Wi-SUN module for B-Route, Enhanced HAN

BP35C0-J11 UART IF Specification

This document describes the specifications of the UART IF command of the Wi-SUN module BP35C0-J11.

Caution

- On the firmware
  - With respect to the firmware (hereinafter collectively “Software”) built into BP35C0-J11, agree to the following licensing prior to use.
  - This Software is firmware dedicated to BP35C0-J11. Do not use the firmware for any product other than BP35C0-J11.
  - Do not assign, transfer, sub-license, or lend this Software to any third parties.
  - Reverse engineering, decompilation, disassembly, reproduction, and change of this Software are prohibited.
- On wireless communication
  - Wireless communication may be unstable due to radio wave environment and communication environment, does not guarantee 100 % data transfer, ROHM assumes absolutely no responsibility even if data is missing.
  - UDP does not provide for the arrival of consecutive packets and data arrival is not guaranteed.
  - Please fully verify with customers before installing this product in customer's set and doing full-scale operation.
  - ROHM assumes no responsibility for any damage or malfunction caused by data interception, loss, theft, leakage to a third party.
  - For customers who are verifying points relating to specific communication, please introduce Wi-SUN Enhanced HAN compatible packet capture. As a rule, support for communication-related content is conditional on the capture log being provided.
    Recommended capture: Keysight's PS-X30 W10121A Wi-SUN protocol catcher
    https://www.keysight.com/jp/ja/assets/7018-04443/flyers/5991-4654.pdf
- This document consists of the “j11_uartif_specification” which is copyrighted by ISB Corporation, and ROHM has received permission from ISB Corporation for the publication of this document.

Wi-SUN Enhanced HAN
Plus Route-B Dual Stack
J11 UART IF Specification

First Edition

English

ISB CORPORATION

Notice

1. The contents of this document are the latest at the time of the publication of this document and may be subject to change without notice.
2. ISB Corporation does not guarantee that there are no errors in the information. Even in the event that any damage or loss arising from any and all errors in the information provided in this document is caused to you, ISB Corporation shall not be responsible whatsoever for such errors.
3. ISB Corporation shall not be responsible whatsoever for any and all third-party infringements of patents, copyrights, and other intellectual property rights that were caused in relation to the use of technical information provided with this document. ISB Corporation shall, in accordance with this document, not grant any and all rights based on ISB Corporation's or third party's patents, copyrights, and other intellectual property rights.
4. Reproducing or copying this document, in whole or in part, is strictly prohibited without advance permission of ISB Corporation.

Document Convention

This document uses the following typographical convention:

Convention	Description
Transition To Rewrite Mode	Words in bold with the first letter of each word capitalized indicate command names.

Revision History

Date	Description
August 30, 2019	First English edition of the Japanese original first edition Rev 1 (1.1)
June 1, 2020	Revision of the first English edition

Copyright

Contents

List of Figures

List of Tables

1. Introduction

1.1 Overview

This UART IF Command Specification is used to control wireless modules compliant with the International Wireless Communications Standards: Wi-SUN Profile for ECHONET Lite (hereinafter referred to as the "Wi-SUN") both for Route B and for Enhanced HAN (hereinafter referred to as the "HAN") specified by "Wi-SUN Alliance" (hereinafter referred to as the "Module").

The following diagram shows the configuration of a protocol stack built in the Module.

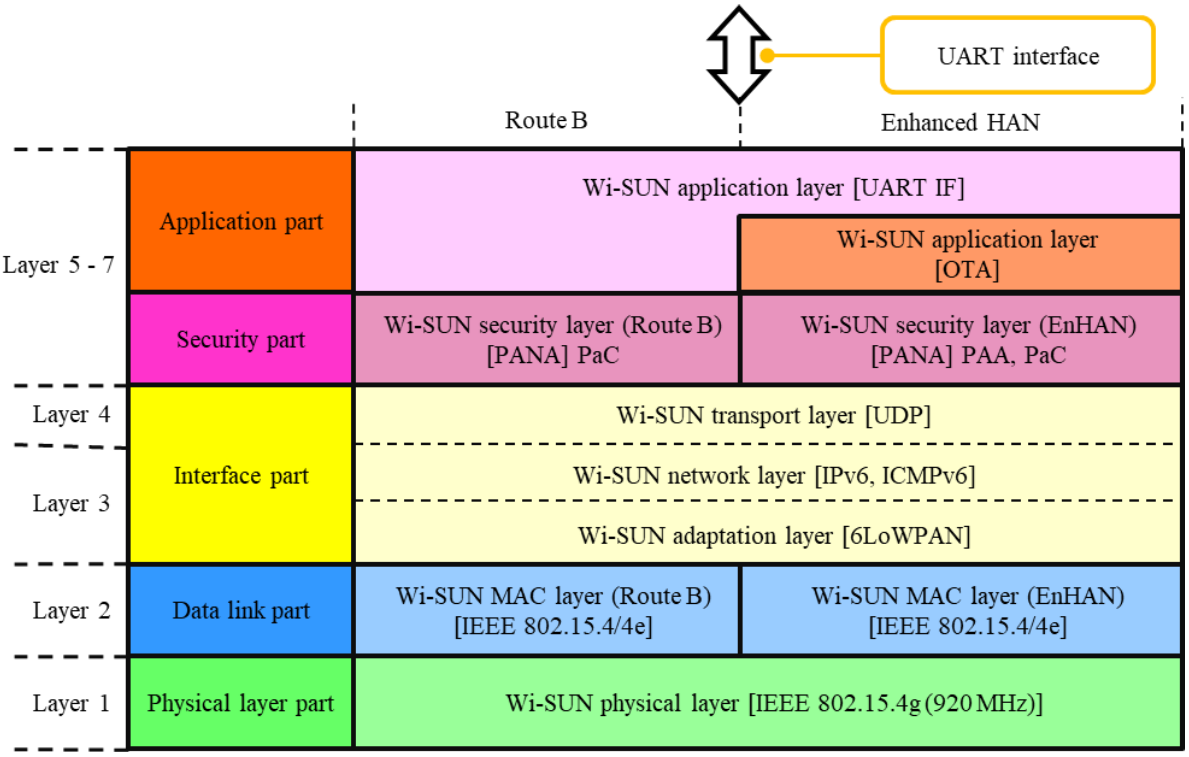
UART interface
Route B
Enhanced HAN
Layer 5 - 7
Application part
Wi-SUN application layer [UART IF]
Wi-SUN application layer [OTA]
Security part
Wi-SUN security layer (Route B) [PANA] PaC
Wi-SUN security layer (EnHAN) [PANA] PAA, PaC
Layer 4
Layer 3
Interface part
Wi-SUN transport layer [UDP]
Wi-SUN network layer [IPv6, ICMPv6]
Wi-SUN adaptation layer [6LoWPAN]
Layer 2
Data link part
Wi-SUN MAC layer (Route B) [IEEE 802.15.4/4e]
Wi-SUN MAC layer (EnHAN) [IEEE 802.15.4/4e]
Layer 1
Physical layer part
Wi-SUN physical layer [IEEE 802.15.4g (920 MHz)]

Fig. 1: Protocol stack configuration

1.2 Terms and definitions

The following table lists terms and definitions used in this document.

Table 1: Terms and definitions

Term	Definition
Route B	Wi-SUN profile for communications between smart meters and HEMS controllers
Enhanced HAN	Wi-SUN profile for communications between HEMS controllers and home electronics
ECHONET Lite	Communication protocols formulated by the ECHONET CONSORTIUM, including control protocols and sensor network protocols used for smart house
NS	Neighbor Solicitation
NA	Neighbor Advertisement
PANA	Protocol for carrying Authentication for Network Access
PAA	PANA Authentication Agent
PaC	PANA Client
EBR	Enhanced Beacon Request
OTA	Over The Air

1.3 Reference documents

Table 2: Reference documents

No.	Document name
1	20160617-Wi-SUN-Echonet-Profile-2v08_clean.pdf
2	Guidelines for Operating HEMS / Smart Meters for Route B (Low-voltage Wattmeter) [Ver. 2.0]
3	Home network communication interface for JJ-300.10 ECHONET Lite (IEEE802.15.4/4g/4e 920 MHz—band Wireless)

2. UART IF commands

UART IF commands are used to control Modules through serial communications.

2.1 Overview

1. UART IF commands handle all data as binary data.
2. UART IF commands are all described in big-endian format.
3. Command types are classified into **Request**, **Response**, and **Notification**.
4. UART IF commands are processed in a single-tasking way.
   Consequently, any other commands received when a UART IF command is executed (before a response to a request is returned) are all discarded to return an error response, except reset request.
5. Each UART IF command is configured of a unique header code, command code, message length, checksum, and data block.
6. The unique code is used to recognize serial data as a UART IF command. The data is discarded until the first 4 bytes correspond to the unique code.
7. The checksum is used to detect errors in serial data.
8. The maximum receive message size of a UART IF command is 1,361 bytes including the header block. (commands defined in this document do not exceed this maximum receive message size.)

2.2 UART IF connection parameters

In order to connect UART IF commands to this Module, use the parameters listed in the table below.

Flow control can be changed after completion of the connection.

For details, refer to §3.2.2.3, "**Change UART Setting**".

Table 3: UART IF connection parameters (values)

Parameter	Value
Baud rate (communication speed)	115,200 bps
Data bit length	8 bit
Parity check	None
Stop bit length	1 bit
Flow control	Disable (variable)

2.3 Command format

A UART IF command is configured of a unique header code, command code, message length, checksum, and data part. The size of the header block is fixed to 12 bytes and that of the data block is variable.

The message length represents a total length of the header block checksum, data block checksum, and data. The minimum message length is 4 bytes used by the header block checksum and data block checksum.

Command header block (12byte)					Command data block (variable)
Unique code (4byte)	Command code (2byte)	Message length (2byte)	Header block checksum (2byte)	Data block checksum (2byte)	Data (variable)

Fig. 2: Command format

Table 4: Command format items

Block	Name	Description	Size
Header block	Unique code	Code used to recognize data as a UART IF command with a unique value	4byte
	Command code	Code used to control the Module	2byte
	Message length	Sum of the length of checksum and that of data block	2byte
	Header block checksum	Error-detecting code	2byte
	Data block checksum		2byte
Data block	Data	Data	Variable

2.4 Unique codes

Unique codes are used to identify serial data as a command.

The unique codes vary with the type of the command code.

Table 5: List of unique codes

Command type	Value
Request command	0xD0EA83FC
Response command	0xD0F9EE5D
Notification command	0xD0F9EE5D

2.5 Command codes

UART IF commands are classified into three types: **Request** command used by user to make a request of a Module, **Response** command used to make a response to the request, and **Notification** command used by the Module to send a notification at any timing.

Table 6: List of command types

Type of command	Overview
Request command	Command used to make a request from user to a Module. The Module processes the **Request** command and returns the result of the processing by using the **Response** command.
Response command	Command used to make a response from the Module to the user.
Notification command	Command used to send a notification from the Module to the user. In cases where the Module makes any status change or receives data, the Module notifies the user of such event at any timing.

2.6 Checksum types

A UART IF command uses two checksums to detect errors. If the checksums do not correspond to each other, the command will return an error response.

If a sum of checksum values exceeds 0xFFFF an overflow will be ignored to take 0x0000 or larger as a checksum value.

Table 7: Types of checksums

Type	Description
Header block checksum	Sum of unique code + command code + message length Example: In cases of **Get MAC Address Request** Calculation formula: (0xD0+0xEA+0x83+FC)+(0x00+0x0E)+(0x00+0x04)=0x034B (unique code)+(**Request** command)+(message length) “0x034B” that is the result of the above calculation is taken as a header block checksum value.
Data block checksum	Sum of all data blocks (excluding checksum portions) Example: In cases where the following values are stored in the data blocks • 0x01,0x05,0x07 Calculation formula: 0x01+0x05+0x07=0x000D “0x000D” that is the result of the above calculation is taken as a data block checksum value.

2.7 Status transition

2.7.1 Module statuses

This section describes Module’s operating statuses. There are three blocks, i.e., whole, HAN, and Route B, which contains a few types of operating statuses, respectively.

Table 8: List of Module statuses

Block	Status
Whole	Not-yet-started status
	Started status
	Rewrite mode status
HAN	Not-yet-started status
	Operating status
	Authentication status
Route B	Not-yet-started status
	Operating status
	Authentication status

2.7.1.1 Whole block status

This section describes the operating statuses of the whole block. The whole block operates in three operating statuses, which make a transition by executing a specific **Request** command.

Table 9: Whole block statuses

Whole block status description	Description
Not-yet-started status	Status in which the Module has completed initiating its operation and **Setup Initial Settings** has not yet been executed
Started status	Status in which **Setup Initial Settings** has been executed and operation mode has been determined
Rewrite mode status	Status in which a boot program used to write firmware is starting up

Note:
It is needed to turn on the power supply again or execute **Reset Hardware** in order to make a transition from the started status to the not-yet-started status.

2.7.1.2 HAN block statuses

This section describes the operating statuses of HAN block. The HAN block operates in three operating statuses, which make a transition by executing a specific **Request** command. In order to make a transition of the operating status of HAN block, the whole block should be in the started status.

Table 10: HAN block statuses

HAN block status description	Description
Not-yet-started status	Status in which the HAN block has not completed **Initiate HAN Operation**
Operating status	Status in which the PAN coordinator is available for MAC connection Status in which the coordinator and end device have succeeded in MAC connection
Authentication status	Status in which the PAN coordinator is available for PANA authentication Status in which the coordinator and end device have succeeded in PANA authentication

2.7.1.3 Route-B block statuses

This section describes the operating statuses of Route-B block. The Route-B block operates in three operating statuses, which make a transition by executing a specific **Request** command. In order to make the status of Route-B block transition to the operating status, the whole block should be in the started status and the HAN block should be in the not-yet-started status.

Table 11: Route-B block statuses

Route-B block status description	Description
Not-yet-started status	Status in which the Route-B block has not completed **Initiate Route-B Operation**
Operating status	Status in which the Route-B block has succeeded in MAC connection
Authentication status	Status in which the Route-B block has succeeded in PANA authentication

2.7.2 Operation modes

This section describes the operation modes of the Module. There are four types of operation modes whose setting can be changed by **Set Initial Settings** (§3.2.2.1).

Table 12: Operation modes

Type of operation mode	Description
PAN coordinator	Mode in which the PAN coordinator serving as the master device of the HAN is put into operation
Coordinator	Mode in which the coordinator serving as the relay device of the HAN is put into operation
End device	Mode in which the end device serving as the slave device of the HAN is put into operation
Dual	Mode in which the end device of the Route B and the PAN coordinator serving as the master device of the HAN are put into operation at a time

2.7.3 State diagram

The following section shows status transition diagram for the Module. Status transition is classified into two types in accordance with the operation mode.

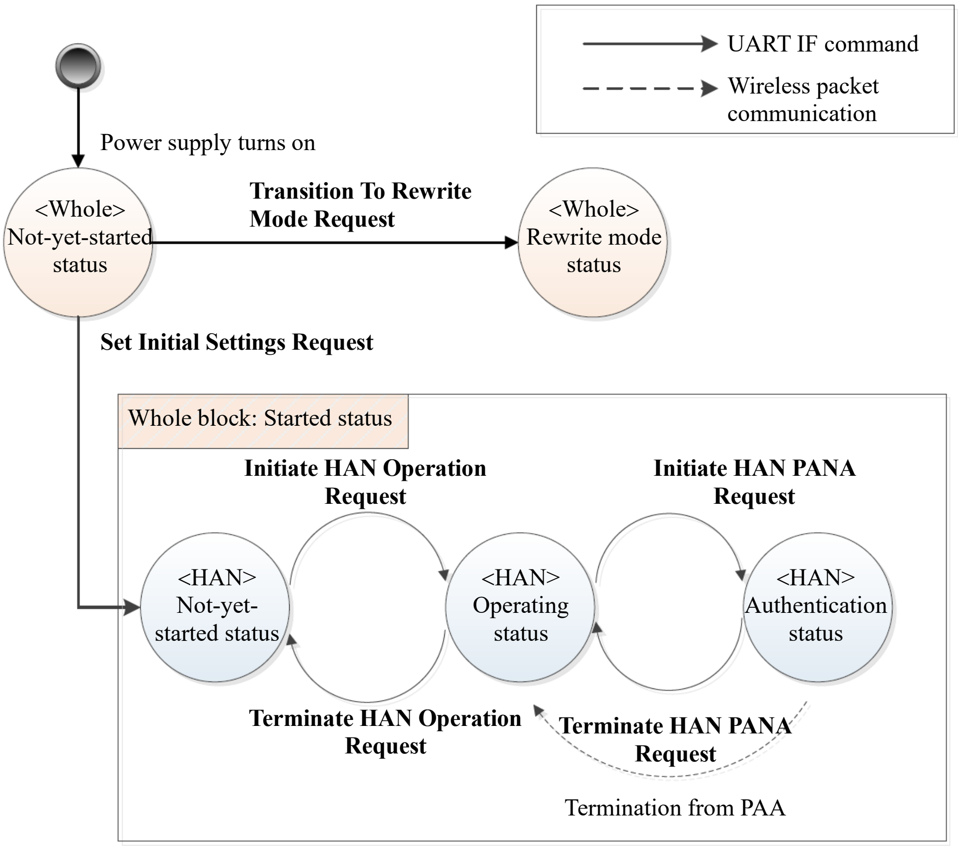
UART IF command
Wireless packet communication
Power supply turns on
<Whole> Not-yet-started status
Transition To Rewrite Mode Request
<Whole> Rewrite mode status
Set Initial Settings Request
Whole block: Started status
Initiate HAN Operation Request
Initiate HAN PANA Request
<HAN> Not-yet-started status
<HAN> Operating status
<HAN> Authentication status
Terminate HAN Operation Request
Terminate HAN PANA Request
Termination from PAA

Fig. 3: Status transition when the operation mode is set to PAN coordinator, coordinator, or end device mode

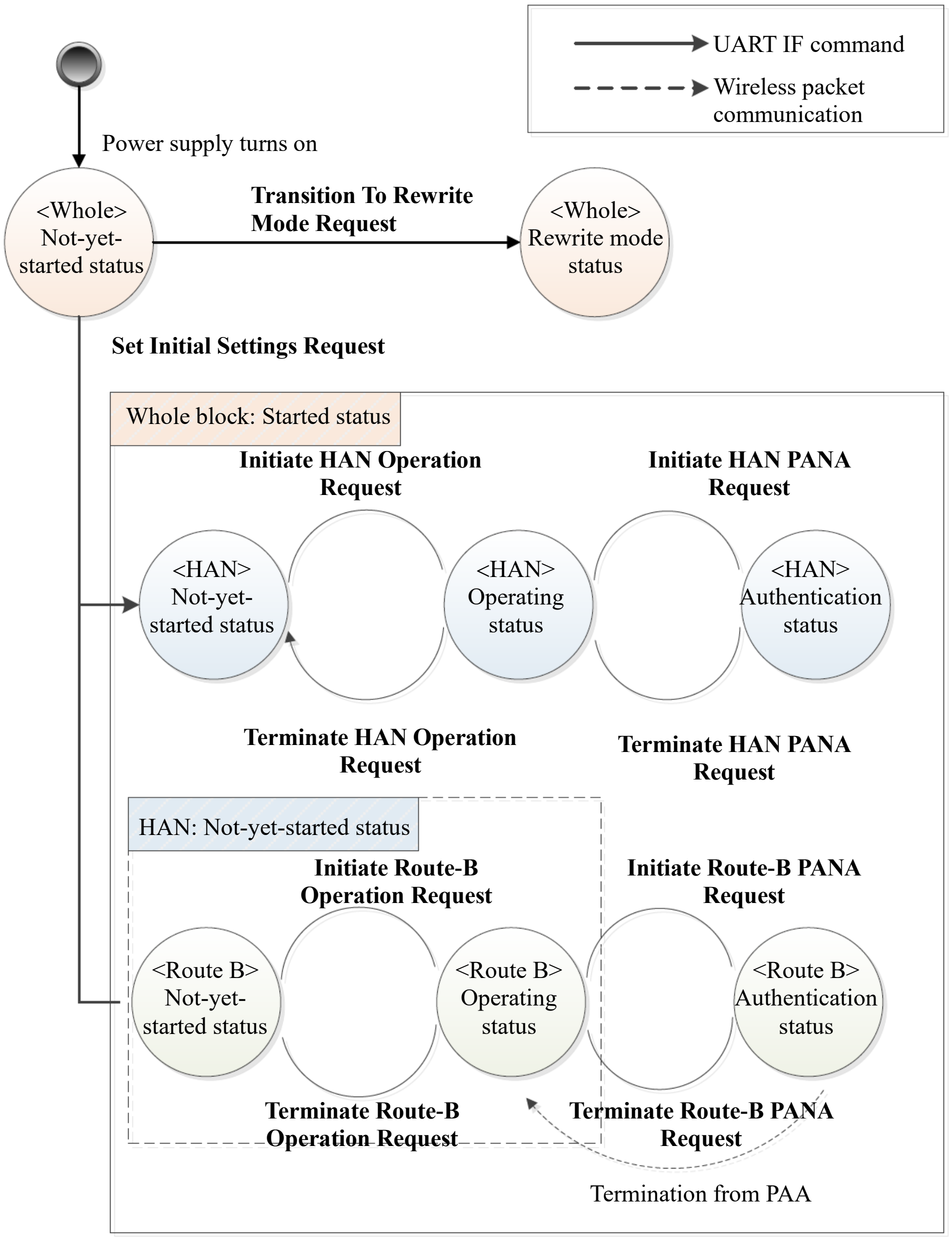
UART IF command
Wireless packet communication
Power supply turns on
<Whole> Not-yet-started status
Transition To Rewrite Mode Request
<Whole> Rewrite mode status
Set Initial Settings Request
Whole block: Started status
Initiate HAN Operation Request
Initiate HAN PANA Request
<HAN> Not-yet-started status
<HAN> Operating status
<HAN> Authentication status
Terminate HAN Operation Request
Terminate HAN PANA Request
HAN: Not-yet-started status
Initiate Route-B Operation Request
Initiate Route-B PANA Request
<Route B> Not-yet-started status
<Route B> Operating status
<Route B> Authentication status
Terminate Route-B Operation Request
Terminate Route-B PANA Request
Termination from PAA

Fig. 4: Status transition when the operation mode is set to Dual mode

2.8 Executability of commands

The UART IF commands vary in their executability with the Module status and operation mode. If the command is not executable, it will return an error response.

The following tables shows executable commands with a checkmark (✓) and unexecutable commands with NA according to the Module status and operation mode.

2.8.1 Operation mode: PAN coordinator

2.8.1.1 Common commands

Table 13: List of executability of common commands when the operation mode is set to PAN coordinator

Command code	Command name	Whole block status	Not-yet-started	Started		
		HAN status	-	Not-yet-started	Operating	Authentication
0x0001	**Get Status**		✓	✓	✓	✓
0x0007	**Get UDP Port Open Status**		NA	NA	✓	✓
0x0009	**Get IP Address**		✓	✓	✓	✓
0x000E	**Get MAC Address**		✓	✓	✓	✓
0x0011	**Get Connection Status**		✓	✓	✓	✓
0x0100	**Get Terminal Information**		✓	✓	✓	✓
0x0102	**Get Neighbor Discovery Setting**		✓	✓	✓	✓
0x0107	**Get Initial Settings**		✓	✓	✓	✓
0x010B	**Get UART Setting**		✓	✓	✓	✓
0x005F	**Set Initial Settings**		✓	✓	NA	NA
0x0101	**Set Neighbor Discovery**		✓	✓	NA	NA
0x010A	**Change UART Setting**		✓	✓	NA	NA
0x0005	**Open UDP Port**		NA	NA	✓	✓
0x0006	**Close UDP Port**		NA	NA	✓	✓
0x0008	**Transmit Data**		NA	NA	✓	✓
0x0051	**Execute Active Scan**		NA	✓	✓	✓
0x00D1	**Transmit To Ping**		NA	NA	✓	✓
0x00DB	**Execute ED Scan**		NA	✓	✓	✓
0x006B	**Get Version Information**		✓	✓	✓	✓
0x00D9	**Reset Hardware**		✓	✓	✓	✓
0x00F0	**Transition To Rewrite Mode**		✓	NA	NA	NA

Note:
Since the boot program runs in the rewrite mode status, commands listed in this document are not acknowledged.

2.8.1.2 HAN commands

Table 14: List of executability of HAN commands when the operation mode is set to PAN coordinator

Command code	Command name	Whole block status	Not-yet-started	Started		
		HAN status	-	Not-yet-started	Operating	Authentication
0x0013	**Get HAN Group Key Validity Period**		NA	✓	✓	✓
0x0026	**Get HAN Acceptance/Connection Mode Status**		NA	NA	✓	✓
0x0028	**Get HAN Group Key**		NA	NA	NA	✓
0x002D	**Get HAN PANA Authentication Information**		NA	✓	✓	✓
0x0067	**Get Setting Of HAN Sleep Device PANA Retransmission Interval** (Note)		NA	NA	NA	✓
0x0104	**Get Setting Of Number Of Times Of Retransmissions Of HAN PaC PANA Authentication Initiation Message**		NA	NA	NA	NA
0x0106	**Get Setting Of Number Of Times Of Retransmissions Of HAN PANA Authentication Message**		NA	✓	✓	✓
0x0109	**Get Setting Of Waiting Time For Completion Of Updating HAN Group Key**		NA	NA	NA	NA
0x0012	**Set HAN Group Key Validity Period**		NA	✓	✓	NA
0x002C	**Set HAN PANA Authentication Information**		NA	✓	✓	✓
0x002E	**Delete HAN PANA Authentication Information Setting**		NA	✓	✓	✓
0x0066	**Set HAN Sleep Device PANA Retransmission Interval**		NA	NA	NA	NA
0x0103	**Set Number Of Times Of Retransmissions Of HAN PaC PANA Authentication Initiation Message**		NA	NA	NA	NA
0x0105	**Set Number Of Times Of Retransmissions Of HAN PANA Authentication Message**		NA	✓	✓	NA
0x0108	**Set Waiting Time For Completion Of Updating HAN Group Key**		NA	NA	NA	NA
0x000A	**Initiate HAN Operation**		NA	✓	NA	NA
0x000B	**Terminate HAN Operation**		NA	NA	✓	NA
0x0025	**Switch HAN Acceptance Connection Mode**		NA	NA	✓	✓
0x0029	**Distribute HAN Group Key**		NA	NA	NA	✓
0x002A	**Check HAN Group Key Update**		NA	NA	NA	NA
0x002B	**Re-authenticate HAN PANA**		NA	NA	NA	✓
0x003A	**Initiate HAN PANA**		NA	NA	✓	NA
0x003B	**Terminate HAN PANA**		NA	NA	NA	✓
0x0061	**Transmit HAN Poll Request**		NA	NA	NA	NA
0x0069	**HAN Purge Request** (Note)		NA	NA	✓	✓
0x006A	**Delete HAN Device From List**		NA	NA	✓	✓
0x00D3	**Disconnect HAN**		NA	NA	✓	✓
0x00DA	**HAN Deep Sleep Request**		NA	NA	NA	NA

Note: Executable only when HAN sleep function setting is enabled.

2.8.1.3 OTA update commands

Table 15: List of executability of OTA update commands when the operation mode is set to PAN coordinator

Command code	Command name	Whole block status	Not-yet-started	Started		
		HAN status	-	Not-yet-started	Operating	Authentication
0x0201	**Initiate OTA Client**		NA	NA	NA	✓
0x0202	**Terminate OTA Client**		NA	NA	NA	✓

2.8.2 Operation mode: coordinator

2.8.2.1 Common commands

The executability of the common commands when the operation mode is set to coordinator is the same as that listed in Table 13: List of executability of common commands when the operation mode is set to PAN coordinator.

2.8.2.2 HAN commands

Table 16: List of Executability of HAN commands when the operation mode is set to coordinator

Command code	Command name	Whole block status	Not-yet-started	Started		
		HAN status	-	Not-yet-started	Operating	Authenti-cation
0x0013	**Get HAN Group Key Validity Period**		NA	NA	NA	NA
0x0026	**Get HAN Acceptance/Connection Mode Status**		NA	NA	✓	✓
0x0028	**Get HAN Group Key**		NA	NA	NA	✓
0x002D	**Get HAN PANA Authentication Information**		NA	✓	✓	✓
0x0067	**Get Setting Of HAN Sleep Equipment PANA Retransmission Intervals**		NA	NA	NA	NA
0x0104	**Get Setting Of Number Of Times Of HAN PaC PANA Authentication Initiation Message Retransmission**		NA	✓	✓	✓
0x0106	**Get Setting Of Number Of Times Of HAN PANA Authentication Message Retransmission**		NA	✓	✓	✓
0x0109	**Get Setting Of Waiting Time For Completion Of Updating HAN Group Key**		NA	✓	✓	✓
0x0012	**Set HAN Group Key Validity Period**		NA	NA	NA	NA
0x002C	**Set HAN PANA Authentication Information**		NA	✓	✓	✓
0x002E	**Delete HAN PANA Authentication Information Setting**		NA	✓	✓	✓
0x0066	**Set HAN Sleep Equipment PANA Retransmission Intervals**		NA	NA	NA	NA
0x0103	**Set Number Of Times Of HAN PaC PANA Authentication Initiation Message Retransmission**		NA	✓	✓	NA
0x0105	**Set Number Of Times Of HAN PANA Authentication Message Retransmission**		NA	✓	✓	NA
0x0108	**Set Waiting Time For Completion Of Updating HAN Group Key**		NA	✓	✓	NA
0x000A	**Initiate HAN Operation**		NA	✓	NA	NA
0x000B	**Terminate HAN Operation**		NA	NA	✓	NA
0x0025	**Switch HAN Acceptance Connection Mode**		NA	NA	✓	✓
0x0029	**Distribute HAN Group Key**		NA	NA	NA	NA
0x002A	**Check HAN Group Key Update**		NA	NA	NA	✓
0x002B	**Re-authenticate HAN PANA**		NA	NA	NA	NA
0x003A	**Initiate HAN PANA**		NA	NA	✓	NA
0x003B	**Terminate HAN PANA**		NA	NA	NA	✓
0x0061	**Transmit HAN Poll Request**		NA	NA	NA	NA
0x0069	**HAN Purge Request** (Note)		NA	NA	✓	✓
0x006A	**Delete HAN Device From List**		NA	NA	✓	✓
0x00D3	**Disconnect HAN**		NA	NA	NA	NA
0x00DA	**HAN Deep Sleep Request**		NA	NA	NA	NA

Note:
Executable only when HAN sleep function setting is enabled.

2.8.2.3 OTA update commands

The executability of the OTA Update commands when the operation mode is set to coordinator is the same as that listed in Table 15: List of executability of OTA update commands
when the operation mode is set to PAN coordinator.

2.8.3 Operation mode: end device

2.8.3.1 Common commands

The executability of the common commands when the operation mode is set to end device is the same as that listed in Table 13: List of executability of common commands when the operation mode is set to PAN coordinator.

2.8.3.2 HAN commands

Table 17: List of executability of HAN commands when the operation mode is set to end device

Command code	Command name Whole block status	Not-yet-started	Started		
	HAN status	-	Not-yet-started	Operating	Authenti-cation
0x0013	**Get HAN Group Key Validity Period**	NA	NA	NA	NA
0x0026	**Get HAN Acceptance/Connection Mode Status**	NA	NA	NA	NA
0x0028	**Get HAN Group Key**	NA	NA	NA	✓
0x002D	**Get HAN PANA Authentication Information**	NA	✓	✓	✓
0x0067	**Get Setting Of HAN Sleep Equipment PANA Retransmission Intervals** (Note)	NA	NA	NA	✓
0x0104	**Get Setting Of Number Of Times Of HAN PaC PANA Authentication Initiation Message Retransmission**	NA	✓	✓	✓
0x0106	**Get Setting Of Number Of Times Of HAN PANA Authentication Message Retransmission**	NA	✓	✓	✓
0x0109	**Get Setting Of Waiting Time For Completion Of Updating HAN Group Key**	NA	✓	✓	✓
0x0012	**Set HAN Group Key Validity Period**	NA	NA	NA	NA
0x002C	**Set HAN PANA Authentication Information**	NA	✓	✓	✓
0x002E	**Delete HAN PANA Authentication Information Setting**	NA	✓	✓	✓
0x0066	**Set HAN Sleep Equipment PANA Retransmission Intervals** (Note)	NA	NA	NA	✓
0x0103	**Set Number Of Times Of HAN PaC PANA Authentication Initiation Message Retransmission**	NA	✓	✓	NA
0x0105	**Set Number Of Times Of HAN PANA Authentication Message Retransmission**	NA	✓	✓	NA
0x0108	**Set Waiting Time For Completion Of Updating HAN Group Key**	NA	✓	✓	NA
0x000A	**Initiate HAN Operation**	NA	✓	NA	NA
0x000B	**Terminate HAN Operation**	NA	NA	✓	NA
0x0025	**Switch HAN Acceptance Connection Mode**	NA	NA	NA	NA
0x0029	**Distribute HAN Group Key**	NA	NA	NA	NA
0x002A	**Check HAN Group Key Update**	NA	NA	NA	✓
0x002B	**Re-authenticate HAN PANA**	NA	NA	NA	NA
0x003A	**Initiate HAN PANA**	NA	NA	✓	NA
0x003B	**Terminate HAN PANA**	NA	NA	NA	✓
0x0061	**Transmit HAN Poll Request** (Note)	NA	NA	✓	✓
0x0069	**HAN Purge Request** (Note)	NA	NA	NA	NA
0x006A	**Delete HAN Device From List**	NA	NA	NA	NA
0x00D3	**Disconnect HAN**	NA	NA	NA	NA
0x00DA	**HAN Deep Sleep Request**	NA	✓	✓	✓

Note:
Executable only when HAN sleep function setting is enabled.

2.8.3.3 OTA update commands

The executability of the OTA update commands when the operation mode is set to end device is the same as that listed in Table 15: List of executability of OTA update commands when the operation mode is set to PAN coordinator.

2.8.4 Operation mode: Dual

2.8.4.1 Common commands

Table 18: List of executability of common commands when the operation mode is set to Dual

Command code	Command name	Whole block status	Not-yet-started	Started		
		HAN status	-	Not-yet-started	Operating	Authentication
		Operating status of Route B	-	Not-yet-started	Operating	Authentication
0x0001	**Get Status**		✓	✓	✓	✓
0x0007	**Get UDP Port Open State**		NA	NA	✓ (Note 1)	✓ (Note 1)
0x0009	**Get IP Address**		✓	✓	✓	✓
0x000E	**Get MAC Address**		✓	✓	✓	✓
0x0011	**Get Connection Status**		✓	✓	✓	✓
0x0100	**Get Terminal Information**		✓	✓	✓	✓
0x0102	**Get Neighbor Discovery Setting**		✓	✓	✓	✓
0x0107	**Get Initial Setting**		✓	✓	✓	✓
0x010B	**Get UART Setting**		✓	✓	✓	✓
0x005F	**Set Initial Settings**		✓	✓	NA	NA
0x0101	**Set Neighbor Discovery**		✓	✓	NA	NA
0x010A	**Change UART Setting**		✓	✓	NA	NA
0x0005	**Open UDP Port**		NA	NA	✓ (Note 1)	✓ (Note 1)
0x0006	**Close UDP Port**		NA	NA	✓ (Note 1)	✓ (Note 1)
0x0008	**Transmit Data**		NA	NA	✓ (Note 1)	✓ (Note 1)
0x0051	**Execute Active Scan**		NA	✓	✓	✓
0x00D1	**Transmit To Ping**		NA	NA	✓ (Note 1)	✓ (Note 1)
0x00DB	**Execute ED Scan**		NA	✓	✓	✓
0x006B	**Get Version Information**		✓	✓	✓	✓
0x00D9	**Reset Hardware**		✓	✓	✓	✓
0x00F0	**Transition To Rewrite Mode** (Note 2)		✓	NA	NA	NA

Notes:

1. Executable when the HAN or Route B status is set to the operating status or authentication status.
2. Since the boot program runs in the rewrite mode status, commands listed in this document are not acknowledged.

2.8.4.2 HAN commands

The executability of the HAN commands when the operation mode is set to Dual is the same as that listed in Table 14: List of executability of HAN commands when the operation mode is set to PAN coordinator.

2.8.4.3 OTA update commands

The executability of the OTA update commands when the operation mode is set to Dual is the same as that listed in Table 15: List of executability of OTA update commands when the operation mode is set to PAN coordinator.

2.8.4.4 Route B commands

Table 19: List of executability of Route B commands when the operation mode is set to Dual

Command code	Command name	Whole block status	Not-yet-started	Started		
		Operating status of Route B	-	Not-yet-started	Operating	Authentic ation
0x0059	**Get Route-B Encryption Key**		NA	NA	NA	✓
0x005E	**Get Route-B PAN ID**		NA	NA	✓	✓
0x0054	**Set Route-B PANA Authentication Information**		NA	✓	✓	NA
0x0053	**Initiate Route-B Operation**		NA	✓ (Note)	NA	NA
0x0056	**Initiate Route-B PANA**		NA	NA	✓	NA
0x0057	**Terminate Route-B PANA**		NA	NA	NA	✓
0x0058	**Terminate Route-B Operation**		NA	NA	✓	NA
0x00D2	**Initiate Route-B PANA Re-authentication**		NA	NA	NA	✓

Note:

The HAN status is also required not to have started.

2.9 Module setting values

The following describes values settable to the Module and default values.

Values set to the Module will be reset to default values when the power supply is turned off or **Reset Hardware** command is executed.

Hold the values set to the Module in the upper-level application as appropriate, and then set the values again after turning on the power supply.

When any of the values is set outside the valid range, an error response will be returned as stated in §2.10.5, “Invalid command parameters”.

2.9.1 Common settings

2.9.1.1 Initial settings

Table 20: Initial settings

Name	Valid range	Description	Default value
Operation mode	0x01 to 0x03, 0x05	0x01: PAN coordinator (HAN) 0x02: Coordinator (HAN) 0x03: End device (HAN) 0x05: Dual (Route B and HAN)	0xFF (255)
HAN sleep function setting	0x00 to 0x01	0x00: Disabled 0x01: Enabled	0x00 (0)
Channel	0x04 to 0x11	Channel numbers based on IEEE802.15.4g For details, see Table 21: Channels.	0xFF (255)
Transmission power	0x00 to 0x02	0x00: 20 mW 0x01: 10 mW 0x02: 1 mW	0x00 (0)

Table 21: Channels

Channel number	Center frequency (MHz)
4	922.5
5	922.9
6	923.3
7	923.7
8	924.1
9	924.5
10	924.9
11	925.3
12	925.7
13	926.1
14	926.5
15	926.9
16	927.3
17	927.7

2.9.1.1.1 Example of initial setting

The following shows examples of parameter settings by HAN configuration.

Set any value to the channel and the transmission power parameters.

Sleep-enabled (Note 1) Dual, PAN coordinator, and coordinator allow connection with not only sleep-enabled coordinators and end devices, but also sleep-disabled coordinators and end devices.

Sleep-disabled (Note 2) Dual, PAN coordinator, and coordinator do not allow connection with sleep-enabled coordinators and end devices.

Notes:

1. Sleep-enabled means that the HAN sleep function setting is enabled.
2. Sleep-disabled means that the HAN sleep function setting is disabled.

