LoRaWAN Overview

Troy Martin
@troymart

Troy Martin

CWISE #002

South Central Western Canada

Like things wireless...

Love cycling....

@troymart

LoRa Alliance®

LoRaWAN™

SEMTECH

LoRaWAN®

LoRaWAN™

Highlights & Use Cases

What is LoRa?

- **Sub - 1 GHz** (e.g 433, 780, 868, 915 MHz)
- Adaptive data rates (**ADR**)
- Modulation derived from **Chirp Spread Spectrum (CSS)** using chirp pulse
- Ideal for sending **small** nuggets of data with **low** data rate over **long** distances
- End-to-end security (**AES 128 bit**) between end-point(s) and application server(s)

BOSTON BREW COMPANY

Cold Brew Coffee

Precision Agriculture

helium

Massive, Decentralized Connectivity

People-Powered Networks

Why is LoRaWAN so awesome?

Ultra low power

Roaming

Public and private deployments

Certification Program

Long range

Low cost

High capacity

Firmware updates over the air

Deep indoor penetration

Geolocation

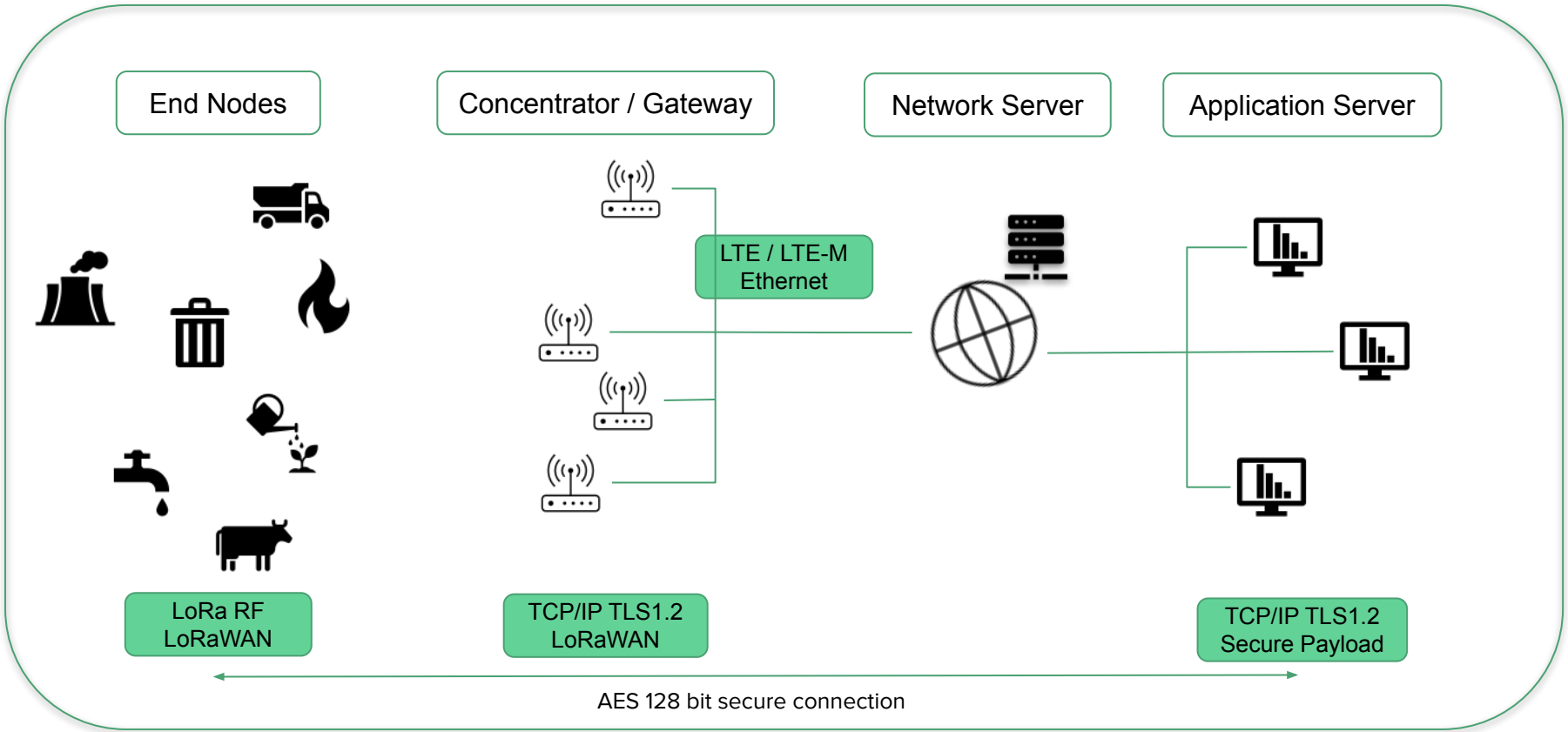
License free spectrum

Ecosystem

End-to-end security

High Level Architecture

LoRaWAN Architecture

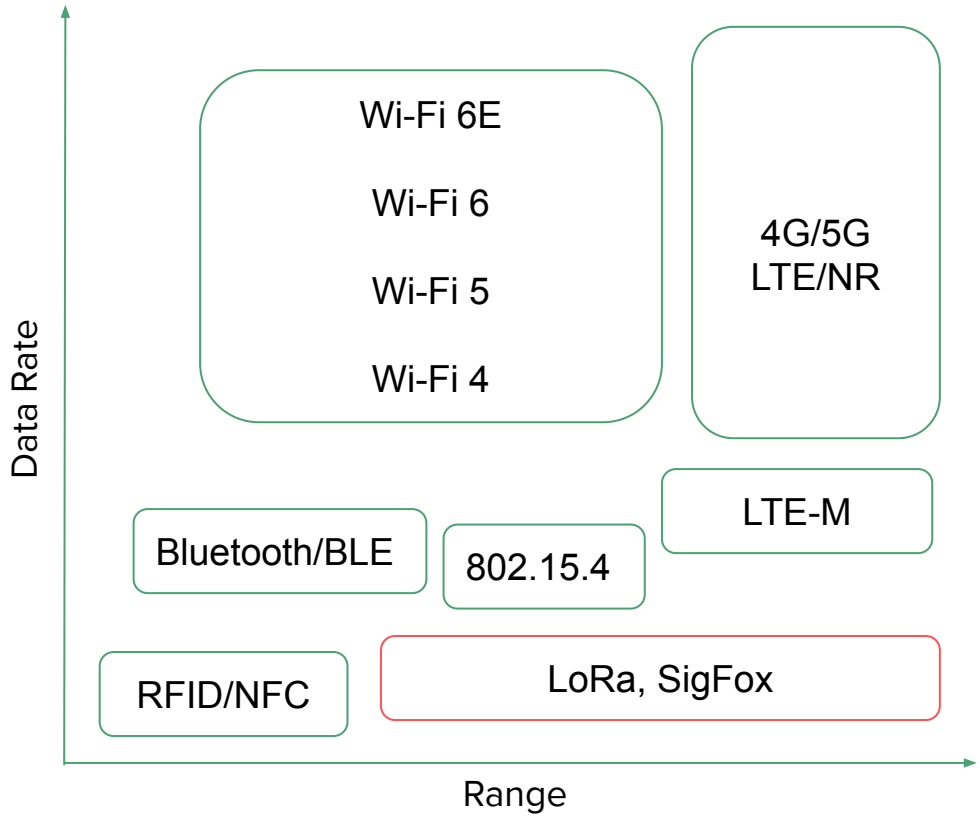


Where does LoRa fit in?

Long range

Low power consumption

Low data rate



Standards

LoRa Alliance

- Open, non-profit association established in 2015
- Supports development of LoRaWAN protocol
- Ensures interoperability of all LoRaWAN products
- Over 500 members globally

International Telecommunication Union (ITU)

- Low Power Wide Area Networking (LPWAN)
- December 7, 2021

LoRa vs LoRaWAN - what is the difference?

LoRa

- Proprietary system made by chip manufacturer Semtech
- PHY layer method using a chirped, multi-symbol format to encode information

LoRaWAN

- Point-to-multipoint networking protocol using the LoRa PHY
- Defines how LoRaWAN devices perform encryption and identification

LoRa vs LoRaWAN - what is the difference?

