TTC標準
Standard

JJ-300.10

ECHONET Lite 及び IoT アプリケーション向け ホームネットワーク通信インタフェース (IEEE802.15.4/4e/4g　920MHz 帯無線)

（Home network Communication Interface for ECHONET Lite and IoT applications (IEEE802.15.4/4e/4g　920MHz-band Wireless)）

第 2.3 版

2024 年 5 月 16 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

目　次

<参考>

１． 国際勧告等との関係

本標準に関連する国際標準等については、本文中に記載している。

２． 上記国際勧告等に対する追加項目等

本標準に関連する国際標準等に対するオプション選択項目、国内仕様として追加した項目、原標準に対する変更項目等については本文中に記載している。

３． 改版の履歴

版数	改訂日	改版内容
1	2013年2月21日	制定
2	2014年2月20日	方式Aに関する仕様内容の追加 （5.6 セキュリティ処理、5.7 フレームフォーマット、5.9 シングルホップスマートメーター・HEMS間推奨通信仕様、を追加、他）
2.1	2014年5月22日	方式Bに関し、ZigBee IPの改定に合わせてパラメータ値を修正。 （6.6.1, 6.6.2, 6.6.3, 6.7, 6.7.3, 表6-29（旧版の表6-31)の記述変更、および旧版の表6-34を削除）
2.2	2015年3月11日	誤記訂正。（5.9.3.2.1 (3), 5.9.3.2.4 (4), 6.2.10.1, 6.3.5.1 11, 6.3.8.4）
2.3	2024年5月16日	記載内容を方式Aのみとし、付録にWi-SUN Allianceの関係する仕様書を追加。

４． 工業所有権

本標準に係る「工業所有権等の実施に係る確認書」の提出状況はTTCのホームページでご覧になれます。

５． その他

(1) 参照する主な勧告、標準

本文中に記載する。

６． 標準作成部門

第1版：次世代ホームネットワークシステム専門委員会

第2版：次世代ホームネットワークシステム専門委員会

第2.1版：次世代ホームネットワークシステム専門委員会

第2.2版：次世代ホームネットワークシステム専門委員会

第2.3版：IoTエリアネットワーク専門委員会

1.　標準の概要

本標準は、ECHONET Lite プロトコルを使用した家電機器、共同検針や特定計量等で使用される計器が接続される IoT ルート無線端末等の遠隔制御やモニタリング等を実現するホームネットワークを構築するためのプロトコルのうち、920MHz 特定小電力無線における仕様を規定した文書である。

2.　本標準で規定する内容

2.1.　規定の対象

ECHONET Lite や IoT アプリケーションを 920MHz 帯無線(IEEE802.15.4/4e/4g)の無線で利用するときには、以下の様な選択肢がある。

a. ネットワーク層プロトコルとして IPv6 ならびに 6LoWPAN を用いる

b. ECHONET Lite や IoT ルートアプリケーション電文を直接 IEEE802.15.4 フレームに載せる

表 2-1： 920MHz 帯無線

プロトコルスタック	プロトコル・規定		
セッション～アプリケーション層	ECHONET Lite、IoT ルートアプリケーション		
トランスポート層プロトコル	UDP	TCP	b. Layer2 のフレーム上に直接搭載
ネットワーク層プロトコル	a.　IPv6 / 6LoWPAN		
データリンク層プロトコル	IEEE802.15.4, IEEE802.15.4e/g		
物理層プロトコル	IEEE802.15.4, IEEE802.15.4g		
媒体	電波(920MHz 帯)		

本標準のスコープは、a であり、そのうち、トランスポート層プロトコルとして UDP を使用する方式（方式 A）について規定する。

2.2.　各方式の概要

本標準では、以下の方式を規定する。

表 2-2:本標準で規定する方式

方式	表 1 における選択肢	関連する団体	
方式 A	a	エコーネットコンソーシアム テレメータリング推進協議会	Wi-SUN Alliance

方式 A は、物理層、データリンク層(IEEE802.15.4/4e/4g)の上に、IPv6/6LoWPAN、UDP 層（およびオプションとして TCP 層）を設けて ECHONET Lite や IoT ルートアプリケーションの電文を載せる。

3.　参照規格・参考文献

本標準が規定する仕様の一部を構成する内容を含む規格および関連する規格を以下に示す。

参照規格・参考文献について改訂があった場合は、本標準に基づく実装は改訂後の最新版を適用することを推奨する。他の参照規格については、その限りではない。

[付録] 2.1 および 2.2 参照

4.　方式 A

4.1.　概要

[付録] 3.1 参照

4.2.　プロトコルスタック

[付録] 3.2 参照

4.3.　物理層部

[付録] 3.3 参照

4.4.　データリンク層　（MAC 層）部

[付録] 3.4 参照

4.5.　インタフェース部

[付録] 3.5 参照

4.6.　シングルホップスマートメーター･HEMS 間推奨通信仕様

[付録] 3.7 参照

4.7.　マルチホップホームネットワーク推奨通信仕様

[付録] 3.10 参照

4.8.　スマートメーター・IoT ルート無線端末間推奨通信仕様

[付録] 3.11 参照

[付録]

Wi-SUN Alliance

Home Area Network (HAN) Working Group

Wi-SUN Profile for HAN

Revision 2v10

Released for TTC JJ-300.10

Home Area Network Working Group

Home Area Network Technical Profile Specification

1. Notices

1.1. Copyright

1.2. Provisional Document

This document is a work-in-progress and is subject to change. The specifications in this document are minimum requirement for implementers. Additional information on this specification will be in Wi-SUN PHY/MAC/Interface specification documents for ECHONET Lite [Wi-SUN-PHY] [Wi-SUN-MAC]

1.3. Revision History

Table 4.8-1 Revision History

Version	Date	Author	Comments
0v00	26 Jan 2013	Edited by NICT	Provide Wi-SUN profile for Echonet Lite r3
0v01	20 Feb 2013	Edited by Phil Beecher	Derived from Wi-SUN profile for Echonet Lite r3
0v02	8 April 2013	Edited by NICT and TOSHIBA	- Introduced security configuration in 3.5.7 for Echonet Lite over IP system - Split previous Recommended usage section into 3.6 single-hop home network section and 3.7 single-hop smart meter-HEMS section (defined PHY/MAC/Interface parameters in each sections)

			- Modified/changed: 6LP1.2, 6LP2, 6LP3, 6LP7, 6LP9 in Table 3.5-1, ND4 in Table 3.5.-8, and 6HC1.2, 6HC2.1, 6HC2.2 in Table 3.5-3. - Typo/grammatical corrections and clarifications
2v01	23 October 2013	Edited by TOSHIBA and Renesas	- Introduced the usage of Route-B credential in 3.7.7 - Changed RX sensitivity value to follow 802.15.4g in Table 3-29. - Profile version number correction: 0v02 should be 2v00. Therefore this revision has to be 2v01. - NS and NA messages have to carry EUI-64 format addresses in Table 3-16. - Added how many KeyDescriptors to hold at same time (§ 3.7.5.3.1) - Some editorial corrections
2v02	24 January 2014	Edited by TOSHIBA	- Added the usage of list termination IE in EB/EBR for single-hop smart meter-HEMS network (§ 3.7.6.1.1) - Transmission of NS message is optional for single-hop smart meter-HEMS network (§ 3.7.4.3.2) - Additional statements for clarification in Network layer section (§ 3.7.4.3) for single-hop smart meter-HEMS network. Unnecessary functions in the single-hop network are made to be optional. - Added a notation “50kbps is optional” in the single-hop smart meter-HEMS network (§ 3.7.2).

			- CSM is not supported if 50kbps is not supported in the single-hop smart meter-HEMS network(§3.7.2) - Changed the notation of supporting 50kbps/100kbps for clarification in the single-hop home network (§3.6.2) - Table/Figure number corrections
2v03	16 June 2014	Edited by TOSHIBA	- Added a remark and a notation in Table 3.6-9 macAckWaitDuration - New Support status 'Irrelevant' in Table 3.7-4 'Network Layer: IPv6' and 3.7-5 'Network Layer: ICMPv6'. - Added a description about maximum link MTU size issue (§3.7.4.5)
2v04	26 September 2014	Edited by Anritsu, NICT, Renesas, and TOSHIBA	- Added §3.8 Recommended usage for single-hop home network among devices (TOSHIBA) - Added §3.9 Recommended usage for the home area network (HAN) employing relay among devices (Anritsu, NICT, and Renesas) Above sub-sections are based on the HAN tiger team discussion. The tiger team members include Anritsu, Mitsubishi, NEC, NICT, NSS, Panasonic, Procubed, Renesas, and Toshiba.
2v05	14 April 2015	Edited by Anritsu, NICT,OKI, Renesas, and TOSHIBA	- Revised: §3.8 and §3.9 - New: Sleeping end device support described in §3.10 - Reference number corrections - Added a clarification of the Header IE list termination usage in §3.6.3.2
2v06	7 September 2015	Edited by Anritsu, NICT,OKI,	- Added clarifications of Active scan and Capability Notification IE usage in the

		TOSHIBA, and TUV	clauses 3.6.6.1.1, 3.7.6, 3.7.6.1.1, 3.8.3.1, 3.8.6.1.1, Table 3.7-3. - Revised clause 3.8.1 - Added resolution of IPv6 ND with Relay device in 3.9.6.1.2 - Unified relay related IE names: SRA ID and SLR IE - Introduced New PANA REQ-Timeout-Modification-Requet AVP for PANA Key Exchange with Sleeping Device in 3.10.5 - Fixed typo.
2v07	16 December 2015	Edited by Anritsu, NICT, OKI, Panasonic, and TOSHIBA	- LOWPAN_IPHC format for multicast packet in 3.5.2 - Header IE list terminator notation in 3.6.3.2 - Recommended “Scanduration’ value in 3.8.6.1.1 - Recommended interval time between Enhanced Active Scans in 3.8.8 - Changed the byte order of the relay related IEs to little endian in 3.9.3.2.3 - Intermediate hop 1-N subfileds are necessary and fixed typo in Figure 3.9-4 SLR IE - Capability Notification IE is necessary for both EBR and EB in 3.9.8. - Behavior when exceeded number of intermediate hops is found in SRA or SLR is described in 3.9.9. - Minimum mandatory for indirect transmission buffer is notified in 3.10.3.1.1. - Variable setting for macTransactionPersistenceTime is described in 3.10.3.1.1

			- A limitation for 6LoWPAN fragmentation is notified in 3.10.4.2. - Destination address of SLR IE for multicast indirect transmission in 3.10.4.3.3 - PANA Time Out. modification sequence is recommended to be limited at initial join sequence. Specified in 3.10.5. - The ranges of REQ_IRT and REQ_MRT are notified in 3.10.5. - How to register sleep end device in a coordinator and aging of registration is described in 3.10.6.1.1. - Data request frame shall not be encrypted. This is noted in 3.10.3.1.2. - Multicast transmission in 3.9.11 - Fixed Typo
2v08	6 July 2016	Edited by Anritsu, OKI, and TOSHIBA	- Reflected from the latest errata document (“Errata for Profile Technical Specifications and Test Specifications” 0v06) - Fixed reference errors - Replaced the recommended scan duration value 6 with 5 for IEEE 802.15.4g conformity - Replaced with new Wi-SUN logo
2v09	1 October 2021	Edited by ROHM and TOSHIBA	- New Route-IoT support described in 3.11 - 1.4 Acknowledgements section added - Fixed Typo
2v09	21 November 2022	Edited by TOSHIBA	- Chaneged Title and WG name on the cover (+header and footer) (“echonet” to “HAN”) - (The version number 2v09 is not changed)
2v10	11 April 2023	Edited by ROHM	- Usage of credential for Route-IoT updated (3.11.7)

1.4. Acknowledgements

The Wi-SUN Alliance acknowledges the substantial efforts of the following individuals who contributed to the production of this document.

HAN Version 2v03 contributors:

- Fumihide Kojima, NICT
- Hiroshi Harada, NICT (Chair)
- Hoang Vinh Dien, NICT (Secretary)
- Mitsuru Kanda, Toshiba (Technical Editor)

HAN Version 2v04 contributors:

- Amarjeet Kumar, Procubed Inc.
- Anand M, Procubed Inc.
- Fumihide Kojima, NICT
- Hiroshi Harada, NICT (Chair)
- Hoang Vinh Dien, NICT (Secretary)
- Keiichi Teramoto, Toshiba
- Koichi Sato, Renesas
- Mitsuru Kanda, Toshiba (Technical Editor)
- Toyoyuki Kato, Anritsu
- HAN tiger team:
    - Akiyoshi Yagi, Mitsubishi Electric
    - Bhupender Virk, Procubed Inc
    - Daisuke Takita, Mitsubishi Electric
    - Fumihide Kojima, NICT
    - Fumio Sato, Toshiba
    - Hiroshi Harada, NICT
    - Yoshihiro Izumi, NISSIN SYSTEMS
    - Junichi Iwana, Renesas
    - Keiichi Teramoto, Toshiba
    - Koichi Sato, Renesas
    - Mikiharu Ishii, NEC
    - Mitsuru Kanda, Toshiba
    - Osamu Miyashita, Anritsu
    - Satoshi Okage, Panasonic
    - Shigekazu.Harada, NEC
    - Takashi Asai, Renesas
    - Tetsuya Tamura, Anritsu
    - Tomohito Ikeya, Anritsu
    - Tomoki Takazoe, Panasonic
    - Toyoyuki Kato, Anritsu
    - Verotiana Rabarijaona, NICT
    - Yoshio Kashiwagi, NISSIN SYSTEMS

HAN Version 2v05 contributors:

- Fumihide Kojima, NICT
- Hiroshi Harada, NICT (Chair)
- Hoang Vinh Dien, NICT (Secretary)
- Mitsuru Kanda, Toshiba (Technical Editor)
- Koichi Sato, Renesas
- Toyoyuki Kato, Anritsu

HAN Version 2v06 contributors:

- Fumihide Kojima, NICT
- Hiroshi Harada, NICT (Chair)
- Mitsuru Kanda, Toshiba (Techinical Editor)
- Olga Kozeruk, TUV
- Verotiana Rabarijaona, NICT

HAN Version 2v07 contributors:

- Fumihide Kojima, NICT
- Hiroshi Harada, NICT (Chair)
- Mitsuru Kanda, Toshiba (Technical Editor)
- Noriyuki Sato, OKI
- Satoshi Okage, Panasonic
- Tomohito Ikeya, Anritsu
- Toyoyuki Kato, Anritsu
- Yoshihisa Nakano, OKI
- Verotiana Rabarijaona, NICT

HAN Version 2v08 contributors:

- Fumihide Kojima, NICT
- Hiroshi Harada, NICT (Chair)
- Mitsuru Kanda, Toshiba (Chair)
- Noriyuki Sato, OKI
- Toyoyuki Kato, Anritsu

HAN Version 2v09 contributors:

- Hiroshi Harada, NICT (Chair)
- Mitsuru Kanda, Toshiba (Technical Editor)
- Kiyoshi Fukui, OKI
- Yuki Matsumura, ROHM

Contents

2. References

2.1. Normative references

This section lists the normative references that define partial specifications of this standard or ones that are related to the standard.

This document is to recommend that any update in those references should be reflected in the subsequent implementations according to the standard.

[6LOWPAN] Transmission of IPv6 Packets over IEEE 802.15.4 Networks (6LoWPAN), IETF RFC 4944

[6LPHC] Compression Format for IPv6 Datagrams in 6LoWPAN Networks, IETF RFC 6282

[6LPND] Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs), IETF RFC 6775

[802.15.4] IEEE Std. 802.15.4 - 2011™, IEEE Standard for Information Technology - Telecommunications and Information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), September 2011

[802.15.4e] IEEE Std. 802.15.4e-2012™, Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) - Amendment 1: MAC sub-layer, April 2012.

[802.15.4g] IEEE Std. 802.15.4g-2012™, Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) - Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks, April 2012.

[802.15.10] "P802.15.10TM/D01 Draft Recommended Practice for Routing Packets in 802.15.4 Dynamically Changing Wireless Networks

[T108] ARIB STD-T108 920MHz-BAND. TELEMETER, TELECONTROL. AND DATA TRANSMISSION RADIO. EQUIPMENT

[AES-CCM] NIST SP800-38C

[AES-GCM] NIST SP800-38D

[EAP] Extensible Authentication Protocol (EAP), IETF RFC 3748

[EAP-PSK] The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method, IETF RFC 4764

[EL] The ECHONET Lite Specification Version 1.01

[IPv6] Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 2460

[IPv6-DHCP] "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, IETF RFC 3633

[AH] IP Authentication Header, IETF RFC 4302

[ESP] IP Encapsulating Security Payload (ESP), IETF RFC 4303

[HMAC-SHA256] Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, IETF RFC 4886

[IPv6-RH] Deprecation of Type 0 Routing Headers in IPv6, IETF RFC 5095

[IPv6-SAA] IPv6 Stateless Address Autoconfiguration, IETF RFC 2462

[ICMP6] Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, IETF RFC 4443

[IP6ADDR] IP Version 6 Addressing Architecture, IETF RFC 4291

[MLE] Mesh Link Establishment, IETF draft-kelsey-intarea-mesh-link-establishment-06

[NAI] The Network Access Identifier, IETF RFC 4282

[ND] Neighbor Discovery for IP version 6 (IPv6), IETF RFC 4861

[PANA] Protocol for Carrying Authentication for Network Access (PANA), IETF RFC 5191

[PANA-ENC] Encrypting the Protocol for Carrying Authentication for Network Access (PANA) Attribute-Value Pairs, IETF RFC 6786

[SLAAC] IPv6 Stateless Address Autoconfiguration, IETF RFC 4862

[TCP] Transmission Control Protocol (TCP), IETF RFC 793

[UDP] User Datagram Protocol (UDP), IETF RFC 768

[ULA] Unique Local IPv6 Unicast Addresses, IETF RFC 4193

[USRK] Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK), IETF RFC 5295

[Wi-SUN-PHY] Wi-SUN PHY specification document for ECHONET Lite, 20120212-PHYWG-Echonet-Profile-0v01

[Wi-SUN-MAC] WI-SUN MAC specification document for ECHONET Lite, 20120212-MACWG-Echonet-Profile-0v01

[Wi-SUN-MAC] WI-SUN Interface specification document for ECHONET Lite, 20120212-IFWG-Echonet-Profile-0v01

[Wi-SUN-CTEST] Wi-SUN conformance test specification for ECHONET Lite

[Wi-SUN-ITEST] Wi-SUN interoperability test specification for ECHONET Lite

2.2. Informative References

None

3. Wi-SUN profiles (ECHONET Lite over IP)

3.1. Overview

This section defines physical (PHY) and data link layers profiles and Wi-SUN ECHONET Lite interface to communicate between devices using IP and IEEE 802.15.4g and 4/4e. Wi-SUN ECHONET-Lite interface is an interface between ECHONET Lite application part and physical and MAC layers for transmission of ECHONET Lite application data from one device to the other devices. **Figure 4.8-1** shows the scope defined by this document. **Figure 4.8-2** shows the Wi-SUN profile layer structure. In this section, the mark of "M" indicates the mandatory functions in the standards [802.15.4], [802.15.4g] and [802.15.4e], and "O" means optional functions. The marks of "Y" and "N" mean the required and not-required functions in ECHONET Lite operation, respectively. Specifications and procedures for certification and interoperability tests are provided by [Wi-SUN-PHY], [Wi-SUN-MAC], [Wi-SUN-IF], [Wi-SUN-CTEST] and [Wi-SUN-ITEST].

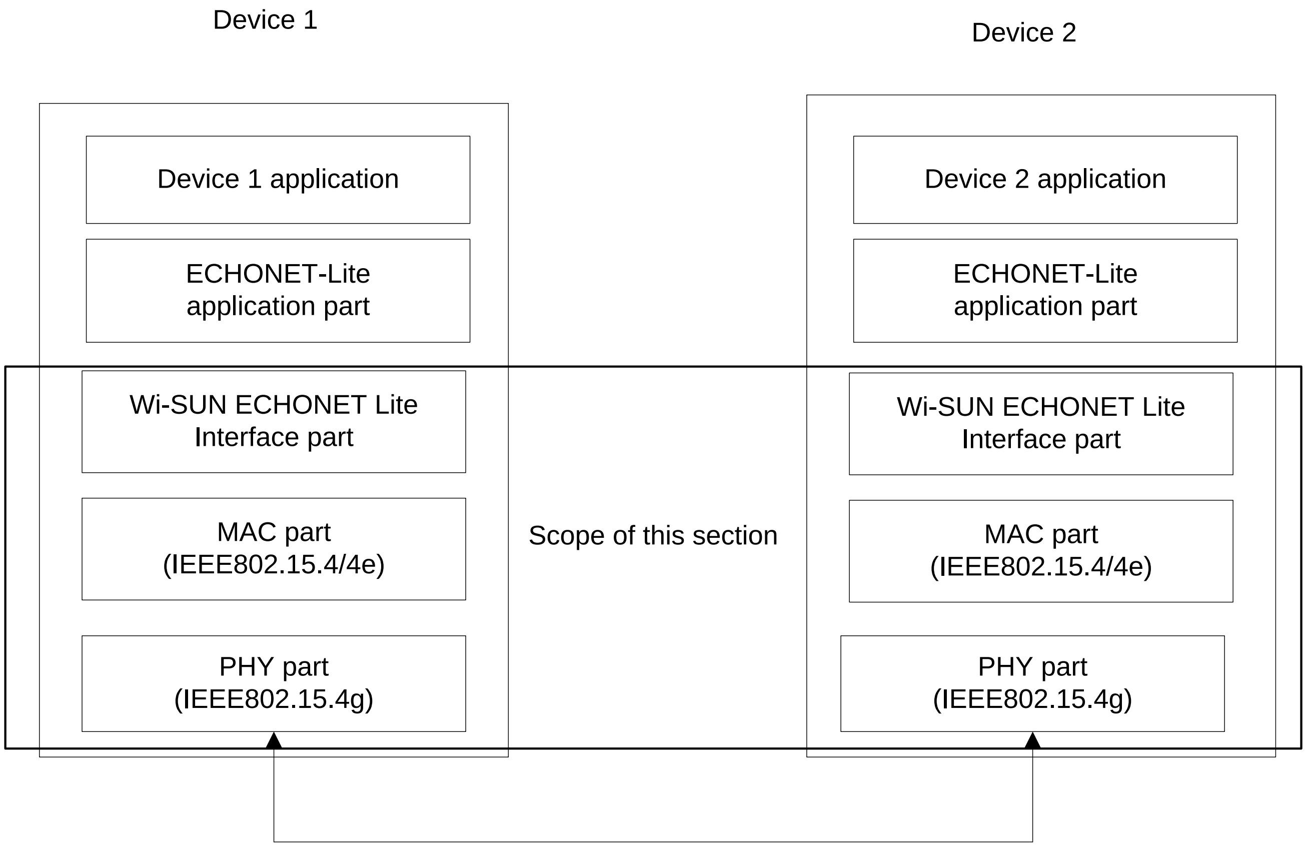

Device 1
Device 2
Device 1 application
ECHONET-Lite application part
Wi-SUN ECHONET Lite Interface part
MAC part (IEEE802.15.4/4e)
PHY part (IEEE802.15.4g)
Scope of this section
Device 2 application
ECHONET-Lite application part
Wi-SUN ECHONET Lite Interface part
MAC part (IEEE802.15.4/4e)
PHY part (IEEE802.15.4g)

Figure 4.8-1 Scope defined by this section

3.2. Protocol stack

Protocol stack for the device defined by this profile is shown in **Figure 4.8-2**.

PHY layer provides the following service under this profile.

- Up-to-2047 bytes PSDU exchange (Note that the profile recommends 255 bytes or less as mentioned later)

Data link (MAC) layer provides the following services under this profile.

- Successful discovery of IEEE 802.15.4 PAN in radio propagation range
- Support of low energy hosts that can change its status between active and sleep status
- Security functions that includes encryption, manipulation detection and replay attack protection (Note that key management is not performed by this layer)

6LoWPAN adaptation layer provides the following services under this profile.

- IPv6 and UDP header compression and decompression
- Fragmentation and defragmentation of IPv6 packet that exceeds maximum payload size operable by data link layer
- Neighbor discovery (Not necessary when done by the network layer)

Network layer provides the following services under this profile.

- IPv6 address management and packetizing
- Neighbor discovery (Not necessary when done by the adaptation layer)
- IPv6 stateless address autoconfiguration and duplicate address detection (DAD)
- IPv6 packet forwarding
- ICMPv6 support
- IPv6 packet multicast transmission and reception

Transport layer provides the following service under this profile.

- Packet delivery that is not guaranteed by UDP

Application layer provides the following services under this profile.

- Detection of functional units (ECHONET object) employed by the other nodes in the network

- Acquisition of parameters and statuses (ECHONET property) for the other nodes
- Configuration of parameters and statuses for other nodes
- Notification of parameters and statuses for the local node
- Security configuration is provided by PANA for ECHONET Lite over IP
  - PANA runs over UDP and provides security capabilities below:
    - Mutual authentication between coordinator and host
    - Link layer ciphering key management after successful authentication

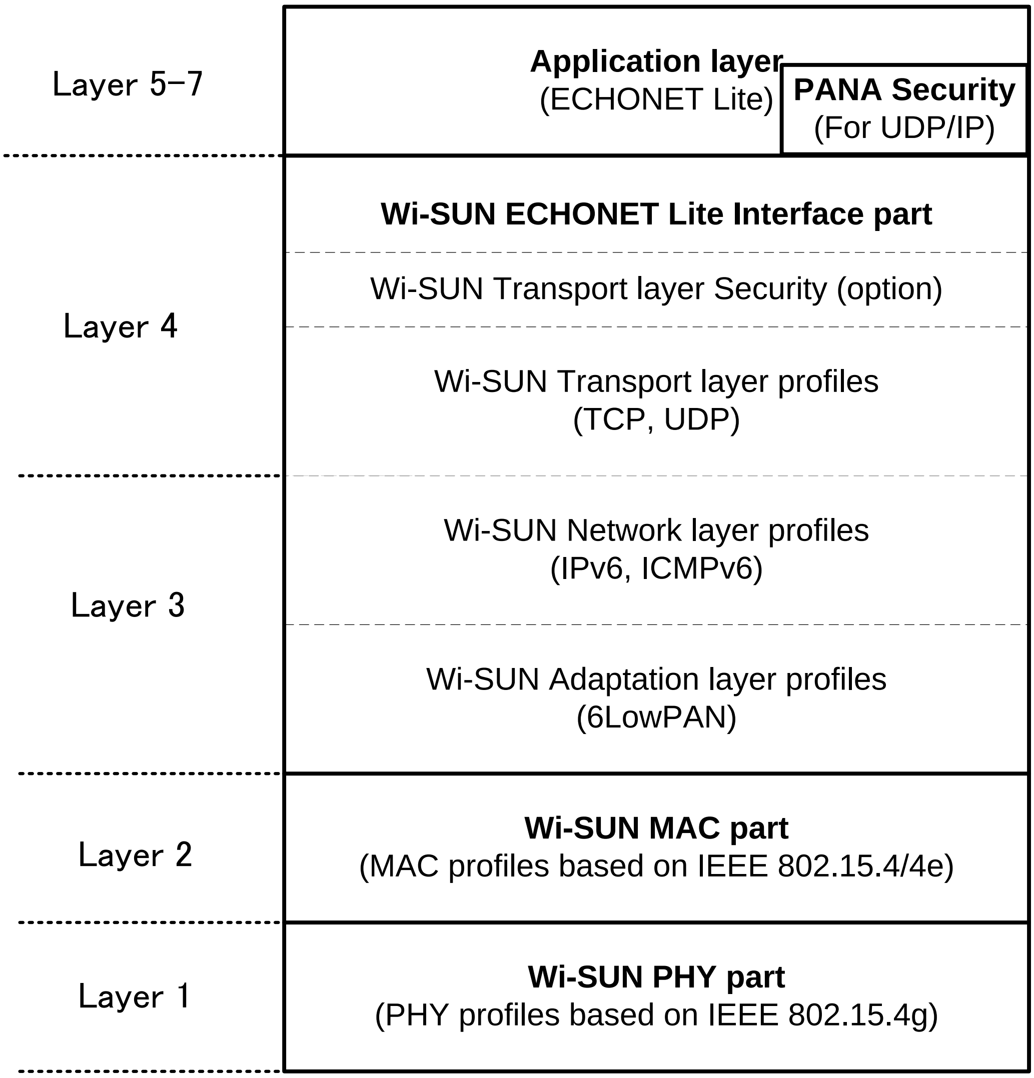

Layer 5-7
Application layer
(ECHONET Lite)
PANA Security
(For UDP/IP)
Layer 4
Wi-SUN ECHONET Lite Interface part
Wi-SUN Transport layer Security (option)
Wi-SUN Transport layer profiles
(TCP, UDP)
Layer 3
Wi-SUN Network layer profiles
(IPv6, ICMPv6)
Wi-SUN Adaptation layer profiles
(6LowPAN)
Layer 2
Wi-SUN MAC part
(MAC profiles based on IEEE 802.15.4/4e)
Layer 1
Wi-SUN PHY part
(PHY profiles based on IEEE 802.15.4g)

Figure 4.8-2 Layer structure defined by this section

3.3. PHY part

3.3.1. Overview

This section defines the PHY profiles required for PHY part supporting ECHONET Lite applications. The profiles are based on features and capabilities defined in standards [802.15.4] and [802.15.4g]. For each profile, references are given to the appropriate sub-clauses in [802.15.4] and [802.15.4g].

3.3.2. PHY specification

3.3.2.1. PLF and PLP capabilities

The requirements for the PHY Layer Function (PLF) and PHY Layer Packet (PLP) are described in **Table 4.8-2**.

Table 4.8-2 PLF and PLP capabilities

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)	Support (Y:Yes, N:No, O:Option)
PLF1	Energy detection (ED)	[802.15.4]8.2.5	FD1:M	FD1:Y
PLF2	Link quality indication (LQI)	[802.15.4]8.2.6	M	Y
PLF3	Channel selection	[802.15.4]8.1.2	M	Y
PLF4	Clear channel assessment (CCA)	[802.15.4]8.2.7	M	Y
PLF4.1	Mode 1	[802.15.4]8.2.7	O.2	Y
PLF4.2	Mode 2	[802.15.4]8.2.7	O.2	N
PLF4.3	Mode 3	[802.15.4]8.2.7	O.2	N

PLP1	PSDU size up to 2047 octets	[802.15.4g]9.2	FD8:M	Y

3.3.2.2. RF capabilities

The requirement for the RF capabilities is described inTable 4.8-3.

Table 4.8-3 RF capabilities

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)	Support (Y:Yes, N:No, O:Option)
RF12	SUN PHYs			
RF12.1	MR-FSK	[802.15.4g] 18.1	FD8:M	Y(*1)
RF12.2	MR-OFDM	[802.15.4g] 18.2	FD8:O	N
RF12.3	MR-O-QPSK	[802.15.4g] 18.3	FD8:O	N
RF12.4	MR-FSK-Generic PHY	[802.15.4g] 8.1.2,10.2	RF12.1:O	N
RF12.5	Transmit and receive using CSM	[802.15.4g] 8.1a	M	Y
RF12.6	At least one of the bands given in Table 66 [802.15.4g]	[802.15.4g] 8.1	FD8:M	Y (920 MHz, *2)
RF13	SUN PHY operating modes			
RF13.4	Operating mode #1 and #2 in 920 MHz band	[802.15.4g] 18.1	FD8:M	Y
RF 13.5	Operating mode #3 and #4 in 920 MHz band	[802.15.4g] 18.1	FD8:O	N
RF14	MR-FSK Options			
RF14.1	MR-FSK FEC	[802.15.4g] 18.1.2.4	O	N
RF14.2	MR-FSK interleaving	[802.15.4g] 18.1.2.5	O	N

RF14.3	MR-FSK data whitening	[802.15.4g] 18.1.3	O	Y
RF14.4	MR-FSK mode switching	[802.15.4g]18.1.4	O	N

*1: The frequency tolerance requirements in [802.15.4g] 18.1.5.3 do not apply. The frequency tolerance shall be +-20ppm.

*2: All channels shown in [802.15.4g] Table 68d within the supported operating mode(s) for the respective band shall be supported.

3.4. MAC part

3.4.1. Overview

This section defines Wi-SUN 15.4 and 15.4e MAC profiles for MAC part. The capabilities are generated from standards [802.15.4] and [802.15.4e], and summarized in the Tables.

Nodes defined by this profile employ 64 bit address out of MAC address modes defined by [802.15.4]. 64 bit EUI-64 address shall be stably allocated to each device. This address is globally unique and is expected permanently stable for the device.

Clause 3.4.2 defines the support required for Beacon-enabled deployments and Clause 3.4.3 defines the support required for Non-Beacon-enabled deployments. Either of those two deployments shall be implemented by this data link profile.

3.4.2. Beacon mode profile

This sub-clause defines Wi-SUN 15.4 and 15.4e MAC profiles for ECHONET Lite, when beacon-enabled PAN is employed.

3.4.2.1. Functional device (FD) types

The requirements for the functional device types are described in **Table 4.8-4**.

Table 4.8-4 Functional device types

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)	Support (Y:Yes, N:No, O:Option)
FD1	FFD	[802.15.4] 5.1	O.1	O.1
FD2	RFD	[802.15.4] 5.1	O.1	O.1
FD3	Support of 64 bit IEEE address	[802.15.4] 5.2.1.1.6	M	Y
FD4	Assignment of short network address (16 bit)	[802.15.4] 5.1.3.1	FD1:M	FD1:Y
FD5	Support of short network address (16 bit)	[802.15.4] 5.2.1.1.6	M	Y
FD8	SUN PHY device	[802.15.4g] 8.1	O.2	Y (#1)

O.1: Optional but at least one of the features described in FD1 and FD2 is required to be implemented

O.2: At least one of these features is supported

#1: MR-FSK is employed.

3.4.2.2. Major capabilities for the MAC sub-layer

The major capabilities for the MAC sub-layer are described in this sub-clause.

3.4.2.2.1.MAC sub-layer functions

The MAC sub-layer function requirements are described in **Table 4.8-5**.

438 **Table 4.8-5 MAC sub-layer functions**

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)	Support (Y:Yes, N:No, O:Option)
MLF1	Transmission of data	[802.15.4] 6.3	M	Y
MLF1.1	Purge data	[802.15.4]6.3.4,6.3.5	FD1:M FD2:O	FD1:Y FD2: N
MLF2	Reception of data	[802.15.4] 6.3	M	Y
MLF2.1	Promiscuous mode	[802.15.4] 5.1.6.5	FD1:M FD2:O	FD1:Y FD2: N
MLF2.2	Control of PHY receiver	[802.15.4] 6.2.9	O	N
MLF2.3	Timestamp of incoming data	[802.15.4] 6.3.2	O	N
MLF3	Beacon management	[802.15.4] 5	M	Y
MLF3.1	Transmit beacons	[802.15.4] 5, 5.1.2.4	FD1:M FD2:O	FD1:Y FD2: N
MLF3.2	Receive beacons	[802.15.4] 5, 6.2.4	M	Y
MLF4	Channel access mechanism	[802.15.4] 5, 5.1.1	M	Y
MLF5	Guaranteed time slot (GTS) management	[802.15.4] 5, 6.2.6, 5.3.9, 5.1.7	O	N
MLF5.1	GTS management (allocation)	[802.15.4] 5, 6.2.6, 5.3.9, 5.1.7	O	N
MLF5.2	GTS management (request)	[802.15.4] 5, 6.2.6, 5.3.9, 5.1.7	O	N
MLF6	Frame validation	[802.15.4] 6.3.3, 5.2, 5.1.6.2	M	Y
MLF7	Acknowledged frame delivery	[802.15.4] 5, 6.3.3, 5.2.1.1.4, 5.1.6.4	M	Y

MLF8	Association and disassociation	[802.15.4] 5, 6.2.2, 6.2.3, 5.1.3	M	Y
MLF9	Security	[802.15.4] 7	M	Y
MLF9.1	Unsecured mode	[802.15.4] 7	M	Y
MLF9.2	Secured mode	[802.15.4] 7	O	Y
MLF9.2.1	Data encryption	[802.15.4] 7	O.4	Y
MLF 9.2.2	Frame integrity	[802.15.4] 7	O.4	Y
MLF10.1	ED	[802.15.4] 5.1.2.1, 5.1.2.1.1	FD1:M FD2:O	FD1:Y FD2: N
MLF10.2	Active scanning	[802.15.4] 5.1.2.1.2	FD1:M FD2:O	FD1:Y FD2:Y
MLF10.3	Passive scanning	[802.15.4] 5.1.2.1.2	M	Y
MLF10.4	Orphan scanning	[802.15.4] 5.1.2.1, 5.1.2.1.3	M	Y
MLF11	Control/define/determine/declare superframe structure	[802.15.4] 5.1.1.1	FD1:O	FD1:O
MLF12	Follow/use superframe structure	[802.15.4] 5.1.1.1	O	Y
MLF13	Store one transaction	[802.15.4] 5.1.5	FD1:M	FD1:Y
MLF14	Ranging	[802.15.4] 5.1.8	RF4:O	N
MLF14.1	DPS	[802.15.4] 5.1.8.3,6.2.15	O	N
MLF15(4g)	MPM for all coordinators when operating at more than 1% duty cycle	[802.15.4g] 5.1.13	M	FD8:Y
MLF15	TSCH Capability	[802.15.4e]Table 8a	O	N

MLF16	LL Capability	[802.15.4e]Table 8b	O	N
MLF17	DSME Capability	[802.15.4e] 6.2, Table 8c	O	N
MLF18	EBR capability	[802.15.4e] 5.3.12	O	Y
MLF18.1	EBR commands	[802.15.4e] 5.3.7	MLF18:O	Y
MLF18.1.1	EBR Enhanced Beacon request command	[802.15.4e] 5.3.7.2	FD1:M FD2:O	FD1:Y FD2:Y
MLF19	LE capability	[802.15.4e] 5.1.1.7, 5.1.11	O	O (#1)
MLF19.1	LE specific MAC sub-layer service specification	[802.15.4e] 6.4.3.7	MLF19:M	MLF19: Y
MLF19.2	Coordinated Sampled Listening (CSL) capability	[802.15.4e]5.1.11.1	MLF19:O.1	N
MLF19.3	Receiver Initiated Transmission (RIT) capability	[802.15.4e]5.1.11.2	MLF19:O.1	N
MLF19.4	LE superframe	[802.15.4e] 5.1.1.7.1, 5.1.1.7.2, 5.1.1.7.3	MLF19:O.1	MLF19: Y
MLF19.5	LE-multipurpose Wake-up frame	[802.15.4e]5.2.2.8	MLF19.2:M	N
MLF19.6	LE, CSL Information Element	[802.15.4e]5.2.4.7	MLF19.2:M	N
MLF19.7	LE RIT Information Element	[802.15.4e]5.2.4.8	MLF19.3:O	N
MLF19.8	LE-commands	[802.15.4e]5.3.12	MLF19.3:M	N
MLF20	MAC Metrics PIB Attributes	[802.15.4e]6.4.3.9	O	N
MLF21	FastA commands	[802.15.4e]5.1.3.3	O	N
MLF23	Channel Hopping	[802.15.4e] Table 52f	O	N

MLF23.1	Hopping IEs	[802.15.4e]5.2.4.16, 5.2.4.17	MLF18:M	N

O.1: Optional but at least one of the features described in FD1 and FD2 is required to be implemented

O.4: At least one of these features shall be supported.