Table 22: Sleep-disabled

Name	PAN coordinator / Dual	Coordinator (sleep-disabled)	End device (sleep-disabled)
Operation mode	0x01/0x05	0x02	0x03
HAN sleep function setting	0x00	0x00	0x00

Table 23: Sleep-enabled

Name	PAN coordinator / Dual	Coordinator (sleep-enabled)	End device (sleep-enabled)
Operation mode	0x01/0x05	0x02	0x03
HAN sleep function setting	0x01	0x01	0x01

Table 24: Sleep-disabled only when the operation mode is set to end device

Name	PAN coordinator / Dual	Coordinator (sleep-enabled)	End device (sleep-disabled)
Operation mode	0x01/0x05	0x02	0x03
HAN sleep function setting	0x00	0x01	0x00

2.9.1.2 Neighbor Discovery setting

Neighbor Solicitation setting in IPv6 Neighbor Discovery is described below.

Table 25: Neighbor Discovery setting

Name	Valid range	Description	Default value
Neighbor Solicitation transmission	0x00 to 0x01	Changes the IPv6 address solution method. When this parameter is set to disabled, an IPv6 address will be solved by transmitting and receiving a Beacon in the MAC layer. When it is set to enabled, an IPv6 address will be solved by using the Neighbor Discovery function. 0x00: Disabled 0x01: Enabled	0x00 (0)

2.9.2 HAN settings

2.9.2.1 HAN group key validity period settings

The validity period of HAN group key means that of the group key (encryption key) managed by PANA PAA.

Table 26: HAN group key validity period settings

Name	Valid range	Description	Default value
Minimum validity period	0x00000000 to 0x00000E10	Minimum validity period (in seconds) of the group key in the range of 0 sec. to 3,600 sec. After a group key is generated, the same key is continually used until the set minimum validity period expires. In other words, no key is regenerated during the set period.	0x00000E10 (3600)
Maximum validity period	0x00015180 to 0x00278D00	Maximum validity period (in seconds) of the group key in the range of 86,400 sec. to 2,592,000 sec. (i.e., 1 day to 30 days). When this set validity period expires, a group key is regenerated.	0x00278D00 (2592000)

2.9.2.2 HAN PANA authentication information settings

Setting of information used in PANA authentication for HAN is described below.

When the operation mode is set to PAN coordinator, set the MAC address and password of the coordinator and the end device to accept connection.

When the operation mode is set to coordinator or end device, set only the password.

Table 27: HAN PANA authentication information settings

Name	Valid range	Description	Default value
MAC address	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	When the operation mode is set to PAN coordinator, the set MAC address is set to PANA authentication information. When the operation mode is set to coordinator or end device, no MAC address setting is needed.	-
Password	String containing 16 ASCII characters in the range of “0 to 9”, “a to z”, and “A to Z”.	Lower-case letters (“a” to “z”) are converted to upper-case letters (“A” to “Z”).	-

2.9.2.3 HAN sleep device PANA retransmission interval settings

The following describes setting of a retransmission interval for PANA message that is used between an end device to which HAN sleep function setting is enabled and the PAN coordinator.

If a request for interval setting is made from the end device to which HAN sleep function setting is enabled to the PAN coordinator and a value specified as the result of the request falls outside the allowable range, the PAN coordinator will return a value that falls within the allowable range.

The allowable range for the PAN coordinator in this Module

Initial retransmission interval: 3 sec

Maximum retransmission interval: 600 sec

Table 28: HAN sleep device PANA retransmission interval settings

Name	Valid range	Description	Default value
Initial retransmission interval	0x0003 to 0x0258	Initial retransmission interval (in seconds) for PANA message in the range of 3 sec. to 600 sec. No value larger than the maximum retransmission interval can be set.	0x0003 (3)
Maximum retransmission interval	0x0003 to 0x0258	Maximum retransmission interval (in seconds) for PANA message in the range of 3 sec. to 600 sec. No value smaller than the initial retransmission interval can be set.	0x001E (30)

2.9.2.4 Setting of number of times of retransmissions of HAN PaC PANA authentication initiation message

The following describes setting of the number of times of the retransmissions of a PANA-Client-Initiation (PCI) message that is an authentication initiation message used by the PaC of PANA.

Table 29: Setting of number of times of retransmissions of HAN PaC PANA authentication initiation message

Name	Valid range	Description	Default value
Number of times of retransmissions of PANA authentication initiation message	0x00 to 0x0A	Number of times of the retransmissions of a PANA-Client-Initiation (PCI) message in the range of 0 to 10.	0x04 (4)

2.9.2.5 Setting of number of times of retransmissions of HAN PANA authentication message

The following describes setting of the number of times of the retransmissions of packets of PANA-Auth-Request (PAR), PANA-Termination-Request (PTR), and PANA-Notification-Request (PNR) that are authentication messages used by PANA.

Table 30: Setting of number of times of retransmissions of HAN PANA authentication message

Name	Valid range	Description	Default value
Number of times of retransmissions of PANA authentication message	0x00 to 0x0A	Number of times of the retransmissions of PANA-Auth-Request (PAR), PANA-Termination-Request (PTR), and PANA-Notification-Request (PNR) in the range of 0 to 10.	0x01 (1)

2.9.2.6 Setting of waiting time for completion of updating HAN group key

The following describes setting of a period of time for PaC to wait for the completion of updating the HAN group key when PAA distributes this key (push).

Table 31: Setting of waiting time for completion of updating HAN group key

Name	Valid range	Description	Default value
Waiting time for completion of updating group key	0x012C to 0xFFFF	Waiting time (in seconds) for completion of updating group key in the range of 300 sec. to 65,535 sec. Note: A period of time from transmission from PNA to reception by MLE	0x012C (300)

2.9.3 Route B setting

2.9.3.1 Route-B PANA authentication information settings

The following describes setting of ID and password used for PANA authentication for Route B.

Table 32: Route-B PANA authentication information settings

Name	Valid range	Description	Default value
Route-B authentication ID	String containing 32 ASCII characters in the range of “0 to 9” and “A to F”.	Authentication ID for Route B provided by an electric power company, etc.	-
Password	String containing 12 ASCII characters in the range of “0 to 9”, “a to z”, and “A to Z”.	Lower-case letters (“a” to “z”) are converted to upper-case letters (“A” to “Z”).	-

2.10 Cautions for UART IF commands

The following section describes cautions in using UART IF commands.

2.10.1 Message length in excess of the maximum receive message size

The maximum receive message size of a UART IF command is 1,361 bytes including the header block.

If a message length or data block in excess of the maximum receive message size is set, the command will return an error response to discard all data received.

2.10.2 Size of data block in excess of message length

If data in the data block is set longer than a specified message length, a portion up to the data block set to the message length will be handled as a command to discard all of remaining data blocks.

Example:

Message length: 7 bytes

Receive message size of data block: 20 bytes

Result: The data block up to 7 bytes is handled as a command to discard 13 bytes of remaining data.

2.10.3 Data in the data block shorter than message length

If data in the data block is set shorter than a specified message length, the command will wait to receive the next data for a period of one second. If the command receives the next data within a period of one second, it will continue waiting to receive the next data for a period of another one second. When the waiting time is exceeded, it will discard data to return an error response.

Example:

Message length: 20 bytes

Receive message size of data block: 7 bytes

Result: Since 13 bytes of data remain, the command waits to receive the next data for a period of one second and, when the waiting time is exceeded, it will discard the remaining data.

2.10.4 Reception of another command when a command is being executed

If any other command is received when a UART IF command is executed in the Module, an error response will be returned. In such cases, after completion of internal processing, execute the UART IF command again.

- If another request is made while a command is being executed to respond to a request,
  wait until a **Response** command is received, and then execute a **Request** command.
- If a **Request** command is received while internal processing is being executed to transmit a **Notification** command,
  receive the **Notification** command, and then execute the **Request** command again.

2.10.5 Invalid command parameters

If the parameter of a **Request** command is set to a value not less than or less than the valid range specified in §2.9, “Module setting values”, an error response will be returned to discard all data received.

2.10.6 Invalid unique code

If no valid unique code can be detected, all data received will be discarded and no **Response** command will be returned.

When a valid unique code is detected, it will be processed as data.

2.10.7 Invalid command code

If an invalid command code is received, an error response will be returned by using 0xFFFF for the command code of a **Response** command to discard all data received.

2.10.8 Invalid header block checksum

If an invalid header block checksum occurs, an error response will be returned by using 0x2FFF for the command code of a **Response** command to discard all data received.

2.10.9 Invalid data block checksum

If an invalid data block checksum occurs, an error response will be returned to discard all data received.

3. Command specification

3.1 List of commands

Table 33: List of commands

Major category	Message classification	Command name	Command type		
			Request	Response	Notification
Common	Get	**Get Status**	0x0001	0x2001	
		Get UDP Port Open Status	0x0007	0x2007	
		Get IP Address	0x0009	0x2009	
		Get MAC Address	0x000E	0x200E	
		Get Connection Status	0x0011	0x2011	
		Get Terminal Information	0x0100	0x2100	
		Get Neighbor Discovery Setting	0x0102	0x2102	
		Get Initial Settings	0x0107	0x2107	
		Get UART Setting	0x010B	0x210B	
	Set	**Set Initial Settings**	0x005F	0x205F	
		Set Neighbor Discovery	0x0101	0x2101	
		Change UART Setting	0x010A	0x210A	
	Operation	**Open UDP Port**	0x0005	0x2005	
		Close UDP Port	0x0006	0x2006	
		Transmit Data	0x0008	0x2008	
		Execute Active Scan	0x0051	0x2051	0x4051
		Transmit To Ping	0x00D1	0x20D1	0x60D1
		Execute ED Scan	0x00DB	0x20DB	
		Notify Data Reception			0x6018
		Notify Startup Completion			0x6019
		Notify Connection Status Change			0x601A
		Notify PANA Authentication Result			0x6028
		Notify Packet Reception Failure			0x6038
	Other	**Get Version Information**	0x006B	0x206B	
		Reset Hardware	0x00D9		
		Transition To Rewrite Mode	0x00F0	0x20F0	

Table 33: List of commands (continued)

Major category	Message classification	Command name	Command type		
			Request	Response	Notification
HAN	Get	**Get HAN Group Key Validity Period**	0x0013	0x2013	
		Get HAN Acceptance/Connection Mode Status	0x0026	0x2026	
		Get HAN Group Key	0x0028	0x2028	
		Get HAN PANA Authentication Information	0x002D	0x202D	
		Get Setting Of HAN Sleep Device PANA Retransmission Interval	0x0067	0x2067G	
		Get Setting Of Number Of Times Of Retransmissions Of HAN PaC PANA Authentication Initiation Message	0x0104	0x2104	
		Get Setting Of Number Of Times Of Retransmissions Of HAN PANA Authentication Message	0x0106	0x2106	
		Get Setting Of Waiting Time For Completion Of Updating HAN Group Key	0x0109	0x2109	
	Set	**Set HAN Group Key Validity Period**	0x0012	0x2012	
		Set HAN PANA Authentication Information	0x002C	0x202C	
		Delete HAN PANA Authentication Information Setting	0x002E	0x202E	
		Set HAN Sleep Device PANA Retransmission Interval	0x0066	0x2066	
		Set Number Of Times Of Retransmissions Of HAN PaC PANA Authentication Initiation Message	0x0103	0x2103	
		Set Number Of Times Of Retransmissions Of HAN PANA Authentication Message	0x0105	0x2105	
		Set Waiting Time For Completion Of Updating HAN Group Key	0x0108	0x2108	

Table 33: List of commands (continued)

Major category	Message classification	Command name	Command type		
			Request	Response	Notification
HAN	Operation	**Initiate HAN Operation**	0x000A	0x200A	
		Terminate HAN Operation	0x000B	0x200B	
		Switch HAN Acceptance Connection Mode	0x0025	0x2025	
		Distribute HAN Group Key	0x0029	0x2029	
		Check HAN Group Key Update	0x002A	0x202A	
		Re-authenticate HAN PANA	0x002B	0x202B	
		Initiate HAN PANA	0x003A	0x203A	
		Terminate HAN PANA	0x003B	0x203B	
		Transmit HAN Poll Request	0x0061	0x2061	
		HAN Purge Request	0x0069	0x2069	
		Delete HAN Device From List	0x006A	0x206A	
		Disconnect HAN	0x00D3	0x20D3	
		HAN Deep Sleep Request	0x00DA	0x20DA	0x60DA
		Notify HAN Acceptance Connection Mode Change			0x6023
		Notify HAN Group Key Distribution Results			0x6026
		Notify HAN Group Key Updating Check Results			0x6027
		Notify HAN Group Key Distribution Complete			0x6029
		Notify Setting Of HAN Sleep Device PANA Retransmission Interval			0x6030
		Notify HAN Indirect Queue Discard			0x6036
		Notify HAN Indirect Queue Transmission			0x6037
		Notify HAN Relay Failure			0x6039

Table 33: List of commands (continued)

Major category	Message classification	Command name	Command type		
			Request	Response	Notification
Route B	Get	**Get Route-B Encryption Key**	0x0059	0x2059	
		Get Route-B PAN ID	0x005E	0x205E	
	Set	**Set Route-B PANA Authentication Information**	0x0054	0x2054	
	Operation	**Initiate Route-B Operation**	0x0053	0x2053	
		Initiate Route-B PANA	0x0056	0x2056	
		Terminate Route-B PANA	0x0057	0x2057	
		Terminate Route-B Operation	0x0058	0x2058	
		Initiate Route-B PANA Re-authentication	0x00D2	0x20D2	
OTA update	Operation	**Initiate OTA Client**	0x0201	0x2201	
		Terminate OTA Client	0x0202	0x2202	
		Notify OTA Operation Initiation			0x6033
		Notify OTA Operation Termination			0x6034

Notes:

- 0xFFFF is used as an error response code, except for cases where the command code is any code other than Request command. See also §2.10.7, “Invalid command code”.
- 0x2FFF is used as an error response code for cases where the command code cannot be determined. See also §2.10.8, “Invalid header block checksum”.

3.2 Common commands

3.2.1 Request/Response commands (get)

Only when a response to a **Request** command (get) results in success, it will give subsequent parameter(s) after the response result parameter in the respective lists of response command parameters described below.

3.2.1.1 Get Status

Request command	0x0001	Response command	0x2001
Function description			
To get the operating status of the Module itself. For gettable statuses, refer to information in §2.7.1, "Module statuses".			

3.2.1.1.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.1.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Whole block statuses	1	0x02 to 0x03	0x02: Not-yet-started 0x03: Started
Route-B block statuses	1	0x01 to 0x03	0x01: Not-yet-started 0x02: Operating 0x03: Authentication
HAN block statuses	1	0x01 to 0x03	0x01: Not-yet-started 0x02: Operating 0x03: Authentication

3.2.1.2 Get UDP Port Open Status

Request command	0x0007	Response command	0x2007
Function description			
To get a list of UDP ports that were opened by executing **Open UDP Port** (§3.2.3.1). It is not available to get the following port numbers used by the system: • 716 (used by PANA); • 19788 (used by MLE).			

3.2.1.2.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.2.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Number of opened UDP ports	1	0x00 to 0x0A	UDP port number is repeated by the set number of opened UDP ports.
UDP port number	2 x number of opened UDP ports	0x0001 to 0xFFFF	Opened UDP port number Note: When the number of opened UDP ports is zero (0), no UDP port number will be given.

3.2.1.3 Get IP Address

Request command	0x0009	Response command	0x2009
Function description			
To get an IPv6 address of the Module itself. An IPv6 address, obtainable as a link local address, is formed from a MAC address.			

3.2.1.3.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.3.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
IPv6 address	16	0xFE80000000000000XXXX X XXXXXXXXXXX XX represents MAC address.	Link-local address + MAC address Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.

3.2.1.4 Get MAC Address

Request command	0x000E	Response command	0x200E
Function description			
To get a MAC address of the Module itself.			

3.2.1.4.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.4.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address

3.2.1.5 Get Connection Status

Request command	0x0011	Response command	0x2011
Function description			
This command allows to get a MAC address of a device connected to the Module itself. MAC addresses that this command can get vary with its operation mode. PAN coordinator and Dual modes: The command can get the addresses of all devices connected to the Module. This is applicable to hop devices to which they are connected via the coordinator. Coordinator mode: The command can get the addresses of PAN coordinator to which the Module is connected and of end device connected to the Module itself. End device mode: The command can get the address of PAN coordinator to which the Module is connected.			

3.2.1.5.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.5.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Self connection status	1	0x00 to 0x01	0x00: Not connected 0x01: Connected Note: If the Module is not connected, all the following parameters will not be given.
Number of units connected	1	0x00 to 0x11	Number of units of devices connected to the Module itself The following MAC address to status parameters are repeated by the set number of units of devices connected to the Module.
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address of devices connected
PAN ID	2	0x0000 to 0xFFFF	PAN ID of devices connected
Block	1	0x01 to 0x02	0x01: Route B 0x02: HAN
Role	1	0x01 to 0x03 0x06 to 0x07	0x01: HAN PAN coordinator 0x02: HAN coordinator 0x03: HAN end device 0x06: HAN hop device 0x07: PAN coordinator for Route B
Status	1	0x01 to 0x02	0x01: Operating 0x02: Authentication

3.2.1.6 Get Terminal Information

Request command	0x0100	Response command	0x2100
Function description			
This command allows to get an IPv6 address of a device connected to the Module itself. MAC addresses that this command can get vary with its operation mode. PAN coordinator and Dual modes: The command can get the addresses of all devices connected to the Module. This is applicable to hop devices to which they are connected via the coordinator. Coordinator mode: The command can get the addresses of PAN coordinator to which the Module is connected and of end device connected to the Module itself. End device mode: The command can get the address of PAN coordinator to which the Module is connected.			

3.2.1.6.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.6.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Operation mode	1	0x00 to 0x03 0x05	0x00: Operation mode not yet determined 0x01: PAN coordinator (HAN) 0x02: Coordinator (HAN) 0x03: End device (HAN) 0x05: Dual (Route B and HAN)
Number of units connected	1	0x00 to 0x11	Number of units of devices connected to the Module itself The following IPv6 address to status parameters are repeated by the set number of units of devices connected to the module.
IPv6 address	16	0xFE80000000000000XXXXXXXXXXXXXXXX XX represents MAC address.	IPv6 address of device connected to the Module Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.
Role	1	0x01 to 0x03 0x06 to 0x07	0x01: HAN PAN coordinator 0x02: HAN coordinator 0x03: HAN end device 0x06: HAN hop device 0x07: PAN coordinator for Route B
Status	1	0x01 to 0x02	0x01: Operating 0x02: Authentication

3.2.1.7 Get Neighbor Discovery Setting

Request command	0x0102	Response command	0x2102
Function description			
To get the set value of Neighbor Discovery.			

3.2.1.7.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.7.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Neighbor Solicitation transmission	1	See Table 25: Neighbor Discovery setting.	See Table 25: Neighbor Discovery setting.

3.2.1.8 Get Initial Settings

Request command	0x0107	Response command	0x2107
Function description			
To get initial settings.			

3.2.1.8.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.8.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Operation mode	1	See Table 20: Initial settings.	See Table 20: Initial settings.
HAN sleep function setting	1	See Table 20: Initial settings.	See Table 20: Initial settings.
Channel	1	See Table 20: Initial settings.	See Table 20: Initial settings.
Transmission power	1	See Table 20: Initial settings.	See Table 20: Initial settings.

3.2.1.9 Get UART Setting

Request command	0x010B	Response command	0x210B
Function description			
To get the setting of flow control out of UART IF connection parameters.			

3.2.1.9.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.1.9.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Flow control	1	0x00 to 0x01	0x00: Disable flow control 0x01: Enable flow control

3.2.2 Request/Response command (set)

3.2.2.1 Set Initial Settings

Request command	0x005F	Response command	0x205F
Function description			
To set initial settings.			

3.2.2.1.1 Request command parameters

Name	Length in bytes	Range	Detail
Operation mode	1	See Table 20: Initial settings.	See Table 20: Initial settings.
HAN sleep function setting	1	See Table 20: Initial settings.	See Table 20: Initial settings.
Channel	1	See Table 20: Initial settings.	See Table 20: Initial settings.
Transmission power	1	See Table 20: Initial settings.	See Table 20: Initial settings.

3.2.2.1.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.2.2.2 Set Neighbor Discovery

Request command	0x0101	Response command	0x2101
Function description			
To make Neighbor Discovery setting.			

3.2.2.2.1 Request command parameter

Name	Length in bytes	Range	Detail
Neighbor Solicitation transmission	1	See Table 25: Neighbor Discovery setting.	See Table 25: Neighbor Discovery setting.

3.2.2.2.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.2.2.3 Change UART Setting

Request command	0x010A	Response command	0x210A
Function description			
This command makes setting of flow control out of UART IF connection parameters to enabled or disabled. The setting of the command to enabled or disabled is reflected after the response is transmitted.			

3.2.2.3.1 Request command parameter

Name	Length in bytes	Range	Detail
Flow control setting	1	0x00 to 0x01	0x00: Disable flow control 0x01: Enable flow control

3.2.2.3.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.2.3 Request/Response command (operation)

3.2.3.1 Open UDP Port

Request command	0x0005	Response command	0x2005
Function description			

This command opens a UDP port corresponding to a specified value to be used for UDP reception.

This command can specify UDP port numbers in the range of 1 to 65535 and open up to 10 ports.

This command can also open ports that carry a port number whose application is specified by Well-known Port Number controlled by PANA.

However, this command cannot open ports used by the system.

Port numbers used by the system are as follows:

- 716 (used by PANA);
- 19788 (used by MLE);
- 31941 (applicable only when OTA Client is in operation).

If both HAN and Route B are put into the not-yet-started status, ports opened by this command will be automatically closed.

3.2.3.1.1 Request command parameter

Name	Length in bytes	Range	Detail
UDP port number	2	0x0001 to 0xFFFF	UDP port numbers to be opened

3.2.3.1.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.2.3.2 Close UDP Port

Request command	0x0006	Response command	0x2006
Function description			

This command closes a UDP port corresponding to a specified value.

This command can specify UDP port numbers in the range of 1 to 65535, but cannot close ports used by the system.

Port numbers used by the system are as follows:

- 716 (used by PANA);
- 19788 (used by MLE);
- 31941 (applicable only when OTA Client is in operation).

3.2.3.2.1 Request command parameter

Name	Length in bytes	Range	Detail
UDP port number	2	0x0001 to 0xFFFF	UDP port numbers to be closed

3.2.3.2.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.2.3.3 Transmit Data

Request command	0x0008	Response command	0x2008
Function description			

This command transmits UDP data.

This command can specify port numbers in the range of 1 to 65535, but it cannot transmit them through ports used by the system. Port numbers used by the system are as follows:

- 716 (used by PANA);
- 19788 (used by MLE);
- 31941 (applicable only when OTA Client is in operation).

When this command transmits data to a sleep-enabled device, the data transmitted will be queued in indirect queue. The indirect queue holds a maximum of 1,232 bytes or 8 packets (the number of fragments). If there is no enough space in the indirect queue, this command will fail to queue data.

3.2.3.3.1 Request command parameters

Name	Length in bytes	Range	Detail
Destination IPv6 address	16	Unicast: 0xFE80000000000000XXXXXXXXXXXXXXXX XX represents MAC address. Multicast: 0xFFYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY YY represents IPv6 multicast.	IPv6 addresses of destination Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.
Source port number	2	0x0001 to 0xFFFF	UDP port numbers of source
Destination port number	2	0x0001 to 0xFFFF	UDP port numbers of destination
Transmission data size	2	0x0001 to 0x04D0	Length in bytes of transmission data 1 to 1,232 bytes
Transmission data	Variable	-	Data corresponding to the size specified by the transmission data size parameter are handled as binary data.

3.2.3.3.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command. Note: In case of failure to receive the command, the following parameters will not be given.
Result of data transmission	1	0xYZ Y represents result of indirect queuing Z represents result of UDP data transmission	Detailed result of UDP data transmission (Z) 0xY0: Succeeded 0xY2: Transmission failed due to limitation on the sum of transmission data amount 0xY3: Transmission failed due to failure in CCA 0xY5: Transmission failed due to unreceived ACK 0xY8: Transmission failed due to other cause of failure 0xYF: No transmission (only queuing) Detailed result of indirect queuing (Y) 0x0Z: No data queued in indirect queue 0x1Z: Data queued in indirect queue 0x2Z: Failed to queue data in indirect queue
Overview of transmission data	1 to 5	-	Data for the first 1 to 5 bytes of transmission data Note: If less than 5 bytes of data is transmitted, all that data as transmitted.

3.2.3.4 Execute Active Scan

Request command	0x0051	Response command	0x2051
		Notification command	0x4051
Function description			
This command executes active scan to find a specified channel. Smart meter (PAN coordinator for Route B), HAN PAN coordinator, or HAN coordinator returns a response through a beacon only when Pairing ID given to EBR matches. In order to execute active scan to find HAN, set the MAC address of the HAN PAN coordinator or HAN INT (0x48414e5f494e4954) to Paring ID. In order to search a smart meter, set the last eight characters of Route-B authentication ID to Pairing ID. Scanning results are notified by using the scan result of its **Notification** command. EBR transmission format varies with the operation mode of the Module. When the operation mode is set to PAN coordinator, data will be handled as that “no Pairing ID set” regardless of ID setting to transmit EBR without Paring ID given. When the operation mode is set to Dual, coordinator, or end device, EBR following the ID setting will be transmitted.			

3.2.3.4.1 Request command parameters

Name	Length in bytes	Range	Detail
Scan time	1	0x01 to 0x0E	Actual scan time per channel = 9.64 ms × 2 ^ scan time Note: When scan time (1 to 14) is set to 10, scanning will be executed for a period of approximately 9.8 seconds per channel.
Scan channel	4	0x00000000 to 0x0003FFF0	Make setting of channels to be scanned by bits (Note).
ID setting	1	0x00 to 0x01	Specify whether or not to make ID setting to EBR. 0x00: No Paring ID set 0x01: Paring ID set
Paring ID	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	Make Pairing ID setting when the ID setting parameter is set to Pairing ID set. In order to make ID setting of HAN_INIT, set the parameter to 0x48414e5f494e4954. In order to search a smart meter, set the last eight characters of Route-B authentication ID to Pairing ID.

Note:
San channel setting

Make scan channel setting by using binary numbers.

The channels represent Channel 0, Channel 1… from the right. Channels set to "1" are scanned. Channels set to "0" are not scanned.

```
b11 11 11 11 11 1   0    1    1   0000
                    |    |    |___ Channel 4 is scanned.
                    |    |_______ Channel 5 is scanned.
                    |_________ Channel 6 is not scanned.
```

In the example shown above, "0x0003FFB0" found by converting a binary number to hexadecimal becomes a set value of the scan channel parameter.

3.2.3.4.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.2.3.4.3 Notification command parameters

Name	Length in bytes	Range	Detail
Scan result	1	0x00 to 0x01	0x00: Responded (responded to a beacon) 0x01: Not responded (not responded to a beacon)
Channel	1	See Table 20: Initial settings.	Scanned channels See Table 20: Initial settings. Note: When the scan result parameter is set to responded, the parameters listed hereunder will be given.
Number of scans	1	0x01 to 0x14	The following MAC address to RSSI parameters are repeated by the set number of scans.
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	MAC addresses of Modules responded to a beacon
PAN ID	2	0x0000 to 0xFFFF	PAN ID of Modules responded to a beacon
RSSI	1	0x98 to 0xDE	Reception RSSI of beacon Unit: dBm (-104 to -34)

3.2.3.5 Transmit To Ping

Request command	0x00D1	Response command	0x20D1
		Notification command	0x60D1
Function description			

This command transmits an **Echo Request** to a specified address.

When this command receives an **Echo Reply** from the destination, it will notify the result.

If the command is requested before the result is notified, this will result in an error.

When a multicast address is set by the destination IPv6 address, this command will wait for an Echo Reply until the 10 second timer runs out. Consequently, if the command is requested during such period of time, this will result in an error.

Three transmission data formats are available:

Arbitrary data (specified by user);

“xx xx xx xx xx xx xx xx ...”

Fixed data pattern 1 (repetition of ASCII code ‘a’ to ‘z’);

“61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 61 62 63…”

Fixed data pattern 2 (increment from ASCII code ‘0001’);

“30303031 30303032 30303033 30303034 30303035 30303036 30303037 30303038

30303039 30303130 30303131 30303132 30303133 30303134 30303135 ...”

When data is transmitted to a sleep-enabled device, the transmitted data will be queued in indirect queue. Consequently, a pole request from the sleep-enabled device is required. In case of no pole request, transmission to Ping will result in not responded.

3.2.3.5.1 Request command parameters

Name	Length in bytes	Range	Detail
Destination IPv6 address	16	Unicast: 0xFE80000000000000XX XXXXXXXXXXXXXX XX represents MAC address. Multicast: 0xFFYYYYYYYYYYYYYY YYYYYYYYYYYYYYYY YY represents IPv6 multicast.	IPv6 addresses of destination Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.
Transmission data size	2	0x0001 to 0x04D0	Length in bytes of transmission data 1 to 1,232 bytes
Transmission data format	1	0x00 to 0x02	0x00: Arbitrary data transmission 0x01: Transmission in fixed data pattern 1 0x02: Transmission in fixed data pattern 2
Transmission data	Variable	-	When the Transmission data format parameter is set to arbitrary data transmission, data corresponding to the size specified by the transmission data size parameter are handled as binary data.

3.2.3.5.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.2.3.5.3 Notification command parameters

Name	Length in bytes	Range	Detail
Ping result	1	0x00 to 0x01	0x00: Not responded (Echo Reply not received) 0x01: Responded (Echo Reply received) Note: When the above responded is notified, the following parameters will be given.
Source IPv6 address	16	0xFE80000000000000XX XXXXXXXXXXXXXX XX represents MAC address.	IPv6 address of the source of Echo Reply Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.
Encryption	1	0x01 to 0x02	0x01: Not encrypted 0x02: Encrypted
RSSI	1	0x98 to 0xDE	Reception RSSI of Echo Reply Unit: dBm (-104 to -34)
Reception data size	2	0x001 to 0x04D0	Length in bytes of reception data 1 to 1,232 bytes
Reception data	Variable	-	Data corresponding to the size specified by the reception data size parameter are handled as binary data.

3.2.3.6 Execute ED Scan

Request command	0x00DB	Response command	0x20DB
Function description			
This command executes an ED scan for a specified channel. Scan results are notified all at once by responding to the command. It takes approximately 320 ms to scan one channel due to fixed scan time. Consequently, if it is requested to scan all channels, a response will be returned in a period of approximately 4.4 seconds (including channel switching time). An ED value got can be converted to a RSSI by the following formula: RSSI = (275 × ED value - 104270) ÷ 1,000			

3.2.3.6.1 Request command parameter

Name	Length in bytes	Range	Detail
Scan channel	4	0x00000000 to 0x0003FFF0	Make setting of channels to be scanned by bits (Note).

Note:
San channel setting

Make scan channel setting by using binary numbers.

The channels represent Channel 0, Channel 1… from the right. Channels set to “1” are scanned. Channels set to “0” are not scanned.

```
b11 11 11 11 11 1    0    1    1   0000
                     |    |    |___ Channel 4 is scanned.
                     |    |________ Channel 5 is scanned.
                     |____________ Channel 6 is not scanned.
```

In the example shown above, “0x0003FFB0” found by converting a binary number to hexadecimal becomes a set value of the scan channel parameter.

3.2.3.6.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Number of scans	1	0x01 to 0x0E	The following channel to scan result parameters are repeated by the set number of scans.
Channel	1	See Table 20: Initial settings.	Channels at which scans were executed See Table 20: Initial settings.
ED value	1	0x00 to 0xFF	ED value of a specified channel

3.2.4 Request/Response command (other)

3.2.4.1 Get Version Information

Request command	0x006B	Response command	0x206B
Function description			
To get firmware version information.			

3.2.4.1.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.4.1.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Firmware ID	2	-	0x0400: Wi-SUN Enhanced HAN Plus Route-B Dual Stack
Major version	1	0x00 to 0xFF	Major version
Minor version	1	0x00 to 0xFF	Minor version
Revision	4	0x00000000 to 0xFFFFFFFF	Revision number

3.2.4.2 Reset Hardware

Request command	0x00D9
Function description	
This command resets hardware. Since the hardware is rest, no **Response** command is returned. This command is received even while other command is executed. Since no **Response** command is returned, whether the hardware was successfully reset should be checked by receiving a **Notify Startup Completion** (§3.2.5.2).	

3.2.4.2.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.4.3 Transition To Rewrite Mode

Request command	0x00F0	Response command	0x20F0
Function description			
This command makes ROHM Module BP35C0-J11 transition to rewrite mode. After transiting to the rewrite mode, firmware can be rewritten.			

3.2.4.3.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.4.3.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.2.5 Notification command (operation)

3.2.5.1 Notify Data Reception

Notification command	0x6018
Function description	

This command notifies the reception of UDP data.

If an error occurs in the reception of the data, this notification will not be executed to notify the error by executing a **Notify Packet Reception Failure** (§3.2.5.5) command.

Furthermore, no specific reception data are notified. For details, refer to the table shown below.

Name	Operation
NS	NA is automatically returned without notification.
NA	No notification is given to internally process the data reception.
PANA	A corresponding PANA response message is transmitted without notification.
MLE	No notification is given to internally process the data reception.
Echo Request	Echo Reply is automatically returned without notification.
Other ICMPv6 notification	Notification is discarded.

3.2.5.1.1 Notification command parameters

Name	Length in bytes	Range	Detail
Source IPv6 address	16	0xFE80000000000000XX XXXXXXXXXXXXXX XX represents MAC address.	IPv6 address of the source of UDP data Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.
Source port number	2	0x0001 to 0xFFFF	UDP port numbers of source
Destination port number	2	0x0001 to 0xFFFF	UDP port numbers of destination
Source PAN ID	2	0x0000 to 0xFFFF	PAN ID of the source of UDP data
Destination address type	1	0x00 to 0x01	0x00: Unicast 0x01: Multicast
Encryption	1	0x01 to 0x02	0x01: Not encrypted 0x02: Encrypted
RSSI	1	0x98 to 0xDE	Reception RSSI of UDP data Unit: dBm (-104 to -34)
Reception data size	2	0x0001 to 0x04D0	Length in bytes of reception data 1 to 1,232 bytes
Reception data	Variable	-	Data corresponding to the size specified by the reception data size parameter are handled as binary data.

3.2.5.2 Notify Startup Completion

Notification command	0x6019
Function description	
To notify the startup of the Module when it is completed after the power supply is turned on or **Reset Hardware** is executed.	

3.2.5.2.1 Notification command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.2.5.3 Notify Connection Status Change

Notification command	0x601A
Function description	

This command notifies a change in the status of a device connected when it is made.

This command notifies only the MAC address of a device whose status was changed.

In order to get the status of any device other than the device stated above, execute **Get Connection Status** (§3.2.1.5) command or **Get Terminal Information** (§3.2.1.6) command.

If the connection status is changed by a self **Request** command, no notification will be made.

Applicable commands are as listed in the table below.

Command	Item not to be notified
Initiate HAN Operation (when succeeded)	MAC connection completed (not connected → operating)
Initiate Route-B Operation (when succeeded)	
Terminate HAN Operation	MAC disconnected (operation → not connected)
Request Termination Of Route-B Operation	
Initiate HAN PANA (when succeeded)	PANA authentication completed (operation → authentication)
Initiate Route-B PANA (when succeeded)	
Terminate HAN PANA	PANA disconnected (authentication → operating)
Terminate Route-B PANA	
Re-authenticate HAN PANA	Note

Note:
This command does not execute a request from coordinator and end device. However, status changes made by **Re-authenticate HAN PANA** executed from the PAN coordinator are notified not by executing **Notify Connection Status Change**, but by executing a **Notify PANA Authentication Result** command.

3.2.5.3.1 Notification command parameters

Name	Length in bytes	Range	Detail
Access point status	1	0x01 to 0x04	0x01: MAC connection completed 0x02: PANA connection completed 0x03: MAC disconnected 0x04: PANA disconnected
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address of devices connected
RSSI	1	0x98 to 0xDE	Reception RSSI of beacon or PANA message Unit: dBm (-104 to -34)

3.2.5.4 Notify PANA Authentication Result

Notification command	0x6028
Function description	

To notify the results of PANA authentication.

Operation mode: Dual

To notify the results of PANA authentication and PANA re-authentication with the PAN coordinator (smart meter) for Route B.

Operation mode: PAN coordinator

To notify the results of PANA re-authentication with the coordinator and end device.

The results of PANA authentication with the coordinator and end device are notified by executing a **Notify Connection Status Change** (§3.2.5.3) command.

Operation mode: coordinator or end device

To notify the results of PANA authentication and PANA re-authentication with the PAN coordinator.

Request and notification of PANA initiation and re-authenticate PANA commands

Requested by which operation mode	Command name	Notified by which operating mode
Coordinator End device	**Initiate HAN PANA**	PAN coordinator Dual
PAN coordinator Dual	**Re-authenticate HAN PANA**	Coordinator End device PAN coordinator Dual
Dual	**Initiate Route-B PANA**	Dual
Dual	**Initiate Route-B PANA Re-authentication**	Dual

3.2.5.4.1 Notification command parameters

Name	Length in bytes	Range	Detail
PANA result	1	0x01 to 0x03	0x01: Authentication succeeded 0x02: Authentication failed 0x03: No response
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC addresses of devices to be authenticated (PAN coordinator, coordinator, and end device)

3.2.5.5 Notify Packet Reception Failure

Notification command	0x6038
Function description	
To notify a packet reception failure, if any.	

3.2.5.5.1 Notification command parameters

Name	Length in bytes	Range	Detail
Reason for reception failure	1	0x01 to 0x40	0x01: Decoding failure 0x02: MAC failure: Except decoding failure 0x20: 6LowPAN failure 0x30: IP failure 0x40: UDP failure
Source IPv6 address	16	0xFE80000000000000XXXXXXXXXXXXXXXXX XX represents MAC address.	IPv6 address of the source of data Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.
Reception data sequence number	1	0x00 to 0xFF	Sequence number of MAC header
Fragment	1	0x00 to 0x01	0x00: Fragment present 0x01: No fragment present
Fragment tag	2	0x0000 to 0xFFFF	Tag given to the fragment packet Note: This parameter is set to "0" in case of no fragment present.
Overview of reception data	1 to 5	-	Data on the first 1 to 5 bytes of reception data

3.3 HAN commands

3.3.1 Request/Response commands (get)

Only when a response to a get **Request** command results in succeeded, parameters after **Response** result will be given.

3.3.1.1 Get HAN Group Key Validity Period

Request command	0x0013	Response command	0x2013
Function description			
To get the validity period of HAN group key set to the Module.			

3.3.1.1.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.1.1.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Minimum validity period	4	See Table 26: HAN group key validity period settings.	See Table 26: HAN group key validity period settings.
Maximum validity period	4	See Table 26: HAN group key validity period settings.	See Table 26: HAN group key validity period settings.

3.3.1.2 Get HAN Acceptance/Connection Mode Status

Request command	0x0026	Response command	0x2026
Function description			
To get HAN acceptance connection mode.			

3.3.1.2.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.1.2.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Acceptance connection mode	1	0x01 to 0x02	0x01: Initial connection mode 0x02: Normal connection mode

3.3.1.3 Get HAN Group Key

Request command	0x0028	Response command	0x2028
Function description			
To get the HAN group key (encryption key). The group key is generated at the time of the first PANA authentication between PAA and PaC. If no devices are connected in PAN coordinator mode, the first PAN authentication will have not been executed. Consequently, all results of the command execution will come to zero (0).			

3.3.1.3.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.1.3.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
HAN group key	16	-	Encryption key randomly generated with currently-valid PAA
Key ID	1	0x01 to 0xFF	Group key identification ID

3.3.1.4 Get HAN PANA Authentication Information

Request command	0x002D	Response command	0x202D
Function description			
This command gets HAN PANA authentication information setting. The response parameter varies with Module operation mode. For details, refer to the response command parameters.			