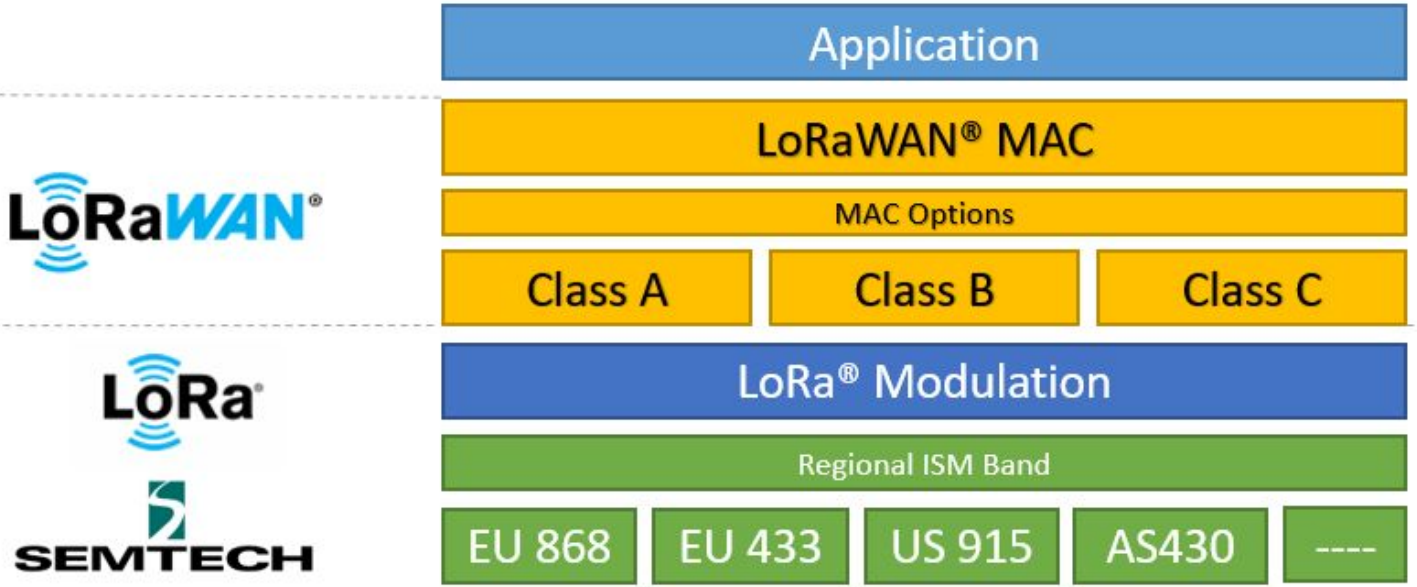
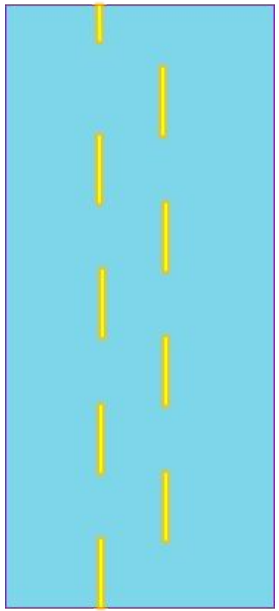
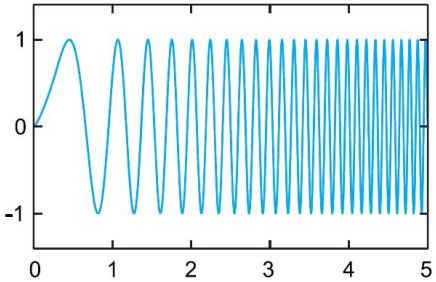


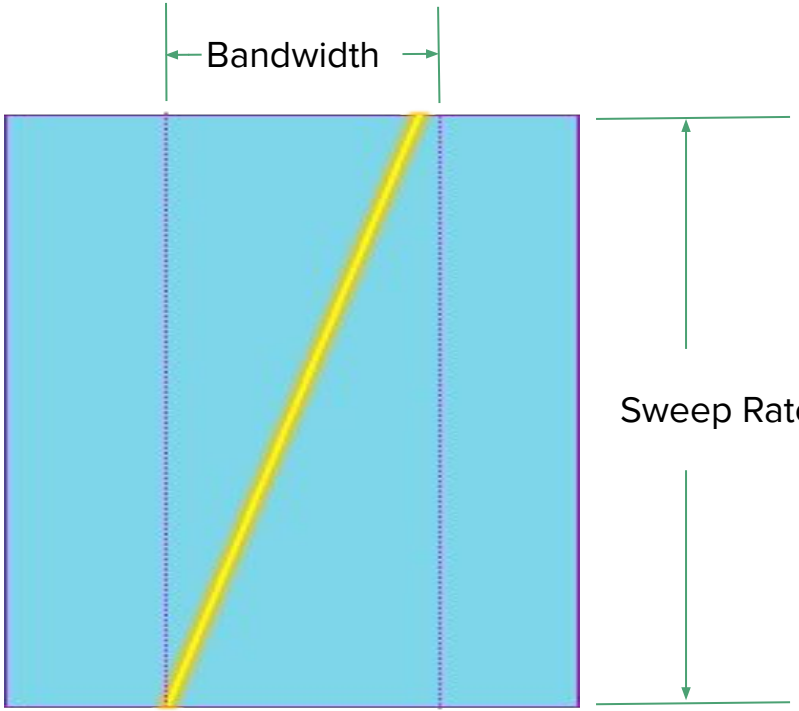
Image source: “What are LoRa and LoRaWAN” (www.lora-developers.semtech.com)

‘Geeky’ Connectivity Details

Frequency Shift Keying (FSK) vs Chirping







2-ary FSK

Chirping

Chirping

- RF **tone sweeps** linearly across spectrum over over time
- Frequency of **tone increases** over time (left to right)
- Different symbols are encoded by **breaking chirps** in different places with respect to time and frequency allow encoding

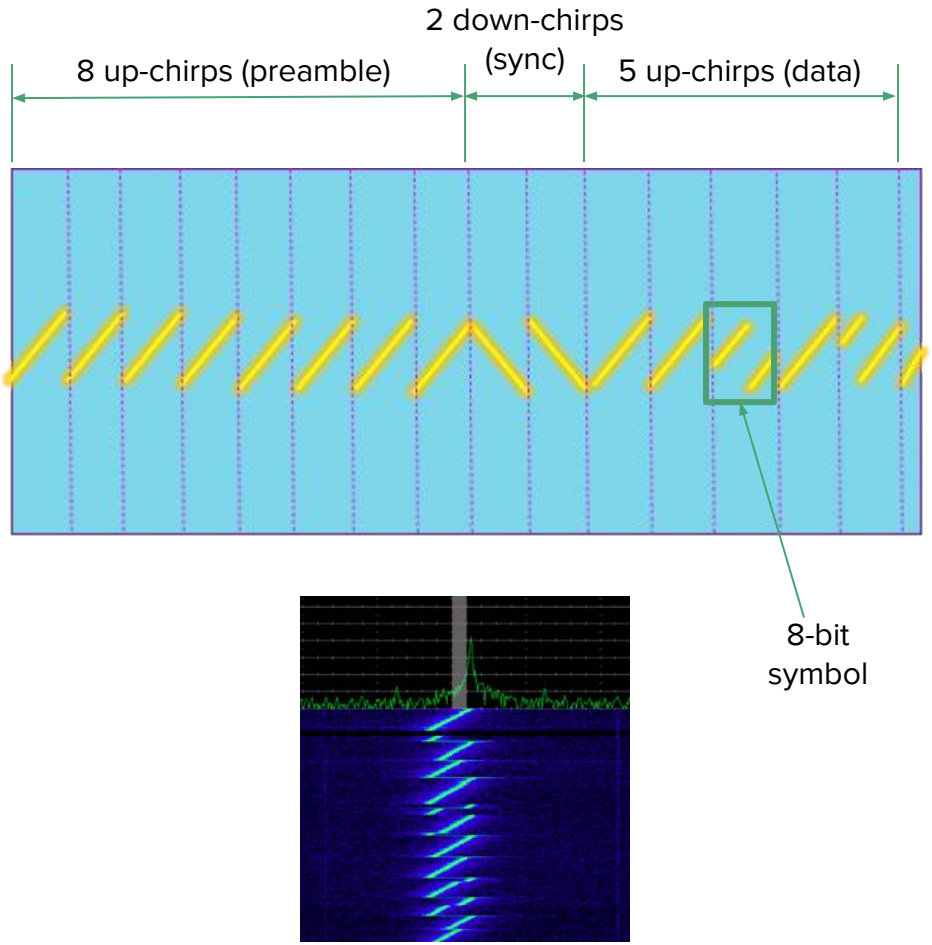


Image sources: “What is LoRa? A technical breakdown” (www.link-labs.com)

