示採用GTS發送，則MAC層將檢測是否存在有效的GTS。如果發送設備是PAN協調器，則它需要檢測是否爲目的設備指定了接收GTS。如果找不到有效的GTS，則MAC層向SSCS發送狀態爲INVALID_GTS的MCPS-DATA.confirm原語。如果找到有效GTS，則MAC等待GTS的到來，以無競爭的方式接入通道發送MPDU。如果TxOptions參數沒有指定GTS傳輸，則MAC層在競爭存取週期

（CAP）以CSMA-CA機制發送資料。TxOptions中GTS發送選項遮罩間接發送選項。

如果TxOptions參數中指示間接發送，並且收到請求原語的是協調器的MAC層，則原語中的資訊將被存入待處理事務列表中。如果無法儲存到列表中，則MAC層放棄該資料的發送並向SSCS發送狀態爲TRANSACTION_OVERFLOW的MCPS-DATA.confirm原語。如果有能力儲存，則把原語中的資訊添加到待處理事務列表中。如果列表中的事務在時間macTransactionPersistenceTime內沒有被處理，則MAC層將放棄該資料訊框(Frame)的發送並向SSCS發送狀態爲TRANSACTION_EXPIRED的MCPS-DATA.confirm原語。如果TxOptions參數指示間接發送同時又指定了GTS發送或者接收請求原語的不是PAN協調器的MAC層，則間接發送選項無效。

如果TxOptions參數指示不使用安全機制，則MAC層訊框(Frame)控制欄位中的安全致能位元爲0，對資料訊框(Frame)不作任何安全保護處理；如果請求原語參數指示使用安全機制，則安全致能位爲1，並從MAC PIB的存取控制列表（ACL）入口獲取目的設備相關的密鑰和安全資訊。如果在ACL中找不到密鑰，MAC層將放棄資料訊框(Frame)的發送並向SSCS發出狀態爲UNAVAILABLE_KEY的MCPS-DATA.confirm證實原語了如果在ACL中找到了密鑰，MAC層將根據密鑰和安全資訊對資料訊框(Frame)作安全處理；若得到資料訊框(Frame)長度超過aMaxMACFrameSize，MAC層將放棄資料訊框(Frame)的發送並向SSCS發出狀態爲FRAME_TOO_LONG的證實原語。如果在安全處理過程中出現了任何其他錯誤，MAC層將放棄資料訊框(Frame)發送並向SSCS發出狀態爲FAILED_SECURITY_CHECK的證實原語。

如果請求的事務太長以至於不能在CAP或GTS內完成發送，MAC層將放棄資料訊框(Frame)發送並向SSCS發出狀態爲FRAME_TOO_LONG的證實原語。如果使用CSMA-CA機制傳輸資料時因故不成功，則MAC層將放棄資料訊框(Frame)發送並向SSCS發出狀態爲CHANNEL_ACCESS_FAILURE的證實原語。

如果要發送資料，MAC層首先要向物理層發送狀態爲TX_ON的PLME-SET-TRX-STATE.request請求原語。如果收到的PLME-SET-TRX-STATE.confirm證實原語狀態爲SUCCESS或TX_ON，MAC就向物理層發送攜帶MPDU的PD-DATA.request資料服務請求原語，收到物理層的PD-DATA.confirm證實原語後，MAC層就向物理層發出狀態爲RX_ON或TRX_OFF的PLME-SET-TRX-STATE.request原語，關閉發射機，完成MAC訊框(Frame)的發送過程。

如果TxOptions參數指示採用要求確認的資料發送，則MAC層在發送完MPDU後置接收機爲致能狀態，等待接收確認訊框(Frame)。如果在macAckWaitDuration個符號週期內沒有收到該資料的確認訊框(Frame)，則MAC層將重發資料訊框(Frame)；如果重發aMaxFrameRetries次仍然未收到確認訊框(Frame)，則MAC層將取消對該MSDU的發送，並向SSCS發出狀態爲NO_ACK的MCPS-DATA.confirm證實原語。

如果MPDU發送成功並且在要求確認的發送中收到了確認訊框(Frame)，MAC層就向SSCS層發送狀態爲SUCCESS的MCPS-DATA.confirm證實原語。如果MCPS-DATA.request原語中存在無效的參數，則MAC層向SSCS發送狀態爲INVALID_PARAMETER的證實原語。

MCPS-DATA.indication原語由對等的MAC層產生並發給SSCS，用以指示接收到一個MSDU。該原語的語法如下：

MCPS-DATA.indication（SrcAddrMode，SrcPANId，SrcAddr，DstAddrMode，DstPANId，DstAddr，msduLength，,msdu，mpduLinkQuality，SecurityUse，ACLEntry）

其中：參數mpduLinkQuality表示接收MPDU時的鏈路品質；參數SecurityUse是一個布林量，指示接收的資料訊框(Frame)是否採用了安全處理；ACLEntry表述資料訊框(Frame)發送設備ACL入口的macSecurityMode屬性值，取值範圍爲0x00～0x08，如果在ACL中找不到發送設備，則該參數置爲0x08。

MCPS-PURGE.request原語由SSCS產生，向MAC層請求撤銷事務佇列中的資料發送事務。其語法如下：

MCPS-PURGE.request（msduHandle）

MAC層收到該請求原語後，如果在事務佇列中找到了控制碼匹配的MSDU，則把該MADU從佇列中刪除並向SSCS返回一個狀態爲SUCCESS的MCPS-PURGE.confirm證實原語。如果在事務佇列中找不到和控制碼相匹配的MSDU，則MAC層向SSCS返回一個狀態爲INVALID_HANDLE的MCPS-PURGE.confirm證實原語。MCPS-PURGE.confirm原語的語法爲：

MCPS-PURGE.confirm（msduHandle，status）

在兩個設備之間成功傳遞MAC資料訊框(Frame)的資訊流程可以用圖7來表示。

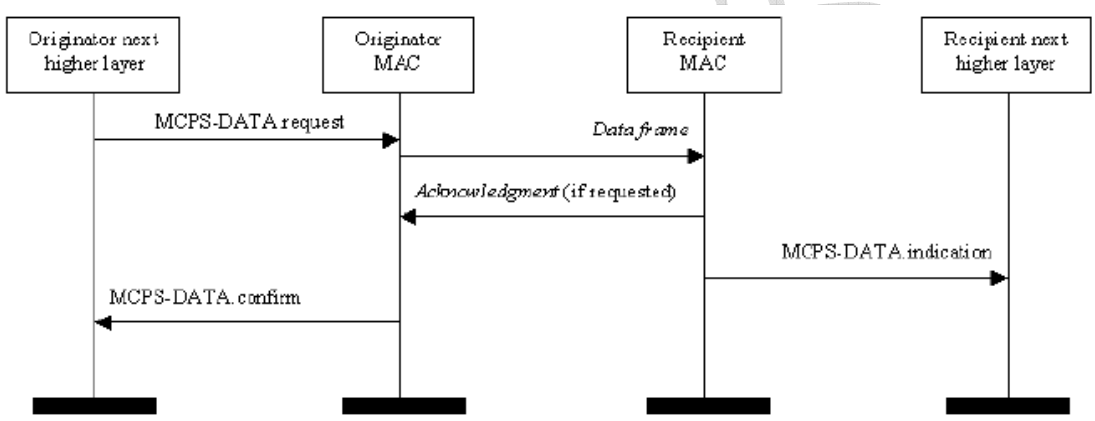


圖7 MAC資料服務流程

3.1.2 MAC 層管理服務

MLME-SAP 支援在 MAC 層和其上層之間傳遞管理命令。其管理功能是透過下列 15 類管理服務原語來實現的。

3.1.2.1 關聯原語 MLME-ASSOCIATE

MLME-SAP 關聯原語（MLME-ASSOCIATE）定義一個設備關聯到一個 PAN 的過程。所有設備都必須支援關聯請求和證實原語，RFD 可選支持關聯指示和回應原語。MLME-ASSOCIATE.request 原語允許設備請求關聯到一個協調器。請求關聯原語的語法如下：

MLME-ASSOCIATE.request（LogicalChannel，CoordAddrMode，CoordPANId，CoordAddress，

CapabilityInformation，SecurityEnable）

其中：參數 LogicalChannel 表示關聯的通道；CoordAddrMode 是協調器的位址模式（2 表示 16 位元短位址，3 表示 64 位擴充位址）；CoordPANId 表示協調器所處 PAN 標識碼；CoordAddress 是和位址模式相匹配的協調器位址；CapabilityInformation 表示關聯設備的工作能力；SecurityEnable 表示安全致能的布林量。

一個尚未關聯到 PAN 中的設備透過其 MLME 的上層關聯請求原語併發送給 MLME，請求關聯到一個協調器。如果設備要關聯到信標致能 PAN 的協調器，MLME 可選在發送關聯請求原語之前跟蹤該協調器的信標。當未關聯設備的 MLME 收到關聯請求原語時，首先調用 PLME-SET.request 原語吧 PHY PIB 屬性 phyCurrentChannel 更新爲 LogicalChannel 值，調用 MAC 層管理命令把 MAC PIB 屬性 macPANId 更新爲 CoordPANId 值;然後產生一個關聯請求命令，發送給關聯請求原語中位址和 PAN 標識碼所指定的協調器。

SecurityEnable 參數只是關聯請求命令訊框(Frame)是否應用安全機制。通常關聯請求命令不使用安全機制，如果設備知道協調器的安全資訊，則也可以在關聯請求命令中應用安全機制。如果 SecurityEnable 值爲 FALSE，MLME 將置訊框(Frame)控制欄位中安全致能位爲 0，關聯請求命令訊框(Frame)中不使用安全處理；如果 SecurityEnable 值爲 TRUE，MLME 將置訊框(Frame)控制欄位中的安全致能位元爲 1，並透過 MAC PIB 中的 ACL 入口獲得要關聯的協調器的密鑰和安全資訊。如果在 ACL 中沒有找到合適的密鑰，MLME 將丟棄該關聯請求命令訊框(Frame)並向其上層發出狀態爲 UNAVAILABLE_KEY 的關聯證實原語 MLME-ASSOCIATE.confirm。如果找到了密鑰，MLME 將把相關的安全資訊應用到關聯請求命令訊框(Frame)。如果在關聯請求命令訊框(Frame)的安全處理中出現了任何其他的錯誤，則 MLME 將丟棄該訊框(Frame)並向其上層發出狀態爲 FAILED_SECURITY_CHECK 的關聯證實原語。

如果關聯請求命令由於 CSMA-CA 演算法指示通道忙而不能送達協調器，MLME 將向其上層發出狀態爲 CHANNEL_ACCESS_FAILURE 的關聯證實原語。

爲了發送關聯請求命令訊框(Frame)，MLME 首先調用物理層管理服務原語 PLME-SET-TRX-STATE.request 把設備置爲發送致能狀態（TX_ON）。當 MLME 收到 PLME-SET-TRX-STATE.confirm 證實原語的狀態爲 SUCCESS 或 TX_ON 時，調用物理層資料服務原語 PD-DATA.request 發送關聯請求命令給協調器；最後接收到 PD-DATA.confirm 證實原語後，MLME 調用 PLME-SET-TRX-STATE.request 把設備置爲接收致能狀態（RX_ON），等待接收關聯請求命令的確認訊框(Frame)。如果重發 aMaxFrameRetries 次關聯請求命令仍沒收到確認訊框(Frame)，MLME 將向其上層發出狀態爲 NO_ACK 的關聯證實原語。

請求關聯設備的 MLME 接收到關聯請求命令的確認訊框(Frame)後，繼續等待關聯回應命令。如果在 aResponseWaitTime 個符號週期內沒有收到來自協調器的關聯回應命令訊框(Frame)，MLME 將向其上層發出狀態爲 NO_DATA 的關聯證實原語。如果關聯請求原語中任何參數的值超出有效範圍，則 MLME 將向其上層發出狀態爲 INVALID_PARAMETER 的關聯證實原語。如果請求關聯設備的 MLME 收到來自協調器的關聯響應命令訊框(Frame)，則 MLME 向其上層發送的關聯證實原語 MLME-ASSOCIATE.confirm 的狀態等於關聯回應命令訊框(Frame)中關聯狀態欄位的內容。

協調器的 MLME 收到關聯請求命令後，就向其上層發出 MLME-ASSOCIATE.indication 關聯指示原語。MLME-ASSOCIATE.indication 原語的語法如下：

MLME-ASSOCIATE.indication （ DeviceAddress ， CapabilityInformation ， SecurityUse ， ACLEntry）

收到關聯指示原語後，協調器將決定接受或拒絕設備的關聯請求，並向 MLME 發出關

聯回應原語 MLME-ASSOCIATE.response。協調器應當在 aResponseWaitTime 個符號週期內作出關聯決策和回應，請求關聯設備將根據關聯回應命令判斷關聯請求是否成功。

關聯回應原語 MLME-ASSOCIATE.response 的語法爲：

MLME-ASSOCIATE.response（DeviceAddress，AssocShortAddress，status，SecurityEnable）

其中：參數 DeviceAddress 是請求關聯設備的位址；AssocShortAddress 是協調器分配給請求關聯設備的 16 位元短位址，如果關聯不成功，則該位址設爲 0xFFFF；參數 status 表示關聯狀態，0x00 表示關聯成功，0x01 表示 PAN 容量飽和，0x02 表示 PAN 拒絕存取，其他值預留。

協調器的 MLME 收到關聯響應原語後，產生關聯回應命令訊框(Frame)，以間接發送方式發送給請求關聯的設備，即把回應命令訊框(Frame)添加到待處理事務列表中由相關設備來索取。如果列表中沒有足夠的空間儲存該事務，MAC 層將放棄該 MSDU 的發送並向其上層發送狀態爲 TRANSACTION_OVERFLOW 的通訊狀態指示原語 MLME-COMM-STATUS.indication。如果添加到列表中的事務在 macTransactionPresitenceTime 時間內沒有被及時處理，MAC 層將放棄處理該事務並向其上層發送狀態爲 TRANSACTION_EXPIRED 的通訊狀態指示原語。

如果因 CSMA-CA 機制存取通道失敗，MAC 層將放棄 MSDU 的發送並向其上層發送狀態爲 CHANNEL_ACCESS_FAILURE 的通訊狀態指示原語。如果關聯回應原語中任何參數的值超出有效範圍，MLME 將向其上層發出狀態爲 INVALID_PARAMETER 的通訊狀態指示原語。

爲了發送關聯回應命令訊框(Frame)，協調器的 MLME 首先調用物理層管理服務原語 PLME-SET-TRX-STATE.request 把設備置爲發送致能狀態（TX_ON）。當 MLME 收到 PLME-SET-TRX-STATA.confirm 證實原語的狀態爲 SUCCESS 或 TX_ON 時，調用物理層資料服務原語 PD-DATA.request 發送關聯回應命令；最後接收到 PD-DATA.confirm 證實原語後，MLME 再調用 PLME-SET-TRX-STATE.request 原語，根據是否需要接收關聯回應命令確認訊框(Frame)，把設備置爲接收致能（RX_ON）或收發都關閉狀態（TRX_OFF）。如果 MPDU 成功發送並且收到有確認要求的關聯回應命令訊框(Frame)的確認資訊，則 MLME 向其上層發送狀態爲 SUCCESS 的通訊狀態指示原語。

關聯證實原語 MLME-ASSOCIATE.confirm 由請求關聯設備的 MLME 產生，把關聯請求的結果通知給上層。關聯證實原語的語法爲：

MLME-ASSOCIATE.confirm（AssocShorAddress，status）

關聯服務的流程可用圖 8 來表示。

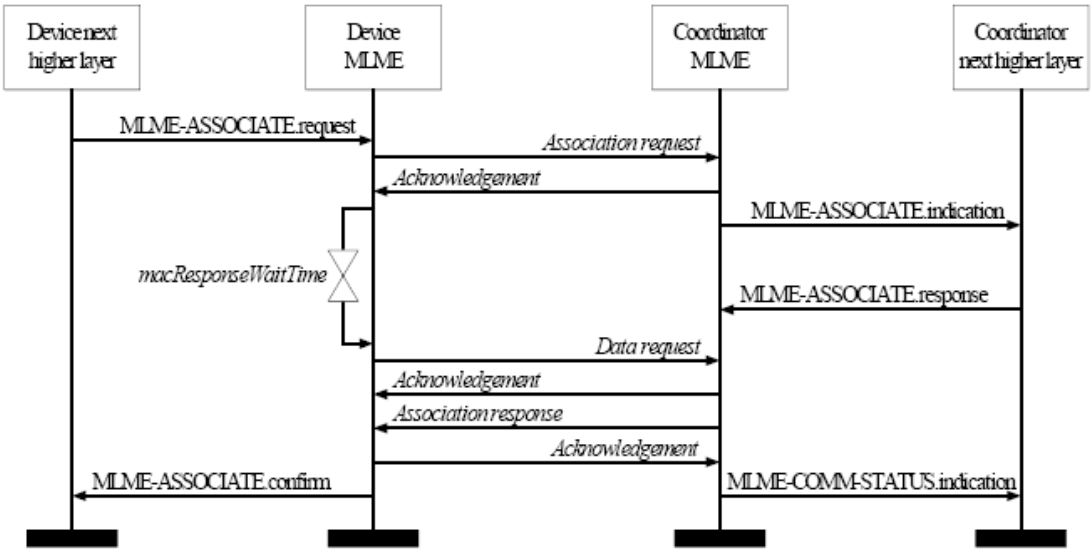


圖 8 關聯服務流程

3.1.2.2 解關聯原語 MLME-DISASSOCIATE

MLME-SAP 解關聯原語（MLME-DISASSOCIATE）定義一個設備從 PAN 中解關聯的過程。各種類型的設備都應能提供解關聯原語的介面。

離開 PAN 的關聯設備可透過關聯請求原語 MLME-DISASSOCIATE.request 把離網意圖告知協調器，協調器也可以用解關聯請求原語來強制一個關聯設備離開 PAN。也就是說，解關聯過程既可以由關聯設備啓動，也可以由協調器啓動。解關聯請求原語的語法爲：

MLME-DISASSOCIATE.request（DeviceAddress，DisassociateReason，SecurityEnable）

其中：參數 DeviceAddress 是接收解關聯通知設備的 64 位元 IEEE 位址；DisassociateReason 是解關聯原因，取值爲 0x00～0xFF；SecurityEnable 是安全致能參數。

收到來自上層的 MLME-DISASSOCIATE.request 原語，MLME 產生一個解關聯通知命令，如果 DeviceAddress 等於 macCoordExtendedAddress，設備將把解關聯通知命令發送給協調器。如果 DeviceAddress 不等於 macCoordExtendedAddress，並且接收原語的是協調器的 MLME，則協調器將以間接方式把解關聯通知命令發送給設備。其他情況設備收到解關聯請求時，MLME 將向其上層發出狀態爲 INVALID_PARAMETER 的解關聯證實原語 MLME-DISASSOCIATE.confirm。

如果解關聯通知命令在協調器上以間接方式發送，則把設備位址添加到信標訊框(Frame)的位址列表字段中，指示一個待處理訊息；同時，協調器把原語中的資訊添加待處理事務列隊中。如果待處理事務佇列中儲存空間不足，MLME 將放棄 MSDU 的發送並向其上層發出狀態爲 TRANSACTION_OVERFLOW 的解關聯證實原語。如果佇列中的事務在 macTransactionPresitenceTime 時間內沒有被及時處理，事務將被從佇列中刪除並且 MLME 向上層發出狀態爲 TRANSACTION_EXPIRED 的解關聯證實原語。

如果由於 CSMA 演算法導致解關聯通知命令不能發送，MLME 將向其上層發出狀態爲 CHANNEL_ACCESS_FAILURE 的解關聯證實原語。

一個設備發送解關聯命令訊框(Frame)時，MLME 首先調用物理層管理服務原語 PLME-SET-TRX-STATE.request 把設備置爲 TX_ON 狀態。當 MLME 收到

PLME-SET-TRX-STATE.confirm 證實原語的狀態爲 SUCCESS 或 TX_ON 時，調用物理層資料服務原語 PD-DATA.request 發送解關聯通知命令；最後接收到 PD-DATA.confirm 證實原語後，MLME 再調用 PLME-SET-TRX-STATE.request 原語，把設備置爲 RX_ON 狀態，等待接收確認訊框(Frame)。如果重傳 aMaxFrameRetries 次仍未收到確認訊框(Frame)，MLME 就向上層發送狀態爲 NO_ACK 的解關聯證實原語。

如果解關聯請求原語中的任何參數超出其有效範圍，MLME 將向上層發出狀態爲 INVALID_PARAMETER 的解關聯證實原語。如果解關聯通知命令發送成功並且收到了確認訊框(Frame)，MLME 就向上層發出狀態爲 SUCCESS 的解關聯證實命令，完成設備的解關聯。

設備收到解關聯通知命令後，MLME 就向上層發出解關聯指示原語 MLME-DISASSOCIATE.indication，通告解關聯的原因。解關聯指示原語的語法如下：
MLME-DISASSOCIATE.indication（DeviceAddress，DisassociateReason，SecurityUse，ACLEntry）

解關聯證實原語 MLME-DISASSOCIATE.confirm 在設備收到解關聯通知命令的確認後，由 MLME 向其上層報告解關聯請求的結果，其語法如下：

MLME-DISASSOCIATE.confirm（status）

解關聯服務的流程可用圖 9 來表示。

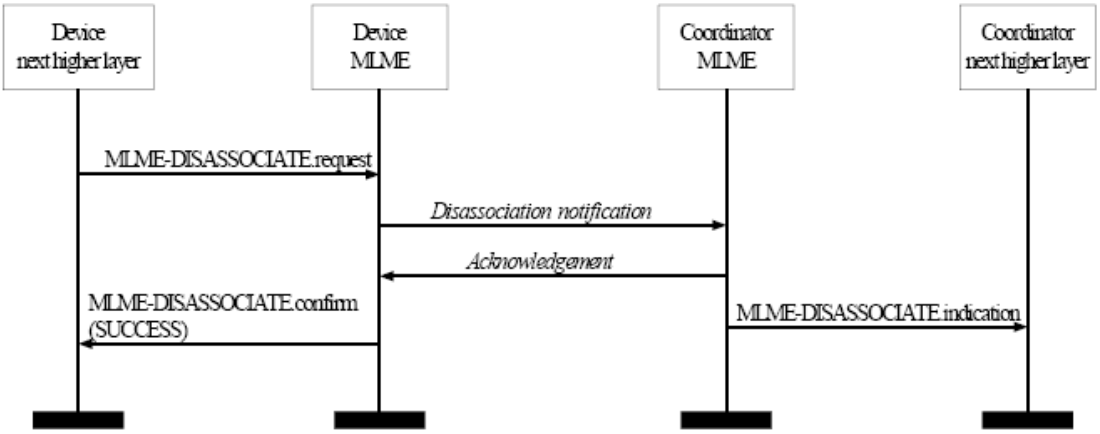


圖 9 解關聯服務流程

3.1.2.3 信標通知原語 MLME-BEACON-NOTIFY

信標通知指示原語 MLME-BEACON-NOTIFY.indication 把 MAC 層接收到的信標訊框(Frame)中的資訊傳遞給上層。各種類型設備都應當支援信標通知原語。信標通知指示原語的語法如下：
MLME-BEACON-NOTIFY.indication（BSN，PANDescriptor，PendAddrSpec，AddrList，sduLength，sdu）
其中：參數 BSN 是信標序號，取值爲 0x00～0xFF；PANDescriptor 是 PAN 描述符，具體定義如表 6 所列；PendAddrSpec 定義了信標位址列表中短位址和長位址的個數，具體見訊框(Frame)格式部分；AddrList 表示信標中待處理事務所屬設備的位址列表，位址數由 PendAddrSpec 決定；sdu 表示信標中攜帶的有效資料；sduLength 是用位元組數表示的有效資料的長度。

表 6 PANDescriptor 各元素的定義

元素名稱	類型	有效範圍	描述
CoordAddrMode	整數	0x02～0x03	發送信標的協調器的位址模式：2 表示 16 位短位址；3 表示 64 位擴充位址
CoordPANId	整數	0x0000～0xFFFF	協調器所在 PAN 的標識碼
CoordAddress	設備位址	CoordAddrMode 決定	發送信標的協調器的位址
LogicalChannel	整數	從物理層支援的通道中選取	網路當前佔用的通道
SuperframeSpec	點陣圖	詳見訊框(Frame)格式部分	信標中指定的超訊框(Frame)配置情況
GTSPermit	布林量	TRUE 或 FALSE	如果發送信標訊框(Frame)的協調器訊框(Frame)在接受 GTS 請求，就爲 TRUE；否則，爲 FALSE
LinkQuality	整數	0x00～0xFF	接收信標訊框(Frame)的鏈路品質
TimeStamp	整數	0x000000～0xFFFFFF	接收信標訊框(Frame)的時間，用符號數表示。精度至少爲 20 位
SecurityUse	布林量	TRUE 或 FALSE	指示信標訊框(Frame)是否採用了安全機制
ACLEntry	整數	0x00～0x08	發送資料訊框(Frame)的設備對應的 ACL 入口的 macSecurityMode 屬性值；如果在 ACL 找不到發送資料的設備，則置 0x08
SecurityFailure	布林量	TRUE 或 FALSE	在安全性處理中出現任何錯誤就置 TRUE；否則置爲 FALSE

3.1.2.4 讀取屬性原語 MLME-GET

獲取 PIB 屬性的原語（MLME-GET）定義從 MAC PIB 中讀取屬性值的過程。各種類型設備都應提供讀取屬性值原語的介面。MLME-GET.request 原語用來獲取指定 PIB 屬性的值，其語法爲：

MLME-GET.request（PIBAttribute）

參數 PIBAttribute 是 PIB 屬性的標識碼。接收到來自上一層的 MLME-GET.request 後，MLME 從 MAC 資料庫中檢索請求原語指定的 PIB 屬性。如果資料庫中找不到該屬性的標識碼，MLME 就向其上層發出狀態爲 UNSUPPORTED_ATTRIBUTE 的證實原語 MLME-GET.confirm；如果找到相關屬性的標識碼，MLME 就向其上層發出狀態爲 SUCCESS 的證實原語。MLME-GET.confirm 原語的語法爲：

MLME-GET.confirm（status，PIBAttribute，PIBAttributeValue）

如果 status 等於 SUCCESS，則 PIBAttributeValue 就是請求原語中要讀取的屬性值。

3.1.2.5 GTS 管理原語 MLME-GTS

GTS 管理原語（MLME-GTS）定義 GTS 的請求和維護。使用 GTS 管理原語和 GTS 的設備通常已經跟蹤了 PAN 協調器的信標。GTS 管理原語對 RFD 是可選支援的。

GTS 請求原語 MLME-GTS.request 由設備用以向 PAN 協調器請求分配一個 GTS 或撤銷已分配的 GTS。GTS 請求原語的語法爲：

MLME-GET.request（GTSCharacteristics，SecurityEnable）

其中參數 GTSCharacteristics 表示 GTS 請求的特徵。如果 GTSCharacteristics 的特徵類型欄位等於 1，表示設備請求分配一個 GTS，GTSCharacteristics 隨後的欄位就表示該新 GTS 的特徵；如果 GTSCharacteristics 的特徵類型欄位等於 0，表示設備請求撤銷已存在的 GTS，那麼 GTSCharacteristics 隨後的欄位就表示該現存 GTS 的特徵。

收到 GTS 請求原語後，MLME 就根據原語中攜帶的資訊產生一個 GTS 請求命令併發送給 PAN 協調器。如果 macShortAddress 屬性等於 0xFFFE 或 0xFFFF，則設備不允許請求 GTS，此時 MLME 向其上層發出狀態爲 NO-SHORT_ARRESS 的 GTS 證實原語 MLME-GTS.confirm。如果由於 CSMA 演算法失敗導致 GTS 請求命令不能發送，則 MLME 向其上層發出狀態爲 CHANNEL_ACCESS_FAILURE 的 GTS 證實原語。

發送 GTS 請求命令訊框(Frame)時，MLME 首先調用物理層管理服務原語 PLME-SET-TRX-STATE.request 把設備置爲 TX_ON 狀態；當 MLME 收到 PLME-SET-TRX-STATE.confirm 證實原語的狀態爲 SUCCESS 或 TX_ON 時，調用物理層資料服務原語 PD-DATA.request 發送 GTS 請求命令；最後接收到 PD-DATA.confirm 證實原語，MLME 再調用 PLME-SET-TRX-DATA.request 原語，把設備置爲 RX_ON 狀態，等待接收確認訊框(Frame)。如果重傳 aMaxFrameRetries 次仍未收到確認訊框(Frame)，MLME 就向其上層發出狀態爲 NO_ACK 的 GTS 證實原語。

GTS 請求得到批准和確認後，請求設備等待來自 PAN 協調器的包含 GTS 描述符的證實信標。如果 PAN 協調器能夠分配 GTS，它就向其上層發出 MLME-GTS.indication 原語，指示分配的 GTS 特徵；同時產生一個帶有分配的 GTS 特徵和請求設備短位址的 GTS 描述符。如果 PAN 協調器不能分配 GTS，它就產生一個開始時隙爲 0 的帶請求設備短位址的 GTS 描述符。不管 PAN 協調器能否分配 GTS，GTS 描述符都會在信標中持續 aGTSDescPersistenceTime 個超訊框(Frame)週期。

如果在 aGTSDescPersistenceTime 個超訊框(Frame)週期之前，請求設備收到 GTS 描述符中的短位址和 macShortAddress 一致的信標訊框(Frame)，請求設備就處理該信標訊框(Frame)的 GTS 描述符。如果在 aGTSDescPersistenceTime 個超訊框(Frame)週期之內沒有收到 GTS 描述符或者向上層發送了失步原因爲信標丟失 BEACON_LOST 的失步指示原語 MLME-SYNC-LOSS.indication，則請求設備的 MLME 將向其上層發出狀態爲 NO_DATA 的 GTS 證實原語。

如果描述符中的 GTS 特徵和設備請求的特徵相一致，則請求的 GTS 分配成功。請求設備的 MLME 就向其上層發出狀態爲 SUCCESS 的 GTS 證實原語，設備就可以使用分到的 GTS 了。如果收到信標中描述符的開始時隙爲 0，則表示 GTS 請求被拒絕，請求設備的 MLME 向其上層發出狀態爲 DENIED 的 GTS 證實原語。如果設備請求的一個 GTS 已經撤銷，請求設備的 MLME 將向其上層發出狀態爲 SUCCESS 的 GTS 證實原語並且 GTSCharacteristics 參數的特徵類型欄位爲 0。PAN 協調器收到請求撤銷 GTS 的命令，確認並撤銷指定 GTS，協調器的 MLME 向上層發出攜帶撤銷的 GTS 特徵的指示原語 MLME-GTS.indication。如果 GTS 請求原語中的任何參數超出有效範圍，MLME 就向其上層發出狀態爲 INVALID_PARAMETER 的 GTS 證實原語。

GTS 證實原語 MLME-GTS.confirm 由請求設備的 MLME 產生，向其上層報告 GTS 請求的結果。GTS 證實原語的語法如下：

MLME-GTS.confirm（GTSCharacteristics，status）

GTS 指示原語 MLME-GTS.indication 用以指示已經分配了一個新 GTS 或撤銷了一個現存的 GTS。GTS 指示原語的語法如下：

MLME-GTS.indication（DevAddress，GTSCharacteristics，ecurityUse，ACLEntry）其中 DevAddress 是分到 GTS 的設備的 16 位元短位址。當 PAN 協調器收到請求分配或撤銷 GTS 命令並執行相關操作後，MLME 向其上層發出 GTS 指示原語。當 PAN 協調器自身啓動撤銷 GTS 時，PAN 協調器的 MLME 也向其上層發出 GTS 指示原語；當 PAN 協調器撤銷設備的一個 GTS 時，設備 MLME 也向上層發出 GTS 指示原語。

分配 GTS 和撤銷現存 GTS 的流程分別如圖 10 和 11 所示。圖 11 中的 I 表示由設備啓動的撤銷 GTS 過程；II 表示由 PAN 協調器啓動的撤銷 GTS 過程。

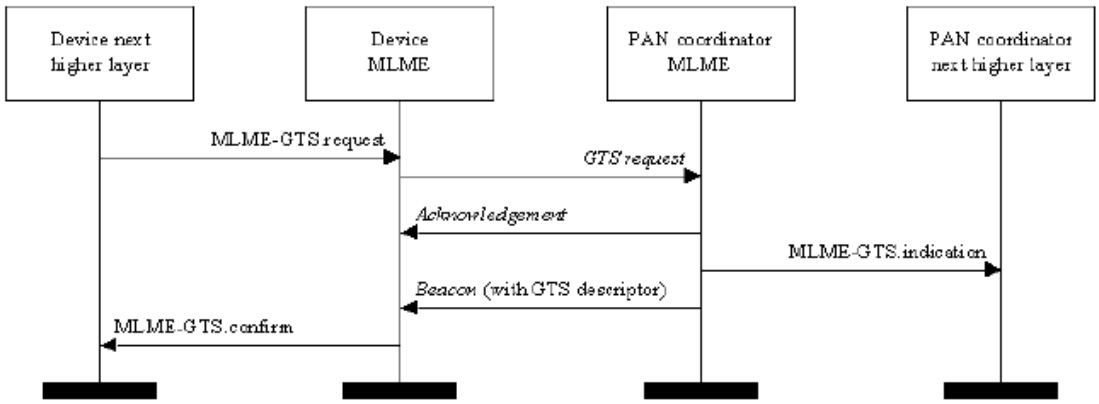


圖 10 設備請求分配 GTS 的流程

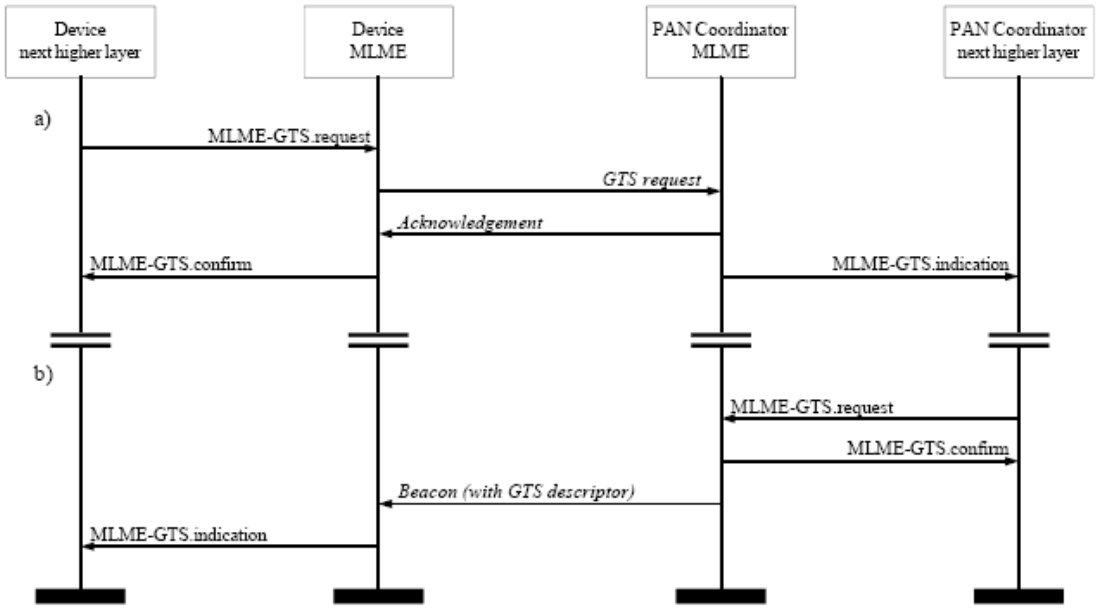


圖 11 撤銷 GTS 的流程

3.1.2.6 孤立通知原語 MLME-ORPHAN

孤立通知原語（MLME-ORPHAN）定義協調器如何向一個落孤的設備發出通知。孤立通知原語對 RFD 是可選支持的。協調器收到落孤設備發出的孤立通知命令後，MLME 產生孤立指示原語 MLME-ORPHAN.indication 向其上層指示存在一個落孤的設備。

MLME-ORPHAN.indication 原語的語法如下：

MLME-ORPHAN.indication（OrphanAddress，SecurityUse，ACLEnty）

其中 OrphanAddress 是落孤設備的 64 位元擴充位址。協調器 MLME 的上層收到孤立指示原語後，判斷該落孤的設備是否是該協調器之前關聯的設備並向 MLME 發出孤立響應原語 MLME-ORPHAN.response。孤立回應原語的語法如下：

MLME-ORPHAN.response(OrphanAddress，ShortAddress，AssociatedMember，SecurityEnable）

其中：ShortAddress 是協調器分配給落孤設備的短位址；AssociatedMember 是布林量，指示落孤設備是否是該協調器此前關聯的設備。

如果落孤設備是協調器的關聯設備，則 MLME-ORPHAN.response 原語中的 AssociatedMember 爲 TRUE，ShortAddress 爲關聯時協調器分配給落孤設備的短位址，MLME 產生一個包含 ShortAddress 欄位的重排列命令，在信標致能 PAN 的 CAP 中發送或立即發送；如果落孤設備不是協調器的關聯設備，則向 MLME 發出的回應原語中 AssociatedMember 爲 FALSE，不再做任何後續操作。如果落孤設備在發出落孤通知命令後的 aResponseWaitTime 個符號週期內沒有收到任何協調器的重排列命令，它就認爲在有效範圍之內沒有關聯的協調器。

發送協調器重拍列命令訊框(Frame)時，MLME 首先調用物理層管理服務原語 PLME-SET-TRX-STATE.request 把發射機設置爲 TX_ON 狀態。當 MLME 收到 PLME-SET-TRX-STATE.confirm 證實原語的狀態爲 SUCCESS 或 TX_ON 時，調用物理層資料服務原語 PD-DATA.request 發送重排列命令；最後接收到 PD-DATA.confirm 證實原語，MLME 再調用 PLME-SET-TRX-STATE.request 原語，把收發信機設置爲 RX_ON 狀態，等待接收確認訊框(Frame)。如果重傳 aMaxFrameRetries 次仍未收到確認訊框(Frame)，MLME 就向其上層發出狀態爲 NO_ACK 的通訊狀態指示原語 MLME-COMM-STATUS.indication。

如果重排命令發送成功並且在要求確認時得到了確認，協調器的 MLME 就向其上層發出狀態爲 SUCCESS 的通訊狀態指示原語。如果 MLME-ORPHAN.response 中的任何參數超出有效範圍，協調器的 MLME 就向其上層發出狀態爲 INVALID_PARAMETER 的通訊狀態指示原語。

協調器和鼓勵設備之間的通訊過程如圖 12 所示。

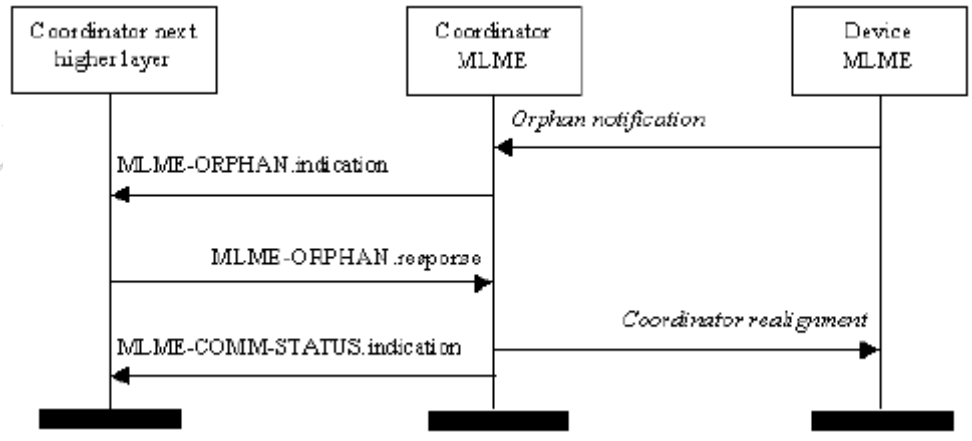


圖 12 協調器和鼓勵設備的通訊流程

3.1.2.7 復位原語 MLME-RESET

復位原語（MLME-RESET）定義吧 MAC 層 PIB 的屬性值恢復爲缺省值的方法。各種類型設備都應支援重定原語。復位請求原語 MLME-RESET.request 由上層產生，向 MLME 申請對 MAC 層作復位操作。重定請求原語的語法如下：

MLME-RESET.request（SetDefaultPIB）

參數 SetDefaultPIB 是布林量，如果等於 TRUE，則復位 MAC 層並把 MAC PIB 的所有屬性設爲缺省值；如果等於 FALSE，則重定 MAC 但 MAC PIB 的屬性值保持不變。復位請求原語通常愛 MLME-START.request 原語和 MLME-ASSOCIATE.request 原語之前使用。如果重定請求原語發給關聯設備或協調器的 MLME，則表明在此之前 MLME 收到瞭解關聯請求原語 MLME-DISASSOIATE.request。

收到重定請求原語後，MLME 調用物理層管理服務原語 PLME-SET-TRX-STATE.request，把收發信機設置爲 TRX_OFF 狀態。收到收發信機設置確認原語後，MAC 層恢復到初始化條件，所有內部變數設置爲缺省值；如果 SetDefaultPIB 等於 TRUE，則 MAC PIB 的屬性也都設置爲缺省值。

如果收到收發信機狀態設置成功的證實原語，MLME 向其上層發出狀態爲 SUCCESS 的重定證實原語 MLME-RESET.confirm；否則重定證實原語的狀態爲關閉收發信機失敗（DISABLE_TRX_FAILURE）。重定證實原語的語法如下：

MLME-RESET.confirm（status）

3.1.2.8 接收機狀態原語 MLME-RX-ENABLE

接收機狀態原語（MLME-RX-ENABLE）定義設備如何在指定的時間段致能和關閉接收機。各種類型設備都應支援接收機狀態原語。

接收機致能請求原語 MLME-RX-ENABLE.request 由上層產生，向 MLME 請求在一段時間內致能接收機。接收機致能請求原語的語法如下：

MLME-RX-ENABLE.request（DeferPermit，RxOnTime，RxOnDuration）

其中：布林量參數 DeferPermit 等於 TRUE 表示當請求的接收機致能時間已經過時時，可以延遲到下一個超訊框(Frame)週期，DeferPermit 等於 FALSE，表示只能在當前的超訊框(Frame)內分配接收機致能時間，該參數對無信標的 PAN 網無效；參數 RxOnTime 表示接收機致能時間起點距超訊框(Frame)開始位置的字元數，取值爲 0x000000～0xFFFFFF，最小精度爲 20 位，該參數對無信標的 PAN 無效；RxOnDuration 表示用符號數計算的接收機致能持續時間，取值爲 0x000000～0xFFFFFF。每個請求原語接收機僅致能一次。

對不使用信標的 PAN，當收到接收機致能請求原語後，MLME 忽略 DeferPermit 和 RxOnTime，請求物理層立即置接收機爲致能狀態並在 RxOnDuration 各符號週期後關閉接收機。

在有信標的 PAN 中，收到接收機致能請求原語後 MLME 首先判斷（RxOnTime+RxOnDuration）是否小於信標間隔。如果不小於信標間隔，則表示請求原語中的參數無效，MLME 向其上層發出狀態爲 INVALID_PARAMETER 的接收機致能證實原語 MLME-RX-ENABLE.confirm；如果（RxOnTime+RxOnDuration）小於信標間隔，MLME 判斷請求的接收機致能能否在當前超訊框(Frame)內執行。如果當前超訊框(Frame)已發送符號數小於（RxOnTime-aTurnaroundTime），MLME 將嘗試在當前超訊框(Frame)執行接收機致能；如果當前超訊框(Frame)已發送符號數不小於（RxOnTime-aTurnaroundTime）並且 DeferPermit 等於 TRUE，MLME 將推遲到寫一個超訊框(Frame)嘗試執行接收機致能。其他情況下，

MLME 將向其上層發出狀態爲 OUT_OF_CAP 的接收機致能證實原語。

爲了執行接收機致能，MLME 調用狀態爲 RX_ON 的物理層管理服務原語 PLME-SET-TRX-STATE.request。如果物理層返回的 PLME-SET-TRX-STATE.confirm 證實原語的狀態爲 TX_ON，MLME 將向其上層發出狀態爲 TX_ACTIVE 的接收機致能證實原語 MLME-RX-ENABLE.confirm；否則，MLME 將向其上層發出狀態爲 SUCCESS 的接收機致能證實原語。

如果（RxOnTime+RxOnDuration）沒有超出 CAP，MLME 在執行 RxOnDuration 個符號週期接收機致能後 向物理層發出狀態爲 TRX_OFF 的 PLME-SET-TRX-STATE.request 原語，關閉收發信機。如果（RxOnTime+RxOnDuration）超出當前 CAP 的持續時間，MLME 需確保接收機和 CAP 之後的任何工作要求不衝突。如果 RxOnDuration 等於 0，則 MLME 請求物理層關閉接收機。

接收機致能證實原語 MLME-RX-ENABLE.confirm 是由 MLME 向其上層報告 MLME-RX-ENABLE.request 原語請求接收機致能的結果。接收機致能證實原語的用法在上述接收機致能請求原語中已經作了介紹，它的語法如下：

MLME-RX-ENABLE.confirm（status）

圖 13 是改變接收機狀態的流程，其中 I 表示在有信標的 PAN 中 MLME 沒有足夠時間在當前超訊框(Frame)執行接收機致能而推遲到下一個超訊框(Frame)的情況；II 表示不使用信標的 PAN 中改變接收機狀態的情況。

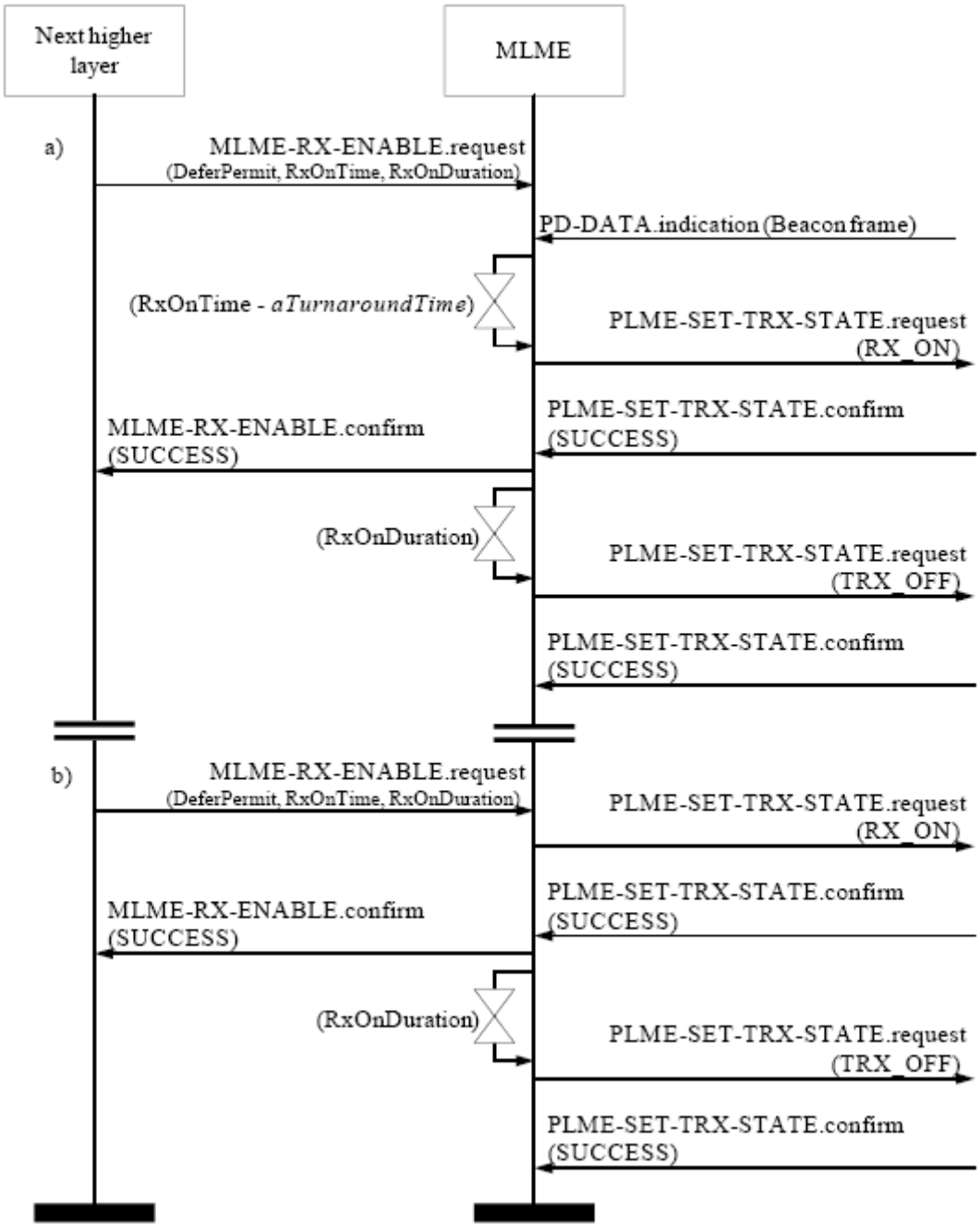


圖 13 接收機狀態改變流程

3.1.2.9 通道掃描原語 MLME-SCAN

通道掃描原語（MLME-SCAN）定義設備如何判斷通訊通道是否有信號傳輸或者是否存在 PAN。各種類型設備都應支援通道掃描原語。

通道掃描請求原語 MLME-SCAN.request 按照指定的通道列表啓動通道掃描。設備可以透過通道掃描判斷通道使用情況、搜索關聯的協調器或者搜索個人工作空間（POS）範圍內所有發送信標的協調器。MLME-SCAN.request 的語法如下：

MLME-SCAN.request（ScanType，ScanChannels，ScanDuration）

其中：參數 ScanType 表示掃描類型的整數，0x00 表示 ED 掃描，0x01 表示主動掃描，0x02 表示被動掃描，0x03 表示孤立設備掃描；ScanChannels 在 32 位元資料的低 27 位元上以點陣圖的形式表示掃描的通道，1 表示掃描，0 表示不掃描；ScanDuration 表示通道掃描持續時間，取 0～14 的整數。

通道掃描請求原語由 MLME 的上層產生並發給 MLME，啓動通道掃描以搜索掃描設備 POS 範圍內的活動情況。ED 掃描用來判斷通道的使用情況；主動和被動掃描用來定位帶有 PAN 識別字的信標；孤立設備掃描用來定位孤立設備所關聯的 PAN。各種掃描類型的詳細介紹在 MAC 層功能描述部分。

ED 掃描或主動掃描可以在 FFD 變成 PAN 協調器之前執行；主動掃描或被動掃描可以在選擇關聯的 PAN 之前使用；孤立設備掃描可以用來定位設備孤立之前關聯的協調器。所有設備都應支援被動掃描和孤立設備掃描。RFD 可選支援 ED 掃描和主動掃描。

收到 MLME-SCAN.request 原語，MLME 對通道掃描列表中的通道進行掃描。掃描期間，掃描設備停止發送信標訊框(Frame)，MAC 層之接受物理層資料服務中和掃描有關的資料訊框(Frame)。

透過 ED 掃描，設備能夠測得每個請求掃描通道上的峰值能量。ED 掃描由 MLME 針對每個掃描通道向物理層重複發送 PLME-ED.request 原語執行能量檢測，檢測時間爲 [aBaseSuperframeDuration×（2^n+1）]個符號週期，其中 n 是 ScanDuration 的參數值。完成一個通道的掃描，MLME 記下該通道最大能量，轉移到請求通道列表中的下一個掃描通道繼續 ED。當掃描的通道數達到實現要求的通道數或者完成了請求通道列表中所有通道的掃描，ED 掃描過程結束。

主動掃描由 FFD 用來搜索其 POS 範圍內正在發送信標訊框(Frame)的協調器。主動掃描時，首先由 MLME 向每個通道發送一個信標請求命令；然後 MLME 致能接收機，記錄每個信標中的 PAN 描述符。掃描當前通道的時間達到 ScanDuration 參數規定的時間，MLME 結束當前通道的掃描轉移到下一個通道掃描。當記錄的 PAN 描述符熟路達到實現要求的最大數目或者對所有通道列表中的通道都完成掃描時，主動掃描過程結束。

和主動掃描一樣，被動掃描也是由設備用來搜索其 POS 範圍內正在發送信標訊框(Frame)的協調器，不同的是被動掃描只接收操作並不發送信標請求命令。對一個通道掃描時，MLME 致能接收機，記錄信標中的 PAN 描述符。掃描當前銑刀達到 ScanDuration 參數規定的時間後，MLME 結束當前通道的掃描轉移到下一個通道掃描。當記錄的 PAN 描述符數目達到實現要求的最大資料或者對所有通道列表中的通道都完成掃描時，被動掃描過程結束。

孤立設備掃描用來定位掃描設備孤立之前所關聯的協調器。孤立設備對每個通道進行掃描時，MLME 首先發送一個孤立通知命令，然後置接收致能狀態等待接收。如果在 aResponseWaitTime 個符號週期內，孤立設備收到一個協調器的重排列目錄，掃描設備關閉接收，孤立設備和它關聯的協調器重新建立了通訊。如果在這個時間週期內沒有收到重排列命令，則轉移到掃描通道列表中的下一個通道掃描。當收到重排列目錄或者完成了列表中所有通道的掃描，孤立設備掃描結束。

ED 掃描的結果記錄在一個 ED 值列表中，MLME 向其上層發出狀態爲 SUCCESS 的掃描證實原語 MLME-SCAN.confirm，報告 ED 掃描結果。

主動掃描和被動掃描結果是記錄的一組 PAN 描述符的值，由 MLME 透過 MLME-SCAN.confirm 原語向上層報告。如果掃描中沒有發現信標，MLME-SCAN.confirm 原語的 PAN 描述符欄位爲空，狀態爲 NO_BEACON；如果掃描過程中發現了信標，MLME-SCAN.confirm 原語的狀態爲 SUCCESS，並攜帶了掃描得到的 PAN 描述符列表和未

掃描通道列表。

孤立設備掃描如果收到了協調器的重排列命令，MLME 向其上層發送狀態爲 SUCCESS 的 MLME-SCAN.confirm 原語；如果未收到重排列命令，MLME-SCAN.confirm 原語的狀態爲 NO_BEACON。孤立設備掃描證實原語中的 PAN 描述符列表和能量檢測列表總爲空。

如果 MLME-SCAN.request 原語中的任何參數超出有效範圍，則 MLME 向其上層發出狀態爲 INVALID_PARAMETER 的通道掃描證實原語。

通道掃描證實原語 MLME-SCAN.confirm 由 MLME 用來向其上層報告通道掃描請求的結果。它的語法如下：

MLME-SCAN.confirm （ status ， ScanType ， UnscannedChannels ， ResultListSize ， EnergyDetectList，PANDescriptorList）

其中：參數 UnscannedChannels 以點陣圖形式用 32 位數的 27 個低有效表示未掃描的通道，1 表示通道未掃描，0 表示掃描過或沒有請求掃描；ResultListSize 表示掃描結果的位元組數；EnergyDetectList 是 ED 掃描的峰值能量列表；PANDescriptorList 是主動掃描和被動掃描中記錄的 PAN 描述符列表。通道掃描證實原語的語法在通道掃描請求原語的描述中已有詳細的介紹。

3.1.2.10 通訊狀態原語 MLME-COMM-STATUS

當傳輸不是由請求原語.request 啓動，或者到達的分組出現安全處理錯誤時，MLME 透過通訊狀態指示原語和上層交互傳輸狀態資訊。MLME-COMM-STATUS.indication 原語的語法如下：

MLME-COMM-STATUS.indication（PANId，SrcAddrMode，SrcAddr，DstAddrMode，DstAddr，status）

3.1.2.11 設置屬性原語 MLME-SET

MAC PIB 屬性設置原語（MLME-SET）定義對 PIB 屬性作寫操作的過程。各種類型設備都應支援 PIB 屬性設置原語。

MAC PIB 屬性設置請求原語 MLME-SET.request 由上層發給 MLME，請求把指定的 PIB 屬性設置爲指定的值。MLME-SET.request 的語法如下：

MLME-SET.request（PIBAttribute，PIBAttributeValue）

其中：參數 PIBAttribute 是請求設置的屬性標識碼；PIBAttributeValue 是擬設置的屬性值。接收到 PIB 屬性設置請求原語後，MLME 在資料庫中檢索請求的屬性。如果資料庫找不到請求的 PIB 屬性，MLME 就向其上層發出狀態爲 UNSUPPORTED_ATTRIBUTE 的屬性設置證實原語 MLME-SET.confirm；如果請求設置的屬性值超出了有效範圍，MLME 就向其上層發出狀態爲 INVALID_PARAMETER 的屬性設置證實原語；如果屬性設置成功，MLME 以狀態爲 SUCCESS 的 MLME-SET.confirm 原語向其上層報告屬性設置結果。

屬性設置證實原語 MLME-SET.confirm 的語法如下：

MLME-SET.request（status，PIBAttribute）

3.1.2.12 更新超訊框(Frame)配置原語 MLME-START

更新超訊框(Frame)配置原語（MLME-START）定義一個 FFD 如何請求啓用新的超訊框(Frame)配置來實現 PAN 初始化、信標產生、設備發現、停止發送信標等。更新超訊框(Frame)配置原語對 RFD 是可選的。

MLME-START.request 原語由上層發給 MLME，請求設備開始使用新的超訊框(Frame)配置。更新超訊框(Frame)配置請求原語的語法如下：
MLME-START.request （ PANId ， LogicalChannel ， BeaconOrder ， SuperframeOrder ， PANCoordinator，BatteryLifeExtension，CoordRealignment，SecurityEnable）
其中：參數 BeaconOrder（BO）跟發送信標的頻率有關，BO 爲 0～14 時，信標間隔（BI）爲（aBaseSuperframeDuration×2^{BO}）個符號週期，取值 15 時表示協調器不發送信標，超訊框(Frame)結構不存在，SuperframeOrder 參數無效；SuperframeOrder（SO）定義了超訊框(Frame)中包括信標在內的啓動部分的長度（SD），SO 爲 0～BO 表示 SD 爲（aBaseSuperframeDuration×2^{SO}）個符號週期，SO=15 表示超訊框(Frame)的信標之後沒有啓動部分，參數 PANCoordinator 是一個布林量，取值 TRUE 表示該設備將成爲一個新的 PAN 的網路協調器，取值 FALSE 表示該設備將發送關聯 PAN 的信標；參數 BatteryLifeExtension 是一個定義節能模式的布林量，取值 TRUE 表示該發送信標設備的接收機在信標訊框(Frame)間隔（IFS）之後關閉 BatLifeExtPeriods 個完整的退避週期，取值 FALSE 表示信標設備的接收機在整個 CAP 一直處於致能狀態；布林量 CoordRealignment 取 TRUE 表示在改變超訊框(Frame)配置之前先發送一個協調器重排列命令，否則取 FALSE；布林量 SecurityEnable 表示發送信標訊框(Frame)時是否使用安全機制。

如果收到 MLME-START.request 原語時設備短位址 macShortAddress 等於 0xFFFF，MLME 就向其上層返回狀態爲 NO_SHORT_ADDRES 的 MLME-START.confirm 證實原語。如果設備擁有合法的短位址，則收到 MLME-START.request 原語後 MLME 設置屬性 macBeaconOrder 的值爲參數 BeaconOrder 的值。如果 macBeaconOrder 值爲 15，MLME 也設置屬性 macSuperframeOrder 的值爲 15，此時該原語配置了一個無信標的 PAN；如果 macBeaconOrder 的值小於 15，MLME 把屬性 macSuperframeOrder 的值設爲爲參數 SuperframeOrder 的值。

當參數 PANCoordinator 的值爲 TRUE 時，該設備將作爲網路協調器建立一個新的 PAN。MLME 把 MAC 層屬性 macPANId 更新爲參數 PANId 的值，調用物理層管理服務原語 PLME-SET.request 把物理層屬性 phyCurrentChannel 更新爲參數 LogicalChannel 的值。

如果參數 CoordRealignment 的值爲 TRUE，MLME 將產生並廣播攜帶 PANId 和 LogicalChannel 參數的協調器重排列命令。如果正在發送信標，則新的超訊框(Frame)配置在下一個信標時生效；如果設備不在發送信標，則新的超訊框(Frame)配置立即生效。信標訊框(Frame)中使用的位址由屬性 macShortAddress 決定，該原語也設置屬性 macBatt-LifeExt 爲參數 BatteryLifeExtension 的值。

爲了發送信標訊框(Frame)，MLME 首先調用 PLME-SET-TRX-STATE.request 原語置發射機爲致能狀態（TX_ON）。在收到狀態爲 SUCCESS 或 TX_ON 的證實原語 PLME-SET-TRX-STATE.confirm 後，再調用物理層資料服務原語 PD-DATA.request 發送信標訊框(Frame)。在收到 PD-DATA.confirm 確認訊框(Frame)後，如果超訊框(Frame)的活動部分長度超出信標訊框(Frame)的長度，則 MLME 調用 PLME-SET-TRX-STATE.request 原語置接收機爲致能狀態（RX_ON）；如果超訊框(Frame)的活動週期僅爲信標訊框(Frame)週期部分，

則接收機置關閉狀態。

一個完整的超訊框(Frame)配置更新過程還包括 MLME 透過證實原語 MLME-START.confim 對請求原語的回應。如果超訊框(Frame)配置更新成功，MLME 向其上層回饋一個狀態爲 SUCCESS 的證實原語；如果更新超訊框(Frame)配置請求原語中出現不支持的參數或任何參數超出了有效取值範圍，則 MLME 向其上層發出狀態爲 INVALID_PARAMETER 的證實原語。

更新超訊框(Frame)配置證實原語 MLME-START.confirm 的語法爲：

MLME-START.confirm（Status）

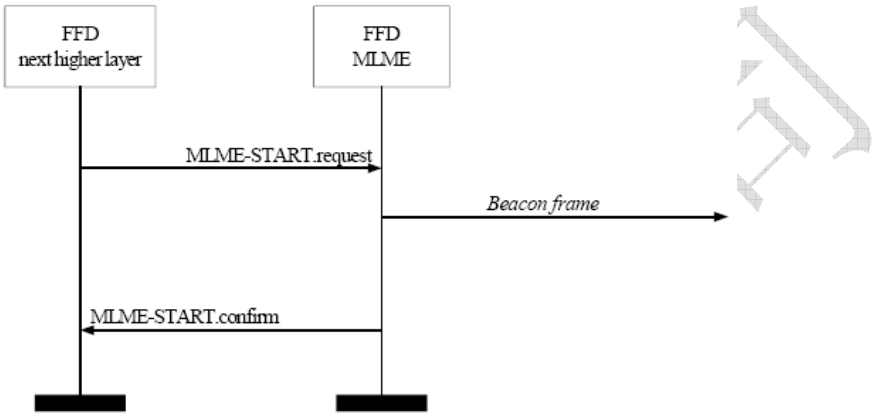


圖 14 是一個 FFD 初始化信標發送的流程。

3.1.2.13 同步原語 MLME-SYNC

同步原語定義設備和協調器獲得同步的過程以及如何向上層報告失步資訊。MLME 的同步原語包括同步請求原語 MLME-SYNC.request 和失步指示原語 MLME-SYNC-LOSS.indication。各種類型設備都應該支援這兩種同步原語。

同步請求原語 MLME-SYNC.request 的語法爲：

MLME-SYNC.request（LogicChannel，TrackBeacon）

其中參數 TrackBeacon 是布林量，取 TRUE 表示 MLME 將同步到下一個信標並跟蹤後續的所有信標，取 FALSE 表示只同步到下一個信標。

同步請求原語由發送信標的 PAN 網中設備的上層產生併發送給 MLME，以便設備和協調器同步。帶信標的 PAN 中設備收到 MLME-SYNC.request 原語後，MLME 首先調用物理層管理服務原語 PLME-SET.request 把物理層屬性 phyCurrentChannel 設置爲 LogicChannel 參數的值；然後致能接收機搜索當前網路中的信標。如果 TrackBeacon 參數爲 TRUE，MLME 將跟蹤信標，即在每個信標出現之前置接收機爲致能狀態，以便對信標進行處理；如果 TrackBeacon 參數爲 FALSE，MLME 則只定位下一個信標訊框(Frame)而不跟蹤後續的信標訊框(Frame)。

如果接收到同步請求原語時 MLME 正在跟蹤信標訊框(Frame)，MLME 並不丟棄該原語，而是當作一個新的同步請求。如果在初始捕獲或跟蹤過程中不能定位信標，則 MLME 上層發出失步原因爲 BEACON_LOST 的失步指示原語。

3.1.2.14 失步原語 MLME-SYNC-LOSS

失步指示原語 MLME-SYNC-LOSS.indication 的語法爲：

MLME-SYNC-LOSS.indication（LossReason）

失步指示原語在設備與協調器失步時由 MLME 產生並向其上層報告失步原因。失步指示原語也可以由 PAN 協調器的 MLME 產生，向其上層報告發生了 PAN 標識碼衝突（PAN_ID_CONFLICT）。

如果設備檢測到 PAN 標識碼衝突並告知協調器，設備 MLME 將其上層發出失步原因爲 PAN_ID_CONFLICT 的失步指示原語；同樣地，PAN 協調器在收到 PAN ID 衝突通知命令後，其 MLME 也向上層發出失步原因爲 PAN_ID_CONFLICT 的是不指示原語。

如果設備沒有執行孤立設備掃描而收到了關聯協調器的重排列命令，MLME 向其上層發出失步原因爲 REALIGNMENT 的失步指示原語。

在收到同步請求原語後，如果設備在連續 aMaxLostBeacons 個超訊框(Frame)週期內都沒“聽”到信標，MLME 就向其上層發出狀態爲失步原因爲 BEACON_LOST 的失步指示原語。

圖 15 是設備和協調器同步的流程。其中 I 是同步單個信標的情況，設備找到信標後判斷協調器中是否有需要傳送給自己的資料，如果有，就請求獲取資料；II 是跟蹤信標的情況，設備在找到一個信標後，設置計時器剛好計數到下一個信標預期出現的時間之前以跟蹤信標。在收到信標後，設備同樣檢查協調器上是否有要遞交給自己的資料。

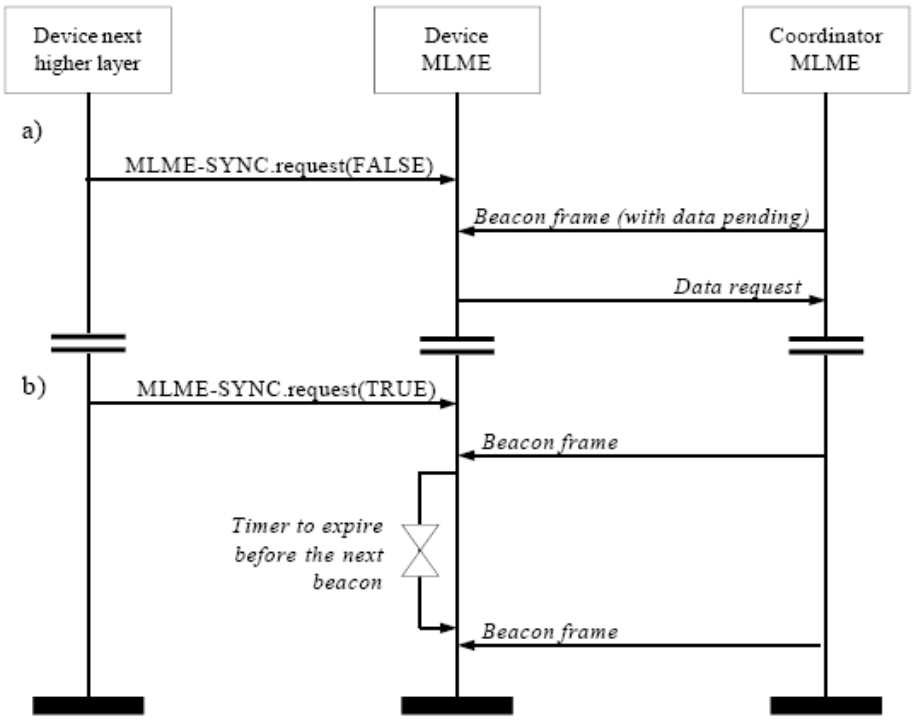


圖 15 設備同步流程

3.1.2.15 輪詢原語 MLME-POLL

輪詢原語定義設備向協調器請求資料的過程。各種類型設備都應該支援輪詢原語。輪詢原語包括輪詢請求 MLME-POLL.request 和輪詢證實 MLME-POLL.confirm。

輪詢請求原語 MLME-POLL.request 由設備上層發送給 MLME，用以向協調器請求資料。輪詢請求原語的語法爲：

MLME-POLL.request（CoordAddrMode，CoordPANId，CoordAddress，SecurityEnable）

接收到 MLME-POLL.request 原語後，MLME 產生並發送一個資料請求命令。如果是向 PAN 協調器請求資料，則資料請求命令中不含任何目的位址資訊；否則，資料請求命令攜帶參數 CoordPANId 和 CoordAddress 中的目的位址資訊。

如果由於 CSMA 演算法失敗而不能發送資料請求命令，MLME 就向其上層發出狀態爲 CHANNEL_ACCESS_FAILURE 的輪詢證實原語 MLME-POLL.confirm。

爲了發送資料請求訊框(Frame)，MLME 首先調用物理層管理服務原語 PLME-SET-TRX-STATE.request 把發射機設置爲 TX_ON 狀態；當 MLME 收到 PLME-SET-TRX-STATE.confirm 證實原語的狀態爲 SUCCESS 或 TX_ON 時，調用物理層資料服務原語 PD-DATA.request 發送資料請求命令；最後接收到 PD-DATA.confirm 證實原語，MLME 再調用 PLME-SET-TRX-STATE.request 原語，把收發信機設置爲 RX_ON 狀態，等待接收確認訊框(Frame)。如果重傳 aMaxFrameRetries 次資料請求命令仍未收到確認訊框(Frame)，MLME 則向其上層發出狀態爲 NO_ACK 的輪詢證實原語。

如果設備收到資料請求命令的確認訊框(Frame)，並且指示有資料需要傳送，則 MLME 請求物理層置接收機爲致能狀態；如果確認訊框(Frame)指示沒有待處理資料，MLME 則向上層發出狀態爲 NO_DATA 的輪詢證實原語。

如果設備收到協調器發送的有效資料長度爲 0 資料訊框(Frame)或 MAC 命令訊框(Frame)，則 MLME 向其上層發出狀態爲 NO_DATA 的輪詢證實原語。如果設備收到協調器發送的有效資料長度不爲 0 的資料訊框(Frame)，則 MLME 向上層發送狀態爲 SUCCESS 的輪詢證實原語，並透過 MAC 層資料服務原語 MCPS-DATA.indication 向上層報告收到的 MSDU。

如果資料請求命令的確認訊框(Frame)指示協調器有資料傳送給設備，但是設備在 aMaxFrameResponseTime 符號週期內沒有收到資料訊框(Frame)，則 MLME 也向上層發出狀態爲 NO_DATA 的證實原語 MLME-POLL.confirm。

如果 MLME-POLL.request 原語中有不支持的參數或者任何參數值超出有效範圍，則 MLME 向其上層發送狀態爲 INVALID_PARAMETER 的輪詢證實原語。

輪詢證實原語 MLME-POLL.confirm 由 MLME 向上層報告設備向協調器請求資料的結果。它的語法爲：

MLME-POLL.confirm（status）

圖 16 是設備向協調器請求資料的流程。其中 I 是協調器中沒有待傳資料的情況，設備 MLME 立即向上層發送 MLME-POLL.confirm 原語；II 是協調器中有待傳送資料的情況，設備接收到資料後 MLME 向上層發送 MLME-POLL.confirm 原語。

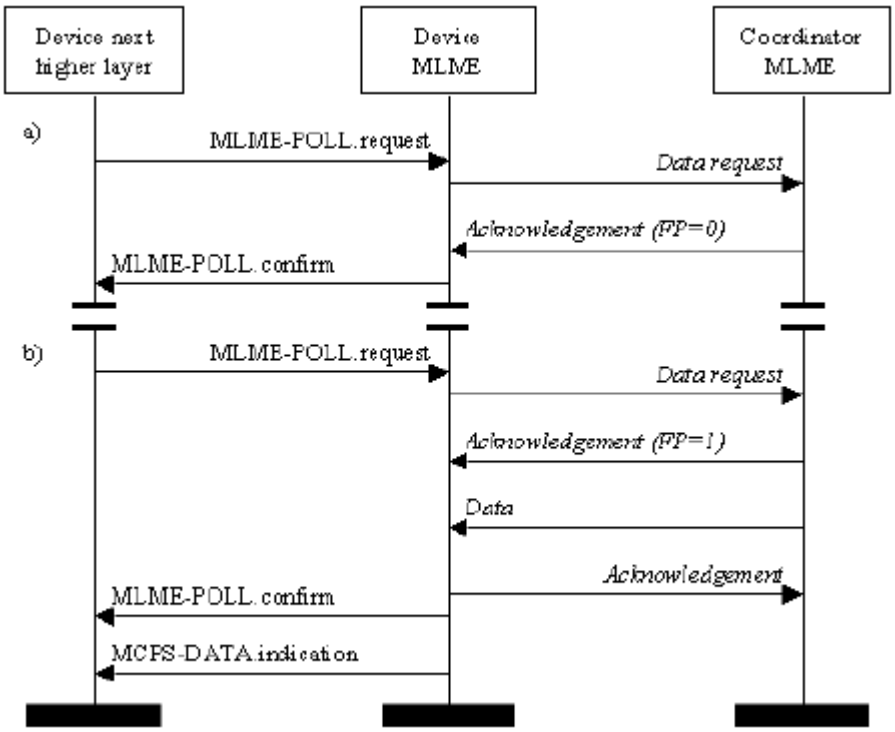


圖 16 設備向協調器請求資料的流程

3.2 MAC 層訊框(Frame)格式

3.2.1 MAC 訊框(Frame)一般格式

MAC 訊框(Frame)，即 MAC 協定資料單元（MPDU），是由一系列欄位按照特定的順序排列而成的。MAC 訊框(Frame)通常三部分：MAC 頭、MAC 有效載荷和 MAC 尾。MAC 頭部分由訊框(Frame)控制欄位、訊框(Frame)序號欄位和位址資訊域組成；MAC 有效載荷部分的長度與訊框(Frame)類型相關，確認訊框(Frame)的有效載荷部分長度爲 0；MAC 尾是訊框(Frame)校驗序列（FCS）。MAC 訊框(Frame)格式如下：

<table>
<tr><td>Octets: 2</td><td>1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>0/2/8</td><td>0/5/6/10/14</td><td>variable</td><td>2</td></tr>
<tr><td rowspan="2">Frame Control</td><td rowspan="2">Sequence Number</td><td>Destination PAN Identifier</td><td>Destination Address</td><td>Source PAN Identifier</td><td>Source Address</td><td rowspan="2">Auxiliary Security Header</td><td rowspan="2">Frame Payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Addressing fields</td></tr>
<tr><td colspan="7">MHR</td><td>MAC Payload</td><td>MFR</td></tr>
</table>

1. 訊框(Frame)控制欄位

訊框(Frame)控制欄位的長度爲 16 位，共分爲 9 個子域。訊框(Frame)控制欄位格式如下：

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	Ack. Request	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

訊框(Frame)類型子域占 3 位（$b_2b_1b_0$）：000 表示信標訊框(Frame)，001 表示資料訊框(Frame)，010 表示確認訊框(Frame)，011 表示 MAC 命令訊框(Frame)，其他取值預留。

安全致能子域佔 1 位元：0 表示 MAC 層沒有對該訊框(Frame)作加密處理；1 表示該訊框(Frame)使用了 MAC PIB 中的密鑰進行保護。

資料待傳指示佔 1 位：1 表示在當前訊框(Frame)之後，發送設備還有資料要傳送給該接收設備，接收設備需要再發送資料請求命令來索取資料；0 表示發送資料訊框(Frame)的設備沒有更多的資料要傳送給接收設備。在信標關閉的 PAN 任何時候都可以使用該指示位，而在信標致能的 PAN 中只在 CAP 期間使用；其他情況則發射設備總是置該指示位元爲 0，接受設備也不檢測該指示。

確認請求子域佔 1 位元：1 表示接收設備在接收到該資料訊框(Frame)或命令訊框(Frame)後，如果判斷其爲有效訊框(Frame)就要向發送設備回饋一個確認訊框(Frame)；0 表示接收設備不需要回饋確認訊框(Frame)。

網內/網際子域佔 1 位元元，表示該資料訊框(Frame)是否在同一個 PAN 內傳輸。如果該指示位爲 1 且存在來源位址和目的位址，則 MAC 訊框(Frame)中將不含源 PAN 標識碼欄位；如果該指示位爲 0 且存在源位址和目的位址，則 MAC 訊框(Frame)中將包含源 PAN 標識碼和目的 PAN 標識碼。

目的位址模式子域佔 2 位元（$b_{11}b_{10}$）：00 表示沒有目的 PAN 標識碼和目的位址，01 預留，10 表示目的位址是 16 位短位址，11 表示目的位址是 64 位擴充位址。如果目的位址模式爲 0 且訊框(Frame)類型域指示該訊框(Frame)不是確認訊框(Frame)或信標訊框(Frame)，則源位址模式應非零，暗指該訊框(Frame)時發送給 PAN 協調器的，PAN 協調器的 PAN 標識碼和源 PAN 標識碼一致。

源位址模式子域佔 2 位元（$b_{15}b_{14}$）：00 表示沒有源 PAN 標識碼和源位址，01 預留，10 表示源位址是 16 位短位址，11 表示源位址是 64 位擴充位址。如果源位址模式爲 0 且訊框(Frame)類型域指示該訊框(Frame)不是確認訊框(Frame)，則目的位址模式應非零，暗指該訊框(Frame)時由與目的 PAN 標識碼一致的 PAN 協調器發出的。

2. 訊框(Frame)序號欄位

序號是 MAC 層爲每訊框(Frame)制定的唯一順序標識碼，訊框(Frame)序號欄位的長度是 8 位。

信標訊框(Frame)的序號是信標序號（BSN），每個協調器的 BSN 是其 MAC PIB 屬性 macBSN 的值，macBSN 初始值爲一個亂數。構造信標訊框(Frame)時，協調器把 macBSN 值複製到訊框(Frame)序號欄位，並把 macBSN 值加 1。

資料訊框(Frame)、確認訊框(Frame)或 MAC 命令訊框(Frame)的序號是資料序號（DSN），DSN 用於確認訊框(Frame)和資料訊框(Frame)或命令訊框(Frame)的匹配。一個設備不管和幾個設備通訊，它都只支持一個 DSN。每個設備的 DSN 是存在 MAC PIB 屬性 macDSN 中的，macDSN 的初始值爲一個亂數。構造資料訊框(Frame)或命令訊框(Frame)時，設備把 macDSN 值複製到訊框(Frame)序號欄位，並把 macDSN 值加 1。

如果要求確認，接收設備就把資料訊框(Frame)或者命令訊框(Frame)的 DSN 值複製到其對應的確認訊框(Frame)DSN 欄位。如果發送設備在 macAckWaitDuration 個符號週期內沒有

收到確認訊框(Frame)，則以原 DSN 重新發送一遍資料訊框(Frame)或命令訊框(Frame)。

3. 目的 PAN 標識碼欄位

目的 PAN 標識碼欄位長度是 16 位元，它指定了訊框(Frame)的期望接收設備所在 PAN 的標識碼。該欄位值爲 0xFFFF 時表示廣播 PAN 標識碼，此時所有監聽信道的設備都把它當作有效的 PAN 標識碼。只有訊框(Frame)控制欄位中目的位址模式值不爲 0 時，訊框(Frame)結構中才存在目的 PAN 標識碼欄位。

4. 目的位址欄位

目的位址是訊框(Frame)的期望接收設備的位址。只有訊框(Frame)控制欄位中目的位址模式值非 0 時，訊框(Frame)結構中才存在目的位址欄位。不同的目的位址模式決定了目的位址欄位的長度爲 16 位元或 64 位元。該欄位值爲 0xFFFF 時表示廣播短位址，此時，所有監聽信道的設備都把它當作有效的短位址。

5. 源 PAN 標識碼欄位

源 PAN 標識碼欄位長度是 16 位元，它指定了訊框(Frame)發送設備的 PAN 標識碼。只有當訊框(Frame)控制欄位中源位址模式值不爲 0 並且網內/網際指示位等於 0 時，訊框(Frame)結構中才包含有源 PAN 標識碼欄位。一個設備的 PAN 標識碼是初始關聯到 PAN 是獲得的，但是在解決 PAN 標識碼衝突時可能會改變。

6. 源位址欄位

源位址是訊框(Frame)發送設備的位址。只有訊框(Frame)控制欄位中源位址模式值非 0 時，訊框(Frame)結構中才存在源位址欄位。不同的源位址模式決定了目的位址欄位的長度爲 16 位或 64 位。

7. 訊框(Frame)有效載荷欄位

有效載荷欄位的長度是可變的，因訊框(Frame)類型的不同而不同。如果訊框(Frame)控制欄位中的安全致能位爲 1，則有效載荷部分是受到安全機制保護的資料。

8. FCS 欄位

FCS 欄位是對 MAC 訊框(Frame)頭和有效載荷計算得到的 16 位 ITU-T CRC 序列。ITU-T 標準的 16 次 CRC 產生多項式爲：

$$G_{16}(x) = x^{16} + x^{12} + x^5 + 1$$

計算 FCS 的 CRC 演算法如下：

- 把計算校驗和的序列（MAC 訊框(Frame)頭和有效載荷）表示成二進位多項式形式，即

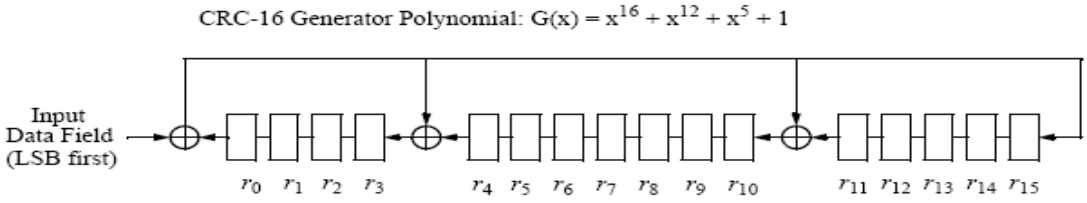
$$M(x) = b_0 x^{k-1} + b_1 x^{k-2} + \Lambda + b_{k-2} x + b_{k-1}$$

- 以產生多項式的最高次冪乘以 M（x）得到被除式 $x^{16}M$（x）
- 用 $x^{16}M$（x）模二除以產生多項式 G_{16}（x）得到餘式，即

$$R(x) = r_0 x^{15} + r_1 x^{14} + \Lambda + r_{14} x + r_{15}$$

- 餘式 R（x）的係數即爲 FCS 的值。

計算 CRC 校驗和演算法的實現方法如圖 17 所示。



1. Initialize the remainder register (r_0 through r_{15}) to zero.
2. Shift MHR and payload into the divider in the order of transmission (LSB first).
3. After the last bit of the data field is shifted into the divider, the remainder register contains the FCS.
4. The FCS is appended to the data field so that r_0 is transmitted first.

