UG235.02: Using Silicon Labs Connect with IEEE 802.15.4

This chapter of the *Connect User's Guide* describes how to use the Silicon Labs Connect stack with IEEE 802.15.4. The *Connect User's Guide* assumes that you have already installed the Simplicity Studio development environment and the Flex SDK, and that you are familiar with the basics of configuring, compiling, and flashing Connect-based applications. Refer to *UG235.01: Developing Code with Silicon Labs Connect* for an overview of the chapters in the *Connect User's Guide*.

KEY POINTS

- Introduction to common terms used in IEEE 802.15.4
- IEEE 802.15.4 frame formats
- IEEE 802.15.4 security
- Common processes in IEEE 802.15.4

The *Connect User's Guide* is a series of documents that provides in-depth information for developers who are using the Silicon Labs Connect Stack for their application development. If you are new to Connect and the Flex SDK, see *QSG138: Getting Started with the Silicon Labs Flex Software Development Kit for the Wireless Gecko (EFR32™) Portfolio*.

Connect is supported for EFR32FG, EFR32MG1x, and EFR32BG1x.

1 Introduction

Silicon Labs Connect is based on the IEEE 802.15.4-2011 standard (abbreviated to IEEE 802.15.4). Therefore, to understand the Silicon Labs Connect stack, you also need a basic knowledge of 802.15.4 which defines various Physical and Media Access Control layers that are designed for low-data rate, low-power, and low-complexity, short-range communications in Personal Area Networks. IEEE 802.15.4 is also the basis of mesh network protocols such as Zigbee® or Thread.

This document provides a short introduction to the IEEE 802.15.4 features that are used in Connect so you can understand its MAC layer without having to read the IEEE 802.15.4 specification.

For more information about IEEE 802.15.4, see http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf.

2 Basic Terms

It is important to define some common terms before delving into the technical details.

2.1 Physical Layer

The Physical (PHY) layer is the lowest layer in a communication stack. It is responsible for the transmission of unstructured data through a medium. In a wireless networking stack, the PHY defines the modulation, bit rate, and parts of the frame that are required for successful data reception (for example, the preamble and sync word).

2.2 Data Link Layer

The Data Link Layer (DLL) is built on top of the PHY in a communication stack. It is responsible for reliable data transfer between two devices (for example, addressing, acknowledgement and integrity checks). In IEEE 802 protocols, the DLL is built up from two layers. The lower one is called the Media Access Control (MAC) layer. Because IEEE 802.15.4 does not have the upper DLL, the MAC layer is interchangeable with DLL.

2.3 Personal Area Network

A Personal Area Network (PAN) is a logical group of devices that can communicate with each other. Protocols built on IEEE 802.15.4 usually communicate inside a PAN.

2.4 PAN coordinator

The PAN coordinator can perform special services in some protocols (for example, allocating short addresses).

2.5 Intra-PAN message

An intra-PAN message is one where the source and destination device are in the same PAN.

2.6 Inter-PAN message

An inter-PAN message is one where the source and destination device are in different PANs.

2.7 Long Address

A long address is a globally unique 64-bit address (EUI64). Each Silicon Labs Wireless Gecko is assigned an EUI64 address at the factory. This is standardized across most IEEE 802 protocols (for example, IPv6 uses the same EUI64 as the MAC address).

2.8 Short Address

A short address is a 16-bit address that is only unique in a PAN. Because IEEE 802.15.4 has a fairly short frame, using long addresses would consume a lot of the frame. Therefore, devices can use short addresses if they also know the PAN ID. 0xFFFE is a reserved special address, which means the device is in the PAN, but does not have a source address and it should use its long address to communicate.

2.9 PAN ID

A PAN ID is a 16-bit long address that identifies a PAN. There is no standardized way to allocate PAN IDs so the application should make sure to use a PAN ID that is not used in the same network.

2.10 Broadcast Address

A broadcast address is special address that should be received by any device. The 0xFFFF short address is the broadcast short address. The 0xFFFF PAN ID is the broadcast PAN ID.

2.11 CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a "listen-before-talk" protocol: To avoid collisions, the radio listens to a channel before transmission. If the channel is "free" (that is, nothing was received), the device can transmit. If the channel is "busy" (that is, something was received), the device waits before trying again. After a certain number of retries, the transmit will fail and an error will be reported to the application.

2.12 Message Integrity Check

Message Integrity Check is used for data authentication: Only the real sender can calculate the MIC of a frame.

3 Frame Format

IEEE 802.15.4 specifies every field in the frame that are used in Silicon Labs Connect as Least Significant Bit (LSB) first.

3.1 Physical Protocol Data Unit (PPDU)

		Octets		
		1		variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

Figure 3-1. Format of the PPDU

- SHR: Synchronization Header
  - Preamble: Required for bit synchronization (clock recovery) on the receiver.
  - SFD: Start of Frame Delimiter (often called sync word)—required for byte synchronization on the receiver.
- PHR: Physical Header
  - Frame Length: the length of the PSDU—because it is 7 bits, this limits the PSDU size to be a maximum of 127 bytes.