3.3.1.4.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.1.4.2 Response command parameters (PAN coordinator or Dual)

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Number of settings	1	0x00 to 0x11	Parameters from MAC address to Password are repeated by the set number of settings.
MAC address	8	See Table 27: HAN PANA authentication information settings.	See Table 27: HAN PANA authentication information settings.
Password	16	See Table 27: HAN PANA authentication information settings.	See Table 27: HAN PANA authentication information settings.

3.3.1.4.3 Response command parameters (coordinator or end device)

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Password	16	See Table 27: HAN PANA authentication information settings.	See Table 27: HAN PANA authentication information settings.

3.3.1.5 Get Setting Of HAN Sleep Device PANA Retransmission Interval

Request command	0x0067	Response command	0x2067
Function description			
To get the setting of a retransmission interval for PANA message to HAN sleep device.			

3.3.1.5.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.1.5.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Number of sleep devices	1	0x00 to 0x04	Parameters from MAC address to Maximum retransmission interval are repeated by the set number of sleep devices.
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	MAC addresses of sleep devices connected to the Module when the operation mode is set to PAN coordinator MAC address of the Module itself when the operation mode is set to end device
Initial retransmission interval	2	See Table 28: HAN sleep device PANA retransmission interval settings.	See Table 28: HAN sleep device PANA retransmission interval settings.
Maximum retransmission interval	2	See Table 28: HAN sleep device PANA retransmission interval settings.	See Table 28: HAN sleep device PANA retransmission interval settings.

3.3.1.6 Get Setting Of Number Of Times Of Retransmissions Of HAN PaC PANA Authentication Initiation Message

Request command	0x0104	Response command	0x2104
Function description			
To get the setting of the number of times of retransmissions of HAN PaC PANA authentication initiation message.			

3.3.1.6.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.1.6.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Number of times of retransmissions of PANA authentication initiation message	1	See Table 29: Setting of number of times of retransmissions of HAN PaC PANA authentication initiation message.	See Table 29: Setting of number of times of retransmissions of HAN PaC PANA authentication initiation message.

3.3.1.7 Get Setting Of Number Of Times Of Retransmissions Of HAN PANA Authentication Message

Request command	0x0106	Response command	0x2106
Function description			
To get the setting of the number of times of retransmissions of HAN PANA authentication message.			

3.3.1.7.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.1.7.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Number of times of retransmissions of PANA authentication initiation message	1	See Table 30: Setting of number of times of retransmissions of HAN PANA authentication message.	See Table 30: Setting of number of times of retransmissions of HAN PANA authentication message.

3.3.1.8 Get Setting Of Waiting Time For Completion Of Updating HAN Group Key

Request command	0x0109	Response command	0x2109
Function description			
To get the setting of waiting time for completion of updating HAN group key.			

3.3.1.8.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.1.8.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Waiting Time for Completion of Updating HAN Group Key	2	See Table 31: Setting of waiting time for completion of updating HAN group key.	See Table 31: Setting of waiting time for completion of updating HAN group key.

3.3.2 Request/Response command (set)

3.3.2.1 Set HAN Group Key Validity Period

Request command	0x0012	Response command	0x2012
Function description			
To make setting of HAN group key validity period.			

3.3.2.1.1 Request command parameters

Name	Length in bytes	Range	Detail
Minimum validity period	4	See Table 26: HAN group key validity period settings.	See Table 26: HAN group key validity period settings.
Maximum validity period	4	See Table 26: HAN group key validity period settings.	See Table 26: HAN group key validity period settings.

3.3.2.1.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.2.2 Set HAN PANA Authentication Information

Request command	0x002C	Response command	0x202C
Function description			
This command makes setting of information necessary for HAN PANA authentication. The request parameter varies with Module operation mode. For details, refer to the request command parameters. This command is available to register the authentication information of up to 17 units of coordinators and end devices in total.			

3.3.2.2.1 Response command parameters (PAN coordinator or Dual)

Name	Length in bytes	Range	Detail
MAC address	8	See Table 27: HAN PANA authentication information settings.	See Table 27: HAN PANA authentication information settings.
Password	16	See Table 27: HAN PANA authentication information settings.	See Table 27: HAN PANA authentication information settings.

3.3.2.2.2 Response command parameters (coordinator or end device)

Name	Length in bytes	Range	Detail
Password	16	See Table 27: HAN PANA authentication information settings.	See Table 27: HAN PANA authentication information settings.

3.3.2.2.3 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.2.3 Delete HAN PANA Authentication Information Setting

Request command	0x002E	Response command	0x202E
Function description			

This command deletes the HAN PANA authentication information setting.

The request parameter varies with Module operation mode.

In case of PAN coordinator or Dual operation mode, when the MAC address parameter is set to HAN PANA authentication information, the MAC address will be individually deleted. When the parameter is not set to MAC address, all parameter settings will be deleted.

Authentication information on devices in the authentication status cannot be deleted.

In coordinator or end device operation mode, the Module's own authentication information will be deleted.

When the Module itself is in the authentication status, it cannot be deleted.

3.3.2.3.1 Request command parameter (PAN coordinator or Dual) - Individual Deletion

Name	Length in bytes	Range	Detail
MAC address	8	See Table 27: HAN PANA authentication information settings.	See Table 27: HAN PANA authentication information settings.

3.3.2.3.2 Request command parameter (PAN coordinator or Dual) - All Deletion

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.2.3.3 Request command parameter (coordinator or end device)

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.2.3.4 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Number of units of undeletable devices	1	0x00 to 0x11	Available only when the Module operation mode is set to PAN coordinator or Dual and all devices' information is deleted.

3.3.2.4 Set HAN Sleep Device PANA Retransmission Interval

Request command	0x0066	Response command	0x2066
Function description			
This command makes setting of a retransmission interval for PANA message to HAN sleep device. For values available for the setting, see For end devices with the valid HAN sleep function, this command makes a request of the PAN coordinator to make setting of a retransmission interval and sets a value received from the PAN coordinator to the retransmission interval. The setting result is notified by using a **Notify Setting Of HAN Sleep Device PANA Retransmission Interval** command stated in §3.3.4.5.			

3.3.2.4.1 Request command parameters

Name	Length in bytes	Range	Detail
Initial validity period	2	See Table 28: HAN sleep device PANA retransmission interval settings.	See Table 28: HAN sleep device PANA retransmission interval settings.
Maximum validity period	2	See Table 28: HAN sleep device PANA retransmission interval settings.	See Table 28: HAN sleep device PANA retransmission interval settings.

3.3.2.4.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.2.5 Set Number Of Times Of Retransmissions Of HAN PaC PANA Authentication Initiation Message

Request command	0x0103	Response command	0x2103
Function description			
To make setting of the number of times to retransmit a message to initiate HAN PaC PANA authentication.			

3.3.2.5.1 Request command parameter

Name	Length in bytes	Range	Detail
None Number of times of retransmissions of PANA authentication initiation message	1	See Table 29: Setting of number of times of retransmissions of HAN PaC PANA authentication initiation message.	See Table 29: Setting of number of times of retransmissions of HAN PaC PANA authentication initiation message.

3.3.2.5.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.2.6 Set Number Of Times Of Retransmissions Of HAN PANA Authentication Message

Request command	0x0105	Response command	0x2105
Function description			
To make setting of the number of times to retransmit a HAN PANA authentication message.			

3.3.2.6.1 Request command parameter

Name	Length in bytes	Range	Detail
Number of times of retransmissions of PANA authentication message	1	See Table 30: Setting of number of times of retransmissions of HAN PANA authentication message.	See Table 30: Setting of number of times of retransmissions of HAN PANA authentication message.

3.3.2.6.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.2.7 Set Waiting Time For Completion Of Updating HAN Group Key

Request command	0x0108	Response command	0x2108
Function description			
To make setting of a period of time to wait for the completion of updating the HAN group key.			

3.3.2.7.1 Request command parameter

Name	Length in bytes	Range	Detail
Waiting time for completion of updating group key	2	See Table 31: Setting of waiting time for completion of updating HAN group key.	See Table 31: Setting of waiting time for completion of updating HAN group key.

3.3.2.7.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3 Request/Response command (operation)

3.3.3.1 Initiate HAN Operation

Request command	0x000A	Response command	0x200A
Function description			
This command initiates HAN operation and, if succeeded, make the Module transition to the operating status. The request parameter varies with Module operation mode. For details, refer to the request command parameters. When the operation mode is set to PAN coordinator or Dual: PAN ID should be set to a unique value. For this purpose, execute an active scan (without Pairing ID given) for an arbitrary channel (a channel specified in the initial settings), derive unique PAN ID not used by devices in the vicinity, and then set this PAN ID to the PAN ID parameter. PAN ID 0xFFFF used for Route B is not allowed to use. When the operation mode is set to coordinator or end device: Execute initial connection (HAN_INIT) or normal connection (set the MAC address of PAN coordinator.			

3.3.3.1.1 Request command parameter (PAN coordinator or Dual)

Name	Length in bytes	Range	Detail
PAN ID	2	0x0000 to 0xFFFE	PAN ID Note: This parameter must be set to a unique value within the same channel.

3.3.3.1.2 Request command parameter (coordinator or end device)

Name	Length in bytes	Range	Detail
Paring ID	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	In case of the MAC address of PAN coordinator, this parameter becomes Paring ID for normal connection. In case of 0xFFFFFFFFFFFFFFFF, this parameter becomes Paring ID for initial connection (HAN_INIT).

3.3.3.1.3 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command. In case of connection failure, the parameters listed hereunder will not be given.
Channel	1	See Table 20: Initial settings.	Channel connected See Table 20: Initial settings.
PAN ID	2	0x0000 to 0xFFFF	PAN ID connected
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	MAC address of Pan coordinator at the access point Note: When the Module operation mode is set to PAN coordinator or Dual, this parameter will not be given.
RSSI	1	0x98 to 0xDE	Reception RSSI of beacon Unit: dBm (-104 to -34) Note: When the Module operation mode is set to PAN coordinator or Dual, this parameter will not be given.

3.3.3.2 Terminate HAN Operation

Request command	0x000B	Response command	0x200B
Function description			
This command terminates HAN operation to make the Module transition to the not-yet-started status. Since this command brings about no communications, it cannot be detected at the access point that the Module was put into the not-yet-started status. When this command is executed, the following information will be initialized or invalidated. • UDP port opened (The command will not be invalidated when Route B is connected.)			

3.3.3.2.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.3.2.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.3 Switch HAN Acceptance Connection Mode

Request command	0x0025	Response command	0x2025
Function description			
This command switches the HAN acceptance connection mode. The HAN acceptance connection mode is available in two types: initial connection mode and normal connection mode. When it is switched to the currently-set mode, an error response will be returned to the command. The initial connection mode is automatically switched to the normal connection mode after a lapse of three minutes. In such cases, a **Notify HAN Acceptance Connection Mode Change** (§3.3.4.1) command will be executed to notify the mode change.			

3.3.3.3.1 Request command parameter

Name	Length in bytes	Range	Detail
Acceptance connection mode	1	0x01 to 0x02	0x01: Initial connection mode 0x02: Normal connection mode

3.3.3.3.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.4 Distribute HAN Group Key

Request command	0x0029	Response command	0x2029
Function description			

This command updates the HAN group key (encryption key) and distribute the HAN group key to devices connected to the Module.

After completion of the distribution of the key, the results are notified to all devices connected to the Module by executing a **Notify HAN Group Key Distribution Results** (§3.3.4.2) command. Since the HAN group key is distributed to all devices connected, time to start notifying the results varies with the number of devices connected.

If the operating status transitions from the authentication status to a different status before notifying the results, no results will be notified.

3.3.3.4.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.3.4.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.5 Check HAN Group Key Update

Request command	0x002A	Response command	0x202A
Function description			
This command checks with the PAN coordinator whether the HAN group key (encryption key) is updated and, if Yes, update the HAN group key. The result of checking for updating of the key is notified by executing a **Notify HAN Group Key Updating Check Results** (§3.3.4.3) command. If the operating status transitions from the authentication status to a different status before notifying the results, no results will be notified.			

3.3.3.5.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.3.5.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.6 Re-authenticate HAN PANA

Request command	0x002B	Response command	0x202B
Function description			
This command re-authenticates a PANA from the PAN coordinator to coordinator or end device. The re-authentication results are notified by executing a **Notify PANA Authentication Result** (§3.2.5.4) command. If the operating status transitions from the authentication status to a different status before notifying the results, no results will be notified.			

3.3.3.6.1 Request command parameter

Name	Length in bytes	Range	Detail
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address of coordinator or end device to be re-authenticated

3.3.3.6.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.7 Initiate HAN PANA

Request command	0x003A	Response command	0x203A
Function description			
This command initiates the PANA authentication function for HAN. The operation of the function varies with the operation mode of the Module. When the operation mode is set to PAN coordinator or Dual, this command will serve as PANA Authentication Agent (PAA) to initiate the PAN authentication function and become ready for accepting a PANA authentication request from the coordinator and end device. When the operation mode is set to PAN coordinator or Dual, this command will serve as PANA Client (PaC) to initiate the PANA authentication function and transmit a request for initiating PANA authentication to the PAN coordinator. The authentication results are notified by executing **Notify PANA Authentication Result** (§3.2.5.4) command. In order to initiate the PANA authentication function, open the following two ports. These ports are not included in the maximum number of ports opened by executing **Open UDP Port** (§3.2.3.1) command. • 716 (used by PANA); • 19788 (used by MLE).			

3.3.3.7.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.3.7.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address of PAN coordinator Note: When the Module operation mode is set to PAN coordinator or Dual, this parameter will not be given.

3.3.3.8 Terminate HAN PANA

Request command	0x003B	Response command	0x203B
Function description			

This command terminates the PANA authentication function for HAN.

The operation of the function varies with the operation mode of the Module.

When the operation mode is set to PAN coordinator or Dual, this command will transmit a PANA disconnection message to all coordinators and end devices connected to the Module to terminate the PANA authentication function.

Values set by executing **Set HAN Group Key Validity Period** (§3.3.2.1) and **Set HAN PANA Authentication Information** (§3.3.2.2) commands are initialized.

When the operation mode is set to coordinator or end device, this command will transmit a PANA disconnection message to the PAN coordinator to terminate the PANA authentication function.

Values set by executing **Set HAN PANA Authentication Information** (§3.3.2.2) command are initialized.

When the PANA authentication function is terminated, the following ports used by the PANA authentication function will be closed:

- 716 (used by PANA);
- 19788 (used by MLE).

When this command receives a PANA disconnection message from the access point, it will notify that effect by executing a **Notify Connection Status Change** (§3.2.5.3) command (Status of the access point: PANA disconnected).

3.3.3.8.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.3.8.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.9 Transmit HAN Poll Request

Request command	0x0061	Response command	0x2061
Function description			
This command makes a poll request in order to check for any data addressed to the Module itself. If data addressed to the Module itself is found as the result of the poll request, the relevant data will be transmitted from a device at the access point.			

3.3.3.9.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.3.9.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Presence of data in indirect queue	1	0x00 to 0x01	0x00: No data present in indirect queue 0x01: Data present in indirect queue

3.3.3.10 HAN Purge Request

Request command	0x0069	Response command	0x2069
Function description			
To discard data addressed to a sleep-enabled device and present in indirect queue.			

3.3.3.10.1 Request command parameter

Name	Length in bytes	Range	Detail
MAC address	8	-	MAC address of a sleep-enabled device corresponding to the relevant data queue to be deleted.

3.3.3.10.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Number of data discarded	1	0x00 to 0x08	Number of discarded data in indirect queue

3.3.3.11 Delete HAN Device From List

Request command	0x006A	Response command	0x206A
Function description			
This command deletes a specified device from the device list. In other words, when this command receives EBR or beacon from a no-longer-required or unintended device, this command is used to delete such device from the device list of the Module. When the operation mode of the Module is set to PAN coordinator or Dual: This command is not available to delete devices in the HAN authentication status. Consequently, use **Disconnect HAN** (§3.3.3.12) command to delete the devices. When the operation mode of the Module is set to coordinator: This command is available to delete devices in the HAN authentication status and the HAN operating status. Note: Since the coordinator is the PaC, the Module just deletes the devices from its device list without disconnecting PANA.			

3.3.3.11.1 Request command parameter

Name	Length in bytes	Range	Detail
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address to be deleted.

3.3.3.11.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.12 Disconnect HAN

Request command	0x00D3	Response command	0x20D3
Function description			
This command executes **Terminate HAN PANA** and **Delete HAN Device From List** for a specified device. When this command normally terminates its execution, the HAN PANA authentication information settings (§2.9.2.2) for the specified device will be deleted. Furthermore, since this command executes **Delete HAN Device From List** (0x006A) in §3.3.3.11, two responses 0x20D3 and 0x206A are returned.			

3.3.3.12.1 Request command parameter

Name	Length in bytes	Range	Detail
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address to be disconnected

3.3.3.12.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.13 HAN Deep Sleep Request

Request command	0x00DA	Response command	0x20DA
		Notification command	0x60DA
Function description			
This command switches the hardware to deep sleep mode. The Module switches to deep sleep mode after transmitting a **Response** command. The Module that entered the deep sleep mode does not wake up until it is requested to release the deep sleep mode. The Module can release the deep sleep mode by transmitting any **Request** command (Note) from user in order to release the deep sleep mode with UART_TXD set to Low. After waking up, the Module executes WakeUp **Notification** command (0x60DA). Note: **Request** command transmitted during the deep sleep mode release is not processed.			

3.3.3.13.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.3.13.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.3.3.13.3 Notification command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.3.4 Notification command (operation)

3.3.4.1 Notify HAN Acceptance Connection Mode Change

Notification command	0x6023
Function description	
When the HAN acceptance connection mode is switched, this command will notify that effect. If the connection mode is switched to normal connection mode within a period of three minutes after the connection mode is set to initial connection mode, this notification will not be made.	

3.3.4.1.1 Notification command parameters

Name	Length in bytes	Range	Detail
Acceptance connection mode	1	0x01 to 0x02	0x01: Default connection mode 0x02: Normal connection mode

3.3.4.2 Notify HAN Group Key Distribution Results

Notification command	0x6026
Function description	

This command notifies the execution results of **Distribute HAN Group Key** (§3.3.3.4) command.

This command updates the HAN group key and the key ID, and then distributes the updated key to devices connected to the Module. Subsequently, it displays the number of units and the MAC address of devices to which the distribution of the updated key was succeeded and the same to which the distribution of the update key was failed, respectively.

When the operation mode of the Module is set to PAN coordinator or Dual, the execution results of this command are notified.

3.3.4.2.1 Notification command parameters

Name	Length in bytes	Range	Detail
HAN group key	16	-	Encryption key randomly generated with the PAA
Key ID	1	0x01 to 0xFF	Newly assigned group key identification
Number of distribution succeeded	1	0x00 to 0x11	MAC address to which the distribution was succeeded is repeated by the set number of distribution succeeded.
MAC address to which distribution was succeeded	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC addresses of coordinators and end devices to which the distribution was succeeded
Number of distribution failed	1	0x00 to 0x11	MAC address to which the distribution was failed is repeated by the set number of distribution failed.
MAC address to which distribution was failed	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC addresses of coordinators and end devices to which the distribution was failed Note: When the Number of distribution failed parameter is set to zero (0), this parameter will not be given.

3.3.4.3 Notify HAN Group Key Updating Check Results

Notification command	0x6027
Function description	

This command notifies the execution results of **Check HAN Group Key Update** (§3.3.3.5) command.

When the HAN group key is updated, the HAN group key and Key ID will be notified.

When the HAN group key is not updated or no response is returned, the HAN group key and Key ID will not be given to the parameter, respectively.

3.3.4.3.1 Notification command parameters

Name	Length in bytes	Range	Detail
Updating result	1	0x01 to 0x03	0x01: Updated 0x02: Not updated 0x03: No response from PAN coordinator
HAN group key	16	-	Encryption key randomly generated with the PAA Note: If updating results in not updated or no response, the HAN group key will not be given.
Key ID	1	0x01 to 0xFF	Newly assigned group key identification Note: If updating results in not updated or no response, the Key ID will not be given.

3.3.4.4 Notify HAN Group Key Distribution Complete

Notification command	0x6029
Function description	

When the HAN group key is updated by **Distribute HAN Group Key** from the PAN coordinator, this command will notify the completion of distribution of the HAN group key.

When the operation mode of the Module is set to coordinator or end device, this command will notify it.

3.3.4.4.1 Notification command parameters

Name	Length in bytes	Range	Detail
Distribution result	1	0x01 0x57	0x01: HAN group key updating completed 0x57: HAN group key updating failed

3.3.4.5 Notify Setting Of HAN Sleep Device PANA Retransmission Interval

Notification command	0x6030
Function description	

This command notifies the results of setting made by executing a **Set HAN Sleep Device PANA Retransmission Interval** (§3.3.2.4) command.

When the setting of a retransmission interval for PANA message to HAN sleep device is completed by the PAN coordinator, this command will notify that effect.

When the operation mode of the Module is set to end device with the valid HAN sleep function, this command will notify it.

3.3.4.5.1 Notification command parameters

Name	Length in bytes	Range	Detail
Setting result	1	0x01 to 0x02	0x01: Retransmission interval setting completed 0x02: No response from PAN coordinator
Initial retransmission interval	2	See Table 28: HAN sleep device PANA retransmission interval settings.	See Table 28: HAN sleep device PANA retransmission interval settings.
Maximum retransmission interval	2	See Table 28: HAN sleep device PANA retransmission interval settings.	See Table 28: HAN sleep device PANA retransmission interval settings.

3.3.4.6 Notify HAN Indirect Queue Discard

Notification command	0x6036
Function description	

When no poll request is made from a sleep-enabled device for a period of 300 seconds after data transmitted to the sleep-enabled device is queued, this command will automatically discard the queue and notify the result of that effect.

3.3.4.6.1 Notification command parameters

Name	Length in bytes	Range	Detail
Number of data discarded	1	0x01 to 0x08	Number of discarded data in indirect queue
Destination IPv6 address	16	Unicast: 0xFE80000000000000XXXXXXXXXXXXXXXX XX represents MAC address.	IPv6 address of the device at the destination corresponding to the queue.

3.3.4.7 Notify HAN Indirect Queue Transmission

Notification command	0x6037
Function description	
When data retained in indirect queue is transmitted upon poll request from the sleep-enabled device, this command will notify that effect. The Module notifies it voluntarily and only when a sleep-enabled device is connected to the Module. When the PAN coordinator transmits data to the sleep-enabled device connected to the coordinator, the coordinator will not notify **Notify HAN Indirect Queue Transmission**.	

3.3.4.7.1 Notification command parameters

Name	Length in bytes	Range	Detail
Result of data transmission	1	0x00 to 0x08	Detailed result of transmission of data retained in indirect queue 0x00: Succeeded 0x02: Transmission failed due to limited sum of transmission data 0x03: Transmission failed due to failure in CCA 0x05: Transmission failed due to unreceived acknowledgement 0x08: Transmission failed due to other cause of failure
Number of remaining queues	1	0x00 to 0x07	Number of transmission data remaining in queues
Destination IPv6 address	16	Unicast: 0xFE80000000000000XXXXXXXXXXXXXXXX XX represents MAC address.	IPv6 address of the device at the destination corresponding to the queue. Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.
Overview of transmission data	1 to 5	-	Data for the first 1 to 5 bytes of transmission data

3.3.4.8 Notify HAN Relay Failure

Notification command	0x6039
Function description	
In case of failure to receive or to transfer/transmit a HAN message for relaying/transferring it, this command notifies such failure.	

3.3.4.8.1 Notification command parameters

Name	Length in bytes	Range	Detail
Failure type	1	0x00 to 0x02	0x00: Relay/Reception failed 0x01: Relay/Transfer/Transmission failed 0x02: Relay/Transfer/Transmission failed (Indirect)
Failure cause	1	0x01 to 0xFF	When the Failure type parameter is set to 0x00 (Relay/Reception failed), the cause of failure to receive will be notified. When the parameter is set to 0x02, MAC failure, except decryption failure, will be notified. When the Failure type parameter is set to 0x01 or 0x02 (Relay/Transfer/Transmission failed), the cause of failure to transmit will be notified. Detailed result of transmission (Z) 0xY2: Transmission failed due to limited sum of transmission data 0xY3: Transmission failed due to failure in CCA 0xY5: Transmission failed due to unreceived acknowledgement 0xY8: Transmission failed due to other cause of failure 0xYF: No transmission (only queuing) Detailed result of indirect queuing (Y) 0x0Z: No data queued in indirect queue 0x1Z: Data queued in indirect queue 0x2Z: Failed to queue data in indirect queue
Sequence number	1	0x00 to 0xFF	Sequence number of MAC header When the Failure type parameter is set to 0x00 (Relay/Reception failed), a sequence number given by the source of data will be notified. When the Failure type parameter is set to 0x01 or 0x02 (Relay/Transfer/Transmission

Name	Length in bytes	Range	Detail
			failed), a sequence number given by the Module itself for the transfer or transmission of data will be notified.
MAC address of source	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address of the source of data When the Failure type parameter is set to 0x00 (Relay/Reception failed), the MAC address of the source of data will be notified. When the Failure type parameter is set to 0x01 or 0x02 (Relay/Transfer/Transmission failed), the MAC address of the Module itself will be notified.
MAC address of transfer destination	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	64-bit MAC address of the transfer destination When the Failure type parameter is set to 0x00 (Relay/Reception failed), the MAC address of the Module itself will be notified. When the Failure type parameter is set to 0x01 or 0x02 (Relay/Transfer/Transmission failed), the MAC address of the destination will be notified.

3.4 Route B commands

3.4.1 Request/Response commands (get)

Only when a response to a get **Request** command results in succeeded, parameters listed after Response result will be given.

3.4.1.1 Get Route-B Encryption Key

Request command	0x0059	Response command	0x2059
Function description			
Used to get a Route-B encryption key.			

3.4.1.1.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.4.1.1.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Route-B encryption key	16	-	Encryption key randomly generated with currently-valid PAA

3.4.1.2 Get Route-B PAN ID

Request command	0x005E	Response command	0x205E
Function description			

This command gets PAN ID used by Route B.

Since PAN ID set by Route B cannot be used on the HAN side, set PAN ID other than that got by this command to the HAN side.

3.4.1.2.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.4.1.2.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.
Route-B PAN ID	2	0x0000 to 0xFFFF	PAN ID used by Route B

3.4.2 Request/Response command (set)

3.4.2.1 Set Route-B PANA Authentication Information

Request command	0x0054	Response command	0x2054
Function description			
To make setting of PANA authentication information for Route B.			

3.4.2.1.1 Request command parameters

Name	Length in bytes	Range	Detail
Route-B authentication ID	32	See Table 32: Route-B PANA authentication information settings.	See Table 32: Route-B PANA authentication information settings.
Password	12	See Table 32: Route-B PANA authentication information settings.	See Table 32: Route-B PANA authentication information settings.

3.4.2.1.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.4.3 Request/Response command (operation)

3.4.3.1 Initiate Route-B Operation

Request command	0x0053	Response command	0x2053
Function description			
This command initiates the operation of Route B and, when it is successfully initiated, make the Route-B block transition to the operating status. This command is executable only when the HAN block is in the not-yet-started status.			

3.4.3.1.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.4.3.1.2 Response command parameters

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command. Note: In case of connection failure, the parameters listed hereunder will not be given.
Channel	1	See Table 20: Initial settings.	Channel connected See Table 20: Initial settings.
PAN ID	2	0x0000 to 0xFFFF	PAN ID connected
MAC address	8	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	MAC address of Pan coordinator at the access point
RSSI	1	0x98 to 0xDE	RSSI of beacon Unit: dBm (-104 to -34)

3.4.3.2 Initiate Route-B PANA

Request command	0x0056	Response command	0x2056
Function description			

This command initiates the PANA authentication function for Route B.

This command initiates PANA Client (PaC), transmits a request for initiating PANA authentication to the PAN coordinator, and subsequently notifies the authentication result by executing a **Notify PANA Authentication Result** (§3.2.5.4) command.

In order to initiate the PANA authentication function, open the following port. This port is not included in the maximum number of ports opened by executing an **Open UDP Port** (§3.2.3.1) command.

- 716 (used by the PANA)

3.4.3.2.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.4.3.2.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.4.3.3 Terminate Route-B PANA

Request command	0x0057	Response command	0x2057
Function description			
This command terminates the PANA authentication function for Route B. This command transmits a PANA disconnection message to the smart meter to terminate the PANA authentication function. When this command receives a PANA disconnection message from the smart meter located at the access point, it will notify that effect by executing a **Notify Connection Status Change** (§3.2.5.3) command (status of the access point: PANA disconnected).			

3.4.3.3.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.4.3.3.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.4.3.4 Terminate Route-B Operation

Request command	0x0058	Response command	0x2058
Function description			
This command terminates the operation of Route B and make Route B transition to the not-yet-started status. Since this command generates no communications, it cannot be detected at the access point that Route B was put into the not-yet-started status. When this command is executed, the following information will be initialized or invalidated. • UDP port opened (The command will not be invalidated when the HAN is connected.)			

3.4.3.4.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.4.3.4.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.4.3.5 Initiate Route-B PANA Re-authentication

Request command	0x00D2	Response command	0x20D2
Function description			

This command re-authenticates the PANA for Route B.

The re-authentication result is notified by executing a **Notify PANA Authentication Result** (§3.2.5.4) command.

If the operating status transitions from the authentication status to a different status before notifying the result, no result will be notified.

3.4.3.5.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.4.3.5.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.5 OTA update commands

3.5.1 Request/Response command (operation)

3.5.1.1 Initiate OTA Client

Request command	0x0201	Response command	0x2201
Function description			

This command initiates OTA Client and put it into operation in the status in which OTA UDP packets can be accepted.

At execution of **Initiate OTA Client**, open the UDP port of 31941 to be used.

3.5.1.1.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.5.1.1.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.5.1.2 Terminate OTA Client

Request command	0x0202	Response command	0x2202
Function description			
This command terminates OTA Client and return it to the status in which no OTA UDP packets can be accepted. At execution of **Terminate OTA Client**, close the UDP port of 31941 in use.			

3.5.1.2.1 Request command parameter

Name	Length in bytes	Range	Detail
None	-	-	-

3.5.1.2.2 Response command parameter

Name	Length in bytes	Range	Detail
Response result	1	-	For command execution results, see Table 34: List of response results to Request command.

3.5.2 Notification command (operation)

3.5.2.1 Notify OTA Operation Initiation

Notification command	0x6033
Function description	

This command notifies the initiation of OTA updating operation.

The initiation is notified when the OTA Client receives an OTA mode initiation packet.

3.5.2.1.1 Notification command parameters

Name	Length in bytes	Range	Detail
Source IPv6 address	16	0xFE80000000000000XXXXXXXXXXXXXXXX XX represents MAC address.	IPv6 address of the source of OTA data Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.

3.5.2.2 Notify OTA Operation Termination

Notification command	0x6034
Function description	
This command notifies the termination of OTA updating operation. The termination is notified when the OTA Client receives an OTA mode termination packet.	

3.5.2.2.1 Notification command parameters

Name	Length in bytes	Range	Detail
OTA result	1	0x01 to 0x03	0x01: Version upgrade succeeded 0x02: Version upgrade failed 0x03: No version upgrade
Source IPv6 address	16	0xFE80000000000000XXXXXXXXXXXXXXXX XX represents MAC address.	IPv6 address of the source of OTA data Note: The lower 2nd bit of the first 1 byte of the MAC address is inverted.

4. List of response results to Request command

The Module acknowledges a **Request** command, processes this command in it, and subsequently returns a **Response** command including a response result.

The table shown below lists response results set to the **Response** command.

Table 34: List of response results to Request command

Response result (DEC)	Response result (HEX)	Description
1	0x01	Command succeeded
2	0x02	The specified address does not exist in the device list.
3	0x03	Invalid command code
4	0x04	Invalid parameter value
6	0x06	Transmission error due to invalid address
10	0x0A	Port opening error: Already open port number
11	0x0B	Port closing error: Unopened port number
14	0x0E	MAC connection failed
15	0x0F	Executability error: Unexecutable due to HAN in the operating status/Mismatched operation mode
16	0x10	Executability error: Unexecutable due to Route B or HAN in the not-yet-started status/Mismatched operation mode
17	0x11	The specified parameter length exceeded the maximum length or was less than the minimum length
18	0x12	Maximum number of opened ports exceeded
19	0x13	Command reception error: Data reception time (1 second) expired
20	0x14	Executability error: Unexecutable operation mode
32	0x20	The same mode was specified as the current mode by **Switch HAN Acceptance Connection Mode Request** command
33	0x21	Executability error: Operation mode in which **Switch HAN Acceptance Connection Mode** is unexecutable
51	0x33	Executability error: Unexecutable due to HAN in the authentication status/Mismatched operation mode
52	0x34	Executability error: Unexecutable due to Route B in the operating status
53	0x35	Executability error: Unexecutable due to Route B in the authentication status
55	0x37	Executability error: Unexecutable due to the whole block in the not-yet-started status
60	0x3C	Cases where **Transmit To Ping Request** command is requested again before executing **Transmit To Ping Notification** command
61	0x3D	Cases where a different **Request** command is executed before the **Response** command is executed or its internal processing is in progress
62	0x3E	Cases where the same PAN ID as that for Route B or 0xFFFF is specified
63	0x3F	Cases where transition to deep sleep mode is failed
70	0x46	Cases where a poll request is failed
81	0x51	PANA execution error: Inadequate setting or information ungenerated
82	0x52	PANA execution error: PANA sequence in operation
83	0x53	PANA execution error: No information in the specified address
88	0x58	PANA execution error: authentication information has been set
89	0x59	PANA execution error: Maximum set number exceeded
97	0x61	Invalid OTA Client status

Table 34: List of response results to Request command (continued)

Response result (DEC)	Response result (HEX)	Description
240	0xF0	Command reception error: Header checksum error
241	0xF1	Command reception error: Data checksum error
242	0xF2	Command reception error: Message length specified by the header is short
243	0xF3	Command reception error: Message length specified by the header exceeded the maximum length

5. Command sequences

This Chapter describes a series of operating sequences that are generated after a **Request** command is issued.