Spreading Factor (SF)

Lower Spreading Factor SF

⬇

Shorter range

⬇

Less time on air

⬇

Lower energy consumption

⬇

Higher data rate

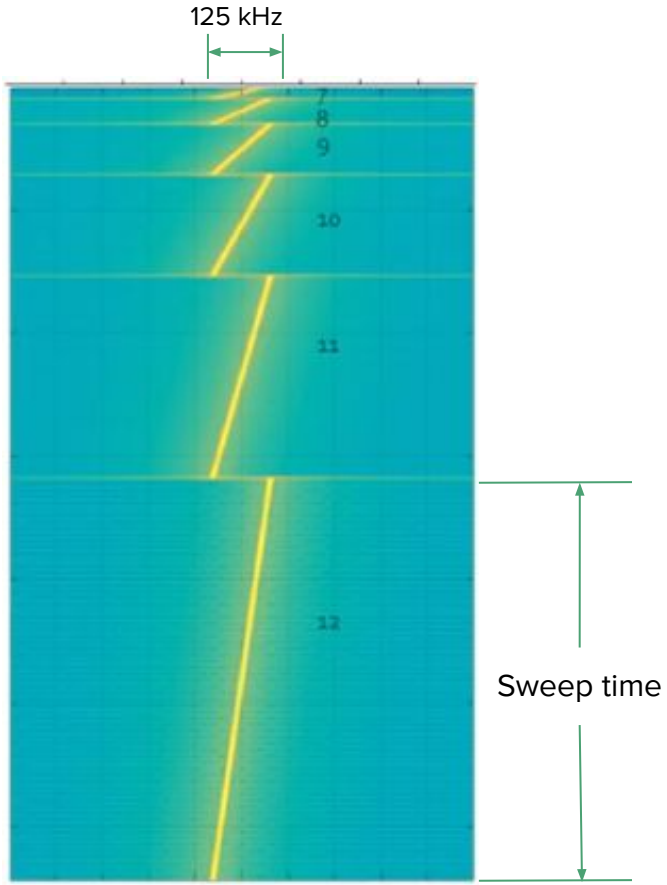


Image source: “LoRa CHIRP spread spectrum” Richard Wenner (www.youtube.com)

Spreading factor SF

Spreading Factor SF	Bandwidth (kHz)	Bit rate (kbit/s)
7	125	5.5
7	250	10.9
7	500	21.9

Example of SF bit rates for EU

Image source: “Maple bourbon sticky buns” @sclements - Wi-Fi Engineer / Sticky Bun Photographer

Duty cycle time-on-air (dwell time) restrictions

Must be respected by **both** end devices and gateways

May or may NOT apply in every **region**

Check with your local **regulatory body**

Frequency plan	EU	US
Duty cycle	0.1% - 10%	No limit
Dwell time	No limit	400 ms for channels 0 - 63

Duty Cycle - details

Duty cycle (take the maximum)	Equation: Time-On-Air = number of seconds per day x duty cycle	Maximum allowed Time-On-Air per day, per device
0.1 %	86400 x 0.1%	86 seconds per day
1 %	86400 x 1%	864 seconds per day
10 %	86400 x 10%	8640 seconds per day

Duty Cycle - details

Duty cycle - example

- A fraction of time when the resource is busy
- Example: 10 time units → what is the percentage of the time when the band, the channel and the device are busy?
  - band 1: 20%, band 2: 40%

Adaptive Data Rate (ADR)

ADR causes SF to change dynamically based on changing link budget

Lower SF reduces battery and airtime consumptions

Rules:

High link budget -> **Increase** Data Rate (SF)

Low link budget -> **Decrease** Data Rate (SF)

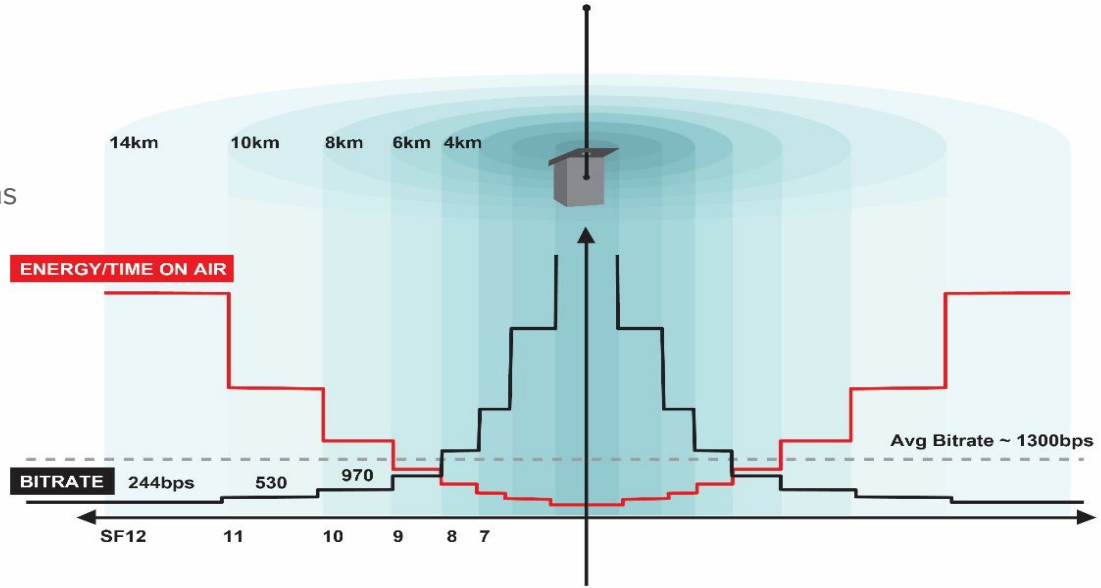
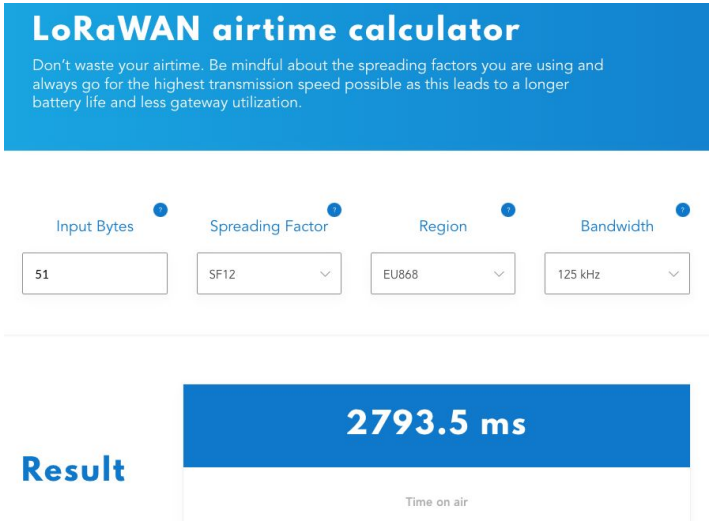


Image source: “What is Adaptive Data Rate” LoRa Developer Documentation (lora-developers.semtech.com)

Gollum's Airtime Rule



Calculator at: https://www.thethingsnetwork.org/airtime-calculator

	11 bytes	53 bytes	125 bytes	242 bytes
SF7	62 ms	123 ms	226 ms	400 ms
SF8	113 ms	216 ms	400 ms	
SF9	206 ms	390 ms		
SF10	371 ms			
SF11				
SF12				

My precious [**Don't waste any airtime**]....!
- Gollum, RF champion

#WLPC

RF for the Rocket Surgeon

Frequencies

Unlicensed **sub-1 GHz** frequency based on location:

EU - 863 - 868, 433 - 434 MHz

China - 779 - 789, 470 - 510 MHz

US - 902 - 928 MHz

Australia - 915 - 928 MHz

Russia - 864 - 870 MHz

India - 865 - 867 MHz

+ Many other!