#1: Implementation is optional.

3.4.2.2.2.MAC frames

The MAC frame requirements are described in **Table 4.8-6**.

Table 4.8-6 MAC frames

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)		Support (Y:Yes, N:No, O:Option)
			Transmitter	Receiver	
MF1	Beacon	[802.15.4] 5.2.2.1	FD1:M	M	Y
MF2	Data	[802.15.4] 5.2.2.2	M	M	Y
MF3	Acknowledgment	[802.15.4] 5.2.2.3	M	M	Y
MF4	Command	[802.15.4] 5.2.2.4	M	M	Y
MF4.1	Association request	[802.15.4] 5.2.2.4, 5.3.1	M	FD1:M	Y
MF4.2	Association response	[802.15.4] 5.2.2.4, 5.3.2	FD1:M	M	Y
MF4.3	Disassociation notification	[802.15.4] 5.2.2.4, 5.3.3	M	M	Y
MF4.4	Data request	[802.15.4] 5.2.2.4, 5.3.4	M	FD1:M	Y
MF4.5	PAN identifier conflict notification	[802.15.4] 5.2.2.4, 5.3.5	M	FD1:M	Y
MF4.6	Orphaned device notification	[802.15.4] 5.2.2.4, 5.3.6	M	FD1:M	Y
MF4.7	Beacon request	[802.15.4] 5.2.2.4, 5.3.7	FD1:M	FD1:M	Y
MF4.8	Coordinator realignment	[802.15.4] 5.2.2.4, 5.3.8	FD1:M	M	Y
MF4.9	GTS request	[802.15.4] 5.2.2.4, 5.3.9	MLF5:O	MLF5:O	N
MF5	4-octet FCS	[802.15.4g] 5.2.1.9	FD8:M	FD8:M	FD8:Y

3.4.3. Non-beacon mode profile

This sub-clause defines Wi-SUN 15.4 and 15.4e MAC profiles for ECHONET Lite, when non-beacon-enabled PAN is employed.

3.4.3.1. Functional device (FD) types

The requirements for the functional device types are described in **Table 4.8-7**.

Table 4.8-7 Functional device types

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)	Support (Y:Yes, N:No, O:Option)
FD1	FFD	[802.15.4] 5.1	O.1	O.1
FD2	RFD	[802.15.4] 5.1	O.1	O.1
FD3	Support of 64 bit IEEE address	[802.15.4] 5.2.1.1.6	M	Y
FD4	Assignment of short network address (16 bit)	[802.15.4] 5.1.3.1	FD1:M	FD1:Y
FD5	Support of short network address (16 bit)	[802.15.4] 5.2.1.1.6	M	Y
FD8	SUN PHY device	[802.15.4g] 8.1	O.2	Y (#1)

O.1: Optional but at least one of the features described in FD1 and FD2 is required to be implemented

O.2: At least one of these features is supported

#1: MR-FSK is employed.

3.4.3.2. Major capabilities for the MAC sub-layer

The major capabilities for the MAC sub-layer are described in this sub-clause.

3.4.3.2.1.MAC sub-layer functions

The MAC sub-layer function requirements are described in **Table 4.8-8**.

Table 4.8-8 MAC sub-layer functions

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory , O:Option)	Support (Y:Yes, N:No, O:Option)
MLF1	Transmission of data	[802.15.4] 6.3	M	Y
MLF1.1	Purge data	[802.15.4] 6.3.4, 6.3.5	FD1:M FD2:O	FD1:Y FD2: N
MLF2	Reception of data	[802.15.4] 6.3	M	Y
MLF2.1	Promiscuous mode	[802.15.4] 5.1.6.5	FD1:M FD2:O	FD1:Y FD2: N
MLF2.2	Control of PHY receiver	[802.15.4] 6.2.9	O	O
MLF2.3	Timestamp of incoming data	[802.15.4] 6.3.2	O	N
MLF3	Beacon management	[802.15.4] 5	M	Y
MLF3.1	Transmit beacons	[802.15.4] 5, 5.1.2.4	FD1:M FD2:O	FD1:Y FD2: N
MLF3.2	Receive beacons	[802.15.4] 5, 6.2.4	M	Y
MLF4	Channel access mechanism	[802.15.4] 5, 5.1.1	M	Y
MLF5	Guaranteed time slot (GTS) management	[802.15.4] 5, 6.2.6, 5.3.9, 5.1.7	O	N
MLF5.1	GTS management (allocation)	[802.15.4] 5, 6.2.6, 5.3.9, 5.1.7	O	N

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory , O:Option)	Support (Y:Yes, N:No, O:Option)
MLF5.2	GTS management (request)	[802.15.4] 5, 6.2.6, 5.3.9, 5.1.7	O	N
MLF6	Frame validation	[802.15.4] 6.3.3, 5.2, 5.1.6.2	M	Y
MLF7	Acknowledged frame delivery	[802.15.4] 5, 6.3.3, 5.2.1.1.4, 5.1.6.4	M	Y
MLF8	Association and disassociation	[802.15.4] 5, 6.2.2, 6.2.3, 5.1.3	M	Y
MLF9	Security	[802.15.4] 7	M	Y
MLF9.1	Unsecured mode	[802.15.4] 7	M	Y
MLF9.2	Secured mode	[802.15.4] 7	O	Y
MLF9.2.1	Data encryption	[802.15.4] 7	O.4	Y
MLF 9.2.2	Frame integrity	[802.15.4] 7	O.4	Y
MLF10.1	ED	[802.15.4] 5.1.2.1, 5.1.2.1.1	FD1:M FD2:O	FD1:Y FD2: N
MLF10.2	Active scanning	[802.15.4] 5.1.2.1.2	FD1:M FD2:O	FD1:Y FD2: Y
MLF10.3	Passive scanning	[802.15.4] 5.1.2.1.2	M	Y
MLF10.4	Orphan scanning	[802.15.4] 5.1.2.1, 5.1.2.1.3	M	Y

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory , O:Option)	Support (Y:Yes, N:No, O:Option)
MLF11	Control/define/determine/declare superframe structure	[802.15.4] 5.1.1.1	FD1:O	N
MLF12	Follow/use superframe structure	[802.15.4] 5.1.1.1	O	N
MLF13	Store one transaction	[802.15.4] 5.1.5	FD1:M	FD1:Y
MLF14	Ranging	[802.15.4] 5.1.8	RF4:O	N
MLF14.1	DPS	[802.15.4] 5.1.8.3,6.2.15	O	N
MLF15(4g)	MPM for all coordinators when operating at more than 1% duty cycle	[802.15.4g] 5.1.13	M	Y
MLF15	TSCH Capability	[802.15.4e] Table 8a	O	N
MLF16	LL Capability	[802.15.4e] Table 8b	O	N
MLF17	DSME Capability	[802.15.4e] 6.2, Table 8c	O	N
MLF18	EBR capability	[802.15.4e] 5.3.12	O	Y
MLF18.1	EBR commands	[802.15.4e] 5.3.7	MLF18:O	Y
MLF18.1.1	EBR Enhanced Beacon request command	[802.15.4e] 5.3.7.2	FD1:M FD2:O	FD1:Y FD2: Y

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory , O:Option)	Support (Y:Yes, N:No, O:Option)
MLF19	LE capability	[802.15.4e] 5.1.1.7, 5.1.11	O	O (#1)
MLF19.1	LE specific MAC sub-layer service specification	[802.15.4e] 6.4.3.7	MLF19:M	MLF19:Y
MLF19.2	Coordinated Sampled Listening (CSL) capability	[802.15.4e] 5.1.11.1	MLF19:O.1	MLF19:O.1
MLF19.3	Receiver Initiated Transmission (RIT) capability	[802.15.4e] 5.1.11.2	MLF19:O.1	MLF19:O.1
MLF19.4	LE superframe	[802.15.4e] 5.1.1.7.1, 5.1.1.7.2, 5.1.1.7.3	MLF19:O.1	N
MLF19.5	LE-multipurpose Wake-up frame	[802.15.4e] 5.2.2.8	MLF19.2:M	MLF19.2:Y
MLF19.6	LE, CSL Information Element	[802.15.4e] 5.2.4.7	MLF19.2:M	MLF19.2:Y
MLF19.7	LE RIT Information Element	[802.15.4e] 5.2.4.8	MLF19.3:O	MLF19.3:O
MLF19.8	LE-commands	[802.15.4e] 5.3.12	MLF19.3:M	MLF19.3:Y
MLF20	MAC Metrics PIB Attributes	[802.15.4e] 6.4.3.9	O	N
MLF21	FastA commands	[802.15.4e] 5.1.3.3	O	N
MLF23	Channel Hopping	[802.15.4e] Table 52f	O	N

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)	Support (Y:Yes, N:No, O:Option)
MLF23.1	Hopping IEs	[802.15.4e] 5.2.4.16, 5.2.4.17	MLF18:M	N

O.1: Optional but at least one of the features described in FD1 and FD2 is required to be implemented

O.4: At least one of these features shall be supported.

#1: Implementation is optional.

3.4.3.2.2.MAC frames

The MAC frame requirements are described in **Table 4.8-9**.

Table 4.8-9 MAC frames

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)		Support (Y:Yes, N:No, O:Option)
			Transmitter	Receiver	
MF1	Beacon	[802.15.4] 5.2.2.1	FD1:M	M	Y
MF2	Data	[802.15.4] 5.2.2.2	M	M	Y
MF3	Acknowledgment	[802.15.4] 5.2.2.3	M	M	Y
MF4	Command	[802.15.4] 5.2.2.4	M	M	Y
MF4.1	Association request	[802.15.4] 5.2.2.4, 5.3.1	M	FD1:M	Y
MF4.2	Association response	[802.15.4] 5.2.2.4, 5.3.2	FD1:M	M	Y
MF4.3	Disassociation notification	[802.15.4] 5.2.2.4, 5.3.3	M	M	Y
MF4.4	Data request	[802.15.4] 5.2.2.4, 5.3.4	M	FD1:M	Y
MF4.5	PAN identifier conflict notification	[802.15.4] 5.2.2.4, 5.3.5	M	FD1:M	Y
MF4.6	Orphaned device notification	[802.15.4] 5.2.2.4, 5.3.6	M	FD1:M	Y
MF4.7	Beacon request	[802.15.4] 5.2.2.4, 5.3.7	FD1:M	FD1:M	Y
MF4.8	Coordinator realignment	[802.15.4] 5.2.2.4, 5.3.8	FD1:M	M	Y
MF4.9	GTS request	[802.15.4] 5.2.2.4, 5.3.9	MLF5:O	MLF5:O	N
MF5	4-octet FCS	[802.15.4g] 5.2.1.9	FD8:M	FD8:M	Y

3.5. Wi-SUN ECHONET Lite interface part

3.5.1. Overview

Wi-SUN ECHONET Lite interface shall be composed of transport layer, network Layer, and adaptation layer. The data from transport/network layer is converted to PHY and MAC layer data via adaptation layer. On the other hand, the data from PHY/MAC layer is converted to network/transport layer data via adaptation layer. As transport layer protocol TCP or UDP may be used.

3.5.2. Requirement

(1) Wi-SUN ECHONET Lite interface shall provide Network Interface (NIC). MAC address in the NIC shall be one that can be extracted from MAC layer.

(2) Wi-SUN ECHONET Lite interface shall know address configuration used in MAC layer in advance.

(3) Wi-SUN ECHONET Lite interface shall analyze IPv6 header by taking address configuration in MAC layer and convert the destination address in IPv6 header to the destination address used in MAC layer

(4) Wi-SUN ECHONET Lite interface shall analyze IPv6 header. When the destination address is multicast address, the interface shall instruct MAC layer to do broadcast transmission.

(5) Wi-SUN ECHONET Lite interface shall use neighbor discovery (ND) function based on either IPv6 or 6LowPAN. The ND function is chosen not by every node but for every system.

3.5.3. Adaptation layer

The adaptation layer in the Wi-SUN ECHONET Lite Interface shall perform compression of IPv6 headers according to RFC6282 [6LPHC] and packet fragmentation according to RFC4944 [6LOWPAN]. The specific configurations are given in Table 4.8-10.

Table 4.8-10 Adaption layer of 6LoWPAN

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
6LP1.1	Addressing Modes (EUI-64)	[6LOWPAN] 3	Y

6LP1.2	Addressing Modes (short address)	[6LOWPAN] 3	N
6LP2	Frame Format	[6LOWPAN] 5	O (#1)
6LP3	Stateless Address Autoconfiguration	[6LOWPAN] 6	Y
6LP4	IPv6 Link Local Address	[6LOWPAN] 7	Y
6LP5	Unicast Address Mapping	[6LOWPAN] 8	Y (#2)
6LP6	Multicast Address Mapping	[6LOWPAN] 9	N
6LP7	Encoding of IPv6 Header Fields	[6LOWPAN] 10.1	N (#3)
6LP8	Encoding of UDP Header Fields	[6LOWPAN] 10.2	N (#3)
6LP9	Non-Compressed Fields	[6LOWPAN] 10.3	Y
6LP10	Frame Delivery in a Link-Layer Mesh	[6LOWPAN] 11	N

(#1) Header Type = LOWPAN_HC1 shall not be used and Header Type = LOWPAN_BC0 and [6LOWPAN] 5.2 are option

(#2) 16bit address (short address) shall not be used

(#3) For header compression, IPHC[6LPHC] shall be used and HC1 and HC2 in [6LOWPAN] shall not be used.

3.5.3.1. Fragmentation

The 6LoWPAN fragmentation requirements shall be implemented in Wi-SUN ECHONET Lite interface are described in Table 4.8-11.

Table 4.8-11 Fragmentations of 6LoWPAN

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
6LPF1	Fragmentation type and Header	[6LOWPAN] 5.3	Y

3.5.3.2. Header compression

The 6LoWPAN Header compression requirements are described in Table 4.8-12.

Basically every node shall support header compression described in [6LPHC] but the header compression used context ID including compression of stateful multicast address shall not be supported. Moreover, compression for IPv6 extension header and UDP header by LOWPAN_NHC shall not be supported. The node that has capability to receive IPv6 packet shall receive non-compressed IPv6 packet, IPv6 packet compressed by the conditions in this section, and IPv6 packet partially compressed by [6LPHC].

Table 4.8-12: 6LoWPAN Header compression

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
6HC1.1	LOWPAN_IPHC (Base Format)	[6LPHC] 3.1.1	Y
6HC1.2	Context Identifier Extension	[6LPHC] 3.1.2	N
6HC2.1	Stateless Multicast Address Compression	[6LPHC] 3.2.3	Y
6HC2.2	Stateful Multicast Address Compression	[6LPHC] 3.2.4	N
6HC4	LOWPAN_NHC (IPv6 Extension Header Compression)	[6LPHC] 4.2	N
6HC5	LOWPAN_NHC (UDP Header Compression)	[6LPHC] 4.3	N

Since Wi-SUN ECHONET Lite interface shall not support context ID and shall support link local address based on EUI-64 address for IPv6 packet, LOWPAN_IPHC encoding header [6LPHC] in IPv6 packet shall be composed in Figure4.8-3.

(bit)

0	1	2	3 4	5	6 7	8	9	10	11	12	13	14	15
0	1	1	TF *1	NH *2	HLIM *3	0	0	1	1	0	0	1	1

Figure4.8-3 LOWPAN_IPHC encoding header for unicast packet

*1: TF = 0b11(Traffic Class and Flow Label are elided)

*2: NH = 0b0(Full 8 bits for Next Header are carried in-line)

*3: HLIM = 0b11(The Hop Limit field is compressed and the hop limit is 255)

When the IPv6 packet is a multicast packet, LOWPAN_IPHC format presented in **Figure 4.8-4** and field values specified in **Table 4.8-13** are used instead of Figure4.8-3**.**

(bit)

0	1	2	3 4	5	6 7	8	9	10 11	12	13	14 15
0	1	1	TF	NH	HLIM	CID	SAC	SAM	M	DAC	DAM

Figure 4.8-4 LOWPAN_IPHC encoding header for multicast packet

Table 4.8-13 Values to be set into LOWPAN_IPHC for multicast packet

Packet Type	Fields									Remarks
	TF	NH	HLIM	CID	SAC	SAM	M	DAC	DAM	
	Bit 3-4	5	6-7	8	9	10-11	12	13	14-15	
Solicited-node multicast for DAD	0b11	0b0	0b11	0	1*1	0b00*1	1*2*3	0*2*3	0b01*2	Destination address takes the form FF02::1:FFXX:XXXX, where “XX:XXXX” is the low-order 24 bits of the target address.
Solicited-node multicast for ND					0	0b11				

Any other type of multicast packets									0b11[*3]	Destination address takes the form FF02::00XX, where XX is 0x01 or 0x02 to be specified in the in-line header.

*1: The UNSPECIFIED address is set to the source address of NS for DAD, as specified in 4.3 of [ND]. It is converted to SAC=1 and SAM=00 according to the method specified in 3.1.1 of [6LPHC]

*2: The solicited-node multicast address is set to the destination address of NS, as specified in 4.3 of [ND]. It is converted to M=1, DAC=0, and DAM=01 according to the method specified in 3.1.1 of [6LPHC].

*3: A link-local multicast address is set to the destination address of other multicast packet which is not NS. It is converted to M=1, DAC=0, and DAM=11 according to the method specified in 3.1.1 of [6LPHC]

3.5.3.3. Neighbor discovery

Wi-SUN ECHONET Lite interface shall support either RFC 4861[ND] or RFC6775 [6LND]. 6LoWPAN Neighbor discovery requirements in RFC6775 are described in Table 4.8-14. The requirements of routing function to realize multihop operation are out of scope of this document.

Table 4.8-14 6LoWPAN Neighbor discovery

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
6ND1	DHCPv6 Address Assignment for 6LBR, 6LR and Host	[6LPND] 3.2	O
6ND2	DHCPv6 Prefix Delegation for 6LBR	[6LPND] 3.2, 7.1	O
6ND3	DHCPv6 Prefix Delegation for 6LR and Host	[6LPND] 3.2, 7.1	O
6ND4	Static IPv6 address configuration on 6LBR	[6LPND] 5.4.1	O
6ND5	Static IPv6 address configuration on 6LR and Host	[6LPND] 5.4.1	O
6ND6	EUI-64 based IPv6 Address Generation	[6LPND] 5.4.1	Y
6ND7	802.15.4 16-bit short address	[6LPND] 1.3	O
6ND8	802.15.4 64-bit extended address	[6LPND] 1.3	Y
6ND9	Duplicate Address Detect	[6LPND] 4.4	O
6ND10	Duplicate Address messages (DAR and DAC)	[6LPND] 4.4	O
6ND11	Support Source Link-Layer Address Option (SLLAO)	[6LPND] 4.1, 5.3	Y
6ND12	Support Address Registration Option (ARO)	[6LPND] 5.5	Y
6ND13	Support Authoritative Border Router Option (ABRO)	[6LPND] 3.3, 3.4, 4.3, 6.3	O
6ND14	Support Prefix Information Option (PIO)	[6LPND] 3.3, 5.4	O
6ND15	Support 6LoWPAN Context Option (6CO)	[6LPND] 4.2	O
6ND16	Multihop Prefix and Context Distribution	[6LPND] 8.1	O
6ND17	Multihop DAD	[6LPND] 8.2	O
6ND18	Support Router Discovery	[6LPND]	Y
6ND19	Support RA based Address Configuration on 6LR and Host	[6LPND]5.4.1	O
6ND20	Support Neighbor Cache Management	[6LPND] 3.5	Y
6ND21	Support Address Registration	[6LPND] 3.2	Y
6ND22	Support Address unregistration	[6LPND] 3.2	Y

6ND23	Support Neighbor Unreachable Detection	[6LPND] 5.5	Y
6ND24	Send Multicast NS	[6LPND] 6.5.5	O
6ND25	Send Unicast NS	[6LPND]5.5	Y

3.5.4. Network layer

Wi-SUN ECHONET Lite interface shall support IPv6 protocol [IPv6] in Table 4.8-15. Hop-by-hop options extension header, Routing extension header, Fragment extension header, Destination Options extension header, AH extension header, and ESP extension header are optional. Wi-SUN ECHONET Lite interface also shall support ICMPv6 protocol [ICMPv6] in Table 4.8-16. Wi-SUN ECHONET Lite interface shall support Echo Request Message (type=128) and Echo Reply Message (type=129), Destination Unreachable Message (type=1), Time Exceeded Message (type=3) and Parameter Problem Message (type=4). For Packet Too Big Message (type=2), Wi-SUN ECHONET Lite interface may not support transmission function but may support receipt function.

Table 4.8-15 Network Layer: IPv6

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
IP1	Header Format	[IPv6] 3	Y
IP1.1	Extension Headers	-	Y
IP1.2	Extension Header Order	[IPv6]4.1	Y
IP1.3	Options	[IPv6] 4.2	Y
IP1.4	Hop-by-Hop Options Header	[IPv6] 4.3	O
IP1.5	Routing Header	[IPv6]4.4	O
IP1.6	Fragment Header	[IPv6] 4.5	O
IP1.7	Destination Options Header	[IPv6] 4.6	O
IP1.8	No Next Header	[IPv6]4.7	Y
IP1.9	AH Header	[AH]	O
IP1.10	ESP Header	[ESP]	O
IP2	Deprecation of Type 0 Routing Headers	[IPv6-RH]	Y
IP3	Path MTU Discovery	[IPv6] 5	Y
IP4	Flow Labels	[IPv6] 6	Y
IP5	Traffic Classes	[IPv6] 7	Y

Table 4.8-16 Network Layer: ICMPv6

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
ICMP1	Message Format	[ICMP6] 2.1	Y
ICMP2	Message Source Address Determination	[ICMP6] 2.2	Y
ICMP3	Message Checksum Calculation	[ICMP6] 2.3	Y
ICMP4	Message Processing Rules	[ICMP6] 2.4	Y
ICMP5	Destination Unreachable Message	[ICMP6] 3.1	Y
ICMP6	Packet Too Big Message	[ICMP6] 3.2	Y
ICMP7	Time Exceeded Message	[ICMP6] 3.3	Y
ICMP8	Parameter Problem Message	[ICMP6] 3.4	Y
ICMP9	Echo Request Message	[ICMP6] 4.1	Y
ICMP10	Echo Reply Message	[ICMP6] 4.2	Y

3.5.4.1. IP addressing

Wi-SUN ECHONET Lite interface shall support IPv6 addressing [IP6ADDR] and IPv6 Stateless Address Autoconfiguration [SLAAC] defined in Table 4.8-17. Wi-SUN ECHONET Lite interface shall support link local address based on EUI-64. In the case, according to description in [6LOWPAN] and [SLAAC], well known link-local prefix FE80::0/64 shall be used as prefix and interface identifier shall be generated from EUI-64 address. IPv6 link-local address, global address, and unique local address derived the short address defined in [802.15.4] shall not be used.

Table 4.8-17 IP Addressing

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
IPAD1	IPv6 Addressing	[IP6ADDR]	Y (*1)
IPAD1.1	Global Unicast Address	[IP6ADDR] 2.5.4	N
IPAD1.2	Link Local Unicast Address	[IP6ADDR] 2.5.6	Y (*2)
IPAD1.3	Unique Local Unicast Address	[ULA]	N
IPAD1.4	Anycast Address	[IP6ADDR] 2.6	N
IPAD1.5	Multicast Address	[IP6ADDR] 2.7	Y (*3)
IPAD1.6	Prefix Length		/64
IPAD2	Stateless Address Autoconfiguration	[SLAAC]	Y
IPAD2.1	Creation of Link Local Address	[SLAAC] 5.3	Y
IPAD2.2	Creation of Global Addresses	[SLAAC] 5.5	N

(*1) Some of the functions may not be used.
(*2) EUI-64 address based Link Local Address shall be supported.
(*3) ff02::1 shall be used for transmission.

3.5.4.2. Neighbor discovery

Wi-SUN ECHONET Lite interface shall support either RFC 4861[ND] or RFC6775 [6LND]. IPv6 Neighbor discovery requirements in RFC4861 are described in Table 4.8-18. Wi-SUN ECHONET Lite interface shall support two functions: Address Resolution and Duplicate Address Detection and shall support two messages: Neighbor Solicitation message: Type = 135 and Neighbor Advertisement message: Type = 136.

Table 4.8-18 IPv6 Neighbor discovery

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option)
ND1	Router and Prefix Discovery	[ND]6	N
ND2	Address Resolution	[ND] 7.2	Y
ND3	Neighbor Unreachability Detection	[ND] 7.3	N
ND4	Duplicate Address Detection	[SLAAC] 5.4	O
ND5	Redirect Function	[ND] 8	N
ND6	Router Solicitation Message	[ND]4.1	N
ND7	Router Advertisement Message	[ND] 4.2	N
ND8	Neighbor Solicitation Message	[ND] 4.3	Y(*1)
ND9	Neighbor Advertisement Message	[ND] 4.4	Y(*2)
ND10	Redirect Message	[ND] 4.5	N
ND11	Source/Target Link-layer Address Option	[ND] 4.6.1	Y
ND12	Prefix Information Option	[ND] 4.6.2	N
ND13	Redirected Header Option	[ND] 4.6.3	N
ND14	MTU Option	[ND] 4.6.4	N

*1: The Source Link-Layer Address option contains an EUI-64 format address.

*2: The Target Link-Layer Address option contains an EUI-64 format address.

3.5.4.3. Multicast

In transmitting multicast packet for ECHONET Lite, ff02::1 is set as destination address based on [EL].

3.5.5. Transport layer

UDP [UDP] shall be implemented and TCP [TCP], may be implemented. The destination port number of UDP and TCP frames and operation procedure for TCP shall follow the specification in [EL].

3.5.6. Application layer

Wi-SUN ECHONET Lite interface shall support ECHONET Lite [EL] as application layer. The node implemented specifications in this document shall support mandatory function defined in [EL].

3.5.7. Security configuration

3.5.7.1. Overview

This clause describes a security mechanism for single-hop network.

PANA [PANA] shall be used as the EAP [EAP] transport for authentication between the coordinator and a host.

EAP-PSK [EAP-PSK] shall be used as the EAP method carried in PANA messages.

The coordinator and the host share a link key after successful authentication. The link key shall be used for AES-128-CCM* ciphering described in [802.15.4] MAC layer security.

3.5.7.2. Authentication

The coordinator shall be PANA Authentication Agent (PAA) and the host shall be PANA Client (PaC).

3.5.7.2.1.PANA

- PANA messages shall be sent using IPv6 UDP.
- PaC knows the IP address of PAA before starting PANA session negotiation.
- The UDP destination port number shall be set to 716.
- The PANA session shall be initiated by the PaC.
- Compliant nodes shall support PRF_HMAC_SHA2_256 (AVP Value=5).
- Compliant nodes shall support AUTH_HMAC_SHA2_256_128 (AVP Value=12).
- An EAP-Response should be piggybacked on the PANA-Auth-Answer message.
- The length of the nonce value in the Nonce AVP shall be 16 octets.
- The lifetime value in the Session-Lifetime AVP shall not be set less than 60 seconds.

3.5.7.2.2.EAP

- EAP-PSK shall be used.
- The length of the pre-shared key is 16 octets.

- The length of Master Session Key (MSK) and Extended Master Session Key (EMSK) is 64 octets.
- EAP Server ID (ID_S) and peer's ID (ID_P) shall use Network Address Identifier (NAI).
- The length of ID_S and ID_P shall not be greater than 63 octets.
- The retransmission in EAP layer shall not be used.

3.5.7.3. Key generation

The lifetime of the link key which shared with the peer after PANA session establishment shall be the same as the PANA session lifetime. Both PAA and PaC shall use the newest derived key after PANA session renewal (PANA Re-Authentication phase or Authentication and Authorization phase). If a PANA session is terminated before the PANA session lifetime expiration, any keys derived in this session shall be revoked.

3.5.7.3.1.PANA

The following algorithms shall be used for PANA message authentication.

Table 4.8-19 PANA algorithm types (defined in [HMAC-SHA256])

Algorithm	Type	Value
PRF	PRF_HMAC_SHA2_256	5
PANA_AUTH_HASH	AUTH_HMAC_SHA2_256_128	12

3.5.7.3.2.EAP-PSK

See [EAP-PSK].

3.5.7.3.3.MAC layer security (link key)

The link key (LK) is derived from the EMSK after successful PANA negotiation.

The master secret Usage-Specific Root Key (USRK) is generated by Key Derivation Function (KDF). The KDF is described in [USRK] and then the LK is derived from the USRK.

USRK = KDF(EMSK, “String(*1)” | “\0” | optional data | length)

- optional data = NULL(0x00)
- length = 64

LK = KDF(USRK, “String(*2)” | “\0” | optional data | length)

- optional data = EAP ID_P | EAP ID_S | IEEE802.15.4 Key Index
- length = 16

*1,*2: These strings are defined in each recommended usage sections.

The KDF algorithm is the same as the PANA PRF (PRF_HMAC_SHA2_256). The length value in the KDF is unsigned 8-bit integer. The IEEE 802.15.4 Key Index is the lower 8-bit value of the MSK Identifier in Key-Id AVP.

PAA shall not assign consecutively MSK Identifiers that has same lower 8-bit value to the same PaC.

As the result of successful PANA authentication, a LK is shared between the PAA and the PaC.

3.5.7.4. Encryption and Integrity check in MAC layer

MAC data frame shall be ciphered by the LK described in [802.15.4].

Compliant nodes shall use the newest LK in every PANA session renewal.

The Frame Counter value in the MAC frame shall be set to zero in every renewal of LK.

The host shall renegotiate new PANA session before the incoming/outgoing Frame Counter overflow.

ENC-MIC-32 (security level 5) shall be used for MAC layer security.

Both coordinator and host shall discard invalid MAC frame.

Key identifier mode is 0x01, Key Source is not used (1 octet Key-Index).

All PANA messages (UDP destination port 716) and IPv6 Neighbor Solicitation (NS) (ICMPv6 Type 135 Code 0)/Neighbor Advertisement (NA) (ICMPv6 Type 136 code 0) messages shall not be applied MAC layer security (do not add MAC Auxiliary Security header).

3.5.7.5. Replay protection

All ciphered MAC frames are protected from replay attacks by checking Frame Counter value in MAC Auxiliary Security header.

3.5.8. Frame format

A sample procedure of frame formatting in the case of UDP communication is shown in **Figure4.8-5 –Figure4.8-8**.

Variable
ECHONET Lite Payload

Figure4.8-5 ECHONET-Lite payload

40 byte	0 － n byte	8 byte	Variable
IPv6 Header	Ext Header	UDP Header	ECHONET Lite Payload

Figure4.8-6 IPv6 frame configured by Wi-SUN ECHONET Lite interface

2 byte	Depends on LOWPAN_IPHC	0 – n byte	Variable
LOWPAN_IPHC Encoded	In-line IP fields	In-line UDP Header Fields	ECHONET Lite Payload

Figure4.8-7 6LowPAN frame configure by Wi-SUN ECHONET Lite interface

Variable	2 byte	Depends on LOWPAN_IPHC	0 – n byte	Variable	2 byte

IEEE802.15.4 header	LOWPAN_IPHC Encoded	In-line IP fields	In-line UDP Header Fields	ECHONET Lite Payload	FCS

Figure4.8-8 IEEE802.15.4 frame configured by MAC layer

3.6. Recommended usage for single-hop home network

3.6.1. Overview

This clause clarifies the recommended usage in constructing single-hop network for ECHONET Lite over IPv6. Note that this profile does not exclude other usages.

Compliant nodes to this clause constructs single hop network where a coordinator is centered. And, with assuming a gateway connection provided by application layer as the connection measure to the outer networks, a closed IP network is assumed inside this profile. On those assumptions, the indoor network construction based on ECHONET Lite provides expandability as well as feasibility.

3.6.2. PHY part

Required specifications in terms of IEEE 802.15.4/4e/4g standards in order to realize this usage are shown in Table 4.8-20 and Table 4.8-21.

Table 4.8-20 Device/PHY layer specifications in order to realize the usage

Item number *1	Recommend (Y:Yes, N:No, O:Option)	Item number *2	Recommend (Y:Yes, N:No, O:Option)	Item number *3	Recommend (Y:Yes, N:No, O:Option)	Item number *3	Recommend (Y:Yes, N:No, O:Option)
FD1	O.1	PLF1	Y	RF12	—	RF13.4	Supporting 100kbps only OR both of 100kbps and 50kbps
FD2	O.1	PLF2	Y	RF12.1	Y	RF13.5	N
FD3	Y	PLF3	Y	RF12.2	N	RF14	—
FD4	N	PLF4	Y	RF12.3	N	RF14.1	N
FD5	N	PLF4.1	Y	RF12.4	N	RF14.2	N
FD8	Y	PLF4.2	N	RF12.5	N	RF14.3	Y
		PLF4.3	N	RF12.6	Y	RF14.4	N

		PLP1	PSDU size up to 255 octets	RF13	—		

*1: Corresponding to item number in Table 4.8-7 Functional device types
*2: Corresponding to item number in Table 4.8-2 PLF and PLP capabilities PLF and PLP capabilities
*3: Corresponding to item number in Table 4.8-3 RF capabilities

Table 4.8-21: Additional PHY layer specifications in order to realize the usage

Parameters	Recommend	Remarks
Modulation scheme	GFSK	
Data rate	100kbps or 50kbps	
Transmission power	20mW or less	
Frequency channel	Channels of No. 33 to 60 defined by ARIB with bundling of an odd channel and the next even channel, or channels of No. 33 to 61 without bundling.	Channels of No. 33 to 38 are also utilized by systems employing 250 mW transmission power.
Frequency channel width	400kHz (with 2 channel bundling), or 200kHz	
Transmission preamble length	1200us - 4000us	
Preamble length assumed at receiver	1200us	

3.6.3.MAC part

3.6.3.1. MAC layer specifications

Required specifications in terms of IEEE 802.15.4/4e/4g standards in order to realize the recommended usage by ECHONET Lite are shown in Table 4.8-22. Non-beacon enabled configurations are selected by MAC layer when these specifications are deployed.

Table 4.8-22 MAC layer specifications in order to realize the usage

Item number *1	Recommend (Y:Yes, N:No, O:Option)	Item number *1	Recommend (Y:Yes, N:No, O:Option)	Item number *1	Recommend (Y:Yes, N:No, O:Option)	Item number *2	Recommend (Y:Yes, N:No, O:Option)
MLF1	Y	MLF7	Y	MLF15	N	MF1	Y
MLF1.1	O*3*5	MLF8	O*6	MLF16	N	MF2	Y
MLF2	Y	MLF9	Y	MLF17	N	MF3	Y
MLF2.1	N	MLF9.1	Y	MLF18	Y	MF4	Y
MLF2.2	O*4	MLF9.2	Y	MLF18.1	Y	MF4.1	O*6
MLF2.3	N	MLF9.2.1	Y	MLF18.1.1	Y	MF4.2	O*6
MLF3	Y	MLF9.2.2	Y	MLF19	N*8	MF4.3	O*6
MLF3.1	Y*5	MLF10.1	Y*5	MLF19.1	N*8	MF4.4	O*3
MLF3.2	Y	MLF10.2	Y	MLF19.2	N*8	MF4.5	N
MLF4	Y	MLF10.3	N	MLF19.3	N	MF4.6	O*3
MLF5	N	MLF10.4	O*3	MLF19.4	N	MF4.7	Y*9
MLF5.1	N	MLF11	N	MLF19.5	N*8	MF4.8	O*3
MLF5.2	N	MLF12	N	MLF19.6	N*8	MF4.9	N
MLF6	Y	MLF13	O*3	MLF19.7	N	MF5	Y*10
		MLF15(4g)	O*7	MLF19.8	N		
				MLF20	N		
				MLF21	N		
				MLF23	N		
				MLF23.1	N		

*1: Corresponding to item number in Table 4.8-8 MAC sub-layer functions
*2: Corresponding to item number in Table 4.8-9 MAC frames
*3: Not mandated for the network constructed only by devices with permanent power supply.
*4: May be employed as necessary.
*5: Not employed by FD2.
*6: Not mandated when done by upper layer.
*7: Employed when 50kbps and 100kbps modes coexist.
*8: Not employed since single-hop communications are assumed.
*9: May be employed by FD2 (not clarified in references).
*10: 2-octet FCS is employed when PSDU size is no more than 255 octets

3.6.3.2. MAC frame format

This section describes frame format, based on [802.15.4] 5.2 MAC frame formats.