圖 17 CRC 演算法實現

3.2.2 特定 MAC 訊框(Frame)格式

3.2.2.1 信標訊框(Frame)格式

信標訊框(Frame)的格式如下：

Octets: 2	1	4/10	0/5/6/10/14	2	variable	variable	variable	2
Frame Control	Sequence Number	Addressing fields	Auxiliary Security Header	Superframe Specification	GTS fields (Figure 45)	Pending address fields (Figure 46)	Beacon Payload	FCS
MHR				MAC Payload				MFR

信標訊框(Frame)中各欄位的排列順序應和 MAC 訊框(Frame)一般格式相一致。其中 GTS 欄位和待處理位址欄位的詳細配置分別如下：

GTS 欄位格式

位元組數：1	0/1	可變長度
GTS 配置	GTS 方向	GTS 列表

待處理位址欄位格式

位元組數：1	可變長度
待處理位址配置	位址列表

1. 信標訊框(Frame)頭部分

信標訊框(Frame)頭部分包括訊框(Frame)控制欄位、信標序號欄位、源 PAN 標識欄位和源位址欄位。

訊框(Frame)控制中訊框(Frame)類型子域的值爲 000，表示信標訊框(Frame)；源位址模式子域根據一般訊框(Frame)格式中的定義設置以指示發送信標的協調器的位址；如果信標訊框(Frame)使用了安全處理，則安全致能子域置爲 1；信標訊框(Frame)控制中其他欄位均置爲 0 並且接收設備不檢測這些欄位。

信標序號欄位置爲 MAC PIB 中屬性 macBSN 的當前值。

信標訊框(Frame)的位址域僅包含源 PAN 標識和源位址，即發送信標設備的 PAN 標識和位址。

2. 超訊框(Frame)配置欄位

超訊框(Frame)配置欄位長度爲 16 位元，欄位格式如下：

比特位:0～3	4～7	8～11	12	13	14	15
信標階數	超訊框(Frame)階數	最後CAP時隙	電池壽命延長	預留	PAN 協調器	關聯與許

信標階數子域的長度是 4 位，它指定了發送信標的時間間隔。如果以“BO”表示信標階，“BI”表示信標間隔，則當 0≤BO≤14 時，信標間隔爲 BI=aBaseSuperframeDuration×2^{BO} 個符號間隔；當 BO=15 時，協調器只有在收到信標發送請求時才發送信標，其他時間不發送信標。

超訊框(Frame)階數子域的長度是 4 位，它指定了包括信標發送在內的超訊框(Frame)活動（即接收致能）時間的長度，協調器只有在活動超訊框(Frame)時才和 PAN 交付資訊。如果以“SO”表示超訊框(Frame)階，“SD”表示超訊框(Frame)活動期的長度，則當 0≤BO≤14 時，SD=aBaseSuperframeDuration×2^{SO} 個符號間隔；當 SO=15 時，表示發送完系表之後超訊框(Frame)一直處於非活動狀態。

最後 CAP 時隙欄位指定超訊框(Frame)中競爭存取週期 CAP 的最後一個超訊框(Frame)時隙，也就指定了 CAP 週期的長度。CAP 週期的長度一般不小於常數 aMinCAPLength 的值，唯一的例外是在維護 GTS 需要暫時增加信標訊框(Frame)的長度時。

電池壽命延長子域長度是 1 位，當要求在 CAP 內發送給信標產生設備的訊框(Frame)在信標訊框(Frame)間隔（IFS）之後第六個退避週期之前開始傳送時，該子域置爲 1；否則，電池壽命延長子域置爲 0。

PAN 協調器，如果發送信標的設備是 PAN 協調器，則 PAN 協調器子域置爲 1；否則，置爲 0。

關聯允許，當屬性 macAssociationPermit 的值爲 True 時，表示該發送信標的協調器允許設備關聯，此時關聯允許子域置爲 1；如果協調器當前不能接受關聯請求，則該子域置爲 0。

3. GTS 配置欄位

GTS 配置欄位長度是 8 位元，其中位 0～2 是 GTS 描述符計數器子域，位 7 是 GTS 允許子域，位 3～6 是預留部分。

GTS 描述符計數器子域指定了信標訊框(Frame)GTS 列表字段中 3 位元組 GTS 描述符的格式。如果該子域的值大於 0，則允許 CAP 長度小於常數 aMinCAPLength 以臨時增加信標訊框(Frame)的長度來容納該子域配置的內容；如果該子域爲 0，則信標訊框(Frame)中就不存在下面的 GTS 方向和 GTS 列表字段。

GTS 允許子域的值由屬性 macGTSPermit 的值來決定。如果 macGTSPermit 的屬性值爲 TRUE，表示 PAN 協調器接受 GTS 請求，此時 GTS 允許子域置爲 1；否則置爲 0。

4. GTS 方向欄位

GTS 方向欄位的長度是 8 位，其中 0～6 位是 GTS 方向遮罩子域，最後位爲預留位。GTS 方向遮罩中的每一位分別指定超訊框(Frame)中一個 GTS 的方向，最低位對應 GTS 列表字段中第一個 GTS 的方向，其他位依次類推。GTS 爲只收 GTS 時，方向遮罩中對應位置爲 1；爲只發 GTS 時，方向遮罩中對應位置爲 0。

5. GTS 列表字段

GTS 列表字段的長度由 GTS 配置欄位的相關值決定，它包含一系列描述當前分配 GTS 特徵的 GTS 描述符。列表中 GTS 描述符的個數最多爲 7 個。每個 GTS 描述符的長度是 24 位。設備短位址子域包含的是 GTS 對應設備的 16 位元短位址；GTS 開始時隙子域指定了 GTS 在超訊框(Frame)結構中的開始時隙位置；GTS 長度子域規定了該 GTS 所包含的相連超訊框(Frame)時隙數。GTS 描述符格式如下：

比特位：0～15	16～19	20～23
設備短位址	GTS 開始時隙	GTS 長度

6. 待處理位址配置欄位

待處理位址配置欄位的長度是 8 位，其中位 0～2 指示信標訊框(Frame)位址列表字段中包含的短位址個數；位 4～6 指示位址列表字段中包含的 64 位擴充位址個數；位 3 和 7 是預留位。

7. 位址列表字段

位址列表字段的長度由待處理位址配置欄位的值決定，它包含的是相關設備的位址，當前發送信標的協調器有資料等待傳送到這些設備。位址列表字段中不應包含廣播短位址 0xFFFF。

位址列表字段中短位址和擴充位址的總數最多爲 7 個，其排列順序是短位址在前，擴充位址在後。如果協調器能夠儲存 7 個以上的事務，則協調器應當以“先到先服務”的方式處理這些事務，以保證信標訊框(Frame)的位址列表中最多有 7 個位址。

8. 信標有效載荷欄位

信標有效載荷欄位是一個可選的位元組序列，它由 MAC 的上一層產生並在信標訊框(Frame)中發送，其最大長度爲 aMaxBeaconPayloadLength 個位元組。如果屬性 macBeaconPayloadLength 的值不爲 0，則把屬性 macBeaconPayload 的內容複製到信標有效載荷欄位。

如果發送的信標訊框(Frame)要求安全處理，則根據 aExtendedAddress 對應的安全套件對信標有效載荷作安全處理。如果接收訊框(Frame)控制欄位的安全致能子域爲 0，則信標載荷欄位包含的位元組序列就是要送到 MAC 上層的資料；如果安全致能子域爲 1，則設備需要根據接收訊框(Frame)源位址對應的安全套件對信標有效載荷欄位的資料作解密處理，得到期望的資料後再傳遞給 MAC 上層。

如果設備接收到的信標中存在有效載荷欄位，則先把有效載荷指示給上層然後處理超訊框(Frame)配置欄位和位址列表字段中的資訊；如果信標中無有效載荷欄位，則立即解析並處理超訊框(Frame)配置欄位和位址列表字段中的資訊。

3.2.2.2 資料訊框(Frame)格式

資料訊框(Frame)中各欄位的排列順序應和 MAC 訊框(Frame)一般格式相一致。資料訊框(Frame)的格式如下：

位元組數：2	1	可變長度	可變長度	2

訊框(Frame)控制	序號	位址資訊	資料有效載荷	FCS
MAC 頭（MHR）			MAC 有效載荷	MAC 尾（MFR）

1. 資料訊框(Frame)頭部分

資料訊框(Frame)頭部分包括訊框(Frame)控制欄位、訊框(Frame)序號欄位、目的 PAN 標識欄位、目的位址欄位和/或源 PAN 標識、源位址欄位。

訊框(Frame)控制欄位中訊框(Frame)類型子域的值爲 001，表示資料訊框(Frame)；訊框(Frame)控制欄位中其他子域的值根據具體應用作適當的設置。

資料訊框(Frame)序號欄位的值設爲屬性 macDSN 的當前值。

位址資訊欄位根據訊框(Frame)控制欄位中的不同設置，可能包含目的位址資訊（目的 PAN 標識和目的位址）和/或源位址資訊（源 PAN 標識和源位址）。

2. 資料有效載荷欄位

資料訊框(Frame)有效載荷欄位包含的是 MAC 上層要求發送的一串位元組。

如果待發送的資料訊框(Frame)要求安全處理，則根據相關安全套件對資料有效載荷進行處理。如果位址資訊部分存在目的位址域，則使用目的位址對應的安全套件；如果不存在目的位址，則採用 macCoordExtendedAddress 屬性對應的安全套件進行處理。

如果接收資料訊框(Frame)控制欄位中安全致能子域爲 0，則資料有效載荷欄位包含的位元組序列就是要傳遞給 MAC 上層的資料；如果安全致能子域爲 1，則設備需根據所選擇的安全套件對資料有效載荷欄位進行解密處理後得到期望的位元組序列再傳遞給 MAC 上層。

3.2.2.3 確認訊框(Frame)格式

確認訊框(Frame)的格式非常簡單。確認訊框(Frame)只有訊框(Frame)頭（MHR）和訊框(Frame)尾（MFR）兩部分。確認訊框(Frame)的格式如下：

位元組數：2	1	2
訊框(Frame)控制	序號	FCS
MAC 頭（MHR）		MAC 尾（MFR）

確認訊框(Frame)的訊框(Frame)頭部分只有訊框(Frame)控制欄位和訊框(Frame)序號欄位。訊框(Frame)控制欄位中訊框(Frame)類型子域的值爲 010，表示確認訊框(Frame)；待處理子域的值根據發送確認訊框(Frame)的設備是否還有後續資料等待接收而進行合理的設置；其他子域則都設爲 0 並在接收端忽略處理。

確認訊框(Frame)的序號欄位的值等於它此前接收到的並將要確認的訊框(Frame)的序號。

3.2.2.4 命令訊框(Frame)格式

命令訊框(Frame)的格式如下：

位元組數：2	1	可變長度	1	可變長度	2
訊框(Frame)控制	序號	位址資訊	命令訊框(Frame)標識	命令有效載荷	FCS
MAC 頭（MHR）			MAC 有效載荷		MAC 尾（MFR）

1. 命令訊框(Frame)頭部分

MAC 命令訊框(Frame)的訊框(Frame)頭部分包括訊框(Frame)控制欄位、訊框(Frame)序號欄位、目的 PAN 標識欄位、目的位址欄位和/或源 PAN 標識欄位、源位址欄位。

訊框(Frame)控制欄位中訊框(Frame)類型子域的值爲 011，標識 MAC 命令訊框(Frame)；其他子域則根據 MAC 命令訊框(Frame)的具體應用作合適的設置。

訊框(Frame)序號欄位設爲屬性 macDSN 的當前值。

位址資訊欄位根據訊框(Frame)控制欄位的不同設置，包含目的位址資訊和/或源位址資訊。

2. 命令訊框(Frame)標識欄位

命令訊框(Frame)標識欄位指示所使用的 MAC 命令，其取值範圍是 0x01～0x09，各取值所標識的命令如表 7 所列。

表 7 MAC 命令訊框(Frame)

命令訊框(Frame)標識	命令名稱	命令訊框(Frame)標識	命令名稱
0x01	關聯請求	0x06	孤立通知
0x02	關聯回應	0x07	信標請求
0x03	解關聯通知	0x08	協調器重排列
0x04	資料請求	0x09	GTS 請求
0x05	PAN ID 衝突通知	0x0a～0xFF	預留

3. 命令有效載荷欄位

命令有效載荷欄位包含的是命令訊框(Frame)標識所指示的具體 MAC 命令的內容。

當待發送的 MAC 命令訊框(Frame)要求安全處理時，根據相關安全套件對命令有效載荷進行處理。如果位址資訊部分存在目的位址域，則使用目的位址對應的安全套件；如果不存在目的位址，則採用 macCoordExtendedAddress 屬性對應的安全套件進行處理。

如果接收命令訊框(Frame)控制欄位中安全致能子域爲 0，則命令有效載荷欄位包含的就是 MAC 命令的內容；如果安全致能子域爲 1，則設備需根據所選擇的安全套件對命令有效載荷欄位進行解密處理後得到 MAC 命令的原始內容。

3.3 MAC 層命令訊框(Frame)

MAC 層定義的 9 種命令訊框(Frame)如表 7 所列。在關閉信標的 PAN 中任何時候都可以發送 MAC 命令訊框(Frame)，而在開啓信標的 PAN 中只有在 CAP 內才可發送 MAC 命令訊框(Frame)。下面分別介紹各種 MAC 命令訊框(Frame)的具體格式。

3.3.1 關聯和解關聯命令

關聯和解關聯命令是設備用以關聯 PAN 或 PAN 中解關聯的一組 MAC 命令，包括關聯請求、關聯相應、解關聯通知 3 種命令。

3.3.1.1 關聯請求

關聯請求命令允許設備請求和一個協調器建立關聯。關聯請求命令由一個尚未關聯的設備發出，意圖關聯到一個 PAN。設備透過掃描過程，可以關聯到一個允許關聯的 PAN 上。標準不強制要求 RFD 能接收關聯請求命令，但要求所有設備都能發送關聯請求命令。關聯請求命令的格式如下（其中省去了訊框(Frame)尾 2 位元組的 FCS 部分）：

位元組數：17/23	1	1
MAC 訊框(Frame)頭（MHR）	命令訊框(Frame)標識	功能資訊

這裡根據具體的命令訊框(Frame)把一般格式 MAC 命令訊框(Frame)頭部分的具體化。

訊框(Frame)控制欄位中源位址模式子域置爲 3（表示 64 位擴充位址）；目的位址模式子域的設置與關聯請求命令所參考的信標訊框(Frame)中指示的位址模式相一致。

如果關聯請求命令使用安全機制，則訊框(Frame)控制欄位中的安全致能子域置爲 1 並根據目的位址所對應的安全套件對命令訊框(Frame)進行處理；否則，安全致能子域置爲 0。

訊框(Frame)控制欄位中待處理訊框(Frame)子域置爲 0；確認請求子域置爲 1。

目的 PAN 標識欄位置爲設備意圖關聯的 PAN 的標識；目的位址欄位根據設備意圖關聯的協調器所發送的信標中指示的位址來設定；源 PAN 標識欄位置爲廣播 PAN 標識 0xFFFF；來源位址欄位置爲常量 aExtendedAddress 的值。

功能資訊欄位的格式如下：

比特位：0	1	2	3	4～5	6	7
備用 PAN 協調器	設備類型	電源	空閒時接收致能	預留	安全能力	分配位址

如果設備能變成 PAN 協調器，則備用 PAN 協調器子域置爲 1，否則置爲 0；如果設備是 FFD，則設備類型子域置爲 1，如果設備是 RFD，則設備類型子域置爲 0；如果設備是交流電源供電則電源子域置爲 1，否則電源子域置爲 0；如果設備在空閒週期並不關閉接收機來節省功率，則閒時接收致能子域置爲 1，否則該子域置爲 0；如果設備能否發送和接收經

安全套件處理的 MAC 訊框(Frame)，則安全能力子域置爲 1，否則該子域置爲 0；如果設備希望協調器分配一個短位址作爲關聯的結果，則分配位址子域置爲 1，如果該子域置爲 0，則特定短位址 0xFFFE 透過關聯相應命令分配給該設備，這種情況下設備和 PAN 之間的通訊只能使用 64 位擴充位址來完成。

3.3.1.2 關聯回應

協調器透過關聯回應命令把請求關聯的結果回饋給請求關聯的設備。該命令只能由協調器發送給當前嘗試關聯的設備。雖然標準不強制要求 RFD 支持發送關聯回應命令，但所有設備都必須能夠接收該命令。關聯回應命令的格式如下：

位元組數：23	1	2	1
MAC 訊框(Frame)頭（MHR）	命令訊框(Frame)標識	短位址	關聯狀態

關聯回應命令的訊框(Frame)控制欄位中目的位址模式和源位址模式都設爲 3，即表示 64 位擴充位址。如果關聯回應命令使用安全機制，則安全致能子域置爲 1 並根據目的位址對應的安全套件對該訊框(Frame)進行安全處理；否則安全致能子域置爲 0。訊框(Frame)控制欄位中待處理訊框(Frame)子域置爲 0；確認請求子域置爲 1。目的和源 PAN 標識欄位置爲屬性 macPANID 的值；目的位址欄位包含的是請求關聯設備的 64 位元擴充位址；源位址欄位包含的是常量 aExtendedAddress 的值。

短位址欄位長度是 16 位。如果協調器不能把設備關聯到 PAN，則該欄位的值爲 0xFFFF 並在關聯狀態欄位指示關聯失敗的原因；如果協調器能夠關聯該設備，則短位址欄位包含的是該請求關聯設備此後與 PAN 通訊時可使用的短位址，直到解關聯。短位址欄位值爲 0xFFFE 時，表示設備已經和 PAN 建立了關聯但沒有分配給該設備短位址，這樣，該設備與 PAN 通訊時就只能使用 64 位擴充位址。

關聯狀態欄位的取值有 3 種：0x00 表示關聯成功、0x01 表示 PAN 容量飽和、0x02 表示 PAN 存取被拒絕。

3.3.1.3 解關聯通知

協調器或關聯設備都可以發送解關聯通知命令。解關聯通知命令的格式如下：

位元組數：17	1	1
MAC 訊框(Frame)頭（MHR）	命令訊框(Frame)標識	解關聯原因

解關聯通知命令的訊框(Frame)控制欄位中目的位址模式和源位址模式都設爲 3，即表示 64 位擴充位址。如果解關聯通知命令使用安全機制，則安全致能子域置爲 1 並根據目的位

址對應的安全套件對該訊框(Frame)進行安全處理；否則安全致能子域置爲 0.訊框(Frame)控制欄位中待處理訊框(Frame)子域置爲 0；確認請求子域置爲 1.目的和源 PAN 標識欄位置爲屬性 macPANID 的值。如果協調器想要一個關聯設備離開 PAN，則目的位址欄位設爲將脫離 PAN 設備的擴充位址；如果一個 ieguanlian 設備主動要求離開 PAN，則目的位址欄位包含的是屬性 MAC CoordExtendedAddress 的值。源位址欄位包含的是常量 aExtendedAddress 的值。

解關聯原因欄位的有效取值有兩種：0x01 表示協調器要求設備離開 PAN，0x02 表示關聯設備主動要求離開 PAN。

3.3.2 協調器交互命令

協調器交互命令是一組用於設備和協調器間交互資訊的命令，它包括資料請求、PAN ID 衝突通知、孤立通知、信標請求、協調器重排列 5 種命令。

3.3.2.1 資料請求

資料請求命令由設備發送，向協調器請求資料。在信標致能 PAN 中，當設備屬性 macAutoRequest 的值爲 TRUE，並且接收到的信標訊框(Frame)指示協調器有資料待傳輸到該設備時設備向協調器發出資料請求命令。協調器透過在信標訊框(Frame)的位址列表字段中加入資料接收設備的位址來指示待處理資料。當設備的 MAC 層收到來自上層的輪詢請求原語 MLME-POLL.request 時，也要發送資料請求命令。另外，當設備收到請求命令（如關聯請求）的確認後 aResponseWaitTime 符號週期，也向協調器發出資料請求命令。資料請求命令的格式如下：

位元組數： 7/11/13/17	1
MAC 訊框(Frame) 頭（MHR）	命令訊框 (Frame)標 識

如果資料請求命令是發送給 PAN 協調器的，則訊框(Frame)控制欄位中的目的位址模式子域置爲 0；否則，根據資料請求命令指向的協調器設置爲其他值。如果設備屬性 macShortAddress 的值爲 0xFFFE 或 0xFFFF，則源位址模式子域置爲 3（即 64 位擴充位址）；否則置爲 2（即 16 位短位址）。如果資料請求命令使用安全機制，則安全致能子域置爲 1 並根據 macCoordExtendedAddress 對應的安全套件對該命令訊框(Frame)作安全處理；否則安全致能子域置爲 0。訊框(Frame)控制欄位中待處理訊框(Frame)子域置爲 0；確認請求子域置爲 1。

如果訊框(Frame)控制欄位中目的位址模式子域設爲 2，則目的 PAN 表示欄位和目的位址欄位分別是屬性 macPANID 和 macCoordShortAddress 的值。源 PAN 標識欄位包含的是屬性 macPANID 的值。如果屬性 macShortAddress 的值等於 0xFFFE（即沒有分配短位址），則來源位址欄位設爲常量 aExtendedAddress 的值；否則，源位址欄位設爲屬性 macShortAddress 的值。

3.3.2.2 PAN ID 衝突通知

當設備檢測到 PAN 標識衝突時，就向 PAN 協調器發出 PAN ID 衝突通知命令。PAN ID 衝突通知命令的格式如下：

位元組數：23	1
MAC 訊框(Frame)頭（MHR）	命令訊框(Frame)標識

PAN ID 衝突通知命令訊框(Frame)控制欄位中目的位址模式和源位址模式子域均置爲 3（即 64 位擴充位址）。發送該命令的設備要根據 macCoordExtendedAddress 對應的安全套件對該命令訊框(Frame)作安全處理。如果安全套件標識爲 0x00，則安全致能子域置爲 0；否則，安全致能子域置爲 1。訊框(Frame)控制欄位中待處理子域置爲 0；確認請求子域置爲 1. 目的 PAN 標識和源 PAN 標識欄位均置爲屬性 macPANID 的值。目的位址欄位分別是屬性 macCoordShortAddress 的值；來源位址欄位是常量 aExtendedAddress 的值。

3.3.2.3 孤立通知

當一個設備和它的協調器失步時，就發出孤立通知命令。孤立通知命令的格式如下：

位元組數：17	1
MAC 訊框(Frame)頭（MHR）	命令訊框(Frame)標識

孤立通知命令訊框(Frame)控制欄位中源位址模式子域均置爲 3（即 64 位擴充位址），目的位址模式子域置爲 2（即 16 位短位址）。發送該命令的設備要根據 macCoordExtendedAddress 對應的安全套件對該命令訊框(Frame)作安全處理。如果安全套件標識爲 0x00，則安全致能子域置爲 0；否則，安全致能子域置爲 1。訊框(Frame)控制欄位中待處理子域置爲 0；確認請求子域置爲 1。目的 PAN 標識欄位和源 PAN 標識欄位均爲廣播 PAN 標識 0xFFFF。目的位址欄位爲廣播短位址 0xFFFF；來源位址欄位爲常量 aExtendedAddress 的值。

3.3.2.4 信標請求

信標請求命令由設備在主動掃描期間用來定位其 POS 範圍內的所有協調器。該命令對 RFD 是可選支援的。信標請求命令的格式如下：

位元組數：7	1

MAC 訊框(Frame)頭（MHR）	命令訊框(Frame)標識

信標請求命令訊框(Frame)控制欄位中目的位址模式子域置爲 2（即 16 位短位址），源位址模式子域置爲 0（即沒有源位址資訊欄位）。訊框(Frame)控制欄位中待處理訊框(Frame)子域置爲 0；確認請求子域置爲 1。目的 PAN 標識欄位爲廣播 PAN 標識 0xFFFF；目的位址欄位爲廣播短位址 0xFFFF。

3.3.2.5 協調器重排列

當系統前收到其 PAN 中的孤立設備發出的孤立通知命令或協調器的任何 PAN 配置屬性發生改變時，就發出協調器重排列命令。對於前者，協調器重排列命令直接發送給孤立設備；對於後者則向 PAN 廣播協調器重排列命令，允許能接收到該命令的任何設備接收。協調器重排列命令的格式如下：

位元組數：17/23	1	2	2	1	2
MAC 訊框(Frame)頭（MHR）	命令訊框(Frame)標識	PAN 標識	協調器短位址	邏輯通道	短位址

如果協調器重排列命令是指向孤立設備的，則該命令訊框(Frame)控制欄位中目的位址模式子域置爲 3（即 64 位擴充位址）；如果該命令是向 PAN 中廣播的，則目的位址模式子域置爲 2（即 16 位短位址）。源位址模式子域置爲 3（即 64 位擴充位址）。如果指向孤立設備的協調器重排列使用安全機制，則安全致能子域置爲 1 並根據目的位址對應的安全套件對該命令訊框(Frame)作安全處理；否則安全致能子域置爲 0。訊框(Frame)控制欄位中待處理訊框(Frame)子域置爲 0。如果該命令是指向孤立設備的，則確認請求子域置爲 1；如果是向 PAN 廣播的，則確認請求子域置爲 0。目的 PAN 標識欄位爲廣播 PAN 標識 0xFFFF。如果重排列命令是指向孤立設備的，則目的位址欄位爲孤立設備的擴充位址；否則目的位址欄位爲廣播短位址 0xFFFF。源 PAN 標識欄位爲屬性 macPANID 的值；來源位址欄位爲常量 aExtendedAddress 的值。

PAN 標識欄位長度爲 16 位元，它表示協調器在此後的通訊中將使用的 PAN 新標識。

協調器短位址欄位長度爲 16 位，它包含協調器屬性 macShortAddress 的值。

短位址欄位長度爲 16 位。如果重排列命令是向 PAN 廣播的，則短位址欄位置爲 0xFFFF；如果該命令是指向孤立設備的，則短位址欄位包含的是該設備與 PAN 通訊時使用的短位址。如果該孤立設備沒有短位址而一直以擴充位址通訊，則短位址欄位置爲 0xFFFE。

3.3.3 GTS 管理命令

GTS 請求時管理 GTS 的命令，設備可使用該命令向 PAN 協調器請求分配一個新的 GTS 或撤銷一個現存的 GTS。該命令對 RFD 是可選支援的。只有具備有效短位址的設備才可以

使用 GTS 請求命令，即發送該命令的設備屬性 macShortAddress 的值不應等於 0xFFFE 或 0xFFFF。GTS 請求命令的格式如圖 18 所示。

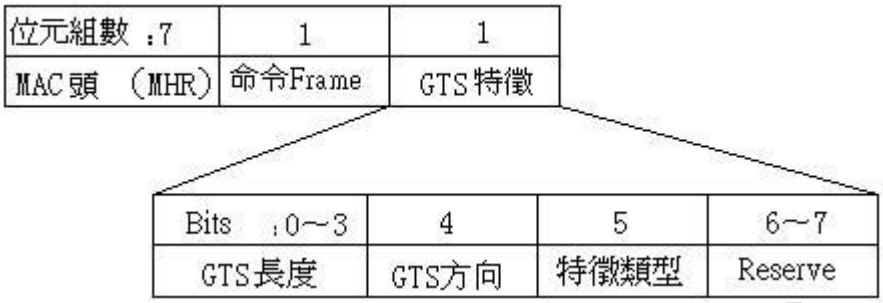


圖 18 GTS 請求命令的格式

GTS 請求命令訊框(Frame)控制欄位中目的位址模式子域爲 0（即沒有目的位址欄位），源位址模式子域爲 2（即 16 位短位址）。發送 GTS 請求命令的設備要根據 macCoordExtendedAddress 對應的安全套件對該命令訊框(Frame)作安全處理。如果安全套件標識爲 0x00，則安全致能子域置爲 0；否則，安全致能子域置爲 1。訊框(Frame)控制欄位中待處理訊框(Frame)子域置爲 0；確認請求子域置爲 1。源 PAN 標識欄位包含的是屬性 macPANID 的值；源位址欄位包含的是屬性 macShortAddress 的值。

GTS 特徵欄位的長度是 8 位。GTS 長度子域表示請求的 GTS 包含的超訊框(Frame)時隙數。GTS 方向子域爲 1 表示只收 GTS；GTS 方向爲 0 表示只發 GTS。特徵類型爲 1 表示請求分配 GTS；特徵類型爲 0 表示撤銷 GTS。

3.4 MAC 層功能描述

3.4.1 通道存取機制

3.4.1.1 超訊框(Frame)結構

PAN 中的協調器可選超訊框(Frame)結構來對通道時間進行劃分。超訊框(Frame)透過發送的信標訊框(Frame)來標定，並且一個超訊框(Frame)可分爲活動區間和非活動區間兩部分。協調器只有在活動區間才和 PAN 交互資訊，而在非活動區間則處於低功耗的睡眠模式。

超訊框(Frame)結構透過兩個屬性 macBeaconOrder 和 macSuperframeOrder 的值來描述。MAC PIB 屬性 macBeaconOrder 描述了協調器發送信標的間隔，如果用“BO”來表示 macBeaconOrder 屬性值，“BI”表示信標間隔，則當 $0 \leq BO \leq 14$ 時，$BI=aBaseSuperframeDuration \times 2^{BO}$ 個符號週期；如果 BO=15，協調器不發送信標，超訊框(Frame)結構不存在，也就不必關注 macSuperframeOrder 的屬性值了。

MAC PIB 屬性 macSuperframeOrder 描述了超訊框(Frame)中包括信標訊框(Frame)在內的活動區間的長度。如果用“SO”表示 macSuperframeOrder 屬性值，用“SD”表示超訊框(Frame)活動區間的長度，則當 $0 \leq SO \leq BO \leq 14$ 時，$SD=aBaseSlotDuration \times 2^{SO}$ 個符號週期；如果 SO=15，則超訊框(Frame)的活動區間僅僅是信標訊框(Frame)部分。

每個超訊框(Frame)的活動區間劃分成 aNumSuperframeSlots 個等間隔的時隙，時隙寬度

爲 2^{SO}xaBaseSlotDuration。超訊框(Frame)活動區間由三部分構成：信標、競爭存取週期（CAP）和無競爭週期（CFP）。信標訊框(Frame)在時隙 0 開始時發送，不使用 CSMA 機制，信標之後就是 CAP，如果存在 CFP，則 CFP 緊跟在 CAP 之後知直到活動區間結束。CFP 由所分配的 GTS 構成。

PAN 要採用超訊框(Frame)結構時應該設置 macBeaconOrder 屬性值在 0～14 之間，macSuperframeOrder 屬性值在 0 到 macBeaconOrder 值之間。如果 PAN 不採用超訊框(Frame)結構（即無信標的 PAN），則 macBeaconOrder 和 macSuperframeOrder 屬性值均設爲 15。在協調器不發送信標的 PAN 中，處理確認訊框(Frame)和緊跟在資料請求命令確認之後的資料訊框(Frame)外，所有的發送都採用無時隙的 CSMA-CA 機制來存取通道。在無信標的 PAN 中也不允許使用 GTS。

圖 19 是一個超訊框(Frame)結構的例子，其中信標間隔 BI 是超訊框(Frame)活動週期 SD 的兩倍，CFP 包含兩個 GTS。

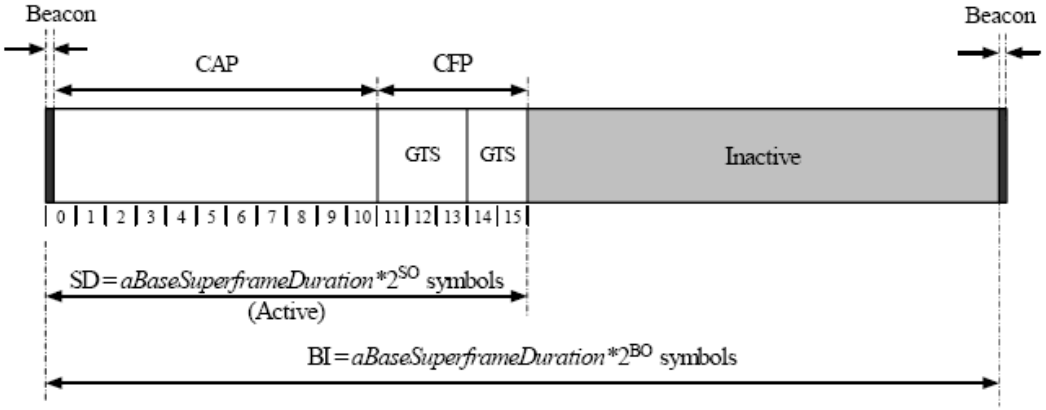


圖 19 超訊框(Frame)結構示例

在超訊框(Frame)結構中，競爭週期 CAP 開始於信標訊框(Frame)結束的時刻，並一直延續到無競爭週期 CFP 開始前的超訊框(Frame)時隙邊界。如果 CFP 長度爲 0，則 CAP 一直到超訊框(Frame)活動區間結束時刻。除非因維護 GTS 的需要而臨時增加信標訊框(Frame)的長度，CAP 的長度至少是 aMinCAPLength 個符號，並根據 CFP 長度的變化而動態地增大或縮小。

除了確認訊框(Frame)和緊跟在資料請求命令確認之後的資料訊框(Frame)外，在 CAP 內傳輸所有其他訊框(Frame)都需要採用時隙 CSMA-CA 機制來存取通道。在 CAP 內傳輸資料的設備必須保證其事務（包括接收確認訊框(Frame)）在 CAP 結束前一個訊框(Frame)間隔（IFS）完成，否則該事務就需要推遲到下一個超訊框(Frame)的 CAP 中處理。MAC 命令訊框(Frame)總是在 CAP 內發送的。

無競爭週期（CFP）緊跟 CAP 並開始於 CAP 結束後的第一個超訊框(Frame)時隙邊界，知道下一個信標的開始。PAN 協調分配的任何保證時隙（GTS）都在 CFP 中佔有連續的超訊框(Frame)時隙，因此 CFP 的長度是隨著所有 GTS 總長度的變化而變化的。CFP 內的傳輸不使用 CSMA-CA 通道存取機制，在 CFP 內傳輸資料的設備應保證當前事務在該設備分配的 GTS 結束前一個訊框(Frame)間隔（IFS）完成。

3.4.1.2 訊框(Frame)間隔（IFS）

MAC 層需要一定的時間處理來自物理層的資料，所以發送訊框(Frame)之後應預留一段空閒時間，即訊框(Frame)間隔（IFS）。如果發送訊框(Frame)需要確認，則 IFS 預留在確認訊框(Frame)之後。IFS 的長度與發送訊框(Frame)的大小有關。發送訊框(Frame)長度不超過 aMaxIFSFrameSize 時，使用長度至少爲 aMinSIFSPeriod 個符號的短訊框(Frame)間隔（SIFS）。當發送訊框(Frame)長度大於 aMaxIFSFrameSize 時，要使用長度至少爲 aMinSIFSPeriod 個符號的長訊框(Frame)間隔（LIFS）。在 CAP 內採用 CSMA-CA 演算法傳輸資料時，要考慮訊框(Frame)間隔的這些要求。圖 20 是訊框(Frame)間隔的示意圖。

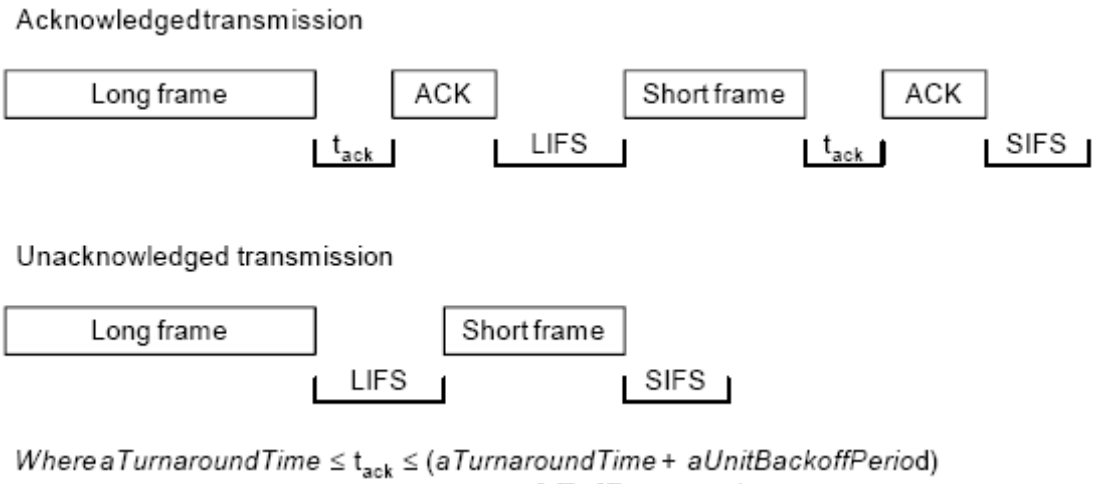


圖 20 訊框(Frame)間隔（IFS）示意圖

3.4.1.3 CSMA-CA 演算法

除了緊隨資料請求命令的確認之後能否馬上發送的訊框(Frame)，在 CAP 內發送資料訊框(Frame)和 MAC 命令訊框(Frame)之前都需要使用 CSMA-CA 演算法來存取通道。信標訊框(Frame)、確認訊框(Frame)和 CFP 內傳輸的資料訊框(Frame)不需要使用 CSMA-CA 演算法。

在使用信標的 PAN 中，MAC 層採用時隙型 CSMA-CA 演算法在 CAP 內傳輸資料。相反，如果在不使用信標的 PAN 中，或在使用信標的 PAN 中無法定位信標，則 MAC 層採用非時隙型 CSMA-CA 演算法。兩種形式 CSMA-CA 演算法的實現都要用到稱作“退避週期”的單位時間，一個退避週期等於 aUnitBackoffPeriod 個符號週期。

在時隙 CSMA-CA 演算法中，PAN 每個設備退避週期的邊界都應該與 PAN 協調器超訊框(Frame)時隙的邊界對齊，即每個設備的第一個退避週期的開始位置總是和信標的開始位置對齊的。使用時隙 CSMA-CA 演算法時，MAC 層應保證物理層的所有發送開始於退避週期的邊界處；使用非時隙 CSMA-CA 演算法時，PAN 中一個設備的退避週期在時間上與任何其他設備的退避週期是不相關的。

每個設備在每次嘗試傳輸時都需要維護 3 個變數：NB、CW 和 BE。變數 NB 是嘗試當前訊框(Frame)發送過程中 CSMA-CA 演算法執行隨機退避的次數，在每個新的傳輸嘗試之前 NB 應初始化爲 0。變數 CW 是競爭視窗的長度，它表示允許發送前要求通道連續空閒的時間（用退避週期數度量）；每次發送嘗試之前 CW 初始化爲 2，並且每次探測到通道忙時也重定爲 2.變數 CW 只用于時隙 CSMA-CA 演算法。變數 BE 是退避指數，設備試圖評估通道前退避的時間與 BE 有關。在非時隙系統或時隙系統的屬性 macBattLifeExt 的值等於 FALSE 時，BE 初始化爲 macMinBE 的屬性值；在時隙系統的屬性 macBattLifeExt 的值等於

TRUE 時，BE 初始化爲 2 和 macMinBE 屬性值中的較小者。所以如果 macMinBE 屬性值設爲 0，則 CSMA-CA 演算法第一次迭代中衝突將不可避免。雖然在 CSMA-CA 演算法的通道評估階段設備接收機處於致能狀態，但設備會丟棄這段時間收到的任何訊框(Frame)。

圖 21 是 CSMA-CA 演算法的流程。在時隙 CSMA-CA 演算法中，MAC 層首先初始化變數 NB、CW 和 BE，然後定位下一個退避週期的邊界（第①步）。在非時隙 CSMA-CA 演算法中，MAC 層初始化變數 NB 和 BE 後直接執行第②步。

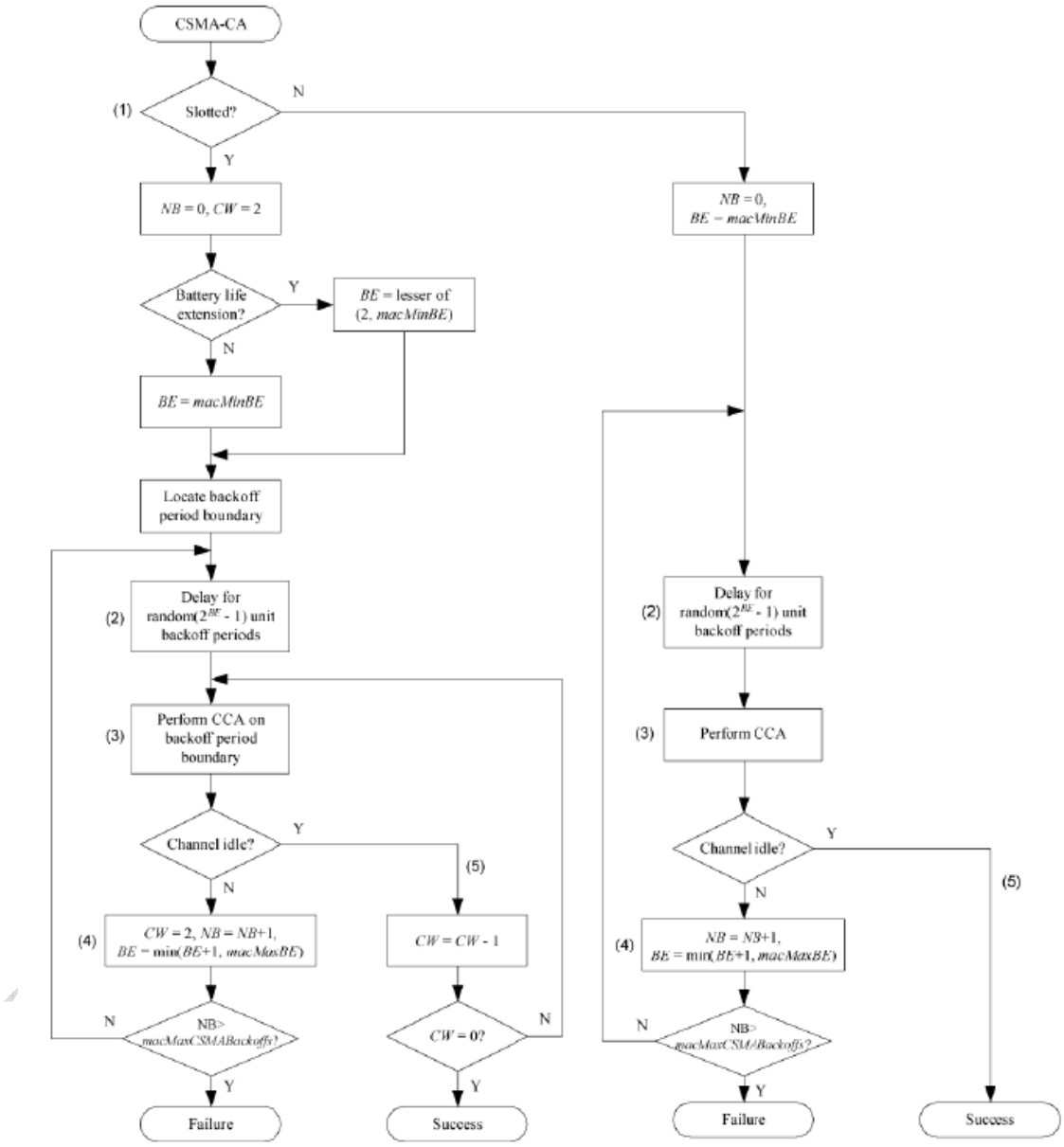


圖 21 CAMS-CA 演算法流程

MAC 層延遲亂數個完整退避週期（第②步）後，請求物理層執行通道評估（CCA）（第③步）。退避週期亂數的取值範圍是 $0 \sim 2^{BE} - 1$。在時隙 CAMS-CA 系統中，CCA 在退避週期的邊界處開始執行；而在非時隙 CSMA-CA 系統中，CCA 立即開始執行。

在時隙 CSMA-CA 中，如果電池壽命擴充子域設爲 0，MAC 層應確保在隨機退避之後 CAMS-CA 演算法的剩餘操作以及完整的傳輸事務能夠在 CAP 結束之前完成。如果退避週期數大於 CAP 剩下的時間，則 MAC 層在 CAP 結束時暫停退避遞減計數並在下一個超訊框

(Frame)的 CAP 開始時恢復 CSMA-CA 演算法的退避遞減計數。如果退避週期小於或等於 CAP 剩餘時間，則 MAC 層應執行退避延遲並評估是否可以繼續執行演算法。如果 CSMA-CA 演算法的剩餘步驟、訊框(Frame)傳輸以及任何確認訊框(Frame)都能在 CAP 結束之前完成，則可以繼續執行 CAMS-CA 演算法。如果 MAC 層能夠繼續 CSMA-CA 演算法，則請求物理層在當前超訊框(Frame)執行 CCA；如果不能繼續執行演算法，則 MAC 層等到下一個超訊框(Frame)的 CAP 開始後重新評估是否可以繼續執行 CSMA-CA 演算法。

在時隙 CSMA-CA 中，如果電池壽命擴充子域設爲 1，MAC 層應確保在隨機退避之後 CAMS-CA 演算法的剩餘操作以及完整的傳輸事務能夠在 CAP 結束之前完成。退避倒計數只在信標 IFS 週期之後的前六個完整退避週期內執行。如果 CSMA-CA 演算法的剩餘步驟、訊框(Frame)傳輸以及任何確認訊框(Frame)都能在 CAP 結束之前完成，則 MAC 層可以繼續執行 CAMS-CA 演算法，並在信標 IFS 週期之後的前六個完整退避週期中的一個開始訊框(Frame)傳輸。如果 MAC 層能夠繼續 CSMA-CA 演算法，則請求物理層在當前超訊框(Frame)執行 CCA；如果不能繼續執行演算法，則 MAC 層等到下一個超訊框(Frame)的 CAP 開始後重新評估是否可以繼續執行 CSMA-CA 演算法。

如果通道評估結果爲忙（第④步），則變數 NB 和 BE 都加 1，並保證 BE 不超過常量 aMaxBE。在時隙 CSMA-CA 演算法中還要把變數 CW 置爲 2。如果變數 NB 的值小於或等於屬性 macMaxCSMABackoffs 的值，則演算法跳轉到第②步；如果變數 NB 的值大於屬性 macMaxCSMABackoffs 的值，則 CSMA-CA 演算法結束，通道存取失敗。

如果通道評估結果爲閑（第⑤步），在時隙 CSMA-CA 系統中 MAC 層要確保在競爭視窗之後才開始傳輸資料訊框(Frame)。爲了達到這個目的，演算法把變數 CW 減 1 並判斷是否等於 0。如果 CW 不等於 0，則演算法跳轉到第③步重新執行 CCA；如果 CW 等於 0，則 MAC 層在下一個退避週期的邊界處開始發送資料訊框(Frame)。如果在非時隙 CSMA-CA 系統中通道評估結果爲閑，則 MAC 層將立即開始發送資料訊框(Frame)。

3.4.2 PAN 的建立和運行機制

3.4.2.1 通道掃描

各種類型設備都應能夠對指定的通道列表進行被動掃描和孤立掃描，FFD 則還應支持能量檢測（ED）掃描和主動掃描。上層向 MAC 層發出包含通道列表的通道掃描請求，即透過掃描請求原語 MLMA-SCAN.request 指令設備開始通道掃描。如果掃描設備在發送信標，則在通道掃描期間暫停信標發送，完成掃描後再重新開始發送信標。通道掃描結果透過證實原語 MLME-SCAN.confirm 包給給 MAC 上層。

ED 掃描使得 FFD 能夠獲知每個請求掃描通道上的峰值能量。根據 ED 掃描結果，在 PAN 建立之前一個可能的 PAN 協調器可以選擇一個合適的通道進行通訊。在 ED 掃描期間，MAC 層將丟棄物理層資料服務收到的所有訊框(Frame)。透過把掃描請求原語 MLME-SCAN.request 中的掃描類型參數 ScanTye 設爲 ED 掃描，設備將對一組指定的邏輯通道執行 ED 掃描。對列表中的每一個通道，MLME 首先透過設置 phyCurrentChannel 把設備切換到該通道；然後連續執行[aBaseSuperframeDuration×2n+1]個符號週期的 ED，其中 n 是掃描請求原語中參數 ScanDuration 的值。ED 是透過 MLME 向物理層發出能量檢測請求原語 PLME-ED.request 來實現的。掃描一個通道就記下它的峰值能量，設備所能記錄的通道

峰值能量個數是與設備實現有關的。當掃描通道數達到設備所能儲存的最大數或設備已完成對所有通道的掃描時，ED 掃描過程結束。

主動掃描使得 FFD 能夠查找其 POS 範圍內的協調器。建立新的 PAN 前，一個可能的 PAN 協調器能夠透過主動掃描選擇合適的 PAN 標識。另外，設備在關聯之前也可以用主動掃描來尋找協調器。在主動掃描期間，MAC 層將丟棄 PHY 層資料服務接收到的除信標以外的所有訊框(Frame)。主動掃描時，MAC 層先保存其當前 PAN 標識，即 macPINId 是當前值；然後把掃描期間的 macPANId 設置爲 0xFFFF，以便能夠接收到所有信標而不只是設備當前 PAN 的信標。主動掃描結束後，MAC 層應恢復掃描前保存的 macPANId 值。透過把掃描請求原語 MLME-SCAN.request 中的掃描類型參數 ScanTye 設爲主動掃描，設備就對一組指定的邏輯通道執行主動掃描。對列表中每一個通道，MLME 首先透過設置 phyCurrentChannel 吧設備切換到該通道，發出信標請求命令；然後設備致能接收機的時間最多爲[aBaseSuperframeDuration×2n+1]個符號週期，其中 n 是 0～14 間的一個值。在這段接收時間內，設備丟棄所有非信標訊框(Frame)，並以 PAN 描述符結構記錄每個唯一信標包含的資訊。如果一個信標包含的 PAN 標識和源位址是掃描該通道前沒出現過的，就認爲該信標是唯一的。設備至少能儲存一個 PAN 描述符，最多儲存個數是與設備實現有關的。對經過安全處理的信標訊框(Frame)進行分析時，忽略安全處理過程中遇到的任何錯誤，並把信標相關資訊記錄在 PAN 描述符的 SecurityUse、ACLEntry 和 SecurityFailure 欄位上。信標致能 PAN 中的協調器忽略主動掃描設備的信標請求命令，繼續按正常方式發送信標；而非信標致能 PAN 中的協調器收到信標請求命令時，就採用非時隙 CSMA-CA 演算法發送一個信標訊框(Frame)。在對一個特定通道進行掃描時，如果發現的信標達到可儲存的最大數或已經完全掃描了該通道，則中止對該通道的掃描。如果設備儲存的 PAN 描述符的個數達到最大允許值或已完成了通道列表中所有通道的掃描，則整個主動掃描過程結束。

被動掃描使得設備（包括 FFD 和 RFD）能夠查找其 POS 範圍內發送信標的協調器。與主動掃描不同的是，被動掃描設備不發送信標請求命令，只是監聽信標。設備關聯前可用被動掃描來查找周圍的協調器。被動掃描期間，MAC 層丟棄 PHY 層資料服務接收到的所有非信標訊框(Frame)。和主動掃描一樣，被動掃描開始前 MAC 層先保存 macPANId 的當前值；然後把掃描期間的 macPANId 設置爲 0xFFFF，以便能接收到所有信標而不只是設備當前 PAN 的信標。被動掃描結束後，MAC 層應恢復掃描前保存的 macPANId 值。透過把掃描請求原語 MLME-SCAN.request 中的掃描類型參數 ScanTye 設爲被動掃描，設備就對一組指定的邏輯通道執行被動掃描。對列表中的每一個通道，MLME 首先透過設置 phyCurrentChannel 把設備切換到該通道；然後啓動設備接收機最多監聽[aBaseSuperframeDuration×2n+1]個符號週期，其中 n 是 0～14 間的一個值。在這段接收時間內，設備丟棄所有非信標訊框(Frame)，並以 PAN 描述符結構記錄每個唯一信標包含的資訊。如果一個信標包含的 PAN 標識和源位址是掃描該通道前沒出現過的，就認爲該信標是唯一的。設備至少能儲存一個 PAN 描述符，最多儲存個數是與設備實現有關的。對經過安全處理的信標訊框(Frame)進行分析時，忽略安全處理過程中遇到的任何錯誤，並把信標相關資訊記錄在 PAN 描述符的 SecurityUse、ACLEntry 和 SecurityFailure 欄位上。在對一個特定通道進行被動掃描時，如果發現的信標達到可儲存的最大數或已經完全掃描了該通道，則中止對該通道的掃描。如果設備儲存的 PAN 描述符的個數達到最大允許值或已完成了通道列表中所有通道的掃描，則整個被動掃描過程結束。

孤立掃描在設備與協調器失去同步之後，用來重新查找該關聯協調器。在孤立掃描期間，MAC 層只接收協調器重排列命令訊框(Frame)，而丟棄 PHY 資料服務收到的所有其他訊框(Frame)。透過把掃描請求原語 MLME-SCAN.request 中的掃描類型參數 ScanTye 設爲孤

立掃描，設備就對一組指定的邏輯通道執行孤立掃描。對列表中的每一個通道，MLME 首先透過設置 phyCurrentChannel 把設備切換到該通道，發出孤立通知命令；然後啓動設備接收機最多監聽 aResponseWaitTime 個符號週期。在這段時間內，如果設備成功接收到協調器重排列命令就關閉接收機。一個協調器接收到孤立通知命令後，就到設備列表中查找發送命令的設備。如果協調器找到了該孤立設備的記錄，就向其發出一個協調器重排列命令。搜索設備和發送協調器重排列命令的過程應在 aResponseWaitTime 個符號週期內完成。協調器重排列命令中英包含其當前 PAN 標識 macPANId、當前邏輯通道和孤立設備的短位址。如果協調器的設備列表中沒有發送孤立通知命令的設備記錄，則不作後續的處理，也不發送重排列命令。當孤立設備接收到一個協調器重排列命令或者對通道列表中的所有通道都執行了掃描，孤立掃描過程結束。

3.4.2.2 PAN 標識衝突處理

在某些情況下，可能會有兩個 PAN 標識碼相同的網路共存於同一個 POS 範圍內。發生這種衝突時，協調器及其設備就要啓動 PAN 標識衝突處理程式。RFD 可選支援 PAN 標識衝突處理程式。

當出現下列情形之一時，PAN 協調器就認爲發生了 PAN 標識衝突：

- PAN 協調器收到一個信標訊框(Frame)中 PAN 協調器欄位等於 1，PAN 標識等於 macPANId；
- PAN 協調器收到其網內設備發出的 PAN 標識衝突通知命令。

當出現下列情形時，PAN 設備認爲發生了 PAN 標識衝突：設備接收到的信標訊框(Frame)中 PAN 協調器欄位等於 1，PAN 標識等於 macPANId，但位址既不等於 macCoordShortAddress 也不等於 macCoordExtendedAddress。

PAN 協調器檢測到 PAN 標識衝突後，首先執行主動掃描，根據通道掃描結果選擇一個新的 PAN 標識；然後發出包含 PAN 新表示的重排列命令，該命令訊框(Frame)中源 PAN 標識欄位等於 macPANId 的屬性值。一旦重排列命令發送完成，PAN 協調器就把 macPANId 的值更換成新的 PAN 標識。

PAN 中一般設備檢測到 PAN 標識衝突後，就向 PAN 協調器發出 PAN 標識衝突通知命令。如果 PAN 協調器正確接收 PAN 標識衝突命令，就向設備發出確認訊框(Frame)，並採取上述解決 PAN 標識衝突的程式。

3.4.2.3 PAN 建立

建立新的 PAN 之前，一個 FFD 透過主動掃描通道選擇一個合適的 PAN 標識，並設置屬性 macShortAddress 爲小於 0xFFFF 的值。在請求原語 MLME-START.request 的指示下，FFD 開始建立一個 PAN。此時該請求原語中 PANCoordinator 參數爲 TRUE，CoordRealigment 參數爲 FASLE。FFD 的 MAC 層接收到請求原語後，把 phyCurrentChannel 屬性值設置爲原語中的邏輯通道，把 macPANId 屬性值設置爲原語中的 PAN 標識。完成這些操作後，MAC 層就透過證實原語 MLME-START.confirm 向其上層報告建立 PAN 的結果，此後該 FFD 就以一個 PAN 協調器的身份開始工作。

3.4.2.4 信標產生

一個設備僅當其 macShortAddress 屬性不等於 0xFFFF 時才允許發送信標訊框(Frame)。FFD 使用請求原語 MLME-START.request 來實現信標發送，根據原語中 PANCoordinator 參數的不同設置，發送信標的 FFD 可以是新建網路的 PAN 協調器，也可以是已建 PAN 的設備。收到請求原語後，MAC 層把屬性 macPANId 的值置爲原語參數 PAN identifier 的值，並把該參數值用作信標訊框(Frame)中的源 PAN 標識欄位。如果屬性 macShortAddress 等於 0xFFFE，則信標訊框(Frame)來源位址欄位爲常量 aExtendedAddress 的值；否則，源位址欄位爲屬性 macShortAddress 的值。

最近一個信標訊框(Frame)的發送時間記錄在屬性 macBeaconTxTime 中，該時間值應該處於每個信標訊框(Frame)中相同的符號邊界處。該符號邊界應和收到信標的時間戳使用的符號邊界一樣。

所有信標訊框(Frame)都在超訊框(Frame)的開始時刻發送，信標間隔是 aBaseSuperframeDuration×2^{BO} 個符號週期。信標的發送優先順序高於任何其他的發送和接收操作。

3.4.2.5 設備發現

一個 FFD 可以透過發送信標來向 PAN 中的其他設備聲明其存在，這就幫助其他設備完成了設備發現功能。

一個不是 PAN 協調器的 FFD 在成功關聯到 PAN 後開始發送信標訊框(Frame)。該 FFD 的信標發送是使用 MLME-START.request 原語來實現的，原語參數 PANCoordinator 的值是 FALSE。收到上層的請求原語後，MLME 使用設備已關聯網路的 PAN 標識 macPANId 和短位址 macShortAddrss 開始發送信標，信標間隔是 aBaseSuperframeDuration×2^{BO} 個符號週期。

3.4.3 關聯和解關聯

3.4.3.1 關聯

線上執行 MAC 層復位（透過 MLME-RESET.request 原語）再進行主動通道掃描或被動通道掃描後，設備就嘗試關聯操作。通道掃描的結果用以選擇一個合適的 PAN。一個協調器僅當其屬性 macAssociationPermit 值爲 TRUE 時才允許關聯，所以設備要根據通道掃描的結果選擇合適的協調器進行關聯嘗試。一個不允許關聯的協調器收到設備的關聯請求命令時不會作任何回應。

設備選定關聯 PAN 後，上層就會請求 MLME 配置關聯過程必需的幾個 PHY 層和 MAC 層 PIB 屬性值：

- phyCurrentChannel 屬性設置爲要關聯的邏輯通道；
- macPANId 屬性設置爲要關聯的 PAN 的標識碼；
- 根據要關聯的協調器的信標訊框(Frame)的指示，把 macCoordExtendedAddress 或

macCoordShortAddress 屬性設置爲適當的值。

爲了優化信標致能 PAN 中的關聯過程，設備可以事先跟蹤意圖關聯協調器的信標。這種優化操作透過設置同步請求原語 MLME-SYNC.request 中的 TrackBeacon 參數值爲 TRUE 來實現。透過關聯請求原語 MLME-ASSOCIATE.request 的指令執行關聯操作的設備會嘗試關聯到一個現存的 PAN 中，而不會試圖建立自己的 PAN。

一個尚未關聯的設備關聯過程是首先向一個現存 PAN 中的協調器發出關聯請求命令，如果協調器正確接收到了關聯請求命令就回饋一個確認訊框(Frame)。協調器發出的關聯請求確認並不表示設備已經關聯，協調器需要時間判決 PAN 當前的資源能否允許一個設備關聯，並且愛 aResponseWaitTime 個符號週期內作出決定。如果協調器發現請求關聯的設備是 PAN 以前的一個關聯設備，則刪除與該設備有關的一切資訊。如果有足夠的系統資源，協調器就給請求關聯設備一個短位址並發出關聯回應命令，關聯回應命令中包含有新位址和表示關聯成功的狀態資訊。如果沒有足夠的系統資源，協調器就向設備發出攜帶有關聯失敗狀態資訊的關聯回應命令。關聯回應命令以間接傳輸的方式發送給請求關聯的設備，即把關聯回應命令訊框(Frame)添加在協調器的待處理事務列表中，由設備來探測和獲取。

如果關聯請求命令中功能資訊欄位的分配位址位元是 1，則協調器根據表 8 所列的取值範圍分配給設備一個 16 位元短位址；如果分配位址位是 0，則協調器分配給請求關聯設備的短位址是 0xFFFE，表示設備關聯成功但是沒有分配有效的短位址，設備在網路中的通訊只能使用 64 位擴充位址。

表 8 短位址的使用

macShortAddress 取值	描　　述
0x0000～0xFFFD	設備可以使用短位址模式
0xFFFE	設備只能使用 64 位元擴充位址 aExtendedAddress
0xFFFF	設備尚未關聯

收到關聯請求命令的確認後，設備最多等待 aResponseWaitTime 個符號週期，以便協調器作出關聯決定。如果設備跟蹤信標，則一旦信標訊框(Frame)中指示協調器發出了關聯回應命令，設備就可以隨時提取；如果設備沒有跟蹤信標，則設備在 aResponseWaitTime 各符號週期後會嘗試提取關聯回應命令。如果設備不能從協調器獲得關聯回應命令訊框(Frame)，就向 MAC 上層發出狀態爲 NO_DATA 的關聯證實原語 MLME-ASSOCIATE.confirm，關聯嘗試失敗。此時，MAC 上層應中止對任何信標的跟蹤。

收到關聯響應命令後，請求關聯設備回饋一個確認訊框(Frame)。如果關聯回應命令的關聯狀態指示關聯成功，則設備保存關聯協調器的位址資訊。透過關聯前的通道掃描，從原始信標中得到的協調器短位址保存到設備的 macCoordShortAddress 屬性中；從關聯回應命令訊框(Frame)頭部分得到的協調器擴充位址保存到設備的 macCoordExtendedAdress 屬性中。設備也要把關聯回應命令訊框(Frame)中短位址欄位的內容，即協調器分配給請求關聯設備的短位址，保存到 macShortAdress 屬性中。如果關聯狀態欄位指示關聯不成功，則設備設置 macPANId 屬性爲缺省值 0xFFFF。

3.4.3.2 解關聯

解關聯過程由 MAC 上層向 MLME 發出的解關聯請求原語

MLME-DISASSOCIATE.request 來啓動。

當協調器想要一個關聯著的設備離開 PAN 時，就以間接傳輸方式向該設備發送解關聯通知命令，即把解關聯通知命令添加在協調器的待處理事務列表中，等待設備來提取。如果設備向協調器請求並正確接收到瞭解關聯通知命令，就向協調器發出確認訊框(Frame)。即便協調器沒有收到解關聯通知命令的確認，它也解關聯該設備。當一個關聯設備想離開 PAN 時，就向它的協調器發出解關聯通知命令。協調器正確收到設備的解關聯通知命令後，回饋一個確認訊框(Frame)。即使沒有收到確認訊框(Frame)，設備也認爲自身解關聯。

如果解關聯通知命令中的源位址等於 macCoordExtendedAddress 屬性值，接收到命令的設備就解關聯了。如果一個協調器接收到解關聯通知命令，並且源位址不等於 macCoordExtendedAddress 屬性值，協調器就查證該源位址是否是其關聯設備的位址；如果是一個設備的位址，則協調器認爲該設備解關聯了。如果上述兩種情況中的任何一種，則該命令誂忽略。一個設備透過刪除它與 PAN 有關的所有資訊來達到自身解關聯；協調器則透過刪除與一個設備相關的所有資訊來使得該設備解關聯。請求設備透過發送解關聯證實原語 MLME-DISASSOCIATE.confirm 來向其 MAC 上層報告解關聯操作的結果。

3.4.4 PAN 同步機制

同步問題主要涉及的是協調器產生信標訊框(Frame)的過程和設備與協調器保持同步的過程。在支持信標的 PAN 中，同步透過接收和解析信標訊框(Frame)來實現；在不支持信標的 PAN 中，同步透過向協調器輪詢資料來實現。

3.4.4.1 支援信標的 PAN 同步

支援信標的 PAN（即 macBeaconOrder＜15）中的設備，爲了檢測待收資料或跟蹤信標，應能夠捕獲信標同步。設備只允許對信標中的 PAN 標識等於 macPANId 的信標進行信標同步。如果設備的 macPANId 屬性等於廣播 PAN 標識 0xFFFF，則不會嘗試捕獲信標同步。

設備捕獲信標的過程透過同步請求原語 MLME-SYNC.request 來啓動。如果 MLME-SYNC.request 原語的參數設定爲跟蹤信標，則設備將嘗試捕獲信標並透過有規律的啓動接收機來跟蹤信標。如果原語參數設定爲不跟蹤信標，則設備將只作一次捕獲信標的嘗試或在下一個信標之後停止跟蹤。

爲了捕獲信標，設備將開啓接收機，最多偵聽 aBaseSuperframeDuration×2^{BO} 個符號週期。如果在這段時間內沒有收到攜帶設備當前 PAN 標識的信標，MLME 重複偵聽過程。一旦丟失的信標數達到 aMaxLostBeasons，MLME 就向 MAC 上層發出失步原因爲信標丟失（BEACON_LOSS）的失步指示原語 MLME-SYNC-LOSS.indication。

MLME 在每訊框(Frame)相同的符號邊界處爲每個接收到的信標訊框(Frame)打上時間戳。選爲時間戳的符號邊界應和發送信標的時間戳相同，並保存在 macBeaconTxTime 屬性中。

如果安全致能子域等於 1，那麼 MLME 將對接收到的信標訊框(Frame)作相應的安全處理。如果安全處理失敗，就丟棄該訊框(Frame)，MLME 發出 MLME-COMM-STATUS.indication 原語來指示這個錯誤。

如果接收到一個信標訊框(Frame)，設備需要判斷該信標是否來自其關聯的協調器。如

果信標訊框(Frame)頭部分的源位址的源 PAN 標識欄位的內容與協調器的源位址和設備的 PAN 標識不相符，則 MLME 丟棄該信標訊框(Frame)。

如果接收到有效的信標訊框(Frame)並且 macAutoRequest 屬性值爲 FALSE，MLME 將透過信標通知指示原語 MLME-BEACON-NOTIFY.indication 向其上層報告信標參數。當接收到有效的信標訊框(Frame)並且 macAutoRequest 屬性值爲 TRUE，如果信標訊框(Frame)中含有有效載荷，則 MLME 先向上層發出 MLME-BEACON-NOTIFY.indication 原語，然後比較信標訊框(Frame)位址列表中的位址。如果信標訊框(Frame)位址列表中包含有設備的短位址或擴充位址，並且源 PAN 標識與設備的 macPANId 相同，MLME 將啓動從協調器中提取資料的程式。

如果啓動了信標跟蹤，MLME 每次在下一個信標訊框(Frame)發送，即下一個超訊框(Frame)開始之前，開啓接收機。如果連續丟失的信標數達到 aMaxLostBeacons，MLME 就向 MAC 上層發出失步原因爲信標丟失（BEACON_LOSS）的失步指示原語 MLME-SYNC-LOSS.indication。

3.4.4.2 不支援信標的 PAN 同步

不支援信標的 PAN（即 macBeaconOrder=15）中的設備在 MAC 上層的控制下，向協調器輪詢資料。當 MLME 收到輪詢請求原語 MLME-POLL.request 時，就指令設備向協調器輪詢，啓動向協調器索取資料的程式。

3.4.4.3 孤立設備重排列

如果 MAC 上層請求發送資料時連續多次收到通訊失敗的指示，它就可能認爲該設備已經被孤立了。當一個設備事務沒有到達協調器時，即重複發送資料 aMaxFrameRetries 次都沒有收到確認訊框(Frame)，稱作“一次通訊失敗”。當 MAC 上層斷言設備已經孤立時，它指示 MLME 要麼啓動孤立設備重排列程式，要麼重定 MAC 層然後執行關聯操作。

如果 MAC 上層決定執行孤立設備重排列程式，就發出 ScanType 參數爲孤立掃描的掃描請求原語 MLME-SCAN.request。MAC 層接收到掃描請求原語後就開始孤立通道掃描。如果孤立掃描成功，即找到了 PAN，設備就根據協調器重排列命令中攜帶的 PAN 資訊來更新 MAC PIB；如果孤立掃描失敗，MAC 上層將決定採取進一步的措施，如重新掃描或重新關聯。

3.4.5 事務處理

因爲 IEEE 802.15.4 標準支援非常低成本的設備，這種設備通常是由電池供電俄。這種功率受限的設備可能要求由設備來觸發傳輸事務而不是協調器。換句話說，要麼當協調器中有資料等待設備接收時就在信標中指示，要麼需要設備自身輪詢協調器以探測是否有資料要接收。這兩種傳輸方式稱作“間接傳輸”。

當協調器收到資料請求原語或收到來自 MLME 的發送 MAC 命令請求，如關聯回應原語，就開始處理接收間接傳輸請求的事務。事務處理完成後，MAC 層要向其高層指示一個

狀態值。如果是請求原語啓動的間接傳輸，則相應的證實原語用來傳遞狀態資訊；相反，如果是回應原語啓動的間接傳輸，則用通訊狀態指示原語 MLME-COMM-STATUS.indication 來傳遞狀態資訊。

包含在間接傳輸請求中的資訊構成了一個事務，協調器至少能夠儲存一個事務。當接收到間接傳輸請求時，如果協調器沒有足夠的空間來儲存事務，則 MAC 層向其上層發出狀態爲 TRANSACTION_OVERFLOW（事務溢出）的 MLME-COMM-STATUS.indication 原語。

如果協調器能夠儲存多個事務，則同一個設備的多個事務應該按照它們到達 MAC 層的先後順序發送。每發送一個事務，如果列表中還有同一設備的其他事務，則 MAC 層置待處理訊框(Frame)子域爲 1，表示協調器中還有資料等待該設備接收。

每個事務在協調器中駐留的時間最多爲 macTransactionPersistenceTime。如果事務在這個時間內沒有白相應的設備取走，則事務資訊將被廢棄，並且 MAC 層向其上層發出狀態爲 TRANSACTION_EXPIRED（事務過期）的 MLME-COMM-STATUS.indication 原語。

如果協調器發送信標，它就把每個事務關聯的位址存放在信標訊框(Frame)的位址列表字段中，把總的位址數存放在待處理位址配置欄位中。如果協調器能夠儲存 7 個以上的事務，則它以“先到先服務”的原則在信標中指示這些事務，以保證信標訊框(Frame)位址列表中最多只有 7 個位址。對要求 GTS 的事務，PAN 協調器不應把它的位址加入信標訊框(Frame)位址列表中，而是在分配給相應設備的 GTS 上傳輸這些事務。

在支援信標的 PAN 中，當設備接收到的信標訊框(Frame)的位址列表中有該設備的位址時，設備將向協調器索取資料。在不支持信標的 PAN 中，當接收到輪詢請求原語 MLME-POLL.request 時，設備就嘗試向協調器索取資料。

事務處理完成後，從協調器儲存空間中刪除事務相關資訊，並向 MAC 上層報告資料傳輸的結果。如果事務要求確認但沒有收到確認，則 MAC 層指示狀態爲 NO_ACK；如果事務傳輸成功，則 MAC 層指示狀態爲 SUCCESS。

3.4.6 訊框(Frame)的傳輸

3.4.6.1 發送

每產生一個資料訊框(Frame)或 MAC 命令訊框(Frame)時，MAC 層就拷貝 macDSN 的值到訊框(Frame)頭（MHR）的序號欄位中，並把 macDSN 加 1。類似的，每產生一個信標訊框(Frame)時，MAC 層拷貝 macBSN 的值到 MHR 的序號欄位中，並把 macBSN 加 1。

訊框(Frame)結構中源位址欄位包含的是發送設備的位址。當一個關聯設備已經分配了短位址（即 macShortAddress 不等於 0xFFFE 或 0xFFFF）時，盡可能使用短位址而不使用 64 位擴充位址（即 aExtendedAddress）。當設備尚未關聯到一個 PAN 或設備屬性 macShortAddress 等於 0xFFFE 時，設備只能使用 64 位元擴充位址來通訊。如果 MHR 中不存在來源位址欄位，則訊框(Frame)的發送設備是 PAN 協調器，目的位址欄位是訊框(Frame)接收設備的位址。如果目的位址欄位不存在，則訊框(Frame)接收設備是 PAN 協調器，源位址欄位是訊框(Frame)發送設備的位址。

如果 MHR 中目的位址資訊和源位址資訊都存在，MAC 層將比較目的 PAN 標識和源 PAN 標識。如果兩個 PAN 標識相同，則訊框(Frame)控制欄位中網內/網際子域置爲 1，並在發送訊框(Frame)中省略源 PAN 標識欄位。如果兩個 PAN 標識不同，則訊框(Frame)控制欄

位中網內/網際子域置爲 0，發送訊框(Frame)源 PAN 標識欄位和目的 PAN 標識欄位都存在。

如果在支援信標的 PAN 中發送訊框(Frame)，發送之前設備將嘗試捕獲信標。如果設備沒有跟蹤信標，不知道它出現的時刻，設備將啓動接收機來尋找信標。如果在規定的時限內設備沒有找到信標，就採用非時隙型 CSMA-CA 演算法把訊框(Frame)發送出去；如果設備找到了信標，則在超訊框(Frame)的適當時刻把訊框(Frame)發送出去。在超訊框(Frame)的 CAP 內發送訊框(Frame)時採用時隙型 CSMA-CA 演算法存取通道，在 GTS 上發送訊框(Frame)時不使用 CSMA-CA 演算法。

在不支援信標的 PAN 中發送訊框(Frame)時，採用非時隙型 CSMA-CA 演算法存取通道。

3.4.6.2 接收和拒絕

每個設備可以根據需要選擇在空閒期間是否打開接收機。空閒期間 MAC 層仍要處理來自上一層的收發任務請求，收發任務請求是指包括接收確認在內的發送請求或接收請求。每處理完一個收發任務，MAC 層根據 macRxOnWhenIdle 的屬性值請求 PHY 層開啓或關閉接收機：如果 macRxOnWhenIdle 等於 TRUE，空閒期間接收機打開；如果 macRxOnWhenIdle 等於 FALSE，接收機關閉。如果 macBeaconOrder 小於 15，則只在 CAP 的空閒階段考慮 macRxOnWhenIdle 的屬性值。

由於無線通訊通道的開放特性，設備接收機開啓時將接收到 POS 範圍內、工作在同一通道上、遵循 IEEE802.15.4 標準的所有設備的發送訊框(Frame)，以及其他干擾信號；因此，MAC 層要能夠對接收訊框(Frame)進行過濾，只把有用的訊框(Frame)遞交給上層。MAC 層的第一級過濾是採用 CRC 校驗演算法，丟棄訊框(Frame)尾（MFR）FCS 欄位的校驗值錯誤的那些接收訊框(Frame)。MAC 層的第二級過濾與其是否工作在混雜模式有關：如果工作在混雜模式（即 macPromiscuousMode 等於 TRUE），則 MAC 層不再作進一步的過濾，把第一級過濾後的所有訊框(Frame)直接遞交給上層；如果工作在非混雜模式（即 macPromiscuousMode 等於 FALSE），則 MAC 層保留同時滿足下面這些的訊框(Frame)：

- 訊框(Frame)控制欄位的訊框(Frame)類型子域沒有非法的訊框(Frame)類型值；
- 訊框(Frame)類型指示爲信標訊框(Frame)時，如果 macPANId 不等於 0xFFFF，源 PAN 標識應和 macPANId 值一致（macPANId 等於 0xFFFF 時，不管源 PAN 標識，設備接收所有信標訊框(Frame)）；
- 如果訊框(Frame)中包含有目的 PAN 標識，則它應與 macPANId 的值一致或等於廣播 PAN 標識 0xFFFF；
- 如果訊框(Frame)中包含有短目的位址，則它應與 macShortAddress 的值一致或等於廣播短位址 0xFFFF；如果目的位址是擴充位址，則它應與 aExtendedAddress 常量值一致；
- 如果一個資料訊框(Frame)或 MAC 命令訊框(Frame)中只有源位址資訊，則只有接收設備爲 PAN 協調器並且源 PAN 標識等於 macPANId 值時，才保留該訊框(Frame)。

如果上述任何一個條件不滿足，MAC 層將丟棄相應的訊框(Frame)。只有這些條件都滿足時，MAC 層才把該訊框(Frame)當作有效訊框(Frame)，並作進一步處理。對接收到的有效訊框(Frame)，如果訊框(Frame)類型欄位指示爲一個資料訊框(Frame)或 MAC 命令訊框(Frame)，並且確認請求欄位等於 1，則 MAC 層要發送一個確認訊框(Frame)。在構造確認訊框(Frame)時，把接收的資料訊框(Frame)或 MAC 命令訊框(Frame)中序號欄位的內容複製到相應確認訊框(Frame)序號欄位中，使事務發起方知道這是對哪個訊框(Frame)的取而。

如果接收訊框(Frame)的安全致能子域等於 1，則 MAC 層對接收訊框(Frame)作相應的安全處理。在主動掃描或被動掃描信標時，即使信標訊框(Frame)的安全處理出錯，信標中包含的資訊也存到 PAN 描述符中，遞交給 MAC 上層。

如果訊框(Frame)控制欄位中網內/網際子域等於 1（即網內傳輸），並且源位址和目的位址欄位都存在時，MAC 層認爲省略了的源 PAN 標識欄位內容等於訊框(Frame)中的目的 PAN 標識欄位。

成功處理訊框(Frame)後，MAC 調用資料指示原語 MCPS-DATA.indication，把訊框(Frame)資訊傳遞給 MAC 上層。

3.4.6.3 從協調器提取資料

支援信標的 PAN 中的設備透過檢測信標中的位址列表字段，可以知道協調器中是否有資料要傳送給它。如果設備位址出現在信標的位址列表中，設備 MLME 就在 CAP 內向協調器發出資料請求命令，資料請求命令訊框(Frame)的確認請求欄位設爲 1。另外還有兩種情況設備會向協調器發出資料請求命令：第一種情況是當 MLME 收到輪詢請求原語 MLME-POLL.request 時；第二種情況是在收到一個請求命令的確認（如關聯過程）aResponseWaitTime 個符號週期後，設備可能發送資料請求命令。資料請求命令只要不是指向 PAN 協調器，都應包含目的位址資訊。

成功接收資料請求命令後，協調器將回饋一個確認訊框(Frame)。如果協調器有足夠的時間來判斷是否有資料等待傳送給請求設備，並且能夠在 macAckWaitDuration 個符號週期內發出資料請求的確認訊框(Frame)，則協調器根據判斷結果設置確認訊框(Frame)的待處理訊框(Frame)欄位（“1”表示有資料待傳，“0”表示沒有資料），告知請求設備是否有資料。如果協調器在發送確認訊框(Frame)前沒有足夠時間作出判斷，則設置待處理訊框(Frame)欄位爲 1。

如果接收到資料請求命令的確認訊框(Frame)中的待處理訊框(Frame)欄位爲 0，則設備認爲協調器中沒有它的資料；如果確認訊框(Frame)中的待處理訊框(Frame)欄位爲 1，設備就啓動接收機以便接收來自協調器的資料訊框(Frame)。在支援信標 PAN 中，設備接收機最多開啓 aMaxFrameResponseTime 個 CAP 符號週期，在不支援信標 PAN 中，設備最多開啓 aMaxFrameResponseTime 個符號週期。如果協調器中確實有請求設備的資料，協調器就把資料訊框(Frame)發送給請求設備；如果協調器中沒有請求設備的資料，協調器就向設備發出一個有效載荷爲空的不需確認的資料訊框(Frame)。協調器在確認資料請求命令後，向請求設備發送資料訊框(Frame)的機制有兩種：

1. 不使用 CSMA-CA 機制。如果協調器 MAC 層能夠在確認後的回退時隙邊界處開始發送資料訊框(Frame)，則訊框(Frame)長在 aTurnaroundTime 到 aTurnaroundTime + aUnitBackoffPeriod 個符號之間，並且 CAP 有足夠的剩餘時間用於發送資料、預留 IFS 和接收確認。如果協調器沒有收到傳輸該資料訊框(Frame)要求的確認，則此後該資料的重傳都要使用 CSMA-CA 機制。

2. 其他情況使用 CSMA-CA 機制。如果請求設備在最大等待時限內沒有接收到協調器發出的資料訊框(Frame)，或者接收到的資料訊框(Frame)有效載荷長度爲 0，則設備認爲協調器中沒有它的資料；如果請求設備收到協調器的資料訊框(Frame)要求確認，則設備回饋一個確認訊框(Frame)。如果設備從協調器接收到的資料訊框(Frame)的訊框(Frame)控制欄位中待處理訊框(Frame)子域等於 1，則表示協調器中還有該設備的資料。此時設備可以再次發

送一個新的資料請求命令，用上述同樣的程式繼續向協調器索取資料。

3.4.6.4 確認

發送資料訊框(Frame)或 MAC 命令訊框(Frame)時，根據需要可以設置訊框(Frame)控制欄位中的確認請求子域爲 1 或 0；而信標訊框(Frame)和確認訊框(Frame)中該欄位總設爲 0。另外，任何廣播訊框(Frame)的確認請求子域也設爲 0。

發送訊框(Frame)的確認請求子域等於 0 時，不要求接收設備，發送設備發出訊框(Frame)就認爲發送成功。圖 22 是發送不需確認的資料訊框(Frame)的資訊流程，其中 AR=0 表示確認請求子域等於 0。

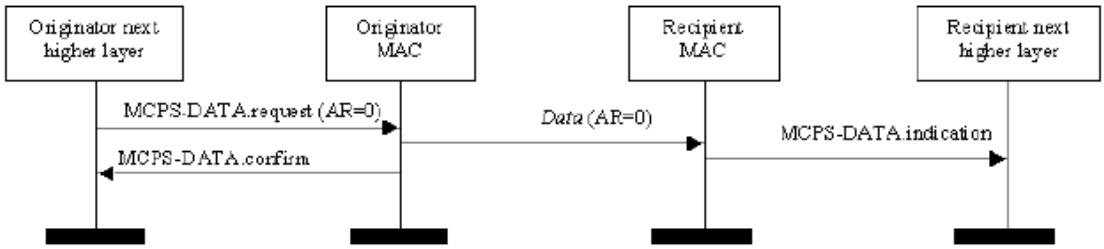


圖 22 無確認的資料訊框(Frame)成功發送

發送訊框(Frame)的確認請求子域等於 1 時，要求接收設備在接收到該訊框(Frame)後作出確認。接收設備正確接收到要求確認的訊框(Frame)後，向發送設備回饋一個確認訊框(Frame)。確認訊框(Frame)的 DSN 等於它所確認的資料訊框(Frame)或 MAC 命令訊框(Frame)的 DSN。

在不支援信標的 PAN 中或在超訊框(Frame)結構的 CFP 內，在接收到資料訊框(Frame)或者 MAC 命令訊框(Frame)後 aTurnarounTime 個符號週期，確認訊框(Frame)開始發送。在超訊框(Frame)的 CAP 內，確認訊框(Frame)的發送時刻位於退避時隙的邊界處，發送確認訊框(Frame)的開始時刻在收到資料訊框(Frame)或 MAC 命令訊框(Frame)後 aTurnarounTime 個符號週期到 aTurnaroundTime + aUnitBackoffPeriod 個符號週期之間。

圖 23 是發送要求確認的資料訊框(Frame)的資訊流程，其中 AR=1 表示確認請求子域等於 1。

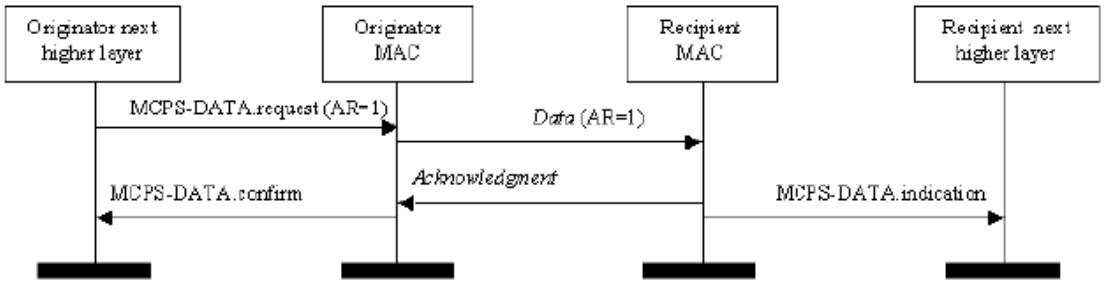


圖 23 有確認的資料訊框(Frame)發送成功

3.4.6.5 重傳

訊框(Frame)發送設備如果把訊框(Frame)控制欄位中確認請求子域設爲 0，則認爲發送的訊框(Frame)都被成功接收，所以也就不需要重傳程式；如果設備發送資料訊框(Frame)或 MAC 命令訊框(Frame)時訊框(Frame)控制欄位中確認請求子域設爲 1，則發送完成後設備等待接收相應的確認訊框(Frame)。如果在 macAckWaitDuration 個符號週期的時限內，訊框(Frame)發送設備收到了一個確認訊框(Frame)，並且該確認訊框(Frame)的 DSN 與發送訊框(Frame)的 DSN 相同，則表示訊框(Frame)發送成功；如果在這個時限內訊框(Frame)發送設備沒有收到確認訊框(Frame)或確認訊框(Frame)的 DSN 與發送訊框(Frame)的 DSN 不一致，則表示訊框(Frame)發送失敗。

如果間接傳輸的一次訊框(Frame)發送失敗，協調器並不重傳失敗的資料訊框(Frame)或 MAC 命令訊框(Frame)，而是繼續放在協調器的事務排隊中。如果直接傳輸的一次訊框(Frame)發送失敗，設備將重新發送資料訊框(Frame)或命令訊框(Frame)，最多可以重傳 aMaxFrameRetries 次。超訊框(Frame)結構中的每次重傳必須在相同時間段內完成，如 CAP 或失敗傳輸時使用的 GTS。如果重傳操作不能在 CAP 結束前完成或不能在當前 GTS 內完成，則整個重傳過程推遲到下一個超訊框(Frame)對應的 CAP 或 GTS 內重新嘗試。如果一個資料訊框(Frame)或 MAC 命令訊框(Frame)重傳 aMaxFrameRetries 次仍然沒有收到確認訊框(Frame)，則 MAC 層判斷爲發送失敗，並把通訊失敗的結果報告給上層。

3.4.6.6 混雜模式

設備可以設置 macPromiscousMode 屬性來啓動混雜模式。如果要求 MLME 設置 macPromiscousMode 爲 TRUE，則 MLME 同時設置 macRxOnWhenIdle 爲 TRUE，並請求 PHY 層啓動接收機；如果要求 MLME 設置 macPromiscousMode 爲 FALSE，則 MLME 同時設置 macRxOnWhenIdle 爲 FALSE，並請求 PHY 層關閉接收機。

3.4.6.7 傳輸可靠性情景

由於無線傳輸媒質的不理想，發送訊框(Frame)不是都成成功到達接收設備。圖 24 列出了訊框(Frame)傳輸過程中可能出現的 3 種情況：

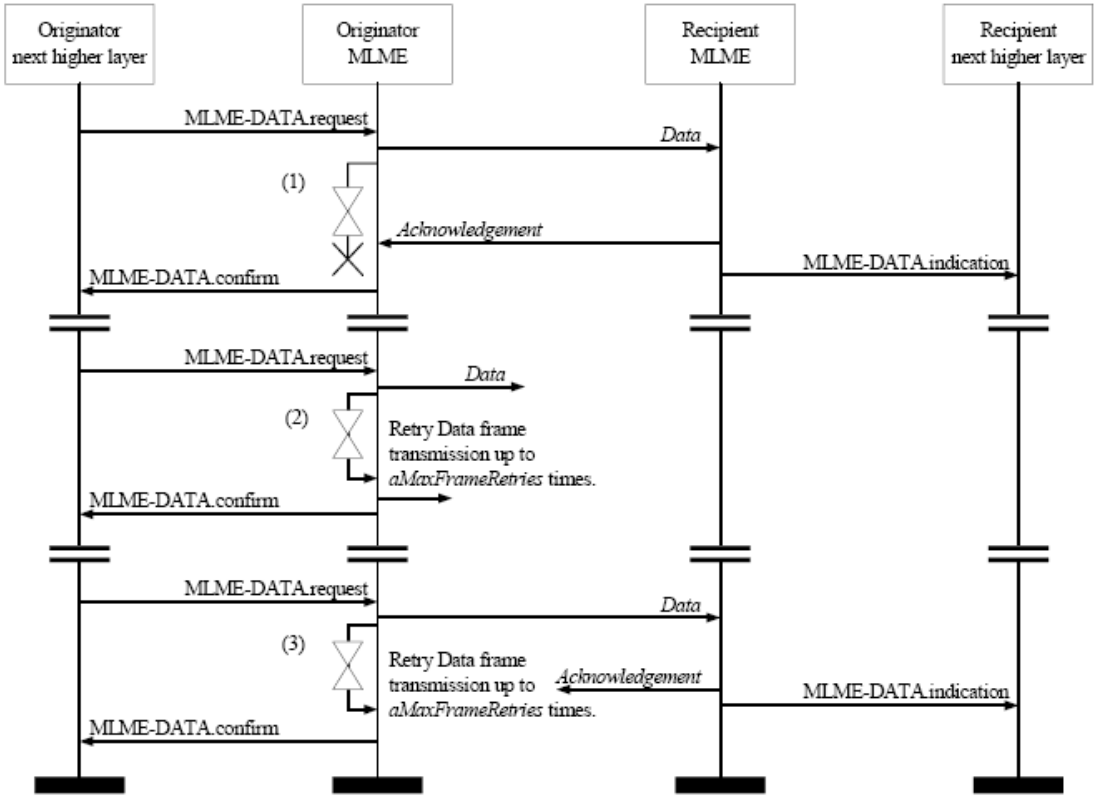


圖 24 訊框(Frame)傳輸的 3 種可靠性情況

①資料發送成功。發送設備的 MAC 層利用 PHY 層的資料服務吧資料訊框(Frame)發送到接收設備。在等待確認時，發送設備 MAC 層啓動一個計時器，計時時間爲 macAckWaitDuration 個符號週期。接收設備 MAC 層收到資料訊框(Frame)後，向發送設備回送一個確認訊框(Frame)，並把收到的訊框(Frame)提交給上層。發送設備 MAC 在計時結束前收到接收設備發回的確認後，就關閉和復位計時器。此時資料發送完成，發送設備 MAC 就向上層發送一個成功證實。

②資料訊框(Frame)丟失。發送設備的 MAC 層利用 PHY 層的資料服務把資料訊框(Frame)發送到接收設備。在等待確認時，發送設備 MAC 層啓動一個計時器，計時時間爲 macAckWaitDuration 個符號週期。接收設備的 MAC 層沒有收到資料訊框(Frame)，因此也不會發送設備回饋確認。發送設備的計時結束前沒有收到確認訊框(Frame)，訊框(Frame)發送失敗，發送設備將再次發送給資料訊框(Frame)。這個重傳過程最多可以重複 aMaxFrameRetries 次。如果一個資料訊框(Frame)的（1+aMaxFrameRetries）次傳輸嘗試都失敗了，發送設備 MAC 就向上層發送一個失敗證實。

③確認訊框(Frame)丟失。發送設備的 MAC 層利用 PHY 層的資料服務吧資料訊框(Frame)發送到接收設備。在等待確認的時候，發送設備 MAC 層啓動一個計時器，計時時間爲 macAckWaitDuration 個符號週期。接收設備 MAC 層收到資料訊框(Frame)後，向發送設備回送一個確認訊框(Frame)，並把收到的訊框(Frame)提交給上層。發送設備 MAC 層沒有收到確認訊框(Frame)，計時器超時，訊框(Frame)發送失敗，發送設備將再次發送該資料訊框(Frame)。這個重傳過程最多可以重複 aMaxFrameRetries 此。如果一個資料訊框(Frame)的（1+aMaxFrameRetries）次傳輸嘗試都失敗了，發送設備 MAC 就向上層發送一個失敗證實。

3.4.7 GTS 分配和管理

保證時隙（GTS）允許設備獨享超訊框(Frame)中的部分時隙，作爲專用通道使用。GTS 是由 PAN 協調器負責分配，只可用於 PAN 協調器和設備之間的通訊。一個 GTS 可佔用一個或多個超訊框(Frame)時隙，只要超訊框(Frame)結構中有足夠的時間資源，PAN 協調器最多可以同時分配 7 個 GTS。

設備使用 GTS 遵循先分配後使用的原則。PAN 協調器根據設備的 GTS 請求以及當前超訊框(Frame)的容量來決定是否分配 GTS 給該設備。PAN 協調器分配 GTS 遵循先到先服務的原則，所有 GTS 都連續排列在超訊框(Frame)的末端，跟隨在 CAP 之後。每個 GTS 不再使用時就被撤銷，PAN 協調器可以隨時撤銷一個 GTS，申請使用 GTS 的設備也可以撤銷 GTS。分配了 GTS 的設備也可以工作在 CAP。在 GTS 發送的資料訊框(Frame)只能使用短位址。

GTS 的管理職能由 PAN 協調器來承擔。爲了方便管理 GTS，PAN 協調器應能夠儲存管理 7 個 GTS 所必需的資訊。這些資訊包括每個 GTS 的開始時隙、長度、方向和關聯設備俄的位址。

GTS 的方向可以是發送或接收，它的定義是相對于 GTS 關聯設備發送資料流程的方向而言的。每個設備可以申請一個發送時隙和/或一個接收時隙，所以用設備位址和方向就可以唯一標識一個 GTS。當設備得到一個 GTS 時，就保存下它的開始時隙、長度和方向資訊。如果設備分到了一個接收 GTS，則在整個 GTS 內設備都開啓接收機；如果設備分到了一個發送 GTS，則在整個 GTS 內 PAN 協調器都開啓接收機。如果設備在接收 GTS 內收到一個要求確認的資料訊框(Frame)，則設備以正常方式發送確認訊框(Frame)；同樣，設備也可以在發送 GTS 內接收確認訊框(Frame)。

只有跟蹤信標的設備才可以請求和使用 GTS。上層向 MLME 發出 TrackBeacon 參數爲 TRUE 的同步請求原語 MLME-SYNC.request 來指令設備跟蹤信標。如果設備與 PAN 協調器之間失去同步，則它分到的 GTS 都丟失。RFD 可選支援 GTS 的使用。

3.4.7.1 CAP 維護

PAN 協調器應保證 CAP 的長度至少爲 aMinCAPLength，如果 CAP 不滿足最小長度，就要採取預防措施。唯一的例外是，當執行 GTS 維護需要臨時增加信標訊框(Frame)的長度時，允許 CAP 的長度小於 aMinCAPLength；如果必須採取預防措施保證 CAP 長度時，則根據需要可以採用下面的一種或多種方法：

- 限制信標訊框(Frame)位址列表中的位址個數；
- 信標中部帶有效載荷；
- 撤銷一個或多個 GTS。

3.4.7.2 GTS 分配

設備使用 MLME-GTS.request 原語請求分配一個新的 GTS，原語中 GTS 特徵集根據應用要求來設定。收到 GTS 請求原語後，MLME 向 PAN 協調器發送 GTS 請求命令。GTS 請

求命令訊框(Frame)中 GTS 特徵欄位的 GTS 類型子域應設爲 1（表示分配 GTS），長度和方向子域按照應用要求來設定。正確接收到 GTS 請求命令後，PAN 協調器回饋一個確認訊框(Frame)。

PAN 協調器收到要求分配 GTS 的請求命令後，首先根據 CAP 的剩餘長度和請求的 GTS 長度判斷當前超訊框(Frame)是否有足夠的容量。如果超訊框(Frame)中 GTS 個數尚未達到最大，並且分配一個 GTS 後 CAP 的長度也不會小於 aMinCAPLength，則 PAN 協調器有足夠的容量。只要 PAN 協調器有足夠的可用帶寬，它就以“先到先服務”的原則分配多個 GTS。PAN 協調器要在 aGTSDescPersistenceTime 個超訊框(Frame)內作出能否分配 GTS 的決定。

設備收到 GTS 請求命令的確認後，繼續跟蹤信標，最多等待 aGTSDescPersistenceTime 個超訊框(Frame)。如果在這段時間內信標中沒有出現該設備的 GTS 描述符，設備的 MLME 就通知上層請求 GTS 失敗。這個通知由 MLME 發送狀態爲 NO_DATA 的證實原語 MLME-GTS.confirm 來實現。

PAN 協調器在判斷是否有足夠的容量滿足 GTS 請求的同時產生一個 GTS 描述符，描述符中包含 GTS 的請求配置和請求設備的短位址。如果 GTS 分配成功，PAN 協調器把 GTS 描述符中的開始時隙設置爲 GTS 開始的超訊框(Frame)時隙，把長度設置爲 GTS 的長度。此外，PAN 協調器還使用 MLME-GTS.indication 指示原語把新分配 GTS 的特徵告知上層。如果當前超訊框(Frame)沒有足夠的容量用來分配請求的 GTS，則 PAN 協調器吧 GTS 描述符的開始時隙設置爲 0，把長度設置爲當前可分配的最大 GTS 長度。然後 PAN 協調器把產生的 GTS 描述符放入信標中，更新信標訊框(Frame)的 GTS 配置欄位。另外 PAN 協調器還要根據分配 GTS 的結果，更新信標訊框(Frame)的超訊框(Frame)配置欄位中的 CAP 最後時隙子域。GTS 描述符在信標中駐留 aGTSDescPersistenceTime 個超訊框(Frame)，然後自動刪除。當 GTS 描述符要臨時增加信標訊框(Frame)的長度時，PAN 協調器允許超訊框(Frame)中的 CAP 長度小於 aMinCAPLength。

當接收的信標訊框(Frame)中包含有 macShortAddress 對應的 GTS 描述符時，設備就對 GTS 描述符進行處理。設備的 MLME 也發送 MLME-GTS.confirm 向其上層報告 GTS 分配請求的結果。如果 GTS 描述符的開始時隙大於 0，則證實原語的狀態爲 SUCCESS；如果 GTS 描述符的開始時隙等於 0 或者長度與請求的 GTS 長度不一致，則證實原語的狀態爲 DENIED。

3.4.7.3 GTS 使用

當設備 MAC 層收到資料請求原語 MCPS-DATA.request 的 TxOptions 參數指示爲 GTS 發送時，設備先要判斷是否有有效的 GTS。如果設備是 PAN 協調器，則它要判斷資料發送請求的目的位址對應的設備是否有接收 GTS；如果設備不是 PAN 協調器，則它要判斷自己是否分配有發送 GTS。如果存在有效的 GTS，則 MAC 在 GTS 內發送資料。如果請求事務能夠在 GTS 結束前完成，則 MAC 層馬上發送 MPDU，不使用 CSMA-CA；如果請求事務不能在當前 GTS 結束前完成，則 MAC 層推遲到下一個超訊框(Frame)相同的 GTS 發送資料。

如果設備有接收 GTS，則設備 MAC 層要保證在 GTS 期間接收機一直處於開啓狀態；PAN 協調器將在 GTS 內發送所有訊框(Frame)，訊框(Frame)控制欄位中確認請求子域爲 1。

當 PAN 協調器 MAC 層收到資料請求原語 MCPS-DATA.request 的 TxOptions 參數指示爲 GTS 發送時，它等到目的接收設備的接收 GTS 開始後才開始發送資料。這種要求 GTS 發送的設備的位址不要添加到信標訊框(Frame)的位址列表中。PAN 協調器 MAC 層必須確

保它的接收機在每個設備的發送 GTS 期間都處於開啓狀態。

每個設備在 GTS 內開始發送之前，應保證資料發送、確認和 IFS 都能夠在 GTS 結束前完成。如果設備錯過了超訊框(Frame)開始的信標訊框(Frame)，則它需要捕獲下一個超訊框(Frame)的信標後才能使用 GTS。如果設備因丟失信標而失步，那麼它就認爲分配給它的信標被撤銷了。

3.4.7.4 GTS 撤銷

設備請求撤銷現存的 GTS 也是使用 MLME-GTS.request 原語。設備不再使用將要撤銷的 GTS，並且重定有關該 GTS 的特徵資訊。設備請求撤銷現存的 GTS 時，MLME 向 PAN 協調器發送 GTS 請求命令。GTS 請求命令訊框(Frame)中 GTS 特徵欄位的 GTS 類型子域應設爲 0（表示撤銷 GTS），長度和方向子域按照要撤銷的 GTS 的特徵設定。PAN 協調器正確接收到撤銷 GTS 的請求命令後就向請求設備發送一個確認訊框(Frame)；設備接收到確認訊框(Frame)後，MLME 就用 MLME-GTS.confirm 原語把撤銷的 GTS 告知其上層。如果 PAN 協調器不能正確接收到撤銷 GTS 請求命令，則需要按照下面“GTS 空閒判斷”中介紹的方法，來判頓設備是否停止使用 GTS。

PAN 協調器接收到撤銷 GTS 的請求命令後，就著手撤銷 GTS。如果沒有一個現存的 GTS 與撤銷 GTS 的請求命令中的 GTS 特徵相符，則 PAN 協調器忽略 GTS 請求命令；如果有一個 GTS 與請求命令中要撤銷的 GTS 特徵相符，則 PAN 協調器的 MLME 撤銷該 GTS，並把 GTS 改變結果通知給上層。撤銷 GTS 後，超訊框(Frame)中 CAP 長度增加，所以 PAN 協調器也要相應地更新信標訊框(Frame)中超訊框(Frame)配置欄位的 CAP 最後時隙子域的值。設備請求撤銷 GTS 時，不需要把 GTS 描述符添加到信標中。

當撤銷 GTS 的過程由 PAN 協調器啓動時，PAN 協調器首先使用 GTS 指示原語 MLME-GTS.indication 把要撤銷的 GTS 通知給 MAC 上層，然後撤銷指定的 GTS 並把該 GTS 的描述符添加到信標中。撤銷的 GTS 描述符的開始時隙值爲 0。該描述符將在信標中駐留 aGTSDescPersistenceTime 個超訊框(Frame)。當 GTS 描述符要臨時增加信標訊框(Frame)的長度時，PAN 協調器允許超訊框(Frame)中的 CAP 長度小於 aMinCAPLength。

當設備接收到的信標中含有 macShortAddress 對應的 GTS 描述符，並且描述符的開始時隙值等於 0 時，設備立即停止使用 GTS，並使用 MLME-GTS.indication 原語吧撤銷的 GTS 通知給設備的 MAC 上層。

3.4.7.5 GTS 重分配

撤銷 GTS 後可能導致超訊框(Frame)變成零散的碎片，圖 25 示意了撤銷超訊框(Frame)GTS 的 3 個階段：第 1 階段超訊框(Frame)的 CFP 有 3 個分配的 GTS，分別開始於第 14 個、第 10 個和第 8 個超訊框(Frame)時隙；第 2 階段撤銷 GTS2，此時 GTS1 和 GTS3 之間就有一段不能利用的空隙；爲了消除空隙，在第 3 階段移動 GTS3 與 GTS1 連接起來，增加 CAP 的長度。PAN 協調器能消除因撤銷 GTS 在 CFP 內產生的空隙，使得 CAP 長度最大化。

