LoRa & LoRaWAN

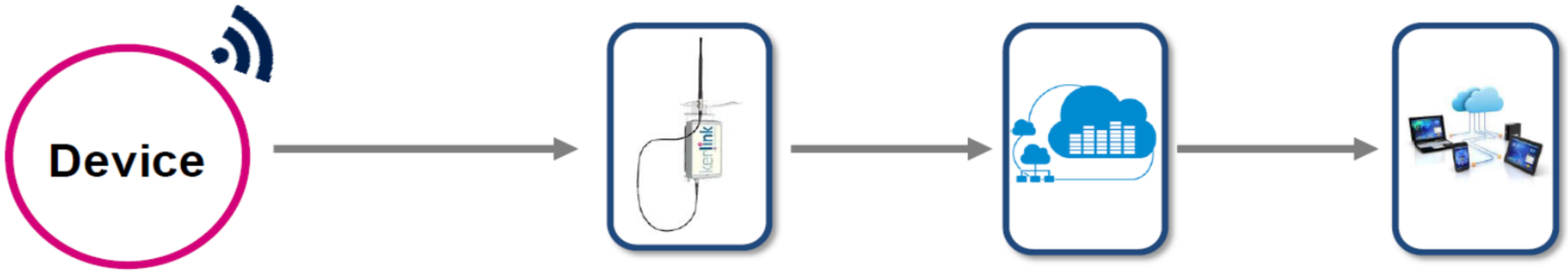
life.augmented

LoRa & LoRaWAN
Key learning

- LoRaWAN elements
- Link budget
- LoRa RF features
- LoRa classes
- Protocol stack overview
- End node network activation
- Certification flow

Theory

What does LoRa network (LoRaWAN) consists of ?



End Point

Gateway

Network server

Application server

Theory
Link budget

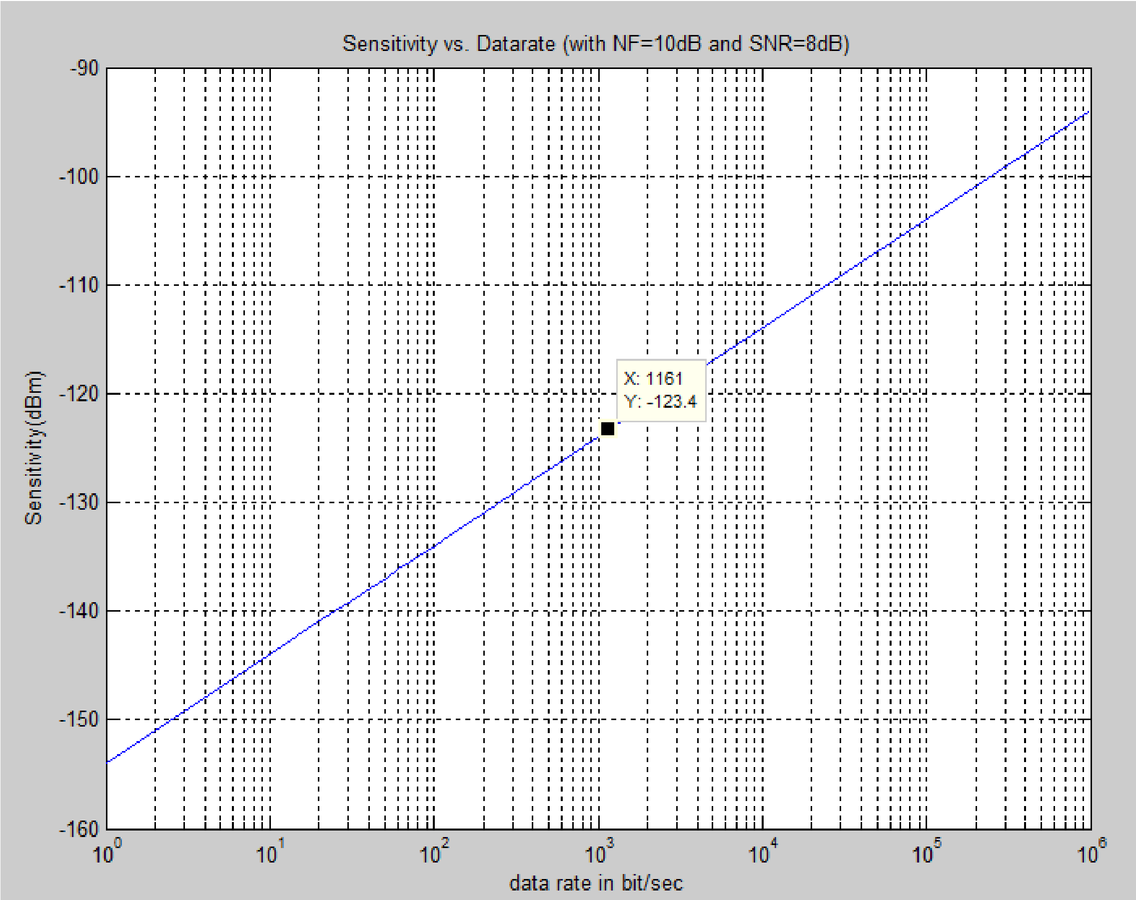
- Long Range requires Large Link Budget

- Link Budget(dB) = Pout + $Gain_{AntTx}$ + $Gain_{AntRx}$ – SensitivityRx
  - Pout is fixed and limited by regulatories
  - $Gain_{AntTx}$ and $Gain_{AntRx}$ are design choices

- Maximizing Link Budget is about maximizing sensitivity

- $Sensitivity_{dBm}$ = -174dBm + 10*log($datarate_{bit/sec}$) + SNR_{dB} + NF_{dB}
  - SNR_{dB} is limited by the Shannon capacity
  - NF_{dB} is positive. It is all the noise generated by the receiver front-end
  - -174dBm is the noise power density at 25°C
  - The only degree of freedom is the **datarate**

- Maximizing sensitivity is about lowering data rate



life.augmented

Theory
LoRa RF features

- Spread spectrum modulation*: Chirp cyclic shift modulation, information in shift
- Half duplex
- Frequency Hopping
- LoRa operates over ISM band
  - 868MHz in EU
  - 915MHz in US
- Power is limited
  - 14dBm in EU
  - 20dBm in US
- Duty cycle is limited
  - 1% in EU