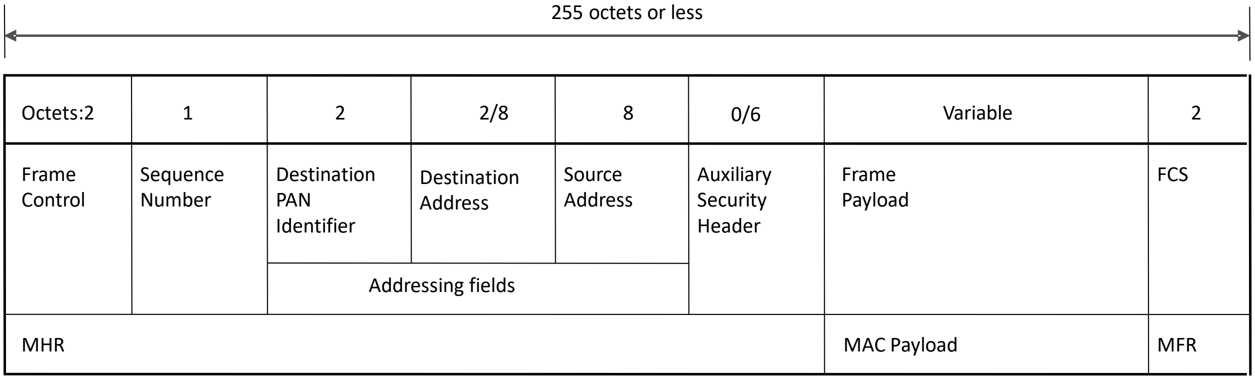
Enhanced Beacon and Enhanced Beacon Request are not allowed to be encrypted. Any frame shall not be encrypted if it contains IEs.

Header IE shall not be used and Payload IE follows MHR without Header IE list terminator when IEs List Present field in the frame control is one.

Note that this omission of Header IE list terminator may be incompatible with [802.15.4e].

3.6.3.2.1.Data frame format

Figure 4.8-9 shows the DATA frame format used in this specification. (Clarifies the usage in this specification, based on [802.15.4e] 5.2.2.2 Data frame format)



Octets:2	1	2	2/8	8	0/6	Variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing fields					
MHR						MAC Payload	MFR

Figure 4.8-9 DATA frame format

(1) Frame Control field

The fields of the Frame Control field are shown in Table 4.8-23.

Table 4.8-23 Frame Control (DATA frame)

bit	fields	remark
2-0	Frame Type	"001", meaning DATA frame
3	Security Enable	"0" if the security is disabled, "1" if security is enabled.
4	Frame Pending	"0", do not use

5	AR (Ack Request)	"0" in case ACK is not requested (broadcast), "1" in case ACK is requested (unicast)
6	PAN ID Compression	"0", based on [802.15.4e] Table 2a
7	Reserved	as a rule set to "0", but don't care
8	Sequence Number Suppression	"0", do not suppress Sequence Number field
9	IE List Present	"0", do not use IEs.
11-10	Destination Addressing Mode	"11", for 64 bit extended address "10", for 16-bit broadcast address
13-12	Frame Version	"10", for extended format*1,*2
15-14	Source Addressing Mode	"11", for 64 bit extended address

*1:This field is always set to 0b10 to indicate a frame non-compatible with 802.15.4-2003/2006, because enhanced acknowledgment frame is assumed.

*2:ECHONET Lite profile assumes the following specifications:

a) ECHONET Lite devices shall be capable of receiving a beacon, data, acknowledgment and command frames (frames with frame type field set to 0,1,2 or 3) with the frame version field set to 10b and process the frame according to 802.15.4;

b) ECHONET Lite devices may be capable of receiving a beacon, data, acknowledgment and command frame with frame version field set to 00 or 01, and will process the frame according to 802.15.4;

c) ECHONET Lite devices shall, when generating beacon, data, acknowledgment and command frame, set the frame version field to 10b" to this table.

(2) Sequence Number field

See [802.15.4] 5.2.1.2 Sequence Number field.

(3) Addressing field

Source address is 64-bit MAC address and destination address is either 16-bit broadcast address (0xFFFF) or 64-bit MAC address. These address fields are transmitted least significant octet first and each octet shall be transmitted least significant bit (LSB) first.

The source PAN Identifier is not included in the address field. PAN Identifier is transmitted from LSBit, treated as 16-bit numerical number.

(4) Auxiliary Security Header field

Table 4.8-24 shows the fields of the Auxiliary Security Header that is used to encrypt the frame.

Table 4.8-24 Auxiliary Security Header

octet	bit	fields		remark
1	b2-b0	Security Control	Security Level	"101", for ENC-MIC-32
	b4-b3		Key Identifier Mode	"01" for 1 octet Key Identifier
	b7-b5		Reserved	-
4	-	Frame Counter		
1	-	Key Identifier		

3.6.3.2.2. ACK frame format

Figure 4.8-10 shows the ACK frame format used in this specification. (clarifies the usage in this specification, based on [802.15.4e] 5.2.2.3 Acknowledgment frame format）

Octets:2	1	2	8	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	FCS
		Addressing fields		
MHR				MFR

Figure 4.8-10 ACK frame format

(1) Frame Control field

Table 4.8-25 shows the fields of the Frame Control field.

Table 4.8-25 Frame Control (ACK frame)

bit	fields	remark
2-0	Frame Type	"010", meaning ACK frame
3	Security Enable	"0", security is disabled
4	Frame Pending	"0", do not use
5	AR(Ack Request)	set to "0"
6	PAN ID Compression	"0", based on [802.15.4e] Table 2a
7	Reserved	set to "0"
8	Sequence Number Suppression	"0", do not suppress Sequence Number field
9	IE List Present	"0" , do not use IEs
11-10	Destination Addressing Mode	"11", for 64 bit extended address
13-12	Frame Version	"10", for extended format
15-14	Source Addressing Mode	"00", do not use Source Address

(2) Sequence Number field

Refer to [802.15.4] 5.2.1.2 Sequence Number field. Ack frame uses the same value of the received Data frame in response.

(3) Addressing field

Destination Address is set to the Source Address of the received frame to respond. Refer to section 3.6.3.2.1 DATA frame format (3) Addressing field of this specification.

3.6.3.2.3.Enhanced Beacon frame format

Figure 4.8-11 shows the Enhanced Beacon frame format used in this specification. (clarifies the usage in this specification, based on [802.15.4e] 5.2.2.1 Beacon frame format).

Octets:2	1	2	8	8	Variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source Address	Payload IE	FCS
		Addressing fields				
MHR					MAC Payload	MFR

Figure 4.8-11 Enhanced Beacon frame format

(1) Frame Control field

Table 4.8-26 shows the fields of the Frame Control field.

Table 4.8-26 Frame Control (Enhanced Beacon frame)

bit	fields	remark
2-0	Frame Type	"000", meaning Beacon frame
3	Security Enable	"0", security is disabled
4	Frame Pending	"0", do not use
5	AR (Ack Request)	"1", ACK is requested (unicast)
6	PAN ID Compression	"0", based on [802.15.4e] Table 2a
7	Reserved	as a rule set to "0", but don't care
8	Sequence Number Suppression	"0", do not suppress Sequence Number field
9	IE List Present	"1" , in case use IEs, "0" in case do not use IEs
11-10	Destination Addressing Mode	"11", for 64 bit extended address
13-12	Frame Version	"10" required for Enhanced Beacon
15-14	Source Addressing Mode	"11", for 64 bit extended address

(2) Sequence Number field

Based on [802.15.4e] 5.2.2.1.1 Beacon frame MHR fields, Sequence Number (macEBSN) held by the device.

(3) Addressing field

Destination Address is set to the source address of the enhancement beacon request. Refer to section 3.6.3.2.1 DATA frame format (3) Addressing field of this specification.

Destination PAN Identifier is set to the source PAN Identifier.

(4) Payload IE field

The same IEs of the Enhanced Beacon Request.

3.6.3.2.4. Enhanced Beacon request command frame format

Figure 4.8-12 shows the Enhanced Beacon request command frame format used in this specification. (Clarifies the usage in this specification, based on [802.15.4e] 5.3.7.2 Enhanced beacon request)

Octets:2	1	2	2	8	Variable	1	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source Address	Payload IE	Command Frame Identifier	FCS
		Addressing fields					
MHR					MAC Payload		MFR

Figure 4.8-12 Enhanced Beacon request command frame format

(1) Frame Control field

Table 4.8-27 shows the fields of the Frame Control field.

Table 4.8-27 Frame Control (Enhanced Beacon request command frame)

bit	fields	remark

2-0	Frame Type	"011", meaning MAC command
3	Security Enable	"0", security is disabled
4	Frame Pending	"0", do not use
5	AR (Ack Request)	"0", ACK is not requested (broadcast)
6	PAN ID Compression	"0", based on [802.15.4e] Table 2a
7	Reserved	set to "0"
8	Sequence Number Suppression	"0", do not suppress Sequence Number field
9	IE List Present	"1" , in case use IEs, "0" in case do not use IEs
11-10	Destination Addressing Mode	"10", for 16-bit broadcast address
13-12	Frame Version	"10" required for Enhanced Beacon Request
15-14	Source Addressing Mode	"11", for 64 bit extended address

(2) Sequence Number field

Refer to [802.15.4] 5.2.1.2 Sequence Number field

(3) Addressing field

Refer to section 3.6.3.2.1 DATA frame format (3) Addressing field of this specification.

(4) Payload IE field

Refer to section 3.6.6.1.1 MAC procedure

(5) Command Frame Identifier field

"0x07",based on [802.15.4e] Table 5.

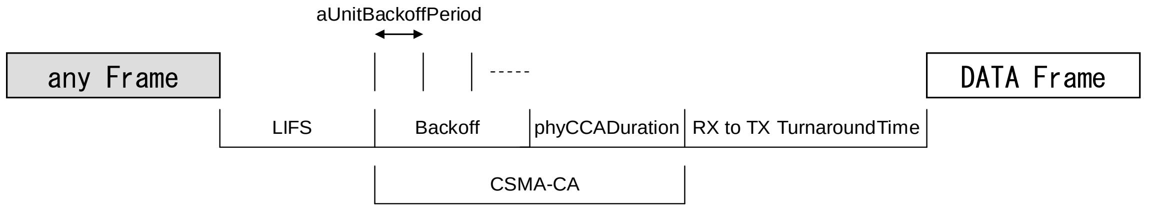
3.6.3.3. MAC functional description

This section describes the MAC features of this specification.

3.6.3.3.1.Transmission timing

(1) Transmission timing of DATA frame

Figure 4.8-13 shows the transmission timing of DATA frame. (Clarifies the timing description of this specification, based on [802.15.4] 5.1.1.4 CSMA-CA algorithm, [802.15.4g] Table 51)



parameter *1	formula	nominal value *2 [μsec]
LIFS	aTurnaroundTime	1000
aUnitBackoffPeriod	phyCCADuration＋ aTurnaroundTime	1130
phyCCADuration	－	130
RX to TX TurnaroundTime	－	300 or more , 1000 or less

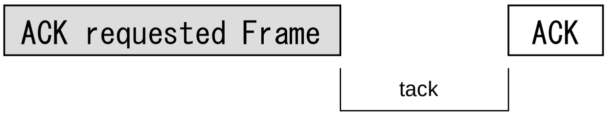
*1: Refer to 3.6.3.3.5 of this specification

*2: For the error range of each value, refer to [802.15.4], [802.15.4e], [802.15.4g].

Figure 4.8-13 Transmission timing description of DATA frame

(2) Transmission timing of ACK frame

Figure 4.8-14 shows the transmission timing of ACK frame. (Clarifies the timing description of this specification, based on [802.15.4] 5.1.1.3 Interframe spacing (IFS))



parameter*1	formula	nominal value [μsec]
tack	RX to TX TurnaroundTime	300 or more, 1000 or less *2

*1: Refer to 3.6.3.3.5 of this specification

*2: TX to RX TurnaroundTime shall be 300μs or less.

Figure 4.8-14 Transmission timing description of ACK frame

3.6.3.3.2.CSMA-CA

Figure 4.8-15 shows the CSMA-CA algorithm including retry. (Clarifies CSMA-CA algorithm including retry of this specification, based on [IEEE802.15.4e] 5.1.1.4 CSMA-CA algorithm)

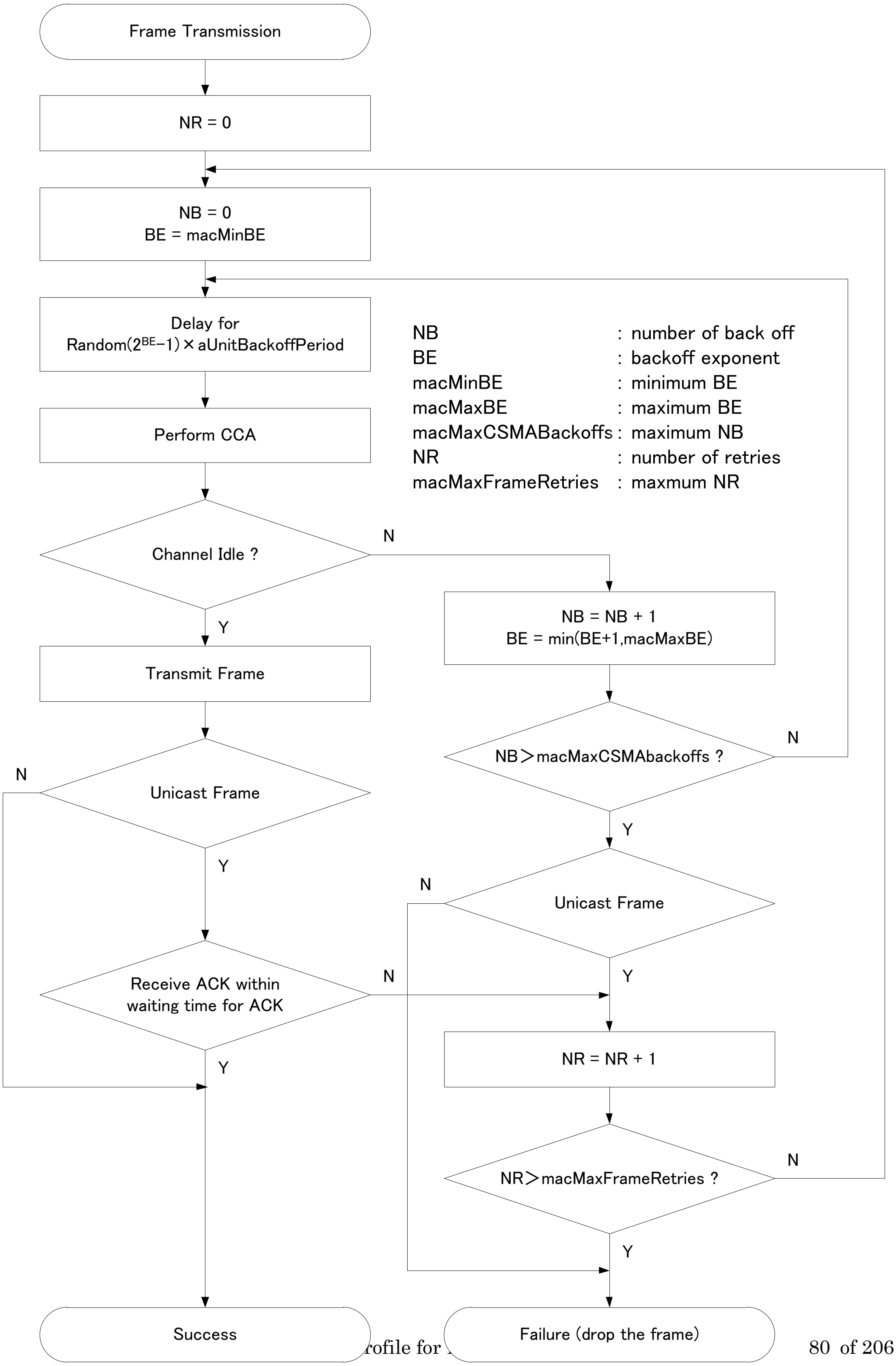
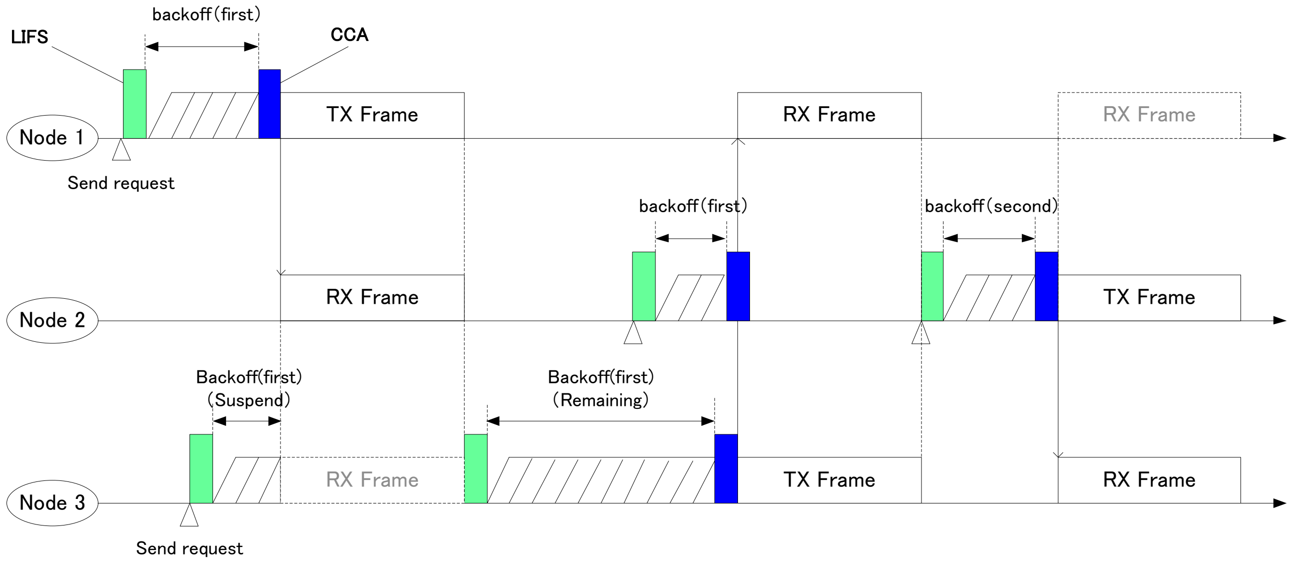

Frame Transmission
NR = 0
NB = 0
BE = macMinBE
Delay for
Random(2^BE−1)×aUnitBackoffPeriod
Perform CCA
Channel Idle ?
N
Y
NB = NB + 1
BE = min(BE+1,macMaxBE)
NB＞macMaxCSMAbackoffs ?
N
Y
Transmit Frame
Unicast Frame
N
Y
Unicast Frame
N
Y
Receive ACK within
waiting time for ACK
N
Y
NR = NR + 1
NR＞macMaxFrameRetries ?
N
Y
Success
Failure (drop the frame)
NB : number of back off
BE : backoff exponent
macMinBE : minimum BE
macMaxBE : maximum BE
macMaxCSMABackoffs : maximum NB
NR : number of retries
macMaxFrameRetries : maxmum NR

Figure 4.8-15 CSMA-CA algorithm

3.6.3.3.3.Backoff operation

Figure 4.8-16 shows the backoff operation of this specification. The operation is principally based on the description of the [802.15.4] 5.1.1.4 CSMA-CA algorithm except for that ECHONET Lite profile assumes optional capability of receiving frames in the backoff period. When a node receives a frame in the backoff period, the backoff process is suspended till the receiving is finished and then resumed. (See node 3 in **Figure 4.8-16**.) In Figure 4.8-16, 'backoff(first)' and 'backoff(second)' reveal backoffs activated when NB is 0 and NB is 1, respectively.



Node	Description of Operation
Node　1	Idle at CCA after backoff (first) -> Transmission
Node 2	Busy at CCA after backoff (first) -> Waiting for Idle (If possible, receive data) *1 -> Idle at CCA after backoff (second) -> Transmission
Node 3	Data reception during the backoff (first) -> Idle transition after receiving data -> Idle at CCA after remaining backoff (first) -> Transmission

In this figure the ACK frame is not shown.

*1: If busy at CCA, it is implementation dependent whether to receive the data, .

Figure 4.8-16 backoff operation

3.6.3.3.4.Transmission time management

(1) Pause duration management

Wait for the pause duration, based on [T108].

(2) Total emission time management

Have a function that limit the sum of emission time per arbitrary one hour to be 360 sec or less, based on [T108].

3.6.3.3.5.MAC Constant and variable

(1) MAC constant

Table 4.8-28 shows the MAC Constant of this specification. (Specify the nominal value of this specification, based on [802.15.4g] Table 51, Table 71)

Table 4.8-28 MAC constant

Constant	Description [unit]	Nominal Value *1	Remark
phyCCADuration	The duration for CCA [μsec]	130	128 or more
aTurnaroundTime	turnaround time between RX and TX [μsec]	1000	
RX to TX TurnaroundTime (=tack)	turnaround time from RX to TX [μsec]	300 or more, 1000 or less	

TX to RX TurnaroundTime	turnaround time from TX to RX [μsec]	less than 300	
macMinLIFSPeriod	minimum LIFS [μsec]	1000	Refer to 3.6.3.3.1
aUnitBackoffPeriod	unit period of backoff [μsec]	1130	Refer to 3.6.3.3.1
macAckWaitDuration*2	time to wait for ACK frame after completion of frame transmission. [ms]	5	See the description of macEnhAckWaitDuration in [802.15.4e]　Table 52. The EACK is regarded as received if the PHY header is received within macEnhAckWaitDuration.

*1: For the error range of each value, refer to [802.15.4], [802.15.4e], [802.15.4g].

*2: The macAckWaitDuration means macEnhAckWaitDuration in this table.

(2) MAC variable

Table 4.8-29 shows the MAC variable of this specification. (specify the default value of this specification, based on [802.15.4] Table 52)

Table 4.8-29 MAC variable

variable	Description	Range	Default	Remark
macMaxBE	maximum value of the backoff exponent	3-15 *1	8	
macMinBE	minimum value of the backoff exponent	0-macMaxBE	8	
macMaxCSMABackoffs	The maximum number of backoffs	0-5	4	
macMaxFrameRetries	The maximum number of retries	0-7	3	

*1: range is extended to increase the variation (however, default value is within the standard range)

3.6.4. Interface part

3.6.4.1. Overview

The interface of a single-hop home network for ECHONET Lite over IPv6 shall be compliant with Clause 3.5 unless otherwise specified in the following sub clauses.

3.6.4.2. Adaptation layer

See 3.5.3 in this document.

3.6.4.2.1.Fragmentation

See 3.5.3.1 in this document.

3.6.4.2.2.Header compression

See 3.5.3.2 in this document

3.6.4.2.3.Neighbor discovery

The coordinator and the host described in this clause shall not support 6LoWPAN ND in Clause 3.5.3.3 due to applying ND based on IPv6 specified in the next clause.

3.6.4.3. Network layer

See 3.5.4 in this document.

3.6.4.3.1.IP addressing

See 3.5.4.1 in this document.

3.6.4.3.2.Neighbor discovery

See 3.5.4.2 in this document.

3.6.4.3.3.Multicast

See 3.5.4.3 in this document.

3.6.4.4. Transport layer

See 3.5.5 in this document.

3.6.4.5. Application layer

See 3.5.6 in this document.

3.6.5. Security configuration

3.6.5.1. Overview

This clause describes a security mechanism for single-hop network.

Most of the security configuration is the same in the clause 3.5.7 except special descriptions in this clause.

3.6.5.2. Authentication

The coordinator shall be PANA Authentication Agent (PAA) and the host shall be PANA Client (PaC).

3.6.5.3. Key generation

3.6.5.3.1.MAC layer security (link key)

The USRK and the LK are generated by following functions.

USRK = KDF(EMSK, “Wi-SUN JP SH-HAN” | “\0” | optional data | length)

- optional data = NULL(0x00)
- length = 64

LK = KDF(USRK, “Wi-SUN JP SH-HAN” | “\0” | optional data | length)

- optional data = EAP ID_P | EAP ID_S | IEEE802.15.4 Key Index
- length = 16

3.6.6. Recommended network configurations

3.6.6.1. Construction of new network

Once turned on, a coordinator constructs a new network compliant to this profile. The network construction is conducted by successive steps of (1) data link layer configuration, (2) network layer configuration and (3) security configuration. Overview of the network construction procedure is shown in Figure 4.8-17.

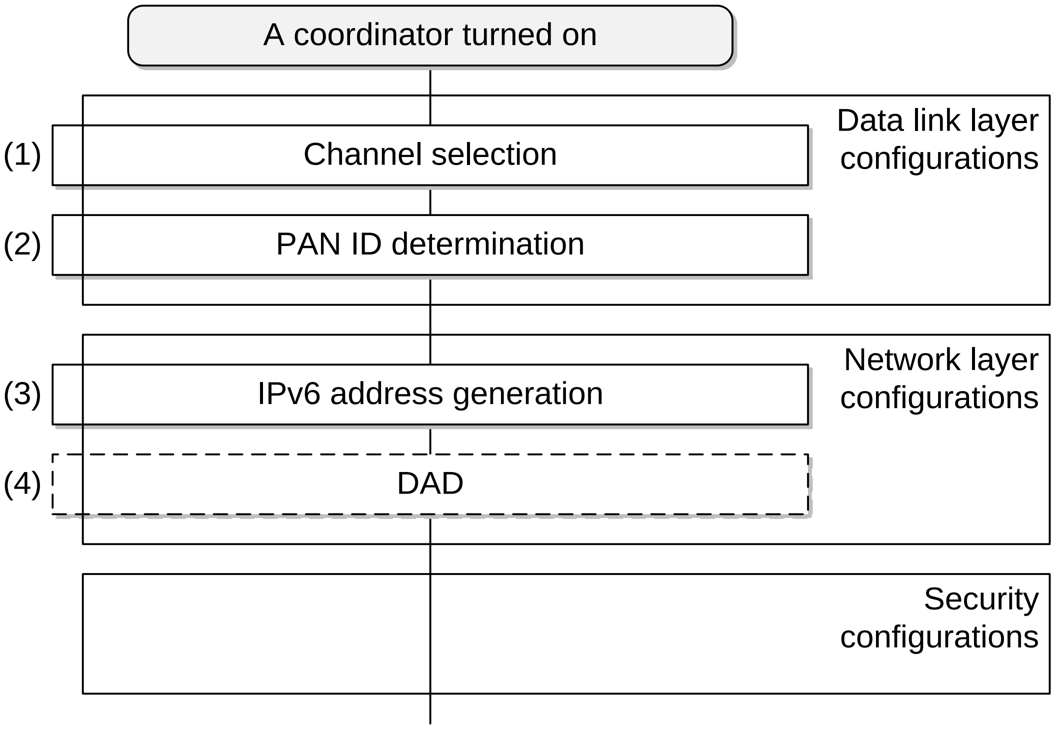


Figure 4.8-17 Overview of network construction procedures

3.6.6.1.1.Data link layer configurations

Once turned on, a coordinator constructs an IEEE 802.15.4 PAN. Detailed procedures for PAN construction is shown as follows.

The coordinator first selects a channel to use. The channel selection is conducted via ED scanning or active scanning, or both. In the selection, channel with less interference to the other systems are more preferable. (Step 1)

Next, the coordinator selects the PAN ID that is not occupied on the selected channel in Step 1, and defines it as the PAN ID for the local network. A special control for PAN ID confliction avoidance is not defined in this profile, since the current specifications can cope with the case by using the existing functions such as discarding by MAC address. Selection criteria of PAN ID out of candidate IDs is out of scope of this profile. (Step 2)

With conducting of the previous steps, PAN construction by the coordinator is completed.

3.6.6.1.2.Network layer configurations

After data link layer configurations are completed, the coordinator conducts initial configurations for network layer (IPv6).

First, the coordinator generates its own IPv6 address. The prefix is FE80::0/64, and interface ID is generated based on the coordinator's MAC address (EUI-64) according to definitions in [6LoWPAN] and [SLAAC]. (Step 3)

The coordinator may provide the global address or an unique local address to IEEE 802.15.4/4e/4g interface that defines IP address generated in Step 3, which is out of scope of this profile.

In general cases, DAD (Duplicate Address Detection) is conducted in this step in order to avoid IP address confliction to the other nodes in the network. However, nodes compliant to this profile always generate their own IPv6 addresses from EUI-64 addresses and there is basically no confliction of IP addresses. Therefore, DAD may be omitted. (Step 4)

3.6.6.1.3.Security configurations

The coordinator conducts security configurations following data link layer and network layer configurations.

3.6.6.2. Association to the network

Once turned on, a new host tries to association to the existing network compliant to this profile. Association procedure by the host includes (1) data link layer configuration, (2) network layer configuration and (3) security configuration just in a same manner as PAN construction by a coordinator. Overview of association procedures to the existing network by a host is shown in Figure 4.8-18.

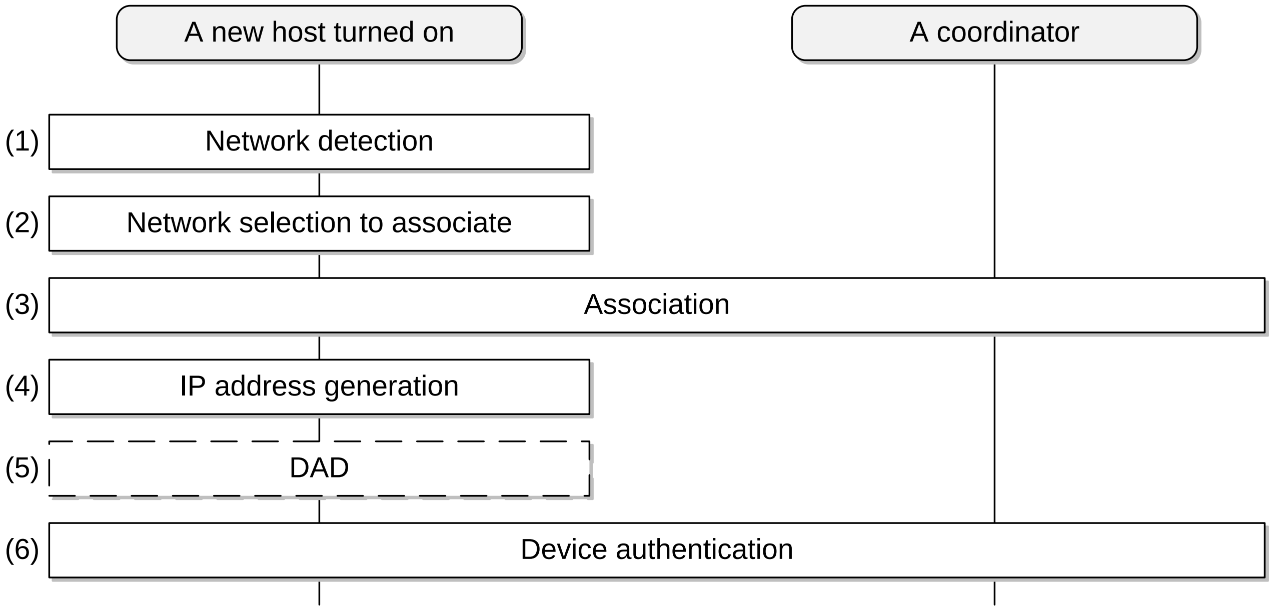


Figure 4.8-18 Overview of association to the network

3.6.6.2.1.Data link layer configurations

After turned on, a new host uses an enhanced active scan feature and sets MLME IE to its information Elements (IE) fields. As a response to the enhanced beacon request command from the host, the coordinator should send an enhanced beacon that set the same MLME IE to its information Elements fields; the host broadcasts an enhanced beacon request with some IEs command that is defined in [802.15.4e] on all available channels out of radio channels defined in [802.15.4] and [T108], a coordinator that receives the command returns an enhanced beacon with some IEs frame as a response, and the new host receives the enhanced beacon. Moreover, the new host recognizes a radio channel and a PAN ID employed by the coordinator, as results of those procedures. The content of MLME IE is out of scope of this profile. (Step 1)

In case only one PAN is detected, the host moves to the next step as for the PAN. In case several PANs are detected, the host needs to select one PAN in order to move to the next step. PAN selection criteria for the latter case is implementation matter and out of scope of this profile. (Step 2)

In case the host fails to associate to the PAN after those association procedures, the host is recommended to retry the procedures from Step 1 or Step 2, where the other network should be tried in Step 2.

At this point, the new host may conduct association procedures defined in [802.15.4]. However, such association procedures by data link layer can be omitted since the coordinator is recognized by upper layer. (Step 3)

3.6.6.2.2.Network layer configurations

After association to IEEE 802.15.4 PAN is completed, the new host generates its own IPv6 address. The prefix is FE80::0/64, and interface ID is generated based on the host’s MAC address (EUI-64) according to definitions in [6LoWPAN] and [SLAAC]. (Step 4)

In general cases, DAD (Duplicate Address Detection) is conducted in this step in order to avoid IP address confliction to the other nodes in the network. However, nodes compliant to this profile always generate their own IPv6 addresses from EUI-64 addresses and there is basically no confliction of IP addresses. Therefore, DAD may be omitted. (Step 5)

At this point, the host initiates the device authentication with the coordinator. This authentication procedure should be a mutual authentication process. (Step 6)

3.6.6.2.3.Security configurations

The new host conducts security configurations after data link layer and network layer configurations.

3.7. Recommended usage for single-hop smart meter-HEMS network

3.7.1. Overview

This clause clarifies the recommended usage in constructing single-hop smart meter-Home Energy Management System (HEMS) which controls home devices for energy efficiency and has an interface of [802.15.4][802.154g][802.15.4e]. HEMS network for ECHONET Lite over IPv6. Note that this profile does not exclude other usages.

Compliant nodes to this clause constructs single hop network with only a smart meter as a coordinator and a HEMS as a host without the other nodes on the same link.

3.7.2. PHY part

Required specifications in terms of IEEE 802.15.4/4e/4g standards in order to realize this usage is shown in **Table 4.8-30**.

Table 4.8-30 Device/PHY layer specifications in order to realize this usage

Item number *1	Support (Y:Yes, N:No, O:Option)	Item number *2	Support (Y:Yes, N:No, O:Option)	Item number *3	Support (Y:Yes, N:No, O:Option)	Item number *3	Recommend (Y:Yes, N:No, O:Option)
FD1	O.1	PLF1	Y	RF12	—	RF13.4	100 kbps *4
FD2	O.1	PLF2	Y	RF12.1	Y	RF13.5	N
FD3	Y	PLF3	Y	RF12.2	N	RF14	—
FD4	N	PLF4	Y	RF12.3	N	RF14.1	N
FD5	N	PLF4.1	Y	RF12.4	N	RF14.2	N
FD8	Y	PLF4.2	N	RF12.5 *5	N	RF14.3	Y

		PLF4.3	N	RF12.6	Y	RF14.4	N
		PLP1	PSDU size is up to 255 octets	RF13	—		

*1: Corresponding to the item number in Table 4.8-7 Functional device types

*2: Corresponding to the item number in **Table 4.8-2** PLF and PLP capabilities

*3: Corresponding to the item number in Table 4.8-3 RF capabilities

*4: Only 100kbps is mandatory for single-hop smart meter-HEMS network. 50kbps is optional.

*5: CSM is not supported if 50kbps is not supported.

The required specifications for the Additional PHY layer are shown in Table 4.8-31. This usage assumes compliance with the domestic regulation [T108] and compliant to the PHY specifications defined in [802.15.4g]. This specification uses GFSK modulation, 100 kbps data rate, 400 kHz occupied bandwidth (bundling 2 channels), and the 20 mW antenna power.   In order to mitigate the impact of the deployment environment, antenna diversity is recommended.