Data source: “RP002-1.0.3 LoRaWAN Regional Parameters” LoRa Alliance specification (lora-alliance.org)

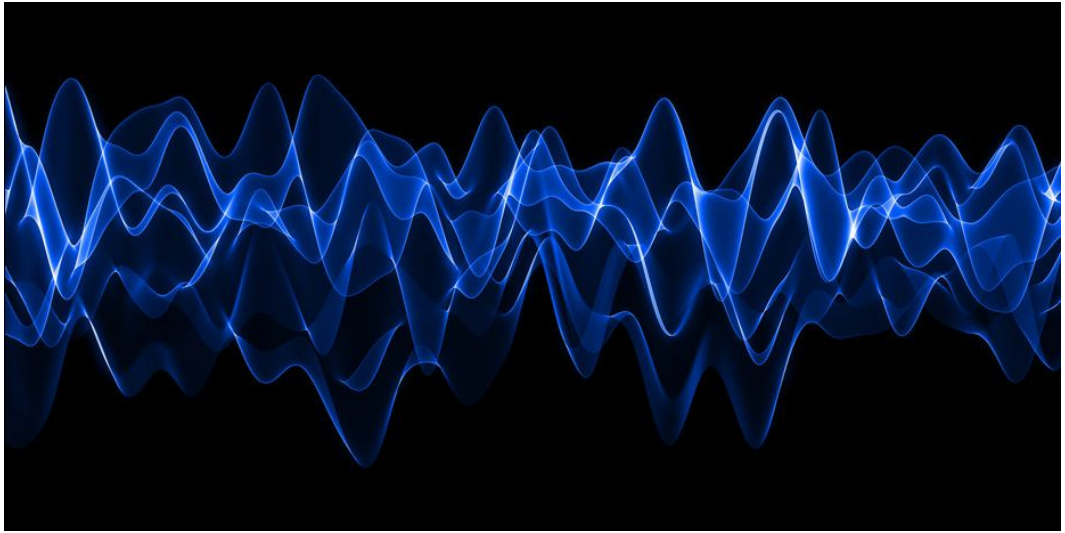


Image source: “ISM Band of Frequency and Allocation” G. Hardestry (www.data-alliance.net)

Frequency plans (US)

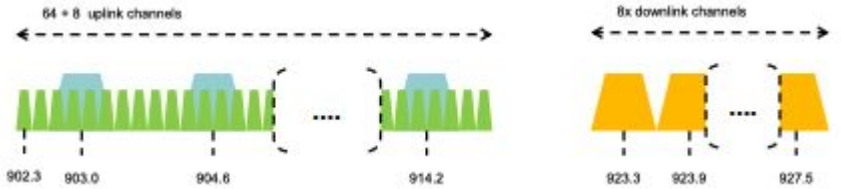
Uplink

64 channels of 125 kHz

8 channels of 500 kHz

Downlink

8 channels of 500 kHz



Data source: “RP002-1.0.3 LoRaWAN Regional Parameters” LoRa Alliance Specification (lora-alliance.org)

LoRaWAN Channels, Frequencies & Sub-bands		
Frequency bands	**Frequency range (MHz)**	**Channels**
Total US Band	902.3 - 914.9	0-63
Uplink sub-bands	**Frequency range (MHz)**	**Channels**
Sub-Band 1	902.3 - 903.7	0 - 7
Sub-Band 2	903.9 - 905.3	8 - 15
Sub-Band 3	905.5 - 906.9	16 - 23
Sub-Band 4	907.1 - 908.5	24 - 31
Sub-Band 5	908.7 - 910.1	32 - 39
Sub-Band 6	910.3 - 911.7	40 - 47
Sub-Band 7	911.9 - 913.3	48 - 55
Sub-Band 8	915.5. -914.9	56 - 63
Downlink sub-bands	**Frequency range (MHz)**	**Channels**
Downlink sub-bands	903.0 - 914.2	64 - 71

Frequency plans (EU)

Uplink

7 channels of 125 kHz

1 channel of 125 / 250 kHz

1 channel FSK

Downlink

1 channel of 125 kHz

Mandatory Channels

868.10, 868.30, & 868.50 MHz

Data source: “RP002-1.0.3 LoRaWAN Regional Parameters” LoRa Alliance Specification (lora-alliance.org)

SNR limit (Signal Quality)

LoRaWAN

Spreading Factor (SF)	SNR limit (dB)
7	-7.5
8	-10
9	-12.5
10	-15
11	-17.5
12	-20

Rx Sensitivity

Bandwidth

Tx Power

Antenna Gain

Thermal noise

+ Many others

Wi-Fi

Data Rate (Mb/s)	SNR limit (dB)
Just to work	4
Basic	5
Smiling users	20
Voice grade	25
256-QAM grade	35
Maximum Effort*	undisclosed

***Max "Data Rate"** is used to advertise unrealistic expectations for user experience" - Jerry Maguire, Wi-Fi Engineer (cut scene)*

Receive Sensitivity

~Data Rate

Lower SF

Distance

Time on air

Higher SF

Spreading factor SF	Receiver sensitivity for bandwidth fixed at 125 kHz	Time on Air (ms)
SF7	-123 dBm	41
SF8	-126 dBm	72
SF9	-129 dBm	144
SF10	-132 dBm	288
SF11	-134.5 dBm	577
SF12	-137 dBm	991

Link budget - comparison

	Tx Power (dBm)	Rx Sensitivity (dB)	Link Budget (dBm)
Wi-Fi	20.5	-75	95.5
LoRa	14	-137	151
NB-IoT	23	-129	152

Data Source: TheThingsNetowork.org

Interference and multi-path

- Propagating **signals interact** with surrounding environment: reflections, refractions, difrations, and scattering
- Rx captures **mix of signals** with different amplitudes, phases, angles of arrival all spread over time
- Testing shows: under conditions of high EM interference - use **smaller BW** and **higher SF**

	Interference	Multipath
White	Immune	Immune
Light-grey	Susceptible	Immune
Dark-grey	Susceptible	Susceptible

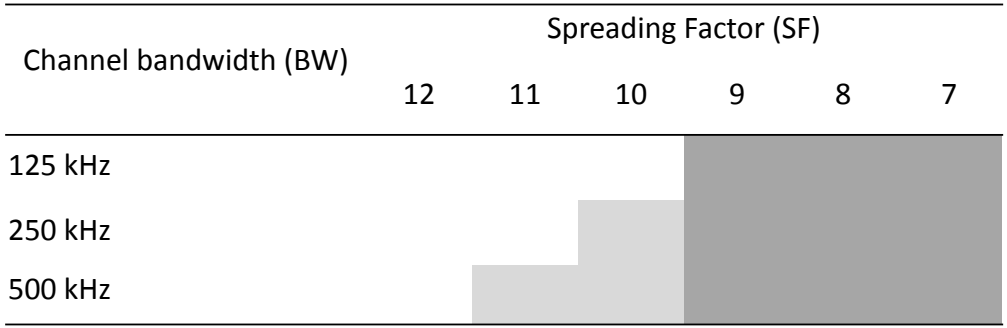


Image source: “LoRa Performance under Variable Interference and Heavy-Multipath Conditions” by K Staniec & M Kowal (www.hindawi.com)

Doppler effect

- Frequency shift due to mobility
- LoRa device moving from or towards the gateway
  - completely negligible in conditions of low data rates and high spreading factors
  - not insignificant for high data rates

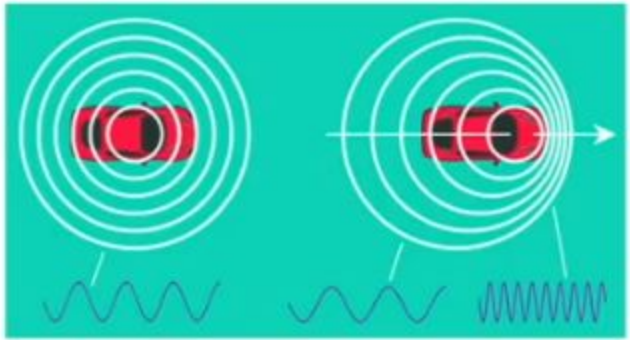


Image source: "What is the Doppler effect?" by Brad Allen Williams (flypaper.soundfly.com)

Range - considerations

Range - considerations

- Range depends on whether there is a line of sight, and whether the gateway is located indoor or outdoor
  - indoor **~ 500 m**
  - outdoor, on top of a house roof **~ 2 km**
  - outdoor, on top of a high-altitude building **> 10 km**
- Gateway elevation example

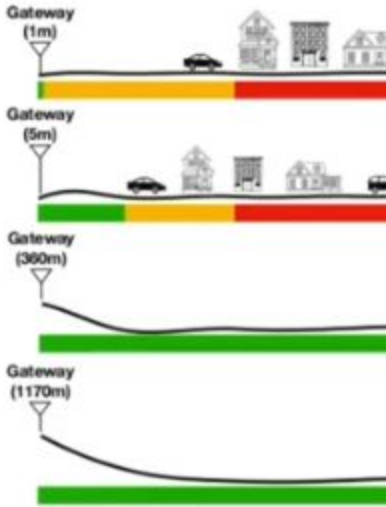


Image source: "How to triple the range of LoRa" by Haystack Technologies Inc.