Datarate	Spreading Factor	Bandwidth (kHz)	Indicative bit Rate (b/s)	Indicative Sensitivity for CR=4/6 In dBm
0	SF12	125	250	-136
1	SF11	125	440	-133
2	SF10	125	980	-132
3	SF9	125	1760	-129
4	SF8	125	3125	-126
5	SF7	125	5470	-123
6	SF7	250	11000	-118
7	FSK	50	50000	TBC

life.augmented

*LoRa modulation is patented

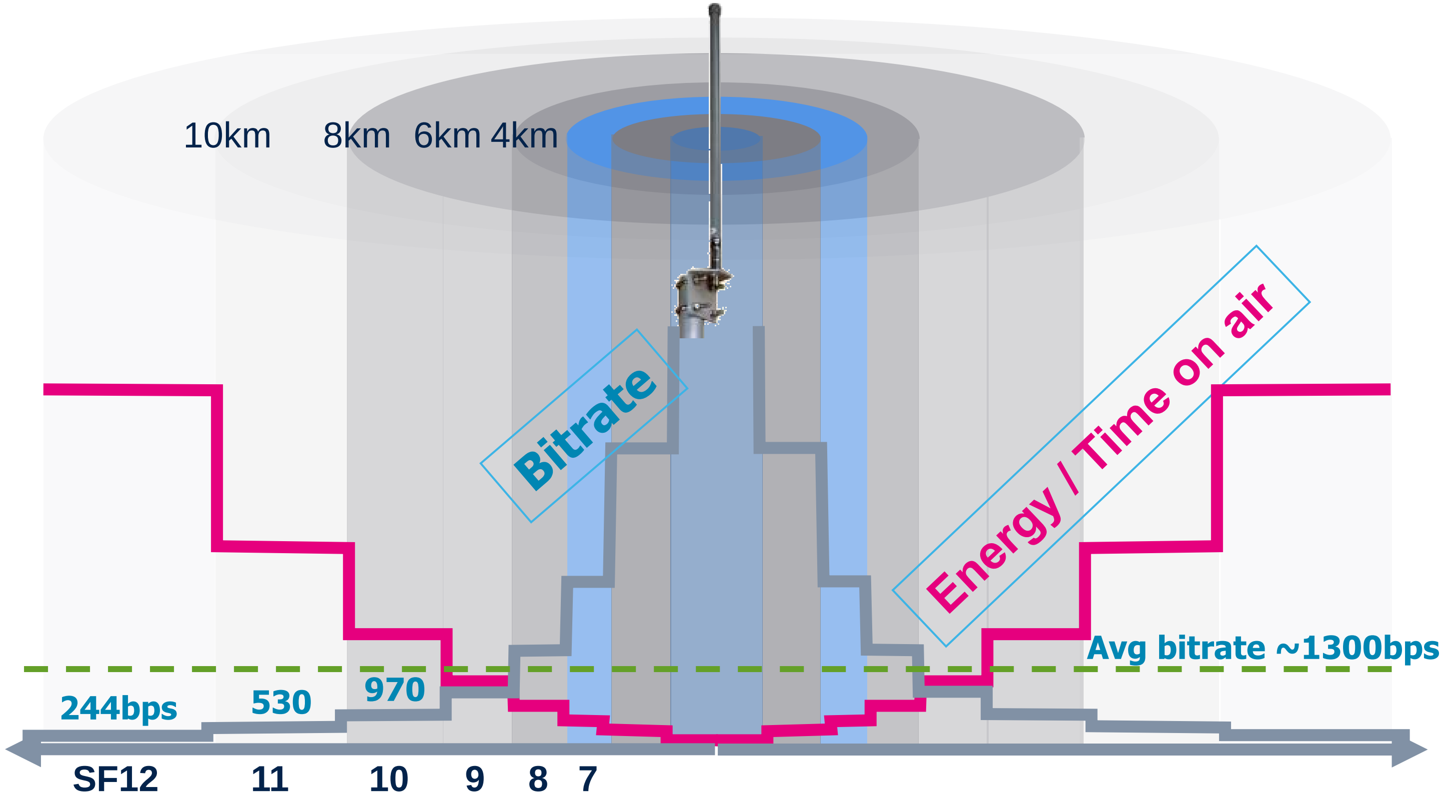
Theory Basics

- Spread Factor (SF): each bit of information is encoded as multiple chips, chip rate Rc and bit rate Rb is given by: **Rc = 2^SF * Rb**
- Bandwidth (BW): frequency of the spread signal in kHz. LoRaWAN supports **125**, 250 and 500kHz. For a given SF, a narrower BW (ex: 125kHz) will increased receive sensitivity and so the TOA.
- Time On Air (TOA): time requested to transmit data over the air for a given SF, The higher is SF, the longer is TOA; the wider is BW, the shorter is TOA
- Bit Rate (BR): number of bits per second on the TX phase
- Forward Error Correction (FEC) and Coding Rate (CR): ratio of byte used to perform the correction. Ex: a CR 4/5 means 25% of the payload is used as error correction code (ECC like) named FEC. The higher percentage of FEC in payload, the longer is TOA
- Range: distance for given setting. The value is dBm rather than km or meters
- Receiver Sensitivity (dBm): the lower the more sensitive is radio receiver. The wider is BW, the lower receiver sensitivity due to integration of additional noise power in the channel.

Theory
Adaptive **D**ata **R**ate

- ADR is good for the network
  - It ensures that the transmission of an end-device only last as long as required i.e. optimize the network capacity