Table 4.8-31 Additional PHY layer specifications in order to realize this usage

Parameters	Recommend	Remarks
Modulation scheme	GFSK	
Data rate	100 kbps	
Transmission power	20 mW or less	
Frequency channel	Channels of No. 33 to 60 defined by ARIB with bundling of an odd and an even channel.	Channels of No. 33 to 38 are also utilized by systems employing 250 mW transmission power.
Occupied bandwidth	400 kHz (with 2 channel bundling),	

Receiver sensitivity	-88 dBm or less （PSDU length = 250 octets, data rate = 100 kbps, PER<10%, Power measured at antenna terminals, Interference not present ）	
Transmission preamble length	1200us - 4000us	
Preamble length assumed at receiver	1200us	
Antenna gain	3 dBi or less	
Antenna diversity	2 antenna selection diversity, recommended	

3.7.3. MAC part

3.7.3.1. MAC layer specifications

Required specifications in terms of IEEE 802.15.4/4e/4g standards are shown in Table 4.8-32. Non-beacon enabled configurations are selected by MAC layer when these specifications are deployed.

Table 4.8-32 MAC layer specifications in order to realize this usage

Item number *1	Support (Y:Yes, N:No, O:Option)	Item number *1	Support (Y:Yes, N:No, O:Option)	Item number *1	Support (Y:Yes, N:No, O:Option)	Item number *2	Support (Y:Yes, N:No, O:Option)
MLF1	Y	MLF7	Y	MLF15	N	MF1	Y
MLF1.1	N	MLF8	N	MLF16	N	MF2	Y
MLF2	Y	MLF9	Y	MLF17	N	MF3	Y
MLF2.1	N	MLF9.1	Y	MLF18	MLF10.2: Y *13	MF4	Y

MLF2.2	N	MLF9.2	Y	MLF18.1	MLF18:Y	MF4.1	N
MLF2.3	N	MLF9.2.1	Y	MLF18.1.1	MLF18:Y	MF4.2	N
MLF3	Y	MLF9.2.2	Y	MLF19	N	MF4.3	N
MLF3.1	FD1:Y FD2:N	MLF10.1	Y*5	MLF19.1	N	MF4.4	N
MLF3.2	Y	MLF10.2	FD1:O *12 FD2:M *11	MLF19.2	N	MF4.5	N
MLF4	Y	MLF10.3	N	MLF19.3	N	MF4.6	N
MLF5	N	MLF10.4	N	MLF19.4	N	MF4.7	Y*9
MLF5.1	N	MLF11	N	MLF19.5	N	MF4.8	N
MLF5.2	N	MLF12	N	MLF19.6	N	MF4.9	N
MLF6	Y	MLF13	N	MLF19.7	N	MF5	Y*10
		MLF15(4g)	N	MLF19.8	N		
				MLF20	N		
				MLF21	N		
				MLF23	N		
				MLF23.1	N		

*1：Corresponding to item number in Table 4.8-5 MAC sub-layer functions

*2：Corresponding to item number in Table 4.8-6 MAC frames

*9：May be employed by FD2 (not clarified in references).

*10：2 octet FCS is employed when PSDU size is no more than 255octets

*11 Active scanning is employed by FD1 for the channel selection and by FD2 for the network identification.

*12 FD1 must have capability to respond to the Active scanning performed by other devices.

*13 FD1 must have capability to respond to the EBR.

3.7.3.2. MAC frame format

See 3.6.3.2 in this document.

3.7.3.3. MAC functional description

See 3.6.3.3 in this document.

3.7.4. Interface part

3.7.4.1. Overview

The interface of a single-hop smart meter-HEMS network for ECHONET Lite over IPv6 shall be compliant with Clause 3.5 unless otherwise specified in the following sub clauses.

3.7.4.2. Adaptation layer

See 3.5.3 in this document.

3.7.4.2.1.Fragmentation

See 3.5.3.1 in this document.

3.7.4.2.2.Header compression

See 3.5.3.2 in this document

3.7.4.2.3.Neighbor discovery

The smart meter and the HEMS described in this clause shall not support 6LoWPAN ND in Clause 3.5.3.3 due to applying ND based on IPv6 specified in the next clause.

3.7.4.3. Network layer

The single-hop smart meter-HEMS network shall support IPv6 protocol [IPv6] in Table 4.8-33.

Table 4.8-33 Network Layer: IPv6

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option, I:Irrelevant)
IP1	Header Format	[IPv6] 3	Y
IP1.1	Extension Headers	-	I
IP1.2	Extension Header Order	[IPv6]4.1	I
IP1.3	Options	[IPv6] 4.2	I
IP1.4	Hop-by-Hop Options Header	[IPv6] 4.3	I
IP1.5	Routing Header	[IPv6]4.4	I
IP1.6	Fragment Header	[IPv6] 4.5	I
IP1.7	Destination Options Header	[IPv6] 4.6	I
IP1.8	No Next Header	[IPv6]4.7	I
IP1.9	AH Header	[AH]	I
IP1.10	ESP Header	[ESP]	I
IP2	Deprecation of Type 0 Routing Headers	[IPv6-RH]	I
IP3	Path MTU Discovery	[IPv6] 5	I
IP4	Flow Labels	[IPv6] 6	N
IP5	Traffic Classes	[IPv6] 7	N

The single-hop smart meter-HEMS network also shall support ICMPv6 protocol [ICMPv6] in Table 4.8-34.

Table 4.8-34 Network Layer: ICMPv6

Item number	Item description	Reference section in standard	Support (Y:Yes, N:No, O:Option, I:Irrelevant)
ICMP1	Message Format	[ICMP6] 2.1	Y
ICMP2	Message Source Address Determination	[ICMP6] 2.2	Y
ICMP3	Message Checksum Calculation	[ICMP6] 2.3	Y
ICMP4	Message Processing Rules	[ICMP6] 2.4	Y
ICMP5	Destination Unreachable Message	[ICMP6] 3.1	Y*1
ICMP6	Packet Too Big Message	[ICMP6] 3.2	I
ICMP7	Time Exceeded Message	[ICMP6] 3.3	I
ICMP8	Parameter Problem Message	[ICMP6] 3.4	Y
ICMP9	Echo Request Message	[ICMP6] 4.1	Y
ICMP10	Echo Reply Message	[ICMP6] 4.2	Y

*1: The port unreachable (code=4) is only applicable.

3.7.4.3.1.IP addressing

See 3.5.4.1 in this document.

3.7.4.3.2.Neighbor discovery

See 3.5.4.2 in this document except for the parts of Neighbor Solicitation Message and Neighbor Advertisement Message. In the single-hop smart meter-HEMS network, the transmission of Neighbor Solicitation Message is optional but the node shall respond by sending a Neighbor Advertisement Message to the received Neighbor Solicitation Message (see Table 4.8-35).

Table 4.8-35 Neighbor Solicitation and Neighbor Advertisement Messages

Item number	Item description	Support (Y:Yes, N:No, O:Option, I:Irrelevant)	Notes
ND4	Duplicate Address Detection	I	
ND8	Neighbor Solicitation (NS) Message	-	See ND8.1, ND8.2 and ND8.3
ND8.1	NS Transmission	O	Optional but at least one of the specifications described in ND8.1 and ND8.2 is required to be supported.
ND8.2	No NS Transmission	O	
ND8.3	NS Reception	Y	
ND9	Neighbor Advertisement (NA) Message	-	See ND9.1, ND9.2, ND9.3 and ND9.4
ND9.1	Solicited NA Transmission	Y	
ND9.2	Solicited NA Reception	ND8.1:Y ND8.2:N	
ND9.3	Unsolicited NA Transmission	N	
ND9.4	Unsolicited NA Reception	N	

3.7.4.3.3.Multicast

See 3.5.4.3 in this document.

3.7.4.4. Transport layer

See 3.5.5 in this document.

3.7.4.5. Application layer

See 3.5.6 in this document.

Application should not send packets larger than 1280 octets as a link MTU.

This means application maximum PDU size is below:

1280 - 'size of IPv6 header (incl. extension header)' - 'size of Transport layer header'

For example: In the case that an application uses UDP and does not use IPv6 extension headers, the application maximum PDU size is below:

1280 - 40(IPv6 header size) - 8(UDP header size) = 1232 octets.

3.7.5. Security configuration

3.7.5.1. Overview

This clause describes a security mechanism for single-hop smart meter-HEMS network.

Most of the security configuration is the same in the clause 3.5.7 except special descriptions in this clause.

3.7.5.2. Authentication

The smart meter shall be PAA and the HEMS shall be PaC.

3.7.5.3. Key generation

3.7.5.3.1.MAC layer security (link key)

The USRK and the LK are generated by following functions.

USRK = KDF(EMSK, “Wi-SUN JP Route B” | “\0” | optional data | length)

- optional data = NULL(0x00)
- length = 64

LK = KDF(USRK, “Wi-SUN JP Route B” | “\0” | optional data | length)

- optional data = EAP ID_P | EAP ID_S | IEEE802.15.4 Key Index
- length = 16

The smart meter and the HEMS shall have two or more KeyDescriptors to hold at least two keys at the same time. Both nodes shall use the latest key at the time of transmission.

3.7.6. Recommended network configurations

Both a smart meter and HEMS have “Pairing ID”, which length is 8 octets, and the ID is used to associate the smart meter with the HEMS. In this specification, suppose the ID is set to a smart meter and HEMS in advance. In addition, NAI and authentication key for PANA/EAP are also set to a smart meter and HEMS in advance.

A smart meter determines the radio channel and PAN ID that is used to construct the network, by following procedure.

1-1: Data link (MAC) layer configuration,

Radio channel selection and PAN ID detection are conducted via ED scanning or Enhanced Active scanning, or both. Selection criteria of radio channel and PAN ID is out of scope of this profile.

1-2: Network layer configuration,

A smart meter generates its own IPv6 link local address compliant to [SLAAC].

After the smart meter that is coordinator completes the network construction, HEMS attempt to connect to the smart meter, as the following configurations.

2-1: Data link (MAC) layer configuration,

HEMS identifies the smart meter network by using Enhanced Active scanning.

2-2: Network layer procedure,

HEMS generates its own IPv6 link local address compliant to [SLAAC].

HEMS should calculate the IPv6 link local address of the smart meter from the source address of Enhanced Beacon message. And HEMS requests a smart meter to authenticate by [PANA] using NAI and authentication key, which are pre-shared. The smart meter establishes PANA session with the HEMS, and the smart meter authenticates HEMS based on NAI and authentication key. When authentication succeeds, the smart meter and the HEMS share the MAC layer encryption key.

After sharing the MAC layer encryption key, the smart meter can communicate with the HEMS, by using encrypted messages. HEMS conducts service discovery procedure using ECHONET Lite protocol, and the smart meter can notify the HEMS of meter readings every 30 minutes.

3.7.6.1. Bootstrapping

Once a smart meter is turned on, it constructs a new network compliant to this profile. This procedure is same as sub clause 3.6.6.1. And, once HEMS is turned on, it attempts to connect to the network that is constructed by the smart meter. This procedure is same as sub-clause 3.6.6.2. Overview of network configuration and association procedure to the network is shown in Figure 4.8-19.

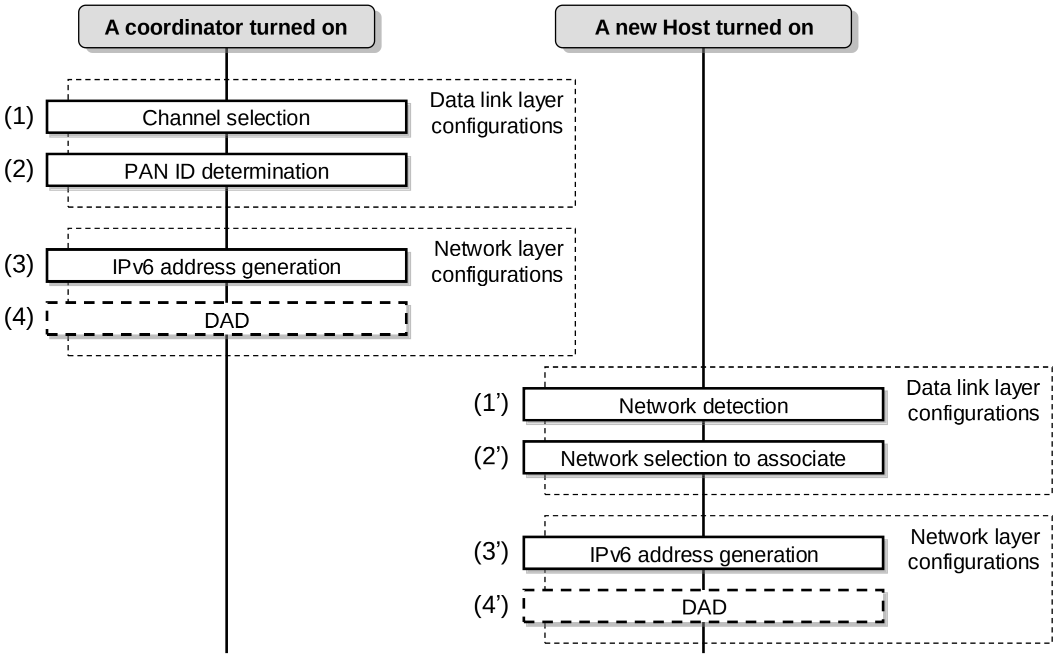


Figure 4.8-19：Overview of network construction procedure

3.7.6.1.1. Data link layer configuration

Data link layer configuration of a coordinator is same as sub clause 3.6.6.1.1, but smart meter must set no information to its Information Elements fields in Enhanced Beacon Request if Active scan is employed.

To detect the smart meter network, HEMS uses an Enhanced Active scan feature and set MLME IE to its Information Elements field which is terminated with a list termination IE (ID=0xf). As a response to the Enhanced Beacon Request command from the HEMS, the smart meter should send an Enhanced Beacon that set the same MLME IE to its Information Elements field which is terminated with a list termination IE (ID=0xf). Association procedure should be omitted. Other data link layer configuration of HEMS is same as sub-clause 3.6.6.2.1.

Configuration information is shown in Table 4.8-36.

Table 4.8-36 Sub-ID (MLME IE)

Sub-ID value	Content length	Name	Description

0x68	Variable	Unmanaged (Pairing ID)	This Sub-ID is used as the information to help HEMS detect the corresponding smart meter network. This Sub-ID is defined by this profile.

3.7.6.1.2.Network layer configuration

A smart meter use IPv6 link local address only. Other network layer configuration of a smart meter is the same as sub-clause 3.6.6.1.2.

HEMS use IPv6 link local address only, too. Other network layer configuration of HEMS is the same as sub-clause 3.6.6.2.2.

Authentication procedure refers to sub clause 3.7.6.3.

3.7.6.2. IP Address Detection

Before the authentication procedure by PANA, HEMS should calculate the IPv6 address of the smart meter. As a way to detect IPv6 address of the opposite device, HEMS uses the source MAC address field of an Enhanced Beacon message from the smart meter, and HEMS estimates IPv6 link local address of the opposite smart meter.

HEMS may be omitted Neighbor Discovery procedure defined in [ND].

3.7.6.3. Authentication and Key Exchange

The HEMS conducts security configurations after data link layer and network layer configurations. In other words, the HEMS acting as a PaC initiates a PANA session to the smart meter acting as the PAA.

3.7.6.4. Application

As stated in 3.7.4.5, use ECHONET Lite as an application protocol, and support using compound data format.

3.7.6.4.1.ECHONET Object

Smart meter and HEMS use the ECHONET object (EOJ) as described in Table 4.8-37.

Table 4.8-37 ECHONET Objects (EOJ)

	Class group code	Class code	Instance code
Smart meter	0x02	0x88	0x01
HEMS	0x05	0xFF	0x01

Note: An instance code is fixed as 0x01.

3.7.6.4.2.ECHONET Lite Service (ESV)

Smart meter and HEMS use The ECHONET Lite service code as described in Table 4.8-38.

Table 4.8-38 ECHONET Lite Service (ESV) Code

Service Code (ESV)	ECHONET Lite Service Content	Symbol
0x51	Property value write request “response not possible”	SetC_SNA
0x52	Property value read “response not possible”	Get_SNA
0x61	Property value write request (response required)	SetC
0x62	Property value read request	Get
0x71	Property value Property value write response	Set_Res
0x72	Property value read response	Get_Res
0x73	Property value notification	INF
0x74	Property value notification (response required)	INFC

0x7A	Property value notification response	INFC_Res

3.7.6.4.3.The ECHONET device object (EPC)

The ECHONET device object (EPC) for Smart meter is described in Table 4.8-39 and Table 4.8-40, and is used between the communication of Smart meter and HEMS.

Table 4.8-39 Definition of Device Object Super Class Properties

Property name	EPC	Contents of property	Access rule
Operation status	0x80	This property indicates the ON/OFF status.	Get
Installation location	0x81	This property indicates the installation location.	Set/Get
Standard version information	0x82	This property indicates the version number of the corresponding standard.	Get
Fault status	0x88	This property indicates whether a fault (e.g. a sensor trouble) has occurred or not.	Get
Manufacturer code	0x8A	Manufacturer code defined by the ECHONET Consortium.	Get
Production number	0x8D	It’s used for specifying a smart meter.	Get
Current time setting	0x97	Current time (HH:MM format)	Get
Current date setting	0x98	Current date (YYYY:MM:DD format)	Get
Status change announcement property map	0x9D		Get

Set property map	0x9E		Get
Get property map	0x9F		Get

Table 4.8-40 Definition of ECHONET Lite Device Object for Smart electric energy meter class

Property name	EPC	Contents of property	Access rule
Operation status	0x80	This property indicates the ON/OFF status.	Get
Composite transformation ratio	0xD3	This property indicates the composite transformation ratio using a 6-digit decimal notation number.	Get
Number of effective digits for cumulative amounts of electric energy	0xD7	This property indicates the number of effective digits for measured cumulative amounts of electric energy.	Get
Measured cumulative amount of electric energy (normal direction)	0xE0	This property indicates the measured cumulative amount of electric energy using an 8-digit decimal notation number.	Get
Unit for cumulative amounts of electric energy (normal and reverse directions)	0xE1	This property indicates the unit (multiplying factor) used for the measured cumulative amount of electric energy and the historical data of measured cumulative amounts of electric energy)	Get
Historical data of measured cumulative amounts of electric energy (normal direction)	0xE2	This property indicates the date of historical data and measured cumulative amounts of electric energy (maximum 8 digits) for normal direction, which consists of 48 data value	Get

		of half-hourly data for the preceding 24 hours.	
Measured cumulative amount of electric energy (reverse direction)	0xE3	This property indicates the measured cumulative amount of electric energy using an 8-digit decimal notation number.	Get
Historical data of measured cumulative amounts of electric energy (reverse direction)	0xE4	This property indicates the date of the historical data and measured cumulative amounts of electric energy (maximum 8 digits) for reverse direction, which consists of 48 data value of half-hourly data for the preceding 24 hours.	Get
Day for which the historical data of measured cumulative amounts of electric energy is to be retrieved	0xE5	This property indicates the day for which the historical data of measured cumulative amounts of electric energy (which consists of 48 pieces of half-hourly data for the preceding 24 hours) is to be retrieved.	Set/Get
Measured instantaneous electric energy	0xE7	This property indicates the measured effective instantaneous measured effective instantaneous electric energy in watts.	Get
Measured instantaneous currents	0xE8	This property indicates the measured effective instantaneous R and T phase currents in amperes.	Get
Cumulative amounts of electric energy measured at fix time (normal direction)	0xEA	This property indicates the most recent cumulative amount of electric energy (normal direction)	Get/INF/INFC

		measured at 30-minute intervals, and measured date of measurement, time of measurement, and cumulative electric energy (normal direction).	
Cumulative amount of electric energy measured at fix time (reverse direction)	0xEB	This property indicates the most recent cumulative amount of electric energy (reverse direction) measured at 30-minute intervals, and measured date of measurement, time of measurement, and cumulative electric energy (reverse direction).	Get/INF/INFC

3.7.6.4.4.The response for consecutive request

Smart meter and HEMS make both request and a response as a set of communication, and perform one response to one request. In case sending the request of Get command consecutively, you need to receive the Get response before requesting another Get request command.

In addition, these specifications are the regulations to one-to-one communications, so a consecutive demand means that the demand from the same equipment continues.

3.7.6.4.5.Handling multiple data

Such as in a case that there is　no change of the serial number accompanying exchange of a smart meter, etc., and when HEMS receives multiple time of the integral-power-consumption value (30-minute value) of the same measurement time, etc. from the same smart meter, the latter data shall be handled as correct data.

3.7.7. Usage of credential in Japanese market Route-B (supplemental)

In Japanese Route-B (smart meter-HEMS) network, a Route-B specific credential (Table 4.8-41) is defined and required to use it. For this purpose, this subsection defines how to use the credential in the communication protocols.

Table 4.8-41 Route-B credential

Name	Description
Route-B authentication ID	Unique ID used to pair up a specific smart meter and HEMS. Character string of 32 comprised of 0~9 and A~F ASCII characters (32 octets). In this profile, this is converted to the ID ([NAI] format) used by PANA (EAP-PSK) and the "Pairing ID" by the rule described later.
(Route B authentication) Password	Password linked to Route B authentication ID (character string of 12 comprised of 0~9, a~z, and A~Z ASCII characters). In this profile, this is used in generating PSK, which is utilized in [EAP-PSK], by the rule described later.

3.7.7.1. Conversion of Route-B authentication ID to EAP Identifiers

Based on the 32 digit, Route-B authentication ID, the following rules are used to generate EAP Identifiers (ID_S, ID_P) ([NAI]).

[NAI generation rules]

Smart meter side NAI (EAP ID_S): "SM" +"Route-B authentication ID" (34 octets)

HEMS meter side NAI (EAP ID_P): "HEMS" +"Route-B authentication ID" (36 octets)

Example:

When Route-B authentication ID is "0023456789ABCEDF0011223344556677",

Smart meter side NAI (EAP ID_S): "SM0023456789ABCEDF0011223344556677"

HEMS side NAI (EAP ID_P): "HEMS0023456789ABCEDF0011223344556677"

3.7.7.2. Conversion of Password to PSK

PSK used in EAP-PSK is generated using the following rules.

[PSK generation rules]

Based on the Password linked to Route-B authentication ID, the following PSK generation function (PSK_KDF) is used to generate the 16 octet PSK.

PSK = PSK_KDF (Password)

= LSBytes16 (SHA-256 (Capitalize (Password))

(lower order 16 octets of the output created by using SHA-256 in the hash function on the capitalized Password character string)

Example:

When the Password is "0123456789ab"

PSK = LSBytes16(SHA-256(“0123456789AB”))

= 0xf58d060cc71e7667b5b2a09e37f602a2

3.7.7.3. Conversion of Route-B authentication ID to Pairing ID

HEMS performs Enhanced Active Scan using IEs field to detect the home smart meter. MLME IE (Group ID=0x1) will be used for the Payload IEs field of the Enhanced Beacon Request sent by HEMS, and the lower order 8 octets (Pairing ID) of the Route-B authentication ID will be included in the IE Contents of Sub-ID=0x68(Unmanaged).When the Pairing ID stored in MLME IE of the Payload IEs matches the Pairing ID stored in the smart meter, the smart meter responds by returning the Enhanced Beacon. This Enhanced Beacon is unicast and also includes the same Pairing ID in the Payload IEs field. After confirmation that the smart meter has the same Pairing ID, HEMS will start PANA negotiation with this smart meter. (Figure 4.8-20)

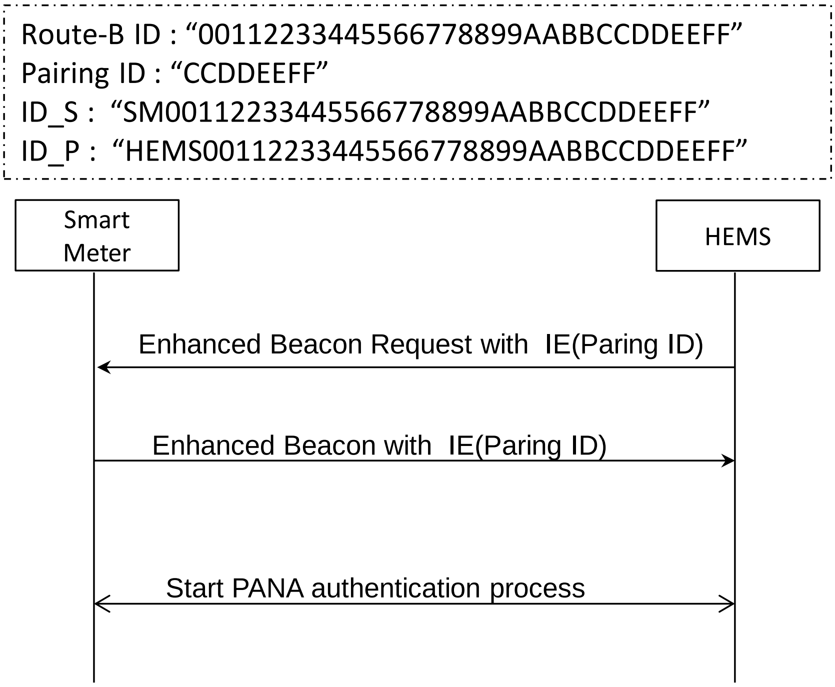

Route-B ID : "00112233445566778899AABBCCDDEEFF"
Pairing ID : "CCDDEEFF"
ID_S : "SM00112233445566778899AABBCCDDEEFF"
ID_P : "HEMS00112233445566778899AABBCCDDEEFF"
Smart Meter
HEMS
Enhanced Beacon Request with IE(Paring ID)
Enhanced Beacon with IE(Paring ID)
Start PANA authentication process

Figure 4.8-20 Smart meter discovery process

.

3.8. Recommended usage for single-hop home area network (HAN) among devices

3.8.1. Overview

This clause clarifies the recommended usage in constructing network for ECHONET Lite over IPv6 communication between a HEMS and multiple devices. Compliant nodes to this clause constructs a network with the HEMS as a central coordinator as shown in **Figure 4.8-21**.

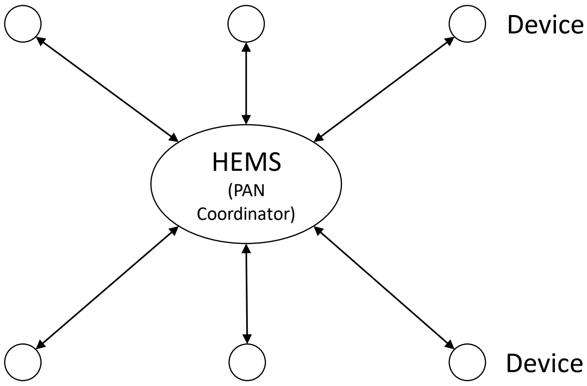


Figure 4.8-21 Home area network for multiple devices

3.8.2. PHY part

See 3.7.2 in this document.

3.8.3. MAC part

See 3.7.3 in this document if there is no additional description in this clause. An upper layer of the relay-unaware device defined in 3.8 should ignore a MAC frame which is security enabled and contains the IE List present field at the same time. Also it should ignore a MAC frame (MSDU) which hasSRA IE or SLR IE defiend in 3.9.3.2.4.

3.8.3.1. Capability Notification IE

Figure 4.8-22 shows the structure of Capability Notification IE. The Sub-ID of this IE is 0x67 (Unmanaged).

Capability Notification IE is a payload IE that is attached to Enhanced Beacon Request command frame or Enhanced Beacon frame to inform to corresponding node regarding what capabilities the sender has. Two flags below are defined to be used to inform what capabilities on HAN relay function the sender has.

- Sleeping-support (bit 5) – see 3.10.3.2.1
- Relay-endpoint (bit 6) – if this flag is set, it indicates that the sender can be a relay endpoint and that means that the sender is either a HEMS or HAN-end-device (defined in 3.9) within the HAN network which relaying function is supported. The detail is specified in 3.9.3.2.1.
- Relay-intermediate (bit 7) – if this flag is set, it indicates that the sender can be a relay device within the HAN network which relaying function is supported. The detail is specified in 3.9.3.2.1.

If the sender of this IE does not support any capabilities regarding HAN relay network, both of these flags must not be set. Also, if the sender needs to inform nothing, it can omit to attach this IE to the EBR or to the EB, disregarding of the presence of this IE in the corresponding EBR. PAN coordinator is also allowed to attach this IE to the EB even if this IE was not attached to the corresponding EBR.

Bits: 0-7	**8-14**	**15**	**Octets: Variable**
Length	Sub-ID (0x67)	Type (Short format)	IE content

Bits: 0-4	**5**	**6**	**7**
Reserved (0)	Sleeping-support	Relay-endpoint	Relay-intermediate
		HAN relay function	

Figure 4.8-22 Capability Notification IE

At the sending of this IE, the sender of Enhanced Beacon Request command must set all the possible functions to this IE. On the other hand, the sender of Enhanced Beacon must set proper and minimum set of necessary functions to this IE according to decision to be made by its self. More detailed procedure for this IE shall be presented in relevant part for each recommended usage in this document respectively.

At the reception of EB or EBR with the Capability Notification IE attached, the device must not discard the frame regardless of its capabilities of sending this IE and support of relay or sleeping functions.

3.8.4. Interface part

3.8.4.1. Overview

The interface of a single-hop home network among devices for ECHONET Lite over IPv6 shall be compliant with clause 3.7.4 unless otherwise specified in the following sub clauses.

3.8.4.2. Adaptation layer

See 3.5.3 in this document.

3.8.4.2.1.Fragmentation

See 3.5.3.1 in this document.

3.8.4.2.2.Header compression

See 3.5.3.2 in this document.

3.8.4.2.3.Neighbor discovery

HEMS and devices described in this clause shall not support 6LoWPAN ND in clause 3.5.3.3 due to applying ND based on IPv6 specified in the next clause.

3.8.4.3. Network layer

See 3.5.4 in this document.

3.8.4.3.1.IP addressing

See 3.5.4.1 in this document.

3.8.4.3.2.Neighbor discovery

See 3.5.4.2 in this document.

3.8.4.3.3.Multicast

See 3.5.4.3 in this document.

3.8.4.4. Transport layer

See 3.5.5 in this document.

3.8.4.5. Application layer

See 3.5.6 in this document.

3.8.5. Security configuration

3.8.5.1. Overview

This clause describes a security mechanism for single-hop home network among devices. Most of the security configuration is the same in the clause 3.5.7 except special descriptions in this clause.

3.8.5.2. Authentication

The HEMS shall be PAA and the devices shall be PaC.

3.8.5.2.1.PANA

PAA and PaC shall conform to 3.5.7.2.1 in this document except two modification described below:

- In addition to PaC-initiated session, PANA session can be initiated by PAA (PAA-initiated).
- PANA session lifetime shall be set to 0xFFFFFFFF (136 years: practically permanent).

In addition, PAA and PaC shall support following items:

- Unicast and multicast messages shall be protected by ciphered MAC frames with “HAN group key” shared by all the nodes authenticated in the network.
- PAA shall distribute HAN group key to PAC in the final phase of PANA authentication.
- HAN group key shall be distributed in a vendor-specific AVP which is newly defined in this document. The Vendor-ID in the vendor-specific AVP shall be 45605 (Wi-SUN Alliance).
- The vendor-specific AVP defined for HAN group key distribution shall be encrypted in Encryption-Encap AVP [PANA-ENC]
- The vendor-specific AVP used for HAN group key distribution shall contain HAN group key, MLE key, Key-ID, authentication counter, and outgoing frame counter of PAA.
- PANA session lifetime shall be set to 0xFFFFFFFF and it has no relation to HAN group key expiration.
- Therefore PANA session lifetime and HAN group key’s lifetime are not necessarily equal.
- PAA shall increment an authentication counter for a PaC each time PAA authenticates the PaC.
- PAA shall maintain an authentication counter for each PaC, and shall keep its value even if the PANA session with the PaC is terminated.
- HAN group key’s lifetime shall be maintained by PAA inside, and is not notified to PaC.
- When PAA updates a HAN group key, PAA shall distribute the new key to PaCs.

- PAA shall update the current HAN group key before the MAC frame counter overflow.
- Updated HAN group key is distributed to PaC with PANA protocol in a unicast manner.
- PaC can request PAA for the current HAN group key.
- MAC key generation function and MAC key defined in 3.7.5.3 are not used.
- It is recommended PAA supports at least 16 PaCs in the network. PAA shall maintain different ID and password for each PaC.

3.8.5.2.2.EAP

See 3.5.7.2.2 in this document.

3.8.5.3. Authentication and key distribution

Figure 4.8-23 shows PANA authentication and HAN group key distribution sequence.

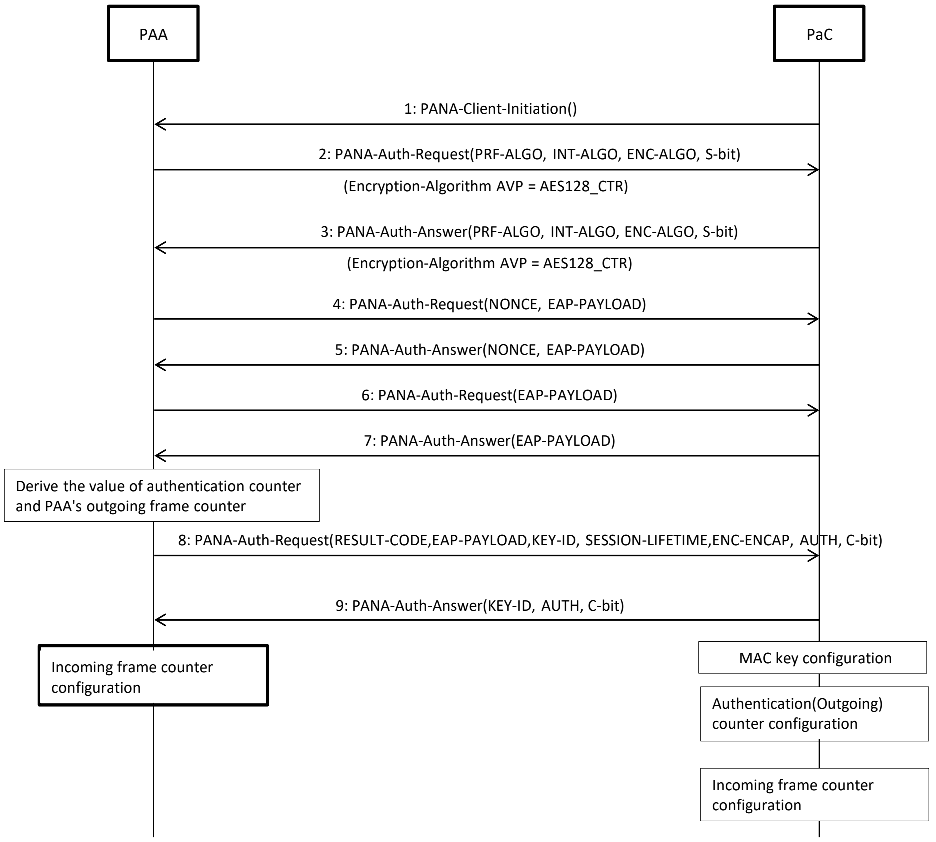

PAA
PaC
1: PANA-Client-Initiation()
2: PANA-Auth-Request(PRF-ALGO, INT-ALGO, ENC-ALGO, S-bit)
(Encryption-Algorithm AVP = AES128_CTR)
3: PANA-Auth-Answer(PRF-ALGO, INT-ALGO, ENC-ALGO, S-bit)
(Encryption-Algorithm AVP = AES128_CTR)
4: PANA-Auth-Request(NONCE, EAP-PAYLOAD)
5: PANA-Auth-Answer(NONCE, EAP-PAYLOAD)
6: PANA-Auth-Request(EAP-PAYLOAD)
7: PANA-Auth-Answer(EAP-PAYLOAD)
Derive the value of authentication counter and PAA's outgoing frame counter
8: PANA-Auth-Request(RESULT-CODE,EAP-PAYLOAD,KEY-ID, SESSION-LIFETIME,ENC-ENCAP, AUTH, C-bit)
9: PANA-Auth-Answer(KEY-ID, AUTH, C-bit)
Incoming frame counter configuration
MAC key configuration
Authentication(Outgoing) counter configuration
Incoming frame counter configuration

Figure 4.8-23 PANA authentication and HAN group key distribution

The default value for initial timeout of PCI (PCI_IRT) is 3 seconds in the single-hop home network among devices unlike original default value (1 second) defined in [PANA]. The default value of the initial retransmission interval for other messages (REQ_IRT) is 3 seconds as well.

3.8.5.3.1.Authentication request by PAA

PAA shall add Encryption-Algorithm AVP to Step2 PAR message in order to convey an encryption algorithm to be used to encrypt vendor-specific AVP contained in Step 8 PAR and subsequent messages. **Table 4.8-42** shows Step2 PAR message including an Encryption-Algorithm AVP.

Table 4.8-42 Authentication and key distribution Step2：Message of PAR(PRF-ALGO,INT-ALGO,ENC-ALGO,S=bit)

Field	Subfield	Size(octet)	Description (value etc.)
PANA Message Header	Reserved	2	
	Message Length	2	52
	Flags	2	‘R’bit=1、’S’bit=1
	Message Type	2	2=PANA-Auth-Request
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	PRF-Algorithm AVP	12	Contains PRF-Algorithm=5
	Integrity-Algorithm AVP	12	Contains Integrity-Algorithm=12
	Encryption-Algorithm AVP	12	Contains Encryption-Algorithm=1(AES128_CTR)

3.8.5.3.2. Authentication response by PaC

PaC shall add an Encryption-Algorithm AVP to Step3 PAN in order to convey an encryption algorithm to be used to encrypt vendor-specific AVP. **Table 4.8-43** shows Step2 PAN including an Encryption-Algorithm AVP.