Devil in the Design Details

LoRaWAN network coverage

- **162 countries** with LoRaWAN deployments in the world
- ~**166** LoRaWAN network operators globally

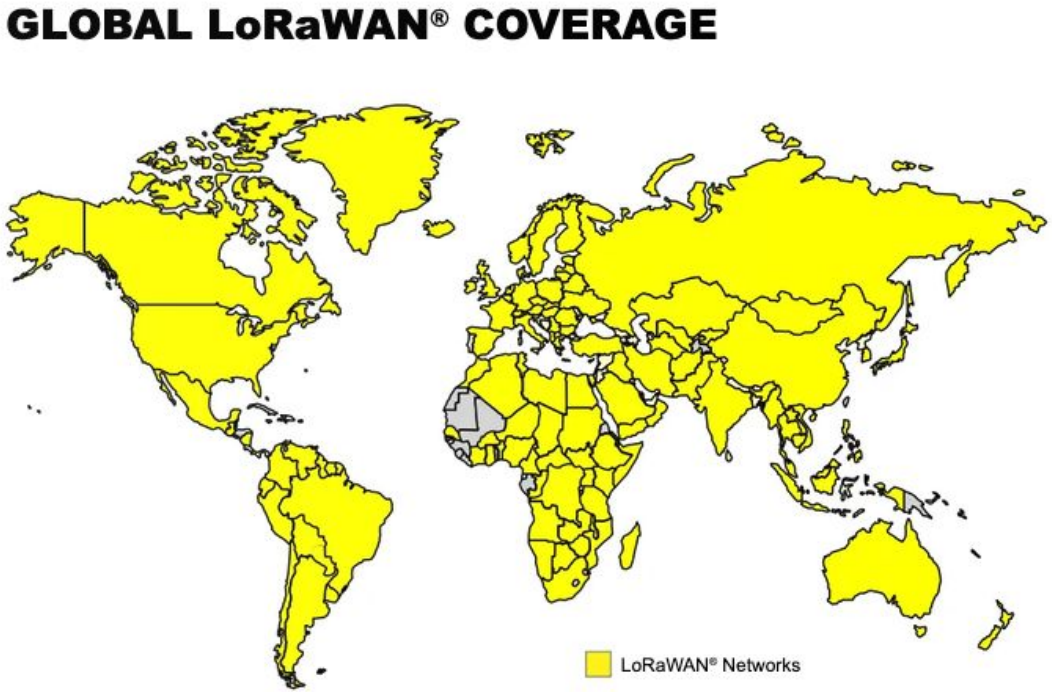
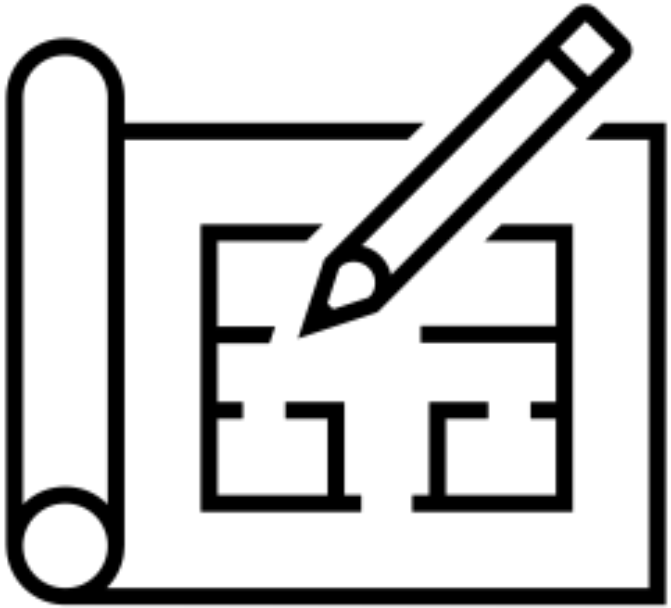


Image source: “LoRa Alliance year end report 2021”

Design Considerations

Suitable use-cases for LoRaWAN:

- Long range - many kilometers
- Low power - several years on coin cell batteries
- Low cost - inexpensive hardware and software
- Low bandwidth (UL)
  - 0.250 - 11 kbit/s (EU)
  - 0.980 - 12.5 kbit/s (NA)
- Coverage everywhere - anywhere you want
- Secure - 128 bit AES encryption end-to-end



Not Suitable for:

- Realtime data - LoRaWAN has rate and size limits
- Phone calls - look at 4G/5G
- Controlling lights in your home - look at Zigbee, BLE, Matter
- Sending photos, watching Netflix - look at Wi-Fi

Regional Parameters

- **Unlicensed** spectrum (ISM)
- Longer range = more restrictions
- Introduced regional parameters
  - Tries to be uniform as possible in different regions of the world
- Some countries support **multiple** frequency plans (e.g. Netherlands with EU868-870 & EU433)
- Max **payload** size also defined in regional parameters

Channel Plan	Common Name
EU863-870	EU868
US902-928	US915
CN779-787	CN779
EU433	EU433
AU915-928	AU915
CN470-510	CN470
AS923	AS923
KR920-923	KR920
IN865-867	IN865
RU864-870	RU864

Data source: “RP002-1.0.3 LoRaWAN Regional Parameters” LoRa Alliance specification (lora-alliance.org)

Data Rate - US915

Tx Power
Bandwidth
Spreading Factor

Data Rate	Configuration (SF+BW)	Bit rate (bit/s)	Uplink/Downlink	Max user payload size (bytes)
0	LoRa: SF12 / 125 kHz	980	Uplink	11
1	LoRa: SF11 / 125 kHz	1760	Uplink	53
2	LoRa: SF10 / 125 kHz	3125	Uplink	125
3	LoRa: SF9 / 125 kHz	5470	Uplink	242
4	LoRa: SF8 / 500 kHz	12500	Uplink	242
5 : 7	Reserved Future Use			
8	LoRa: SF12 / 500 kHz	980	Downlink	53
9	LoRa: SF11 / 500 kHz	1760	Downlink	129
10	LoRa: SF10 / 500 kHz	3900	Downlink	242
11	LoRa: SF9 / 500 kHz	7000	Downlink	242
12	LoRa: SF8 / 500 kHz	12500	Downlink	242
13	LoRa: SF7 / 500 kHz	21900	Downlink	242
14	Reserved Future Use			
15	Define in LoRaWAN			

Data Rate - EU868

Device classes

Class A

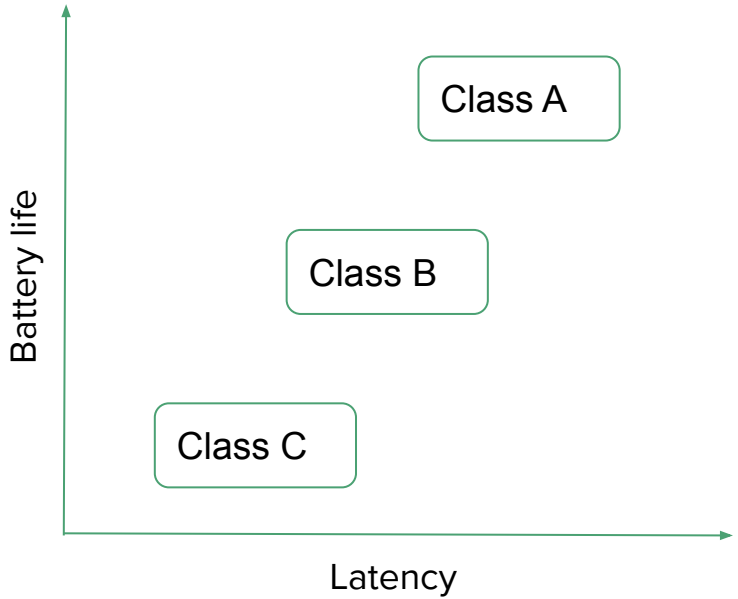
- **ALL** end-devices must support class A
- Schedule **up to two Rx** window(s) (RW) immediately after a corresponding uplink Tx