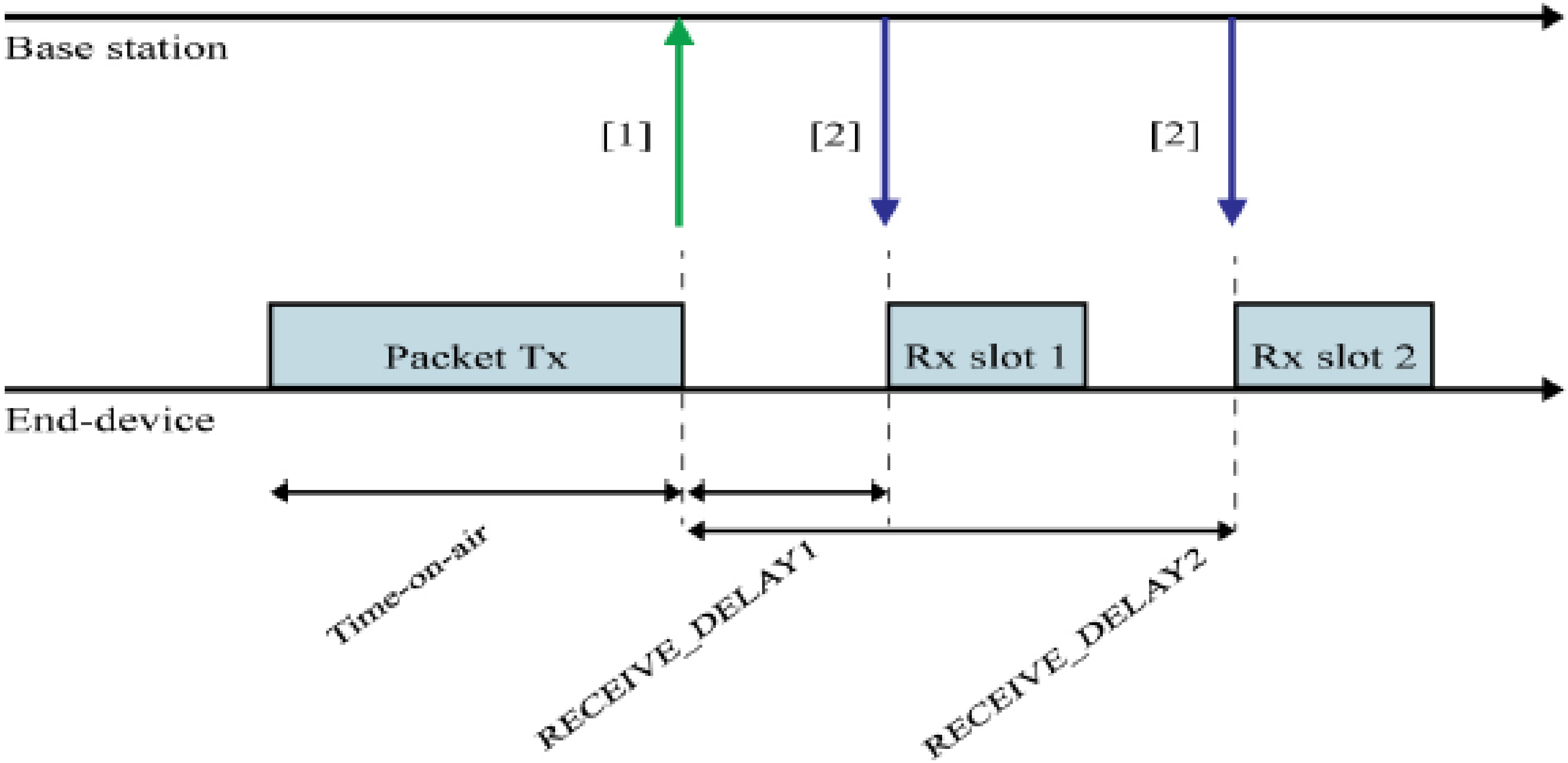
- ADR is good for the device
  - Devices with a good radio channel use a higher data rate, therefore lower energy is required to transmit a message



life.augmented

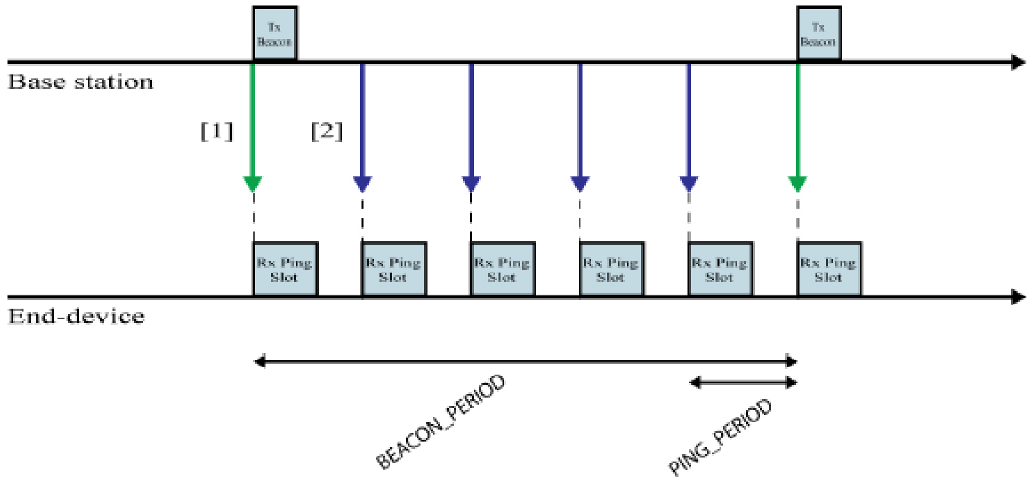
Theory
Class A

- Node transmits uplink data at any time (randomly)
- Uplink message may be received by multiple gateways
- For every uplink there are possible 2 downlink slots
- Network server selects gateway and downlink slot