Table 4.8-43 Authentication and key distribution Step3：Message of PAN(PRF-ALGO,INT-ALGO,ENC-ALGO,S-bit)

Field	Subfield	Size(octet)	Description
PANA Message Header	Reserved	2	
	Message Length	2	52
	Flags	2	’S’bit=1
	Message Type	2	2=PANA-Auth-Answer
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	PRF-Algorithm AVP	12	Contains PRF-Algorithm=5
	Integrity-Algorithm AVP	12	Contains Integrity-Algorithm=12
	Encryption-Algorithm AVP	12	Contains Encryption-Algorithm=1(AES128_CTR)

3.8.5.3.3. Distribution of HAN group key by PAA

When PAR with ‘C’ bit set is transmitted to PaC after successful authentication, HAN-Group-Key AVP (vendor-specific AVP) described below shall be added (Authentication / Key distribution: Step 8). HAN group key, MLE Key, Key-ID, authentication counter value (AuthCounter), and outgoing frame counter of PAA are included in HAN-Group-Key AVP. PAA increments an AuthCounter value by one with each authentication (See 3.8.5.4.5 for details). HAN-Group-Key AVP shall be encrypted using Encryption-Encap AVP.

See 3.8.5.4.6 for more information about HAN group key generation.

See 3.8.5.4.7 for more information about HAN-Group-Key AVP encryption.

See 3.8.5.4.3 for more information about HAN-Group-Key AVP.

After distribution of HAN group key, PAA sets the following information on its MAC layer:

Incoming frame counter of the PaC to which PAA sent the HAN group key
= AuthCounter || 00 00 00 (Note: ‘||’ indicates concatenation.)

Table 4.8-44 shows the detail of the PAR message with HAN-Group-Key AVP.

Table 4.8-44 Authentication / Key distribution (Step 8): Message of PAR (Result-Code, EAP-Payload, Key-ID, SESSION_LIFETIME, ENC-ENCAP [HAN-Group-Key AVP], AUTH and 'C' bit)

Field	Sub field	Size(octet)	Description
PANA Message Header	Reserved	2	
	Message Length	2	132
	Flags	2	'R'bit=1、'C'bit=1
	Message Type	2	2=PANA-Auth-Request
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	Result-Code AVP	12	contains Result-Code
	EAP-Payload AVP	12	contains EAP-Payload
	Key-Id AVP	12	contains EAP MSK Identifier
	Session-Lifetime AVP	12	contains PANA session lifetime
	Encryption-Encap AVP	60	HAN-Group-Key AVP is a vendor specific AVP which contains a HAN group key. This AVP is defined in this document. It is encrypted and encapsulated in Encryption-Encap AVP.
	HAN–Group-Key AVP	52	
	AUTH AVP	24	contains Message Authentication Code

3.8.5.3.4.Response to HAN group key reception by PaC

If a PaC receives a PAR message with HAN-Group-Key AVP (vendor-specific AVP) from PAA (Authentication / Key distribution: Step 8), the PaC replies a PAN (Key-ID, AUTH and 'C'bit) message (Authentication / Key distribution: Step 9). The PaC acquires HAN group key, Key-ID, AuthCounter and PAA's outgoing frame counter value and sets them on its MAC layer.

See 3.8.5.4.7 for more information about HAN-Group-Key AVP decryption.

Security information set in MAC layer is shown below.

MAC layer key (LK) = HAN group key

Key Index = Key-ID in HAN-Group-Key AVP

Outgoing frame counter = AuthCounter || 00 00 00 (Note: '||' indicates concatenation.)

Incoming frame counter for PAA = PAA's outgoing frame counter (Frame Counter Out)

If the PAA rejects the entry of a new device due to the restriction of its resources (e.g. upper limit number of macDeviceTable), the PAA returns PANA_AUTHORIZATION_REJECTED (2) to the device (PaC) in PANA authentication procedure.

3.8.5.4. Key update

There are two types of key update method: Push and Pull. Push type is PAA distributes the updated key to PaC and Pull type is PaC acquires the updated key from PAA. Push type is mandatory for both PAA and PaC. Pull type is mandatory for PAA and optional for PaC.

3.8.5.4.1.Distribution of updated HAN group key by PAA (Push)

The sequence of key update for Push type is shown below.

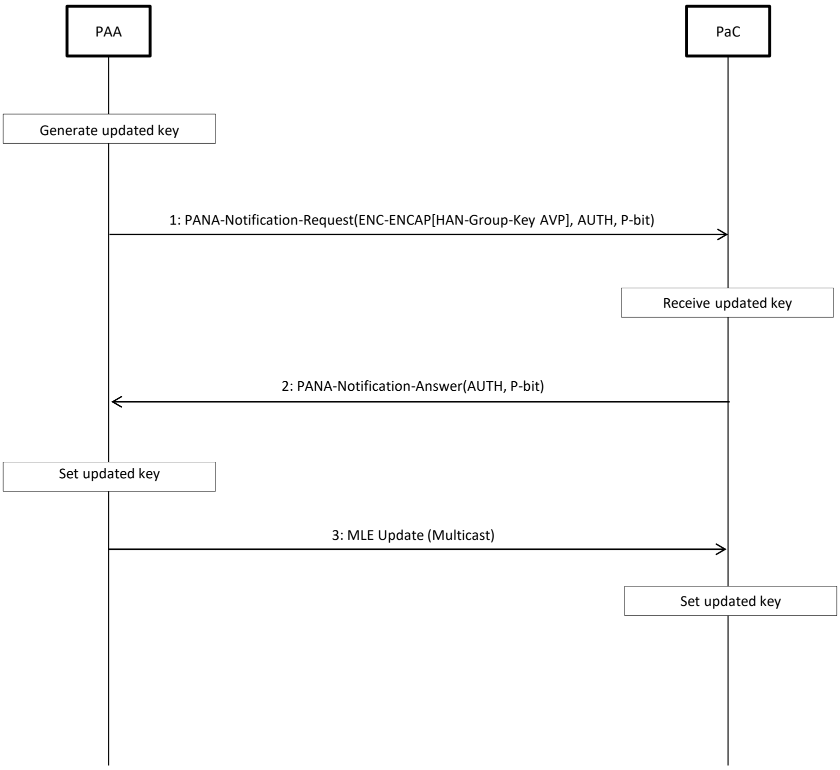

PAA
PaC
Generate updated key
1: PANA-Notification-Request(ENC-ENCAP[HAN-Group-Key AVP], AUTH, P-bit)
Receive updated key
2: PANA-Notification-Answer(AUTH, P-bit)
Set updated key
3: MLE Update (Multicast)
Set updated key

Figure 4.8-24 Key update sequence for Push type

If PAA updates a HAN group key, it adds HAN-Group-Key AVP (vendor-specific AVP) to PNR message and transmits it to each PaC by unicast manner (Push type key update: Step 1). HAN-Group-Key AVP contains HAN group key, MLE Key, Key-ID, AuthCounter, and outgoing frame counter value of PAA. HAN-Group-Key AVP shall be encrypted using Encryption-Encap AVP.

PAA shall reset the AuthCounter value to 0 in HAN-Group-Key AVP and reset Each PaC 's incoming frame counter to 0 as is the case in the HAN group key distribution. The AuthCounter will thus become 0 and the outgoing frame counter of PAA itself and the incoming frame counter of each PaC will become 0x00000000.

See 3.8.5.4.6 for more information about HAN group key generation.

See 3.8.5.4.7 for more information about HAN-Group-Key AVP encryption.

See 3.8.5.4.3 for more information about HAN-Group-Key AVP.

The detail of PNR message with vendor specific AVP is shown below.

Table 4.8-45 Key update Push (Step 1): Message of PNR (ENC-ENCAP [HAN-Group-Key] and AUTH) and P-bit

Field	Sub field	Size(octet)	Description
PANA Message Header	Reserved	2	
	Message Length	2	84
	Flags	2	‘R’bit=1、’P’bit=1
	Message Type	2	4=PANA-Notification-Request
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	Encryption-Encap AVP	60	HAN-Group-Key AVP is a vendor specific AVP containing HAN group key, which is defined in this document. It is encrypted and encapsulated in Encryption-Encap AVP.
	HAN-Group-Key AVP	52	
	AUTH AVP	24	contains Message Authentication Code

PAA initiates a new HAN group key distribution for each PaC with valid session. If PaC receives this PNR message from PAA, it activates the new MLE key and responses PNA message (Key update Push: Step 2).

When PAA finishes distribution of the new HAN group key to all PaCs with valid session, it transmits a multicast packet of encrypted MLE Update message using the new MLE-key to the link-scope all-nodes multicast address (FF02::1) (Key update Push: Step 3). Frame Counter field of auxiliary security header in this MLE message is set to zero. The cryptographic protection of MLE Update message is set to ENC-MIC-32 (Security level 5). The input values for cryptographic protection of MLE Update message are shown in **Table 4.8-46**. The MLE Update message carries Network Parameter TLV with Parameter ID=1 (PAN ID) shown in

Table 4.8-47. PaC should discard the MLE Update message if different PAN ID is contained in the MLE Update message. When PAA sends this MLE Update message or PaC receives it and succeeds in decrypting it, the key update procedure finishes. Both PAA and PaCs use an old HAN group key for sending and receiving frames until completing the key update. Once they complete the key update, they change the key for transmission and reception to the new HAN group key.

If PAA is unable to receive PNA message from PaC due to retransmission timeout, it terminates the session for that PaC.

PaC must wait at least 300 seconds in all for MLE Update message to be broadcasted by PAA after responding with PNA message once. If the MLE Update message cannot be received within the period, the PaC should query a current key by Pull method first. And if the PaC cannot receive a PNA (Pull response), the PaC must assume that the valid session for itself does no longer exist.

Table 4.8-46 CCM* inputs for MLE Update message

Value	How to generate the Value
a data	Source IP Address | Destination IP Address | Auxiliary Security Header
	Note) Use AUX Header in the MLE message as above ”Auxiliary Security Header”
m data	From the Command Type field to the end of TLV in the MLE message
CCM nonce	Source Address | Frame Counter | Security Level
	Note) "Source Address" is retrieved from MAC Header, "Frame Counter" is retrieved from Aux Header of the MLE message, and "SerucirtyLevel" is retrieved from the Security Control field of the MLE message Byte order must be big endian.
Key	Use latest MLE key which received from PAA

Table 4.8-47 The payload of MLE Update message

Field	Value	Length (bits)	Description
Initial byte	0	8	Initial byte of "0" indicates that the message is secured (encrypted and authenticated) as described in [802.15.4] and [802.15.4g].
Aux Header (6 octets)			
Security Control (1 octet)			
Security Level	0b101	3	Security Level = 5
Key Identifier Mode	0b01	2	Length of Key Identifier field is 1 octet.
Reserved	0b000	3	
Frame Counter (4 octets)			
Frame Counter	0	32	
Key Identifier (1 octet)			
Key Source	-	0	No Key Source is used.
Key Index	Key-ID	8	"Key-ID" shall be same value as it to be set in Key-ID field of HAN Group Key AVP sent with previous PNR message from PAA.
Command (10 octets)			
Command Type	0x05	8	Update command to inform of changes to link parameters shared by all nodes in a network.
TLV (9 octets)			
Type	0x07	8	"Network Parameter"
Length	0x07	8	Length of the Value field in octets.
Value (7 octet)			
Parameter ID	0x01	8	"PAN ID"
Delay	0x0	32	No delay shall be specified.
Value	Arbitrary	16	PAN ID participating currently.
MIC	Arbitrary	32	ENC-MIC-32

Note: All values in TLV are in network byte order (big endian).

PAA is allowed to perform PAA-Initiated PANA Authentication in any time and to try to re-establish a PANA session for a PaC with the session terminated due to key update failure. (Authentication / Key distribution: Step 2 is changed to "Unsolicited PANA-Auth-Request (PRF-ALGO, INT-ALGO, ENC-ALGO and S-bit)" and restarts from here.)

PaC has some possible recovery methods from the loss of key information in the lower layer and where key update procedure does not complete due to failure of receiving the PNR message from PAA. PaC can periodically send either PANA Ping message or Pull message below in detail to PAA if the session lifetime is valid, and also PaC can start key update procedure again from sending PCI message if the session lifetime expires.

3.8.5.4.2.Acquisition of HAN group key by PaC (Pull)

The sequence of key acquisition for Pull type is shown below.

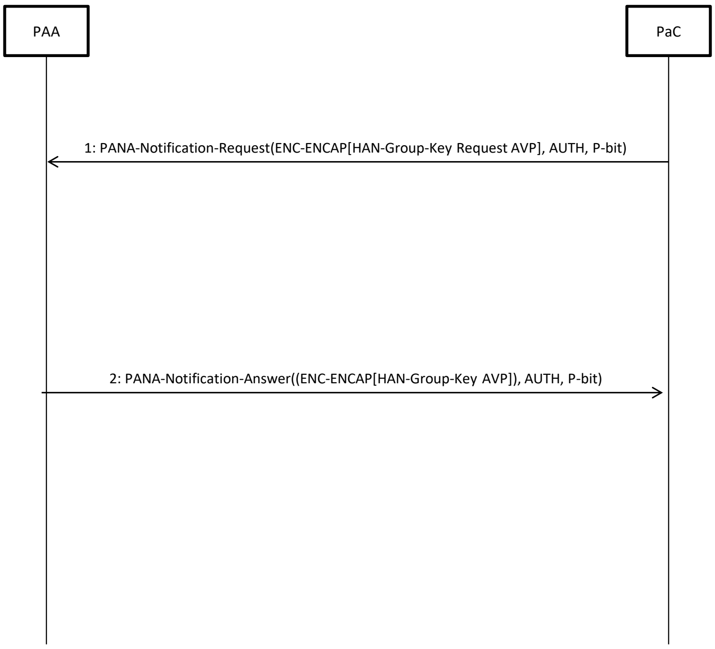

PAA
PaC
1: PANA-Notification-Request(ENC-ENCAP[HAN-Group-Key Request AVP], AUTH, P-bit)
2: PANA-Notification-Answer((ENC-ENCAP[HAN-Group-Key AVP]), AUTH, P-bit)

Figure 4.8-25 Key acquisition sequence for Pull type

PaC can request to acquire a HAN group key from PAA at any time within valid session (Pull).

HAN-Group-Key-Request AVP (vendor-specific AVP) is used to request a HAN group key. In this case, the AVP contains Key-ID of current HAN group key in the PaC. HAN-Group-Key-Request AVP shall be encrypted using Encryption-Encap AVP.

The detail of the PNR message with HAN-Group-Key-Request AVP is shown below.

Table 4.8-48 Key update Pull (Step 1): Message of PNR (ENC-ENCAP[HAN-Group-Key Request AVP],AUTH,P-bit)

Field	Sub field	Size(octet)	Description
PANA Message Header	Reserved	2	
	Message Length	2	64
	Flags	2	‘R’=1、’P’=1
	Message Type	2	4= PANA-Notification-Request
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	Encryption-Encap AVP	24	HAN-Group-Key Request AVP is a vendor specific AVP containing Key-ID, which is defined in this document. It is encrypted and encapsulated in Encryption-Encap AVP.
	HAN-Group-Key Request AVP	16	
	AUTH AVP	24	contains Message Authentication Code

If PAA receives a PNR message with HAN-Group-Key-Request AVP (vendor-specific AVP) from a PaC, it returns a PNA message with HAN-Group-Key AVP (vendor-specific AVP). The HAN-Group-Key AVP contains HAN group key, MLE Key, Key-ID, AuthCounter, and outgoing frame counter of PAA. The HAN-Group-Key AVP shall be encrypted using Encryption-Encap AVP. If the Key-ID in the HAN-Group-Key-Request AVP is equal to that of current HAN group key, the PNA message which PAA returns does not contain HAN-Group-Key AVP (PAA returns PNA message without vendor-specific AVP).

See 3.8.5.4.6 for more information about HAN group key generation.

See 3.8.5.4.7 for more information about HAN-Group-Key-Request AVP encryption.

See 3.8.5.4.3 for more information about HAN-Group-Key-Request AVP.

The detail of the PNA message with vendor-specific AVP is shown below.

Table 4.8-49 Key update Pull (Step 2): Message of PNA (((ENC-ENCAP[HAN-Group-Key]),AUTH, P-bit))

Field	Sub field	Size(octet)	Description
PANA Message Header	Reserved	2	
	Message Length	2	84
	Flags	2	’P’=1
	Message Type	2	4= PANA-Notification-Answer
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	Encryption-Encap AVP	60	HAN-Group-Key AVP is a vender-specific AVP containing HAN-Group-Key, which is added in this specification. It is encrypted and then encapsulated in Encryption-Encap AVP.
	HAN-Group-Key AVP	52	
	AUTH AVP	24	contains Message Authentication Code

If PaC receives this PNA message with HAN-Group-Key AVP from PAA, PaC sets security information on its MAC layer. See 3.8.5.5 for more information.

3.8.5.4.3.Vendor-specific AVP

The definition of the HAN-Group-Key AVP and the HAN-Group-Key-Request AVP are as follows.