    Note: IEEE 802.15.4-2015 defines a different, 16-bit PHR with an 11-bit length field. Silicon Labs Connect does not currently support this format.
- PHY Payload
  - PSDU (Physical Service Data Unit): The payload of the Physical Protocol Data Unit (PPDU).

3.2 MAC Protocol Data Unit (MPDU)

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing fields						
MHR							MAC Payload	MFR

Figure 3-2. General MAC Frame Format

- MHR: MAC Header
  - Frame Control Field (FCF): see Section 3.2.1 Frame Control Field.
  - Sequence Number: sequentially increasing number, used to pair ACK frames with normal frames.
  - Addressing fields: see Section 3.2.1 Frame Control Field.
  - Aux. Security header: see Section 3.3 MAC Security.
- MAC payload: the payload of the Medium Access Control Protocol Data Unit (MPDU).
- MFR (MAC footer): has a single field—Frame Check Sequence (FCS), which is a 2-byte Cyclic Redundancy Check (CRC) of the MHR and the payload.

3.2.1 Frame Control Field

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Destination Addressing Mode	Frame Version	Source Addressing Mode

Figure 3-3. Format of the Frame Control Field

- Frame Type: Sets the frame type to one of these:
  - 0 – Beacon. used to advertise a PAN
  - 1 – Data. data used by an upper layer
  - 2 – Acknowledgement (ACK)
  - 3 – MAC Command which is the frame intended for the MAC layer (for example, part of the join process)
- Security Enabled: the Auxiliary Security Header is enabled when this bit is set to 1.
- Frame Pending: used for data polling.
- Acknowledgement Request (AR): frame should be ACKed by the receiver.
- Addressing modes: As Figure 3-3 shows, IEEE 802.15.4 frames are both source and destination addressed. However, both of these fields can be configured for various addressing modes:
  - 0 – no address. For example, both addresses are missing from ACK frames. For data and command frames only one (either source or destination) field can be omitted: If the source address is omitted, it means the PAN coordinator sent the frame. If the destination address is missing, it means it should be received by the PAN coordinator.
  - 2 – short address: The address field includes a short address and a PAN ID (total of 32 bits).
  - 3 – long address: The address field includes a long address and a PAN ID (total of 80 bits).
- PAN ID Compression: If both source and destination addresses are present and the PAN ID is the same for both (intra-PAN message), this bit should be set and the source PAN ID should be omitted. This shortens the addressing fields for short-addressed intra-PAN messages to 48 bits (one 16-bit source address, one 16-bit destination address, and one 16-bit PAN ID).
- Frame Version: Selects the frame version for compatibility with other versions of IEEE 802.15.4.

3.3 MAC Security

IEEE 802.15.4 supports the following security services:

- Data confidentiality
- Data authenticity
- Replay attack protection

The Auxiliary Security Header can have various arrangements, depending on the security and key setup available. However, with Silicon Labs Connect, when security is enabled it:

- Always uses a 128-bit key, which was set by the application (that is, there is no IEEE 802.15.4 key identifier field).
- Uses all three of the above services.

This means that the Auxiliary Security Header is five bytes long as in Figure 3-4:

Octets: 1	4
Security Control	Frame Counter

Figure 3-4. Format of the Auxiliary Security Header

Only the lowest three bits are used from Security Control, which selects the security mode (always 5).

The Frame Counter is a counter on each device that enables replay protection: The counter is part of the authenticated data (that is, MIC is calculated over it) and a receiver should not accept frames with the same/lower The Frame Counter must be valid even if the device reboots.

To guarantee data authenticity, a 4-byte MIC will be added at the end of the MAC payload (before the FCS). In the security mode supported by Silicon Labs Connect, the security headers and footers use nine bytes of the MAC payload.

4 Common 802.15.4 MAC Processes

4.1 ACK Process

If a device sends a data or command frame with the ACK request bit set, the device which receives it should respond with an ACK frame. The ACK frame includes the same sequence number as the frame that it responds to. ACK frames only include FCF, sequence number, and FCS from the MAC fields, and have no payload. This means that the PSDU of an ACK frame is five bytes.

4.2 Data Polling Process

A device can poll messages from another device. Typically, an end device that normally does not have the radio enabled would poll a coordinator. This process starts with the end device sending a data request command to the coordinator. The coordinator responds with an ACK with the frame pending bit set in the FCF. The end device must then wait for the next frame (or a timeout) with its radio on which the coordinator will send.

4.3 Association Process

To join a network, a device should go through an association process. The process can be described as follows (where 'E' (end device) would like to join to 'C' (PAN coordinator)). All the command frames above are MAC command frames.

