IoT Networking, part II

LPWAN, LoRaWAN, The Things Network

Sebastian Büttrich 202402

Networking / part I / Recap

- Criteria for networking options in IoT:
  Power, reach, bandwidth, cost,
  security, business aspects and more

- Properties of the physical layer: Frequency, bandwidth and their impact

- Basic terms: **LPWAN**, LOS/NLOS, *Modulation (Spread Spectrum)*

- The most relevant options (in 2018) and their main characteristics:
  LoRa, ~~Sigfox~~, NB-IOT, RPMA, Zigbee, Bluetooth, WiFi, Cellular (GSM, LTE-..)

Short recap: Modulation & encoding

In electronics and telecommunications, **modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a modulating signal that typically contains information to be transmitted.** Most radio systems in the 20th century used frequency modulation (FM) or amplitude modulation (AM) to make the carrier carry the radio broadcast.

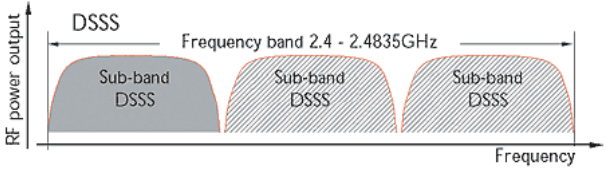
Modulation techniques include
Spread Spectrum (e.g. FHSS Frequency Hopping) used in Bluetooth,
direct-sequence spread spectrum (DSSS) used in 802.11b,
Orthogonal frequency-division multiplexing (OFDM) used in 802.11a/g/n/c,
Chirp spread spectrum (CSS) as used in LoRa.

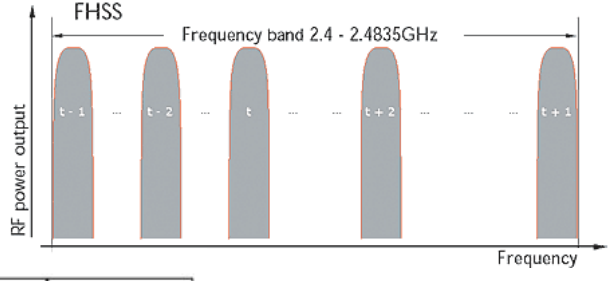
These techniques are crucial for the **robustness against noise and utilization of spectrum.**

Read more here:
https://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

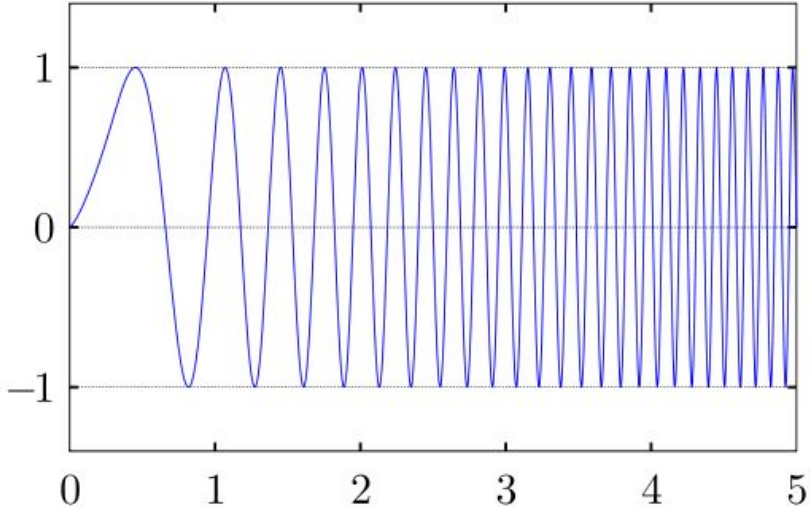
Modulation & encoding

Spread Spectrum
(e.g. **FHSS Frequency Hopping Hedy Lamarr, 1942)**)
used in Bluetooth, 802.11
direct-sequence spread spectrum (DSSS) used in 802.11b,





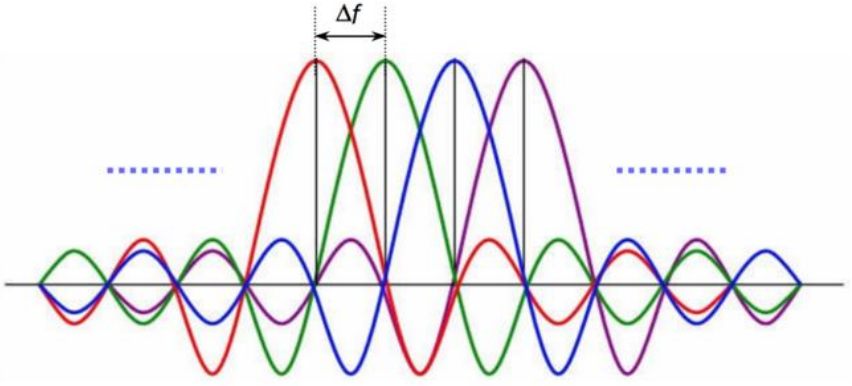
Chirp spread spectrum (CSS) as used in LoRa.