5.1 Sequence of Reset Hardware

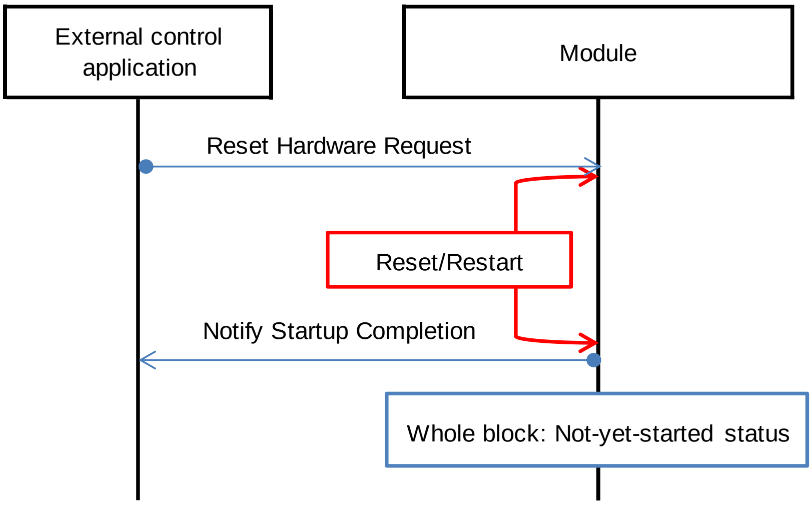
External control application
Module
Reset Hardware Request
Reset/Restart
Notify Startup Completion
Whole block: Not-yet-started status

Fig. 5: Sequence of Reset Hardware

5.2 Sequence of Execute Active Scan

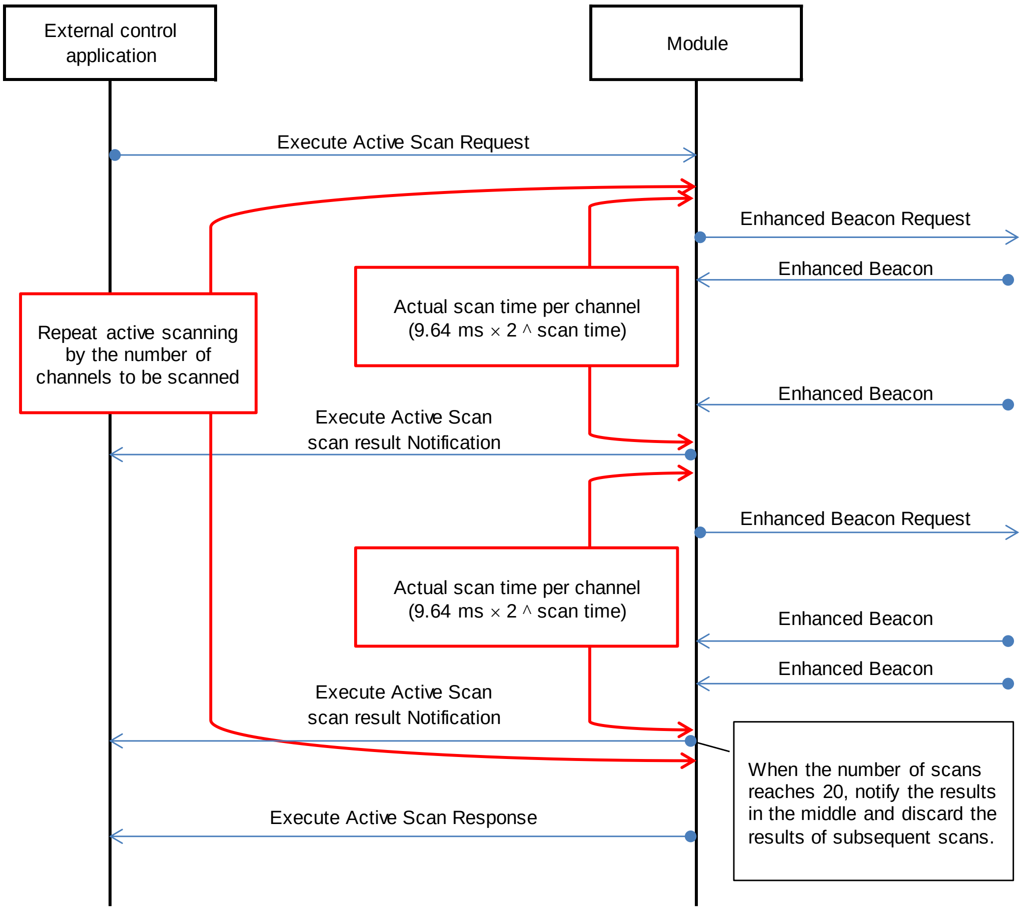
External control application
Module
Execute Active Scan Request
Enhanced Beacon Request
Enhanced Beacon
Repeat active scanning by the number of channels to be scanned
Actual scan time per channel (9.64 ms × 2 ^ scan time)
Enhanced Beacon
Execute Active Scan scan result Notification
Enhanced Beacon Request
Actual scan time per channel (9.64 ms × 2 ^ scan time)
Enhanced Beacon
Enhanced Beacon
Execute Active Scan scan result Notification
When the number of scans reaches 20, notify the results in the middle and discard the results of subsequent scans.
Execute Active Scan Response

Fig. 6: Sequence of Execute Active Scan

5.3 Sequence of Initiate HAN Operation

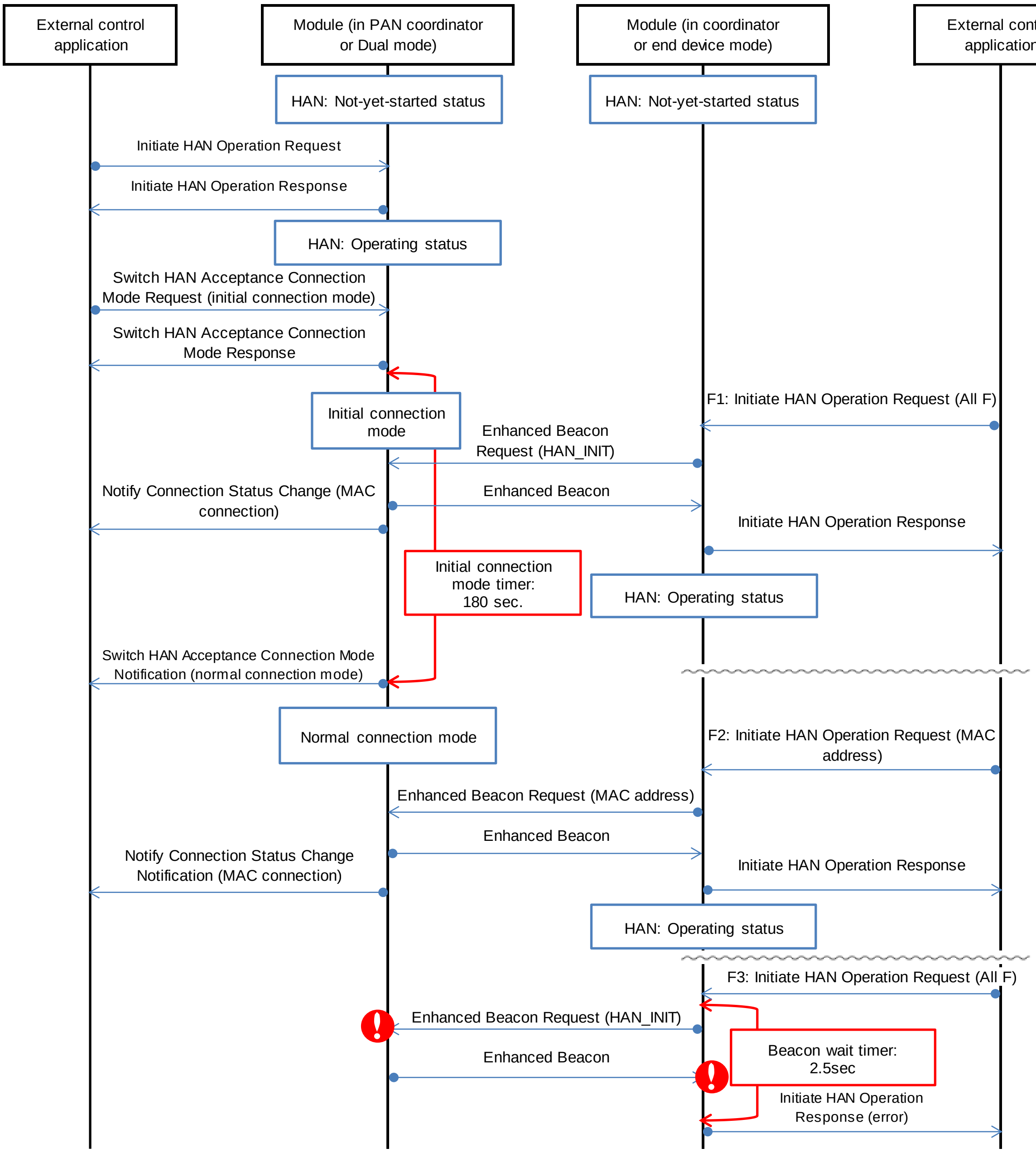
External control application
Module (in PAN coordinator or Dual mode)
Module (in coordinator or end device mode)
External control application
HAN: Not-yet-started status
HAN: Not-yet-started status
Initiate HAN Operation Request
Initiate HAN Operation Response
HAN: Operating status
Switch HAN Acceptance Connection Mode Request (initial connection mode)
Switch HAN Acceptance Connection Mode Response
Initial connection mode
F1: Initiate HAN Operation Request (All F)
Enhanced Beacon Request (HAN_INIT)
Notify Connection Status Change (MAC connection)
Enhanced Beacon
Initiate HAN Operation Response
Initial connection mode timer: 180 sec.
HAN: Operating status
Switch HAN Acceptance Connection Mode Notification (normal connection mode)
Normal connection mode
F2: Initiate HAN Operation Request (MAC address)
Enhanced Beacon Request (MAC address)
Enhanced Beacon
Notify Connection Status Change Notification (MAC connection)
Initiate HAN Operation Response
HAN: Operating status
F3: Initiate HAN Operation Request (All F)
Enhanced Beacon Request (HAN_INIT)
Beacon wait timer: 2.5sec
Enhanced Beacon
Initiate HAN Operation Response (error)

Fig. 7: Sequence of Initiate HAN Operation

5.4 Sequence of Terminate HAN Operation

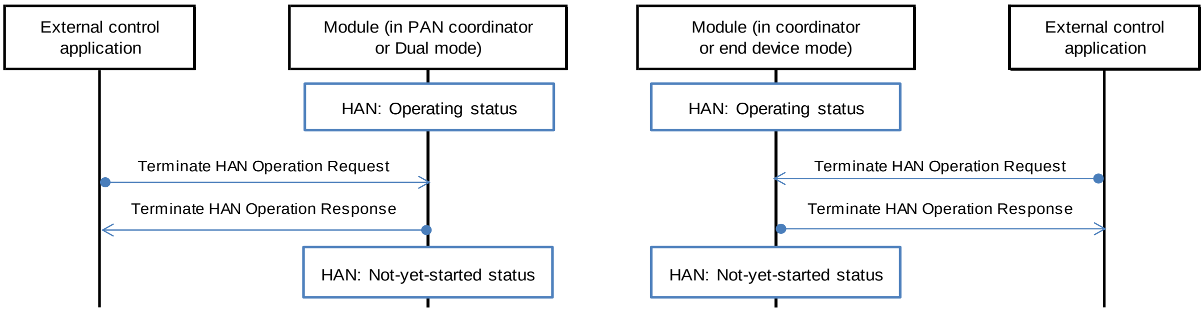
External control application
Module (in PAN coordinator or Dual mode)
Module (in coordinator or end device mode)
External control application
HAN: Operating status
HAN: Operating status
Terminate HAN Operation Request
Terminate HAN Operation Request
Terminate HAN Operation Response
Terminate HAN Operation Response
HAN: Not-yet-started status
HAN: Not-yet-started status

Fig. 8: Sequence of Terminate HAN Operation

5.5 Sequence of Initiate HAN PANA

5.5.1 Sequence of Initiate HAN PANA (without indirect communication)

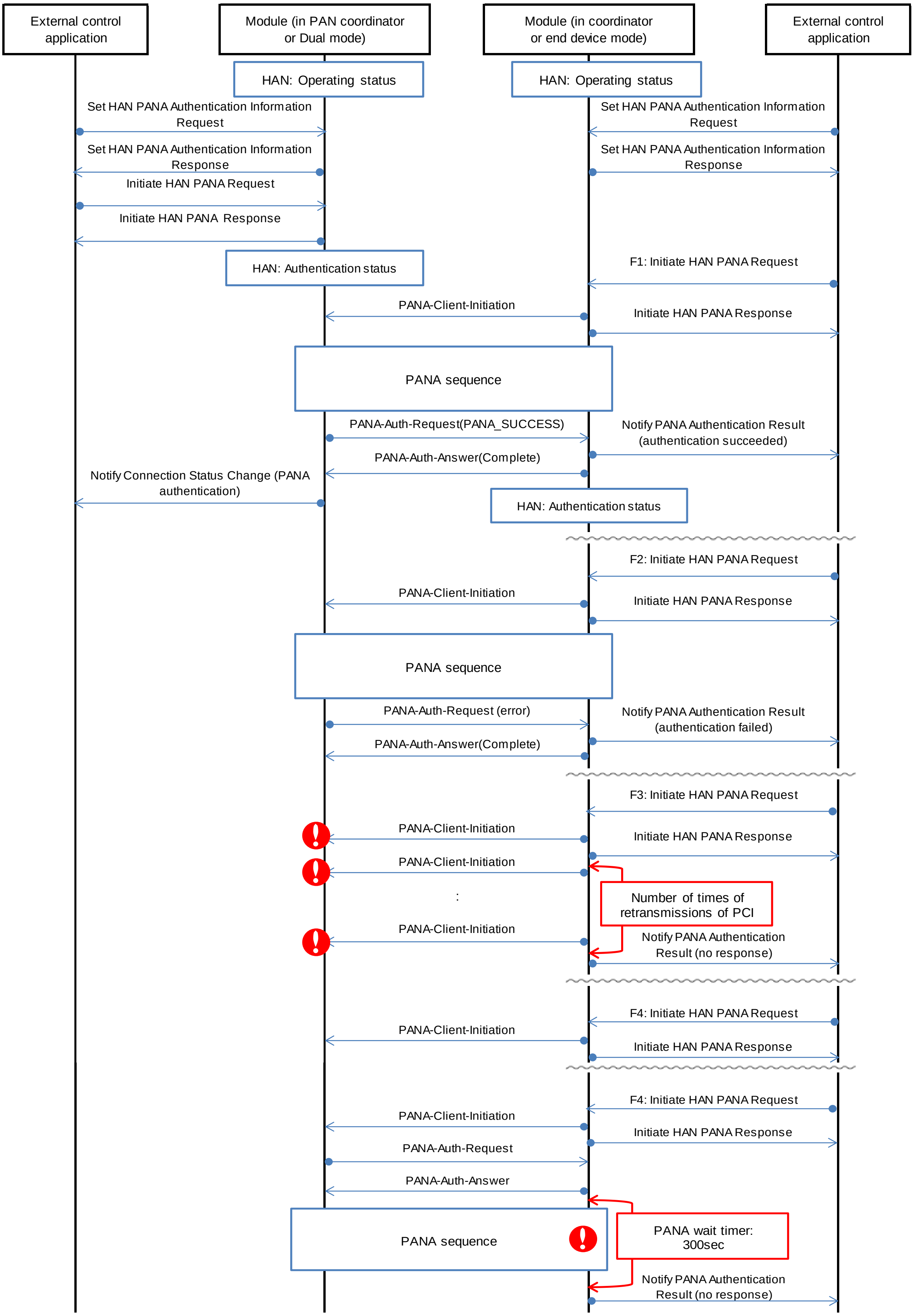
External control application
Module (in PAN coordinator or Dual mode)
Module (in coordinator or end device mode)
External control application
HAN: Operating status
HAN: Operating status
Set HAN PANA Authentication Information Request
Set HAN PANA Authentication Information Request
Set HAN PANA Authentication Information Response
Set HAN PANA Authentication Information Response
Initiate HAN PANA Request
Initiate HAN PANA Response
HAN: Authentication status
F1: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
PANA sequence
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
PANA-Auth-Answer(Complete)
Notify Connection Status Change (PANA authentication)
HAN: Authentication status
F2: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
PANA sequence
PANA-Auth-Request (error)
Notify PANA Authentication Result (authentication failed)
PANA-Auth-Answer(Complete)
F3: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
PANA-Client-Initiation
Number of times of retransmissions of PCI
:
PANA-Client-Initiation
Notify PANA Authentication Result (no response)
F4: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
F4: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
PANA-Auth-Request
PANA-Auth-Answer
PANA sequence
PANA wait timer: 300sec
Notify PANA Authentication Result (no response)

Fig. 9: Sequence of Initiate HAN PANA (with HAN sleep function disabled)

5.5.2 Sequence of Initiate HAN PANA (with indirect communication)

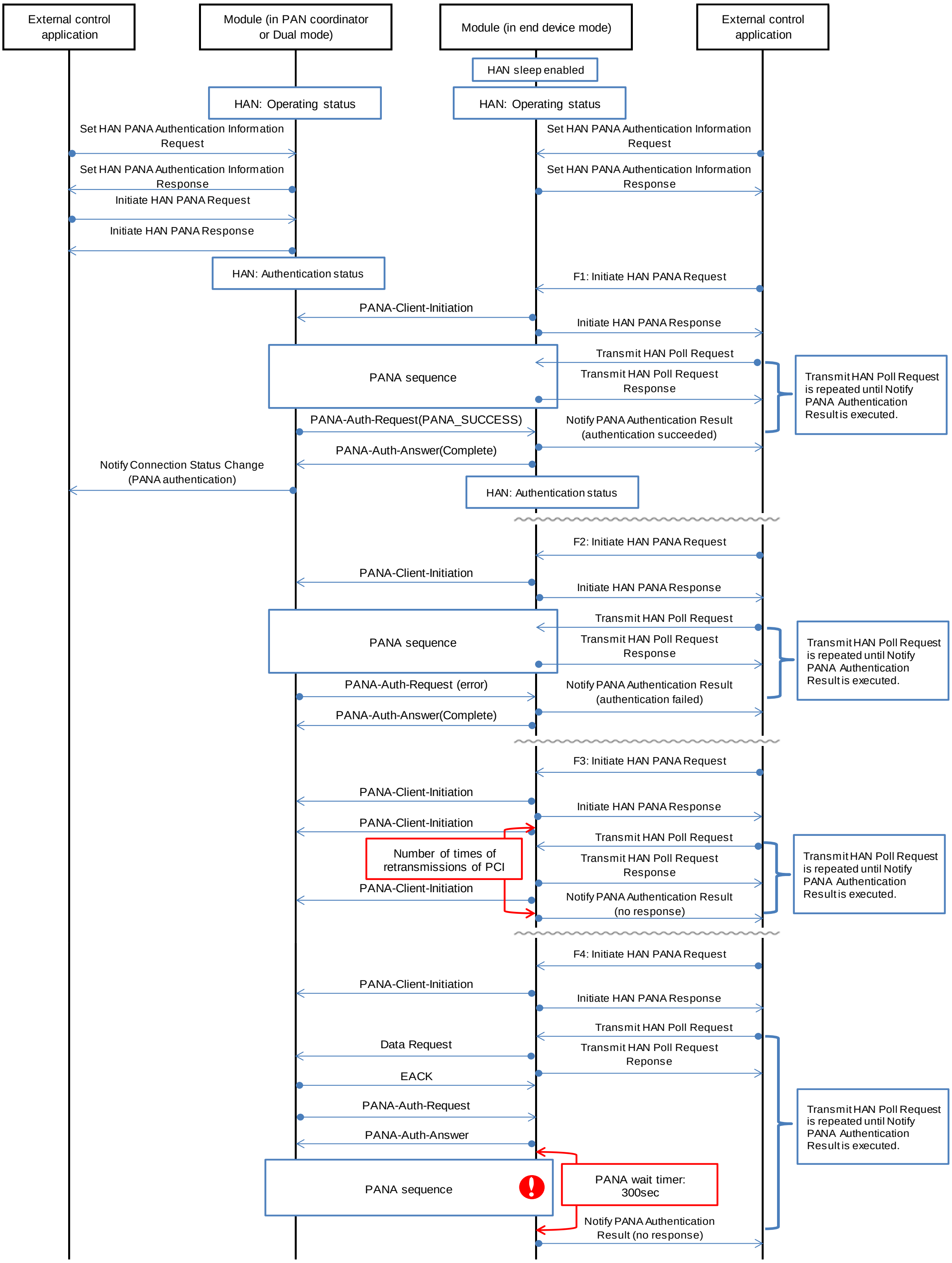
External control application
Module (in PAN coordinator or Dual mode)
Module (in end device mode)
External control application
HAN sleep enabled
HAN: Operating status
HAN: Operating status
Set HAN PANA Authentication Information Request
Set HAN PANA Authentication Information Request
Set HAN PANA Authentication Information Response
Set HAN PANA Authentication Information Response
Initiate HAN PANA Request
Initiate HAN PANA Response
HAN: Authentication status
F1: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
Transmit HAN Poll Request
PANA sequence
Transmit HAN Poll Request Response
Transmit HAN Poll Request is repeated until Notify PANA Authentication Result is executed.
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
PANA-Auth-Answer(Complete)
Notify Connection Status Change (PANA authentication)
HAN: Authentication status
F2: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
Transmit HAN Poll Request
PANA sequence
Transmit HAN Poll Request Response
Transmit HAN Poll Request is repeated until Notify PANA Authentication Result is executed.
PANA-Auth-Request (error)
Notify PANA Authentication Result (authentication failed)
PANA-Auth-Answer(Complete)
F3: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
PANA-Client-Initiation
Transmit HAN Poll Request
Number of times of retransmissions of PCI
Transmit HAN Poll Request Response
Transmit HAN Poll Request is repeated until Notify PANA Authentication Result is executed.
PANA-Client-Initiation
Notify PANA Authentication Result (no response)
F4: Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
Transmit HAN Poll Request
Data Request
Transmit HAN Poll Request Reponse
EACK
PANA-Auth-Request
Transmit HAN Poll Request is repeated until Notify PANA Authentication Result is executed.
PANA-Auth-Answer
PANA sequence
PANA wait timer: 300sec
Notify PANA Authentication Result (no response)

Fig. 10: Sequence of Initiate HAN PANA (with HAN sleep function disabled)

5.6 Sequence of Terminate HAN PANA

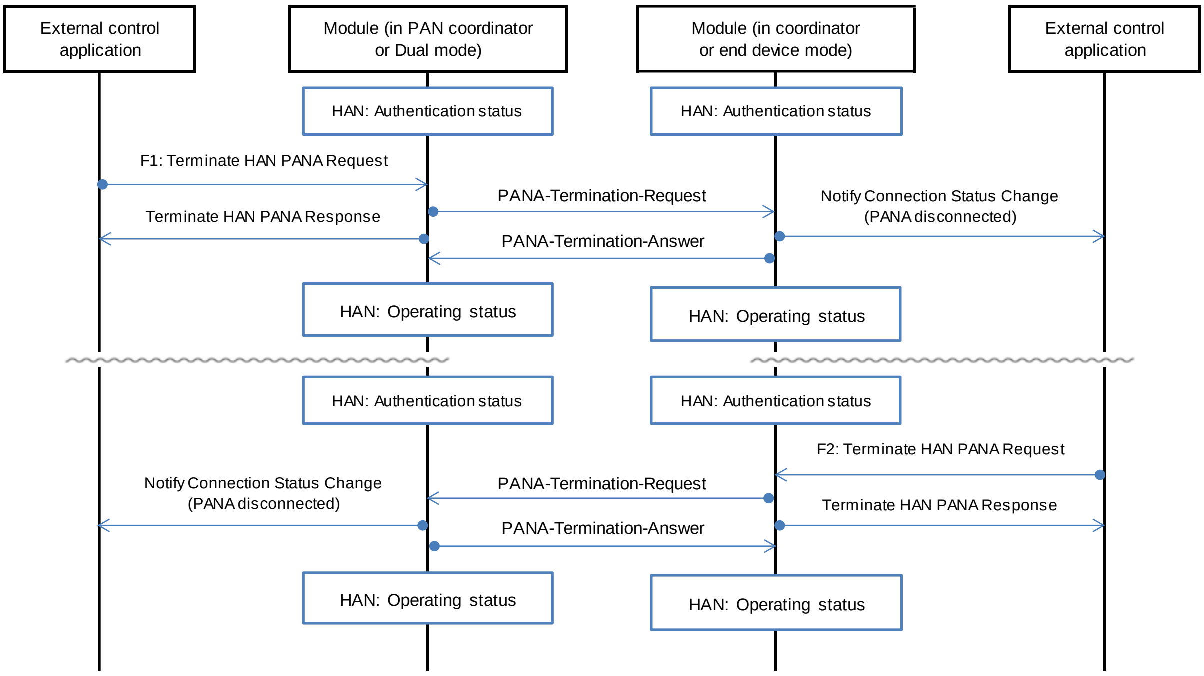
External control application
Module (in PAN coordinator or Dual mode)
Module (in coordinator or end device mode)
External control application
HAN: Authentication status
HAN: Authentication status
F1: Terminate HAN PANA Request
PANA-Termination-Request
Notify Connection Status Change (PANA disconnected)
Terminate HAN PANA Response
PANA-Termination-Answer
HAN: Operating status
HAN: Operating status
HAN: Authentication status
HAN: Authentication status
F2: Terminate HAN PANA Request
Notify Connection Status Change (PANA disconnected)
PANA-Termination-Request
Terminate HAN PANA Response
PANA-Termination-Answer
HAN: Operating status
HAN: Operating status

Fig. 11: Sequence of Terminate HAN PANA

5.7 Sequence of Distribute HAN Group Key (push)

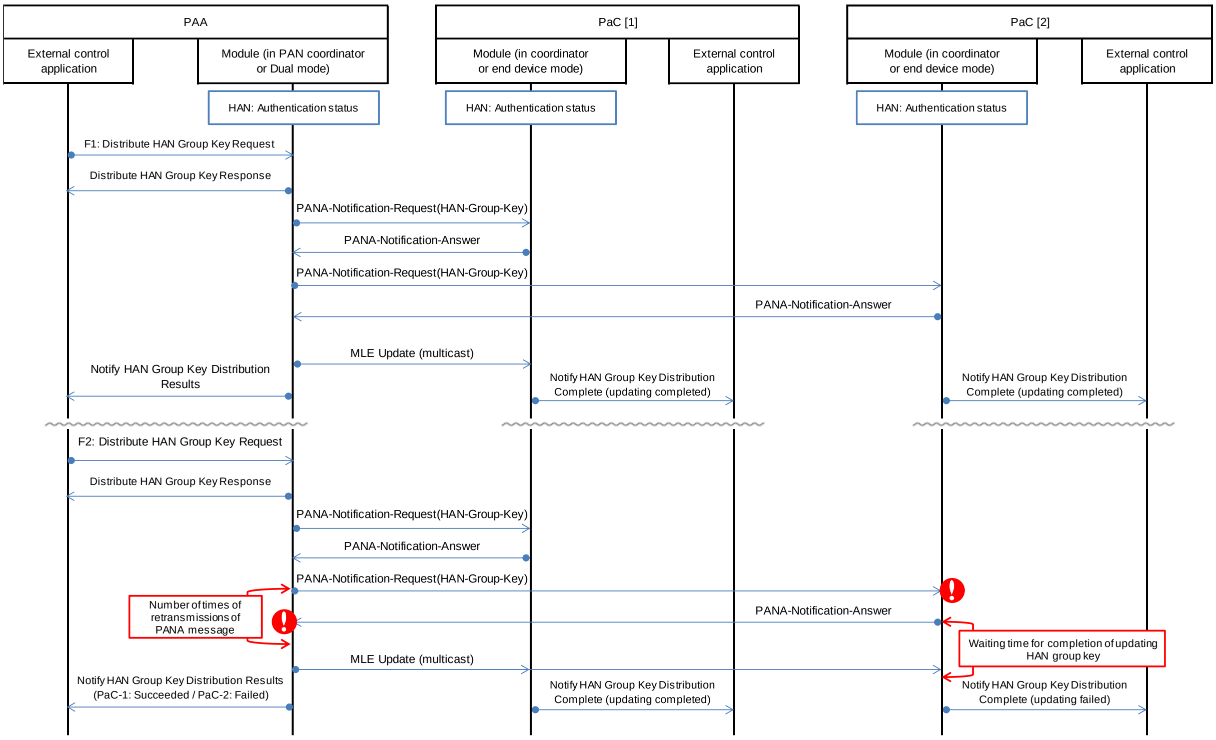
PAA
External control application
Module (in PAN coordinator or Dual mode)
PaC [1]
Module (in coordinator or end device mode)
External control application
PaC [2]
Module (in coordinator or end device mode)
External control application
HAN: Authentication status
HAN: Authentication status
HAN: Authentication status
F1: Distribute HAN Group Key Request
Distribute HAN Group Key Response
PANA-Notification-Request(HAN-Group-Key)
PANA-Notification-Answer
PANA-Notification-Request(HAN-Group-Key)
PANA-Notification-Answer
MLE Update (multicast)
Notify HAN Group Key Distribution Results
Notify HAN Group Key Distribution Complete (updating completed)
Notify HAN Group Key Distribution Complete (updating completed)
F2: Distribute HAN Group Key Request
Distribute HAN Group Key Response
PANA-Notification-Request(HAN-Group-Key)
PANA-Notification-Answer
PANA-Notification-Request(HAN-Group-Key)
Number of times of retransmissions of PANA message
PANA-Notification-Answer
Waiting time for completion of updating HAN group key
MLE Update (multicast)
Notify HAN Group Key Distribution Results (PaC-1: Succeeded / PaC-2: Failed)
Notify HAN Group Key Distribution Complete (updating completed)
Notify HAN Group Key Distribution Complete (updating failed)

Fig. 12: Sequence of Distribute HAN Group Key (push)

5.8 Sequence of Check HAN Group Key Update (pull)

5.8.1 Sequence of Check HAN Group Key Update (pull) (without indirect communication)

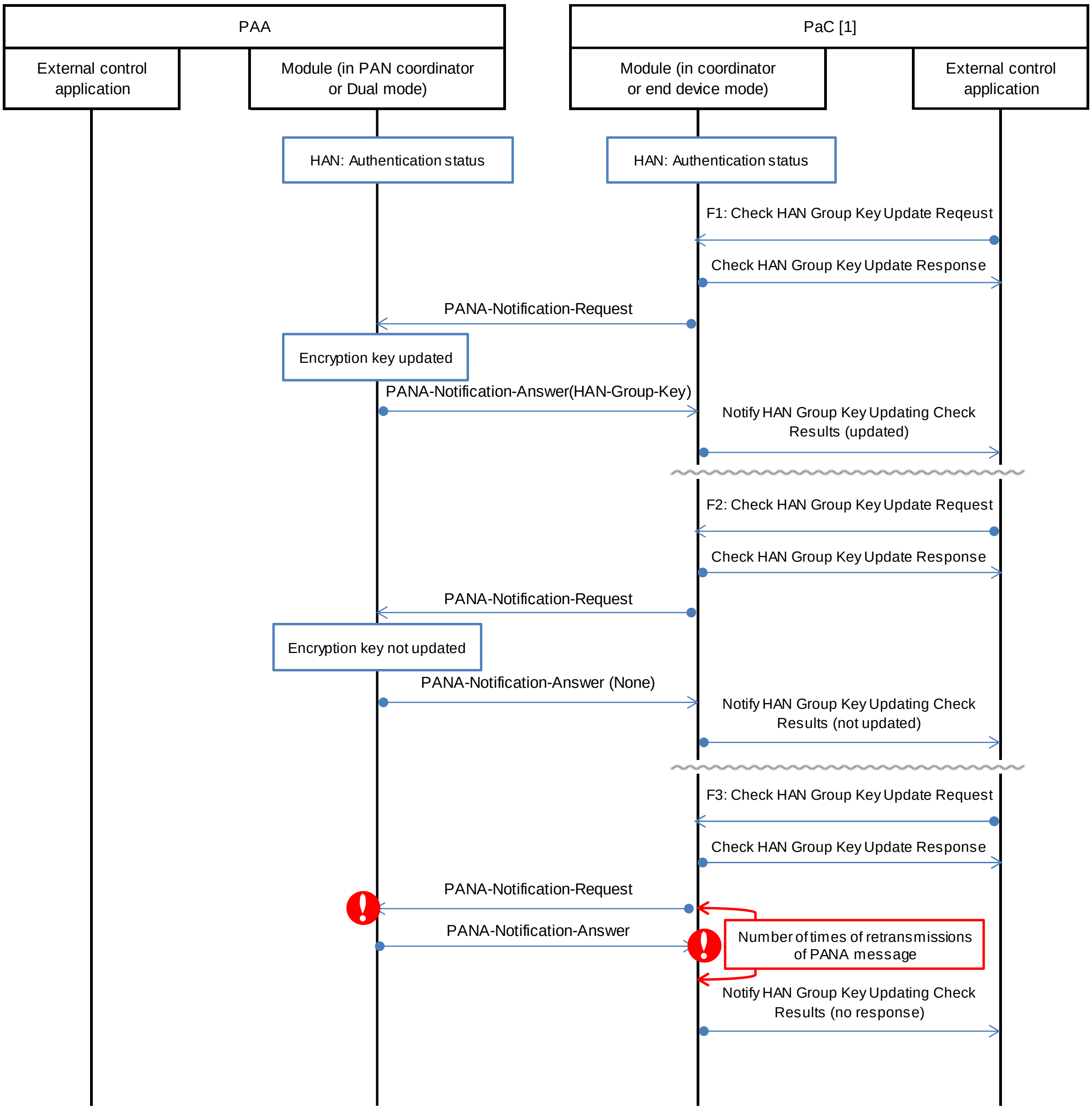
PAA
External control application
Module (in PAN coordinator or Dual mode)
PaC [1]
Module (in coordinator or end device mode)
External control application
HAN: Authentication status
HAN: Authentication status
F1: Check HAN Group Key Update Reqeust
Check HAN Group Key Update Response
PANA-Notification-Request
Encryption key updated
PANA-Notification-Answer(HAN-Group-Key)
Notify HAN Group Key Updating Check Results (updated)
F2: Check HAN Group Key Update Request
Check HAN Group Key Update Response
PANA-Notification-Request
Encryption key not updated
PANA-Notification-Answer (None)
Notify HAN Group Key Updating Check Results (not updated)
F3: Check HAN Group Key Update Request
Check HAN Group Key Update Response
PANA-Notification-Request
PANA-Notification-Answer
Number of times of retransmissions of PANA message
Notify HAN Group Key Updating Check Results (no response)

Fig. 13: Sequence of Check HAN Group Key Update (pull) (without indirect communication)

5.8.2 Sequence of Check HAN Group Key Update (pull) (with indirect communication)

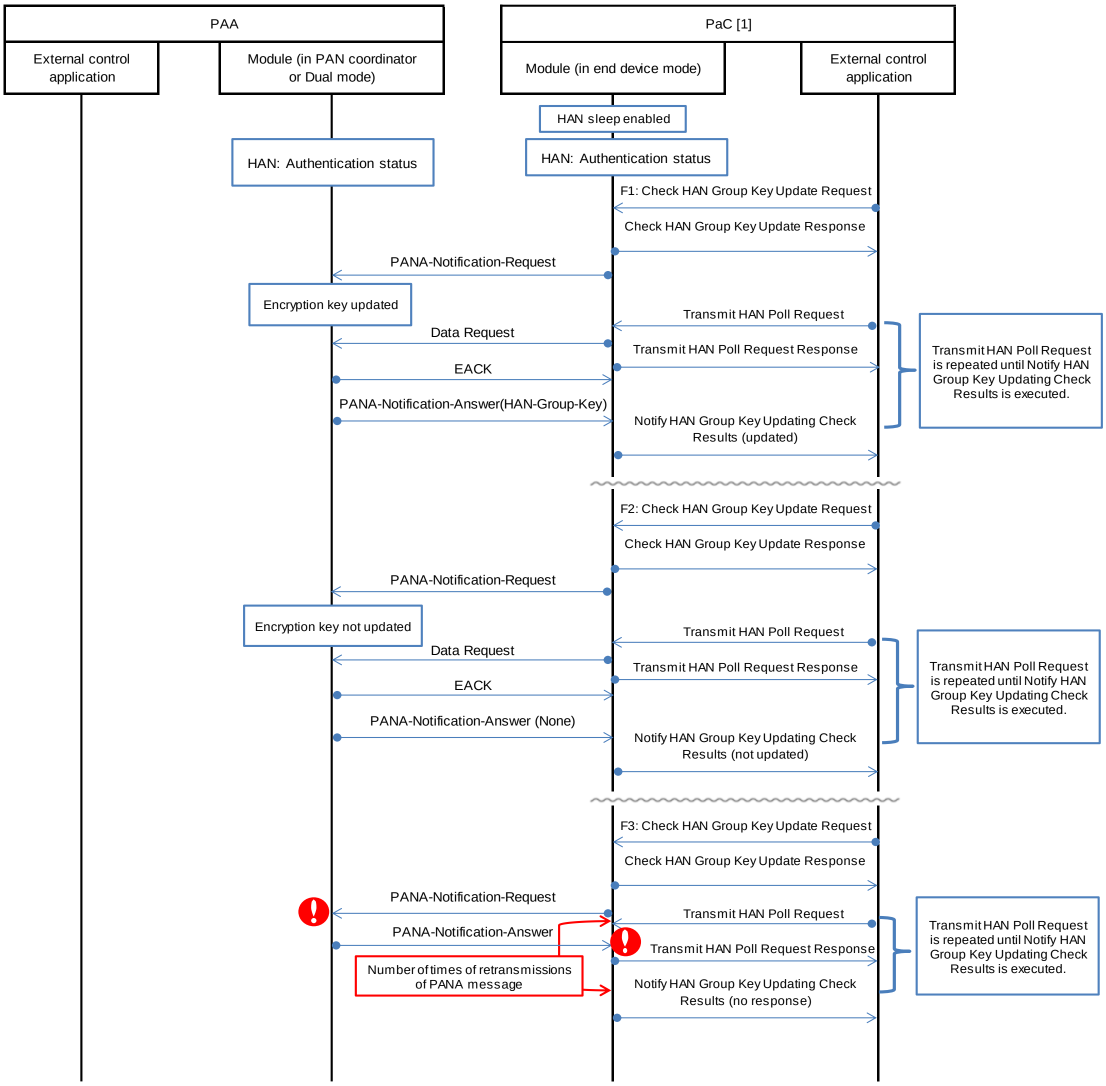
PAA
External control application
Module (in PAN coordinator or Dual mode)
PaC [1]
Module (in end device mode)
External control application
HAN sleep enabled
HAN: Authentication status
HAN: Authentication status
F1: Check HAN Group Key Update Request
Check HAN Group Key Update Response
PANA-Notification-Request
Encryption key updated
Transmit HAN Poll Request
Data Request
Transmit HAN Poll Request Response
EACK
PANA-Notification-Answer(HAN-Group-Key)
Notify HAN Group Key Updating Check Results (updated)
Transmit HAN Poll Request is repeated until Notify HAN Group Key Updating Check Results is executed.
F2: Check HAN Group Key Update Request
Check HAN Group Key Update Response
PANA-Notification-Request
Encryption key not updated
Transmit HAN Poll Request
Data Request
Transmit HAN Poll Request Response
EACK
PANA-Notification-Answer (None)
Notify HAN Group Key Updating Check Results (not updated)
Transmit HAN Poll Request is repeated until Notify HAN Group Key Updating Check Results is executed.
F3: Check HAN Group Key Update Request
Check HAN Group Key Update Response
PANA-Notification-Request
Transmit HAN Poll Request
PANA-Notification-Answer
Transmit HAN Poll Request Response
Number of times of retransmissions of PANA message
Notify HAN Group Key Updating Check Results (no response)
Transmit HAN Poll Request is repeated until Notify HAN Group Key Updating Check Results is executed.

