IEEE P802.15

Wireless Personal Area Networks

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)
Title	IEEE Std 802.15.4e-D0.01
Date Submitted	2009/08/25
Source	[Ludwig Winkel, Zafer Sahinoglu, Liang Li], and feeded by the following subgroups: PA, FA, E-GTS, Low-Energy, Short-Header] Voice: [] E-mail: [ludwig.winkel@siemens.com,] [liang_1@yahoo.com,] [zafer@merl.com]
Re:	[]
Abstract	[1st draft IEEE Std 802.15.4e-D0.01 based on submissions of the PA-, FA-, E-GTS-, Low-Energy-subgroups, of TG4e.]
Purpose	[]
Notice	This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15.

IEEE P802.15.4e™/D0.01 Draft Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements— Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 1: Add MAC enhancements for industrial applications and CWPAN

Prepared by the LAN/MAN Standards Committee Working Group of the

IEEE Computer Society Committee

IEEE Standards Activities Department
445 Hoes Lane
Piscataway, NJ 08854, USA

Abstract: First draft of 802 WG15 TG4e. Amendment to IEEE Std 802.15.4-2009
Keywords: Amendment for application domains like Process automation, Low latency, Commercial, and enhancements for Security, low energy, etc.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-0-XXXX-XXXX-X STDXXXXX
Print: ISBN 978-0-XXXX-XXXX-X STDPDXXXXX

This page is left blank intentionally.

Introduction

This introduction is not part of IEEE P802.15.4e/D0.01, Draft Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements— Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 1: Add MAC enhancements for industrial applications and CWPAN.

Notice to users

Text formatted as this line means an editor note and will be removed before publication.

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this draft standard was submitted to the IEEE-SA Standards Board for approval, the LAN/MAN Standards Committee Working Group had the following membership:

Bob Heile, *Chair*
Pat Kinney, *Vice Chair*

Participant1
Participant2
Participant3
Participant4
Participant5
Participant6
Participant7
Participant8
Participant9

The following members of the [individual/entity] balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

(to be supplied by IEEE)

Participant1
Participant2
Participant3
Participant4
Participant5
Participant6
Participant7
Participant8
Participant9

Contents

Draft Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements— Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 1: Add MAC enhancements for industrial applications and CWPAN

NOTE—The editing instructions contained in this <amendment/corrigendum> define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.

1. Overview

2. Normative references

3. Definitions

Insert in alphabetical order the following definitions.

low latency network (LLNW): A PAN organized as star-network with a superframe structure and using frames with a MAC header of 1 octet length (frame type b100). The gateway of a low latency network indicates the existence of such a low latency network by periodically sending beacons with a MAC header of 1 octet (frame type b100).

4. Acronyms and abbreviations

Insert in alphabetical order the following acronyms.

LLNW	Low Latency Network
PA	Process automation
FA	Factory automation
LL	Low latency

5. General description

5.1 Introduction

Insert before 5.2 the following text.

In addition, several behaviors are amended for

— different industrial and other application domains and

— functional improvements.

The different industrial and other application domains have quite different requirements as they are often also diametrical opposition to each other so that the resulting solutions cannot be the same (see Annex M). That is the rational for specifying more than one solution because they are more than one problem to solve. Those solutions are marked in the normative clauses with terms that are given in Annex M.

5.2 Components of the IEEE 802.15.4 WPAN

5.3 Network topologies

5.3.1 Star network formation

5.3.2 Peer-to-peer network formation

Insert before 5.4 the following subclauses.

5.3.3 LL-Star network for wireless low latency networks

5.3.3.1 General

Due to the stringent latency requirements of low latency applications, the star network becomes a topology of choice with a superframe structure that supports low latency communication between the gateway device and its sensor/actuator devices. Both to accelerate frame processing and to reduce transmission time, short MAC frames with a 1-octet MAC header (shortened frame control) are deployed.

5.3.3.2 TDMA Access

The PHY is accessed by a TDMA scheme, which is defined by a superframe of fixed length. The superframe is synchronized with a beacon transmitted periodically from the gateway. Access within the superframe is divided into time slots. The superframe can be configured to provide the full spectrum from complete deterministic access to shared access. For deterministic access each device is assigned to a particular time slot of fixed length. Shared Group timeslots allow multiple access for a group of nodes within a duration enclosing an arbitrary number (up to the whole superframe) of dedicated time slots.

To ensure coexistence with other RF technologies in the 2.4GHz ISM band, no channel hopping is applied.

5.3.3.3 Addressing

The LL-star network supports two addressing schemes. The first addressing mode is based on the time slot assigned to a device for communication, i.e. the time slot corresponds exactly to a single device. The second mode supports the short address format.

5.3.3.4 Network Topology

The LL sensor network requires a star topology (see Figure 1.a). Sensor/actuator devices are connected to a single gateway. The sensors send the sensor-data unidirectionally to the gateway. Actuators are configured to exchange data bidirectionally with the gateway.

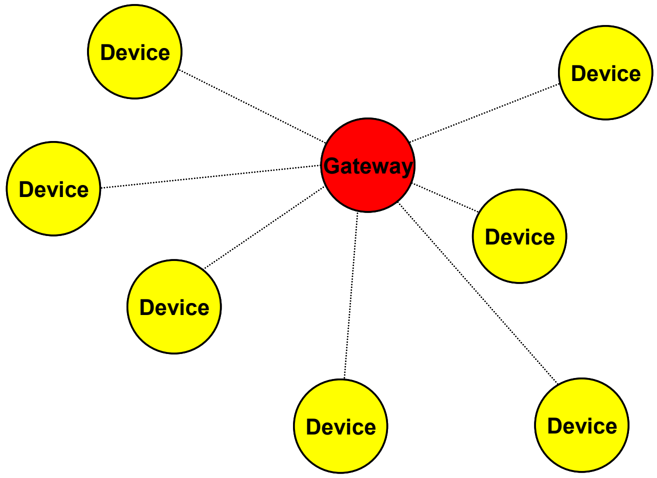


Figure 1.a—Star topology LL-MAC.

The selection of channels and time slots for communication is planned in a network management instance. The sensors and actuators are configured over the gateway based on planning information of the network management instance.

5.4 Architecture

5.5 Functional overview

5.5.1 Superframe structure

Insert after the heading of 5.5.1 the following subclause.

5.5.1.1 General

Insert after the first sentence of 5.5.1 the following paragraph and subclauses.

There are different superframe structures possible:

- Superframe structure based on beacons of frame type Beacon as defined in 7.2.2.1. These beacons have a long MAC header.
- Superframe structure based on beacons with a 1-octet MAC header as defined in 7.2.2a.1. These beacons have a short MAC header.

Insert before 5.5.2 the following subclause.

5.5.1.2 Superframe structure based on Beacons

If *macFAlowLatencePAN* is set to TRUE, the device is the gateway in a low latency network as described in 5.3.3.

The superframe is divided into a beacon slot and *macFAnumTimeSlots* number of time slots of equal length, see Figure 1.b.

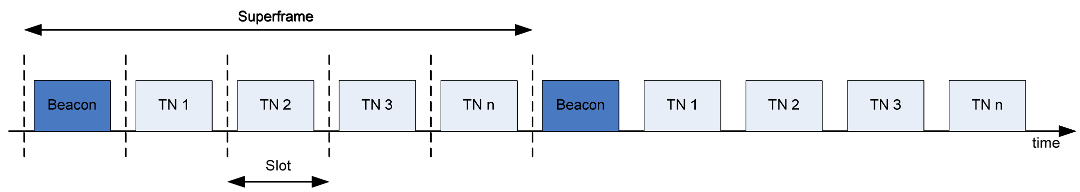


Figure 1.b—Superframe with dedicated time slots.

The first time slot of each superframe contains a beacon frame. The beacon frame is used for synchronization with the superframe structure. It is also used for re-synchronization of devices that went into power save or sleep mode.

The remaining time slots are assigned to the sensor and actuator devices in the network, so that there is no explicit addressing necessary inside the frames provided that there is exactly one device assigned to a time slot (see 7.5.1.1a.6). The determination of the sender is achieved through the indexing of time slots. If there are more than one device assigned to a time slot, the time slot is referred to as shared group time slot, and a simple addressing scheme is used as described in 7.1.1.

As shown in Figure 1.c, there is a specific order in the meaning or usage of the time slots.

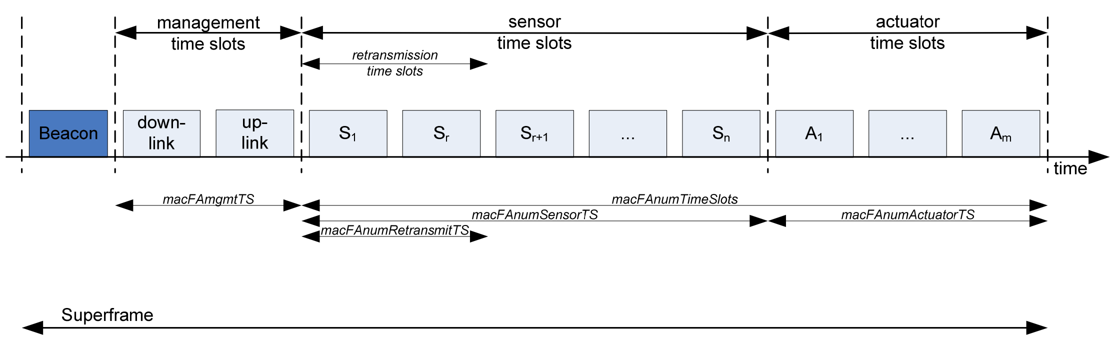


Figure 1.c—Usage and order of slots in a superframe.

— Beacon Time Slot: always there (cf. 7.5.1.1a.2)

— Management Time Slots: one time slot for downlink, one time slot for uplink, existence is configurable in *macFAmgmtTS* during setup (cf. 7.5.1.1a.3)

— Sensor Time Slots: *macFAnumSensorTS* time slots for uplink (uni-directional communication), *macFAnumRetransmitTS* time slots at the beginning are reserved for retransmissions according to the Group Acknowledgement field contained in the beacon (cf. 7.5.1.1a.4, 7.2.2a.1.2 and 7.5.7a.3).

— Actuator Time Slots: *macFAnumActuatorTS* time slots for uplink / downlink (bi-directional communication) (cf. 7.5.1.1a.5)

It is also possible to use a separate Group Acknowledgement (G_{ACK}) frame (see 7.2.2a.3.4) in order to facilitate retransmissions of the sensor transmissions within the same superframe. The use of a separate G_{ACK} is configurable during configuration mode. If the use of a separate G_{ACK} is configured, the structure of the superframe is as depicted in Figure 1.d

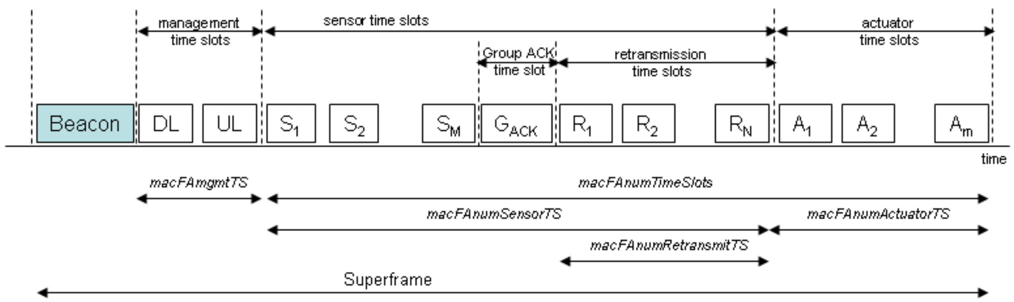


Figure 1.d—Usage and order of slots in a superframe with configured use of separate GACK

Descriptions of the configuration parameters and intervals for the superframe with a separate GACK are only different for the Sensor Time Slots:

— Beacon Time Slot

— Management Time Slots

— Sensor Time Slots: macFAnumSensorTS denotes the total number of time slots available for sensors for uplink (uni-directional) communication. Typically, one time slot is allocated to each sensor. In this case, M denotes the number of sensors. The macFAnumRetransmitTS denotes the number of time slots allocated for sensors that failed their original transmissions prior to the GACK and need to retransmit their message. N denotes the number of sensors that need to retransmit. One time slot is allocated for each retransmitting sensor.

— GACK: It contains an M-bit bitmap to indicate successful and failed sensor transmissions in the same order as the sensor transmissions (cf. 7.2.2a.3.4).

— Actuator Time Slots

In this configuration mode, no group acknowledgment field is present in the beacon frame, because it is explicitly reported in the G_{ACK} time slot.

5.5.2 Data transfer model

5.5.2.1 Data transfer to a coordinator

Insert after Figure 6 the following paragraph and figure.

When a device wishes to transfer data to a gateway in a low latency network, it first listens for the network beacon. When the beacon is found, the device synchronizes to the superframe structure. At the appropriate time, the device transmits its data frame to the gateway. If the device transmits its data frame in a dedicated time slot or as slot owner of a shared group time slot, the data frame is transmitted without using CSMA-CA. If the device transmits its data frame in a shared group timeslot and is not the slot owner, the data frame is transmitted using slotted CSMA-CA as described in 7.5.1.5, or ALOHA, as appropriate. The gateway may acknowledge the successful reception of the data by transmitting an optional acknowledgment frame. Successful data transmissions in dedicated time slots or by the slot owner are acknowledged by the gateway with a Group Acknowledgement either in the next beacon or as a separate GACK frame. This sequence is summarized in Figure 6.a.

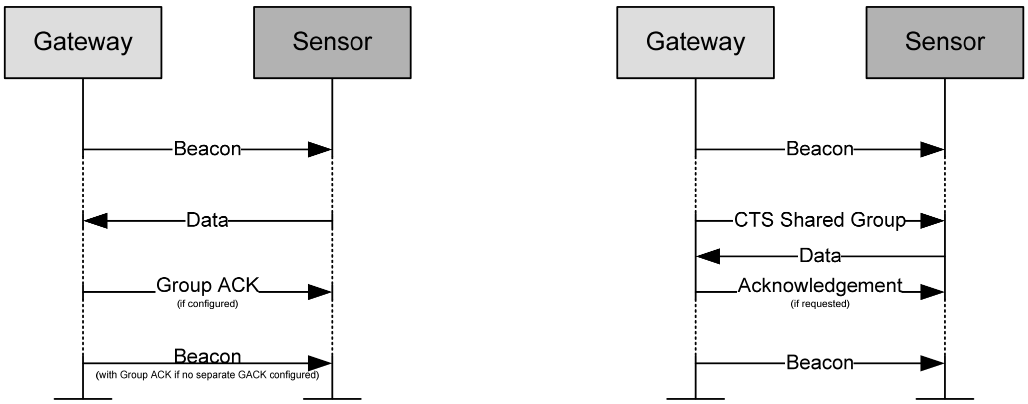


Figure 6.a—Communication to a gateway in a low latency network (left: dedicated time slot, right: shared group time slot)

5.5.2.2 Data transfer from a coordinator

Insert after Figure 8 the following paragraph and figure.

In low latency networks, a data transfer from a gateway is only possible in the macFAnumActuatorTS actuator time slots (cf. 5.5.1.2) and if the Actuator Direction subfield in the Flags field of the beacon indicates downlink direction (see 7.2.2a.1.2).

When the gateway wishes to transfer data to an actuator in a low latency network, it indicates in the network beacon that the actuator direction is downlink. At the appropriate time, the gateway transmits its data frame to the device without using CSMA-CA. The device may acknowledge the successful reception of the data by transmitting an acknowledgement frame to the gateway in the same time slot of the next superframe. In order to do so, the atuator direction has to be uplink in that superframe. This sequence is summarized in Figure 8.a.

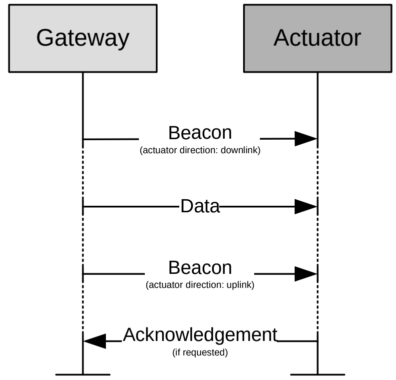


Figure 8.a—Communication from a gateway to an actuator in a low latency network

5.5.4 Improving probability of successful delivery

5.5.4.1 CSMA-CA mechanism

Insert before 5.5.4.2 the following paragraph.

Low Latency Networks use a slotted CSMA-CA channel access mechanism, where the backoff slots are aligned

— with the start of the beacon transmission in management time slots.

— with tSlotTxOwner in shared group time slots.

The backoff slots of all devices within one Low Latency Network are aligned to the gateway. Each time a device wishes to transmit data frames with CSMA-CA at the appropriate places, it locates the boundary of the next backoff slot and then waits for a random number of backoff slots. If the channel is busy, following this random backoff, the device waits for another random number of backoff slots before trying to access the channel again. If the channel is idle, the device begins transmitting on the next available backoff slot boundary. Acknowledgment and beacon frames are sent without using a CSMA-CA mechanism.

5.5.4.2 ALOHA mechanism for the UWB device

5.5.5

5.5.6

5.5.7

5.5.8

5.6 Concept of primitives

6. PHY specification

6.1

7. MAC sublayer specification

7.1 MAC sublayer service specification

7.1.1 MAC data service

7.1.1.1 MCPS-DATA.request

Insert before 7.1.1.1.1 the following sentence.

For PA, the following requirement applies in addition:

These addresses shall be specified in any of the destination addresses in DstAddr and additionalDstAddr.

7.1.1.1.1 Semantics of the service primitive

Insert after the heading of 7.1.1.1.1 the following subclause.

7.1.1.1.1.1 General

Insert before 7.1.1.1.2 the following paragraph and subclause.

The semantics of the MCPS-DATA.confirm primitive for PA shall have additional parameter numberOfAdditionalDstAddr and additionalDstAddr compared to 7.1.1.1.1.1, see 7.1.1.1.1.2.

7.1.1.1.1.2 PA-Semantics of the service primitive

The semantics of the MCPS-DATA.request primitive are as follow:

```
MCPS-DATA.request        (
          SrcAddrMode,
          DstAddrMode,
          DstPANId,
          DstAddr,
          msduLength,
          msdu,
          msduHandle,
          TxOptions,
          SecurityLevel,
          KeyIdMode,
          KeySource,
          KeyIndex,
          numberOfAdditionalDstAddr
          additionalDstAddr,
                )
```

Table 41.a specifies parameters for the MCPS-DATA.request primitive.

Table 41.a—MCPS-DATA.request parameters

Name	Type	Valid Range	Description
SrcAddrMode	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
DstAddrMode	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
DstPANId	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
DstAddr	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
msduLength	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
msdu	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
msduHandle	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
TxOptions	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
SecurityLevel	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
KeyIdMode	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
KeySource	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
KeyIndex	Table 41	Table 41	See Table 41 in IEEE802.15.4-2006.
numberOfAdditionalDstAddr	Integer	0x00-0x04	If the number of additionalDstAddr is zero, no additionalDstAddr will follow.
additionalDstAddr	List of DstAddr	0x0000-0xffff for each DstAddr	One or more alternate destination addresses. The data SPDU should be transferred to the destination specified by either DstAddr or any of destinations in additionalDstAddr.

7.1.1.1.2 When generated

Insert before 7.1.1.1.3 the following paragraph.

For PA, the following requirement applies in addition:

These addresses shall be specified in any of the destination addresses in DstAddr and additionalDstAddr.

7.1.1.1.3 Effect on receipt

Insert before 7.1.1.2 the following paragraph.

For PA, the following requirement applies in addition:

If numberOfAdditionalDstAddr is not zero and the transmission to the first transfer attempt to destAddr fails, then MAC should transfer the data SPDU to any of the alternate destinations specified in additionalDstAddr using the linkHandle provided in linkHandleList. MAC should transfer the requested data SPDU on one of these links. MAC will select a link to transmit (or retransmit if ACK is not received) in earliest possible opportunity.

7.1.1.2 MCPS-DATA.confirm

7.1.1.2.1 Semantics of the service primitive

Insert after the heading of 7.1.1.2.1 the following subclause header.

7.1.1.2.1.1 General

Insert before 7.1.1.2.2 the following paragraph and subclause.

The semantics of the MCPS-DATA.confirm primitive for PA shall have the parameter according to 7.1.1.2.1.2.

7.1.1.2.1.2 PA-Semantics of the service primitive

The PA-Semantics of the service primitive is as follows:

```
MCPS-DATA.confirm                                  (
          msduHandle,
          status,
          Timestamp,
          DstAddr,
          )
```

Table 78.a specifies parameters for the MCPS-DATA.request primitive.

Table 78.a—MCPS-DATA.confirm parameters

Name	Type	Valid Range	Description
msduHandle	Table 78	Table 78	See Table 78.
status	Table 78	Table 78	See Table 78.
Timestamp	Table 78	Table 78	See Table 78.
DstAddr	Device address	As specified by the DstAddrMode parameter of MCPS-DATA.request	Destination address to which the data SPDU was transferred.

7.1.1.2.2 When generated

7.1.1.2.3 Appropriate usage

Insert before 7.1.1.3 the following paragraph.

For PA, the following requirement applies in addition:
If the transmission attempt was successful, DstAddr is set to the address of the destination to which the data SPDU was transferred.

7.1.1.3 MCPS-DATA.indication

7.1.2 MAC management service

Insert after the heading of 7.1.2 the following subclause.

7.1.2.1 General

Insert before 0 the following subclause.

7.1.2.2 PA-MAC management service

For PA the MAC management services shown in Table 82.a are mandatory. The primitives are discussed in the subclauses referenced in the table.

Table 82.a—Summary of the primitives accessed through the MLME-SAP for PA

Name	Request	Indication	Response	Confirm
MLME-SET-SLOTFRAME	7.1.21.1.1	—	—	7.1.21.1.2
MLME-SET-LINK	7.1.21.2.1	—	—	7.1.21.2.2
MLME-TSCH-MODE	7.1.21.3.1	—	—	7.1.21.3.2
MLME-LISTEN	7.1.21.4.1	—	—	7.1.21.4.2
MLME-ADVERTISE	7.1.21.5.1	7.1.21.5.2	—	7.1.21.5.3
MLME-KEEP-ALIVE	7.1.21.6.1	—	—	7.1.21.6.2
MLME-JOIN	7.1.21.7.1	7.1.21.7.2	—	7.1.21.7.3
MLME-ACTIVATE	7.1.21.8.1	7.1.21.8.2	—	7.1.21.8.3
MLME-DISCONNECT	7.1.21.9.1	7.1.21.9.2	—	7.1.21.9.3

7.1.2.3 LL-MAC management service

Other primitives might be needed to be extended for 1-octet MHR data frames.

7.1.2.4 C-MAC management service

For the commercial (C) applications the MAC management services shown in Table 82.a are mandatory. The primitives are discussed in the subclauses referenced in the table.