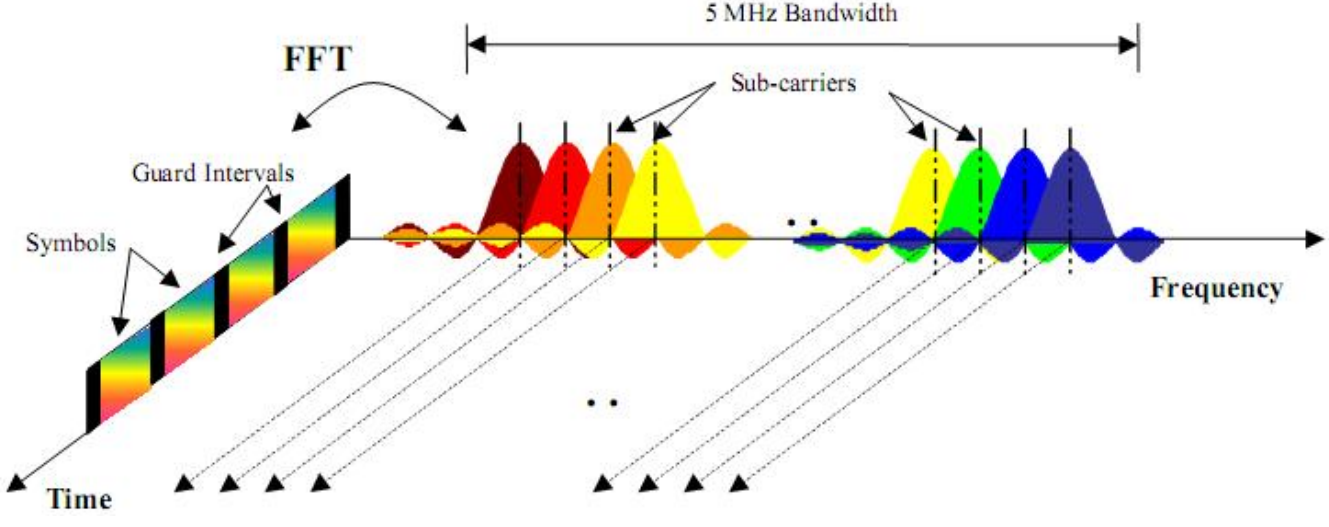
Source:
IEBMedia http://www.iebmedia.com/index.php?id=4466,
wikipedia

Modulation & encoding: OFDM

Idea: Overlapping carriers with a spacing such that neighbouring carriers' sidebands cancel each other out.
(Orthogonality)