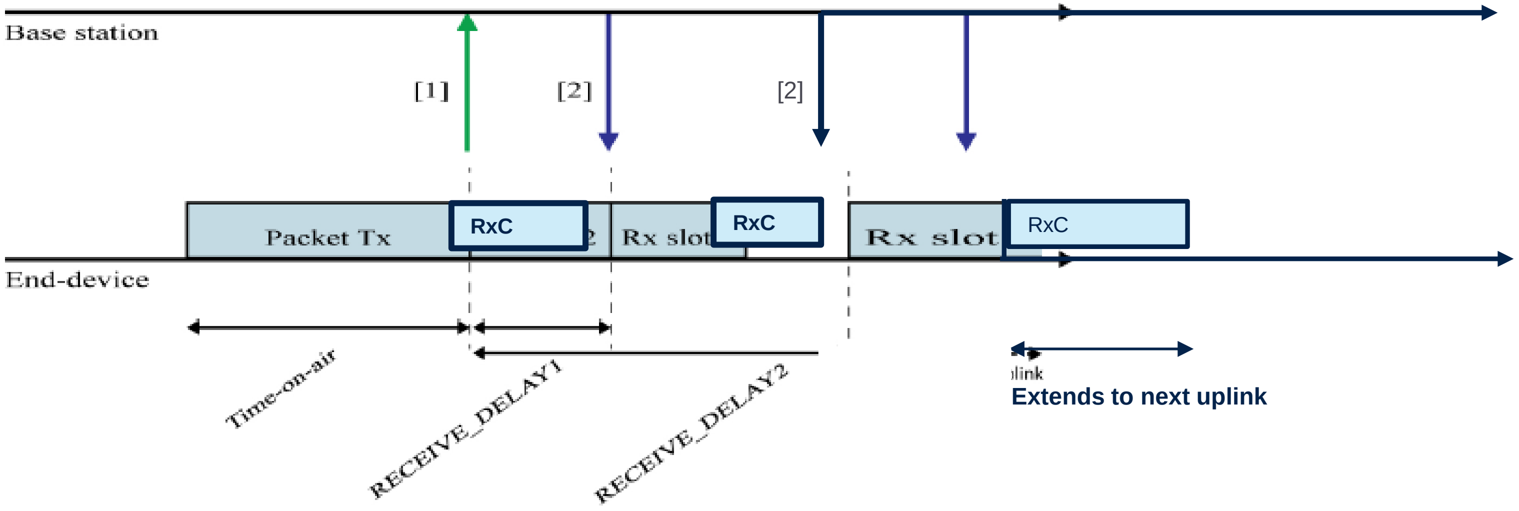
Theory
Class B

- LoRa **Class B** devices provide the Class A functionality and in addition to this, it opens extra receive windows at scheduled times. To achieve the required synchronization from the network, the endpoint receives a time synchronized Beacon from the gateway. This allows the server to know when the end-device is listening.
- End-Device always starts and Joins network as Class A end-device (Class B capable but disabled)
- Class B enabled request always comes from Application layer of the End-Device
- Server may change the End-Device's Ping-slot downlink frequency or data rate thanks to PingSlotChannelReq MAC command
- End-device may change the periodicity of its Ping-slots thanks to PingSlotInfoReq MAC command
- When a Class A Rx1 or Rx2 receive slot collides with a Class B Multicast or Unicast slot, the End-device listen to the Class A RX in priority



Theory
Class C

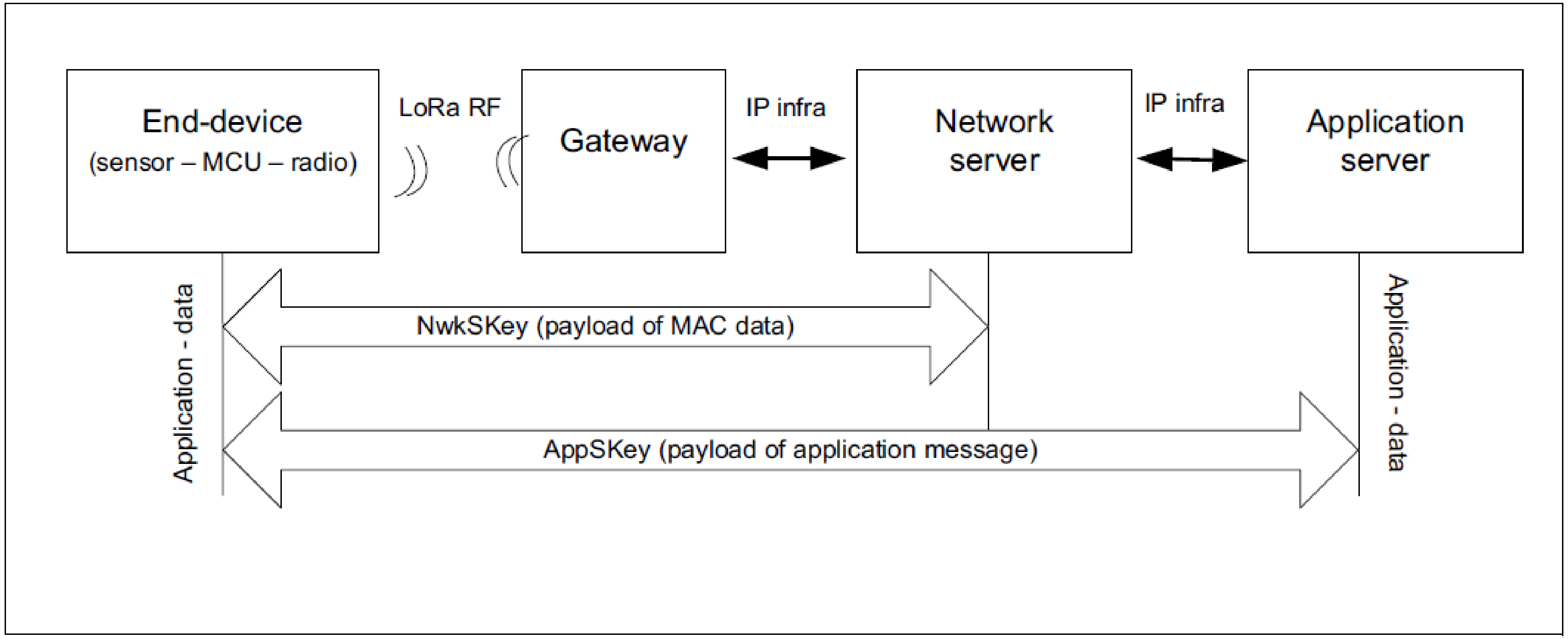
- LoRa **Class C** devices provide nearly continuously open receive windows. They only closed when the endpoint is transmitting. This type of endpoint is suitable where large amounts of data are needed to be received rather than transmitted.



When an End-Device is in Class C enabled, then he listens to a channel/DR parameters combination referred as RxC