Table 83.b—Summary of the primitives accessed through the MLME-SAP for PA

Name	Request	Indication	Response	Confirm
MLME-GTS	???	???	—	???
MLME-START	???	—	—	—
MCPS-DATA	???	—	—	—
MLME-BEACON-NOTIFY	—	—	—	???
MLME-EGTSinfo	???	???	—	—
MLME-LINKSTATUSPRT	???	???	—	???

7.1.3 Association primitives

LL: tbd – changes & additions to be provided

7.1.4 Disassociation primitives

LL: tbd – changes & additions to be provided

7.1.5 Beacon notification primitive

LL: tbd – changes & additions to be provided

7.1.16 Primitives for requesting data from a coordinator

7.1.17 Primitives for specifying dynamic preamble (for UWB PHYs)

7.1.20 MAC enumeration description

Insert before the heading of 7.1.20 the following subclauses.

7.1.21 PA-specific MAC sublayer service specification

7.1.21.1 MLME-SET-SLOTFRAME

7.1.21.1.1 MLME-SET-SLOTFRAME.request

7.1.21.1.1.1 General

The MLME-SET-SLOTFRAME.request primitive is used to add, delete, or change a slotframe at the MAC layer.

7.1.21.1.1.2 Semantics

The semantics of the MLME-SET-SLOTFRAME.request primitive is as follows:

```
MLME-SET-SLOTFRAME.request          (
          slotframeId,
          operation,
          size,
          channelPage,
          channelMap,
          activeFlag
                                    )
```

Table 119.a specifies parameters for the MLME-SET-SLOTFRAME.request primitive.

Table 119.a—MLME-SET-SLOTFRAME.request parameters

Name	Type	Valid Range	Description
slotframeId	Integer	0x00-0xff	Unique identifier of the slotframe.
operation	Enumeration	ADD DELETE MODIFY	Operation to perform on the slotframe.
size	Integer	0x0000-0xffff	Number of slots in the new frame.
channelPage	Integer	Selected from the available channel pages supported by the PHY (see 6.1.2)	Channel page supported by PHY.
channelMap	Bitmap	Array of bits	Indicating which frequency channels in the channel page are to be used for channel hopping. 27-bit bit field for Channel Page 0, 1, and 2
activeFlag	Enumeration	TRUE FALSE	Slotframe is active. Slotframe is not active.

7.1.21.1.1.3 When generated

An MLME-SET-SLOTFRAME.request is generated by the device management layer and issued to the MLME to create, delete, or update a slotframe on the MAC layer.

7.1.21.1.1.4 Effect on receipt

On receipt of an MLME-SET-SLOTFRAME.request, the MLME shall verify the parameters passed with the primitive. If the requested operation is ADD, the MLME shall attempt to add an entry into the macSlotframeTable. If the operation is MODIFY, it shall attempt to update an existing slotframe record in the table. If the operation is DELETE, all parameters except slotframeId and operation shall be ignored, and the slotframe record must be deleted from the macSlotFrameTable. If there are links in the slotframe that is being deleted, the links shall be deleted from the MAC layer. If the device is in the middle of using a link in the slotframe that is being updated or deleted, the update should be postponed until after the link operation completes.

7.1.21.1.2 MLME-SET-SLOTFRAME.confirm

7.1.21.1.2.1 General

The MLME-SET-SLOTFRAME.confirm primitive reports the results of the MLME-SET-SLOTFRAME.request command.

7.1.21.1.2.2 Semantics

The semantics of the MLME-SET-SLOTFRAME.confirm primitive is as follows:

```
MLME-SET-SLOTFRAME.confirm          (
          slotframeId,
          operation,
          status
                              )
```

Table 119.b specifies parameters for the MLME-SET-SLOTFRAME.confirm primitive.

Table 119.b—MLME-SET-SLOTFRAME.confirm parameters

Name	Type	Valid Range	Description
slotframeId	Integer	0x00-0xff	Unique identifier of the slotframe to be added, modified, or deleted.
operation	Enumeration	ADD DELETE MODIFY	Operation to perform on the slotframe.
status	Enumeration	SUCCESS INVALID_PARAMETER SLOTFRAME_NOT_FOUND MAX_SLOTFRAMES_EXCEEDED	Results of the MLME-SET-SLOTFRAME.request command.

7.1.21.1.2.3 When generated

The MLME-SET-SLOTFRAME.confirm primitive is generated by the MLME when the MLME-SET-SLOTFRAME.request is completed.

If any of the arguments fail a range check, the status shall be INVALID_PARAMETER. If a new slotframe is being added and the macSlotFrameTable is already full, the status shall be MAX_SLOTFRAMES_EXCEEDED. If an update or deletion is being requested and the corresponding slotframe cannot be found, the status shall be SLOTFRAME_NOT_FOUND. If an add is being requested with a slotframeID corresponding to an existing slotframe, the status shall be INVALID PARAMETER.

7.1.21.1.2.4 Effect on receipt

On receipt of a MLME-SET-SLOTFRAME.confirm primitive, the device management application is notified of the status of its corresponding MLME-SET-SLOTFRAME.request.

7.1.21.2 MLME-SET-LINK

7.1.21.2.1 MLME-SET-LINK.request

7.1.21.2.1.1 General

The MLME-SET-LINK.request primitive requests to add a new link, modify or delete an existing link at the MAC layer. The operationType parameter indicates whether the MLME-SET-LINK operation is to add or to delete a link.

7.1.21.2.1.2 Semantics

The semantics of the MLME-SET-LINK.request primitive is as follows:

```
MLME-SET-LINK.request  to add a link (
        operationType (ADD_LINK or MODIFY_LINK),
        linkHandle,
        slotframeId,
        timeslot,
        chanOffset,
        linkOptions,
        linkType,
        nodeAddr
                      )
MLME-SET-LINK.request  to delete a link (
        operationType (DELETE_LINK),
        linkHandle,
                      )
```

Table 119.c specifies parameters for the MLME-SET-LINK.request primitive with the ADD_LINK or MODIFY_LINK operationType.

Table 119.c– MLME-SET-LINK.request parameters

Name	Type	Valid Range	Description
operation	Enumeration	ADD_LINK, MODIFY_LINK, DELETE_LINK	Type of link management operation to be performed.
linkHandle	Integer	0x00–0xFF	Unique identifier (local to specified slotframe) for the link.
slotframeId	Integer	0x00-0xFF	Slotframe ID of the link to be added.
timeslot	Integer	0x0000-0xFFFF	Timeslot of the link to be added.
chanOffset	Integer	0x01-0xFF	Channel offset of the link.
linkOptions	Bitmap	b000 – b111	b001 = Transmit. b010 = Receive. b100 = Shared.
linkType	Enumeration	NORMAL ADVERTISING	Type of link. Links marked advertising are to be included in the advertisement frame generated in response to a MLME-ADVERTISE.request.
nodeAddr	Integer	0x0000-0xffff	Address list of neighbor devices connected to the link. 0xffff means the broadcasting to every node.

7.1.21.2.1.3 When generated

When operationType=ADD_LINK or MODIFY_LINK:

MLME-SET-LINK.request primitive is generated by the device management layer to add a link or to modify an existing link in a slotframe.

When operationType=DELETE_LINK:

MLME-SET-LINK.request primitive is generated by the device management layer to delete an existing link at the MAC layer.

7.1.21.2.1.4 Effect on receipt

When operationType=ADD_LINK or MODIFY_LINK:

On receipt of the MLME-SET-LINK.request, the MAC layer shall attempt to add the indicated link to the macLinkTable and add the new neighbor to its neighbor table, if needed. Upon completion, the result of the operation must be reported through the corresponding MLME-SET-LINK.confirm primitive. The use of the Shared bit in the linkOptions bitmap indicates that if the link is also a transmit link that the device must back off according to the method described in section 7.5.5. Its behavior is not defined for receive links. Resolution between the short form nodeAddr and its long form address (8 octets) may be needed for security purposes. This is determined by NHL (next higher layer).

When operationType=DELETE_LINK:

On receipt of the MLME-SET-LINK request the device shall attempt to remove the link from the macLinkTable. If the link is currently in use, the deletion shall be postponed until after the link operation completes.

7.1.21.2.2 MLME-SET-LINK.confirm

7.1.21.2.2.1 General

The SET-LINK.confirm primitive indicates the result of add, modify or delete link operation.

7.1.21.2.2.2 Semantics

The semantics of the MLME-SET-SLOTFRAME.confirm primitive is as follows:

```
MLME-SET-LINK.confirm  (
          status,
          linkHandle
                         )
```

Table 119.d specifies parameters for the MLME-SET-LINK.confirm primitive.

Table 119.d—MLME-SET-LINK.confirm parameters

Name	Type	Valid Range	Description
status	Enumeration	SUCCESS INVALID_PARAMETER UNKNOWN_SLOTFRAME MAX_LINKS_EXCEEDED MAX_NEIGHBORS_EXCEEDED	Result of the add or modify link operation.
linkHandle	Integer	0x00 – 0xFF	Unique (local to specified slotframe) identifier for the link.

7.1.21.2.2.3 When generated

The MLME-SET-LINK.confirm is generated as a result of the MLME-SET-LINK.request operation.

If any of the arguments fail a range check, the status shall be INVALID_PARAMETER. If a new slotframe is being added and the macSlotFrameTable is already full, the status shall be MAX_SLOTFRAMES_EXCEEDED. If an update or deletion is being requested and the corresponding slotframe cannot be found, the status shall be SLOTFRAME_NOT_FOUND. If an add is being requested with a slotframeID corresponding to an existing slotframe, the status shall be INVALID PARAMETER.

7.1.21.2.2.4 Effect on receipt

The layer that issued the MLME-SET-LINK.request to the MAC may process the result of the operation. The status of the primitive shall indicate SUCCESS if the operation completed successfully. Otherwise, the status indicates the cause of the failure. If the operationType=ADD_LINK of the MLME-SET_LINK.request and the linkHandle already exists, the status of the primitive shall indicate INVALID PARAMETER.

7.1.21.3 MLME-TSCH-MODE

7.1.21.3.1 MLME-TSCH-MODE.request

The MLME-TSCH-MODE.request puts the MAC into TSCH mode, or out of TSCH mode.

7.1.21.3.1.1 Semantics

The semantics of the MLME-TSCH-MODE.request primitive is as follows:

```
MLME-TSCH-MODE.request          (
        modeSwtich
        )
```

Table 119.e specifies parameters for the MLME-TSCH-MODE.request primitive.

Table 119.e—MLME-TSCH-MODE.request parameters

Name	Type	Valid Range	Description
modeSwitch	Enumeration	ON, OFF	Target mode. This mode indicates whether TSCH mode should be started or stopped.

7.1.21.3.1.2 When generated

The MLME-TSCH-MODE.request may be generated by the higher layer after the device has received advertisements from the network and is synchronized to a network (i.e. in response to an MLME-ADVERTISE.indication).

7.1.21.3.1.3 Effect on receipt

Upon receipt of the request, the MAC shall start operating its TSCH state machine using slotframes and links already contained in its database. To successfully complete this request the device must already be synchronized to a network. Once in TSCH mode, non-TSCH frames are ignored by the device until it is taken out of TSCH mode or the MAC is reset by a higher layer.

7.1.21.3.2 MLME-TSCH-MODE.confirm

The MLME-TSCH-MODE.confirm primitive reports the result of the MLME-TSCH-MODE.request primitive.

7.1.21.3.2.1 Semantics

The semantics of the MLME-TSCH-MODE.confirm primitive is as follows:

```
MLME-TSCH-MODE.confirm          (
    modeSwitch,
    status
```

)

Table 119.f specifies parameters for the MLME-TSCH-MODE.confirm primitive.

Table 119.f—MLME-TSCH-MODE.confirm parameters

Name	Type	Valid Range	Description
modeSwitch	Enumeration	ON, OFF	Target mode. This mode indicates whether this confirmation is due to TSCH mode ON request or OFF request.
status	Enumeration	SUCCESS NO_SYNC	

7.1.21.3.2.2 When generated

The MLME-TSCH-MODE.confirm is generated by the MAC layer to indicate completion of the corresponding request. If the corresponding request was to turn on the TSCH-MODE, but the MAC layer has not been synchronized to a network, the status shall be NO_SYNC. Otherwise, the status shall be SUCCESS.

If the corresponding request was to turn off the TSCH-MODE, the status shall be SUCCESS, and the MAC layer will stop the TSCH-MODE operation.

7.1.21.3.2.3 Effect on receipt

The higher layer may use the confirmation to process the result of MLME-TSCH-MODE.request.

7.1.21.4 MLME-LISTEN

7.1.21.4.1 MLME-LISTEN.request

7.1.21.4.1.1 Semantics

The semantics of the MLME-LISTEN.request primitive is as follows:

```
MLME-LISTEN.request     (
          time,
          numPageChannel,
          pageChannels[]
                        )
```

Table 119.g specifies parameters for the MLME-LISTEN.request primitive.

Table 119.g—MLME-LISTEN.request parameters

Name	Type	Valid Range	Description
onTime	Integer	0x0000 – 0xFFFF	The amount of time (10–millisecond units) to stay on each channel. 0x0000 indicates that the MAC stops listening
offTime	Integer	0x0000 – 0xFFFF	The amount of time (10–millisecond units) to wait between channel changes.
numPageChannel	Integer	0x01-0xFF	The number of page channel descriptors in the page channels array.
pageChannelsDes[]	Table 119.h	Table 119.h	Array of page channel descriptor. See Table 119.h for the format of page channel descriptor.

Table 119.h—MLME-LISTEN.request pageChannelDesc parameters

Name	Type	Valid Range	Description
channelPageId	Integer	Selected from the available channel pages supported by the PHY (see 6.1.2)	Channel page ID.
numChannel	Integer	0x01-0xFF	The number of channels in this channel page to be included in listening.
Channels[]	Array of Channel	Table 2.	The array of channels on which to listen. See Table 2 for the valid range of channels in each channel page.

7.1.21.4.1.2 When generated

The MLME-LISTEN.request shall be generated by the next higher layer to initiate the search for a TSCH network.

7.1.21.4.1.3 Effect on receipt

Upon receipt of the request the MAC layer shall activate the radio on the indicated channel and wait for an Advertisement command. The MAC shall listen on Channel[0] for onTime, inactivate the radio for offTime, then repeat with Channels[1], etc. After listening to the last channel in Channels[], the MAC returns to Channel[0]. Valid Advertisement command frames received in this state shall result in the generation of MLME-ADVERTISE.indication. All other frames shall be dropped. The MAC shall stay in the listening state until it receives a MLML-LISTEN.request with an onTime of 0x0000, or a MLME-TSCH-MODE.request is received. The higher layer selects the advertiser and the network before setting the slotframe, link(s), and TSCH mode. Advertisements will continue to be received, and passed on to the higher layer until leaving the listen state.

7.1.21.4.2 MLME-LISTEN.confirm

7.1.21.4.2.1 Semantics

The semantics of the MLME-LISTEN.confirm primitive is as follows:

```
MLME-LISTEN.confirm     (
```

```
        status
                    )
```

Table 119.i specifies parameters for the MLME-LISTEN.confirm primitive.

Table 119.i—MLME-LISTEN.confirm parameters

Name	Type	Valid Range	Description
status	Enumeration	SUCCESS INVALID_PARAMETER	

7.1.21.4.2.2 When generated

The MAC layer shall generate MLME-LISTEN.confirm when it completes the listen operation started by MLME-LISTEN.request.

7.1.21.4.2.3 Effect on receipt

On receipt of the primitive, the higher layer may continue with its joining state machine.

7.1.21.5 MLME-ADVERTISE

7.1.21.5.1 MLME-ADVERTISE.request

7.1.21.5.1.1 Semantics

The semantics of the MLME-ADVERTISE.request primitive is as follows:

```
MLME-ADVERTISE.request          (
        advertiseInterval,
        channelPage,
        channelMap,
        hoppingSequenceId,
        timeslotTemplateId,
        securityLevel,
        joinPriority,
        numSlotframe,
        slotframes[]
                    )
```

Table 119.j specifies parameters for the MLME-ADVERTISE.request primitive.

Table 119.j—MLME-ADVERTISE.request parameters

Name	Type	Valid Range	Description
advertiseInterval	Integer	0x0000 – 0xFFFF	Interval specifying the transmission of the Advertisement command (in 10 ms units)
channelPage	Integer	Selected from the available channel pages supported by the PHY (see 6.1.2)	Channel page supported by PHY.
channelMap	Bitmap	Array of bits	Map of channels to be included in the Advertisement command.
hoppingSequenceId	Integer	0x0 – 0xF	ID of hopping sequence used.
timeslotTemplateId	Integer	0x0 – 0xF	ID of timeslot template used.
securityLevel	Enumeration	Table 95	Security level in the Advertisement command. See Table 95 in IEEE802.15.4-2006.
joinPriority	Integer	0x00 – 0xFF	Join priority to be indicated in the Advertisement command.
numSlotframe	Integer	0x0 – 0xF	Number of slotframes to be indicated in the Advertisement command.
Slotframes[]	See Table 119.k	See Table 119.k	See Table 119.k.

Table 119.k—MLME-ADVERTISE.request Slotframe parameters (per slotframe)

Name	Type	Valid Range	Description
slotframeId	Integer	0x00 – 0xFF	Slotframe ID.

7.1.21.5.1.2 When generated

The next higher layer requests the MAC layer to start sending Advertisement command frames using MLME-ADVERTISE.request so that new nodes can find the network and this device.

7.1.21.5.1.3 Effect on receipt

Upon receipt of the request the MAC layer shall send the Advertisement command frame on the first available TX link. Whenever the time specified in AdvertiseInterval lapses from the previous transmission of Advertisement command frame, the MAC layer shall repeat the Advertisement command frame on next TX link available. The remaining parameters specify the slotframes to be included in the Advertisement command frames. Links in the specified slotframes with an Advertising linkType are to be included in the Advertisement command.

7.1.21.5.2 ADVERTISE.indication

The MLME-ADVERTISE.indication indicates that a device received an Advertisement command frame.

7.1.21.5.2.1 Semantics

The semantics of the MLME-ADVERTISE.indication primitive is as follows:

```
MLME-ADVERTISE.indication          (
        PANId,
        timingInformation,
        channelPage,
        channelMap,
        hoppingSequenceId,
        timeslotTemplateId,
        securityLevel,
        joinPriority,
        linkQuality,
        numSlotframes,
        slotframes[]
                                   )
```

Table 119.l specifies parameters for the MLME-ADVERTISE.indication primitive.

Table 119.l—MLME-ADVERTISE.indication parameters

Name	Type	Valid Range	Description
PANId	Integer	0x0000 – 0xFFFF	The PAN identifier indicated in the Advertisement command.
timingInformation			The time information (absolute slot number) of the timeslot in which the Advertisement command was received.
channelPage	Integer	Selected from the available channel pages supported by the PHY (see 6.1.2)	Channel page.
channelMap	Bitmap	Array of bits	Bit map of channels.
hoppingSequenceId	Integer	0x0 – 0xF	ID of hopping sequence used.
timeslotTemplateId	Integer	0x0 – 0xF	ID of timeslot template used.
securityLevel	Enumeration	Table 95	Security level in advertisement packet See Table 95 in IEEE802.15.4-2006.
joinPriority	Integer	0x00 – 0xFF	Join priority indicated in advertisement.
linkQuality	Integer	0x00 – 0xFF	Link quality indicated in the frame by the PHY layer.
numSlotframes	Integer	0x0 – 0xF	Number of slotframes indicated in the Advertisement command received.
slotframes[]	See Table 119.k	See Table 119.k	See Table 119.k

7.1.21.5.2.2 When generated

The MLME-ADVERTISE.indication shall be generated when an Advertisement command frame has been received by the device. Upon receiving a valid Advertisement command, the device shall be synchronized to the network and ready to enable the TSCH-MODE if requested by the higher layer.

7.1.21.5.2.3 Effect on receipt

The higher layer may wait and record more than one advertisement and then select the desired advertising device before configuring the superframe(s) and link(s) and before enabling TSCH-MODE. After joining a TSCH network, the high layer uses the indication to collect the list of neighbors and information about neighbors.

7.1.21.5.3 MLME-ADVERTISE.confirm

7.1.21.5.3.1 Semantics

The semantics of the MLME-ADVERTISE.confirm primitive is as follows:

```
MLME-ADVERTISE.confirm          (
        status
                                )
```

Table 119.m specifies parameters for the MLME-ADVERTISE.confirm primitive.

Table 119.m—MLME-ADVERTISE.confirm parameters

Name	Type	Valid Range	Description
Status	Enumeration	SUCCESS INVALID_PARAMETER	

7.1.21.5.3.2 When generated

The MAC layer shall generate MLME-ADVERTISE.confirm when it starts sending the Advertisement command.

7.1.21.5.3.3 Effect on receipt

On receipt of the primitive, the higher layer may expect that it will receive the Join command on any of the links provided in the Advertisement command.

7.1.21.6 MLME-KEEP-ALIVE

7.1.21.6.1 MLME-KEEP-ALIVE.request

7.1.21.6.1.1 Semantics

The semantics of the MLME-KEEP-ALIVE.request primitive is as follows:

```
MLME-KEEP-ALIVE.request         (
        dstAddr,
        linkHandle,
```

period

)

Table 119.n specifies parameters for the MLME-KEEP-ALIVE.request primitive.

Table 119.n—MLME-KEEP-ALIVE.request parameters

Name	Type	Valid Range	Description
dstAddr	Integer	0x0000 - 0xFFFF	Address of neighbor device to maintain the timing. Keepalives with dstAddr of 0xFFFF do not not expect to be acknowledged.
period	Integer	0x0001 – 0xFFFF	Duration of quiet time in seconds that a Keep-Alive command frame should be sent if no traffic is present.

7.1.21.6.1.2 When generated

7.1.21.6.1.3 Effect on receipt

Upon receipt of the request, the MAC layer shall monitor the frame sent to the destination node specified in the dstAddr parameter. If no frame is sent to the destination node for any duration defined by the period parameter, the MAC shall send an empty (no MAC payload) frame to the node dstAddr. The Sequence Number subfield of the MHR of the frame shall be set to the least significant byte of the absolute slot number. Resolution between the short form dstAddr and its long form address (8 octets) may be needed for security purposes. This is determined by NHL (next higher layer).

7.1.21.6.2 MLME-KEEP-ALIVE.confirm

7.1.21.6.2.1 Semantics

The semantics of the MLME-KEEP-ALIVE.confirm primitive is as follows:

```
MLME-KEEP-ALIVE.confirm          (
          status
               )
```

Table 119.o specifies parameters for the MLME-KEEP-ALIVE.confirm primitive.