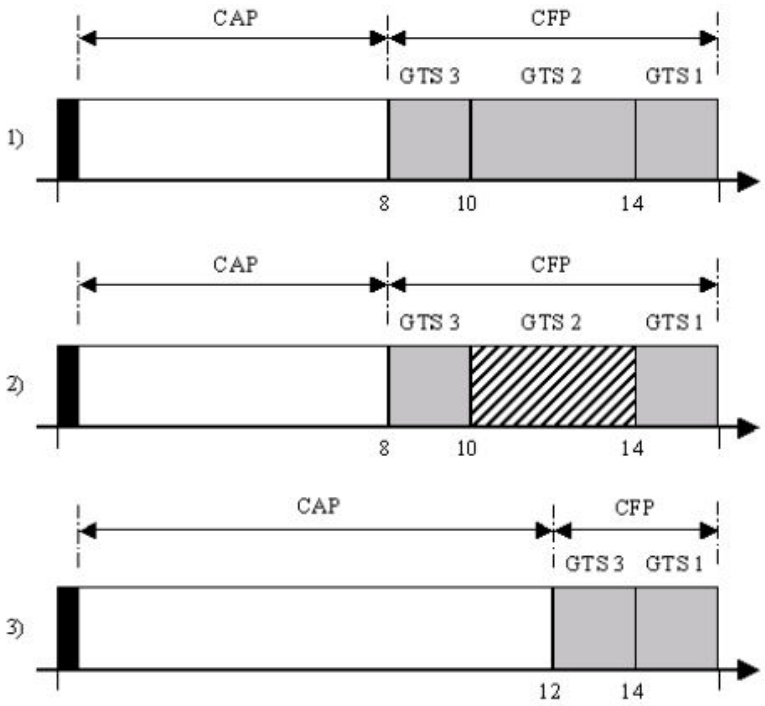


圖 25 GTS 撤銷和 CFP 碎片整理

當 PAN 協調器撤銷 GTS 時，它把撤銷的 GTS 描述符添加到信標中，向設備指示 GTS 的撤銷；當撤銷 GTS 的過程由設備請求啓動時，撤銷的 GTS 描述符不添加到信標中。撤銷一個 GTS 後，PAN 協調器將把那些開始時隙位置小於撤銷的 GTS 開始時隙的設備 GTS 向 CFP 的尾部方向平移，更新這些 GTS 的開始時隙，並把平移調整過的 GTS 描述符添加到信標中。撤銷 GTS 後平移整合 GTS 的原則，是使 CFP 的末端和 GTS 時隙之間都沒有空隙。

當需要對多個 GTS 重分配時，PAN 協調器可選擇分佈實現，並保證每個 GTS 描述符在信標中駐留 aGTSDescPersistenceTime 個超訊框(Frame)週期。當設備接收到的信標中含有 macShortAddress 對應的 GTS 描述符，並且方向和長度與設備當前的一個 GTS 相同，則設備把當前 GTS 的開始時隙調整爲信標中 GTS 描述符指示的開始時隙，並可立即應用。

當 PAN 協調器必須添加 GTS 描述符到信標中時，允許超訊框(Frame)中的 CAP 長度小於 aMinCAPLength 以臨時增加信標訊框(Frame)的長度。aGTSDescPersistenceTime 個超訊框(Frame)週期後，PAN 協調器將從信標中刪除 GTS 描述符。

3.4.7.6 GTS 空閒判斷

當 PAN 協調器不能正確接收設備撤銷 GTS 的請求命令時，可以透過下面的規則來判斷設備是否停止使用 GTS：

- 對於發送 GTS，如果在至少 2×n 個超訊框(Frame)週期內 PAN 協調器在一個設備的 GTS 上沒有收到設備發出的資料訊框(Frame)，則認爲設備已不再使用該發送 GTS；
- 對於接收 GTS，如果在至少 2×n 個超訊框(Frame)週期內 PAN 協調器在一個設備的 GTS 上沒有收到設備發出的確認訊框(Frame)，則認爲設備已不再使用該接收 GTS。

其中 n 值得定義如下：

$$n = \begin{cases} 2^{(8-macBeaconOrder)} & 0 \le macBeaconOrder \le 8 \\ 1 & 9 \le macBeaconOrder \le 14 \end{cases}$$

3.4.8 MAC 訊框(Frame)的安全處理

在上層要求的情況系，MAC 層可以爲發送和接收訊框(Frame)提供安全服務。IEEE802.15.4 支援 4 種安全服務：存取控制、資料加密、訊框(Frame)完整性、順序保鮮。

協定同時提供了 3 種安全模式：不安全模式、ACL 模式和安全模式。決定如何提供安全的資訊保存在 MAC PIB 中。

3.4.8.1 ACL 入口

MAC PIB 安全屬性包括 1 個預設 ACL 入口和 1 組個別 ACL 入口。預設 ACL 入口時 PAN 中所有設備都知道的一個入口，它用於未知的一個或多個設備之間的通訊；個別 ACL 入口則用於兩個已知設備間以共用密鑰的方式通訊。

預設 ACL 入口包括 3 個屬性：macDefaultSecurity、macDefaultSecuritySuite 和 macDefaultSecurityMaterial。macDefaultSecurity 屬性指示不在 ACL 中的設備是否使用安全服務；macDefaultSecuritySuite 屬性表示不在 ACL 中的設備發送和接收訊框(Frame)使用的預設安全套件；macDefaultSecurityMaterial 屬性表示不在 ACL 中的設備安全通訊時發送和接收訊框(Frame)使用的密鑰材料。如果 macDefaultSecurity 等於 FALSE，則不使用 macDefaultSecuritySuite 和 macDefaultSecurityMaterial。

其他 ACL 入口包含在 macACLEntryDescriptorSet 屬性中，它是一組 ACL 入口描述符。每個 ACL 入口對應一個信任設備，包括該設備的 PAN 標識、64 位元擴充位址、短位址（如果不知道就爲 0xFFFF），以及它的安全套件和相關密鑰材料。

3.4.8.2 不安全模式

不安全模式不提供任何安全服務，它是 MAC 層預設的安全模式。工作在不安全模式的設備既不使用 ACL 入口，也不對接收訊框(Frame)作任何安全相關的操作。工作在不安全模式的設備先對到達的訊框(Frame)進行過濾，然後檢查其安全致能子域。如果訊框(Frame)的安全致能位元等於 1，並且設備沒有執行主動或被動掃描，則 MAC 層調用資料指示原語 MCPS-DATA.indication，把訊框(Frame)遞交給上層。指示原語中 SecurityUse 參數設爲 TRUE，ACLEntry 參數設爲 0x08。如果設備在執行主動或被動掃描，則它接受安全致能位等於 1 的信標訊框(Frame)，並把該信標訊框(Frame)對應的 PAN 描述符中的 SecurityUse、ACLEntry 和 SecurityFailure 欄位分別設置爲 TRUE、0x08 和 TRUE。如果 MAC 層收到的資料訊框(Frame)安全致能位元等於 0，則透過 MCPS-DATA.indication 原語把訊框(Frame)遞交給上層，指示原語中 SecurityUse 參數設爲 FALSE，ACLEntry 參數設爲 0x08。

3.4.8.3 ACL 模式

ACL 模式提供給 MAC 層一種判斷接收的訊框(Frame)是否源自存取控制列表（ACL）中設備的機制。工作在 ACL 模式的設備不應對 MAC 訊框(Frame)做任何修改或加密操作，ACL 模式只是提供給設備一種根據源位址對接收訊框(Frame)進行過濾的方法，而並不是一種安全識別訊框(Frame)產生設備的方法（即不能確保訊框(Frame)的實際產生者就是源位址對應的設備）。工作在 ACL 模式的設備 MAC 層先對到達的訊框(Frame)進行過濾，然後檢查其安全致能子域。如果訊框(Frame)的安全致能位元等於 1，並且設備沒有執行主動或被動掃描，則 MAC 層調用資料指示原語 MCPS-DATA.indication，把訊框(Frame)遞交給上層。指示原語中 SecurityUse 參數設爲 TRUE，ACLEntry 參數的設置則要看 ACL 中是否存在訊框(Frame)的源位址指示的發送設備。如果 ACL 中包含有訊框(Frame)的發送設備，則把 ACLEntry 參數設爲發送設備關聯的 ACL 入口的 macSecurityMode 屬性值；如果 ACL 中沒有訊框(Frame)發送設備，則把 ACLEntry 參數設爲 0x08。如果設備在執行主動或被動掃描，則它接受安全致能位等於 1 的信標訊框(Frame)，並把該信標訊框(Frame)對應的 PAN 描述符中的 SecurityUse 和 SecurityFailure 欄位都設置爲 TRUE，描述符中 ACLEntry 欄位的設置則要看 ACL 中是否包含發送信標的設備。如果 ACL 中包含有信標訊框(Frame)的發送設備，則把 ACLEntry 參數設爲發送設備關聯的 ACL 入口的 macSecurityMode 屬性值；如果 ACL 中沒有訊框(Frame)發送設備，則把 ACLEntry 參數設爲 0x08。如果 MAC 層收到的資料訊框(Frame)安全致能位元等於 0，則透過 MCPS-DATA.indication 原語把訊框(Frame)遞交給上層，指示原語中 SecurityUse 參數設爲 FALSE，ACLEntry 參數的設置則要看 ACL 中是否存在訊框(Frame)的源位址指示的發送設備。如果 ACL 中包含有訊框(Frame)的發送設備，則把 ACLEntry 參數設爲發送設備關聯的 ACL 入口的 macSecurityMode 屬性值；如果 ACL 中沒有訊框(Frame)發送設備，則把 ACLEntry 參數設爲 0x08。設備透過搜索 macACLEntryDescroptorSet 中每個 ACL 入口來判斷接收訊框(Frame)的發送設備是否包含在 ACL 中。如果有一個 ACL 入口的 ACLPANId 值等於接收到的 PAN 標識，ACLExtendedAddress 或 ACLShortAddress 的值等於接收訊框(Frame)的源位址，則表示 ACL 中包含有該接收訊框(Frame)的發送設備。如果接收訊框(Frame)沒有源位址，則 ACLEntry 設爲 0x08。

3.4.8.4 安全模式

安全模式提供給 MAC 一種既使用 ACL 功能又爲訊框(Frame)提供加密保護的機制。工作在安全模式的設備 MAC 接收到訊框(Frame)或者接收到上層的訊框(Frame)發送請求時，就分別按照下面的方法進行處理。

安全模式時，如果設備 MLME 收到上層要求發送一個安全訊框(Frame)的請求（即 TxOptions 的安全致能位爲 1），它就掃描 ACL 入口，尋找要使用的正確入口。MLME 首先搜索 macACLEntryDescriptorSet，尋找 ACLPANId 值和 ACLExtendedAddress 或 ACLShortAddress 的值與要產生的訊框(Frame)的目的位址資訊相匹配的 ACL 入口。如果找到了相匹配的 ACL 入口，MLME 就用該 ACL 入口 ACLSecuritySuite 欄位的安全套件和 ACLSecurityMaterial 欄位的安全材料處理要發送的訊框(Frame)；如果 MLME 在 macACLEntryDescriptorSet 中沒有找到 ACLPANId 值和 ACLExtendedAddress 或

ACLShortAddress 的值與要產生的訊框(Frame)的目的位址資訊相匹配的 ACL 入口，MLME 將檢測 macDefaultSecurity。如果 macDefaultSecurity 等於 TRUE，MLME 就用 macDefaultSecuritySuite 的安全套件和 macDefaultSecurityMaterial 的安全材料處理要發送的訊框(Frame)。如果 MLME 在 macACLEntryDescriptorSet 中找不到與目的位址資訊相匹配的 ACL 入口，並且 macDefaultSecurity 等於 FALSE，則 MLME 向其上層發出狀態爲 UNAVILABLE_KEY 的通訊狀態指示原語 MLME-COMM-STATUS.indication。

MLME 從 ACL 得到合適的安全套件和安全材料後，首先把訊框(Frame)控制欄位中的安全致能位設爲 1，然後對訊框(Frame)進行加密。如果安全套件指定了加密要求，則加密操作只應用于 MAC 有效載荷部分的有效載荷欄位，即信標有效載荷欄位、命令有效載荷欄位或資料有效載荷欄位。如果一訊框(Frame)不含有效載荷欄位，則不需要進行加密。加密後的資料插入到訊框(Frame)中原始資料所在的有效載荷欄位。

如果安全套件指定要使用訊框(Frame)完整性保護，則完整性碼應用于 MHR 連同 MAC 有效載荷部分。完整碼計算的結果和有效載荷欄位的其他資料一起放在 MAC 有效載荷的有效載荷欄位。如果要發送訊框(Frame)的有效載荷欄位沒有資料，則該欄位只放完整碼。確認訊框(Frame)中不使用完整碼。

加密和完整性保護操作的順序和具體方法，以及加密後的資料和完整性檢驗碼在有效載荷欄位如何存放，都是由所選擇的安全套件來決定的。詳見 MAC 層安全套件規範部分。

如果任何安全操作失敗，MLME 都不發送請求的訊框(Frame)，而是向上層發出狀態爲 FAILED_SECURITY_CHECK 的 MLME-COMM-STATUS.indication 原語，告知安全處理失敗；如果安全處理後訊框(Frame)長超過 aMaxMACFrameSize，MLME 也不發送請求的訊框(Frame)，而是向上層發出狀態爲 FRAME_TOO_LONG 的 MLME-COMM-STATUS.indication 原語，告知通訊失敗的原因；如果成功完成了安全操作並且按安全套件的規定修改了有效載荷欄位，則設備安全處理後的訊框(Frame)計算訊框(Frame)校驗序列 FCS，就得到一個完整的 MAC 協定資料單元（MPDU）。

接收的訊框(Frame)也可能是收到安全保護的。工作于安全模式時，設備 MLME 收到訊框(Frame)後，首先實行過濾操作，然後檢測器安全致能欄位判斷該訊框(Frame)是否採用了安全保護。

如果接收訊框(Frame)的安全致能欄位爲 0，並且是關聯請求命令訊框(Frame)，則協調器的 MLME 調用關聯指示原語 MLME-ASSOCIATE.indication 把訊框(Frame)訊息提交給上層。如果接收訊框(Frame)是信標請求命令訊框(Frame)且安全致能欄位爲 0，則支持信標的 PAN 中的協調器忽略信標請求命令，繼續以正常方式發送信標；而不支持信標的 PAN 中的協調器以非時隙 CSMA-CA 演算法發送一個信標。如果設備正在執行主動或被動掃描時收到一個信標的安全致能欄位爲 0，設備將接受該信標訊框(Frame)並把它對應的 PAN 描述符中的 SecurityUse 和 SecurityFailure 欄位分別設爲 FALSE 和 TRUE，ACLEntry 欄位的設置則要看 ACL 中是否存在訊框(Frame)發送設備。如果 ACL 中包含有訊框(Frame)的發送設備，則把 ACLEntry 欄位設爲發送設備關聯的 ACL 入口的 macSecurityMode 屬性值；如果 ACL 中沒有訊框(Frame)發送設備，則把 ACLEntry 參數設爲 0x08。其餘情況下，如果接收訊框(Frame)的安全致能欄位爲 0，則設備調用 MCPS-DATA.indication 原語把訊框(Frame)提交給 MAC 上層。資料指示原語中 SecurityUse 參數設爲 FALSE，ACLEntry 參數的設置則要看 ACL 中是否存在訊框(Frame)的源位址指示的發送設備。如果 ACL 中包含有訊框(Frame)的發送設備，則把 ACLEntry 參數設爲發送設備關聯的 ACL 入口的 macSecurityMode 屬性值；如果 ACL 中沒有訊框(Frame)發送設備，則把 ACLEntry 參數設爲 0x08。

如果接收訊框(Frame)的安全致能欄位爲 1，則設備在 MAC PIB 安全屬性中掃描 ACL

入口，尋找要使用的正確入口。MLME 首先搜索 macACLEntryDescriptorSet，尋找 ACLPANId 值和 ACLExtendedAddress 或 ACLShortAddress 的值與接收訊框(Frame)源位址資訊相匹配的 ACL 入口。如果找到了相匹配的 ACL 入口，MLME 就用該 ACL 入口 ACLSecuritySuite 欄位的安全套件和 ACLSecurityMaterial 欄位的安全材料來處理接收的訊框(Frame)；如果 MLME 在 macACLEntryDescriptorSet 中沒有找到 ACLPANId 值和 ACLExtendedAddress 或 ACLShortAddress 的值與接收訊框(Frame)的源位址資訊相匹配的 ACL 入口，MLME 將檢測 macDefaultSecurity。如果 macDefaultSecurity 等於 TRUE，MLME 就用 macDefaultSecuritySuite 的安全套件和 macDefaultSecurityMaterial 的安全材料來處理接收的訊框(Frame)。如果 MLME 在 macACLEntryDescriptorSet 中找不到與接收訊框(Frame)的源位址資訊相匹配的 ACL 入口，並且 macDefaultSecurity 等於 FALSE，設備也沒有執行主動掃描或被動掃描，則 MLME 調用 MCPS-DATA.indication 原語把訊框(Frame)提交給 MAC 上層。資料指示原語中 SecurityUse 參數設爲 TRUE，ACLEntry 參數設爲 0x08。如果設備正在執行主動掃描或被動掃描，則儘管找不到該信標的相關安全材料，設備還是接受該信標訊框(Frame)，並且把該信標對應的 PAN 描述符的 SecurityUse、ACLEntry 和 SecurityFailure 欄位分別設置爲 TRUE、0x08 和 TRUE。

MLME 從 ACL 中搜索到合適的安全套件和安全材料後，MAC 層就對接收的訊框(Frame)進行安全處理。如果安全套件中有加密要求，則對 MAC 有效載荷中有效載荷欄位的資料進行解密。如果有效載荷欄位沒有資料，則不需執行解密操作。解密後的資料存放到有效載荷欄位替換原始的加密資料。如果安全套件要求訊框(Frame)完整性校驗，則首先把完整性校驗碼和安全套件的其他資料從 MAC 有效載荷的有效載荷欄位中刪除，然後對 MHR 連同 MAC 有效載荷一起作完整性驗證。至於執行解密操作和完整性驗證的順序和具體方法以及安全資料在有效載荷欄位中的存放位置是由具體使用的安全套件來決定的。

一個沒有執行主動掃描或被動掃描的設備，如果至少出現了一個安全操作失敗，則 MLME 丟棄該資料訊框(Frame)，並調用裝態爲 FAILED_SECURITY_CHECK 的通訊狀態指示原語 MLME-COMM-STATUS.indication 向上層報告。如果接收設備正在執行主動掃描或被動掃描，則儘管安全操作失敗，設備還是接受該信標訊框(Frame)，並且把該信標對應的 PAN 描述符的 SecurityUse 和 SecurityFailure 欄位都設置爲 TRUE，ACLEntry 欄位的設置則因情況而定。如果解密操作中的密鑰能夠在 macACLEntryDescriptorSet 中找到，則 ACLEntry 設爲 TRUE；如果解密操作中的密鑰能夠在 macDefaultSecurityMaterial 中找到，則 ACLEntry 設爲 FALSE。如果安全操作成功完成並且有效載荷欄位已經修改成了合適的內容，則設備調用 MCPS-DATA.indication 原語，把得到的 MSDU 提交給 MAC 上層所進一步處理。資料指示原語中的 SecurityUse 參數設爲 TRUE，ACLEntry 參數的值因實際情況而定。如果解密操作中的密鑰能夠在 macACLEntryDescriptorSet 中找到，則 ACLEntry 設爲 TRUE；如果解密操作中的密鑰能夠在 macDefaultSecurityMaterial 中找到，則 ACLEntry 設爲 FALSE。

3.5 MAC 層安全規範

設備工作在安全模式時可能會用到安全套件。安全套件是爲提供安全服務而對 MAC 訊框(Frame)執行的一組操作。從安全套件的名稱上就能看出它所使用對稱加密演算法、模式和完整性校驗碼的比特長度。IEEE802.15.4 標準中的安全套件使用的加密演算法都是高級加密標準（AES）。該標準定義了 7 種安全套件，如表 9 所列，表中的“X”表示安全套件提供的安全服務。每個安全套件對應一個 1 位元組長度的標識碼，標識碼 0x00 表示不使用安

全模式。每個能提供安全保護的設備至少應支援 AES-CCM-64 安全套件。

表 9 安全套件

安全套件標識碼	安全套件名稱	提供的安全服務			
		存取控制	資料加密	訊框 (Frame) 完整性	順序保鮮（可選）
0x00	不使用安全模式				
0x01	AES-CTR	X	X		X
0x02	AES-CCM-128	X	X	X	X
0x03	AES-CCM-64	X	X	X	X
0x04	AES-CCA-32	X	X	X	X
0x05	AES-CBC-MAC-128	X		X	
0x06	AES-CBC-MAC-64	X		X	
0x07	AES-CBC-MAC-32	X		X	

3.5.1 安全套件構造模組

3.5.1.1 CTR 加密模式

計數器模式（CTR）對稱加密演算法的加密過程是，分組密碼產生器以共用密鑰和現時值（nonce）產生一個密鑰流，密鑰流與等長的明文“異或”後得到密文。現時值在每次加密時都不同，它可以是時間戳、計數器或者爲防止非授權的資訊重發而設定的特殊記號。CTR 模式的解密過程是產生同樣的密鑰流與密文“異或”後譯出對應的明文。

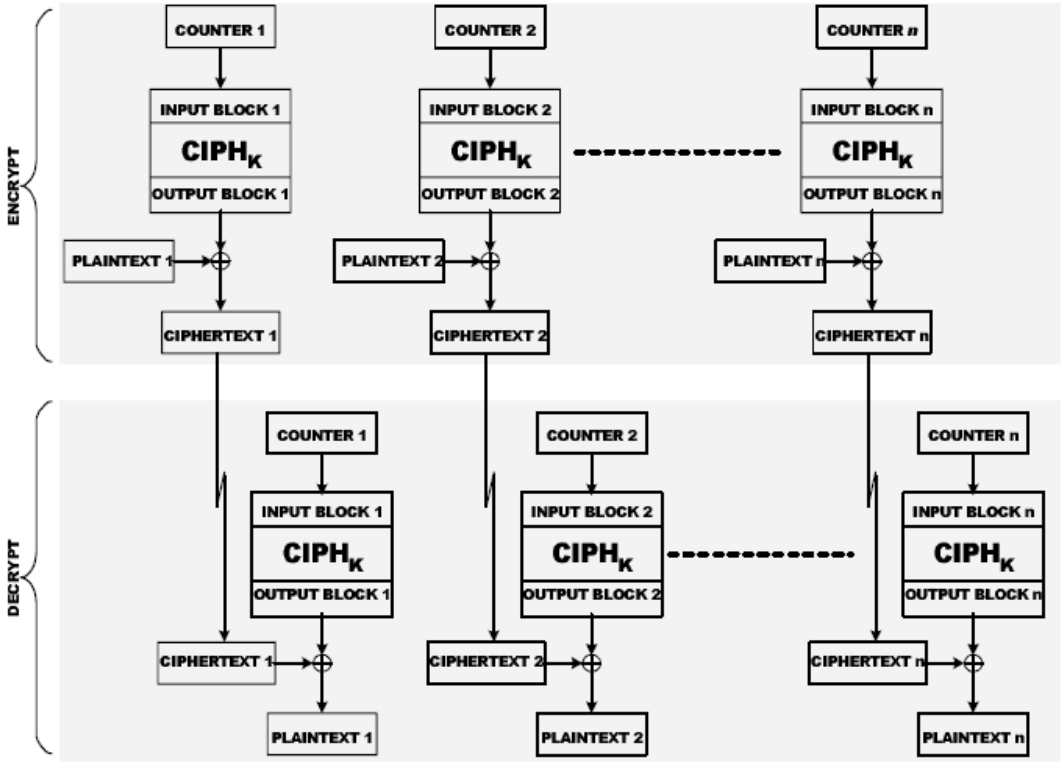


圖 26 CTR 模式的加密和解密原理

圖 26 是 CTR 模式的加密和解密原理。加密時，一組輸入分組（即計數器）經過分組密碼產生模組後得到一組輸出分組，一條明文劃分成與輸出分組等長的分組後分別與對應的輸出分組“異或”得到密文分組；反之解密過程亦然。這些計數器的特定是產生的輸入分組各不相同，這個要求不單局限於一條訊息，對所有以同一共用密鑰加密的訊息，所有的計數器必須各不相同。一條訊息對應的計數器分別表示爲 T_1，T_2，…，T_n，共用密鑰爲 K 的分組密碼產生模組表示爲 $CIPH_K$，則 CTR 模式可以定義爲：

$$o_j = CIPH_K(T_j) \qquad j = 1,2,\Lambda\ ,n$$

加密：

$$C_j = P_j \oplus O_j \qquad j = 1,2,\Lambda\ ,n-1$$

$$C_n^* = P_n^* \oplus MSB_u(O_n)$$

$$o_j = CIPH_K(T_j) \qquad j = 1,2,\Lambda\ ,n$$

解密：

$$P_j = C_j \oplus O_j \qquad j = 1,2,\Lambda\ ,n-1$$

$$P_n^* = C_n^* \oplus MSB_u(O_n)$$

CTR 加密時，每個計數器分組都啓動分組密碼產生功能，各輸出分組與對應的明文分組“異或”得到密文分組。最後一個明文分組的長度 u 可能小於輸出分組的長度，此時與最後一個輸出分組的 u 個高有效位“異或”得到最後一個密文分組。

CTR 解密時，每個計數器分組都啓動分組密碼產生功能，各輸出分組域對應的密文分組“異或”得到明文分組。最後一個密文分組的長度 u 可能小於輸出分組的長度，此時與最後一個輸出分組的 u 個高有效位“異或”得到最後一個明文分組。

在 CTR 加密和解密時，對應各個計數器的分組密碼產生功能可以並行工作；類似的，只要能夠得到計數器分組，每個密文分組對應的明文分組都可以獨立地解密得到。甚至於可以在明文或密文到來之前，實現執行分組密碼產生功能。

3.5.1.2 CBC-MAC 認證模式

密碼分組鏈結訊息認證碼（CBC-MAC）對稱認證演算法以 CBC 模式用分組密碼產生器得到訊息完整性驗證碼，以計算完整碼的訊息開始部分是實際認證資料的長度。驗證操作時，計算接收訊息的完整碼並與接收到的完整碼進行比較。

CBC-MAC 演算法利用分組密碼產生器得到輸入資料的完整性校驗碼。分組密碼產生器利用已知的密鑰把長度等於分組密碼長度的輸入向量轉換（加密）爲等長度的輸出向量。如果用 I 表示輸入向量，O 表示輸出向量，e 表示加密操作，則一次分組加密過程可以描述爲：

$$O = e(I)$$

用於計算訊息完整碼（MIC）的資料劃分成長度等於分組長度的資料分組 D_1，D_2，…，D_n。如果資料的比特長度不是分組長度的整數倍，則最後一個輸入分組 D_n 的低有效位用 0 來補足。MIC 的計算透過下面的鏈式計算得到：

$$O_1 = e(D_1)$$
$$O_2 = e(D_2 \oplus D_1)$$
$$O_3 = e(D_3 \oplus D_2)$$
M
$$O_n = e(D_n \oplus O_{n-1})$$

選取 O_n 的 M 個高有效位作爲 MIC，M 是 8 倍數並且滿足條件 $32 < M < 128$。圖 27 是 MIC 產生的原理框圖。

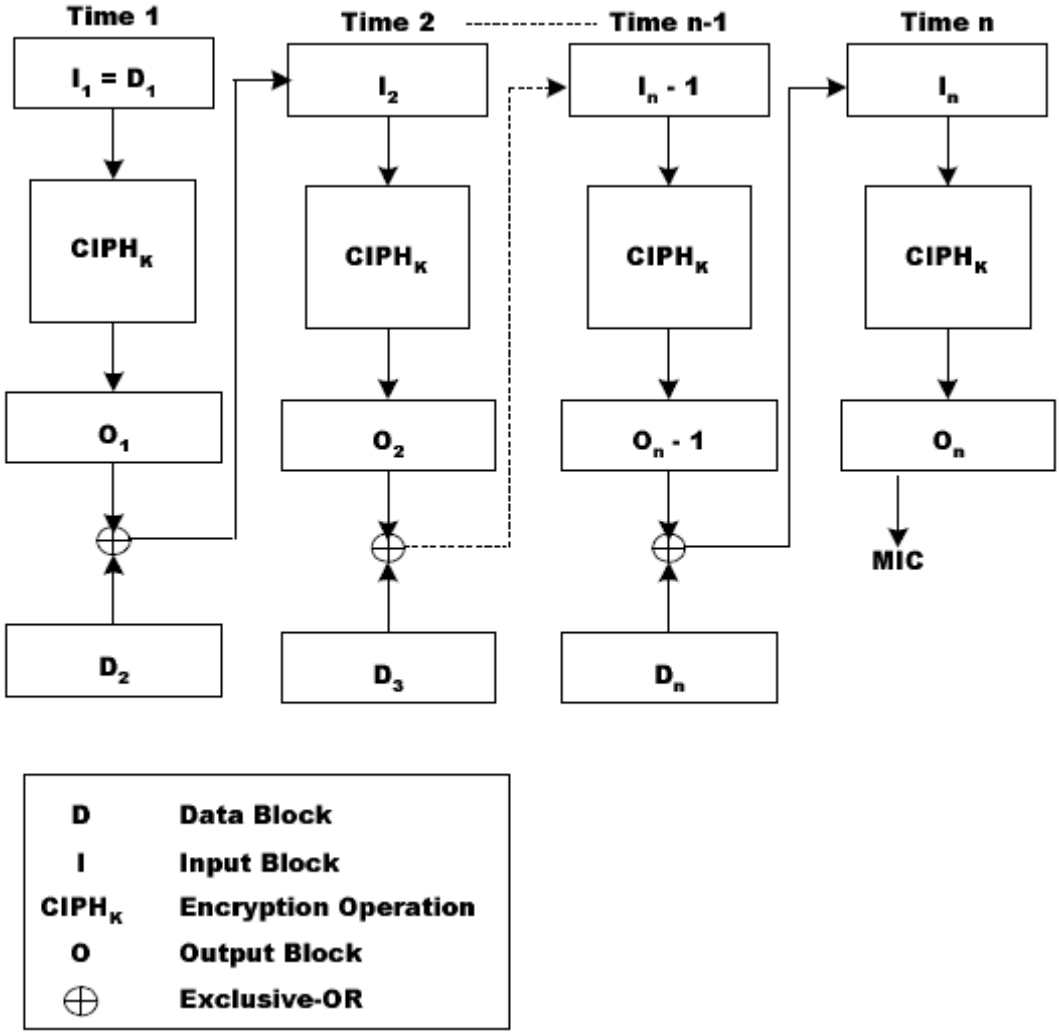


圖 27 MIC 產生的原理框圖

3.5.1.3 CCM 聯合加密和認證模式

CTR 加密結合 CBC-MAC（CCM）聯合對稱加密和認證演算法首先計算 MIC，然後對 MIC 和明文資料進行加密；輸出則由加碼的資料和加密的完整碼組成。

該安全套件的對稱認證操作首先以 CBC 模式用分組加密計算得到完整碼，用於計算完整碼的輸入資料是由現時值（nonce）、認證資料和明文資料組成的。驗證完整性時先根據接收資料計算完整碼，再與收到的完整碼比較。

該安全套件的加密操作首先根據已知密鑰和現時值以 CTR 模式計算密鑰流，然後把密鑰流與完整碼和明文“異或”得到密文。解密操作時先產生密鑰流，然後與密文“異或”得到明文和完整碼。

CCM 模式一般要選擇兩個參數。第一個參數是認證欄位的長度 M，即選取的 MIC 長度。參數 M 的選擇需要折中考慮訊息擴充度和訊息遭無法察覺的位元篡改概率，它的有效值是 4、6、8、10、12、14 和 16 位元組，表示 M 值得欄位長度是 3 位元，編碼 001～111 分別表示它的 7 個有效值。第二個參數是用以表示訊息長度的欄位的長度 L。參數 L 的選擇需要

折中考慮最大訊息長度和現時值（nonce）的長度。不同的應用要求不同的折中，L 的有效值爲 2～8 位元組，表示 L 值得欄位長度是 3 位元，編碼 001～111 分別表示它的 7 個有效值。

爲了發送一個訊息，發送者必須提供下面這些資訊：

- 分組加密的密鑰 K。
- 15—L 位元組長的現時值 N。在使用同一個密鑰加密的過程中，不能出現重複的現時值。
- 要發送的訊息 m。訊息長度範圍是 $0 \leqslant l(m) < 2^{8L}$ 位元組，即能夠用 L 位元組的長度欄位來表示。
- 附加認證資料 a。它的長度範圍是 $0 \leqslant l(a) < 2^{64}$ 位元組。附加認證資料只用於計算認證碼，不加密，也不包含在輸出分組中。

CCM 的第一步是用 CBC-MAC 計算認證欄位 T，即 MIC。首先定義一系列分組 B_0，B_1，…，B_n，然後用於 CBC-MAC。第一個 16 位元組分組 B_0 的格式如圖 28 所示。

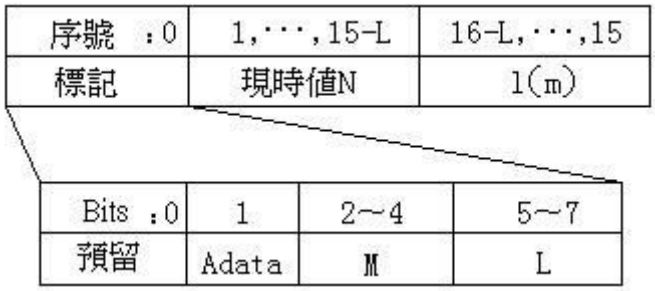


圖 28 CCM 認證第一個分組格式

標誌位元組中，Adata 位元用於指示是否有附加認證資料。如果 l（a）= 0，則 Adata 置爲 0；如果 l（a）＞ 0，則 Adata 置爲 1。如果 l（a）＞ 0，則透過對 l（a）和 a 的編碼會增加一些分組。首先對 l（a）進行編碼：如果 $0<l(a)<2^{16}-2^8$，則 l（a）欄位爲 2 個位元組，以最高有效位元在前的方式對 l（a）值編碼；如果 $2^{16}-2^8 \leqslant l(a) < 2^{32}$，則 l（a）有 6 個位元組，前 2 個位元組是 0xFFFE，後 4 個位元組以最高有效位元在前的方式對 l（a）值編碼；如果 $2^{32} \leqslant l(a) < 2^{64}$，則 l（a）有 10 個位元組，前 2 個位元組是 0xFFFF，後 8 個位元組以最高有效位元在前的方式對 l（a）值編碼。把 l（a）欄位與附加資料 a 級聯，劃分成 16 位元組的分組，最後一個分組不足 16 位元組時用 0 補足，並把附加認證資料的分組添加在 B_0 之後。

附件認證分組之後添加訊息分組。發送的訊息 m 也劃分成 16 位元組的分組，最後一個分組不足 16 位元組時用 0 補足。

得到資料分組 B_0，B_1，…，B_n 後，透過 CMC-MAC 計算訊息認證碼 T。

$$X_1 = E(K, B_0)$$
$$X_{i+1} = E(K, X_i \oplus B_i) \quad i = 1,2,\Lambda\ ,n$$
$$T = MSB_{8M}(X_{n+1})$$

其中：E（）表示分組密碼的加密功能，K 是共用密鑰，X_i 是加密輸出分組，MSB_{8M}（X_{n+1}）表示 CBC-MAC 鏈式加密最後一次輸出分組的高有效位元 8 個位元組。

CCM 的加密採用 CTR 模式。CTR 模式的密鑰流分組定義爲：

$$S_i = E(K, A_i) \quad i = 1,2,\Lambda$$

其中輸入分組 A_i 的格式如圖 29 所示。

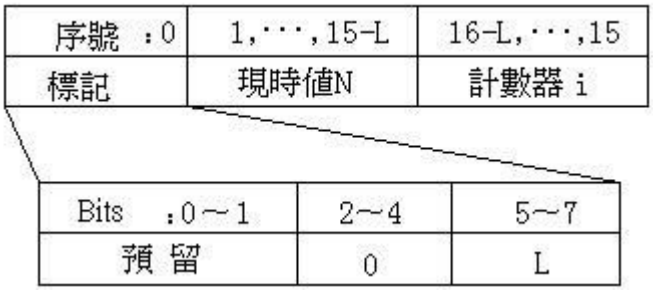


圖 29 加密分組格式

訊息明文 m 與級聯密鑰流 S_1，S_2，S_3……的前 l（m）個位元組得到加密的訊息。第一個密鑰流 S_0 用來加密認證碼 T，得到加密的認證碼 $U = T \oplus MSB_{8M}(S_0)$。最後得到 CCM 加密認證後的資料 c 是加密的訊息級聯加密的 MIC。

解碼時，必須獲知以下資訊：分組加密的密鑰 K、現時值 N、附加認證資料 a、加密認證後的訊息 c。

解碼時首先計算密鑰流，把密文與密鑰流“異或”恢復出訊息 m 和認證碼 T。利用恢復出的訊息 m 和附加認證資料 a 再次計算認證碼，並與回復得到的 T 進行比較。如果認證碼不正確，接收機將只指示完整性驗證失敗，而不會有其他任何資訊。

3.5.1.4 AES 加密演算法

高級加密標準（AES）是現行的國際加密標準，該分組加密演算法的密鑰長度有 128、192 和 256 三種。IEEE802.15.4 採用的分組長度爲 128 位、密鑰長度爲 128 位元的 AES 加密演算法。AES 的加密和解密流程如圖 30 所示。

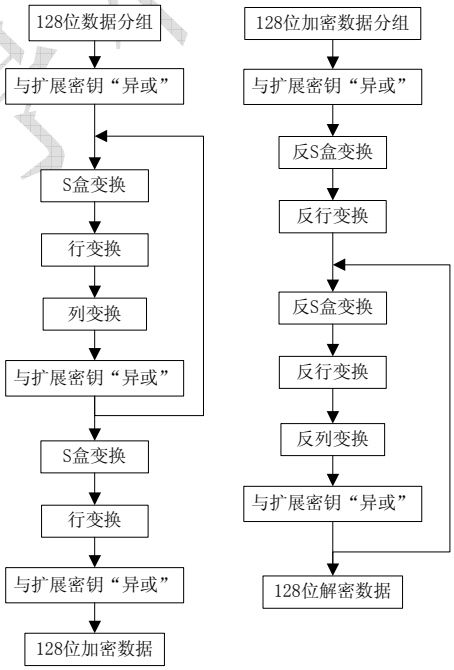


圖 30 AES 的加密和解密流程

3.5.1.5 PIB 安全材料

存放在 MAC PIB 中的安全資訊因不同的安全套件而有所不同。

對稱密鑰是 ACL 入口對應的 AES 密鑰，一個 AES 密鑰不能用於不同的安全套件。

訊框(Frame)計數器時運行計數器，它放在 MAC 有效載荷的有效載荷欄位，每發送一個安全訊框(Frame)計數器加 1。訊框(Frame)計數器不能溢出，它可用來保證 CCM 現時值的唯一性和接收訊框(Frame)的新鮮度。

密鑰序列計數器時由上層固定的，它放在 MAC 有效載荷的有效載荷欄位。如果訊框(Frame)計數器計滿，則可用密鑰序列計數器來保證 CCM 現時值的唯一性和接收訊框(Frame)的新鮮度。如果啓用了保鮮功能，則即使接收端保鮮操作失敗，上層也不應減小該計數器。

外部訊框(Frame)計數器和外部密鑰序列計數器時 ACL 入口中的可選欄位，它們分別表示接收到的與 ACL 入口對應的最近一個安全訊框(Frame)的訊框(Frame)計數器和密鑰序列計數器的值。它們也可以用來驗證接收訊框(Frame)的新鮮度。

3.5.2 AES-CTR 安全套件

AES-CTR 安全套件利用共用資料、訊框(Frame)計數器和密鑰序列計數器對 MAC 有效載荷的有效載荷欄位進行加密和解密。AES-CTR 套件可提供存取控制、資料加密和順序保鮮三種安全服務。

3.5.2.1 資料格式

AES-CTR 安全套件的安全材料存放在 macDefaultSecurityMaterial 或 ACL 的 ACLSecurityMaterial 欄位中，由對稱密鑰、訊框(Frame)計數器、密鑰序列計數器以及可選的外部訊框(Frame)計數器和密鑰序列計數器組成。AES-CTR 安全材料的格式如下：

位元組數：16	4	1	（4）	（1）
對稱密鑰	訊框(Frame)計數器	密鑰序列計數器	可選外部訊框(Frame)計數器	可選外部密鑰序列計數器

AES-CTR 加密訊框(Frame)有效載荷的有效載荷欄位由三部分組成：訊框(Frame)計數器、密鑰序列計數器和加密的有效載荷。加密的有效載荷長度等於加密前的有效載荷欄位長度，所以 AES-CTR 加密訊框(Frame)的有效載荷長度增加了 5 個位元組。AES-CTR 有效載荷欄位格式如下：

位元組數：4	1	可變長度

訊框(Frame)計數器	密鑰序列計數器	加密的有效載荷

在 AES-CTR 套件中，CTR 加密功能的輸入分組由標誌位元組、源位址、訊框(Frame)計數器、密鑰序列計數器和分組計數器組成。輸入分組的標誌位元組的設置只是爲了區別 AES-CCM 的標誌位元組。輸入分組各欄位的順序和長度如圖 31 所示。這些輸入分組對應於 CTR 模式中的 T_1，T_2，…，T_n。

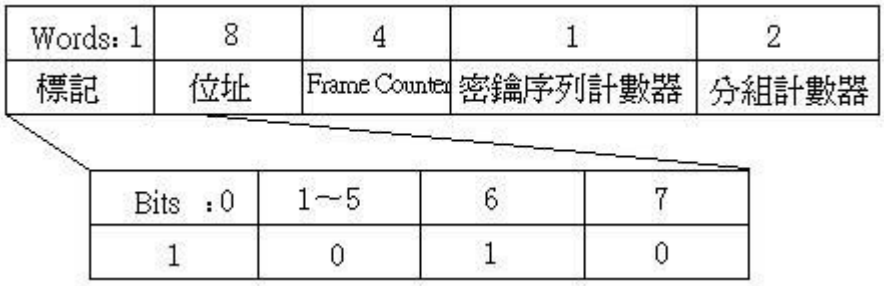


圖 31 AES-CTR 輸入分組格式

3.5.2.2 安全參數

AES-CTR 套件的 CTR 加密可以參數化以下兩點：

- 分組加密功能使用的是 AES 加密演算法。
- 各計數器的輸入分組中只是分組計數器欄位不同，其他欄位都是相同的。第一個輸入分組的分組計數器值爲 0，其他輸入分組的分組計數器依次加 1，即輸入分組 T_i 對應的分組計數器值爲 i—1。

3.5.2.3 安全操作

用 AES-CTR 套件保護輸出訊框(Frame)時，MAC 層需要執行以下操作：

①從 MAC PIB 中獲取設備的 64 位元擴充位址 aExtendedAddress、訊框(Frame)計數器、密鑰序列計數器值，構造輸入分組。

②按照 AES-CTR 的安全參數用 CTR 模式對 MAC 訊框(Frame)有效載荷的有效載荷欄位加密。

③以訊框(Frame)計數器、密鑰序列計數器和②的輸出構造新的有效載荷欄位。

④增加訊框(Frame)計數器。如果訊框(Frame)計數器增加成功，則把新計數器值存入 MAC PIB 中；如果因溢出導致訊框(Frame)計數器增加失敗，則設備放棄對發送訊框(Frame)的操作並向上層發出狀態爲 FAILED_SECURITY_CHECK 的指示原語 MLME-COMM-STATUS.indication。

用 AES-CTR 套件處理輸入訊框(Frame)時，MAC 層需要執行以下操作：

①如果輸入訊框(Frame)相關的 macDefaultSecurityMaterial 或 ACL 的 ACLSecurityMaterial 欄位中包含外部訊框(Frame)計數器和外部密鑰序列計數器，則透過檢

驗接收的密鑰序列計數器大於或等於外部密鑰序列計數器來保證順序鮮度。如果接收的密鑰序列計數器大於或等於外部密鑰序列計數器，則檢驗接收的訊框(Frame)計數器大於或等於外部訊框(Frame)計數器。如果上述任何一個檢驗失敗，設備將拒絕該輸入訊框(Frame)並向上層發出狀態爲 FAILED_SECURITY_CHECK 的指示原語 MLME-COMM-STATUS.indication。

②從輸入訊框(Frame)或 ACL 中獲取 64 位源位址，從 MAC 訊框(Frame)有效載荷的有效載荷欄位提取出訊框(Frame)計數器和密鑰序列計數器，構造計數器輸入分組。如果因不能獲得資料而不能構造 nonce 值，則設備將向上層發出狀態爲 FAILED_SECURITY_CHECK 的指示原語 MLME-COMM-STATUS.indication。

③按照 AES-CTR 的安全參數和②構造的輸入分組對加密的有效載荷欄位解密。

④把輸入訊框(Frame)的有效載荷欄位替換成③中解密出的資料。如果執行了①的順序保鮮操作並且檢驗成功，則把相應的外部訊框(Frame)計數器和外部密鑰序列計數器更新爲接收訊框(Frame)的訊框(Frame)計數器和密鑰序列計數器的值。

3.5.3 AES-CCM 安全套件

AES-CCM 安全套件利用共用資料、訊框(Frame)計數器和密鑰序列計數器對 MHR 和 MAC 有效載荷部分進行認證和校驗，並對 MAC 有效載荷部分的有效載荷欄位進行加密和解密。在 IEEE802.15.4 中，AES-CCM 的實現支持 32 位、64 位和 128 位完整碼。AES-CCM 套件可提供存取控制、資料加密、完整性認證和順序保鮮 4 種安全服務。

3.5.3.1 資料格式

AES-CCM 安全套件的安全材料存放在 macDefaultSecurityMaterial 或 ACL 的 ACLSecurityMaterial 欄位中，由對稱密鑰、訊框(Frame)計數器、密鑰序列計數器以及可選的外部訊框(Frame)計數器和密鑰序列計數器組成。AES-CCM 安全材料各欄位的順序和長度與 AES-CTR 相同。

AES-CCM 安全訊框(Frame)的有效載荷的有效載荷欄位由 4 部分組成：訊框(Frame)計數器、密鑰序列計數器、加密的有效載荷和加密的完整碼。加密的有效載荷長度等於加密前的有效載荷欄位長度，完整碼的長度可以選擇 4、8 或 16 個位元組，所以 AES-CCM 安全訊框(Frame)的有效載荷長度增加了 9、13 或 21 個位元組。AES-CCM 有效載荷欄位格式如下：

位元組數：4	1	可變長度	4/8/16
對稱密鑰	密鑰序列計數器	加密的有效載荷	加密的完整碼

在 AES-CCM 套件中，用於 CCM 認證和加密的現時值（nonce）的長度是 13 位元組，它由 64 位元源位址、訊框(Frame)計數器和密鑰序列計數器構成。AES-CCM 現時值（nonce）的格式如下：

位元組數：8	4	1
來源位址	訊框(Frame)計數器	密鑰序列計數器

3.5.3.2 安全參數

AES-CCM 套件的 CCM 操作可以參數化以下四點：

- 分組加密功能使用的是 AES 加密演算法；
- 表示訊息長度 L 的欄位長度是 2 位元組；
- 認證碼欄位長度 M 可根據需要選擇 4、8 或 16 位元組；
- 現時值（nonce）具有上述 AES-CCM 現時值的格式。

3.5.3.3 安全操作

用 AES-CCM 套件保護輸出訊框(Frame)時，MAC 層需要執行以下操作：

①從 MAC PIB 中獲取設備的 64 位元擴充位址 aExtendedAddress、訊框(Frame)計數器、密鑰序列計數器值，構造現時值。

②按照 AES-CCM 的安全參數，用①構造的現時值對 MHR 和 MAC 有效載荷部分進行 CCM 認證，對有效載荷欄位和認證時得到的完整碼進行加密。CCM 認證加密過程中，以 MAC 有效載荷部分的有效載荷欄位作爲訊息 m；MHR 及 MAC 有效載荷除去有效載荷欄位的部分作爲附件愛認證資料 a。

③以訊框(Frame)計數器、密鑰序列計數器和②的輸出構造新的有效載荷欄位。

④增加訊框(Frame)計數器。如果訊框(Frame)計數器增加成功，則把新計數器值存入 MAC PIB 中；如果因溢出導致訊框(Frame)計數器增加失敗，則設備放棄對發送訊框(Frame)的操作並向上層發出狀態爲 FAILED_SECURITY_CHECK 的指示原語 MLME-COMM-STATUS.indication。

用 AES-CCM 套件處理輸入訊框(Frame)時，MAC 層需要執行以下操作：

①如果輸入訊框(Frame)相關的 macDefaultSecurityMaterial 或 ACL 的 ACLSecurityMaterial 欄位中包含外部訊框(Frame)計數器和外部密鑰序列計數器，則透過檢驗接收的密鑰序列計數器大於或等於外部密鑰序列計數器來保證順序鮮度。如果接收的密鑰序列計數器大於或等於外部密鑰序列計數器，則檢驗接收的訊框(Frame)計數器大於或等於外部訊框(Frame)計數器。如果上述任何一個檢驗失敗，設備將拒絕該輸入訊框(Frame)並向上層發出狀態爲 FAILED_SECURITY_CHECK 的指示原語 MLME-COMM-STATUS.indication。

②從輸入訊框(Frame)或 ACL 中獲取 64 位元來源位址，從 MAC 訊框(Frame)有效載荷的有效載荷欄位刪除訊框(Frame)計數器和密鑰序列計數器，構造現時值（nonce）。如果因不能獲得資料而不能構造 nonce 值，則設備將向上層發出狀態爲 FAILED_SECURITY_CHECK 的指示原語 MLME-COMM-STATUS.indication。

③按照②構造的現時值，用 CCM 模式對加密的有效載荷欄位進行解密和完整性認證。

如果完整碼校驗失敗，則設備丟棄該訊框(Frame)並向上層發出狀態爲 FAILED_SECURITY_CHECK 的指示原語 MLME-COMM-STATUS.indication。

④把輸入訊框(Frame)的有效載荷欄位替換成③中解密出的資料。如果執行了①的順序保鮮操作並且檢驗成功，則把相應的外部訊框(Frame)計數器和外部密鑰序列計數器更新爲接收訊框(Frame)的訊框(Frame)計數器和密鑰序列計數器的值。

3.5.4 AES-CBC-MAC 安全套件

AES-CBC-MAC 安全套件對 MHR 和 MAC 有效載荷部分進行認證，AES-CBC-MAC 的實現支持 32 位、64 位和 128 位完整碼。AES-CBC-MAC 套件可提供存取控制和完整性認證兩種安全服務。

3.5.4.1 資料格式

AES-CBC-MAC 安全套件的安全材料存放在 macDefaultSecurityMaterial 或 ACL 的 ACLSecurityMaterial 欄位中，它只包含 1 個 128 位對稱密鑰。

AES-CBC-MAC 安全訊框(Frame)的有效載荷欄位是在原有的有效載荷之後添加完整碼，格式如下：

位元組數：可變長度	4/8/16
有效載荷	完整碼

AES-CBC-MAC 套件用來計算完整碼的輸入資料由 3 部分組成：MHR、MAC 有效載荷以及表示認證資料長度的欄位。把輸入資料從高位到低位元劃分成一系列 16 位元組長的輸入分組。AES-CBC-MAC 輸入資料格式如下：

位元組數：1	n	m
n + m	MHR	MAC 有效載荷

3.5.4.2 安全參數

AES-CBC-MAC 套件的 CBC-MAC 操作可以參數化以下 3 點：

- 分組加密功能使用的是 AES 加密演算法；
- CBC-MAC 功能的輸入資料格式如上述定義；
- 完整碼長度 M 可根據需要選擇 32、64 或 128 位元。

3.5.4.3 安全操作

用 AES-CBC-MAC 套件保護輸出訊框(Frame)時，MAC 層需要執行以下操作：

①計算 MHR 和 MAC 有效載荷部分的總長度（位元組數），並編碼存放爲 1 個位元組。

②按照 AES-CBC-MAC 的安全參數及輸入格式，用 CBC-MAC 認證計算 MHR 和 MAC 有效載荷的完整碼。

③在現有的有效載荷欄位後添加②的輸出得到新的有效載荷欄位。

用 AES-CBC-MAC 套件處理輸入訊框(Frame)時，MAC 層需要執行以下操作：

①計算 MHR 和 MAC 有效載荷部分（不包含完整碼）的總長度（位元組數），並編碼存放爲 1 個位元組。

②把接收訊框(Frame)的有效載荷欄位分解成有效載荷和完整碼兩個子欄位；以①計算得到的長度、接收的 MHR 以及不包含的完整碼的 MAC 有效載荷作爲輸入，用 CBC-MAC 計算完整碼並與接收到的完整碼進行比較認證。如果完整碼校驗失敗，則設備丟棄該訊框(Frame) 並向上層發出狀態爲 FAILED_SECURITY_CHECK 的指示原語 MLME-COMM-STATUS.indication。

③把完整碼從 MAC 有效載荷的有效載荷欄位中刪除。

3.6 MAC-PHY 資訊交互流程

圖 32 至圖 38 給出了 IEEE Std802.15.4 的幾項主要功能的 MAC-PHY 資訊交互流程，包括 PAN 的建立、通道掃描、關聯、資料傳輸等。

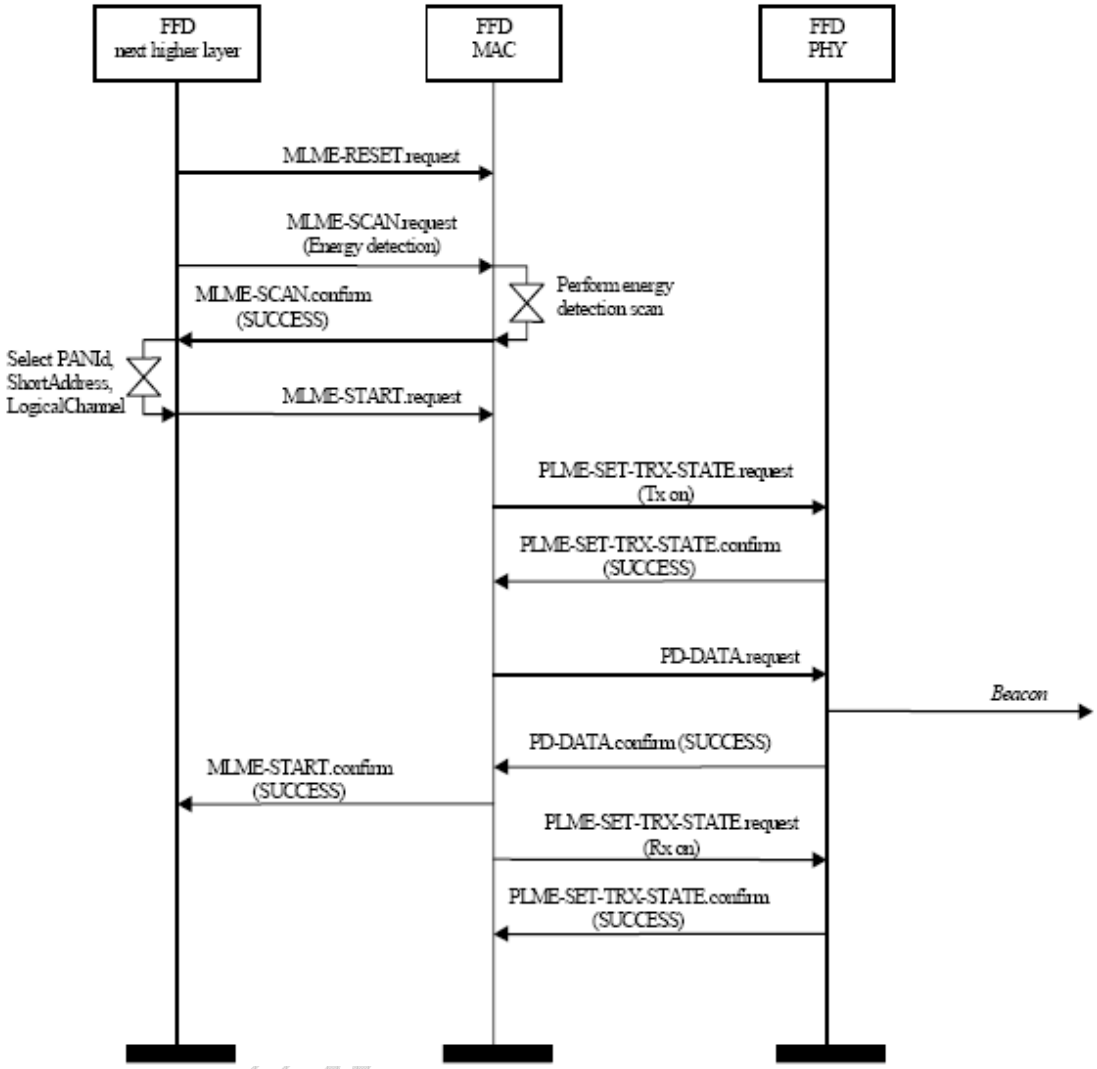


圖 32 建立 PAN 的資訊流程—PAN 協調器

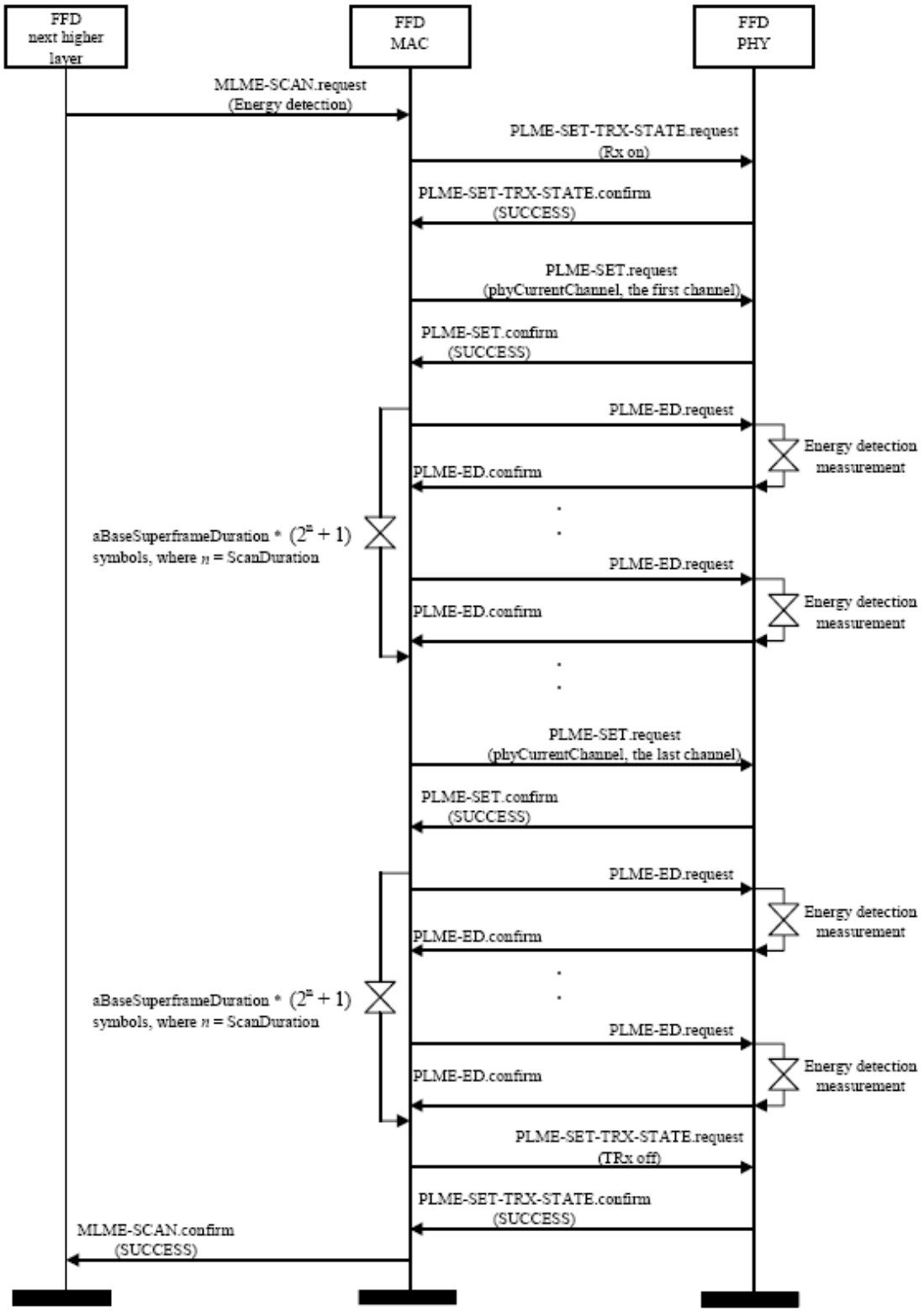


圖 33 ED 掃描資訊流程

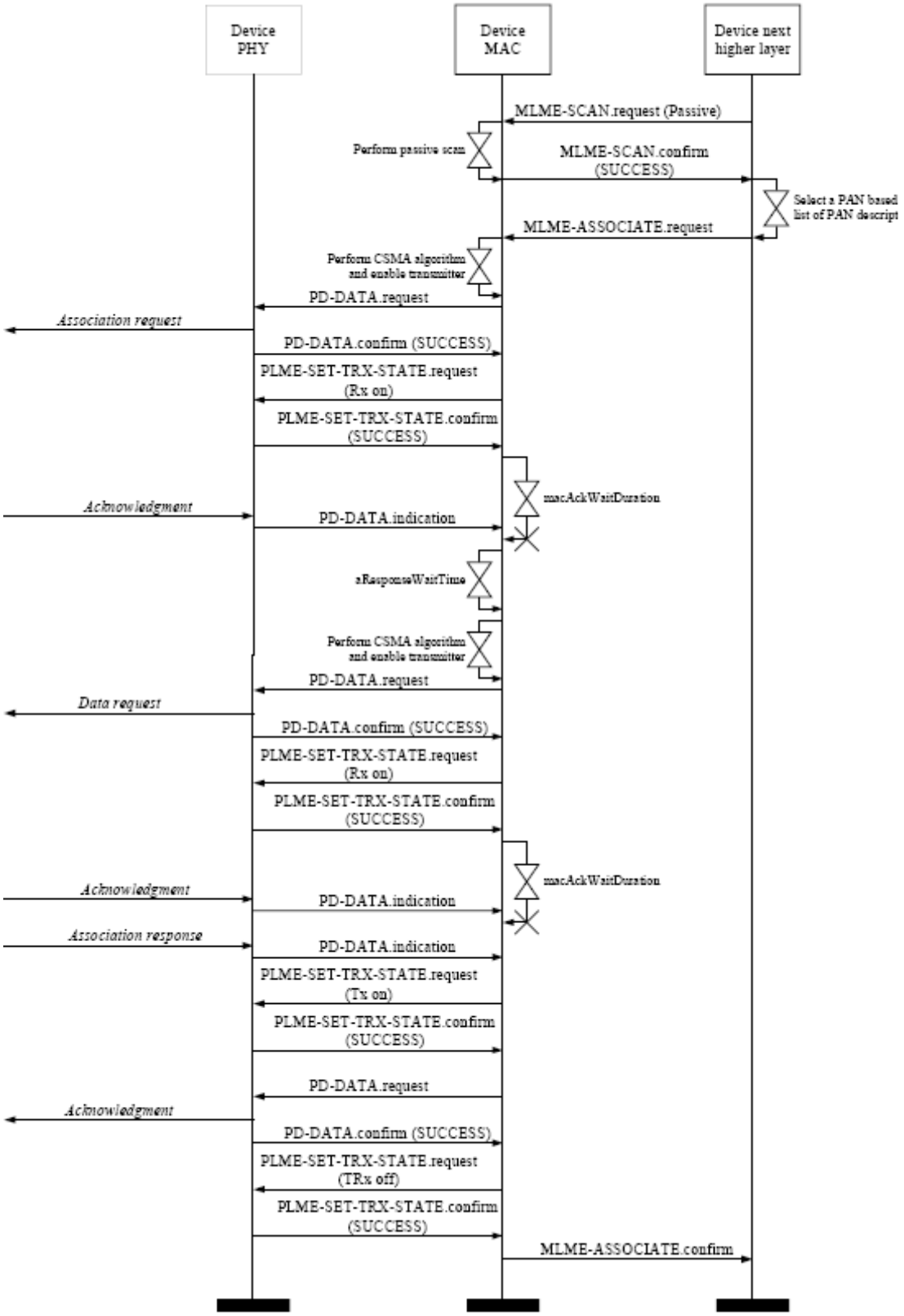


圖 34 關聯的資訊流程—請求設備

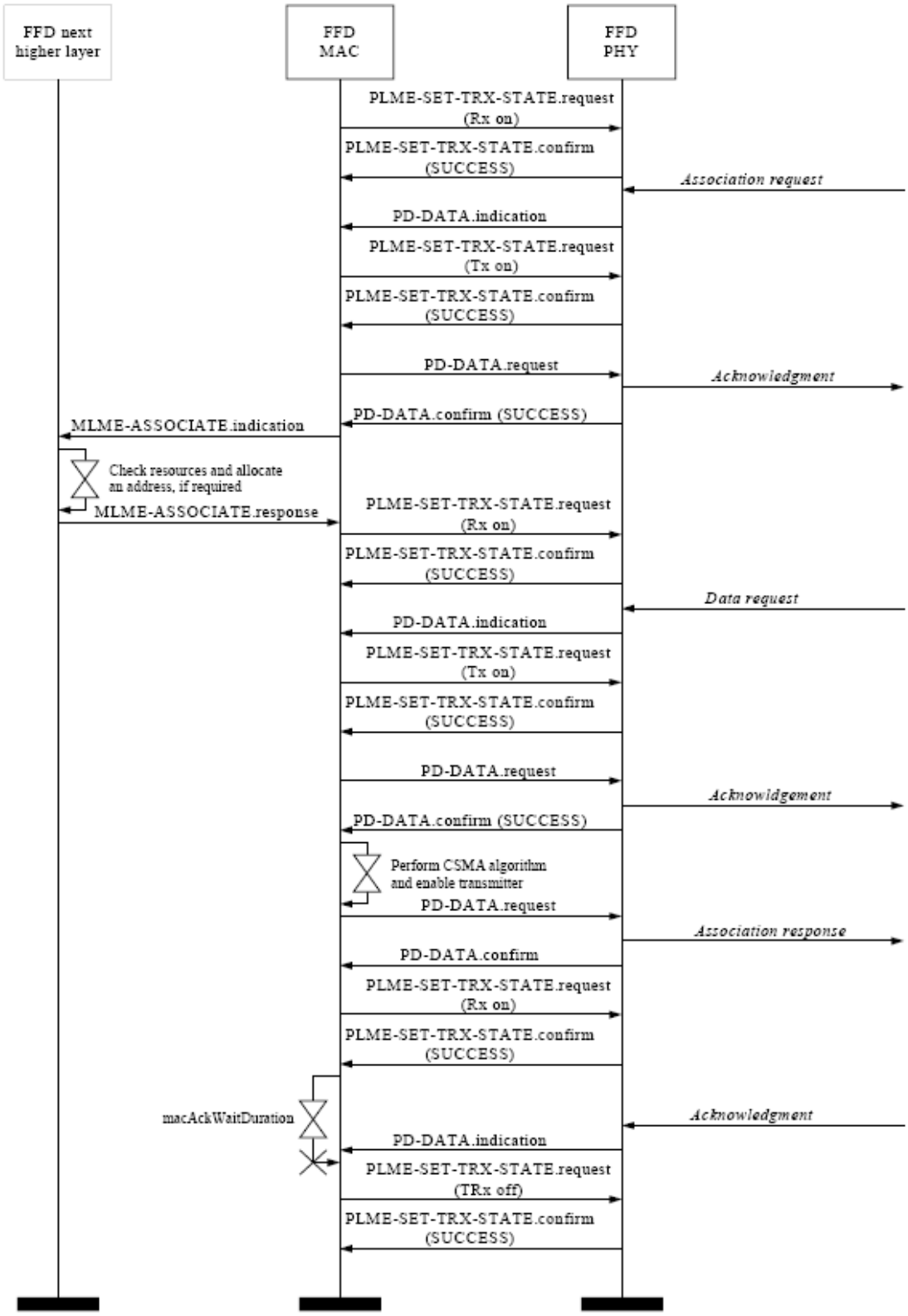


圖 35 關聯的資訊流程—協調器

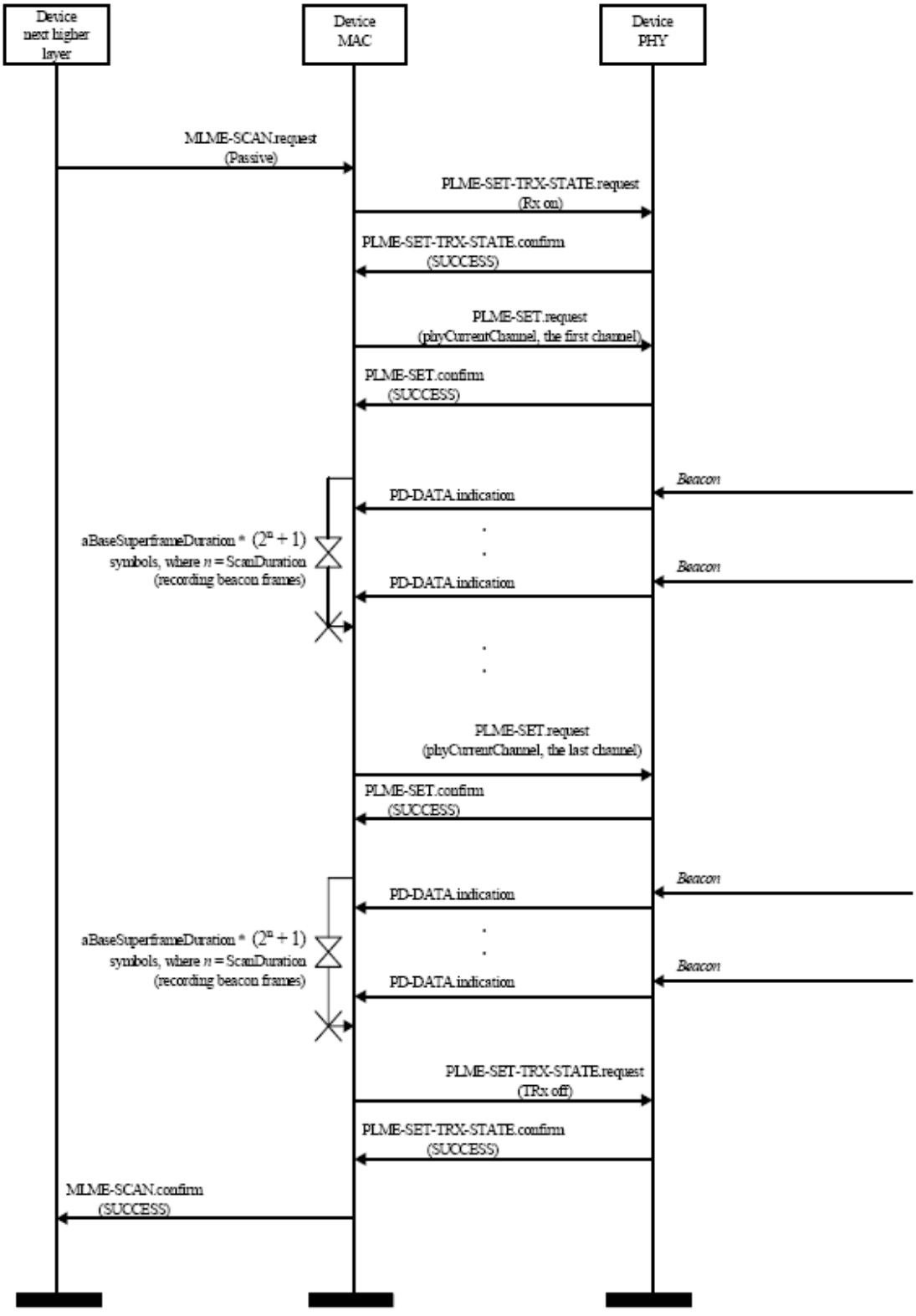


圖 36 被動掃描的資訊流程

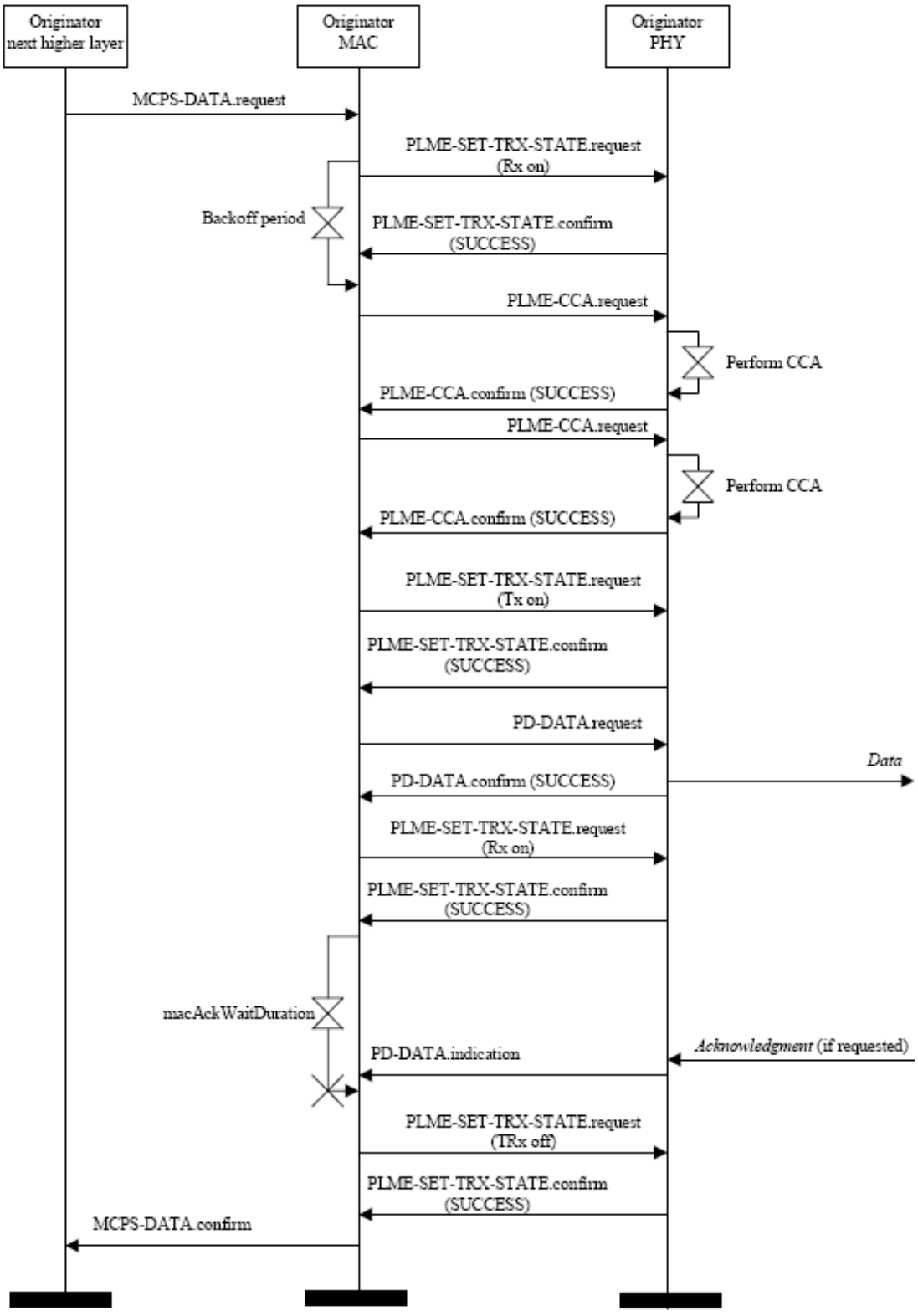


圖 37 資料傳輸的資訊流程—發送設備

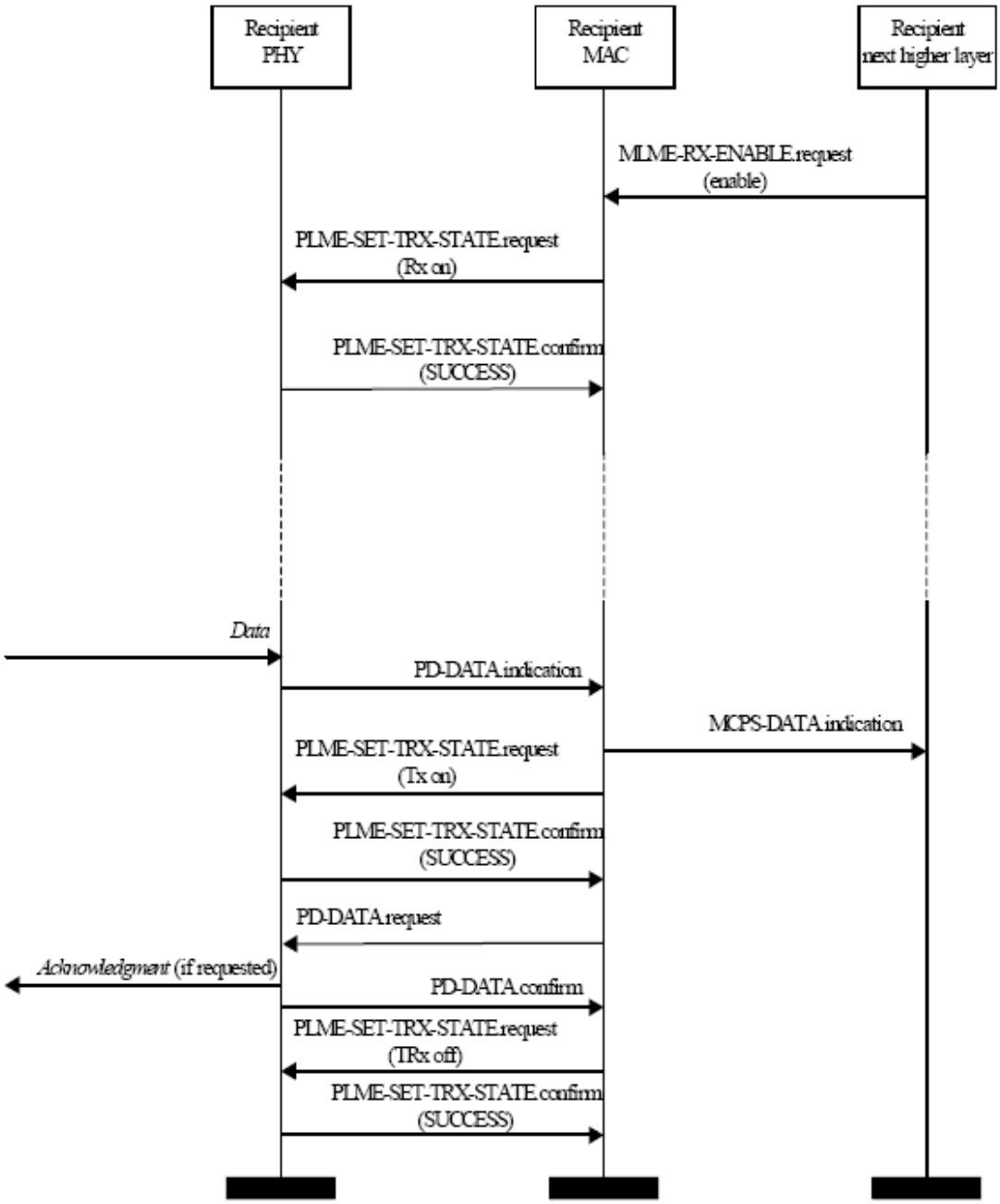


圖 38 資料傳輸的資訊流程—接收設備

第二部分 ZigBee 協定規範

ZigBee 聯盟致力於開發一種極低成本、極低功耗的雙向無線通訊設備。ZigBee 技術將應用於消費電子、家庭樓宇自動化、工業控制、PC 外設、醫療傳感、玩具、遊戲等方面。

ZigBee 規範檔詳細描述了 ZigBee 協定標準。遵照 ZigBee 標準，任何廠商生產的設備和平臺將具有互操作性、低成本和高可用性。

ZigBee 協定堆疊具有多層結構，每一層都爲其上層提供了一組特定的服務：資料實體提供輸出傳輸服務，管理實體提供其他的服務。每個服務實體透過一個服務存取點（SAP）與上層介面，每個 SAP 支援一組服務原語來實現所需的功能。ZigBee 協定堆疊是基於 OSI 七層參考模型的，但是只定義了目標應用市場所要求功能的相關協定層。IEEE802.15.4 標準定義了 ZigBee 協定堆疊的物理層（PHY）和媒體存取控制層（MAC）。ZigBee 聯盟在 IEEE802.15.4 標準的基礎上定義了網路層（NWK）和應用層框架。應用層框架包括應用支援子層（APS）、ZigBee 設備物件（ZDO）和廠商定義的應用物件。

IEEE802.15.4 支援工作在兩個獨立頻段 868/915MHz 和 2.4GHz 的 PHY 層。IEEE802.15.4 的 MAC 子層採用 CSMA-CA 機制對無線通道的存取進行控制。MAC 子層還負責信標發送、同步和提供可靠的傳輸機制。ZigBee 的 NWK 層負責設備加入和離開網路、訊框(Frame)安全和訊框(Frame)路由。另外 NWK 層還負責路由發現和維護、發現單跳鄰居並儲存鄰居相關資訊。ZigBee 協調器的 NWK 層還負責建立一個新網路並爲新關聯設備分配位址。

ZigBee 應用層包括 APS、應用框架（AF）、ZDO 和廠商定義的應用物件。APS 子層負責維護綁定表並在綁定設備間傳遞資訊。綁定是根據服務和需求吧兩個設備進行匹配的能力。ZDO 的任務包括定義設備在網路中的角色（ZigBee 協調器、路由器或終端設備）、初始化和回應綁定請求並在網路設備之間建立安全關係。另外 ZDO 還負責網路設備發現並獲知其所能提供的應用服務。

ZigBee 網路層支援星狀、樹狀和網狀拓撲。在星狀拓撲中，網路由一個稱作 ZigBee 協調器的設備控制，ZigBee 協調器負責網路中設備的初始化和維護，而其他設備（即終端設備）直接與 ZigBee 協調器通訊。在網狀和樹狀拓撲中，ZigBee 協調器負責建立網路並選定網路關鍵參數，但是可以透過 ZigBee 路由器來擴充網路。在樹狀拓撲中，路由器採用分層路由策略在網路中移動資料和控制資訊。樹狀網路可以採用 IEEE802.15.4 定義的面向信標的通訊方式。網狀網路則允許完全對等通訊，網狀網路中的 ZigBee 路由器不得發送規則的信標。

本文件介紹的是 ZigBee V1.0 規範。

1. 應用層規範

1.1 應用層規範概述

ZigBee 應用層包括 APS 子層、ZDO（包含 ZDO 管理平臺）和廠商定義的應用物件。APS 子層的任務是維護綁定表和在綁定設備之間傳遞資訊。ZDO 負責定義設備在網路中的角色（如 ZigBee 協調器或終端設備）、發現設備並決定設備所能提供的應用服務、初始化並回應綁定請求和在網路設備之間建立安全關係。

應用支援子層（APS）提供了網路層（NWK）和應用層（APL）之間的介面，其介面功能是透過 ZDO 和廠商定義的應用物件都可以使用的一組服務來實現的。APS 子層的服務透過兩個實體來提供：APS 資料實體（APSDE）透過 APSDE 服務存取點（APSDE-SAP）提供；APS 管理實體（APSME）透過 APSME 服務存取點（APSME-SAP）提供。APSDE 提供的資料傳輸服務在同一網路的兩個或多個設備之間傳輸應用層 PDU；APSME 提供設備發現和綁定服務，並維護一個管理物件資料庫 — APS 資訊庫（AIB）。

ZigBee 應用框架是應用物件駐留在 ZigBee 設備中的環境。在應用框架內，應用物件透過 APSDE-SAP 發送和接收資料。應用物件的控制和管理透過 ZDO 公共介面來實現。透過 APSDE-SAP 提供的資料服務包括資料傳輸的請求、證實、回應和指示原語。請求原語支援對等應用實體間的資料傳輸；證實原語報告請求原語調用的結果；指示原語用來指示從 APS 到目的應用物件實體的資料傳輸。ZigBee 可定義多達 240 個不同的應用物件，以標號 1～240 的端點爲介面。另外還定義了兩個端點：0 端點用於 ZDO 的資料介面，255 端點用作向所有應用物件提供廣播資料的介面，241～254 號端點預留給未來應用。使用 APSDE-SAP 提供的這些服務，應用框架提供給應用物件兩種資料服務：鍵值對服務和一般訊息服務。鍵值對（KVP）服務允許採用狀態變數的方法操作應用物件定義的屬性。該狀態變數包含獲取（get）、獲取回應（get response）、設置（set）和事件（event）四種事務，其中後兩種事務能以要求回應的請求方式發送，這樣就有相應的設置回應（set response）和事件回應（event response）事務。另外，KVP 採用壓縮 XML 標記資料結構。這種解決方案爲小型設備提供了很好的命令/控制機制，並保留了向完全 XML 的擴充性。但是，ZigBee 的許多目標應用領域採用專用協定，很難映射到 KVP；另外由於狀態變數方法要能支援 get、set、event 中任何一個事務就要求設備維護儲存狀態變數，這就增加了 KVP 的開銷。針對這些情況，ZigBee 也支援一般的訊息（MSG）服務。MSG 服務類型採用與 KVP 一樣的傳輸機制；所不同的是，MSG 的 APS 資料訊框(Frame)不攜帶任何內容，而是留給配置檔開發者來定義。

ZigBee 的定址包括節點定址和端點定址。圖 1 的ZigBee 系統有兩個節點，每個節點有一個射頻端。其中一個節點包含 2 個開關，另一個節點包含 4 個電燈。一個節點包含 1 個或多個設備描述，但只有一個 IEEE 802.15.4 無線射頻端。節點的每個設備描述爲一個子單元，節點加入 ZigBee 網路時被分配一個位址。圖 1 中第 1 個開關控制 1、2、3 號燈，而第 2 個開關僅控制 4 號燈。如果僅僅能定址射頻端，就不可能識別或定址每個子單元，所以第 2 個開關就不可能只開啓 4 號燈。於是，ZigBee 提供了另一個層次的定址 — 端點定址。端點定址結合 IEEE 802.15.4 機制使用，每個開關和電燈可以用一個端點號來識別。例如在上面的例子中，第 1 個開關可使用端點 3，第 2 個開關可使用端點 21；類似地，每個電燈也有各自的端點。端點 0 留給設備管理，用來定址節點中的描述符。節點中每個可識別的子單元（如開關和電燈）都分配有一個 1～240 範圍內特定的端點。物理設備的描述是根據其包含的資料屬性描述。如溫度計包含一個輸出屬性“溫度”，表示房間的當前溫度；鍋爐控制器可用這個屬性作爲輸入，根據從溫度計接收到的溫度值來控制鍋爐。這兩種物理設備及其屬性將用相關設備描述來定義。這種簡單的房間溫度計有溫度感應電路供外部鍋爐控制器查詢，它以簡單描述在一個端點上描述並發佈服務。一個更複雜的溫度計可以有一個可選的“心跳”報告計時器，使設備以設定的週期報告當前房間溫度。這種實現將在一個不同的端點發佈它的服務。爲了允許市場產品的多樣性，製造商可以增加包含自己額外屬性的簇。製造商專用簇不是 ZigBee 規範的內容，所以這些簇的互操作性不能保證。這些服務將在與上述端點不同的端點上發佈。

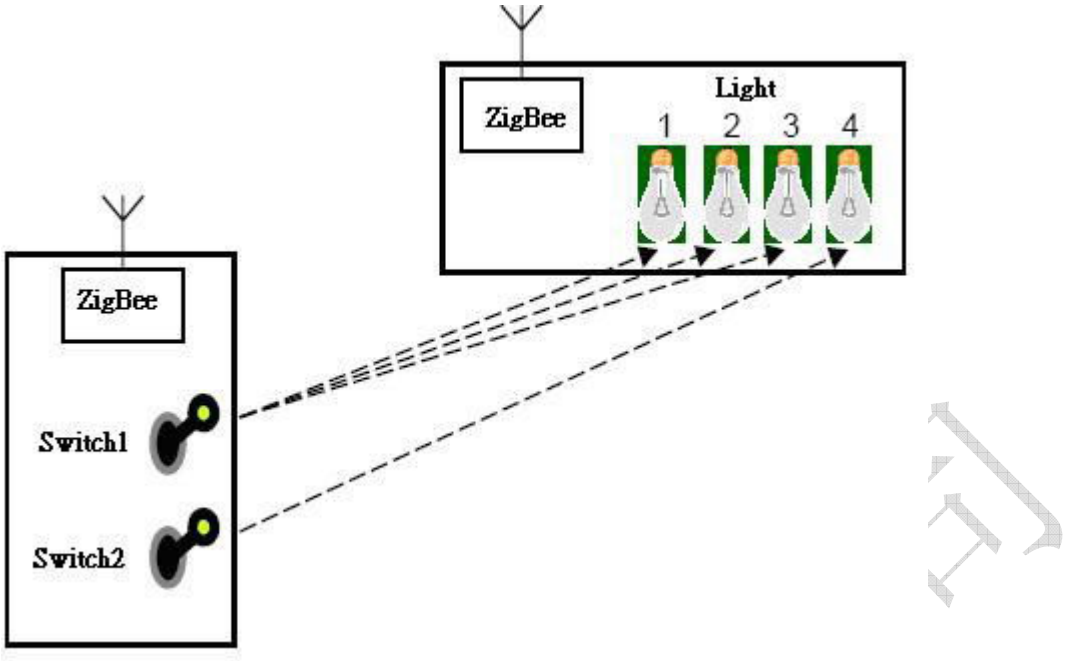


圖 1 一種簡單的照明控制 ZigBee 系統

配置檔是一種關於訊息、訊息格式和處理動作的協定，它使得不同設備上的應用根據該協定發送命令、請求資料、處理命令/請求能實現可互操作的、分散式應用。例如，一個節點上的溫度計與另一個節點上的鍋爐通訊，它們共同構成一個加熱應用配置檔。配置檔由 ZigBee 廠商開發，爲特定的技術需求提供解決方案。另外，配置檔也是一種在 ZigBee 標準內統一互操作技術方案、在特定市場範圍內專注可用性的方式。例如，照明設備廠商提供的 ZigBee 配置檔要能夠與幾種不同的照明類型或控制方式互操作。

簇透過簇標識來識別，簇標識與流出或流入設備的資料關聯。在特定配置檔的範圍內簇標識是唯一的。綁定判斷就是匹配同一個配置檔內的一個輸出簇標識和一個輸入簇標識。在上面的加熱配置檔中，綁定發生在一個以溫度簇標識爲輸出的設備和一個以溫度簇爲輸入的設備間。綁定列表包含 8 位元的溫度簇標識以及源設備和目的設備位址。

設備發現是 ZigBee 設備以廣播或單播方式初始化查詢來發現其他 ZigBee 設備的過程。有兩個格式的設備發現請求：IEEE 位址請求和 NWK 位址請求。IEEE 位址請求時單播方式並且 NWK 位址已知；NWK 位址請求時廣播方式並以已知的 IEEE 位址作爲資料載荷。對廣播或單播設備發現訊息的回應因邏輯設備類型的不同而不同：ZigBee 終端設備根據請求格式發送 IEEE 或 NWK 位址來回應設備發現查詢；ZigBee 協調器發送 IEEE 或 NWK 位址以及該 ZigBee 協調器關聯的所有設備的 IEEE 或 NWK 位址來回應設備發現查詢；ZigBee 路由器發送 IEEE 或 NWK 位址以及該 ZigBee 路由器關聯的所有設備的 IEEE 或 NWK 位址來回應設備發現查詢。

服務發現是外部設備獲知接收設備端點所能提供的服務的過程。服務發現可以透過發送針對設備每個端點的查詢或透過使用匹配服務特性（廣播或單播）來實現。服務發現使用複雜、使用者、節點或電源描述符外加簡單描述符來實現。ZigBee 的服務發現過程是網路中設備介面的關鍵。

ZigBee 中有一個應用級概念：在不同節點的各個端點上使用簇標識。這就是綁定 — 在互補的應用設備和端點間產生邏輯鏈路。如在上述加熱系統中可以把溫度計和鍋爐控制器綁定；圖 1 中，開關 1 和電燈 1~3 綁定；而開關 2 只和電燈 4 綁定。節點間哪個簇被綁定的資訊儲存在綁定列表中。開關 1 的綁定列表中的 3 個條目允許它控制 3 盞電燈，另外，一盞電

燈也可以同時受幾個開關控制。綁定總是在通訊鏈路建立後執行。一旦鏈路建立，實現將決定一個新節點是否是網路的一部分。這將依賴于應用的操作安全性和實現的方式。只有所有設備實現的安全性允許時才允許綁定。綁定列表在 ZigBee 協調器中實現，這是因爲在網路工作的任何時間都需要綁定列表，並且 ZigBee 協調器通常是幹線供電的。

ZigBee 的訊息傳遞有 3 種方式：直接定址、間接定址和廣播定址。一旦設備關聯，命令就可以從一個設備發送到另一個設備。命令發送給目的位址（射頻位址加端點）的應用物件。值得注意的是，綁定並不是使用直接定址的先決條件。直接定址認爲設備發現和服務發現已經識別到一個特定的設備和支援請求設備要求服務的端點。直接定址定義了一種包含完全位址和端點資訊的訊息傳輸方式。直接定址要求控制設備獲知目標設備的位址、端點、簇標識和屬性標識，並且在直接定址資訊產生之前要把這些資訊提交給 ZigBee 協調器的綁定列表。一個完整的 IEEE 802.15.4 位址達到 10 個位元組（PAN 標識加 64 位元 IEEE 位址），另外還有端點所要求的位元組。特別簡單的設備，如電池供電的開關，可能不希望儲存這些開銷並且軟體也不需要這些資訊，這時間接定址則更合適。當一個源設備用間接定址方式向一個目的設備發送命令時，它不包含目的設備的位址（不知道或沒有儲存）而是透過 APSDE-SAP 指定間接定址。間接定址訊息中包含的源位址、源端點和簇標識透過綁定列表轉換成目的設備的位址資訊，並把訊息轉發給目的設備。當簇中包含幾個屬性時，簇標識用來定址而屬性標識用在命令中來標識簇中的特定屬性。屬性沒有用在間接定址機制中，而是看作資料載荷的一部分。然而，應用可以解析和使用屬性。應用可能向一個目的設備的所有端點廣播訊息，這種廣播定址方式叫作“應用廣播”。目的位址是 16 位元網路廣播位址，廣播標記在 APS 訊框(Frame)的控制欄位設置。APS 訊框(Frame)的源位址資訊包含簇標識、配置檔標識和源端點欄位。