Theory
Crypto covertage range

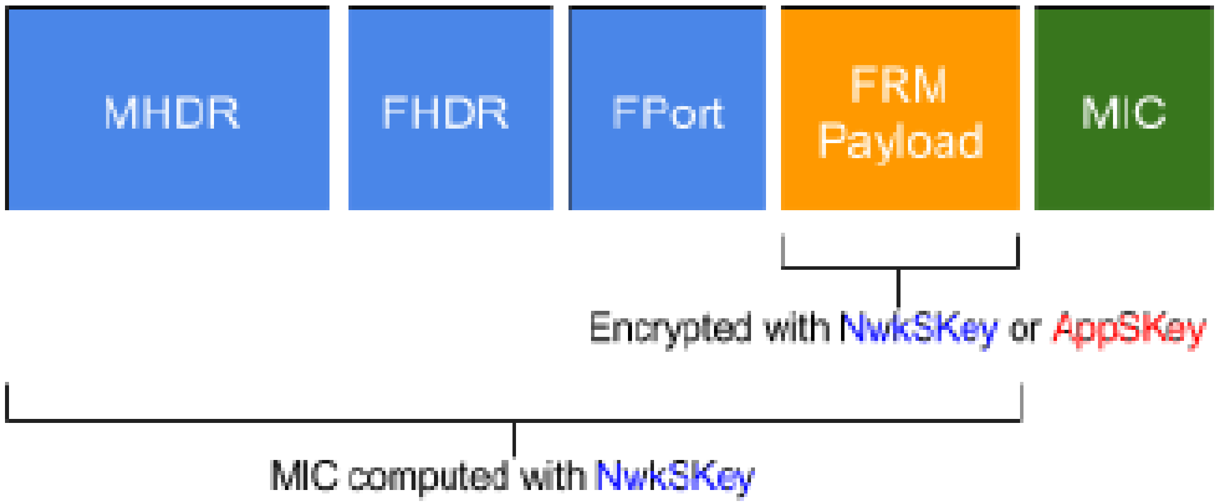
- The confidentiality of LoRaWAN messages is protected by AES-128 encrypting the FRMPayloadfield. LoRaWAN differentiates between **MAC messages** destined for the network server and **Application messages** destined for the application server through the FPort field (which is not encrypted), thus <u>two different encryption keys</u> are used for the FRMPayload field depending on the intended destination.
- End-devices in LoRaWAN thus needs two 128-bit encryption keys, one Network Session Key (**NwkSKey**) for encrypting MAC messages and one Application Session Key (**AppSKey**) for encryption application messages.
- The **AppSKey** is an encryption key shared between an end-device and the application server, while the **NwkSKey** is an encryption key shared between the end-device and the network server.



life.augmented

Theory
LoRa network security

In order to provide message integrity, a Message Integrity Code (MIC) is computed for each packet using AES-CMAC and the NwkSKey. The MIC is computed over the entire PHYPayload (after the **FRMPayload** has been encrypted) in order to detect packet tampering.



Theory
LoRa network activation methods

1. **OTAA**: Over the Air Activation = Over the air handshaking
   - End-device send a Join Request (J.S) message to A.S including DevEUI, AppEUI, AppKey
     - DevEUI (Global unique end-device identifier) will allow the network to identify the device
     - AppEUI to identify which A.S the end-device is talking to
     - AppKey to crypt message send to A.S.
     - End device receives the Join Accept from the A.S and proceed with
     - Join Accept (authenticates and decrypt the Join Accept)
     - Extract and store DevAddr (the 32-bit device address)
     - Derives the 2 security: Network session Key (NwkSKey) and Application Session Key (AppSKey)

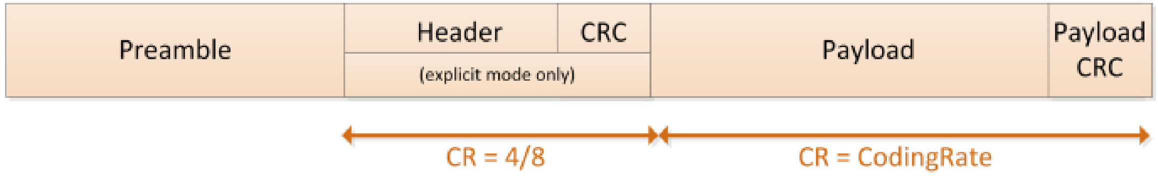
2. **ABP**: Activation By Personalization (no Over the air handshaking)
   - The Device ready out-of-the-box to talk on the network
   - The DevAddr, NwkSKey and AppSKey are programed at factory level (no Over the air handshaking)

life.augmented

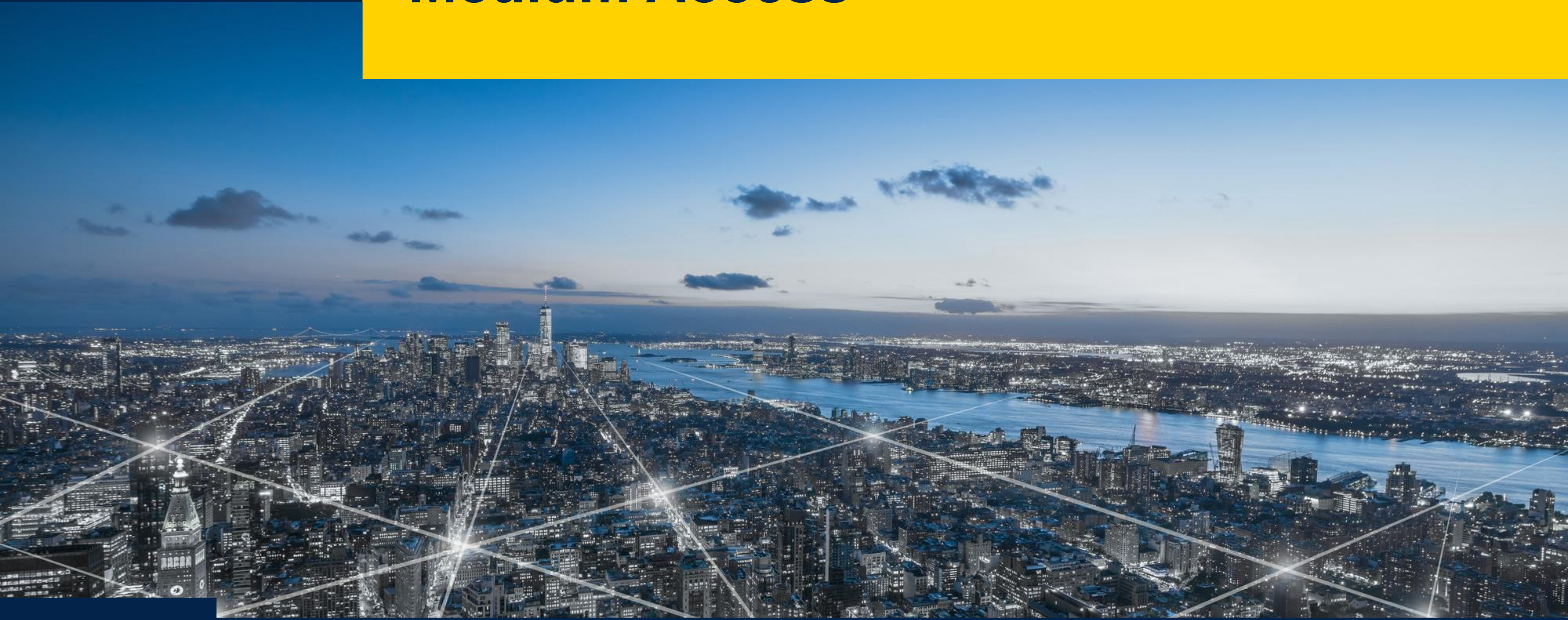
Physical layer

life.augmented

- Physical (Phy) Packet Structure
  - preamble is used to synchronize receiver with the incoming signal.
    - 0x34 so 8 preamble symbols
  - header provides information on the payload with Coding Rate=4/8:
    - The payload length in bytes.
    - The forward error correction **C**oding **R**ate (**CR**)
    - The presence of an optional 16-bits CRC for the payload.
  - Payload contains the MacHeader and MacPayload and a MAC integrity code
    - Compatible with **802.15.4** recommendations
  - Optional CRC in uplink message