Table 119.o—MLME-KEEP-ALIVE.confirm parameters

Name	Type	Valid Range	Description
Status	Enumeration	SUCCESS INVALID_PARAMETER	

7.1.21.6.2.2 When generated

The MAC layer shall generate MLME-KEEP-ALIVE.confirm to acknowledge that it received MLME-KEEP-ALIVE request.

7.1.21.6.2.3 Effect on receipt

Non.

7.1.21.7 MLME-JOIN

7.1.21.7.1 MLME-JOIN.request

7.1.21.7.1.1 Semantics

The semantics of the MLME-JOIN.request primitive is as follows:

```
MLME-JOIN.request        (
          dstAddr,
          securityInformation,
          numNeighbors,
          neighbors[]
                         )
```

Table 119.p specifies parameters for the MLME-JOIN.request primitive.

Table 119.p—MLME-JOIN.request parameters

Name	Type	Valid Range	Description
dstAddr	Integer	0x0000 - 0xFFFF	Address of neighbor device to send Join command
securityInformation	Table 119.q	Table 119.q	See Table 119.q for the detail.
numNeighbors	Integer	0x0 – 0xF	Number of neighbors found by the joining device.
neighbors	Table 119.r	Table 119.r	Neighbor information for the number of neighbors specified in numNeighbors. See Table 119.r for the definition of a neighbor.

Table 119.q—MLME-JOIN.request securityInformation parameters

Name	Type	Valid Range	Description
TBD	TBD	TBD	The securityInformation definition will be defined with Security sub-group.

Table 119.r—MLME-JOIN.request neighbors parameters

Name	Type	Valid Range	Description
neighborId	Integer	0x0000 – 0xFFFF	16 bit address of neighbor.
RSSI	Integer	-128 to 127	Received signal strength (in dBm) of frames received from the neighbor.

7.1.21.7.1.2 When generated

Device management of a new device (or device who lost connection with the TSCH network) will invoke this service primitive to join the TSCH network.

7.1.21.7.1.3 Effect on receipt

Upon receipt of the request, the MAC layer shall send either a Join command frame or data frame containing a higher layer management packet requesting to join the network, using any link to the dstAddr. The content of the Join command frame will be formatted using the other parameters and the format of Join command frame is specified in 7.3.12. If a data frame with the higher layer management packet is used instead of a Join command frame, the content of the higher layer payload of the data frame containing the request to join the network is constructed using the other parameters. The explicit format of the higher layer payload is out of scope of this document. Resolution between the short form dstAddr and its long form address (8 octets) may be needed for security purposes. This is determined by NHL (next higher layer).

7.1.21.7.2 MLME-JOIN.indication

7.1.21.7.2.1 Semantics

The semantics of the MLME-JOIN.indication primitive is as follows:

```
MLME-JOIN.indication      (
          linkHandle,
          newNodeAddr,
          securityInformation,
          numNeighbors,
          neighbors[]
               )
```

Table 119.s specifies parameters for the MLME-JOIN.indication primitive.

Table 119.s—MLME-JOIN.indication parameters

Name	Type	Valid Range	Description
linkHandle	Integer	0x00 – 0xFF	Unique identifier for the link that Join command frame is received on.
newNodeAddr	array of octets	64-bit binary string	64-bit long address of new device sending the Join command.
securityInformation	Table 77-Q	Table 77-Q	See Table 77-Q.
numNeighbors	Integer	0x0 – 0xF	Number of neighbors reported by the joining device.
Neighbors	Table 119.r	Table 119.r	Neighbor information for the number of neighbors specified in numNeighbors. See Table 119.r for the definition of a neighbor in neighbors.

7.1.21.7.2.2 When generated

MLME-JOIN.indication indicates the Device Management layer that the MAC layer has received a Join command frame from a new device attempting to join the TSCH network.

7.1.21.7.2.3 Effect on receipt

Upon receipt of the MLME-JOIN.indication, the Device Management layer shall invoke the device management procedure to transfer the join attempt of the new device to the Device Manager.

7.1.21.7.3 MLME-JOIN.confirm

7.1.21.7.3.1 Semantics

The semantics of the MLME-JOIN.confirm primitive is as follows:

```
MLME-JOIN.confirm          (
          status
                           )
```

Table 119.t specifies parameters for the MLME-JOIN.confirm primitive.

Table 119.t—MLME-JOIN.confirm parameters

Name	Type	Valid Range	Description
Status	Enumeration	SUCCESS INVALID_PARAMETER	

7.1.21.7.3.2 When generated

The MAC layer shall generate MLME-JOIN.confirm to acknowledge that it received the MLME-JOIN.request primitive.

7.1.21.7.3.3 Effect on receipt

Non

7.1.21.8 MLME-ACTIVATE

7.1.21.8.1 MLME-ACTIVATE.request

7.1.21.8.1.1 Semantics

The semantics of the MLME-ACTIVATE.request primitive is as follows:

```
MLME-ACTIVATE.request (
        dstAddr,
        securityInformation,
        slotframes[]
            )
```

Table 119.u and Table 119.w specify parameters for the MLME-ACTIVATE.request primitive.

Table 119.u—MLME-ACTIVATE.request parameters

Name	Type	Valid Range	Description
dstAddr	Integer	0x0000 - 0xFFFF	Address of neighbor device to send Activate command.
securityInformation	Table 119.v	Table 119.v	See Table 119.v for details.
slotframes[]	Table 119.k	Table 119.k	See Table 119.k.

Table 119.v—MLME-ACTIVATE.request securityInformation parameters

Name	Type	Valid Range	Description
TBD	TBD	TBD	The securityInformation definition will be defined with the Security sub-group.

Table 119.w—MLME-ACTIVATE.request slotframe parameters (per slotframe)

Name	Type	Valid Range	Description
slotframeId	Integer	0x00 – 0xFF	Slotframe ID.
slotframeSize	Integer	0x00 – 0xFFFF	Slotframe size.
numLink	Integer	0x0 – 0xF	Number of links for the specified slotframe to be indicated in the Advertisement command.
links	Table 119.x	Table 119.x	See Table 119.x for parameters (per link)

Table 119.x—MLME-ACTIVATE.request Link parameters (per link)

Name	Type	Valid Range	Description
timeslot	Integer	0x0000 – 0xFFFF	Timeslot.
chanOffset	Integer	0x00 – 0xFF	Channel offset.
linkOption	Enumeration	TX RX SHARED_TX	Option of the link.

7.1.21.8.1.2 When generated

An Activate command is generated by a higher layer in response to a Join command or a Join data frame.

7.1.21.8.1.3 Effect on receipt

Upon receipt of the request, the MAC layer shall send either the Activate command frame to activate the new joining device, or a data frame containing a higher layer management packet to activate the new joining device. The MAC shall send the Activate command frame to the node using the linkHandle parameter. The content of the Activate command is formatted using the other parameters. If a data frame with a higher layer management packet is used instead of Activate command frame, the content of the higher layer payload to activate the network is constructed using the other parameters. The explicit format of the higher layer payload is out of scope of this document. Resolution between the short form dstAddr and its long form address (8 octets) may be needed for security purposes. This is determined by NHL (next higher layer).

7.1.21.8.2 MLME-ACTIVATE.indication

7.1.21.8.2.1 Semantics

The semantics of the MLME-ACTIVATE.indication primitive is as follows:

```
MLME-ACTIVATE.indication          (
          srcAddr,
          securityInformation,
               )
```

Table 119.y specifies parameters for the MLME-ACTIVATE.indication primitive.

Table 119.y—MLME-ACTIVATE.indication parameters

Name	Type	Valid Range	Description
srcAddr	Integer	0x0000 - 0xFFFF	Address of neighbor from whom the Activate command was received.
securityInformation	Table 77-V	Table 77-V	See Table 77-V.

7.1.21.8.2.2 When generated

MLME-ACTIVATE.indication indicates the device management layer that the MAC layer has received an Activate command frame from the neighbor indentified in srcAddr.

7.1.21.8.2.3 Effect on receipt

Upon receipt of the MLME-ACTIVATE.indication, the device management layer shall process the securityInformation received to set up secure connections. Resolution between the short form srcAddr and its long form address (8 octets) may be needed for security purposes. This is determined by NHL (next higher layer).

7.1.21.8.3 MLME-ACTIVATE.confirm

7.1.21.8.3.1 Semantics

The semantics of the MLME-ACTIVATE.confirm primitive is as follows:

```
MLME-ACTIVATE.confirm (
          status
                )
```

Table 119.z specifies parameters for the MLME-ACTIVATE.confirm primitive.

Table 119.z—MLME-ACTIVATE.confirm parameters

Name	Type	Valid Range	Description
Status	Enumeration	SUCCESS INVALID_PARAMETER	

7.1.21.8.3.2 When generated

The MAC layer shall generate MLME-ACTIVATE.confirm to acknowledge that it received MLME-ACTIVATE.request.

7.1.21.8.3.3 Effect on receipt

7.1.21.9 MLME-DISCONNECT

7.1.21.9.1 MLME-DISCONNECT.request

7.1.21.9.1.1 Semantics

The semantics of the MLME-DISCONNECT.request primitive is as follows:

```
MLME-DISCONNECT.request          (
```

)

7.1.21.9.1.2 When generated

MLME-DISCONNECT.request primitive is used to initiate the graceful disconnection from TSCH network.

7.1.21.9.1.3 Effect on receipt

Upon receipt of the request, the MAC layer shall send a disassociation notification command frame or a data frame containing a higher layer management packet to indicate that it is about to leave the TSCH network on all unicast transmit links. The Sequence Number subfield of the MHR of the frame shall be set to the least significant byte of the absolute slot number.

After the MAC sends the disassociation notification command frame for *macDisconnectTime*, it shall release all slotframe and link resources.

7.1.21.9.2 MLME-DISCONNECT.indication

7.1.21.9.2.1 Semantics

The semantics of the MLME-DISCONNECT.indication primitive is as follows:

```
MLME-DISCONNECT.indication          (
        srcAddress,
             )
```

Table 119.aa specifies parameters for the MLME-DISCONNECT.indication primitive.

Table 119.aa—MLME-DISCONNECT.indication parameters

Name	Type	Valid Range	Description
srcAddr	Integer	0x0000 – 0xFFFF	16-bit short address of the neighbor node from which the DISCONNECT command frame was received.

7.1.21.9.2.2 When generated

MLME-DISCONNECT.indication indicates to the device management layer that the MAC layer has received a Disconnect command frame from a neighbor node, the address of which is indicated by srcAddress.

7.1.21.9.2.3 Effect on receipt

Upon receipt of the MLME-DISCONNECT.indication, the device management layer shall process the disconnection of the neighbor from which the Disconnect command frame is received. Resolution between the short form srcAddr and its long form address (8 octets) may be needed for security purposes. This is determined by NHL (next higher layer).

7.1.21.9.3 MLME-DISCONNECT.confirm

7.1.21.9.3.1 Semantics

The semantics of the MLME-DISCONNECT.confirm primitive is as follows:

```
MLME-DISCONNECT.confirm          (
          status
          )
```

Table 119.bb specifies parameters for the MLME-DISCONNECT.confirm primitive.

Table 119.bb—MLME-DISCONNECT.confirm parameters

Name	Type	Valid Range	Description
Status	Enumeration	SUCCESS	

7.1.21.9.3.2 When generated

The MAC layer shall generate MLME-DISCONNECT.confirm to acknowledge that it received MLME-DISCONNECT request.

7.1.21.9.3.3 Effect on receipt

None.

7.1.22 LL-specific MAC sublayer service specification

(tbd) Subclauses without text will be filled up later on.

7.1.22.1 Primitives for Superframe Configuration of low latency networks

7.1.22.1.1 General

These primitives control the different modes for the configuration and operation of the superframe in a low latency network.

7.1.22.1.2 MLME-SFCF.discovery

7.1.22.1.2.1 General

This primitive switches the sFCF network into discover mode.

7.1.22.1.2.2 Semantics of the Service Primitive

The semantics of the MLME-SFCF.discovery primitive is as follows:

```
MLME-SFCF.discovery (
        …
            )
```

Table eXX specifies the parameters for the MLME-SFCF.discovery primitive.

7.1.22.1.2.3 When generated

7.1.22.1.2.4 Appropriate usage

7.1.22.1.3 MLME-SFCF.discovery_confirm

7.1.22.1.3.1 General

This primitive indicates the end of the discover mode and gives the status of the discover mode to the next higher layer.

7.1.22.1.3.2 Semantics of the Service Primitive

The semantics of the MLME-SFCF.discovery_confirm primitive is as follows:

```
MLME-SFCF.discovery_confirm (
        …
            )
```

Table eXX specifies the parameters for the MLME-SFCF.discovery_confirm primitive.

7.1.22.1.3.3 When generated

7.1.22.1.3.4 Appropriate usage

7.1.22.1.4 MLME-SFCF.configuration

7.1.22.1.4.1 General

This primitive switches the sFCF network into configuration mode.

7.1.22.1.4.2 Semantics of the Service Primitive

The semantics of the MLME-SFCF.configuration primitive is as follows:

```
MLME-SFCF.configuration (
        ...
            )
```

Table eXX specifies the parameters for the MLME-SFCF.configuration primitive.

7.1.22.1.4.3 When generated

7.1.22.1.4.4 Appropriate usage

7.1.22.1.5 MLME-SFCF.configuration_confirm

7.1.22.1.5.1 General

This primitive indiciates the end of the configuration mode and gives the status of the configuration mode to the next higher layer.

7.1.22.1.5.2 Semantics of the Service Primitive

The semantics of the MLME-SFCF.configuration_confirm primitive is as follows:

```
MLME-SFCF.configuration_confirm (
        ...
            )
```

Table eXX specifies the parameters for the MLME-SFCF.configuration_confirm primitive.

7.1.22.1.5.3 When generated

7.1.22.1.5.4 Appropriate usage

7.1.22.1.6 MLME-SFCF.online

7.1.22.1.6.1 General

This primitive switches the sFCF network into online mode.

7.1.22.1.6.2 Semantics of the Service Primitive

The semantics of the MLME-SFCF.online primitive is as follows:

```
MLME-SFCF.online (
        …
            )
```

Table eXX specifies the parameters for the MLME-SFCF.online primitive.

7.1.22.1.6.3 When generated

7.1.22.1.6.4 Appropriate usage

7.1.22.1.7 MLME-SFCF.online_indication

7.1.22.1.7.1 General

This primitive indicates any problems during the online mode to the next higher layer.

7.1.22.1.7.2 Semantics of the Service Primitive

The semantics of the MLME-SFCF.online_indication primitive is as follows:

```
MLME-SFCF.online_indication (
        …
            )
```

Table eXX specifies the parameters for the MLME-SFCF.online_indication primitive.

7.1.22.1.7.3 When generated

7.1.22.1.7.4 Appropriate usage

7.1.23 C-specific MAC sublayer service specification

7.2 MAC frame formats

7.2.1 General MAC frame format

Change the first paragraph 7.2.1.

The MAC frame format is composed of a MHR, a MAC payload, and a MFR. The fields of the MHR appear in a fixed order; however, the addressing fields may not be included in all frames. Furthermore, some frame types use a MHR of only 1 octet length with a shortened Frame Control field. The general MAC frame shall be formatted as illustrated in Figure 79.

7.2.1.1 Frame Control field

7.2.1.1.1 Frame Type subfield

Change Table 120.

Frame type value b2 b1 b0	Description
000	Beacon
001	Data
010	Acknowledgment
011	MAC command
100	MHR of 1 octet
101~~0~~-111	Reserved

7.2.2 Format of individual frame types

7.2.2.1 Beacon frame format

7.2.3 Frame compatibility

Insert before 7.3 the following subclause.

The contribution from TSCH named "7.2 New Frame Formats" is not correct related neither to IEEE 802.15.4-2006 nor to IEEE 802.15.4-2009 and have a lot of problems:

- The Table and Figure numbers are not related.

- The first sentence is an editor note and not a std paragraph.

- Figure 85 shall be a PPT or WORD editable figure.

- Table 109 is not similar to IEEE 802.15.4 MHR representations. It should be according to Figure 92 or so.

- Table 110 is unclear.

7.2.4 PA-Frame Formats

Secure Extended ACKs with payload is to be jointly defined with Security subgroup. ACK/NACK frame in Figure 93.a is authenticate only/no payload and should be a subset of the Extended ACK definition.

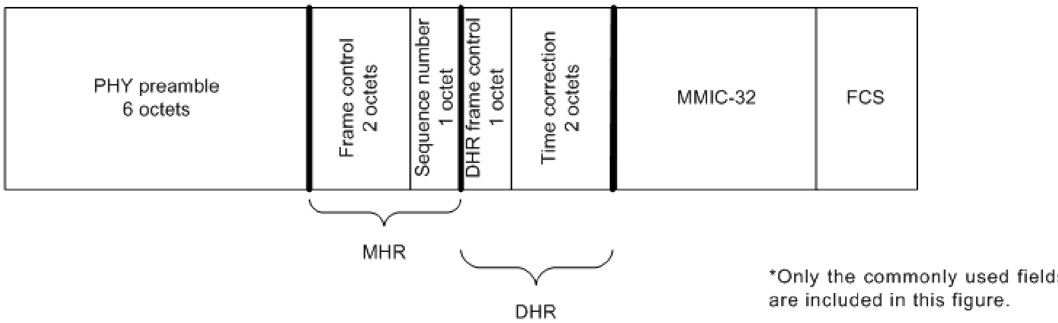


Figure 93.a—Typical acknowledgement frame layout

The source address of an ACK/NACK is the address of the device that transmits the ACK/NACK. The destination address is the address of the intended recipient of the ACK/NACK.

Every ACK/NACK frame shall be authenticated with a MMIC, but not encrypted. Some fields are virtual, used in creating the MMIC but not actually transmitted.

The format of an IEEE Std 802.15.4:2006 MHR is summarized in Figure 93.b.

octets	bits							
	7	6	5	6	3	2	1	0
1	Frame control (octet 0)							
2	Frame control (octet 1)							
3	Sequence number							

Figure 93.b—Acknowledgement frame MHR

As shown in table 109, attributes include:

- Frame control attributes for ACK/NACKs, as follows:
  - — Frame type shall be data.
  - — Security shall be disabled, as it is handled in the DHR.
  - — Frame pending shall be false.
  - — Ack.Request shall be false (IEEE Std 802.15.4 does not recognize this as an ACK).
  - — Source addressing mode shall be 0x00 (i.e., implicit), except for cases described below where the source address and PAN ID are included in the MHR.
  - — Destination addressing mode shall be 0x00 (i.e., implicit).
  - — Frame version shall be 0x~~01~~ 0x10.
- Sequence number shall be incremented after each use as described in 7.3.

The acknowledgers EUI-64 shall be included in the source address field of the ACK/NACKs MHR if so requested in the received DPDU's DHDR. Normally, the 16-bit DL source address of the ACK/NACK is not transmitted, because it matches the destination address of the received DPDU. However, in duocast or n-cast acknowledgements, one or more acknowledgements may be sent by different devices. Therefore, in cases where the acknowledger's address is different from the destination address of the received DPDU, the acknowledgement shall also include the acknowledger's 16-bit DL source address in the MHR, with the assumption that the acknowledger's EUI-64 is already known by the recipient of the acknowledgement.

All correspondent devices must be operating within the same security context or they will not possess appropriate information to authenticate the frame.

A prototype DHR following a MHR is summarized in Figure 93.c.

octets	**bits**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
1 octet	DHR ACK/NACK Frame control							
4 octets (virtual)	Echoed MMIC of received DPDU							
0-2 octets	Time correction (LSB) When requested							
0-1 octets	Timeslot offset When needed							
0-4 octets	DAUX sub-header Usually absent							

Figure 93.c—Acknowledgement frame MHR

As shown in table 110, attributes include:

- The DHR ACK/NACK frame control octet is described in table 111
- Echoed MMIC of received DPDU. For a discussion of handling of this virtual field, see 7.3.4. To unambiguously connect the ACK/NACK with the DPDU, the MMIC of the DPDU is included in the ACK/NACK's DHR as a virtual field, with octet ordering matching the DPDUs MMIC. This virtual field is used to calculate the ACK/NACK's MMIC, but not transmitted. If the received MMIC is longer than 4 octets, only the final 4 octets of the MMIC are echoed as a virtual field.
- Time correction (LSB). Used by DL clock sources to correct the time of the DL clock recipient, if it is requested in the received DPDU's DHDR. This 2-octet value, when included in the ACK/NACK, echoes the time that the DPDU was received. The value, in 2-20 s (approximately 0.954 µs), reports an offset from the scheduled start time of the current timeslot in the acknowledger's time base. The reported value is based on DPDU's start time. See.9.1.9.3.2
- Acknowledger's timeslot offset is provided, when needed, within a slow hopping period. This one-octet value, when included in the NACK/ACK, indicates the current timeslot in the acknowledger's time base. It shall be included only when the received DPDU is received in a different slow hopping timeslot than is used for the acknowledgement. The first timeslot in a slow hopping period has an offset of zero. When the corrected timeslot offset is nonzero, the time correction (previous field), when included, shall be an offset of the corrected scheduled timeslot time, Security requires that a device's time increases from timeslot to timeslot. Therefore, if the timeslot is corrected to an earlier timeslot by a clock recipient, there shall be an interruption in service, equal to the magnitude of the timeslot correction plus at least one timeslot. See 9.1.9.4.9
- Auxiliary sub-header (DAUX). DAUX may be included in an ACK/NACK, for the limited purpose of echoing received signal quality (see).9.3.5.5

In an ACK/NACK DPDU, the DHR frame control octet communicates the ACK/NACK selections, as shown in Figure 93.d.

octets	bits							
	7	6	5	4	3	2	1	0
1	Include clock correction 0= no 1= yes	Include slow-hopping timeslot offset 0= no 1= yes	ACK/NACK type 0= ACK 1=ACK/ECN 2= NACK0 3=NACK1		Auxiliary sub-header 0= no DAUX 1= DAUX included	MMIC alternative (LSB) 0= reserved 1= MMIC-32 2= MMIC-64 3= reserved		Reserved =0

Figure 93.d—DHR ACK/NACK frame control

The DL protocol version number and MAC security key always match the received DPDU, and therefore are not indicated in the ACK/NACK.

Bit content is as follows:

- Bit 7 shall indicate whether the ACK/NACK includes clock correction information.
- Bit 6 shall indicate whether the ACK/NACK includes a slow hopping offset.
- Bits 5 and 4 shall indicate whether the PDU is an ACK or a NACK, as follows:
  - — 00 is an acknowledgement.
  - — 01 is an acknowledgement with an explicit congestion notification (ECN). See. A router that is signaling ECN bits in the forward direction should also signal the ECN through DL acknowledgements, if the priority of the DPDU is 7 or less. A device receiving an ECN through a DL acknowledgement may treat this signal as early notification that it is likely to receive an ECN at upper layers.
  - — 02 is a NACK0, signaling that the DPDU was received but could not be acknowledged due to message queue congestion. See.9.1.9.4.4
  - — 03 is a NACK1, signaling that the DPDU was received but was not accepted due to recent history of forwarding problems along the route. See .9.1.9.4.4
- Bit 3 shall indicate whether the ACK/NACK includes a DAUX sub-header. DAUX may be included in an ACK/NACK for the limited purpose of reporting received signal quality.
- Bits 2 and 1 shall indicate the MMIC alternative.
- Bit 0 is reserved and shall be set to 0.