Class B

- **Beacons**
- Devices can schedule **additional RWs**

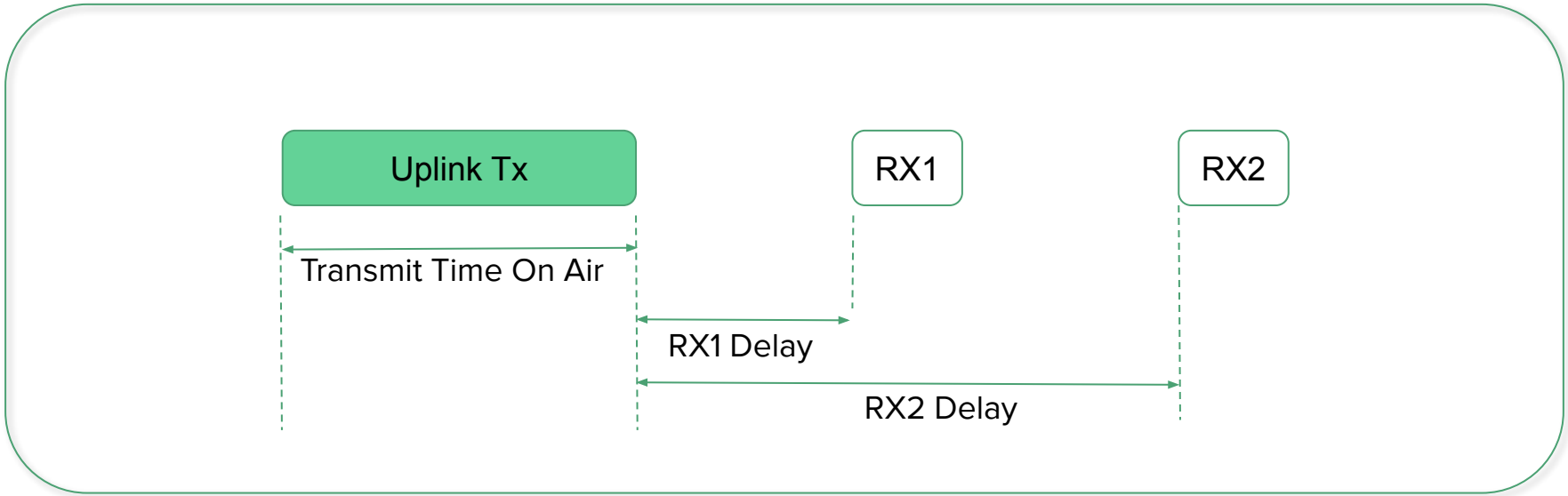
Class C

- Devices **continuously listen** and can receive almost anytime (not when transmitting)