Medium Access



life.augmented

Medium ACcess

- MAC Packet structure
  - **MHDR**: mac message type (Join Request/Accept message OR Data up/down message)
  - **FHDR**: contains the DevAddr, Adaptative Data Rate control, frame counter, Acknowledgement, MAC commands if any
  - **Fport**=0: FRMPayload contains MAC commands only, otherwise (Fport=1..223) are application specific.
  - The message integrity code (**MIC**) is calculated over all the fields in the message (AES).

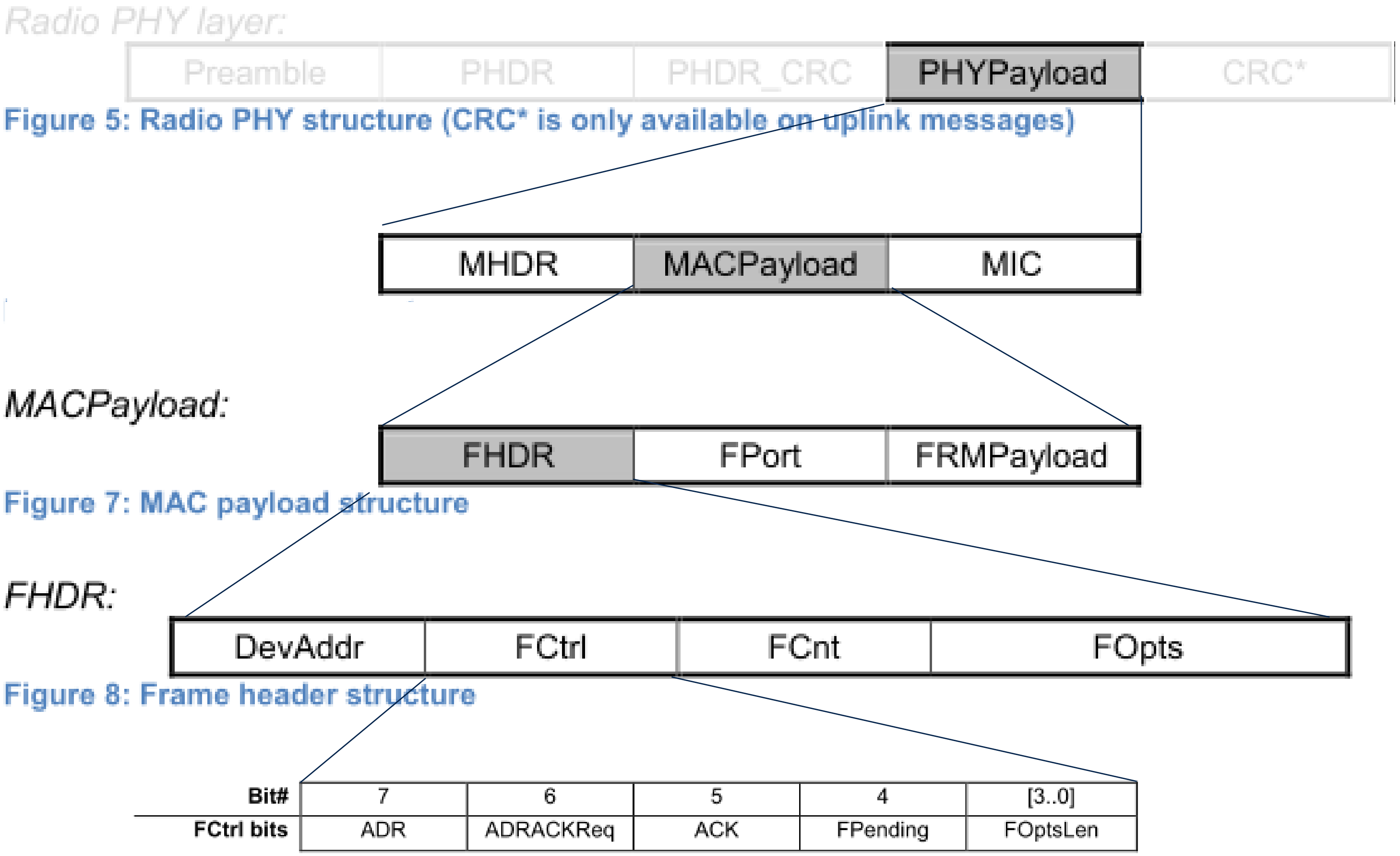


Figure 5: Radio PHY structure (CRC* is only available on uplink messages)