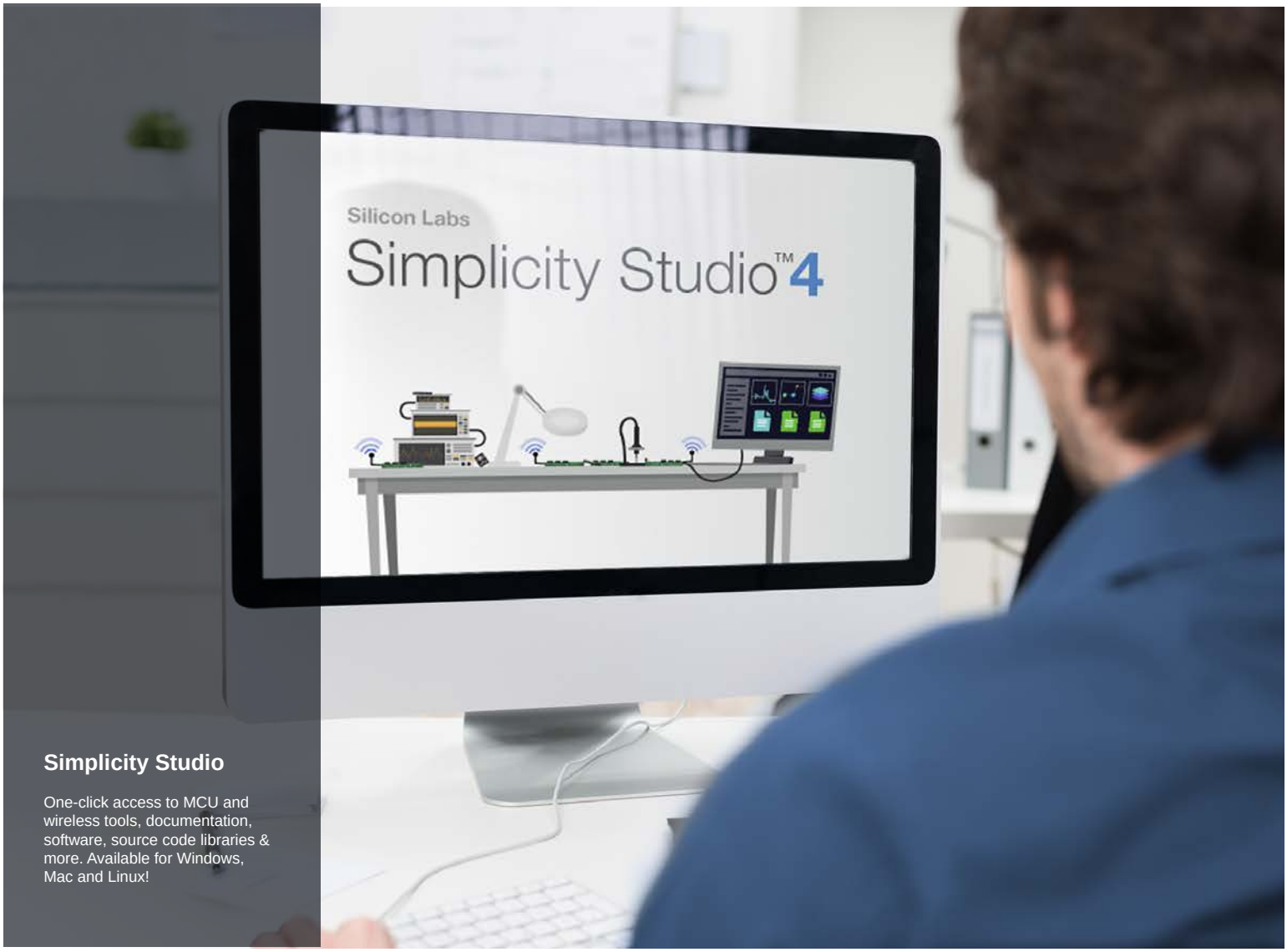
Step	Direction	Frame Type	Source Address	Destination Address	PAN Addressing	Other Fields
1	E --> C	Beacon request command	—	broadcast	broadcast destination	—
2	C --> E	Beacon	short	—	source specified	Superframe specification[1]
3	E --> C	Association request command	long	short	destination specified	Capability information[2]
4	C --> E	Acknowledgement	—	—	—	—
5	E --> C	Data request command	long	short	intra-pan	—
6	C --> E	Acknowledgement	—	—	—	Frame pending bit set
7	C --> E	Association request command	long	short	intra-pan	Given short address and status[3]
8	E --> C	Acknowledgement	—	—	—	—

Notes:

[1] Superframe specification lets E know that C is a PAN coordinator and if it permits joining (among other things)

[2] Capability info tells the coordinator how to handle the new device (for example, does it need a short address assigned to it, does it have the radio on when in idle, and so on.).

[3] The association response includes a status (that is, success or reason of failure) and the assigned short address. If a short address was not assigned, it is set to the special 0xfffe address. After association, E can communicate with its short address in the PAN. If E did not request a short address, it can still communicate within the PAN using its long address.



Simplicity Studio

One-click access to MCU and wireless tools, documentation, software, source code libraries & more. Available for Windows, Mac and Linux!

IoT Portfolio
www.silabs.com/IoT

SW/HW
www.silabs.com/simplicity

Quality
www.silabs.com/quality

Support and Community
community.silabs.com

SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

http://www.silabs.com