Source:
IEBMedia http://www.iebmedia.com/ir
wikipedia



Agenda

- LoRa
- LoRaWan
- TheThingsNetwork

IoT – Internet of Things

within **IoT**

LPWAN – Low Power Wide Area Networks

one possible LPWAN: LoRaWAN

Physical Layer – LoRa

MAC Layer – LoRaWAN

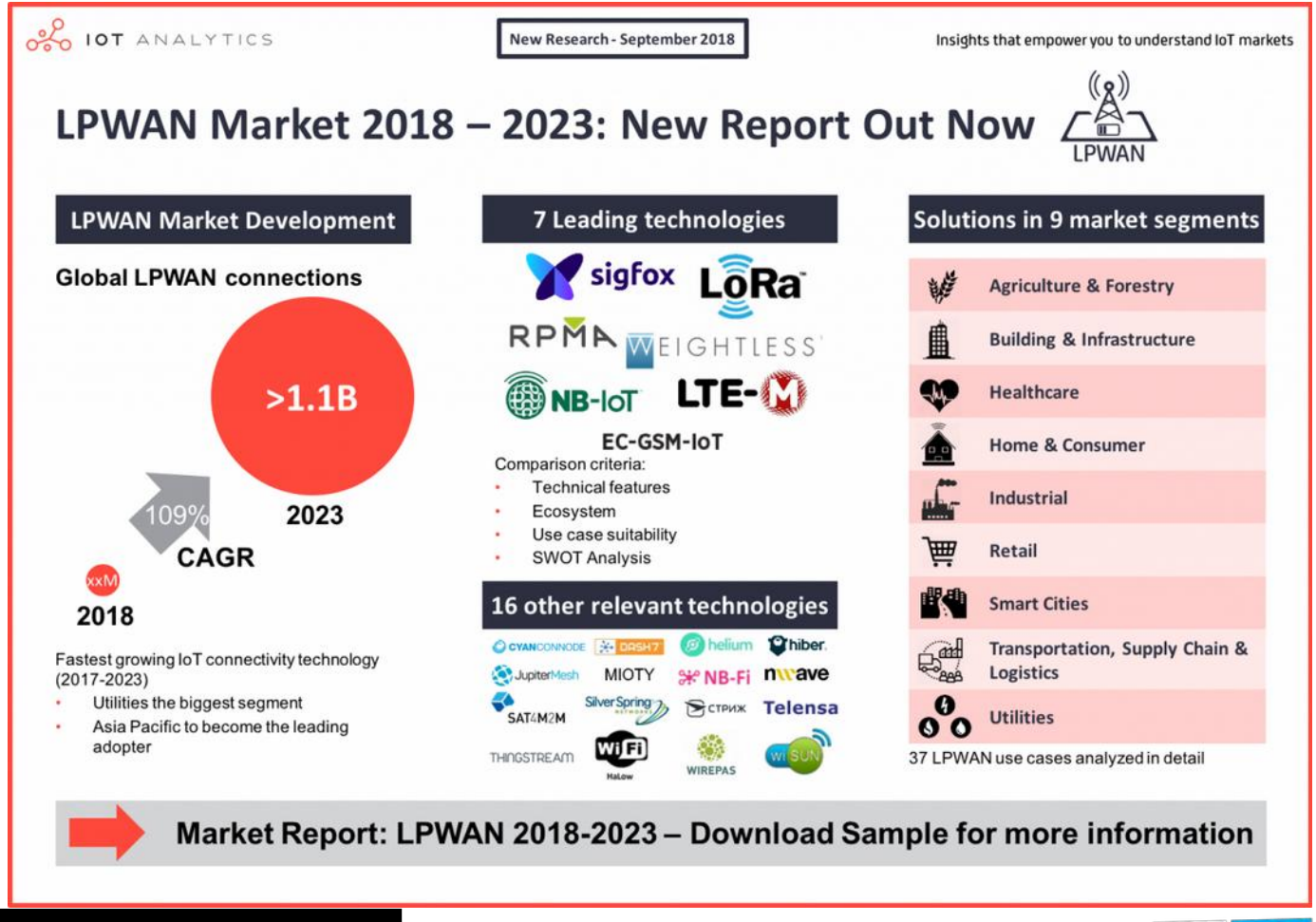
one possible LoRaWAN: The Things Network

LoRa™

LoRaWAN™

THE THINGS NETWORK

LPWAN / market



____ / a note

In what follows, keep an eye on the sources of information -

some of the documents come from industry organizations and companies – so there will be bias.

Alwas read any source with a critical eye.

While the author of these slides
is not affiliated with any of the entities,
he clearly has preferences!

LoRa / 1

LoRa is a **proprietary Layer 1 (physical layer) standard** owned by Semtech

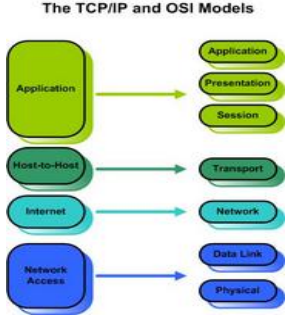
Chirp Spread Spectrum (CSS)