7.2.5 LL-Frame Formats

7.2.5.1 General MAC Frame Format with MHR of 1 octet

7.2.5.1.1 General

This subclause describes the general MAC frame format that is used within a low latency network. A new frame type is defined in Table X1. All other conformant frames can be also sent as long as they fit into the available time slot.

The general structure of frame with a shortened frame control (MHR of 1 octet) is shown in Figure 93.e.

Octets: 1	variable	2
Shortend Frame Control	Frame Payload	FCS
MHR	MAC Payload	MFR

Figure 93.e—General MAC frame format with shortened frame control field

The MAC frame does have a very short MAC header (MHR) of one octet containing the Shortened Frame Control with the frame type, followed by the MAC payload and the MAC footer (MFR).

7.2.5.1.2 Shortened Frame Control field

7.2.5.1.2.1 General

The Shortened Frame Control field is 1 octet in length and contains information defining the frame type. The Shortened Frame Control Field shall be formatted as illustrated in Figure 93.f.

Bits: 0-2	3	4	5	6-7
Frame Type	Security Enabled	Frame Version	ACK Request	Sub Frame Type

Figure 93.f—Format of the Shortened Frame Control field

7.2.5.1.2.2 Frame Type subfield

The Frame Type subfield is 3 bits in length and shall be set to b100 indicating this type of shortened MAC frame.

The Frame Type subfield corresponds to the Frame Type subfield of the general MAC frame format in 7.2.1. in meaning and position. The new type b100 allows efficient recognition of frames with a Shortened Frame Control field, but allows the usage of all other MAC frames within the superframe structure associated with this frame type.

7.2.5.1.2.3 Security Enabled subfield

The Security Enabled subfield is 1 bit in length, and it shall be set to one if the frame is protected by the MAC sublayer and shall be set to zero otherwise. The Auxiliary Security Header field of the MHR shall be present only if the Security Enabled subfield is set to one.

7.2.5.1.2.4 Frame Version subfield

The Frame Version subfield is 1 bit in length and specifies the version number corresponding to the frame. This subfield shall be set to 0 to indicate a frame compatible with IEEE Std 802.15.4-2006 and newer additions. All other subfield values shall be reserved for future use.

7.2.5.1.2.5 ACK Request subfield

The ACK Request subfield is 1 bit in length and specifies whether an acknowledgment is required from the recipient device on receipt of a data or MAC command frame. If this subfield is set to one, the recipient device shall send an acknowledgment frame only if, upon reception, the frame passes the third level of filtering (see 7.5.6.2). If this subfield is set to zero, the recipient device shall not send an acknowledgment frame.

7.2.5.1.2.6 Sub Frame Type subfield

The Sub Frame Type subfield is 2 bits in length and indicates the type of frame with a Shortened Frame Control field. Possible values are given in Table 122.g.

Table 122.g—Values of Frame Subtype subfield

Value of Sub Frame Type subfield	Frame with Shortened Frame Control field of type
b00	Beacon frame
b01	Command frame
b10	Acknowledgement frame
b11	Data frame

7.2.5.1.3 Frame Payload field

The Frame Payload field has a variable length and contains information specific to individual sub frame types.

7.2.5.1.4 FCS field

The FCS field is 2 octets in length and contains a 16-bit ITU-T CRC. The FCS is calculated over the MHR and MAC payload parts of the frame. The calculation of the FCS follows the same rules as defined in 7.2.1.9.

7.2.5.2 Format of individual frame types with MHR of 1 octet

7.2.5.2.1 General

Four sub frame types are defined: beacon, data, acknowledgment, and MAC command. These sub frame types are discussed in 7.2.5.1. The definition of the sub frame types is given in Table 122.g.

7.2.5.2.2 Beacon frame format

7.2.5.2.2.1 General

The Beacon frame with shortened frame control (1 octet MAC header) is sent during the beacon slot in every superframe. The structure of a Beacon frame depends on the current transmission mode (see 7.5.7a). The general structure of the beacon frame is shown in Figure 93.h.

Octets: 1	1 or variable	2
Shortend Frame Control	Flags / Beacon Payload	FCS
MHR	MAC Payload	MFR

Figure 93.h—Format of the Shortened Beacon Frame

The beacon frame does have a very short MAC header (MHR) of one octet containing the frame type and sub frame type, followed by the beacon payload and the MAC footer (MFR). The beacon payload contains the transmission mode and several flags and information fields, those existences depend on the current transmission mode.

7.2.5.2.2.2 Beacon frame MHR fields

The beacon frame does have a very short MAC header (MHR) of one octet containing the Shortened Frame Control field.

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 120, and the Sub Frame Type subfield shall contain the value that indicates a beacon frame, as shown in Table 122.g.

7.2.5.2.2.3 Flags / Beacon Payload in online mode

The beacon payload in online mode is of variable length. It contains flags which includes the transmission mode, the Gateway ID and configuration sequence number, the size of a base time slot, and a group acknowledgement. The structure of the beacon payload for beacon frames indicating online mode is depicted in Figure 93.i.

Octets: 1	1	1	1	variable
Flags	Gateway ID	Configuration Sequence Number	Timeslot Size	Group Acknowledgement

Figure 93.i—Beacon payload in online mode

The Flags field contains several control information. The structure of the Flags field is shown in Figure 93.j.

Bits: 0-2	3	4	5-7
Transmission Mode	Actuator Direction	Reserved	Number of Base Timeslots per Management Timeslot

Figure 93.j—Structure of Flags field of Beacons with 1-octet MAC-Header in online mode

The Transmission Mode subfield defines the transmission mode. It is set to the value for online mode as specified in Table 122.k.

Table 122.k—Transmission Mode settings

Bits 0-2	Transmission Mode
000	Online Mode (see 7.5.7a.3)
100	Discovery Mode (see 7.5.7a.1)
110	Configuration Mode (see 7.5.7a.2)
1x1	Mode Reset: The devices reset their state of the discovery or configuration mode. The setting of bit 1 is of no significance.

The Actuator Direction subfield indicates the transmission direction of all actuator time slots. The bit defines the transmission direction of all actuator time slots during this superframe. If the Actuator Direction subfield is set to 0, the direction of all actuator time slots is uplink (from actuator to gateway). If the Actuator Direction subfield is set to 1, the direction of all actuator time slots is downlink (from gateway to actuator).

The Number of Base Timeslots per Management Timeslot subfield contains the number of base time slots per management time slot. This value applies to both the downlink and the uplink management time slot. A value of 0 indicates that there are no management time slots available in the superframe.

The Group Acknowledgement field is a bitmap of length (macFAnumTimeSlots – macFAnumRetransmitTS) bits as shown in Figure 1.c and Figure 93.l to indicate failed sensor and actuator transmissions from the previous superframe. In the separate group acknowledgment configuration, this field is not present in the beacon. The Group Acknowledgement field contains a bit field where each bit corresponds to a time slot associated with a sensor device or an actuator device excluding retransmission time slots. Bit b_0 of the Group Acknowledgement bitmap corresponds to the first time slot after the *macFAnumRetransmitTS* retransmission time slots, bit b_1 of the Group Acknowledgement bitmap corresponds to the second time slot, and so on. Bit value 1 means the sensor transmission was successful, and bit value 0 means the sensor transmission in the previous superframe failed and the sensor is allocated a time slot for retransmission in the current superframe. Because concatenated time slots are multiples of base time slots, a concatenated time slot of length of n base time slots will have n bits in the group acknowledgement bitmap at the corresponding positions.

b_0	b_1	...	$b_{(\text{macFAnumTimeSlots - macFAnumRetransmitTS – 1})}$
acknowledgement of transmission in time slot macFAnumRetransmitTS+1	acknowledgement of transmission in time slot macFAnumRetransmitTS+2	...	acknowledgement of transmission in time slot macFAnumTimeSlots

Figure 93.l—Structure of Group Acknowledgement bitmap

If the gateway received a data frame successfully in a time slot associated with a sensor device or an actuator device during the previous superframe, it shall set the corresponding bit in the Group Acknowledgement field to 1, otherwise to 0 (corrupted transmission, no transmission). If the data frame has been received during a shared group time slot, all corresponding bits of this shared group time slot will be set accordingly in the Group Acknowledgement bitmap.

7.2.5.2.2.4 Flags / Beacon payload for discovery and configuration mode

The beacon payload in discovery or configuration mode is 1 octet of length. It contains a flags field which contains the transmission mode. The structure of the beacon payload for beacon frames indicating discovery or configuration mode is depicted in Figure 93.m.

Bits: 0-2	3-7
Transmission Mode	Reserved

Figure 93.m—Beacon payload in discovery / configuration mode

The Transmission Mode field is represented by 3 bits in discovery and configuration mode. The values that are allowed for the setting of the transmission mode are given in Table 122.k, x meaning 0 or 1.

Bits 3 through 7 are reserved and set to 0 on transmission.

7.2.5.2.3 Data frame format

7.2.5.2.3.1 General

The structure of the data frame with shortened frame control is illustrated in Figure 93.n.

Octets: 1	variable	2
Shortend Frame Control	Data Payload	FCS
MHR	MAC Payload	MFR

Figure 93.n—Format of Data Frame with Shortened Frame Control Field

The data frame does have a very short MAC header (MHR) of one octet containing the frame type and sub frame type, followed by the data payload and the MAC footer (MFR).

7.2.5.2.3.2 Data frame MHR fields

The data frame does have a very short MAC header (MHR) of one octet containing the Shortened Frame Control field.

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 79, and the Sub Frame Type subfield shall contain the value that indicates a data frame, as shown in Table 122.g.

7.2.5.2.3.3 Data Payload field

The payload of a data frame with shortened frame control shall ocntain the sequence of octets that the next higher layer has requested the MAC sublayer to transmit.

7.2.5.2.4 Acknowledgement frame format

7.2.5.2.4.1 General

The structure of the acknowledgement frame with shortened frame control is shown in Figure 93.o.

Octets: 1	1	variable	2
Shortend Frame Control	Acknow-ledgement Type	Acknowledgement Payload	FCS
MHR	MAC Payload		MFR

Figure 93.o—Format of the Shortened Acknowledgement Frame

The acknowledgement frame does have a very short MAC header (MHR) of one octet containing the frame type and sub frame type, followed by the acknowledgement type and, if applicable, the acknowlegdement payload, and the MAC footer (MFR).

7.2.5.2.4.2 Acknowledgement frame MHR fields

The acknowledgement frame does have a very short MAC header (MHR) of one octet containing the Shortened Frame Control field.

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 79, and the Sub Frame Type subfield shall contain the value that indicates an acknowledgement frame, as shown in Table 122.g.

7.2.5.2.4.3 Acknowledgement Type field

The Acknowledgement Type field is 1 octet in length and indicates the type of frame that is acknowledged. Possible values are listed in Table 122.p.

Table 122.p—Acknowledgement Types

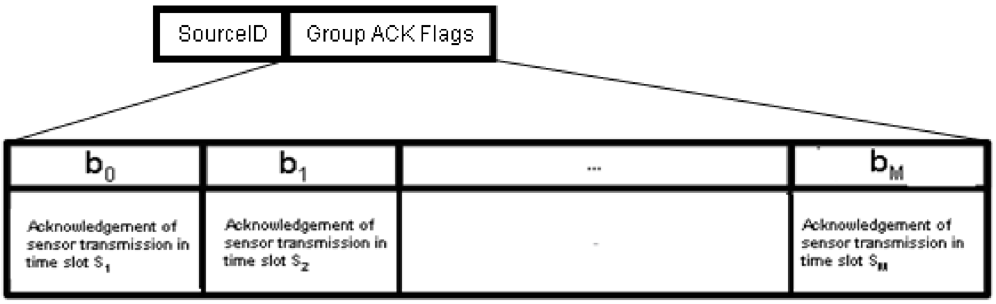
Numeric Value	Acknowledged Frame Type	Acknowledgement Payload
0x11	Discover Response	No
0x92	Configuration Request	No
0x01	Data	No
0x02	Data Group ACK	Yes (see 7.2.5.2.4.5)

7.2.5.2.4.4 Acknowlegement Payload field

The Acknowledgement Payload field is only available in certain acknowledgement types as depcited in Table 122.p. The structure and the length of the Acknowledgement Payload field depends on the value of the Acknowledgement Type field.

7.2.5.2.4.5 Data Group ACK (GACK)

The structure of the Acknowledgement Payload field of the group acknowledgement frame is shown in Figure 93.q.



Comment [MB-03D1]: M should be M-1

Figure 93.q—Format of the GACK Frame

The Source ID field identifies the transmitting gateway.

The Group Ack Flags field is a bitmap that indicates the states of transmissions of the sensors in the sensor time slots of the current superframe. A bit set to 1 indicates the fact that the coordinator received the data frame successfully in the corresponding time slot. A value of 0 means that the coordinator failed in receiving a data frame in the corresponding slot from the sensor.

7.2.5.2.5 MAC Command frame format

7.2.5.2.5.1 General

There are different types of MAC command frames with a shortened frame control. They follow the same general structure of MAC command frames with shortened frame control as shown in Figure 93.r. Only the Command Payload is different.

Octets: 1	variable	2
Shortend Frame Control	Command Payload	FCS
MHR	MAC Payload	MFR

Figure 93.r—Format of the shortened Command frames

The MAC command frame does have a very short MAC header (MHR) of one octet containing the frame type and sub frame type, followed by the command payload and the MAC footer (MFR).

7.2.5.2.5.2 MAC command frame MHR fields

The MAC command frame does have a very short MAC header (MHR) of one octet containing the Shortened Frame Control field.

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 120, and the Sub Frame Type subfield shall contain the value that indicates a MAC command frame, as shown in Table 122.g.

7.2.5.2.5.3 Command Payload field

The first octet of the command payload contains the command frame identifier. Table 82 contains the values that are defined.

The remaining octets of the Command Payload field are of variable length and contain data specific to the different command frame types.

7.3 MAC command frames

Change the first two paragraphs according to the text below.

The command frames defined by the MAC sub-layer are listed in Table 82. An FFD shall be capable of transmitting and receiving all command frame types, with the exception of the GTS request command, while the requirements for an RFD are indicated in the table. MAC commands shall only be transmitted in the CAP for beacon-enabled PANs, in management time slots of Low Latency networks, or at any time for non-beacon-enabled PANs.

How the MLME shall construct the individual commands for transmission is detailed in 7.3.1 through 7.3.12~~9~~. MAC command reception shall abide by the procedure described in 7.5.6.2.

7.3.1 Association request command

Change the Table 123 according to the Table below.

LL: Unclear in 15-09-0401-03-004e-draft-text-for-factory-automation.doc: Table 82 the row:

0x0a	Range notification		X	7.3.4.1

Table 123—MAC command frames

Command frame identifier	Command name	RFD		Subclause
		Tx	Rx	
0x01	Association request	X		0
0x02	Association response		X	7.3.2
0x03	Disassociation notification	X	X	7.3.3
0x04	Data request	X		7.3.4
0x05	PAN ID conflict notification	X		7.3.5
0x06	Orphan notification	X		7.3.6
0x07	Beacon request			7.3.7
0x08	Coordinator realignment		X	7.3.8
0x09	GTS request			7.3.9
~~0x0a–0xff~~	~~Reserved~~			—
0x0a	Advertisement		X	7.3.10.1
0x0b	Join	X		7.3.10.2
0x0c	Activate		X	7.3.10.3
0x0d	Discover Response	X		
0x0e	Configuration Response	X		
0x0f	Configuration Request		X	
0x10	CTS Shared Group		X	
0x11	Request to send (RTS)	X	X	
0x12	Clear to Send (CTS)		X	
0x13–0xff	Reserved			—

7.3.7 Beacon request command

Insert after the heading of 7.3.7 the following subclause.

7.3.7.1 General

Insert before 7.3.8 the following subclauses.

7.3.7.2 SUN-Enhanced Beacon request command

7.3.7.2.1 General

The enhanced beacon request command is intended to be used by a device to locate a subset of all coordinators within its POS during an active scan.

This command is optional for an FFD and an RFD.

The enhanced beacon request command shall be formatted as illustrated in Figure 100.a.

Octets:7	1	1	0/1	0/1	Variable
MHR fields	Command Frame Identifier (see Table 123)	Request Field	Link Quality	Percent filter	Extended Payload

Figure 100.a—SUN-Enhanced Beacon request command

The Destination Addressing Mode subfield of the Frame Control field shall be set to two (i.e., 16-bit short addressing), and the Source Addressing Mode subfield shall be set to zero (i.e., source addressing information not present).

The Frame Pending subfield of the Frame Control field shall be set to zero and ignored upon reception.

The Acknowledgment Request subfield and Security Enabled subfield shall be set to zero. If the enhanced beacon request is being sent on a particular PAN Identifier that is not the broadcast PAN identifier the Security Enable subfield may be set to 1, otherwise it shall be set to 0.

The Destination PAN Identifier field shall contain the any appropriate PAN identifier. If the broadcast PAN identifier is used, any device may respond however if a specific PAN identifier is used only devices using that PAN identifier will respond to the enhanced beacon request.

The Destination Address field shall contain the broadcast short address (i.e., 0xffff).

7.3.7.2.2 Request Field

7.3.7.2.2.1 General

The request field is a 1 octet field indicating what optional request discriminators are included in the Enhanced Beacon Request Command Payload. The Request Field is as shown in Table 125.b.

Table 125.b—LL-specific MAC PIB attributes

Bit	SubField
0	Permit Joining On
1	LinkQuality
2	Percent filter
3 - 6	Reserved
7	Extended Payload

For any bits set in the request field the following is done.

7.3.7.2.2.2 Permit Joining On

Only devices with permit joining on shall respond to the enhanced beacon request.

7.3.7.2.2.3 LinkQuality Level

Following the Request field the enhanced beacon request will include a field containing a value for LinkQuality. The device will respond to the enhanced beacon request if the MCPS-DATA.indication indicates a mpduLinkQuality equal or lower than this value (where lower values represent higher quality links).

7.3.7.2.2.4 Percent filter

Following the Request Field a byte will be included of a scaled value from 0x00 to 0x64 representing zero to 100 percent probability for a given device to respond to the enhanced beacon request. The device will then randomly determine if it is to respond to the enhanced beacon request based on meeting this probability. For example if the probability is set to 10% then 1 of 10 devices would randomly be expected to respond.

7.3.7.2.2.5 Extended Payload

If this bit is set the extended payload field shall be included in the enhanced beacon request. The extended payload should be provided as the MSDU in the MCPS-DATA.indication to the local SSCS entity in which case the SSCS entity would be responsible for handling beacon responses based on data in this extended payload.

7.3.8 Coordinator realignment command

7.3.9 GTS request command

Insert before 7.4 the following subclauses.

7.3.10 PA-commands

7.3.10.1 Advertisement command

7.3.10.1.1 General

The Advertisement command is used by FFDs to invite new devices into the network. When a device wishes to join a network, it shall use the information in Advertisement command frames to synchronize to the network and request an association. Figure 103.a shows the format of the Advertisement command.

octets: variable (see 7.2.2.4)	**1**	**6**	**1**	**1**	**1**	**1**	**1**	**variable**	**1**	**variable**	**0/4/8/ 16**	**2**
MHR	Command Frame Identifier (see table 82)	Timing Information	Security Control Field	Join Control	Timeslot Template and Hopping Sequence ID	Channel Page/Map Length	Channel Page	Channel Map	Number of Slot-frames	Slotframe Info. and Links (for Each Slotframe)	MIC	MFR

Figure 103.a—Advertisement command format

7.3.10.1.2 MHR field

The Source Addressing Mode subfield of the Frame Control field shall be set to three (64-bit extended addressing). The Destination Addressing Mode subfield shall be set to the broadcast address, i.e. 0xFFFF.

The Frame Pending subfield of the Frame Control field shall be set to zero and ignored upon receipt, and the Acknowledgment Request subfield shall be set to zero. The Source PAN Identifier field shall contain the PAN identifier of the node. The Source Address field shall contain the value of an ExtendedAddress.

The Sequence Number subfield shall be set to the least significant byte of the absolute slot number.

7.3.10.1.3 Command Frame Identifier field

The Type field shall be set to Advertisement (0x0a).

7.3.10.1.4 Timing Information field

The Timing Information field shall be set to the time information (i.e. Absolute Slot Number) of the timeslot being used for transmission of this command frame.

7.3.10.1.5 Security Control field

Figure 103.b shows the Security Control field.

Bit 4–7	Bit 0–3
Reserved	Security Level

Figure 103.b—Security Control field

The Security Level subfield should be set to the security level supported. The definition of the Security Level subfield can be found in Table 95 in 7.6.2.2.1.

7.3.10.1.6 Join Control field

Figure 103.c shows the Join Control field.

Bit 4–7	0–3
Reserved	Join Priority

Figure 103.c—Join Control field

The Join Priority subfield can be used by a joining device to decide which Network Devices to include in its Association Request if it hears advertisements from more than one device.

A lower value of join priority indicates that the device is a preferred one to connect to.

7.3.10.1.7 Timeslot Template and Hopping Sequence ID field

The Timeslot Template and Hopping Sequence ID field shall be set to the ID of the timeslot template and the ID of the hopping sequence used by the MAC. The timeslot templates and hopping sequences are defined in MAC PIB.

Figure 103.d shows the Timeslot Template and Hopping Sequence ID field.

Bit 4–7	0–3
Hopping Sequence ID	Timeslot Template ID

Figure 103.d—Timeslot Template and Hopping Sequence ID field

7.3.10.1.8 Channel Page/Map Length field

The Channel Page/Map field shall be set to the combined length of following channel page and channel map fields.

7.3.10.1.9 Channel Page field

The Channel Page field shall be set to the channel page of channels that the joining device shall use for its hopping sequence.

7.3.10.1.10 Channel Map field

The Channel Map field shall be set to the channel map of channels that the joining device shall use for its hopping sequence.

7.3.10.1.11 Number of Slotframes field

The Number of Slotframes field is set to the total number of slotframes for which information is being advertised in this command frame.

7.3.10.1.12 Slotframe Information and Links (for each slotframe) field

7.3.10.1.13 General

Slotframe Information and Links field is included for each slotframe. The format of Slotframe Information and Links field is depicted as shown in Figure 103.e.

Octets: 1	2	1	Variable
Slotframe ID	Slotframe Size	Number of Links	Link Info. for each Link

Figure 103.e—Slotframe and Links field

7.3.10.1.14 Slotframe ID subfield

Slotframe ID shall be set to the ID that uniquely identifies the slotframe.