ZigBee 設備物件（ZDO）代表功能的基本類，在應用物件、設備配置檔和 APS 之間提供一個介面。ZDO 位於應用框架和應用支持子層之間，它滿足 ZigBee 協定棧中所有應用的共同要求。ZDO 主要負責以下工作：初始化應用支援子層（APS）、網路層（NWK）和安全服務規範（SSS）；集合終端應用的配置資訊以判定和實現發現、安全管理、網路管理和綁定管理。ZDO 在應用框架層和應用物件之間有一個公共介面，應用物件透過這個公共介面控制設備和網路功能。ZDO 與 ZigBee 協定堆疊的下層介面時，在端點 0 上透過 APSDE-SAP 交互資料資訊，透過 APSME-SAP 交互控制資訊。ZDO 的公共介面在 ZigBee 協定堆疊的應用框架層內提供設備位址管理、發現、綁定和安全功能。發現管理提供給應用物件，當 ZigBee 終端設備收到設備發現查詢命令時，它將返回 IEEE 位址；當 ZigBee 協調器或路由器收到設備查詢命令時，還要返回關聯在該協調器或路由器上的所有其他設備的位址。除了設備發現功能，服務發現功能用來探定設備中各個應用物件對應的端點所能提供的服務。透過服務發現，設備能夠發現啓動的端點以及滿足一定準則的特定服務。提供給應用物件的綁定管理用來綁定 ZigBee 設備間的應用物件，以明確應用物件透過協定堆疊的各層和 ZigBee 網路節點的鏈結關係。綁定表根據綁定調用和結果來編制，終端設備綁定、設備間的綁定和解綁定命令透過 ZigBee 設備配置檔來支援。提供給應用物件的安全管理用來開啓或關閉 ZigBee 系統的安全服務。如果安全服務開啓，則需要執行密鑰管理程式來管理主密鑰、網路密鑰以及建立鏈路密鑰的方式。

1.2 ZigBee 應用支援子層（APS）

1.2.1 APS 概述

應用支援子層透過一組 ZigBee 設備物件（ZDO）和廠商定義的應用物件都可使用的服務，提供了網路層和應用層之間的介面。這些服務透過兩個實體來提供；APS 資料實體（APSDE）透過 APSDE-SAP 提供資料傳輸服務；APS 管理實體（APSME）透過 APSME-SAP 提供管理服務並維護一個管理物件資料庫—APS 資訊庫（AIB）。

APSDE 提供資料服務給網路層以及 ZDO 和應用物件，使得應用 PDU 能夠在兩個或多個設備間傳輸。APSDE 提供以下服務：

- 產生應用級 PDU（APDU）。APS 在應用 PDU 上增加適當的協定頭產生 APS PDU。
- 綁定。根據服務和需求把兩個設備進行匹配。一旦綁定了兩個設備，APSDE 就能夠把從一個綁定設備接收到的資訊發送給下一個設備。

APSME 提供管理服務，允許應用於協定堆疊進行交互。APSME 能夠提供根據設備的服務和需求來匹配兩個設備的能力。這種服務稱作“綁定服務”。APSME 應能構造和維護一個表來儲存這種資訊。此外，APSME 還提供以下兩種服務：

- AIB 管理—獲取和設置設備 AIB 屬性的能力。
- 安全管理—透過使用安全密鑰設置與其他設備之間信任關係的能力。

1.2.2 服務規範

APS 提供了上一層實體（NHLE）和 NWK 層之間的介面。APS 子層概念上包含一個管理實體—APS 子層管理實體（APSME）。透過該管理實體提供的服務介面可以調用 APS 子層的管理功能。另外 APSME 還負責維護一個與 APS 子層有關的被管理物件資料庫，該資料庫稱作“APS 子層資訊庫（AIB）”。圖 2 描述了 APS 子層的元件和介面。APS 子層透過兩個服務存取點（SAP）提供了兩類服務，即透過 APS 資料實體 SAP（APSDE-SAP）提供的資料服務和透過 APS 管理實體 SAP（APSME-SAP）提供的管理服務。這兩類服務經 NLDE-SAP 和 NLME-SAP 提供了 NHLE 與 NWK 層之間的介面。除了這些外部介面，APS 子層的 APSME 和 APSDE 之間還隱含了一個介面，允許 APSME 使用 APS 資料服務。

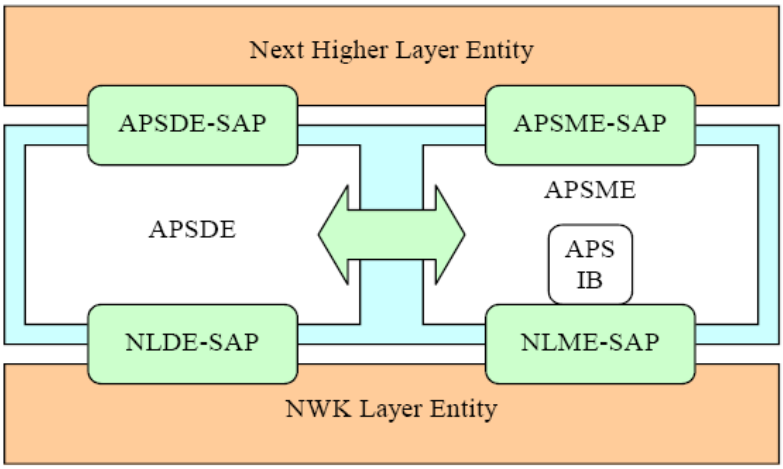


圖 2　APS 子層的參考模型

1.2.2.1 APS 資料服務

APSDE-SAP 支援在對等應用實體之間傳輸應用協定資料單元。APS 資料服務透過 3 個原語來實現：APSDE-DATA.request、APSDE-DATA.confirm 和 APSDE-DATA.indication。

APS 資料請求原語 APSDE-DATA.request 請求吧本地 NHLE 的一個 PDU（即 ASDU）傳送到一個對等的 NHLE 實體。該原語的語法如下：

APSDE-DATA.request（DstAddrMode，DstAddress，DstEndpoint，ProfileId，ClusterId，SrcEndpoint，asduLength，asdu，TxOptions，DiscoverRoute，RadiusCounter）

其中各參數的定義如下：DstAddrMode 爲整數，指示目的位址定址模式，0x00 表示目的位址 DstAddress 和目的端點 DstEndpoint 都不存在，0x01 表示 DstAddress 爲 16 位元短位址並且 DstEndpoint 存在，0x02 表示 DstAddress 爲 64 位元擴充位址並且 DstEndpoint 存在；DstAddress 爲 ASDU 目的實體的設備位址，其格式由 DstAddrMode 參數決定；DstEndpoint 爲 ASDU 目的實體的端點位址，它的取值範圍是 0x00～0xFF；ProfileId 表示該訊框(Frame)應用配置檔的標識，其取值範圍是整數 0x0000～0xFFFF；ClusterId 表示間接定址發送訊框(Frame)時綁定操作中所用物件的標識，如果沒有使用間接定址，則忽略該參數；SrcEndpoint 表示發送 ASDU 源端點位址，其取值範圍是整數 0x00～0xFE；asduLength 表示 ASDU 長度的位元組數；TxOptions 的前 5 位爲 0，最後 3 位元用來設置發送選項（最後 1 位元爲 1 表示安全致能傳輸，倒數第 2 位爲 1 表示採用 NWK 密鑰，倒數第 3 位爲 1 表示要求確認的傳輸）；DiscoverRoute 參數把應用層的控制資訊提供給網路層，指定路由發現時將採取的措施。取值 0x00 表示抑制路由發現，即利用現存的路由資訊來處理資料發送請求；0x01 表示致能路由發現，即如果現存路由中沒有該請求所要求的路由，則執行路由發現；0x02 表示強制路由發現，即處理資料發送請求之前總是要求執行路由發現；RadiusCounter 爲一個無符號整數，表示允許廣播訊框(Frame)在網路中傳播的跳數，其取值範圍是 0x00～0xFF。

當本地 NHLE 有資料 PDU（也即 ASDU）要發送到一個對等的 NHLE 時，就產生 APS 資料請求原語 APSDE-DATA.request。當 APS 子層實體收到 APSDE-DATA.request 原語後，就開始傳送 NHLE 提供的 ASDU。如果 DstAddrMode 參數設爲 0x00，則忽略 DstAddress 和 DstEndpoint 參數，生產的 APDU 中也不含 DstEndpoint 參數值；如果 DstAddrMode 參數設爲 0x01，則 DstAddress 參數包含一個 16 位元短位址並把 DstEndpoint 參數值放在產生的

APDU 中；如果 DstAddrMode 參數設爲 0x02，則 DstAddress 參數包含一個 64 位 IEEE 位址，並把 DstEndpoint 參數值放在產生的 APDU 中。DiscoverRoute 參數根據應用要求網路層執行的路由發現動作來設定，應用可能會要求 APS 確認或應用級訊息回應來判定訊息是否可靠送達了目的地。應用可使用 DiscoverRoute 參數請求網路層執行路由發現，以增加訊息傳遞的可靠性。如果發送網路廣播訊息（DstAddress 設爲 0xFFFF），應用可指定 RadiusCounter 參數，0x00 表示指向網路中的所有設備，取 0x01～0xFF 之間的值表示廣播訊息在網路中傳播的範圍，用跳數來表示。

如果採用直接定址（即存在目的位址）方式發送 APDU，則 APSDE 向網路層發出 NLDE-DATA.request 原語，把構造的 APDU 訊框(Frame)發送到 NWK 層。收到 NWK 層的 NLDE-DATA.confirm 證實原語後，APSDE 也向其上層發出同樣狀態的 APSDE-DATA.confirm 原語。如果採用間接定址方式發送 APDU 並且是 ZigBee 協調器或路由器的 APSDE 收到了資料發送請求原語，設備就搜索綁定表，尋找與 SrcEndpoint 參數指定的發送設備端點綁定的設備。如果沒有找到綁定設備，APSDE 就向上層狀態爲 NO_BOUND_DEVICE 的證實原語 APSDE-DATA.confirm。如果找到一個或多個綁定設備，則 APSDE 用綁定設備的目的位址和端點資訊構造 APDU 並調用 NLDE-DATA.request 原語發送到 NWK 層；收到相應的 NLDE-DATA.confirm 證實原語後，APSDE 接著構造發送到下一個綁定設備的 APDU，直到沒有剩餘的綁定設備。收到最初的請求後，APSDE 就向上層發出狀態爲 SUCCESS 的 APSDE-DATA.confirm 證實原語，表示資訊將被轉發給綁定表中的每一個綁定設備。如果採用間接定址方式發送 APDU 並且是 ZigBee 終端設備（非 ZigBee 協調器、非 ZigBee 路由器）的 APSDE 收到了資料發送請求原語，則 APSDE 構造沒有目的端點欄位的 APDU 並透過 NLDE-DATA.request 原語發送給 NWK 層。收到 NLDE-DATA.confirm 證實原語後，APSDE 也向其上層發出同樣狀態的 APSDE-DATA.confirm 原語。

如果 TxOptions 參數指定要求加密傳輸，APS 子層就要採用安全服務來保護 ASDU。如果安全處理失敗，APSDE 將向上層發出狀態爲 SECURITY_FAIL 的證實原語 APSDE-DATA.confirm。APSDE-DATA.confirm 原語報告本地 NHLE 請求向一個對等的 NHLE 傳送資料的結果。該證實原語的語法如下：

APSDE-DATA.confirm（DstAddrMode，DstAddress，DstEndpoint，SrcEndpoint，Status）

其中：前 4 個參數的定義同 APSDE-DATA.request 原語；Status 參數表示相應請求的狀態，該枚舉量可取值爲 SUCCESS、NO_BOUND_DEVICE、SECURITY_FAIL 或是 NLDE.confirm 原語返回的任意狀態值。

APSDE-DATA.confirm 原語由 APS 子層實體產生，作爲對 APSDE-DATA.request 原語的回應。該證實原語返回 SUCCESS 狀態指示請求發送成功，或返回狀態爲錯誤程式 NO_BOUND_DEVICE、SECURITY_FAIL 或是 NLDE.confirm 原語返回的任意狀態值。APSDE-DATA.confirm 原語由 APS 發送給上層，通知其請求資料發送的結果。如果發送嘗試成功，該證實原語的狀態參數設備 SUCCESS，否則狀態參數指示錯誤原因。

APSDE-DATA.indication 原語用來指示一個資料 PDU 從 APS 子層傳送到本地應用實體。該指示原語的語法如下：

APSDE-DATA.indication（DstEndpoint，SrcAddrMode，SrcAddress，SrcEndpoint，ProfileId，ClusterId，asduLength，asdu，WasBroadcast，SecurityStatus）

其中：參數 DestEndpoint 表示 ASDU 要傳送到本地實體目標端點；SrcAddrMode 參數表示原語中使用的原位址模式和發送 APDU 要使用的位址模式，其取值同 APSDE-DATA.request 原語中的 DstAddrMode 參數；SrcAddress 和 SrcEndpoint 參數分別表示發送 ASDU 的設備位址和源端點；ProfileId 參數表示產生該訊框(Frame)的配置檔標識；ClusterId 表示被接收物件

的標識；asdu 和 asduLength 參數分別表示 APSDE 指示的 ASDU 內容和長度位元組數；WasBroadcast 參數是一個布林量，如果接收到的是廣播訊息，則設爲 TRUE，否則設爲 FALSE；SecurityStatus 參數是一個枚舉量，如果接收到的 ASDU 沒有採取任何安全措施則設爲 UNSECURED，如果接收的 ASDU 受 NWK 密鑰保護就設爲 SECURED_NWK_KEY，如果接收的 ASDU 受鏈路密鑰保護就設爲 SECURED_LINK_KEY。

當 APS 子層接收到來自本地 NWK 層實體定址正確的資料訊框(Frame)時，就向其上一層發出 APSDE-DATA.indication 指示原語。如果 ASDU 訊框(Frame)頭的控制欄位顯示採用了安全機制，則需要作相應的安全處理。APS 的上一層收到該指示原語就得到了資料到達設備的通知。

1.2.2.2 APS 管理服務

APS 管理實體 SAP（APSME-SAP）支援在 APSME 和上層之間傳送管理命令。APSME 透過 APSME-SAP 介面支援的原語包括 APSME-BIND、APSME-UNBIND、APSME-GET 和 APSME-SET。

APSME-BIND 和 APSME-UNBIND 原語定義設備上以層如何向本地綁定表中增加綁定記錄和從綁定表中刪除記錄。

綁定請求原語 APSME-BIND.request 允許 APS 的上一層請求把兩個設備綁定到一起，該原語由 ZigBee 協調器或該請求的源位址參數 SrcAddr 指示設備的 APS 上層發出，APSME-BIND.request 原語的語法如下：

APSME-BIND.request （SrcAddr，SrcEndpoint，ClusterId，DstAddr，DstEndpoint）

其中：SrcAddr 和 DstAddr 參數是有效的 64 位元 IEEE 位址，分別表示本次綁定的源位址和目的位址；SrcEndpoint 和 DstEndpoint 參數分別表示本次綁定的源端點和目的端點；ClusterId 表示將被綁定到目的設備的源設備的簇標識。

綁定請求原語由上層發給 APS 子層，在 ZigBee 協調器或綁定源設備上啓動以個綁定操作。ZigBee 協調器或原語 SrcAddr 參數指示設備的 APS 接收到來自 NHLE 的 APSME-BIND.request 原語後，APSME 將嘗試在其綁定表中建立原語指定的綁定記錄。如果綁定記錄建立成功，APSME 就向其上層發出狀態爲 SUCCESS 的綁定證實原語 APSME-BIND.confirm；如果綁定表中容量不夠建立綁定記錄，APSME 就向其上層發出狀態爲 TABLE_FULL 的 APSME-BIND.confirm 原語。

APSME-BIND.confirm 原語用來通知上層其請求直接綁定或代理綁定兩個設備的結果。綁定證實原語的語法如下：

APSME-BIND.confirm （Status，SrcAddr，SrcEndpoint，ClusterId，DstAddr，DstEndpoint）

其中：參數 Status 是一個枚舉量，表示綁定請求的結果，其值可取 SUCCESS、ILLEGAL_DEVICE、ILLEGAL_REQUEST、TABLE_FULL、NOT_SUPPORTED；其他參數的定義同綁定請求原語。

APSME-BIND.confirm 原語由 APSME 產生併發送給 NHLE，作爲對綁定請求原語 APSME-BIND.request 的回應。如果綁定請求成功，設置 Status 參數爲 SUCCESS；否則 Status 參數設置爲一個錯誤程式 ILLEGAL_DEVICE、ILLEGAL_REQUEST 或 TABLE_FULL。NHLE 接收到該證實原語後，就獲知了綁定請求的結果。

解綁定請求原語 APSME-UNBIND.request 允許 APS 的上一層請求解除兩個設備的綁定，該原語由 ZigBee 協調器或該請求的源位址參數 SrcAddr 指示設備的 APS 上層發出。

APSME-UNBIND.request 的語法如下：

APSME-UNBIND.request （SrcAddr，SrcEndpoint，ClusterId，DstAddr，DstEndpoint）

其中：參數 SrcAddr 和 DstAddr 分別是綁定記錄的源 IEEE 位址和目的 IEEE 位址；SrcEndpoint 和 DstEndpoint 參數分別是綁定記錄的源端點和目的端點；ClusterId 參數是被綁定的兩個設備中源設備的簇標識。

APSME-UNBIND.request 原語由上層發給 APS 子層，在 ZigBee 協調器或綁定源設備上啓動解除綁定操作。如果以個尚未加入網路的設備接收到該原語，APSME 就向其上層發出狀態參數值爲 ILLEGAL_REQUEST 的解綁定證實原語 APSME-UNBIND.confirm；如果 ZigBee 協調器或者解綁定請求原語中 SrcAddr 對應的設備收到來自 NHLE 的 APSME-UNBIND.request 原語；如果綁定表中找不到請求的記錄，APSME 就向 NHLE 發出 Status 參數置爲 INVALID_BINDING 的 APSME-UNBIND.confirm 原語；如果綁定的設備不在網路中，APSME 就向 NHLE 發出 Status 參數置爲 ILLEGAL_DEVICE 的 APSME-UNBIND.confirm 原語。

APSME-UNBIND.confirm 原語用來通知上層其請求直接解除或代理解除兩個綁定設備的結果。APSME-UNBIND.confirm 原語的語法如下：

APSME-UNBIND.confirm(Status，SrcAddr，SrcEndpoint，ClusterId，DstAddr，DstEndpoint）

其中：參數 Status 是枚舉量，表示解綁定請求的結果，其值可取 SUCCESS、ILLEGAL_DEVICE、INVALID_BINDING；其他參數的定義同解綁定請求原語。

APSME-UNBIND.confirm 原語由 APSME 產生並發給其 NHLE，作爲對 APSME-UNBIND.request 原語的回應。如果請求成功，Status 參數置爲 SUCCESS 來指示成功的解綁定請求；否則，Status 置爲一個錯誤程式 ILLEGAL_DEVICE、ILLEGAL_REQUEST 或 INVALID_BINDING。NHLE 接收到 APSME-UNBIND.confirm 原語就被告知了請求解綁定的結果。

APSME-GET 和 APSME-SET 原語定義了 APS 上層如何對 APS 資訊庫（AIB）的屬性進行讀寫。APSME-GET.request 原語允許上層讀取 AIB 屬性值，其語法如下：

APSME-GET.request （AIBAttribute）

其唯一參數 AIBAttribute 是要讀取的 AIB 屬性的標識。

APSME 接收到 APSME-GET.request 原語後，就到其資料庫中檢索請求的 AIB 屬性。如果資料庫中找不到請求的 AIB 屬性標識，APSME 就向其上層發出狀態爲 UNSUPPORTED_ATTRIBUTE 的證實原語 APSME-GET.confirm。如果在資料庫中檢索到了請求的 AIB 屬性，APSME 就向其上層發出狀態爲 SUCCESS 的 APSME-GET.confirm 原語，並攜帶 AIB 屬性標識和屬性值。

APSME-GET.confirm 原語用來向 APS 上層報告請求讀取 AIB 屬性值的結果。該原語的語法如下：

APSME-GET.confirm （Status，AIBAttribute，AIBAttributeValue）

其中：參數 Status 是枚舉量，指示請求讀 AIB 屬性值的結果，其取值爲 SUCCESS 或 UNSUPPORTED_ATTRIBUTE；參數 AIBAttribute 和 AIBAttributeValue 是請求讀取的屬性標識和屬性值。

APSME-GET.confirm 原語由 APSME 發給其上層，作爲對 APSME-GET.request 原語的回應。該原語返回狀態爲 SUCCESS 時表示成功讀取到了請求的屬性值，否則返回狀態爲錯誤程式 UNSUPPORTED_ATTRIBUTE。上層接收到 APSME-GET.confirm 原語就獲知了其請求讀取 AIB 屬性值的結果。

APSME-SET.request 原語與許上層向 AIB 中寫入屬性值，該請求原語的語法如下：

APSME-SET.request （AIBAttribute，AIBAttributeValue）

其中兩個參數分別表示要寫的 AIB 屬性標識和屬性值。

APSME-SET.request 原語由上層產生並發給 APSME，請求寫入一個 AIB 屬性值。APSME 收到該請求原語就嘗試把給定的值寫入到 AIB 屬性中。如果資料庫中找不到 AIBAttribute 參數指定的屬性，APSME 就向其上層發出狀態爲 UNSUPPORTED_ATTRIBUTE 的證實原語 APSME-SET.confirm；如果 AIBAttributeValue 參數指定的值超出了指定屬性的有效取值範圍，APSME 就向其上層發出狀態爲 INVALID_PARAMETER 的證實原語 APSME-SET.confirm；如果把指定的值成功寫入到請求的 AIB 屬性，APSME 就向其上層發出狀態爲 SUCCESS 的 APSME-SET.confirm 原語。

APSME-SET.confirm 原語用來向 APS 上層報告其請求寫入 AIB 屬性值的結果。該原語的語法如下：

APSME-SET.confirm （Status，AIBAttribute ）

其中：Status 參數是枚舉量，指示請求寫 AIB 屬性的結果，其取值爲 SUCCESS、INVALID_PARAMETER 或 UNSUPPORTED_ATTRIBUTE；AIBAttribute 參數表示被寫的 AIB 屬性標識。

APSME-SET.confirm 原語由 APSME 產生並發給其上層，作爲對 APSME-SET.request 原語的回應。該原語返回狀態爲 SUCCESS 時表示成功寫入了請求的屬性值，否則返回狀態爲錯誤程式 UNSUPPORTED_ATTRIBUTE 或 INVALID_PARAMETER。上層接收到 APSME-SET.confirm 原語就獲知了其請求寫入 AIB 屬性值的結果。

1.2.3 訊框(Frame)格式

每個 APS 訊框(Frame)（APDU）包括兩個基本部分：APS 訊框(Frame)頭和 APS 有效載荷。訊框(Frame)頭由訊框(Frame)控制資訊和位址資訊組成；有效載荷則是可變長度的，與訊框(Frame)類型相關的有效資訊。APS 訊框(Frame)頭中各欄位是以固定順序排列的，但不是所有訊框(Frame)都包含位址資訊欄位。APS 訊框(Frame)的一般格式如下：

<table>
<tr><td>位元組數：1</td><td>0/1</td><td>0/1</td><td>0/2</td><td>0/1</td><td>可變長度</td></tr>
<tr><td rowspan="2">訊框(Frame)控制</td><td>目的端點</td><td>簇標識</td><td>配置檔標識</td><td>源端點</td><td rowspan="2">訊框(Frame)有效載荷</td></tr>
<tr><td colspan="4">位址欄位</td></tr>
<tr><td colspan="5">APS 訊框(Frame)頭</td><td>APS 有效載荷</td></tr>
</table>

訊框(Frame)控制欄位長度爲 8 位，定義了訊框(Frame)類型、定址方式和其他控制標記。訊框(Frame)控制欄位各位的定義如下：

比特位：0～1	2～3	4	5	6	7
訊框(Frame)類型	傳遞模式	間接定址模式	安全	確認請求	預留

其中**訊框(Frame)類型**子域長度爲 2 位元，00 表示資料訊框(Frame)，01 表示命令訊框(Frame)，10 表示確認訊框(Frame)，11 暫時預留。**傳遞模式**子域長度爲 2 位，00 表示正常單播傳遞，01 表示間接定址，10 表示廣播，11 暫時預留。如果傳遞模式子域的值爲 01，傳

遞過程中使用間接定址方式，訊框(Frame)格式中將根據間接定址模式子域的值省略目的端點或源端點；如果傳遞模式子域的值爲 10，該訊框(Frame)爲廣播訊息，廣播訊息將到達所有設備和所有端點。**間接定址模式**子域長度爲 1 位元，它在傳遞模式子域置爲間接定址時用來指定訊框(Frame)格式中是否存在源端點或目的端點欄位。如果該子域設爲 1，訊框(Frame)格式中省略目的端點欄位，表示到 ZigBee 協調器的間接傳輸；如果該子域設爲 0，訊框(Frame)格式中省略源端點欄位，表示來自 ZigBee 協調器的間接傳輸。如果訊框(Frame)控制欄位中傳遞模式子域不是間接定址，則忽略間接定址模式子域。**安全**子域由後述的安全服務提供模組來管理。**確認請求**子域長度 1 位元，用來指定當前發送是否要求接收方回送確認訊框(Frame)。如果該子域設爲 1，接收方收到有效訊框(Frame)後需要構造並向發送方回送一個確認訊框(Frame)；如果該子域設爲 0，則接收方在收到有效訊框(Frame)後並不向發送方回送確認訊框(Frame)。

目的端點欄位長度爲 8 位元，用來指定最終接收訊框(Frame)的端點。目的端點值爲 0x00，表示訊框(Frame)傳遞給 ZigBee 設備物件（ZDO）；目的端點值爲 0x01～0xf0，表示訊框(Frame)傳送給運行在該端點上的應用；目的端點值爲 0xff，表示訊框(Frame)傳送給所有活動的端點。其他端點值暫時預留。

簇標識欄位長度爲 8 位元，它指定了綁定操作中將使用的簇標識。訊框(Frame)控制欄位中的訊框(Frame)類型子域決定了訊框(Frame)格式中是否存在簇標識欄位。只有資料訊框(Frame)中使用簇標識，命令訊框(Frame)不用簇標識。

配置檔標識欄位長度爲 2 位元組，用來指定該訊框(Frame)應用的 ZigBee 配置檔標識。每個傳遞訊框(Frame)的設備使用配置檔標識對訊息進行過濾。該欄位只存在於資料訊框(Frame)或確認訊框(Frame)中。

源端點欄位長度爲 8 位元，用來指示該訊框(Frame)的初始發起端點。源端點值 0x00 表示訊框(Frame)由設備的 ZDO 發出；源端點值 0x01～0xf0 表示訊框(Frame)由運行在該端點上的應用發出；其他端點值暫時預留。如果訊框(Frame)控制欄位的傳遞模式子域指示爲間接定址傳遞模式並且間接位址模式子域爲 0，則訊框(Frame)格式中部含有源端點欄位。

訊框(Frame)有效載荷欄位長度可變，包含的是與訊框(Frame)類型相關的有效資訊。

ZigBee 定義了 3 種 APS 訊框(Frame)類型：資料、APS 命令和確認。下面分別詳細介紹 3 種類型的訊框(Frame)格式。

資料訊框(Frame)中各欄位的順序應與一般 APS 訊框(Frame)格式中的順序一致。資料訊框(Frame)的格式如下：

位元組數：1	0/1	1	2	0/1	可變長度
訊框(Frame)控制	目的端點	簇標識	配置檔標識	源端點	資料有效載荷
APS 訊框(Frame)頭					APS 有效載荷

APS 資料訊框(Frame)訊框(Frame)頭部分包含訊框(Frame)控制、簇標識、配置檔標識和源端點欄位。目的端點欄位的存在與否有賴於訊框(Frame)控制欄位傳遞模式子域的值。資料訊框(Frame)的訊框(Frame)控制欄位中訊框(Frame)類型子域應置爲 00，源端點存在子域（即間接定址模式子域）應置爲 1，其他子域則根據資料訊框(Frame)的應用意圖作適當的設置。

發送的資料訊框(Frame)，其資料有效載荷欄位包含的是上層請求 APS 資料服務發送的

一串位元組；接收的資料訊框(Frame)，其資料有效載荷欄位包含的是 APS 資料服務接收到的一串位元組，如果協調器本身也是目的設備，則 APS 吧接收到的資料訊框(Frame)有效載荷遞交給上一層，否則 APS 把資料訊框(Frame)轉發給目的設備。

APS 命令訊框(Frame)中各欄位的順序也應該與 APS 訊框(Frame)的一般格式相一致。APS 命令訊框(Frame)的訊框(Frame)頭僅含訊框(Frame)控制欄位，APS 有效載荷部分則含 APS 命令標識欄位和 APS 命令有效載荷欄位。APS 命令訊框(Frame)的格式如下：

位元組數：1	1	可變長度
訊框(Frame)控制	APS 命令標識	APS 命令有效載荷
APS 訊框(Frame)頭	APS 有效載荷	

APS 命令訊框(Frame)的訊框(Frame)控制欄位中，訊框(Frame)類型子域的值應置爲 01。APS 命令標識欄位指明了所用的 APS 命令。APS 命令有效載荷欄位則根據具體使用的 APS 命令作適當的設置。

APS 確認訊框(Frame)中各欄位的順序與 APS 訊框(Frame)的一般格式相一致。APS 確認訊框(Frame)的格式如下：

位元組數：1	0/1	1	2	0/1
訊框(Frame)控制	目的端點	簇標識	配置檔標識	源端點
APS 訊框(Frame)頭				

APS 確認訊框(Frame)只有訊框(Frame)頭部分，它包含訊框(Frame)控制、簇標識和配置檔標識欄位。如果訊框(Frame)控制欄位中傳遞模式子域指示爲直接定址，則確認訊框(Frame)訊框(Frame)頭還應包含源端點和目的端點欄位；如果傳遞模式子域指示爲間接定址，則根據訊框(Frame)控制欄位中間接定址模式子域的值決定確認訊框(Frame)中還應包含源端點或目的端點欄位。

APS 確認訊框(Frame)的訊框(Frame)控制欄位中訊框(Frame)類型子域應置爲 10，其他子域則根據確認訊框(Frame)的應用情況作適當的設置。當確認訊框(Frame)中存在源端點欄位時，它反映的是被確認訊框(Frame)中目的端點欄位的值；同樣，當確認訊框(Frame)中存在目的端點欄位時，它反映的是被確認訊框(Frame)中源端點欄位的值。

1.2.4 常量和 PIB 屬性

描述 APS 子層特徵的常量有：

1. apscMaxAddrMapEntries，位址映射入口數量的最大值。
2. apscMaxDescriptorSize，非複雜描述符所含位元組數的最大值。該常量爲 64。

3. apscMaxDiscoverySize，發現過程能返回位元組數的最大值。該常量爲 64。

4. apscMaxFrameOverhead，APS 子層在有效載荷上添加開銷的最大位元組數。沒有安全處理時該常量爲 6，採取安全處理時該常量爲 20。

5. apscMaxFrameRetries，發送失敗後允許重發的最大次數。該常量爲 3。

6. apscAckWaitDuration，等待確認訊框(Frame)的最大時間（單位爲 s）。

APS 資訊庫由管理設備的 APS 層所需的屬性組成，另外還包括管理安全服務模組所需的一些屬性。這些屬性將在安全服務規範部分介紹，這裡只介紹下面兩個屬性；

1. apsAddressMap，這是一個集合類型的屬性，屬性標識爲 0xc0。它表示當前 64 位 IEEE 位址與 16 位元 NWK 位址映射的集合。位址映射如下：

入口號　0x00～apscMaxAddrMapEntries

64 位 IEEE 位址　0x00000000～0xffffffff

16 位 NWK 位址　0x0000～0xffff

2. apsBindingTable，這是一個集合類型的屬性，屬性標識爲 0xc1。它表示設備中當前綁定表記錄的集合。

1.2.5 功能描述

1.2.5.1 綁定

APS 維護一個綁定表，允許 ZigBee 設備爲來自特定源端點特定簇標識的訊框(Frame)建立一個指定的目的地。綁定表用在間接定址機制中。ZigBee 協調器或源位址指定的設備應能支援實現特定長度的綁定表。綁定表應事先下面的映射關係：

$$(a_s,e_s,c_s)=\{(a_{d1},e_{d1}),(a_{d2},e_{d2}),\cdots,(a_{dn},e_{dn})\}$$

其中：a_s 是綁定鏈路源設備的位址；e_s 是綁定鏈路源設備的端點標識；c_s 是綁定鏈路使用的簇標識；a_{di} 是綁定鏈路第 i 個目的設備位址；e_{di} 是綁定鏈路第 i 個目的設備的端點標識。

ZigBee 協調器或 SrcAddr 指示的設備上執行的 APSME-BIND.request 或 APSME-UNBIND.request 原語分別啓動建立綁定鏈路或解除綁定鏈路過程。只有 ZigBee 協調器或請求原語中 SrcAddr 指示的設備可以啓動該過程，如果任何其他設備試圖啓動綁定或解除綁定過程，APSME 將中斷該過程並向上層發出狀態爲 ILLEGAL_REQUEST 的 APSME-BIND.confirm 或 APSME-UNBIND.confirm 原語，把非法請求通知給 NHLE。

綁定或解除綁定過程啓動後，ZigBee 協調器或 SrcAddr 指示設備的 APSME 將首先提取出綁定鏈路起點和終點的位址和端點。如果啓動了綁定過程，APSME 將根據這些位址和端點資訊在綁定表中添加一個新記錄；如果啓動的是解除綁定過程，APSME 將根據這些位址和端點資訊從綁定表中刪除一個記錄。請求綁定操作時，如果 ZigBee 協調器或 SrcAddr 指示設備沒有足夠資源用來增加新的綁定記錄，APSME 將中斷綁定過程並向 NHLE 發出狀態爲 TABLE_FULL 的 APSME-BIND.confirm 原語。請求解除綁定操作時，如果 APSME 在綁定表中檢索不到請求的綁定記錄就中斷解除綁定過程，並通知 NHLE 其請求解除的是無效綁定。該通知以狀態爲 INVALID_BINDING 的 APSME-UNBIND.confirm 原語發送給上層。如果在綁定表中找到了匹配的記錄，APSME 將把該記錄從綁定表中刪除。如果成功建立或解除了綁定鏈路，APSME 就向其上層發出狀態爲 SUCCESS 的相應證實原語。成功實現直接綁定（解綁定）的資訊流程如圖 3。

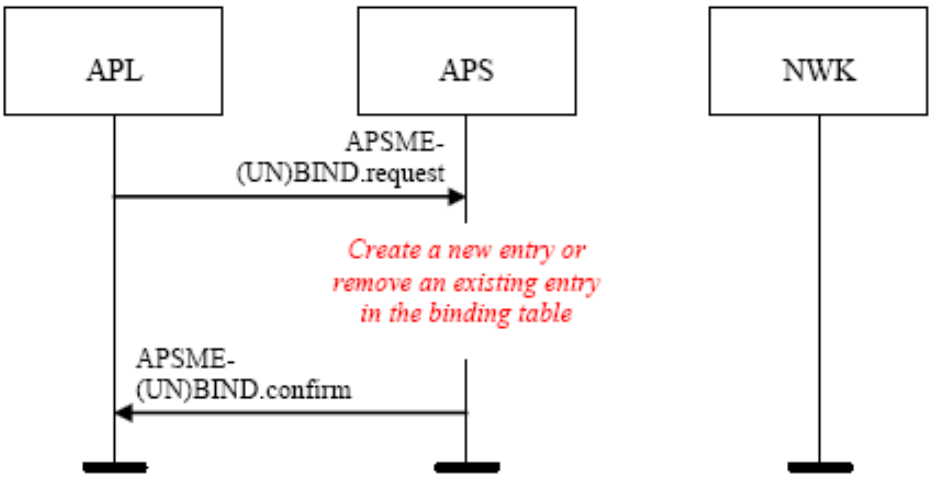


圖 3 綁定（解綁定）的資訊流程

1.2.5.2 發送、接收和確認

只有當前處於網路中的設備才能從 APS 子層發送訊框(Frame)。任何其他設備收到發送訊框(Frame)的請求時都將丟棄訊框(Frame)並把錯誤通知給請求發送的上層。狀態爲 CHANNEL_ACCESS_FAILURE 的 APSME-DATA.confirm 原語表示由於通道忙而導致發送失敗。APS 子層處理或產生的所有訊框(Frame)都應遵循 APS 一般訊框(Frame)格式進行構造，再調用 NWK 層資料服務來發送。發送可以是直接或間接的。直接發送應同時包括目的端點和源端點欄位，這種情況下訊框(Frame)控制欄位中傳遞模式子域應設爲 0x00（正常單播）或 0x02（廣播）。設備 APS 層發起間接傳輸時，如果綁定表儲存在 ZigBee 協調器中，則它將把訊框(Frame)發送給 ZigBee 協調器，再由協調器根據綁定表對訊息進行轉發。間接傳輸，即訊框(Frame)結構中傳遞模式子域爲 01 時，根據傳輸相對 ZigBee 協調器的方向，訊框(Frame)結構中應只包含源端點欄位或目的端點欄位。如果間接傳輸指向 ZigBee 協調器，則訊框(Frame)結構的間接定址模式子域爲 1 並省略目的端點欄位；相反，如果間接傳輸是 ZigBee 協調器轉發的訊息，則訊框(Frame)結構的間接位址模式子域置爲 0 並省略源端點欄位。

如果源設備本身儲存了綁定表，則源設備發起的傳輸應採用直接方式，從綁定表相應的綁定記錄中提取目的位址。採用直接傳輸時，訊框(Frame)控制欄位中傳遞模式子域位置爲 0x00.

如果存在目的端點欄位，則它包含的是接收 APDU 的端點；如果存在源端點欄位，則它包含的是發送 APDU 的端點。如果要求訊框(Frame)安全保護，則要根據後續關於安全服務的機制進行處理。當構造好 APS 訊框(Frame)並準備發送時，APS 把攜帶適當目的位址和源位址的訊框(Frame)遞交給 NWK 資料服務。APS 層透過向 NWK 層發送 NLDE-DATA.request 原語來發起 APDU 發送，NWK 層透過 NLDE-DATA.confirmed 原語來返回 APS 訊框(Frame)的傳輸結果。

APS 子層應能夠對來自 NWK 層資料服務的訊框(Frame)進行過濾，只把 NHLE 感興趣的訊框(Frame)提交給上層。如果 APSDE 接收到經過安全保護的訊框(Frame)，則需要對症

作相應的解密處理來去除安全保護引入的開銷。如果 APSDE 接收到的訊框(Frame)同時包含目的端點和源端點，則它被當作直接傳輸的訊框(Frame)。此時，APSDE 把它直接提交給 NHLE。如果 ZigBee 協調器的 APSDE 接收到的訊框(Frame)值包含源位址，訊框(Frame)控制欄位中傳遞模式子域爲間接定址值 0x01，該訊框(Frame)被當作間接傳輸的訊框(Frame)。如果設備不是 ZigBee 協調器，當接收到的訊框(Frame)中不含目的端點且訊框(Frame)控制欄位中傳遞模式子域爲間接定址值 0x01 時，設備 APS 層將丟棄該訊框(Frame)。

如果 ZigBee 協調器的 APSDE 接收到間接傳輸訊框(Frame)，它將檢索綁定表，搜索與 NWK 層通訊源位址以及接收訊框(Frame)中包含的簇標識和源端點相匹配的綁定記錄。如果在綁定表中沒有找到匹配的記錄，則接收訊框(Frame)將被丟棄；如果找到了匹配的綁定記錄，APSDU 將爲綁定記錄中每個目的端點構造一個 APDU，並調用 NWK 資料服務吧各訊框(Frame)轉發出去。

在發送 APS 資料訊框(Frame)或命令訊框(Frame)時，可以對確認請求子域作適當的設置。確認訊框(Frame)發送時，其確認請求子域總是設爲 0（無須確認）。另外，各種廣播訊框(Frame)的確認請求子域也設爲 0。

如果最終接收方收到的訊框(Frame)確認請求（AR）子域爲 0，則表示該訊框(Frame)不需要回饋確認，發送方發出該訊框(Frame)就認爲發送成功。圖 4 表示了一個無須確認 APS 資料訊框(Frame)傳輸的資訊流程。

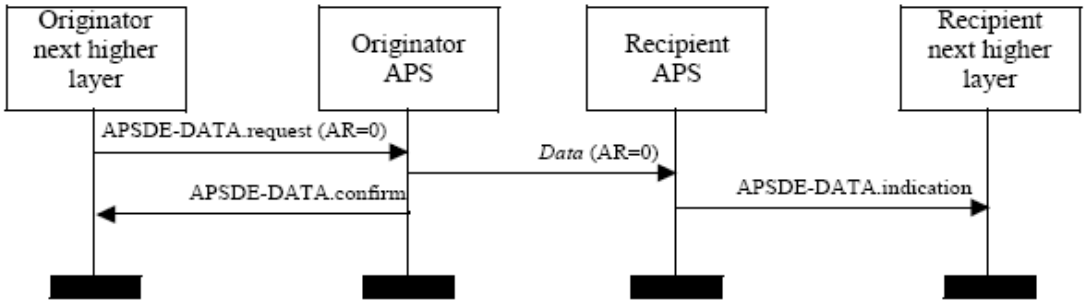


圖 4 傳輸 APS 資料訊框(Frame)的資訊流程（不確認）

如果最終接收方收到訊框(Frame)的確認請求（AR）子域爲 1，則它需要對接收訊框(Frame)進行確認。如果接收方正確接收到要求確認的訊框(Frame)，它將產生並向發送方發送一個確認訊框(Frame)。如果採用間接傳輸模式，則 ZigBee 協調器要向該發送的發起方發送一個確認，然後在每一次資訊轉發時都把資料訊框(Frame)訊框(Frame)控制欄位的確認請求子域置爲 1，要求接收者對轉發的訊框(Frame)進行確認。APS 只有在判定接收訊框(Frame)有效後才著手發送確認訊框(Frame)。圖 5 是發送一個需要確認的資料訊框(Frame)的資訊流程。

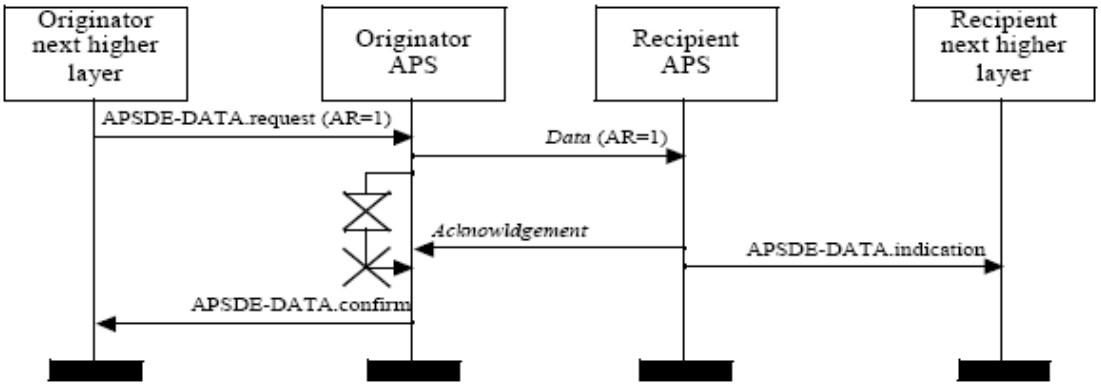


圖 5 傳輸 APS 資料訊框(Frame)的資訊流程（確認）

當設備發送訊框(Frame)的確認請求子域置爲 0 時，它就認爲該訊框(Frame)能被目的端點成功接收，因此不執行重發程式；當設備發送訊框(Frame)的確認請求子域置爲 1 時，它最多等待 apscAckWaitDuration 秒以接收相應的確認訊框(Frame)。

如果設備在 apscAckWaitDuration 秒時間內收到一個確認訊框(Frame)的簇標識與原始發送訊框(Frame)的簇標識相同，確認訊框(Frame)的源端點等於原始發送訊框(Frame)的目的端點，則認爲發送成功，設備無須再作進一步動作。如果設備在 apscAckWaitDuration 秒時間內沒有收到確認訊框(Frame)，或者收到的確認訊框(Frame)簇標識與原始發送訊框(Frame)簇標識不同，或確認訊框(Frame)的源端點不等於待確認訊框(Frame)的目的端點，則認爲發送嘗試失敗。如果一次發送嘗試失敗，設備將重發該訊框(Frame)並等待確認，最多可以重發 apscMaxFrameRetries 次。如果重發 apscMaxFrameRetries 次後仍未收到確認，則 APS 子層就認爲發送失敗，並且把發送失敗的事實通知給上一層。

1.3 ZigBee 應用框架

1.3.1 建立 ZigBee 配置檔

ZigBee 網路中設備間通訊的關鍵是配置檔協定。家庭照明控制配置檔是最早的配置檔，該配置檔允許 6 個設備類型相互交換控制資訊構成一個家庭無線自動化應用。這些設備結合在一起交換約定訊息（採用 KVP 服務類型）來實現控制，如開燈、關燈、發送光感應器的測量結果到照明控制或感應器檢測到移動時發出報警資訊。

配置檔的另一個例子是設備配置檔，它定義了 ZigBee 設備間的公共動作。例如，無線網路依賴這種能力來實現自治設備加入網路，發現其他設備和發現網路設備上的服務。設備和服務發現是設備配置檔使用 MSG 服務類型所支援的特性。

ZigBee 定義的配置檔一般分爲 3 類：專用的、有版權的和公共的。這些類型的具體定義和原則是 ZigBee 聯盟內部的行政問題，不屬於 ZigBee 規範涉及的內容。在技術規範上需要清楚的唯一原則就是：配置檔標識是唯一的。一旦得到配置檔標識，就允許配置檔設計者定義一下內容：設備描述、簇標識、服務類型（KVP 或 MSG）。

ZigBee 聯盟發佈配置檔標識的關鍵原則是配置檔標識要能應用於市場。配置檔應覆蓋足夠廣範圍的設備以允許可能出現的不同設備間互操作，但覆蓋範圍過大又會導致描述設備

介面的簇標識短缺。反過來，配置檔覆蓋的設備範圍又不能太窄，否則會導致許多設備需要各自的配置檔標識來描述，從而浪費配置檔標識編址空間，影響描述設備介面的互操作性。ZigBee 聯盟的政策小組負責建立配置檔定義準則，並指導配置檔申請者修剪其配置檔標識請求。

配置檔標識是 ZigBee 協定中的主要枚舉特性。每個配置檔標識分別定義了設備描述和簇標識的一個關聯枚舉。例如，對配置檔標識“1”，存在一組用 16 位元值描述的設備描述和一組用 8 位元值描述的簇標識，也就是說一個配置檔中可以有 65536 個設備描述和 256 個簇標識。對於 KVP 服務類型，每個簇標識還支援一組用 16 位元值描述的屬性，也就是說，每個配置檔標識有 256 個簇標識，每個簇標識包含 65536 個屬性。配置檔開發者的任務就是定義並分配設備描述、簇標識和該配置檔標識裡的屬性。在定義設備描述、簇標識和屬性標識時必須仔細斟酌，以確保能有效產生簡單的描述符並簡化資訊交換時的處理過程。使用設備描述和簇標識的前提是知道要處理的配置檔標識。在向設備發送任何資訊之前，ZigBee 協定認爲透過服務發現已經判定了設備和端點所支援的配置檔。同樣的，綁定過程也在類似的服務發現和配置檔匹配的前提下執行，因爲綁定的匹配結果是由源位址、源端點、簇標識、目的位址和目的端點表示的。

一個 ZigBee 設備可以支援多個配置檔，提供這些配置檔中各種簇標識的子集，支援多個設備描述。這種支持能力是採用下面分層編址方案來定義的：

（1）設備。整個設備只有一個無線射頻端，具有唯一的 IEEE 位址和 NWK 位址。

（2）端點。它是一個 8 位的欄位，描述一個射頻端所支持的不同應用。端點 0x00 用於定址設備配置檔，這是每個 ZigBee 都必須使用的端點。端點 0xff 用來定址所有活動端點，而端點 0xf1～0xfe 暫時預留。因此，一個物理 ZigBee 射頻端在端點 0x01~0xf0 上共支援 240 個應用。

把設備端點分配給各種應用的唯一要求是，爲每個端點產生簡單的描述符並能被服務發現過程得到。

一旦設備支援明確的配置檔並且這些檔中的簇標識和設備描述一致，就可以在設備上佈置應用。每個應用分配一個端點，用一個簡單描述符來描述。透過簡單描述符和 ZigBee 設備配置檔中的其他服務發現機制，就可以實現服務發現，支援設備綁定，便於互補設備間的應用資訊交互 。需要強調的是，服務發現是基於配置檔標識、輸入簇標識列表和輸出簇標識列表，而設備描述值是詳細列出設備強制支援和可選支援的簇標識。另外，設備描述枚舉通常用在 PDA 或其他輔助綁定設備來提供對設備能力的外部描述。

如果廠商希望開發的 ZigBee 設備既要支援標準配置檔“XX”，又要提供自有的專用擴充，那麼這些擴充將發佈在其他端點上。僅支援標準配置檔標識“XX”而不支援廠商擴充的設備也只會發佈其對配置檔標識“XX”的支援，不會回應廠商專用擴充，也不會用廠商專用擴充來產生訊息。

在前面的例子中，假設設備支援的標準 ZigBee 配置檔標識“XX”包含的是該標準配置檔的初始版本。如果 ZigBee 聯盟對該標準配置檔進行升級，增加新的特性，那麼升級後的版本將用一個新的配置檔標識“XY”來描述。僅支援配置檔標識“XX”的設備應後向相容支援配置檔標識“XY”新設備，這種相容性透過新設備發佈同時支援配置檔標識“XX”和“XY”來實現。在這種方式中，新設備在同一個應用中既可以使用配置檔標識“XX”與舊設備通訊，又可以使用配置檔標識“XY”與新設備通訊。ZigBee 中的服務發現特徵使得網路中的設備能夠判定支援等級。

1.3.2 標準資料類型

ZigBee 設備是用它的一系列屬性來定義的，這種屬性能夠採用 KVP 服務類型或用 MSG 服務類型把屬性組合進特定應用資訊中，用設置、獲取和事件命令進行寫、讀和報告。這就需要定義這些屬性的資料類型和格式。設備描述展示了設備屬性的有效值、範圍和單位。ZigBee 定義的資料類型如表 1 所列。在 KVP 命令訊框(Frame)中，屬性資料類型欄位包含的就是用表中適當的資料類型標識來表示屬性的資料類型。

表 1 ZigBee 標準資料類型

資料類型標識 $b_3b_2b_1b_0$	資料類型	資料長度/位元組
0000	無資料	0
0001	無符號 8 位元整數	1
0010	有符號 8 位元整數	1
0011	無符號 16 位元整數	2
0100	有符號 16 位元整數	2
0101～1010	預留	—
1011	半精度	2
1100	絕對時間	4
1101	相對時間	4
1110	字串	由第一個位元組定義
1111	位元組串	由第一個位元組定義

無資料類型（0000）是一種特殊的資料類型，表示屬性沒有關聯資料。無符號 8 位元整數範圍是 0～255，有符號 8 位元整數的範圍是-128～+127。無符號 16 位元整數的範圍是 0～65535，最小解析度是 1 位元；有符號 16 位元整數的範圍是-32768～+32767，最小解析度是 1 位元。

有些數值（如光強度）的範圍很寬。當周圍光強度是 1 lx 時，眼睛對光強度增加 1 lx 非常敏感；然而，如果周圍光強度爲 100 lx，則再增加 1 lx 就不易察覺。這種數值最好用 ZigBee 半精度數來表示，它允許解析度隨數值範圍的不同而變化。ZigBee 半精度數的格式是基於二進位浮點數標準 IEEE 754 的。必須記住，只有在絕對必要並且程式和處理能力支援的情況下使用半精度資料類型。ZigBee 半精度資料格式如圖 6 所示。

	符號	指數					隱藏	尾數									
	S	E_4	E_3	E_2	E_2	E	H	M_9	M_8	M_7	M_6	M_5	M_4	M_3	M_2	M_1	M_0
bit	15	14	13	12	11	10		9	8	7	6	5	4	3	2	1	0

圖 6 ZigBee 半精度數的格式

它表示的值透過下面的公式來計算：

$$value = (-1)^{Sign} \times (Hidden + Mantissa / 1024) \times 2^{(Exponent - 15)}$$

對歸一化數（$> 2^{-14}$），Hidden 位等於 1，解析度恒爲 11 位；對非歸一化數，Hidden 位等於 0，解析度不再是 11 位，並且數越小解析度越低。Hidden 位不在鏈路中傳送，爲了表示 ZigBee 半精度數，Hidden 位爲 1。正數的符號位元爲 0，負數的符號位元爲 1。指數部分是 5 位元，2 的實際指數是（exponent — 15）。另外，還保留了一些特殊值：

不是數 它表示未定義的數，它用指數 31、尾數非零的半精度資料格式表示。

無窮大 指數爲 31，尾數爲 0 時表示無窮大。符號位元用來區分正無窮大和負無窮大。0x7c00 表示+∞，0xfc00 表示—∞。

零 指數和尾數都爲 0 時表示零。符號位元用來區分正零和負零，即 0x0000 表示+0，0x8000 表示—0。

非歸一化數 $<2^{-14}$ 的數是非歸一化數，非歸一化數的指數部分爲 0，Hidden 位元設爲 0.。

尾數表示的最大值是 0x3ff / 1024，所以半精度格式能表示的最大數是：

$$(-1)^{Sign} \times (1 + 1023 / 1024) \times 2^{(30 - 15)} = \pm 1.9990234 \times 32768 = \pm 65504$$

例如：+2 的半精度格式爲$+2^{(16 - 15)} \times 1.0 = 0x4000$，而—2 表示爲 0xc000。類似的，0.625 表示爲$+2^{(17 - 15)} \times 1.625 = 0x4680$，而—0.625 表示爲 0xc680。

ZigBee 中絕對時間用一個無符號的 32 位元整數來表示。絕對時間是從 2000 年 1 月 1 日零點開始到當前時刻的秒數。相對時間也是用一個無符號 32 位元整數表示，它用 ms 來度量。

字串資料包含的是根據語言和複雜描述符字元集編碼成的資料位元組。字串資料由兩部分組成：第 1 個位元組存放字串的長度；從第 2 個位元組開始就是實際的字元資料，它的長度是 e × n 位元組。這裡 e 是單個字元編碼的長度，n 是字串的長度。

1.3.3 ZigBee 描述符

ZigBee 設備用描述符資料結構對自身進行描述。描述符中的實際資料分別在各自的設備描述中定義。ZigBee 描述符分爲 5 種：節點、節點電源、簡單的、複雜的、使用者。其中前三種描述符是各種 ZigBee 設備必須支援的，而後兩種描述符則是可選支持的。節點描述符描述了節點的類型和能力；節點電源描述符描述了節點電源特性；簡單描述符包含了節點中的設備描述；複雜描述符則包含了有關設備描述的進一步資訊；使用者描述符是使用者可定義的描述符。

節點描述符、節點電源描述符、簡單描述符和使用者描述符的發送按照它們各自表中的順序進行，最新發送表中最上層的欄位，最後發送表中最低層的欄位。複雜描述符的格式如下：

位元組數：1	可變長度	…	可變長度
欄位計數	欄位 1	…	欄位 n

欄位計數欄位長度爲 1 位元組，它指定了複雜描述符包含的欄位數。這些欄位的格式如下：

位元組數：1	可變長度
壓縮 XML 標記	欄位資料

壓縮 XML 標記子域長度是 1 位元組，它指定了當前欄位的 XML 標記。欄位資料子域長度可變，它包含的是當前欄位的資料。

服務發現程式用 ZigBee 設備配置檔請求原語定址端點 0（即 ZDO）來查詢描述符資訊。查詢結果透過 ZigBee 設備配置檔指示原語返回。節點和節點電源描述符應用於整個節點，其他描述符則要制定到節點中的每個端點。如果一個節點中包含多個子單元，則每個子單元

對應一個端點，讀取特定端點的描述符時需要在 ZigBee 設備配置檔原語中指定端點號。

1.3.3.1 節點描述符

節點描述符包含的是有關 ZigBee 節點能力的資訊，該描述符對各個節點都是強制支援的。在一個節點中只有一個節點描述符。節點描述符包含的欄位和它們的傳輸順序如表 2 所列。

表 2 節點描述符的欄位

欄位名	長度/位	欄位名	長度/位
邏輯類型	3	MAC 能力標誌	8
預留	5	廠商程式	16
APS 標誌	3	最大緩存空間	8
頻帶	5	最大發送長度	16

1. 節點描述符的**邏輯類型**欄位長度是 3 位，它指定了 ZigBee 節點的設備類型：000 表示 ZigBee 協調器，001 表示 ZigBee 路由器，010 表示 ZigBee 終端設備。

2. **APS 標誌**欄位長度爲 3 位元，它指示該節點應用支援子層的能力；該欄位暫不支援，應設爲 0。

3. 節點描述符的**頻帶**欄位長度是 5 位，它指示該節點 IEEE 802.15.4 射頻端所支持的頻帶。支持 868～868.6MHz 頻段時，該欄位的 0 比特位設爲 1，其他 4 位設爲 0；支持 902～928MHz 時，該欄位的 2 比特位設爲 1，其他 4 位設爲 0；支持 2400～2483.5MHz 時，該欄位的 3 比特位設爲 1，其他 4 位設爲 0.

4. **MAC 能力標誌欄位**長度是 8 位元，它指示了該節點設備 IEEE 802.15.4 MAC 層的能力。MAC 能力標記欄位的格式如下：

比特位：0	1	2	3	4～5	6	7
備用 PAN 協調器	設備類型	電源	空閒時接收機致能	預留	安全能力	預留

備用 PAN 協調器子域長度爲 1 位元，如果該節點能夠充當 PAN 協調器則該位元設爲 1，否則設爲 0。**設備類型**子域長度爲 1 位元，如果該節點是全功能設備（FFD），則該位元設爲 1；如果節點是精簡精簡功能設備，則該位元設爲 0。**電源**子域長度是 1 位元，如果節點是幹線供電，則該位元設爲 1，否則該位設爲 0。該位元的資訊從節點電源描述符的當前電源欄位獲得。**空閒時接收機致能**子域長度爲 1 位元，如果設備在空閒時並不關閉接收機來節省功率則該位設爲 1，否則該位設爲 0。**安全能力**子域長度爲 1 位元，如果設備能夠用 IEEE 802.15.4 安全套件來發送和接收安全訊框(Frame)則該位設爲 1，否則該位設爲 0。

5. **廠商程式**欄位長度 16 位元，它指示的是 ZigBee 聯盟分配給設備製造商的程式。

6. **最大緩存空間**子域長度是 8 位元，它的有效取值範圍是 0x00～0x7f，它表示該節點應用支援子層資料單元（ASDU）長度的最大位元組數。

7. **最大發送長度**欄位爲 16 位元，它的有效取值範圍是 0x0000～0x7fff，它表示該節點發送或接收訊框(Frame)的長度最大位元組數。ZigBee 規範目前還不支援該欄位，應設爲 0。

1.3.3.2 節點電源描述符

節點電源描述符動態指示節點電源的狀態，它是每個節點必須支持的描述符。每個節點只能有一個節點電源描述符。節點電源描述符的各欄位及傳輸順序如表 3 所列。

表 3 節點電源描述符的格式

欄位名	長度/位
當前電源模式	4
可用電源	4
當前電源	4
當前電量	4

1. 節點電源描述符中**當前電源模式**欄位長度是 4 位元，它表示節點當前的休眠/節能模式。該欄位爲 0000 表示接收機模式與節點描述符中空閒時致能接收子域同步；0001 表示接收機根據節點電源描述符的定義週期性地喚醒；0010 表示接收機在使用者干預（如按鈕）下才喚醒。

2. **可用電源**欄位長度是 4 位元，它表示節點可以得到的供電模式。供電模式分別爲幹線供電，充電電池供電，一次性乾電池供電時，分別設置該欄位的 0、1、2 位元爲 1，其他 3 個位元設爲 0。

3. **當前電源**欄位長度是 4 位元，它表示節點當前使用的供電模式。當前供電模式分別爲幹線供電，充電電池供電，一次性乾電池供電時，分別設置該欄位的 0、1、2 位元爲 1，其他 3 個位元設爲 0。

4. **當前電量**欄位長度是 4 位元，它表示電源的當前電量：0000 表示電量將耗盡；0100 表示 33%電量；1000 表示 66%電量；1100 表示 100%電量。

1.3.3.3 簡單描述符

簡單描述符包含的是節點中各端點的特定資訊。簡單描述符是節點中每個端點必須支持的描述符。簡單描述符包含的欄位及傳輸順序如表 4 所列。

表 4 簡單描述符的欄位

欄位名	長度/位
端點	8
應用配置檔標識	16
應用設備標識	16
應用設備版本	4
應用標誌	4
應用輸入簇計數	8
應用輸入簇列表	8 × i 位，這裡 i 是應用輸入簇計數欄位的值
應用輸出簇計數	8
應用輸出簇列表	8 × j 位，這裡 j 是應用輸出簇計數欄位的值

1. 簡單描述符的**端點**欄位長度是 8 位元，它表示該描述符對應的節點。應用智慧使用

節點 1～240。

2. **應用配置檔標識**欄位長度是 16 位元，它表示該端點支援的配置檔。配置檔標識從 ZigBee 聯盟得到。

3. **應用設備標識**欄位長度是 16 位元，它表示端點支援的設備描述。設備描述標識從 ZigBee 聯盟得到。

4. **應用設備版本**欄位長度 4 位元，它表示端點支援的設備描述的版本。該欄位當前有效值爲 0000，表示 1.0 版本。

5. **應用標誌**欄位長度是 4 位元，它表示特定應用的標誌。節點上的應用支援一種特性就將相應的位設爲 1，其餘 3 位都設爲 0。位 0 設爲 1 表示可得複雜描述符，位 1 設爲 1 表示可得使用者描述符。

6. **應用輸入簇計數**欄位長度是 8 位元，表示端點支持的輸入簇個數，這些輸入簇將列在應用輸入簇列表字段。如果該欄位爲 0，則簡單描述符將不含應用輸入簇列表字段。

7. **應用輸入簇列表**字段長度是 8i 位元。這裡“i”是應用輸入簇計數欄位的值，該欄位是端點支持的輸入簇列表，這些輸入簇將在綁定過程中使用。

8. **應用輸出簇計數**欄位長度是 8 位元，表示端點支持的輸出簇個數，這些輸入簇將列在應用輸出簇列表字段。如果該欄位爲 0，則簡單描述符將不含應用輸處簇列表字段。

9. **應用輸出簇列表**字段長度是 8j 位元。這裡“j”是應用輸出簇計數欄位的值，該欄位是端點支持的輸出簇列表，這些輸出簇將在綁定過程中使用。

1.3.3.4 複雜描述符

複雜描述符包含的是節點中各個設備描述的擴充資訊。負載描述符的使用時可選的。由於該描述符中資料的擴充和複雜性，它用壓縮 XML 標記的 XML 形式來表示。表 5 列出了複雜描述符中的各欄位，這些欄位可以任意順序傳輸。由於該描述符要在空中傳輸，所以複雜描述符的總長度不得超過 maxCommandSize。

表 5 複雜描述的欄位

欄位名	XML 標記	壓縮 XML 標記值 $b_3b_2b_1b_0$	資料類型
預留	—	0000	—
語言和字元集	<語言字元>	0001	—
廠商名稱	<廠商名稱>	0010	字串
模型名稱	<模型名稱>	0011	字串
序列號	<序列號>	0100	字串
設備 URL	<設備 URL>	0101	字串
圖示	<圖示>	0110	未定義
圖示 URL	<圖示 URL>	0111	字串
預留	—	1000～1111	—

1. 複雜描述符的**語言和字元集**欄位長度是 3 位元組，它表示複雜描述符中字串使用的語言和字元集。前兩個位元組表示 ISO639-1 語言程式，後一個位元組是字元集標識，表示字元集中字元的編碼方式。如果沒有指定語言和字元集，則預設語言爲英語（語言程式“EN”），預設字元集爲 ISO646 ASCII 字元集。

2. **廠商名稱**欄位長度可變，它包含的是表示設備生產商名稱的字串。

3. **模型名稱**欄位長度可變，它包含的是表示設備生產商模型名稱的字串。

4. **序列號**欄位長度可變，它包含的是表示設備製造商序列號的字串。

5. **設備 URL** 欄位長度可變，它包含的是表示 URL 的字串，透過這個 URL 可以得到設備的更多資訊。

6. **圖示**欄位長度可變，它包含在電腦、閘道或 PDA 上顯示設備圖示的資料。目前 ZigBee 規範尚未定義該資料格式。

7. **圖示** URL 欄位長度可變，它包含一個表示 UR.L 的字串，透過該字串可以得到該設備的圖示。

1.3.3.5 使用者描述符

使用者描述符包含的資訊允許使用者使用使用者友好的字串來標識設備，如“Bedroom TV”、“Stairs light”等。使用者描述符的使用時可選的。該描述符只有一個 16 位元組的欄位，最多包含 16 個字元。

1.3.4 AF 訊框(Frame)格式

AF 訊框(Frame)的一般格式如下：

比特數：4	4	可變長度	可變長度	可變長度
事務計數	訊框(Frame)類型	事務 1	…	事務 n

其中各事務欄位的格式爲：

比特數：8	可變長度
事務序號	事務資料
事務頭	事務有效載荷

每個事務包含由事務序號構成的事務頭和與訊框(Frame)類型有關資料構成的事務有效載荷。

AF 訊框(Frame)的一般格式中，**事務計數**欄位長度爲 4 位，表示該訊框(Frame)包含的事務數 n。這些事務在訊框(Frame)類型欄位後依次排列。**訊框(Frame)類型**欄位長度是 4 位，它表示其後各事務使用的服務類型。0001 表示 KVP，0010 表示 MSG，其他取值暫時預留。

事務序號欄位長度爲 8 位元，它指定了事務的標識，以便回應命令訊框(Frame)可與可請求訊框(Frame)聯繫起來。應用物件本身有一個 8 位元計數器，把該計數器拷貝到事務序號欄位，並且每發送一個命令就增加 1。如果設備發送一個要求確認的 KVP 命令，目標設備將使用包含原始請求命令事務序號的相關命令作出回應。類似的，該欄位也可以用來實現 MSG 命令的確認。事務資料欄位長度可變，它包含的是一個事務的具體資料。該欄位的內容與訊框(Frame)類型欄位有關，它是一個 KVP 訊框(Frame)或 MSG 訊框(Frame)。

AF 訊框(Frame)分爲兩類：鍵值對（KVP）和訊息（MSG）。KVP 訊框(Frame)類型使得應用能夠操作應用配置檔定義的屬性。屬性有一個指示器（即鍵）和相關聯的值，它們可以

用命令進行設置和請求。這些命令的發送和接收是透過 ASDU 資料欄位，用 APS APSDE-DATA.request 和 APSDE-DATA.indication 原語來實現的。設置或讀取屬性的命令的發送和接收可以採用直接定址方式，也可以透過 ZigBee 協調器的綁定表採用間接定址方式。APS 簇標識應與包含被操作屬性的簇相匹配。APS 安全套件應指示出命令所要求的安全套件。

KVP 命令訊框(Frame)的格式如下：

比特數：4	4	16	0/8	可變長度
命令類型標識	屬性資料類型	屬性標識	錯誤程式	屬性資料

其中：**命令類型標識**欄位長度是 4 位元，該欄位各種取值對應的命令如表 6 所列。需要注意的是，透過 ZigBee 協調器間接發送命令時，值允許設置（set）和事件（event）命令。**屬性資料類型**欄位長度是 4 位，該欄位的取值爲前述資料類型部分中的一種資料類型的標識碼。**屬性標識**欄位長度是 16 位元，它指定了命令操作的目標設備屬性。該欄位的取值在相關設備描述中定義。**錯誤程式**欄位長度是 8 位，該欄位只存在於回應命令中，用來指示事務的狀態。錯誤程式欄位的取值範圍如表 7 所列。**屬性資料**欄位的長度與屬性類型有關，它包含的是屬性標識欄位指定的屬性值。該欄位與特定命令、屬性資料類型和設備描述有關。屬性資料欄位的長度要麼透過屬性資料類型來反映，要麼包含在該欄位的第一個位元組中。如果是後一種情況，除非源和目的實體都支援資料拆分，否則該欄位的長度需滿足整個命令訊框(Frame)的長度不超過 maxCommandSize。

表 6 命令類型標誌欄位值

命令類型標誌值 $b_3b_2b_1b_0$	描　　述
0000	預留
0001	設置
0010	事件
0011	預留
0100	具有確認的獲取
0101	具有確認的設置
0110	具有確認的事件
0111	預留
1000	獲取回應
1001	設置回應
1010	事件回應
1011～1111	預留

表 7 錯誤碼欄位值

錯誤程式	描　　述
0x00	成功
0x01	無效端點
0x02	預留
0x03	不支援屬性
0x04	無效命令類型

0x05	無效屬性資料長度
0x06	無效屬性資料
0x07～0x0f	預留
0x10～0xff	應用定義的錯誤

MSG 訊框(Frame)類型使得應用配置檔能夠以自由的形式定義自己的訊框(Frame)格式。MSG 允許那些難以定義成 KVP 訊框(Frame)結構的應用也能靈活地定義適合它們需要的命令。MSG 訊框(Frame)透過 APS APSDE-DATA.request 原語發送，透過 APSDE-DATA.indication 原語接收。應用物件用設備描述來定義每個簇的服務類型，因此也定義了支援相應服務的訊框(Frame)類型。對於 MSG 訊框(Frame)，設備描述還負責定義訊息的用法。MSG 事務訊框(Frame)的格式如下：

比特數：8	可變長度
事務長度	事務資料

事務長度欄位的長度是 8 位元，它指定了事務資料欄位包含資料的位元組數。**事務資料**欄位包含的是特定應用配置檔定義的訊息，除非源和目的實體都支援資料拆分，否則該欄位的長度不超過 maxCommandSize。

1.3.5 KVP 命令訊框(Frame)

ZigBee 規範 1.0 目前支援下面這些 KVP 命令：

- 設置、要求確認的設置、要求確認的讀取命令，它們是對屬性值進行操作；
- 設置回應和讀取回應命令，它們分別是對接收到的要求確認設置屬性命令和要求確認讀取屬性值命令的回應；
- 事件和要求確認的事件命令，它們用來通知另一個設備某個屬性值發生了改變；
- 事件回應命令，它是對要求確認的事件命令的回應。

KVP 命令格式採用基於 WBXML（WAP 二進位 XML）的壓縮 XML（擴充標記語言）。在這種壓縮格式中，原文標記被壓縮成一個單字節的表示格式。根據 XML 模式，壓縮 XML 可以擴充成一個不壓縮的 XML 描述，用到其他系統中。正常操作情況下，ZigBee 無線鏈路不發送不壓縮的 XML。

當一個設備想從另一個設備讀取一個屬性值的時候，就產生要求確認的讀取命令。該命令訊框(Frame)的格式如下：

比特數：8	4	4	16
事務序號	命令類型標識	屬性資料類型	屬性標識
事務頭	事務有效載荷		

其中：**事務序號**欄位設爲應用層維護的序號加 1；**命令類型標識**欄位設爲二進位 0100；**屬性資料類型**欄位根據要操作的屬性作相應的設置；**屬性標識**欄位包含的是要讀取的屬性的標識碼。

收到要求確認的讀取命令訊框(Frame)，接收設備將判斷是否定義了命令請求的屬性。如果沒有定義該屬性，接收設備將產生並向讀取命令發送設備回饋一個讀取回應命令訊框(Frame)，並把該回應命令訊框(Frame)的錯誤程式設爲適當的值來指示讀取屬性命令出現的

錯誤。如果接收設備定義了讀取命令請求的屬性，接收設備將產生並向讀取命令發送設備回饋一個讀取回應命令訊框(Frame)，該回應命令中攜帶了被請求屬性的值。讀取回應命令訊框(Frame)的格式如下：

比特數：8	4	4	16	8	可變長度
事務序號	命令類型標識	屬性資料類型	屬性標識	錯誤程式	屬性資料
事務頭	事務有效載荷				

讀取回應命令訊框(Frame)是對要求確認讀取命令的回應。其中：事務序號欄位應設爲相應讀取命令訊框(Frame)中的事務序號值。**命令類型標識**欄位應設爲二進位 1000。**屬性資料類型**欄位應設爲被請求屬性的類型。**屬性標識**欄位包含的是被請求屬性的標識碼。如果設備定義了被請求的屬性，並且讀取命令訊框(Frame)中部含錯誤，則**錯誤程式**欄位設爲 0x00，表示讀取屬性值成功；否則，錯誤程式欄位就設置爲適當的錯誤程式。**屬性資料**欄位包含的是被請求屬性的值，它應是特定資料類型格式的整數個位元組。如果該欄位的長度不是由屬性的資料類型直接定義，則該欄位的第一個位元組便是剩餘資料的長度（位元組數）。接收到讀取回應命令訊框(Frame)後，如果錯誤程式欄位等於 0x00，則表示讀取屬性成功並可以使用讀到的屬性值；如果錯誤程式欄位不等於 0x00，則表示讀取屬性的事務失敗。

當一個設備想設置另一個設備的屬性值時，就產生設置和要求確認的設置命令訊框(Frame)。當要求接收設備對設置命令進行確認時，使用要求確認的設置命令。設置命令訊框(Frame)的格式如下：

比特數：8	4	4	16	可變長度
事務序號	命令類型標識	屬性資料類型	屬性標識	屬性資料
事務頭	事務有效載荷			

其中：**事務序號**欄位設爲應用層維護的序號數加 1。**命令類型標識**欄位設爲二進位 0001 或 0101，分別表示設置或要求確認的設置命令訊框(Frame)。**屬性資料類型**欄位應置爲要設置屬性的資料類型。**屬性標識**欄位包含的是要設置的屬性標識碼。**屬性資料**欄位包含的是要寫到屬性標識欄位指定屬性的資料，該資料應是特定資料類型的整數位元組長度。如果該欄位的長度不是由屬性的資料類型直接定義的，則該欄位的第一個位元組便是剩餘資料的長度（位元組數）。收到設置命令訊框(Frame)後，接收設備先判斷是否定義了請求設置的屬性。如果被請求的屬性沒有定義，接收設備將忽略設置命令；如果定義了被請求的屬性，接收設備將把屬性資料欄位中的資料寫到屬性標識欄位指定的屬性中。當收到要求確認的設置命令訊框(Frame)時，接收設備先判斷是否定義了請求設置的屬性。如果被請求的屬性沒有定義，接收設備將產生並向設置命令發送設備回饋一個設置響應命令訊框(Frame)，該回應命令訊框(Frame)的錯誤程式欄位設爲合適的值來指示設置過程中產生的錯誤；如果定義了被請求的屬性，接收設備將把屬性資料欄位中的資料寫到屬性標識欄位指定的屬性中，並向設置命令發送設備回饋一個設置回應命令訊框(Frame)，合理設置錯誤程式欄位。設置相應命令訊框(Frame)的格式如下：

比特數：8	4	4	16	8
事務序號	命令類型標識	屬性資料類型	屬性標識	屬性資料
事務頭	事務有效載荷			

其中：**事務序號**欄位應設爲要求確認設置命令訊框(Frame)中的事務序號值。**命令類型**

標識欄位設爲二進位 1001。**屬性資料類型**欄位設爲被設置屬性的資料類型。**屬性標識**欄位包含的是被設置屬性的標識碼。如果定義了被請求的屬性，並且要求確認的設置命令沒有錯誤，則設置回應命令中的**錯誤程式**欄位設爲 0x00，表示請求設置成功；否則，**錯誤程式**欄位將根據錯誤情況設置爲非 0x00 值。接收到設置回應命令訊框(Frame)，如果錯誤程式欄位爲 0x00，則表示請求設置成功；否則就表示設置屬性的事務失敗。

當一個設備要通知另一個設備某個屬性值發生改變時，就發送事件或要求確認的事件命令訊框(Frame)。當要求接收設備回饋確認時，使用帶確認的事件命令。事件命令訊框(Frame)的格式如下：

比特數：8	4	4	16	可變長度
事務序號	命令類型標識	屬性資料類型	屬性標識	屬性資料
事務頭	事務有效載荷			

其中：**事務序號**欄位應設爲應用層維護的序號加 1。**命令類型標識**欄位設爲二進位 0010 或 0110，分別表示事件命令和要求確認的事件命令。**屬性資料類型**欄位包含的是屬性標識欄位指定屬性的新值。接收到事件命令訊框(Frame)時，接收設備就獲知了屬性標識欄位指定屬性的新值。當接收到要求確認的事件命令時，接收設備獲知屬性標識欄位指定屬性的新值，並向發送設備回饋一個事件響應命令訊框(Frame)。事件回應命令訊框(Frame)的格式如下：

比特數：8	4	4	16	8
事務序號	命令類型標識	屬性資料類型	屬性標識	錯誤碼
事務頭	事務有效載荷			

它是對要求確認的事件命令的回應。其中：**事務序號**欄位設置爲要求確認事件命令訊框(Frame)中事務序號欄位的資料。**命令類型標識**欄位設爲二進位 1010。如果要求確認的事件命令訊框(Frame)中不含錯誤，則時間回應命令中錯誤程式欄位設爲 0x00，表示通知成功；否則，錯誤程式欄位指示儀個相應的錯誤。當接收到事件回應命令時，事件命令的發送設備就被告知屬性值改變的通知結果。如果回應命令的錯誤程式欄位爲 0x00，表示通知事務成功；否則，就表示通知事務失敗。

1.3.6 AF 功能描述

一般應用框架訊框(Frame)結構允許把幾個獨立的事務組合到一個訊框(Frame)中，這種事務的組合叫作“聚合”。只有那些共用相同服務類型（KVP 或 MSG）和簇標識的事務才能聚合到一起，且聚合的訊框(Frame)長度不能超過最大允許值。當接收到 KVP 事務的聚合集時，接收設備將依次處理各個事務；對那些要求回應的事務，接收設備也組合以個回應事務的聚合集，一併回饋給發送設備。接收方應保證回應事務聚合集的長度不超過 APS 訊框(Frame)長限制，如果超過單個 APS 訊框(Frame)長，接收設備將對聚合回應訊框(Frame)進行拆分，透過多次發送，並在不超過長度限制的前提下吧儘量多的回應訊框(Frame)聚合到一起發送。

應用框架能夠過濾經 APS 子層資料服務到達的訊框(Frame)，只把有用的訊框(Frame)提交給駐留在活動端點上的應用。應用框架透過 APSDE-DATA.indication 原語從 APS 子層接收資料，並提交給 DstEndpoint 和 ProfileId 參數指定的端點。如果應用框架接收到非活動

端點的訊框(Frame)，它將丟棄該訊框(Frame)；否則，應用框架將判斷原語指定的配置檔標識與指定端點實現的配置檔標識是否匹配。如果配置檔標識不匹配，應用框架將拒絕該訊框(Frame)；如果配置檔匹配，則應用框架將把接收訊框(Frame)的有效載荷遞交給指定端點上的應用。

1.4 ZigBee 設備配置檔

1.4.1 設備配置檔概述

ZigBee 設備配置檔定義了設備描述和簇，它的工作原理與所有 ZigBee 配置檔一樣；但與專用配置檔不同的是，ZigBee 設備配置檔中的設備描述和簇標識定義的是所有 ZigBee 設備都支援的能力。ZigBee 設備配置檔支援 ZigBee 協定內設備間通訊的四種關鍵功能：

設備和服務發現，終端設備綁定請求處理，綁定和解綁定命令處理，網路管理。

設備發現爲設備提供了判別 PAN 中其他設備身份的能力。64 位元 IEEE 位址和 16 位元網路位址都支援設備發現功能。設備發現訊息可以使用下面兩種方式：

1. 廣播定址。網路中的所有設備都要根據邏輯設備類型和匹配原則對設備發現請求作出回應。ZigBee 終端設備以其自身位址作爲回應；ZigBee 協調器和 ZigBee 路由器除以自身的位址作爲回應外，還要根據設備發現請求類型返回與其關聯的設備位址。廣播設備發現中的回應設備採用的是單播回應的 APS 確認服務。

2. 單播定址。僅指定的單個設備對設備發現請求作出回應。ZigBee 終端設備以其自身位址作出回應；ZigBee 協調器或路由器除了以自身位址回應外，還要返回每個關聯設備的位址。

服務發現爲設備提供了判別 PAN 中其他設備提供服務的能力。服務發現訊息可以使用下面兩種方式：

1. 廣播定址。每個與服務發現請求準則匹配的設備都應作出回應，返回相應的資訊；對帶有休眠關聯設備的 ZigBee 協調器或 ZigBee 路由器，如果休眠設備與服務發現請求的準則匹配，則 ZigBee 協調器或 ZigBee 路由器將緩存服務發現資訊並代表休眠設備作出回應。

2. 單播定址。僅指定的設備回應服務發現請求。對帶有休眠關聯設備的 ZigBee 協調器或 ZigBee 路由器，如果休眠設備與服務發現請求的準則匹配，則 ZigBee 協調器或 ZigBee 路由器將緩存服務發現資訊並代表休眠設備作出回應。

服務發現支援下面 7 種查詢類型：

1. 活動端點。這種命令允許探詢設備判定活動端點。該命令可以使用廣播或單播方式定址。

2. 匹配簡單描述符。這種命令允許探詢設備從匹配的目的設備獲知配置檔 ID、輸入/輸出簇標識列表，並要求返回端點標識。該命令可以使用廣播或單播方式定址。對廣播服務發現請求，回應設備應採用單播回應的 APS 確認服務作出回應。

3. 簡單描述符。這種命令允許探詢設備獲得端點的簡單描述符。該命令應使用單播定址方式。

4. 節點描述符。這種命令允許探詢設備獲得指定設備的節點描述符。該命令應使用單播定址方式。

5. 電源描述符。這種命令允許探詢設備獲得指定設備的電源描述符。該命令應使用單

播定址方式。

6. 複雜描述符。這種可選命令允許探詢設備獲得指定設備的複雜描述符。該命令應使用單播定址方式。

7. 使用者描述符。這種可選命令允許探詢設備獲得指定設備的使用者描述符。該命令應使用單播定址方式。

終端設備綁定提供下面兩種功能：

1. 爲應用提供“簡單綁定”的能力，透過使用者干預來識別命令/控制設備對。典型的應用是要求使用者按兩個設備上的按鈕來完成安裝。

2. 爲應用提供簡化綁定方法的能力，透過使用者干預來識別命令/控制設備對。典型的應用是要求使用者按兩個設備俄上的按鈕來完成安裝。再次使用同樣的機制將刪除綁定列表的記錄。

綁定功能提供了建立綁定表記錄的能力，綁定表記錄把控制資訊映射到其目標物件；解綁定功能則提供了刪除綁定表記錄的能力。

網路管理功能提供了從設備中獲知管理資訊的能力和實施管理資訊控制的能力。網路管理功能從設備中獲得的管理資訊包括網路發現結果、到鄰近節點的鏈路品質、路由表和綁定表。實施管理資訊控制就是指網路解關聯。

ZigBee 設備配置檔使用單一的設備描述。其中的強制簇是在所有 ZigBee 設備中都存在的，某些資訊的回應方式是與邏輯設備類型有關的；而可選簇則是與邏輯設備類型無關的。

ZigBee 設備配置檔採用 MSG 服務類型。

ZigBee 設備配置檔採用了一種使用者端/伺服器的拓撲。執行設備發現、服務發現、綁定或網路管理請求的設備充當的是使用者端的角色，而對這些請求進行服務和作出回應的設備充當的是伺服器的角色。一個設備中使用者端和伺服器兩種角色不是排他性的，一個設備既可以是使用者端也可以是伺服器。使用者端透過設備配置檔訊息發送請求。伺服器對請求進行處理，使用者端就接收到伺服器對其發送請求的回應。伺服器是使用者端請求的目標，它對來自使用者端的請求進行處理並作出回應。

ZigBee 設備配置檔中的簇標識格式如下：

比特位：0～6	7
訊息號	請求/回應位：請求=0，回應=1

1.4.2 使用者端服務

ZigBee 設備配置檔使用者端服務支援從使用者端向伺服器傳送設備發現和服務發現請求、終端設備綁定請求、綁定和解綁定請求、網路管理請求。另外，使用者端服務還支援接收伺服器對使用者端這些請求的回應。ZigBee 設備配置檔設備和服務發現使用者端服務支援的原語包括：NWK_addr_req、IEEE_addr_req、Node_Desc_req、Power_desc_req、Simple_Desc_req、Active_EP_req、Match_Desc_req、Complex_Desc_req、User_Desc_req、Discovery_Register_req、End_Device_annce、User_Desc_set。終端設備綁定、綁定和解綁定使用者端服務支援的原語包括：End_Device_Bind_req、Bind_req、Unbind_req。網路管理使用者端服務支援的原語包括：Mgmt_NWK_Disc_req、Mgmt_Lqi_req、Mgmt_Rtg_req、Mgmt_Bind_req、Mgmt_Leave_req、Mgmt_Direct_Jonit_req。下面分別介紹每個原語的語法和功能。

1.4.2.1 設備和服務發現使用者端服務

1. NWK_addr_req 原語

NWK_addr_req 原語由本地設備根據已知的遠端設備 IEEE 位址產生，試圖產訊遠端設備的 16 位元網路位址。該原語的目的定址應採用廣播方式。NWK_addr_req 原語的語法如下：

ClusterID=0x00　　NWK_addr_req　　（IEEEAddr，RequestType，StartIndex ）

其中：參數 IEEEAddr 表示遠端設備要匹配的 IEEE 位址；參數 RequestType 是整數變數，表示該命令的請求類型，0x00 表示單設備回應，0x01 表示擴充回應，其他取值預留；參數 StartIndex 是整數變數，其取值範圍是 0x00～0xff，當該命令爲擴充回應時，StartIndex 表示關聯設備列表中被請求設備的起始索引。

遠端設備接收到網路位址請求命令後，比較 IEEEAddr 參數和本地 IEEE 位址。如果遠端設備的 IEEE 位址與 IEEEAddr 參數不匹配，該請求將被丟棄，也不作出回應；如果遠端設備的 IEEE 位址與 IEEEAddr 參數匹配，遠端設備將根據 RequestType 作出回應。如果 RequestType 參數是預留值，回應命令將返回一個狀態 INV_REQUESTTYPE；如果 RequestType 是單設備請求或擴充請求，遠端設備俄將產生一個單播訊息對本地設備的請求作出回應，該回應以遠端設備的 16 位元 NWK 位址作爲源位址，匹配的 IEEE 位址作爲回應有效載荷。如果 RequestType 是單設備請求，回應訊息以 SUCCESS 狀態發送。如果 RequestType 是擴充請求並且遠端設備是帶有關聯設備的 ZigBee 協調器或路由器，則遠端設備首先把匹配的 IEEE 位址和 NWK 位址放入回應訊息有效載荷中，再從關聯設備 NWK 位址列表的 StartIndex 位置開始放入完整的位址記錄，直到回應訊框(Frame)長達到 APS 訊框(Frame)的最大長度，回應命令的狀態時 SUCCESS。

2. IEEE_address_req 原語

IEEE_addr_req 原語由本地設備根據已知的遠端設備 NWK 位址產生，試圖查詢遠端設備的 64 位元 IEEE 位址。該原語的目的定址應採用單播方式。IEEE_addr_req 原語的語法如下：

ClusterID=0x01　　IEEE_addr_req　　（NWKAddrOfInterest，RequestType，StartIndex）

其中：參數 NWKAddrOfInterest 表示用於 IEEE 位址映射的 NWK 位址；參數 RequestType 是整數變數，表示該命令的請求類型，0x00 表示單設備回應，0x01 表示擴充回應，其他取值預留；參數 StartIndex 是整數變數，其取值範圍是 0x00～0xff，當該命令爲擴充回應時，StartIndex 表示關聯設備列表中被請求設備的起始索引。

遠端設備接收到 IEEE 位址請求命令後，產生一個單播訊息對 IEEE_addr_req 指示的源位址作出回應，遠端設備 64 位元 IEEE 位址放在 IEEE_addr_rsp 有效載荷的第一個欄位。另外，如果 RequestType 爲擴充請求並且遠端設備是帶有關聯設備的 ZigBee 協調器或路由器，遠端設備應首先把自身的 64 位 IEEE 位址放在回應訊框(Frame)的有效載荷部分，再從關聯設備 IEEE 位址列表的 StartIndex 位置開始放入完整的 IEEE 位址記錄，直到回應訊框(Frame)長達到 APS 訊框(Frame)的最大長度，回應命令的狀態時 SUCCESS。

3. Node_Desc_req 原語

Node_Desc_req 原語由本地設備產生，用來查詢遠端設備的節點描述符。該原語的目的定址只能採用單播放時。Node_Desc_req 原語的語法如下：

ClusterID=0x02　　Node_Desc_req （NWKAddrOfInterest）　　該原語的唯一參數 NWKAddrOfInterest 表示被請求遠端設備的 NWK 位址。當遠端設備接收到節點描述符請求

命令後，產生一個單播訊息對 Node_Desc_req 指示的源位址作出回應，回應命令訊框(Frame)中包含遠端設備的節點描述符。

4. Power_Desc_req 原語

Power_Desc_req 原語由本地設備產生，用來查詢遠端設備的電源描述符。該原語的目的定址只能採用單播方式。Power_Desc_req 原語的語法如下：

ClusterID=0x03　　Power_Desc_req　（NWKAddrOfInterest）

該原語的唯一參數 NWKAddrOfInterest 表示被請求遠端設備的 NWK 位址。當遠端設備接收到電源描述符請求命令後，產生一個單播訊息對 Poer_Desc_req 指示的源位址作出相應，回應命令訊框(Frame)中包含遠端設備的電源描述符。

5. Simple_Desc_req 原語

Simple_Desc_req 原語由本地設備產生，用來查詢遠端設備指定端點的簡單描述符。該原語的目的定址只能採用單播放時。Simple_Desc_req 原語的語法如下：

ClusterID=0x04　　Simple_Desc_req（NWKAddrOfInterest，endpoint）

其中：參數 NWKAddrOfInterest 表示被請求遠端設備的 NWK 位址；endpoint 表示目的設備的端點。當遠端設備接收到簡單描述符請求命令後，產生一個單播訊息對 Simple_Desc_req 指示的源位址作出回應，回應命令訊框(Frame)中包含遠端設備指定端點的簡單描述符。

6. Active_Ep_req 原語

Simple_Ep_req 原語由本地設備產生，用來獲得遠端設備的活動端點列表。該原語的目的定址只能採用單播方式。Active_Ep_req 原語的語法如下：

ClusterID=0x05　　Active_Ep_req（NWKAddrOfInterest）

該原語的唯一參數 NWKAddrOfInterest 表示被請求遠端設備的 NWK 位址。當遠端設備接收到活動端點請求命令後，產生一個單播訊息對 Active_Ep_req 指示的源位址作出回應，響應命令訊框(Frame)中包含遠端設備的活動端點列表。

7. Match_Desc_req 原語

Match_Desc_req 原語由本地設備產生，用來探詢支援某種匹配規則的遠端設備，滿足請求的匹配規則的遠端設備以位址和端點作爲回應。該原語的目的定址可以採用廣播或單播放時。Match_Desc_req 原語的語法如下：

ClusterID=0x06　　Match_Desc_req（NWKAddrOfInterest，ProfileID，NumInClusters，InClusterList，NumOutClusters，OutClusterList）

其中：參數 NWKAddrOfInterest 表示被請求遠端設備的 NWK 位址；參數 NumInClusters 表示 InClusterLIst 中列出的用於匹配的輸入簇的個數；參數 InClusterList 是用於匹配遠端設備的輸入簇標識的列表，該列表的元素爲本地設備的輸出簇標識；參數 NumOutClusters 表示 OutClusterList 中列出的用於匹配的輸出簇的個數；參數 OutClusterList 是用於匹配遠端設備的輸出簇標識的列表，該列表的元素爲本地設備的輸入簇標識。

遠端設備收到匹配描述符請求命令後，將對所有活動端點上的簡單描述符進行評估匹配。如果 ProfileID 匹配，並且 InClusterList 或 OutClusterList 中存在一個元素對應地域遠端設備活動端點簡單描述符的 AppInClusterList 或 AppOutClusterList 中的一個元素相匹配，就表示找到了匹配的設備。需要注意的是，該原語中參數 NumInClusters 和 NumOutClusters 可以設爲 0，並省略參數 InClusterList 和 OutClusterList，此時，只要 ProfileID 匹配就表示找到了匹配的遠端設備。如果檢測到了匹配，遠端設備將產生一個單播訊息對本地設備的請求作出回應，回應訊框(Frame)中包含遠端設備的位址和檢測到匹配的端點號。

8. Complex_Desc_req 原語

Complex_Desc_req 原語由本地設備產生，用疑惑的遠端設備的複雜描述符。該原語的

目的定址只能採用單播放時。Complex_Desc_req 原語的語法如下：

ClusterID=0x10　　Complex_Desc_req （NWKAddrOfInterest）

該原語的唯一參數 NWKAddrOfInterest 表示被請求遠端設備的 NWK 位址。當遠端設備接收到複雜描述符請求命令後，產生一個單播訊息對 Complex_Desc_req 指示的源位址作出回應。如果遠端設備支援複雜描述符，則回應命令中包含遠端設備的複雜描述符；如果遠端設備不支援複雜描述符，則回應命令返回一個狀態 NOT_SUPPORTED。

9. User_Desc_req 原語

User_Desc_req 原語由本地設備產生，用以獲得遠端設備的使用者描述符。該原語的目的定址只能採用單播方式。User_Desc_req 原語的語法如下：

ClusterID=0x11　　User_Desc_req（NWKAddrOfInterest）

該原語的唯一參數 NWKAddrOfInterest 表示被請求遠端設備的 NWK 位址。當遠端設備接收到使用者描述符請求後，產生一個單播訊息對 User_Desc_req 指示的源位址作出回應。如果遠端設備支援使用者描述符，則回應命令訊框(Frame)中包含遠端設備的使用者描述符；如果遠端設備不支援使用者描述符，則回應命令返回一個狀態 NOT_SUPPORTED。