- HAN-Group-Key AVP

Octets	Fields	Remark
2	AVP code	1
2	AVP flags	1, meaning V bit, indicates Vendor-ID field is present
2	AVP length	AVP value length is 40
2	Reserved	As a rule set to 0, but don’t care
4	Vendor-ID	45605
16	HAN Group Key	16 octets HAN Group Key
16	MLE Key	16 octets MLE Key
1	Key-ID	The Key-Index (one octet) of the Auxiliary security header in a MAC header. If the HAN group key is different from provided in last time, it's must set another Key-ID
1	Auth counter	One octet authorization counter
2	Reserved	As a rule set to 0, but don’t care
4	Frame counter out	Four octets frame counter. This is a PAA’s outgoing frame counter of the Auxiliary security header in a MAC header.

```
0                1               2                3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         AVP Code(1)        |      AVP Flags(V bit=1)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        AVP Length(40)      |      Reserved             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Vendor-Id (45605)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                    |
+                                                    +
|               HAN Group Key                          |
+                                                    +
|                                                    |
+                                                    +
|                                                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                    |
+                                                    +
|               MLE Key                               |
+                                                    +
|                                                    |
+                                                    +
|                                                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Key-ID    | Auth Counter  |   Reserved              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Frame Counter Out                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- ·HAN-Group-Key-Request AVP

Octets	Fields	Remark
2	AVP code	2
2	AVP flags	1, meaning V bit, indicates Vendor-ID field is present
2	AVP length	AVP value length is 1
2	Reserved	As a rule set to 0, but don’t care
4	Vendor-ID	45605
1	Key-ID	It is used as the Key-Index (one octet) of the Auxiliary security header in a MAC header

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          AVP Code(2)          |      AVP Flags(V bit=1)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         AVP Length(1)         |        Reserved               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Vendor-Id (45605)                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Key-ID    |        Padding                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

3.8.5.4.4.HAN group key Management

PAA should update HAN group key by Push before expiration, before outgoing frame counter overflows, or before incoming frame counter overflows. PAA manages both of maximum and minimum lifetimes for the HAN group key. The maximum lifetime shall have enough margin of the time for the frame counter overflow (one month, 30 days recommended). Also the minimum lifetime shall have enough margin in order to prevent frequent updating a key by the PaC continuously authentication (one hour recommended).

PAA can update the HAN group key after minimum lifetime of key update interval and shall update the HAN group key if there is a PaC of which authentication counter reached 255. PAA will update the HAN group key and reset the authentication counters of all PaCs to 0. In other cases, PAA checks authentication counter of a PaC whenever it is (re)authenticated and update the HAN group key if the authentication counter reached 255 as well.

In the minimum lifetime of key update interval, If PAA receives authentication request from a PaC of which authentication counter　reached 255, PAA shall refuse the request with Result-Code＝PANA_AUTHORIZATION_REJECTED(2) to the PaC and shall not update key in the period of minimum lifetime.

This lifetime for the HAN group key shall start to be counted down at immediate after the PANA session against very first PaC has established successfully or the key update and distribution has been completed.

3.8.5.4.5.Authentication counter (AuthCounter) management

PAA manages the value of the authentication counter (AuthCounter) which indicates the number of PaC's authentication times.

AuthCounter is one byte value, and effective range is 0 to 255. PAA increments its value when PAA authenticates a PaC in either 'Authentication and Authorization' phase or 'Re-Authentication' phase. PAA will notify AuthCounter value 0 of the PaC at successful authentication in the first time.

PAA manages AuthCounter value in each PaC. The range is 0 to 255. Even if PAA terminates the session of the PaC, AuthCounter value of the PaC is kept until updating HAN group key. PAA can identify the individual PaC with its IPv6 address.

3.8.5.4.6.HAN group key generation

The length of the HAN group key is 128 bits and the key is generated with a pseudo random function by PAA (HEMS) at start-up or key-update. PAA (HEMS) sets this HAN group key to its MAC layer as a common security key for unicast and multicast. And a 128-bit MLE key is also generated with a pseudo random function by PAA in the same manner. This MLE key is used for encrypting MLE Update message in the Push type key-update.

3.8.5.4.7.Encryption/decryption key generation for vendor-specific AVP

The HAN-Group-Key AVP and the HAN-Group-Key-Request AVP are vendor-specific AVPs .They are transmitted after encrypted in the Encryption-Encap AVP [PANA-ENC]. Encryption/decryption algorithm of Encryption-Encap is derived from PANA_PAA_ENCR_KEY/PANA_PAC_ENCR_KEY according to the [PANA-ENC]. The prf+ uses the PRF_HMAC_SHA 2_256 algorithm in the pseudorandom-number function.

3.8.5.4.8.Network reconfiguration notification

The HEMS (PAA) uses a PTR message to notify network reconfiguration to the device (PaC). PAA transmits PTR messages to all of PaC which has an effective session. Each PaC which received a PTR, replies a PTA to the PAA. After receiving PTA messages from all of PaC which has an effective session, the PAA immediately starts network reconfiguration. The PAA can transit to network reconfiguration even if there is any no-responded PaC (the session of no-responded PaC will be terminated).

PAA does not need to respond to the Enhanced Active Scan during waiting PTA responses from PaCs or incomplete network reconfiguration.

Each device starts to do Enhanced Active Scan after sending PTA and tries to reconnect / re-authenticate to the HEMS.

3.8.5.5. Encryption and Integrity check

The MAC data frame shall be ciphered based on [802.15.4] using the latest HAN group key distributed by PAA. In order to realize both of confidentiality and integrity, ENC-MIC-32 (Security level 5) is used. The node shall discard a frame with invalid MIC.

Key identifier mode is 0x01. Key Source in the key identifier field is not used and one-octet Key Index is used.

Exception of MAC security

All PANA messages (UDP destination port 716), MLE message (UDP port 19788) and IPv6 Neighbor Solicitation (NS) (ICMPv6 Type 135 Code 0)/Neighbor Advertisement (NA) (ICMPv6 Type 136 code 0) messages shall not be applied MAC layer security (do not add MAC auxiliary security header).

3.8.5.6. Replay protection

See 3.5.7.5 in this document.

3.8.6. Recommended network configurations

The HEMS and devices share a “Pairing ID” with 8-octet length, and this ID is used in the network discovery. There are two network discovery procedures defined in this document. They are “Initial setup mode” and “Normal operation mode”. The “Initial setup mode” is a special mode for devices joining the network in the first time. Once the devices learns their network (HEMS' MAC address as the Pairing ID in the Normal operation mode), the HEMS and devices move to "Normal operation mode". The "Normal operation mode" is used in the regular operation. In addition, NAI and pre-shared key for PANA/EAP are also set to each node in advance.

The HEMS sets the radio channel and PAN ID in accordance with following procedure.

1-1: Data link (MAC) layer configuration,

Radio channel selection and PAN ID selection are conducted via ED scan and Enhanced Active Scan. The criteria of the radio channel selection and PAN ID selection is out of scope in this document.

1-2: Network layer configuration,

The HEMS generates its own IPv6 link local address compliant to [SLAAC].

After the HEMS as a coordinator completes the network construction, the devices attempt to connect to the HEMS in accordance with the following configurations.

2-1: Data link (MAC) layer configuration,

The device identifies the HEMS network by Enhanced Active Scan.

2-2: Network layer procedure,

The device generates its own IPv6 link local address compliant to [SLAAC].

3.8.6.1. Bootstrapping

Once the HEMS is turned on, it constructs a new network compliant to this document. This procedure is same as sub clause 3.6.6.1. And, once the device is turned on, it attempts to connect to the network that is constructed by the HEMS. This procedure is same as sub clause 3.6.6.2. Overview of network configuration and association procedure to the network is shown in **Figure 4.8-26**.

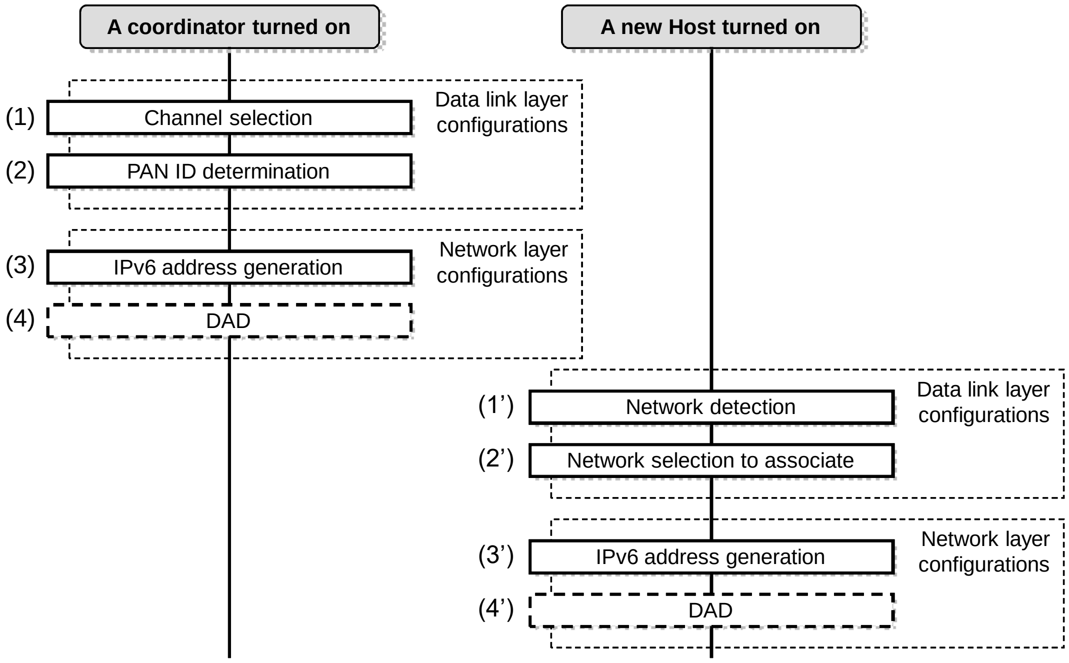


Figure 4.8-26 Overview of network construction procedure

3.8.6.1.1.Data link layer configuration

Data link layer configuration of a coordinator is same as sub clause 3.6.6.1.1, but coordinator must set no information to its Information Elements fields in Enhanced Beacon Request if Active scan is employed.

In order to detect the HEMS network, the device uses an Enhanced Active Scan and sets MLME IE to its Information Elements field which is terminated with a list termination IE (ID=0xf). As a response to the Enhanced Beacon Request command from the device, the HEMS should send an Enhanced Beacon that sets the same MLME IE to its Information Elements field which is terminated with a list termination IE (ID=0xf). Association procedure should be omitted. Other data link layer configuration of the device is same as sub-clause 3.6.6.2.1.

Configuration information is shown in **Table 4.8-50**

Table 4.8-50 Sub-ID (MLME IE)

Sub-ID value	Content length	Name	Description
0x68	Variable	Unmanaged (Pairing ID)	This Sub-ID is used as the information to help the device detects the corresponding HEMS network. This Sub-ID is defined by this profile.

"ScanDuration" value for Enhanced Active Scan, that is specified in [802.15.4], is recommended to set to 5 in order to establish the network connection in a short time.

3.8.6.1.2.Network layer configuration

The HEMS uses IPv6 link local address only. Other network layer configuration of the HEMS is the same as sub clause 3.6.6.1.2.

The device also uses IPv6 link local address only. Other network layer configuration of the device is the same as sub clause 3.6.6.2.2.

Authentication procedure refers to sub clause 3.7.6.3.

3.8.6.2. IP Address Detection

Before starting the PANA authentication procedure, the device figure out the HEMS' IPv6 link local address from the source MAC address in the Enhanced Beacon message responded by the HEMS.

The device may omit Neighbor Discovery procedure defined in [ND].

3.8.6.3. Authentication and Key Exchange

The device performs security setup after its data link layer and network layer configurations. In other words, the device acts as a PaC and initiates a PANA session to the HEMS (PAA)..

3.8.6.4. Application

As stated in 3.8.4.5, use ECHONET Lite as an application protocol, and support using compound data format.

3.8.7. Usage of credential

In HAN network, a HAN specific credential (**Table 4.8-51**) is defined and required to use it. For this purpose, this subsection defines how to use the credential in the communication protocols.

Table 4.8-51 HAN Credential

Name	Description
HAN authentication ID	Unique ID used to pair up a specific HAN device and HEMS. Character string of 24 comprised of 0~9 and A~F ASCII characters (24 octets). The first character string of eight characters is “01000000” and the following string of 16 characters (16 octets) is described in hexadecimal notation of MAC address of the HAN device (end-device or HEMS). In this profile, this is converted to the ID ([NAI] format) used by PANA (EAP-PSK) by the rule described later.
(HAN authentication) Password	Password linked to the HAN authentication ID (character string of 16 comprised of 0~9, a~z, and A~Z ASCII characters). In this profile, this is used in generating PSK, which is utilized in [EAP-PSK], by the rule described later.

3.8.7.1. Conversion of HAN authentication ID to EAP Identifiers

Based on the 24 digit HAN authentication ID, the following rules are used to generate the EAP Identifiers (ID_S, ID_P) ([NAI]).

[NAI generation rules]

HEMS side NAI (EAP ID_S): ”CTRL” + ”HAN authentication ID of HEMS” (24 octets)

HAN device side NAI (EAP ID_P): ”NODE” + ”HAN authentication ID of HAN device” (24 octets)

Example:

When HEMS HAN authentication ID is "0100000011112222333334444"

and HAN device HAN authentication ID is “0100000055556666777788888”

HEMS side NAI (EAP ID_S): "CTRL0100000011112222333334444"

HAN device side NAI (EAP ID_P): "NODE0100000055556666777788888"

The MAC address in the HEMS is supposed to be “1111222233334444”

The MAC address in the HAN device is supposed to be “5555666677778888”

3.8.7.2. Conversion of Password to PSK

PSK used in the EAP-PSK negotiation is generated using the following rules.

[PSK generation rules]

Based on the Password linked to the HAN authentication ID, the following PSK generation function (PSK_KDF) is used to generate the 16 octet PSK.

PSK = PSK_KDF(Password)

= LSBytes16(SHA-256(Capitalize(Password))

(lower order 16 octets of the output created by using SHA-256 in the hash function on the capitalized Password character string)

Example:

When the Password is ”0123456789abcdef”

PSK = LSBytes16(SHA-256(“0123456789ABCDEF”))

= 0x91d828cb942c2df1eeb02502eccae9e9

3.8.8. Discovery and selection of the HEMS network

The HAN device performs Enhanced Active Scan with IEs field in order to detect a HEMS. MLME IE (Group ID=0x1) will be used for the Payload IEs field of the Enhanced Beacon Request sent by the HAN device, and the eight octets Pairing ID defined in both Initial setup mode and Normal operation mode will be included in the IE Contents of Sub-ID=0x68(Unmanaged). When the Pairing ID stored in MLME IE of the Payload IEs matches the Pairing ID stored in the HEMS, the HEMS responds by returning the Enhanced Beacon. This Enhanced Beacon is unicast and includes the same Pairing ID in the Payload IEs field of the Enhanced Beacon Request. After confirmation that the HEMS has the same Pairing ID, the HAN device will start PANA negotiation with this HEMS. (**Figure 4.8-27**)

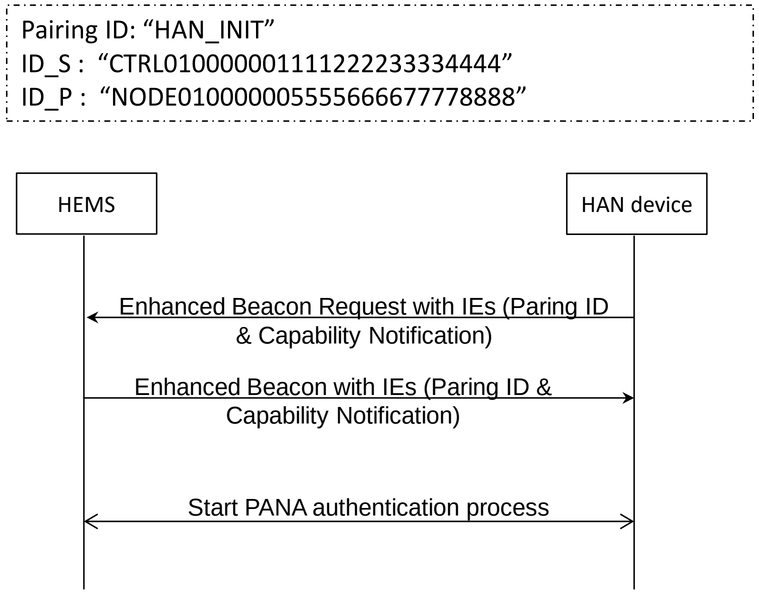

Pairing ID: “HAN_INIT”
ID_S : “CTRL0100000001111222233334444”
ID_P : “NODE0100000005555666677778888”
HEMS
HAN device
Enhanced Beacon Request with IEs (Paring ID & Capability Notification)
Enhanced Beacon with IEs (Paring ID & Capability Notification)
Start PANA authentication process

Figure 4.8-27 HEMS discovery procedure (Initial setup mode)

< Initial setup mode (**Figure 4.8-27**) >

The HEMS enters the Initial setup mode before a new HAN device trying to connect to the HEMS. The HAN device uses an Enhanced Active Scan and detects the target HEMS. The Initial setup mode has a valid period and the recommended value is five minutes. During this mode, the Pairing ID shall be “HAN_INIT”. The HAN device starts PANA authentication procedure with the corresponding HEMS after Enhanced Active Scan with this Pairing ID. After the expiration of the valid period, the HEMS disables the Pairing ID “HAN_INIT” for the Initial setup mode and turn into the Normal operation mode. After successful PANA authentication in the Initial setup mode, the HAN device sets the HEMS' MAC address as the Pairing ID in the Normal operation mode. If PANA authentication failed, the HAN device tries to find the corresponding HEMS until PANA authentication succeeds. The HAN device can use an Enhanced Active Scan again to the all radio channels if it finds no HEMS on all channels or authentication fails.

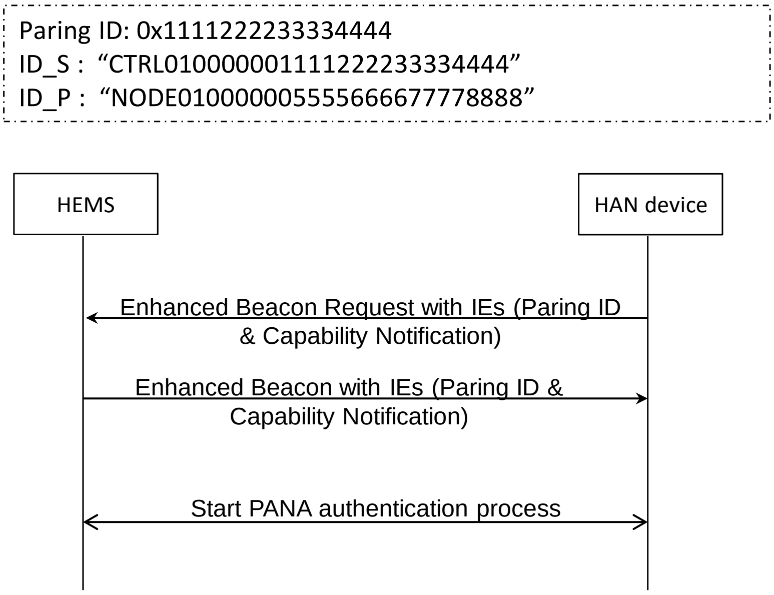

Paring ID: 0x1111222233334444
ID_S : "CTRL01000000111122223333444"
ID_P : "NODE01000000555566667777888"
HEMS
HAN device
Enhanced Beacon Request with IEs (Paring ID & Capability Notification)
Enhanced Beacon with IEs (Paring ID & Capability Notification)
Start PANA authentication process

Figure 4.8-28 HEMS discovery procedure (normal mode)

< Normal operation mode (**Figure 4.8-28**) >

The HEMS' MAC address is used as the Pairing ID in the Normal operation mode.

When the HAN device detects that the session is being expired, the HAN device may proceed Enhanced Active Scan to discover HEMS. In this case, it is not desired that the HAN device continues frequent Enhanced Active Scan for a long time from radio traffic perspective. When the HAN device continues the Enhanced Active Scan for more than 5 minutes, after that, the HAN device is recommended to set at least 3 minutes interval between each Enhanced Active Scan.

Once the HAN device connects to a HEMS, the HAN device should calculate the IPv6 link local address of the HEMS from the source MAC address of Enhanced Beacon message. And the HAN device starts a PANA authentication with its NAI and PSK which are pre-shared. The HEMS authenticates the HAN device(s) based on the NAI and PSK. The

HEMS distributes a HAN group key for which the HEMS and the HAN device share the MAC layer encryption key after successful authentication.

After sharing the MAC layer encryption key, the communication between the HEMS and the HAN device(s) is encrypted by the HAN group key. The HEMS conducts a service discovery procedure and sends some commands to the HAN device using ECHONET Lite protocol, and the HAN device(s) can run some operations based on the requests and respond their execution results to the HEMS.

3.9. Recommended usage for multi-hop home area network employing relay device

3.9.1. Overview

This clause clarifies the recommended usage in the case the relaying is employed by the multiple devices that are shown in 3.8. **Figure 4.8-29** shows a typical example assumed network topologies.

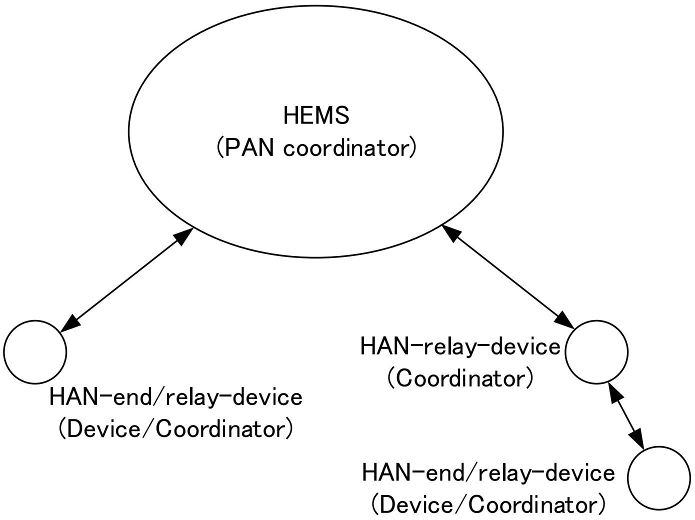


Figure 4.8-29 Network topology for HAN employing relay among devices

Since this clause shows only the required amendment from the previously clarified specifications, it is recommended that authors should refer the existing 3.8 for the other specifications as necessary.

3.9.1.1. Installation order of HAN-relay-device and HAN-end-device

In the situation of **Figure 4.8-30** device A is as HEMS, device B with relaying capability is named HAN-relay-device and device C without relaying capability is named as HAN-end-device. In the network topology assuming relaying as shown in **Figure 4.8-30**, B is assumed to be installed before C. Details is described in 3.9.3.3.

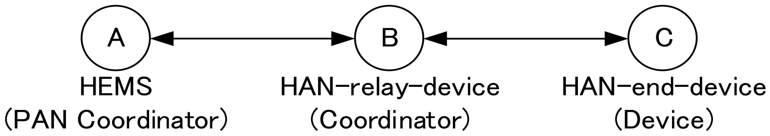


Figure 4.8-30 Installation order of HAN-relay-device and HAN-end-device

3.9.2. PHY part

Since there is no new amendment, the HEMS and the devices shall follow 3.8.2.

3.9.3. MAC part

This clause shows amendments for HAN employing relay in MAC layer. The other specifications should be referred in 3.8.3.

3.9.3.1. MAC sub-layer function

Table 4.8-52 shows amendments in MAC sub-layer functions.

Table 4.8-52 Amendments in MAC sub-layer functions

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)	Support (Y:Yes, N:No, O:Option)
MLF24	Relay support in HAN			O
MLF24.1	MHR management for forwarding			MLF24:Y
MLF24.2	Frame counter management			MLF24:Y
MLF24.3	Multicast transmission			MLF24:Y
MLF24.4	IEs for relay in HAN			MLF24:Y

3.9.3.1.1.MHR management for forwarding

The device supporting this function shall conduct relaying of the MAC payload by the MAC layer management entity by updating Source/Destination addresses in the MAC header according to the IE as described later.

3.9.3.1.2.Frame counter management

The device supporting this function shall realize the frame counter information exchange between HAN-end-device and the HAN-relay-device that is on the next hop towards the PAN coordinator after the HAN-end-device is authorized via PANA.

3.9.3.2. MAC frame format

This clause shows the amendments in MAC frame format.

This profile employs the [802.15.10] Short Route Announcement (SRA) IE and the Short L2R Routing (SLR) IE to support HAN relay.

3.9.3.2.1.Capability Notification IE (CN IE)

‘Relay-endpoint’ flag and ‘HAN-relay-device’ flag in CN IE are used to exchange capability of relay enabled HAN. At the sending of this IE, the sender of Enhanced Beacon Request command must set flags for all the available functions to this IE as request. On the other hand, the sender of Enhanced Beacon must set flags for the functions to use in response to the CN IE in the EBR. The following shows an example to handle relay and sleep function capabilities change.

i) If the sender of EB is HEMS or HAN-end-device which supports the relay function, Relay-endpoint (bit 6) in the sending EB shall be set to "1". Otherwise, it must be set to "0".

ii) If a HAN-relay-device received EBR but it has CN IE which sets all flags to "0", or no CN IE attached, the HAN-relay-device must not respond with EB to the requesting device.

3.9.3.2.2.DATA frame

Differently from the definition in 3.8.3., Payload IE deployments of SLR IE as described later are assumed. The Payload IEs shall be included in the portion of the data frame to be encrypted together with the data payload.

3.9.3.2.3.Enhanced beacon frame

Similarly to the definition in 3.8.3., Payload IE deployment of SRA IE is assumed.

3.9.3.2.4.IEs for relay in HAN

The SRA IE and theSLR IE are depicted in Figure 4.8-31 and

Bits: 0-10	11-14	15	Octets: Variable
Length	Group ID (MLME IE)	Type = 1 (Payload)	Sub IE

Bits: 0-7	8-14	15	Octets: Variable
Length	Sub ID	Type = 0 (Short)	IE Content

Octets:2/8	2/8	1	0/1	0/Variable
Source Address	Destination Address	L2R Sequence Number	Number of Intermediate Address	Intermediate Address List

Octets: 0/2/8	…	Octets: 0/2/8
Intermediate hop 1	…	Intermediate hop N

Figure 4.8-32 respectively.

The MLME IEs to be defined in this clause shall be nested within single MLME IE together with the other MLME IEs to be conveyed with same frame if existing.

The contents of these IEs should be aligned to little endian byte order.

The SRA IE (Sub-ID=0x3A)　is included in the Enhanced beacon frame that is transmitted by Coordinators except for PAN coordinators, in order to indicate the addresses of HAN-relay-device(s) as well as the PAN coordinator. Details of its fields are shown below.

(1) Vendor Specific Usage field

This field indicates if the following field represents the Sequence Number of the SRA IE (0) or if it is vendor specific. This field is set to 1 to specify the use of the following field according to the HAN relay requirements.

(2) SN or Vendor Specific field

Since the Vendor Specific Usage field is set to 1, this field is defined as vendor specific for HAN Relay usage. The first 4 bits are reserved. The bits 5 to 7 contain the Priority field. This field indicates the priority of the HAN-relay-devices that transmits the IE in the Enhanced beacon. In this specification, this Priority field can be ignored by received node (HAN-end-device).

(3) Source Address field

This field contains the address of the PAN coordinator.

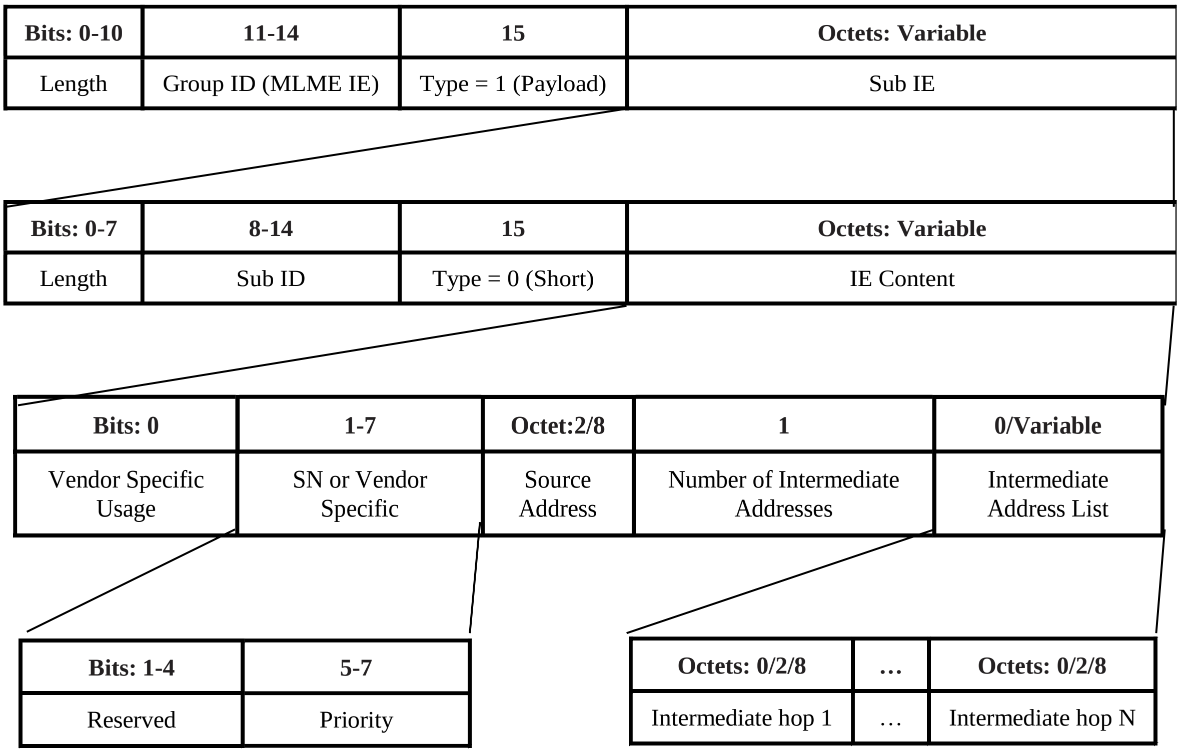
(4) Number of Intermediate Addresses field

This field indicates the number of intermediate HAN-relay-devices to the PAN coordinator that excludes the initiating device of the IE in order starting next to the HAN-end-device.

(5) Intermediate Address List field

This field indicates the addresses of intermediate HAN-relay-devices to the PAN coordinator that excludes the initiating device of the IE. The indicated addresses are shown in the sub-fields of Intermediate hop 1-N.

The addressing mode used in the SRA IE shall be the same address mode as in the MHR. This IE can support up to 12 hops if EUI-64 addresses are used, and up to 49 hops if 16-bit addresses are used.



Bits: 0-10	11-14	15	Octets: Variable
Length	Group ID (MLME IE)	Type = 1 (Payload)	Sub IE

Bits: 0-7	8-14	15	Octets: Variable
Length	Sub ID	Type = 0 (Short)	IE Content

Bits: 0	1-7	Octet:2/8	1	0/Variable
Vendor Specific Usage	SN or Vendor Specific	Source Address	Number of Intermediate Addresses	Intermediate Address List

Bits: 1-4	5-7
Reserved	Priority

Octets: 0/2/8	…	Octets: 0/2/8
Intermediate hop 1	…	Intermediate hop N

Figure 4.8-31 SRA IE

The SLR IE (Sub-ID=0x3D) is included in several frames such as data frame and indicates Source/Destination information of end-to-end devices of the frame payload. This IE also indicates the addresses of the intermediate HAN-relay-devices that relay the frame towards the PAN coordinator according to the SRA IE received during Enhanced Active Scan. Details of its fields are shown below.

(1) The Source Address field contains the address of the device originating the frame.

(2) The Destination Address field contains the address of the destination device of the frame.

(3) L2R Sequence number field

This field indicates the identifier of the frame payload. By referring the value of this field, duplicated frames can be discarded in the multicast transmission.

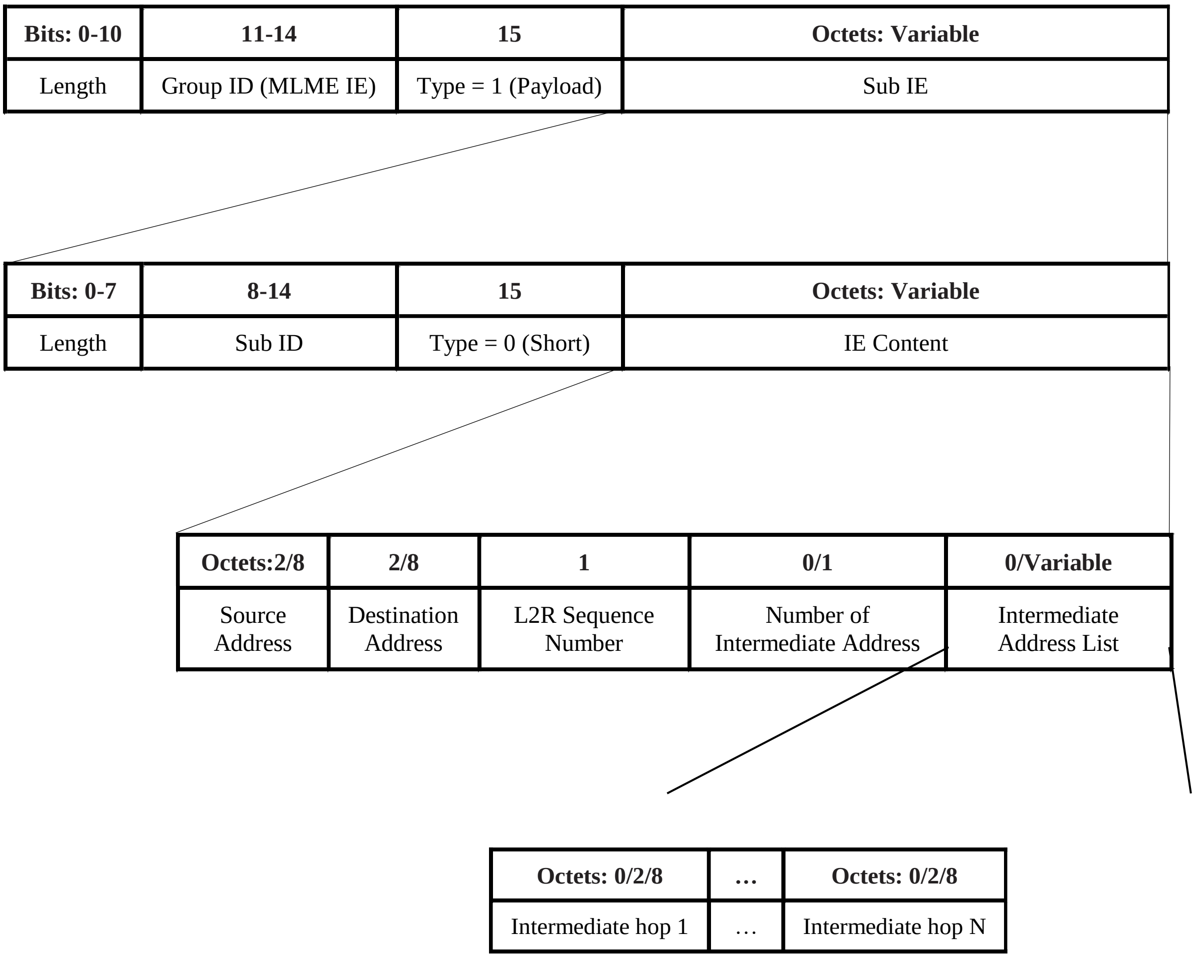
(4) Number of intermediate Address field

This field indicates the number of intermediate HAN-relay-devices to the PAN coordinator that excludes the initiating device of the IE in order starting next to the HAN-end-device.

The Number of Intermediate Address field is always present, and if it is set to zero, the Intermediate Address List field is omitted.

(5) Intermediate Address List field

This field indicates the addresses of intermediate HAN-relay-devices to the PAN coordinator that excludes the initiating device of the IE. The indicated addresses are shown in the sub-fields of Intermediate hop 1-N.



Bits: 0-10	11-14	15	Octets: Variable
Length	Group ID (MLME IE)	Type = 1 (Payload)	Sub IE

Bits: 0-7	8-14	15	Octets: Variable
Length	Sub ID	Type = 0 (Short)	IE Content

Octets:2/8	2/8	1	0/1	0/Variable
Source Address	Destination Address	L2R Sequence Number	Number of Intermediate Address	Intermediate Address List

Octets: 0/2/8	…	Octets: 0/2/8
Intermediate hop 1	…	Intermediate hop N

Figure 4.8-32 SLR IE

3.9.3.3. Examples of typical device operation

Figure 4.8-33 shows an example of relay operation in the MAC layer. At turned on, the HEMS starts the PAN as the PAN coordinator, defines the employed channel according to the situation. After that, a HAN-relay-device named as device A is turned on and finds the HEMS via the scan procedure. Here, HEMS responds to the Enhanced beacon request from device A by returning an Enhanced beacon without SRA IE. That is, frame exchanges between device A and HEMS is conducted without exploiting relay in MAC layer. Then, in the **Figure 4.8-33**, a HAN-end-device named as device B is turned on. Here it should be noted that device A is assumed to be a coordinator. While device B can also find device A after its scan procedure in the similar manner, device A returns an Enhanced beacon with a SRA IE since device A is not the PAN coordinator and needs to show the relay route to the PAN coordinator. After that, device B can send a frame whose final destination is HEMS by constructing it as a MAC frame including a suitable SLR IE and initially addressed to device A according to the received SRA IE information. At receiving the frame, device A relays the frame by updating the Source/Destination addresses in the MAC header according to the SLR IE in MAC layer. As a result, the frame initiated on device B reached to HEMS through device A. Since HEMS acquires the relay route to device B as well as confirms the existence of device A and B, which is required on the higher layer operations, by reversing the addresses in the Intermediate hops field in the received SLR IE, HEMS can realize the relayed transmission to device B hereafter.

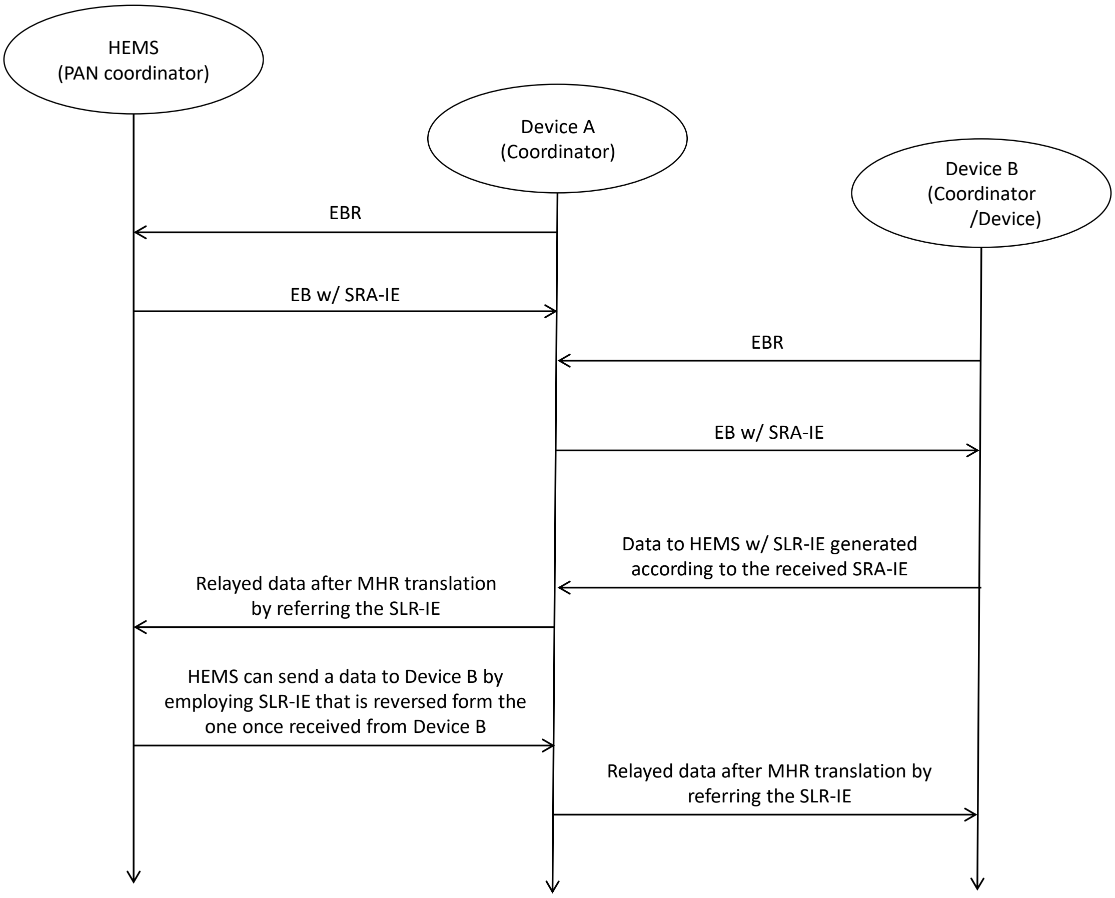

HEMS
(PAN coordinator)
Device A
(Coordinator)
Device B
(Coordinator
/Device)
EBR
EB w/ SRA-IE
EBR
EB w/ SRA-IE
Data to HEMS w/ SLR-IE generated according to the received SRA-IE
Relayed data after MHR translation by referring the SLR-IE
HEMS can send a data to Device B by employing SLR-IE that is reversed form the one once received from Device B
Relayed data after MHR translation by referring the SLR-IE

Figure 4.8-33 Example of relay operation in MAC layer

3.9.3.3.1. Examples of operations in case HAN-relay-device is installed after HAN-end-device

When a HAN-relay-device is newly installed in the situation a HEMS and a HAN-end-device are operating a network, the HAN-end-device shall reset after installing the HAN-relay-device.

3.9.4. Interface part

3.9.4.1. Overview

The interface of a home area network employing relay devices for ECHONET Lite over IPv6 shall be compliant with clause 3.8.4 unless otherwise specified in the following sub clauses.

3.9.4.2. Adaptation layer

See 3.8.4.2 in this document.

3.9.4.2.1.Fragmentation

See 3.8.4.2.1 in this document.

3.9.4.2.2.Header compression

The 6LoWPAN Header compression requirements shall be compliant with clause 3.8.4.2.2, except identification method of source destination IP addresses at the final destination. When final destination node of 6LoWPAN packet needs to identify or reproduce the source and/or destination IP address of receiving 6LoWPAN packet, it must be done based on original source address and final destination address conveyed with theSLR IE, instead of source and destination addresses contained in the MHR.

3.9.4.2.3.Neighbor Discovery

See 3.8.4.2.3 in this document

.

3.9.4.3. Network layer

See 3.8.4.3 in this document.

3.9.4.4. Transport layer

See 3.8.4.4 in this document.

3.9.4.5. Application layer

See 3.8.4.5 in this document.

3.9.5. Security configuration

3.9.5.1. Overview

HEMS and devices shall conform to specification described in 3.8.5.1 in this document unless otherwise described in this clause.

3.9.5.2. Authentication

HEMS and devices shall conform to specification described in 3.8.5.2 in this document unless otherwise described in this clause.

3.9.5.2.1.PANA

3.8.5.2.1 shall be supported, additionally assuming that the PAA-PaC session is supported by the relay in MAC as in 3.9.3, as necessary.

PANA termination sequence between HEMS and HAN-relay-device is just run in regular manner. HAN-relay-device should keep at least 15 (=16 – relay device itself) routing information entries at same time (The number ‘16’ is same as the minimum capacity for PaCs defined in 3.8.5.2.1).

3.9.5.2.2.EAP

3.8.5.2.2 shall be supported.

3.9.5.3. Authentication and key distribution

The specification defined in 3.8.5.3 shall basically be supported in this section, so there is no difference to that on authentication and encryption key distribution to be done between HEMS and HAN-relay-device. Additionally, HAN-relay-device shall be allowed to not accept any communication to be requested from HAN-end-device while HAN-relay-device is ongoing authentication and key distribution process.