7.3.10.1.15 Slotframe Size subfield

Slotframe Size shall be set to the size of the slotframe in number of timeslots.

7.3.10.1.16 Number of Links subfield

The Number of Links subfield shall be set to the number of links that belong to the specific slotframe indicated in preceding slotframe ID.

7.3.10.1.17 Link Information (for each link) subfield

The Link Information subfield describes the attributes of each link. The format of Link Information subfield is depicted as shown in Figure 103.f.

Octets: 2	1	1
Timeslot	Channel Offset	Link Option

Figure 103.f—Link Information field

7.3.10.1.18 Timeslot subfield

The Timeslot subfield shall be set to the timeslot of this link.

7.3.10.1.19 Channel Offset Information subfield

The Channel Offset Information subfield shall be set to the channel offset of this link.

7.3.10.1.20 Link Option subfield

The Link Option subfield indicates whether this link is a TX link, an RX link, or a SHARED TX link. SHARED TX links can be used for a joining device to send its Join command. RX links are used for a new device to receive Advertisement commands. RX links can also be used for a joining device to receive its Activate command from the network. It is possible for one link to be used as both SHARED_TX and RX link.

7.3.10.1.21 MIC

The message integrity check of the Advertisement command frame.

7.3.10.2 Join command

7.3.10.2.1 General

The Join command is used by a device to join the TSCH network through the advertiser. This command shall only be sent by a new device that wishes to join the TSCH network or a device that lost connection with the TSCH network.

All devices shall be capable of transmitting this command, although an RFD is not required to be capable of receiving it.

The Join command shall be formatted as illustrated in Figure 103.g.

octets: variable (see 7.2.2.4)	1	1	1	1	0/3	variable	0/3	tbd	0/4/8/16
MHR	Command Frame Identifier (see table 82)	Capability Information (see Figure 56)	Clock Accuracy Capability	Number of Neighbors	Neighbor 1	...	Neighbor n	Join Security Information (TBD by Security sub-group)	MIC

Figure 103.g—Join command format

7.3.10.2.2 MHR fields

The Source Addressing Mode subfield of the Frame Control field shall be set to three (64-bit extended addressing). The Destination Addressing Mode subfield shall be set to the same mode as indicated in Advertisement command frame to which the Join command refers.

The Frame Pending subfield of the Frame Control field shall be set to zero and ignored upon receipt, and the Acknowledgment Request subfield shall be set to one.

The Destination PAN Identifier field shall contain the identifier of the PAN to which to join. The Destination Address field shall contain the address from the Advertisement frame that was transmitted by the coordinator to which the Join command is being sent. The PAN ID Compression subfield may be set to one and the Source PAN Identifier may be omitted. The Source Address field shall contain the value of an ExtendedAddress.

The Sequence Number subfield shall be set to the least significant byte of the absolute timeslot number.

7.3.10.2.3 Command Frame Identifier field

The Type field shall be set to *Join (0x0b)*.

7.3.10.2.4 Capability Information field

The Capability Information field shall be formatted as illustrated in Figure 94.

7.3.10.2.5 Clock Accuracy Capability field

The Clock Accuracy Capability field shall be formatted as illustrated in Figure 103.h.

Bit: 0	1 - 7
10ppm capable	reserved

Figure 103.h—Clock Accuracy Capability

7.3.10.2.6 Join Security Information field

The definition of Join Security Information field shall contain the security information that the new device to mutually authenticate the new joining device and Security Manager. This will be defined by Security sub-group.

7.3.10.2.7 Number of Neighbor field

The Number of Neighbor field indicates the number of neighbors included in this command frame.

7.3.10.2.8 Neighbor field

The Neighbor field shall contain the information about the neighbors of the new device. The Neighbor field shall be formatted as illustrated in Figure 103.h.

Octets: 2	1
16 bit address of the neighbor	RSSI

Figure 103.i—Neighbor

7.3.10.2.9 MIC

This field contains the message integrity check of the Join command frame.

7.3.10.3 Activate command

7.3.10.3.1 General

The Activate command allows the advertiser to communicate the results of a Join attempt back to the device requested joining. The Activate command can also include the description of slotframe and links for the joining device to communicate with the TSCH network.

This command shall only be sent by the advertiser to the device that is currently trying to join.

All devices shall be capable of receiving this command, although an RFD is not required to be capable of transmitting it.

The Activate command shall be formatted as illustrated in Figure 103.j.

Octets: (see 7.2.2.4)	**1**	**2**	**1**	**varaibale**	**tbd**	**0/4/8/16**
MHR fields	Command frame Identifier (see Table 82)	Short Address	Number of Slot-frames	Slotframe Info. and Links (for Each Slotframe)	Activate Security Information (TBD by Security sub-group)	MIC

Figure 103.j— Activate command format

7.3.10.3.2 MHR

The Destination Addressing Mode subfield of the Frame Control field shall be set to three (i.e., 64-bit extended addressing). The Source Addressing Mode subfield of the Frame Control field shall be set to two (i.e., 16-bit addressing.

The Frame Pending subfield of the Frame Control field shall be set to zero and ignored upon receipt, and the Acknowledgment Request subfield shall be set to one.

The Source PAN Identifier field shall contain the value of macPANId. The Source Address field shall contain the value of a CoordShortAddress.

The Destination PAN Identifier field should be set to 0xFFFF. Destination Address field shall contain the extended address of the device requesting to join the network.

The Sequence Number subfield shall be set to the least significant byte of the absolute timeslot number.

7.3.10.3.3 Command Frame Identifier field

The Type field shall be set to Activate (0x0c).

7.3.10.3.4 Short Address field

If the advertiser was not able to join this device to its PAN, the Short Address field shall be set to 0xffff, and the Join Status field shall contain the reason for the failure. If the was advertiser is able to Join the device to its PAN, this field shall contain the short address that the device shall use in its communications on the PAN until it is disconnected.

The device shall use the source PANID of the Activate command as its PANID.

7.3.10.3.5 Number of Links field

The Number of Links field shall be set to the total number of links assigned to new device being activated.

7.3.10.3.6 Link field

Link field shall have the description of link allocated to new device being activated. The format of Link field shall be according to 7.3.10.1.11.

7.3.10.3.7 Activate Security Information field

The definition of Activate Security Information field shall contain the security information that the new device should use to securely communicate to the TSCH network. It may include keys for data link and session layers.

7.3.10.3.8 MIC

This field contains the message integrity check of the Activate command frame.

7.3.11 LL-commands

7.3.11.1 7.3.10 Discover Response command

7.3.11.1.1 General

The Discover Response command contains the configuration parameters that have to be transmitted to the gateway as input for the configuration process in a Low Latency network.

This command shall only be sent by a device that has received a beacon with shortened frame control (see 7.2.2a.1) indicating discovery mode as determined through the procedures of the discovery mode (see 7.5.7a.1).

All devices shall be capable of transmitting this command, although an RFD is not required to be capable of receiving it.

The command payload of the discover response frame shall be formatted as illustrated in Figure 103.k.

Octets: 1	variable
Command Frame Identifier (see Table 82)	Discovery Parameters

Figure 103.k—Discover response command MAC payload

7.3.11.1.2 7.3.10.1 MHR fields

7.3.11.1.2.1 General

The discover response command can be sent using both MAC command frames (7.2.2.4) or MAC command frames with shortened frame control (7.2.2a.4).

7.3.11.1.2.2 7.3.10.1.1 Using MAC command frames

The Frame Type subfield of the Frame Control field shall contain the value that indicates a MAC command frame, as shown in Table 120.

The Source Addressing Mode subfield of the Frame Control field shall be set to 3 (64-bit extended addressing).

The Source Address field shall contain the value of aExtendedAddress.

7.3.11.1.2.3 7.3.10.1.2 Using MAC command frames with shortened frame control

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 120, and the Sub Frame Type subfield shall contain the value that indicates a MAC command frame, as shown in Table 122.g.

7.3.11.1.3 7.3.10.2 Command Frame Identifier field

The Command Frame Identifier field contains the value for the discover response command frame as defined in Table 123.

7.3.11.1.4 7.3.10.3 Discovery Parameters field

The Discovery Parameters field contains the configuration parameters that have to be transmitted to the gateway as input for the configuration process. The discovery parameters consist of:

— full MAC address

— required time slot duration, this is defined by the application of the device (e.g. size of sensor data)

— sensor / actuator type indicator

7.3.11.2 Configuration Response Frame

7.3.11.2.1 General

The Configuration Response command contains the configuration parameters that are currently configured at the device as input for the configuration process in a Wireless Factory Automation network.

This command shall only be sent by a device that has received a beacon with shortened frame control (see 7.2.2a.1) indicating configuration mode as determined through the procedures of the configuration mode (7.5.7a.2).

All devices shall be capable of transmitting this command, although an RFD is not required to be capable of receiving it.

The command payload of the Configuration Response Frame shall be formatted as illustrated in Figure 103.l.

Octets: 1	variable
Command Frame Identifier (see Table 123)	Configuration Parameters

Figure 103.l—Configuration response command MAC payload

7.3.11.2.2 MHR fields

The configuration response command can be sent using both MAC command frames (7.2.2.4) or MAC command frames with shortened frame control (7.2.2a.4).

7.3.11.2.3 7.3.11.1.1 Using MAC command frames

7.3.11.2.3.1 General

The Frame Type subfield of the Frame Control field shall contain the value that indicates a MAC command frame, as shown in Table 120.

The Source Addressing Mode subfield of the Frame Control field shall be set to 1 (8-bit short addressing) or 3 (64-bit extended addressing).

The Source Address field shall contain the value of aVeryShortAddress or aExtendedAddress respectively.

7.3.11.2.3.2 Using MAC command frames with shortened frame control

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 120, and the Sub Frame Type subfield shall contain the value that indicates a MAC command frame, as shown in Table 122.g.

7.3.11.2.4 Command Frame Identifier field

The Command Frame Identifier field contains the value for the configuration response frame as defined in Table 123.

7.3.11.2.5 Configuration Parameters field

The Configuration Parameters field contains the configuration parameters that are currently configured at the device. The configuration parameters consist of:

- full MAC address
- short MAC address
- required time slot duration, this is defined by the application of the device (e.g. size of sensor data)
- sensor / actuator
- assigned time slots

7.3.11.3 Configuration Request Frame

7.3.11.3.1 General

The Configuration Request command contains the configuration parameters that the receiving device is requested to use during online mode in a Wireless LL-network.

This command shall only be sent by a gateway in response to a received Configuration Response frame of a device during configuration mode.

Only gateways are requested to be capable of transmitting this command, RFD are required to be capable of receiving it.

The command payload of the Configuration Request Frame shall be formatted as illustrated in Figure 103.m.

Octets: 1	variable
Command Frame Identifier (see Table 123)	Configuration Parameters

Figure 103.m—Configuration request command MAC payload

7.3.12.1 MHR fields

7.3.11.3.1.1 General

The configuration request command can be sent using both MAC command frames (7.2.2.4) or MAC command frames with shortened frame control (7.2.2a.4).

7.3.11.3.1.2 Using MAC command frames

The Frame Type subfield of the Frame Control field shall contain the value that indicates a MAC command frame, as shown in Table 120.

The Source Addressing Mode subfield of the Frame Control field shall be set to 1 (8-bit short addressing) or 3 (64-bit extended addressing).

The Destination Address field shall contain the value of source address of the corresponding Configuration Response frame.

7.3.11.3.1.3 Using MAC command frames with shortened frame control

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 120, and the Sub Frame Type subfield shall contain the value that indicates a MAC command frame, as shown in Table 122.g.

7.3.11.3.2 Command Frame Identifier field

The Command Frame Identifier field contains the value for the configuration response frame as defined in Table 123.

7.3.11.3.3 Configuration Parameters field

The Configuration Parameters field contains the new configuration parameters that are sent to the device in order to (re-)configure it. The configuration parameters consist of:

- full MAC address
- short MAC address

- transmission channel
- existence of management frames
- time slot duration
- assigned time slots

7.3.11.4 Clear to Send (CTS) Shared Group Frame

7.3.11.4.1 General

The Clear to Send Shared Group command indicates to the devices of the star network that they now may use the time slot for transmitting their own data with a simplified CSMA/CA.

This command shall only be sent by a gateway in a time slot after tSlotTxOwner has been elapsed and the slot owner is not transmitting.

Only gateways are requested to be capable of transmitting this command, devices are required to be capable of receiving it.

The command payload of the Clear to Send Shared Group frame shall be formatted as illustrated in Figure 103.n.

Octets: 1	1
Command Frame Identifier (see Table 123)	Network ID

Figure 103.n—Clear to send shared group command MAC payload

7.3.11.4.2 MHR fields

The clear to send shared group command can be sent using MAC command frames with shortened frame control (7.2.2a.4).

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 120, and the Sub Frame Type subfield shall contain the value that indicates a MAC command frame, as shown in Table 122.g.

7.3.11.4.3 Command Frame Identifier field

The Command Frame Identifier field contains the value for the clear to send shared group frame as defined in Table 123.

7.3.11.4.4 Network ID field

The Network ID field contains an identifier specific to the gateway.

7.3.11.5 Request to Send (RTS) Frame

7.3.11.5.1 General

The Request to Send command may be used by devices to indicates to the gateway and to the other devices of the star network that it wants to transmit data with a simplified CSMA/CA. The request to send frame is transmitted using a simplified CSMA/CA.

This command shall only be sent by a device in a time slot after tSlotOwner has been elapsed and and a clear to send shared group frame has been received from the gateway.

Devices are requested to be capable of transmitting and receiving this command.

The command payload of the Request to Send frame shall be formatted as illustrated in Figure 103.o.

Octets: 1	1	1
Command Frame Identifier (see Table 82)	Short Originator Address	Network ID

Figure 103.o—Request to send command MAC payload

7.3.11.5.2 MHR fields

The request to send command can be sent using MAC command frames with shortened frame control (7.2.2a.4).

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 79, and the Sub Frame Type subfield shall contain the value that indicates a MAC command frame, as shown in Table 122.g.

7.3.11.5.3 Command Frame Identifier field

The Command Frame Identifier field contains the value for the request to send frame as defined in Table 123.

7.3.11.5.4 Short Originator Address

The Short Originator Address field contains the 1-octet short address of the device sending this request to send frame.

7.3.11.5.5 Network ID field

The Network ID field contains an identifier specific to the gateway. It has to be identical to the Network ID of the corresponding received CTS shared group frame.

7.3.11.6 Clear to Send (CTS) Frame

7.3.11.6.1 General

The Clear to Send command indicates to a specific device of the star network that it may now use the time slot for transmitting its own data with a simplified CSMA/CA.

This command shall only be sent by a gateway in a time slot after tSlotOwner has been elapsed and the slot owner is not transmitting.

Only gateways are requested to be capable of transmitting this command, devices are required to be capable of receiving it.

The command payload of the Clear to Send Shared Group frame shall be formatted as illustrated in Figure 103.p.

Octets: 1	1	1
Command Frame Identifier (see Table 82)	Short Destination Address	Network ID

Figure 103.p—Clear to send command MAC payload

7.3.11.6.2 MHR fields

The clear to send command can be sent using MAC command frames with shortened frame control (7.2.2a.4).

In the Shortened Frame Control field, the Frame Type subfield shall contain the value that indicates a MAC frame with a shortened frame control, as shown in Table 120, and the Sub Frame Type subfield shall contain the value that indicates a MAC command frame, as shown in Table 122.g.

7.3.11.6.3 Command Frame Identifier field

The Command Frame Identifier field contains the value for the clear to send shared group frame as defined in Table 123.

7.3.11.6.4 Short Destination Address

The Short Destination Address field contains the 1-octet short address of the device to which this clear to send frame is directed.

7.3.11.6.5 Network ID field

The Network ID field contains an identifier specific to the gateway. It has to be identical to the Network ID of the corresponding received RTS frame.

7.4 MAC constants and PIB attributes

7.4.1 MAC constants

7.4.2 MAC PIB attributes

Insert after the heading of 7.4.2 the following subclause header.

7.4.2.1 General

Insert before 7.5 the following subclauses.

7.4.2.2 PA-specific MAC PIB attributes

7.4.2.2.1 General

Subclause 7.4.2.1 applies except that the attributes macMinBE and macMaxBE in Table 127 shall be according to Table 127.a and an additional attribute macDisconnectTime is required, see Table 127.a.

Table 127.a—PA-specific MAC PIB attributes

Attribute	Identifier	Type	Range	Description	Default
macMinBE	0x4f	Integer	0–macMaxBE	The minimum value of the backoff exponent (BE) in the CSMA-CA algorithm or the TSCH CA algorithm. See 7.5.1.4 for a detailed explanation of the backoff exponent. See 7.5.4.2 for use of the backoff exponent in TSCH mode.	3/1
macMaxBE	0x57	Integer	3–8	The maximum value of the backoff exponent, BE, in the CSMA-CA algorithm or the TSCH CA algorithm. See 7.5.1.4 for a detailed explanation of the backoff exponent. See 7.5.4.2 for use of the backoff exponent in TSCH mode.	5/7
macDisconnectTime	0x64	Integer	0x00-0xFFFF	Time to send out Disconnect frames before disconnecting	

7.4.2.2.2 PA-MAC PIB attributes for macSlotframeTable

The attributes contained in the MAC PIB for macSlotframeTable are presented in Table 127.b.

Table 127.b—PA-MAC PIB attributes for macSlotframeTable

Attribute	Identifier	Type	Range	Description	Default
slotframeId	0x64	Integer	0x00-0xFF	Identifier of the slotframe	
slotframeSize	0x65	Integer	0x0000-0xFFFF	Number of timeslots in the slotframe	
activeFlag	0x66	Boolean	0x0-0x1	Flag indicating if the slotframe is currently activated	
channelPage	0x67	Integer	0x00-0x1F	Channel Page of channels used in this slotframe	
channelMap	0x68	Bitmap		Bitmap of active channels.	

7.4.2.2.3 PA-MAC PIB attributes for macLinkTable

The attributes contained in the MAC PIB for macLinkTable are presented in Table 127.c.

Table 127.c— PA-MAC PIB attributes for macLinkTable

Attribute	Identifier	Type	Range	Description	Default
linkId	0x69	Integer	0x00-0xFF	Identifier of Link	
linkOption	0x6a	Bitmap	0x00-0x7	Flags indicating whether the link is used for transmit, receive, or shared transmissions:	
linkType	0x6b	Integer	0x00-0x2	Enumeration indicating the type of link: Normal, Join, or Advertising	
slotframeId	0x6c	Integer	0x00-0xFF	Identifier of Slotframe to which this link belongs	
nodeAddress	0x6d	IEEE address	16 bit address	Address of the node connected to this link	
timeslot	0x6e	Integer	0x0000-0xFFFF	Timeslot for this link	
channelOffset	0x6f		0x00-0xFF	Channel offset for this link	

7.4.2.2.4 PA-MAC PIB attributes for macTimeslotTemplate

The attributes contained in the MAC PIB for macTimeslotTemplate are presented in Table 127.d.

Table 127.d—PA-MAC PIB attributes for macTimeslotTemplate

Attribute	Identifier	Type	Range	Description	Default
Timeslot Template Id	0x70	Integer	0x0-0xF	Identifier of Timeslot Template	
TsCCAOffset	0x71	Integer	0x0000-0xFFFF	The time between the beginning of timeslot and start of CCA operation	
TsCCA	0x72	Integer	0x0000-0xFFFF	Duration of CCA	
TsTxOffset	0x73	Integer	0x0000-0xFFFF	The time between the beginning of the timeslot and the start of packet transmission	
TsRxOffset	0x74	Integer	0x0000-0xFFFF	Beginning of the timeslot to when the receiver must be listening	
TsRxAckDelay	0x75	Integer	0x0000-0xFFFF	End of packet to when the transmitter must listen for Acknowledgment	
TsTxAckDelay	0x76	Integer	0x0000-0xFFFF	End of packet to start of Acknowledgment	
TsRxWait	0x77	Integer	0x0000-0xFFFF	The time to wait for start of packet	
TsAckWait	0x78	Integer	0x0000-0xFFFF	The minimum time to wait for start of an Acknowledgment	
TsRxTx	0x79	Integer	0x0000-0xFFFF	Transmit to Receive turnaround (12 symbols)	
TsMaxAck	0x7a	Integer	0x0000-0xFFFF	Transmission time to send Acknowledgment	
TsMaxTx	0x7b	Integer	0x0000-0xFFFF	Transmission time to send the maximum length packet (133 bytes)	

7.4.2.2.5 PA-MAC PIB attributes for macHoppingSequence

To be jointly defined with Channel Hopping/Channel Diversity subgroup.

The attributes contained in the MAC PIB for macHoppingSequence are presented in Table 127.c.

Table 127.e— PA-MAC PIB attributes for macHoppingSequence

Attribute	Identifier	Type	Range	Description	Default

7.4.2.3 LL-specific MAC PIB attributes

Subclause 7.4.2.1 applies and an additional attributes are required, see Table 127.a.

Table 127.f—LL-specific MAC PIB attributes

Attribute	Identifier	Type	Range	Description	Default
macFAlowLatencyPAN	0x7c	Boolean	TRUE or FALSE	Indicates that the PAN is using the mechanisms as described in 5.3.3, 5.5.1.2, and related clauses.	Set by configuration
macFAnumTimeSlots	0x7d	Integer	0 … 254	Number of time slots within superframe excluding time slot for beacon frame	20
macFAnumSensorTS	0x7e	Integer	0 … macFAnum-TimeSlots	Number of sensor time slots within superframe for unidirectional communication (uplink)	20
macFAnumRetransmitTS	0x7f	Integer	0 … macFAnum-SensorTS/2	Number of sensor time slots reserved for retransmission (see 5.5.1.2 and 7.5.1.1a.1)	0
macFAnumActuatorTS	0x80	Integer	0 … macFAnum-TimeSlots	Number of actuator time slots within superframe for bidirectional communication	0
macFAmgmtTS	0x81	Boolean	TRUE or FALSE	Indicates existence of management time slots in Online Mode	FALSE
macFAlowLatencyNWid	0x82	Integer	0x00–0xff	The 8-bit identifier of the LLNW on which the device is operating. If this value is 0xff, the device is not associated.	0xff

7.5 MAC functional description

7.5.1 Channel access

7.5.1.1 Superframe structure

Insert after the frist paragraph the following text.

For LL-applications an additional superframe structure with beacons is required using a shortened frame control, see 7.5.1.1.3.

7.5.1.1.1 Contention access period (CAP)

7.5.1.1.2 Contention-free period (CFP)

Insert before 7.5.1.2 the following subclauses.

7.5.1.1.3 LL-Superframe structure

7.5.1.1.3.1 General Structure of Superframe

The superframe is divided into a beacon slot and *macFAnumTimeSlots* base time slots of equal length, see Figure 104.a.