10. Discovery_Register_req 原語

Discovery_Register_req 原語使得網路中的設備能夠向 ZigBee 協調器註冊發現資訊。該原語的目的定址只能採用單播放時。其目的位址就是 ZigBee 協調器的位址。Discovery_Register_req 原語的語法如下：

ClusterID=0x12　　Discovery_Register_req （NWKAddr，IEEEAddr ）

其中：參數 NEKAddr 和 IEEEAddr 分別是本地設備的 NWK 位址和 IEEE 位址。ZigBee 協調器接收到發現註冊請求命令後，將產生一個單播訊息對 Discovery_Register_req 指示的源位址作出回應，回應命令訊框(Frame)中包含請求的狀態。如果 ZigBee 協調器不支持 Discovery_Register_req，則回應命令返回狀態 NOT_SUPPORTED；如果 ZigBee 協調器支援 Discovery_Register_req，它將使用設備和服務發現命令上載本地設備的發現資訊。這樣，以後的發現請求就可以指向 ZigBee 協調器，ZigBee 協調器能夠提供註冊設備的設備和服務資訊。

11. End_Device_annce 原語

End_Device_annce 原語使得 ZigBee 終端設備加入和重新加入網路時能夠通知 ZigBee 協調器。該原語的目的位址採用廣播方式。End_Device_annce 原語的語法如下：

ClusterID=0x13　　End_Device_annce （NWKAddr，，IEEEAddr）

其中：參數 NWKAddr 和 IEEEAddr 分別是本地設備的 NWK 位址和 IEEE 位址。當遠端設備（ZigBee 協調器或綁定操作的源設備）收到該命令後，將利用訊息中的 IEEEAddr 來匹配遠端設備中綁定表記錄。如果存在匹配的記錄，遠端設備用 IEEEAddr 對應的 NWKAddr 來更新 APS 資訊庫位址映射。

12. User_Desc_set 原語

User_Desc_set 原語由本地設備產生，用來配置遠端設備的使用者描述符。該原語的目的定址只能採用單播放時。User_Desc_set 原語的語法如下：

ClusterID=0x14　　User_Desc_set（NWKAddrOfInterest，UserDescription）

其中：參數 NWKAddr 表示被請求設備的 NWK 位址；參數 UserDescription 是 ASCII 字串，表示要配置的遠端設備使用者描述符。遠端設備收到該命令後，就用提供的資料配置使用者描述符，請求命令的結果透過 User_Desc_conf 命令返回給本地設備。如果遠端設備不支援使用者描述符設置命令或不存在使用者描述符，則 User_Desc_conf 命令返回狀態 NOT_SUPPORTED；如果存在使用者描述符，則遠端設備用 User_Desc_set 命令中的

UserDescription 配置使用者描述符，並用 User_Desc_conf 命令返回狀態 SUCCESS。

1.4.2.2 綁定和解綁定使用者端服務

1. End_Device_Bind_req 原語

End_Device_Bind_req 原語由本地設備產生，用來執行終端設備與遠端設備的綁定。End_Device_Bind_req 通常在使用者執行某種動作（如按下按鈕）時產生。該原語的目的位址是 ZigBee 協調器，目的定址應採用單播方式。End_Device_Bind_req 原語的語法如下：

ClusterID=0x20　　End_Device_Bind_req（LocalCoordinator，BindingTarget，Endpoint，ProfileID，NumInClusters，InClusterList，，NumOutClusters，，OutClusterList）

其中：參數 LocalCoordinator 表示 ZigBee 協調器的位址；參數 BindingTarget 表示綁定目標的 16 位元位址；參數 Endpoint 表示原語產生設備的端點，其取值爲 1～240；參數 ProfileID 表示在 ZigBee 協調器預先設置的超時間隔內收到的兩個 End_Device_Bind_req 要匹配的配置檔 ID；參數 NumInClusters 表示用於設備綁定的 InClusterLIst 中包含的簇標識數目；參數 InClusterLIst 表示遠端設備要匹配的輸入簇標識列表，該列表中的元素爲本地設備所支援的輸出簇標識；參數 NumOutClusters 表示用於設備綁定的 OutClusterList 中包含的簇標識數目；參數 OutClusterList 表示遠端設備要匹配的輸出簇標識列表，該列表中的元素爲本地設備所支援的輸入簇標識。

ZigBee 協調器接收到第一個 End_Device_Bind_req 後保留至預設的超時時限，等待第二個 End_Device_Bind_req。如果在預設時限內沒有收到第二個 End_Device_Bind_req，ZigBee 協調器將產生一個狀態爲 TIMEOUT 的 End_Device_Bind_rsp 原語作爲對產生請求原語的本地設備的回應；如果在規定時限內收到第二個 End_Device_Bind_req，則基於 ProfileID、InClusterList 和 OutClusterList 檢測兩個 End_Device_Bind_req 的匹配性。如果 ProfileID 不匹配或 InClusterList 或 OutClusterList 中沒有匹配的元素，ZigBee 協調器將產生狀態爲 NO_MATCH 的 End_Device_Bind_rsp 原語，分別對兩個本地設備的請求作出回應；如果 ProfileID 匹配，並且至少有一個輸入或輸出簇 ID 匹配，則 ZigBee 協調器將產生狀態爲 SUCCESS 的 End_Device_Bind_rsp 原語，分別對兩個本地設備的 End_Device_Bind_req 作出相應。此時，ZigBee 協調器需要每個本地設備的 64 位元 IEEE 位址。如果這些位址未知，ZigBee 協調器要使用 IEEE_Addr_req 命令和相應的 IEEE_Addr_rsp 回應命令來獲取位址。爲了便於綁定操作，ZigBee 協調器任意指定一個匹配的簇 ID 值向 BindingTarget 發出 Unbind_req 命令。如果返回狀態爲 NO_ENTRY，ZigBee 協調器將針對每個匹配的簇 ID 值發出 Bind_req 命令；否則 ZigBee 協調器認爲 End_Device_Bind_req 意圖刪除已有的綁定記錄，於是針對其餘的匹配簇 ID 分別發出 Unbind_req 命令。該過程中的第一個 Unbind_req 命令以及其後的 Bind_req 或 Unbind_req 命令都是指向第一個 End_Device_Bind_req 命令指定的 BindingTarget 的，即這些命令的 64 位源位址和目的位址分別由第一和第二個 End_Device_Bind_req 命令中的 16 位網路位址得到；源端點和目的端點分別是第一和第二個 End_Device_Bind_req 命令中包含的端點。

2. Bind_req 原語

Bind_req 原語由本地設備產生，意圖爲其參數中的源位址和目的位址建立一條綁定表記錄。該原語的目的定址只能採用單播方式，其目的位址必須是 ZigBee 協調器的位址或 SrcAddress。Bind_req 原語的語法如下：

ClusterID=0x21　　Bind_req（SrcAddress，SrcEndp，ClusterID，DstAddress，DstEndp）

其中：參數 SrcAddress 是源設備的 IEEE 位址；SrcEndp 是綁定記錄的源端點；ClusterID 是源設備要綁定到目的設備的簇標識；DstAddress 是目的設備的 IEEE 位址；DstEndp 是綁定記錄的目的端點。接收到 Bind_req 命令後，遠端設備（ZigBee 協調器或 SrcAddress 指定的設備）將根據命令提供的參數建立綁定表記錄。如果遠端設備支援綁定管理器並且建立了一個綁定表記錄，則響應狀態爲 SUCCESS；否則，遠端設備的回應狀態爲 NOT_SUPPORTED。

3. Unbind_req 原語

Unbind_req 原語由本地設備用來刪除源位址和目的位址指定的一個綁定表記錄。該原語的定址只能採用單播方式，其目的位址必須是 ZigBee 協調器的位址或 SrcAddress。Unbind_req 原語的語法如下：

ClusterID=0x22　　Unbind_req（SrcAddress，SrcEndp，ClusterID，DstAddress，DstEndp）

其中各參數的定義同 Bind_req 原語。接收到 Unbind_req 命令後，遠端設備首先判斷是否支援該請求。如果不支援該請求，遠端設備將返回狀態爲 NOT_SUPPORTED 的回應命令；如果遠端設備（ZigBee 協調器或 SrcAddress 指定的設備）支援該請求，則根據命令參數提供的位址參數刪除相應的綁定表記錄。如果 SrcAddress 指定的遠端設備不支援綁定管理器，就返回狀態 NOT_SUPPORTED；如果位址、端點和簇標識參數指定的綁定表記錄不存在，則返回狀態 NO_ENTRY；其他情況下，遠端設備將刪除指定的綁定表記錄並返回狀態 SUCCESS。

1.4.2.3 網路管理使用者端服務

1. Mgmt_NWK_Disc_req 原語

Mgmt_NWK_Disc_req 原語由本地設備用來請求遠端設備執行通道掃描，報告本地設備附近存在的網路情況。該原語的定址應採用單播方式。Mgmt_NWK_Disc_req 原語的語法如下：

ClusterID=0x30　　Mgmt_NWK_Disc_req（ScanChannels，ScanDuration，StartIndex）

其中：參數 ScanChannels 爲 32 位，其低有效位的 27 位分別表示 27 個有效通道是否掃描，1 表示掃描，0 表示不掃描；參數 ScanDuration 用來定義掃描每個通道所用的時間；參數 StartIndex 表示回應命令報告的掃描結果在 NLME-NETWORK-DISCOVERY.confirm 的 NetworkList 中的起始索引。遠端設備接收到 Mgmt_NWK_Disc_req 命令後，執行網路層請求原語 NLME-NETWORK-DISCOVERY.request 來掃描通道，掃描結果透過 Mgmt_NWK_Disc_rsp 命令報告給本地設備。如果遠端設備不支援 Mgmt_NWK_Disc_req 命令，就返回狀態爲 NOT_SUPPORTED 的 Mgmt_NWK_Disc_rsp 命令；如果掃描成功，Mgmt_NWK_Disc_req 命令的狀態爲 SUCCESS 並包含掃描結果，報告的結果從掃描結果 NetworkList 的元素 StartIndex 開始；如果掃描不成功，則 Mgmt_NWK_Disc_rsp 命令包含 NLME-NETWORK-DISCOVERY.confirm 原語報告的錯誤程式。

2. Mgmt_Lqi_req 原語

Mgmt_Lqi_req 原語由本地設備產生，用來獲取遠端設備的臨近列表以及遠端設備與每個鄰居之間的 LQI 值。該原語的定址應採用單播方式，其目的位址是 ZigBee 協調器或 ZigBee 路由器的位址。Mgmt_Lqi_req 原語的語法如下：

ClusterID=0x31　　Mgmt_Lqi_req（StartIndex）

其唯一參數 StartIndex 表示鄰居列表中被請求元素的起始索引。接收到 Mgmt_Lqi_req 命令後，遠端設備（ZigBee 協調器或 ZigBee 路由器）將透過 NLME-GET.request 原語檢索鄰居

表和相關 LQI 值，並透過 Mgmt_Lqi_req 命令報告查詢結果。如果遠端設備不支援 Mgmt_Lqi_req 命令，則返回狀態爲 NOT_SUPPORTED 的 Mgmt_Lqi_rsp 命令；如果成功獲得鄰居表，則 Mgmt_Lqi_rsp 命令的狀態爲 SUCCESS，包含的鄰居資訊從列表的元素 StartIndex 開始；如果獲取鄰居表不成功，則 Mgmt_Lqi_rsp 命令包含 NLME-GET.confirm 原語報告的錯誤程式。

3. Mgmt_Rtg_req 原語

Mgmt_Rtg_req 原語由本地設備產生，用來獲取遠端設備的路由表資訊。該原語的定址應採用單播方式，其目的位址必須是 ZigBee 協調器或 ZigBee 路由器的位址。Mgmt_Rtg_req 原語的語法如下：

ClusterID=0x32　　Mgmt_Rtg_req （StartIndex）

其唯一參數 StartIndex 表示路由表中被請求元素的起始索引。接收到 Mgmt_Rtg_req 命令後，遠端設備（ZigBee 協調器或 ZigBee 路由器）將透過 NLME-GET.request 原語向 NWK 層索取路由表中的相關記錄，並透過 Mgmt_Rtg_rsp 命令報告請求結果。如果遠端設備不支援 Mgmt_Rtg_req 這種可選的管理請求，它將返回狀態爲 NOT_SUPPORTED 的 Mgmt_Rtg_rsp 命令。如果成功獲得路由表，則 Mgmt_Rtg_rsp 命令狀態爲 SUCCESS，並報告獲得的路由資訊，這些路由資訊從路由表的第 StartIndex 個記錄開始；如果獲取路由表不成功，則 Mgmt_Rtg_rsp 命令包含 NLME-GET.confirm 原語報告的錯誤程式。

4. Mgmt_Bind_req 原語

Mgmt_Bind_req 原語由本地設備產生，用來獲取遠端設備的綁定表資訊。該原語的定址應採用單播方式，其目的位址必須是 ZigBee 協調器或 ZigBee 路由器的位址。Mgmt_Bind_req 原語的語法如下：

ClusterID=0x33　　Mgmt_Bind_req （StartIndex）

其唯一參數 StartIndex 表示綁定表中被請求元素的起始索引。接收到 Mgmt_Bind_req 命令後，遠端設備（ZigBee 協調器或 ZigBee 路由器）將透過 APSME-GET。request 原語向 APS 子層索取綁定表中的相關記錄，並透過 Mgmt_Bind_rsp 命令報告請求結果。如果遠端設備不支援 Mgmt_Bind_req 這種可選的管理請求，它將返回狀態爲 NOT_SUPPORTED 的 Mgmt_Bind_rsp 命令。如果成功獲得綁定表，則 Mgmt_Bind_rsp 命令狀態爲 SUCCESS，並報告獲得的綁定資訊，這些綁定資訊從綁定表的第 StartINdex 個記錄開始；如果獲取綁定表不成功，則 Mgmt_Bind_rsp 命令包含 APSME-GET.confirm 原語報告的錯誤程式。

5. Mgmt_Leave_req 原語

Mgmt_Leave_req 原語由本地設備產生，請求遠端設備離開網路或請求另一個設備離開網路。該請求由本地設備的管理應用指向遠端設備，遠端設備根據 Mgmt_Leave_req 提供的參數執行 NLME-LEAVE.request。Mgmt_Leave_req 原語的語法如下：

ClusterID=0x34　　Mgmt_Leave_req（DeviceAddress）

其唯一參數 DeviceAddress 表示要離開網路的設備 64 位元 IEEE 位址。接收到 Mgmt_Leave_req 命令後，遠端設備根據 Mgmt_Leave_req 命令提供的設備位址 DeviceAddress，發出 NLME-LEAVE.request 原語，並透過 Mgmt_Leave_rsp 命令把請求設備離開網路的結果報告給本地設備。如果遠端設備不支援 Mgmt_Leave_req 這種可選的管理請求，它將返回狀態爲 NOT_SUPPORTED 的 Mgmt_Leave_rsp 命令。如果成功實現指定設備離開網路，則 Mgmt_Leave_rsp 相應命令狀態爲 SUCCESS；如果請求指定設備離開網路不成功，則 Mgmt_Leave_rsp 命令包含 NLME-LEAVE.confirm 原語報告的錯誤程式。

6. Mgmt_Direct_Join_req 原語

Mgmt_Direct_Join_req 原語由本地設備產生，情趣遠端設備允許 DeviceAddress 指定的

設備立即加入網路。該請求由本地設備的管理應用指向遠端設備，遠端設備根據 Mgmt_Direct_Join_req 提供的參數執行 NLME-DIRECT_JOIN.request。Mgmt_Direct_Join_req 原語的語法如下：

ClusterID=0x35　　Mgmt_Direct_Join_req（DeviceAddress，CapabilityInformation）

其中：參數 DeviceAddress 表示要加入網路的設備 64 位元 IEEE 位址；CapabilityInformation 表示要加入網路的設備的功能。收到 Mgmt_Direct_Join_req 命令後，遠端設備根據 Mgmt_Direct_Join_req 命令提供的設備位址 DeviceAddress 和功能資訊 CapabilityInformation，發出 NLME-DIRECT_JOIN.request 原語，並透過 Mgmt_Direct_Join_rsp 命令把請求設備加入網路的結果報告給本地設備。如果遠端設備不支援 Mgmt_Direct_Join_req 這種可選的管理請求，它將返回狀態爲 NOT_SUPPORTED 的 Mgmt_Direct_Join_rsp 命令。如果指定設備成功加入網路，則 Mgmt_Direct_Join_rsp 回應命令狀態爲 SUCCESS；如果請求指定設備加入網路不成功，則 Mgmt_Direct_Join_rsp 命令包含 NLME-DIRECT_JOIN.confirm 原語報告的錯誤程式。

1.4.3 伺服器服務

設備配置檔伺服器服務處理設備和服務發現請求、終端設備綁定請求、綁定請求、解綁定請求和網路管理請求，並把對這些請求的回應返回給使用者端。ZigBee 設備配置檔設備和服務發現伺服器服務支援的原語包括：NWK_addr_rsp、IEEE_addr_rsp、Node_Desc_rsp、Power_Desc_rsp、Simple_Desc_rsp、Active_EP_rsp、Match_Desc_rsp、Complex_Desc_rsp、User_Desc_rsp、Discovery_Register_rsp、User_desc_conf。終端設備綁定、綁定和解綁定伺服器服務支援的原因包括：End_Device_Bind_rsp、Bind_rsp、Unbind_rsp。網路管理伺服器服務支援的原語包括：Mgmt_NWK_Disc_rsp、Mgmt_Lqi_rsp、Mgmt_Rtg_rsp、Mgmt_Bind_rsp、Mgmt_Leave_rsp、Mgmt_Direct_Jonit_rsp。每個原語的語法和功能分別介紹如下。

1.4.3.1 設備和服務發現伺服器服務

1. NWK_addr_rsp 原語

遠端設備在接收到廣播的 NWK_addr_req 後，檢測其自身的 IEEE 位址與 NWK_addr_req 的 IEEEAddr 參數是否匹配，然後產生 NWK_addr_rsp 原語。NWK_addr_rsp 回應原語的定址爲單播方式，它的語法如下：

ClusterID=0x80　　NWK_addr_rsp（Status，IEEEAddrRemoteDev，NWKAddrRemoteDev，NumAssocDev，StartIndex，NWKAddrAssocDevList）

其中：參數 Status 爲整數，表示 NWK_addr_req 執行結果的狀態，0x00 表示 SUCCESS，0x01 表示 INV_REQUESTTYPE，0x02 表示 DEVICE_NOT_FOUND，其他取值暫時預留；IEEEAddrRemoteDev 和 NWKAddrRemoteDev 分別表示遠端設備的 64 位元 IEEE 位址和 16 位 NWK 位址；NumAssocDev 表示遠端設備關聯設備的個數，其取值範圍是 0x00～0xff，如果 NumAssocDev 等於 0，則省略後兩個參數 StartIndex 和 NWKA 當地人 AssocDevList；參數 StartIndex 表示關聯設備列表的起始索引號；NWKAddrAssocDevLIst 是關聯設備的 NWK 位址列表，位址數由 NumAssocDev 指定，如果遠端設備的 IEEE 位址與 NWK_addr_req

中的 IEEEAddr 參數不匹配，遠端設備將丟棄 NWK_addr_req 請求，不返回任何回應訊息；如果遠端設備的 IEEE 位址與 NWK_addr_req 中的 IEEEAddr 參數匹配，遠端設備將產生一個單播響應資訊，NWK_addr_rsp 的有效載荷包含遠端設備匹配的 IEEE 位址和 NWK 位址；如果遠端設備是帶有關聯設備的 ZigBee 協調器或 ZigBee 路由器，則 NWK_addr_rsp 中還應包含這些關聯設備的 NWK 位址列表。

2. IEEE_addr_rsp 原語

IEEE_addr_rsp 原語是遠端設備對單播的 IEEE_addr_req 原語的回應。IEEE_addr_rsp 回應原語的定址爲單播放時，它的語法如下：

ClusterID=0x81　IEEE_addr_rsp（Status，IEEEAddrRemoteDev，NWKAddrRemoteDev，NumAssocDev，StartIndex，NWKAddrAssocDevList）

其中：參數 Status 爲整數，表示 IEEE_addr_req 執行結果的狀態，0x00 表示 SUCCESS，0x01 表示 INV_REQUESTTYPE，0x02 表示 DEVICE_NOT_FOUND，其他取值暫時預留；IEEEAddrRemoteDev 和 NWKAddrRemoteDev 分別表示遠端設備的 64 位元 IEEE 位址和 16 位 NWK 位址；NUmAssocDev 表示遠端設備關聯設備的個數，其取值範圍是 0x00～0xff，如果 IEEE_addr_req 的 RequestType 爲擴充回應並且遠端設備沒有關聯設備，則 NumAssocDev 爲 0 且省略後兩個參數 StartIndex 和 NWKAddrAssocDevList，如果 RequestType 爲單設備回應，則 NumAssocDev 及其後的參數都省略；參數 StartIndex 表示關聯設備列表的起始索引號；NWKAddrAssocDevList 是關聯設備的 NWK 位址列表，位址數由 NumAssocDev 指定。遠端設備收到 IEEE_addr_req 後，產生一個單播響應訊息 IEEE_addr_rsp，響應有效載荷的第一個欄位是遠端設備的 IEEE 位址。另外，如果 RequestType 爲擴充形影並且遠端設備爲帶有關聯設備的 ZigBee 協調器或 ZigBee 路由器，則在遠端設備 IEEE 位址之後還要添加關聯設備的 NWK 位址列表，關聯位址列表從索引號 StartIndex 開始，位址數爲 NumAssocDev。如果 RequestType 爲擴充回應但遠端設備沒有關聯設備，則 NumAssocDev 爲 0，其後的兩個參數省略；如果 RequestType 爲單設備回應，則包括 NumAssocDev 在內的後 3 個參數都省略。

3. Node_Desc_rsp 原語

Node_Desc_rsp 原語是遠端設備對 Node_Desc_req 請求原語的回應 該原語的語法如下：

ClusterID=0x82　Node_Desc_rsp（Status，NWKAddrOfInterest，NodeDiscriptor）

其中：參數 Status 表示 Node_Desc_req 命令的狀態，其值爲 SUCCESS 或 DEVICE_NOT_FOUND，目前 ZigBee 規範 1.0 只支援 SUCCESS 狀態；NWKAddrOfInterest 表示請求設備的 NWK 位址；NodeDiscriptor 是遠端設備的節點描述符。當遠端設備收到本地設備的 Node_Desc_req 請求原語後，產生狀態爲 SUCCESS 的 Node_Desc_rsp 響應原語，攜帶遠端設備節點描述符，發送給發起請求的本地設備。

4. Power_Desc_rsp 原語

Power_Desc_rsp 原語是遠端設備對 Power_Desc_req 請求原語的回應。該原語的語法如下：

ClusterID=0x83　Power_Desc_rsp（Status，NWKAddrOfInterest，PowerDiscriptor）

其中：參數 Status 表示 Power_Desc_req 命令的狀態，其值爲 SUCCESS 或 DEVICE_NOT_FOUND，目前 ZigBee 規範 1.0 只支援 SUCCESS 狀態；NWKAddrOfInterest 表示請求設備的 NWK 位址；PowerDiscriptor 是遠端設備的電源描述符。當遠端設備收到本地設備的 Power_Desc_req 請求原語後，產生狀態爲 SUCCESS 的 Power_Desc_rsp 響應原語，攜帶遠端設備電源描述符，發送給發起請求的本地設備。

5. Simple_Desc_rsp 原語

Simple_Desc_rsp 原語是遠端設備對 Simple_Desc_req 請求原語的回應。該原語的語法如下：

ClusterID=0x84　Simple_Desc_rsp（Status，NWKAddrOfInterest，Length，SimpleDiscriptor）

其中：參數 Status 表示 Simple_Desc_req 命令的狀態，其值爲 SUCCESS、INVALID_EP、NOT_ACTIVE 或 DEVICE_NOT_FOUND，目前 ZigBee 規範 1.0 不支援 DEVICE_NOT_FOUND 狀態；NWKAddrOfInterest 表示請求設備的 NWK 位址；Length 表示其後簡單描述符長度的位元組數；SimpleDiscriptor 是遠端設備的簡單描述符。遠端設備收到本地設備的 Simple_Desc_req 請求原語後，首先檢驗端點參數 endpoint 的取值是否有效，然後到遠端設備的活動端點簡單描述符列表中查找對應的簡單描述符。如果請求原語端點參數爲 0 或大於 240，遠端設備向本地設備發出狀態爲 INVALID_EP 的 Simple_Desc_rsp 回應，此時 SimpleDiscriptor 欄位爲空。如果請求原語的端點值有效，但遠端設備沒有該端點簡單描述符，則遠端設備向本地設備發出狀態爲 NOT_ACTIVE 的 Simple_Desc_rsp 回應，此時 SimpleDiscriptor 欄位也爲空。如果請求原語的端點值有效，且遠端設備有該端點簡單描述符，則遠端設備向本地設備發出狀態爲 SUCCESS 的 Simple_Desc_rsp 回應，並返回遠端設備指定端點的簡單描述符。

6. Active_Ep_rsp 原語

Active_Ep_rsp 原語是遠端設備對 Active_Ep_req 請求原語的回應。該原語的語法如下：

ClusterID=0x85　Active_Ep_rsp（Status，NWKAddrOfInterest，，ActiveEPCount，，ActiveEPList）

其中：參數 Status 表示 Active_Ep_req 命令的狀態，其值爲 SUCCESS 或 DEVICE_NOT_FOUND，目前 ZigBee 規範 1.0 不支援 DEVICE_NOT_FOUND 狀態；NWKAddrOfInterest 表示請求設備的 NWK 位址；ActiveEPCount 表示遠端設備活動端點數；ActiveEPList 是活動端點號的列表。收到本地設備的 Active_Ep_req 請求原語後，遠端設備檢測每個有效端點，找出其中支持了簡單描述符的端點即爲活動端點。遠端設備記錄活動端點數和端點號，向本地設備發出狀態爲 SUCCESS 的 Active_Ep_rsp 回應。

7. Match_Desc_rsp 原語

Match_Desc_rsp 原語是遠端設備對 Match_Desc_req 請求原語的回應。該原語的語法如下：

ClusterID=0x86　Match_Desc_rsp(Status，NWKAddrOfInterest，MatchLength，，MtchList）

其中：參數 Status 表示 Match_Desc_req 命令的狀態，其值爲 SUCCESS 或 DEVICE_NOT_FOUND，目前 ZigBee 規範 1.0 不支援 DEVICE_NOT_FOUND 狀態；NWKAddrOfInterest 表示請求設備的 NWK 位址；MatchLength 表示滿足匹配準則的遠端設備端點數；MatchList 是匹配端點號列表。收到本地設備的 Match_desc_req 請求原語後，遠端設備根據 Match_Desc_req 中的參數 Profile、InClusterList 或 OutClusterList 對每個端點進行匹配檢測。在 ProfileID 匹配的前提下，還要檢測 InClusterList 或 OutClusterList 中是否存在於遠端設備端點的簇標識匹配的元素。如果遠端設備沒有滿足匹配條件的端點，則對 Match_Desc_req 不作任何回應；如果遠端設備存在滿足匹配條件的端點，則向本地設備發出狀態爲 SUCCESS 的 Match_Desc_rsp 回應，並列出所有匹配的端點。

8. Complex_Desc_rsp 原語

Complex_Desc_rsp 原語是遠端設備對 Complex_Desc_req 請求原語的回應。該原語的語法如下：

ClusterID=0x90　　Complex_Desc_rsp（Status，NWKAddrOfInterest，Length，ComplexDiscriptor）

其中：參數 Status 表示 Complex_Desc_req 命令的狀態，其值爲 SUCCESS 或 NOT_SUPPORTED；NWKAddrOfInterest 是請求設備的 NWK 位址；Length 表示其後複雜描述符長度的位元組數；ComplexDiscriptor 是遠端設備的簡單描述符。如果 Status 參數值爲 NOT_SUPPORTED，則省略後兩個參數。收到 Complex_Desc_req 命令後，遠端設備首先判斷其自身是否支持複雜描述符。如果不支援複雜描述符，遠端設備將返回狀態爲 NOT_SUPPORTED 的 Complex_Desc_rsp 回應；如果支援複雜描述符，遠端設備則把複雜描述符承諾高度粗放在 Length 參數位置，把複雜描述符的內容存放在 ComplexDiscriptor 參數位置，並以狀態 SUCCESS 向本地設備發出 Complex_Desc_rsp 回應。

9. User_Desc_rsp 原語

User_Desc_rsp 原語是遠端設備對 User_Desc_req 請求原語的回應。該原語的語法如下：

ClusterID=0x91　　User_Desc_rsp（Status，，NWKAddrOfInterest，，Length，，UserDiscriptor）

其中：參數 Status 表示 User_Desc_req 命令的狀態，其值爲 SUCCESS 或 NOT_SUPPORTED；NWKAdderOfInterest 是請求設備的 NWK 位址；Length 表示其後使用者描述符長度的位元組數；UserDiscriptor 是遠端設備的使用者描述符。如果 Status 參數值爲 NOT_SUPPORTED，則省略後兩個參數。收到 User_Desc_req 命令後，遠端設備首先判斷其自身是否支持使用者描述符。如果不支援使用者描述符，遠端設備將返回狀態爲 NOT_SUPPORTED 的 User_Desc_rsp 回應；如果支援使用者描述符，遠端設備則把使用者描述符長度存放在 Length 參數位置，把使用者描述符的內容存放在 UserDiscriptor 參數位置，並以狀態 SUCCESS 向本地設備發出 User_Desc_rsp 回應。

10. Discovery_Register_rsp 原語

Discovery_Register_rsp 原語是遠端設備收到 Discovery_Register_req 命令後作出的回應。該原語的語法如下：

ClusterID=0x92　　Discovery_Register_rsp（Status）

其唯一參數 Status 表示 Discovery_Register_req 命令的狀態，其取值爲 SUCCESS 或 NOT_SUPPORTED。如果遠端設備支援發現註冊，則對 Discovery_Register_req 請求作出狀態爲 SUCCESS 的 Discovery_Register_rsp 回應；否則，回應狀態爲 NOT_SUPPORTED。目前 1.0 版本的 ZigBee 規範並不支援發現註冊。

11. User_Desc_conf 原語

User_Desc_conf 原語是遠端設備對 User_Desc_set 命令的回應，用以告知本地設備其請求配置遠端設備使用者描述符的結果。該原語的語法如下：

ClusterID=0x94　　User_Desc_conf（Status）

其唯一參數 Status 表示 User_Desc_set 命令的狀態，其取值爲 SUCCESS 或 NOT_SUPPORTED。如果遠端設備不支援 User_Desc_set 命令或不存在使用者描述符，則返回狀態爲 NOT_SUPPORTED 的 User_Desc_conf 回應；否則，遠端設備配置使用者描述符並返回狀態爲 SUCCESS 的回應。

1.4.3.2 綁定和解綁定伺服器服務

1. End_Device_Bind_rsp 原語

End_Device_Bind_rsp 原語是 ZigBee 協調器對 End_Device_Bind_req 命令的回應。該原語的語法如下：

ClusterID=0xA0　　End_Device_Bind_rsp（Status）

其唯一參數 Status 表示 End_Device_Bind_req 命令的狀態，取值爲 SUCCESS、NOT_SUPPORTED、TIMEOUT 或 NO_MATCH。如果 End_Device_Bind_req 命令指向的命令不是 ZigBee 協調器或 ZigBee 協調器不支持終端設備綁定，則遠端設備返回狀態爲 NOT_SUPPORTED 的 End_Device_Bind_rsp 回應。ZigBee 協調器接收到第一個 End_Device_Bind_req 時，儲存請求並啓動一個計時器，如果在預設的時限內沒有收到第二個 End_Device_Bind_req 則 ZigBee 協調器將返回狀態爲 TIMEOUT 的 End_Device_Bind_rsp 回應；如果 ZigBee 協調器在定時時限內收到第二個 End_Device_Bind_req，則比較兩個 End_Device_Bind_req，判斷它們的匹配性。如果 ProfileID 不匹配，或 ProfileID 匹配但 InClusterList 和 OutClusterList 中沒有匹配的元素，則 ZigBee 協調器將返回狀態爲 NO_MATCH 的 End_Device_Bind_rsp 回應。如果 ProfileID 匹配，且 InClusterList 或 OutClusterList 中存在匹配的簇標識，則 ZigBee 協調器將返回狀態爲 SUCCESS 的 End_Device_Bind_rsp 回應，並且 ZigBee 協調器向 OutClusterList 中元素匹配的本地設備的父設備發出 Bind_req 請求。

2. Bind_rsp 原語

Bind_rsp 原語是 Bind_req 命令的回應。該原語的語法如下：

ClusterID=0xA1　　Bind_rsp（Status）

其唯一參數 Status 表示 Bind_req 命令的狀態，取值爲 SUCCESS、NOT_SUPPORTED 或 TABLE_FULL。如果遠端設備處理了 Bind_req 並在綁定表中增加了相應的記錄，就返回狀態爲 SUCCESS 的 Bind_rsp；如果遠端設備不是 ZigBee 協調器或 SrcAddress 指定的設備，則返回狀態爲 NOT_SUPPORTED 的 Bind_rsp；如果遠端設備是 ZigBee 協調器或 SrcAddress 指定的設備，但沒有足夠的綁定表資源來處理綁定請求，則返回狀態爲 TABLE_FULL 的 Bind_rsp 回應原語。如果 Bind_rsp 的狀態爲 SUCCESS，則透過 APSME-BIND.request 原語把 Bind_req 的參數添加到綁定表中形成相應的綁定記錄。

3. Unbind_rsp 原語

Unbind_rsp 原語是 Unbind_req 命令的回應。該原語的語法如下：

ClusterID=0xA2　　Unbind_rsp（Status）

其唯一參數 Status 表示 Unbind_req 命令的狀態，取值爲 SUCCESS、NOT_SUPPORTED 或 NO_ENTRY。如果遠端設備處理了 Unbind_req 並在綁定表中刪除了相應的記錄，就返回狀態爲 SUCCESS 的 Unbind_rsp；如果遠端設備不是 ZigBee 協調器或 SrcAddress 指定的設備，則返回狀態爲 NOT_SUPPORTED 的 Unbind_rsp；如果遠端設備是 ZigBee 協調器或 SrcAddress 指定的設備，但綁定表中沒有請求解除的綁定記錄，則返回狀態爲 NO_ENTRY 的 Unbind_rsp 回應原語。如果 Unbind_rsp 的狀態爲 SUCCESS，則透過 APSME-UNBIND.request 原語從遠端設備綁定表中刪除 Unbind_req 參數指定的綁定記錄。

1.4.3.3 網路管理伺服器服務

1. Mgmt_NWK_Disc_rsp 原語

Mgmt_NWK_Disc_rsp 原語是 Mgmt_NWK_Disc_req 命令的回應，用以向本地設備報告網路發現請求的結果。該原語的語法如下：

ClusterID=0xB0　　Mgmt_NWK_Disc_rsp（Status，NerworkCount，StartIndex，NetworkListCount，NetWorkList）

其中：參數 Status 表示 Mgmt_NWK_Disc_req 命令的狀態，其取值爲 NOT_SUPPORTED 或 NLME-NETWORK-DISCOVERY.confirm 返回的狀態；參數 NetworkCount 表示 NLME-NETWORK-DISCOVERY.confirm 報告的網路總數；參數 StartIndex 表示該回應報告的網路發現結果在 NLME-NETWORK-DISCOVERY.confirm 的 NetWorkList 中的起始索引；NetworkListCount 表示該回應報告的網路描述符的個數；NetWorkList 表示該回應報告的 NetworkListCount 個網路描述符構成的列表，該網路列表從 NLME-NETWORK-DISCOVERY.confirm 的 NetWorkList 中的第 StartIndex 個元素開始。如果遠端設備不支援 Mgmt_NWK_Disc_req 管理命令，則 Mgmt_NWK_Disc_rsp 的狀態爲 NOT_SUPPORTED 並省略其後的其他參數欄位；如果遠端設備支援 Mgmt_NWK_Disc_req 管理命令，則根據 Mgmt_NWK_Disc_req 提供的 ScanChannels 參數執行網路發現請求 NLME-NETWORK-DISCOVERY.request，在收到 NLME-NETWORK-DISCOVERY.confirm 後，透過 Mgmt_NWK_Disc_rsp 向本地設備報告網路發現的結果。Mgmt_NWK_Disc_rsp 中參數 NetworkCount 的值與 NLME-NETWORK-DISCOVERY.confirm 中參數 NetworkCount 的值相同；Mgmt_NWK_Disc_rsp 的 NetWorkList 從 NLME-NETWORK-DISCOVERY.confirm 參數 NetWorkList 的第 StartIndex 個元素開始，盡可能多地報告發現的網路，只要保證 MSDU 不超過 aMaxMACFrameSize 個位元組。

2. Mgmt_Lqi_rsp 原語

Mgmt_Lqi_rsp 原語是 Mgmt_Lqi_req 命令的回應，用以向本地設備報告遠端設備鄰居表請求的結果。該原語的語法如下：

ClusterID=0xB1　　Mgmt_Lqi_rsp（Status，NeighborTableEntries，StartIndex，NeighborTableListCount，NeighborTableList）

其中：參數 Status 表示 Mgmt_Lqi_req 命令的狀態，其取值爲 NOT_SUPPORTED 或 NLME-GET.confirm 原語返回的狀態；參數 NeighborTableEntries 表示遠端設備鄰居表的記錄總數；StarIndex 表示 Mgmt_Lqi_rsp 報告的 NeighborTableList 在遠端設備鄰居表中的起始索引；NeighborTableListCount 表示遠端設備報告的鄰居列表 NeighborTableList 中包含的鄰居數；NeighborTableList 是遠端設備報告的鄰居描述符列表，它是從鄰居表的第 StartIndex 個記錄記錄開始的連續 NeighborTableListCount 個鄰居描述符。鄰居描述符中包括設備位址及相關 LQI 等，其具體參數如表 8 所列。如果遠端設備不支援 Mgmt_Lqi_req 管理命令，則 Mgmt_Lqi_rsp 的狀態爲 NOT_SUPPORTED 並省略其後的其他參數；如果遠端設備支援 Mgmt_Lqi_req 管理命令，則遠端設備將執行 NLME-GET.request 原語來獲取 nwkNeighborTable 屬性並據此產生 Mgmt_Lqi_rsp 命令。如果成功獲取 nwkNeighborTable 但不支援 NeighborTableList 記錄的一個或多個欄位，則 Mgmt_Lqi_rsp 返回的狀態爲 NOT_SUPPORTED 並省略 Status 之後的其他參數；否則，Mgmt_Lqi_rsp 的狀態與 NLME-GET.confirm 原語返回的狀態相同，如果該狀態不是 SUCCESS，則 Status 之後的其他參數都將被省略。如果遠端設備成功獲取 nwkNeighborTable 屬性並支援 NeighborTableList 記錄的各個欄位，則從第 StartIndex 個索引開始，把 nwkNeighborTable 中的鄰居描述符複製到 Mgmt_Lqi_rsp 命令的 NeighborTableList 欄位。Mgmt_Lqi_rsp 命令應在 MSDU 長度限制 aMaxMACFrameSize 的範圍內盡最大可能報告鄰居表。

表 8 鄰居表記錄的格式

名稱	類型	有效範圍	描述

PAN Id	整數	0x0000～0x3fff	鄰居設備的 16 位元 PAN 標識
Extended address	整數	擴充 64 位 IEEE 位址	每個設備唯一的 64 位元 IEEE 位址
Network address	網路位址	網路位址	鄰居設備的 16 位元網路位址
Device type	整數	0x00～0x03	鄰居設備的類型：0x00=ZigBee 協調器；0x01=ZigBee 路由器；0x02=ZigBee 終端設備
RxOnWhenIdle	布林量	TRUE 或 FALSE	指明在 CAP 的空閒期間，鄰居設備的接收機是否致能：TRUE=接收機開啓；FALSE=接收機關閉
Relationship	關係	0x00～0x03	鄰居與當前設備之間的關係：0x00=鄰居是當前設備的父設備；0x01=鄰居是當前設備的子設備；0x02=鄰居是當前設備的兄弟設備；0x03=非以上任何一種關係
Depth	整數	0x00～nwkcMaxDepth	鄰居設備的樹深度。數值 0x00 指明，該設備是用於網路的 ZigBee 協調器
Permit joining	布林量	TRUE 或 FALSE	指明鄰居設備是否接收入網請求：TRUE=鄰居設備接受入網請求；FALSE=鄰居設備俄不接受入網請求
LQI	整數	0x00～0xff	從本設備 RF 發送估計得到的鏈路品質

3. Mgmt_Rtg_rsp 原語

Mgmt_Rtg_rsp 原語是 Mgmt_Rtg_req 命令的回應，用以向本地設備報告請求遠端設備路由表的結果。該原語的語法如下：

ClusterID=0xB2　　Mgmt_Rtg_rsp（Status，RoutingTableEntries，StartIndex，RoutingTableListCount，RoutingTableList）

其中：參數 Status 表示 Mgmt_Rtg_req 命令的狀態，其取值爲 NOT_SUPPORTED 或 NLME-GET.confirm 原語返回的狀態；參數 RoutingTableEntries 表示遠端設備路由表的記錄總數；StartIndex 表示 Mgmt_Rtg_rsp 報告的 RoutingTableList 在遠端設備路由表中的起始索引；RoutingTableListCount 表示遠端設備報告的路由列表 RoutingTableList 中包含的路由數；RoutingTableList 是遠端設備報告的路由記錄列表，它是由路由表的第 StartIndex 個記錄開始的連續|RoutingTableListCount 個路由。路由記錄包含的參數如表 9 所列。如果遠端設備不支援 Mgmt_Rtg_req 管理命令，則 Mgmt_Rtg_rsp 返回狀態爲 NOT_SUPPORTED 並省略其後的其他參數；如果遠端設備支援 Mgmt_Rtg_req 管理命令，則遠端設備將執行 NLME-GET.request 原語來獲取 nwkRouteTable 屬性並據此產生 Mgmt_Rtg_rsp 命令。Mgmt_Rtg_rsp 的狀態與 NLME-GET.confirmed 原語返回的狀態相同，如果該狀態不是 SUCCESS，則 Status 之後的其他參數都將被省略。如果成功獲取路由表屬性，遠端設備就從 nwkRouteTable 的第 StartIndex 個索引開始，把完整的路由記錄複製到 Mgmt_Rtg_rsp 命令的 RoutingTableList 欄位。Mgmt_Rtg_rsp 命令應在 MSDU 長度限制 aMaxMAXFrameSize 的範圍內盡最大可能報告路由表。

表 9 路由表記錄的格式

名稱	類型	有效範圍	描述
目的位址	2 位元組	本路由的 16 位網路位址	目的位址

狀態	3 位	路由狀態	0x0=活動 0x1=DISCOVERY_UNDERWAY 0x2=DISCOVERY_FAILED 0x3=不活動 0x4～0x7=預留
下一跳位址	2 位元組	通往目的位址的下一跳 16 位網路位址	下一跳位址

4. Mgmt_Bind_rsp 原語

Mgmt_Bind_rsp 原語是 Mgmt_Bind_req 命令的回應，用以向本地設備報告請求遠端設備綁定表的結果。該原語的語法如下：

ClusterID=0xB3　　Mgmt_Bind_rsp（Status，BindingTableEntries，StartIndex，BindingTableListCount，BindingTableList）

其中：參數 Status 表示 Mgmt_Bind_req 命令的狀態，其取值爲 NOT_SUPPORTED 或 APSME-GET.confirm 原語返回的狀態；參數 BindingTableEntries 表示遠端設備綁定表的記錄總數；StartIndex 表示 Mgmt_Bind_rsp 報告的 BindingTableList 在遠端設備綁定表中的起始索引；BindingTableListCount 表示遠端設備報告的綁定列表 BindingTableList 中包含的綁定表記錄數；BindingTableList 是遠端設備報告的綁定記錄列表，它是從綁定表的第 StartIndex 個記錄開始的連續 BindingTableListCount 個綁定記錄。綁定記錄包含的參數如表 10 所列。如果遠端設備不支援 Mgmt_Bind_req 管理命令，則 Mgmt_Bind_rsp 返回狀態爲 NOT_SUPPORTED 並省略其後的其他參數；如果遠端設備支援 Mgmt_Bind_req 管理命令，則遠端設備將執行 APSME-GET.request 原語來獲取 apsBindingTable 屬性並據此產生 Mgmt_Bind_rsp 命令。Mgmt_Bind_rsp 的狀態與 APSME-GET.confirm 原語返回的狀態相同，如果該狀態不是 SUCCESS，則 Status 之後的其他參數都將被省略。如果成功獲取綁定表，遠端設備就從 apsBindingTable 的第 StartIndex 個索引開始，把完整的綁定記錄複製到 Mgmt_Bind_rsp 命令的 BindingTableList 欄位。Mgmt_Bind_rsp 命令應在 MSDU 長度限制 aMaxMACFrameSize 的範圍內盡最大可能報告綁定表。

表 10 綁定記錄表的格式

名稱	類型	有效範圍	描述
SrcAddr	IEEE 位址	有效 64 位 IEEE 位址	綁定記錄的源 IEEE 位址
SrcEndpoint	整數	0x01～0xff	綁定記錄的源端點
ClusterId	整數	0x00～0xff	與目標設備綁定的源設備上的簇標識
DstAddr	IEEE 位址	有效 64 位 IEEE 位址	綁定記錄的目的 IEEE 位址
DstEndpoint	整數	0x01～0xff	綁定記錄的目的端點

5. Mgmt_Leave_rsp 原語

Mgmt_Leave_rsp 原語是 Mgmt_Leave_req 命令的回應，用以向本地設備報告其試圖使遠端設備離開網路的結果。該原語的語法如下：

ClusterID=0xB4　　Mgmt_Leave_rsp（Status）

其唯一參數 Status 表示 Mgmt_Leave_req 命令的狀態，其取值爲 NOT_SUPPORTED 或

NLME-LEAVE.confirm 原語返回的狀態。如果遠端設備不支援 Mgmt_Leave_req 命令，則 Mgmt_Leave_rsp 返回狀態爲 NOT_SUPPORTED；如果遠端設備支援 Mgmt_Leave_req 命令，則執行 NLME-LEAVE.request 原語與當前所處的網路解關聯。Mgmt_Leave_rsp 的狀態與 NLME-LEAVE.confirm 原語返回的狀態一致。一旦設備解關聯，它將按照預編程的邏輯執行 NLME-NETWORK-DISCOVERY 和 NLME-JOIN 原語，試圖重新加入一個網路。

6. Mgmt_Direct_Join_rsp 原語

Mgmt_Direct_Join_rsp 原語是 Mgmt_Direct_Join_req 命令的回應。該原語的語法如下：

ClusterID=0xB5　　Mgmt_Direct_Join_rsp（Status）

其唯一參數 Status 表示 Mgmt_Direct_Join_req 命令的狀態，其取值爲 NOT_SUPPORTED 或 NLME-DIRECT-JOIN.confirm 原語返回的狀態。如果遠端設備不支援 Mgmt_Direct_Join_req 命令，則 Mgmt_Direct_Join_rsp 返回狀態爲 NOT_SUPPORTED；如果遠端設備支援 Mgmt_Direct_Join_req 命令，則遠端設備執行 NLME-DIRECT-JOIN.request 原語，直接把 Mgmt_Direct_Join_req 命令中 DeviceAddress 參數指定的設備關聯到網路。Mgmt_Direct_Join_rsp 的狀態與 NLME-DIRECT-JOIN.confirm 原語返回的狀態一致。

1.5 ZigBee 設備物件（ZDO）

1.5.1 設備物件描述

ZigBee 設備物件（ZDO）是駐留于應用層（APL）的一種應用解決方案，它位於 ZigBee 協定棧的應用支援子層（APS）之上。ZDO 負責初始化應用，支援子層（APS）、網路層（NWK）、安全服務提供模組（SSP）及非 1～240 端點應用的任何其他 ZigBee 設備層；另外 ZDO 還負責從終端應用收集配置資訊來實現設備和服務發現、安全管理、網路管理、綁定管理和節點管理功能。

設備和服務發現功能應支援在單個 PAN 內的設備和服務發現。對 ZigBee 協調器、ZigBee 路由器和 ZigBee 終端設備三種不同類型的設備，發現功能分別執行不同的操作。對於要進入休眠狀態的 ZigBee 終端設備，設備和服務發現應設法把 NWK 位址、IEEE 位址、活動端點、簡單描述符、節點描述符和電源描述符上載並保存到關聯的 ZigBee 協調器或 ZigBee 路由器，以允許對這些休眠設備執行設備和服務操作。對 ZigBee 協調器和 ZigBee 路由器，設備和服務發現應代表其關聯的休眠 ZigBee 終端設備對發現請求作出回應。對所有類型的 ZigBee 設備，設備和服務發現應支援其他設備的設備和服務發現請求並允許本地應用對象產生發現請求。在設備發現中，如果單播查詢 ZigBee 協調器或 ZigBee 路由器的 IEEE 位址，則被查詢設備應返回其 IEEE 位址，並可選同時返回其關聯設備的 NWK 位址；如果單播查詢 ZigBee 終端設備的 IEEE 位址，則被查詢設備返回 IEEE 位址；如果根據指定的 IEEE 位址廣播查詢 ZigBee 協調器或 ZigBee 路由器的 NWK 位址，則被查詢設備返回其 NWK 位址並可選同時返回其關聯設備的 NWK 位址；如果根據指定的 IEEE 位址廣播查詢 ZigBee 終端設備的 NWK 位址，則被查詢設備應返回其 NWK 位址，回應設備採用單播回應的 APS 確認服務對廣播查詢作出回應。在服務發現中，根據不同的請求輸入類型，服務發現功能作出不同的回應。對 NWK 位址及活動端點查詢類型，指定設備應返回所有應用駐留的端點號。對 NWK 位址或廣播位址及包含配置檔 ID、輸入和輸出簇的服務匹配查詢類型，指定設備先判斷所有活動端點與配置檔 ID 是否匹配；如果沒有沒有輸入輸出簇，則與請求的配置檔

ID 匹配的端點都被返回；如果請求中提供了輸入和/或輸出簇，則還要判斷輸入輸出簇是否匹配，並在回應中以端點列表的形式把匹配的端點返回給請求設備。回應設備應使用單播回應的 APS 確認服務對廣播查詢作出回應。對 NWK 位址及節點描述符或電源描述符查詢類型，指定設備應返回節點描述符或電源描述符。對 NWK 位址、端點號及簡單描述符查詢類型，指定位址應返回設備對應端點的簡單描述符。另外，對可選的 NWK 位址及複雜或使用者描述符查詢類型，如果設備支援該請求類型則指定設備應返回複雜描述符或使用者描述符。

安全管理功能決定是否採用安全機制。如果採用安全機制，則應建立密鑰、傳遞密鑰和認證。安全管理由 ZDO 調用 APSME 原語執行以下操作來實現。首先，設備聯繫位於 ZigBee 協調器的信用中心獲取該設備與信用中心之間的主密鑰。這一步使用 APSME-Key 原語，如果設備本身就是 ZigBee 協調器或預先配置了設備與信用中心之間的主密鑰，則可以省略這一步。其次設備要建立與信用中心之間的鏈路密鑰，這一步使用 APSME-Establish-Key 原語。然後設備透過與信用中心之間的安全通訊來獲取 NWK 密鑰，這一步使用 APSME-Transport-Key 原語。如果需要，則可以爲網路中的訊息目的設備建立鏈路密鑰和主密鑰，這一步使用 APSME-Key 和 APSME-Establish-Key 原語。如果設備是 ZigBee 路由器，則使用 APSME-Device-Update 原語把加入網路的設備通知給信用中心。

網路管理功能透過編程應用或在安裝過程中對 ZigBee 協調器、ZigBee 路由器或 ZigBee 終端設備的邏輯設備類型進行配置。如果設備類型是 ZigBee 路由器或 ZigBee 終端設備，網路管理功能應爲設備提供選擇現存 PAN 並加入網路的能力，和在網路通訊中斷後允許設備重新關聯到同一 ZigBee 協調器或 ZigBee 路由器的能力；如果設備類型是 ZigBee 協調器或 ZigBee 路由器，網路管理功能應爲設備提供選擇空閒通道建立新 PAN 的能力。網路管理主要涉及以下內容：配置網路掃描過程中的通道列表；管理網路掃描過程來發現鄰近網路及其 ZigBee 協調器和路由器標識；允許 ZigBee 協調器選擇通道建立新網路和 ZigBee 路由器或 ZigBee 終端設備加入一個現存網路；支援孤立設備重新加入網路；支援直接加入網路和透過網路層代理加入網路；還可能支援允許外部網路管理的管理實體。

綁定管理功能包括下面這些內容：一是建立綁定表資源空間，資源空間的大小由定制的應用來決定或由安裝過程中的配置參數來設定；二是處理增加或刪除 APS 綁定表記錄的綁定請求；三是支援來自外部應用的綁定和解綁定命令以支持輔助綁定，綁定和解綁定命令透過 ZigBee 設備配置檔來支援；四是對於 ZigBee 協調器，支持終端設備綁定。終端設備綁定是在按鈕或其他手動方式基礎上的綁定。

對於 ZigBee 協調器和 ZigBee 路由器，節點管理功能允許遠端管理命令執行網路發現；提供遠端管理命令去檢索路由表；提供遠端管理命令去檢索綁定表；提供遠端管理命令去使遠端設備離開網路或指令另一個設備離開網路；提供遠端管理命令去獲取遠端設備與其近鄰之間的 LQI。

1.5.2 層介面描述

與端點 1～240 上應用的設備描述符不同，ZDO 除透過 APSDE-SAP 與 APS 介面外，還透過 APSME-SAP 與 APS 層介面，透過 NLME-SAP 與 NWK 層介面。與其他端點上的應用一樣，ZDO 在端點 0 上透過配置檔使用 APSDE-SAP 通訊。ZDO 使用的配置檔是 ZigBee 設備配置檔。

1.5.3 物件定義和行爲

1.5.3.1 物件概述

ZDO 包括下面五種對象：設備和服務發現、網路管理、綁定管理、安全管理、節點管理。顧名思義，設備和服務發現物件是完成設備發現和服務發現功能。網路管理物件是處理網路活動，如網路發現、設備加入/離開網路、建立網路、重定網路連接等。綁定管理物件處理終端設備綁定、綁定和解綁定。安全管理物件處理安全服務，如密鑰載入、密鑰建立、密鑰傳遞、認證等。節點管理物件承擔節點管理功能，其中設備和服務發現、網路管理是所有類型的 ZigBee 設備都要強制支援的物件，而其他三個物件則是可選支援的。ZDO 的 ZigBee 設備配置檔原語在產生包時可採用安全機制，這些在 APSDE 端點 0 上產生的應用包除了使用各自的鏈路密鑰外還要使用網路密鑰。設備中任何端點應用都可以存取的方法稱作“公用方法”，而那些只允許端點 0 上的應用存取的方法稱作“私有方法”。對不同邏輯類型的設備在不同的狀態下其功能表現有所不同。

1.5.3.2 狀態機功能描述

1. ZigBee 協調器

ZigBee 協調器初始化時，需要向 ZDO 網路管理物件提供一套網路配置參數：Config_NWK_Mode_and_Params；另外還要提供活動端點列表以及描述各活動端點和應用的節點描述符、電源描述符、簡單描述符時所需的配置元素，這些配置元素包含在配置屬性：Config_Node_Descriptor、：Config_Power_Descriptor 和：Config_Simple_Descriptor 中。在設備支援的情況下，還應提供複雜描述符和使用者描述符的配置元素資訊、綁定記錄最大數和主密鑰，這些配置資訊包含在配置屬性：Config_Complex_Descriptor、：Config_User_Descriptor、：Config_Max_Bind 和：Config_Master_Key 中。設備應用使用 NLME-NETWORK-DISCOVERY.request 原語對：Config_NWK_Mode_and_Params 屬性中 ChannelList 指定的通道進行掃描，掃描結果透過 NLME-NETWORK-DISCOVERY.confirm 原語中的 NetworkList 參數列出設備工作範圍記憶體在的活動 PAN。設備應用把 ChannelList 與 NetworkLIst 進行比較，選擇空閒通道。一旦確定了空閒通道，設備應用將根據配置屬性的值設置 NIB 屬性 nwkSecurityLevel 和 nwkSecureAllFrames。然後，設備應用將使用 NLME-NETWORK-FORMATION.request 原語，依據：Config_NWK_Mode_and_Params 屬性中的相關參數，在選定的空閒通道上建立一個新的 PAN。設備應用透過 NLME-NETWORK-FORMATION.confirm 原語返回的狀態判斷 PAN 建立是否成功。另外，設備還將根據 NLME-PERMIT-JOINING.request 提供的預設參數值設置屬性：Confit_Permit_Join_Duration，並分別根據：Config_NWK_BroadcastDeliveryTime 和：Config_NWK_TransactionPersistenceTime 設置網路資訊參數 nwkNetworkBroadcastDeliveryTime 和 nwkTransactionPersistenceTime。在 ZDO 完成初始化轉入正常工作狀態之前，應保證端點 1～240 調用 APS 原語能返回合適的錯誤狀態。

在正常工作狀態時，ZigBee 協調器應在滿足配置屬性：Config_Permit_Join_Duration 和：Config_Max_Assoc 的前提下允許其他設備加入網路。當一個新設備加入網路時，設備應用

透過 NLME-JOIN.indication 原語獲知新入網設備的資訊。ZigBee 協調器能夠對指向其本身的或其關聯休眠設備的設備發現或服務發現請求作出回應。ZigBee 協調器應支持 NLME-PERMIT-JOINING.request 和 NLME-PERMIT-JOINING.confirm，以便對設備俄加入網路的過程進行應用控制。ZigBee 協調器還應支持 NLME-LEAVE.request 和 NLME-LEAVE.confirm，以便對關聯設備離開網路的行爲進行應用控制。ZigBee 協調器應維護一個關聯設備列表，以便孤立設備重新加入網路。該列表中包含的設備在孤立後要重新加入網路時，透過 ZigBee 協調器支持的 NLME-DIRECT-JOIN.request 和 NLME-DIRECT-JOIN.confirm 直接加入網路，而不需要執行關聯過程。ZigBee 協調器應處理來自 ZigBee 路由器和 ZigBee 終端設備的 End_Device_Bind_req，並作出回應 End_Device_Bind_rsp。ZigBee 協調器要處理來自 ZigBee 終端設備的 End_Device_annce 訊息。

當網路中使用安全機制時，ZigBee 協調器還要承擔信用中心的任務。新加入網路的設備透過 APSME-DEVICE-UPDATE.indication 原語通知信用中心，信用中心根據網路存取控制策略決定一個設備在網路中的去留。信用中心要求設備離開網路時，使用 APSME-REMOVE-DEVICE.req 原語。信用中心允許一個設備繼續留在網路中時，就是用 APSME-TRANSPORT-KEY.熱情爲設備建立一個主密鑰。建立主密鑰後，信用中心使用 APSME-ESTABLISH-KEY.req 爲設備建立一個鏈路密鑰。然後，信用中心還要使用 APSME-TRANSPORT-KEY.req 爲設備提供一個 NWK 密鑰。透過提供共同的主密鑰，信用中心可以在任何兩個設備之間建立鏈路密鑰。信用中心應按照一定的策略週期性地更新 NWK 密鑰，網路中的所有設備使用 APSME-TRANSPORT-KEY.req 來更新 NWK 密鑰。

2. ZigBee 路由器

ZigBee 路由器初始化時，需要向 ZDO 網路管理物件提供一套網路配置參數：Config_NWK_Mode_and_Params；在設備支援的情況下，還應提供複雜描述符和使用者描述符的配置元素資訊、綁定記錄最大數和主密鑰，這些配置資訊包含在配置屬性：Config_Complex_Descriptor 、： Config_User_Descriptor 、： Config_Max_Bind 和 ： Config_Master_Key 中。設備應使用 NLME-NETWORK-DISCOVERY.request 原語對：Config_NEK_Mode_and_Params 屬性中 ChannelList 指定的通道進行掃描，掃描結果透過 NLME-NETWORK-DISCOVERY.confirm 原語中的 NetworkList 參數列出設備工作範圍記憶體在的活動 PAN。設備將執行 NLME-NETWORK-DISCOVERY.request 過程：Config_NWK_Scan_Attempts 次，每次持續時間爲：Config_NWK_Time_btwn_Scans。重複執行網路發現請求的目的是爲 NWK 層提供更精確的近鄰列表和相關鏈路品質指示。設備應用將比較 ChannelList 和 NetworkList，選擇一個想加入的現存網路。一旦確定了要加入的 PAN，設備應用將使用 NLME-JOIN.request 來加入該網路並透過檢查 NLME-JOIN.confirm 返回的狀態確定設備在 PAN 中關聯的 ZigBee 路由器或 ZigBee 協調器。能夠成爲路由器的設備應支援 NLME-START-ROUTER.request 和 NLME-START-ROUTER.confirm，以使得它能夠在加入的 PAN 中以 ZigBee 協調器的身份開始工作。另外，設備還將根據 NLME-PERMIT-JOINING.request 提供的預設參數值設置屬性：Config_Permit_Join_Duration，並分別根據：Config_NWK_BroadcastDeliveryTime 和：Config_NWK_TransactionPersistenceTime 設置網路資訊參數 nwkNetworkBroadcastDeliveryTime 和 nwkTransactionPersistenceTime。在 ZDO 完成初始化轉入正常工作狀態之前，應保證端點 1～240APS 原語調用能返回合適的錯誤狀態。如果網路中採用了安全機制，設備應等待信用中心透過 APSME-TRANSPORT-KEY.ind 提供一個主密鑰；然後用 APSME-ESTABLISH-KEY.rsp 回應信用中心的請求，建立一個鏈路密鑰；最後設備還要等待信用中心透過 APSME-TRANSPORT-KEY.ind 提供一個 NWK 密鑰。在成功獲

得 NWK 密鑰後，設備就透過了認證，設備應用吧 NIB 屬性 nwkSecurityLevel 和 nwkSecurreAllFrames 設置爲網路中使用的值，使用 NLME-START-ROUTER.request 就可以開始在網路中承擔 ZigBee 路由器的工作了。

在正常工作狀態下，ZigBee 路由器應在滿足配置屬性：Config_Permit_Join_Duration 和：Config_Max_Assoc 的前提下允許其他設備加入網路。當一個新設備加入網路時，設備應用透過 NLME-JOIN.indication 屬性獲知新加入網路的設備情況。如果允許設備加入 PAN，ZigBee 路由器應使用狀態爲 SUCCESS 的 NLME-JOIN.confirm 原語來指示設備成功加入網路。如果網路中採用了安全機制，設備應用將透過 APSME-DEVICE-UPDATE.req 吧新加入的設備通知給信用中心。ZigBee 路由器能夠對指向其本身的或其關聯休眠設備的設備發現或服務發現請求作出回應。ZigBee 路由器的應用也要保證綁定記錄數不超過：Config_Max_Bind 屬性值。如果支持安全機制，ZigBee 路由器應支持：Config_Master_Key 配置屬性並在鏈路密鑰建立過程中使用主密鑰。如果遠端目的位址要與 ZigBee 路由器進行安全通訊，ZigBee 路由器應支持 APSME-KEY.req 以便於遠端設備建立主密鑰，還應支持 APSME-ESTABLISH-KEY.request 、 APSME-ESTABLISH-KEY.confirm 和 APSME-ESTABLISH-KEY.response 以完成鏈路密鑰的建立過程。ZigBee 路由器應具備儲存、添加、刪除已知目的設備鏈路密鑰的能力。ZigBee 路由器應支持 APSME-TRANSPORT-KEY.ind 以從信用中心接收密鑰，應透過 APSME-KEY.req 請求信用中心更新 NWK 密鑰。ZigBee 路由器應支持 NLME-PERMIT-JOINING.request 和 NLME-PERMIT-JOINING.confirm，以允許對設備加入網路的過程進行應用控制。ZigBee 路由器還應支持 NLME-LEAVE.request 和 NLME-LEAVE.confirm，以便對關聯設備離開網路的行爲進行應用控制。ZigBee 路由器應維護一個當前關聯設備列表，以便孤立設備重新加入網路。

3. ZigBee 終端設備

終端設備初始化時，需要向 ZDO 網路管理物件提供一套網路配置參數：Config_NWK_Mode_and_Params；在設備支援的情況下，還應提供複雜描述符和使用者描述符的配置元素資訊、綁定記錄最大數和主密鑰，這些配置資訊包含在配置屬性：Config_Complex_Descriptor 、： Config_User_Descriptor 、： Config_Max_Bind 和 ： Config_Master_Key 中。設備應用使用 NLME-NETWORK-DISCOVERY.request 原語對：Config_NWK_Mode_and_Params 屬性中 ChannelList 指定的通道進行掃描，掃描結果透過 NLME-NETWORK-DISCOVERY.confirm 原語中的 NetworkList 參數列出設備工作範圍記憶體在的活動 PAN。設備將執行 NLME-NETWORK-DISCOVERY.request 過程：Config_NWK_Scan_Attempts 次，每次持續時間爲：Config_NWK_Time_btwn_Scans。重複執行網路發現請求的目的是爲 NWK 層提供更精確的近鄰列表和相關鏈路品質指示。設備應用將比較 ChannelList 和 NetworkList，選擇一個想加入的現存網路。一旦確定了要加入的 PAN，設備應用將使用 NLME-JOIN.request 來加入該網路並透過檢驗 NLME-JOIN.confirm 返回的狀態確定設備在 PAN 中關聯的 ZigBee 路由器或 ZigBee 協調器。終端設備成功加入網路後將發送 End_Device_annce 命令來廣播 64 位 IEEE 位址和 16 位 NWK 位址。如果網路採用了安全機制，終端設備將等待信用中心透過 APSME-TRANSPORT-KEY.ind 提供一個主密鑰；然後用 APSME-ESTABLISH-KEY.rsp 回應信用中心的請求，建立一個鏈路密鑰；最後設備還要等待信用中心透過 APSME-TRANSPORT-KEY.ind 提供一個 NWK 密鑰。在成功獲得 NEK 密鑰後，設備就加入了網路並透過認證。

在正常工作狀態下，ZigBee 終端設備應能回應任何設備發現或服務發現請求。如果遠端目的位址要與 ZigBee 終端設備進行安全通訊，ZigBee 終端設備應支持 APSME-KEY.req

以便與遠端設備建立主密鑰，還應支持 APSME-ESTABLISH-KEY.request、APSME-ESTABLISH-KEY.confirm 和 APSME-ESTABLISH-KEY.response 以完成鏈路密鑰的建立過程。ZigBee 路由器應具備儲存、添加、刪除已知目的設備鏈路密鑰的能力。ZigBee 終端設備應支持 APSME-TRANSPORT-KEY.ind 以從信用中心接收密鑰，應透過 APSME-KEY.req 請求信用中心更新 NWK 密鑰。

1.5.3.3 設備和服務發現

設備管理使用 ZigBee 設備配置檔執行設備發現和服務發現功能。表 11 中列出了設備和服務發現物件的全部屬性，其中所有請求屬性是各種邏輯類型的 ZigBee 設備可選支援的，部分回應屬性是各種邏輯類型的 ZigBee 設備強制支援的，另有部分回應屬性是可選支援的。

表 11 設備和服務發現的屬性

屬　　性	M/O	類型	屬　　性	M/O	類型
NWK_addr_req	O	公共	Match_Desc_req	O	公共
NWK_addr_rsp	M	公共	Match_Desc_rsp	M	公共
IEEE_addr_req	O	公共	Complex_Desc_req	O	公共
IEEE_addr_rsp	M	公共	Complex_Desc_rsp	O	公共
Node_Desc_req	O	公共	User_Desc_req	O	公共
Node_Desc_rsp	M	公共	User_Desc_rsp	O	公共
Power_Desc_req	O	公共	Discovery_Register_req	O	公共
Power_Desc_rsp	M	公共	Discovery_Register_rsp	O	公共
Simple_Desc_req	O	公共	End_Device_annce	O	公共
Simple_Desc_rsp	M	公共	End_Device_annce_rsp	O	公共
Active_EP_req	O	公共	User_Desc_set	O	公共
Active_EP_rsp	M	公共	User_Desc_conf	O	公共

注：M—強制，O—可選。

1.5.3.4 安全管理器

安全管理物件決定網路是否採用安全機制，安全管理執行建立密鑰、傳遞密鑰和認證的功能。安全管理物件本身是各種邏輯類型 ZigBee 設備的可選支援物件。如果設備支援安全管理物件，則該物件中的所有請求和回應屬性是各種類型設備都要強制支援的；如果設備不支援安全管理物件，則該物件包含的任何屬性都不會出現在設備中。安全管理物件的各種屬性如表 12 所列。

表 12 安全管理屬性

屬　　性	M/O	類型
APSME-ESTABLISH-KEY.request	M	公共
APSME-ESTABLISH-KEY.response	M	公共
APSME-TRANSPORTKEY.request	M	公共

APSME-TRANSPORTKEY.response	M	公共
APSME-AUTHENTICATE.request	M	公共
APSME-AUTHENTICATE.response	M	公共
APSME-DEVICEUPDATE.request	M	私有
APSME-REMOVEDEVICE.request	M	私有
APSME-KEY.request	M	私有

1.5.3.5 綁定管理器

綁定管理功能支援終端設備綁定、綁定和解綁定。當綁定指示到達 ZigBee 協調器或路由器時，綁定管理使用 ZigBee 設備配置檔和 APSME-SAP 原語實現該功能。綁定管理也是各種邏輯類型的 ZigBee 設備的可選物件。如果設備支援綁定管理對性，則該物件的全部請求屬性都是各種邏輯類型設備可選支援的，同時，ZigBee 協調器或 ZigBee 路由器和綁定表記錄源位址對應的 ZigBee 終端設備應支援相關的回應屬性；如果設備不支援綁定管理物件，則各種邏輯類型的 ZigBee 設備都不支援該物件中的任何屬性。綁定管理物件屬性如表 13 所列。

表 13 綁定管理屬性

屬　　性	M/O	類型
End_Device_Bind_req	O	公共
End_Device_Bind_rsp	O	公共
Bind_req	O	公共
Bind_rsp	O	公共
Unbind_req	O	公共
Unbind_rsp	O	公共
APSME-BIND.request	O	私有
APSME-BIND.confirm	O	私有
APSME-UNBIND.request	O	私有
APSME-UNBIND.confirm	O	私有

1.5.3.6 網路管理器

網路管理功能支援網路發現、網路構建、允許/禁止關聯、關聯和解關聯、路由發現、網路重定、無線接收機狀態致能/禁止、讀取和設置網路管理資訊庫資料。網路管理物件使用 NLME-SAP 原語來完成這些管理功能。網路管理是各種類型 ZigBee 設備的強制物件。該物件中的網路發現、讀取和設置屬性是各種類型 ZigBee 設備都要強制支援的。如果設備是 ZigBee 協調器，則應支援構建網路請求和證實、離開網路指示、加入網路指示、網路允許加入請求和證實、直接加入網路請求和證實，不支援加入網路請求，加入網路證實、離開網路請求、離開網路證實；如果設備是 ZigBee 路由器，則還應支援啓動路由器請求和證實、加入網路請求和證實、加入網路指示、離開網路請求和證實、離開網路指示、直接加入網路請求和證實、網路允許加入請求和證實，不支援構建網路請求和證實；如果設備是 ZigBee

終端設備，則還應加入網路請求和證實，離開網路請求和證實，不支援構建網路請求和證實、啓動路由器請求和證實、加入網路指示、離開網路指示、網路允許加入請求。對於各種邏輯類型的 ZigBee 設備，網路同步請求、指示和證實、網路重定請求和證實都是可選支援的屬性。網路管理物件的屬性如表 14 所列。

表 14 網路管理屬性

屬　　性	M/O	類型
NLME-GET.request	M	私有
NLME-GET.confirm	M	私有
NLME-SET.request	M	私有
NLME-SET.confirm	M	私有
NLME-NETWORK-DISCOVERY.request	M	公共
NLME-NETWORK-DISCOVERY.confirm	M	公共
NLME-NETWORK-FORMATION.request	O	私有
NLME-NETWORK-FORMATION.confirm	O	私有
NLME-JOIN.request	O	私有
NLME-JOIN.confirm	O	私有
NLME-DIRECT-JOIN.request	O	公共
NLME-DIRECT-JOIN.confirm	O	公共
NLME-LEAVE.request	O	私有
NLME-LEAVE.confirm	O	私有
NLME-RESET.request	O	私有
NLME-RESET.confirm	O	私有
NLME-SYNC.request	O	公共
NLME-SYNC.indication	O	公共
NLME-SYNC.confirm	O	公共

1.5.3.7 節點管理

節點管理支援請求和回應管理功能的能力。這些管理功能之時使得接收到請求的設備的工作狀態對外部設備視覺化。節點管理物件是各種邏輯類型的 ZigBee 設備都可選支援的物件。如果設備支援節點管理物件，則該物件中的各種請求和回應屬性頁是可選支援的。

1.5.4 配置屬性

ZDO 的配置屬性如表 15 所列。

表 15 配置屬性

屬　　性	M/O	類型
：Config_Node_Descriptor	M	公共

：Config_Power_Descriptor	M	公共
：Config_Simple_Descriptors	M	公共
：Config_NWK_Mode_and_Params	M	公共
：Config_NWK_Scan_Attempts	M	私有
：Config_NWK_Time_btwn_Scans	M	私有
：Config_Complex_Descriptor	O	公共
：Config_User_Descriptor	O	公共
：Config_Max_Bind	O	私有
：Config_Master_Key	O	私有
：Config_EndDev_Bind_Timeout	O	私有
：Config_Permit_Join_Duration	O	公共
：Config_NWK_Security_Level	O	私有
：Config_NWK_Secure_All_Frame	O	私有
：Config_NWK_Leave_removeChildren	O	私有
：Config_NWK_BroadcastDeliveryTime	O	私有
：Config_NWK_TransactionPersistenceTime	O	私有

各種屬性的定義如下：

：Config_Node_Descriptor 是設備節點描述符的內容。該屬性在應用首次載入時建立或是設備在網路中運行前初始化，它用於在服務發現中向外部查詢設備描述節點特性。

：Config_Power_Descriptor 是設備電源描述符的內容。該屬性在應用首次載入時建立或是設備在網路中運行前初始化，它用於在服務發現中向外部查詢設備描述節點電源特性。

：Config_Simple_Descriptors 是設備每個活動端點簡單描述符的內容。該屬性在應用首次載入時建立並且是唯讀的，它用於在服務發現中向外部查詢設備描述介面特性。

：Config_NWK_Mode_and_Params 屬性包含執行網路發現時要掃描的通道列表 ChannelList、協定版本號、協定堆疊配置檔、信標階數、超訊框(Frame)階數、電池壽命擴充和安全設置欄位。：Config_Node_Descriptor 屬性包含有一個描述設備邏輯設備類型的欄位。邏輯設備類型和設備 ZDO 使用的詳細邏輯允許設備應用使用：Config_NWK_Mode_and_Params 中的參數構建或加入一個與該設備支援應用一致的網路。

：Config_NWK_Scan_Attempts 屬性是一個整數值，表示設備 NWK 層在決定要關聯的 ZigBee 協調器或路由器前執行網路發現掃描 NLME-NETWORK-DISCOVERY.request 的次數。該屬性的預設值是 5，有效取值範圍爲 1～255。

：Config_NWK_Time_btwn_Scans 屬性是一個整數值，表示：Config_NWK_Scan_Attempts 次重複掃描中每次掃描持續的時間（s）。該屬性的預設值是 1，有效取值範圍 1～255。

：Config_Complex_Descriptor 是設備可選的複雜描述符的內容。該屬性在應用首次載入時建立或是設備在網路中運行前初始化，它用於在服務發現中向外部查詢設備描述設備的擴充特性。

：Config_User_Descriptor 是設備可選的使用者描述符的內容。該屬性在應用首次載入時建立或是設備在網路中運行前初始化，它用於在服務發現中向外部查詢設備提供的有關該設備的描述性字串。

：Config_Max_Bind 是一個常量，它表示 ZigBee 協調器或 ZigBee 路由器中綁定表支援的最大綁定記錄數。

：**Config_Master_Key** 是設備採用安全機制時使用的主密鑰。該屬性在應用首次載入時建立或是設備在網路中運行前初始化，用在安全操作過程中。

：**Config_EndDev_Bind_Timeout** 是終端設備綁定時的超時時間值，它只用在 ZigBee 協調器中判斷兩個終端設備綁定請求是否在該超時窗口內到達。

：**Config_Permit_Join_Duration** 是 NLME-PERMIT-JOINING.request 設定的允許入網持續時間。該屬性的預設值是 0，可以根據配置檔的需要設置爲不同的值。

：**Config_NWK_Security_Level** 屬性只用在信用中心，用以設定網路的安全級別。

：**Config_NWK_Secure_All_Frame** 屬性只用在信用中心，用以決定是否對所有訊框(Frame)都採取安全機制。

：**Config_NWK_Leave_removeChildren** 屬性決定當設備被要求離開網路時其子設備是否也離開網路。該屬性值在協定堆疊配置檔中定義。

：**Config_NWK_BroadcastDeliveryTime** 表示廣播訊息在網路中傳輸的時間（s）。該屬性值在協定堆疊配置檔中定義。

：**Config_NWK_TransactionPersistenceTime** 表示設備儲存並在信標上指示一個事務的最長時間（以超訊框(Frame)週期爲單位）。該屬性在 ZigBee 協調器和 ZigBee 路由器中是強制支援的，在 ZigBee 終端設備中不使用該屬性，屬性值在協定堆疊配置檔中定義。該屬性反映的是 MAC PIB 屬性 macTransactionPersistenceTime 的值，高層對該屬性值的更改也將反映到 MAC PIB 屬性中。

2. 網路層規範

2.1 網路層規範概述

網路層應提供保證 IEEE 802.15.4 MAC 層正確工作的能力並爲應用層提供合適的服務介面。爲了與應用層介面，網路層概念上也包括兩個服務實體 — 網路層資料實體和網路層管理實體，提供必要的功能。網路層資料實體（NLDE）透過 NLDE-SAP 爲應用層提供資料服務；網路層管理實體（NLME）透過 NLME-SAP 爲應用層提供管理服務。NLME 要借助 NLDE 完成部分管理任務，另外它還要維護一個有關管理物件的資料庫 — 網路層資訊庫（NIB）。

NLDE 提供的資料服務允許在同一網路中的兩個或多個設備之間傳輸應用協定資料單元（APDU）。具體來說，NLDE 提供的服務：一是在應用支援子層 PDU 基礎上添加適當的協定頭產生網路協定資料單元（NPDU）；二是根據拓撲路由，把 NPDU 發送到通訊鏈路的目的位址設備或通訊鏈路的下一跳。

NLME 提供的管理服務允許應用與協定堆疊之間交互。具體來說，NLME 提供的服務包括配置新設備、建立新網路、設備請求加入/離開網路和 ZigBee 協調器或路由器請求設備離開網路、定址、近鄰發現、路由發現、接收控制等。

圖 7 是 ZigBee 網路層參考模型。NWK 層透過兩個服務接入點（SAP）提供了兩種服務，即透過 NWK 層資料實體 SAP（NLDE-SAP）提供的 NWK 資料服務和透過 NWK 層管理實體 SAP（NLME-SAP）提供的 NWK 管理服務。網路層的這兩種服務透過 MCPS-SAP 和 MLME-SAP 提供了應用層和 MAC 子層之間的介面。除了這些外部介面，在 NWK 內部 NLME 和 NLDE 之間還存在一個隱含介面，允許 NLME 使用 NWK 資料服務。

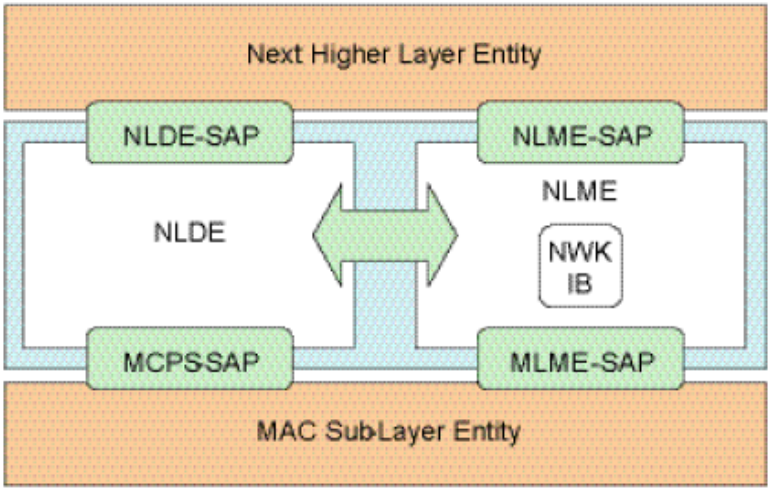


圖 7 ZigBee 網路層參考模型

2.2 網路層服務規範

2.2.1 網路層資料服務

NLDE-SAP 支援在對等應用實體之間傳送應用協定資料單元（APDU）。NLDE-SAP 支持的原語包括 NLDE-DATA 請求、證實和指示原語。

1. NWK 資料請求原語 NLDE-DATA.request

NWK 資料請求原語 NLDE-DATA.request 請求把一個 APDU（即 NSDU）從本地 APS 子層傳送到一個或多個對等的 APS 子層實體。當有 APDU（即 NSDU）需要傳送到對等的 APS 子層實體時，本地 APS 子層實體就產生 NLDE-DATA.request 原語。該請求原語的語法如下：

NLDE-DATA.request（DstAddr，NsduLength，Nsdu，NsduHandle，Radius，DiscoverRoute，SecurityEnable）

其中：參數 DstAddr 表示 NSDU 要傳送到目的實體的網路位址；NsduLength 表示待傳送的 NSDU 包含的位元組數；Nsdu 表示待傳送的 NSDU 的內容；NsduHandle 表示 NWK 實體要傳送的 NSDU 的控制碼；Radius 表示允許訊框(Frame)在網路中傳播的跳數；DiscoverRoute 參數可用來控制訊框(Frame)傳送時的路由發現操作，0x00 表示禁止路由發現，0x01 表示允許路由發現，0x02 表示強制路由發現；SecurityEnable 參數可用來致能當前訊框(Frame)的 NWK 層安全處理。如果 NIB 中的安全級別屬性爲 0，表示沒有安全機制，該參數被忽略；如果該參數值爲 TRUE，則對當前訊框(Frame)應用 NIB 安全級別指定的安全機制；如果該參數值爲 FALSE，則對當前訊框(Frame)不使用進行安全處理。

如果一個尚未關聯到網路中的設備 NWK 層收到 NLDE-DATA.request 原語，它將返回狀態爲 INVALID_REQUEST 的 NLDE-DATA.confirm 證實原語。一個已關聯設備的 NWK 層收到 NLDE-DATA.request 原語後，爲了發送原語提供的 NSDU，NLDE 首先構造 NPDU。如果在發送 NSDU 之前 NLDE 就向上層發出了 NLDE-DATA.confirm 證實原語，則後續處理將被取消。爲了構造新的 NPDU，NWK 訊框(Frame)頭的目的位址欄位應設定了 DstAddr 參

數值，源位址欄位應設置爲 MAC PIB 屬性 macShortAddress 的值。訊框(Frame)控制欄位中的發現路由子域設置爲 DiscoverRoute 參數的值。如果請求原語提供了 Radius 參數值，則把它放在 NWK 訊框(Frame)頭的傳播範圍子域；如果請求原語沒有提供 Radius 參數的有效值，則把 NWK 訊框(Frame)頭的傳播範圍子域設置爲 NIB 屬性 nwkMaxDepth 值的兩倍。NWK 層將爲訊框(Frame)產生一個序號並放在 NWK 訊框(Frame)頭的序號欄位中。當 NPDU 構造完成後，就可以根據路由發送 NSDU 了。如果尋找到了合適的路由，NWK 層實體就調用 MCPS-DATA.request 原語來發送 NSDU。MCPS-DATA.request 原語中的 SrcAddrMode 和 DstAddrMode 參數均設爲 0x02，表示源位址和目的位址都使用 16 位網路位址；SrcPANId 和 DstPANId 參數應設置爲 MAC PIB 屬性 macPANId 的當前值；SrcAddr 參數應設置爲 MAC PIB 屬性 macShortAddr 的值；DstAddr 參數設置爲路由過程決定的下一跳的位址；TxOptions 參數與 0x01 逐位相“與”後應不爲零，表示要求確認的發送。在接收到 MCPS-DATA.confirm 證實原語後，NLDE 才向上層發送 NLDE-DATA.confirm 證實原語，該原語的狀態等於 MCPS-DATA.confirm 返回的狀態。如果 NIB 中安全級別屬性不爲 0 並且 NLDE-DATA.request 原語的 SecurityEnable 參數值爲 TRUE，則在發送訊框(Frame)之前還要進行 NWK 層安全處理。如果某種原因使得 NWK 層安全處理失敗，則該訊框(Frame)被丟棄並且 NLDE 向上層發送狀態等於安全套件返回狀態的 NLDE-DATA.confirm 證實原語。

2. NWK 資料證實原語 NLDE-DATA.confirm

NWK 資料證實原語 NLDE-DATA.confirm 用來報告請求從本地 APS 子層實體向對等的 APS 子層實體發送 NSDU 的結果。該原語由本地 NLDE 產生，作爲對接收到的 NLDE-DATA.request 原語的回應。NLDE-DATA.confirm 原語的語法如下：

NLDE-DATA.confirm（NsduHandle，Status）

其中：參數 NsduHandle 表示被證實 NSDU 的控制碼；Status 表示相應請求的狀態，其取值爲 INVALID_REQUEST、MAX_FRM_COUNTER、NO_KEY、BAD_CCM_OUTPUT 或是安全套件返回的狀態，或是 MCPS-DATA.confirm 原語返回的狀態。發起請求設備的 APS 子層收到 NLDE-DATA.confirm 原語就被告知了其請求發送 APDU 的結果。如果發送嘗試成功，則該原語的狀態參數爲 SUCCESS；否則，狀態參數將指示出發送失敗的原因。

3. NWK 資料指示原語 NLDE-DATA.indication

NWK 資料指示原語 NLDE-DATA.indication 指示儀個資料 PDU（NSDU）從 NWK 傳送到本地 APS 子層實體。NLDE 收到來自 MAC 層實體的正確定址資料訊框(Frame)後就向 APS 子層發出該指示原語。NLDE-DATA.indication 原語的語法如下：

NLDE-DATA.indication（SrcAddress，NsduLength，Nsdu，LinkQuality）

其中：參數 SrcAddress 表示接收到的 NSDU 的起始設備 16 位元位址；NsduLength 表示接收的 NSDU 包含的位元組數；Nsdu 表示接收的 NSDU 的內容；LinkQuality 表示 MAC 層接收到該訊框(Frame)時的鏈路品質，它是 MCPS-DATA.indication 原語中的一個參數。APS 子層收到該指示原語就被告知有資料訊框(Frame)到達。

2.2.2 網路層管理服務

NLME-SAP 允許在上層和 NLME 之間傳送命令訊框(Frame)。NLME-SAP 支援的管理原語有 NLME-NETWORK-DISCOVERY 請求和證實原語、NLME-NETWORK-FORMATION 請求和證實原語、NLME-PERMIT-JOINING 請求、證實和指示原語、NLME-START-ROUTER 請求和證實原語、NLME-JOIN 請求、證實和指示原語、NLME-RESET 請求和證實原語、

NLME-SYNC 請求和證實原語、NLME-GET 請求和證實原語、NLME-SET 請求和證實原語。

2.2.2.1 網路發現

NLME-SAP 支援發現正在運行的網路，網路發現過程中使用的原語是 NLME-NETWORK-DISCOVERY。NLME-NETWORK-DISCOVERY.request 原語由 ZigBee 設備上層產生併發送給 NLME，請求發現設備 POS 內正在運行的網路。該請求原語的語法如下：

NLME-NETWORK-DISCOVERY.request（ScanChannels，ScanDuration）

其中：參數 ScanChannels 爲 32 位元資料，其 27 個低有效位元分別對應一個通道，用來指示網路發現過程中要掃描的通道，1 表示要掃描，0 表示不掃描；ScanDuration 用來計算掃描每個通道時持續的時間，每個通道的掃描時間爲 aBaseSuperframeDuration×（2n+1）個符號週期，其中 n 即爲 ScanDuration 的值。NWK 層收到網路發現請求原語後，掃描 ScanChannels 參數指定的通道，搜索設備 POS 範圍內當前正在運行的網路。如果設備是 IEEE 802.15.4 FFD，則它將主動掃描；如果設備是 RFD，倘若它支援主動掃描，就執行主動掃描，否則使用 MLME-SCAN.request 原語執行被動掃描。接收到 MLME-SCAN.confirm 原語後，設備近鄰表將根據掃描返回的資訊被更新，並且會產生一個網路描述符列表。NLME 就向上層發送 NLME-NETWORK-DISCOVERY.confirm 原語，返回搜索發現網路的資訊，Status 參數值等於 MLME-SCAN.confirm 原語返回的狀態。

NLME-NETWORK-DISCOVERY.confirm 原語由 NLME 產生併發送給上一層，用以報告 NLME-NETWORK-DISCOVERY.request 請求網路發現操作的結果。該證實原語的語法爲：

NLME-NETWORK-DISCOVERY.confirm（NetworkCount，NetworkDescriptor，Status）

其中：參數 NetworkCount 表示發現的網路個數；NetworkDescriptor 表示發現的各個網路描述符列表；Status 參數值爲 MLME-SCAN.confirm 原語返回的狀態值。網路描述符包含 7 個資訊欄位，PanID 是發現網路的 16 位元 PAN 標識，其最高兩個有效位暫時預留，應設爲 0；LogicalChannel 表示網路當前使用的邏輯通道；StackProfile 表示發現網路中使用的 ZigBee 協定堆疊的配置檔標識；ZigBee version 表示發現網路使用的 ZigBee 版本；BeaconOrder 規定了網路發送 MAC 層信標的頻率；SuperframeOrder 規定了信標網路超訊框(Frame)中活動週期的長度；PermitJoining 爲 TRUE 時表示網路中當前至少有一個 ZigBee 路由器允許設備加入。

2.2.2.2 網路構建

NLME-NETWORK-FORMATION.request 原語允許上層請求設備自任協調器建立一個 ZigBee 新網路，並對其超訊框(Frame)配置進行修改。該請求原語的語法如下：

NLME-NETWORK-FORMATION.request（ScanChannels，ScanDuration，BeaconOrder，SuperframeOrder，PANId，BatteryLifeExtension）

其中：ScanChannels 爲 32 位元資料，其 27 個低有效位元分別對應一個通道，用來指示準備新建網路時要掃描的通道，1 表示要掃描，0 表示不掃描；ScanDuration 用來計算掃描每個通道時持續的時間，每個通道的掃描時間爲 aBaseSuperframeDuration×（2n+1）個符號週期，其中 n 即爲 ScanDuration 的值；BeaconOrder 是上層指定建立網路的信標階數；

SuperframeOrder 是上層指定建立網路的超訊框(Frame)階數；PANId 是可選的 PAN 標識，表示上層預訂的建立新網路的標識，如果上層沒有指定 PANId，則 NWK 層將選擇一個 PAN ID，該參數的最高兩個有效位應爲 0；BatterLifeExtension 如果爲 TRUE，NLME 將請求 ZigBee 協調器支援電池壽命延長模式，否則 NLME 將請求 ZigBee 協調器不支援電池壽命延長模式。

一個不能承擔 ZigBee 協調器的設備或是一個已成爲網路協調器的設備的 NLME 收到 NLME-NETWORK-FORMATION.request 原語後，將向上層發送狀態爲 INVALID_REQUEST 的證實原語 NLME-NETWORK-FORMATION.confirm。如果設備要被初始化成一個 ZigBee 協調器，NLME 請求 MAC 子層在指定的一組通道上線執行一次能量檢測掃描，再執行一次主動掃描。爲了執行這兩次掃描，NLME 先向 MAC 子層發出 ScanType 參數爲能量檢測掃描的掃描請求原語 MLME-SCAN.request 原語，再向 MAC 子層發出 ScanType 參數爲主動掃描的掃描請求原語。完成主動掃描後，NLME 接收到 MAC 子層返回的掃描證實原語 MLME-SCAN.confirm，選擇一個合適的通道。如果上層指定了 PANId 參數，NWK 層要確認指定的 PAN 標識與選定通道上已經運行網路的 PAN 標識不衝突。如果發生衝突，則在可能的前提下，要從掃描通道組中重新選擇一個通道；如果沒有合適的通道滿足 PAN 不衝突，則 NWK 將發出狀態爲 STARTUP_FAILURE 的 NLME-NETWORK-FORMATION.confirm 原語。如果上層沒有指定 PAN 標識，NWK 層將選擇一個與選定通道上其他網路 PAN 標識不衝突的標識作爲新建 PAN 的標識。一旦選定了合適的通道和 PAN 標識，NLME 將指定 0x0000 爲設備的 16 位元 MAC 位址。指定 16 位短位址透過調用 MLME-SET.request 原語設置 MAC PIB 屬性 macShortAddress 來實現。如果不能找到合適的通道或 PAN 標識，NLME 將發出 Status 參數爲 STARTUP_FAILURE 的 NLME-NETWORK-FORMATION.confirm 原語。要初始化一個新的或修改一個現成的超訊框(Frame)配置，NLME 將向 MAC 子層發出 MLME-START.request 原語。MLME-START.request 原語中的 PANCoordinator 參數設爲 TRUE，BeaconOrder 和 SuperframeOrder 參數與 NLME-NETWORK-FORMATION.request 原語中的參數值相同。如果 MLME-START.request 是初始化一個新的超訊框(Frame)，則其參數 CoordRealignment 設爲 FALSE；如果 MLME-START.request 是改變現存超訊框(Frame)的配置屬性，則參數 CoordRealignment 設爲 TRUE。收到 MLME-START.confirm 證實原語後，NLME 才向上層發送證實原語 NLME-NETWORK-FORMATION.confirm，該原語的狀態等於 MLME-START.confirm 原語返回的狀態。