Fig. 14: Sequence of Check HAN Group Key Update (pull) (with indirect communication)

5.9 Sequence of Re-authenticate HAN PANA

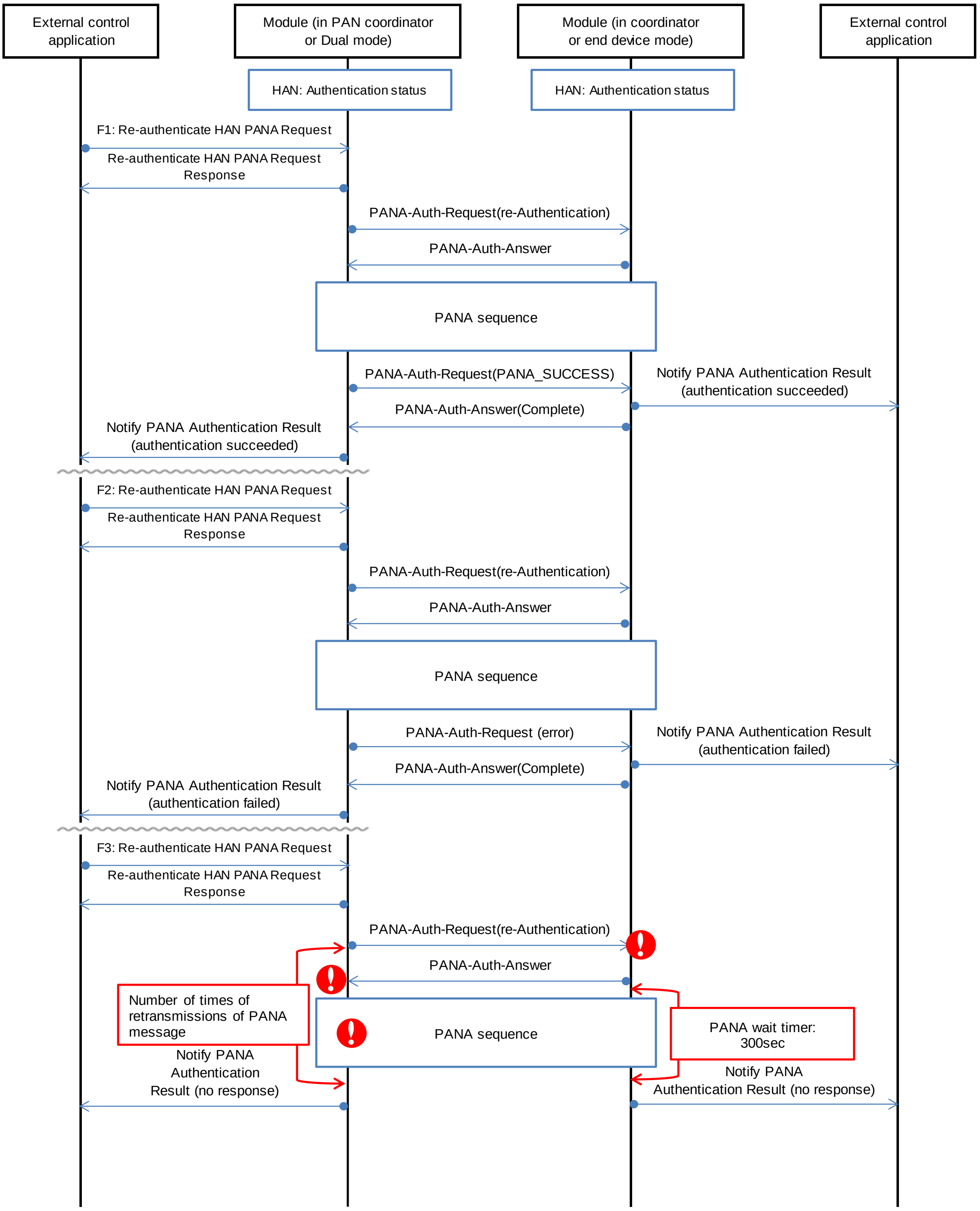
External control application
Module (in PAN coordinator or Dual mode)
Module (in coordinator or end device mode)
External control application
HAN: Authentication status
HAN: Authentication status
F1: Re-authenticate HAN PANA Request
Re-authenticate HAN PANA Request Response
PANA-Auth-Request(re-Authentication)
PANA-Auth-Answer
PANA sequence
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
PANA-Auth-Answer(Complete)
Notify PANA Authentication Result (authentication succeeded)
F2: Re-authenticate HAN PANA Request
Re-authenticate HAN PANA Request Response
PANA-Auth-Request(re-Authentication)
PANA-Auth-Answer
PANA sequence
PANA-Auth-Request (error)
Notify PANA Authentication Result (authentication failed)
PANA-Auth-Answer(Complete)
Notify PANA Authentication Result (authentication failed)
F3: Re-authenticate HAN PANA Request
Re-authenticate HAN PANA Request Response
PANA-Auth-Request(re-Authentication)
PANA-Auth-Answer
Number of times of retransmissions of PANA message
PANA sequence
PANA wait timer: 300sec
Notify PANA Authentication Result (no response)
Notify PANA Authentication Result (no response)

Fig. 15: Sequence of Re-authenticate HAN PANA

5.10 Sequence of Disconnect HAN

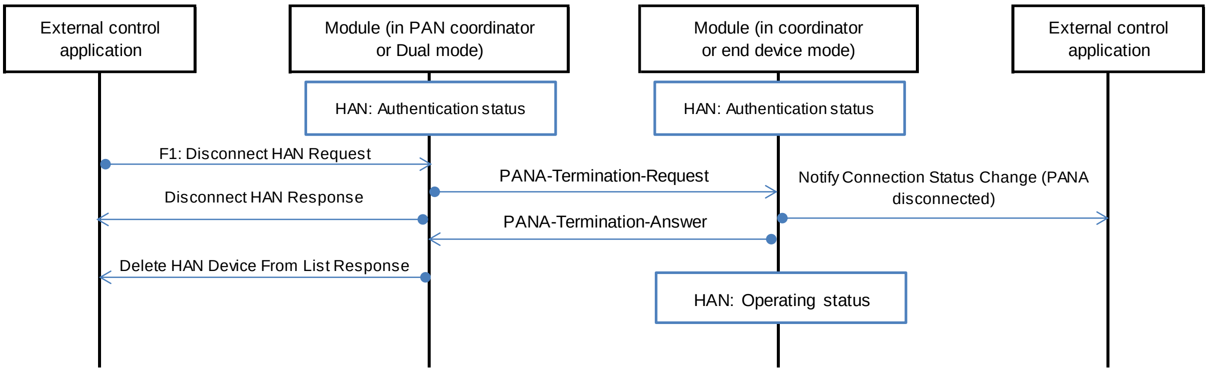
External control application
Module (in PAN coordinator or Dual mode)
Module (in coordinator or end device mode)
External control application
HAN: Authentication status
HAN: Authentication status
F1: Disconnect HAN Request
PANA-Termination-Request
Notify Connection Status Change (PANA disconnected)
Disconnect HAN Response
PANA-Termination-Answer
Delete HAN Device From List Response
HAN: Operating status

Fig. 16: Sequence of Disconnect HAN

5.11 Sequence of Set HAN Sleep Device PANA Retransmission Interval

5.11.1 Sequence of Set HAN Sleep Device PANA Retransmission Interval (with indirect communication)

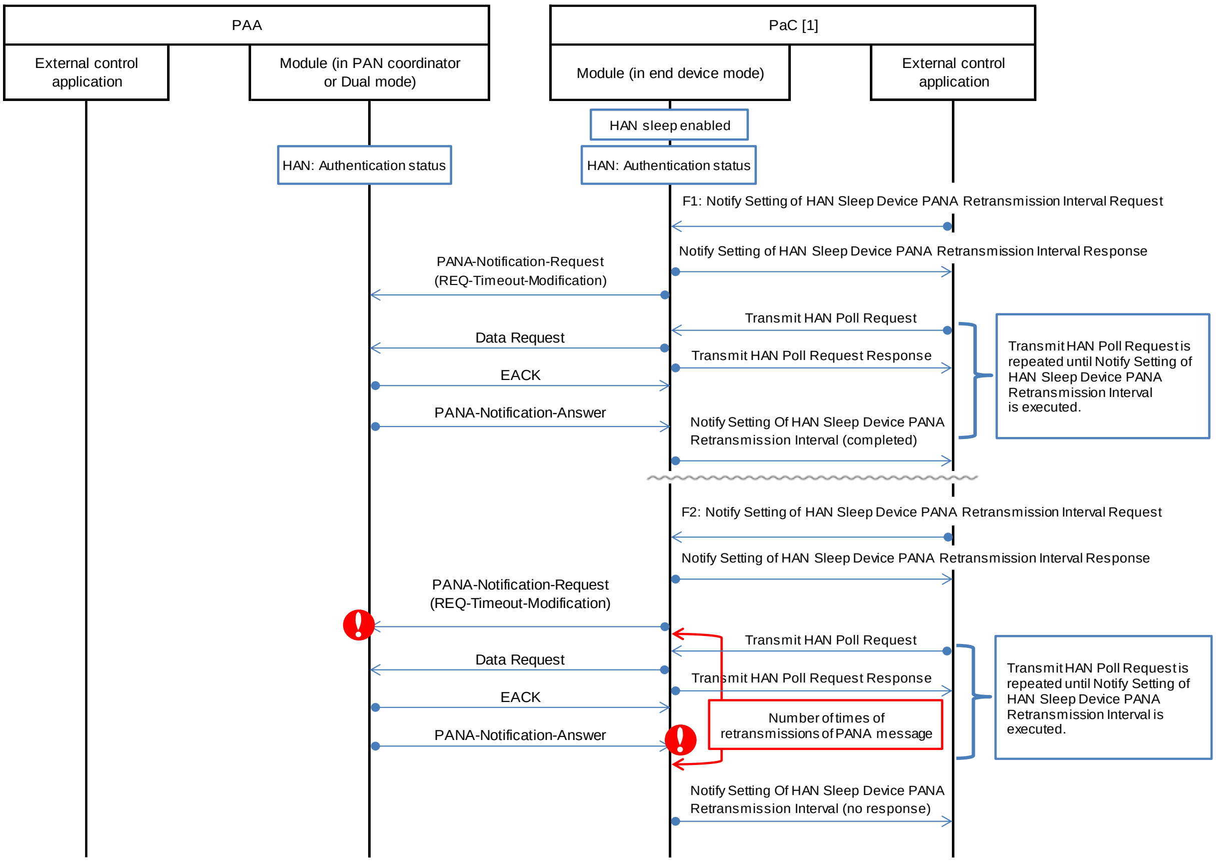
PAA
External control application
Module (in PAN coordinator or Dual mode)
PaC [1]
Module (in end device mode)
External control application
HAN sleep enabled
HAN: Authentication status
HAN: Authentication status
F1: Notify Setting of HAN Sleep Device PANA Retransmission Interval Request
Notify Setting of HAN Sleep Device PANA Retransmission Interval Response
PANA-Notification-Request (REQ-Timeout-Modification)
Transmit HAN Poll Request
Data Request
Transmit HAN Poll Request Response
EACK
PANA-Notification-Answer
Notify Setting Of HAN Sleep Device PANA Retransmission Interval (completed)
Transmit HAN Poll Request is repeated until Notify Setting of HAN Sleep Device PANA Retransmission Interval is executed.
F2: Notify Setting of HAN Sleep Device PANA Retransmission Interval Request
Notify Setting of HAN Sleep Device PANA Retransmission Interval Response
PANA-Notification-Request (REQ-Timeout-Modification)
Transmit HAN Poll Request
Data Request
Transmit HAN Poll Request Response
EACK
Number of times of retransmissions of PANA message
PANA-Notification-Answer
Notify Setting Of HAN Sleep Device PANA Retransmission Interval (no response)
Transmit HAN Poll Request is repeated until Notify Setting of HAN Sleep Device PANA Retransmission Interval is executed.

Fig. 17: Sequence of Set HAN Sleep Device PANA Retransmission Interval (with indirect communication)

5.12 Sequence of Transmit Data and Notify Data Reception

5.12.1 Sequence of Transmit Data and Notify Data Reception (without ND)

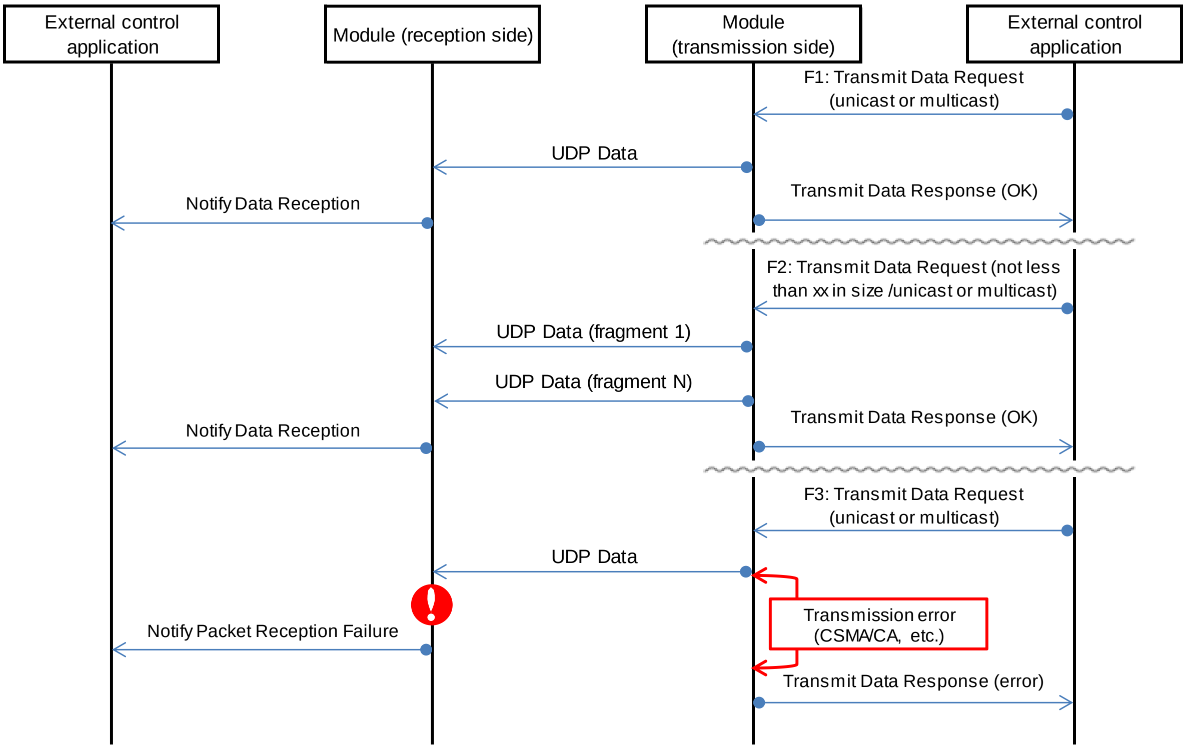
External control application
Module (reception side)
Module (transmission side)
External control application
F1: Transmit Data Request (unicast or multicast)
UDP Data
Transmit Data Response (OK)
Notify Data Reception
F2: Transmit Data Request (not less than xx in size /unicast or multicast)
UDP Data (fragment 1)
UDP Data (fragment N)
Transmit Data Response (OK)
Notify Data Reception
F3: Transmit Data Request (unicast or multicast)
UDP Data
Transmission error (CSMA/CA, etc.)
Notify Packet Reception Failure
Transmit Data Response (error)

Fig. 18: Sequence of Transmit Data and Notify Data Reception (without ND)

5.12.2 Sequence of Transmit Data and Notify Data Reception (with ND)

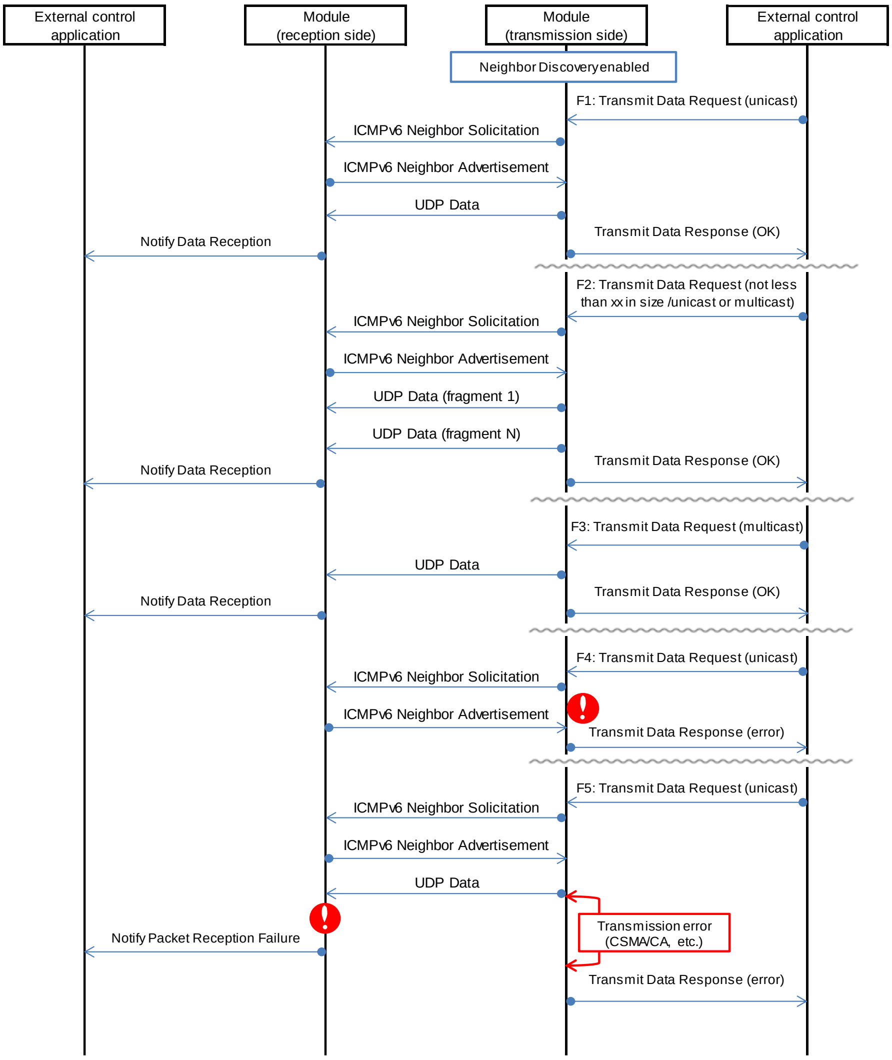
External control application
Module (reception side)
Module (transmission side)
External control application
Neighbor Discovery enabled
F1: Transmit Data Request (unicast)
ICMPv6 Neighbor Solicitation
ICMPv6 Neighbor Advertisement
UDP Data
Transmit Data Response (OK)
Notify Data Reception
F2: Transmit Data Request (not less than xx in size /unicast or multicast)
ICMPv6 Neighbor Solicitation
ICMPv6 Neighbor Advertisement
UDP Data (fragment 1)
UDP Data (fragment N)
Transmit Data Response (OK)
Notify Data Reception
F3: Transmit Data Request (multicast)
UDP Data
Transmit Data Response (OK)
Notify Data Reception
F4: Transmit Data Request (unicast)
ICMPv6 Neighbor Solicitation
ICMPv6 Neighbor Advertisement
Transmit Data Response (error)
F5: Transmit Data Request (unicast)
ICMPv6 Neighbor Solicitation
ICMPv6 Neighbor Advertisement
UDP Data
Transmission error (CSMA/CA, etc.)
Notify Packet Reception Failure
Transmit Data Response (error)

Fig. 19: Sequence of Transmit Data and Notify Data Reception (with ND)

5.12.3 Sequence of Transmit Data and Notify Data Reception (with indirect communication) - (1)

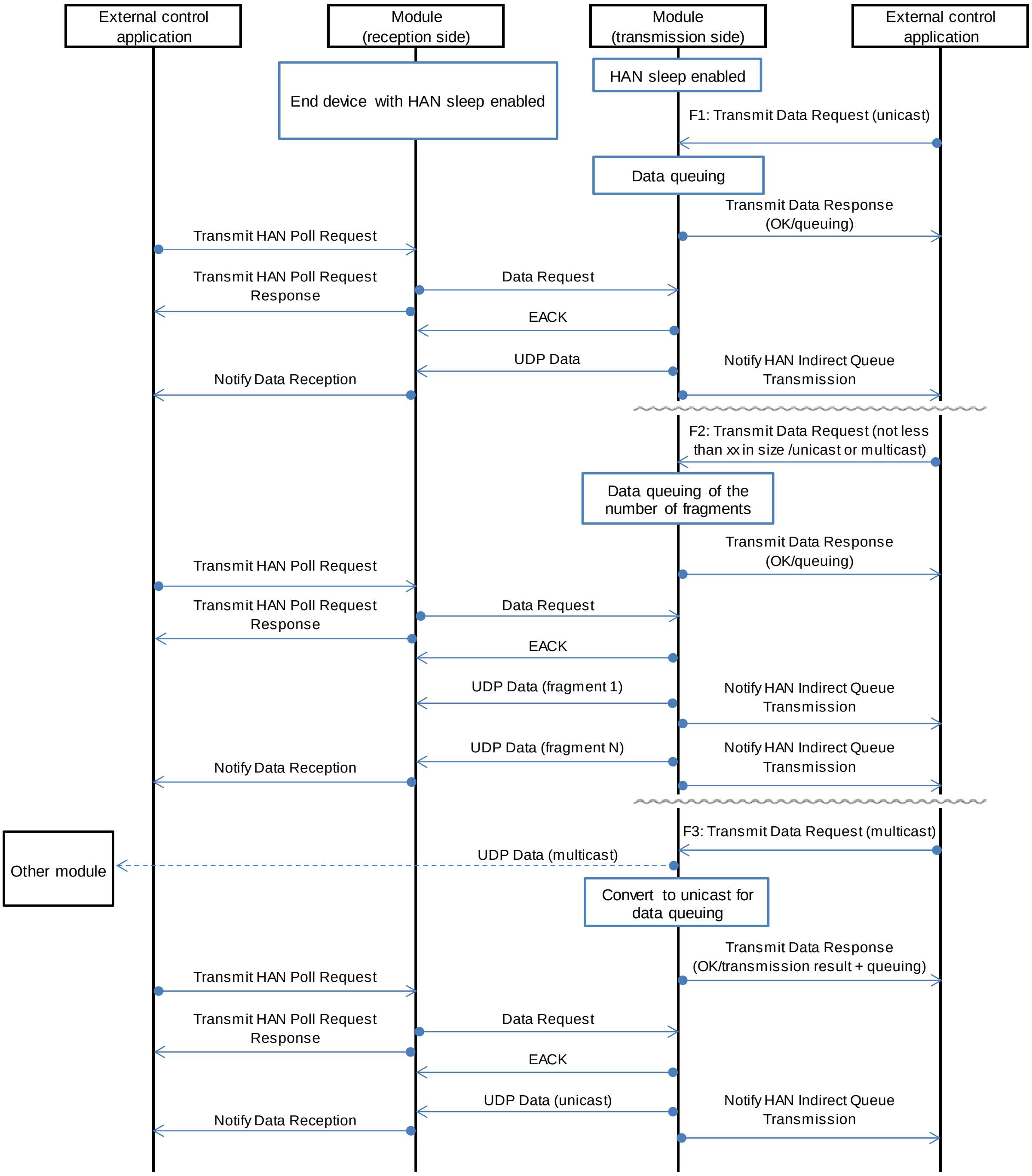
External control application
Module (reception side)
Module (transmission side)
External control application
End device with HAN sleep enabled
HAN sleep enabled
F1: Transmit Data Request (unicast)
Data queuing
Transmit Data Response (OK/queuing)
Transmit HAN Poll Request
Transmit HAN Poll Request Response
Data Request
EACK
UDP Data
Notify Data Reception
Notify HAN Indirect Queue Transmission
F2: Transmit Data Request (not less than xx in size /unicast or multicast)
Data queuing of the number of fragments
Transmit Data Response (OK/queuing)
Transmit HAN Poll Request
Transmit HAN Poll Request Response
Data Request
EACK
UDP Data (fragment 1)
Notify HAN Indirect Queue Transmission
UDP Data (fragment N)
Notify HAN Indirect Queue Transmission
Notify Data Reception
F3: Transmit Data Request (multicast)
Other module
UDP Data (multicast)
Convert to unicast for data queuing
Transmit Data Response (OK/transmission result + queuing)
Transmit HAN Poll Request
Transmit HAN Poll Request Response
Data Request
EACK
UDP Data (unicast)
Notify HAN Indirect Queue Transmission
Notify Data Reception

Fig. 20: Sequence of Transmit Data and Notify Data Reception (with indirect communication) - (1)

5.12.4 Sequence of Transmit Data and Notify Data Reception (with indirect communication) - (2)

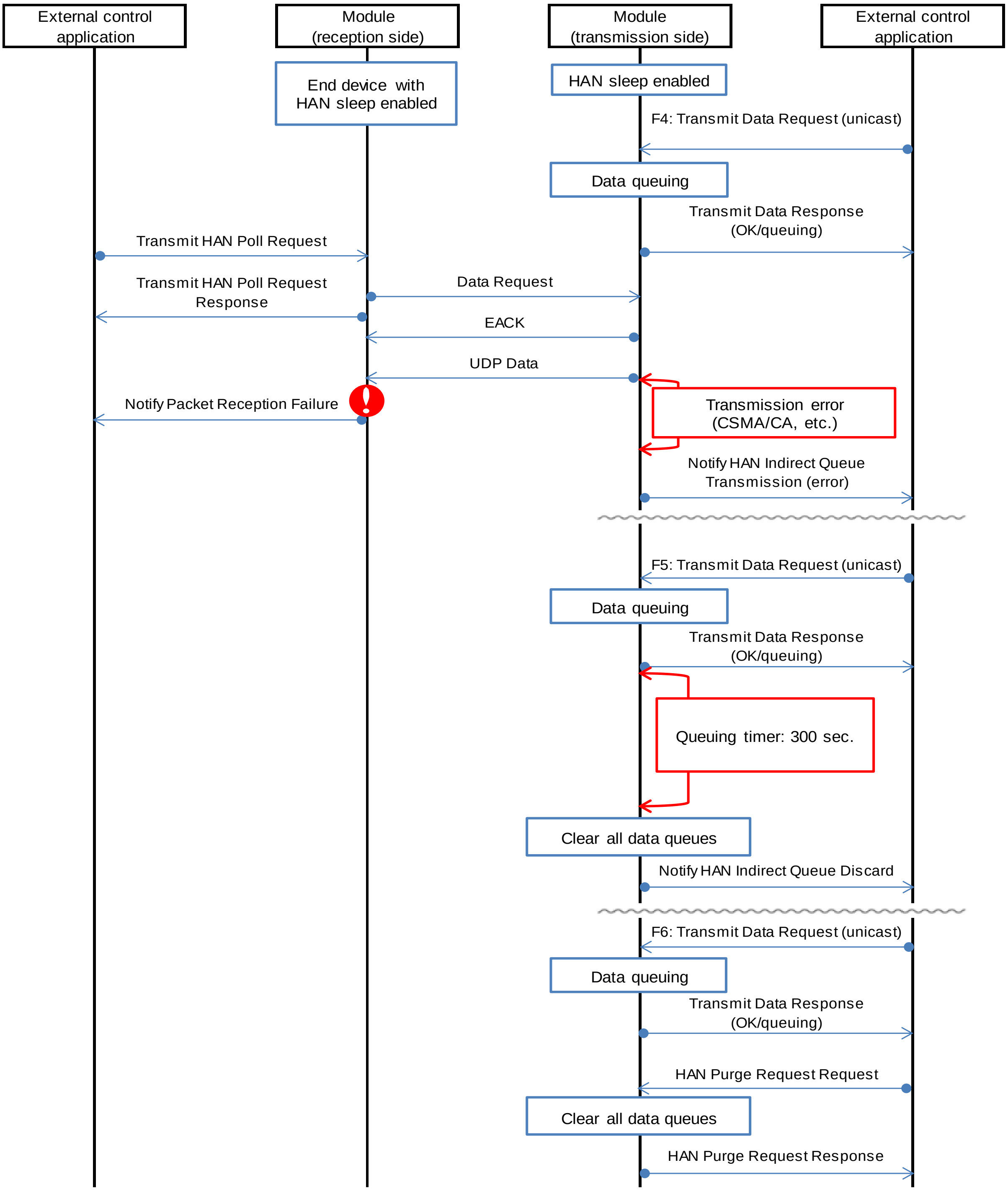
External control application
Module (reception side)
Module (transmission side)
External control application
End device with HAN sleep enabled
HAN sleep enabled
F4: Transmit Data Request (unicast)
Data queuing
Transmit Data Response (OK/queuing)
Transmit HAN Poll Request
Transmit HAN Poll Request Response
Data Request
EACK
UDP Data
Notify Packet Reception Failure
Transmission error (CSMA/CA, etc.)
Notify HAN Indirect Queue Transmission (error)
F5: Transmit Data Request (unicast)
Data queuing
Transmit Data Response (OK/queuing)
Queuing timer: 300 sec.
Clear all data queues
Notify HAN Indirect Queue Discard
F6: Transmit Data Request (unicast)
Data queuing
Transmit Data Response (OK/queuing)
HAN Purge Request Request
Clear all data queues
HAN Purge Request Response

Fig. 21: Sequence of Transmit Data and Notify Data Reception (with indirect communication) - (2)

5.12.5 Sequence of Transmit Data and Notify Data Reception (with relay)

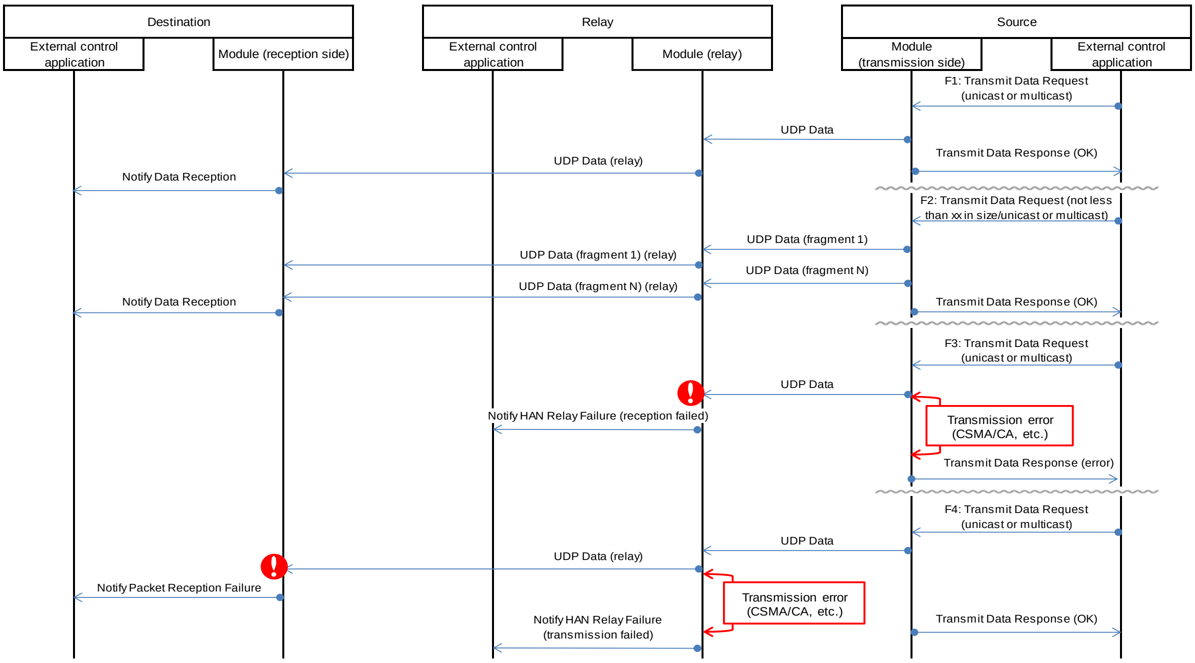
Destination
External control application
Module (reception side)
Relay
External control application
Module (relay)
Source
Module (transmission side)
External control application
F1: Transmit Data Request (unicast or multicast)
UDP Data
UDP Data (relay)
Transmit Data Response (OK)
Notify Data Reception
F2: Transmit Data Request (not less than xx in size/unicast or multicast)
UDP Data (fragment 1)
UDP Data (fragment 1) (relay)
UDP Data (fragment N)
UDP Data (fragment N) (relay)
Notify Data Reception
Transmit Data Response (OK)
F3: Transmit Data Request (unicast or multicast)
UDP Data
Notify HAN Relay Failure (reception failed)
Transmission error (CSMA/CA, etc.)
Transmit Data Response (error)
F4: Transmit Data Request (unicast or multicast)
UDP Data
UDP Data (relay)
Notify Packet Reception Failure
Transmission error (CSMA/CA, etc.)
Notify HAN Relay Failure (transmission failed)
Transmit Data Response (OK)

Fig. 22: Sequence of Transmit Data and Notify Data Reception (with relay)

5.13 Sequence of Transmit To Ping

5.13.1 Sequence of Transmit To Ping (without ND)

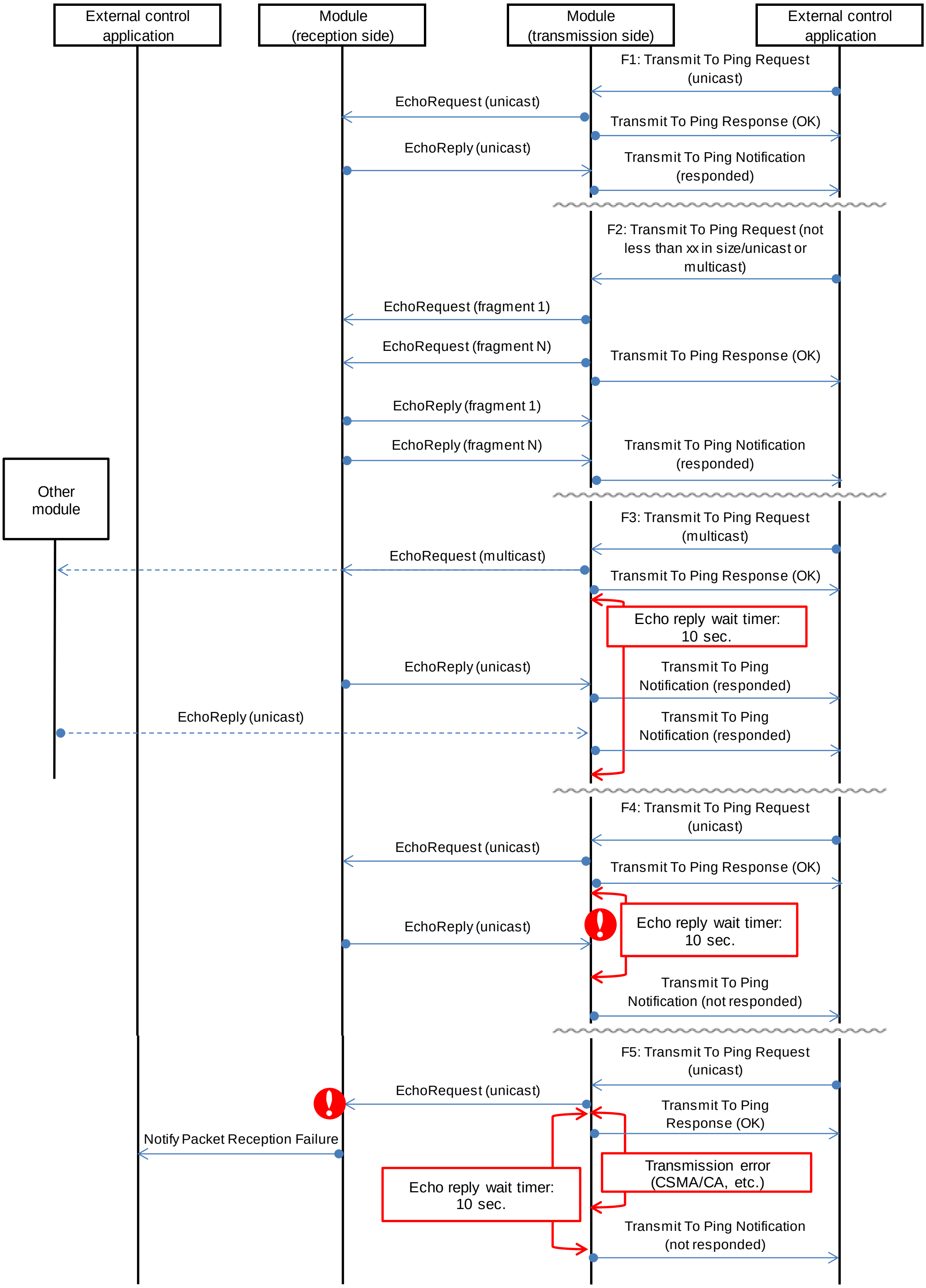
External control application
Module (reception side)
Module (transmission side)
External control application
F1: Transmit To Ping Request (unicast)
EchoRequest (unicast)
Transmit To Ping Response (OK)
EchoReply (unicast)
Transmit To Ping Notification (responded)
F2: Transmit To Ping Request (not less than xx in size/unicast or multicast)
EchoRequest (fragment 1)
EchoRequest (fragment N)
Transmit To Ping Response (OK)
EchoReply (fragment 1)
EchoReply (fragment N)
Transmit To Ping Notification (responded)
Other module
F3: Transmit To Ping Request (multicast)
EchoRequest (multicast)
Transmit To Ping Response (OK)
Echo reply wait timer: 10 sec.
EchoReply (unicast)
Transmit To Ping Notification (responded)
EchoReply (unicast)
Transmit To Ping Notification (responded)
F4: Transmit To Ping Request (unicast)
EchoRequest (unicast)
Transmit To Ping Response (OK)
EchoReply (unicast)
Echo reply wait timer: 10 sec.
Transmit To Ping Notification (not responded)
F5: Transmit To Ping Request (unicast)
EchoRequest (unicast)
Transmit To Ping Response (OK)
Notify Packet Reception Failure
Transmission error (CSMA/CA, etc.)
Echo reply wait timer: 10 sec.
Transmit To Ping Notification (not responded)

Fig. 23: Sequence of Transmit To Ping (without ND)

5.13.2 Sequence of Transmit To Ping (with ND)

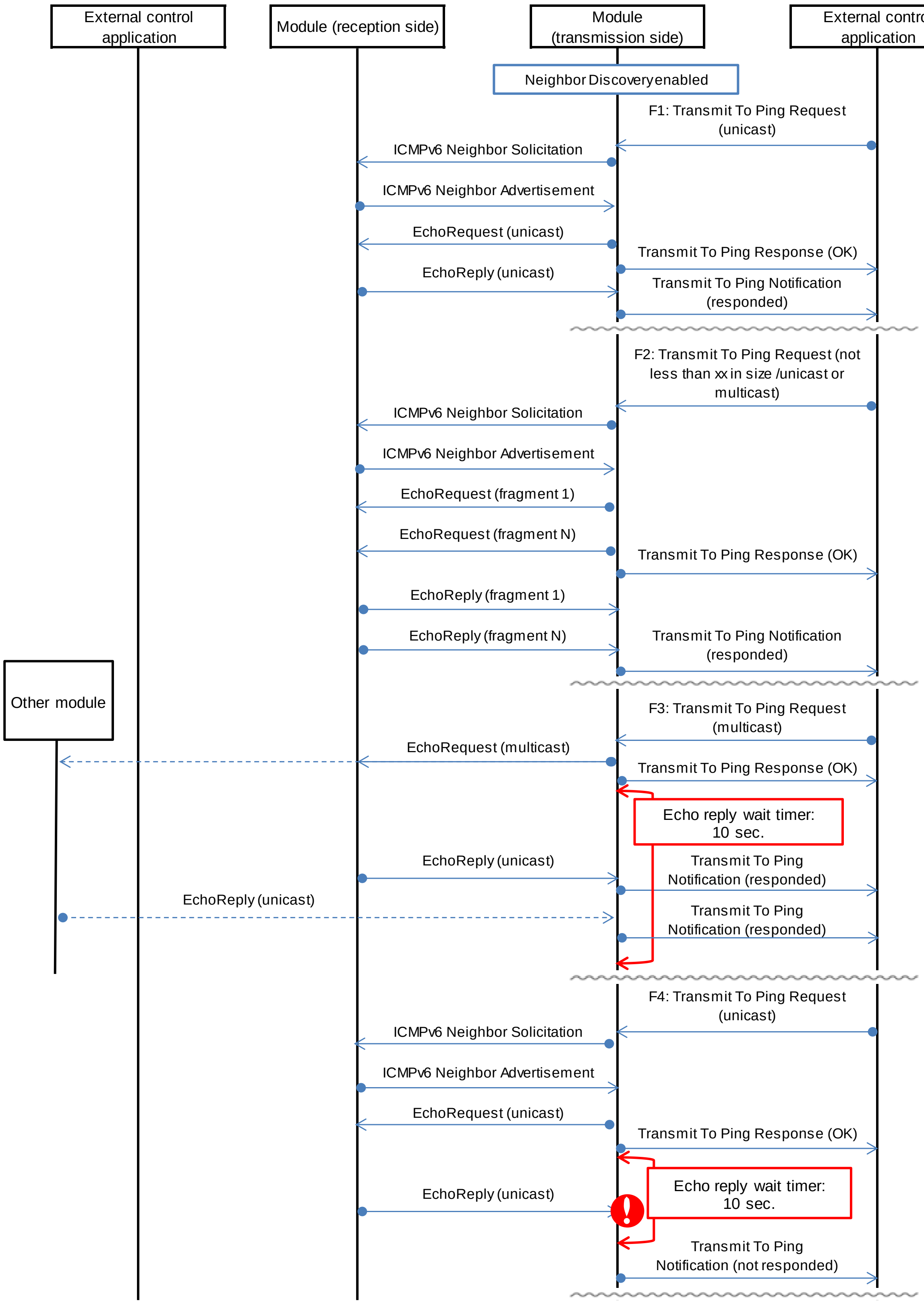
External control application
Module (reception side)
Module (transmission side)
External control application
Neighbor Discovery enabled
F1: Transmit To Ping Request (unicast)
ICMPv6 Neighbor Solicitation
ICMPv6 Neighbor Advertisement
EchoRequest (unicast)
Transmit To Ping Response (OK)
EchoReply (unicast)
Transmit To Ping Notification (responded)
F2: Transmit To Ping Request (not less than xx in size /unicast or multicast)
ICMPv6 Neighbor Solicitation
ICMPv6 Neighbor Advertisement
EchoRequest (fragment 1)
EchoRequest (fragment N)
Transmit To Ping Response (OK)
EchoReply (fragment 1)
EchoReply (fragment N)
Transmit To Ping Notification (responded)
Other module
F3: Transmit To Ping Request (multicast)
EchoRequest (multicast)
Transmit To Ping Response (OK)
Echo reply wait timer: 10 sec.
EchoReply (unicast)
Transmit To Ping Notification (responded)
EchoReply (unicast)
Transmit To Ping Notification (responded)
F4: Transmit To Ping Request (unicast)
ICMPv6 Neighbor Solicitation
ICMPv6 Neighbor Advertisement
EchoRequest (unicast)
Transmit To Ping Response (OK)
Echo reply wait timer: 10 sec.
EchoReply (unicast)
Transmit To Ping Notification (not responded)

Fig. 24: Sequence of Transmit To Ping (with ND)

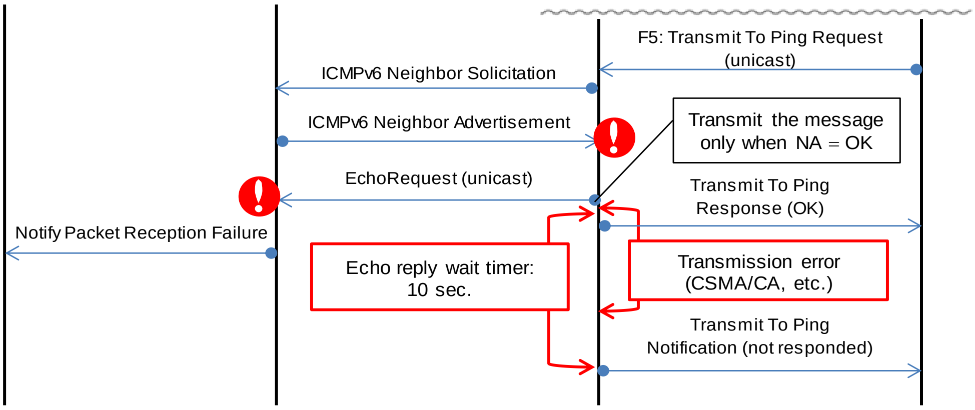
F5: Transmit To Ping Request (unicast)
ICMPv6 Neighbor Solicitation
ICMPv6 Neighbor Advertisement
Transmit the message only when NA = OK
EchoRequest (unicast)
Transmit To Ping Response (OK)
Notify Packet Reception Failure
Echo reply wait timer: 10 sec.
Transmission error (CSMA/CA, etc.)
Transmit To Ping Notification (not responded)