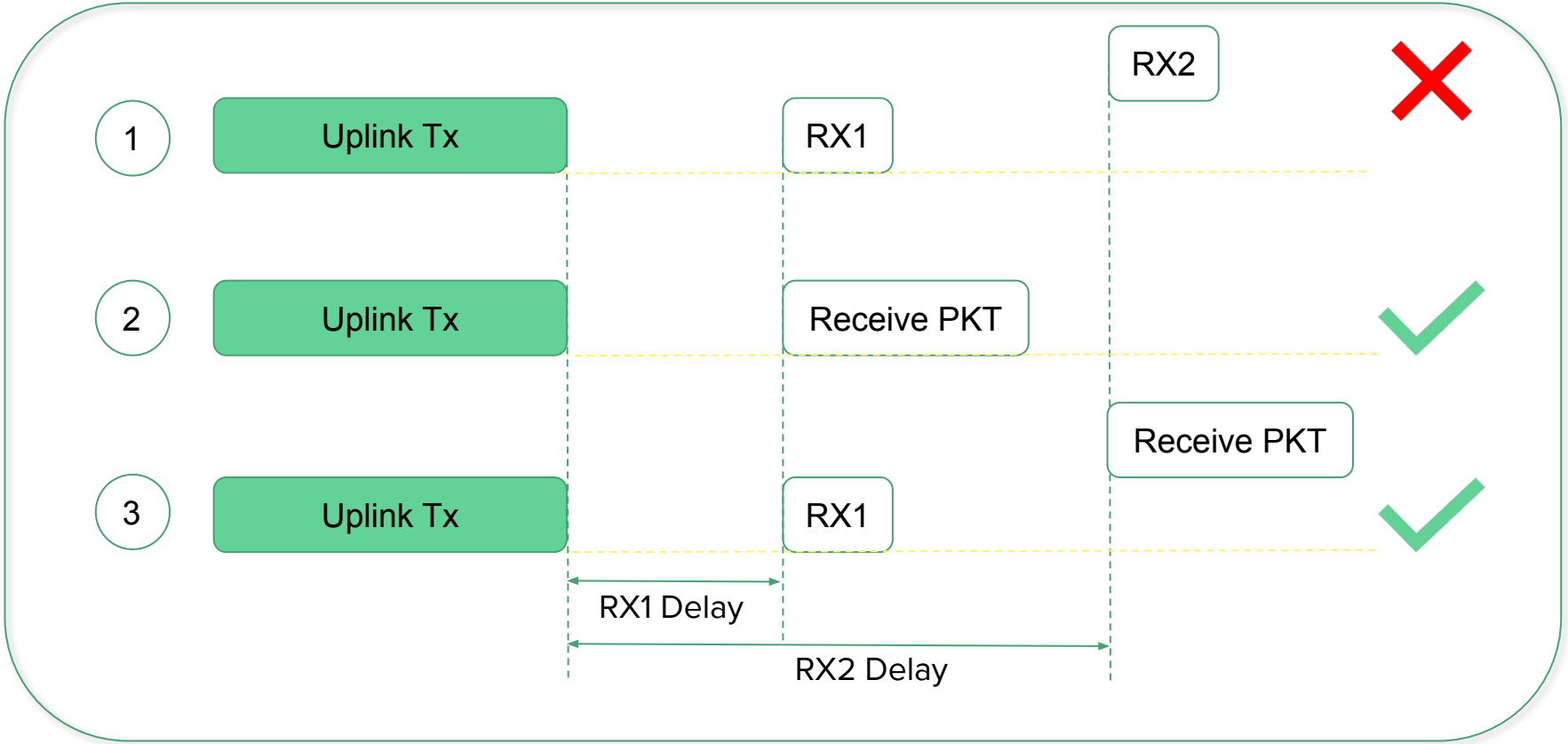


Global Timers

Class A

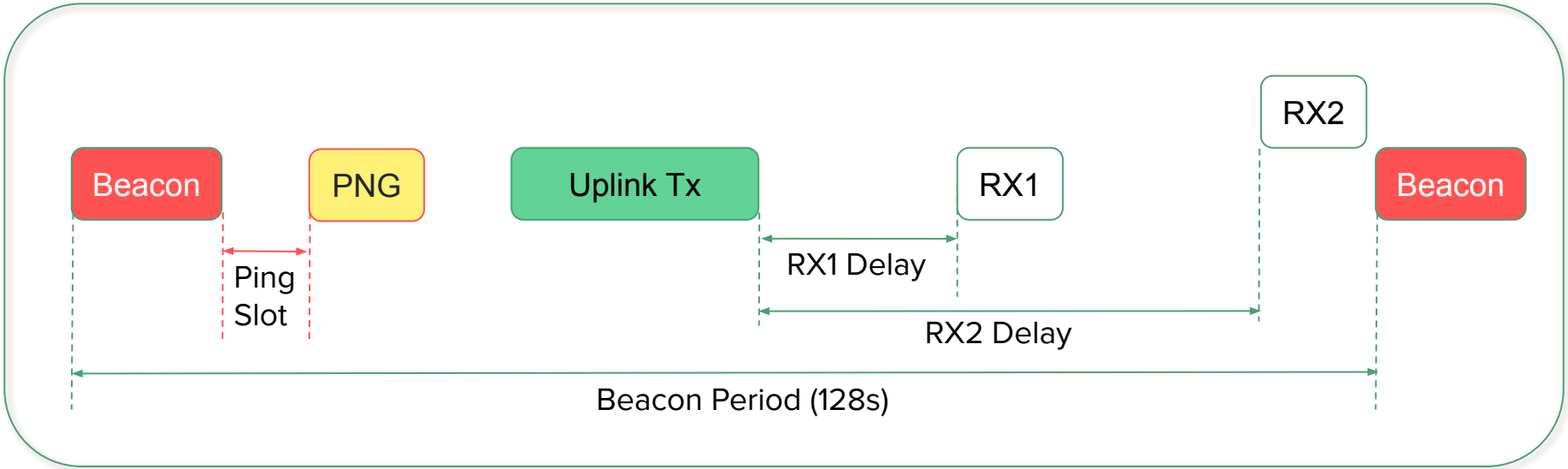


Class A - Examples

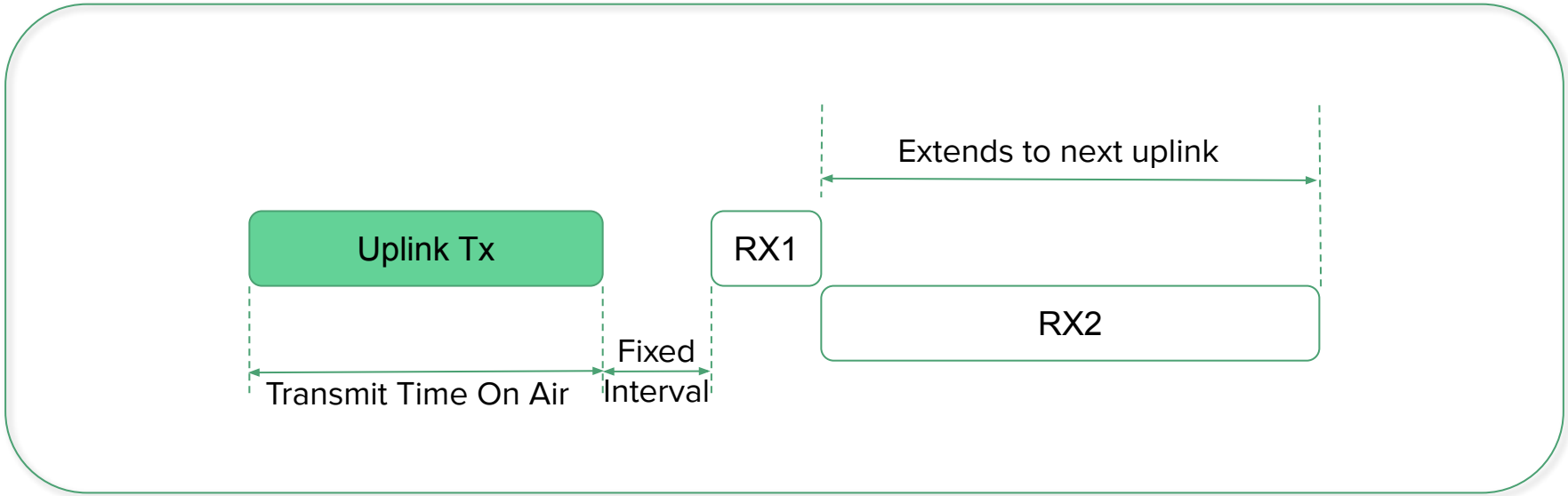


Original Image: The Things Network: https://www.thethingsnetwork.org/docs/lorawan/classes/

Class B


Beacon
PNG
Uplink Tx
RX1
RX2
Beacon
Ping
Slot
RX1 Delay
RX2 Delay
Beacon Period (128s)

Class C


Extends to next uplink
Uplink Tx
RX1
RX2
Fixed
Interval
Transmit Time On Air

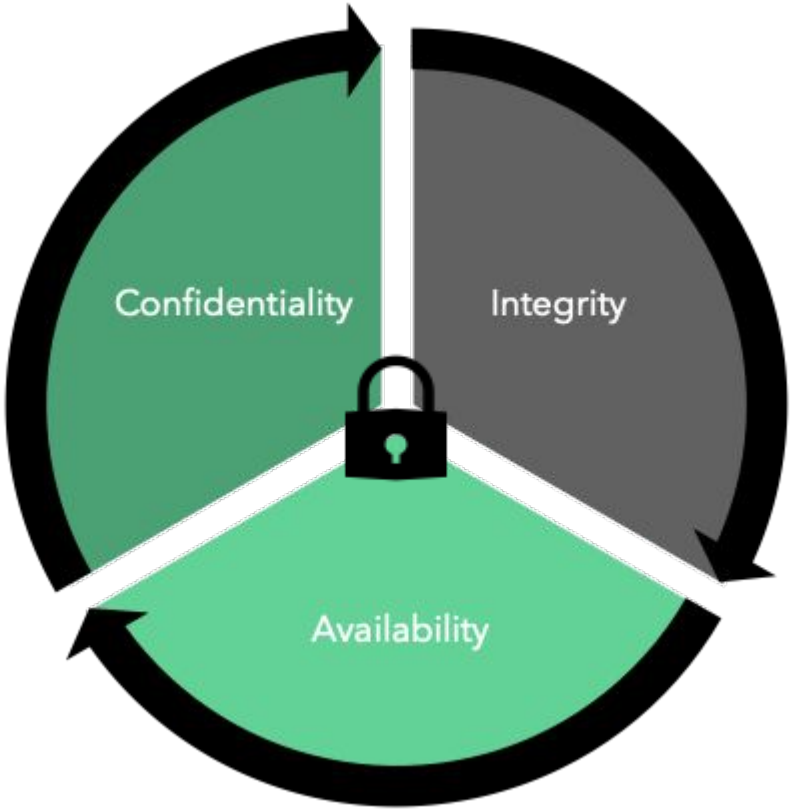
‘Deets’ on LoRaWAN Security

Is LoRa PHY secure?

Physical layer does not provide security mechanisms

Optional CRC field - helps detecting transmission errors

Three pillars of security



LoRaWAN two-layer security

Two-layer security with AES encryption algorithm:

128 bit Network Security Key (**NwkSKey**)

128 bit Application Security Key (**AppSKey**)

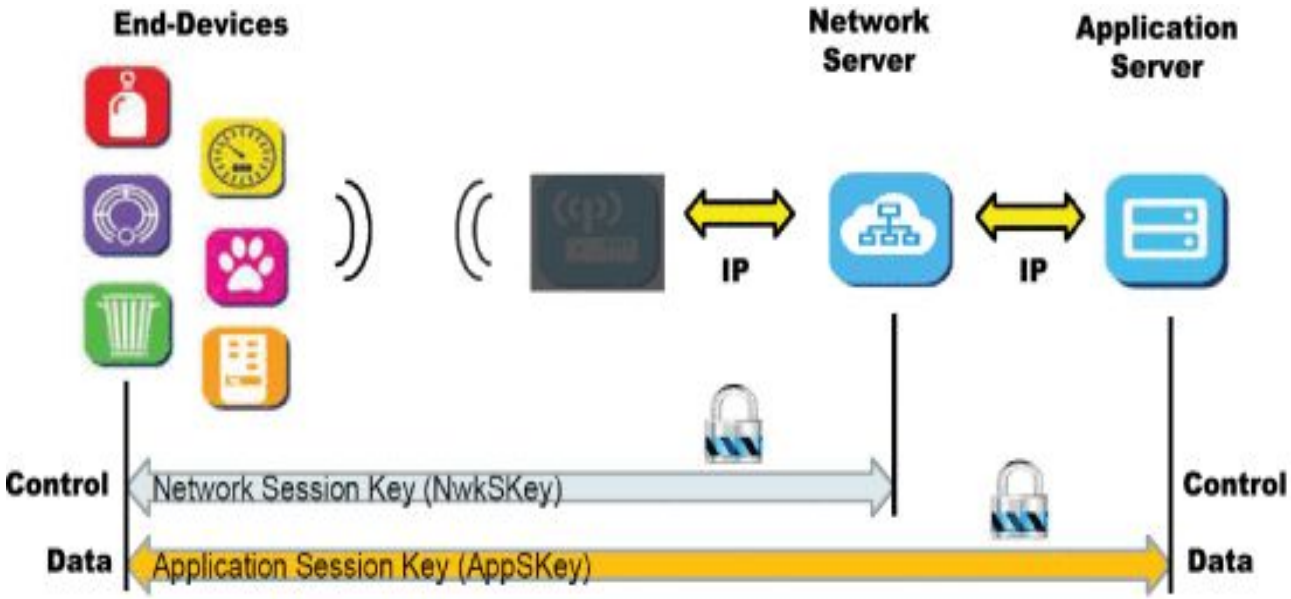


Image Source: "AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments" K. Tsai, et al (ieeexplore.ieee.org)

Frame Security

MAC header, Frame header and encrypted payload are protected by a Message Integrity Code (MIC)

Modified or spoofed data fails as MIC calculated receiver will not equal the received MIC

Each pair of end-device and network server (application server) has an unique NwkSKey (AppSKey)