Bandwidth 125/250/500 kHz

Frequencies in Europe initially*: **ISM 433/868 Mhz**

Data Rate up to 11 kbps

Focus is on **long range, power efficiency, robustness.**



https://www.semtech.com/lora/what-is-lora

* 2.4 Ghz added 2021, other regions have other frequencies

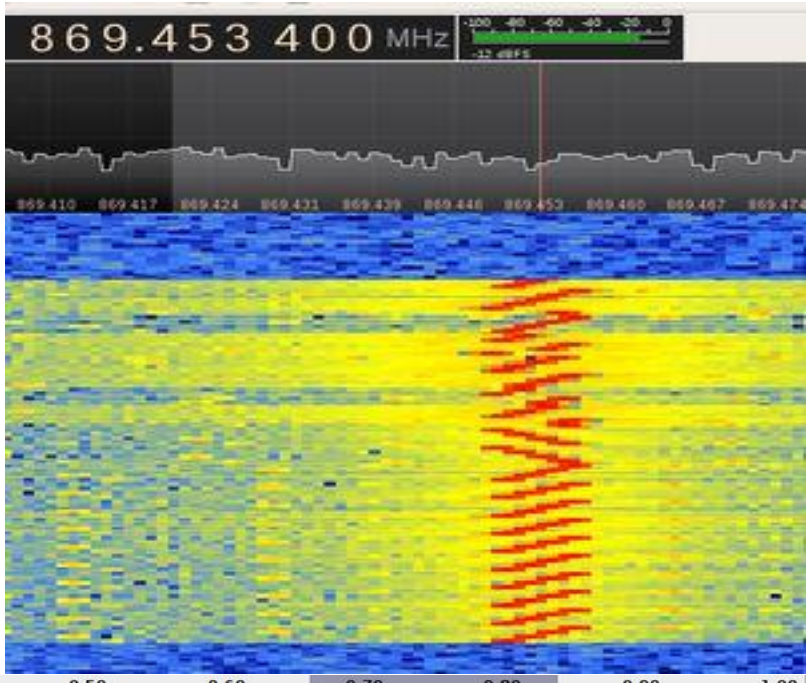
LoRa / 2 / CSS

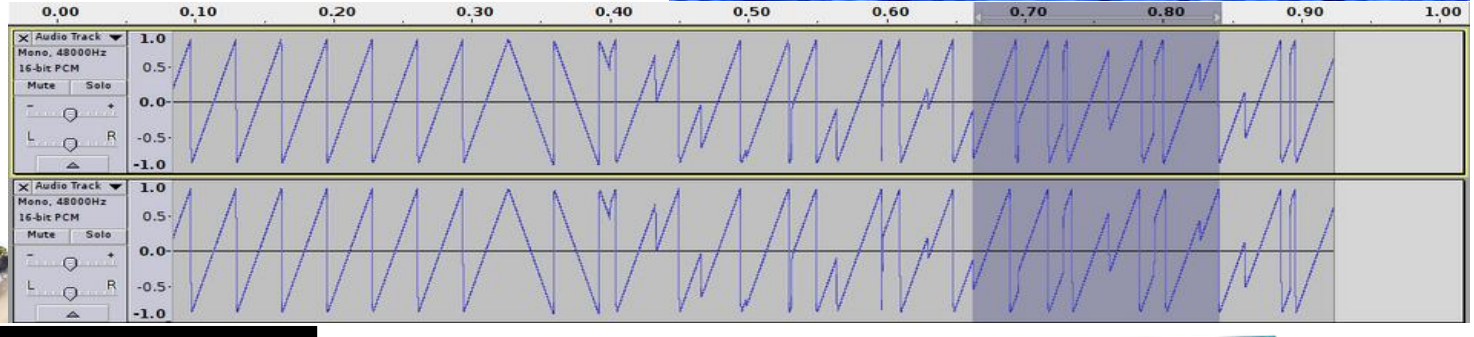
Chirp Spread Spectrum

What is a chirp?

Source: https://revspace.nl/DecodingLora

Preamble (of variable length), here:
10 up, 2 down ->



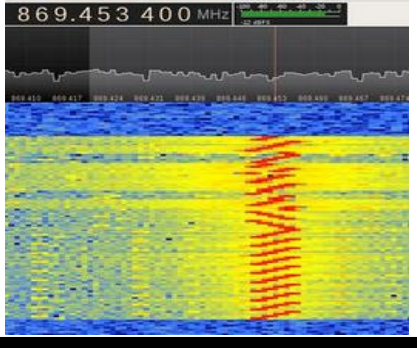


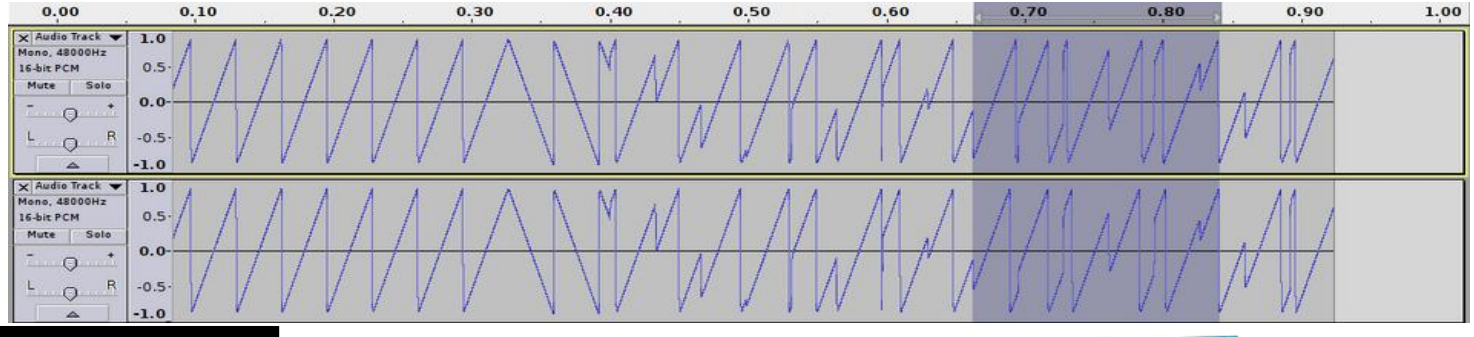
LoRa / 2a / How to study spectrum?