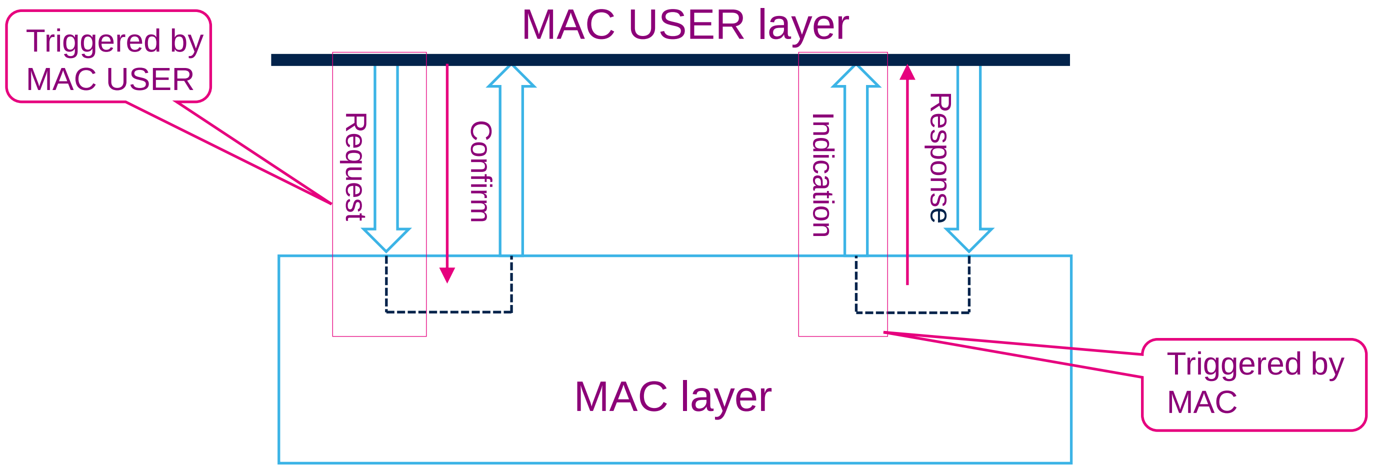
Figure 7: MAC payload structure

Figure 8: Frame header structure

Medium Access
IEEE 802.15.4 introduction: MAC API

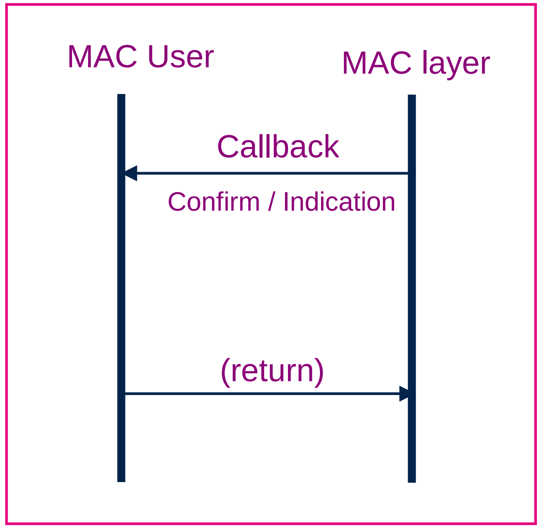
LoRaWAN protocol stack MAC layer implements IEEE 802.15.4 standard. Communications are passed between the MAC layer and the next highest stack layer (MAC user) by means of “service primitives”

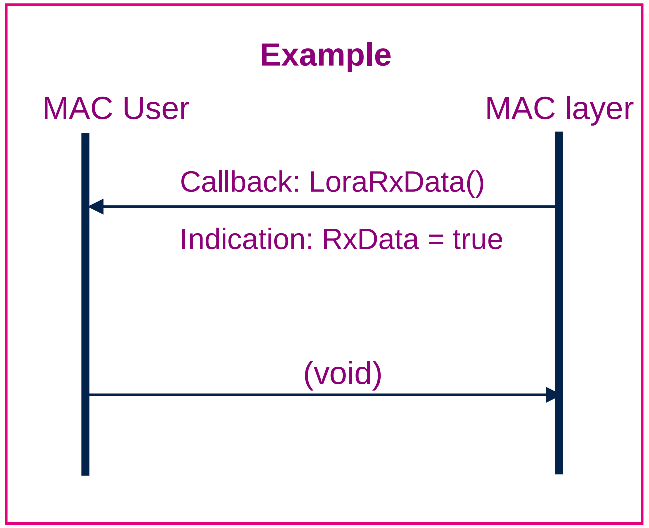
- Request ; initiated by the MAC user
- Confirm ; MAC user may solicit Confirm from the MAC layer
- Indication ; initiated by the MAC layer
- Response ; MAC layer may solicit Response from the MAC user



Medium Access
IEEE 802.15.4 implementation: callback mechanism

Request is issued by the MAC User by means of call to one of the MAC layer API functions. The most straightforward way for the MAC layer to reply (with Confirm and/or Indication) is via callback function.





Medium Access
MAC Commands example

For network administration, a set of MAC commands may be exchanged exclusively between the Network Server and the MAC layer on an end-device. MAC layer commands are never visible to the Application Server or the application running on the end-device.

CID	Command	Transmitted by		Short Description
		End-device	Gateway	
0x02	*LinkCheckReq*	x		Used by an end-device to validate its connectivity to a network.
0x02	*LinkCheckAns*		x	Answer to LinkCheckReq command. Contains the received signal power estimation indicating to the end-device the quality of reception (link margin).
0x03	*LinkADRReq*		x	Requests the end-device to change data rate, transmit power, redundancy, or channel mask.
0x03	*LinkADRAns*	x		Acknowledges the LinkADRReq.
0x04	*DutyCycleReq*		x	Sets the maximum aggregated transmit duty-cycle of a device.
0x04	*DutyCycleAns*	x		Acknowledges a DutyCycleReq command.
0x05	*RXParamSetupReq*		x	Sets the reception slots parameters.
0x05	*RXParamSetupAns*	x		Acknowledges a RXParamSetupReq command.
0x06	*DevStatusReq*		x	Requests the status of the end-device.
0x06	*DevStatusAns*	x		Returns the status of the end-device, namely its battery level and its radio status.
0x07	*NewChannelReq*		x	Creates or modifies the definition of a radio channel.
0x07	*NewChannelAns*	x		Acknowledges a NewChannelReq command.
0x08	*RXTimingSetupReq*		x	Sets the timing of the of the reception slots.
0x08	*RXTimingSetupAns*	x		Acknowledges RXTimingSetupReq command.
0x09	*TXParamSetupReq*		x	Used by the Network Server to set the maximum allowed dwell time and Max EIRP of end-device, based on local regulations.
0x09	*TXParamSetupAns*	x		Acknowledges TXParamSetupReq command.
0x0A	*DlChannelReq*		x	Modifies the definition of a downlink RX1 radio channel by shifting the downlink frequency from the uplink frequencies (i.e. creating an asymmetric channel).
0x0A	*DlChannelAns*	x		Acknowledges DlChannelReq command.
0x0B to 0x0C	***RFU***			
0x0D	*DeviceTimeReq*	x		Used by an end-device to request the current GPS time
0x0D	*DeviceTimeAns*		x	Sent by the Network Server, answer to the DeviceTimeReq request
0X0E to 0x7F	RFU			
0x80 to 0xFF	Proprietary	x	x	Reserved for proprietary network command extensions

life.augmented

Medium Access
Data Rate Adaptation

- Retransmission messages
  - When an End-Device send a “Confirmed” Uplink frame toward the network, it expects to receive an “ack” from the network in one of the subsequent Rx slot. If it does not receive an “ack”, then it will try to re-transmit the same data again
- Re-transmission strategy
  - The re-transmission can happen either on a new frequency or also can happen at a different data rate (preferable lower) than the previous one. A sending recommended strategy to adopt will be :