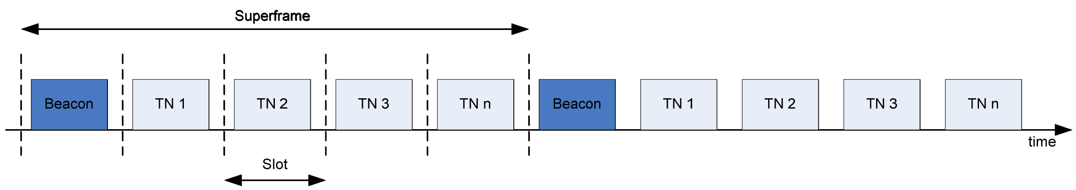


Figure 104.a—Superframe with dedicated time slots

The first time slot of each superframe contains a beacon frame. The beacon frame is used for synchronization with the superframe structure. It is also used for re-synchronisation of devices that went into power save or sleep mode.

The remaining time slots are assigned to specific devices of the network. Each time slot may have assigned a so-called slot owner. The slot owner has access privileges in the time slot (dedicated time slot). There is no explicit addressing necessary inside the frames if the slot owner transmits in its time slot. The determination of the sender is achieved through the number of the time slot. More than one device can be assigned to a time slot (shared group time slot). The devices use a contention-based access method (modified CSMA/CA) a simple addressing scheme.

Multiple adjacent base time slots can be concatenated to a single, larger time slot.

As shown in Figure 104.b, there is a specific order in the meaning or usage of the time slots.

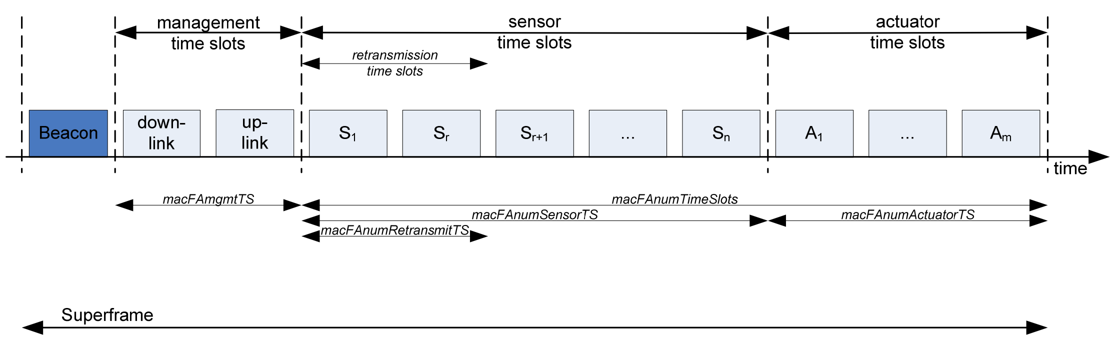


Figure 104.b—Usage and order of slots in a superframe

- Beacon Time Slot: always there (cf. clause 5.2)
- Management Time Slots: one time slot downlink, one time slot uplink, existence is configurable in *macFAmgmtTS* during setup (cf. clause 5.3)

— Time slots for sensors: *macFAnumSensorTS* time slots uplink (uni-directional communication), *macFAnumRetransmitTS* time slots at the beginning can be reserved for retransmissions (cf. clause 5.4)

— Time slots for actuators: *macFAnumActuatorTS* time slots uplink / downlink (bi-directional communication) (cf. clause 5.5)

7.5.1.1.3.2 Beacon Time Slot

The beacon time slot is reserved for the gateway to indicate the start of a superframe with the transmission of a beacon. The beacon is used to synchronize the devices and to indicate the current transmission mode. The beacon contains also acknowledgements for the data transmitted in the last superframe.

The beacon time slot is available in every superframe.

7.5.1.1.3.3 Management Time Slots

The first portion of a superframe after the beacon time slot is formed by the management time slots, i.e. the downlink/uplink management time slots.

The downlink direction is defined as sending data *to* the device (sensor, actuator). The uplink direction is defined as sending data *from* the device (sensor, actuator).

Management time slots provide a mechanism for bidirectional transmission of management data in downlink and uplink direction. Downlink and uplink time slots are provided in equal number in a superframe. There are two management time slots per superframe at maximum. Management down-/uplink time slots are implemented as shared group access time slots.

Management down-/uplink time slots are used in discovery and configuration mode and are optional in the online mode.

7.5.1.1.3.4 Sensor Time Slots

After the management time slots, time slots for the transmission of sensor data are contained in a superframe. Sensor time slots allow for unidirectional communication (uplink) only.

The first *macFAnumRetransmitTS* of the *macFAnumSensorTS* sensor time slots are dedicated time slots for retransmissions of failed uplink transmission attempts in dedicated time slots of the previous superframe. The dynamic assignment of nodes to retransmission time slots is described in 7.5.7a.3.

7.5.1.1.3.5 Actuator Time Slots

Actuator time slots allow for bidirectional communication between the gateway and the device (actuator). The direction of the communication is signalled in the beacon as described in 7.2.2a.1. Actuator time slots are used for the transmission of device data to the gateway (uplink) as well as of actuator information from the gateway to the device (downlink).

7.5.1.1.3.6 Channel access within time slots

Each time slot is described by four time attributes as illustrated in Figure 104.c and described in Table 127.d.

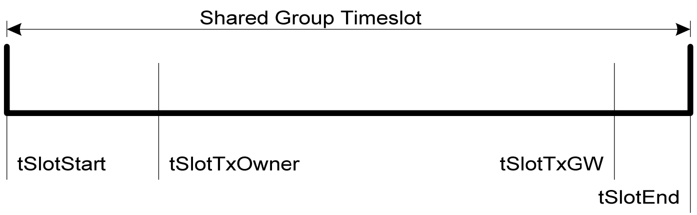


Figure 104.c—Time attributes of time slots

Table 127.d—Time attributes of time slots

Attribute	Description
tSlotStart	starting time of time slot
tSlotTxOwner	end time of priviledged access by device that owns the time slot
tSlotTxGW	if time slot is unused, gateway can use the time slot
tSlotEnd	end time of time slot

From tSlotStart till tSlotTxOwner, the device that owns the slot, the slot owner, has exclusive access to the time slot.

From tSlotTxOwner till tSlotTxGW, any device may use the time slot with a modified CSMA/CA access scheme as described in 7.5.1.5, if the time slot is not used by the slot owner.

From tSlotTxGW till tSlotEnd, the gateway may use the time slot, if the time slot is still unused.

Dedicated time slots are reserved for a single device (slot owner). This is achieved by setting tSlotTxOwner and tSlotTxGW to tSlotEnd. A dedicated time slot allows the transmission of exactly one packet. Dedicated time slots are only used during online mode (cf. 7.5.7a.3).

Shared group time slots with contention-based access for every allowed device can be achieved by setting tSlotTxOwner to tSlotStart.

7.5.1.2 Incoming and outgoing superframe timing

7.5.1.4 CSMA-CA algorithm

Insert after the heading of 7.5.1.4 the following subclause.

7.5.1.4.1 General

Insert before 7.5.2 the following subclauses.

7.5.1.4.2 PA-CCA Algorithm

When a device is operating in the TSCH mode (see 7.1.21.3) the CCA is used to promote coexistence with other users of the radio channel. For other devices in the same network the start time of transmissions, TxTxOffset, is closely aligned making intra-network collision avoidance using CCA ineffective. The TSCH devices also do channel hopping so there is no backoff period used when CCA prevents a transmission.

When a device has a packet to transmit. it waits for a link it can transmit it in. If CCA has been enabled, the MAC requests the PHY to perform a CCA at the designated time in the timeslot, TxCCAOffset, without any backoff delays. Figure 107.a extend Figure 107 for the TSCH mode.

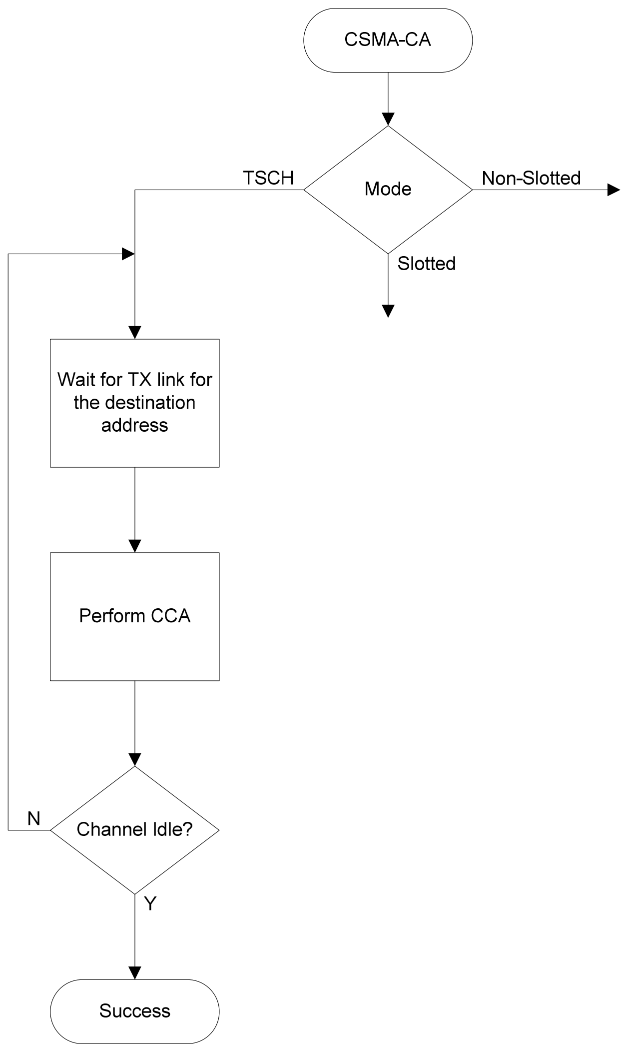


Figure 107.a—PA-CSMA-CA Algorithm

7.5.1.4.3 PA-CA Algorithm

Shared links (links with the linkOption shared bit set) are intentionally assigned to more than one device for transmission. This can lead to collisions and result in a transmission failure detected by not receiving an acknowledgement. To reduce the probability of repeated collisions when the packets are retransmitted a retransmission backoff algorithm shall be implemented for shared links.

When a packet is transmitted on a shared link for which an acknowledgement is expected and none is received, the transmitting device shall invoke the TSCH CA retransmission algorithm. Subsequent retransmissions may be in either shared links or dedicated links. This backoff algorithm has the following properties:

- The retransmission backoff wait applies only to the transmission on shared links. There is no waiting for transmission on dedicated links.
- The retransmission backoff is calculated in the number of shared link transmission links.
- The backoff window increases for each consecutive failed transmission in a shared link.
- A successful transmission in a shared link resets the backoff window to the minimum value.
- The backoff window does not change when a transmission is a failure in a dedicated link.
- The backoff window does not change when a transmission is successful in a dedicated link and there transmission queue is still not empty afterwards.
- The backoff window is reset to the minimum value if the transmission in a dedicated link is successful and the transmit queue is then empty.

In TSCH mode, backoff is calculated in shared links, so the CSMA-CA aUnitBackoffPeriod is not used.

macMaxBE and macMinBE have different default values when the device is in TSCH mode (see table 86).

The device shall use an exponential backoff mechanism analogous to that described in 7.5.1.4.1. A device upon encountering a transmission failure in a shared link shall initialize the backoff exponent (BE) to macMinBE. The MAC sublayer shall delay for a random number in the range 0 to $2^{BE}–1$ shared links (on any slotframe) before attempting a retransmission on a shared link. Retransmission on a dedicated link may occur at any time. For each successive failure on a shared link, the device should increase the backoff exponent until the backoff exponent = macMaxBE. Successful transmission on a shared link resets the backoff exponent to macMinBE.

If an acknowledgment is still not received after macMaxFrameRetries retransmissions, the MAC sublayer shall assume the transmission has failed and notify the next higher layer of the failure.

7.5.1.4.4 LL-Simplified CSMA-CA

This subclause defines a simplified CSMA-CA algorithm that is used during Management Time slots and Shared Group Timeslots in low latency networks.

The simplified CSMA-CA is a slotted CSMA-CA mechanism and follows the same algorithm as described in 7.5.1.4.1. However, some MAC PIB attributes have different default values as shown in Table 127.b.

MAC PIB attribute	Default Value in Low Latency Networks
macMinBE	3
macMaxBE	3
macMaxCSMABackoffs	0

Table 127.b—Default values for MAC PIB attributes for slotted CSMA-CA in LL-Networks

The backoff slots of *aUnitBackoffPeriod* symbols are aligned with the start of the beacon transmission in management time slots and with tSlotTxOwner in shared group time slots.

7.5.1.5 PA-Slotframe structure

7.5.1.5.1 General

A slotframe is a collection of timeslots repeating in time. The number of timeslots in a given slotframe (slotframe size) determines how often each timeslot repeats, thus setting a communication schedule for nodes that use the timeslots. When a slotframe is created, it is associated with a slotframe ID for identification. Every new slotframe instance in time is called a slotframe cycle. Figure 107.c shows how nodes may communicate in a sample three-timeslot slotframe. Nodes A and B communicate during timeslot 0, nodes B and C communicate during timeslot 1, and timeslot 2 is not being used. Every three timeslots, the schedule repeats. The total number of timeslots that has elapsed since the start of the network is called the Absolute Slot Number (ASN). The pairwise assignment of a directed communication between devices in a given timeslot on a given channel offset is a link. Logical channel selection in a link is made by taking (Absolute Slot Number + channel offset) % Number of channels. Mapping of logical channel to physical channel is to be jointly defined with Channel Hopping/Channel Diversity subgroup

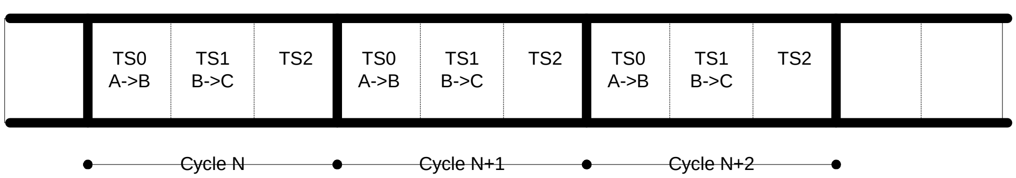


Figure 107.c—Example of a three-timeslot slotframe

Several performance parameters are determined by slotframe size and how timeslots are assigned within a slotframe for communication. In general, shorter slotframes result in lower latency and increased bandwidth, but at the expense of increased power consumption. Long slotframes generally result in higher latency and lower bandwidth, but power consumption is reduced and the number of communication resources (links) is increased. This affects the scale of the network.

7.5.1.5.2 Multiple slotframes

A given network using timeslot-based access may contain several concurrent slotframes of different sizes. Slotframe size defines the bandwidth of a timeslot. A timeslot within a slotframe of a particular size repeats twice as fast as a timeslot within a slotframe that is twice as long, thus allowing for double throughput on any given link. Multiple slotframes may be used to define a different communication schedule for various groups of nodes or to run the entire network at different duty cycles.

A network device may participate in one or more slotframes simultaneously, and not all devices need to participate in all slotframes. By configuring a network device to participate in multiple overlapping slotframes of different sizes, it is possible to establish different communication schedules and connectivity matrices that all work at the same time.

Slotframes can be added, removed, and modified while the network is running. Even though this is the case, all slotframes logically start in the same place in time. Cycle 0, timeslot 0 of every slotframe occurs at the beginning of epoch, which is determined by the network device that starts the network. Because of this, timeslots in different slotframes are always aligned, even though beginnings and ends of slotframes may not be (see Figure 107.d). Because all slotframes begin at the same time, it is always possible to identify time of a given slotframe cycle and timeslot, and ASN is the same across slotframes.

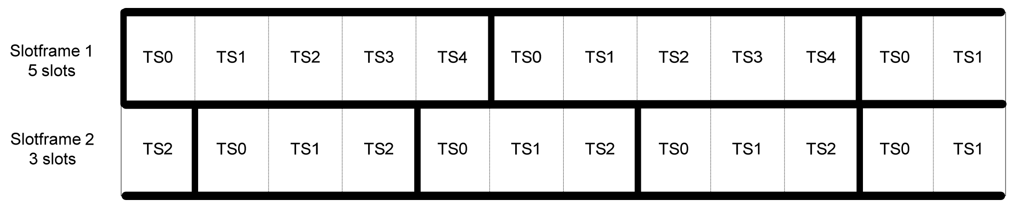


Figure 107.d—Multiple slotframes in the network

7.5.2 Starting and maintaining PANs

7.5.2.5 Device discovery

Insert before 7.5.3 the following subclause.

7.5.2.6 TSCH network formation

7.5.2.6.1 Overview

There are two components of network formation in the TSCH network:

- advertising and
- joining.

As a part of advertising, network devices that are already part of the network may send command frames announcing the presence of the network. Advertisement command frames include time synchronization information and a unique PAN ID. A new device trying to join listens for the Advertisement command frames. If the device is pre-provisioned with a PAN ID, then it matches the advertised PAN ID with the provisioned one at the higher layer. If there is no provisioned PAN ID, the device does not look for a match. When at least one acceptable Advertisement command frame is received, the new device can attempt to join the network. A new device joins the network by sending a Join request command frame to an advertising node. In a centralized management system this join command is routed to the PAN coordinator. In a distributed management system it can be processed locally. When the device is accepted into the network, the advertiser activates the device by setting up slotframes and links between the new device and other existing devices. These slotframes and links can also be deleted and modified and new slotframes and links added any time after a device has joined the network. The sequence of messages exchanged to synchronize a device to the networks is shown in Figure 107.a. The join sequence is shown in Figure 107.b.

A new network starts when the PAN coordinator starts to advertise (typically at the request of Network Manager residing in the PAN coordinator). Being the first node in the network, the PAN coordinator starts at least one slotframe, to which other network devices may later synchronize.

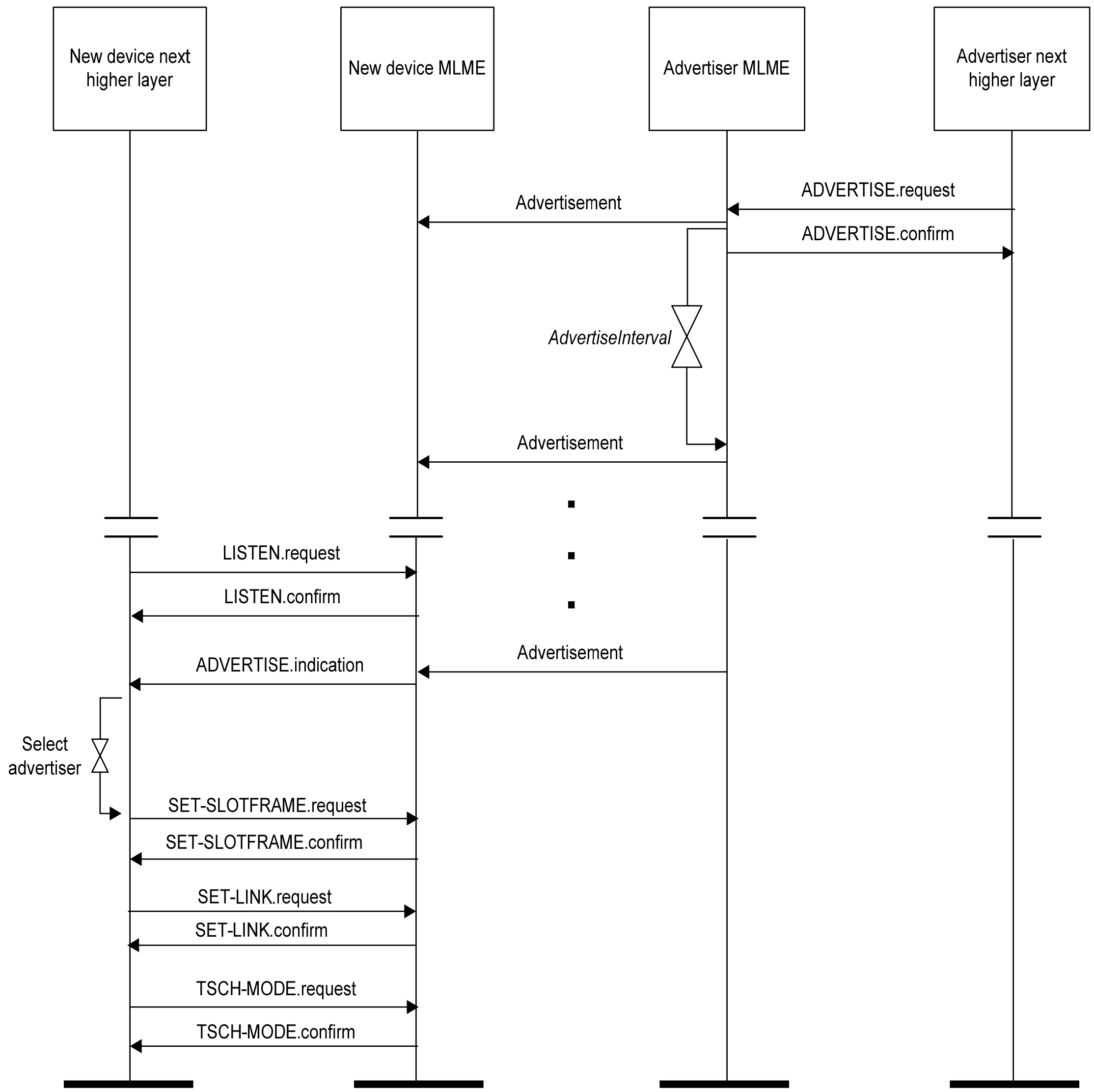


Figure 107.a—Message sequence chart for TSCH procedure to find an advertising device

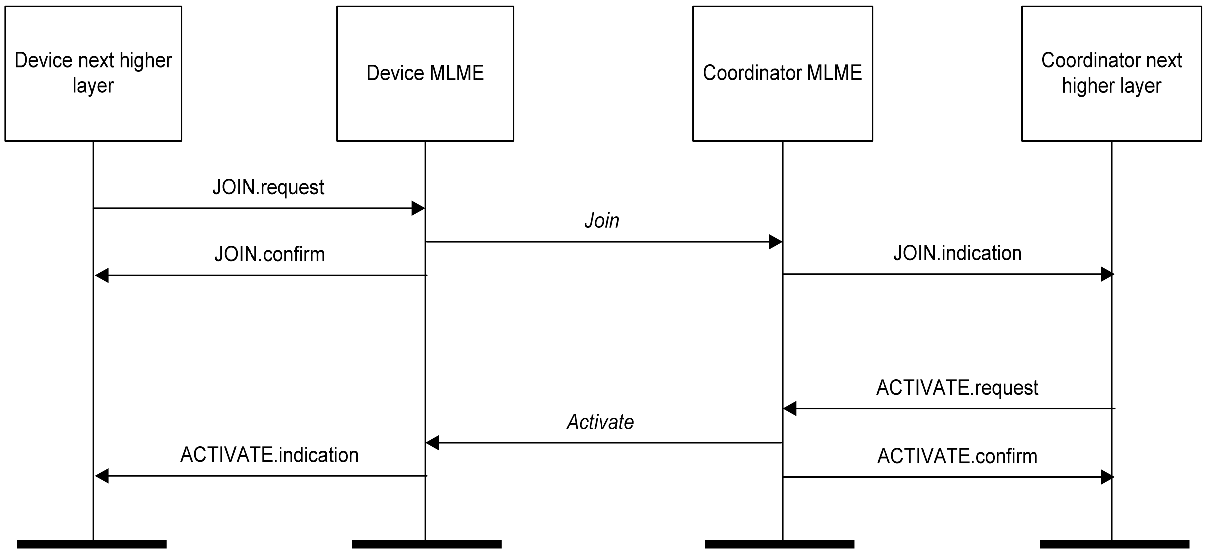


Figure 107.b—Message sequence chart for join and activate procedures

7.5.2.6.2 Advertising

In order for new devices to join a network they must first learn network information from some devices that are already part of the network. This is done through advertising. Network devices may send Advertisement command frames to invite new devices into the network. This is shown in Figure 107.a. The advertising device begins advertising on receipt of a ADVERTISE.request command from its NHL (next higher layer). At some time the device wishing to join the network begins listening (as result of receiving a LISTEN.request from its NHL). Once the listening device has heard an advertisement, it will generate an ADVERTISE.indication to a higher layer. The higher layer may initialize the slotframe and links contained in the advertisement and switch the device into TSCH mode with a TSCH-MODE.request or wait for additional ADVERTISE.indications before doing so. At this point the device is synchronized to the network and may send in a Join request.