NLME-NETWORK-FORMATION.confirm 原語由 NLME 產生，向上層報告請求初始化一個新網路的 ZigBee 協調器的結果。NLME-NETWORK-FORMATION.confirm 原語是對請求原語 NLME-NETWORK-FORMATION.request 的回應，它的語法如下：

NLME-NETWORK-FORMATION.confirm（Status）

其唯一參數 Status 表示請求把設備初始化成 ZigBee 協調器或請求改變超訊框(Frame)配置的結果，取值爲 INVALID_REQUEST、STARTUP_FAILURE 或是 MLME-START.confirm 原語返回的裝它值。如果 NLME 把設備成功初始化爲 ZigBee 協調器或成功改變了超訊框(Frame)配置，則證實原語 NLME-NETWORK-FORMATION.confirm 的狀態參數爲 SUCCESS；否則，狀態參數值將反映請求失敗的原因。

2.2.2.3 允許設備入網

NLME-PERMIT-JOINING 請求和證實原語定義了 ZigBee 協調器或路由器如何允許設備加入到網路中。NLME-PERMIT-JOINING.request 原語由 ZigBee 協調器或路由器的上層產生

併發送給 NLME，用以把 MAC 子層的允許關聯標誌位元設置爲一個固定時限，在這段時間內 ZigBee 協調器或路由器允許其他設備加入到它所在的網路。該請求原語的語法如下：

NLME-PERMIT-JOINING.request（PermitDuration）

其唯一參數 PermitDuration 表示 ZigBee 協調器或路由器允許關聯的時間長度（s），其取值範圍是整數 0x00～0xff。其中 0x00 表示禁止設備關聯，0xff 表示總允許設備關聯，其他值則表示在規定的時限內允許設備關聯到ZigBee 協調器或路由器。

只有 ZigBee 協調器或路由器的上層能夠發送 NLME-PERMIT-JOINING.request 原語，如果一個 ZigBee 終端設備的 NWK 層收到該請求原語，NLME-PERMIT-JOINING.confirm 證實原語將返回狀態 INVALID_REQUEST。當接收到 NLME-PERMIT-JOINING.request 原語的 PermitDuration 等於 0x00 時，NLME 就向 MAC 子層發出 MLME-SET.request 原語把 MAC PIB 屬性 macAssociationPermit 設爲 FALSE。MLME 在收到來自 MAC 層的證實原語 MLME-SET.confirm 後，再向上一層發送與 MLME-SET.confirm 相同狀態的證實原語 NLME-PERMIT-JOINING.confirm。當接收到 NLME-PERMIT-JOINING.request 原語的 PermitDuration 參數值等於 0xff 時，NLME 就向 MAC 子層發出 MLME-SET.request 原語把 MAC PIB 屬性 macAssociationPermit 設爲 TRUE，MLME 在收到證實原語 MLME-SET.confirm 後，再向上一層發送相同狀態的證實原語 NLME-PERMIT-JOINING.confirm。如果接收到 NLME-PERMIT-JOINING.request 原語的 PermitDuration 參數值不等於 0x00 或 0xff，NLME 將採用同樣的方法把 MAC PIB 屬性 macAssociationPermit 設爲 TRUE，在接收到證實原語 MLME-SET.confirm 後啓動一個計時器，計時時長爲 PermitDuration 秒，啓動計時器後，NLME 就向上層發送 NLME-PERMIT-JOINING.confirm 證實原語，狀態等於 MAC 子層返回的狀態。計時期滿後，NLME 再次調用 MLME-SET.request 原語把屬性 macAssociationPermit 設置爲 FALSE。

NLME-PERMIT-JOINING.confirm 證實原語是對 NLME-PERMIT-JOINING.request 原語的回應，它由 ZigBee 協調器或路由器的 NLME 發送，告知應用層請求允許關聯的請求結果。該原語的語法如下：

NLME-PERMIT-JOINING.confirm（Status）

其唯一參數 Status 表示請求允許關聯的狀態，取值爲 INVALID_REQUEST 或 MLME-SET.confirm 原語返回的狀態值。

2.2.2.4 配置 ZigBee 路由器

NLME-START-ROUTER 原語用來把一個新加入網路的設備初始化成 ZigBee 路由器，或用來重新配置一個 ZigBee 路由器的超訊框(Frame)。NLME-START-ROUTER.request 原語的語法如下：

NLME-START-ROUTER.request（BeaconOrder，SuperframeOrder，BatteryLifeExtension）

其中：參數 BeaconOrder 表示上層期望的網路信標階數；SuperframeOrder 表示上層期望的網路超訊框(Frame)階數；BatteryLifeExtension 取值爲 TRUE 時，NLME 將請求 ZigBee 路由器運行時支援電池壽命延長模式，取值爲 FALSE 時，NLME 將請求 ZigBee 路由器運行時不支援電池壽命延長模式。

如果一個非 ZigBee 網路路由器設備的 NLME 收到 NLME-START-ROUTER.request 原語，它將向上層發送 Status 參數值爲 INVALID_REQUEST 的 NLME-START-ROUTER.confirm 證實原語。爲了初始化一個新路由器的超訊框(Frame)配置或配置一個現存路由器的超訊框

(Frame)，NLME 向 MAC 子層發送 MLME-START.request 原語。如果 MLME-START.request 原語用來初始化一個新超訊框(Frame)，則該原語的 CoordRealignment 參數設爲 FALSE；如果 MLME-START.request 原語用來改變 PAN 的任何配置屬性，則 CoordRealignment 參數設爲 TRUE。NLME 在收到 MAC 層對 MLME-START.request 的回應 MLME-START.confirm 後，才向上層發送證實原語 NLME-START-ROUTER.confirm，狀態與 MLME-START.confirm 返回的狀態相同。並且僅當 MLME-START.confirm 返回狀態爲 SUCCESS，設備才開始履行 ZigBee 路由器的職能，包括資料訊框(Frame)尋路、路由發現、路由準備、接收其他設備加入網路的請求等；否則設備將被禁止執行這些行爲。

NLME-START-ROUTER.confirm 原語由 NLME 產生併發送給上一層，作爲對 NLME-START-ROUTER.request 的回應。該原語的語法如下：

NLME-START-ROUTER.confirm（Status）

其唯一參數 Status 表示 NLME-START-ROUTER.request 請求的結果，取值爲 INVALID_REQUEST 或 MLME-START.confirm 返回的狀態值。如果 NLME 成功初始化或改變了一個 ZigBee 路由器的超訊框(Frame)配置，NLME-START-ROUTER.confirm 的狀態參數設爲 SUCCESS；否則，狀態參數將反映出 NLME 請求失敗的原因。

2.2.2.5 設備入網

NLME-JOIN.request 原語定義了上層如何請求透過關聯加入網路、直接加入網路和在孤立後重新加入網路。該請求原語的語法如下：

NLME-JOIN.request（PANId，JoinAsRouter，RejoinNetwork，ScanChannels，ScanDuration，PowerSource，RxOnWhenIdle，MACSecurity）

其中：參數 PANId 表示設備要加入網路的 PAN 標識碼，兩個最高有效位應爲 0；JoinAsRouter 只是在關聯加入網路時有效，直接加入或孤立後重新加入網路時無效，如果設備加入網路後成爲 ZigBee 路由器，則該參數設爲 TRUE，否則設爲 FALSE；如果設備直接加入或在孤立後重新加入網路，RejoinNetwork 參數設爲 TRUE，如果設備透過關聯方式加入網路，RejoinNetwork 參數設爲 FALSE；ScanChannels 的 27 個低有效位元分別對應一個通道，1 表示要掃描，0 表示不掃描，設備透過關聯方式進入網路時忽略該參數；ScanDuration 規定了掃描每個通道需要持續的時間；PowerSource 是 MLME-ASSOCIATE.request 原語中 CapabilityInformation 參數的一般分，參數值 0x01 表示設備由幹線供電，0x00 表示其他電源供電；RxOnWhenIdle 參數決定設備在 CAP 的空閒部分是否能接收資料包，參數值 0x01 表示設備空閒時開啓接收機，0x00 表示設備空閒時關閉接收機，非信標網路中的 ZigBee 協調器和 ZigBee 路由器，其 RxOnWhenIdle 參數值應爲 0x01；MACSecurity 是 MLME-ASSOCIATE.request 原語中 CapabilityInformation 參數的一部分，參數值 0x01 表示 MAC 層使用安全處理，0x00 表示 MAC 層不使用安全處理。

當一個已經處在網路中的設備 NLME 收到 NLME-JOIN.request 原語時，將向其上層發送狀態爲 INVALID_REQUEST 的證實原語 NLME-JOIN.confirm。當一個尚未加入到網路中的設備收到 NLME-JOIN.request 原語時，它將嘗試加入到 PANId 參數指定的網路中。如果 RejoinNetwork 參數爲 FALSE，NLME 將向 MAC 層發送 MLME-ASSOCIATE.request 原語。MLME-ASSOCIATE.request 原語中 CoordAddress 參數設爲設備近鄰表中滿足下列條件的一個路由器的位址：

1. 該路由器屬於 PANId 參數標識的網路；

2. 路由器能接受設備加入請求；

3. 設備與該路由器之間的鏈路品質滿足要去。

如果設備的近鄰表中存在一個滿足上述條件的設備，MLME-ASSOCIATE.request 原語中的 LogicalChannel 參數將設置爲近鄰表中該設備位址對應的通道。如果不止一個設備滿足上述條件，則設備將選擇樹深度最小的設備作爲關聯路由器。如果近鄰表中沒有滿足上述條件的設備，NLME 將向上層發送 Status 參數爲 NOT_PERMITED 的 NLME-JOIN.confirm 原語；否則 NLME 將向上層發送 Status 參數等於 MLME-ASSOCIATE.confirm 返回狀態的 NLME-JOIN.confirmed 原語。如果 RejoinNetwork 參數爲 FALSE 並且 JoinAsRouter 參數設爲 FALSE，則設備加入網路將成爲終端設備，不參與路由安排。如果一個尚未加入網路的設備收到 NLME-JOIN.request 原語並且 RejoinNetwork 參數爲 TRUE，它將向 MAC 層發送 MLME-SCAN.request 原語，ScanType 參數設置爲孤立掃描，掃描週期設置爲 ScanDuration 參數值。NLME 在收到掃描證實原語 MLME-SCAN.confirm 後，如果找不到要加入的網路，則向上層發送 Status 參數爲 NO_NETWORKS 的證實原語 NLME-JOIN.confirm；否則 NLME-JOIN.confirm 原語的狀態爲掃描證實原語返回的狀態。

當以個新設備透過 MAC 關聯過程加入到網路中時，其關聯的 ZigBee 協調器或路由器的 NLME 就向其上層發送指示原語 NLME-JOIN.indication。ZigBee 協調器或路由器的 NLME 在收到關聯指示原語 MLME-ASSOCIATE.indication。ZigBee 協調器或路由器的 NLME 在收到關聯指示原語 MLME-ASSOCIATE.indication 並向 MAC 層發送回應原語 MLME-ASSOCIATE.response 後，才向上層發送入網指示原語 NLME-JOIN.indication。該原語的語法如下：

NLME-JOIN.indication （ ShortAddress ， ExtendedAddress ， CapabilityInformation ， SecureJoin）

其中：參數 ShortAddress 表示新加入設備的 16 位元網路位址；ExtendedAddress 表示新加入設備的 64 位元 IEEE 位址；CapabilityInformation 規定了新加入設備的工作能力；如果隱含的 MAC 關聯過程採用了安全機制，則 SecureJoin 參數設爲 TRUE，否則，SecureJoin 參數設爲 FALSE。

NLME-JOIN.confirmed 原語由請求加入網路的設備 NLME 發送給上層，作爲對請求原語 NLME-JOIN.request 的回應。該原語的語法如下：

NLME-JOIN.confirmed（PANId，Status）

其中：參數 PANId 是該證實原語對應的 NLME-JOIN.request 原語中的 PAN 標識；Status 表示設備請求加入網路的結果，其取值爲 INVALID_REQUEST、NOT_PERMITTED、NO_NETWORKS 或是 MLME-ASSOCIATE.confirm 或 MLME-SCAN.confirm 原語返回的狀態值。

NLME-DIRECT-JOIN.request 原語允許 ZigBee 協調器或路由器的上層請求把另一個設備直接加入到網路中來。該過程僅在 ZigBee 協調器或路由器的內部完成，不需要任何空中傳輸。NLME-DIRECT-JOIN.request 原語的語法如下：

NLME-DIRECT-JOIN.request（DeviceAddress，CapabilityInformation）

其中：參數 DeviceAddress 表示將被直接加入到網路中的設備的 64 位元 IEEE 位址；CapabilityInformation 表示將被直接加入到網路中的設備的工作能力，它是 8 位元的資料，各位的定義如下：

比特位：0	1	2	3	4～5	6	7
備用 PAN 協調器	設備類型	電源	空閒時接收機致能	預留	安全能力	預留

ZigBee 協調器或路由器的 NLME 收到 NLME-DIRECT-JOIN.request 原語後，將嘗試把 DeviceAddress 參數指定的設備加入到近鄰表中。在該原語中，CapabilityInformation 參數的“備用 PAN 協調器”比特位應設爲 0。如果加入網路的設備是 ZigBee 路由器，則“設備類型”比特位元設爲 1；如果加入網路的設備是 ZigBee 終端設備，則“設備類型”比特位元設爲 0。如果設備的供電電源是交流電源，則“電源”比特位設爲 1，否則設爲 0。如果設備在空閒期間開啓接收機，則“空閒時接收機致能”比特位應設爲 1，肉則應設爲 0。如果設備支援安全處理，則“安全能力”比特位應設爲 1，否則設爲 0。如果 NLME 能夠把設備直接加入到網路，就向上層發送狀態爲 SUCCESS 的證實原語 NLME-DIRECT-JOIN.confirm。如果 NLME 發現原語請求加入的設備已經存在于近鄰表中，就向上層發送狀態爲 ALREADY_PRESENT 的 NLME-DIRECT-JOIN.confirm 原語。如果 NLME 發現設備列表中沒有足夠的空間添加新設備，就向上層發送狀態爲 TABLE_FULL 的 NLME-DIRECT-JOIN.confirm 原語。

NLME-DIRECT-JOIN.confirm 原語是對 NLME-DIRECT-JOIN.request 原語的回應。它由 ZigBee 協調器或路由器的 NLME 產生併發送給上層，向上層報告其請求直接加入設備的結果。該證實原語的語法如下：

NLME-DIRECT-JOIN.confirm（DeviceAddress，Status）

其中：參數 Status 表示 NLME-DIRECT-JOIN.request 請求的狀態，其取值爲 SUCCESS、ALREADY_PRESENT 或 TABLE_FULL.。

2.2.2.6 離開網路

NLME-LEAVE 一組原語定義了設備的上層如何請求設備自身離開網路或請求另一個設備離開網路；同時還定義了 ZigBee 協調器的上層如何獲知一個設備已經離開網路的資訊。NLME-LEAVE.request 原語由設備上層產生併發送給 NLME，設備用該原語來請求離開網路，另外 ZigBee 協調器或路由器還可以用該原語請求其他設備離開網路。NLME-LEAVE.request 原語的語法如下：

NLME-LEAVE.request（DeviceAddress，RemoveChildren，MACSecurityEnable）

其中：參數 DeviceAddress 如果爲空，則表示設備請求把自己從網路中刪除，否則該參數表示原語請求要從網路中刪除的設備的 IEEE 位址；RemoveChildren 參數值如果等於 TRUE，則被從網路中刪除的設備同時還要刪除它的子設備，如果等於 FALSE，則只是 DeviceAddress 指定的設備自身離開網路；MACSecurityEnable 用來控制 MAC 層原語中 SecurityEnable 參數的值。

如果一個尚未加入網路的設備的 NLME 收到 NLME-LEAVE.request 原語，NLME 將向上層發送狀態爲 INVALID_REQUEST 的證實原語 NLME-LEAVE.confirm。如果一個已入網設備的 NLME 收到的 NLME-LEAVE.request 原語中 DeviceAddress 參數爲空，RemoveChildren 參數等於 FALSE,則 NLME 將把設備自身從網路中刪除，之後 NLME 將清空路由表並向 MAC 子層發送一個復位請求原語 MLMLE-RESET.request。如果 NLME 接收到 MLME-RESET.confirm 證實原語的 Status 參數不是 SUCCESS，NLME 將重新發送復位請求。NLME 還要把近鄰表中其前父設備對應記錄中的關係欄位設爲 0x03，表示沒有關係。如果一個已入網設備的 NLME 收到 NLME-LEAVE.request 原語，並且原語中 DeviceAddress 參數爲空，RemoveChildren 參數等於 TRUE，則 NLME 把設備自身從網路中刪除之前要先刪除設備的子設備。每完成一次刪除子設備的操作，NLME 都向上層發送一個

NLME-LEAVE.confirm 原語，證實原語中 DeviceAddress 參數等於剛刪除設備的 IEEE 位址，如果刪除子設備成功，則 Status 參數等於 SUCCESS，如果因爲任何原因導致刪除子設備失敗，則 Status 參數等於 LEAVE_UNCONFIRMED。同時，NLME 還要把近鄰表中被刪除子設備對應記錄中的關係欄位設爲 0x03，表示沒有關係。在刪除了所有的子設備之後，NLME 才把設備自身從網路中刪除。如果 ZigBee 協調器或 ZigBee 路由器的 NLME 收到的 NLME-LEAVE.request 原語中 DeviceAddress 參數不爲空，NLME 將判定指定的設備是否存在于近鄰表中。如果被請求的設備不存在，NLME 就向上層發送狀態爲 UNKNOWN_DEVICE 的 NLME-LEAVE.confirm 原語。如果被請求的設備儲存在與近鄰表中，NLME 將嘗試使指定的設備離開網路。此時，如果 RemoveChildren 參數等於 TRUE，則該原語還要求被請求設備的子設備離開網路。每完成一次刪除子設備的操作，NLME 都向上層發送一個 NLME-LEAVE.confirmed 原語，證實原語中 DeviceAddress 參數等於刪除設備的 IEEE 位址，如果刪除子設備成功，則 Status 參數等於 SUCCESS，如果因爲任何原因導致刪除子設備失敗，則 Status 參數等於 LEAVE_UNCONFIRMED。同時，被請求設備還要把近鄰表中被刪除子設備對應記錄中的關係欄位設爲 0x03，表示沒有關係。

NLME-LEAVE.confirm 原語是對 NLME-LEAVE.request 原語的回應。它由 NLME 產生併發送給上層，向上層回饋其請求設備自身或另一個設備離開網路的結果。該原語的語法如下：

NLME-LEAVE.confirm（DeviceAddress，Status）

其中：參數 DeviceAddress 是請求原語意圖刪除設備的 64 位元 IEEE 位址；Status 表示相應請求的狀態，其取值爲 SUCCESS、INVALID_REQUEST、UNKNOWN_DEVICE 或 LEAVE_UNCONFIRM。

NLME-LEAVE.indication 原語允許 ZigBee 設備被父設備從網路中刪除時能夠通知給上層。另外，一個 ZigBee 設備透過解關聯離開網路時，可以透過該指示原語通知給設備關聯的 ZigBee 路由器或 ZigBee 協調器的上層。該原語的語法如下：

NLME-LEAVE.indication（DeviceAddress）

其唯一參數 DeviceAddress 值如果爲空，則表示發送原語的設備自身被其父設備刪除；否則 DeviceAddress 參數就表示離開網路的設備的 64 位元 IEEE 位址。

2.2.2.7 設備重定

網路層重定請求原語 NLME-RESET.request 允許設備上層請求 NLME 執行重定操作。這是一個不含參數的原因，其語法如下：

NLME-RESET.request（）

NLME 接收到上層的復位請求後，也向 MAC 子層發送復位請求 MLME-RESET.request，其參數 SetDefaultPIB 設爲 TRUE。NEK 層在收到 MAC 層的復位證實原語 MLME-RESET.confirm 後，也對 NEK 層進行復位，即清除所有內部變數和路由發現表記錄，並把所有 NIB 屬性設爲預設值。如果 MAC 層復位成功並且 NWK 層復位成功，NLME 就向上層發送狀態爲 SUCCESS 的證實原語 NLME-RESET.confirm；否則，證實原語狀態參數值爲 DISABLE_TRX_FAILURE。

NLME-RESET.confirmed 原語是對 NLME-RESET.request 原語的回應，它由 NLME 發送給上層，以告知其請求重定網路層的結果。該原語的語法如下：

NLME-RESET.confirm（Status）

其唯一參數 Status 表示復位操作的結果，參數值等於 MAC 復位確認原語 MLME-RESET.confirm 返回的狀態值。網路層重定的資訊流程如圖 8 所示。

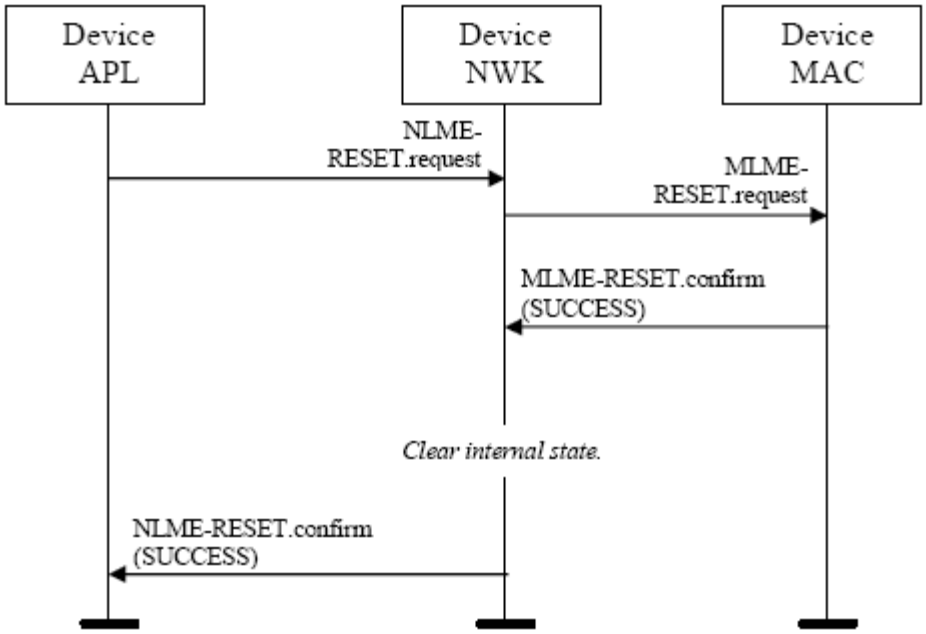


圖 8 網路層重定的資訊流程

2.2.2.8 接收機同步

網路層同步請求原語 NLME-SYNC.request 定義設備的 APL 層如何與 ZigBee 協調器或路由器同步，以及如何從 ZigBee 協調器或路由器提取待接收的資料。每當 APL 層要與 ZigBee 協調器或路由器同步，或檢查是否有資料需要接收時，就向 NLME 發送同步請求原語。該原語的語法如下：

NLME-SYNC.request（Track）

其唯一參數 Track 的取值決定是否要維持與信標的同步。如果 Track 參數值爲 FALSE 並且設備工作在非信標的網路中，NLME 就向 MAC 子層發送請求原語 MLME-POLL.request。接收到 MLME-POLL。confirmed 證實原語後，如果 MAC 請求原語成功，NLME 就向上層發送 Status 參數值爲 SUCCESS 的 NLME-SYNC.confirm；否則，Status 參數值爲 SYNC_FAILURE。如果 Track 參數值爲 FALSE 並且設備工作在信標網路中，NLME 將手心調用 MLME-SET.request 原語吧 MAC PIB 屬性 macAutoRequest 設爲 TRUE；再向 MAC 層發送 TrackBeacon 參數設爲 FALSE 的同步請求原語 MLME-SYNC.request；最後，NLME 才向上層發送 Status 參數 SUCCESS 的網路層同步證實原語 NLME-SYNC.confirm。如果 Track 參數值爲 TRUE 並且設備工作在非信標的網路中，NLME 將直接向上層返回一個狀態爲 INVALID_PARAMETER 的證實原語 NLME-SYNC.confirm。如果 Track 參數值爲 TRUE 並且設備工作在信標網路中，NLME 將首先調用 MLME-SET.request 原語把 MAC PIB 屬性 macAutoRequest 設爲 TRUE；再向 MAC 層發送 TrackBeacon 參數設爲 TRUE 的同步請求原語 MLME-SYNC.request；最後，NLME 才向上層發送 Status 參數爲 SUCCESS 的網路層同步證實原語 NLME-SYNC.confirm。

證實原語 NLME-SYNC.confirm 是對請求原語 NLME-SYNC.request 的回應，它由 NLME

層發送給上層，用以報告其請求同步或從 ZigBee 協調器或路由器提取資料的結果。該原語的語法如下：

NLME-SYNC.confirm（Status）

其唯一參數 Status 表示請求同步的結果，取值爲 SUCCESS、SYNC_FAILURE 或 INVALID_PARAMETER。各狀態值對應的條件在請求原語中有詳細的介紹。圖 9 和 10 分別是非信標網路和信標網路中的設備成功同步到 ZigBee 協調器的資訊流程。

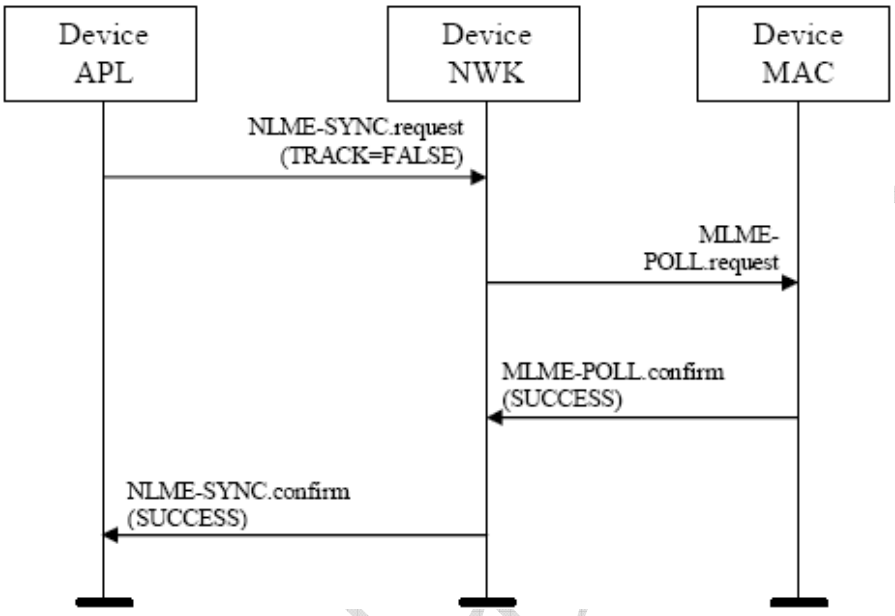


圖 9 無信標網路中設備同步到 ZigBee 協調器的流程

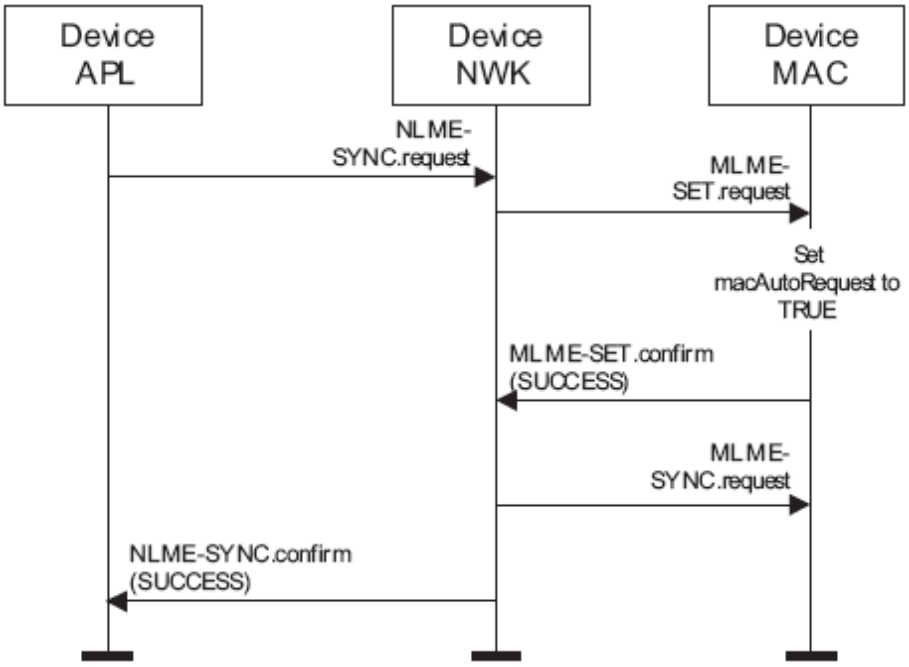


圖 10 信標網路中設備同步到 ZigBee 協調器的流程

網路層同步指示原語NLME-SYNC.indication用來把MAC層失步的資訊通知給APL層。當 NLME 收到來自 MAC 層的失步指示原語 MLME-SYNC-LOSE.indication 中的參數 LossReason 等於 BEACON_LOST 時，就向上層發送 NLME-SYNC.indication 原語。該原語的語法如下：

NLME-SYNC.indication（）

2.2.2.9 NIB 維護

NLME-GET.request 原語允許 APL 層讀取 NIB 屬性值。該原語的語法爲：

NLME-GET.request（NIBAttribute）

其唯一參數 NIBAttribute 表示要讀取的 NIB 屬性的標識碼。NLME 收到 NLME-GET.request 原語後就到資料庫中檢索要讀取的 NIB 屬性。如果在資料庫中找不到要讀取 NIB 屬性的標識碼，NLME 就向上層發送狀態爲 UNSUPPORTED_ATTRIBUTE 的證實原語 NLME-GET.confirm。如果在資料庫中成功找到了要讀取的 NIB 屬性，NLME 就向上層發送狀態爲 SUCCESS 的 NLME-GET.confirm 原語，並返回 NIB 屬性標識碼和屬性值。

NLME-GET.confirm 原語是對 NLME-GET.request 原語的回應，NLME 用它向上層報告請求讀取 NIB 屬性的結果。該原語的語法如下：

NLME-GET.confirm（Status，NIBAttribute，NIBAttributeLength，NIBAttributeValue）

其中：參數 Status 表示請求讀取 NIB 屬性值的結果，其取值爲 SUCCESS 或 UNSUPPORTED_ATTRIBUTE ； NIBAttribute 是讀取的 NIB 屬性的標識碼 ； NIBAttributeLength 表示返回的 NIB 屬性值的位元組數；NIBAttributeValue 表示讀取的 NIB 屬性值。

NLME-SET.request 原語允許 APL;層設置 NIB 屬性值。該原語的語法爲：

NLME-SET.request（NIBAttribute，NIBAttributeLength，NIBAttributeValue）

其中：參數 NIBAttribute 是要設置的 NIB 屬性的標識碼；NIBAttributeLength 表示要設置的 NIB 屬性值的位元組數；NIBAttributeValue 表示設置的 NIB 屬性值。NLME 收到 NLME-SET.request 原語後就嘗試把給定的值寫入到資料庫中對應的 NIB 屬性。如果在資料庫中找不到 NIBAttribute 參數指定的屬性，NLME 就向上層發送狀態爲 UNSUPPORTED_ATTRIBUTE 的證實原語 NLME-SET.confirm。如果 NIBAttributeValue 參數的值超出了要設置的 NIB 屬性有效範圍，NLME 就向上層發送狀態爲 INVALID_PARAMETER 的 NLME-SET.confirm 原語。如果成功設置了指定 NIB 屬性的值，NLME 向上層發送的 NLME-SET.confirmed 原語的狀態就爲 SUCCESS。

NLME-SET.confirm 原語是對 NLME-SET.request 原語的回應，NLME 用它向上層報告請求設置 NIB 屬性的結果。該原語的語法如下：

NLME-SET.confirmed（Status，NIBAttribute）

其中：參數 Status 表示請求設置 NIB 屬性的結果，其取值爲 SUCCESS、INVALID_PARAMETER 或 UNSUPPORTED_ATTRIBUTE ;NIBAttribute 是設置的 NIB 屬性的標識碼。

2.3 網路層訊框(Frame)格式

2.3.1 NWK 訊框(Frame)的一般格式

一個 NWK 訊框(Frame)（即 NPDU）由兩個基本部分組成：NWK 頭和 NWK 有效負載。NWK 頭部分包含訊框(Frame)控制、位址和序號資訊；NWK 有效負載部分包含的資訊因訊框(Frame)類型的不同而不同，它是可變長度的。NWK 頭中欄位按固定的順序排列，但不是每個 NWK 訊框(Frame)都包含完整的位址和序號資訊欄位。NWK 訊框(Frame)的一般格式如下：

<table>
<tr><td>位元組數：2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>可變長度</td></tr>
<tr><td rowspan="2">訊框(Frame)控制</td><td>目的位址</td><td>來源位址</td><td>半徑</td><td>序號</td><td>訊框(Frame)有效載荷</td></tr>
<tr><td colspan="4">路由欄位</td><td></td></tr>
<tr><td colspan="5">NWK 頭</td><td>NWK 有效載荷</td></tr>
</table>

訊框(Frame)頭部分的**訊框(Frame)控制**欄位長度爲 16 位，各子域的劃分如下：

比特位:0～1	2～5	6～7	8	9	10～15
訊框(Frame)類型	協定版本	發現路由	預留	安全	預留

其中**訊框(Frame)類型**子域占 2 位，取值 00 表示 NWK 資料訊框(Frame)，01 表示 NWK 命令訊框(Frame)。**協定版本**子域占 4 位元，表示的是設備使用的 ZigBee NWK 協定版本。一個設備使用的協定版本可以從 NWK 常量 nwkcProtocolVersion 中得到。**發現路由**子域占 2 位，用來控制發送訊框(Frame)時的路由發現操作，00 表示禁止路由發現，01 表示致能路由發現，10 表示強制路由發現。**安全**子域佔 1 位元，並且僅當該訊框(Frame)需執行 NWK 層安全操作時，安全子域置爲 1；如果該訊框(Frame)在其他層執行安全操作或完全不使用安全操作，則安全子域置爲 0。

訊框(Frame)頭部分的**目的位址**欄位在訊框(Frame)結構中總是存在的。它的長度是 2 位元組，包含的是目的設備的 16 位元網路位址或廣播位址 0xffff。設備網路位址總是與 IEEE 802.15.4-2003 的 MAC 短位址相同。

訊框(Frame)頭部分的**源位址**欄位在訊框(Frame)結構中總是存在的。它的長度是 2 位元組，包含的是該訊框(Frame)源設備的 16 位元網路位址。設備網路位址總是與 IEEE 802.15.4-2003 的 MAC 短位址相同。

訊框(Frame)頭部分的**半徑**欄位在訊框(Frame)結構中總是存在的，它的長度是 1 位元組，指定了訊框(Frame)傳輸的範圍。每個接收設備都把該欄位的值減 1.

訊框(Frame)頭部分的**序號**欄位在每個訊框(Frame)中都是存在的，它的長度是 1 位元組。設備每發送一個新的訊框(Frame)就把序號值加 1，序號欄位和源位址欄位的一對值可以唯一確定一個訊框(Frame)。

2.3.2 特定 NWK 訊框(Frame)的格式

NWK 層定義了兩種類型的訊框(Frame)：資料訊框(Frame)和命令訊框(Frame)。

NWK 資料訊框(Frame)的格式如下：

位元組數：2	6	可變長度
訊框(Frame)控制	路由訊息	資料有效載荷
NWK 頭		NWK 有效載荷

NWK 資料訊框(Frame)中各欄位的排列順序與一般 NWK 訊框(Frame)格式相同。資料訊框(Frame)頭部分的**訊框(Frame)控制**欄位中，訊框(Frame)類型子域的值爲 00，其他子域根據資料訊框(Frame)的具體應用情況來設置。**路由資訊**部分包含的是位址和廣播欄位的適當組合，這些欄位的設置與訊框(Frame)控制欄位有關。資料有效載荷欄位包含的是上層要求 NWK 發送的一串位元組。

NWK 命令訊框(Frame)的格式如下：

位元組數：2	6	1	可變長度
訊框(Frame)控制	路由訊息	NWK 命令標識	NWK 命令有效載荷
NWK 頭		NWK 有效載荷	

NWK 命令訊框(Frame)中各欄位的排列順序與一般 NWK 訊框(Frame)中欄位的排列一致。NWK 命令訊框(Frame)頭的**訊框(Frame)控制**欄位中訊框(Frame)類型子域的值爲 01，其他子域根據 NWK 命令訊框(Frame)的具體應用來設置。NWK 頭的**路由資訊**部分是多個位址和廣播欄位的適當組合，它們與訊框(Frame)控制欄位的設置有關。

NWK 命令訊框(Frame)的有效負載部分包括 NWK 命令標識和 NWK 命令有效負載兩個欄位。**NWK 命令標識**欄位長度是 1 位元組，表示正使用的 NWK 命令名稱。命令標識 0x01 表示路由請求命令，0x02 表示路由應答命令，0x03 表示路由錯誤命令，0x04 表示離開網路命令。**NWK 命令有效載荷**部分則是當前命令的具體內容。

2.4 網路層命令訊框(Frame)

NWK 命令標識 0x01 表示路由請求命令，它允許發送該命令的設備請求其無線覆蓋範圍的其他設備針對一個特定的目的設備執行路由搜索，在網路中建立狀態資訊以使得訊息能夠更方便快捷地傳遞到目的設備。路由請求命令訊框(Frame)的有效載荷部分如下：

位元組數：1	1	1	2	1

命令訊框(Frame)標識	命令選項	路由請求標識	目的位址	路徑成本
NWK 有效載荷				

使用 NWK 資料服務發送 NWK 路由請求命令時，MAC 訊框(Frame)頭要作如下設置：

目的 PAN 標識應設置爲發送路由請求命令的設備的 PAN 標識；目的位址設置爲廣播位址 0xffff；源 MAC 位址和源 PAN 標識應設置爲發送路由請求命令的設備位址和 PAN 標識，該設備可能並不是路由請求命令的原始發起設備，而是轉發設備；訊框(Frame)控制欄位的設置應指定爲該訊框(Frame)爲 MAC 資料訊框(Frame)並禁止 MAC 安全處理，因爲 NWK 層發起的任何安全訊框(Frame)都應採用 NWK 層安全處理。由於該訊框(Frame)是廣播訊框(Frame)，所以應設定爲不需確認。位址模式和 PAN 內標誌位元應根據位址欄位的情況設置。

爲了發送路由請求命令訊框(Frame)，NWK 訊框(Frame)頭部分的源位址欄位應設爲命令發起設備的位址。NWK 訊框(Frame)頭部分的目的位址應設爲廣播位址。路由請求命令訊框(Frame)的有效負載部分包含命令訊框(Frame)標識欄位、命令選項欄位、路由請求標識欄位、目的位址欄位和路徑成本。其中，**命令訊框(Frame)標識**欄位應設爲 0x01 以指示爲路由請求命令訊框(Frame)；**命令選項**欄位長度是 1 位元組，前 7 位元預留，最後 1 位是路由修復子域。並且僅當該路由請求命令是 MESH 網路拓撲路由修復操作的一部分時，路由修復才設爲 1。**路由請求標識**是一個 8 位元的路由請求序號，一個特定設備的 NWK 層每發出一個路由請求命令，路由請求序號就加 1。**目的位址**欄位是 2 位元組長度的位址，表示該路由請求命令意圖搜索到該目的位址的路由。**路徑成本**欄位長度是一位元組，它用來累計路由請求命令訊框(Frame)在網路中傳遞的路由成本資訊。

NWK 命令表示 0x02 表示路由應答命令，它允許路由請求命令指定的目的設備在收到請求時通知路由請求的發起設備；它還允許路由請求命令經過路徑上的 ZigBee 路由器建立狀態資訊，以使得從源設備向目的設備發送資料訊框(Frame)時更加高效。路由應答命令的有效負載格式如下：

位元組數：1	1	1	2	2	1
命令訊框(Frame)標識	命令選項	路由請求標識	原始位址	回應位址	路徑成本
NWK 有效載荷					

使用 MAC 資料服務發送 NWK 路由應答命令時，MAC 訊框(Frame)頭要做如下設置：

目的 MAC 位址和目的 PAN 標識應分別設置爲返回到相應的路由請求命令訊框(Frame)發起設備路徑中第一跳的網路位址和 PAN 標識，該目的 PAN 標識應與回應路由請求命令發起設備的 PAN 標識相同。源 MAC 位址和源 PAN 標識應分別設置爲發送路由應答命令設備的位址和 PAN 標識，該發送設備不一定是路由應答命令的發起設備，而只是轉發設備。訊框(Frame)控制欄位的設置應制定該訊框(Frame)爲 MAC 資料訊框(Frame)並禁止 MAC 安全處理，因爲 NWK 層發起的任何安全訊框(Frame)都應採用 NWK 層安全處理。在 MAC 訊框(Frame)的發送選項中應指定該訊框(Frame)要求確認。位址模式和 PAN 內標誌位元應支援位址欄位的相應設置。

爲了使路由應答到達目的設備並正確完成路由發現過程，NWK 訊框(Frame)頭部分必須提供以下資訊。NWK 訊框(Frame)控制欄位中訊框(Frame)類型子域應設爲 01，表示該訊框

(Frame)是 NWK 層命令訊框(Frame)。NWK 訊框(Frame)頭部分的目的位址欄位應設置爲路由應答設備返回到相應請求發起設備的路徑中第一跳的網路位址。NWK 訊框(Frame)頭部分的源位址欄位則應設爲該訊框(Frame)當前發送設備的 16 位元網路位址。路由應答命令訊框(Frame)的有效負載部分包含命令訊框(Frame)標識欄位、命令選項欄位、路由請求標識欄位、路由請求發起設備位址和應答設備位址、路徑成本。其中**命令訊框(Frame)標識**欄位應設爲 0x02，以指示爲路由應答命令訊框(Frame)；**命令選項**欄位長度是 1 位元組，前 7 位元預留，最後 1 位是路由修復子域。並且僅當該路由請求命令是 MESH 網路拓撲路由修復操作的一部分時，路由修復才設爲 1。**路由請求標識**欄位應設置爲相應的路由請求命令訊框(Frame)中路由請求標識值。**發起設備位址**欄位長度是 2 位元組，它包含的是該訊框(Frame)正在應答的路由請求命令發起設備的 16 位元網路位址。**應答設備位址**欄位長度是 2 位元組，當前路由請求和應答過程就是爲了發現該設備的路由，該欄位的值總是與相應的路由請求命令訊框(Frame)有效負載部分的目的位址欄位的值相同。**路徑成本**欄位用來累計路由應答命令訊框(Frame)在網路中傳遞時的總鏈路成本。

當設備不能完成資料訊框(Frame)的轉發時，它就用路由錯誤命令來通知資料訊框(Frame)的源設備，告知資料訊框(Frame)轉發失敗資訊。路由錯誤命令訊框(Frame)的有效負載格式如下：

位元組數：1	1	2
命令訊框(Frame)標識	錯誤程式	目的位址

使用 MAC 資料服務發送 NWK 路由錯誤命令時，MAC 訊框(Frame)頭要做如下設置：

目的 MAC 位址和目的 PAN 標識應分別設爲從遭遇轉發失敗的設備返回到資料訊框(Frame)源設備的路徑中第一跳的位址和 PAN 標識。源 MAC 位址和源 PAN 標識應設爲發送路由錯誤命令設備的位址和 PAN 標識。訊框(Frame)控制欄位的設置應制定該訊框(Frame)爲 MAC 資料訊框(Frame)並禁止 MAC 安全處理，因爲 NWK 層發起的任何安全訊框(Frame)都應採用 NWK 層安全處理。至於該訊框(Frame)是否要求確認則由實現者來決定。位址模式和 PAN 內標誌位元應支援位址欄位的相應設置。

爲了發送路由錯誤命令訊框(Frame)，NWK 訊框(Frame)頭部分的目的位址欄位應設爲遭遇轉發失敗的資料訊框(Frame)的源位址欄位值。NWK 訊框(Frame)頭部分的源位址欄位則應設爲路由錯誤命令發送設備的位址。NWK 路由錯誤命令訊框(Frame)有效負載部分的錯誤程式欄位根據發生錯誤的具體原因設置爲表 16 中不同的值。有效負載部分的目的位址欄位長度是 2 位元組，它包含的是遭遇轉發失敗的資料訊框(Frame)意圖指向的轉發位址。

表 16 路由錯誤程式及錯誤原因

數　值	錯誤
0x00	無路由可用
0x01	樹狀鏈路失敗
0x02	非樹狀鏈路失敗
0x03	電池電壓低
0x04	無路由能力
0x05～0xff	預留

一個設備離開網路時，NLME 用 NWK 離開命令來通知其父設備和子設備；另外設備還

可以使用離開命令來請求另外一個設備離開網路。NWK 離開命令的有效負載部分格式如下：

位元組數：1	1
命令訊框(Frame)標識	命令選項

使用 MAC 資料服務發送 NWK 離開命令時，MAC 訊框(Frame)頭要做如下設置：

目的 MAC 位址和目的 PAN 標識應分別設爲該訊框(Frame)指向的近鄰設備的位址和 PAN 標識。源 MAC 位址和源 PAN 標識應設爲發送離開命令的設備位址和 PAN 標識。訊框(Frame)控制欄位的設置應制定該訊框(Frame)爲 MAC 資料訊框(Frame)並禁止 MAC 安全處理，因爲 NWK 層發起的任何安全訊框(Frame)都應採用 NWK 層安全處理。該 MAC 訊框(Frame)應設置爲要求確認。位址模式和 PAN 內標誌位元應支援位址欄位的相應設置。

爲了發送離開命令訊框(Frame)，NWK 訊框(Frame)頭部分的目的位址欄位應設爲該 NWK 訊框(Frame)指向的近鄰設備的網路位址。NWK 訊框(Frame)頭部分的源位址欄位則應設爲離開命令發送設備的位址。NWK 訊框(Frame)頭中的半徑欄位應設爲 1。NWK 離開命令訊框(Frame)有效負載部分的命令選項欄位格式如下：

比特位：0～5	6	7
預留	請求/指示	刪除子設備

其中**請求/指示**子域長度是 1 位，該子域取值爲 1，表示離開命令請求另一個設備離開網路；該子域取值爲 0，則指示離開命令的發送設備計畫離開網路。**刪除子設備**子域長度是 1 位，其值是 1，表示離開網路設備的子設備也要離開網路。

2.5 網路層功能詳述

2.5.1 網路和設備維護

所有 ZigBee 設備都應具有兩個最基本的功能，即加入網路和離開網路。ZigBee 協調器和 ZigBee 路由器還應提供如下功能：允許設備加入網路，允許設備離開網路，參與分配邏輯網路位址，維護近鄰設備列表。其中允許設備加入/離開網路功能支援兩種實現方式：一種是根據 MAC 層的關聯/解關聯指示；另一種是根據應用層的直接加入/離開請求。此外，ZigBee 協調器還應具備建立一個新網路的功能。

2.5.1.1 建立新網路

建立新網路的過程是透過使用 NLME-NETWORK-FORMATION.request 原語來初始化的。只有能夠擔當 ZigBee 協調器的、尚未加入到網路中的全功能設備才能嘗試建立一個新網路。如果在任何其他 ZigBee 設備上初始化建立新網路過程，NLME 將終止該過程並通知上層 — 這是一個非法的請求，即 NLME 向上層發送一個 Status 參數值爲 INVALID_REQUEST 的證實原語 NLME-NETWORK-FORMATION.confirm。

當設備 NLME 收到 NLME-NETWORK-FORMATION.request 請求原語有效時，NLME 將首先請求 MAC 子層在一組指定的通道或預設的所有通道上執行能量檢測掃描，搜索可能存在的干擾 此時的通道掃描由 NLME 向 MAC 子層發送掃描請求原語 MLME-SCAN.request 來實現，其中 ScanType 參數設爲能量檢測掃描。通道掃描結果透過 MLME-SCAN.confirm 證實原語回饋給 NLME。接收到成功的能量檢測通道掃描結果後，NLME 將根據能量遞增的順序對通道排序並剔出其中能量強度不符合要求的通道。然後，NLME 在剩下的通道上執行主動掃描來搜索其他 ZigBee 設備。此時 NLME 向 MAC 子層發送的 MLME-SCAN.request 原語中 ScanType 參數設爲主動掃描，ChannelList 參數設爲能量強度滿足要求的一組通道。爲了找到最適合建立新網路的通道，NLME 將檢索主動掃描返回的 PAN 描述符，找到其中現存網路最少的第一個通道作爲建立的新網路的工作通道。如果找不到合適的通道，NLME 將中止建立新網路的過程並通知上層：建立新網路失敗。這是透過向應用層發送 Status 參數值爲 STARTUP_FAILURE 的 NLME-NETWORK-FORMATION.confirm 原語來實現的。如果找到一個合適的通道，NLME 將爲新網路選擇一個 PAN 標識。在決定新網路的 PAN 標識時，首先檢查 NLME-NETWORK-FORMATION.request 原語中的可選參數 PANId 是否指定了 PAN 標識。如果建立網路的請求原語中指定了 PAN 標識並且與現存網路的 PAN 標識不衝突，那麼 PANId 的值就是新網路的 PAN 標識；否則，設備將隨機選擇一個 PAN 標識，只要它不是廣播 PAN 標識 0xffff 並且在選定通道上的網路是唯一的。另外，PAN 標識不得大於 0x3fff，因爲 16 位元 PAN 標識的最高 2 個有效位預留給將來使用的。一旦 NLME 選定了 PAN 標識，就透過 MLME-SET.request 原語把 MAC 層屬性 macPANID 設爲選定的 PAN 標識。如果沒有唯一的 PAN 標識可選，NLME 將中止建立新網路的過程並通知上層：建立新網路失敗。這也是透過向應用層發送 Status 參數值爲 STARTUP_FAILURE 的 NLME-NETWORK-FORMATION.confirm 原語來實現的。選定 PAN 標識後，NLME 將選擇 16 位網路位址 0x0000 作爲 ZigBee 協調器的位址，並將 MAC 層 PIB 屬性 macShortAddress 的值設爲 0x0000。選定網路位址後，NLME 將向 MAC 層發送 MLME-START.request 原語啓動新的 PAN。MLME-START.request 的參數根據 NLME-NETWORK-FORMATION.request 原語傳遞的參數進行設置，如通道掃描結果、選定的 PAN 標識等。PAN 啓動狀態透過 MLME-START.confirm 原語來回饋。NLME 接收到 PAN 啓動狀態後就向上層發送證實原語 NLME-NETWORK-FORMATION.confirm，把請求初始化 ZigBee 協調器的狀態通知給應用層，該證實原語的 Status 參數設爲 MAC 層返回原語的 MLME-START.confirm 中的狀態值。成功建立一個新網路的資訊流程如圖 11 所示。

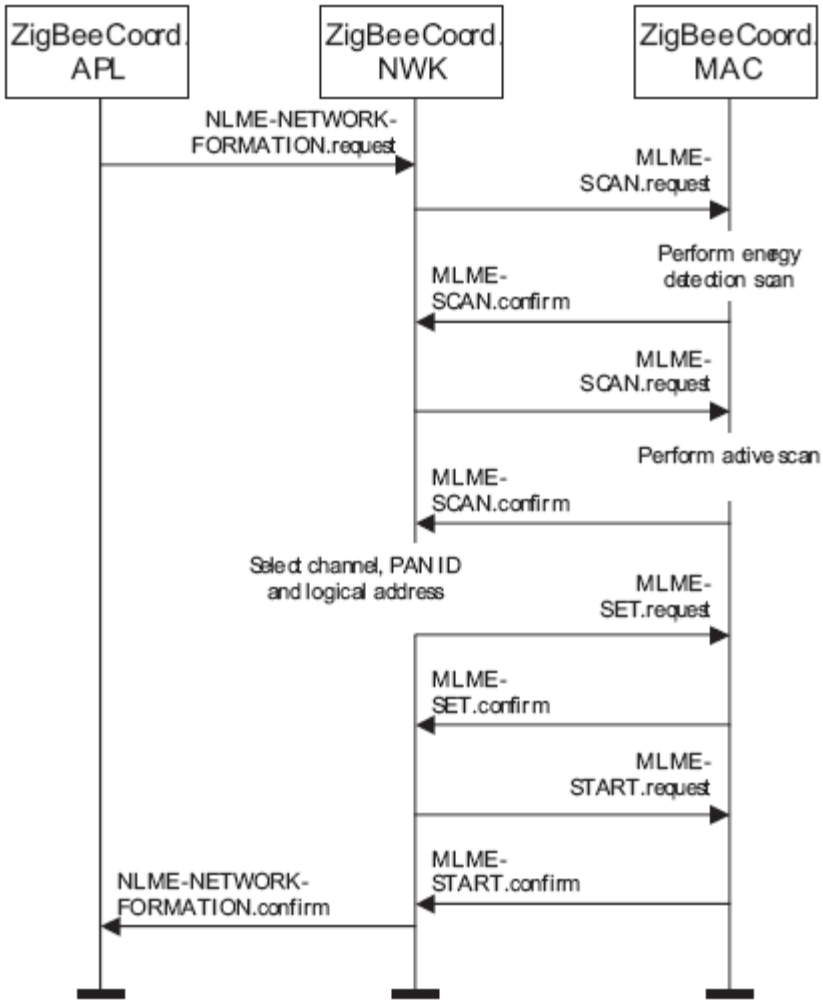


圖 11 ZigBee 協調器成功建立新網路的資訊流程

2.5.1.2 允許設備加入網路

允許設備加入網路的過程是透過 NLME-PERMIT-JOINING.request 原語來初始化。只有 ZigBee 協調器或 ZigBee 路由器才能夠允許其他設備加入網路。如果允許設備加入網路過程初始化發生在一個 ZigBee 終端設備上，設備 NLME 將中止該過程。如果 NLME-PERMIT-JOINING.request 原語中 PermitDuration 參數爲 0x00，NLME 將調用 MAC 屬性設置原語 MLME-SET.request，把 MAC PIB 屬性 macAssociationPermit 設爲 FALSE。如果 NLME-PERMIT-JOINING.request 原語中 PermitDuration 參數爲 0x01～0xfe 之間的值，NLME 將把 MAC PIB 屬性 macAssociationPermit 設爲 TRUE 並啓動一個計時週期爲 PermitDuration 的計時器，計時期滿後，NLME 再把屬性 macAssociationPermit 設爲 FALSE。如果 NLME-PERMIT-JOINING.request 原語中 PermitDuration 參數爲 0xff，NLME 將把 MAC PIB 屬性 macAssociationPermit 設爲 TRUE 並且不限時，除非再次收到 NLME-PERMIT-JOINING.request 才會重新設置 macAssociationPermit 屬性值。ZigBee 協調器或 ZigBee 路由器在有限時段內允許設備加入網路的資訊流程如圖 12 所示。

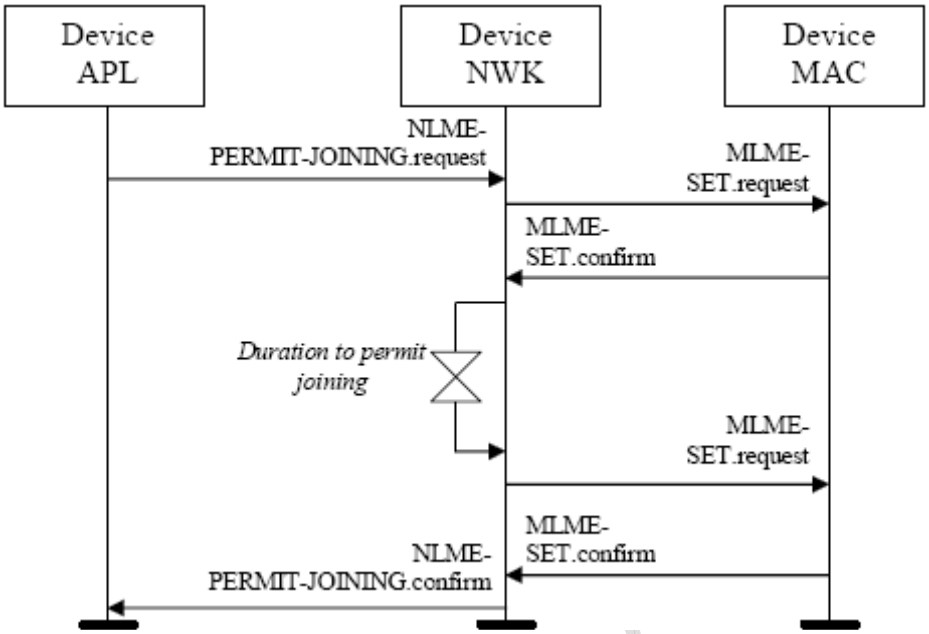


圖 12 ZigBee 協調器或路由器限時允許設備加入網路的資訊流程

2.5.1.3 設備入網

當網路中的設備允許一個新設備加入網路時，這兩個設備就構成了父子關係。新加入的設備是子設備，而第一個設備是父設備。一個子設備可以透過下面兩種方式加入網路：透過 MAC 層關聯過程加入網路或由先前指定的父設備直接加入網路。只有 ZigBee 協調器或 ZigBee 路由器能夠允許設備加入網路，而 ZigBee 終端設備則不能。

子設備透過 MAC 層關聯加入網路的過程是透過向 NWK 層發送 NLME-NETWORK-DISCOVERY.request 原語來初始化的。該請求原語中 ScanChannels 參數指定了網路發現過程中要掃描的通道列表，Scanduration 參數指定了掃描每個通道花費的時間。NWK 層收到網路發現請求原語後，就向 MAC 子層發送 MLME-SCAN.request 原語，請求 MAC 層執行被動掃描或主動掃描。在掃描過程中，每接收到一個有效負載長度非零的信標訊框 (Frame)，掃描設備的 MAC 層就向 NLME 發送一個 MLME-BEACON-NOTIFY.indication 指示原語。該指示原語中包含的資訊由信標設備位址資訊、是否允許關聯以及信標有效負載等。掃描設備的 NLME 將檢查信標有效負載中的協定 ID 欄位，看它是否與自身的 ZigBee 協定標識匹配。如果不匹配，該信標就被忽略；如果匹配，掃描設備就把接收信標中的相關資訊拷貝到近鄰表中。當 MAC 層完成掃描想 NLME 發送 MLME-SCAN.confirm 原語後，NWK 層就向其上層發送 NLME-NETWORK-DISCOVERY.confirm 原語，把偵聽到的每個網路的描述資訊傳遞給應用層。每個網路描述資訊包括 ZigBee 版本、協定堆疊配置檔、PAN ID、邏輯通道以及是否允許加入網路等。接收到 NLME-NETWORK-DISCOVERY.confirm 原語後，應用層就獲知了設備鄰近區域記憶體在網路的資訊。如果要從中選擇一個網路加入，設備應用層就向 NLME 發送 NLME-JOIN.request 原語，原語中 PANId 參數設置爲選定網路的 PAN 標識，RejoinNetwork 參數設置爲 FALSE，JoinAsRouter 參數則根據加入網路的設備是否是路由設備來設置。只有尚未加入網路的設備才能初始化透過 MAC 關聯加入網路的過程，任何其他

設備初始化該過程時，NLME 將中止該過程並告知其上層。這是透過向上層發送 Status 參數爲 INVALID_REQUEST 的證實原語 NLME-JOIN.confirm 來實現的。一個尚未加入網路的設備 NWK 層收到 NLME-JOIN.request 原語後，將從近鄰表中搜索合適的父設備。一個合適的父設備應有期望的 PAN ID，應允許關聯並且鏈路成本至多爲 3.如果近鄰表記錄中有潛在父設備欄位，則該欄位的值也應爲 1.如果近鄰表中沒有合適的父設備，NLME 就向上層發送狀態參數爲 NOT_PERMITTED 的 NLME-JOIN.confirm 原語。如果近鄰表中有多個設備可以作爲父設備，則選擇其中與 ZigBee 協調器深度最小的設備爲父是設備。一旦確定了合適的父設備，NLME 就向 MAC 層發送 MLME-ASSOCIATE.request 原語。關聯狀態透過證實原語 MLME-ASSOCIATE.confirm 回饋給 NLME。如果透過關聯加入網路不成功，NWK 層收到的來自 MAC 層的 MLME-ASSOCIATE.confirm 原語中狀態參數將指示出失敗原因。如果狀態參數指示近鄰設備拒絕新設備加入，那麼意圖加入網路的設備應把近鄰表中該近鄰設備對應記錄中的潛在父設備欄位設爲 0，以防止 NWK 層再次發送關聯請求給這個拒絕關聯的近鄰設備。每次發送 MLME-SCAN.request 原語的時候，近鄰表中每個記錄的潛在父設備欄位都設爲 1.如果要加入網路的設備把 JoinAsRouter 參數設置爲 TRUE，但潛在的父設備不允許新的路由器關聯（如它關聯的路由器已經達到最大值 nwkMaxRouters），加入請求也會失敗。這種情況下，NLME-JOIN.confirm 原語中的狀態爲 NOT_PERMITTED。此時，子設備的應用層可以嘗試以終端設備加入網路，吧 NLME-JOIN.request 原語中的 JoinAsRouter 參數設置爲 FALSE。如果設備嘗試加入網路失敗，則 NWK 層將針對第二個設備重新初始化 MAC 層關聯過程。NWK 層將重複這個過程知道設備成功加入到 PAN 或嘗試了所有合適的父設備。如果設備不能成功加入到應用層指定的 PAN 中，NLME 將透過發送 NLME-JOIN.confirm 原語來中止加入網路的過程，此時，設備得不到有效的邏輯位址，不能在網路中發送資料。如果子設備成功加入到網路中，NWK 層收到 MLME-ASSOCIATE.confirm 原語中包含一個 16 位元的邏輯位址，子設備以後就可以使用該邏輯位址來通訊。子設備的 NWK 層還要設置相應近鄰表記錄中的 Relationship 欄位，指示該近鄰設備是它的父設備。如果設備試圖加入一個安全網路中成爲路由器，那麼它在發送信標之前需要等待父設備的認證。如果設備成功加入網路，並且收到上層發送 NLME-START-ROUTER.request 原語，設備 NWK 層就向 MAC 層發送 MLME-START.request 原語，設置超訊框(Frame)配置並在要求的時候開始發送信標訊框(Frame)。只有 BeaconOrder 參數不等於 15 時，路由器才發送信標訊框(Frame)。PANId、LogicalChannel、BeaconOrder 和 SuperframeOrder 參數都應設置爲其近鄰表中父設備對應記錄的值。PANCoordinator 和 CoorRealignment 參數都應設爲 FALSE。接收到 MLME-START.confirm 原語後，NWK 也向上層發送一個同樣狀態的 NLME-START-ROUTER.confirm 證實原語。子設備透過關聯加入網路的資訊流程如圖 13 所示。

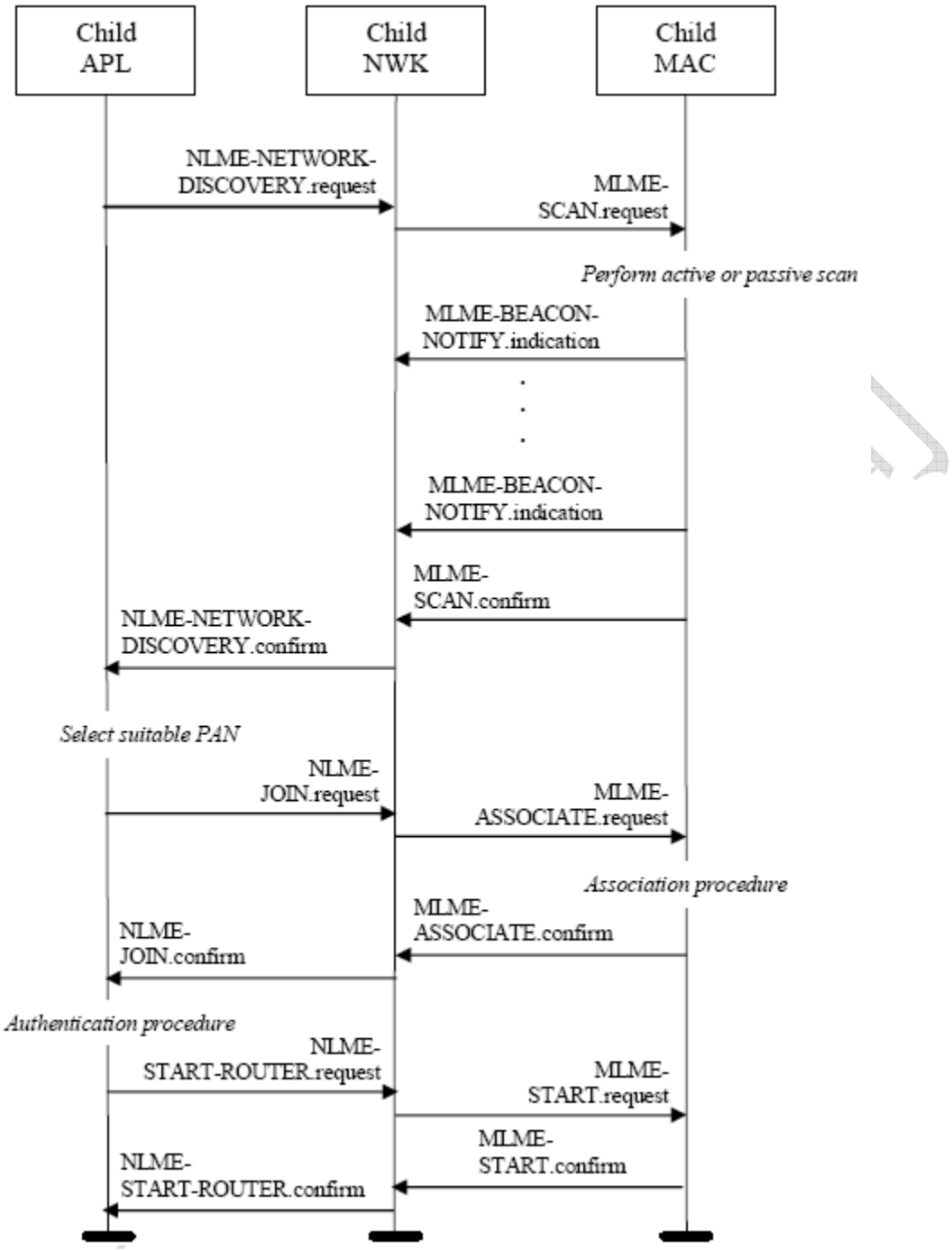


圖 13 子設備透過關聯加入網路的資訊流程

ZigBee 協調器或路由器透過 MAC 層關聯把一個設備加入到網路的過程是由 MAC 層指示原語 MLME-ASSOCIATE.indication 來初始化的。收到該指示原語後，潛在父設備的 NLME 首先判斷想加入的設備是否已經存在於網路中，即 NLME 搜索近鄰表看是否有有匹配的 64 位擴充位址。如果找到匹配的擴充位址，NLME 將獲得對應的 16 位網路位址並向 MAC 層發送關聯回應；如果找不到匹配的擴充位址，NLME 在可能的情況下將爲新設備分配一個唯一的 16 位網路位址。ZigBee 協調器爲每個潛在的父設備分配了有限的位址空間，一旦位址空間占滿，父設備就不接收入網請求了。如果潛在的父設備用盡了分配的位址空間，NLME

將中止設備加入網路的過程，並在隨後的 MLME-ASSOCIATE.response 回應原語中反映這一事實。如果潛在的父設備接受了新設備的入網請求，NLME 將在近鄰表中爲新加入的子設備增加一條記錄，記錄設備資訊，並向 MAC 層發送 MLME-ASSOCIATE.response 回應原語，指示關聯成功。回應傳輸到子設備的狀態透過 MLME-COMM-STATUS.indication 指示原語回饋給網路層。如果回應命令傳輸到子設備不成功，即 MLME-COMM-STATUS.indication 原語的狀態不是 SUCCESS，則 NLME 將中止設備加入網路的過程；如果回應命令傳輸成功，NLME 將向上層發送 NLME-JOIN.indication 原語，告知一個新設備已經加入到網路中。父設備接收入網請求的資訊流程如圖 14 所示。

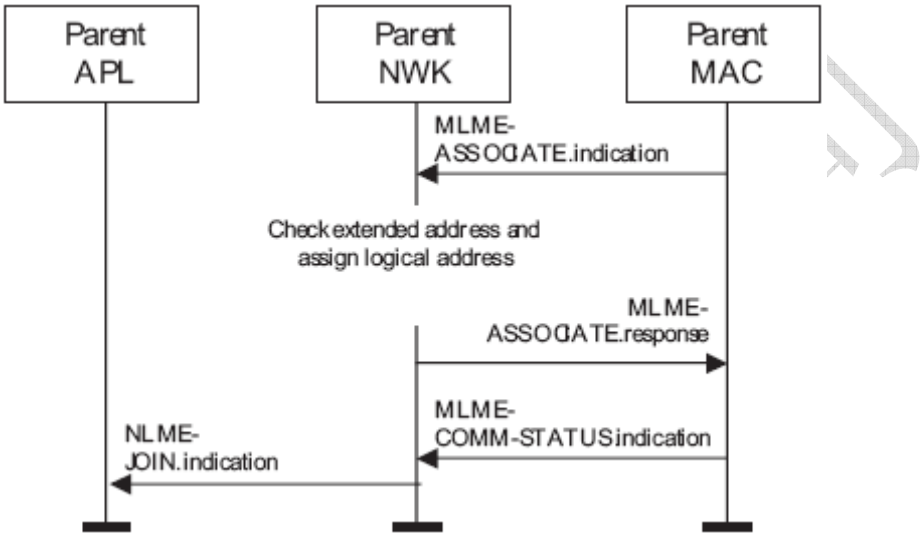


圖 14 父設備接收入網請求的資訊流程

ZigBee 協調器或路由器把設備直接加入到網路的過程透過 NLME-DIRECT-JOIN.request 原語來初始化，原語中 DeviceAddress 參數設爲將被加入到網路的設備位址。收到 NLME-DIRECT-JOIN.request 原語後，NLME 首先判斷指定的設備是否已經存在於網路中，這是透過搜索近鄰表判斷是否有匹配的 64 位擴充位址來實現的。如果找到匹配的位址，NLME 將中止該過程，並向上層發送 Status 參數爲 ALREADY_PRESENT 的證實原語 NLME-DIRECT-JOIN.confirm；如果找不到匹配的位址，NLME 在可能的情況下將爲新設備分配一個 16 位元網路位址。每個潛在父設備分到的位址空間是有限的，如果它有足夠的空間接受一個新設備，則它還要在近鄰表中增加一條新紀錄，記錄新設備的資訊。如果位址空間容量不夠，NLME 將中止該過程，向上層發送 Status 參數爲 TABLE_FULL 的 NLME-DIRECT-JOIN.confirm 原語。如果有足夠的空間，NLME 就向上層發送 Status 參數爲 SUCCESS 的證實原語 NLME-DIRECT-JOIN.confirm。ZigBee 協調器或 ZigBee 路由器把設備直接成功加入網路的過程如圖 15 所示。

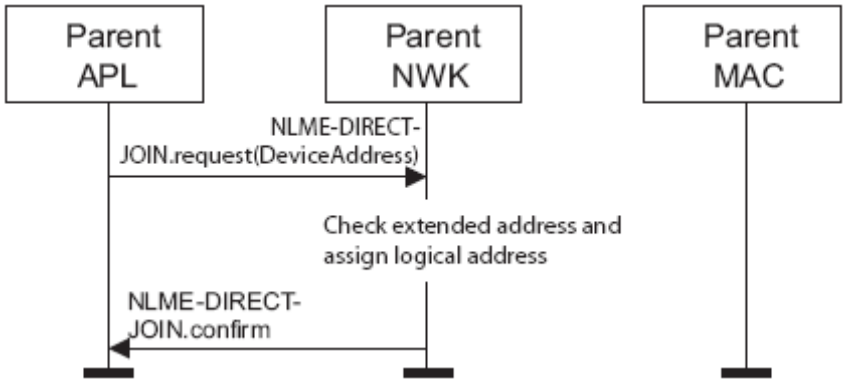


圖 15 ZigBee 協調器或路由器把設備直接加入網路的資訊流程

一個被直接加入到網路中的子設備爲了完成與父設備的關係建立，將啓動孤立申明過程，即子設備透過孤立申明加入網路；一個加入到網路中的子設備又與父設備失去聯繫時，要重新加入網路也要啓動孤立申明過程，即子設備透過孤立申明重新加入網路。子設備透過孤立申明加入網路的過程是透過 NLME-JOIN.request 原語來啓動的，原語中 RejoinNewwork 參數設爲 TRUE。收到來自上層的 NLME-JOIN.request 原語後，NLME 首先請求 MAC 子層執行在所有可用通道上的孤立掃描。NLME 向 MAC 層發送 MLME-SCAN.request 原語啓動孤立掃描,掃描結果透過 MLME-SCAN.confirm 原語回饋給 NLME。如果孤立掃描成功（即設備找到其父設備），NLME 將向上層發送 Status 參數爲 SUCCESS 的證實原語 NLME-JOIN.request，把設備加入或重新加入網路請求成功的訊息通知給上層。如果孤立掃描失敗，NLME 將中止請求入網過程，並向上層發送 Status 參數爲 NO_NETWORKS 的證實原語 NLME-JOIN.request，把設備沒有找到網路的訊息通知給上層。圖 16 是一個子設備透過孤立掃描加入或重新加入網路的資訊流程。

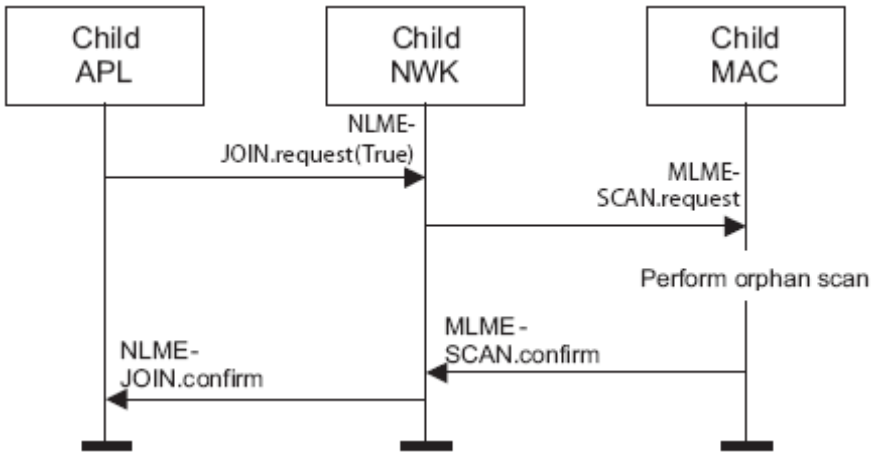


圖 16 子設備透過孤立掃描或重新加入網路的資訊流程

設備的 MAC 層向上層發送 MLME-ORPHAN.indication 原語告知一個孤立設備的存在。只有 ZigBee 協調器或 ZigBee 路由器才可以接受 MLME-ORPHAN.indication 原語，其他設備收到 MLME-ORPHAN.indication 原語時 NLME 將中止該過程。ZigBee 協調器或 ZigBee 路由器收到 MLME-ORPHAN.indication 原語後，首先判斷孤立設備是否是它的子設備。這個判斷過程是透過比較孤立設備與近鄰表中子設備的擴充位址來實現的。如果 ZigBee 協調

器或 ZigBee 路由器發現孤立設備是它的子設備，NLME 將獲取該子設備的 16 位元網路位址並透過孤立回應發送給 MAC 子層。孤立回應時透過向 MAC 層發送 MLME-ORPHAN.response 原語來實現的，孤立回應命令向子設備傳送的結果狀態透過 MLME-COMM-STATUS.indication 原語回饋給 NLME。如果 ZigBee 協調器或 ZigBee 路由器發現孤立設備不是它的子設備，NLME 就透過孤立回應原語把這一情況反映給 MAC 層。圖 17 是父設備把孤立的子設備加入或重新加入到網路過程的資訊流程。

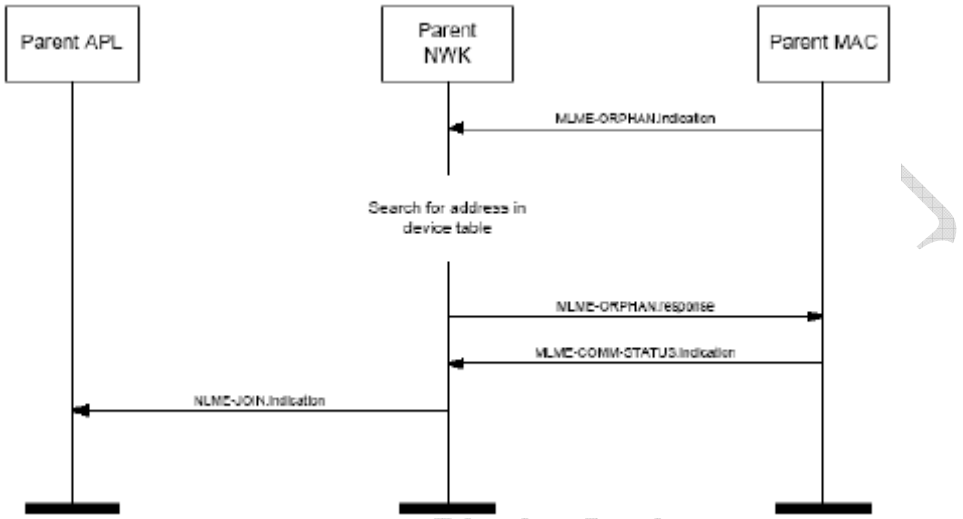


圖 17 父設備把孤立的子設備加入網路的資訊流程

設備的近鄰表包含了傳輸範圍內每個設備的資訊。近鄰表中儲存的資訊有多種用途，但並不是每個 ZigBee 設備運行時都要求下面提到的全部欄位。近鄰表中每個記錄應包含近鄰設備的下列資訊：PAN 標識、擴充位址（如果近鄰設備是父設備或子設備）、網路位址、設備類型、關係。另外，有些資訊不是近鄰表記錄中必須的欄位但具體實現時可以包含這些資訊：空閒時接收機開啓指示、任何近鄰設備的擴充位址、深度、信標階數、允許入網指示、發送失敗指示、潛在父設備指示、平均 LQI、邏輯通道、接收信標訊框(Frame)時間戳、信標發送時間偏移；近鄰表中甚至還可以包含近鄰設備的其他資訊。設備每次接收到近鄰設備的任何訊框(Frame)時，都要對近鄰表中相應的記錄進行更新。近鄰表中各資訊欄位的定義如下：

PAN 標識　近鄰設備的 16 位元 PAN 標識，其取值範圍是 0x0000～0x3FFF。這是每一個近鄰表記錄都必須包含的資訊。

擴充位址　每個設備唯一的 64 位元擴充位址。如果近鄰設備是該設備的父設備或子設備，就必須包含該欄位。

網路位址　近鄰設備的 16 位元網路位址，其取值範圍是 0x0000～0xFFFF。這是每一個近鄰表記錄都必須包含的資訊。

設備類型　近鄰設備的類型，0x00 表示 ZigBee 協調器，0x01 表示 ZigBee 路由器，0x02 表示 ZigBee 終端設備。這是每一個近鄰表記錄都必須包含的資訊。

關係　近鄰設備與當前設備之間的關係，0x00 表示近鄰設備是父設備，0x01 表示近鄰設備是子設備，0x02 表示近鄰設備是兄弟設備，0x03 表示其他關係。這是每一個近鄰表記錄都必須包含的資訊。

空閒時接收機開啓指示　指示近鄰設備的接收機在 CAP 的空閒期間是否開啓，TRUE

表示開啓，FALSE 表示關閉。如果近鄰設備是父設備或是 ZigBee 路由器/ZigBee 協調器的子設備，近鄰表記錄必須包含該欄位。

近鄰設備的擴充位址　近鄰設備的 64 位元擴充位址。這是近鄰表記錄中的可選欄位。

深度　近鄰設備在網路拓撲中的深度，即到 ZigBee 協調器的最小跳數，深度值 0x00 表示近鄰設備是 ZigBee 協調器。這是近鄰表記錄中的可選欄位。

信標階數　它指定了發送信標的頻率。這是近鄰表記錄中的可選欄位。

允許入網指示　指示近鄰設備是否接受其他設備的入網請求，TRUE 表示接受入網請求，FALSE 表示不接受入網請求。這是近鄰表記錄中的可選欄位。

發送失敗指示　其值指示此前向及您設備發送是否失敗，其取值爲 0x00～0xFF，值越大表示失敗次數越多。這是近鄰表記錄中的可選欄位。

潛在父設備指示　指示近鄰設備是否被指定爲一個潛在的父設備，0x00 表示近鄰設備不是潛在的父設備，0x01 表示近鄰設備是潛在的父設備。這是近鄰表記錄中的可選欄位。

平均 LQI　當前設備到近鄰設備的鏈路品質估計。這是近鄰表記錄中的可選欄位。

邏輯通道　近鄰設備工作使用的邏輯通道。這是近鄰表記錄中的可選欄位。

接收信標訊框(Frame)時間戳　設備接收到近鄰設備最近一個信標訊框(Frame)的時間（用符號數表示），這個值等於設備接收信標時打的時間戳，其取值範圍是 0x000000～0xFFFFFF。

信標發送時間偏移　近鄰設備發送信標和它的父設備發送信標之間的時間差(用符號表示)，設備用接收到近鄰設備信標時間戳減去這個時間差就可以計算出近鄰設備的父設備發送信標的時間。信標發送時間偏移的取值範圍是 0x000000～0xFFFFFF。

2.5.1.4 分散式位址分配機制

當 NIB 屬性 nwkUseTreeAlloc 的值等於 TRUE 時，ZigBee 網路採用分散式網路位址分配機制，即爲每一個潛在的父設備分配一個子段的網路位址。這些位址在一個特定的網路中是唯一的。它由父設備分配它的子設備。ZigBee 協調器規定網路中每個設備最多可接受的子設備數。在一個設備的所有子設備中，最多可以有 nwkMaxRouters 個具備路由器功能的設備，其餘的預留給 ZigBee 終端設備。每個設備有一個深度，它表示設備發送的訊框(Frame)只採用父子鏈路達到 ZigBee 協調器時需要的最小跳數。ZigBee 協調器自身的深度是 0，而它的子設備的深度是 1。多跳網路的最大深度大於 1，網路的最大深度也由 ZigBee 協調器來決定。給定父設備最多允許的子設備數 nwkMaxChildren（Cm）、網路最大深度 nwkMaxDepth（Lm）、設備的子設備中最多允許的路由器數 nwkMaxRouters（Rm）就可以根據下面的公式計算深度爲 d 的父設備給它的每個具有路由器功能的子設備分配的位址段中的位址數 Cskip（d）：

$$Cskip(d)=\begin{cases}1+Cm\bullet(Lm-d-1) & Rm=1\\ \dfrac{1+Cm-Rm-Cm\bullet Rm^{Lm-d-1}}{1-Rm} & Rm\neq 1\end{cases}$$

如果一個設備的 Cskip（d）值等於 0，則它不能接受其他設備爲子設備，這個設備就只能是 ZigBee 終端設備。設備的 NLME 就調用 MLME-SET.request 原語把 MAC 層 PIB 屬性 macAssociationPermit 設爲 FASLE。ZigBee 終端設備的 NLME 收到 PermitDuration 參數大於或等於 0x01 的 NLME-PERMIT-JOINING.request 原語時，就響應一個 Status 參數等於

INVALID-REQUEST 的證實原語 NLME-PERMIT-JOINING.confirm，終止允許設備加入過程。如果一個 Cskip（d）值大於 0 的父設備可以接受子設備，並根據子設備是否具有路由器功能而分配不同的位址。

具有路由器功能的子設備分得的網路位址之間的偏移是 Cskip（d）。父設備分配給第一個具有路由器功能的子設備的網路位址比其自身位址大 1；父設備分配給第二個具有路由器功能的子設備的位址與第一個具有路由器功能子設備的位址偏移是 Cskip（d）。如此類推，父設備最多爲 nwkMaxRouters 個這樣的子設備分配位址。父設備爲子設備中的終端設備分配的位址是連續的，第 n 個 ZigBee 終端設備類型的子設備位址爲：

$$A_n = A_{parent} + Cskip(d) \bullet Rm + n$$

其中：1≤n≤（Cm — Rm），A_{parent} 表示父設備的網路位址。圖 18 所示的 ZigBee 網路中 nwkMaxChildren = 4，nwkMaxRouters = 4，nwkMaxDepth = 3。表 17 列出了不同深度的父設備分配位址時的偏移量 Cskip（d），並在圖中標出了各設備分配的位址。因爲分配給各設備的位址段在設備間是不能共用的，所以有可能一個父設備的位址已經用完，而另一個父設備還有位址沒有使用。這時，位址已經用完的父設備將不再接受新設備的入網請求，新設備只有尋找別的父設備。如果新設備工作範圍內沒有可以接受入網請求的父設備，那麼新設備就不能加入到網路中。

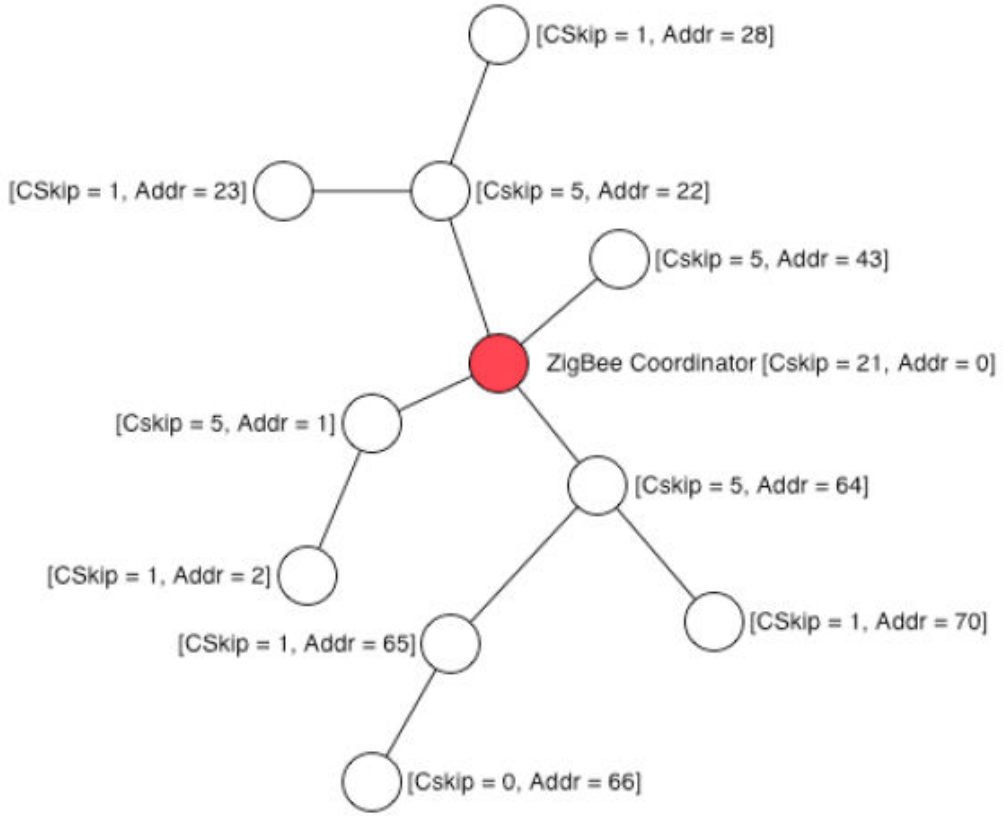


圖 18 ZigBee 網路的位址分配實例

表 17 實例中不同深度的父設備分配位址時的偏移量

父設備的網路深度 d	偏移量 Cskip（d）
0	21
1	5

2	1
3	0

2.5.1.5 上層位址分配機制

當 NIB 屬性 nwkUseTreeAlloc 的值等於 FALSE 時，ZigBee 網路採用另一種位址分配機制。設備上層透過設置 NIB 屬性 nwkNextAddress、nwkAvailableAddresses 和 nwkAddressIncrement 來分配位址段。在這種位址分配機制中，如果一個設備的 nwkAvailableAddresses 屬性值等於 0，則該設備不能接受關聯請求。這類設備的 NLME 就調用 MLME-SET.request 原語把 MAC 層 PIB 屬性 macAssociationPermit 設爲 FALSE；同時，這類設備的 NLME 收到 PermitDuration 參數大於或等於 0x01 的 NLME-PERMIT-JOINING.request 原語時，就響應一個 Status 參數等於 INVALID_REQUEST 的證實原語 NLME-PERMIT-JOINING.confirm，終止允許設備加入過程。如果設備的 nwkAvailableAddresses 屬性值大於 0，則設備的 NLME 就調用 MLME-SET.request 原語把 MAC 層 PIB 屬性 macAssociationPermit 設爲 TRUE，可以接受其他設備的關聯請求。同時，這類設備的 NLME 收到 PermitDuration 參數大於或等於 0x01 的 NLME-PERMIT-JOINING.request 原語時，就響應一個 Status 參數等於 SUCCESS 的 NLME-PERMIT-JOINING.confirm 原語。如果設備正在接受一個新設備的關聯，則它將把 nwkNextAddress 屬性值作爲分配給新關聯設備的網路位址。關聯成功後，把 nwkNextAddress 屬性值增加 nwkAddressIncrement，把 nwkAvailableAddresses 屬性值減 1。

需要明確的是，nwkMaxDepth 粗略決定了從拓撲樹的根設備到最遠的終端設備的距離；同時，nwkMaxDepth 也大體上決定了網路的直徑。特別地，在 ZigBee 協調器處於網路中心的理想網路規劃中，網路直徑應爲 2×nwkMaxDepth；而在實際應用中，網路直徑可能要小些。這種情況下，nwkMaxDepth 和 2×nwkMaxDepth 分別代表了網路直徑的下界和上界。另外，在 ZigBee 規範 1.0 中，網路拓撲樹不是動態平衡的，那麼在例如長線形的應用環境中，可能存在這種情況：網路中的設備還遠遠沒有達到位址容量時，網路已經用盡了所有的位址資源。

2.5.1.6 設備離網

ZigBee 子設備離開網路的方式有兩種：一種是子設備主動向父設備請求離開網路；另一種是父設備命令子設備離開網路。

當設備接收到來自上層的 NLME-LEAVE.request 原語或接收到來自父設備的離開網路命令訊框(Frame)有效負載中命令選項欄位的請求/指示子域爲 1 時，設備自身就啓動離開網路的過程。設備啓動離開過程時，NLME 將向各個子設備發送離開請求命令。如果離開網路過程由設備上層啓動，並且 NLME-LEAVE.request 原語的 RemoveChildren 參數等於 FALSE，那麼設備發送給子設備的離開命令訊框(Frame)有效負載中命令選項欄位的刪除子設備子域應設爲 0；如果 RemoveChildren 參數等於 TRUE，那麼設備發送給子設備的離開命令訊框(Frame)中刪除子設備子域應設爲 1。如果離開網路過程因收到父設備的離開命令訊框(Frame)而啓動，那麼設備發送的離開命令訊框(Frame)中刪除子設備子域的設置與接收到的離開命令訊框(Frame)相同。如果設備收到的離開命令訊框(Frame)要求刪除子設備並且設備

存在子設備，那麼 NLME 將依次強制其子設備離開網路。刪除子設備後，設備的 NLME 將調用 MAC 層資料服務 MCPS-DATA.request 向父設備發送離開指示命令，即離開命令訊框(Frame)有效負載中請求/指示子域設爲 0。如果該設備離開網路時沒被要求刪除子設備，那麼它發給父設備的離開指示命令有效負載中的刪除子設備子域應設爲 0；如果設備離開網路時被要求刪除子設備但它沒有子設備或者已經成功刪除了所有子設備，那麼它發給父設備的離開指示命令有效負載中的刪除子設備子域應設爲 1，否則設爲 0。最後，設備的 NLME 向 MAC 層發送解關聯請求原語 MLME-DISASSOCIATE.request，原語中 DeviceAddress 參數等於父設備的位址，DisassociateReason 參數等於 0x02。在接收到解關聯證實原語 MLME-DISASSOCIATE.confirm 後，NLME 才向上層發送離網證實原語 NLME-LEAVE.confirm 原語中 DeviceAddress 參數等於 0。如果上述過程中 MCPS-DATA.confirm 返回狀態爲 SUCCESS，要求設備刪除的子設備都被成功刪除，並且 MLME-DISASSOCIATE.confirm 原語返回的狀態也是 SUCCESS 時，NLME-LEAVE.confirm 原語中的 Status 參數值才是 SUCCESS；否則，Status 參數值爲 LEAVE_UNCONFIRMED。

任何設備的 NLME 收到離開命令訊框(Frame)時，都必須檢測它與離開命令發送設備之間的關係。如果離開命令訊框(Frame)接收設備是該命令發送命令的父設備，它將檢測命令訊框(Frame)有效負載部分刪除子設備子域的值。如果刪除子設備子域的值爲 1，那麼父設備可以重新利用以前分配給欲離開網路設備的 16 位元網路位址；如果刪除子設備子域的值爲 0，那麼父設備不可重新利用此前分配該設備的 16 位元網路位址。此外，父設備還要把近鄰表中有關該離網設備的記錄中的關係欄位置爲 0x03，表示兩者之間已經沒有關係了。如果離開命令訊框(Frame)接收設備是該命令發送設備的子設備，它將檢測命令訊框(Frame)有效負載部分請求/指示子域的值。如果請求/指示子域的值爲 1，即父設備要求子設備離開網路，那麼離開命令接收設備的 NLME 將啓動上述的離網過程；如果請求/指示子域的值爲 0，即父設備把其自身將離網的事實通知給子設備，那麼子設備的 NLME 將向上層發送離網指示原語 NLME-LEAVE.indication，原語中 DeviceAddress 參數設爲將要離網的父設備的 64 位元擴充位址。