The specification below shall be applied to these procedures to be done between HEMS and HAN-end-device.

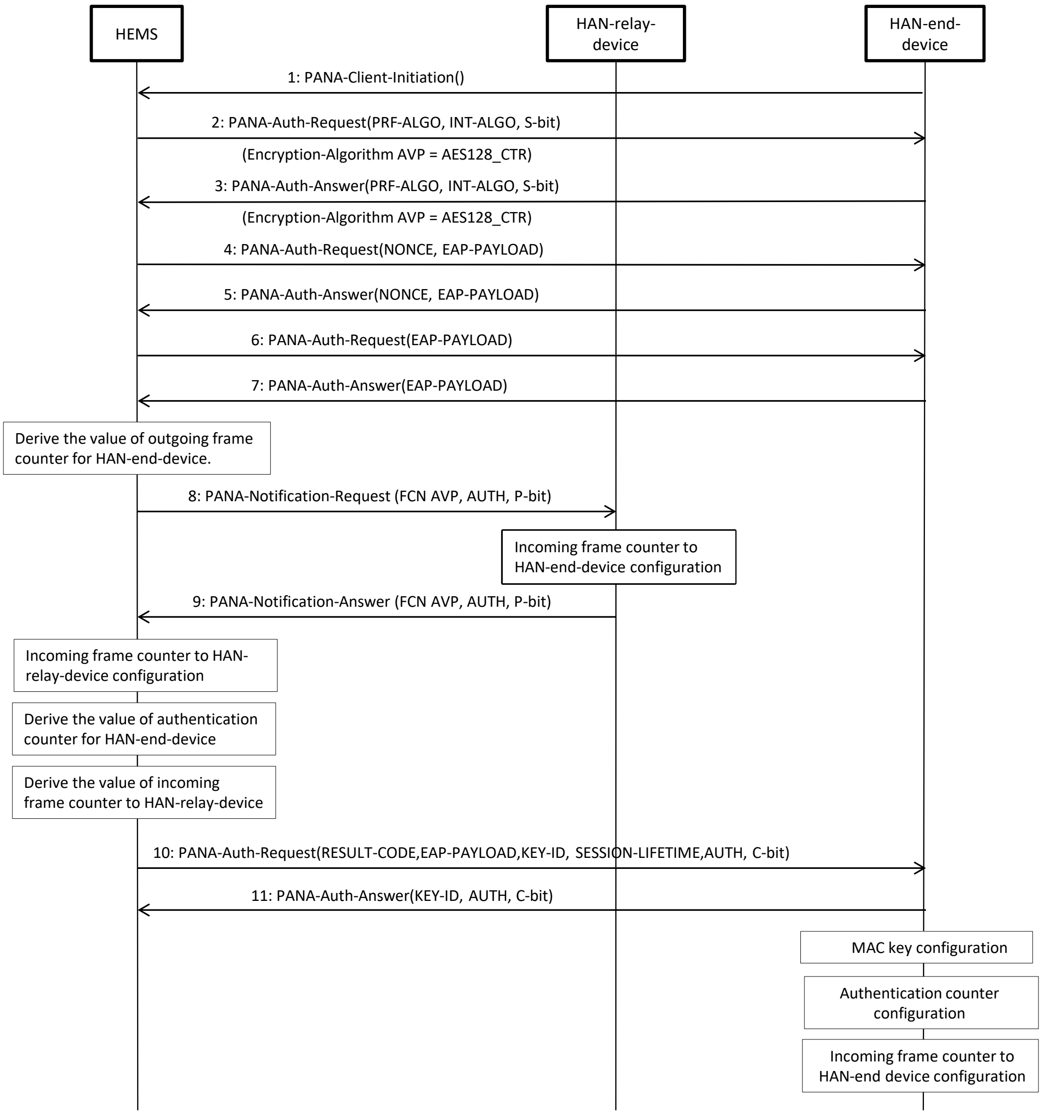

HEMS
HAN-relay-device
HAN-end-device
1: PANA-Client-Initiation()
2: PANA-Auth-Request(PRF-ALGO, INT-ALGO, S-bit)
(Encryption-Algorithm AVP = AES128_CTR)
3: PANA-Auth-Answer(PRF-ALGO, INT-ALGO, S-bit)
(Encryption-Algorithm AVP = AES128_CTR)
4: PANA-Auth-Request(NONCE, EAP-PAYLOAD)
5: PANA-Auth-Answer(NONCE, EAP-PAYLOAD)
6: PANA-Auth-Request(EAP-PAYLOAD)
7: PANA-Auth-Answer(EAP-PAYLOAD)
Derive the value of outgoing frame counter for HAN-end-device.
8: PANA-Notification-Request (FCN AVP, AUTH, P-bit)
Incoming frame counter to HAN-end-device configuration
9: PANA-Notification-Answer (FCN AVP, AUTH, P-bit)
Incoming frame counter to HAN-relay-device configuration
Derive the value of authentication counter for HAN-end-device
Derive the value of incoming frame counter to HAN-relay-device
10: PANA-Auth-Request(RESULT-CODE,EAP-PAYLOAD,KEY-ID, SESSION-LIFETIME,AUTH, C-bit)
11: PANA-Auth-Answer(KEY-ID, AUTH, C-bit)
MAC key configuration
Authentication counter configuration
Incoming frame counter to HAN-end device configuration

Figure 4.8-34 Authentication and key distribution sequence for HAN-end-device

In the above sequence chart, any message to be exchanged between HEMS and HAN-end -device shall be forwarded via HAN-relay-device.

Regarding the procedure from step 1 to step 7, except that all the messages to be exchanged are forwarded by the HAN-relay-device, it shall be identical to usual procedures of authentication and keys distribution to be done between ordinary HEMS and devices unsupporting the relay function, but subsequent procedure shall be as follows.

1) Based on the method described in 3.8.5.3.3, HEMS derives outgoing frame counter value for HAN-end-device from the authentication counter value relevant to HAN-end-device, stores the derived counter value and HAN-end-device's IPv6 address into Frame Counter Notification AVP, and sends PNR message containing this AVP to HAN-relay-device (**Figure 4.8-34** Step 8). HEMS extracts frame counter value from the Frame Counter Notification AVP received from HAN-relay-device, and sets this value as the incoming frame counter relevant to HAN-relay-device.

2) HAN-relay-device generates Frame Counter Notification AVP that contains own IPv6 address and outgoing frame count, attaches this AVP to PNA message, and then send it to HEMS (**Figure 4.8-34** Step 9). HAN-relay-device extracts frame counter value from the Frame Counter Notification AVP received from HEMS, and sets this value as the incoming frame counter relevant to HAN-end-device.

3) Then HEMS sends a PAR message to HAN-end-device (**Figure 4.8-34** Step 10). Here, the counter value notified by prior PNA message from HAN-relay-device is copied to the Frame Counter Out field in the Frame Counter Notification AVP which is attached to this PAR message. By means of this, HAN-end-device can obtain latest value for incoming frame counter relevant to HAN-relay-device.

4) In response to this, HAN-end-device responds HEMS by sending PAA message (**Figure 4.8-34** Step 11).

5) Then HAN-end-device derives its own outgoing frame counter value according to the authentication counter value notified by HEMS (see 3.8.5.3.3), and sets it into its own configuration, together with key information, and incoming frame counter value relevant to HAN-relay-device that were received from HEMS.

The detail of Frame Counter Notification AVP is specified in “3.9.5.4.3 Vendor-specific AVP”. PNR message that contains this vendor-specific AVP shall be specified as follows.

Table 4.8-53 Frame Counter Notification (Step10): Message of PNR (Frame Counter, AUTH)

Field	Sub field	Size(octet)	Description
PANA Message	Reserved	2	
	Message Length	2	64

Header	Flags	2	‘R’bit=1、’P’bit=1
	Message Type	2	4=PANA-Notification-Request
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	Encryption-Encap AVP	40	Frame Counter Notification-AVP is a Vendor-specific AVP which is introduced to this revision. It shall be encapsulated with Encryption-Encap-AVP after encrypted.
	Frame-Counter-Notification AVP	32	
	AUTH AVP	24	AVP containing Message Authentication Code. Message

3.9.5.3.1.Authentication request by PAA

3.8.5.3.1 shall be supported.

3.9.5.3.2.Authentication response by PaC

3.8.5.3.2 shall be supported.

3.9.5.3.3.Distribution of HAN group key

When PaC is a HAN-relay-device, 3.8.5.3.3 shall be supported.

When PaC is a HAN-end-device, a part of contents in Group Key Distribution AVP differ, but the other part shall support 3.8.5.3.3. **Table 4.8-54** shows content of Group Key Distribution AVP.

Table 4.8-54 Field values in Group Key Distribution AVP

	PaC

Fields in Group Key Distribution AVP	HAN-relay-device	HAN-end-device
Group Key	Group Key	
Group Key ID	Key Identifier for Group Key	
Auth Counter	Authentication Counter	
Frame Counter Out	Outgoing Frame Counter of PAA	Incoming Frame Counter for HAN-relay-device

3.9.5.3.4.Response to HAN group key reception by PaC

When PaC is a HAN-relay-device, 3.8.5.3.4 shall be supported in this section.

When PaC is a HAN-end-device, it differs that Group Key Distribution AVP attached to PAR message from PAA contains Incoming Frame Counter value for HAN-relay-device instead of Outgoing Frame Counter value of PAA. Therefore security related information to be set to MAC layer shall be as follows.

LK ＝ Group Key

Key ID ＝ Key Identifier for the Group Key

Outgoing Frame Counter ＝ Auth Counter || 00 00 00

Incoming Frame Counter for PAA ＝Incoming Frame Counter for HAN-relay-device

3.9.5.4. Key update

3.9.5.4.1.Distribution of updated HAN group key by PAA (Push)

3.8.5.4.1 shall be supported. As far as it is assured that frame counter of HEMS and all devices can be set to zero simultaneously at this moment, extra process does not need to be added.

3.9.5.4.2.Acquisition of HAN group Key by PaC (Pull)

The specification defined in 3.8.5.4.2 shall basically be supported in this section. However, when PaC is a HAN-end-device, a part of contents in HAN Group Key AVP shall be different. See "**Table 4.8-54 Field values in Group Key Distribution AVP**" about the detail.

3.9.5.4.3.Vendor-specific AVP

Other than AVPs defined in 3.8.5.4.2, the Frame Counter Notification AVP defined below shall be used in relay network.

- Frame-Counter-Notification AVP

When HEMS must notify incoming frame counter value for the HAN-end-device to the HAN-relay-device, this AVP shall be attached to PANA Notification Request message. HAN-relay-device that received PNR message containing this AVP shall respond the HEMS by sending PNA (AUTH) message.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          AVP Code(3)          |      AVP Flags(1)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         AVP Length(4)         |       Reserved                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Vendor-Id (45605)                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          IPv6 address (1st 4octets)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          IPv6 address (2nd 4octets)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          IPv6 address (3rd 4octets)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          IPv6 address (4th 4octets)                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Frame Counter Out                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4.8-35 shows the Pull sequence. The HEMS shall contain its incoming frame counter value in the Frame-Counter-Notification (FCN) AVP of the PANA Notification Request message to the HAN-relay-device (step2). HAN-relay-device shall contain its outgoing frame counter value in the Frame-Counter-Notification AVP of the PANA Notification Answer message to the HEMS (step3). The HEMS shall contain the outgoing frame counter value of the HAN-relay-device in the HAN-Group-Key AVP to the HAN-end-device (step4).

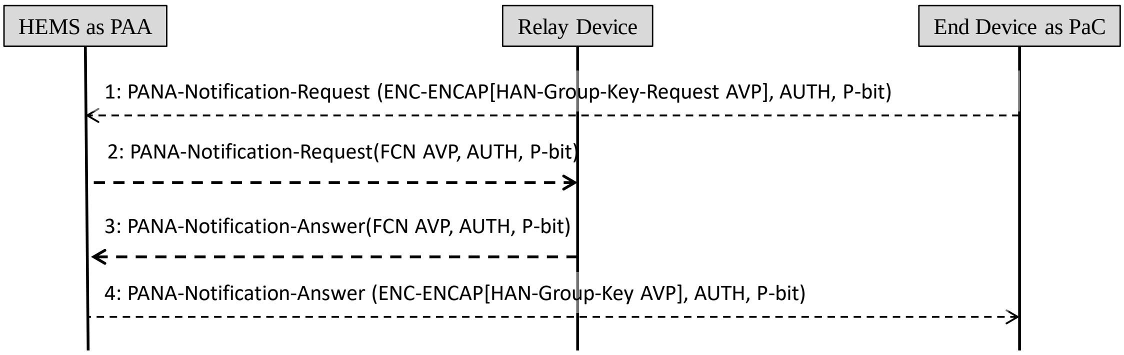

HEMS as PAA
Relay Device
End Device as PaC
1: PANA-Notification-Request (ENC-ENCAP[HAN-Group-Key-Request AVP], AUTH, P-bit)
2: PANA-Notification-Request(FCN AVP, AUTH, P-bit)
3: PANA-Notification-Answer(FCN AVP, AUTH, P-bit)
4: PANA-Notification-Answer (ENC-ENCAP[HAN-Group-Key AVP], AUTH, P-bit)

Figure 4.8-35 Pull Sequence

The Frame Counter Out field shall set a value of outgoing counter, and the IPv6 address field shall indicate owner of the outgoing counter value to be stored in the Frame Counter Out field. This vendor specific AVP shall be sent with encryption by using Encryption Encap AVP, and shall be decrypted on the recipient.

3.9.5.4.4.HAN group key Management

3.8.5.4.4 shall be supported, additionally assuming that the frame counters for the HAN-end-devices can be relayed to the HEMS by the HAN-relay-device when PAA-PaC session is supported by relay on MAC layer, as in 3.9.5.3.

3.9.5.4.5.Authentication counter (AuthCounter) management

3.8.5.4.5 shall be supported.

3.9.5.4.6.HAN group key generation

3.8.5.4.6 shall be supported.

3.9.5.4.7.Encryption/decryption key generation for vendor-specific AVP

3.8.5.4.7 shall be supported.

3.9.5.4.8.Network reconfiguration notification

The specification defined in 3.8.5.4.8 shall basically be supported in this section. Regarding the relation between HAN-relay-device and HAN-end-device, 3.8.5.4.8 shall be supported as well. For example, while HAN-relay-device as PaC is under ongoing Enhanced Active Scan against PAA, the HAN-relay-device may ignore another Enhanced Active Scan from HAN-end-device on the other side until it as PaC receives the response from the PAA.

3.9.5.5. Encryption and Integrity check

3.8.5.5 shall be supported.

3.9.5.6. Replay protection

3.8.5.6 shall be supported.

3.9.6. Recommended network configurations

Follow the 3.8.6.

3.9.6.1. Bootstrapping

Follow the 3.8.6.1 on all devices including a HAN-relay-device and a HAN-end-device.

3.9.6.1.1.Data link layer configuration

The HEMS shall include Pairing ID and Capability Notification IE when it returns an Enhanced Beacon.

A HAN-relay-device shall include a SRA IE as well as a Pairing ID as MLME IEs when it returns an Enhanced Beacon. A device which associates with the HAN-relay-device stores the SRA IE information as a route to the HEMS.

MAC association procedure should be omitted.

Data link configuration except above terms follows the 3.8.6.1.1.

3.9.6.1.2.Network layer configuration

The HEMS, a HAN-relay-device and a HAN-end-device use IPv6 link local address only. Network layer configuration follows the 3.8.6.1.2. with the exception that if a HAN-end-device which needs a HAN-relay-device to relay frames to the HEMS (PAN coordinator) performs IPv6 ND before PANA session, a HAN-end-device should send a frame prior to IPv6 ND to allow HEMS to send a unicast frame to the device as follows.

- A MAC frame with the SLR IE

Source Address in MHR	The HAN-end-device
Destination Address in MHR	HEMS (PAN coordinator)
Intermediate Address in SLR IE	Necessary the HAN-relay-device(s)
MAC payload	6LoWPAN dispatch with NALP (0x00 in the fist byte)*

*: NALP is defined in [6LOWPAN].

Authentication procedure is described in the 3.8.6.3.

3.9.6.2. IP Address Detection

Follow the 3.8.6.2, except that the IP address should be obtained from its SRA-IE not from its MAC header when an EB with SRA IE is included in the received frame.

3.9.6.3. Authentication, Key Exchange, Route information notification to the HEMS

The device performs security setup after data link layer and network layer configurations. In other words, the device acting as a PaC initiates a PANA session to the HEMS acting as the PAA.

A device which doesn’t communicates with the HEMS directly but communicates with a HAN-relay-device shall set a SLR IE in a frame when it transmits a PCI message. The route information from the device to the HEMS shall be stored in the SLR IE.

When the HEMS sends a PANA message to a device which doesn’t associated with the HEMS directly, the HEMS shall set aSLR IE in the frame as route information from the HEMS to the device. TheSLR IE is generated from the route information stored in theSLR IE in the PCI message from the device.

A device which relays a message between the HEMS and the joining device refers to the SLR IE in the received frame and forwards the frame with replacing the MAC destination address to the next hop address and the MAC source address to its address. IEs and PANA message fields shall not be changed.

A PANA message exchanged between the HEMS and a device which associates with the HEMS directly shall not include a SLR IE.

3.9.6.4. Application

Follow the 3.8.6.4.

3.9.7. Usage of credential

Use the HAN authentication ID and Password described in the 3.8.7.

3.9.7.1. Conversion of HAN authentication ID to EAP Identifiers

NAI is generated according to the3.8.7.1.

3.9.7.2. Conversion of Password to PSK

PSK is generated according to the 3.8.7.2.

3.9.8. Discovery and selection of the HEMS network

A HAN device performs Enhanced Active Scan using IEs field to detect the HEMS or a HAN-relay-device. MLME IE (Group ID=0x1) will be used for the Payload IEs field of the Enhanced Beacon Request sent by the HAN device. The eight octets (Pairing ID) defined in both initial mode and normal mode will be included in the IE Contents of Sub-ID=0x68 (Unmanaged) and also the appropriate sender's capability set according to 3.8.3.1 will be included in the IE Contents of Sub-ID=0x67 (Unmanaged) (Capability Notification IE). When the Pairing ID stored in MLME IE of the Payload IEs matches the Pairing ID stored in the HEMS or a HAN-relay-device, the HEMS or the HAN-relay-device responds by returning the Enhanced Beacon. This Enhanced Beacon is unicast and also includes the same Pairing ID and Capability Notification IE which is set according to 3.8.3.1 in the Payload IEs field. After confirmation that the HEMS or the HAN-relay-device has the same Pairing ID and the appropriate capability, the HAN device will start PANA negotiation with the HEMS or the HAN-relay-device.

< Initial setup mode >

The HEMS or a HAN-relay-device is set to initial setup mode in advance before a new HAN device tries to connect to the HEMS or the HAN-relay-device. The HAN device uses an enhanced active scan feature and detects the target HEMS or the target HAN-relay-device. The HEMS or the HAN-relay-device initial mode has a valid period and its suggested value is five minutes. During the time, Pairing ID is set to the fixed strings “HAN_INIT”. The HAN device starts PANA authentication process with the corresponding the HEMS or the HAN-relay-device after enhanced active scanning by Pairing ID. After the valid period expires, the HEMS or the HAN-relay-device invalidates the Pairing ID “HAN_INIT” for initial mode and turns into normal mode. When authentication succeeds, the HAN device set the HEMS’s or the HAN-relay-device’s MAC address for Pairing ID. If authentication fails, HAN device tries to find the corresponding HEMS or HAN-relay-device until PANA authentication succeeds. The HAN device can use an enhanced active scan again to the all channels if it finds no HEMS or HAN-relay-device on all channels or authentication fails.

< Normal operation mode >

The HEMS or a HAN-relay-device set its MAC address for Pairing ID in normal operation mode to be ready for scanning from a device by enhanced active scan. HAN-relay-device would have two Pairing IDs, one is its parent device MAC address and the other is its own MAC address.

Once a HAN device connects to the HEMS or a HAN-relay-device, HAN device should calculate the IPv6 link local addresses of the HEMS and the HAN-relay-device from the MAC source address or theSRA IE of Enhanced Beacon message. And HAN device requests the HEMS to authenticate by [PANA] using NAI and authentication key, which are pre-shared. The HEMS establishes PANA session with the HAN device, and the HEMS authenticates HAN device based on NAI and authentication key. The HEMS delivers HAN-Group-Key for which the HEMS and the HAN device share the MAC layer encryption key after successful authentication. Furthermore, a device which connected to a HAN-relay-device obtains a MAC security transmit frame counter of the HAN-relay-device according to the 3.9.5.3 and set the counter value to the Frame Counter of the associated Device Descriptor of the MAC layer.

After sharing the MAC layer encryption key, the HEMS can communicate with the HAN device, by using encrypted messages. The HEMS conducts service discovery procedure and sends some commands to the HAN device using ECHONET Lite protocol, and the HAN device can do some operations based on the requests and respond execution results to the HEMS.

3.9.9. Route Information

Following the procedure described in the 3.9.6.3, a HAN-relay-device notifies a HAN device of route information to the HEMS by using a SRA IE in an Enhanced Beacon and the device stores the route information. The HAN device sets the route information to theSLR IE when it sends a unicast frame to the HEMS, including the period of PANA authentication. If the number of intermediate records exceeds supported number, a device shall ignore and discard the frame.

The HEMS obtains route information to the HAN device by referring the SLR IE in the received frames during PANA authentication and stores the route information. During PANA authentication or later, the HEMS sets the route information to the SLR IE when it sends a unicast frame to the HAN device. In case PANA authentication fails, the HEMS discards the route information. If the number of records of intermediate node exceeds supported number, a device shall ignore and discard the frame.

After PANA authentication, the HEMS and the HAN device shall not update the route information which they have stored during PANA authentication. In case route change becomes necessary, when such like replacing the HAN-relay-device, scanning and PANA authentication shall be carried out again. In that case, the HEMS needs to keep the new route information to the same device temporarily during PANA authentication, and only if the PANA authentication succeeds, the old route information is replaced with the new one.

3.9.10. Unicast Transmission

The HEMS and a HAN device shall directly transmit a frame without SLR IE if HAN-relay-device is not used to send the frame to a final destination. The HEMS and a HAN device shall transmit a frame withSLR IE if HAN-relay-device(s) is used to send the frame to a final destination.

When a HAN-relay-device receives a frame which has SLR IE, it forwards the frame after putting its own MAC address to the source MAC address field and the next hop address to the destination MAC address field. The next hop address is determined by referring the SLR IE in the received frame. A HAN-relay-device shall not change IEs and frame payload in the frame.

Note that when an encrypted MAC frame is received, a HAN-relay-device decrypts the frame first, and then changes the MAC header address fields, encrypts the updated frame and forwards the encrypted frame to the next hop.

3.9.11. Multicast Transmission

When a device wants to transmit a frame to a multicast group, the frame is treated as a broadcast frame by the MAC sublayer and is filtered by the recipients at the next higher layer.

3.9.11.1. Transmission by the HEMS

When the HEMS wants to transmit a multicast frame, it shall transmit the frame twice. The first frame is transmitted without the SLR IE in order to allow reception by devices that do not support relay. The second frame is transmitted with the SLR IE in order to allow HAN-relay devices to forward the multicast frame.

If the network solely comprises devices of the same type, i.e. supporting or not supporting relay, the HEMS transmits the multicast frame only once with or without the SLR IE respectively. The determination of whether devices of the same type are deployed in the network is out of the sscope of this profile.

3.9.11.2. Transmission by HAN-relay and HAN-end devices

When a HAN-relay or HAN-end device supporting relay wants to transmit a multicast frame, the SLR IE is inserted in the frame.

If a HAN-end device that does not support relay wants to transmit a multicast frame, the frame shall be sent without an SLR IE.

When the HEMS, a HAN-relay, or a HAN-end device supporting relay transmits a multicast frame with the SLR IE, the Source Address field is set to the address of the originator and the Destination Address field is set to the broadcast address. The Number of Intermediate Addresses field is set to 0 and the Intermediate Address List field is omitted.The Source Address and the Destination Address fields of the MHR are also set to the originator’s address and the broadcast address respectively.

3.9.11.3. Multicast frame reception

When device receives a multicast frame:

- If it is a HAN-end-device or the HEMS, it removes the MHR and the SLR IE and delivers the frame to the next higher layer.
- If it is a HAN-relay-device, it leaves the SLR IE intact and sets the source address of the MHR to its own address. The frame is then forwarded.

The source device and any device receiving the frame records the Sequence Number and the Original source address found in the SLR IE. If a frame with the same Sequence Number and Original source address is received, the frame is dropped in order to avoid duplicate forwarding.

An appropriate jitter is applied to each multicast frame transmission in order to reduce the number of possible collisions.

3.10. Recommended usage for home area network among devices with an extension of sleeping end device support

3.10.1. Overview

This clause clarifies the recommended extension to the usage in constructing network for ECHONET Lite over IPv6 communication between a HEMS and multiple devices described in 3.8. A HEMS with the sleeping end device (e.g. a battery operated device like a gas meter) support extension described in this clause shall communicate with a device described in 3.8 in same manner described in 3.8. Compliant nodes to this clause constructs a network with the HEMS as a central coordinator as shown in **Figure 4.8-36**. A HAN consists of HEMS (PAN coordinator) and devices or/and sleeping end devices. In the relay supported HAN specified in 3.9, not all coordinator shall support sleeping end device but a coordinator which needs to connect to sleeping end device directly shall support this functionality. For example, if a PAN coordinator supports sleeping end device and relay devices don’t support it, a sleeping end device only connect to the PAN coordinator. If a PAN coordinator doesn’t support and one of relay devices support this extension, a sleeping end device is able to connect only to the relay device which supports the extension as example illustrated in **Figure 4.8-37**.

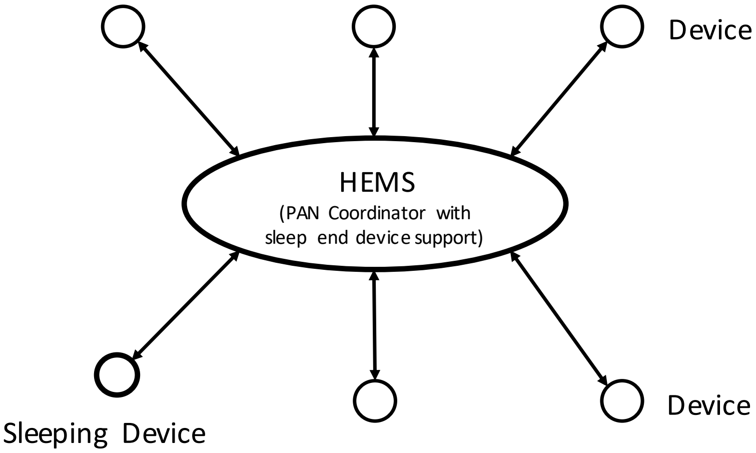


Figure 4.8-36 Home network with sleeping end device support for multiple devices

Note that this recommended usage does not exclude any extensions such as relay function.

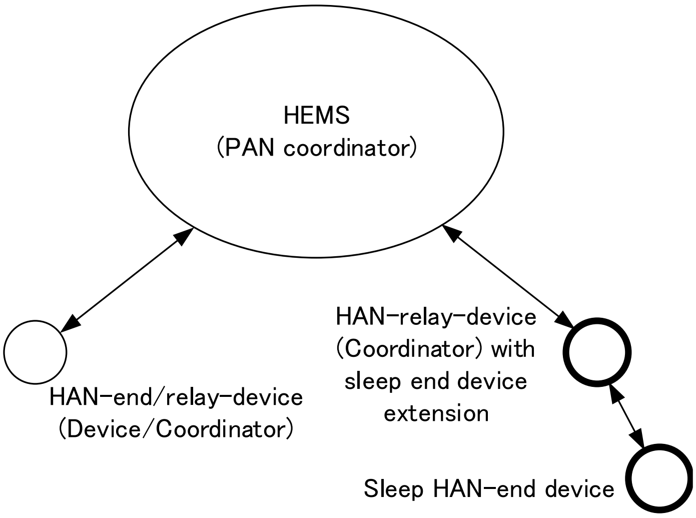


Figure 4.8-37 An example home area network with an relay device which supports sleeping end device

3.10.2. PHY part

See 3.8.2 in this document.

3.10.3. MAC part

This clause shows amendments for HAN supporting a sleeping end device in MAC layer. What is specified here supersedes 3.8 and 3.9 but other specifications should follow3.8.3 and 3.9.3 respectively.

3.10.3.1. MAC sub-layer function

Table 4.8-55 shows amendments in MAC sub-layer functions.

2537 **Table 4.8-55 Amendments in MAC sub-layer functions**

Item number	Item description	Reference section in standard	Status in standard (M:Mandatory, O:Option)	Support (Y:Yes, N:No, O:Option)
MLF25	Sleeping End Device support in HAN	3.10 in this document	New in this usage	O
MLF25.1	Transmission of Capability Notification IE in EBR and reception of Capability Notification IE in EB		New in this usage	MLF25, FD2:Y
MLF25.2	Transmission of Capability Notification IE in EB and reception of Capability Notification IE in EBR		New in this usage	MLF25, FD1:Y
MLF25.3	Multicast Transaction Handling for the Indirect Transmission		New in this usage	MLF25, FD1: Y
MLF 1.1	Purge data	[802.15.4] 6.3.4, 6.3.5	FD1:M FD2:O	MLF25, FD1:Y FD2:N
MLF13	Store one transaction	[802.15.4] 5.1.5	FD1:M	MLF25, FD1:Y FD2:N
MF4.4	Data request	[802.15.4] 5.2.2.4, 5.3.4	Transmitter: M Receiver: FD1:M	Transmitter: MLF25, FD2:Y Receiver: MLF25, FD1:Y

2538

3.10.3.1.1. Coordinator requirement for the handling indirect transmission

This clause describes what the coordinator which supports sleeping end device connectivity needs to suffice.

The coordinator needs to support capability exchange specified in 3.10.8.

The coordinator supporting sleeping end device shall support indirect transmission, which is enabled by supporting “Purge data” functionality, a frame buffer for “Store one transaction” and handling “Data request” format. Acknowledgment frame specified in 3.6.3.2.2 shall support “pending bit” to inform existence of a stored frame in the buffer to sleeping end device when it asked by “Data request” command frame.

When the next higher layer of MAC layer in the coordinator sends a frame, it needs to invoke MCPS-DATA.request as follows.

- If the sending frame is unicast frame to a sleeping end device, MCPS-DATA.request with indicating “indirectTX” as TRUE shall be invoked.
- If the sending frame is unicast frame to other than sleeping end devices, MCPS-DATA.request by indicating “indirectTX” as FALSE shall be invoked as usual.
- If the sending frame is broadcast frame and the coordinator has a sleeping end device as a neighbor by exchanging capability as described in 3.10.8, MCPS-DATA.request with “DstAddr” set as “0xffff” and with “indirectTX” set as “FALSE” shall be invoked and then MCPS-DATA.request shall be invoked per sleeping end devices by setting each MAC address with “indirectTX set as “TRUE”.
- If the sending frame is broadcast frame but the coordinator has no sleeping end device as a neighbor, MCPS-DATA.request shall be invoked by setting “DstAddr” as “0xffff” and setting “indirectTX” as “FALSE”

When a frame is buffered and a sleeping end device queried by “Data request” command frame, the coordinator send an acknowledgment frame with pending bit =TRUE. If there is no buffered frame for the sleeping end device, acknowledgment frame with pending bit =FALSE will be returned.

In this profile specification, it is required that a coordinator including HEMS and relay device should have 8 indirect transmission buffers (8 x 255B) at least to assure to send fragmented IP packet (MTU = 1280 bytes).

In this profile specification, macTransactionPersistenceTime in MAC PIB should be configured as ‘0x3d09’ to extend timeout for indirect transmission to incorpolate a long-sleep application device like a gas meter. The value ‘0x3d09’ corresponds to ‘5 minutes’ in non beacon enabled mode with the PHY specified in 3.7.2.This profile specification doesn’t avoid to use bigger value for this PIB if the implementer requires longer sleep application device.

3.10.3.1.1.1. Purging operation

The next higher layer of MAC layer in a coordinator is recommended to invoke MCPS-PURGE.reuqest primitive in the situations described as following example

- When a data request command frame doesn't come from the sleeping end device for fair amount of time

3.10.3.1.2. Sleeping end device requirement for the handling indirect transmission

The sleeping end device shall support transmission of "Data request" command frame to retrieve a buffered frame from the coordinator. When a sleeping end device needs to send a frame, it is done as well as other non-sleeping end device. When a sleeping end device wakes up and needs to check any frame is buffered during the sleep, it send a "Data request" command frame to the coordinator with which capability exchange is done during network joining.

The Data request command frame shall not be encrypted in this profile.

If acknowledgment frame with pending bit =TRUE is returned, the sleeping end device shall wait a frame from the coordinator for enough time to receive. (c.f. macMAXFrameTotalWaitTime is specified in [802.15.4].)

3.10.3.2. MAC frame format

This clause shows the amendments in MAC frame format. If the HAN support relay functionality, it shall follow 3.9.3.2 as well.

3.10.3.2.1. Capability Notification IE

Capability Notify IE is a payload IE that is attached to Enhanced Beacon Request command frame or Enhanced Beacon frame to inform to corresponding node regarding what capabilities the sender has. A flags below is defined to be used to inform weather the device supports sleeping end device extension. If the relay function is supported, flags for relaying support should be carried in same frame.

- Sleeping-support (bit 5) – if this flag is set, it indicates that the sender support sleeping extension. If the IE is carried by EBR, that indicates whether the sender device is sleeping end device. If the IE carried by EB, that indicates whether the sender supports indirect transmission to communicate with a sleeping end device. If a coordinator doesn’t support sleeping end device extension or it doesn’t have enough buffers for indirect transmission, it should not reply EB in response of EBR or should reply EB without this IE or with this IE setting this flag as zero.

3.10.3.2.2. Acknowledgement frame

The acknowledgment frame for this recommendation shall support pending bit for transmission in a coordinator and for reception in sleeping end device to support indirect transmission.

3.10.4. Interface part

3.10.4.1. Overview

The interface of a single-hop home network among devices for ECHONET Lite over IPv6 shall be compliant with clause 3.7.4 unless otherwise specified in the following sub clauses.

3.10.4.2. Adaptation layer

It shall follow 3.8.4.2 in this document except other than the following limitation. The 6LoWPAN fragmentation should not be performed with more than 8 fragments since this profile just requires a coordinator to have 8 indirect transmission buffers at least (see 3.10.3.1.1).

3.10.4.3. Network layer

See 3.8.4.3 in this document.

3.10.4.3.1. IP addressing

See 3.8.4.3.1 in this document.

3.10.4.3.2. Neighbor discovery

See 3.8.4.3.2 in this document.

3.10.4.3.3. Multicast

See 3.8.4.3.3 in this document for the basic operation. When the network layer needs to send IP Multicast (e.g. The destination address is FF02::1.) in a coordinator (PAN coordinator or relay device), it needs to invoke MCPS-DATA.request primitive of MAC layer for the regular devices and for each sleeping end device with indirect transmission respectively. A coordinator is informed whether a neighbor device is sleeping end device or not during bootstrap sequence. A data frame for the regular devices shall be with IP header which destination is multicast address and with MAC header which destination is broadcast address (0xffff) and a data frame for each sleeping end device shall be with IP header which destination is multicast address and with MAC header which destination is the end device address and shall be sent by unicast indirect transmission.

For example, a PAN coordinator invokes MCPS-DATA.request with MAC destination address as 0xffff to send an IP multicast packet. After that, it invokes MCPS-DATA.request with a MAC address for each sleeping end device to send the same IP packet. It will be done twice if a PAN coordinator has 2 sleeping end devicesregistered. A data frame which is sent by indirect transmission is stored into a frame buffer once and it is actually sent when Data request command is sent to the coordinator from an end device.