Frame counters are incremented and never reused

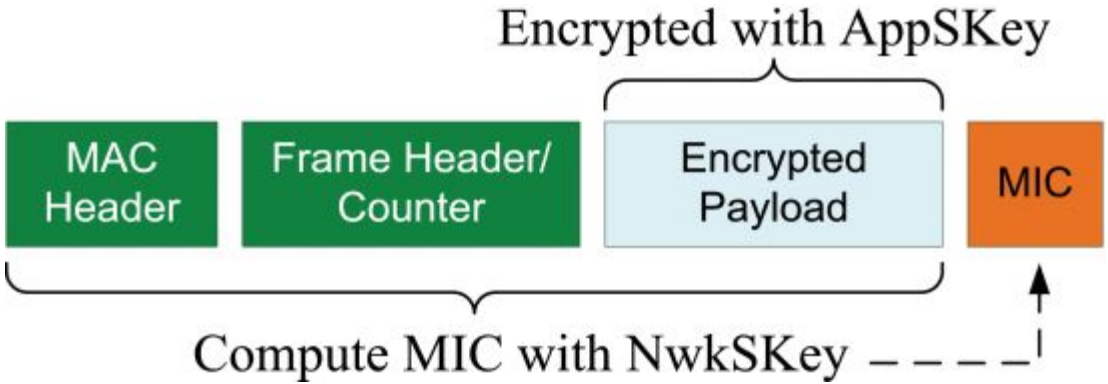


Image Source: "AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments" K. Tsai, et al (ieeexplore.ieee.org)

Two ways to establish a LoRaWAN session

Over-the-air activation (OTAA)	Activation by personalization (ABP)
Device manufacturers autonomously generate essential provisioning parameters	A simplified (less secure) commissioning process
New and secure keys are derived each session, for length of the session	IDs and Keys are personalized at fabrication
Devices can store multiple “identities” to dynamically and securely switch networks and operators during its lifetime	Devices become immediately functional upon powering up; the join procedure is skipped
High-grade, tamper-proof security options are available	DevAddr are tied to a specific network/service; the NetID is a portion of the device network address
Join any LoRaWAN network	Preconfigured network

Key Security Elements

Join Procedure

- Establishes mutual authentication
- Only authorized devices allowed to join network

Message Authentication

- MAC and application messages have non-repudiation & integrity
- End-to-end encryption from device to application

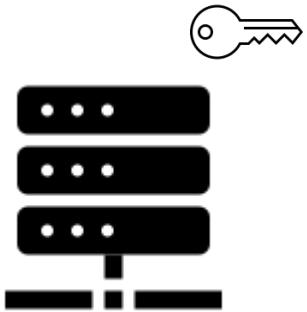
Join Server

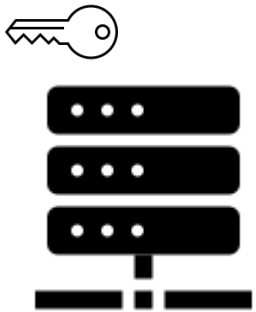
Dedicated server to handle **dynamic DevAddr** and **session key** generation during device activation in any LoRaWAN network

Authentications both **Network** and **Applications** servers

Stores **root keys**

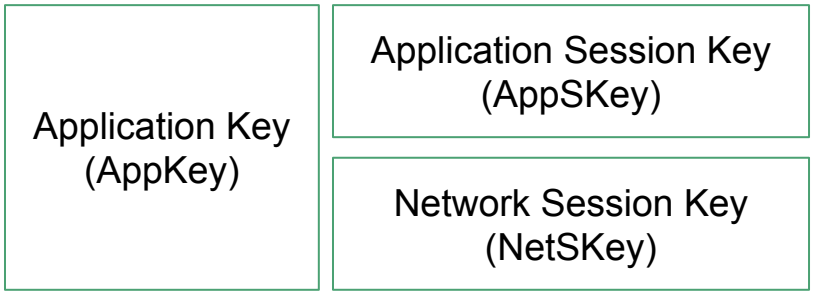
Recommended way to deploy



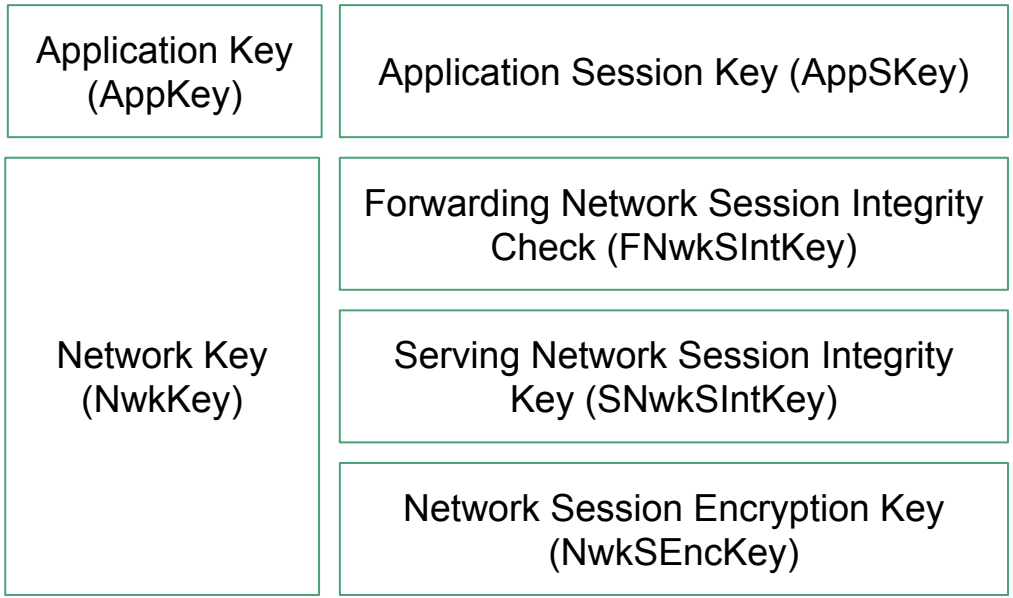


LoRaWAN keys...

Keys in LoRaWAN version 1.0.x



Keys in LoRaWAN version 1.1.x

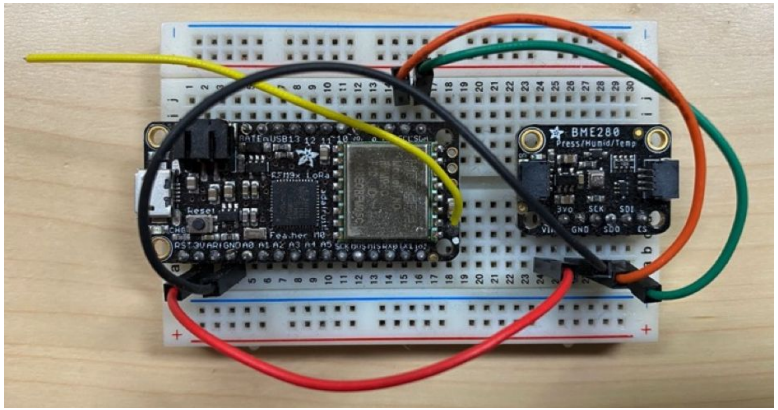


Building a LoRaWAN home lab

Choose your LoRaWAN end-device(s)

Vast ecosystem

- Water meters
- Temperature meters
- Soil sensor stations
- Air quality stations
- GPS trackers
- + Many more



Choose your LoRaWAN gateway

Regional frequency support

Packet forwarder

Number of channels

RF filters

IP routing

Remote management

4G / 5G / Ethernet / Wi-Fi backhaul

Choose your server(s)

Server

- Network
- Application
- Join

Public / **Private**
(TheThingsNetwork,ChripStack)

Cloud (e.g. Azure-IoT, Google-IoT)

Summary

What is LoRa?

- **Sub - 1GHz** (e.g 433, 780, 868, 915 MHz)
- Adaptive data rates (**ADR**)
- Modulation derived from **Chirp Spread Spectrum (CSS)** using chirp pulse
- Ideal for sending **small** nuggets of data with **low** data rate over **long** distances
- End-to-end security (**AES 128 bit**) between end-point(s) and application server(s)

Best Practices (Optimization)

LoRaWAN Certified

Eliminated Unnecessary Join Requests

Limit Transmission Length, Payload Size, and Duty Cycle

Synchronization, Backoff, and Jitter

Use a good Random Number Generator

Use ADR for Stationary Devices

Use OTAA over ABP

Power Cycles / Persistent Memory

Frame Counters

Ack (wait at least 3) before assuming packet loss

Support Force Rejoin Command or Downlink

FIN ACK

@troymart