Fig. 24: Sequence of Transmit To Ping (with ND) (continued)

5.13.3 Sequence of Transmit To Ping (with indirect communication) - (1)

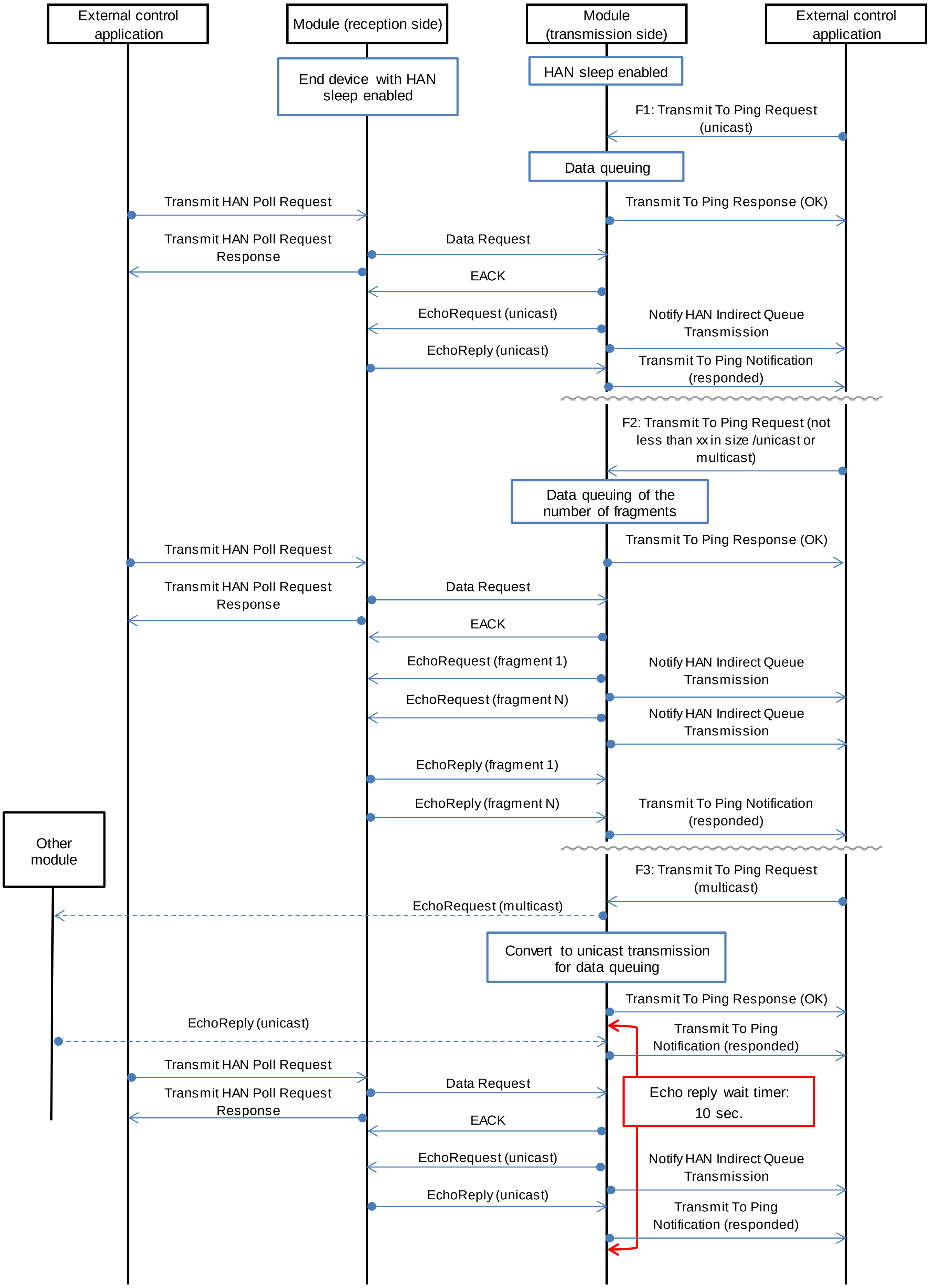
External control application
Module (reception side)
Module (transmission side)
External control application
End device with HAN sleep enabled
HAN sleep enabled
F1: Transmit To Ping Request (unicast)
Data queuing
Transmit HAN Poll Request
Transmit To Ping Response (OK)
Transmit HAN Poll Request Response
Data Request
EACK
EchoRequest (unicast)
Notify HAN Indirect Queue Transmission
EchoReply (unicast)
Transmit To Ping Notification (responded)
F2: Transmit To Ping Request (not less than xx in size /unicast or multicast)
Data queuing of the number of fragments
Transmit HAN Poll Request
Transmit To Ping Response (OK)
Transmit HAN Poll Request Response
Data Request
EACK
EchoRequest (fragment 1)
Notify HAN Indirect Queue Transmission
EchoRequest (fragment N)
Notify HAN Indirect Queue Transmission
EchoReply (fragment 1)
EchoReply (fragment N)
Transmit To Ping Notification (responded)
Other module
F3: Transmit To Ping Request (multicast)
EchoRequest (multicast)
Convert to unicast transmission for data queuing
Transmit To Ping Response (OK)
EchoReply (unicast)
Transmit To Ping Notification (responded)
Transmit HAN Poll Request
Transmit HAN Poll Request Response
Data Request
Echo reply wait timer: 10 sec.
EACK
EchoRequest (unicast)
Notify HAN Indirect Queue Transmission
EchoReply (unicast)
Transmit To Ping Notification (responded)

Fig. 25: Sequence of Transmit To Ping (with indirect communication) - (1)

5.13.4 Sequence of Transmit To Ping (with indirect communication) - (2)

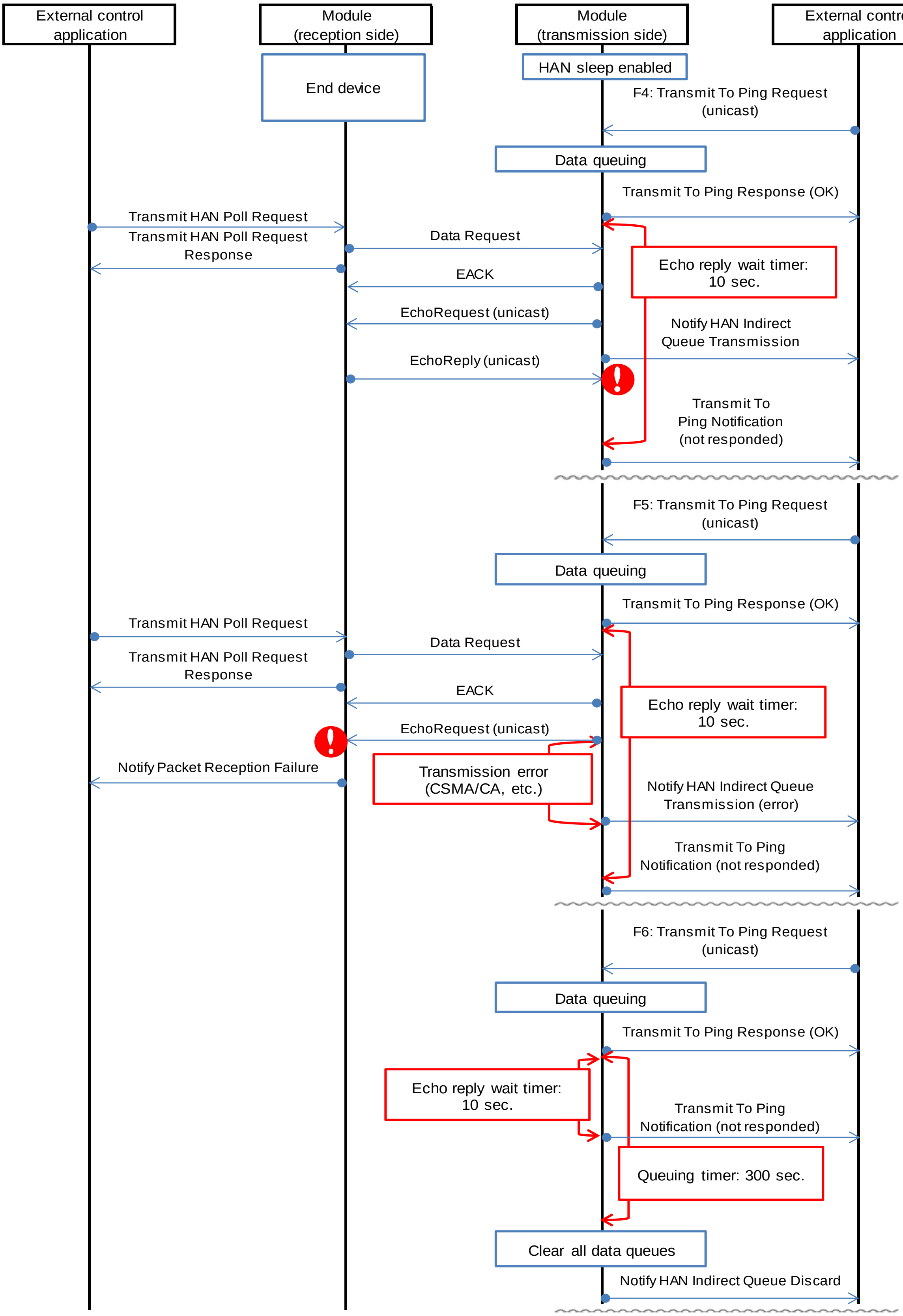
External control application
Module (reception side)
Module (transmission side)
External control application
End device
HAN sleep enabled
F4: Transmit To Ping Request (unicast)
Data queuing
Transmit To Ping Response (OK)
Transmit HAN Poll Request
Transmit HAN Poll Request Response
Data Request
Echo reply wait timer: 10 sec.
EACK
EchoRequest (unicast)
Notify HAN Indirect Queue Transmission
EchoReply (unicast)
Transmit To Ping Notification (not responded)
F5: Transmit To Ping Request (unicast)
Data queuing
Transmit To Ping Response (OK)
Transmit HAN Poll Request
Data Request
Transmit HAN Poll Request Response
EACK
Echo reply wait timer: 10 sec.
EchoRequest (unicast)
Notify Packet Reception Failure
Transmission error (CSMA/CA, etc.)
Notify HAN Indirect Queue Transmission (error)
Transmit To Ping Notification (not responded)
F6: Transmit To Ping Request (unicast)
Data queuing
Transmit To Ping Response (OK)
Echo reply wait timer: 10 sec.
Transmit To Ping Notification (not responded)
Queuing timer: 300 sec.
Clear all data queues
Notify HAN Indirect Queue Discard

Fig. 26: Sequence of Transmit To Ping (with indirect communication) - (2)

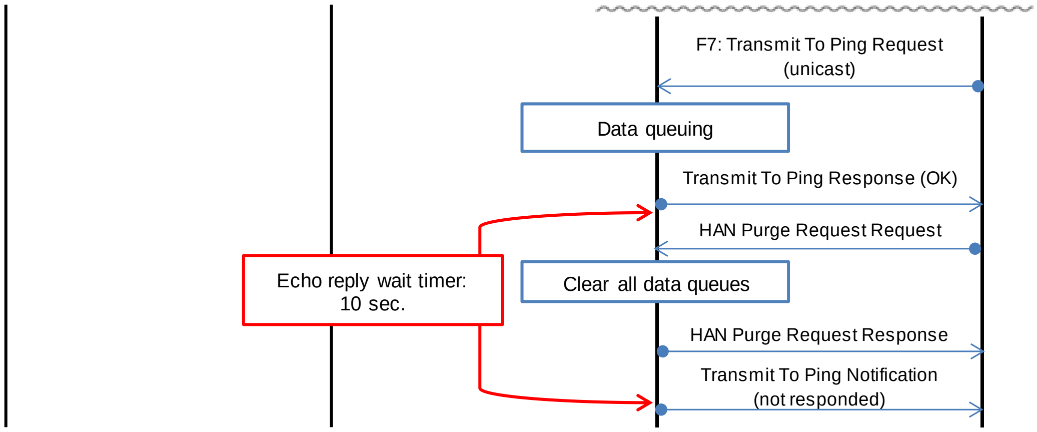
F7: Transmit To Ping Request
(unicast)
Data queuing
Transmit To Ping Response (OK)
HAN Purge Request Request
Echo reply wait timer:
10 sec.
Clear all data queues
HAN Purge Request Response
Transmit To Ping Notification
(not responded)

Fig. 26: Sequence of Transmit To Ping (with indirect communication) - (2) (continued)

5.13.5 Sequence of Transmit To Ping (with relay)

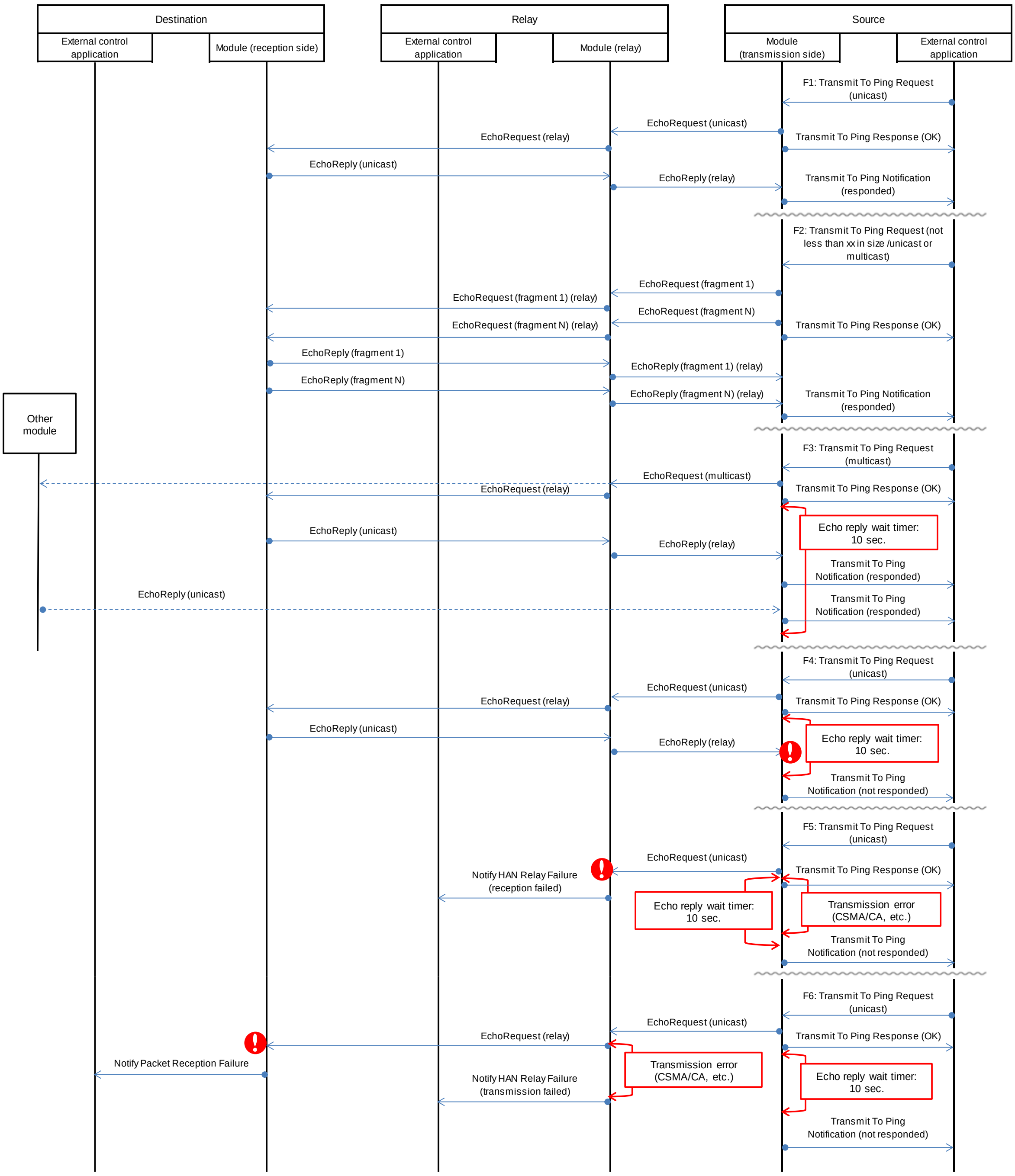
Destination
External control application
Module (reception side)
Relay
External control application
Module (relay)
Source
Module (transmission side)
External control application
F1: Transmit To Ping Request (unicast)
EchoRequest (unicast)
EchoRequest (relay)
Transmit To Ping Response (OK)
EchoReply (unicast)
EchoReply (relay)
Transmit To Ping Notification (responded)
F2: Transmit To Ping Request (not less than xx in size /unicast or multicast)
EchoRequest (fragment 1)
EchoRequest (fragment 1) (relay)
EchoRequest (fragment N)
EchoRequest (fragment N) (relay)
Transmit To Ping Response (OK)
EchoReply (fragment 1)
EchoReply (fragment 1) (relay)
EchoReply (fragment N)
EchoReply (fragment N) (relay)
Transmit To Ping Notification (responded)
Other module
F3: Transmit To Ping Request (multicast)
EchoRequest (multicast)
EchoRequest (relay)
Transmit To Ping Response (OK)
Echo reply wait timer: 10 sec.
EchoReply (unicast)
EchoReply (relay)
Transmit To Ping Notification (responded)
EchoReply (unicast)
Transmit To Ping Notification (responded)
F4: Transmit To Ping Request (unicast)
EchoRequest (unicast)
EchoRequest (relay)
Transmit To Ping Response (OK)
EchoReply (unicast)
Echo reply wait timer: 10 sec.
EchoReply (relay)
Transmit To Ping Notification (not responded)
F5: Transmit To Ping Request (unicast)
EchoRequest (unicast)
Notify HAN Relay Failure (reception failed)
Transmit To Ping Response (OK)
Echo reply wait timer: 10 sec.
Transmission error (CSMA/CA, etc.)
Transmit To Ping Notification (not responded)
F6: Transmit To Ping Request (unicast)
EchoRequest (unicast)
EchoRequest (relay)
Transmit To Ping Response (OK)
Notify Packet Reception Failure
Transmission error (CSMA/CA, etc.)
Notify HAN Relay Failure (transmission failed)
Echo reply wait timer: 10 sec.
Transmit To Ping Notification (not responded)

Fig. 27: Sequence of Transmit To Ping (with relay)

5.14 Sequence of Initiate Route-B Operation

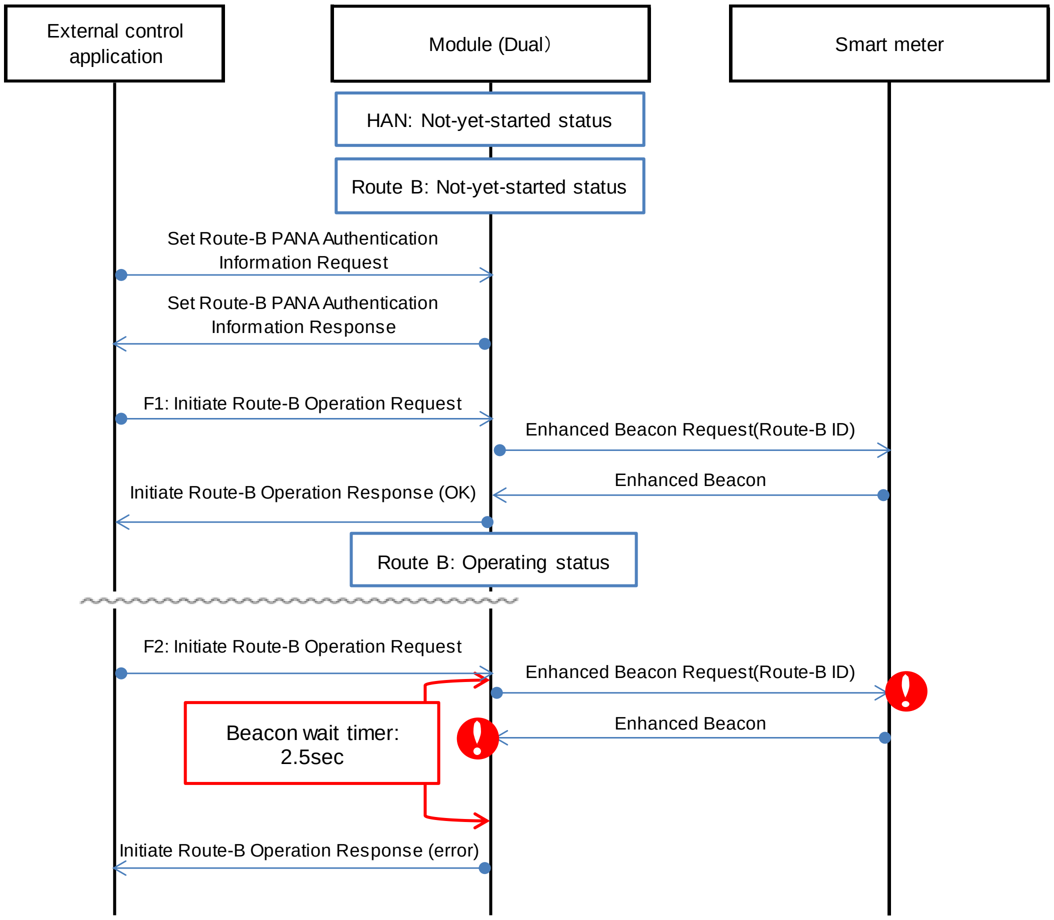
External control application
Module (Dual)
Smart meter
HAN: Not-yet-started status
Route B: Not-yet-started status
Set Route-B PANA Authentication Information Request
Set Route-B PANA Authentication Information Response
F1: Initiate Route-B Operation Request
Enhanced Beacon Request(Route-B ID)
Enhanced Beacon
Initiate Route-B Operation Response (OK)
Route B: Operating status
F2: Initiate Route-B Operation Request
Enhanced Beacon Request(Route-B ID)
Beacon wait timer: 2.5sec
Enhanced Beacon
Initiate Route-B Operation Response (error)

Fig. 28: Sequence of Initiate Route-B Operation

5.15 Sequence of Terminate Route-B Operation

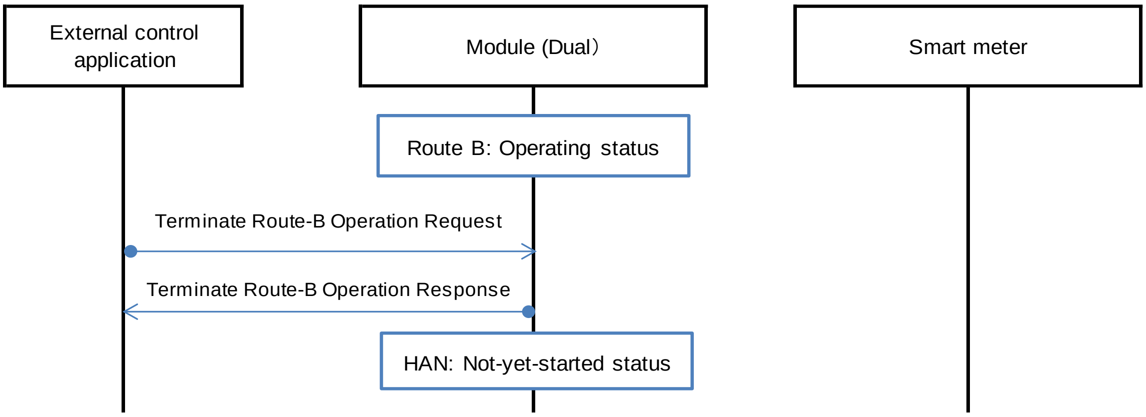
External control application
Module (Dual）
Smart meter
Route B: Operating status
Terminate Route-B Operation Request
Terminate Route-B Operation Response
HAN: Not-yet-started status

Fig. 29: Sequence of Terminate Route-B Operation

5.16 Sequence of Initiate Route-B PANA

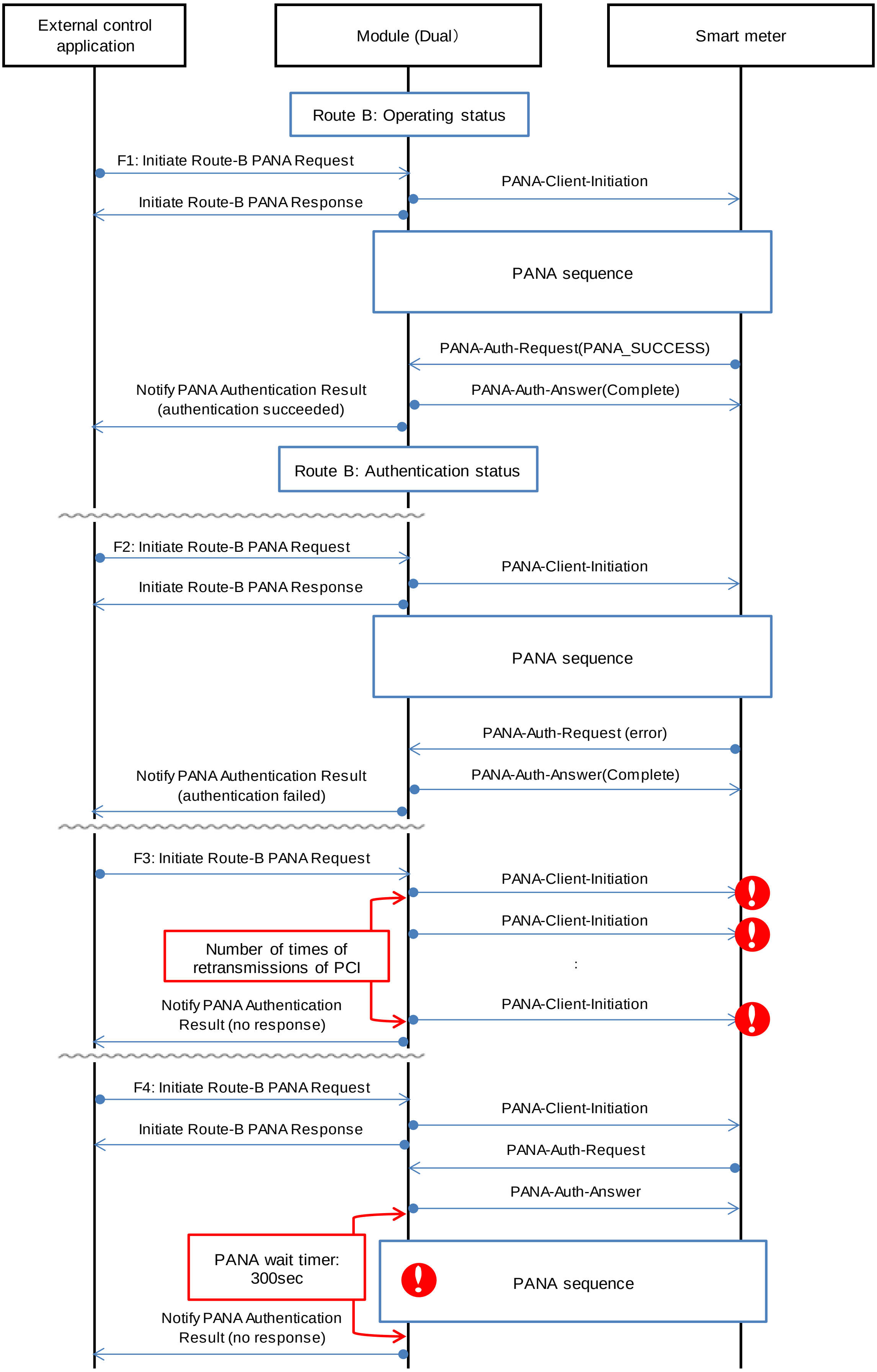
External control application
Module (Dual）
Smart meter
Route B: Operating status
F1: Initiate Route-B PANA Request
PANA-Client-Initiation
Initiate Route-B PANA Response
PANA sequence
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
PANA-Auth-Answer(Complete)
Route B: Authentication status
F2: Initiate Route-B PANA Request
PANA-Client-Initiation
Initiate Route-B PANA Response
PANA sequence
PANA-Auth-Request (error)
Notify PANA Authentication Result (authentication failed)
PANA-Auth-Answer(Complete)
F3: Initiate Route-B PANA Request
PANA-Client-Initiation
PANA-Client-Initiation
Number of times of retransmissions of PCI
:
Notify PANA Authentication Result (no response)
PANA-Client-Initiation
F4: Initiate Route-B PANA Request
PANA-Client-Initiation
Initiate Route-B PANA Response
PANA-Auth-Request
PANA-Auth-Answer
PANA wait timer: 300sec
PANA sequence
Notify PANA Authentication Result (no response)

Fig. 30: Sequence of Initiate Route-B PANA

5.17 Sequence of Terminate Route-B PANA

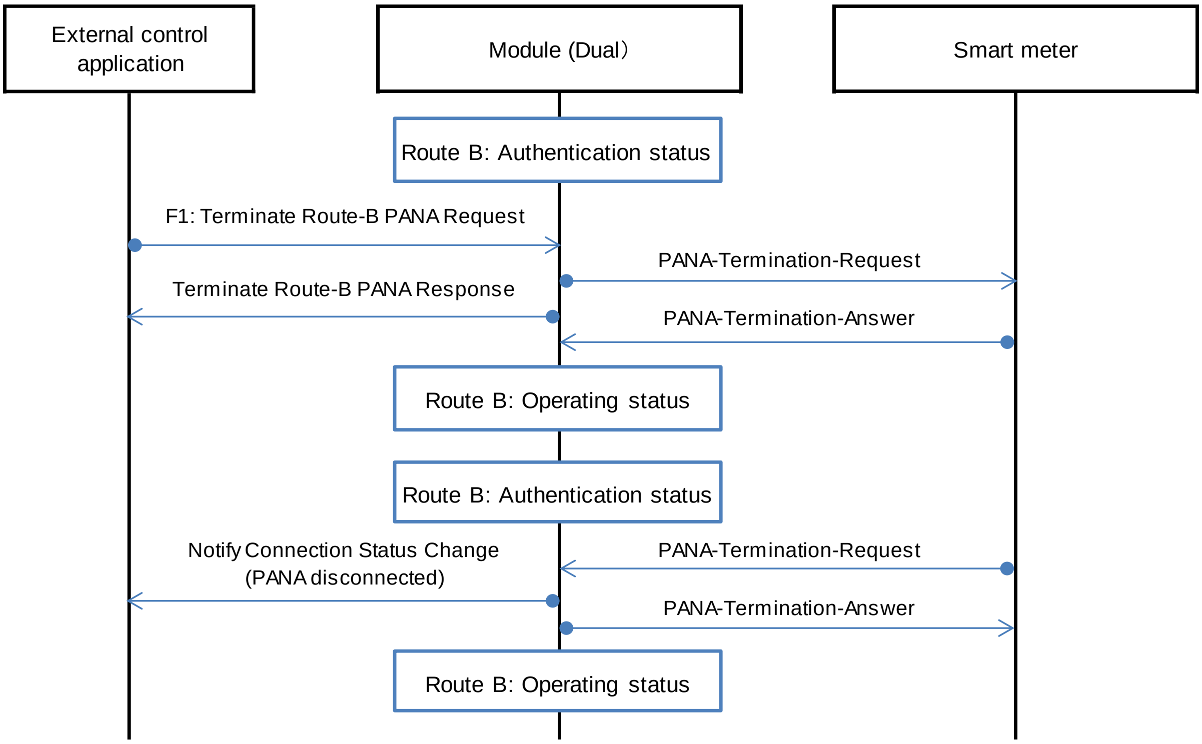
External control application
Module (Dual）
Smart meter
Route B: Authentication status
F1: Terminate Route-B PANA Request
PANA-Termination-Request
Terminate Route-B PANA Response
PANA-Termination-Answer
Route B: Operating status
Route B: Authentication status
Notify Connection Status Change
(PANA disconnected)
PANA-Termination-Request
PANA-Termination-Answer
Route B: Operating status

Fig. 31: Sequence of Terminate Route-B PANA

5.18 Sequence of Initiate Route-B PANA Re-authentication

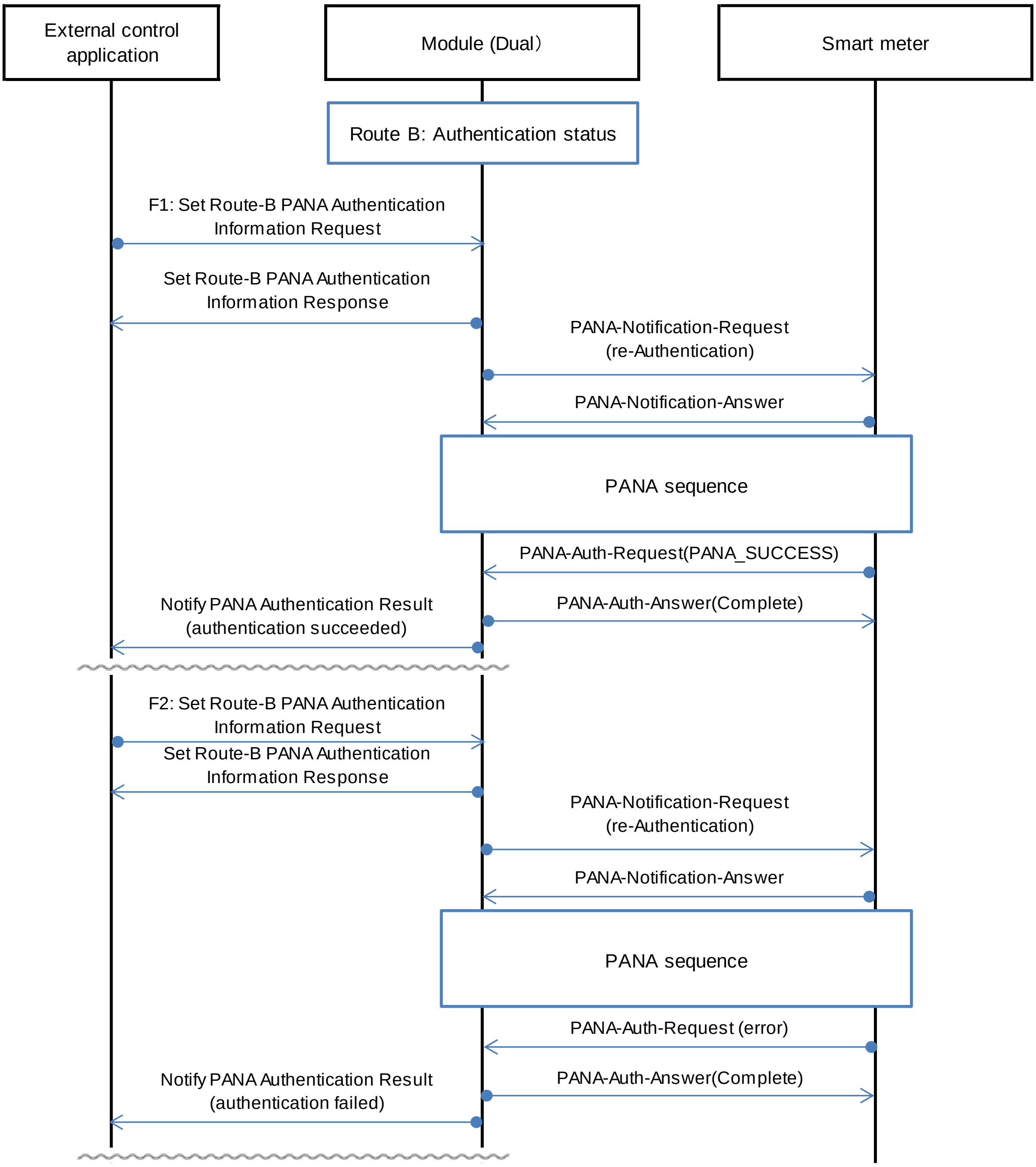
External control application
Module (Dual)
Smart meter
Route B: Authentication status
F1: Set Route-B PANA Authentication Information Request
Set Route-B PANA Authentication Information Response
PANA-Notification-Request (re-Authentication)
PANA-Notification-Answer
PANA sequence
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
PANA-Auth-Answer(Complete)
F2: Set Route-B PANA Authentication Information Request
Set Route-B PANA Authentication Information Response
PANA-Notification-Request (re-Authentication)
PANA-Notification-Answer
PANA sequence
PANA-Auth-Request (error)
Notify PANA Authentication Result (authentication failed)
PANA-Auth-Answer(Complete)

Fig. 32: Sequence of Initiate Route-B PANA Re-authentication

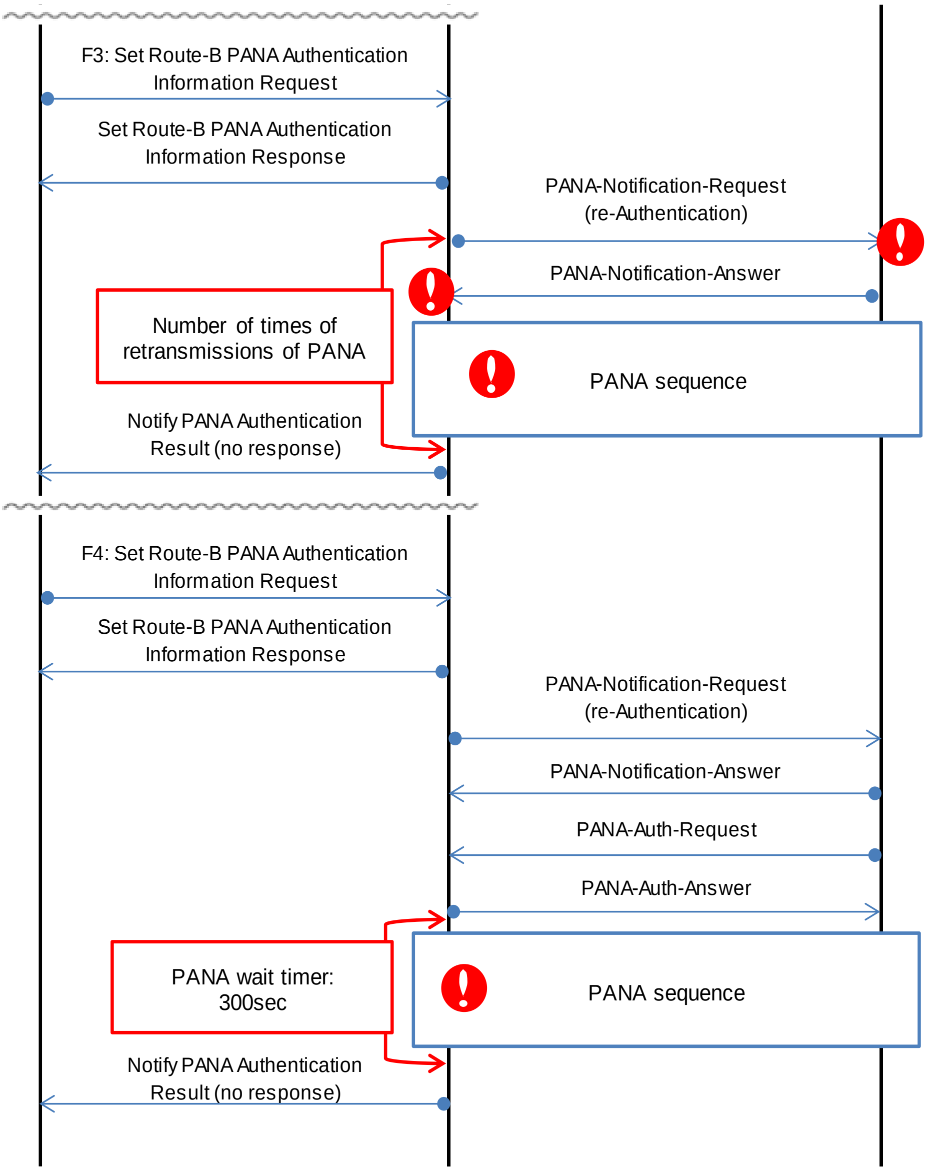
F3: Set Route-B PANA Authentication Information Request
Set Route-B PANA Authentication Information Response
PANA-Notification-Request (re-Authentication)
PANA-Notification-Answer
Number of times of retransmissions of PANA
PANA sequence
Notify PANA Authentication Result (no response)
F4: Set Route-B PANA Authentication Information Request
Set Route-B PANA Authentication Information Response
PANA-Notification-Request (re-Authentication)
PANA-Notification-Answer
PANA-Auth-Request
PANA-Auth-Answer
PANA wait timer: 300sec
PANA sequence
Notify PANA Authentication Result (no response)