父設備強制子設備離開網路時，它將發送 NLME-LEAVE.request 原語，其中 DeviceAddress 參數設爲被要求離網子設備的位址。顯然，只有 ZigBee 協調器或 ZigBee 路由器可以啓動強制子設備離網的過程，如果任何其他設備試圖啓動該過程，NLME 將中止該過程並向上層發送 Status 參數等於 INVALID_REQUEST 的 NLME-LEAVE.confirm 原語，告知其請求非法。當上層發送NLME-LEAVE.request原語啓動強制子設備離網過程時，NLME 將首先判斷指定的設備是否在網路中，即 NLME 透過搜索近鄰表查看是否有與指定設備匹配的擴充位址。如果找不到匹配的擴充位址，NLME 將中止離網過程並向上層發送 Status 參數等於 UNKNOWN_DEVICE 的 NLME-LEAVE.confirm 原語；如果找到匹配的擴充位址，NLME 將調用 MAC 層資料服務 MCPS-DATA.request 向子設備發送離網命令訊框(Frame)。離網命令訊框(Frame)有效負載部分請求/指示子域的值應設爲 1。如果要求離網的子設備遞迴地刪除子設備，則發送的離網命令訊框(Frame)中刪除子設備子域設爲 1；否則設爲 0。發送離網命令訊框(Frame)後，NLME 將啓動計時器，等待一個超市週期。如果不要求離網設備刪除子設備，則超時週期爲 nwkTransactionPersistenceTime；如果要求離網設備刪除子設備，則超時週期爲 nwkTransactionPersistenceTime×Cskip（d）。在超時前，設備應收到透過 MAC 層指示原語 MCPS-DATA.indication 傳遞的離開指示命令訊框(Frame)，該訊框(Frame)的源位址是被要求離開網路的子設備的位址，離網命令訊框(Frame)中請求/指示子域的值爲 0。在超時週期內，設備還可能要等待接收子設備的解關聯指示 MLME-DISASSOCIATE.indication。在接收到這些資訊後，NLME 向上層發送

NLME-LEAVE.confirm 原語，其中 DeviceAddress 參數設爲離網設備的 64 位元擴充位址。如果傳輸離網命令訊框(Frame)的 MAC 層證實原語 MCPS-DATA.confirm 返回的狀態爲 SUCCESS，在超時前設備收到子設備的離網指示命令訊框(Frame)，並且設備不要求子設備遞迴刪除子設備或要求遞迴刪除子設備時設備收到的離網指示命令訊框(Frame)中刪除子設備子域的值爲 1，那麼 NLME-LEAVE.confirm 原語的 Status 參數值爲 SUCCESS；否則，Status 參數值爲 LEAVE_UNCONFIRMED。子設備接收到父設備的離網命令訊框(Frame)後，要執行此前介紹的設備主動要求離開網路的過程。

圖 19 和圖 20 分別是多種情形下離網請求和離網命令在設備間傳遞的資訊流程。

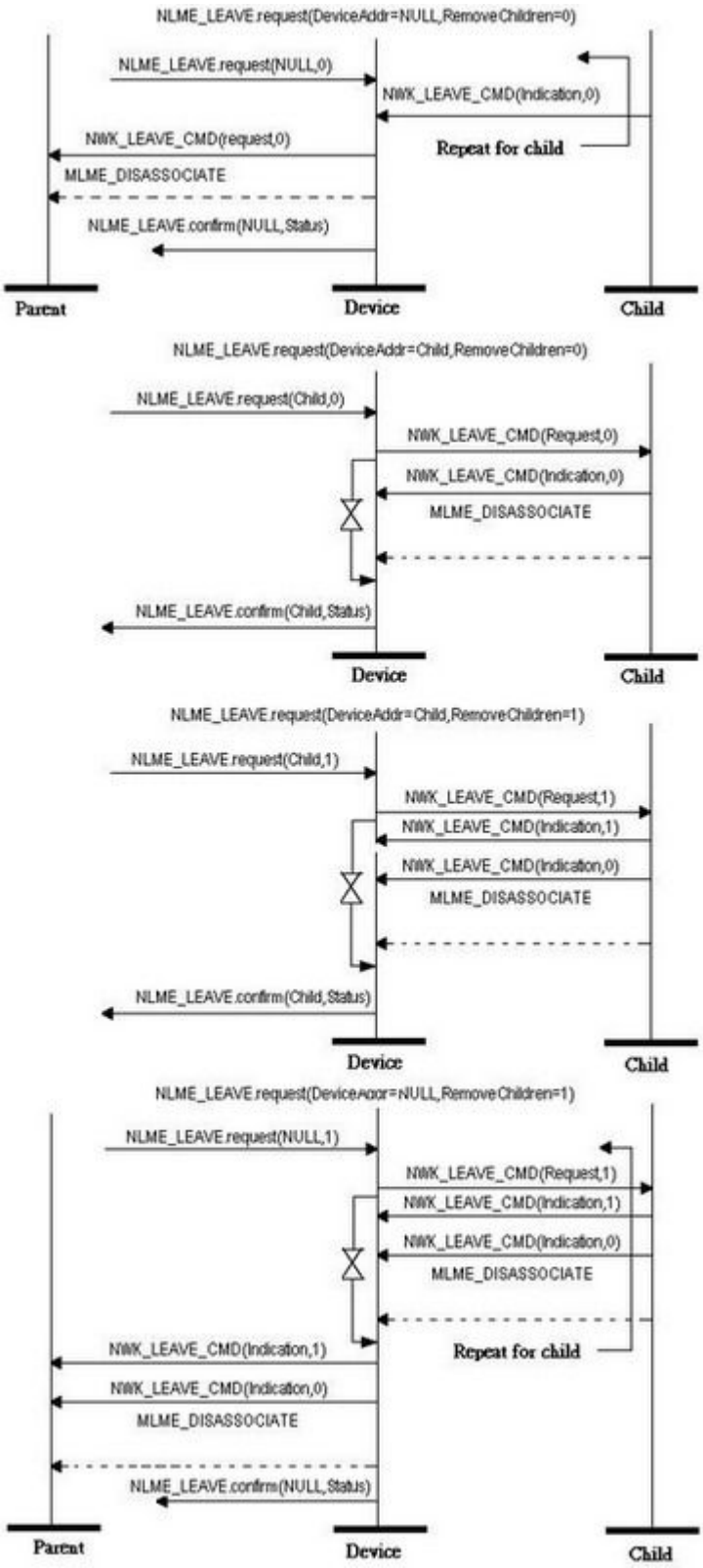


圖 19 多種情形下離網請求在設備間傳遞的資訊流程

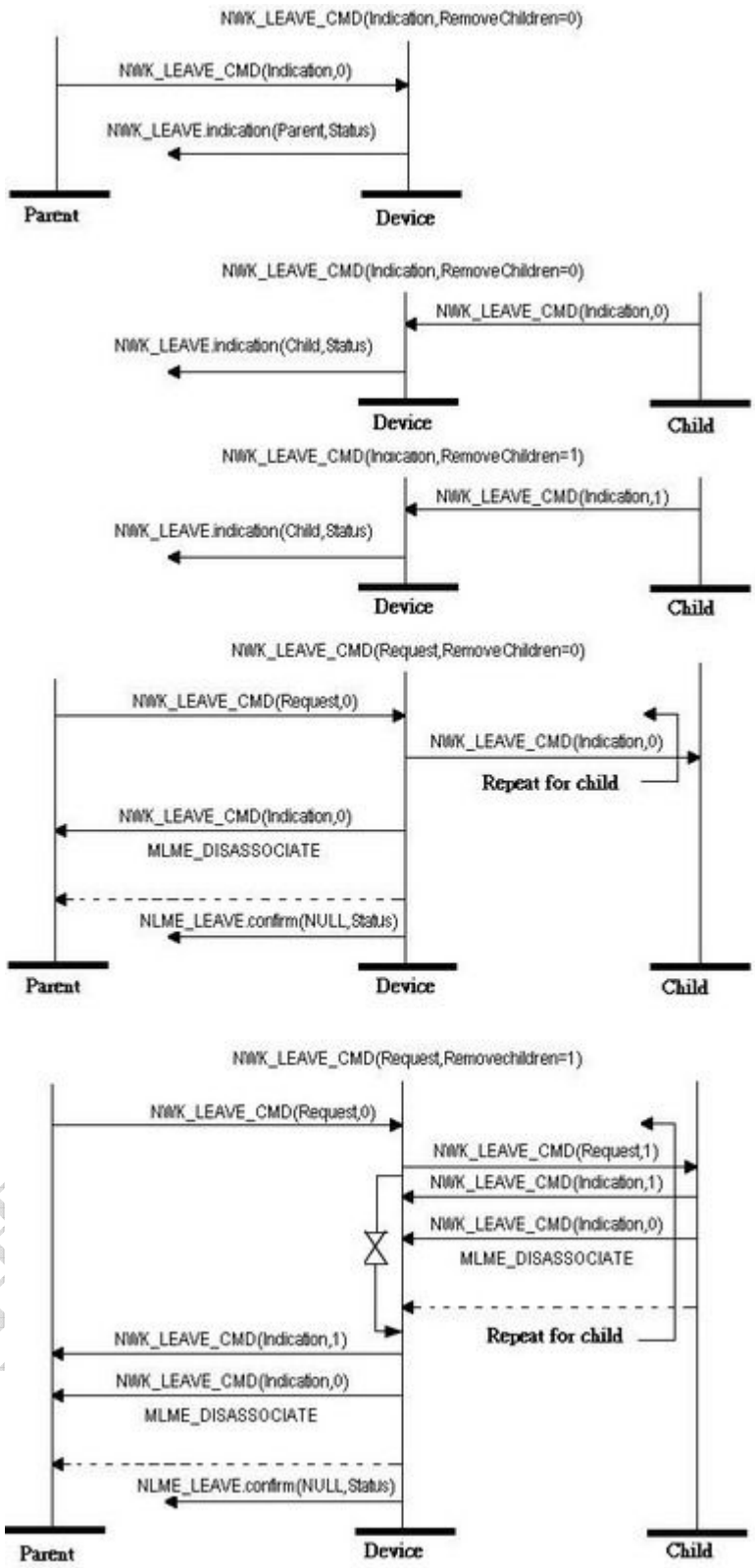


圖 20 多種情形下離網命令在設備間傳遞的資訊流程

2.5.1.7 變更 ZigBee 協調器配置

改變 ZigBee 協調器的配置也是 NWK 層的功能之一。如果 ZigBee 協調器的上層向改變網路的配置，它將請求 MAC 層改變 PIB 屬性。ZigBee 協調器的配置包括以下幾項內容：設備是否願意擔當 ZigBee 協調器，MAC 超訊框(Frame)的信標階數，MAC 超訊框(Frame)的階數，是否使用電池壽命延長模式。改變 ZigBee 協調器的配置由上層向 NLME 發送 NLME-NETWORK-FORMATION.request 原語來實現，嘗試改變配置的狀態透過 NLME-NETWORK-FORMATION.confirm 原語來回饋。

2.5.1.8 設備重定

在透過關聯嘗試入網之前和透過解關聯嘗試離網之後，設備在加電後立即對 NWK 層進行復位。NWK 層復位是由上層向 NLME 發送復位請求原語 NLME-RESET.request 來實現的，復位嘗試的結果透過證實原語 NLME-RESET.confirm 回饋給上層。重定過程將清除設備路由表的記錄，有些設備可能還要在不變的記憶體中儲存某些 NEK 層參量並在復位後恢復。然而，設備重定後將丟棄網路位址，它需要重新搜索關聯並從協調器獲取新的網路位址。新的網路位址可能不同於老的網路位址。此時，任何設備要與重定設備通訊時，都必須使用高層協定和過程重新發現設備。

2.5.2 發送和接收

只有當前關聯在網路中的設備才能從網路層發送資料訊框(Frame)。如果尚未關聯的設備收到發送訊框(Frame)請求，它將丟棄該訊框(Frame)並向上層發送狀態爲 INVALID_REQUEST 的 NLDE-DATA.confirm。NWK 層發送的資料訊框(Frame)要按照 NWK 訊框(Frame)的格式進行構造，並調用 MAC 子層資料服務進行發送。除了源位址和目的位址欄位外，所有 NWK 資料訊框(Frame)中還應包括半徑欄位和序號欄位。上層請求發送的資料訊框(Frame)，半徑欄位的值可由 NLDE-DATA.request 原語的 Radius 參數來提供。如果 NLDE-DATA.request 原語不提供半徑欄位的值，則 NWK 訊框(Frame)頭的半徑欄位應設爲 nwkMaxDepth 屬性值的 2 倍。每個設備的 NWK 層都維護一個訊框(Frame)序號變數，它的初始值是一個亂數。NWK 層每構造一個新的 NWK 訊框(Frame)，序號變數就加 1。構造的 NWK 訊框(Frame)可以是上層請求發送的新資料訊框(Frame)，也可以是新的網路層命令訊框(Frame)。加 1 後的序號值插入到 NWK 訊框(Frame)頭的序號欄位位置。構造好的 NPDU 如果還要求安全處理，則把它提交給安全服務提供模組按指定的安全套件做相應的安全處理。如果 NLDE-DATA.request 中的 SecurityEnable 參數等於 FALSE 或 NWK 層安全級別 nwkSecurityLevel 等於 0，NWK 層訊框(Frame)不需要做安全處理。此時 NWK 訊框(Frame)控制欄位中安全子域的值設爲 0。成功完成安全處理後，安全套件再把訊框(Frame)返回給 NWK 層發送。經過安全處理的訊框(Frame)將附加正確的輔助訊框(Frame)頭。如果資料訊框(Frame)的安全處理失敗，NWK 層將透過 NLDE-DATA.confirm 原語的狀態把結果回饋給上層；如果 NWK 命令訊框(Frame)的安全處理失敗，則 NWK 將直接丟棄該訊框(Frame)並不做進一步的處理。當構造好 NWK 訊框(Frame)準備發送時，NLDE 調用 MAC 層資料服務

原語 MCPS-DATA.request 把訊框(Frame)遞交給 MAC 層。發送結果透過證實原語 MCPS-DATA.confirm 回饋給 NWK 層。

要接收資料，設備就必須開啓接收機。應用層可用 NLME-SYNC.request 原語來啓動接收過程。在信標致能網路中，NWK 接收到該原語後就指令設備同步到其父設備的下一個信標並可選跟蹤後續的信標。NWK 層將向 MAC 層發送 MLME-SYNC.request 原語來實現與父設備信標的同步。在非信標網路中，NLME-SYNC.request 原語將指令 NWK 層調用 MLME-POLL.request 原語來輪詢父設備，查看是否有待接收的資料。在非信標網路中，ZigBee 協調器或 ZigBee 路由器的 NWK 層應盡最大可能確保設備在不發射的時候開啓接收機。在信標致能網路中，設備 NWK 層應確保設備在其超訊框(Frame)或父設備超訊框(Frame)的活動週期內不發射時開啓接收機。NWK 層可使用 MAC PIB 屬性 macRxOnWhenIdle 來控制接收機的開關。如果接收機開啓，NWK 層將透過 MAC 資料服務開始接收訊框(Frame)。接收到每個訊框(Frame)時，NWK 訊框(Frame)頭的半徑欄位的值被減 1。如果減 1 後半徑欄位的值等於 0，那麼在任何情況下設備都不再轉發該訊框(Frame)，而只會提交給上一層或由 NWK 層做相關處理。接收資料訊框(Frame)的目的位址與設備的網路位址一致時，NWK 將把該訊框(Frame)提交給上一層；同時，廣播資料訊框(Frame)也要提交給上一層。如果接收設備是 ZigBee 協調器或一個運行著的 ZigBe 路由器，那麼它將轉發目的位址與設備網路位址不一致的資料訊框(Frame)；而在其他情況下，資料訊框(Frame)將被立即丟棄。目的位址與接收設備網路位址一致的路由應答命令訊框(Frame)的處理過程在後續路由部分中介紹。目的位址與接收設備網路位址不一致的路由應答命令訊框(Frame)將被丟棄。路由錯誤命令訊框(Frame)的處理方式與資料訊框(Frame)的處理方式相同。NWK 層透過指示原語 NLDE-DATA.indication 把接收到的資料訊框(Frame)通知給上層。接收到訊框(Frame)時，NLDE 將檢測訊框(Frame)控制欄位的安全子域。如果安全子域的值不爲 0，NLDE 將把接收的訊框(Frame)提交給安全服務模組按指定的安全套件做解安全處理。

2.5.3 路由功能

ZigBee 協調器和路由器應提供以下路由功能：代表上層轉發資料訊框(Frame)；代表其他 ZigBee 路由器轉發資料訊框(Frame)；爲後面的資料訊框(Frame)建立路由而參與路由發現；代表終端設備參與路由發現；參與端到端路由修復；參與本地路由修復；使用路由發現和路由修復中指定的 ZigBee 路徑成本度量。此外，ZigBee 協調器和路由器還可能提供下列路由功能：爲記住最好的可用路由而維護路由表；代表上層啓動路由發現；代表其他 ZigBee 路由器啓動路由發現；啓動端到端路由修復；代表其他 ZigBee 路由器啓動本地路由修復。

2.5.3.1 路由成本

在路由發現和維護中，ZigBee 路由演算法使用路徑成本度量來進行路由比較。爲了比較這個度量，這裡賦予路徑中每段鏈路度量一鏈路成本，構成路徑的所有鏈路的成本之和就是整條路徑的度量—路徑成本。更正式地，如果把一組有序的設備[D_1，D_2，…，D_L]定義長度爲 L 的路徑 P，而其中的一段鏈路[D_i，D_{i+1}]定義爲長度爲 2 的子路徑，那麼路徑成本可以表示爲：

$$C\{P\}=\sum_{i=1}^{L-1}C\{[D_i,D_{i+1}]\}$$

這裡 $C\{[D_i,D_{i+1}]\}$ 是鏈路成本，鏈路 1 的成本 C{1}是取值在[0…7]範圍內的函數。它定義爲：

$$C\{1\}=\left\{\min\left(7,round\left(\frac{1}{p_1^{\,4}}\right)\right)\right\}^{7}$$

其中 p_1 表示包在鏈路 1 上傳遞的概率。這樣，具體實現時可以選擇常數 7 作爲鏈路成本，也可以選擇反應概率 p_1 的函數作爲鏈路成本。如果一個設備提供了鏈路成本的這兩種選項，那麼透過設置 NIB 屬性 nwkReportConstantCost 的值爲 TRUE 可以強制使用常數 7 作爲鏈路成本。現在剩下的問題就是如何得到概率 p_1。p_1 的估計是一個實現問題，完全由設計者按照自己的方式來實現。一種是可以透過在一段時間內統計丟訊框(Frame)來計算 p_1，人們普遍認爲這種方法得到的概率 p_1 是最精確的。然而，最直接的方法是基於 MAC 和 PHY 層提供的每訊框(Frame)平均 LQI 來估計 p_1，一個函數可以把平均 LQI 映射到 C{1}上，根據 LQI 透過查表就可以得到鏈路成本。

2.5.3.2 路由表

ZigBee 路由器或 ZigBee 協調器可能維護了一個路由表，路由表中存放的資訊如表 18 所列。路由表記錄中路由狀態資訊的取值如表 19 所列。ZigBee 路由器或 ZigBee 協調器還可能預留一些路由表記錄專用于路由修復和在其他路由能力都耗盡的時候才使用。在後面的路由演算法中會用到“路由表能力”這個術語，所謂路由表能力是指設備使用路由表能夠建立起一條到達特定目的設備的路由。如果一個設備是 ZigBee 協調器或 ZigBee 路由器，它維護的路由表中有空閒的路由表記錄或已經有一個與目的設備對應的路由表記錄，並且正在嘗試路由修復的設備預留了專用于路由修復的路由表記錄，那麼就說它具有“路由表能力”。如果 ZigBee 路由器或 ZigBee 協調器維護了一個路由表，那麼它還應該維護一個路由發現表。路由發現表包含的資訊如表 20 所列。路由表記錄在設備中是長期存在的，而路由發現表記錄僅維持一次路由發現操作的時間並且可以重複使用。如果一個設備維護了一個路由發現表，並且路由發現表中有空閒的記錄，那麼就說這個設備具有“路由發現表能力”。如果一個設備既有路由表能力，又有路由發現表能力，那麼就或設備具有“路由能力”。

表 18 路由表各欄位的定義

字 段 名	欄位長度	描　　述
目的位址	2 位元組	本路由最終目的設備的 16 位元網路位址
狀態	3 位	路由狀態
下一個跳點位址	2 位元組	去往目的位址的路由上下一跳的 16 位網路位址

表 19 路由狀態值及意義

數 值	狀　　態
0x0	ACTIVE（活動）
0x1	DISCOVERY_UNDERWAY（正在執行路由發現）
0x2	DISCOVERY_FAILED（路由發現失敗）
0x3	INACTIVE（不活動）
0x4～0x7	預留

表 20 路由發現表

字 段 名	欄位長度/位元組	描述
路由請求標識	1	路由請求命令訊框(Frame)的序號，該序號在每次設備發起路由請求時遞增
來源位址	2	路由請求發起設備的 16 位元網路位址
發送位址	2	最新發送最低成本路由請求命令訊框(Frame)的設備網路位址。該資訊用於決定最後路由應答命令訊框(Frame)應遵循的路徑
前期成本	1	從路由請求源位址設備到當前設備的累加路徑成本
剩餘成本	1	從當前設備到目的設備的累加路徑成本
到期時間	2	用以設定路由發現到期時間的遞減計時器上的時間（單位爲 ms），其初始值是 nwkcRouteDiscoveryTime 的屬性值

2.5.3.3 基本路由演算法

設備 NWK 接收到資料訊框(Frame)時按照下面的程式爲訊框(Frame)安排路由。如果 NWK 接收到的資料訊框(Frame)來自其上層並且目的位址爲廣播位址，NWK 層就按照後續部分將要介紹的程式來廣播該資料訊框(Frame)。如果接收設備是 ZigBee 路由器或 ZigBee 協調器，訊框(Frame)的目的設備是 ZigBee 終端設備並且還是接收設備的子設備，那麼接收設備將使用 MCPS-DATA．request 原語把訊框(Frame)直接發送給目的設備，即下一跳的目的位址就等於最終目的位址。具有路由能力的設備應檢查 NWK 訊框(Frame)頭部分訊框(Frame)控制欄位中的發現路由子域，如果發現路由子域的值等於 0x02，那麼設備將立即啓動路由發現過程。如果發現路由子域的值不等於 0x02，設備將在路由表中查找與訊框(Frame)目的位址對應的記錄。如果找到訊框(Frame)目的位址對應的路由表記錄，並且其中路由狀態的值爲 ACTIVE，那麼設備就用 MCPS-DATA．request 原語轉發收到的訊框(Frame)。轉發訊框(Frame)時，MCPS-DATA．request 原語中 SrcAddrMode 和 DstAddrMode 參數值應都爲 0x02，即使用 16 位短位址；原語中 SrcPANId 和 DstPANId 參數值都應爲轉發設備的 MAC PIB 屬性 macPANId 的值；SrcAddr 參數應設爲轉發設備的 MAC PIB 屬性 macShortAddress 的值，DstAddr 參數應設爲目的位址對應的路由表記錄中下一跳位址欄位的值；TxOptions 參數與 0x01 逐位相與操作後結果總是非零值，即轉發的訊框(Frame)要求確認。如果找到訊框(Frame)目的位址對應的路由表記錄，但其中路由狀態的值爲 DISCOVERY_UNDERWAY，則表示設備正在爲該訊框(Frame)執行路由發現操作。此時設備可以選擇緩存該訊框(Frame)以等待路由發現完成，也可以選擇在 NIB 屬性 nwkUseTreeRouting 等於 TRUE 時用分級路由把該訊框(Frame)沿著樹傳遞。如果沿樹傳遞訊框(Frame)，NWK 頭的訊框(Frame)控制欄位中的發現路由子域應設爲 0x00。如果找到訊框

(Frame)目的位址對應的路由表記錄，但其中路由狀態的值爲 DISCOVRY_FAILED 或 INACTIVE，則在 NIB 屬性 nwkUseTreeRouting 等於 TRUE 時刻採用分級路由把該訊框(Frame)沿著樹傳遞。如果設備路由表中找不到訊框(Frame)目的位址對應的路由記錄，設備將檢測 NWK 頭部分訊框(Frame)控制欄位的發現路由子域。如果發現路由子域的值等於 0x01，設備將啓動路由發現過程；如果發現路由子域的值等於 0x00 並且 NIB 屬性 nwkUseTreeRouting 等於 TRUE，設備將用分級路由把該訊框(Frame)沿著樹傳遞。如果發現路由子域的值等於 0x00 並且 NIB 屬性 nwkUseTreeRouting 等於 FALSE，設備路由表中又找不到訊框(Frame)目的位址對應的路由記錄，則 NLDE 將丟棄該訊框(Frame)並向上層發送 Status 參數等於 INVALID_REQUEST 的 NLDE-DATA．request 原語。

對於一個沒有路由能力的設備，如果 NIB 屬性 nwkUseTreeRouting 等於 TRUE，設備將採用分級路由沿著樹轉發訊框(Frame)。在分級路由演算法中，如果訊框(Frame)的目的設備是當前設備的後代設備，那麼設備就把訊框(Frame)轉發給適當的子設備。如果訊框(Frame)的目的設備就是當前設備的一個子設備，並且該子設備是終端設備，那麼該終端設備的 macRxOnWhenIdle 狀態可能會導致不能立即遞交訊框(Frame)。當子設備的 macRxOnWhenIdle 值等於 FALSE 時，設備只能採用間接傳輸來遞交訊框(Frame)。如果訊框(Frame)的目的設備不是當前設備的後代設備，那麼設備將把訊框(Frame)提交給父設備。ZigBee 網路中除 ZigBee 協調器之外的每一個設備都是 ZigBee 協調器的後代設備，而任何一個 ZigBee 終端設備都沒有後代設備。對一個位址爲 A、深度爲 d 的 ZigBee 路由器，如果下面的邏輯運算式成立，那麼位址爲 D 的目的設備就是該路由器的後代設備：

$$A < D < A+Cskip\ (d-1)$$

如果確定了訊框(Frame)的目的設備是當前接收設備的後代，那麼當目的設備是當前接收設備的子設備且爲終端設備時，下一跳位址 N 爲：

$$N=D$$

這裡 D＞A+RmxCskip（d）。當目的設備是當前接收設備的其他後代設備時，下一跳的位址 N 爲：

$$N = A+1+\left[\frac{D-(A+1)}{Cskip(d)}\right]\times Cskip(d)$$

如果 NWK 層接收到的資料訊框(Frame)來自 MAC 子層並且目的位址爲廣播位址，NWK 層將首先重新廣播該訊框(Frame)再把該訊框(Frame)送給上層處理。如果 NWK 層接收到的來自 MAC 子層的資料訊框(Frame)不是廣播訊框(Frame)，那麼 NWK 層就將判斷該訊框(Frame)的目的位址是否等於當前接收設備的邏輯位址。如果訊框(Frame)的目的位址等於當前設備的邏輯位址，NWK 層就把訊框(Frame)傳遞給上層處理；否則，當前接收設備就只是該訊框(Frame)的一個中間設備，此時 NWK 層對該訊框(Frame)的處理過程與上文介紹的 NWK 層處理來自上層的單播資料訊框(Frame)的過程一樣。圖 21 是 ZigBee 的基本路由演算法。

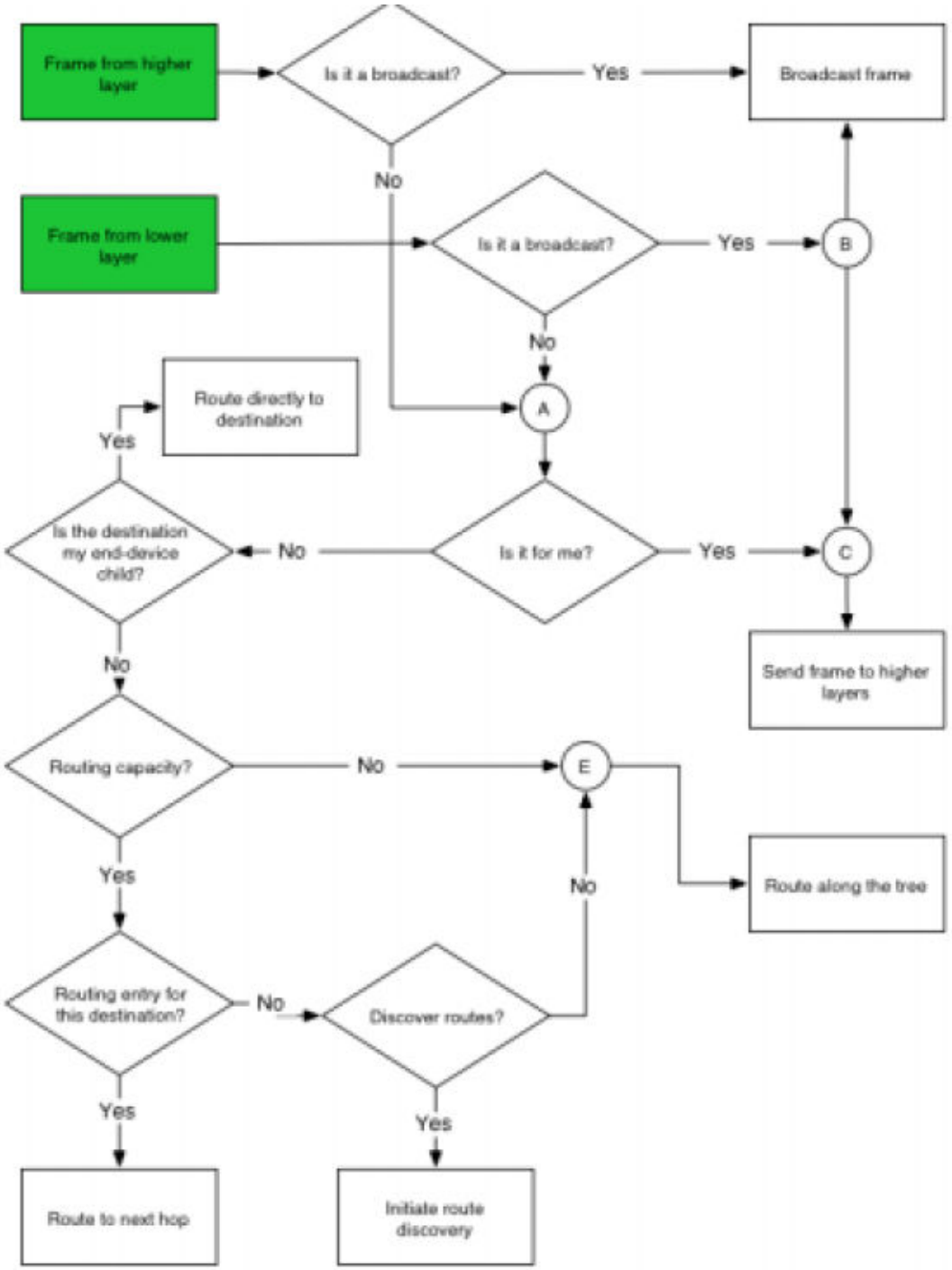


圖 21 ZigBee 的基本路由演算法

2.5.3.4 路由發現

路由發現是網路中的設備相互配合，發現並建立路由的過程。路由發現總是針對特定的源設備和目的設備執行的。在下面三種情況下，NWK 層將啓動路由發現過程：第一種情況是 NWK 層收到來自上層的 NLDE-DATA.request 原語中 DiscoverRoute 參數值爲 0x02；第二種情況是 NWK 層收到來自上層的 NLDE-DATA.request 原語中 DiscoverRoute 參數值爲 0x01

並且沒有 DstAddr 參數對應的路由表記錄；第三種情況是 NWK 層收到來自 MAC 層的資料訊框(Frame)，NWK 頭的目的位址不是當前設備的位址或是廣播位址，並且其訊框(Frame)控制欄位中發現路由子域的值等於 0x02 或 0x01，當前設備路由表中沒有 NWK 頭目的位址對應的記錄了。在上述任何一種情況下，如果當前設備沒有路由能力並且 NIB 屬性 nwkUseTreeRouting 的值等於 TRUE，NWK 層將用分級路由演算法沿樹遞交該資料訊框(Frame)；如果設備沒有路由能力並且 NIB 屬性 nwkUseTreeRouting 的值等於 FALSE，NWK 層將丟棄該訊框(Frame)。

對具有路由能力的設備，如果其路由表中沒有訊框(Frame)目的位址對應的記錄，它將建立一條狀態爲 DISCOVERY_UNDERWAY 的路由表記錄；如果路由表中有一條對應於訊框(Frame)目的位址的記錄，並且狀態爲 ACTIVE，那麼設備將使用該路由轉發資料訊框(Frame)並保持該路由表記錄的狀態不變；如果路由表中存在訊框(Frame)的目的位址對應的記錄，但狀態不等於 ACTIVE，那麼設備將使用該路由表記錄，並把其狀態設爲 DISCOVERY_UNDERWAY；同時，設備還要建立相應的路由發現表記錄。

每個發送路由請求命令訊框(Frame)的設備都要維護一個計數器，用來產生路由請求標識。每當設備產生一個新的路由請求命令訊框(Frame)時，路由請求計數器加 1，並把路由請求計數器的值存放在設備路由請求發現表的路由請求標識欄位中。路由發現表中路由請求計時器的計時週期應設爲 nwkcRouteDiscoveryTime 毫秒，計時期滿後，設備將把對應的路由請求記錄從路由發現表中刪除。如果此時目的位址對應的路由表記錄中 Status 欄位的值仍然是 DISCOVERY_UNDERWAY，並且路由發現表沒有該目的位址對應的其他記錄，則設備同時還要刪除該路由表記錄。NWK 層可選擇緩存接收的訊框(Frame)等待路由發現或在 NIB 屬性 nwkUseTreeRouting 等於 TRUE 時，把 NWK 頭訊框(Frame)控制欄位中的發現路由子域設爲 0 並沿著樹遞交訊框(Frame)。

設備建立了路由發現表和路由表記錄後，就要按照前面介紹過的訊框(Frame)格式構造路由請求命令訊框(Frame)的有效負載部分。命令訊框(Frame)標識欄位應設爲 0x01 表示路由請求；路由請求標識欄位應設爲路由發現表記錄中存放的值；目的位址欄位應設爲該路由發現過程所指向目的設備的 16 位元網路位址；路徑成本欄位應設爲 0。準備好路由請求命令廣播訊框(Frame)後，NWK 層就調用 MCPS-DATA.request 原語把它遞交給 MAC 子層。路由發現過程的啓動設備廣播路由請求命令訊框(Frame)時，NWK 在初次廣播之後還應重複廣播 nwkcInitialRREQRetries 次，即總計廣播 nwkcInitialRREQRetries+1 次路由請求命令訊框(Frame)。每兩次廣播時間的時間間隔是 nwkcRREQRetryInterval 毫秒。

接收到路由請求命令訊框(Frame)後，設備將判斷自己是否具有路由能力。如果設備沒有路由能力，它將檢測接收的訊框(Frame)是否來自有效路徑。如果接收訊框(Frame)來自設備的一個子設備並且源設備是該子設備的一個後代或者接收訊框(Frame)來自設備的父設備並且源設備不是當前的後代，那麼這樣的路徑就是有效的。如果接收到的路由請求命令訊框(Frame)不是來自有效路徑，設備將丟棄該訊框(Frame)。如果路由請求命令訊框(Frame)是來自有效路徑，設備將檢測路由請求命令訊框(Frame)的目的設備是否是當前設備或當前設備的終端子設備。如果當前設備或其一個終端子設備是該路由請求命令訊框(Frame)的目的設備，它將回應一個路由應答命令訊框(Frame)。設備用路由應答命令訊框(Frame)回應路由請求時，設備將構造一個訊框(Frame)類型爲 0x01（命令訊框(Frame)）的訊框(Frame)。路由應答的源位址應設爲路由應答產生設備的 16 位元網路位址，目的位址應設爲計算出的下一跳的位址，而對應的路由請求發起設備的位址則是應答訊框(Frame)的最終目的位址，它是放在有效負載部分的發起位址欄位內的。計算出當前設備到下一跳設備的鏈路成本並插入到路由應答命令訊框(Frame)的路徑成本欄位。路由應答命令發起設備將調用

MCPS-DATA.request 原語把路由應答單播發送到下一跳設備。如果當前設備不是路由請求命令訊框(Frame)的目的位址，設備將計算從前一跳設備到其自身的這段鏈路的成本，並累加到路由請求命令訊框(Frame)的路徑成本值中。然後，設備將調用 MCPS-DATA.request 服務原語吧路由請求命令訊框(Frame)向目的位址單播轉發。此時單播發送的下一跳位址的決定方法與資料訊框(Frame)一樣，即把當前的路由請求命令訊框(Frame)看作一個資料訊框(Frame)，而該資料訊框(Frame)的目的設備則是路由請求命令訊框(Frame)有效負載部分目的位址欄位指定的設備。

如果接收路由請求命令訊框(Frame)的設備具有路由功能，它將檢測路由請求命令訊框(Frame)的目的設備是否是當前設備或當前設備的終端子設備。如果當前設備或其一個終端子設備是路由請求命令訊框(Frame)的目的設備，設備將判斷是否存在對應于路由請求標識和源位址欄位的路由發現表記錄。如果路由發現表中沒有這樣的記錄，設備將產生該路由請求的路由發現表記錄。路由發現表記錄中的各欄位根據路由請求命令訊框(Frame)中對應的欄位設置，唯一的例外就是路由發現表中前期成本欄位的值要在路由請求命令訊框(Frame)路徑成本的基礎上累加前一跳設備到當前設備的鏈路成本。如果 nwkSymLink 屬性值爲 TRUE，即對稱鏈路路由，則設備還要建立一個路由表記錄。路由表記錄中目的位址欄位設置爲路由請求命令訊框(Frame)的源位址，下一跳欄位設置爲路由請求命令前一個發送設備的位址，狀態欄位設置爲 ACTIVE。然後設備應向路由請求命令訊框(Frame)的發起設備發送一個路由應答命令。如果路由發現表中存在一個對應于路由請求標識和源位址欄位的路由發現表記錄，設備將判斷當前路由發現過程中得到的路徑成本是否小於現存的路由發現表記錄中對應的前期成本欄位的值。如果當前路由發現得到的路徑成本大於現存的路由發現表記錄中的前期成本，設備將丟棄該路由請求命令訊框(Frame)，不需再作進一步處理；否則，設備就把路由發現表記錄中前期成本和發送設備位址欄位的值更新爲當前路由發現得到的路徑成本值和路由請求命令訊框(Frame)的前一個發送設備的位址。同樣，如果 nwkSymLink 屬性值爲 TRUE，則設備還要建立一個路由表記錄。路由表記錄中目的位址欄位設置爲路由請求命令訊框(Frame)的源位址，下一跳欄位設置爲路由請求命令前一個發送設備的位址，狀態欄位設置爲 ACTIVE。然後設備應向路由請求命令訊框(Frame)的發起設備發送一個路由應答命令。在上述任何一種情況下，如果設備是代表其終端子設備發送路由應答命令，則路由應答命令訊框(Frame)有效負載中應答位址欄位應設爲終端子設備的位址而不是應答設備的位址。

如果具有路由能力的設備不是接收到的路由請求命令訊框(Frame)的目的設備，它將判斷是否存在該路由請求命令的路由請求標識和源位址對應路由發現表記錄。如果不存在這樣的路由發現表記錄，設備將產生一條記錄，並把路由請求計時器的定時週期設爲 nwkcRouteDiscoveryTime 毫秒。如果存在路由請求目的位址對應的路由表記錄但狀態值不是 ACTIVE，則把狀態值設備 DISCOVERY_UNDERWAY；如果不存在路由請求目的位址對應的路由表記錄，則建立一條記錄。如果 nwkSymLink 屬性值爲 TRUE，則設備還要建立一個路由表記錄。路由表記錄中目的位址欄位設置爲路由請求命令訊框(Frame)的源位址，下一跳欄位設置爲路由請求命令前一個發送設備的位址，狀態欄位設置爲 ACTIVE。當路由請求計時器計時期滿後，設備將把對應的路由請求記錄從路由發現表中刪除。如果此時目的位址對應的路由表記錄中 Status 欄位的值仍然是 DISVOVERY_UNDERAY，並且路由發現表沒有該目的位址對應的其他記錄，則設備還要同時刪除該路由表記錄。如果路由發現表中存在一個對應于路由請求標識和源位址欄位的路由發現表記錄，設備將判斷當前路由發現過程中得到的路徑成本是否小於現存的路由發現表記錄中對應的前期成本欄位的值。如果當前路由發現得到的路徑成本大於現存的路由發現表記錄中的前期成本，設備將丟棄該路由請求命令

訊框(Frame)，不需再作進一步處理；否則，設備就把路由發現表記錄中前期成本和發送設備位址欄位的值更新爲當前路由發現得到的路徑成本值和路由請求命令訊框(Frame)的前一個發送的位址。如果 nwkSymLink 屬性值爲 TRUE，設備還要把目的位址欄位等於路由請求命令訊框(Frame)源位址的所有路由表記錄中的下一跳欄位更新爲路由請求命令訊框(Frame)的前一個發送設備的位址；狀態值設爲 ACTIVE。最後，設備將調用 MCPS-DATA.request 原語轉播路由請求命令訊框(Frame)。

NWK 層重複轉播路由請求命令訊框(Frame)時，兩次廣播之間的隨機延時按照下面的公式來計算：

$$2\times R[nwkcMinRREQJitter，nwkcMaxRREQJitter]$$

這裡 R[a，b]表示在區間[a，b]上的隨機函數，時延抖動的單位的 ms。具體實現時，實現者可以調整抖動量時的轉播時路由成本大的路由請求命令比路由成本小的路由請求命令延時更大。NWK 層愛第一次轉發路由請求命令訊框(Frame)後還要再重複廣播 nwkcRREQRetries 次，即最多可以轉播 nwkcRREQRetries+1 次受到的路由請求命令訊框(Frame)。NWK 層在重複廣播路由請求命令訊框(Frame)的過程中，如果收到源位址和路由請求標識相同、路徑成本更低的路由請求命令訊框(Frame)，則可以選擇丟棄正在等待重發的路由請求命令訊框(Frame)。設備同樣要把路由請求命令訊框(Frame)有效負載部分目的位址欄位的值對應的路由表記錄中的狀態欄位設置爲 DISCOVERY_UNDAYWAY；如果這樣的路由表記錄不存在，則設備要建立一條這樣的路由表記錄。

當用路由應答命令訊框(Frame)來回應路由請求時，設備將構造一個訊框(Frame)類型欄位值爲 0x01 的 NWK 命令訊框(Frame)，設備中有一條對應于路由請求源位址和路由請求標識的路由發現表記錄。路由應答命令訊框(Frame)頭的源位址欄位設爲當前設備的 16 位元網路位址；目的位址欄位設爲相應的路由發現表記錄中發送設備位址欄位的值，即路由請求命令訊框(Frame)前一跳設備的位址。路由應答命令訊框(Frame)有效負載部分的 NWK 命令標識欄位應設爲 0x02，表示路由應答命令；路由請求標識欄位的設置與路由請求命令訊框(Frame)中該欄位的值相同；發起位址欄位的值設爲路由請求命令訊框(Frame)頭部分的源位址欄位的值；路徑成本欄位的值應設爲當前設備到對應的路由發現表記錄中發送設備位址欄位指定設備的鏈路成本。構造好路由應答命令訊框(Frame)後，設備就調用 MCPS-DATA.request 原語把它單播發送到最終目的設備（即路由請求的發起設備），而當前發送的下一跳就是路由發現表記錄中發送設備位址欄位指定的設備。圖 22 就是設備接收到路由請求命令訊框(Frame)時的處理過程。

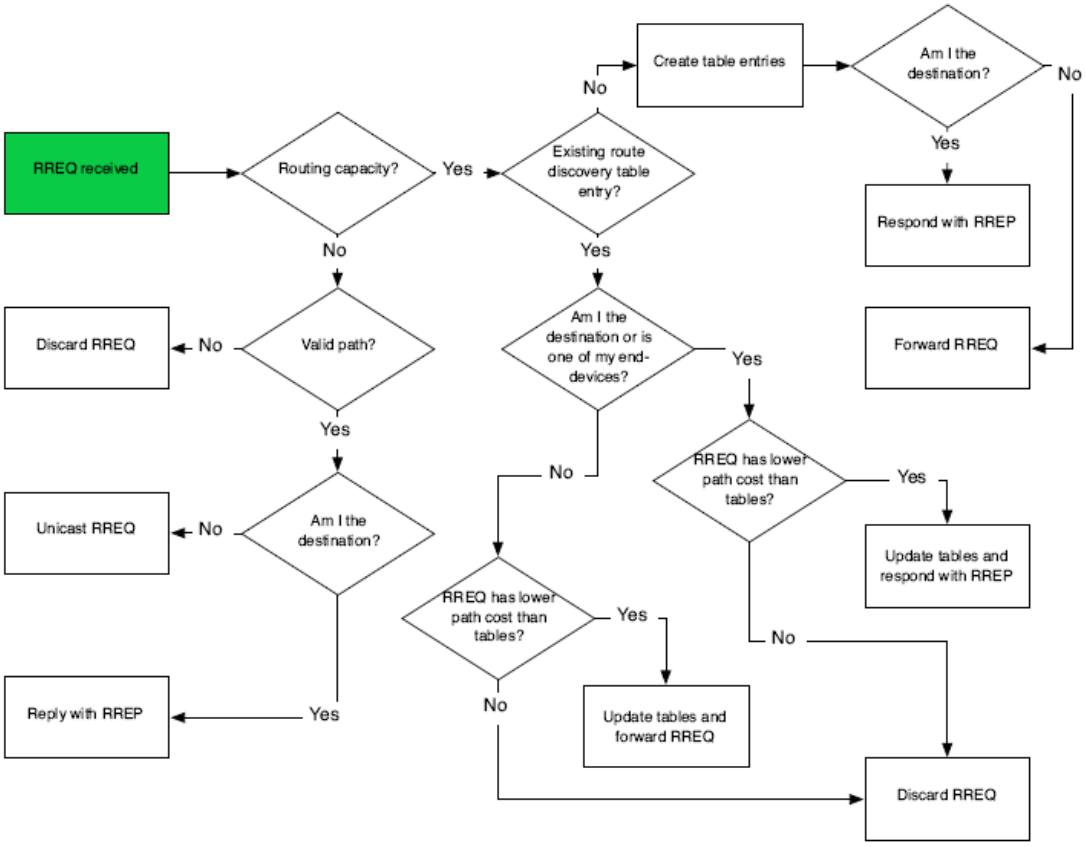


圖 22 設備接收到路由請求命令訊框(Frame)的處理流程

設備接收到路由應答命令訊框(Frame)時，將按照圖 23 的流程進行處理。

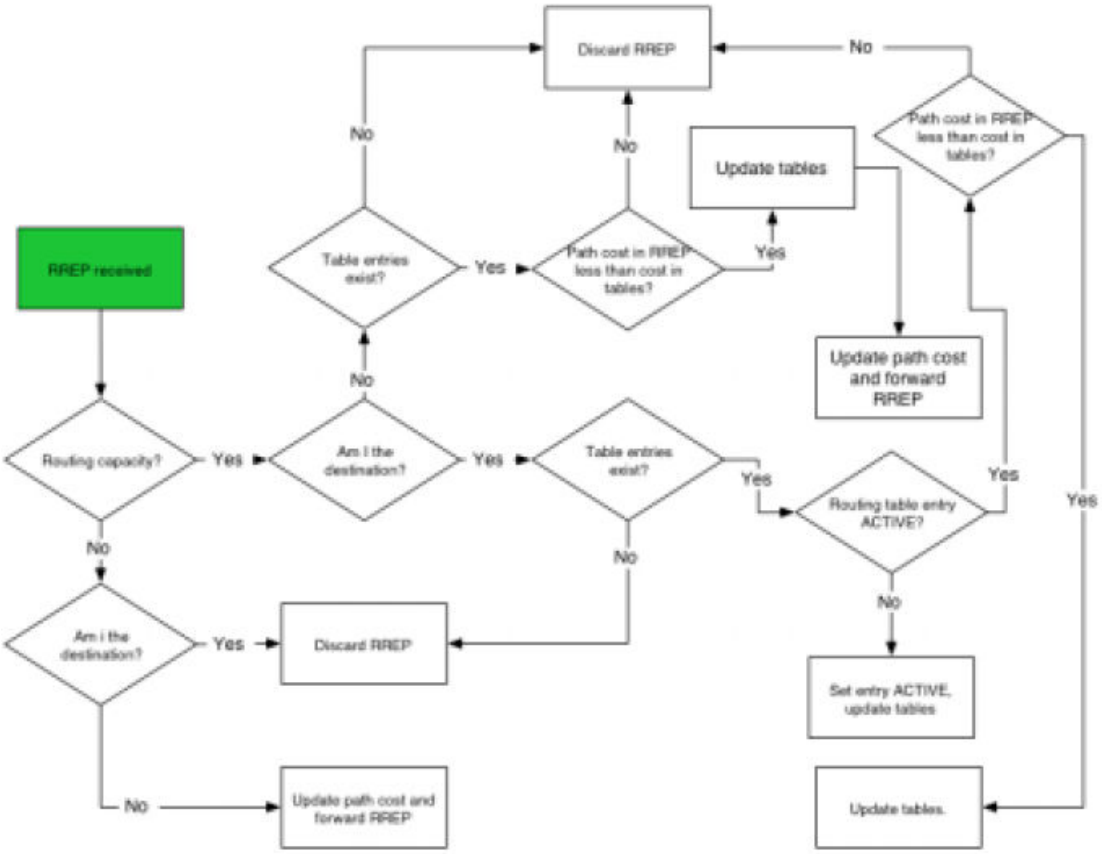


圖 23 設備接收到路由應答命令訊框(Frame)的處理流程

如果接收設備沒有路由能力但設備 NIB 屬性 nwkUseTreeRouting 的值爲 TRUE，則設備將沿樹向前轉發路由應答。如果接收設備沒有路由能力且設備 NIB 屬性 nwkUseTreeRouting 的值爲 FALSE，設備將丟棄路由應答命令訊框(Frame)。設備在向前轉發路由應答命令訊框(Frame)之前要更新有效負載中路徑成本欄位的值：計算當前設備與下一跳設備之間的鏈路成本並累加到路由應答命令的路徑成本欄位中。

如果接收設備具有路由能力，設備將把自身位址與路由應答命令訊框(Frame)中發起位址欄位的值進行比較，判斷其自身是否是路由應答命令訊框(Frame)的目的設備。如果接收設備是路由應答命令訊框(Frame)的目的設備，它就到路由發現表中查找路由應答命令訊框(Frame)有效負載中路由請求標識對應的記錄。如果沒有對應的路由發現表記錄，設備將丟棄該路由應答命令訊框(Frame)並終止路由應答處理；如果存在這樣的路由發現表記錄，則設備還要到路由表中查找路由應答命令訊框(Frame)有效負載中應答位址對應的記錄。如果沒有對應的路由表記錄，設備將丟棄該路由應答命令訊框(Frame)並刪除路由請求標識對應的路由發現表記錄，終止路由應答處理。如果對應的路由表記錄和路由發現表記錄都存在，但路由表記錄中狀態欄位的值爲 DISCOVERY_UNDERWAY，則設備將把路由表記錄中的狀態修改爲 ACTIVE 並把下一跳欄位的值設置爲路由應答命令訊框(Frame)前一個發送設備的位址；同時，設備還要把路由發現表記錄中剩餘成本欄位設置爲路由應答命令訊框(Frame)中路徑成本欄位的值。如果對應的路由表記錄中狀態欄位的值已經是 ACTIVE，則設備將比較路由應答命令訊框(Frame)中的路徑成本和路由發現表記錄中的剩餘成本。如果路由應答命令訊框(Frame)中的路徑成本小於剩餘成本，設備將更新路由發現表中的剩餘成本欄位和路由表中的下一跳欄位的值；如果路由應答中的路徑成本不小於剩餘成本，設備將丟棄該路由應答，不作進一步處理。如果接收路由應答的設備不是目的設備，設備就到路由發現表中

查找路由應答命令訊框(Frame)有效負載中發起位址和路由請求標識對應的記錄。如果沒有這樣的路由發現表記錄，設備將丟棄該路由應答命令訊框(Frame)；如果存在這樣的路由發現表記錄，設備將比較路由應答命令訊框(Frame)中的路徑成本值和路由發現表記錄中剩餘成本值。如果路由發現表記錄中的剩餘成本值小於路由應答命令中的路徑成本值，設備就丟棄該路由應答命令訊框(Frame)；否則，設備將查找路由應答中應答位址對應的路由表記錄。如果存在路由發現表記錄而找不到相應的路由表記錄，設備將丟棄路由應答命令訊框(Frame)。如果找到相應的路由表記錄，設備就把路由表記錄中下一跳欄位更新爲路由應答命令訊框(Frame)前一個發送設備的位址，並把路由發現表記錄中剩餘成本欄位的值更新爲路由應答命令訊框(Frame)的路徑成本值。完成這些路由記錄更新後，設備將向目的位址轉發路由應答。在轉發路由應答之前，設備還要更新路由應答命令訊框(Frame)中的路徑成本值。設備找到路由發現表中對應于路由請求標識和源位址的記錄，該記錄中發送設備位址欄位的值即爲路由應答的下一跳位址。計算當前設備到下一跳的鏈路成本並累加到路由應答命令訊框(Frame)的路徑成本欄位中，NWK 命令訊框(Frame)頭部分的目的位址欄位設爲下一跳位址，然後設備就調用 MCPS-DATA.request 原語把路由請求命令單播發到下一跳設備。MCPS-DATA.request 原語中 DstAddr 參數應設爲從路由發現表中得到的下一跳位址。

2.5.3.5 路由維護

每個設備的 NWK 層針對它需要發送資料訊框(Frame)的每個近鄰設備都有一個失敗計數器。任何一個發送鏈路失敗計數器的值超過 nwkcRepairThreshold 時，設備就要啓動路由修復程式。實現者可以選擇一種簡單的計算失敗的方法來產生失敗計數器的值，也可以選擇更精確的時間窗方法。需要注意的是，網路中不要過於頻繁地啓動路由修復，否則就會擁塞網路，影響正常的業務支援。

Mesh 網路中的路由修復。當 mesh 網路中一條鏈路或一個設備失敗時，上行設備將啓動路由修復程式。如果由於沒有路由能力或其他限制使得上行設備不能啓動路由修復，設備將向源設備發送路由錯誤命令，NWK 命令中的錯誤程式將指示出鏈路失敗的原因。如果上行設備能夠啓動路由修復，它將廣播路由請求命令來修復路由，路由請求命令中源位址設爲失敗鏈路上行設備的位址，目的位址設爲傳輸失敗的訊框(Frame)的目的位址。該路由請求命令訊框(Frame)有效負載中名列選項欄位的路由修復子域應設爲 1，表示這是路由修復的路由請求命令。當一個設備正在修復一個特定目的設備的路由時，它不應向該目的設備發送訊框(Frame)。對路由修復啓動時要傳送到目的設備的訊框(Frame)和在路由修復完成前又到達的訊框(Frame)，修復設備要麼把它們緩存起來，直到路由修復完成，要麼丟棄這些訊框(Frame)，具體採取哪種措施根據設備的能力來決定。當一個路由節點接收到路由請求命令訊框(Frame)時，它將根據前面介紹過的路由發現過程來處理。如果該路由節點或它的一個終端子設備是路由請求命令訊框(Frame)的目的位址，那麼該路由節點將回應看一個路由應答命令訊框(Frame)。路由應答命令訊框(Frame)有效負載中路由修復子域的值設爲 1，表示路由修復應答。如果在 nwkcRouteDiscoveryTime 毫秒內失敗鏈路的上行設備沒有收到路由應答命令訊框(Frame)，它將向失敗訊框(Frame)的源設備發送一個路由錯誤命令訊框(Frame)。如果上行設備在規定的時間內收到了路由修復應答命令訊框(Frame)，它將按照新的路由轉發那些緩存的資料。接收到路由錯誤命令訊框(Frame)的源設備如果沒有路由能力但 NIB 屬性 nwkUseTreeRouting 值等於 TRUE，它將採用分級路由演算法沿著樹向目的設備單播發送路由請求命令訊框(Frame)；如果源設備具有路由能力，它將啓動正常的路由發現

過程。如果一個 RFD 類型的終端設備不能向其父設備發送資訊，它將啓動孤立申明過程。如果終端設備孤立掃描成功並與父設備重新建立通訊，那麼該終端設備將恢復此前在網路中的操作。如果該終端設備的孤立掃描失敗，它將嘗試透過新的父設備重新加入網路，此時新的父設備要爲該終端設備分配一個新的 16 位網路位址。如果由於臨近區域內沒有能夠繼續接受子設備的設備使得終端設備找不到父設備，那麼該終端設備將不能重新加入到網路中。此時可能就需要人爲干預，使得其重新加入網路。

樹狀網路中的路由修復。當樹狀網路中的一個設備與父設備的信標失去同步或不能向父設備發送訊息時，它可能啓動孤立掃描過程搜索其關聯的父設備或啓動關聯過程定址一個新的父設備。如果孤立掃描失敗或設備重新與一個新的父設備關聯，它將從新的父設備收到一個新的 16 位元網路位址並恢復此前在網路中的操作。這樣，網路同樣還是以樹狀拓撲運行。設備在嘗試重新加入網路、得到新的網路位址之前，應使用 MAC 層解關聯程式與它所有的子設備解除關聯。如果該設備不能存取其子設備，那麼它就認爲該子設備已經與網路解關聯並把該子設備的 16 位元網路位址從近鄰表中刪除，然後設備才重新加入網路，開始以新的網路位址運行。如果一個設備不能向它的子設備發送訊息，它將丟棄該訊息並向訊框(Frame)的發起設備發送路由錯誤命令訊框(Frame)，表示訊息沒有送達目的位址。

2.5.4 信標發送時序

在多跳拓撲中爲了避免一個設備的信標訊框(Frame)與近鄰設備的信標訊框(Frame)或資料訊框(Frame)碰撞，信標發送的時序安排是必不可少的。然而，指示在樹狀拓撲中要求信標發送時序，而 mesh 拓撲並不需要，應爲 ZigBee mesh 網路中不允許發送信標。

ZigBee 協調器將決定網路中每個設備的信標階數和超訊框(Frame)階數。因爲多跳信標網路的一個目的就是允許路由節點有休眠的機會以省電，所以信標階數應設置得比超訊框(Frame)階數大得多。按照這種方式設置信標階數和超訊框(Frame)階數，可使任何鄰近區域內每個設備超訊框(Frame)的活動部分在時間上是互不重疊的。換句話說，把時間劃分成約（macBeaconInterval / macSuperframeDuration）個互不重疊的時隙，網路中每個設備超訊框(Frame)的活動部分分別佔用一個時隙。圖 24 是按照這種時序安排得到的一個信標設備的訊框(Frame)結構。

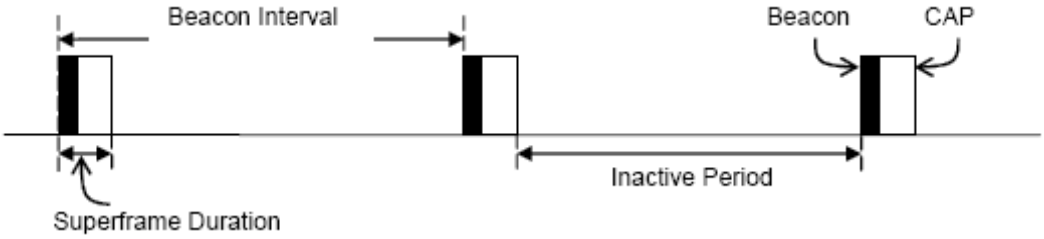


圖 24 ZigBee 信標設備的典型訊框(Frame)結構

設備的信標應用在時隙的起始點發送，發送時間是相對于父設備的信標發送時間來測定的。設備與父設備信標發送的時間偏移應包含在多跳信標網路每個設備信標訊框(Frame)的有效負載中。因此，一個設備接近到近鄰設備的信標訊框(Frame)後，不但知道了近鄰設備的信標發送時間，還知道了該近鄰設備父設備的信標發送時間。因爲用信標訊框(Frame)的時間戳減去時間偏移就可以得到父設備的信標發送時間。接收設備要把信標訊框(Frame)的時間戳和有效負載中的時間偏移都保存在近鄰表中。讓設備知道近鄰父設備的活動週期的目

的，是透過減輕隱藏節點問題維護父—子通訊鏈路的完整性。

樹狀網路中的通訊是使用父—子鏈路沿著樹安排路由來實現的。因爲每個子設備都要跟蹤父設備的信標訊框(Frame)，所以從父設備到子設備的發送是透過間接傳輸技術實現的。從子設備到父設備的發送則應在父設備的 CAP 週期內完成。一個新設備在加入網路的過程中，要根據 MAC 層掃描收集的資訊建立近鄰表。根據這些近鄰資訊，新設備將選擇一個合適的信標發送和 CAP 時間，使得其超訊框(Frame)結果的活動部分不會與任何一個近鄰設備或近鄰設備的父設備重疊。如果在鄰近區域內找不到不重疊的時隙，設備將不發送信標而只是以一個終端設備運行在網路中。如果有可用的不重疊時隙，新設備將選定其信標與父設備信標之間的時間偏移量，並包含到信標有效負載中。在保證互操作性的前提下，選擇信標發送時間，避免衝突的任何演算法都可以採用。爲了對抗漂移，新設備應跟蹤父設備的信標並適時調整自己的信標發送時間，使得它與父設備之間的信標發送時間保持不變。因此，網路中每個設備的信標訊框(Frame)必須與 ZigBee 協調器的信標訊框(Frame)保持同步。圖 25 是父—子設備超訊框(Frame)的位置關係。

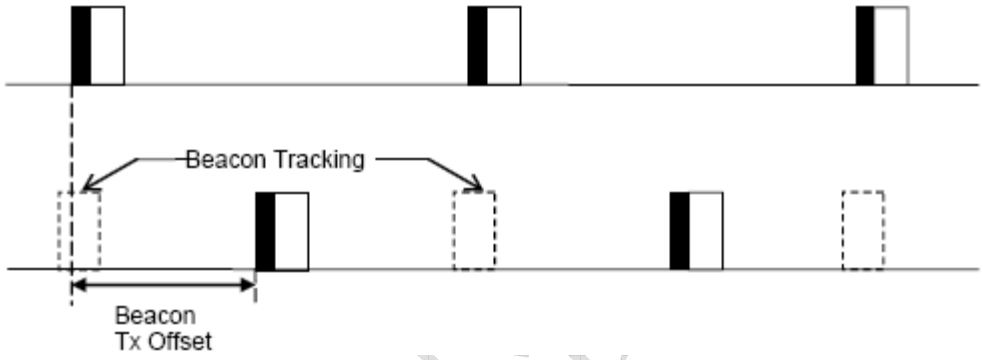


圖 25 父—子設備超訊框(Frame)的位置關係

網路支援的設備密度與超訊框(Frame)階數和信標階數之比成反比。超訊框(Frame)階數和信標階數的壁紙越小，每個設備的非活動週期就越長，那麼在同一個鄰近區域內就有更多的設備可以發送信標訊框(Frame)。在樹狀網路中推薦使用的超訊框(Frame)階數是 0，即超訊框(Frame)時長是 15.36ms，推薦使用的信標階數是 6～10，即信標間隔在 0.98304～15.72864s。使用推薦的超訊框(Frame)和信標配置，網路中設備的典型占空比將在約 2%～0.1%。

爲了使用上述信標時序演算法，必須對 IEEE 802.15.4 的 MAC 子層作些增強。MLME-START.request 原語中應增加一個參數 StartTime，用來指定開始發送信標的時間。該原語的新格式如下：

MLME-START.request（PANId，LogicalChannel，BeaconOrder，SuperframeOrder，PANCoordinator，BatteryLifeExtension，CoordRealignment，SecurityEnable，StartTime）

2.5.5 廣播通訊

ZigBee 網路中的任何一個設備都可以啓動廣播發送，向同一網路中的其他設備廣播網路層資料訊框(Frame)。APS 子層實體把 NLDE-DATA.request 原語的 DstAddr 參數設爲 0xffff 就啓動了廣播發送過程。爲了廣播 MSDU，NWK 層向 MAC 子層發送 MCPS-DATA.request 原語。原語中 DstAddrMode 參數設爲 0x02，表示使用 16 位網路位址；DstAddr 參數設爲廣播網路位址 0xffff；PANId 參數設爲 ZigBee 網路的 PAN 標識。目前 1.0 版本的 ZigBee 規範

不支援在多個網路間的廣播。廣播發送不使用 MAC 層確認，而在非信標網路中取而代之的是一種被動確認機制。被動確認的原理是每個設備保持監測每個近鄰設備是否成功轉發了廣播訊框(Frame)。禁止 MAC 層確認是透過設置 TxOptions 參數的確認傳輸標誌位元爲 FALSE 來實現的，該參數中其他標誌位元的設置應根據網路配置來設置。

每個設備都應記錄任何新的廣播事務，不管是本地發起的廣播還是從近鄰設備接收的廣播訊框(Frame)。記錄廣播資訊的記錄叫作“廣播事務記錄（BTR）”，它至少包含廣播訊框(Frame)的序號和源位址。BTR 保存在廣播事務表（BTT）中。設備從近鄰設備接收到廣播訊框(Frame)後，就把廣播訊框(Frame)中的序號和源位址與 BTT 中的記錄進行比較。如果設備 BTT 中有該廣播訊框(Frame)的記錄，設備就更新 BTR，記下轉發該訊框(Frame)的近鄰設備，然後丟棄廣播訊框(Frame)。如果 BTT 中沒有該廣播訊框(Frame)的記錄，它將產生一條新的 BTR，記下轉發該訊框(Frame)的近鄰設備，然後 NWK 層把新接收廣播訊框(Frame)的訊息通知給上層。如果半徑欄位的值大於 0，設備就轉發該廣播訊框(Frame)；否則，設備就丟棄該廣播訊框(Frame)。轉發廣播訊框(Frame)之前，設備將等待一個隨機時間週期 — 廣播抖動，廣播抖動的範圍由屬性 nwkMaxBroadcastJitter 的值來限定。如果接收到廣播訊框(Frame)時，設備 NWK 層發現 BTT 已滿並且沒有過時的記錄，設備就忽略該廣播訊框(Frame)，不轉發也不向上層報告。在非信標 ZigBee 網路中，如果在 nwkPassiveAckTimeout 秒時間內設備的任何一個近鄰都沒有轉發前一個廣播訊框(Frame)，設備就重發前一個廣播訊框(Frame)，最多重發 nwkMaxBroadcastRetries 次。從建立 BTR 開始，nwkNetworkBroadcastDeliveryTime 秒後設備就把記錄的狀態改爲過時，此後如果新接收的廣播訊框(Frame)需要空間就可以覆蓋過時的 BTR 了。

當 MAC PIB 屬性 macRxOnWhenIdle 等於 FALSE 的 ZigBee 路由器收到廣播訊框(Frame)時，它將採用不同的程式來轉發廣播訊框(Frame)。此時，ZigBee 路由器將使用 MAC 層單播，以不延時的方式向它的各個近鄰設備轉發該訊框(Frame)。類似的，如果 ZigBee 路由器的屬性 macRxOnWhenIdle 等於 TRUE，並且有一個或多個近鄰設備的 macRxOnWhenIdle 屬性等於 FALSE，那麼設備出了執行一般的廣播程式外，還要用 MAC 層單播依次向這些近鄰設備轉發廣播訊框(Frame)。爲了保證這些單播到達目的設備，ZigBee 路由器可以採用間接發送方式。爲了方便重發廣播訊框(Frame)，每個 ZigBee 路由器的 NWK 層至少能夠緩存 1 訊框(Frame)資料。

圖 26 是一個設備與兩個近鄰設備之間廣播事務的資訊流程。

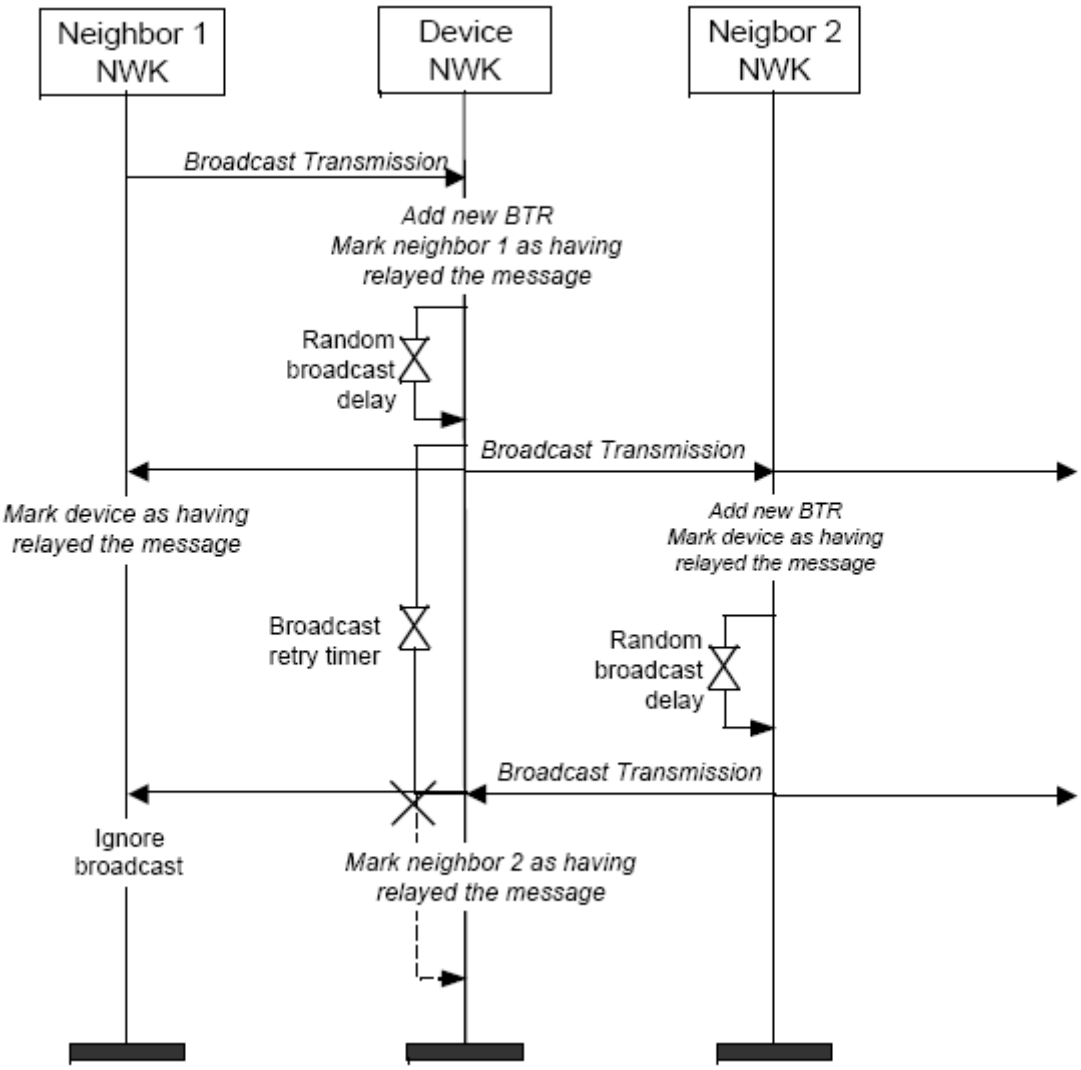


圖 26 近鄰設備間廣播事務的資訊流程

2.5.6 MAC 信標中的 NWK 資訊

NWK 層使用 MAC 子層信標訊框(Frame)的有效負載向近鄰設備傳遞 NWK 層資訊。當設備信標訊框(Frame)超訊框(Frame)配置欄位的官來你允許子域設置爲 1 時，表示該設備允許關聯。信標中包含的網路資訊使得正在執行網路發現的新設備能夠方便選擇網路和關聯設備。當設備信標訊框(Frame)超訊框(Frame)配置欄位的關聯允許子域設置爲 0 時，表示該設備不允許關聯，信標有效負載不必包含這些網路資訊。MAC 子層信標訊框(Frame)有效負載的格式如下：

位:0～7	8～11	12～15	16～17	18	19～22	23	24～47
協定 ID	協定堆疊配置檔	協定版本	預留	路由器能力	設備深度	終端設備能力	發送偏移量（可選）

信標有效負載中，協定 ID 欄位表示當前使用的網路層協定的標識碼，其取值範圍是 0x00～0xff；協定堆疊配置檔欄位表示 ZigBee 協定堆疊配置檔的標識碼，其取值範圍是 0x00～

0x0f；協定版本欄位表示 ZigBee 協定的版本，其取值範圍是 0x00～0x0f；路由器能力欄位設爲 TRUE 表示設備能夠接受具有路由器功能的設備的入網請求，否則就設爲 FALSE；設備深度欄位表示設備在拓撲樹上的深度，即到 ZigBee 協調器的最小跳數，其取值範圍是 0x00～nwkMaxDepth，0x00 表示設備就是 ZigBee 協調器；終端設備能力欄位設爲 TRUE 表示設備能夠接受 ZigBee 終端設備的入網請求，否則就設爲 FALSE；發送偏移欄位表示設備俄與其父設備發送信標的時間差，其取值範圍是 0x000000～0xffffff，時間單位是符號週期。用設備的信標發送時間減去該事件便宜就可以得到父設備的信標發送時間。

ZigBee 協調器的 NWK 層在新網路建立後立即更新信標有效負載；其他 ZigBee 設備則在完成關聯後和網路配置改變時，立即更新信標有效負載。設備使用 MLME-SET.request 原語把信標有效負載寫到 MAC 子層 PIB 中。信標有效負載的長度寫在屬性 macBeaconPayloadLength 中，信標有效負載部分的內容寫在屬性 macBeaconPayload 中。

3. 安全服務規範

3.1 安全服務規範概述

ZigBee 提供的安全服務包括密鑰建立、密鑰運輸、訊框(Frame)保護和設備管理的方法。這些服務共同構成了 ZigBee 設備的安全體系。我們知道，ZigBee 協定棧是以 IEEE 802.15.4 爲基礎的，所以 ZigBee 安全體系是對 802.15.4 安全規範的補充和增強。|ZigBee 安全體系提供的安全級別依賴於對稱密鑰的保密讀、使用的保護機制、加密機制的正確實現和相關的安全規定。

由於受成本限制，ZigBee 設備中使用同一射頻終端的不同應用不是邏輯隔離。另外，一個設備不能辨別另一個設備是否實現了不同應用之間的加密隔離，甚至不能判別自身協定棧的不同層間是否進行了加密隔離；所以 ZigBee 設備使用同一射頻端的不同應用是相互信任的，並且各種應用對協定堆疊下層（如 APS、NWK 或 MAC）的存取時完全通暢的。所有這些使得 ZigBee 設備是一個開放的信任模型；協定堆疊的不同層和雲行在同一設備上的不同應用都是互相信任的。歸納起來就是，ZigBee 提供的安全服務只在不同設備的介面間提供加密保護，而不提供同一設備不同協定層之間介面的加密隔離。

ZigBee 的開放信任模型允許同一設備的不同層使用相同的密鑰材料，允許在設備到設備的基礎上實現端到端的安全，而不需在兩個通訊設備的特定層間來實現。在網路安全上還要考慮的一個問題是：是否允許未經允許的惡意網路設備使用網路來傳輸訊框(Frame)？基於這些情況，ZigBee 系統的安全體系設計需要作如下選擇：第一，必須遵循“訊框(Frame)的發起層負責訊框(Frame)的最初安全處理”的原則。例如，如果 MAC 層解關聯訊框(Frame)需要保護，就要使用 MAC 層安全處理；同樣，如果 NWK 命令訊框(Frame)需要保護，就要使用 NWK 層安全處理。第二，如果要防止惡意設備盜用網路服務，則除了路由器和新加入網路之間的通訊訊框(Frame)外，對其他訊框(Frame)都要使用 NWK 層安全處理。這樣，只要加入網路並成功獲取網路密鑰的設備才能以一跳以上的方式在網路傳遞訊框(Frame)。第三，開放的信任模型允許每層可以重複使用密鑰來提供安全保護，如啓動的網路密鑰將用於保護 APS 層廣播訊框(Frame)、NWK 訊框(Frame)和 MAC 層命令訊框(Frame)。重複使用密鑰有利於降低儲存成本。第四，爲了簡化設備間的互操作，網路中的所有設備以及設備中的所有層都使用相同的安全級別。特別是 PIB 和 NIB 中的安全級別指示應該相同。如果一個

應用需要的安全級別高於網路提供的安全等級，那麼它只有獨立構造一個更高安全級別的網路。此外，在實現中還必須正確處理並在應用配置檔中包含下面幾條規則：處理加密和解密包時的錯誤；檢測並處理計數器失步和計數器溢出；檢測並處理密鑰失步；在需要時週期性地更新過期的密鑰。

ZigBee 網路的安全是基於鏈路密鑰和網路密鑰的。兩個對等的 APL 實體之間單播通訊的安全保護採用兩設備共用的 128 位元鏈路密鑰；而廣播通訊的安全保護則採用網路中所有設備共用的 128 位元網路密鑰。設備透過密鑰運輸、密鑰建立或預先安裝來獲得鏈路密鑰；透過密鑰運輸或預先安裝啦 ihuode 網路密鑰。用以獲取鏈路密鑰的密鑰建立技術是基於主密鑰的，設備應透過密鑰運輸或預先安裝的方式來獲得主密鑰。一個安全網路能夠提供多種安全服務，在使用時最好避免不同的安全服務重複使用相同的密鑰，因爲這種多餘的交互可能會帶來安全漏洞。使用不相關的密鑰能夠保證執行不同安全協定時的邏輯隔離。運輸主密鑰用密鑰載入密鑰來保護，運輸其他密鑰則用密鑰運輸密鑰來保護。網路密鑰可用於 ZigBee 的 MAC 層、NWK 層和 APL 層，這樣，所有這些層都可以得到同樣的網路密鑰和相關的發送和接收訊框(Frame)計數器；而鏈路密鑰和主密鑰可以只用於 APS 子層，這樣就只有 APL 層能得到該鏈路密鑰和主密鑰。

ZigBee 應用採用 802.15.4 無線標準進行通訊。IEEE802.15.4 定義了 PHY 層和 MAC 層，ZigBee 在這兩層的基礎上構建了 NWK 層和 APL 層。PHY 層提供物理射頻的基本通訊能力；MAC 層提供的服務保證了設備間單跳鏈路的可靠通訊；ZigBee NWK 層提供了構建不同網路拓撲所需要的路由和多跳高你；APL 層包括 APS 子層、ZDO 和各種應用。ZDO 負責整個設備的管理，APS 子層爲 ZDO 和 ZigBee 應用提供服務。ZigBee 安全體系涉及 ZigBee 協定棧的三層，MAC、NWK 和 APS 層分別負責各自訊框(Frame)的安全傳輸。此外，APS 子層還提供安全關係建立和維護的服務，ZDO 管理一個設備的安全規定和安全配置。

當 MAC 層發起的訊框(Frame)需要保護時，ZigBee 就使用 IEEE 802.15.4 標準定義的 MAC 層安全機制。ZigBee 對 IEEE 802.15.4 標準 MAC 層的加密演算法 CCM 稍作修改得到了 CMM*演算法。CMM*在包含 CCM 所有特徵的基礎上，增加了只加密和只完整性驗證的安全保護能力。有了 CMM*的這些額外能力，ZigBee 就可以不使用 IEEE 802.15.4 標準定義的 CTR 和 CBC-MAC 安全演算法，簡化安全處理。另外，MAC 層的其他安全模式不同的安全級別要求不同的密鑰，而使用 CMM*可以把同一個密鑰用於 CMM*的所有安全級別。如果在 ZigBee 協定堆疊全部使用 CMM*，則 MAC、NWK 和 APS 層可以重複使用同一個密鑰。

MAC 層負責自己的安全處理，但上層將決定 MAC 層使用的安全級別。ZigBee 中需要安全的訊框(Frame)將用 MAC PIB 屬性 macDefaultSecurityMaterial 或 macACLEntryDescriptorSet 中的安全材料進行處理。上層設置的 macDefaultSecurityMaterial 應與 NWK 層的網路密鑰和計數器一致，設置的 macACLEntryDescriptorSet 應與 APS 層的任何鏈路密鑰一致。使用的安全套件應爲 CMM*，上層設置的安全級別應與 NIB 屬性 nwkSecurityLevel 的值一致。在 ZigBee 中，MAC 層鏈路密鑰是首選的。如果得不到 MAC 層鏈路密鑰就用預設的密鑰。圖 27 是 ZigBee 的 MAC 層訊框(Frame)使用安全處理的例子。

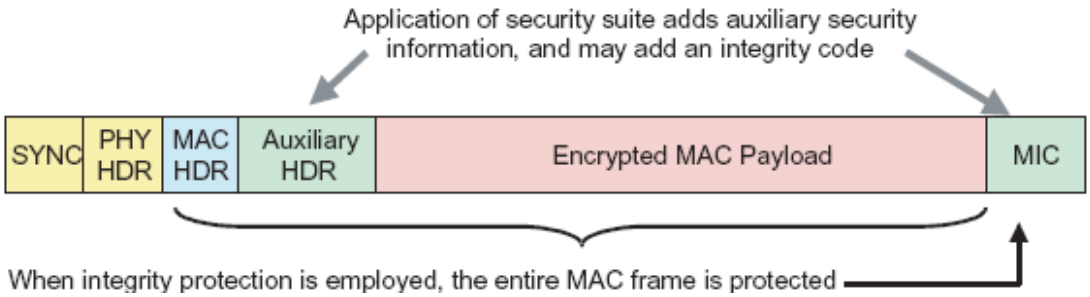


圖 27 採用 MAC 層安全處理的 ZigBee 訊框(Frame)

當 NWK 層發起的訊框(Frame)需要安全保護時，或是上層發起的訊框(Frame)、NIB 屬性 nwkSecureAllFrames 等於 TRUE 並且 NLDE-DATA.request 原語中 SecurityEnable 參數不等於 FALSE 時，ZigBee 將使用 NWK 層訊框(Frame)保護機制對訊框(Frame)進行安全處理。類似 MAC 層，NWK 層訊框(Frame)保護也要使用高級加密標準（AES）和 CMM*加模式。NWK 訊框(Frame)使用的安全級別由 NIB 屬性 nwkSecurityLevel 來設定。上層對 NWK 層安全的管理主要表現在設置啓動的網路密鑰和備用網路密鑰，決定 NWK 層安全級別。我們知道，NWK 層的任務之一是在多跳鏈路上發送資訊；而作爲該任務的一部分，NWK 層要向近鄰設備廣播路由請求訊息並處理接收的路由應答訊息。如果有合適的鏈路密鑰可用，NWK 層將使用鏈路密鑰對輸出的 NWK 訊框(Frame)進行處理；如果沒有可用的鏈路密鑰，爲了防止非法使用者聽到訊息，NWK 層將使用啓動的網路密鑰來處理輸出的 NWK 訊框(Frame)，用啓動的或備用的網路密鑰來處理經過安全保護的輸入 NWK 訊框(Frame)。在這種情況下，訊框(Frame)格式明確指示出訊框(Frame)保護所使用的密鑰，接收設備就可以知道使用什麼密鑰來處理輸入的訊框(Frame)，並且可以判斷出接收的訊框(Frame)是網路中所有設備都可讀的還是僅僅接收設備自身可讀。圖 28 是對 NWK 訊框(Frame)進行安全處理的例子。

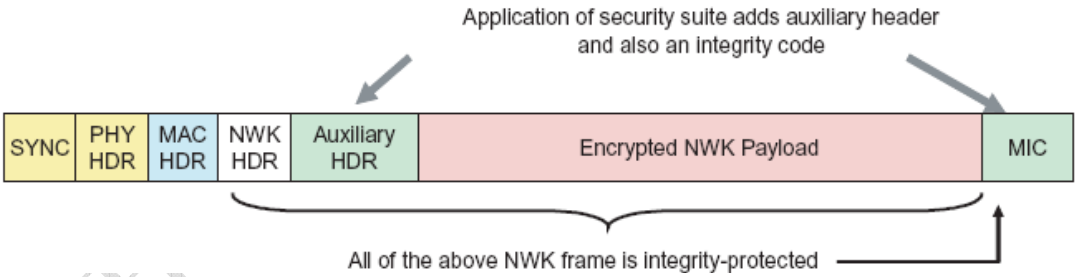


圖 28 採用 NWK 層安全處理的 ZigBee 訊框(Frame)

當 APL 層發起的訊框(Frame)需要安全保護時，APS 子層將對它進行安全處理。APS 層對訊框(Frame)的安全處理可以基於鏈路密鑰或網路密鑰。圖 29 是對 APL 訊框(Frame)進行安全處理的例子。APS 層的另一個安全職責是爲應用和 ZDO 提供密鑰建立、密鑰傳遞和設備管理服務。

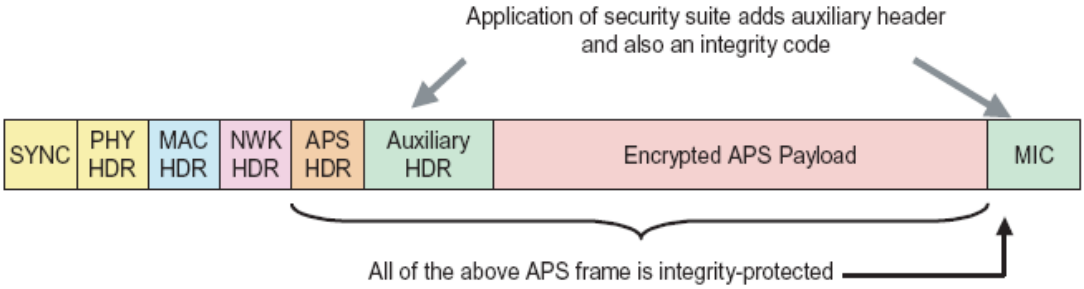


圖 29 採用 APS 層安全處理的 ZigBee 訊框(Frame)

APS 子層密鑰建立服務提供的機制，使得一個 ZigBee 設備可以透過另一個 ZigBee 設備推導出共用的鏈路密鑰。密鑰建立過程包括發起設備和回應設備兩個實體。密鑰建立從信用提供步驟開始。信用資訊（如主密鑰）提供建立鏈路密鑰的起始點，提供信用資訊可以採用帶內或帶外方式。一旦提供了信用資訊，密鑰建立協定就包括 3 步：瞬息資料交換，使用瞬息資料得到鏈路密鑰，對鏈路密鑰計算正確的確認。在對稱密鑰建立（SKKE）協定中，發起設備使用主密鑰在回應設備的配合下建立起鏈路密鑰。主密鑰可能是設備製造過程中預裝的、信用中心安裝的或是基於使用者輸入資料（如 PIN、口令或密鑰等）產生的。爲了維持整個信用基礎，ZigBee 必須相信主密鑰的安全性和真實性。

密鑰傳遞服務提供了安全和不安全的密鑰傳遞方式。安全的密鑰傳遞命令提供了一種從密鑰源（如信用中心）向其他設備傳遞主密鑰、鏈路密鑰、網路密鑰的方式。不安全的密鑰傳遞命令提供了一種向設備載入初始密鑰的方式。這種方法對載入的密鑰不作加密保護。爲了實現不加密的密鑰傳遞安全性，可以在帶外通道上傳送密鑰傳遞命令。

設備更新服務提供了一種安全方式，一個設備（如 ZigBee 路由器）借助這種方式通知第二個設備（如信用中心），告知第三個設備的狀態發生了改變，需要更新（如設備加入或離開網路）。透過這種方式，信用中心就能維護一個網路中活動設備的精確列表。

刪除設備服務提供了一種安全方式，使得一個設備（如信用中心）能夠借助這種方式通知另一個設備（如路由器），告知其一個子設備將被從網路中刪除。例如，當一個設備不滿足信用中心對網路設備的安全要求時，信用中心就可以使用刪除設備服務來刪除該設備。

請求密鑰服務提供了一種安全方式，使得一個設備可以借助這種方式向另一個設備（如信用中心）請求當前網路密鑰或端到端應用主密鑰。轉換密鑰服務提供了一種安全方式，使得一個設備可以通知另一個設備切換使用不同啓動網路密鑰。

出於安全目的，ZigBee 定義了信任中心的任務。信用中心是網路中設備都信任的、爲網路和端到端應用配置管理分配密鑰的一個設備。網路中每個設備只能認可一個信用中心，並且每個安全網路中也只能有一個信用中心。在高安全要求的商業應用中，一個預載入了信用中心位址和初始主密鑰的設備承擔信用中心的任務。如果應用能忍受瞬間的攻擊，則主密鑰也可以採用帶內非安全的密鑰傳輸方式來發送。如果信用中心不是預載入的，則 PAN 協調器就是預設的信任中心或由 PAN 協調器指定的設備作信用中心。在低安全要求的住宅應用中，設備使用網路密鑰與信用中心安全通訊，網路密鑰可以預配置或透過帶內非安全密鑰傳遞方式傳遞。信用中心執行的功能可細分爲三部分：信用管理器、網路管理器和配置管理器。設備信任信用管理器和配置管理器。網路管理器負責網路管理，向其管理的設備分發網路密鑰和維護網路密鑰。配置管理器負責綁定兩個應用並保證它管理的設備間端到端的通訊安全。爲了簡化信用管理，這三種管理功能是集中於同一個設備的，即信用中心。

3.2 MAC 層安全服務

MAC 層的安全處理包括安全發送流出的 MAC 訊框(Frame)和安全接收流入的 MAC 訊框(Frame)。上層透過設置密鑰、訊框(Frame)計數器和安全級別來控制 MAC 安全處理操作。以下是 MAC 層對流出 MAC 訊框(Frame)和流入 MAC 訊框(Frame)安全處理的詳細步驟。

3.2.1 流出 MAC 訊框(Frame)的安全處理

一個 MAC 訊框(Frame)由訊框(Frame)頭 MacHeader 和有效負載 Payload 組成。MAC 訊框(Frame)的安全處理按照以下步驟進行：

1. 從 MAC PIB 獲取安全材料，包括密鑰、流出訊框(Frame)計數器 FrameCount、密鑰序號計數器 SeqCount 和安全等級標識碼。首先，MAC 層嘗試在 MAC PIB 屬性 macACLEntryDescriptorSet 中查找流出訊框(Frame)目的位址對應的安全材料和安全級別標識碼。如果查找失敗，MAC 層就在 MAC PIB 屬性 macDefaultSecurityMaterial 中查找安全材料，在 macDefaultSecuritySuite 中查找安全等級。如果 4 位元組長度的流出訊框(Frame)計數器的值等於 2^{32}-1 或找不到安全材料中的部分元素，則安全處理失敗，不再對訊框(Frame)做進一步安全處理。

2. 設置安全控制欄位 SecField。安全控制欄位長度是 1 位元組，其中安全級別子域長度是 3 位，設置爲第 1 步得到的安全等級標識碼；密鑰標識碼子域長度是 2 位，設置爲 00；擴充現時值子域長度是 1 位，設置爲 0；最後兩個預留位設置爲 00。

3. 執行 CMM*模式的加密和認證操作。根據安全級別得到對應的完整性認證序列長度 M（位元組）；比特串 Key 是從安全材料中得到的密鑰；13 位元組長度的現時值 N 由本地設備的 64 位元擴充位址、安全控制欄位 SecFiled 和訊框(Frame)計數器 FrameCount 構成。如果安全級別要求加密，那麼位元組串 a 設爲 MacHeader，位元組串 m 設爲 Payload；否則，位元組串 a 設爲 MacHeader || Payload，位元組串 m 長度爲 0。

4. 如果第 3 步 CMM*模式的輸出爲“invalid”，則安全處理失敗，不做進一步處理；否則用 c 表示上面第 3 步的輸出結果。

5. 如果安全級別要求加密，則安全處理後的流出 MAC 訊 框 (Frame) 尾 MacHeader || FrameCount || SeqCount || c；否則，安全處理後的流出 MAC 訊框(Frame)爲 MacHeader || FrameCount || SeqCount || Payload || c。

6. 如果經過安全處理後 MAC 訊框(Frame)長度大於 aMaxPHYPacketSize，則安全處理失敗，不做進一步處理；否則，執行下一步操作。

7. 流出 MAC 訊框(Frame)計數器加 1，並保存到第 1 步獲取安全材料的位置。

3.2.2 流入 MAC 訊框(Frame)的安全處理

MAC 層接收到的安全訊框(Frame)由訊框(Frame)頭 MacHeader、訊框(Frame)計數器 ReceivedFrameCount、序號計數器 ReceivedSeqCount 和有效負載 SecuredPayload 組成。MAC 層對流入安全訊框(Frame)的處理過程如下：

1. 如果 ReceivedFrameCount 的值爲 2^{32}-1，則安全處理失敗，不做進一步處理；否則，

執行下一步操作。

2. 從 MAC PIB 獲取安全材料，包括密鑰、可選的外部訊框(Frame)計數器 FrameCount、可選的密鑰序號計數器 SeqCount 和安全等級標識碼。首先，MAC 層嘗試在 MAC PIB 屬性 macACLEntryDescriptorSet 中查找流出訊框(Frame)目的位址對應的安全材料和安全級別標識碼。如果查找失敗，MAC 層就在 MAC PIB 屬性 macDefaultSecurityMaterial 中查找安全材料，在 macDefaultSecuritySuite 中查找安全等級。如果不能獲得安全材料或存在的 SeqCount 與 ReceivedSeqCount 不匹配，則安全處理失敗，不再做進一步處理。

3. 如果 FrameCount 存在且 ReceivedFrameCount 小於 FrameCount，則安全處理失敗，不再做進一步處理；否則，執行下一步操作。