Advertisement command frames contain the following information:

- PAN ID.
- Time information so new devices can synchronize to the network.
- Channel page and a list of RF channels in that channel page being used.
- Link and slotframe information so new devices know when they can transmit to the advertising device.
- Link and slotframe information so new devices know when to listen for transmits from the advertising network device.

7.5.2.6.3 Joining

After a new device hears at least one valid Advertisement command frame, it may synchronize to the network and start joining. Advertisement command frames contain information about the links through which the new device may communicate with the advertising neighbor, and through it forward frames to the Network Manager. The joining procedure may include a security handshake to mutually authenticate the joining device and the Network Manager and establish the secure session between the new device and the Network Manager in addition to allocating the communication resource to the joining device. The content of authentication messages is beyond the scope of this document.

The joining process is shown in Figure 107.b. The joining device sends in a join message which contains its identity, capability and security information, and a list of potential neighbors heard during listening. The advertising device that receives this join request may process it locally or send it to a Network manager. If the device is to be allowed into the network, then an activate command is sent containing some slotframes and links that the device may use to communicate to its neighbors, which may or may not be the neighbor to whom the join request was sent. After receiving the activate command, the device may be instructed to remove slotframes and links obtained from advertisements. The device may receive additional slotframes and links from a Network Manager or peer as required by the application.

7.5.3 Association and disassociation

7.5.4 Synchronization

Insert before 7.5.4.1 the following paragraph.

For PA, Subclause 7.5.4 specifies in addition the procedures for coordinators to generate beacon frames for devices to synchronize to the TSCH network. For PANs not supporting beacons, synchronization is performed by time synchronized communication within a timeslot of the slotframe.

7.5.4.1 Synchronization with beacons

Insert before 7.5.5 the following subclauses.

7.5.4.4 Synchronization in TSCH network

7.5.4.4.1 Timeslot communication

During a timeslot in a slotframe, one node typically sends a frame, and another sends back an acknowledgement if it successfully receives that frame. An acknowledgement can be positive (ACK) or negative (NACK). A positive acknowledge indicates that the receiver has successfully received the frame and has taken ownership of it for further routing. A negative acknowledgement indicates that the receiver cannot accept the frame at this time, but has heard it with no errors. Both ACKs and NACKs carry timing information used by nodes to maintain network synchronization. Frames sent to a unicast node address require that a link-layer acknowledgement be sent in response during the same timeslot as shown in Figure 107.c. If an acknowledgement is requested and not received within the timeout period, retransmission of the frame waits until the next assigned transmit timeslot (in any active slotframe) to that address occurs.

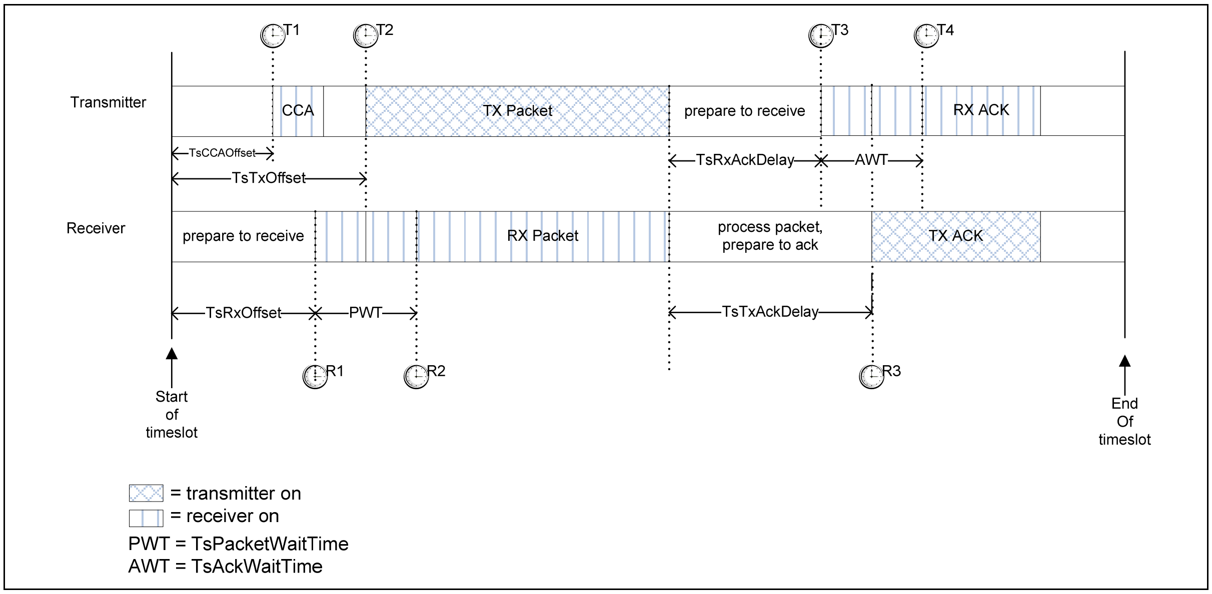


Figure 107.c—Timeslot diagram of acknowledged transmission

As shown in Figure 107.c, the timeslot starts at time T=0 from the transmitting device’s perspective. The transmitter waits TsCCAOffset µs, and then performs CCA (if active). At TsTxOffset µs, the device begins transmitting the packet. The transmitter then waits TsRxAckDelay µs, then goes into receive mode to await the acknowledgement. If the acknowledgement doesn't arrive within TsAckWait (AWT) µs the device may idle the radio and that no acknowledgement will arrive.

On the receiver's side, at it's estimate of T=0 it waits TsRxOffset µs and then goes into receive for TsRxWait (PWT) µs. If the frame has not started by that time, it may idle the receiver. Otherwise, once the frame has been received, the receiver waits TsTxAckDelay µs and then sends an acknowledgement.

The transmitter or receiver may resynchronize clocks as described in 7.5.4.4.2.

EXAMPLE:

Below is the calculation of a 10 ms length timeslot template (from the transmitter's perspective):

TsTxOffset	2120 µs
TsMaxPacket	4256 µs
TsRxAckDelay	800 µs
TsAckWait	400 µs
TsMaxAck	2400 µs
Total	9976 µs

This allows for a maximum 133 octet frame (total including all SHR, PHR, MHR, etc.) to be sent, and an acknowledgement of up to 75 octets to be returned within 10 ms.

7.5.4.4.2 Node synchronization

7.5.4.4.2.1 General

Device-to-device synchronization is necessary to maintain connection with neighbors in a slotframe-based network. There are two methods for a device to synchronize to the network.

7.5.4.4.2.2 Acknowledgement-based synchronization

Unicast communication provides a basic method of time synchronization through the exchange of data and acknowledgement frames. The algorithm involves the receiver calculating the delta between the expected time of frame arrival and its actual arrival, and providing that information to the sender node.

The algorithm can be described as follows:

— Transmitter node sends a frame, timing the start symbol to be sent at TsTxOffset.

— Receiver records the timestamp TsRxActual of receiving the start symbol of the packet.

— Receiver calculates TimeAdj = TsTxOffset – TsRxActual.

— Receiver send back TimeAdj as part of acknowledgement packet.

— Transmitter receives the acknowledgement. If the receiver node is a clock source node, the transmitter adjusts its network clock by TimeAdj.

7.5.4.4.2.3 Frame-based synchronization

A node may synchronize its own network clock if it receives a frame from a clock source neighbor. The mechanism is similar to that of ACK-based synchronization. The receiver calculates the delta between expected time of frame arrival and its actual arrival time, and adjusts its own clock by the difference.

The algorithm can be described as follows:

— Receiver records the timestamp *TsRxActual* of receiving the start symbol of the packet.

— Receiver calculates *TimeAdj = TsTxOffset – TsRxActual.*

— Receiver adjusts its own network time by *–TimeAdj.*

Note that this procedure should only be executed if the node from which the frame is received is a clock source for the receiver.

Figure 107.d illustrates both time synchronization mechanisms. In both cases, the receiver calculates TimeAdj to either send back to the transmitter or to use locally.

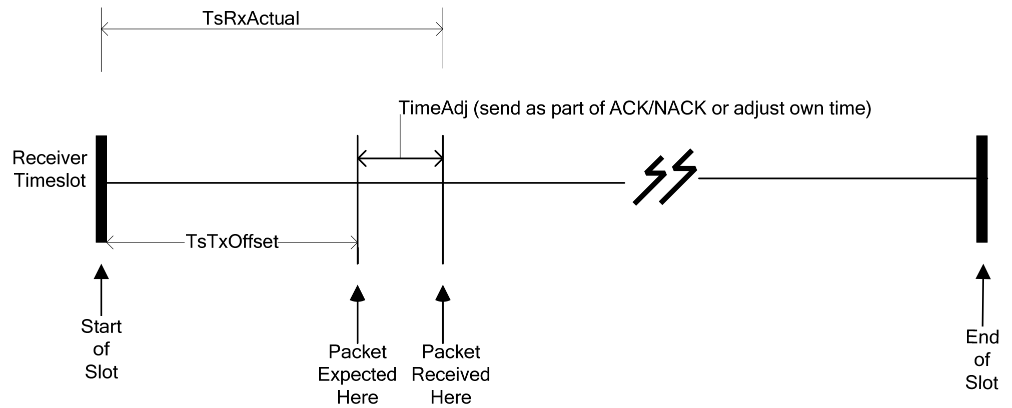


Figure 107.d—Time synchronization

7.5.4.4.2.4 Network time synchronization

Precise time synchronization is critical to the operation of networks based on time division multiplexing. Since all communication happens in timeslots, the network devices must have the same notion of when each timeslot begins and ends, with minimal variation. The acknowledgement and frame-based synchronization are used for pair-wise synchronization, as outlined below. In a typical TSCH network, time propagates outwards from the PAN coordinator. It is very important to maintain unidirectional time propagation and avoid timing loops. A network device must periodically synchronize its network clock to at least one other network device. It may also provide its network time to one or more network devices. A network device determines whether to follow a neighbor's clock based on the presence of a ClockSource flag in the corresponding neighbor's record (configured by the Network Manager). The direction of time propagation is independent of data flow in the network.

A network device may have more than one neighbor as its clock source. In such cases, the device may synchronize its clock to any of the neighbors that are acting as its clock source.

Figure 107.e shows typical time propagation in TSCH network. The arrows indicate the direction of clock distribution. In this example, the PAN coordinator acts as the clock source for the entire network. Network Device (ND) 20 synchronizes to the PAN coordinator only, while ND 22 synchronizes its clock to both ND 20 and ND 21. If ND 20 and ND 23 were to be connected, ND 20 must provide time to ND 23. Setting it up otherwise would create a timing loop.

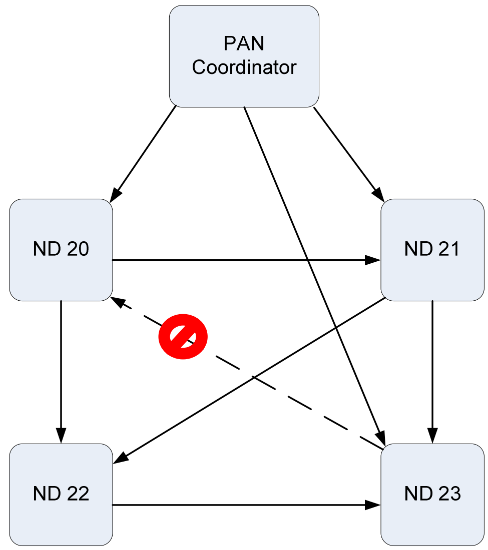


Figure 107.e—Time propagation in TSCH network

7.5.4.4.2.5 Keep-Alive mechanism

In order to ensure that it remains synchronized with the TSCH network (and to detect when paths may be down) a network device shall ensure that it communicates with each of its clock sources at least once per Keep Alive period.

If a network device has not sent a packet to its clock parent within this interval, it shall send a Keep-Alive command frame and use the ACK to perform ACK-based synchronization as usual.

7.5.5 Transaction handling

7.5.6.2 Reception and rejection

Change text in 7.5.6.2.

Each device may choose whether the MAC sublayer is to enable its receiver during idle periods. During these idle periods, the MAC sublayer shall still service transceiver task requests from the next higher layer. A transceiver task shall be defined as a transmission request with acknowledgment reception, if required, or a reception request. On completion of each transceiver task, the MAC sublayer shall request that the PHY enables or disables its receiver, depending on the values of *macBeaconOrder* and *macRxOnWhenIdle*. If *macBeaconOrder* is less than 15, the value of *macRxOnWhenIdle* shall be considered relevant only during idle periods of the CAP of the incoming superframe. If *macBeaconOrder* is equal to 15 or macFAlowLatencyPAN is FALSE, the value of *macRxOnWhenIdle* shall be considered relevant at all times. If macFAlowLatencyPAN is TRUE, the value of macRxOnWhenIdle is not considered relevant.

Due to the nature of radio communications, a device with its receiver enabled will be able to receive and decode transmissions from all devices complying with this standard that are currently operating on the same channel and are in its POS, along with interference from other sources. The MAC sublayer shall, therefore, be able to filter incoming frames and present only the frames that are of interest to the upper layers.

For the first level of filtering, the MAC sublayer shall discard all received frames that do not contain a correct value in their FCS field in the MFR (see 7.2.1.9 and 7.2.5.1.4). The FCS field shall be verified on reception by recalculating the purported FCS over the MHR and MAC payload of the received frame and by subsequently comparing this value with the received FCS field. The FCS field of the received frame shall be considered to be correct if these values are the same and incorrect otherwise.

The second level of filtering shall be dependent on whether the MAC sublayer is currently operating in promiscuous mode. In promiscuous mode, the MAC sublayer shall pass all frames received after the first filter directly to the upper layers without applying any more filtering or processing. The MAC sublayer shall be in promiscuous mode if *macPromiscuousMode* is set to TRUE.

If the MAC sublayer is not in promiscuous mode (i.e., *macPromiscuousMode* is set to FALSE), it shall accept only frames that satisfy all of the following third-level filtering requirements:

— The Frame Type subfield shall not contain a reserved frame type.

— The Frame Version subfield shall not contain a reserved value.

— If a destination PAN identifier is included in the frame, it shall match *macPANId* or shall be the broadcast PAN identifier (0xffff).

— If a short destination address is included in the frame, it shall match either *macShortAddress*, macVeryShortAddress, or the broadcast address (0xffff). Otherwise, if an extended destination address is included in the frame, it shall match *aExtendedAddress*.

— If the frame type indicates that the frame is a beacon frame (frame type b000), the source PAN identifier shall match *macPANId* unless *macPANId* is equal to 0xffff, in which case the beacon frame shall be accepted regardless of the source PAN identifier. If the frame type indicates that the frame is a beacon frame of an LLNW (frame type b100, subframe type b00) and indicates online mode, the Gateway ID field shall match macFAlowLatencyNWid.

— If only source addressing fields are included in a data or MAC command frame, the frame shall be accepted only if the device is the PAN coordinator and the source PAN identifier matches macPANId.

If any of the third-level filtering requirements are not satisfied, the MAC sublayer shall discard the incoming frame without processing it further. If all of the third-level filtering requirements are satisfied, the frame shall be considered valid and processed further. For valid frames that are not broadcast, if the Frame Type subfield indicates a data or MAC command frame and the Acknowledgment Request subfield of the Frame Control field is set to one, the MAC sublayer shall send an acknowledgment frame. Prior to the transmission of the acknowledgment frame, the sequence number included in the received data or MAC command frame shall be copied into the Sequence Number field of the acknowledgment frame. This step will allow the transaction originator to know that it has received the appropriate acknowledgment frame.

If the PAN ID Compression subfield of the Frame Control field is set to one and both destination and source addressing information is included in the frame, the MAC sublayer shall assume that the omitted Source PAN Identifier field is identical to the Destination PAN Identifier field.

The device shall process the frame using the incoming frame security procedure described in 7.5.9.2.3.

If the status from the incoming frame security procedure is not SUCCESS, the MLME shall issue the corresponding confirm or MLME-COMM-STATUS.indication primitive with the status parameter set to the status from the incoming frame security procedure, indicating the error, and with the security-related parameters set to the corresponding parameters returned by the unsecuring process.

If the valid frame is a data frame, the MAC sublayer shall pass the frame to the next higher layer. This is achieved by issuing the MCPS-DATA.indication primitive containing the frame information. The securityrelated parameters of the MCPS-DATA.indication primitive shall be set to the corresponding parameters returned by the unsecuring process.

If the valid frame is a MAC command or beacon frame, it shall be processed by the MAC sublayer accordingly, and a corresponding confirm or indication primitive may be sent to the next higher layer. The security-related parameters of the corresponding confirm or indication primitive shall be set to the corresponding parameters returned by the unsecuring process.

7.5.6.4.2 Acknowledgment

Insert before 7.5.6.4.3 the following paragraph.

When operating in TSCH mode (see 7.1.21.3), the acknowledgement frame is sent at the time specified by the macTimeslotTemplate being used (see 7.4.2 and 7.5.4.4.1).

7.5.6.4.3 Retransmissions

Insert after the heading of 7.5.6.4.3 the following subclause.

7.5.6.4.3.1 General

Insert before 7.5.6.5 the following subclause.

7.5.6.4.3.2 PA-Retransmissions

A device that sends a data or MAC command frame with its Acknowledgment Request subfield set to one shall wait for TsRxAckDelay µs. If an acknowledgment frame is received within macAckWaitDuration symbols and contains the same DSN as the original transmission, the transmission is considered successful, and no further action regarding retransmission shall be taken by the device. If an acknowledgment is not received within the appropriate timeout or an acknowledgment is received containing a DSN that was not the same as the original transmission, the device shall conclude that the single transmission attempt has failed.

If a single transmission attempt has failed and the transmission was indirect, the coordinator shall not retransmit the data or MAC command frame. Instead, the frame shall remain in the transaction queue of the coordinator and can only be extracted following the reception of a new data request command. If a new data request command is received, the originating device shall transmit the frame using the same DSN as was used in the original transmission.

If a single transmission attempt has failed and the transmission was direct, the device shall repeat the process of transmitting the data or MAC command frame and waiting for the acknowledgment, up to a maximum of macMaxFrameRetries times. The retransmitted frame shall contain the same DSN as was used in the original transmission. Each retransmission shall only be attempted if it can be completed within the same portion of the superframe, i.e., the CAP or a GTS in which the original transmission was attempted. If this timing is not possible, the retransmission shall be deferred until the same portion in the next superframe. In TSCH mode (see 7.1.21.3), retransmissions only occur on subsequent transmit links to the same recipient on any active slotframe. If an acknowledgment is still not received after macMaxFrameRetries retransmissions, the MAC sublayer shall assume the transmission has failed and notify the next higher layer of the failure.

7.5.6.5 Promiscuous mode

7.5.7 GTS allocation and management

7.5.7.6 GTS expiration

Insert before 7.5.8 the following subclauses.

7.5.7.7 LL-Transmission Modes in star networks using short MAC headers

7.5.7.7.1 General

The transitions between the different transmission modes are illustrated in Figure 111.a.

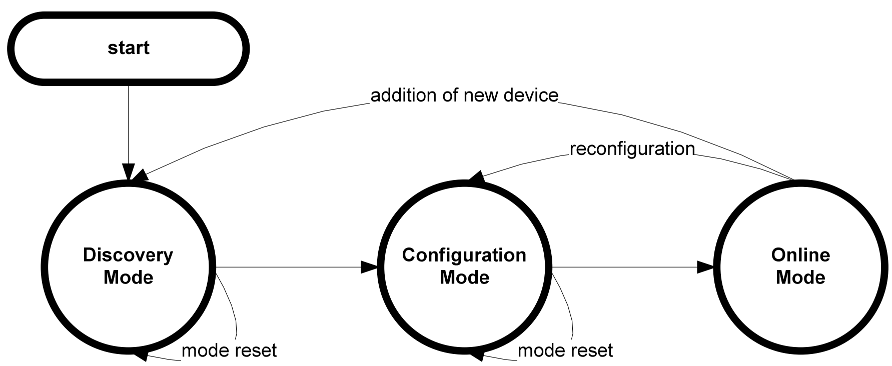


Figure 111.a—Transitions between transmission modes

The discovery mode is the first step during network setup: the new devices are discovered and configured in the second step, the configuration mode. After the successful completion of the configuration mode, the network can go into online mode. Productivity data, that is, data and readings from the devices such as sensors and actuators, can only be transmitted during online modus. In order to reconfigure a network, the configuration mode can be started again.

7.5.7.7.1.1 Discovery Mode

The Discovery Mode is the first step during network setup or for the addition of new devices to an existing network.

In discovery mode, the superframe contains only the time slot for the beacon (cf. 7.5.1.1a.2) and two management time slots, one downlink and one uplink (cf. 7.5.1.1a.3).

A new device scans the different channels until it detects a gateway sending beacons that indicate discovery mode.

If a new device received a beacon indicating discovery mode, it tries to get access to the transmission medium in the uplink management time slot in order to send a Discover Response frame to the gateway. The Discover Response frame is described in 7.3.10. The Discover Response frame contains the current configuration of the device. The new device shall repeat sending the Discover Response frame until it receives an Acknowledgement frame for it or the Discovery Mode is stopped by the gateway. The Acknowledgement frame is described in 7.2.2a.3.