Trans Nb	Data Rate
1 (first)	DR
2	DR
3	Max(DR-1,0)
4	Max(DR-1,0)
5	Max(DR-2,0)
6	Max(DR-2,0)
7	Max(DR-3,0)
8	Max(DR-3,0)

- First “confirmed” Uplink frame is sent with the Data Rate DR and the next retransmission (in case of) will follow the “rule” table
- If after the 8 transmissions, the frame has not been “ack” then the MAC will return error to the application layer.
- For each retransmission , the frequency channel is randomly selected as standard transmissions.

life.augmented

Medium Access
Duty Cycle limitation

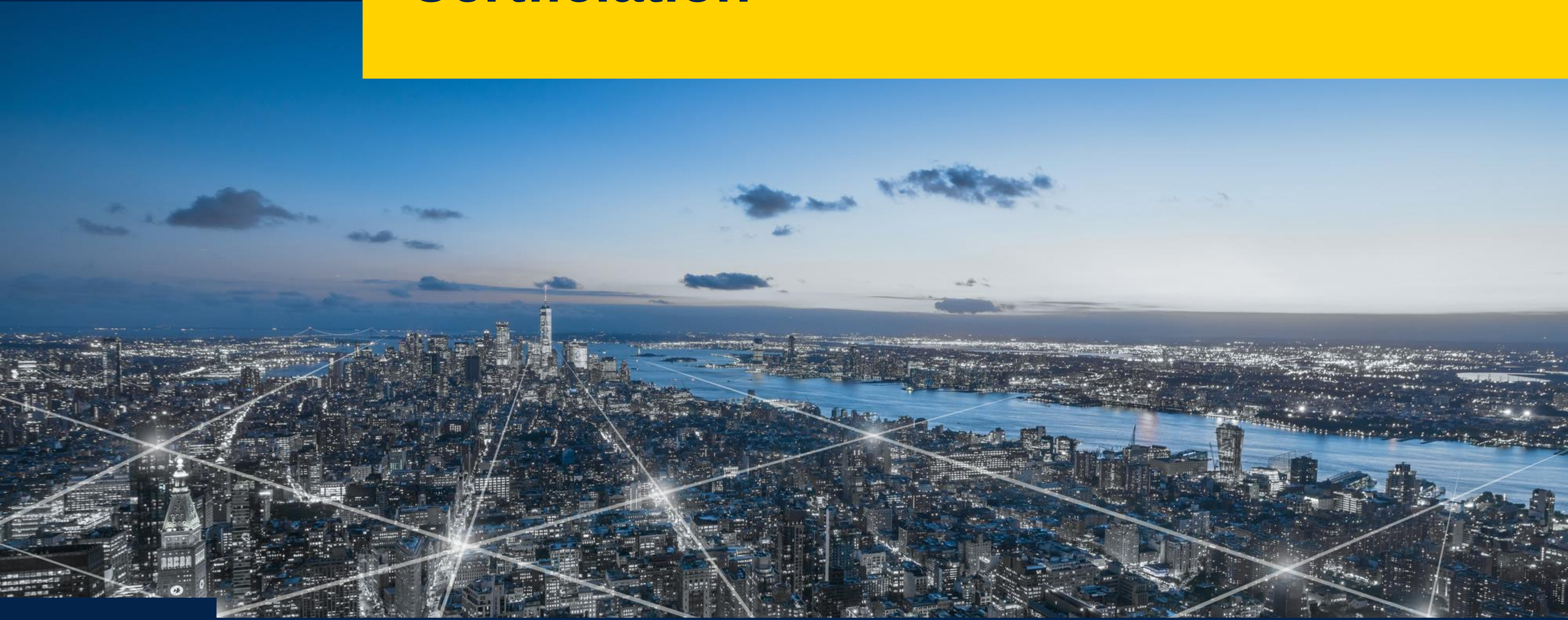
- The current LoRaWAN specification exclusively uses duty-cycled limited transmissions to comply with the ETSI regulations.
  - The LoRaWAN enforces a per sub-band duty-cycle (1%) limitation. Each time a frame is transmitted in a given sub-band, the time of emission and the on-air duration of the frame are recorded for this sub-band. The same sub-band cannot be used again during the next Toff seconds. During the unavailable time of a given sub-band, the device may still be able to transmit on another sub-band.
  - $\mathrm{Toff}_{\mathrm{subband}} = \dfrac{\mathrm{TimeOnAir}}{\mathrm{DutyCycle}_{\mathrm{subband}}} - \mathrm{TimeOnAir}$ it Tx during 0.5sec, subband unavailable during 49.5sec
  - Other subbands can be tried. If all subbands are unavailable due to DC limitation, device has to wait…

According to EN300220-1 there is a duty cycle limitation in ISM band: “In a period of 1 hour the duty cycle shall not exceed the spectrum access and mitigation requirement values…”. For 868MHz sub-band used by Lora it is **1%**.

Note : The ETSI regulations allow the choice of using either a **duty-cycle limitation** or a so-called **Listen Before Talk Adaptive Frequency Agility** (LBT AFA) transmissions management. The current LoRaWAN L2 V1.0.x specification exclusively uses duty-cycled limited transmissions to comply with the ETSI regulations.

life.augmented

Certficiation



life.augmented

Certification

LORA Certifications requirements

- LoRa Alliance membership

  https://www.lora-alliance.org/

- LoRa Conformance to Standard, established by passing tests in an authorized test house
- Documentation of Product (including version numbers for HW/FW/SW)
- Payment of applicable fees
- Certification procedure

  https://www.lora-alliance.org/certification-overview

LoRa Conformance tests setup

- The conformance to Standard is verified by an Authorized Test House through a series of tests.

- Tests are related to LoRa functionalities and cover both PHY and MAC layers. Some of them set packet error rates requirements too.

- Both radio performance tests and regulatory testing (CE / FCC) are out of scope for the LoRa Certification, but test houses are generally also able to perform them.

Certification

LoRa Alliance Authorized Test Houses

- 7layers
- Dekra
- Etteplan
- IMST
- TÜV Rheinland

life.augmented

Hints: Typical period of certification: about 1 week ; Price: about few k€

Thank you

© STMicroelectronics - All rights reserved.
The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies. All other names are the property of their respective owners.

life.augmented