4. 設置安全控制欄位 SecField。安全控制欄位長度是 1 位元組，其中安全級別子域長度是 3 位，設置爲第 1 步得到的安全等級標識碼；密鑰標識碼子域長度是 2 位，設置爲 00；擴充現時值子域長度是 1 位，設置爲 0；最後兩個預留位設置爲 00。

5. 執行 CCM*模式的解密和完整性校驗操作。根據安全級別得到對應的完整性認證序列長度 M（位元組）；比特串 Key 是從安全材料中得到的密鑰；13 位元組長度的現時值 N 是由發送設備的 64 位元擴充位址、安全控制欄位 SecField 和訊框(Frame)計數器 ReceivedFrameCount 構成的。把字串 SecuredPayload 分割成兩部分 Payload1 || Payload2，其中右邊部分長度是 M 位元組。如果安全級別要求加密，那麼位元組串 a 設爲 MacHeader || ReceivedFrameCount || ReceivedSeqCount，位元組串 c 設爲 SecurePayload；否則，位元組串 a 設爲 MacHeader || ReceivedFrameCount || ReceivedSeqCount || Payload1，位元組串 c 設爲 Payload2。

6. 返回 CCM*操作的結果。如果上一步輸出爲“invalid”，則安全處理失敗，不做進一步處理；否則，用 m 表示流入訊框(Frame)安全處理後的結果。如果安全級別要求加密，則解密處理後的 MAC 訊框(Frame)UnsecuredMacFrame 等於 a || m；否則，UnsecuredMacFrame 等於 a。

7. 如果可選的 FrameCount 存在，則把它設置爲 ReceivedFrameCount 的值並更新 MAC PIB 的相關屬性值。

3.2.3 與安全有關的 MAC PIB 屬性

CCM*模式使用的安全材料與 IEEE 802.15.4 中 CCM 模式使用的安全材料一樣。對於 MAC PIB 屬性 macDefaultSecurityMaterial，上層設置對稱密鑰、流出訊框(Frame)計數器和可選的外部密鑰序號計數器。外部密鑰序號計數器等於 NIB 中網路安全材料描述符 nwkSecurityMaterialSet 的 nwkActiveKeySeqNumber 屬性值。macDefaultSecurityMaterial 安全材料不使用外部訊框(Frame)計數器，可選的外部密鑰序號計數器等於網路密鑰的序號。對於屬性 macACLEntryDescriptorSet，上層設置對稱密鑰和流出訊框(Frame)計數器。此時，流出訊框(Frame)計數器等於 AIB 屬性 apsDeviceKeyPairSet 中網路密鑰對描述符相應元素的值。可選的外部訊框(Frame)計數器應設爲流入訊框(Frame)計數器的值，不使用外部密鑰序號計數器。

3.3 NWK 層安全服務

NWK 層的安全處理包括安全發送流出的 NWK 訊框(Frame)和安全接收流入的 NWK 訊框(Frame)。上層透過設置密鑰、訊框(Frame)計數器和安全級別來控制 NWK 安全處理操作。下面介紹 NWK 層對流出 NWK 訊框(Frame)和流入 NWK 訊框(Frame)安全處理的詳細步驟。

3.3.1 流出 NWK 訊框(Frame)的安全處理

一個 NWK 訊框(Frame)包含訊框(Frame)頭 NwkHeader 和有效負載 Payload。如果 NWK 訊框(Frame)要求安全處理並且 nwkSecurityLevel > 0，則按照以下步驟進行安全處理：

1. 從 NIB 中獲取 nwkActiveKeySeqNumber 並用來查找啓動的網路密鑰；從 NIB 屬性那 nwkSecurityMaterialSet 中獲取流出訊框(Frame)計數器 OutgoingFrameCount 和密鑰序號 KeySeqNumber；從 NIB 屬性 nwkSecurityLevel 中獲取安全級別。如果流出訊框(Frame)計數器的值等於 2^{32}-1 或不能獲取密鑰，則安全處理失敗，不做進一步處理；否則，執行下一步操作。

2. 構造輔助訊框(Frame)頭 AuxiliaryHeader。安全控制欄位的安全級別子域按照第 1 步獲取的安全級別進行設置，密鑰標識子域設置爲 01 表示網路密鑰，擴充現時值子域設置爲 1。源位址欄位設爲本地設備的 64 位元擴充位址。訊框(Frame)計數器欄位設置爲第 1 步得到的流出訊框(Frame)計數器的值。密鑰序號欄位設置爲第 1 步得到的密鑰序號。

3. 執行 CCM*模式的加密和認證操作根據安全級別得到對應的完整性認證序列長度 M（位元組）；比特串 Key 是第 1 步得到的密鑰；13 位元組長度的現時值 N 是由第 2 步的安全控制欄位、訊框(Frame)計數器欄位和源位址欄位構成的。如果安全級別要求加密，則位元組串 a 設爲 NwkHeader || AuxiliaryHeader，位元組串 m 設爲 Payload；否則，位元組串 a 設爲 NwkHeader || AuxiliaryHeader || Payload，位元組串 m 設爲長度爲 0 的空值。

4. 如果上一步 CCM*操作的輸出爲“invalid”，則安全處理失敗，不做進一步處理；否則，用 c 表示上一步的輸出。

5. 如果安全級別要求加密，則安全處理後的訊框(Frame)爲 NwkHeader || AuxiliaryHeader || c；否則，安全處理後的流出訊框(Frame)爲 NwkHeader || AuxiliaryHeader || Payload || c。

6. 如果經過安全處理後 NWK 訊框(Frame)長度大於 aMaxMACFrameSize，則安全處理失敗，不做進一步處理；否則，執行下一步操作。

7. 把流出訊框(Frame)計數器的值加 1，並保存到 NIB 屬性 nwkActiveKeySeqNumber 對應安全材料描述符的 OutgoingFrameCounter 元素中，即更新密鑰對應的輸出訊框(Frame)計數器的值。

8. 用“000”覆蓋安全控制欄位中安全級別子域的值。

3.3.2 流入 NWK 訊框(Frame)的安全處理

NWK 層接收到的安全訊框(Frame)由訊框(Frame)頭 NwkHeader、輔助訊框(Frame)頭 AuxiliaryHeader 和有效負載 SecuredPayload 組成。NWK 層對流入安全訊框(Frame)的處理過程也能夠如下：

1. 從 NIB 屬性 nwkSecurityLevel 獲知安全級別並用它覆蓋接收訊框(Frame)輔助訊框(Frame)頭部分的安全控制欄位安全級別子域；從輔助訊框(Frame)頭 AuxiliaryHeader 得到序號 SequenceNumber、發送設備位址 SenderAddress 和接收訊框(Frame)計數器

ReceivedFrameCount。如果得到的 ReceivedFrameCount 值等於 2^{32}-1，則安全處理失敗，不再做進一步處理；否則執行下一步操作。

2. 透過 SequenceNumber 與 NIB 屬性 nwkSecurityMaterialSet 中密鑰序號的匹配，獲得相應的安全材料（包括密鑰和其他屬性）。如果得不到安全材料，則安全處理失敗，不再做進一步處理。如果接收訊框(Frame)的 SequenceNumber 是比 nwkSecurityMaterialSet 中的所有序號更新的一個密鑰序號，並且源位址爲信用中心，則把 NIB 屬性 nwkActiveKeySeqNumber 的值設爲接收訊框(Frame)的 SequenceNumber 值。

3. 如果安全材料中存在一個 SenderAddress 對應的流入訊框(Frame)計數器 FrameCount，但 ReceivedFrameCount 小於 FrameCount，則安全處理失敗，不再做進一步處理；否則，執行下一步操作。

4. 執行 CCM*模式解密和完整性校驗操作。根據安全級別得到對應的完整性校驗序列長度 M（位元組）；比特串 Key 是從安全材料中得到的密鑰；13 位元組長度的現時值 N 由 AuxiliaryHeader 中的安全控制欄位、訊框(Frame)計數器欄位和源位址欄位構成。把字串 SecuredPayload 分割成兩部分 Payload1 || Payload2，其中右邊部分長度是 M 位元組。如果安全級別要求加密，那麼位元組串 a 設爲 NwkHeader || AuxiliaryHeader，位元組串 c 設爲 SecuredPayload；否則，位元組串 a 設爲 NwkHeader || AuxiliaryHeader || Payload1，位元組串 c 設爲 Payload2。

5. 返回 CCM*操作結果。如果上一步輸出爲“invalid”，則安全處理失敗，不做進一步處理；否則用 m 表示流入訊框(Frame)安全處理後的結果。如果安全級別要求加密，則解密處理後的 NWK 訊框(Frame)UnsecuredNwkFrame 等於 a || m；否則，UnsecuredNwkFrame 等於 a。

6. 把 FrameCount 設爲（ReceivedFrameCount+1），並把 FrameCount 和 SenderAddress 儲存到 NIB 中。

3.3.3 與安全有關的 NIB 屬性

下面這些 NWK PIB 屬性都是與 NWK 層安全管理相關的屬性。它們都可以分別用 NLME-GET.request 和 NLME-SET.request 原語來讀和寫。

nwkSecurityLevel 是流入和流出 NWK 訊框(Frame)的安全級別。該屬性的取值範圍是 0x00～0x07，不同取值所表示的安全操作在後面章節將有詳細介紹。

nwkSecurityMaterialSet 是一組網路安全材料描述符，它可以包含 0、1 或 2 個描述符。網路安全材料描述符包含的元素有密鑰序號 KeySeqNumber、流出訊框(Frame)計數器 OutgoingFrameCounter、流入訊框(Frame)計數器描述符 IncomingFrameCounterSet 和密鑰 Key。其中流入訊框(Frame)計數器描述符 IncomingFrameCounterSet 由兩部分組成：發送設備位址 SenderAddress 和流入訊框(Frame)計數器 IncomingFrameCounter。

nwkActiveKeySeqNumber 是 nwkSecurityMaterialSet 中啓動的網路密鑰的序號，其取值範圍是 0x00～0xff。

nwkAllFresh 是一個布林量，用以指示在流入訊框(Frame)計數器超出時是否要對所有流入的 NWK 訊框(Frame)做新鮮度檢測。

nwkSecureAllFrame 是一個布林量，用以指示是否對所有流入和流出的 NWK 訊框(Frame)做安全處理。如果該屬性爲 TRUE，則除了訊框(Frame)控制欄位中安全子域爲 0 的當前設備接收訊框(Frame)外，設備還要對所有的流入和流出 NWK 訊框(Frame)做安全處理。當該

屬性爲 TRUE 時，NWK 層不轉發訊框(Frame)控制欄位中安全子域爲 0 的 NWK 訊框(Frame)。但需要注意的是，NLDE-DATA.request 原語中 SecurityEnable 參數的優先順序高於 nwkSecureAllFrame 屬性。

3.4 APS 層安全服務

APS 層的安全處理安全發送流出的 APS 訊框(Frame)、安全接收流入的 APS 訊框(Frame)以及安全監理和管理密鑰。上層透過向 APS 發送原語來管理密鑰，這些原語將在後續章節中詳細描述。在對流出訊框(Frame)進行保護時，安全級別也由上層來制定。

3.4.1 流出 APS 訊框(Frame)的安全處理

APS 訊框(Frame)有訊框(Frame)頭 ApsHeader 和有效負載 Payload 兩部分，APS 訊框(Frame)的安全處理遵照以下步驟：

1. 獲取安全材料和密鑰標識 KeyIdentifier。當要處理的事 APSDE-DATA.request 原語請求發送的 APS 資料訊框(Frame)時，如果 useNwkKeyFlag 參數爲 TRUE，則根據 NIB 屬性 nwkActiveKeySeqNumber 到 nwkSecurityMaterialSet 中查找相應的啓動網路密鑰、流出訊框(Frame)計數器、密鑰序號等安全材料。KeyIdentifier 應設爲 01，表示網路密鑰。如果 useNwkKeyFlag 參數爲 FALSE ,則從 AIB 屬性 apsDeviceKeyPairSet 中獲取流出訊框(Frame)目的位址對應的安全材料。如果才喲娜個間接定址傳輸訊框(Frame)，則目的位址應爲綁定管理器的位址。KeyIdentifier 應設爲 00，表示資料密鑰。當要處理的事 APS 命令訊框(Frame)時，首先嘗試從 AIB 屬性 apsDeviceKeyPairSet 中獲取流出訊框(Frame)目的位址對應的安全材料。除密鑰傳遞命令外，KeyIdentifier 都應設爲 00，表示資料密鑰。如果密鑰傳遞命令傳遞的是網路密鑰，則 KeyIdentifier 應設爲 02，表示密鑰傳遞密鑰；如果密鑰傳遞命令傳遞的是應用鏈路密鑰、應用主密鑰或信用中心主密鑰，則 KeyIdentifier 應設爲 03，表示密鑰載入密鑰。如果從 AIB 中獲取安全材料失敗，則根據 nwkActiveKeySeqNumber 到 NIB 中查找相應的安全材料。KeyIdentifier 設爲 01，表示網路密鑰。

2. 如果密鑰標識 KeyIdentifier 等於 01（即網路密鑰），則 APS 在安全處理之前首先要核實 NWK 層沒有應用安全處理。如果 NWK 層應用了安全處理，APS 層不作任何網路安全處理。APS 層根據 NIB 屬性 nwkSecureAllFrames 值爲 TRUE 和 nwkSecurityLevel 值不爲零，就可以知道 NWK 層使用了安全處理。

3. 從第 1 步得到的安全材料中提取流出訊框(Frame)計數器。如果 KeyIdentifier 等於 01，則還要提取密鑰序號。如果流出訊框(Frame)計數器的值等於 2^{32}-1 或得不到密鑰，則安全處理失敗，不再作進一步處理；否則，執行下一步操作。

4. 從 NIB 屬性 nwkSecurityLevel 獲取安全級別 如果要處理的事 APS 命令訊框(Frame)，則安全級別強制爲 7，即 ENC-MIC-128。

5. 構造 APS 輔助訊框(Frame)頭。安全控制欄位中安全級別子域爲第 4 步獲得的安全等級；密鑰標識子域設爲 KeyIdentifier；擴充現時值子域設爲 0。訊框(Frame)計數器欄位設爲第 3 步得到的流出訊框(Frame)計數器的值。如果 KeyIdentifier 等於 01，則輔助訊框(Frame)頭中存在密鑰序號欄位並設爲第 3 步得到的密鑰序號；否則，輔助訊框(Frame)頭部分不存在密鑰序號欄位。

6. 執行 CCM*模式的加密和認證操作。根據安全級別得到對應的完整性校驗序列長度 M（位元組）；比特串 Key 是第 1 步得到的密鑰；13 位元組長度的現時值 N 是由第 5 步得到的安全控制欄位、訊框(Frame)計數器欄位和當前設備的 64 位元擴充位址構成。如果安全級別要求加密，則位元組串 a 設爲 ApsHeader || AuxiliaryHeader，位元組串 m 設爲 Payload；否則，位元組串 a 設爲 ApsHeader || AuxiliaryHeader || Payload，位元組串 m 設爲長度爲 0 的空值。

7. 如果上一步 CCM*操作的輸出爲“invalid”，則安全處理失敗，不再作進一步處理；否則，用 c 表示上一步的輸出。

8. 如果安全級別要求加密，則安全處理後的訊框(Frame)爲 ApsHeader || AuxiliaryHeader || c；否則，安全處理後的流出訊框(Frame)爲 ApsHeader || AuxiliaryHeader || Payload || c。

9. 如果經過安全處理後的 APS 訊框(Frame)將導致 MSDU 長度大於 aMaxMACFrameSize，則安全處理失敗，不做進一步處理；否則，執行下一步操作。

10. 把流出訊框(Frame)計數器加 1，並根據安全處理中使用的密鑰把訊框(Frame)計數器的值保存到 NIB、AIB 和 MAC PIB 的適當位置。

11. 用“000”覆蓋安全控制欄位的安全級別子域。

3.4.2 流入 APS 訊框(Frame)的安全處理

APS 層接收到的安全訊框(Frame)由訊框(Frame)頭 ApsHeader、輔助訊框(Frame)頭 AuxiliaryHeader 和經過安全處理的有效負載 Payload 組成。APS 層對流入安全訊框(Frame)的處理過程如下：

1. 從輔助訊框(Frame)頭 AuxiliaryHeader 中得到密鑰序號 SequenceNumber、密鑰標識 KeyIdentifier 和接收訊框(Frame)計數器的值 ReceivedFrameCounter。如果接收訊框(Frame)計數器 ReceivedFrameCounter 的值等於 2^{32}-1，則安全處理失敗，不再做進一步處理；否則，執行下一步操作。

2. 以 APS 訊框(Frame)的源位址爲索引，從 AIB 位址映射表中得到源位址 SourceAddress。如果得不到源位址或源位址不完整，則安全處理失敗，不再做進一步處理。如果 ApsHeader 部分訊框(Frame)控制欄位的發送模式子域等於 1，即間接定址，則源位址應爲綁定管理器的位址。

3. 根據密鑰標識 KeyIdentifier 得到合適的安全材料。如果 KeyIdentifier 爲“00”（即資料密鑰），則從 AIB 屬性 apsDeviceKeyPairSet 中獲取與流入訊框(Frame)SourceAddress 對應的安全材料。如果 KeyIdentifier 爲“01”（即網路密鑰），則從 NIB 屬性 nwkSecurityMaterialSet 中獲取與 SequenceNumber 匹配的安全材料。如果接收訊框(Frame)的密鑰序號比 nwkSequenceMaterialSet 中的序號更新，則把 nwkActiveKeySeqNumber 設置爲接收訊框(Frame)的密鑰序號值。如果此時能從 AIB 中找到與流入訊框(Frame)SourceAddress 對應的安全材料，則安全處理失敗，不再做進一步處理。如果 KeyIdentifier 爲“02”（即密鑰傳遞密鑰），則從 AIB 屬性 apsDeviceKeyPairSet 中獲取與流入訊框(Frame)SourceAddress 對應的安全材料並從安全材料中密鑰傳遞密鑰。如果 KeyIdentifier 爲“03”（即密鑰載入密鑰），則從 AIB 屬性 apsDeviceKeyPairSet 中獲取與流入訊框(Frame)SourceAddress 對應的安全材料並從安全材料中得到密鑰載入密鑰。

4. 如果第 3 步得到的安全材料中有一個與 SourceAddress 對應的流入訊框(Frame)計數器 FrameCount，但 ReceivedFrameCount 的值小於 FrameCount，則安全處理失敗，不再做進一

步處理；否則，執行下一步操作。

5. 獲取安全級別 SecLevel。如果 ApsHeader 部分訊框(Frame)控制欄位的訊框(Frame)類型子域指示接收訊框(Frame)爲 APS 資料訊框(Frame)，則 SecLevel 應設爲 NIB 屬性 nwkSecurityLevel 的值；否則，SecLevel 應設爲 7（即 ENC-MIC-128）。用 SecLevel 覆蓋 AuxiliaryHeader 部分安全控制欄位安全級別子域的值。

6. 執行 CCM*模式的解密和完整性校驗。根據安全級別得到對應的完整性校驗序列長度 M（位元組）；比特串 Key 是從安全材料中得到的密鑰；13 位元組長度的現時值 N 由 AuxiliaryHeader 中的安全控制欄位、訊框(Frame)計數器欄位和 SourceAddress 欄位構成。把字串 SecuredPayload 分割成兩部分 Payload1 || Payload2，其中右邊部分長度是 M 位元組。如果安全級別要求加密，那麼字串 a 設爲 ApsHeader || AuxiliaryHeader，位元組串 c 設爲 SecuredPayload；否則，位元組串 a 設爲 ApsHeader || AuxiliaryHeader || Payload1，位元組串 c 設爲 Payload2。

7. 返回 CCM*操作結果。如果上一步輸出爲“invalid”，則安全處理失敗，不做進一步處理；否則用 m 表示流入訊框(Frame)安全處理後的結果。如果安全級別要求加密，則解密處理後的 APS 訊框(Frame)UnsecuredApsFrame 等於 a || m；否則，UnsecuredNwkFrame 等於 a。

8. 把 FrameCount 設爲（ReceivedFrameCount+1）並把 FrameCount 和 SourceAddress 儲存到合適的安全材料中。

3.4.3 建立密鑰服務

APSME 提供的建立密鑰服務允許兩個設備相互配合建立鏈路密鑰。在運行密鑰建立協定之前，每個設備上必須安裝初始信用資訊（如主密鑰）。提供建立密鑰服務的原語包括請求原語 APSME-ESTABLISH-KEY.request、證實原語 APSME-ESTABLISH-KEY.confirmed、指示原語 APSME-ESTABLISH-KEY.indication 和回應原語 APSME-ESTABLISH-KEY.response。

1. 請求原語 APSME-ESTABLISH-KEY.request

APSME-ESTABLISH-KEY.request 原語用來啓動密鑰建立協定。當一個設備需要與另一個設備安全通訊時使用該原語。一個設備將充當啓動設備，另一個設備充當響應設備。啓動設備發出 APSME-ESTABLISH-KEY.request 原語並在參數中指明回應設備的位址和使用的密鑰建立協定(即 SKKE 直接或間接)，啓動密鑰建立協定。APSME-ESTABLISH-KEY.request 原語提供以下介面：

APSME-ESTABLISH-KEY.request（ResponderAddress，UseParent，ResponderParentAddress，KeyEstablishmentMethod）

其中：參數 ResponderAddress 是回應設備的 64 位元擴充位址；參數 UseParent 是一個布林量，用來指示是否使用回應設備的父設備來轉發訊息；如果 UseParent 爲 TRUE，則參數 ResponderParentAddress 包含的是回應設備父設備的 64 位元擴充位址，否則不使用也不需要設置 ResponderParentAddress 參數；參數 KeyEstablishmentMethod 表示請求的密鑰建立方法，取值 0x00 表示 SKKE，0x01～0x03 暫時預留。

當啓動設備要求與一個回應設備建立鏈路密鑰時，其上層就產生 APSME-ESTABLISH-KEY.request 原語。如果啓動設備出於 NWK 安全目的希望使用回應設備的父設備作聯絡時，它將設置 UseParent 參數爲 TRUE 並在 ResponderParentAddress 參數

中指定回應設備父設備的 64 位元擴充位址。APSME 接收到 KeyEstablishmentMethod 參數等於 SKKE 的 APSME-ESTABLISH-KEY.request 原語就執行 SKKE 協定。本地 APSME 是 SKKE 協定的發起設備，ResponderAddress 參數指定設備的 APSME 是協定的回應設備。UseParent 參數控制是否需要透過回應設備的父設備來間接向回應設備發送訊息。

2. 證實原語 APSME-ESTABLISH-KEY.confirm

密鑰建立協定執行完成或失敗後，APSME 向 ZDO 發送證實原語 APSME-ESTABLISH-KEY.confirm。該原語提供以下介面：

APSME-ESTABLISH-KEY.confirm（Address，Status）

其中：參數 Address 表示與當前設備一起執行密鑰建立協定的設備 64 位元擴充位址；參數 Status 表示執行密鑰建立協定的最終狀態。在密鑰建立協定執行完成後，回應設備和發起設備的 APSME 都要向 ZDO 發送 APSME-ESTABLISH-KEY.confirmed 原語。如果密鑰建立成功，發起設備和回應設備都將更新 AIB 的相關屬性，記錄新的鏈路密鑰，發起設備就可以與回應設備安全通訊。如果密鑰建立不成功，則 AIB 不改變。

3. 指示原語 APSME-ESTABLISH-KEY.indication

回應設備接收到發起設備的密鑰建立初始資訊時，APSME 就向 ZDO 發送密鑰建立指示原語 APSME-ESTABLISH-KEY.indication。該原語提供以下介面：

APSME-ESTABLISH-KEY.indication（InitiatorAddress，KeyEstablishmentMethod）

其中：參數 InitiatorAddress 是密鑰建立協定發起設備的 64 位元擴充位址；參數 KeyEstablishmentMethod 表示建立密鑰的方法。回應設備收到發起設備的密鑰建立請求，並且 AIB 中存在發起設備的主密鑰時，回應設備 APSME 向 ZDO 發送密鑰建立指示原語。ZDO 收到 APSME-ESTABLISH-KEY.indication 原語後，根據原語參數來決定是否與發起設備俄建立一個密鑰，並用 APSME-ESTABLISH-KEY.response 原語作出回應。

4. 回應原語 APSME-ESTABLISH-KEY.response

回應設備 ZDO 用 APSME-ESTABLISH-KEY.response 原語來回應密鑰建立指示原語。ZDO 決定是繼續還是終止與發起設備的密鑰建立過程，並在 Accept 參數中指示它的決定。APSME-ESTABLISH-KEY.response 原語提供的介面如下：

APSME-ESTABLISH-KEY.response（InitiatorAddress，Accept）

其中：參數 InitiatorAddress 表示密鑰建立發起設備的 64 位元擴充位址；參數 Accept 是布林量，表示是否接受發起設備的密鑰建立請求。如果 Accept 參數值爲 TRUE，回應設備的 APSME 將執行 KeyEstablishmentMethod 參數指定的密鑰建立協定；如果 Accept 參數值爲 FALSE，回應設備的 APSME 將終止執行密鑰建立協定並清除密鑰建立協定相關的中間資料。

圖 30 是兩個設備成功建立密鑰的資訊流程。

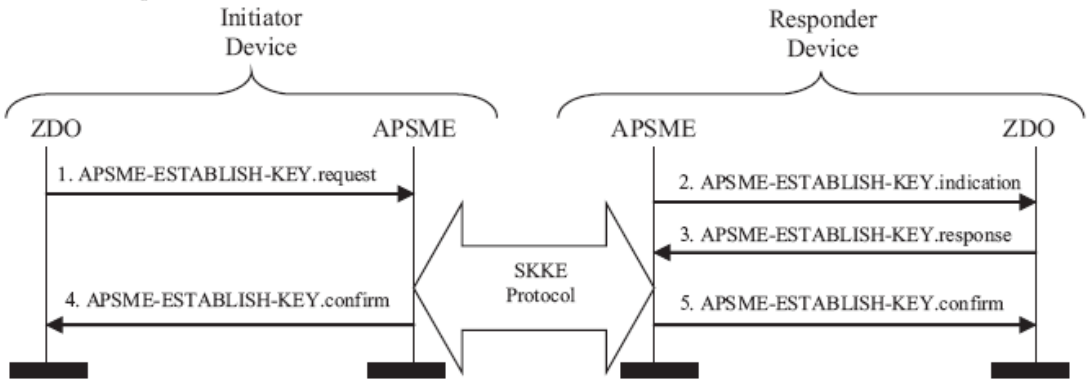


圖 30 兩個設備成功建立密鑰的資訊流程

3.4.4 傳遞密鑰服務

APSME 提供的傳遞密鑰服務，允許發起設備向回應設備傳遞密鑰材料。發起設備要向響應設備發送密鑰時，發起設備 ZDO 就產生 APSME-TRANSPORT-KEY.request 原語。密鑰傳遞請求原語提供的介面如下：

APSME-TRANSPORT-KEY.request（DestAddress，KeyType，TransportKeyData）

其中：參數 DestAddress 表示目的設備的 64 位元擴充位址；參數 KeyType 是傳遞的密鑰材料的類型標識碼，0x00 代表信用中心主密鑰，0x01 代表網路密鑰，0x02 代表應用主密鑰，0x03 代表應用鏈路密鑰；參數 TransportKeyData 是傳遞的密鑰和有關使用參數。TransportKeyData 參數的類型與 KeyType 參數值有關，如果 KeyType=0x00，TransportKeyData 參數的內容包括 DestAddress 父設備的 64 位元位址 ParentAddress 和 16 位元組長度的信用中心主密鑰 Trust-Mater-Key；如果 KeyType=0x01，TransportKeyData 參數的內容包括網路密鑰序號 KeySeqNumber、16 位元組長度的網路密鑰 NetworkKey、是否使用目的設備父設備的指示參數 UseParent 和目的設備的父設備位址 ParentAddress；如果 KeyType=0x02 或 0x03，TransportKeyData 參數的內容包括 64 位元擴充位址 ParentAddress、目的設備是否請求主密鑰的指示參數 Initiator 和 16 位元組長度的應用主密鑰或鏈路密鑰。

APSME 收到 APSME-TRANSPORT-KEY.request 原語後，產生一個傳遞密鑰命令包。如果 KeyType 參數值爲 0x00（即信用中心主密鑰），傳遞密鑰命令的密鑰描述符欄位要做如下設置：密鑰子域設爲 TransportKeyData 參數中 Trust-Master-Key 的值；目的位址子域設爲 DestAddress 參數值；源位址子域設爲當前設備的位址。該命令訊框(Frame)要進行安全保護，如果安全處理成功，APSME 就調用 NLDE-DATA.request 原語把該命令發送到 TransportKeyData 參數中 ParentAddress 指定的設備。如果 KeyType 參數值爲 0x01（即網路密鑰），傳遞密鑰命令中密鑰子域設爲 TransportKeyData 參數中 NetworkKey 的值；序號子域設爲 TransportKeyData 參數中 KeySeqNumber 的值；目的位址子域設爲 DestAddress 參數值；源位址子域設爲當前設備的位址。該命令訊框(Frame)要進行安全保護，如果安全處理成功，APSME 就調用 NLDE-DATA.request 原語把該命令發送到指定的設備。如果 TransportKeyData 參數中 UseParent 等於 TRUE，APSME 把密鑰傳遞命令發送給 TransportKeyData 參數中 ParentAddress 指定的設備；否則，APSME 把密鑰傳遞命令發送給 DestAddress 參數指定的設備。如果 KeyType 參數值爲 0x02 或 0x03（即應用主密鑰或鏈路密鑰），傳遞密鑰命令中密鑰子域設爲 TransportKeyData 參數中 Key 的值；合作設備位址子域設爲 TransportKeyData 參數中 ParentAddress 的值；如果 TransportKeyData 參數中 Initiator 的值爲 TRUE，發起設備子域設爲 1，否則，發起設備子域設爲 0。密鑰傳遞命令訊框(Frame)需要進行安全保護，如果安全處理成功，APSME 就調用 NLDE-DATA.request 原語把該命令發送到 DestAddress 指定的設備。

設備接收到密鑰傳遞命令，成功解密和完整性那個校驗得到密材料後，使用指示原語 APSME-TRANSPORT-KEY.indication 來通知 ZDO。APSME-TRANSPORT-KEY.indication 原語提供的介面如下：

APSME-TRANSPORT-KEY.indication（SrcAddress，KeyType，TransportKeyData）

其中：參數 SrcAddress 是傳遞密鑰原始設備的 64 位元擴充位址；參數 KeyType 是傳遞的密鑰材料的類型標識碼，0x00 表示信用中心主密鑰，0x01 代表網路密鑰，0x02 代表應用主密

鑰，0x03 代表應用鏈路密鑰；參數 TransportKeyData 是傳遞的密鑰和有關使用參數。TransportKeyData 參數的類型與 KeyType 參數值有關，如果 KeyType=0x00，則 TransportKeyData 參數是 16 位元組長度的信用中心主密鑰 Trust-Mater-Key；如果 KeyType=0x01，則 TransportKeyData 參數的內容包括網路密鑰序號 KeySeqNumber、16 位元組長度的網路密鑰 NetworkKey；如果 KeyType=0x02 或 0x03，則 TransportKeyData 參數的內容包括 64 位元擴充位址 PartnerAddress、目的設備是否請求主密鑰的指示參數 Initiator 和 16 位元組長度的應用主密鑰或鏈路密鑰。

接收到傳遞密鑰命令後，APSME 將執行流入訊框(Frame)安全處理，然後檢測密鑰類型欄位的值。如果密鑰類型欄位的值爲 2 或 3（即應用主密鑰或鏈路密鑰），則 APSME 產生的原語 APSME-TRANSPORT-KEY.indication 中 SrcAddress 參數設爲密鑰傳遞命令訊框(Frame)的來源位址；KeyType 參數設爲命令訊框(Frame)中密鑰類型欄位的值；TransportKeyData 參數中 Key 設爲命令訊框(Frame)中密鑰欄位的值，PartnerAddress 設爲命令訊框(Frame)中合作設備欄位的值。如果命令訊框(Frame)中發起設備欄位的值爲 1，則 TransportKeyData 參數中 Initiator 設爲 TRUE；否則，Initiator 設爲 FALSE。如果密鑰類型欄位的值爲 0 或 1（即信用中心主密鑰或 NWK 密鑰）並且目的位址欄位等於當前設備位址，則 APSME 產生的原語 APSME-TRANSPORT-KEY.indication 中 SrcAddress 參數設爲密鑰傳遞命令訊框(Frame)的來源位址；KeyType 參數設爲命令訊框(Frame)中密鑰類型欄位的值；TransportKeyData 參數中 Key 設爲命令訊框(Frame)中密鑰欄位的值。在傳遞網路密鑰時，TransportKeyData 參數中 KeySeqNumber 參數還要設爲命令訊框(Frame)中序號欄位的值。如果密鑰類型欄位的值爲 0 或 1（即信用中心主密鑰或 NWK 密鑰）但目的位址欄位不等於當前設備位址，APSME 將調用 NLDE-DATA.request 原語把密鑰傳遞命令轉發給目的位址欄位指定的設備。

接收到沒有經過安全處理的密鑰傳遞命令訊框(Frame)時，APSME 也要檢測密鑰類型欄位。如果密鑰類型欄位爲 0（即信用中心主密鑰）目的位址欄位等於當前設備位址，並且設備沒有信用中心主密鑰和位址，則 APSME 將向 ZDO 發送 APSME-TRANSPORT-KEY.indication 原語。如果密鑰類型欄位爲 1（即網路密鑰），目的位址欄位等於當前設備位址，並且設備沒有網路密鑰，則 APSME 將向 ZDO 發送 APSME-TRANSPORT-KEY.indication 原語。原語中 SrcAddress 參數設爲密鑰傳遞命令訊框(Frame)中來源位址欄位的值；KeyType 參數設爲命令訊框(Frame)中密鑰類型欄位的值；TransportKeyData 參數中 Key 設爲命令訊框(Frame)中密鑰欄位的值，如果傳遞的是網路密鑰，則 TransportKeyData 參數中 KeySeqNumber 還要設爲命令訊框(Frame)中序號欄位的值。

3.4.5 設備更新服務

APSME 提供的設備更新服務允許一個設備（如路由器）向另一個設備（如信用中心）通知第三個設備的狀態改變情況（如加入或離開網路）。當設備需要向另一個設備發送其他設備狀態更新資訊時，ZDO 發出設備更新請求原語。APSME-UPDATE-DEVICE.request 原語提供的介面如下：

APSME-UPDATE-DEVICE.request（DestAddress，DeviceAddress，Status，DeviceShortAddress）

其中：參數 DestAddress 表示發送設備更新資訊的目的位址；參數 DeviceAddress 是發生狀態更新的設備的 64 位元擴充位址；Status 表示 DeviceAddress 指定設備的更新狀態，其值 0x00

表示設備以安全方式入網，0x01 表示設備以非安全方式入網，0x02 表示設備離開網路，0x03～0x07 爲預留值；參數 DeviceShortAddress 是狀態更新設備的 16 位元網路位址。接收到 APSME-UPDATE-DEVICE.request 原語後，APSME 將首先產生更新設備命令訊框(Frame)。命令訊框(Frame)中設備位址欄位設爲 DeviceAddress 參數值；狀態欄位設爲 Status 參數值；設備短位址欄位設爲 DeviceShortAddress 參數值。更新設備命令訊框(Frame)需要做安全保護，如果安全處理成功，APSME 就調用 NLDE-DATA.request 原語把安全處理過的命令訊框(Frame)發送給 DestAddress 參數指定的設備。

設備 APSME 收到更新設備命令訊框(Frame)後，就向 ZDO 發送設備更新指示原語。APSME-UPDATE-DEVICE.indication 原語提供的介面如下：

APSME-UPDATE-DEVICE.indication（SrcAddress，DeviceAddress，Status，DeviceShortAddress）

其中：參數 SrcAddress 表示設備更新命令訊框(Frame)發起設備的 64 位元擴充位址；其他參數的定義與 APSME-UPDATE-DEVICE.request 原語相同。

3.4.6 刪除設備服務

APSME 提供的刪除設備服務允許一個設備（如信用中心）通知另一個設備（如路由器），告知其一個子設備將被刪除出網路。當設備請求一個父設備把它的一個子設備從網路中刪除時，ZDO 就向 APSME 發送刪除設備請求原語。APSME-REMOVE-DEVICE.request 原語提供的介面如下：

APSME-REMOVE-DEVICE.request（ParentAddress，ChildAddress）

其中：參數 ParentAddress 表示設備請求其刪除子設備的父設備的 64 位元擴充位址；ChildAddress 表示被請求刪除的子設備位址。接收到 APSME-REMOVE-DEVICE.request 原語後，設備將首先產生刪除設備命令訊框(Frame)。命令訊框(Frame)中子設備位址欄位設爲 ChildAddress 參數值。刪除設備命令訊框(Frame)需要做安全保護，如果安全處理成功，APSME 就調用 NLDE-DATA.request 原語把安全處理過的命令訊框(Frame)發送給 ParentAddress 參數指定的設備。

設備收到刪除設備命令訊框(Frame)後，APSME 就向 ZDO 發送刪除設備指示原語 APSME-REMOVE-DEVICE.indication。該原語提供的介面如下：

APSME-REMOVE-DEVICE.indication（SrcAddress，ChildAddress）

其中：參數 SrcAddress 表示請求當前設備刪除一個子設備的設備位址；ChildAddress 表示被請求刪除的當前設備的子設備位址。

3.4.7 請求密鑰服務

APSME 提供的請求密鑰服務允許設備向另一個設備請求當前網路密鑰或主密鑰。APSME-REQUEST-KEY.request 原語允許 ZDO 請求當前網路密鑰或一個新的端到端應用主密鑰。該原語提供的介面如下：

APSME-REQUEST-KEY.request（DestAddress，KeyType，PartnerAddress）

其中：參數 DestAddress 表示請求密鑰命令訊框(Frame)的目的位址；參數 KeyType 表示請求的密鑰類型，其取值 0x01 表示網路密鑰，0x02 表示應用密鑰，其他值暫時預留；當 KeyType

爲應用密鑰時，PartnerAddress 參數是一個設備的 64 位元擴充位址，當前設備請求密鑰時，PartnerAddress 參數指定的設備將接收到同樣的密鑰。接收到 APSME-REQUEST-KEY.request 原語後，設備將首先產生請求密鑰命令訊框(Frame)。命令訊框(Frame)中密鑰類型欄位設爲 KeyType 參數值；如果 KeyType 參數值爲 0x02，則命令訊框(Frame)中伴隨設備欄位設爲 PartnerAddress 參數值。請求密鑰命令訊框(Frame)需要做安全保護，如果安全處理成功，APSME 就調用 NLDE-DATA.request 原語把安全處理過的命令訊框(Frame)發送給 DestAddress 參數指定的設備。

設備收到請求密鑰命令訊框(Frame)後，APSME 就向 ZDO 發送 APSME-REQUEST-KEY.indication 原語。請求密鑰指示原語提供的介面如下：

APSME-REQUEST-KEY.indicatrion（SrcAddress，KeyType，PartnerAddress）

其中：參數 SrcAddress 表示發送請求密鑰命令訊框(Frame)的設備位址；其餘兩個參數的定義與 APSME-REQUEST-KEY.request 原語相同。

3.4.8 切換密鑰服務

APSME 提供的切換密鑰服務允許一個設備（如信用證用心）通知另一個設備切換到新的網路密鑰。APSME-SWITCH-KEY.request 原語提供的介面如下；

APSME-SWITCH-KEY.request（DestAddress，KeySeqNumber）

其中：參數 DestAddress 表示切換密鑰命令的目的設備位址；參數 KeySeqNumber 表示新的啓動網路密鑰的序號。接收到 APSME-SWITCH-KEY.request 原語後，設備將首先產生切換密鑰命令訊框(Frame)，命令訊框(Frame)中序號欄位設爲 KeySeqNumber 參數值。切換密鑰命令訊框(Frame)需要做安全保護，如果安全處理成功，APSME 就調用 NLDE-DATA.request 原語把安全處理過的命令訊框(Frame)發送給 DestAddress 參數指定的設備。

設備收到切換密鑰命令訊框(Frame)後，APSME 就向 ZDO 發送 APSME-SWITCH-KEY.indication 原語。切換密鑰指示原語提供的介面如下：

APSME-SWITCH-KEY.indicaton（SrcAddress，KeySeqNumber）

其中：參數 SrcAddress 表示發送切換密鑰命令的源設備位址；參數 KeySeqNumber 表示新的啓動網路密鑰的序號。

3.4.9 APS 安全命令訊框(Frame)

APS 層與安全相關的命令訊框(Frame)有建立密鑰命令訊框(Frame)、傳遞密鑰命令訊框(Frame)、更新設備命令訊框(Frame)、刪除設備命令訊框(Frame)、請求密鑰命令訊框(Frame)和切換密鑰命令訊框(Frame)。這些命令的名稱和對應標識碼如表 21 所列，其中前 4 個命令是建立密鑰命令。

表 21 APS 層安全相關命令名稱和標識

命令名稱	標識值	命令名稱	標識值
APS_CMD_SKKE_1	0x01	APS_CMD_UPDATE_DEVICE	0x06
APS_CMD_SKKE_2	0x02	APS_CMD_REMOVE_DEVICE	0x07
APS_CMD_SKKE_3	0x03	APS_CMD_REQUEST_KEY	0x08
APS_CMD_SKKE_4	0x04	APS_CMD_SWITCH_KEY	0x09
APS_CMD_TRANSPORT_KEY	0x05		

密鑰建立過程中使用的 APS 命令訊框(Frame)有 APS_CMD_SKKE_1、APS_CMD_SKKE_2、APS_CMD_SKKE_3 和 APS_CMD_SKKE_4。SKKE 命令訊框(Frame)的一般格式如下：

位元組數：1	1	8	8	16
訊框(Frame)控制	命令標識碼	發起設備位址	回應設備位址	資料
APS 頭	有效載荷			

其中**命令標識碼**欄位指示了 APS 命令類型，4 種 SKKE 訊框(Frame)SKKE-1、SKKE-2、SKKE-3 和 SKKE-4 的命令標識碼分別是 0x01、0x02、0x03 和 0x04。**發起設備位址**欄位是密鑰建立協定發起設備的 64 位元擴充位址。**回應設備位址**欄位是密鑰建立協定回應設備的 64 位元擴充位址。SKKE 命令訊框(Frame)中資料欄位的內容與命令標識碼欄位有關。

傳遞密鑰命令訊框(Frame)的格式如下：

位元組數：1	1	1	可變長度
訊框(Frame)控制	APS 命令標識碼	密鑰類型	密鑰描述符
APS 頭	有效載荷		

這裡 **APS 命令標識碼**欄位設爲 0x05。**密鑰類型**欄位爲 0x00 表示信用中心主密鑰，0x01 表示網路密鑰，0x02 表示應用主密鑰，0x03 表示應用鏈路密鑰。**密鑰描述符**欄位的內容與密鑰類型欄位有關，它包含的是沒有經過安全處理的密鑰和相關參數。信用中心主密鑰描述符由 16 位元組的密鑰、8 位元組的目的位址和 8 位元組的源位址構成。網路密鑰描述符由 16 位元組的密鑰、1 位元組的密鑰序號、8 位元組的目的位址和 8 位元組的源位址構成。應用主密鑰和鏈路密鑰描述符由 16 位元組的密鑰、8 位元組的伴隨設備位址和 1 位元組發起設備標誌構成。

APS 更新設備命令訊框(Frame)的格式如下：

位元組數：1	1	8	2	1
訊框(Frame)控制	APS 命令標識碼	設備位址	設備短位址	狀態

APS 頭	有效載荷

這裡 **APS 命令標識碼**欄位設爲 0x06。**設備位址**欄位是發生狀態更新的設備的 64 位元擴充位址；**設備短位址**欄位是發送狀態更新的設備的 16 位元短位址。**狀態**欄位爲 0x00 表示設備以安全方式加入網路、0x01 表示設備以非安全方式加入網路、0x03 表示設備離開網路。

APS 刪除設備命令訊框(Frame)的格式是如下：

位元組數：1	1	8
訊框(Frame)控制	APS 命令標識碼	子設備位址
APS 頭	有效載荷	

這裡 **APS 命令標識碼**欄位設爲 0x07。**子設備位址**欄位是該命令意圖刪除的子設備 64 位元擴充位址。

APS 請求密鑰命令訊框(Frame)的格式如下：

位元組數：1	1	1	8
訊框(Frame)控制	APS 命令標識碼	密鑰類型	伴隨設備位址
APS 頭	有效載荷		

這裡 **APS 命令標識碼**欄位設爲 0x08。如果命令請求的是網路密鑰，則密鑰類型欄位設爲 1；如果請求的是應用密鑰，則密鑰類型欄位設爲 2。當密鑰類型欄位的值爲 2 時，伴隨設備位址欄位是一個 64 位擴充位址，該命令的接收設備將向伴隨設備和該命令訊框(Frame)的發起設備都發送密鑰；如果密鑰類型欄位的值爲 1，則該命令訊框(Frame)中不含伴隨設備位址欄位。

APS 切換密鑰命令在的格式如下：

位元組數：1	1	1
訊框(Frame)控制	APS 命令標識碼	序號
APS 頭	有效載荷	

這裡 **APS 命令標識碼**欄位設爲 0x09。**序號**欄位包含的是網路密鑰序號。

3.5 安全處理公共基礎

下面介紹的是在多個 ZigBee 協定層中使用的、與安全處理有關的特性。NWK 層和 APS 層安全處理時增加的輔助訊框(Frame)頭的格式如下：

位元組數：1	4	0/8	0/1
安全控制	訊框(Frame)計數器	來源位址	密鑰序號

安全控制欄位由安全級別、密鑰標識、擴充現時值子域組成，最後兩個比特位預留。安全級別子域占 3 位，它表示對流出訊框(Frame)要進行的安全處理方式，也指示流入訊框(Frame)實現了的安全方式。不同的安全級別透過對症有效載荷的加密/不加密和所採用訊息完整碼（MIC）的不同長度，提供不同的安全保護能力。CCM*模式中 MIC 的長度可取的值是 0、32、64 或 128 位。表 22 列出了 8 種安全級別的安全處理方式。密鑰表示子域占 2 位，它表示用於訊框(Frame)保護的密鑰類型，0x00 表示鏈路密鑰，0x01 表示網路密鑰，0x02 表示密鑰傳遞密鑰，0x03 表示密鑰載入密鑰。擴充現時值子域佔 1 位元，如果輔助訊框(Frame)頭中存在發送設備位址欄位則該子域設爲 1；否則該子域設爲 0。**源位址**欄位表示對該訊框(Frame)進行安全保護的設備的 64 位元擴充位址。當安全控制欄位的擴充現時值子域爲 1 時，輔助訊框(Frame)頭中一定存在來源位址欄位。**訊框(Frame)計數器**用來指示訊框(Frame)的新鮮度，避免處理重複的訊框(Frame)。當安全控制欄位中密鑰標識子域爲 1（即網路密鑰）時，輔助訊框(Frame)頭中才存在**密鑰序號**欄位，它表示用於訊框(Frame)保護的網路密鑰對應的序號。

表 22 CCM*模式的安全級別及相應安全處理

安全級別標識	安全級別欄位	安全屬性	資料加密	訊 框 (Frame) 完整性
0x00	000	None	OFF	NO（M=0）
0x01	001	MIC-32	OFF	YES（M=4）
0x02	010	MIC-64	OFF	YES（M=8）
0x03	011	MIC-128	OFF	YES（M=16）
0x04	100	ENC	ON	NO（M=0）
0x05	101	ENC-MIC-32	ON	YES（M=4）
0x06	110	ENC-MIC-64	ON	YES（M=8）
0x07	111	ENC-MIC-128	ON	YES（M=16）

ZigBee 中 MAC、NWK 和 APS 層的安全處理都採用 CCM*模式。AES-CCM*安全模式是對 802.15.4 MAC 層使用的 AES-CCM 模式的擴充，它能單獨提供加密或完整性校驗功能，也能同時提供這兩種安全處理措施。各種安全級別所使用的安全處理措施已經明確列舉在表 22 中。CCM*模式中的現時值（nonce）是在 CCM*加密和完整性保護以及在 CCM*解密和完整性校驗中都要使用的一個輸入資料。現時值由訊框(Frame)中包含的資料和安全通訊的雙方設備能獨立獲取的資料構成。CCM*現時值各欄位的排列順序和長度如下：

位元組數：8	4	1
來源位址	訊框(Frame)計數器	安全控制

現時值中訊框(Frame)控制和訊框(Frame)計數器欄位與輔助訊框(Frame)頭中的訊框(Frame)控制和訊框(Frame)計數器欄位相同；現時值中源位址欄位設爲安全訊框(Frame)發起設備的 64 位元位址。當輔助訊框(Frame)頭安全控制欄位的擴充現時值子域爲 1 時，現時值中來源位址欄位的值等於輔助訊框(Frame)頭中來源位址欄位的值。

3.6 安全服務功能詳述

ZigBee 協調器透過設置 NIB 屬性 NwkSecurityLevel 來設置整個網路的安全級別。如果 NwkSecurityLevel 屬性值爲 0，則網路是不安全的；否則，網路就是安全的。ZigBee 協調器還透過設置 AIB 屬性 apsTrustCenterAddress 來配置信用中心的位址。信用中心缺省位址是協調器自身的位址，即 ZigBee 協調器是預設的網路信用中心。ZigBee 協調器可以設置信用中心位址來指定其他設備充當 ZigBee 網路的信用中心。

信用中心是 ZigBee 網路中其他設備都信任的設備，信用中心的應用爲網路和端到端應用配置管理分發密鑰。透過配置，信用中心可以工作在商業模式或住宅模式。信用中心可以透過直接發送鏈路密鑰或發送主密鑰幫助設備建立端到端的應用密鑰。在要求高安全性的商業應用中，信用中心需要維護一個它所控制的設備、主密鑰、鏈路密鑰和網路密鑰列表，並強制執行網路密鑰更新和網路准入制度。在商業模式中，信用中心需要的儲存容量隨著網路中設備數量的增加而增加，NIB 屬性 nwkAllFresh 應設爲 TRUE。在安全性要求較低的住宅應用中，信用中心不需要維護網路中設備、主密鑰或鏈路密鑰列表，但需要維護網路密鑰以控制網路的准入制度。在住宅模式中，信用中心需要的儲存容量不隨網路設備數量的增加而增加，NIB 屬性 nwkAllFresh 應設爲 FALSE。

ZigBee 安全處理包含的程式有加入安全網路、認證新加入的設備、更新網路密鑰、恢復網路密鑰、建立端到端應用密鑰和離開安全網路。

3.6.1 加入安全網路

圖 31 是一個設備加入安全網路時與路由器通訊的資訊流程。要加入網路的設備首先發送 NLME-NETWORK-DISCOVERY.request 原語，網路層收到網路發現請求原語後就向 MAC 層發送 MLME-SCAN.request 原語，MAC 層收到掃描請求原語後就發出不加密的信標請求命令訊框(Frame)。設備收到近鄰路由器的信標後，NWK 就向上層發送證實原語 NLME-NETWORK-DISCOVERY.confirm，原語中 NetworkList 參數列出了附近的所有 PAN 以及各個網路的 nwkSecurityLevel 和 nwkSecureAllFrames 屬性。圖中的路由器已經置於允許關聯狀態。設備根據 NLME-NETWORK-DISCOVERY.confirm 原語返回的資訊決定要加入哪個 PAN 後，就發出入網請求原語 NLME-JOIN.request。如果設備有要加入 PAN 的網路密鑰，NLME-JOIN.request 原語中 SecurityEnable 參數就設爲 TRUE；否則 SecurityEnable 參數就設爲 FALSE。NWK 層收到 NLME-JOIN.request 原語後就向 MAC 層發送關聯請求原語，MAC 層收到 MLME-ASSOCIATE.request 原語後向路由器發送一個關聯請求命令。路由器 MAC 層收到設備的管理請求命令後，向 NWK 層發送 MLME-ASSOCIATE.indication 原語，並根據關聯請求命令是否經過安全處理把指示原語中的 SecurityUse 參數設爲 TRUE 或 FALSE。然後，路由器的 NWK 層向 ZDO 發送 NLME-JOIN.indication 原語。這時，路由器就知道了請求入網設備的位址以及關聯請求命令是否經過了網路密鑰的安全處理。另外，路由器的

NWK 層還要向 MAC 層發送關聯回應原語 MLME-ASSOCIATE.response，MAC 層收到該原語後就向請求入網的設備發送一個關聯回應命令訊框(Frame)。設備收到關聯響應命令後，向 ZDO 發送入網證實原語 NLME-JOIN.confirm。至此，設備“已經加入網路但尚未認證”。認證過程將在後面單獨介紹。如果入網的設備不做路由器，則在成功執行認證過程後立即“加入網路並透過認證”；如果入網的設備要承擔路由器的任務，則只有在成功執行認證過程並且啓動路由器功能後設備才“加入網路並透過認證”。設備 ZDO 向 NWK 層發送 NLME-START.request 原語後，繼而 NWK 層向 MAC 層發送 MLME-START.request 原語來啓動路由器功能。如果路由器拒絕設備入網，則關聯回應命令訊框(Frame)中關聯狀態欄位設爲非“0x00”的值，當拒絕入網資訊透過 NLME-JOIN.confirm 原語傳到請求入網設備的 ZDO 時，設備就不啓動認證過程。

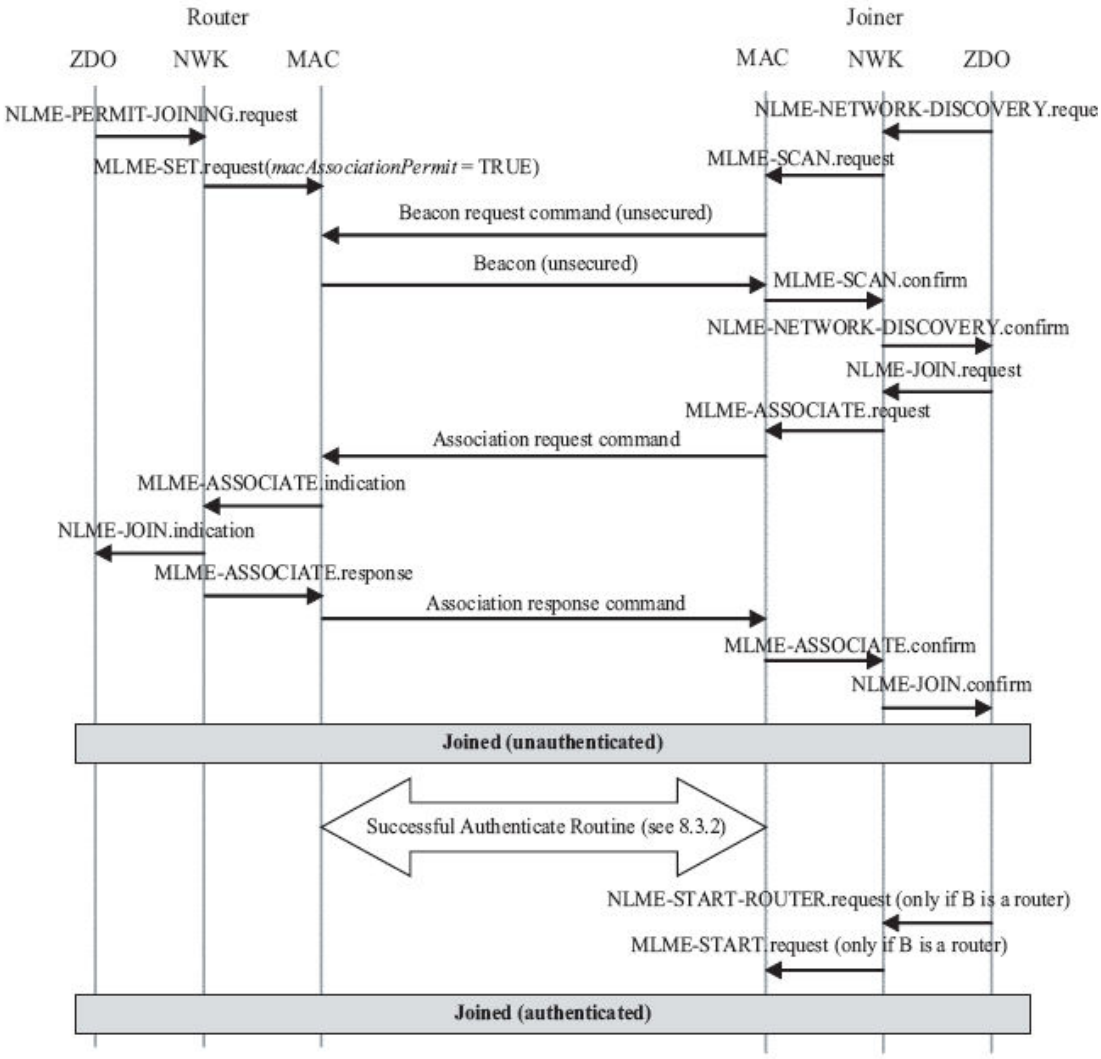


圖 31　設備加入安全網路時與路由器通訊的資訊流程

3.6.2 認證新入網的設備

當設備加入到一個安全網路，處於“已經加入網路但尚未認證”狀態時，它還必須透過認證才能工作。如果設備關聯的路由器不是信用中心，則他在收到 NLME-JOIN.indication

原語後立即發送 APSME-UPDATE-DEVICE.request 原語，開始認證過程。更新設備請求原語中 DestAddress 參數設爲 AIB 屬性 apsTrustCenterAddress 的值；DeviceAddress 參數設爲新加入設備的位址；如果新加入設備的關聯請求命令經過了安全處理，則 Status 參數設爲 0x00，否則，Status 參數設爲 0x01。如果路由器是信用中心，則它以信用中心身份工作就開始了認證過程。

信用中心在收到更新設備命令後，或者如果設備關聯的路由器就是信用中心，那麼在它收到 NLME-JOIN.indication 原語後，信用中心就開始參與認證過程。信用中心的行爲至少與一下五個因素有關：信用中心是否允許新設備加入網路，信用中心工作在住宅模式還是商業模式，在住宅模式中設備是以安全方式還是非安全方式加入，在商業模式中信用中心是否有新加入設備的主密鑰以及 NIB 屬性 nwkSecureAllFrames 的值。

在認證過程的任何時候，如果信用中心不允許新設備加入網路，它將採取措施把設備從網路中刪除。如果信用中心不是新入網設備的路由器，它就發送 APSME-REMOVE-DEVICE.request 原語來刪除沒有透過認證的設備。APSME-REMOVE-DEVICE.request 原語中，ParentAddress 參數設爲發起更新設備命令的路由器位址，ChildAddress 參數設爲新加入網路沒有透過認證的設備位址。如果信用中心是新加入設備的路由器，那麼它將透過發送 NLME-LEAVE.request 原語來刪除未透過認證的設備，原語中 DeviceAddress 參數設爲新加入網路未透過認證的設備位址。

如果工作於住宅模式的信用中心允許新設備加入，它就調用密鑰傳遞原語 APSME-TRANSPORT-KEY.request 向新入網的設備發送當前使用的網路密鑰，原語中 DestAddress 參數設爲新加入設備的位址，KeyType 參數設爲 0x01（即網路密鑰）。如果新加入的設備已有網路密鑰（即更新設備命令中 Status 欄位爲 0x00），則該原語參數 TransportKeyData 中 KeySeqNumber 設爲 0，NetworkKey 設爲全 0，UseParent 設爲 FALSE。如果新加入的設備沒有預置網路密鑰，則該原語參數 TransportKeyData 中 KeySeqNumber 設爲網路密鑰順序計數器的值，NetworkKey 設爲要傳遞的網路密鑰。如果信用中心就是新加入設備的路由器，則 UseParent 參數設爲 FALSE；否則，UseParent 參數設爲 TRUE，ParentAddress 參數設爲產生更新設備命令的路由器位址。在新入網設備沒有預置網路密鑰的情況下，發送的傳遞密鑰原語將指令路由器以不安全方式向新加入的設備發送網路密鑰。如果在路由器和新加入設備的外部輸入結束之後立即以低功率僅發送一次密鑰，那麼可以認爲這種沒有加密的密鑰傳遞方式還是安全的。

如果工作於商業模式的信用中心允許新設備加入，則它的行爲與新加入設備是否預置了信用中心主密鑰有關。如果信用中心與新入網的設備之間沒有共用主密鑰，它就調用密鑰傳遞原語 APSME-TRANSPORT-KEY.request 向新入網的設備發送一個主密鑰。密鑰傳遞原語中 DestAddress 參數設爲新加入設備的位址，KeyType 參數設爲 0x00（即信用中心主密鑰）。原語參數 TransportKeyData 中 TrustCenterMasterKey 設爲傳遞的信用中心主密鑰，如果新入網設備關聯的路由器就信用中心，則 ParentAddress 設爲當前設備的位址；否則，ParentAddress 設爲產生更新設備命令的路由器位址。同樣，在新入網設備沒有預置信用中心主密鑰的情況下，傳遞密鑰原語將指令路由器以不安全方式向新加入的設備發送主密鑰。完成信用中心主密鑰傳遞後，信用中心發送 APSME-ESTABLISH-KEY.request 原語來啓動建立鏈路密鑰的過程。建立密鑰原語中 ResponderAddress 參數設爲新加入設備的位址，KeyEstablishmentMethod 參數設爲 0x00（即 SKKE）。另外，如果 NIB 屬性 nwkSecureAllFrames 等於 FASLE 或信用中心就是路由器，則 UseParent 參數設爲 FALSE；否則，UseParent 參數設爲 TRUE 並且 ResponderParentAddress 參數設備爲產生更新設備命令的路由器位址。信用中心收到 Status 參數等於 0x00（即建立密鑰成功）的 APSME-ESTABLISH-KEY.confirm 原語後，再次調用

APSME-TRANSPORT-KEY.request 原語向新加入的設備傳遞網路密鑰。傳遞密鑰請求原語中 KeyType 參數設爲 0x01（即網路密鑰），TransportKeyData 中 KeySeqNumber 設爲該網路密鑰順序計數器的值，NetworkKey 設爲要傳遞的網路密鑰，UseParent 設爲 FALSE。

設備成功關聯到一個安全網路後，它將進入認證過程。成功透過認證後，新入網的設備就把 NIB 屬性 nwkSecurityLevel 和 nwkSecureAllFrames 設置爲其關聯路由器信標中指示的值。如果一個加入安全網路並透過認證的設備，其 nwkSecureAllFrames 屬性值爲 TRUE，那麼除了那些發送給或是來自尚未透過認證的子設備的訊框(Frame)外，NWK 層將對其他所有的流入和流出訊框(Frame)執行 NWK 層安全操作。如果 nwkSecureAllFrames 屬性值爲 FALSE，就沒有這種約束。新入網設備在認證過程中的行爲與設備的狀態有關。新加入的設備在認證前有 3 種可能的初始狀態，即在住宅模式應用中預置了網路密鑰、在商業模式應用中預置了信用中心主密鑰和位址以及沒有預置密鑰的狀態。在安全網路中，如果在預設的時間內沒有透過認證，設備就要離開網路。

如果一個成功關聯到安全網路中的設備預置了網路密鑰，它應該把密鑰的流程訊框(Frame)計數器設爲 0，清空該密鑰的流入訊框(Frame)計數器，等待接收信用中心發送的一個全零的假網路密鑰。新加入的設備收到 KeyType 參數等於 0x01 的 APSME-TRANSPORT-KEY.indication 原語後，把 AIB 屬性 apsTrustCenterAddress 設爲該指示原語中 SrcAddress 參數值。此時，新加入的設備已經透過認證，將進入住宅模式的正常工作狀態。

如果新關聯的設備預置了信用中心主密鑰和信用中心位址（即 AIB 屬性 apsTrustCenterAddress），它就等待建立鏈路密鑰和從信用中心接收網路密鑰。因此，在收到 InitiatorAddress 參數等於信用中心位址、KeyEstablishmentMethod 參數等於 SKKE 的 APSME-ESTABLISH-KEY.indication 原語後，新設備以 APSEM-ESTABLISH-KEY.response 原語爲回應，該回應原語中 InitiatorAddress 參數設爲信用中心位址，Accept 參數設爲 TRUE。在收到 Adress 參數等於信用中心位址，Status 參數等於 0x00 的證實原語 APSME-ESTABLISH-KEY.confirm 後，新加入的設備就等待接收網路密鑰。在接收到 SourseAddress 參數等於信用中心位址，KeyType 參數等於 0x00 的 APSME-TRANSPORT-KEY.indication 原語後，設備就從 TransportKeyData 參數中提取出網路密鑰。此時，新加入的設備已經透過認證，將進入商業模式的正常工作狀態。

如果新加入的設備沒有預置網路密鑰或信用中心主密鑰和位址，它就等待接收未保護的信用中心主密鑰或網路密鑰。需要注意的是，以不加密的方式傳遞密鑰是存在安全風險的，如果處於安全考慮，最好還是預置密鑰。如果收到的 APSME-TRANSPORT-KEY.indication 原語中 KeyType 參數等於 0x01，新入網設備就從 TransportKeyData 參數中提取網路密鑰，並把 NIB 屬性 apsTrustCenterAddress 設置爲該原語中 SrcAddress 參數的值。此時，新加入的設備已經透過認證，將進入住宅模式的正常工作狀態。如果收到的 APSME-TRANSPORT-KEY.indication 原語中 KeyType 參數等於 0x00，新入網設備就從 TransportKeyData 參數中提取信用中心主密鑰，並把 AIB 屬性 apsTrustCenterAddress 設置爲該原語中 SrcAddress 參數的值。然後，在收到 InitiatorAddress 參數等於信用中心位址、KeyEstablishmentMethod 參數等於 SKKE 的 APSME-ESTABLISH-KEY.indication 原語後，新設備以 APSME-ESTABLISH-KEY.response 原語爲回應，該回應原語中 InitiatorAddress 參數設爲信用中心位址，Accept 參數設爲 TRUE。在收到 Address 參數等於信用中心位址，Status 參數等於 0x00 的證實原語 APSME-ESTABLISH-KEY.confirm 後，新加入的設備就等待接收網路密鑰。在接收到 SourceAddress 參數等於信用中心位址，KeyType 參數等於 0x00 的 APSME-TRANSPORT-KEY.indication 原語後，設備就從 TransportKeyData 參數中提取出網路

密鑰。此時，新加入的設備已經透過認證，將進入商業模式的正常工作狀態。

圖 32 和圖 33 分別是住宅應用模式和商業應用模式時認證過程的資訊流程，這裡假設信用中心和路由器是不同的設備。在圖 32 中，信用中心和路由器之間傳遞的更新設備命令和傳遞密鑰命令要使用網路密鑰進行 APS 層安全管理。如果 NIB 屬性 nwkSecureAllFrames 等於 TRUE，則還要在 NWK 層用網路密鑰對這些命令訊框(Frame)作安全處理。從路由器發送給新加入設備的密鑰傳遞沒有經過安全處理。在圖 33 中，如果 NIB 屬性 nwkSecureAllFrames 等於 TRUE，在信用中心與新加入設備之間傳遞的 SKKE 命令以路由器作爲聯絡轉發設備，這種轉發方式的目的是在NWK 層應用網路密鑰對信用中心和路由器之間的 SKKE 命令進行安全處理，而在路由器與新入網設備之間傳遞的 SKKE 命令則不作安全處理。如果 NIB 屬性 nwkSecureAllFrames 等於 FALSE，則在信用中心與新入網設備之間傳遞的 SKKE 命令都不作安全處理。信用中心與新入網設備之間最後的密鑰傳遞命令在 APS 層用信用中心鏈路密鑰進行安全處理。如果 NIB 屬性 nwkSecureAllFrames 等於 TRUE，則在 NWK 層還要用網路密鑰對該命令訊框(Frame)進行處理。

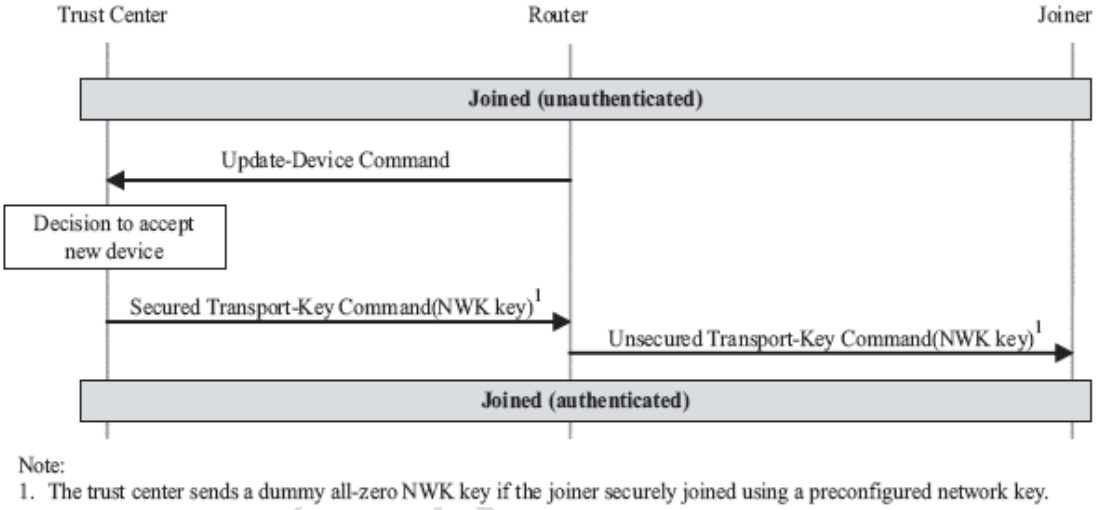


圖 32 住宅應用模式的認證過程

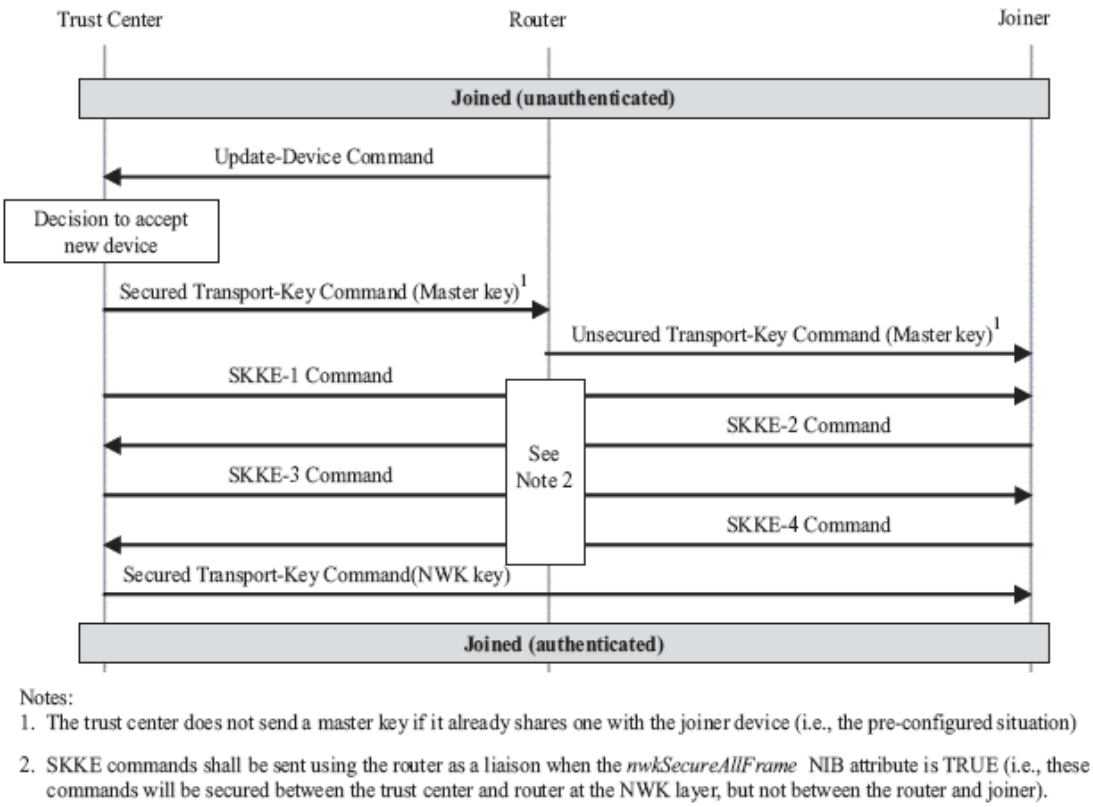


圖 33 商業應用模式的認證過程

3.6.3 更新網路密鑰

在住宅應用模式中，信用中心從不更新網路密鑰。這是透過降低安全性來實現降低複雜度的。在商業應用模式中，信用中心要維護一個關於網路中所有設備的列表。更新網路密鑰時，信用中心首先把新密鑰發送給列表中的每個設備，再讓每個設備切換使用新的密鑰。信用中心透過發送 APSME-TRANSPORT-KEY.request 原語來分發新密鑰，原語中 DestAddress 參數設爲列表中設備的位址，KeyType 參數設爲 0x01，TransportKeyData 參數中 KeySeqNumber 設爲新網路密鑰順序計數器的值，NetworkKey 設爲傳遞的新密鑰，UseParent 設爲 FALSE。如果舊網路密鑰的順序計數器值用 N 來表示，則新網路密鑰的順序計數器值爲（N+1）mod 256。信用中心透過發送 APSME-SWITH-KEY.request 原語來指令網路中的設備切換到新的網路密鑰，原語中 DestAddress 參數設爲列表中設備的位址，KeySeqNumber 參數設爲新網路密鑰順序計數器的值。

在住宅應用模式的正常工作狀態下，設備將不接受更新網路密鑰。在這種情況下，設備將忽略收到的 KeyType 參數等於 0x01 的傳遞密鑰命令和切換密鑰命令。在商業應用模式的正常工作狀態下，設備收到 KeyType 參數等於 0x01 的 APSME-TRANSPORT-KEY.indication 原語時，如果原語中 SrcAddress 參數的值等於網路信用中心的位址，設備就接受原語參數 TransportKeyData 中的網路密鑰。如果設備能夠儲存備用網路密鑰，參數 TransportKeyData 包含的密鑰和序號將取代儲存的備用網路密鑰。如果設備不能儲存備用網路密鑰，參數 TransportKeyData 包含的密鑰和序號舊愛那個直接取代當前使用的網路密鑰。在商業應用模式的正常工作狀態下，設備收到 APSME-SWITCH-KEY.indication 原語後，就從當前使用的

網路密鑰切換到指示原語中 KeySeqNumber 參數對應的新網路密鑰。

圖 34 是兩個設備成功更新網路密鑰過程中的資訊流程。在這個例子中，信用中心向設備 1 和設備 2 分別發送序號爲 N 的網路密鑰。設備 1 是 FFD，能夠儲存兩個網路密鑰；設備 2 是 RFD，只能儲存一個網路密鑰，即當前使用的網路密鑰。接收到傳遞密鑰命令後，設備 1 就用新網路密鑰取代其儲存的備用網路密鑰，而設備 2 只能用新網路密鑰取代啓動的網路密鑰。此後，接收到切換密鑰命令時，設備 1 將啓動新的網路密鑰，而設備 2 在接收密鑰傳遞命令時已經切換到了新的網路密鑰，所以它忽略該切換密鑰命令。

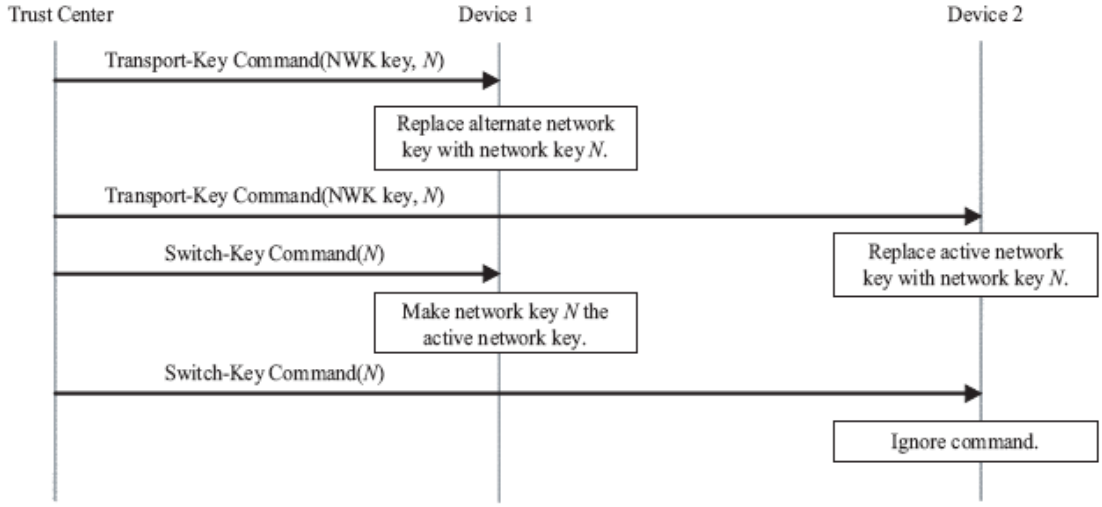


圖 34 設備成功更新網路密鑰的資訊流程

3.6.4 恢復網路密鑰

在住宅應用模式的正常工作狀態下，網路密鑰是不更新的。所以住宅應用模式下的網路設備不會產生請求網路密鑰的 APSME-REQUEST-KEY.request 原語，信用中心也忽略可能收到的 KeyType 參數等於 0x01 的 APSME-REQUEST-KEY.indication 原語。

在商業應用模式的正常工作狀態下，網路設備可以發送 APSME-REQUEST-KEY.request 原語請求當前網路密鑰。原語中 DestAddress 參數設爲信用中心的位址，KeyType 參數設爲 0x01，ParentAddress 參數設爲 0。在商業應用模式的正常工作狀態下，信用中心收到 KeyType 參數等於 0x01 的 APSME-REQUEST-KEY.indication 原語時，它將判斷 SrcAddress 參數指定的設備是否存在於設備列表中。如果設備存在於列表中，信用中心就發送 APSME-TRANSPORT-KEY.request 原語，原語參數 DestAddress 設爲請求密鑰設備的位址，參數 KeyType 設爲 0x01，參數 TransportKeyData 中的 NetworkKey 是傳遞的網路密鑰，KeySeqNumber 設爲該網路密鑰的序號，UseParent 設爲 FALSE。然後，信用中心發送 APSME-SWITCH-KEY.request 原語指令設備切換到新的密鑰。該切換密鑰原語中，DestAddress 參數設爲請求密鑰的設備位址，KeySeqNumber 參數更新網路密鑰的順序計數器的值。圖 35 是網路密鑰恢復過程的資訊流程。網路設備向信用中心請求當前的網路密鑰，信用中心以當前網路密鑰回應後，指令設備切換到該密鑰。

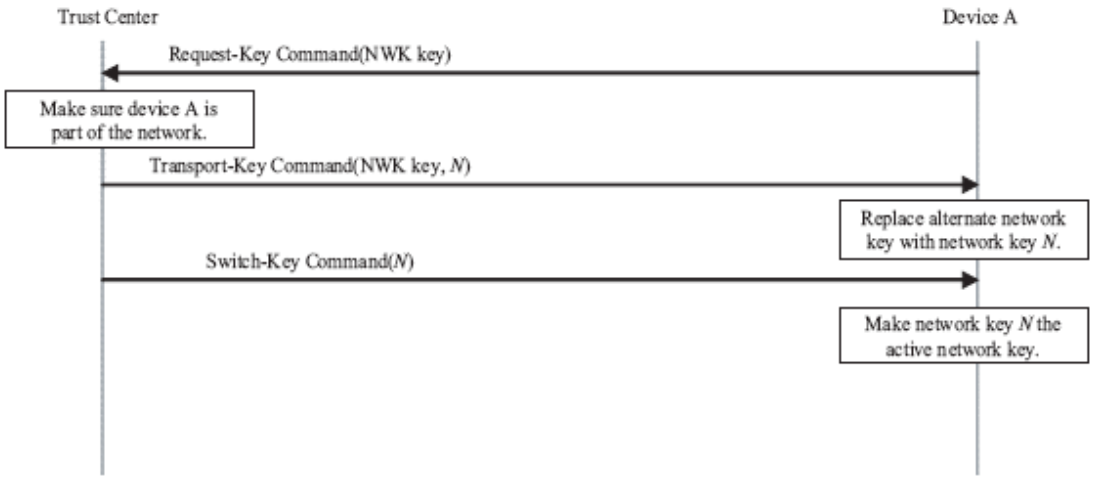


圖 35 網路密鑰恢復的資訊流程

3.6.5 建立端到端應用密鑰

建立端到端應用密鑰過程涉及的物件包括發起設備、信用中心和回應設備。發起設備發送 APSME-REQUEST-KEY.request 原語，啓動建立鏈路密鑰的過程。該請求密鑰原語中 DstDevice 參數應設爲網路信用中心的位址，KeyType 參數應設爲 0x02（即應用密鑰），PartnerAddress 參數應設爲回應設備的位址。

此後，如果發起設備收到鏈路密鑰，即收到 APSME-TRANSPORT-KEY.indication 原語中 KeyType 參數等於 0x03，並且 SrcAddress 參數等於 AIB 屬性 apsTrustCenterAddress 的值，那麼 TransportKeyData 參數中包含的密鑰就是發起設備與 PartnerAddress 參數指定設備間的鏈路密鑰。發起設備得到鏈路密鑰後，需要更新 AIB 屬性 DeviceKeyPairSet。如果 DeviceKeyPairSet 屬性中沒有 PartnerAddress 參數指定設備的密鑰對描述符，設備就新產生一個描述符；如果 DeviceKeyPairSet 屬性中已經存在回應設備的密鑰對描述符，設備就更新描述符中的元素值。描述符中 DeviceAddress 元素設爲 PartnerAddress 參數的值；LinkKey 元素設爲 TransportKeyData 參數包含的鏈路密鑰；OutgoingFrameCounter 和 IncomingFrameCounter 元素都設爲 0。

同樣，如果發起設備收到應用主密鑰，即收到的 APSME-TRANSPORT-KEY.indication 原語中 KeyType 參數等於 0x02，並且 SrcAddress 參數等於 AIB 屬性 apsTrustCenterAddress 的值，那麼 TransportKeyData 參數中包含的密鑰就是發起設備與 PartnerAddress 參數指定設備間的主密鑰。發起設備得到主密鑰後，需要更新 AIB 屬性 DeviceKeyPairSet。如果 DeviceKeyPairSet 屬性中沒有 PartnerAddress 參數指定設備的密鑰對描述符，設備就新產生一個描述符；如果 DeviceKeyPairSet 屬性中已經存在回應設備的密鑰對描述符，設備就更新描述符中的元素值。描述符中 DeviceAddress 元素設爲 PartnerAddress 參數的值；MasterKey 元素設爲 TransportKeyData 參數包含的主密鑰；OutgoingFrameCounter 和 IncomingFrameCounter 元素都設爲 0。如果 APSME-TRANSPORT-KEY.indication 原語 TransportKeyData 參數中 Initiator 的值爲 TRUE，發起設備就發送 APSME-ESTABLISH-KEY.request 原語，啓動建立鏈路密鑰的過程。原語中 ResponderAddress 參數設爲 TransportKeyData 參數中 PartnerAddress 的值，UseParent 參數設爲 FALSE，KeyEstablishmentMethod 參數設爲 0x00（即 SKKE）。響應設備收到

APSME-ESTABLISH-KEY.indication 原語即被告知發起設備想與它建立鏈路密鑰。如果回應設備決定建立鏈路密鑰，它就發送 APSME-ESTABLISH-KEY.response 原語，原語中 InitiatorAddress 參數設爲發起設備的位址，Accept 參數設爲 TRUE。如果回應設備拒絕建立鏈路密鑰，Accept 參數就設爲 FALSE。如果回應設備同意建立與發起設備時間的鏈路密鑰，則兩設備配合執行 SKKE 協定後，發起設備和回應設備的 APS 都向上層發送 APSME-ESTABLISH-KEY.confirm 原語。

信用中心收到 KeyTyple 參數等於 0x02 的 APSME-REQUEST-KEY.indication 原語後，它根據設置送出應用鏈路密鑰或主密鑰。信用中心將發送兩個 APSME-TRANSPORT-KEY.request 原語。如果信用中心預設爲傳遞應用鏈路密鑰，原語中 KeyType 參數就設爲 0x03；如果信用中心預設爲傳遞應用主密鑰，原語中 KeyType 參數就設爲 0x02。第一個 APSME-TRANSPORT-KEY.request 原語中 DestAddress 參數設爲請求密鑰設備的位址；TransportKeyData 參數中 PartnerAddress 與 APSME-REQUEST-KEY.indication 原語 TransportKeyData 參數的 PartnerAddress 值相同，Initiator 設爲 TRUE，Key 設爲新的密鑰 K。第二個 APSME-TRANSPORT-KEY.request 原語中 DestAddress 參數設爲 APSME-REQUEST-KEY.indication 原語中 TransportKeyData 參數的 PartnerAddress 值；TransportKeyData 參數中 PartnerAddress 設爲請求密鑰設備的位址，Initiator 設爲 FALSE，Key 設爲新的密鑰 K。

圖 36 是端到端鏈路密鑰建立過程的資訊流程。該過程從發起設備向信用中心發送請求密鑰命令開始，然後信用中心啓動一個超時計時器。在定時週期內，信用中心將丟棄非發起設備發出的有關這一對設備的新的密鑰請求命令。收到請求命令後，信用中心就向發起設備和回應設備發送包含應用鏈路密鑰或主密鑰的傳遞密鑰命令。因爲只有發送給發起設備的傳遞密鑰命令中的 Initiator 欄位被設爲 TRUE，所以如果信用中心送出的是主密鑰，則只能由發起設備透過發送 SKKE-1 命令來啓動密鑰建立協定。如果回應設備決定接受建立於發起設備之間的鏈路密鑰，則繼續交換 SKKE-2、SKKE-3 和 SKKE-4 命令，完成 SKKE 協定。SKKE 協定完成或超時後，發起設備和回應設備都要把協定執行的狀態報告給各自的 ZDO。如果建立密鑰成功，發起設備和回應設備之間就有了共用的鏈路密鑰，相互之間可以進行安全通訊了。

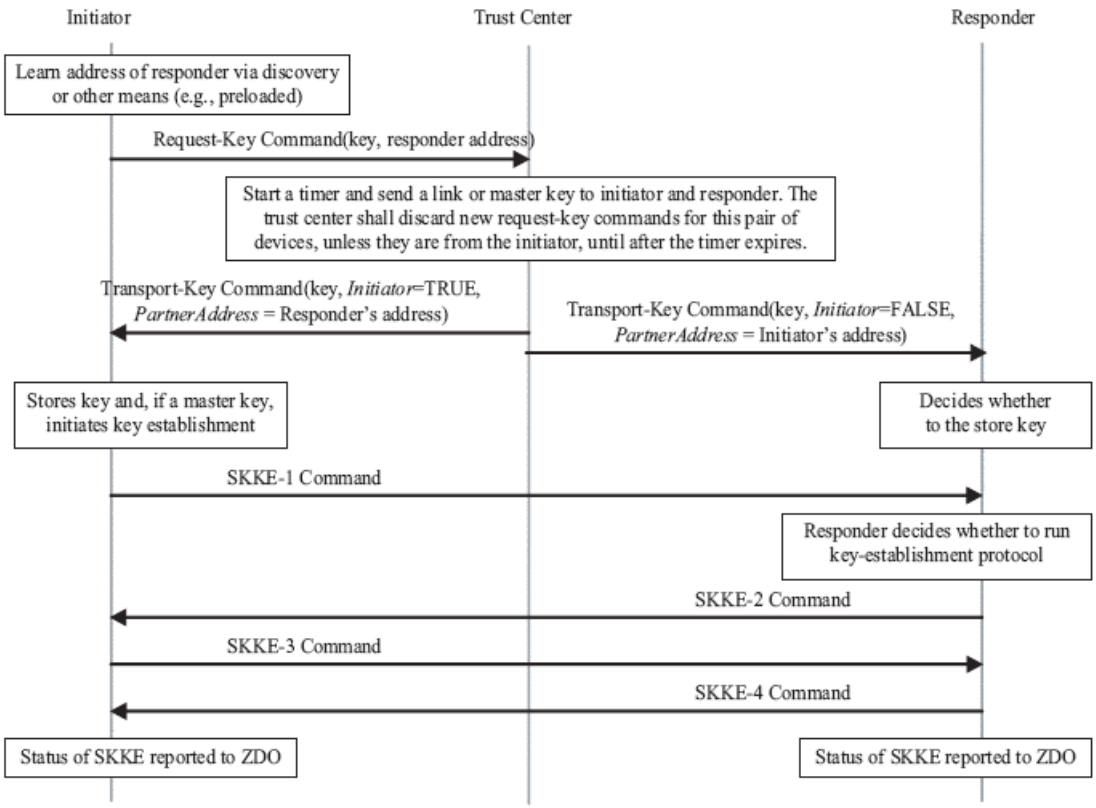


圖 36 端到端鏈路密鑰建立的資訊流程

3.6.6 離開網路

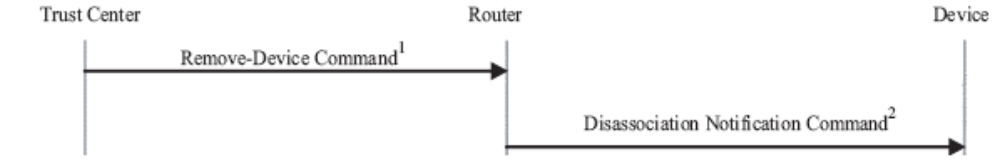
如果信用中心要求一個設備離開網路並且信用中心不是該設備的路由器，信用中心就發送 APSME-REMOVE-DEVICE.request 原語。原語中 ParentAddress 參數設爲要離開網路設備路由器的位址，ChildAddress 參數設爲要離開網路的設備位址。如果設備離開了網路，信用中心也可以透過收到的 APSME-UPDATE-DEVICE.indication 原語得到設備離網通知。該原語中 Status 參數應設爲 0x02（表示設備離開網路），DeviceAddress 參數設爲離開網路的設備位址，SrcAddress 參數設爲離網設備的父設備位址。如果網路工作在商業應用模式，則信用中心要從網路設備列表中刪除離開網路的設備位址。

離開網路設備的路由器負責接收刪除設備命令或發送更新設備命令。路由器收到 APSME-REMOVE-DEVICE.indication 原語後，如果原語 SrcAddress 參數等於 AIB 屬性 apsTrustCenterAddress 的值，路由器就發送 NLME-LEAVE.request 原語。NLME-LEAVE.request 中 DeviceAddress 參數的值與 APSME-REMOVE-DEVICE.indication 原語中 DeviceAddress 參數的值相同。如果 SrcAddress 參數值不等於 AIB 屬性 apsTrustCenterAddress 的值，路由器就忽略 APSME-REMOVE-DEVICE.indication 原語。路由器收到 NLME-LEAVE.indication 原語後，如果路由器不是網路信用中心，它將發送 APSME-REMOVE-DEVICE.request 原語，把它一個子設備離開網路的資訊通知給信用中心。APSME-REMOVE-DEVICE.request 原語中 DestAddress 參數設爲信用中心位址，Status 參數設爲 0x02，DeviceAddress 參數的設置與 NLME-LEAVE.indication 原語的 DeviceAddress 參數相同。如果離網設備的路由器同時還是網路的信用中心，則它不需要發送

APSME-REMOVE-DEVICE.request 原語。

設備透過接收或發送解關聯通知命令離開網路。在安全的 ZigBee 網路中，解關聯通知命令發送前要根據安全級別 nwkSecurityLevel 用網路密鑰進行保護；同樣，設備接收到安全的解關聯通知命令後也要做相反的安全處理。

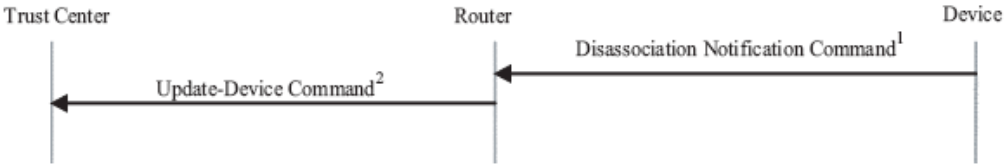
圖 37 是信用中心要求路由器刪除一個子設備的資訊流程。如果信用中心想要一個設備離開網路並且信用中心不是該設備的路由器，信用中心就像該設備的路由器發送刪除設備命令。在安全網路中，如果存在鏈路密鑰，則刪除設備命令要經過鏈路密鑰的安全處理；否則，刪除設備命令要用網路密鑰進行安全處理。路由器收到解除設備命令後就向要離開網路的子設備發送解關聯通知命令。



Note:
1. If a trust center wants a device to leave and if the trust center is not the router for that device, the trust center shall send the router a remove-device command with the address of the device it wishes to leave the network.
2. A router shall send a disassociation command to cause one of its children to leave the network.

圖 37 信用中心指令路由器刪除一個子設備的資訊流程

圖 38 是一個設備離開網路時通知其路由器及信用中心的資訊流程。主動離開網路的設備向路由器發送經過網路密鑰安全處理過的解關聯通知命令；路由器向信用中心發送經過安全處理的設備更新命令。在安全網路中，路由器與信用中心之間如果存在鏈路密鑰，則設備更新命令要用鏈路密鑰進行保護；否則，設備更新命令要用網路密鑰進行保護。



Note:
1. A device leaving the network shall send a disassociation command to its router.
2. Upon receipt of a valid disassociation command, a router shall send an update-device command to the trust center to inform it that a device has left the network.

圖 38 設備離開網路時通知其路由器及信用中心的資訊流程

參考文獻

[1] IEEE Std 802.15.4-2003:Wireless Medium AccessControl(MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)[OL].htttp://www.ieee802.org/15/pub/TG4.html.
[2] ZigBee Alliance. ZigBee Specification 1.0[OL].http://www.zigbee.org