Figure 111.b illustrates the discovery mode.

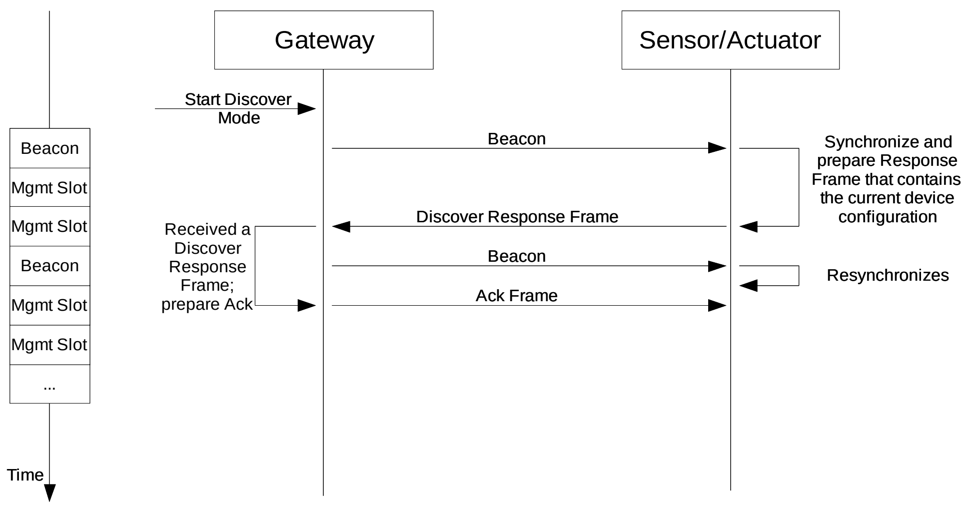


Figure 111.b—Flow diagram of Discovery Mode

7.5.7.7.1.2 Configuration Mode

The Configuration Mode is the second step during network setup. It is also used for network reconfiguration.

In configuration mode, the superframe contains only the time slot for the beacon (cf. 7.5.1.1a.2) and two management time slots, one downlink and one uplink (cf. 7.5.1.1a.3).

If a device received a beacon indicating configuration mode, it tries to get access to the transmission medium in the uplink management time slot in order to send a Configuration Response frame to the gateway. The Configuration Response frame is described in 7.3.11. The Configuration Response frame contains the current configuration of the device. The new device shall repeat sending the Configuration Response frame until it receives a Configuration Request frame for it or the Configuration Mode is stopped by the gateway. The Configuration Request frame is described in 7.3.12. The Configuration Request frame contains the new configuration for the receiving device. After successfully receiving the Configuration Request frame, the device sends an Acknowledgement frame to the gateway. The Acknowledgement frame is described in 7.2.2a.3.

Figure 111.c illustrates the configuration mode.

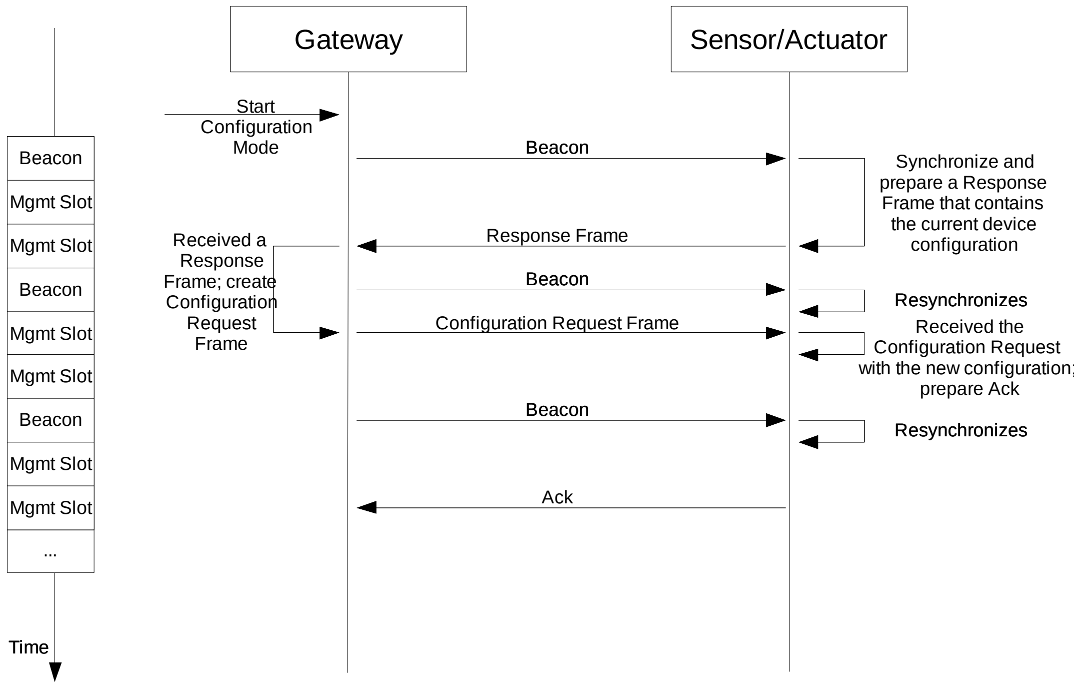


Figure 111.c—Flow diagram of configuration mode

7.5.7.7.1.3 Online Mode

User data is only sent during Online mode. The superframe starts with a beacon and is followed by several time slots. The devices can sent their data during the time slots assigned to them during configuration mode. The different types of time slots are described in clause 5.

The existence and length of management time slots in online mode is signalled in the configuration request frame.

The successful reception of data frames by the gateway is acknowledged in the Group Acknowledgement bitmap of the beacon frame of the next superframe (cf. 7.2.2a.1.2) or in a separate Data Group Acknowledgement frame (cf. 7.2.2a.3.4) if so configured. This is the case for both sensor time slots and actuator time slots if the actuator direction is uplink. Figure 111.d illustrates an example of the online mode for uplink transmissions. The network has 3 dedicated time slots, and sensor 2 is assigned to time slot 2.

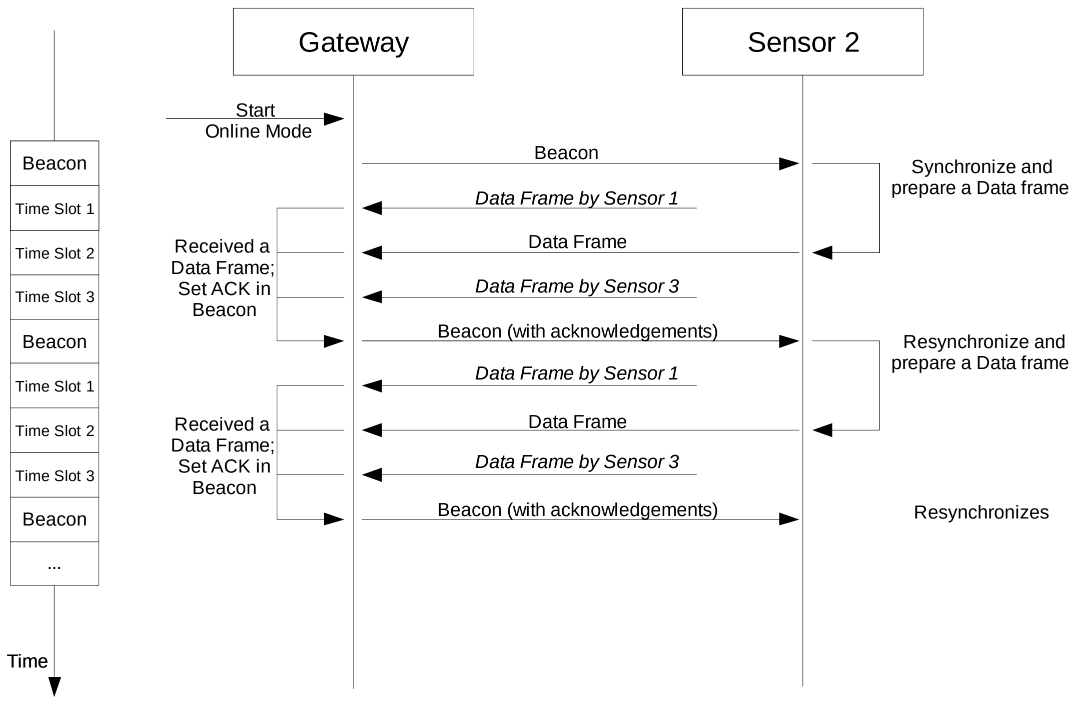


Figure 111.d—Flow diagram of online mode for sensor devices

If retransmission time slots are configured (*macFAnumRetransmitTS* > 0), the retransmission slots are assigned to the owners of the first *macFAnumRetransmitTS* with the corresponding bit in the group acknowledgement bitmap set to 0. Each sensor node has to execute the following algorithm in order to determine its retransmission time slot *r*. The gateway has to execute a similar algorithm in order to determine the senders of the frames in the retransmission slots.

Assume that the sensor node has been assigned to sensor time slot *s*. ack[i] means the bit b_{i-1} in the group acknowledgment bitmap according to Figure 93.l in 7.2.5.2.2.3.

```
if (ack[s] == false) {
            num_failed   :=   number   of   (ack[i]   ==   0   with
(macFAnumRetransmitTS+1) ≤ i ≤ (s-1))
            if (num_failed < macFAnumRetransmitTS) {
                        retransmission_possible = true
                        r = num_failed + 1
            }
            else {
                        retransmission_possible = false
            }
}
```

The successful reception of data frames by actuator devices (actuator direction is downlink) is acknowledged by an explicit acknowledgement frame by the corresponding actuator devices in the following superframe. This means that after setting the actuator direction bit in the beacon (cf. 7.2.2a.1.2) to downlink and sending a data frame to one or more actuator devices, the gateway shall set the actuator direction bit to uplink in the directly following superframe. Actuator devices having successfully received a data frame from the gateway during the previous superframe shall sent an acknowledgement frame to the gateway. Actuator devices that did not receive a data frame from the gateway, may send data frames to the gateway during this superframe with actuator direction bit set to uplink. Figure 111.e illustrates the online mode with actuator devices. The network has 3 dedicated actuator time slots, and actuator 2 is assigned to time slot 2.

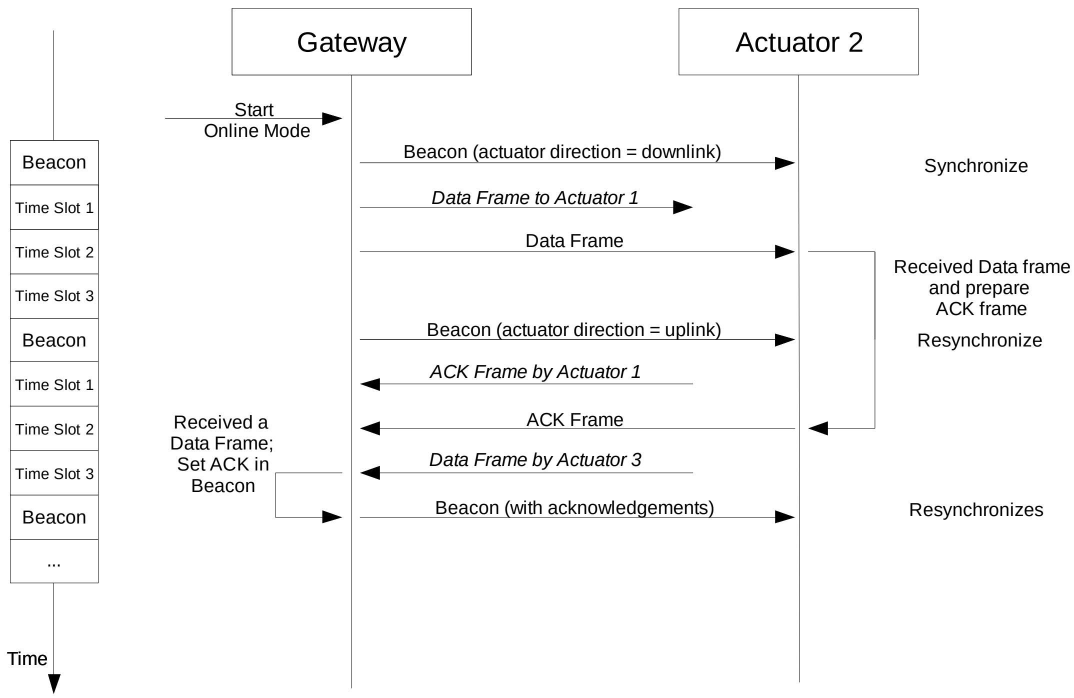


Figure 111.e—Flow diagram of online mode for actuator devices

7.5.8 Ranging

7.6 Security suite specifications

7.7 Message sequence charts illustrating MAC-PHY interaction

Annex A
(normative)

Service-specific convergence sublayer (SSCS)

Annex B
(normative)

CCM* mode of operation

Annex C
(informative)

Test vectors for cryptographic building blocks

Annex D
(normative)

Protocol implementation conformance statement (PICS) proforma

Annex E
(informative)

Location topics

Annex F
(informative)

Coexistence with other IEEE standards and proposed standards

Annex G
(informative)

Regulatory requirements

Annex H
(informative)

UWB PHY optional chaotic pulses

Annex I
(informative)

Example UWB PHY transmit data frame encoding

Annex J
(informative)

MPSK PHY requirements

Annex K
(informative)

Considerations for 950 MHz band

Annex L
(informative)

Bibliography

L.1 Documents for MAC enhancements in support of LL-applications

— 15-09/0254r0 Proposal for Factory Automation presentation of proposal for factory automation at March 09 IEEE 802.15.4e meeting

— 15-08/0827r0 Shared Group Timeslots presentation with further details on Shared Group Timeslots

— 15-09/0228r0 Proposal for Factory Automation text of proposal for factory automation at March 09 IEEE 802.15.4e meeting

— 15-08/0420r2 Extending the MAC Superframe of 802.15.4 Spec presentation with separate GACK mechanism

— 15-08/0503r0 Preliminary Proposal for Factory Automation presentation of preliminary proposal for factory automation at July 08 IEEE 802.15.4e meeting

— 15-08/0571r1 Proposal for Factory Automation presentation of proposal for factory automation at September/November 08 IEEE 802.15.4e meetings

— 15-08/0572r0 Proposal for Factory Automation text of proposal for factory automation at September 08 IEEE 802.15.4e meeting

Annex M
(informative)

Requirements of indistrial and other application domains

M.1 General

The intentions of these add-ons are to enhance and add functionality to the 802.15.4-2009 MAC to

a) better support the industrial markets and
b) permit compatibility with modifications being proposed within the Chinese WPAN.

This functionality will facilitate industrial applications (such as addressed by IEC 62591 and the ISA100.11a), and those enhancements defined by the Chinese WPAN standard that aren't included in the Amendment of TG4c.

Industrial applications have requirements that are not addressed by the edition 2009 such as low latency, robustness in the harsh industrial RF environment, and determinism.

The Chinese Wireless Personal Area Network (CWPAN) standard has identified enhancements to improve network reliability and increase network throughput to support higher duty-cycle data communication applications.

This amendment addresses coexistence with wireless protocols such as 802.11, 802.15.1, 802.15.3, and 802.15.4.

Specifically, the MAC enhancements are grouped into two categories:

a) Industrial and other application domains and
b) Additional functional improvements.

To identify easier the specific amendments to which category these apply in the normative clauses, the specific subclauses are named with the following acronyms in the order as they appear here.

a) Process automation (PA),
b) Low latency networks (LL)
c) Commercial (C)
d) ?Smart utility networks (SUN)? (reserved for future requests)
e) ?(RFID)? (reserved for future requests)

The question marks will disappear in the final version. These marked topics are potential candidates, but it is not decided nor limited to those.

Additional functional improvements are:

a) Low Energy (LE)
b) ?Overhead reduction/Security(ORS)? (reserved for future submissions)

The question marks will disappear in the final version. These marked topics are potential candidates, but it is not decided nor limited to those.

The convention as used in Clause 7 is that same headings needed for different solutions based on different requirements have a prefix as the given acronyms above to differentiate the subclauses.

EXAMPLES;

- — PA-Heading
- — LL-Heading
- — C-Heading

M.2 Process automation (PA)

Typical parts of the application domain of process automation are facilities for

- — Oil & gas industry,
- — Food & beverage products,
- — Chemical products
- — Pharmacutical products
- — Water/waist water treatnments
- — etc.

For this application domain exists the following major requirements:

- — IEEE 802.15.4 header extensions for mesh support
    - Additional addresses (source, destination)
    - Sequence number
    - TTL („transmissions to live“)
- — Framework for chosing path selection mechanisms
    - Path selection protocol
    - Link metrics

M.3 Low latency networks (LL)

M.3.1 Typical application domains for LL-networks

Typical parts of the application domain of low latency networks are facilities for

- — Factory automation as for automotive manufacturing
- — Robots
- — Suspension tracks

- Portable machine tools
- Milling, turning
- Robot revolver
- Filling
- Cargo
- Airport logistics
- Post
- Packaging industry
- Special engineering
- Conveyor technique
- etc.

For this application domain exists the following major requirements:

- High determinism
- High reliability
- Low latency:
    - transmission of sensor data in □ 10 ms
    - low round-trip time
- Many sensors per gateway
    - might be more than 100 sensors per gateway
- Assume controlled envi-ronment (factory floor)
- Configuration for optimal performance
- Network management and frequency planning for avoidance of co-existence issues.
- Roaming capability (no channel hopping)

M.3.2 Application overview

Factory automation comprises today a large number of sensors and actuators observing and controlling the production. Sensors and actuators are located for example at robots, suspension tracks and portable tools in the automotive industry, collect data on machine tools, such as milling or turning machines and control revolving robots. Further application areas are control of conveyor belts in cargo and logistics scenarios or special engineering machines. Depending on the specific needs of different factory automation branches many more examples could be named.

Common to these sensor applications in factory automation context is the requirement of low latency and high cyclic determinism. The performance should allow for reading sensor data from 20 sensors within 10ms.

Cabling these sensors is very time consuming and expensive. Furthermore, cables are a frequent source for failures due to the harsh environment in a factory and may cause additional costs by production outage.

Wireless access to sensors and actuators solves the cabling issue and provides also advantages in case of mobility and retrofit situations.

Wireless technologies that could be applied for the factory automation scenario include 802.11 (WLAN), 802.15.1 (Bluetooth) and 802.15.4. 804.15.4 is designed for sensor applications and offers the lowest energy consumption as well as the required communication range and capacity. Moreover, four 802.15.4 channels can be utilized in good coexistence with three non-overlapping WLAN channels (cf. **Error! Reference source not found.**). Bluetooth offers good realtime capabilities, but interferes inevitably with any existing WLAN installations.

802.15.4 is a worldwide and successfully applied standard for wireless and low power transmission of sensor data. Different protocols on top of 802.15.4 (WirelessHART™ according to IEC 62591, ISA100 or ZigBee) in the context of process automation are already in the process of standardization. Those protocols aim at different requirements, but employ the same physical layer hardware as the proposed solution for factory automation, which indicates potential hardware synergies and cost savings. Thus, a solution for factory automation based on 802.15.4 would be beneficial.

802.15.4 operates usually in Carrier Sense Multiple Access (CSMA) mode which gives no guarantees for media access. Optionally, 802.15.4 specifies the beacon-enabled mode which defines a TDMA like superframe structure with Guaranteed Time Slots (GTS) for deterministic access. The performance of 7 GTS in an interval of 15ms does not fulfill the factory automation requirements and makes not full use of the available capacity. Therefore a modification of the 802.15.4 MAC for application in industrial factory automation, i.e. defining a fine granular deterministic TDMA access, is envisaged.

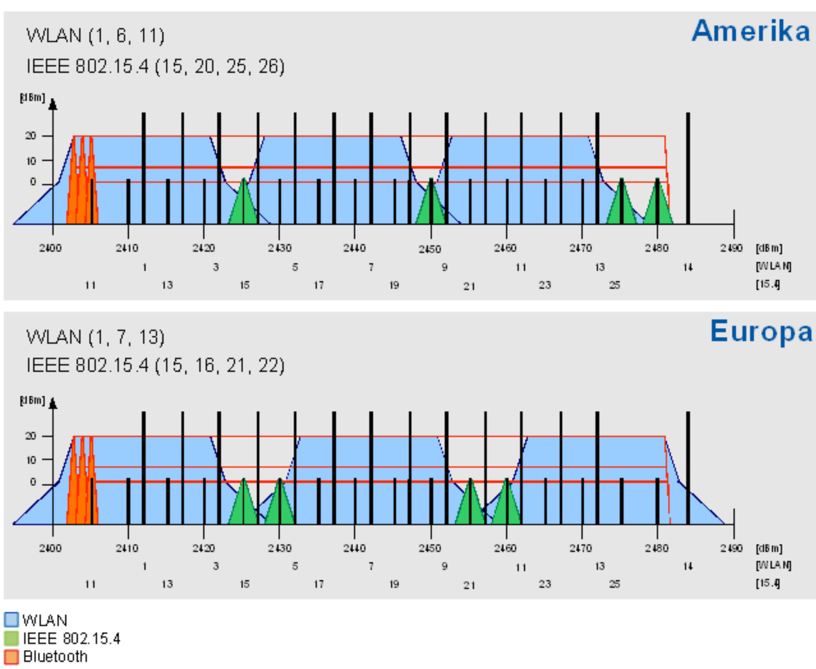


Figure M.1—RF technology coexistence in the 2.4GHz ISM band.

M.3.3 Requirements and Assumptions

The above mentioned factory automation applications impose the following requirements to a wireless system:

- high determinism,
- high reliability,
- low latency, i.e. transmission of sensor date in ≤ 10ms,
- low round trip time,
- support for many sensors per gateway.

The proposed TDMA scheme, as described in the remainder of this document, supports these requirements. Allocating a dedicated time slot for each sensor provides a deterministic system. The 802.15.4 DSSS coding together with the exclusive channel access for each sensor ensures high reliability of the system. Small time slots and short packets lead to superframes as small as 10ms, which provides a latency of less than 10ms and a low round trip time. The number of slots in a superframe determines the number of sensors that can access each channel. By operating the gateway with multiple transceivers on different channels, a high number of sensors is supported.

The proposed system needs to be operated in a controlled configuration to achieve the required performance. Thus, it is assumed that the system is operated in a controlled environment with frequency planning. The TDMA channels are allocated in a way that.

M.4 Commercial (C)

Typical parts of the application domain of commercial networks are facilities for

- etc.

For this application domain exists the following major requirements:

- ...

M.5 Low energy (LE)

For this general improvement....

M.6 Channel Diversity

Annex M.6 provides tutorial material for a better understanding for the different solutions specified in Clauses 7.