Fig. 32: Sequence of Initiate Route-B PANA Re-authentication (continued)

5.19 Sequence of Execute ED Scan

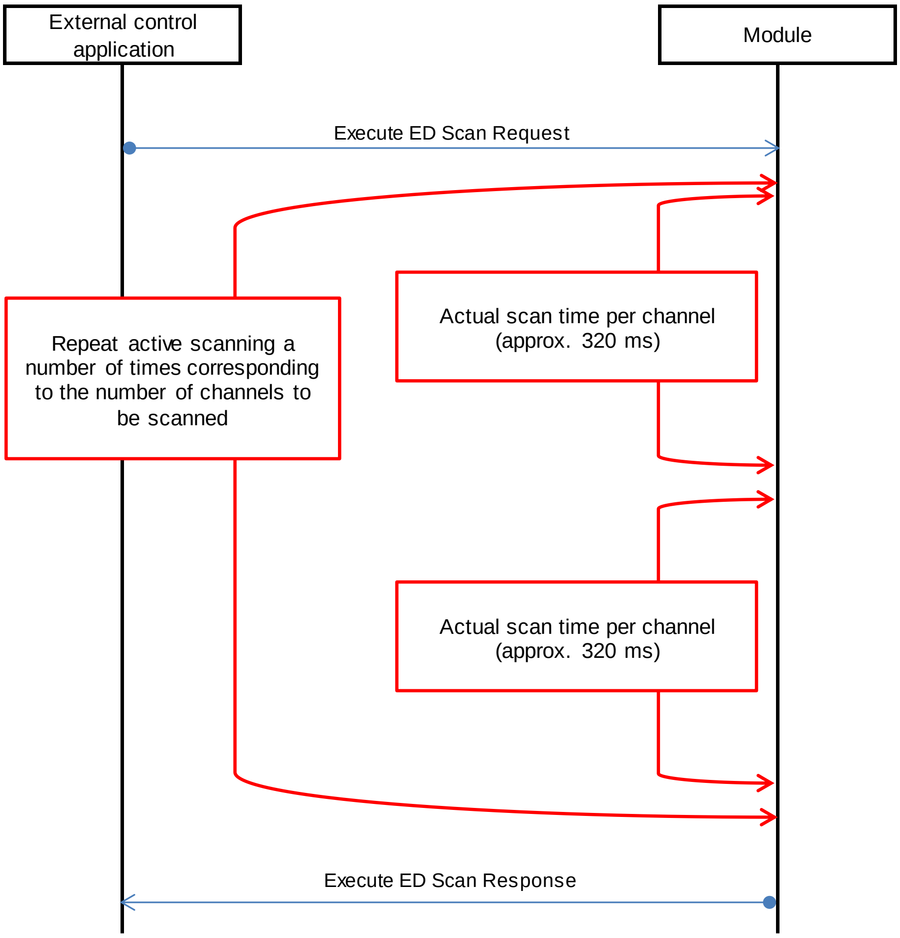
External control application
Module
Execute ED Scan Request
Repeat active scanning a number of times corresponding to the number of channels to be scanned
Actual scan time per channel (approx. 320 ms)
Actual scan time per channel (approx. 320 ms)
Execute ED Scan Response

Fig. 33: Sequence of Execute ED Scan

5.20 Sequence of HAN Deep Sleep Request

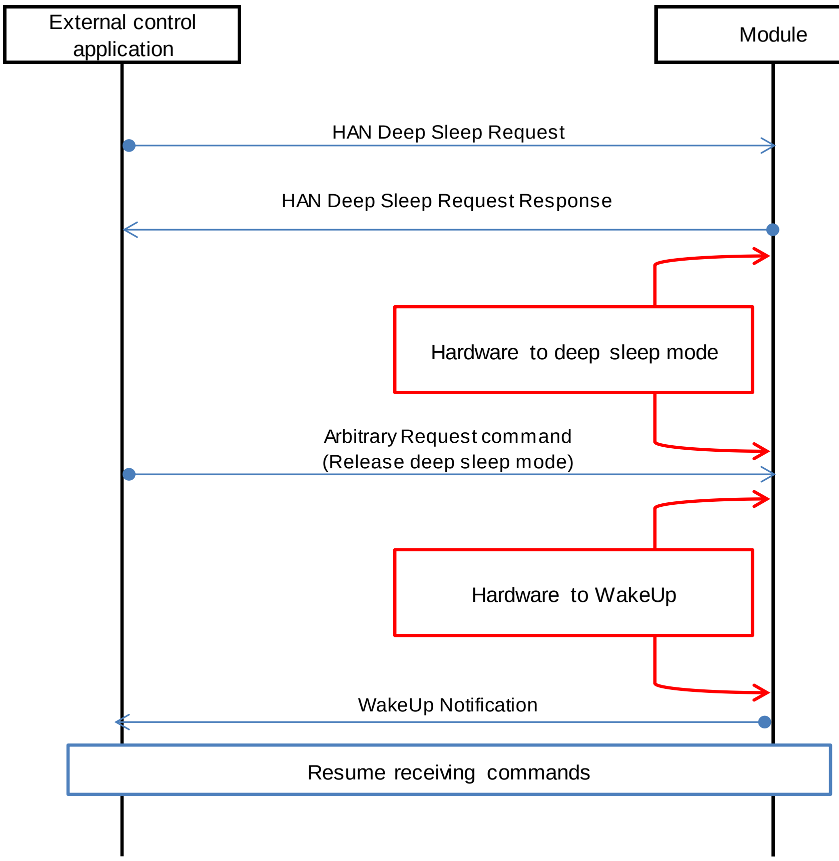
External control application
Module
HAN Deep Sleep Request
HAN Deep Sleep Request Response
Hardware to deep sleep mode
Arbitrary Request command
(Release deep sleep mode)
Hardware to WakeUp
WakeUp Notification
Resume receiving commands

Fig. 34: Sequence of HAN Deep Sleep Request

5.21 Command response wait time

Some of sequences described in Chapter 5, “Command sequences” require time from a request for a command to a response to the command or the completion of the sequence. The table shown below lists reference values for wait time in such sequences.

Recommended wait time for the upper-level application is the wait time listed below plus one second.

Recommended wait time for commands not listed in the table is two seconds without any exception.

Table 35: Time to respond to/complete command sequence

Sequence	Period	Time (sec.)	Remarks
Sequence of **Execute Active Scan** [When the Channel parameter is set to All channels]	**Request** to **Response**	35.8	Scan time: 8 Scan channels: Channels 4 to 17
Sequence of **Execute Active Scan** [When the Channel parameter is set to Channel 1]	**Request** to **Notification**	2.6	Scan time: 8 Scan channels: Channel 4
Sequence of **Initiate HAN Operation** [F3]	**Request** to **Response**	2.5	
Sequence of **Initiate HAN PANA** (without indirect communication) [F3]	**Request** to **Notification**	118.8 to 199.2	Number of times of the retransmissions of PANA authentication initiation message: 4 times
Sequence of **Initiate HAN PANA** (without indirect communication) [F4]	**Request** to **Notification**	311.3	
Sequence of **Distribute HAN Group Key** (push) [F2]	**Request** to **Notification**	7.8 to 10.2	Number of times of retransmissions of PANA authentication message: 1 time
Sequence of **Check HAN Group Key Update** (pull) (without indirect communication) [F3]	**Request** to **Notification**	7.8 to 10.2	Number of times of retransmissions of PANA authentication message: 1 time
Sequence of **Re-authenticate HAN PANA** [F3]	**Request** to **Notification**	310.2	
Sequence of **Set HAN Sleep Device PANA Retransmission Interval** (with indirect communication) [F2]	**Request** to **Notification**	7.8～10.2	Number of times of retransmissions of PANA authentication message: 1 time
Sequence of **Transmit Data** and **Notify Data Reception** (without ND) [F1]	**Request** to **Response**	0.9	
Sequence of **Transmit Data** and **Notify Data Reception** (without ND) [F2]	**Request** to **Response**	7.0	Maximum wait time for 1,232 bytes of data
Sequence of **Transmit Data** and **Notify Data Reception** (without ND) [F3]	**Request** to **Response**	0.9	
Sequence of **Transmit Data** and **Notify Data Reception** (with ND) [F4]	**Request** to **Response**	2.7	
Sequence of **Transmit Data** and **Notify Data Reception** (with ND) [F5]	**Request** to **Response**	0.9	
Sequence of **Transmit Data** and **Notify Data Reception** (with indirect communication) - (2) [F5]	**Request** to **Notification**	310.5	

Table 35: Time to respond to/complete command sequence (continued)

Sequence	Period	Time (sec.)	Remarks
Sequence of **Transmit Data** and **Notify Data Reception** (with relay) [F3]	**Request** to **Response**	0.9	
Sequence of **Transmit To Ping** (without ND) [F4]	**Request** to **Notification**	10.5	
Sequence of **Transmit To Ping** (without ND) [F5]	**Request** to **Notification**	10.9	
Sequence of **Transmit To Ping** (with ND) [F4]	**Request** to **Notification**	10.4	
Sequence of **Transmit To Ping** (with ND) [F5]	**Request** to **Notification**	10.8	
Sequence of **Transmit To Ping** (with indirect communication) - (2) [F4]	**Request** to **Notification**	10.4	
Sequence of **Transmit To Ping** (with indirect communication) - (2) [F5]	**Request** to **Notification**	10.4	
Sequence of **Transmit To Ping** (with indirect communication) - (2) [F6]	**Request** to **Notification**	310.6	
Sequence of **Transmit To Ping** (with indirect communication) - (2) [F7]	**Request** to **Notification**	10.4	
Sequence of **Transmit To Ping** (with relay) [F4]	**Request** to **Notification**	10.4	
Sequence of **Transmit To Ping** (with relay) [F5]	**Request** to **Notification**	10.6	
Sequence of **Initiate Route-B Operation** [F2]	**Request** to **Response**	2.6	
Sequence of **Initiate Route-B PANA** [F3]	**Request** to **Notification**	491.9 to 706.0	
Sequence of **Initiate Route-B PANA** [F4]	**Request** to **Notification**	311.5	
Sequence of **Initiate Route-B PANA Re-authentication** [F3]	**Request** to **Notification**	180.1 to 236.7	
Sequence of **Initiate Route-B PANA Re-authentication** [F4]	**Request** to **Notification**	302.7	
Sequence of **Execute ED Scan** [All channels]	**Request** to **Response**	4.5	
Sequence of **Execute ED Scan** [Channel 1]	**Request** to **Response**	0.4	

Appendix A Recommended procedures

This Chapter describes examples of recommended procedures for individual cases.

The procedures described in this Chapter do not guarantee operations in customer's system.

A.1 HAN connection

Connection configuration:

PAN coordinator [A] <–> Coordinator [B] <–> End device [C]

Each step represents the relevant command name. Descriptions inside the parentheses provide an explanation about the command parameter, respectively.

PAN coordinator [A]:

1. **Setup Initial Settings** (operation mode: PAN coordinator, channel: Arbitrary channel)
2. **Execute Active Scan** (scan channel: arbitrary channel, pairing ID: no Pairing ID set)
   → Collect PAN ID used around, and then derive unique PAN ID.
3. **Set HAN PANA Authentication Information** (information on [B] and [C])
4. **Initiate HAN Operation** (ID setting: set the PAN ID derived in step 2)
5. **Initiate HAN PANA**
6. **Switch HAN Acceptance Connection Mode** (switch to initial connection mode)
   → Wait for the connection of [B] and, after the connection is made, proceed to the next step.
7. **Switch HAN Acceptance Connection Mode** (switch to normal connection mode)
   → Return the mode to normal connection mode so as to prevent the connection of [C] to [A].
8. **Open UDP Port** (open an arbitrary port)

Coordinator [B]:

1. **Setup Initial Settings** (operation mode: coordinator, scan channel: channel of [A])
2. **Set HAN PANA Authentication Information** (information on [B] itself)
3. **Initiate HAN Operation** (connection mode: Initial connection (HAN_INIT))
4. **Initiate HAN PANA**
   → After completion of the connection with [A], wait for executing **Notify PANA Authentication Result**, and then proceed to the next step.
5. **Switch HAN Acceptance Connection Mode** (switch to initial connection mode)
   (Wait for the connection of [C])
6. **Transmit Data** (transmit data to [A], and then specify a port opened by [A])

End device [C]:

1. **Setup Initial Settings** (operation mode: end device, scan channel: channel of [A])
2. **Set HAN PANA Authentication Information** (information on [C] itself)
3. **Initiate HAN Operation** (connection mode: initial connection (HAN_INIT))
4. **Initiate HAN PANA**
   → After completion of the connection with [B], wait for executing **Notify PANA Authentication Result**, and then proceed to the next step.
5. **Transmit Data** (transmit data to [A], and then specify a port opened by [A])

A.2 Route-B connection

Connection configuration:

Smart meter <–> Dual [A] <–> Coordinator [B] <–> End device [C]

Each step represents the relevant command name. Descriptions inside the parentheses provide an explanation about the command parameter, respectively.

Dual [A] (Route-B connection)

1. **Setup Initial Settings** (operation mode: Dual, scan channel: arbitrary channel)
2. **Execute Active Scan** (scan channel: all channels, Pairing ID: set the last eight characters of Route-B authentication ID to Pairing ID)
   → Search a channel in which the smart meter operates.
3. **Setup Initial Settings** (operation mode: Dual, scan channel: channel smart meter)
   → If the channel in which the smart meter operates is the same as a preset channel, omit this setting.
4. **Set Route-B PANA Authentication Information**
5. **Initiate Route-B Operation**
6. **Open UDP Port** (open Port 3610 used for ECHONET-Lite communication)
7. **Initiate Route-B PANA**
   → Wait for the success of authentication with the smart meter upon receipt of **Notify PANA Authentication Result**, and then proceed to the next step.
8. **Transmit Data** and **Notify Data Reception** (data addressed to the smart meter, destination port number: Set 3610 to the destination port)

Dual [A] (HAN connection):

1. **Execute Active Scan** (scan channel: channel of the smart meter, pairing ID: no pairing ID set)
   → Collect PAN ID used around, and then derive unique PAN ID.
2. **Set HAN PANA Authentication Information** (information on connected device)
3. **Initiate HAN Operation** (ID setting: set the PAN ID derived in step 1)
   Subsequent steps are the same as step 5 and subsequent steps listed in PAN coordinator [A] in A.1, “HAN connection”.

Coordinator [B] and end device [C]:

See A.1, “HAN connection”.

Appendix B Pairing

Pairing is the process required to mutually retain information on devices after these devices are connected with each other for the first time. Pairing devices with the upper-level application makes it possible to simplify the second and subsequent connection operations with the same pair of devices.

This Chapter describes examples for pairing devices for HAN and Route B, respectively.

B.1 HAN connection

Devices are paired with each other by setting the PAN coordinator to initial connection mode and searching the PAN coordinator from coordinator and end device. Information on the devices connected each other that is retained after completion of pairing is Channel and Pairing ID (i.e., MAC address of PAN coordinator).

For specific examples for command execution, refer to the following sequences:

Sequence for pairing: B.1.3, “Sequence of HAN pairing”

Sequence after pairing: B.1.4, “Sequence of normal connection of HAN”

B.1.1 PAN coordinator

When the HAN acceptance connection mode is set to HAN normal connection mode, the PAN coordinator will return a response only to EBR whose Pairing ID corresponds to the MAC address of the PAN coordinator itself. Consequently, devices that do not know the MAC address of the PAN coordinator cannot be connected.

In pairing devices, the HAN reception connection mode is switched to initial connection mode so that the coordinator or end device can search the PAN coordinator with active scan. After switching the mode to initial connection mode, the PAN coordinator will return a response not only to the EBR whose Pairing ID is set to the MAC address of the PAN coordinator itself, but also to EBR whose Pairing ID is set to HAN_INIT.

B.1.2 Coordinator/end device

Since the PAN coordinator searches a channel in operation, an active scan with HAN_INIT (0x48414e5f494e4954) set to Pairing ID is executed.

Subsequently, a channel that returned a response to active scan is set to connect the channel to the PAN coordinator. After completion of the connection, the channel and MAC address (i.e., Pairing ID) of the PAN coordinator are saved.

After completion of pairing, the connection with the PAN coordinator is enabled by using the retained channel and Paring ID without changing the active scan and PAN coordinator acceptance connection mode.

B.1.3 Sequence of HAN pairing

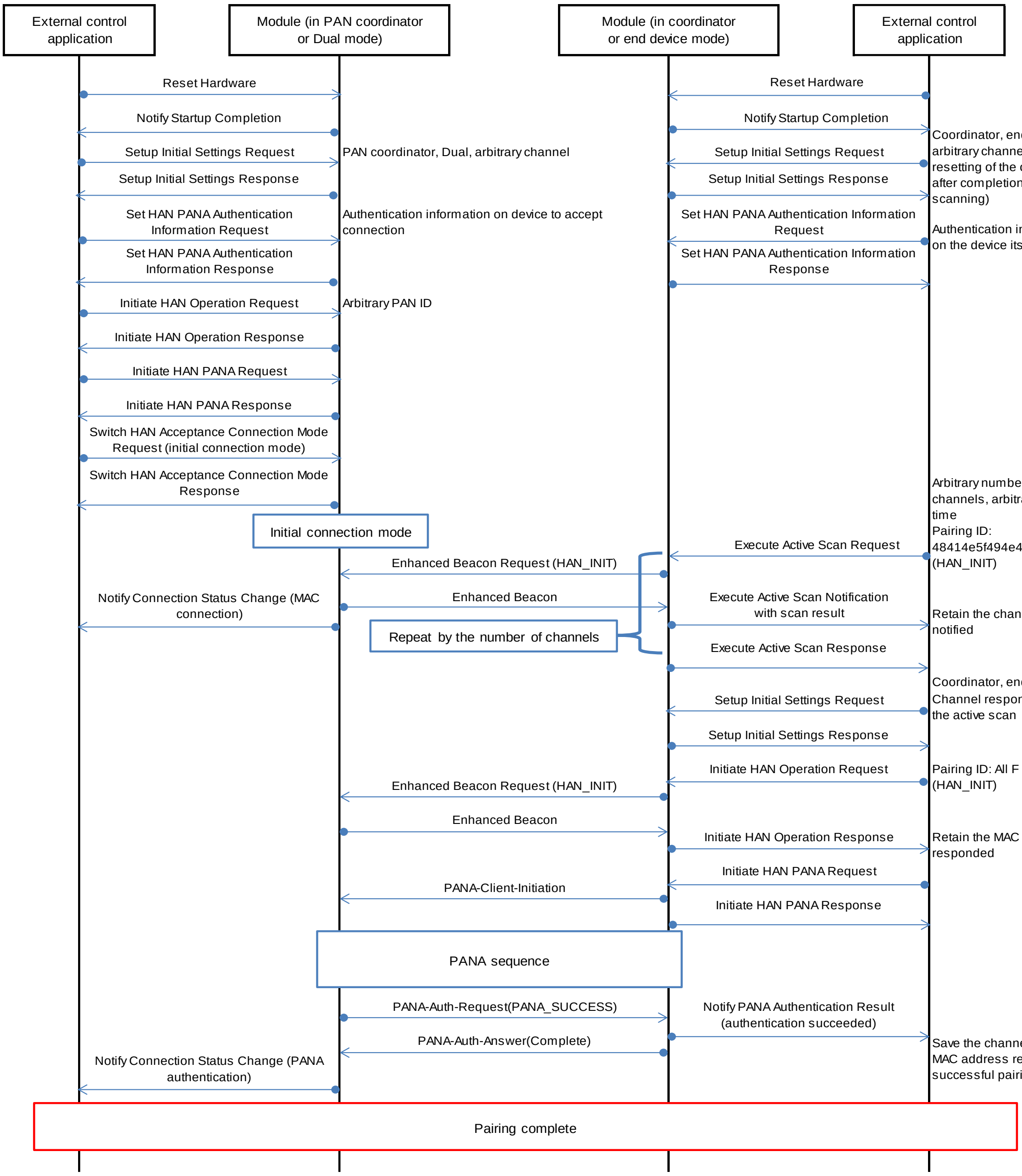
External control application
Module (in PAN coordinator or Dual mode)
Module (in coordinator or end device mode)
External control application
Reset Hardware
Reset Hardware
Notify Startup Completion
Notify Startup Completion
Setup Initial Settings Request
PAN coordinator, Dual, arbitrary channel
Setup Initial Settings Request
Coordinator, end device, arbitrary channel (Make resetting of the channel after completion of scanning)
Setup Initial Settings Response
Setup Initial Settings Response
Set HAN PANA Authentication Information Request
Authentication information on device to accept connection
Set HAN PANA Authentication Information Request
Authentication information on the device itself
Set HAN PANA Authentication Information Response
Set HAN PANA Authentication Information Response
Initiate HAN Operation Request
Arbitrary PAN ID
Initiate HAN Operation Response
Initiate HAN PANA Request
Initiate HAN PANA Response
Switch HAN Acceptance Connection Mode Request (initial connection mode)
Switch HAN Acceptance Connection Mode Response
Initial connection mode
Arbitrary number of channels, arbitrary scan time
Pairing ID: 48414e5f494e4954 (HAN_INIT)
Execute Active Scan Request
Enhanced Beacon Request (HAN_INIT)
Notify Connection Status Change (MAC connection)
Enhanced Beacon
Execute Active Scan Notification with scan result
Retain the channel notified
Repeat by the number of channels
Execute Active Scan Response
Coordinator, end device, Channel responded by the active scan
Setup Initial Settings Request
Setup Initial Settings Response
Initiate HAN Operation Request
Pairing ID: All F (HAN_INIT)
Enhanced Beacon Request (HAN_INIT)
Enhanced Beacon
Initiate HAN Operation Response
Retain the MAC address responded
Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
PANA sequence
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
PANA-Auth-Answer(Complete)
Save the channel and MAC address retained by successful pairing
Notify Connection Status Change (PANA authentication)
Pairing complete

Fig. 35: Sequence of HAN pairing

B.1.4 Sequence of normal connection of HAN

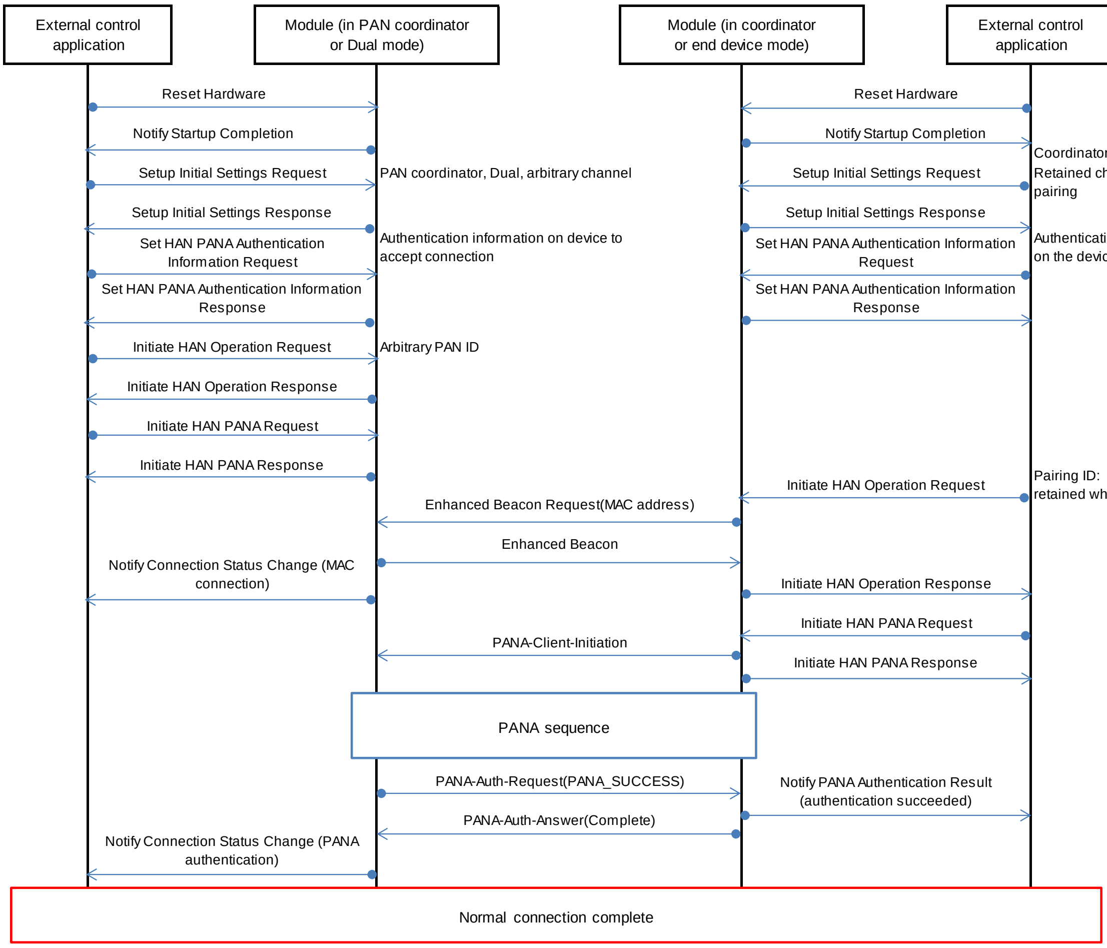
External control application
Module (in PAN coordinator or Dual mode)
Module (in coordinator or end device mode)
External control application
Reset Hardware
Notify Startup Completion
Setup Initial Settings Request
PAN coordinator, Dual, arbitrary channel
Setup Initial Settings Response
Set HAN PANA Authentication Information Request
Authentication information on device to accept connection
Set HAN PANA Authentication Information Response
Initiate HAN Operation Request
Arbitrary PAN ID
Initiate HAN Operation Response
Initiate HAN PANA Request
Initiate HAN PANA Response
Reset Hardware
Notify Startup Completion
Coordinator, end device, Retained channel when pairing
Setup Initial Settings Request
Setup Initial Settings Response
Authentication information on the device itself
Set HAN PANA Authentication Information Request
Set HAN PANA Authentication Information Response
Initiate HAN Operation Request
Pairing ID: MAC address retained when pairing
Enhanced Beacon Request(MAC address)
Enhanced Beacon
Notify Connection Status Change (MAC connection)
Initiate HAN Operation Response
Initiate HAN PANA Request
PANA-Client-Initiation
Initiate HAN PANA Response
PANA sequence
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
PANA-Auth-Answer(Complete)
Notify Connection Status Change (PANA authentication)
Normal connection complete

Fig. 36: Sequence of normal connection of HAN

B.2 Connection of Route B

The smart meter searches a channel in operation to implement pairing. Information on the devices connected each other that is retained after completion of pairing is channel only.

The Route B is connected by using Route-B authentication ID and password provided by the electric power company, etc.

For specific examples for command execution, refer to the following sequences:

Sequence for pairing: B.2.3, “Sequence of pairing of Route B”

Sequence after pairing: B.2.4, “Sequence of normal connection of Route B”

B.2.1 PAN coordinator

The PAN coordinator serves as a smart meter.

Basically, this operation is not required if you are a subscriber of Route B and have Route-B authentication information.

B.2.2 End device (Dual)

Since the PAN coordinator (i.e., smart meter) searches a channel in operation, an active scan with the last eight characters of Route-B authentication ID set to Pairing ID is implemented.

The channel of the PAN coordinator that returned a response to the active scan to connect the PAN coordinator is set to make a connection with the PAN coordinator.

After completion of the connection, the channel of the PAN coordinator is saved.

After completion of pairing, the Route B can be connected without implementing an active scan by using the channel retained by the upper-level application.

Note:
Only when the operation mode is set to Dual, the PAN coordinator can be connected as the end device of the Route B.

B.2.3 Sequence of pairing of Route B

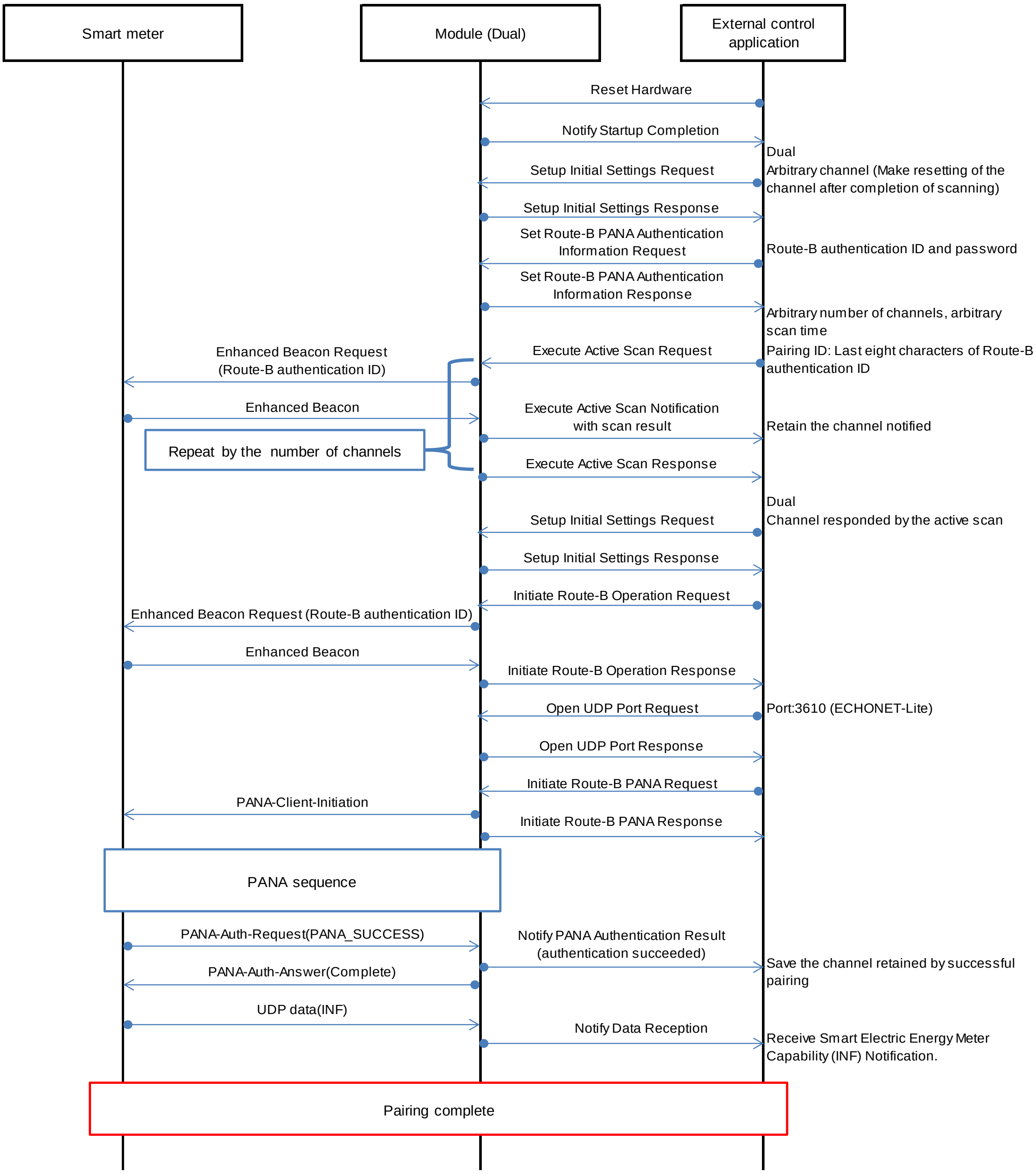
Smart meter
Module (Dual)
External control application
Reset Hardware
Notify Startup Completion
Dual
Arbitrary channel (Make resetting of the channel after completion of scanning)
Setup Initial Settings Request
Setup Initial Settings Response
Set Route-B PANA Authentication Information Request
Route-B authentication ID and password
Set Route-B PANA Authentication Information Response
Arbitrary number of channels, arbitrary scan time
Pairing ID: Last eight characters of Route-B authentication ID
Enhanced Beacon Request (Route-B authentication ID)
Execute Active Scan Request
Enhanced Beacon
Execute Active Scan Notification with scan result
Retain the channel notified
Repeat by the number of channels
Execute Active Scan Response
Dual
Channel responded by the active scan
Setup Initial Settings Request
Setup Initial Settings Response
Initiate Route-B Operation Request
Enhanced Beacon Request (Route-B authentication ID)
Enhanced Beacon
Initiate Route-B Operation Response
Open UDP Port Request
Port:3610 (ECHONET-Lite)
Open UDP Port Response
Initiate Route-B PANA Request
PANA-Client-Initiation
Initiate Route-B PANA Response
PANA sequence
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
Save the channel retained by successful pairing
PANA-Auth-Answer(Complete)
UDP data(INF)
Notify Data Reception
Receive Smart Electric Energy Meter Capability (INF) Notification.
Pairing complete

Fig. 37: Sequence of pairing of Route B

B.2.4 Sequence of normal connection of Route B

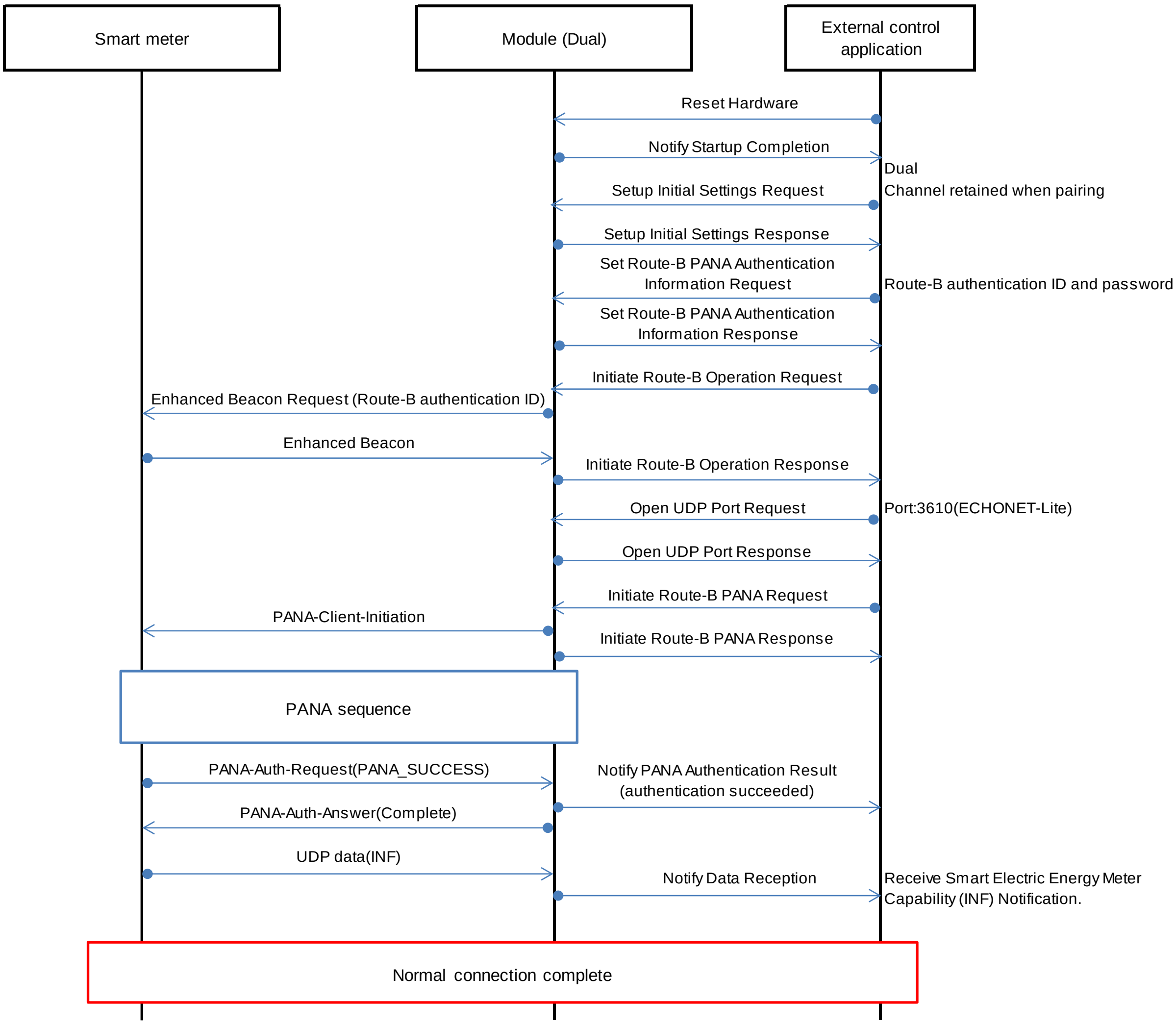
Smart meter
Module (Dual)
External control application
Reset Hardware
Notify Startup Completion
Dual
Channel retained when pairing
Setup Initial Settings Request
Setup Initial Settings Response
Set Route-B PANA Authentication Information Request
Route-B authentication ID and password
Set Route-B PANA Authentication Information Response
Initiate Route-B Operation Request
Enhanced Beacon Request (Route-B authentication ID)
Enhanced Beacon
Initiate Route-B Operation Response
Open UDP Port Request
Port:3610(ECHONET-Lite)
Open UDP Port Response
Initiate Route-B PANA Request
PANA-Client-Initiation
Initiate Route-B PANA Response
PANA sequence
PANA-Auth-Request(PANA_SUCCESS)
Notify PANA Authentication Result (authentication succeeded)
PANA-Auth-Answer(Complete)
UDP data(INF)
Notify Data Reception
Receive Smart Electric Energy Meter Capability (INF) Notification.
Normal connection complete

Fig. 38: Sequence of normal connection of Route B

Appendix C HAN connection management

C.1 Time to update HAN connection device information list

Connection device information is managed as a list in the Module in order to control devices that the Module itself in the HAN block connects or are connected to the Module itself. Connection device information for 17 units of devices (including those connected with Route B) is managed on this device information list.

The table below shows time to update the connection device information list managed in the Module.

Table 36: Time to update HAN connection device information list

Status	Registration	Manual deletion	Automatic deletion
Operating	Register a connection device in the operating status by executing **Execute Active Scan** or **Initiate HAN Operation**.	Delete the connection device by executing **Delete HAN Device From List**.	Delete the connection device in the operating status after a lapse of 80 minutes.
Authentication	Update a connection device to the authentication status by initiating HAN PANA authentication.	When the operation mode is set to PAN coordinator or Dual, delete the connection device by executing **Disconnect HAN**. When the operation mode is set to coordinator, delete the connection device by executing **Delete HAN Device From List**.	Automatic deletion is not available in the authentication status.

Cautions:

- Data communications from devices whose connection device information is not registered on the list are discarded.
- When the end device is disconnected from the PAN coordinator through HAN in the configuration of PAN coordinator <–> coordinator <–> end device, execute **Disconnect HAN** for the end device from the PAN coordinator list, but it is not deleted from the coordinator list. Delete end devices on the coordinator list by making the upper-level application execute **Delete HAN Device From List**.
- No communications can be continued in the operating status without executing PANA authentication. Devices in the operating status are automatically deleted from the connection device information list after a lapse of 80 minutes or more since they are put into the operating status.
- If a device is stopped due to power interruption, etc. without disconnection after it is put into the authentication status, the device will not be automatically deleted from the connection device information list. This causes the device information to remain. In such cases, make the upper-level application to delete the device as appropriate.