When a relay device performs unicast indirect transmission to send multicast packet with SLR IE, it shall replace destination address, ‘0xffff’ in SLR IE with EUI-64 address of a sleeping end device as well as it replaces MAC destination address ‘0xffff’ with sleeping end device’s EUI-64.

3.10.4.4. Transport layer

See 3.8.4.4 in this document.

3.10.4.5. Application layer

See 3.8.4.5 in this document.

3.10.5. Security configuration

See 3.8.5, or see 3.9.5 if the HAN supports relay. All the transactions use indirect transmission for the communication from a coordinator to a sleeping end device. A data request from a sleeping end device to a coordinator is recommended to be done frequently so that time out may not happen during boot strap sequence. A PNR (PANA Notification Request) message with a REQ-Timeout-Modification-Request AVP (vendor specific AVP) is used to extend PANA time out in the HEMS to avoid a sleeping device to be deleted due to PANA session time out. In the response to PNR, the HEMS shall reply with the PNA with requested REQ-Timeout-Modification-Request AVP to the originator of PNR (the joining sleeping device). If the requested values are not valid or unacceptable, the HEMS shall return the default value (REQ_IRT = 3, REQ_MRT = 30) or acceptable value to the originator of the PNR. Since a broadcast frame for MLE update may be lost, an implementation for the sleeping end device is recommended to detect key update from a data frame. An implementation of sleeping end device may have no process to receive and deal MLE update if it can detect key update from a data frame.This procedure is recommended to be limited only for initial sequence immediately after PANA sequence of the bootstrapping before a device sends a data frame to make the management simple in the HEMS.

When the HEMS handles key distribution in the network with sleeping end devices, it may take much time to finish all of key distributions. That may cause an issue that the HEMS takes much more time to update key. To reduce it, the HEMS may handle multiple PANA transactions for PaCs at same time.

The definition of the REQ-Timeout-Modification-Requet AVP is as follows.

- REQ-Timeout-Modification-Requet AVP

Octets	Fields	Remark
2	AVP code	4
2	AVP flags	1, meaning V bit, indicates Vendor-ID field is present
2	AVP length	AVP value length is 4
2	Reserved	As a rule set to 0, but don’t care
4	Vendor-ID	45605

2	REQ_IRT	Requested REQ_IRT in seconds. It shall be in the range 3 - 600.
2	REQ_MRT	Requested REQ_MRT in seconds, shall be more than or equal to REQ_IRT and it shall be in the range 3 - 600

Table 4.8-56 REQ Timeout Modification Request : Message of PNR (ENC-ENCAP [REQ-Timeout-Modification-Request], AUTH, P-bit)

Field	Sub field	Size(octet)	Description
PANA Message Header	Reserved	2	
	Message Length	2	64
	Flags	2	‘R’bit=1、’P’bit=1
	Message Type	2	4=PANA-Notification-Request
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	Encryption-Encap AVP	24	REQ-Timeout-Modification-Request AVP is a vendor specific AVP containing RQT_IRT, RQT_MRT which is defined in this document. It is encrypted and encapsulated in Encryption-Encap AVP.
	REQ-Timeout-Modification-Request AVP	16	
	AUTH AVP	24	contains Message Authentication Code

Table 4.8-57 REQ Timeout Modification Request : Message of PNA (ENC-ENCAP[REQ-Timeout-Modification-Request],AUTH, P-bit)

Field	Sub field	Size(octet)	Description
PANA Message	Reserved	2	
	Message Length	2	64

Header	Flags	2	’P’=1
	Message Type	2	4= PANA-Notification-Answer
	Session Identifier	4	
	Sequence Number	4	
PANA Payload	Encryption-Encap AVP	60	REQ-Timeout-Modification-Request AVP is a vender-specific AVP containing RQT_IRT, RQT_MRT, which is added in this specification. It is encrypted and then encapsulated in Encryption-Encap AVP.
	REQ-Timeout-Modification-Request AVP	52	
	AUTH AVP	24	contains Message Authentication Code

3.10.6. Recommended network configurations

3.10.6.1. Bootstrapping

3.10.6.1.1. Data link layer configuration

See 3.8.6.1.1, or see 3.9.6.1.1 if the HAN supports relay functionality for other than the exception as follows.

When the sleeping end device invokes an active scan in order to detect a HEMS (PAN coordinator), it shall emit EBR including Capability Notification IE as well as MLME IE which sub ID is the Pairing IE. Coordinator which supports sleeping end device shall response EB including Capability Notification IE as well as MLME IE which sub ID is the Pairing IE as described in 3.10.3.2.1. When a non-sleeping end device described in 3.8 and 3.9 emits EBR without Capability Notification IE or emits EBR with Capability Notification IE but sleeping-support flag set as false ,a coordinator shall response EB as described in 3.8 and 3.9 respectively. If a transactions of EBR and EB with Capability Notification IE with sleeping-support flag between a coordinator and a sleeping end device, the sleeping end device is registered in the coordinator as a device to use indirect transmission to communicate. A coordinator in this profile shall have capability to register one sleeping end device at least. If a coordinator receive an EBR from another sleeping end device when there is no more capability to register a sleep end device, the coordinator response EB with disabled sleeping-support flag. If a coordinator which registered a sleep end device doesn’t receive any frame during 3 times of macTransacionPersitenceTime, it can remove the registration.

3.10.6.1.2. Network layer configuration

See 3.8.6.1.2 or see 3.9.6.1.2 if the HAN supports relay functionality.

3.10.6.2. IP Address Detection

Follows 3.8.6.2 or follow 3.9.6.2 if the HAN supports relay functionality.

3.10.6.3. Authentication and Key Exchange

Follows 3.8.6.3 or follow 3.9.6.3 if the HAN supports relay functionality.

3.10.6.4. Application

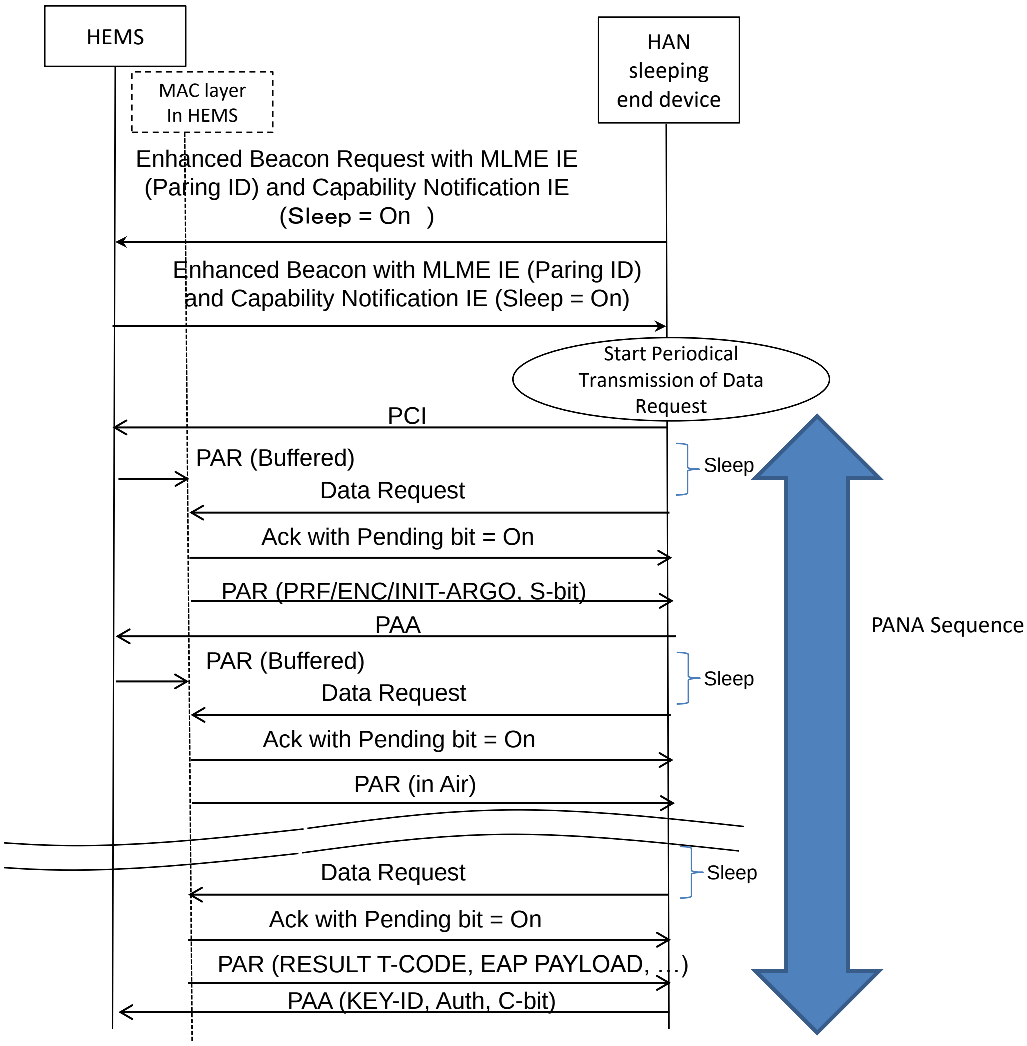
Follows 3.8.6.4 or follow 3.9.6.4 if the HAN supports relay functionality.

3.10.7. Usage of credential

Follows 3.8.7 or follow 3.9.7 if the HAN supports relay functionality.

3.10.8. Discovery and selection of the HEMS network

See 3.8.8 or see 3.9.8 for HAN with relay support with exceptions of using Capability Notification IE as described in 3.10.3.2.1 and of using indirect transmission for the communication from coordinator to sleeping end device as described in 3.10.3.1 and 3.10.3.2. An example sequence is illustrated in **Figure 4.8-38**.


HEMS
MAC layer In HEMS
HAN sleeping end device
Enhanced Beacon Request with MLME IE (Paring ID) and Capability Notification IE (Sleep = On)
Enhanced Beacon with MLME IE (Paring ID) and Capability Notification IE (Sleep = On)
Start Periodical Transmission of Data Request
PCI
PAR (Buffered)
Data Request
Sleep
Ack with Pending bit = On
PAR (PRF/ENC/INIT-ARGO, S-bit)
PAA
PAR (Buffered)
Data Request
Sleep
Ack with Pending bit = On
PAR (in Air)
Data Request
Sleep
Ack with Pending bit = On
PAR (RESULT T-CODE, EAP PAYLOAD, …)
PAA (KEY-ID, Auth, C-bit)
PANA Sequence

2740

2741 **Figure 4.8-38 An example sequence for network discovery**

2742

3.11. Recommended usage for Route-IoT network

3.11.1. Overview

This clause clarifies the recommended usage in constructing network between a smart meter and IoT devices (Route-IoT). The “IoT device” is a generic expression for a terminal which is attached to a gas meter, water meter, and so on to communicate with a (electricity) smart meter. Compliant nodes to this clause construct a network with the smart meter as a central coordinator as shown in **Figure 4.8-39**. This network consists of one smart meter and one or more IoT devices that act as end devices or sleeping end devices or relay devices. All coordinators described in this clause shall support sleeping end device. In this network, non ECHONET Lite application can be adopted as an upper layer application.

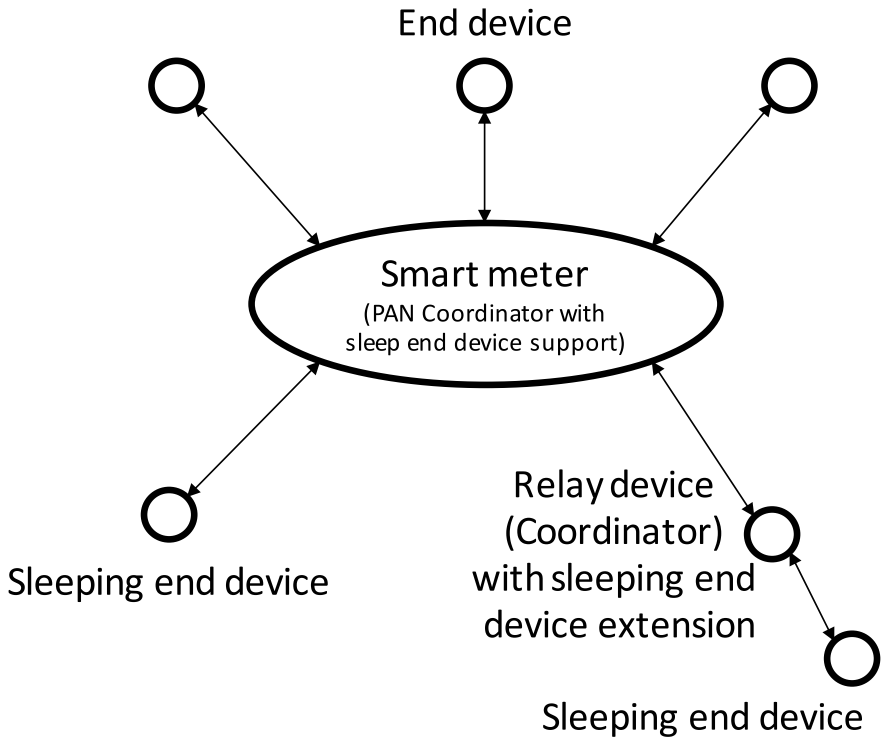


Figure 4.8-39 Route-IoT network for multiple devices

3.11.2. PHY part

See 3.8.2 in this document.

3.11.3. MAC part

This clause shows additional specifications for Route-IoT in MAC layer. What is specified here supersedes 3.8, 3.9, and 3.10 but other specifications should follow 3.8.3, 3.9.3, and 3.10.3 respectively.

3.11.3.1. Capability Notification IE (CN IE)

Figure 4.8-40 shows the structure of modified CN IE.

In this CN IE, the "Application specific" field (bit 1-4) is introduced in this recommended usage. The bit 1 is a flag to use this field. If this flag is set, it indicates that sender set the application specific content (bit 2-4). This content is opaque at the MAC level and used by upper layers. If this flag is not set (0), the content (bit 2-4) shall be set to 0.

Bits: 0-7	**8-14**	**15**	**Octets: Variable**
Length	Sub-ID (0x67)	Type (Short format)	IE content

Bits: 0	**1**	**2-4**	**5**	**6**	**7**
Reserved (0)	flag	content	Sleeping-support	Relay-endpoint	Relay-intermediate
	Application specific			HAN relay function	

Figure 4.8-40 Capability Notification IE with Application specific field

3.11.4. Interface part

3.11.4.1. Overview

The interface of Route-IoT network shall be compliant with clause 3.10.4 unless otherwise specified in the following sub clauses.

3.11.4.2. Adaptation layer

See 3.10.4.2 in this document.

3.11.4.3. Network layer

See 3.8.4.3 in this document.

3.11.4.3.1. IP addressing

See 3.8.4.3.1 in this document.

3.11.4.3.2. Neighbor discovery

See 3.8.4.3.2 in this document.

3.11.4.3.3. Multicast

See 3.8.4.3.3 in this document.

3.11.4.4. Transport layer

See 3.8.4.4 in this document.

3.11.4.5. Application layer

See 3.8.4.5 in this document.

3.11.5. Security configuration

See 3.10.5 and 3.8.5, or see 3.9.5 if the network supports relay.

3.11.6. Recommended network configurations

The smart meter(s) and IoT device(s) share a “Pairing ID” with 8-octet length, and this ID is used in the network discovery. The IoT device selects a suitable smart meter for the IoT device to connect to from one or more smart meter candidates in the network discovery. The Pairing ID, NAI and pre-shared key for PANA/EAP are set to each node in advance.

Note:

The Pairing ID may be shared by several smart meters and IoT devices, or it may be unique for each smart meter and IoT device pair. The Pairing-ID is given in advance, which is assigned by someone (e.g., power company) via offline.

See 3.8.6 in this document for radio channel and PAN ID settings.

3.11.6.1. Bootstrapping

3.11.6.1.1. Data link layer configuration

See 3.10.6.1.1 in this document.

3.11.6.1.2. Network layer configuration

See 3.8.6.1.2 or see 3.9.6.1.2 if the network supports relay functionality.

IP Address Detection

Follows 3.8.6.2 or follow 3.9.6.2 if the network supports relay functionality.

3.11.6.1.3. Authentication and Key Exchange

Follows 3.8.6.3 or follow 3.9.6.3 if the network supports relay functionality.

3.11.6.1.4. Application

Follows 3.8.6.4 or follow 3.9.6.4 if the network supports relay functionality.

3.11.7. Usage of credential

In Route-IoT network, a Route-IoT specific credential (**Table 4.8-58**) is defined and required to use it. For this purpose, this subsection defines how to use the credential in the communication protocols.

Table 4.8-58 Route-IoT Credential

Name	Description
HAN authentication ID	Smart meter: Character string of 24 comprised of 0~9 and A~F ASCII characters (24 octets). The first character string of eight characters is “01000000” and the following string of 16 characters (16 octets) is described in hexadecimal notation of MAC address of smart meter. In this profile, this is converted to the ID ([NAI] format) used by PANA (EAP-PSK) by the rule described later. IoT device: Character string of 24 comprised of 0~9 and A~Z ASCII characters (14 octets). In this profile, this ID is used by PANA (EAP-PSK) as it is.
(HAN authentication) Password	Password linked to the HAN authentication ID (character string of 16 comprised of 0~9, a~z, and A~Z ASCII characters). In this profile, this is used in generating PSK, which is utilized in [EAP-PSK], by the rule following 3.8.7.2.

3.11.7.1. Conversion of HAN authentication ID to EAP Identifiers

Based on the HAN authentication ID, the following rules are used to generate the EAP Identifiers.

[NAI generation rules]

Smart meter side NAI (EAP ID_S): ”CTRL” + ”HAN authentication ID of Smart meter” (24 octets)

IoT device side NAI (EAP ID_P): ”HAN authentication ID of IoT device” (14 octets)

Example:

When Smart meter HAN authentication ID is "010000001111222233334444"

and IoT device HAN authentication ID is “55556666777788”

Smart meter side NAI (EAP ID_S): "CTRL010000001111222233334444"

IoT device side NAI (EAP ID_P): "55556666777788"

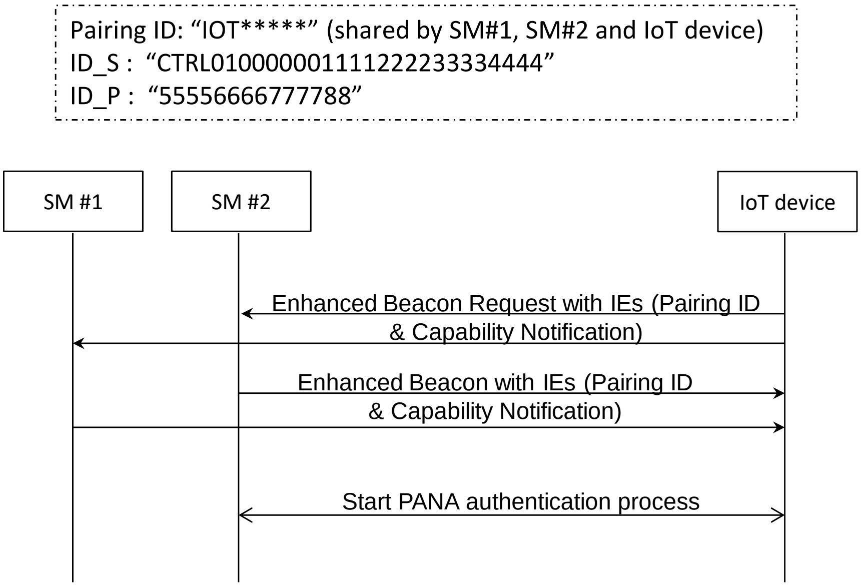
The MAC address in the Smart meter is supposed to be “1111222233334444”

The MAC address in the IoT device is “AAAABBBBCCCCDDDD”,
which is not related to the HAN authentication ID

3.11.8. Discovery and selection of the smart meter network

An IoT device uses an Enhanced Active Scan and detects one or more smart meters. The IoT device selects one smart meter to connect to based on the received EB. The IoT device starts the PANA authentication procedure with the selected smart meter after Enhanced Active Scan. If PANA authentication failed, the IoT device tries to authenticate PANA to other detected smart meters until PANA authentication succeeds. The IoT device can use an Enhanced Active Scan again to the all radio channels if it finds no smart meter on all channels or authentication fails.

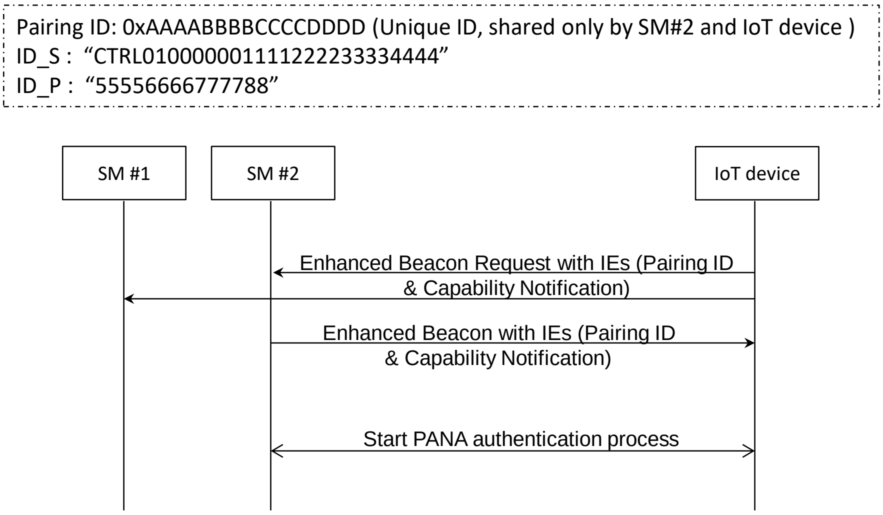
Figure 4.8-41 shows an example sequence for a shared Pairing ID in the smart meter discovery procedure. **Figure 4.8-42** shows an example sequence for a unique Pairing ID in the smart meter discovery procedure.


Pairing ID: "IOT*****" (shared by SM#1, SM#2 and IoT device)
ID_S : "CTRL01000000111112222233334444"
ID_P : "55556666777788"
SM #1
SM #2
IoT device
Enhanced Beacon Request with IEs (Pairing ID & Capability Notification)
Enhanced Beacon with IEs (Pairing ID & Capability Notification)
Start PANA authentication process

2858

2859 **Figure 4.8-41 Smart meter discovery procedure (Shared Pairing ID case)**

2860


Pairing ID: 0xAAAABBBBCCCCDDDD (Unique ID, shared only by SM#2 and IoT device)
ID_S : "CTRL01000000111112222233334444"
ID_P : "55556666777788"
SM #1
SM #2
IoT device
Enhanced Beacon Request with IEs (Pairing ID & Capability Notification)
Enhanced Beacon with IEs (Pairing ID & Capability Notification)
Start PANA authentication process

2861

2862 **Figure 4.8-42 Smart meter discovery procedure (Unique Pairing ID case)**

2863

4. Wi-SUN profiles (ECHONET Lite over non IP)

4.1. Overview

This section defines physical (PHY) and data link layers profiles and Wi-SUN ECHONET Lite interface to communicate between devices using non-IP and IEEE 802.15.4g and 4/4e. Wi-SUN ECHONET-Lite interface is an interface between ECHONET Lite application part and physical and MAC layer parts and transmits ECHONET Lite application data from one device to the other devices. Figure4.8-43 shows the scope of this section. Figure 4.2-1 shows the Wi-SUN profile layer structure.

In this section, the mark of "M" indicates the mandatory functions in the standards [802.15.4], [802.15.4g] and [802.15.4e], and "O" means optional functions. The marks of "Y" and "N"mean the required and not-required functions in ECHONET Lite operation, respectively. Specifications and procedures for certification and interoperability tests are provided by [Wi-SUN-PHY], [Wi-SUN-MAC], [Wi-SUN-IF], [Wi-SUN-CTEST] and [Wi-SUN-ITEST].

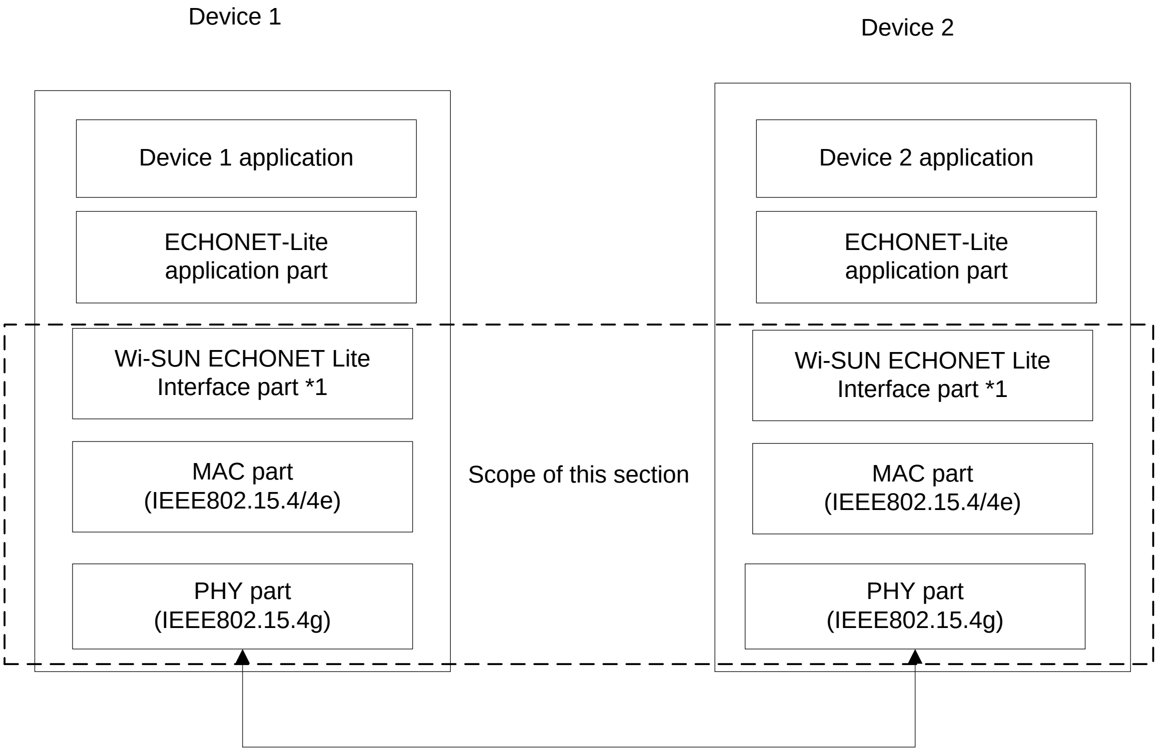

Device 1
Device 2
Device 1 application
ECHONET-Lite application part
Wi-SUN ECHONET Lite Interface part *1
MAC part (IEEE802.15.4/4e)
PHY part (IEEE802.15.4g)
Device 2 application
ECHONET-Lite application part
Wi-SUN ECHONET Lite Interface part *1
MAC part (IEEE802.15.4/4e)
PHY part (IEEE802.15.4g)
Scope of this section

Figure4.8-43 Scope defined by this section (*1: Not required in case addressing architectures are same between ECHONET Lite application layer and data link layer)

4.2. Protocol stack

Protocol stack for the device defined by this profile is shown in Figure4.8-44.

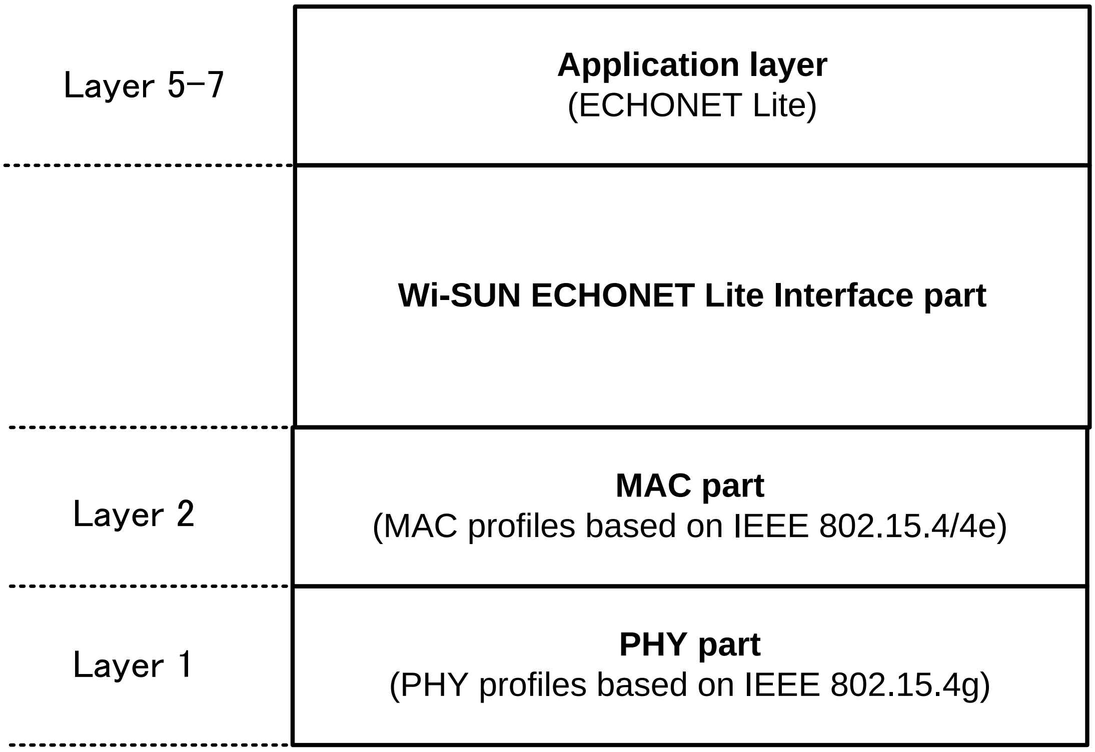

Layer 5−7
Application layer
(ECHONET Lite)
Wi-SUN ECHONET Lite Interface part
Layer 2
MAC part
(MAC profiles based on IEEE 802.15.4/4e)
Layer 1
PHY part
(PHY profiles based on IEEE 802.15.4g)

Figure4.8-44 Layer structure defined by this section (*1: Not required in case addressing architectures are same between ECHONET Lite application layer and data link layer)

PHY layer provides the following service under this profile.

- Up-to-2047 bytes PSDU exchange (Note that the profile recommends 255 bytes or less as mentioned later)

Data link (MAC) layer provides the following services under this profile.

- Successful discovery of IEEE 802.15.4 PAN in radio propagation range
- Support of low energy hosts that can change its status between active and sleep status
- Security functions that includes encryption, manipulation detection and replay attack protection (Note that key management is not performed by this layer)

Application layer provides the following services under this profile.

- Detection of functional units (ECHONET object) employed by the other nodes in the network
- Acquisition of parameters and statuses (ECHONET property) for the other nodes
- Configuration of parameters and statuses for other nodes
- Notification of parameters and statuses for the local node

4.3. PHY part

Refer to “3.3 PHY part”

4.4. MAC part

Refer to “3.4 MAC part”

4.5. Wi-SUN ECHONET Lite Interface part

4.5.1. Overview

Wi-SUN ECHONET Lite interface shall provide a function to communicate between ECHONET Lite application part and Wi-SUN PHY and MAC layer. This part is not required in case addressing architectures are same between ECHONET Lite application layer and data link layer. This interface can improve high frame utilization efficiency by reducing overhead when IP is used.

4.5.2. Requirement

(1) Wi-SUN ECHONET Lite interface shall specify unique destination address and shall configure an ECHONET Interface header by specifying source address and Interface Type. In the case, the Interface Type shall use 0xEC00.

(2) Wi-SUN ECHONET Lite interface shall know address configuration used in MAC layer in advance. The address configuration may be 64 bit IEEE Address.

(3) Wi-SUN ECHONET Lite interface shall convert the unique specified destination address in Wi-SUN ECHONET Lite to MAC address used in MAC part and transmit to MAC part.

(4) Wi-SUN ECHONET Lite interface shall analyze the unique specified destination address. When the destination address is multicast address, the interface shall instruct MAC layer to do broadcast transmission.

4.6. Application layer

Wi-SUN ECHONET Lite interface shall support ECHONET Lite [EL] as application layer. The node implemented specifications in this document shall support mandatory function defined in [EL].

4.7. Security

There are two ways for security in Non-IP based communications. Either way shall be selected.

- Data encryption on MAC layer
- Data encryption on Wi-SUN ECHONET Lite interface

AES-CCM and/or AES-GCM shall be used in the case of data encryption for Wi-SUN ECHONET Lite interface [EL][CMAC][AES-CCM][AES-GCM]. To use AES-CCM and/or AES-GCM, MIC (message integrity code) shall be used. In the case of data encryption on MAC layer, the MIC and/or AAD（Additional Authenticated Data）shall be included in the IEEE802.15.4 MAC frame defined by [802.15.4], respectively. On the other hand, in the case of data encryption on Wi-SUN ECHONET Lite interface, the MIC shall be included in the security header described in Section 4.9.1.4.5. Multiple keys can be managed and stored in the interface part. Since field of security ID in the security header (Figure4.8-55**)** is 1 byte, 255 keys can be managed.

4.8. Device ID

As an optional function, Wi-SUN ECHONET Lite interface may use unique device ID allocated for each ECHONET Lite device. The device ID is used in order to identify ECHONET devices. The value in this field is to be defined in the future according to the implementers' preferences and not in the current version. The length of the device ID is 8 bytes. MAC address may be used for initial setting of the device ID. In the case, there are two kinds of payloads: information payload and setting payload. Information payload will be used for the transmission and receipt of ECHONET Lite information data, and setting payload will be used for the transmission and receipt of device ID.

4.9. Frame format

This section describes frame format to support f Wi-SUN ECHONET Lite payload. The frame format is dependent whether Wi-SUN ECHONET Lite interface part is used or not.

4.9.1. The case interface part is employed

4.9.1.1. The case when data is encrypted on MAC layer

A sample procedure of frame formatting in the case when data is encrypted on MAC layer is shown in Figure4.8-45 - Figure4.8-47. This is the case that destination and source MAC addresses in ECHONET Interface header are different from those in IEEE 802.15.4 MAC header. But integration between those in both headers may be possible.

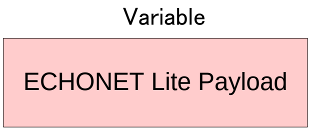


Figure4.8-45 ECHONET-Lite payload

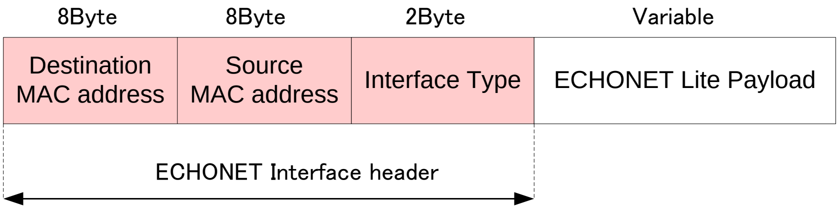


Figure4.8-46 Frame configured by Wi-SUN ECHONET Lite interface

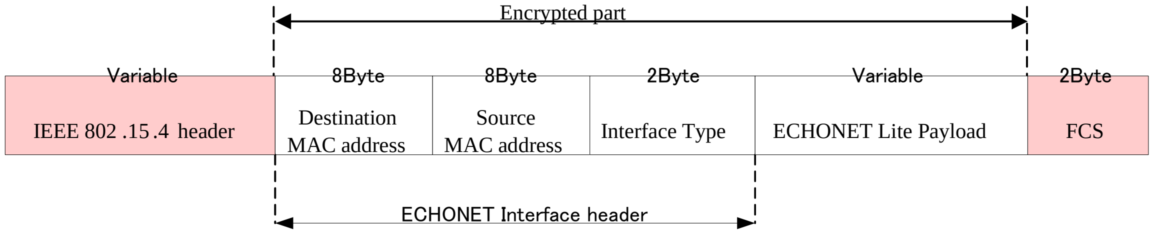


Figure4.8-47 IEEE802.15.4 frame configured by MAC layer

4.9.1.2. The case when data is encrypted on Wi-SUN ECHONET Lite interface

A sample procedure of frame formatting in the case when data is encrypted on Wi-SUN ECHONET Lite interface is shown in Figure4.8-48 - Figure4.8-50. This is the case that destination and source MAC addresses in ECHONET Interface header are different from those in IEEE 802.15.4 MAC header. But integration between those in both headers may be possible.

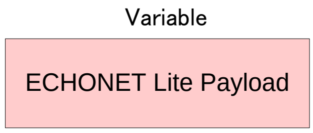


Figure4.8-48 ECHONET-Lite payload

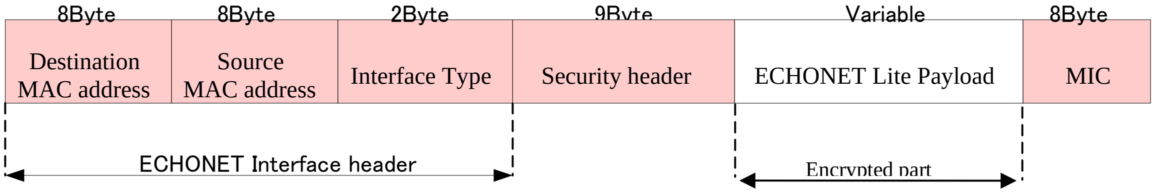


Figure4.8-49 Frame configured by Wi-SUN ECHONET Lite interface

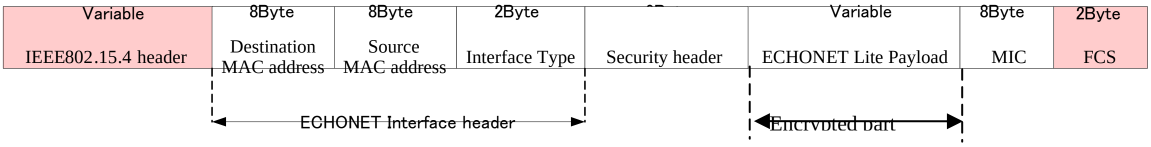


Figure4.8-50 IEEE802.15.4 frame configured by MAC layer

4.9.1.3. The case when data is encrypted on Wi-SUN ECHONET Lite interface and optional device ID is used

A sample procedure of frame formatting in the case when data is encrypted on Wi-SUN ECHONET Lite interface and optional device ID is used is shown in Figure 4.9-7 - Figure 4.9-9. This is the case that destination and source MAC addresses in ECHONET Interface header are different from those in IEEE 802.15.4 MAC header. But integration between those in both headers may be possible.

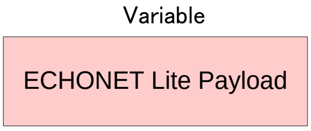


Figure4.8-51 ECHONET-Lite payload

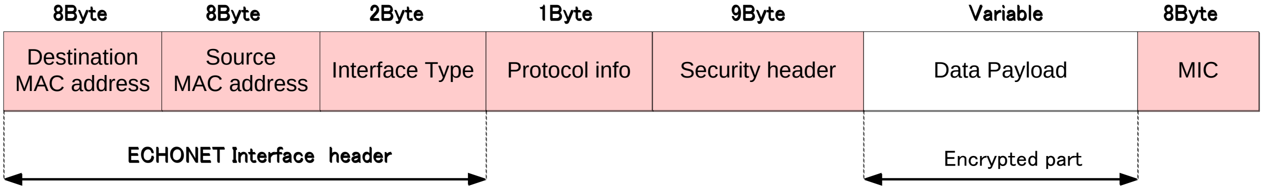


Figure4.8-52 Frame configured by Wi-SUN ECHONET Lite interface

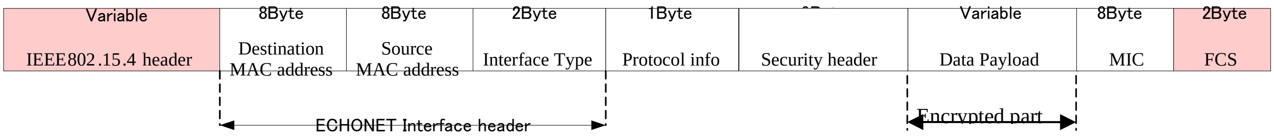


Figure4.8-53 IEEE802.15.4 frame configured by MAC layer

4.9.1.4. Elements in frame

4.9.1.4.1.ECHONET Lite payload

ECHONET Lite payload consists of ECHONET Lite information generated by ECHONET Lite application part.

4.9.1.4.2.ECHONET Interface header

Ether2 header is unique header used in WI-SUN ECHONET Lite interface. Figure4.8-54 shows the format.

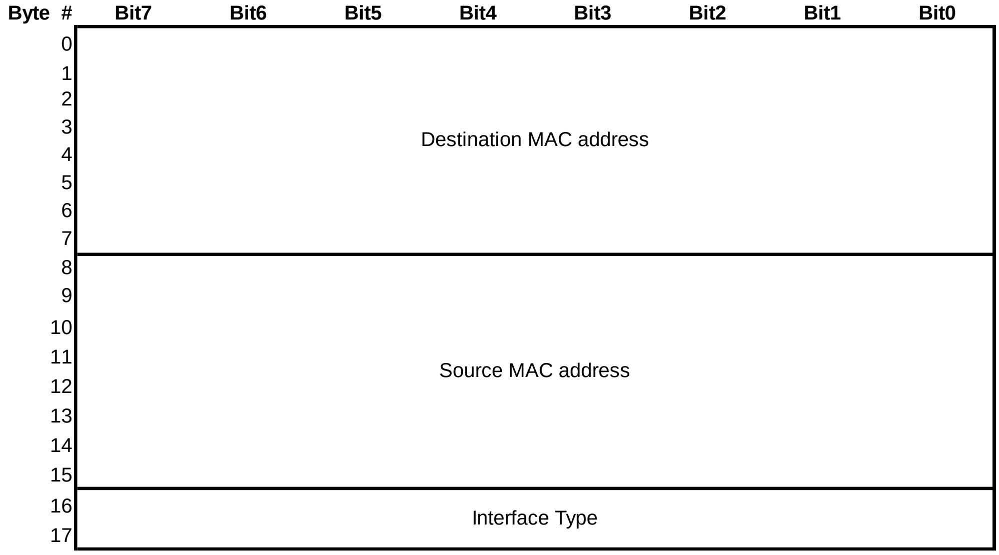


Figure4.8-54 Format of ECHONET Interface header

(a) Destination address

Destination address defined by collaborating between ECHONET Lite application part and Wi-SUN ECHONET Lite interface.

(b) Source address

Source address defined by Wi-SUN ECHONET Lite interface on the basis of address configuration in MAC part

(c) Interface Type

0xEC00：Interface Type for ECHONET Lite

4.9.1.4.3.IEEE802.15.4 header

IEEE802.15.4 header is a header for data transmission and receipt and is generated by MAC part.

4.9.1.4.4.FCS (Frame check sequence)

FCS is a frame check sequence generated by MAC part.

4.9.1.4.5.Security header

Security header defines information on encryption of transmission data.　Figure4.8-55 shows the format.

Byte #	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
0	Security key　ID							
1	Nonce：Reset information							
2								
3								
4								
5	Nonce：Message counter							
6								
7								
8								

Figure4.8-55 Format of security header

(a) Security key ID

Security key ID is an identifier corresponds to encryption key used.

(b) Nonce (byte# 1-8)

A unique number is set to each transmission data and encrypted with data. The followings define each element.

Reset information (byte# 1-4): The number is incremental when the device is reset.

Message counter (byte# 5-8): This is counter that counts the number of messages transmitted

4.9.1.4.6.MIC (Message Integrity Code)

The code is used for AES-CCM encryption.

4.9.1.4.7.Protocol info

Protocol info defines class of protocol. The info is mainly used when unique device ID is used and consists of version information and protocol class. Figure4.8-56 shows the format.

Byte #	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
0	Version info				Protocol class			

Figure4.8-56 Format of protocol info

(a) Version info: 4 bit is assigned and 16 versions are defined

(b) Protocol class: Classify setting payload and information payload

0000: information payload, 0001: setting payload

4.9.1.4.8.Data payload

Data payload carries either information data or setting data based on device ID. The class of data payload is defined by protocol class. Figure4.8-57 and Figure4.8-58 show the formats for them. Figure4.8-58 shows format of settings request payload and settings response payload. The Device ID for request is ID of request device. And The Device ID for response is ID of response device.

Byte #	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
	ECHONET Lite Payload (Variable)							
1	MIC(Message Integrity Code)							
2								
3								
4								
5								
6								
7								
8								

Figure4.8-57 Format of information data payload

Byte #	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
0	Message identifier							
1	Device ID							
2								
3								
4								
5								
6								
7								
8								
9	MIC(Message Integrity Code)							
10								
11								
12								
13								
14								
15								
16								

Figure4.8-58 Format of setting data payload

(Interface part sets setting data payload including Device ID.)

(a) Message identifier: Identify between setting request and setting response

00000000: Setting request

00000001: Setting response

4.9.2. The case interface part is not employed

When ECHONET Lite application part employs IEEE802.15.4 MAC address directly, the Wi-SUN ECHONET Lite interface part is not required. A sample procedure of frame formatting is shown in Figure4.8-59 - Figure4.8-60.

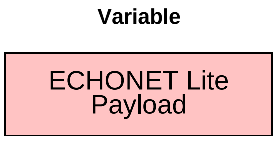


Figure4.8-59 ECHONET-Lite payload

IEEE802.15.4 header	ECHONET Lite Payload	FCS

Figure4.8-60IEEE802.15.4 frame configured by MAC layer

4.10. Recommended usage for single-hop network

4.10.1. Overview

This clause clarifies the recommended usage in constructing single-hop network for ECHONET Lite over non IP. Note that this profile does not exclude other usages.

Compliant nodes to this clause constructs single hop network where a coordinator is centered. And, with assuming a gateway connection provided by application layer as the connection measure to the outer networks, a closed IP network is assumed inside this profile. On those assumptions, the indoor network construction based on ECHONET Lite provides expandability as well as feasibility.

4.10.2. Construction of new network

Once turned on, a coordinator constructs a new network compliant to this profile. The network construction are conducted by successive steps of (1) data link layer configuration, (2) network layer configuration and (3) security configuration. Overview of the network construction procedure is shown in Figure4.8-61 .

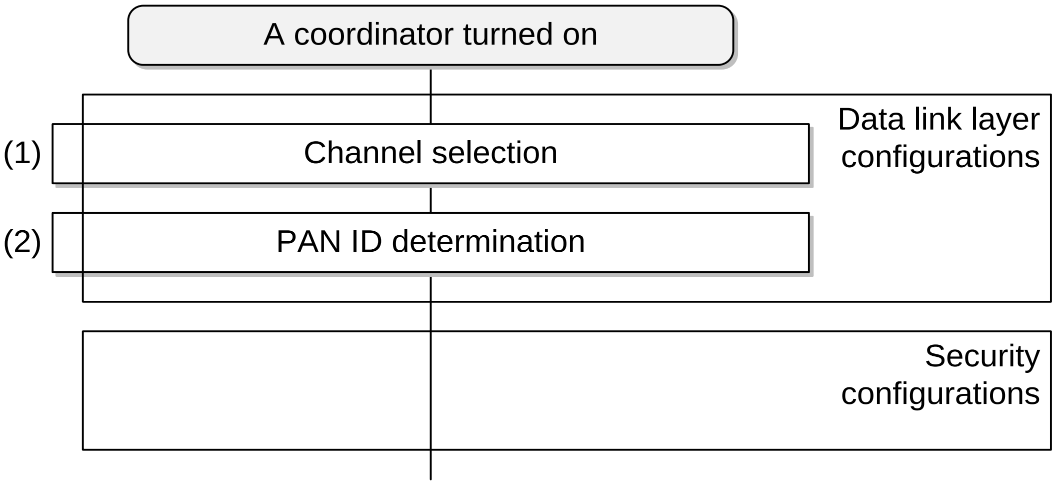


Figure4.8-61 Overview of network construction procedure

4.10.2.1. Data link layer configurations

Once turned on, a coordinator constructs a IEEE 802.15.4 PAN. Detailed procedures for PAN construction is shown as follows.

The coordinator first selects an employed channel. The channel selection is conducted via ED scanning or active scanning. In the selection, channel with less interference to the other systems are more preferable. (Step 1)

Next, the coordinator selects the PAN ID that is not occupied on the selected channel in Step 1, and define it as the PAN ID for the local network. Selection criteria of PAN ID out of candidate IDs is out of scope of this profile. (Step 2)

With conducting of the previous steps, PAN construction by the coordinator is completed.

4.10.2.2. Security configurations

The coordinator conducts security configurations following data link layer and network layer configurations. Security technologies employed in the constructed network should be selected according to the application requests. This profile does not describe a concrete procedure for security configurations conducted by the coordinator.

4.10.3. Association to the network

Once turned on, a new host tries to association to the existing network compliant to this profile. Association procedure by the host includes (1) data link layer configuration, (2) network layer configuration and (3) security configuration just in a same manner as PAN construction by a coordinator. Overview of association procedures to the existing network by a host is shown in Figure4.8-62.

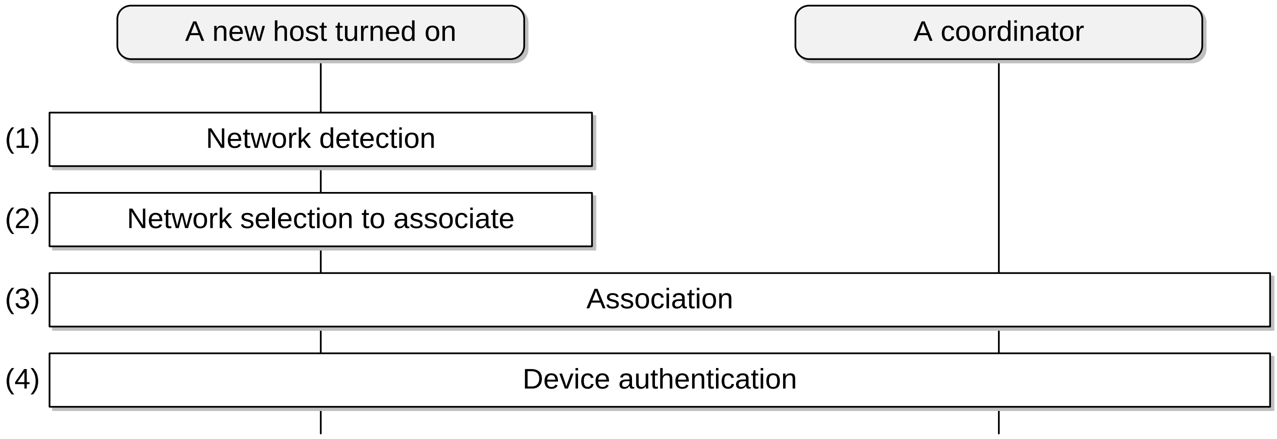


Figure4.8-62 Overview of association to the network

4.10.3.1. Data link layer configurations

After turned on, a new host conducts IEEE 802.15.4 PAN detection existing around. The PAN detection is conducted by the successive procedures; the host broadcasts a beacon request commands that is defined in [802.15.4] on all available channels out of radio channels defined in [802.15.4] and [T108], a coordinator that receives the command returns a beacon frame as a response, and the new host receives the beacon. Moreover, the new host recognizes a radio channel and PAN ID employed by the coordinator, as results of those procedures. (Step 1)

In case only one PAN is detected, the host moves to the next step as for the PAN. In case several PANs are detected, the host needs to select one PAN in order to move to the next step. PAN selection criteria for the latter case is implementation matter and out of scope of this profile. (Step 2)

The new host conducts association procedures defined in IEEE 802.15.4 to the selected PAN in Step 2. (Step 3)

In case the host fails to associate to the PAN by those association procedures, for example owing to rejection by the coordinator, the host is recommended to retry the procedures from Step 1 or Step 2, where the other network should be tried in Step 2.

4.10.3.2. Security configurations

The new host conducts security configurations after data link layer and network layer configurations. Security technologies employed in the constructed network should be selected according to the application requests. This profile does not describe concrete procedures for security configurations.

4.10.4. Specifications for device/PHY layer/MAC layer in order to realize the recommended usage

Refer to "3.6.2 and 3.6.3."