C.2 Maintenance of HAN connection

Since HAN specification provides no keepalive function, HAN connection should be maintained by the upper-level application.

The following section describes recommended keepalive operation with HAN.

- Check for the maintenance of HAN connection by checking responses from the coordinator or end device to the PAN coordinator through the periodic execution of **Transmit To Ping**, **Transmit Data**, **Check HAN Group Key Update** (pull) commands, etc.
- If the PAN coordinator no longer returns periodic responses, execute PANA re-authentication.
- In case of a PANA re-authentication failure, search the PAN coordinator by an active scan, and then execute pairing again.

Appendix D Indirect communication

When the operation mode is set to end device and the HAN sleep function is enabled, the designation of end device is changed to “sleeping end device” in order to perform indirect communication between devices connected.

In indirect communication, transmission data to the sleeping end device are all queued. The transmission data queued are all transmitted to the sleeping end device upon receipt of an inquiry request (poll request) from the sleeping end device.

In other words, the sleeping end device can receive data addressed to itself at any timing.

Indirect communication is performed only between the sleeping end device and devices connected with the sleeping end device. For example, when data is transmitted from the PAN coordinator to the sleeping end device connected with the coordinator, the data transmitted will be queued with the coordinator.

Since data queued is discarded after a lapse of 300 seconds, the sleeping end device should periodically issue **Transmit HAN Poll Request** command in order to receive data transmitted to the sleeping end device itself.

D.1 Indirect queue

Transmission data queued with a device connected with the sleeping end device are retained in the indirect queue.

The upper limit of the indirect queue is 1,232 bytes or eight packets (the number of fragments).

If the indirect queue exceeds either one of the upper limits when a command involving transmission operation, such as **Transmit Data** or **Transmit To Ping** command, is issued, queuing will fail.

A period of data retention in the indirect queue is 300 seconds after it initiates queuing (300 seconds after the first packet is added with the indirect queue in an empty status). In other words, if even one packet is retained in the indirect queue, the data retention period will not be extended by the subsequent queuing operation.

If the data retention period expires with data remaining in the indirect queue such as cases where no poll request is made from the sleeping end device for a period of 300 seconds, data in the indirect queue will be automatically discarded. The discard is notified by executing **Notify HAN Indirect Queue Discard** (§3.3.4.6).

D.2 Sequence of indirect communication

The following section shows an example of the sequence of indirect communication in the **Transmit Data** command.

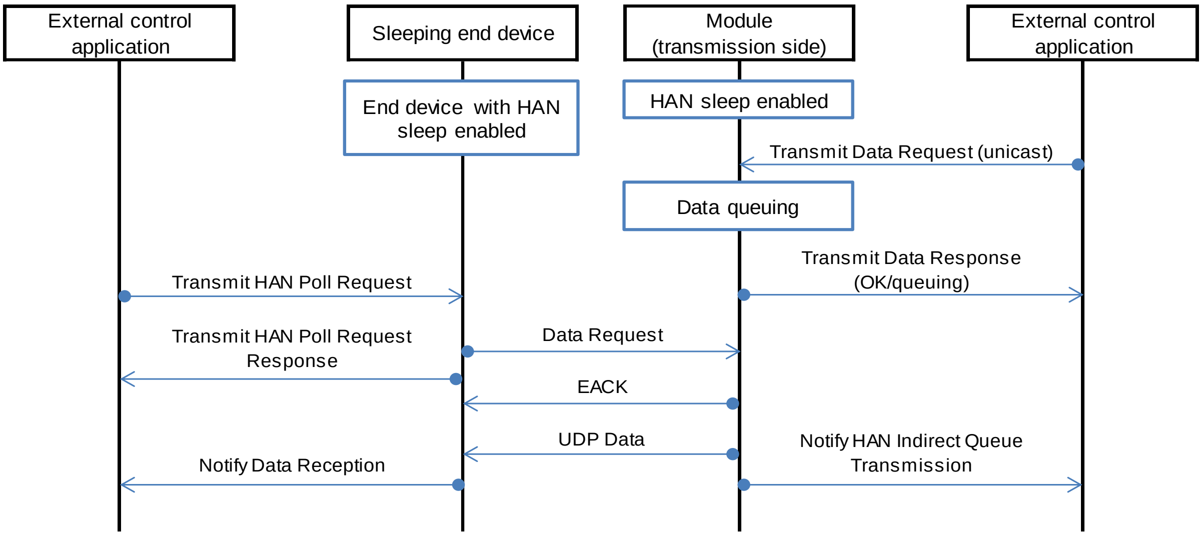
External control application
Sleeping end device
Module (transmission side)
External control application
End device with HAN sleep enabled
HAN sleep enabled
Transmit Data Request (unicast)
Data queuing
Transmit Data Response (OK/queuing)
Transmit HAN Poll Request
Transmit HAN Poll Request Response
Data Request
EACK
UDP Data
Notify HAN Indirect Queue Transmission
Notify Data Reception

Fig. 39: Example of sequence of indirect communication

D.3 Necessity to respond to poll request

The table below lists sequences that require a poll request in Chapter 5, “Command sequences”.

Table 37: Necessity to respond to poll request in command sequence

Sequence	Poll request	Overview
Sequence of **Reset Hardware**	No necessary	No effect on indirect operation
Sequence of **Execute Active Scan**	No necessary	Unnecessary because Beacon does not perform indirect operation.
Sequence of **Initiate HAN Operation**	No necessary	Unnecessary because Beacon does not perform indirect operation.
Sequence of **Terminate HAN Operation**	No necessary	No effect on indirect operation
Sequence of **Initiate HAN PANA**	Necessary	Periodic poll requests are necessary until PANA authentication is complete.
Sequence of **Terminate HAN PANA**	Conditionally necessary	Unnecessary if timing to terminate PANA cannot be grasped. If such timing can be grasped by the upper-level application, periodic poll requests are necessary until the termination of PANA is complete.
Sequence of **Distribute HAN Group Key** (push)	Conditionally necessary	Unnecessary if timing to distribute group key cannot be grasped. If such timing can be grasped by the upper-level application, periodic poll requests are necessary until the distribution of group key is complete.
Sequence of **Check HAN Group Key Update** (pull)	Necessary	Periodic poll requests are necessary until checking for updating of HAN group key is complete.
Sequence of **Re-authenticate HAN PANA**	Conditionally necessary	Unnecessary if timing to execute PANA re-authentication cannot be grasped. If such timing can be grasped by the upper-level application, periodic poll requests are necessary until PANA re-authentication is complete.
Sequence of **Disconnect HAN**	Conditionally necessary	Unnecessary if timing to terminate PANA cannot be grasped. If such timing can be grasped by the upper-level application, periodic poll requests are necessary until the termination of PANA is complete.
Sequence of **Set HAN Sleep Device PANA Retransmission Interval**	Necessary	Periodic poll requests are necessary until the setting of a retransmission interval for PANA message to HAN sleep device is complete.
Sequence of **Transmit Data and Notify Data Reception**	Necessary	Periodic poll requests are necessary until data transmission/reception is complete.
Sequence of **Transmit To Ping**	Necessary	Periodic poll requests are necessary until data transmission/reception to/from Ping is complete.

Appendix E Deep sleep function

The deep sleep function is designed to make hardware transition to a deep sleep mode.

Since indirect communication using the deep sleep function is different from that using the HAN sleep function, the deep sleep function can be used regardless of whether the HAN sleep function is enabled or disabled.

The **HAN Deep Sleep Request** command is executable only when the operation mode is set to end device.

When the **HAN Deep Sleep Reques**t command is issued, the hardware will transit to the deep sleep mode.

When the hardware is in the deep sleep mode, timers stop running. Note that this causes timer operation not to be performed as shown in Chapter 5, “Command sequences”.

The timer used to calculate the sum of transmission data amount per hour specified in ARIB STD-T108 remains in operation even in the deep sleep mode.

The deep sleep function monitors the UART-TXD terminal while in the deep sleep mode and will release the deep sleep mode when Low signal is detected. The deep sleep mode can be released by transmitting an arbitrary command (see Note) or data (e.g. 1 byte of 0x00) from user. After the deep sleep mode is released, that effect is notified using WakeUp **Notification** (see §3.3.3.13.3, “Notification command parameter”).

Furthermore, since RF is set to OFF after completion of WakeUp **Notification**, the hardware cannot receive any command or data. RF is set to ON by executing transmission from the Module, thus allowing the hardware to receive commands and data.

Note: Commands transmitted during the deep sleep mode release are not processed.

E.1 Command sequences

The following section shows examples of use of the deep sleep function with HAN sleep function enabled or disabled.

E.1.1 Sequence of deep sleep function (with HAN sleep function enabled)

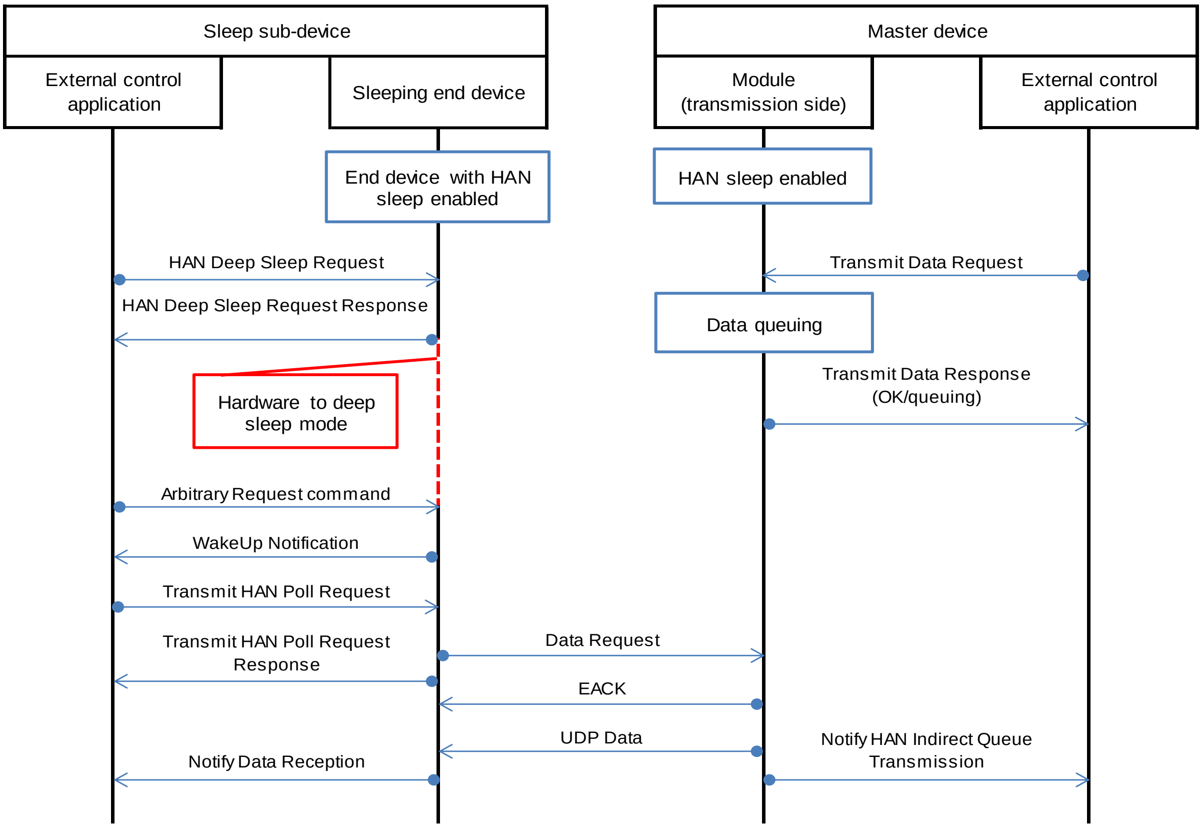
Sleep sub-device
External control application
Sleeping end device
Master device
Module (transmission side)
External control application
End device with HAN sleep enabled
HAN sleep enabled
HAN Deep Sleep Request
Transmit Data Request
HAN Deep Sleep Request Response
Data queuing
Hardware to deep sleep mode
Transmit Data Response (OK/queuing)
Arbitrary Request command
WakeUp Notification
Transmit HAN Poll Request
Transmit HAN Poll Request Response
Data Request
EACK
UDP Data
Notify HAN Indirect Queue Transmission
Notify Data Reception

Fig. 40: Sequence of deep sleep function (with HAN sleep function enabled)

E.1.2 Sequence of deep sleep function (with HAN sleep function disabled)

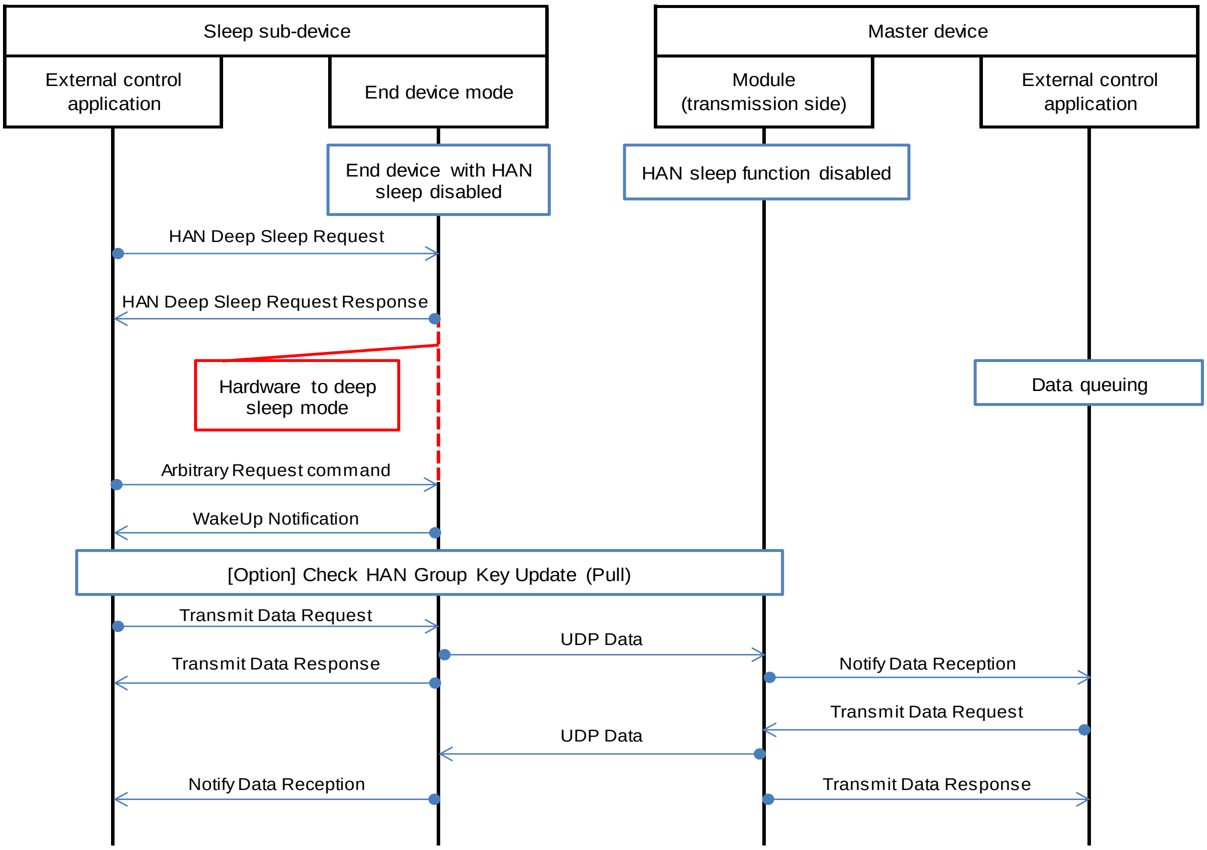
Sleep sub-device
External control application
End device mode
Master device
Module (transmission side)
External control application
End device with HAN sleep disabled
HAN sleep function disabled
HAN Deep Sleep Request
HAN Deep Sleep Request Response
Hardware to deep sleep mode
Data queuing
Arbitrary Request command
WakeUp Notification
[Option] Check HAN Group Key Update (Pull)
Transmit Data Request
UDP Data
Transmit Data Response
Notify Data Reception
Transmit Data Request
UDP Data
Notify Data Reception
Transmit Data Response

Fig. 41: Sequence of deep sleep function (with HAN sleep function disabled)

E.2 Timing to fail transition to deep sleep mode

The following section lists statuses in which the **HAN Deep Sleep Request** command results in failure.

In these statuses, the hardware does not accept the command to return an error response.

1. PANA sequence is in operation;
2. OTA port is opening;
3. OTA sequence is in operation;
4. The sequence of HAN sleep function with indirect communication is in operation;
5. MAC transmission data queuing is in progress;
6. PHY is receiving data;
7. PHY is in operation.

Appendix F Check Items in order to return error response

F.1 Response result: 0x01

Description
Command succeeded

F.2 Response result: 0x02

Description
The specified address does not exist in the device list.
Occurrence example
HAN Purge Request command [0x0069] issued to an address that is not in the device list.
Check item
Check whether the specified address is on the device list by issuing the **Get Connection Status Request** [0x0011] command or **Get Terminal Information Request** command [0x0100].
Recommended operation
No commands can be executed for a specified address.

F.3 Response result: 0x03

Description
Invalid command code
Occurrence example
Cases where any illicit command other than **Request** commands was issued
Check item
Check whether the command issued is defined in this document.
Recommended operation
Reissue the command by specifying the correct command code.

F.4 Response result: 0x04

Description
Invalid parameter value
Occurrence example
Cases where the parameter value of the command fell outside the range or was an invalid value
Check item
Check whether the specified value is correct.
Recommended operation
Reissue the command by specifying the correct parameter value.

F.5 Response result: 0x06

Description
Transmission error due to invalid address
Occurrence example
Cases where an address not on the device list was specified by issuing the **Transmit Data Request** command [0x0008].
Check item
Issue the **Get Terminal Information Request** command [0x0100] to check whether the specified address is on the device list.
Recommended operation
Reissue the command by specifying the correct address.

F.6 Response result: 0x0A

Description
Port opening error: Already open port number
Occurrence example
Cases where the **Open UDP Port Request** command [0x0005] was issued to an opened port number
Check item
Issue the **Get UDP Port Open Status Request** [0x0007] to check whether the specified port number is open.
Recommended operation
Specify an unopened port number to issue the **Open UDP Port Request** command [0x0005].

F.7 Response result: 0x0B

Description
Port closing error: Unopened port number
Occurrence example
Cases where the **Close UDP Port Request** command [0x0006] was issued to an unopened port
Check item
Issue the **Get UDP Port Open Status Request** [0x0007] to check whether the specified port number is open.
Recommended operation
Specify the opened port number to issue the **Close UDP Port Request** command [0x0006].

F.8 Response result: 0x0E

Description
MAC connection failed
Occurrence example
Cases where EBR could not be transmitted or EB could not be received after issuing the **Initiate Route-B Operation Request** [0x0053] or **Initiate HAN Operation Request** [0x000A] command
Check item
Referring to Appendix B "Pairing”, ensure that pairing has been set so as to allow pairing of master and slave devices (e.g. channel, Pairing ID, acceptance connection mode, HAN sleep function, and Route-B authentication ID).
Recommended operation
Specify a correct channel and Pairing ID to issue the **Initiate HAN Operation Request** command [0x000A].

F.9 Response result: 0x0F

Description
Executability error: Unexecutable due to HAN in the operating status/Mismatched operation mode
Occurrence example
Cases where a command that became NA (not executable) due to HAN in the operating status in the table shown in §2.8 “Executability of commands” was issued
Check item
Issue the **Get Status Request** command [0x0001] to check whether the current status is ✓ (executable) in the table shown in §2.8, “Executability of commands”.
Recommended operation
Make the current status transition to a status marked with ✓ (executable) in the table shown in §2.8, “Executability of commands” to reissue the command.

F.10 Response result: 0x10

Description
Executability error: Unexecutable due to Route B or HAN in the not-yet-started status/Mismatched operation mode
Occurrence example
Cases where a command that became NA (not executable) due to HAN in the not-yet-started status in the table shown in §2.8 “Executability of commands” was issued
Check item
Issue the **Get Status Request** command [0x0001] to check whether the current status is ✓ (executable) in the table shown in §2.8, “Executability of commands”.
Recommended operation
Make the current status transition to a status marked with ✓ (executable) in the table shown in §2.8, “Executability of commands” to reissue the command.

F.11 Response result: 0x11

Description
The specified parameter length exceeded the maximum length or was less than the minimum length
Occurrence example
Cases where the parameter length exceeds the maximum length or is less than the minimum value
Check item
Check whether parameters are based on the format of each command.
Recommended operation
Issue a command by specifying correct parameters.

F.12 Response result: 0x12

Description
Maximum number of opened ports exceeded
Occurrence example
Cases where the **Open UDP Port Request** command [0x0005] is issued in excess of the maximum number of opened ports
Check item
Issue the **Get UDP Port Open Status** command [0x0007] to check whether unnecessary ports remain opened.
Recommended operation
Issue the **Close UDP Port** command [0x0006] to close the unnecessary ports. Subsequently, issue the **Open UDP Port Request** command [0x0005].

F.13 Response result: 0x13

Description
Command reception error: Data reception time (1 second) expired
Occurrence example
Cases where the UART stopped transmission when a command was being issued and one second elapsed
Check item
Ensure that the command message length corresponds to the length of data portion transmitted from the UART.
Recommended operation
Reissue the command due to an inter-UART communication failure.

F.14 Response result: 0x14

Description
Executability error: Unexecutable operation mode
Occurrence example
Cases where a command that became NA (not executable) due to the current status in the table shown in §2.8 “Executability of commands” was issued
Check item
Issue the **Get Terminal Information Request** command [0x0100] to check whether the current operation mode is set to an intended operation mode.
Recommended operation
If the current operation mode is set to the intended operation mode, ignore this error because the issued command is not executable. If it is set to an unintended operation mode, change the operation mode, and then reissue the command.

F.15 Response result: 0x20

Description
The same mode was specified as the current mode by **Switch HAN Acceptance Connection Mode Request** command
Occurrence example
Cases where the same connection mode as the current mode was issued by issuing the **Switch HAN Acceptance Connection Mode Request** command [0x0025].
Check item
None
Recommended operation
Since the operation mode is set to already-specified connection mode, ignore this error.

F.16 Response result: 0x21

Description
Executability error: Operation mode in which **Switch HAN Acceptance Connection Mode** is unexecutable
Occurrence example
Cases where an end device issued the **Switch HAN Acceptance Connection Mode Request** command [0x0025]
Check item
None
Recommended operation
Since the operation mode is set to a mode in which the command is not executable, ignore this error.

F.17 Response result: 0x33

Description	Executability error: Unexecutable due to HAN in the authentication status/Mismatched operation mode
Occurrence example	Cases where a command that became NA (not executable) due to HAN in the authentication status in the table shown in §2.8 “Executability of commands” was issued
Check item	Check for the executability of the command. Issue the **Get Status Request** command [0x0001] to check whether the current status is ✓ (executable) in the table shown in §2.8, “Executability of commands”. Check for the status of an opposing device. Issue the **Get Connection Status Request** command [0x0011] to ensure that a device to be disconnected is in the HAN authentication status.
Recommended operation	Make the current status transition to a status marked with ✓ (executable) in the table shown in §2.8 “Executability of commands” to reissue the command. Specify a device in the authentication status to issue the **Delete HAN Device From List** command [0x006A].

F.18 Response result: 0x34

Description	Executability error: Unexecutable due to Route B in the operating status
Occurrence example	Cases where a command that became NA (not executable) due to the Route B in the operating status in the table shown in §2.8 “Executability of commands” was issued
Check item	Issue the **Get Status Request** command [0x0001] to check whether the current status is ✓ (executable) in the table shown in §2.8, “Executability of commands”
Recommended operation	Make the current status transition to a status marked with ✓ (executable) in the table shown in §2.8, “Executability of commands” to reissue the command.

F.19 Response result: 0x35

Description	Executability error: Unexecutable due to Route B in the authentication status
Occurrence example	Cases where a command that became NA (not executable) due to the Route B in the authentication status in the table shown in §2.8 “Executability of commands” was issued
Check item	Issue the **Get Status Request** command [0x0001] to check whether the current status is ✓ (executable) in the table shown in §2.8, “Executability of commands”
Recommended operation	Make the current status transition to a status marked with ✓ (executable) in the table shown in §2.8, “Executability of commands” to reissue the command.

F.20 Response result: 0x37

Description
Executability error: Unexecutable due to the whole block in the not-yet-started status
Occurrence example
Cases where a command that became NA (not executable) due to the whole block in the not-yet-started status in the table shown in §2.8 “Executability of commands” was issued
Check item
Issue the **Get Status Request** command [0x0001] to check whether the current status is ✓ (executable) in the table shown in §2.8, “Executability of commands”.
Recommended operation
Make the current status transition to a status marked with ✓ (executable) in the table shown in §2.8, “Executability of commands” to reissue the command.

F.21 Response result: 0x3C

Description
Cases where **Transmit To Ping Request** command is requested again before executing **Transmit To Ping Notification** command
Occurrence example
Cases where **Transmit To Ping Request** command [0x00D1] command was issued before receiving the **Transmit To Ping Notification** command [0x60D1]
Check item
Check whether the **Transmit To Ping Notification** command [0x60D1] has been received.
Recommended operation
Wait until the **Transmit To Ping Notificatio**n command [0x60D1] is received, and then issue the **Transmit To Ping Request** command [0x00D1].

F.22 Response result: 0x3D

Description
Cases where a different **Request** command is executed before the **Response** command is executed or its internal processing is in progress
Occurrence example
Cases where the **Request** command was issued before receiving the **Response** command
Check item
Check whether the **Response** command has been received.
Recommended operation
Wait until the **Response** command is received, and then reissue the command.

F.23 Response result: 0x3E

Description
Cases where the same PAN ID as that for Route B or 0xFFFF is specified
Occurrence example
Cases where the same PAN ID or 0xFFFF as that for the Route B was specified by issuing the **Initiate HAN Operation Request** command [0x000A]
Check item
Issue the **Initiate Route-B Operation Response** command [0x2053] to check whether the specified PAN ID is not 0xFFFF and PAN ID is the same as that for the Route B.
Recommended operation
Specify PAN ID different from that for the Route B (except 0xFFFF) to reissue the **Initiate HAN Operation Request** [0x000A].

F.24 Response result: 0x3F

Description
Cases where transition to deep sleep mode is failed
Occurrence example
Cases where the **HAN Deep Sleep Request** command [0x00DA] command was issued in the status in which the deep sleep function was disabled.
Check item
Check whether the internal processing of the command is in progress. See also E.2, “Timing to fail transition to deep sleep mode”.
Recommended operation
In cases where the hardware operates as OTA Client: Wait until the **Notify OTA Operation Termination** command [0x6034] is received, and then issue the **HAN Deep Sleep Request** command [0x00DA]. In cases where the hardware operates as OTA Server: Issue the **Close UDP Port Request** command [0x0006] to close the OTA update port (31941), and then issue the **HAN Deep Sleep Request** command [0x00DA]. In cases where the PANA sequence is in operation: Wait until the PANA sequence result **Notification** commands [0x6026, 0x6027, 0x6028, 0x6029, 0x6030] are received, and then issue the **HAN Deep Sleep Request** command [0x00DA]. Other than those above: Reissue the **HAN Deep Sleep Request** command [0x00DA].

F.25 Response result: 0x46

Description
Cases where a poll request is failed
Occurrence example
Cases where a carrier was sensed or ACK could not be received after the **Transmit HAN Poll Request** command [0x0061] was issued and before the poll request was transmitted
Check item
None
Recommended operation
Since the wireless LAN is highly likely to be congested, reissue the **Transmit HAN Poll Request** command [0x0061].

F.26 Response result: 0x51

Description
PANA execution error: Inadequate setting or information ungenerated
Occurrence example
Coordinator/end device: Cases where the **Get HAN PANA Authentication Information Request** command [0x002D] command or the **Initiate HAN PANA Request** command [0x003A] in the status in which PANA authentication information was not set PAN coordinator/Dual: Cases where the **Distribute HAN Group Key Request** command [0x0029] was issued in the status in which there were no devices put in the HAN authentication status
Check item
Coordinator/end device: None PAN coordinator/Dual: None
Recommended operation
Coordinator/end device: Issue the **Set HAN PANA Authentication Information Request** [0x002C], and then reissue the command. PAN coordinator/Dual: Connect an arbitrary device, and then reissue the **Distribute HAN Group Key Request** command [0x0029].

F.27 Response result: 0x52

Description
PANA execution error: PANA sequence in operation
Occurrence example
Cases where the **Initiate Route-B PANA Request** command [0x0056] was issued after the **Initiate Route-B PANA Request** command [0x0056] was issued and before the **Notify PANA Authentication Result** command [0x6028] was received
Check item
Check whether the **Request** command was transmitted before the **Notify PANA Authentication Result** command [0x6028] was received.
Recommended operation
Ensure the reception of the **Notify PANA Authentication Result** command [0x6028], and then reissue the command.

F.28 Response result: 0x53

Description
PANA execution error: No information in the specified address
Occurrence example
Cases where the **Delete HAN PANA Authentication Information Setting Request** command [0x002E] by specifying an address to which no PANA authentication information was set
Check item
Check whether the specified address is correct.
Recommended operation
If the address is correct, no authentication information has been set. Consequently, it is necessary to delete authentication information. Ignore this error.

F.29 Response result: 0x58

Description
PANA execution error: authentication information has been set
Occurrence example
Cases where the **Set HAN PANA Authentication Information Request** command [0x002C] was issued twice
Check item
None
Recommended operation
Since authentication information has been set, ignore this error.

F.30 Response result: 0x59

Description
PANA execution error: Maximum set number exceeded
Occurrence example
Cases where the **Set HAN PANA Authentication Information Request** command [0x002C] for the 18th device was issued
Check item
Issue the **Get HAN PANA Authentication Information Request** command [0x002D] to check whether any unnecessary authentication information has been set.
Recommended operation
Delete the unnecessary authentication information by issuing the **Delete HAN PANA Authentication Information Setting Request** command [0x002E]. Subsequently, issue the **Set HAN PANA Authentication Information Request** command [0x002C].

F.31 Response result: 0x61

Description
Invalid OTA Client status
Occurrence example
Cases where the **Terminate OTA Client Request** command [0x0202] was issued in the status in which the **Initiate OTA Client Request** command [0x0201] was not issued
Check item
None
Recommended operation
Since OTA Client has been terminated, ignore this error.

F.32 Response result: 0xF0

Description
Command reception error: Header checksum error
Occurrence example
Invalid checksum of the command header block
Check item
Check whether the header checksum of the command issued is correct.
Recommended operation
Correct the header checksum to a correct value, and then reissue the command.

F.33 Response result: 0xF1

Description
Command reception error: Data checksum error
Occurrence example
Invalid checksum of the command header block
Check item
Check whether the data checksum of the command issued is correct.
Recommended operation
Correct the data checksum to a correct value, and then reissue the command.

F.34 Response result: 0xF2

Description
Command reception error: Message length specified by the header is short
Occurrence example
Cases where the command message length was less than 4 bytes
Check item
Check whether the message length of the command issued is correct.
Recommended operation
Correct the message length to a correct value, and then reissue the command.

F.35 Response result: 0xF3

Description
Command reception error: Message length specified by the header exceeded the maximum length
Occurrence example
Cases where the command message length exceeded 1,353 bytes
Check item
Check whether the message length of the command issued is correct.
Recommended operation
Correct the message length to a correct value, and then reissue the command.

Appendix G Troubleshooting

G.1 Radio wave status and installation location

- A communicable distance significantly depends on the environment in which the hardware is installed. In order to check the radio wave status, use a command that allows for checking RSSI levels (e.g. commands listed below). If the RSSI level is constantly low (i.e., -80 dBm or less), review the installation location.
    - **Transmit To Ping**:
    - **Notify Data Reception**;
    - **Notify Connection Status Change**;
    - **Initiate HAN Operation**;
    - **Initiate Route-B Operation**;
    - **Execute Active Scan**.
- If communication failures are frequently caused, the channel in use may be noisy or congested. The communication quality may be improved by changing it to a different channel.
- When the transmission output power is set lower from the default of 20 mW, the communicable distance will become shorter. When the transmission output power is set lower, review the installation location.

G.2 Limitation on the sum of transmission data amount

- The amount of data that can be wirelessly transmitted per hour is limited to 4.5 MB (integrated value of wireless transmission size including preambles). Trying to transmit data beyond this limited data amount will cause all commands involving wireless transmission to fail.
- Data transmission is limited, but data can be continually received.
- When the coordinator reaches the limited sum of transmission data amount, relay operation will be suspended. Be noted that, even if the coordinator does not execute a command involving wireless transmission, the amount of data wirelessly transmitted for relay transfer will be integrated, making it easier to reach the upper limit of the sum of transmission data amount in coordinator mode than in the PAN coordinator and end device modes.

G.3 No response is returned even if a Request command is transmitted

1. Check whether power is supplied to the hardware and the **Notify Startup Completion** is received.
2. Check whether the connection parameters of UART interface, such as baud rate, are met.
   See Table 3: UART IF connection parameters (values).
3. Check whether the unique code prefixed to the UART IF command is correct.
   Since data is discarded until the unique code is detected, check whether the unique code is correct.

G.4 HAN

G.4.1 Failure in the initiation of HAN operation

If a response to the **Initiate HAN Operation** executed in coordinator or end device mode resulted in a MAC connection failure (0x0E), check whether:

1. The set channel is the same as that of PAN coordinator;
2. Mac address set to Pairing ID, if any, corresponds to the MAC address of the PAN coordinator;
3. The connection mode of the PAN coordinator is set to initial connection mode when All 0xFF (HAN_INIT) is set to Paring ID.

G.4.2 Failure in PANA authentication

1. Check whether the PAN coordinator mode properly sets the PANA authentication information (i.e., MAC address and password) on a device that failed in authentication.
2. Check whether PANA authentication information (i.e., password) is properly set to the coordinator or end device, and further check whether the password corresponds to that set to the PAN coordinator.
3. In case of sleeping end devices, a poll request should be transmitted to receive a PANA message. For this purpose, periodically transmit a poll request until PANA authentication is complete.

G.4.3 Reception from the opposing device is disabled

1. Check whether the destination specified by the opposing device (e.g. MAC address or IPv6 address format) is correct.
2. Check whether the opposing device opens the destination port number.
   Since a packet transmitted to an unopened port results in a reception failure, the destination port number used by the source should have been opened before the port number is transmitted.

G.4.4 Cause of reception failure is a decryption failure (0x01) or a failure in MAC (0x02)

If the cause of a failure in the reception of the notification of packet reception failure is a decryption failure (0x01) or a failure in MAC (0x02), the device of the source may not match to the encryption key or the frame counter.

If the cause is the PAN coordinator, issue the **Re-authenticate HAN PANA** command.

If the cause is the coordinator or end device, check for the update of the encryption key by issuing the **Check HAN Group Key Update** command. If the phenomenon is still not remedied, issue the **Initiate HAN PANA** command to authenticate HAN PANA.

G.4.5 Notify Packet Reception Failure is executed at the time of multicast transmission

If an end device is connected through the coordinator and the PAN coordinator and end device are installed in a location in which radio wave communication can be performed, **Notify Packet Reception Failure** may be executed when the end device directly receives a packet that the PAN coordinator transmitted using multicast. The cause of reception failure is a failure in MAC (0x02).

Since the end device is not connected directly with the PAN coordinator, it determines the reception to be that from a stranger and then notifies the reception failure. Since a packet relayed by the coordinator (i.e., a packet to be received) is normally received, ignore the notification of reception failure in this case.

G.5 Route B

G.5.1 Initiate Route-B Operation command fails

If a response results in a MAC connection failure (0x0E):

1. Check whether the smart meter operates over the set channel.
   In order to check the channel over which the smart mater operates, set the last eight characters of Route-B authentication ID to Pairing ID of the **Execute Active Scan** command, and scan all channels.
2. Check whether the set Route-B authentication ID is correct.
   Since the authentication ID is used for MAC connection, the Route-B authentication ID should correspond to the authentication ID set to the smart meter.

G.5.2 PANA authentication fails

Check whether the Route-B authentication ID and the password are correct.
In case of an authentication failure, either one or both of the Route-B authentication ID and the password may not match to the smart meter.

G.5.3 Reception from the smart meter is disabled

See the causes described in G.4.3, “Reception from the opposing device is disabled”.

G.5.4 Cause of reception failure is a decryption failure (0x01) or a failure in MAC (0x02)

If the cause of reception failure is a decryption failure (0x01) or a failure in MAC (0x02), the smart meter may not match to the encryption key or the frame counter. In this case, execute authentication by the **Initiate Route-B PANA Re-authentication** command.

If the phenomenon is still not remedied, execute the **Terminate Route-B PANA** command, and then make resetting of Route-B authentication ID and password to execute authentication by issuing the **Initiate Route-B PANA**.

Notes

1) The information contained herein is subject to change without notice.

2) Before you use our Products, please contact our sales representative and verify the latest specifications :

3) Although ROHM is continuously working to improve product reliability and quality, semiconductors can break down and malfunction due to various factors.
Therefore, in order to prevent personal injury or fire arising from failure, please take safety measures such as complying with the derating characteristics, implementing redundant and fire prevention designs, and utilizing backups and fail-safe procedures. ROHM shall have no responsibility for any damages arising out of the use of our Poducts beyond the rating specified by ROHM.

4) Examples of application circuits, circuit constants and any other information contained herein are provided only to illustrate the standard usage and operations of the Products. The peripheral conditions must be taken into account when designing circuits for mass production.

5) The technical information specified herein is intended only to show the typical functions of and examples of application circuits for the Products. ROHM does not grant you, explicitly or implicitly, any license to use or exercise intellectual property or other rights held by ROHM or any other parties. ROHM shall have no responsibility whatsoever for any dispute arising out of the use of such technical information.

6) The Products specified in this document are not designed to be radiation tolerant.

7) For use of our Products in applications requiring a high degree of reliability (as exemplified below), please contact and consult with a ROHM representative : transportation equipment (i.e. cars, ships, trains), primary communication equipment, traffic lights, fire/crime prevention, safety equipment, medical systems, servers, solar cells, and power transmission systems.

8) Do not use our Products in applications requiring extremely high reliability, such as aerospace equipment, nuclear power control systems, and submarine repeaters.

9) ROHM shall have no responsibility for any damages or injury arising from non-compliance with the recommended usage conditions and specifications contained herein.

10) ROHM has used reasonable care to ensure the accuracy of the information contained in this document. However, ROHM does not warrants that such information is error-free, and ROHM shall have no responsibility for any damages arising from any inaccuracy or misprint of such information.

11) Please use the Products in accordance with any applicable environmental laws and regulations, such as the RoHS Directive. For more details, including RoHS compatibility, please contact a ROHM sales office. ROHM shall have no responsibility for any damages or losses resulting non-compliance with any applicable laws or regulations.

12) When providing our Products and technologies contained in this document to other countries, you must abide by the procedures and provisions stipulated in all applicable export laws and regulations, including without limitation the US Export Administration Regulations and the Foreign Exchange and Foreign Trade Act.

13) This document, in part or in whole, may not be reprinted or reproduced without prior consent of ROHM.

ROHM SEMICONDUCTOR

Thank you for your accessing to ROHM product informations.
More detail product informations and catalogs are available, please contact us.

ROHM Customer Support System

http://www.rohm.com/contact/