SDR Software Defined Radio

RTL-SDR, USB Dongles of many types
(from $20 up)

software:
gnuradio
gqrx
audacity for audio analysis

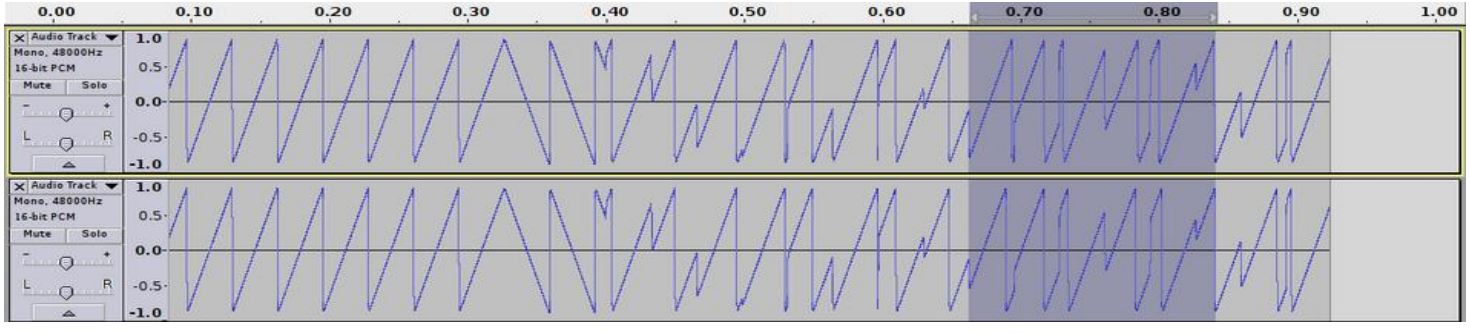




LoRa / 3 / CSS details

Modulation details, reverse engineering:

Semtech: AN1200.22 - LoRa Modulation Basics – Dev portal or https://www.frugalprototype.com/wp-content/uploads/2016/08/an1200.22.pdf
https://lora-alliance.org/lorawan-for-developers/
https://revspace.nl/DecodingLora#Modulation_basics
https://myriadrf.org/blog/lora-modem-limesdr/
https://static1.squarespace.com/static/54cecce7e4b054df1848b5f9/t/57489e6e07eaa0105215dc6c/1464376943218/Reversing-Lora-Knight.pdf



LoRa / 4 / SF & CR

Spreading Factor SF

$$\mathrm{SF} = \frac{\text{chip rate}}{\text{symbol rate}}$$

(think of it as “one bit is spread out over so and so many pulses”:
one symbol = $2^{\text{SF chirps}}$

Control rate CR, determines depth of forward error coding

(Think of it as saying
CCCAAAFFFEEE or CAFECAFECAFE
instead of CAFE)

LoRa / 5 / Interleaving

“Mixing up the letters to gain robustness against *burst errors*”

```
Transmitted sentence:              ThisIsAnExampleOfInterleaving...
Error-free transmission:           TIEpfeaghsxlIrv.iAaenli.snmOten.
Received sentence, burst error:    TIEpfe______Irv.iAaenli.snmOten.
after deinterleaving:              T_isI_AnE_amp_eOfInterle_vin_...
```

LoRa / 6 / Data Rate

Data Rate depends on Bandwidth, CR, SF

$$R_b = SF * \frac{\left[\frac{4}{4+CR}\right]}{\left[\frac{2^{SF}}{BW}\right]} * 1000$$

SF = Spreading Factor (6,7,8,9,10,11,12)

CR = Code Rate (1,2,3,4)

BW = Bandwidth in KHz
(10.4,15.6,20.8,31.25,41.7,62.5,125,250,500)

Rb = Data rate or Bit Rate in bps

https://www.rfwireless-world.com/calculators/LoRa-Data-Rate-Calculator.html

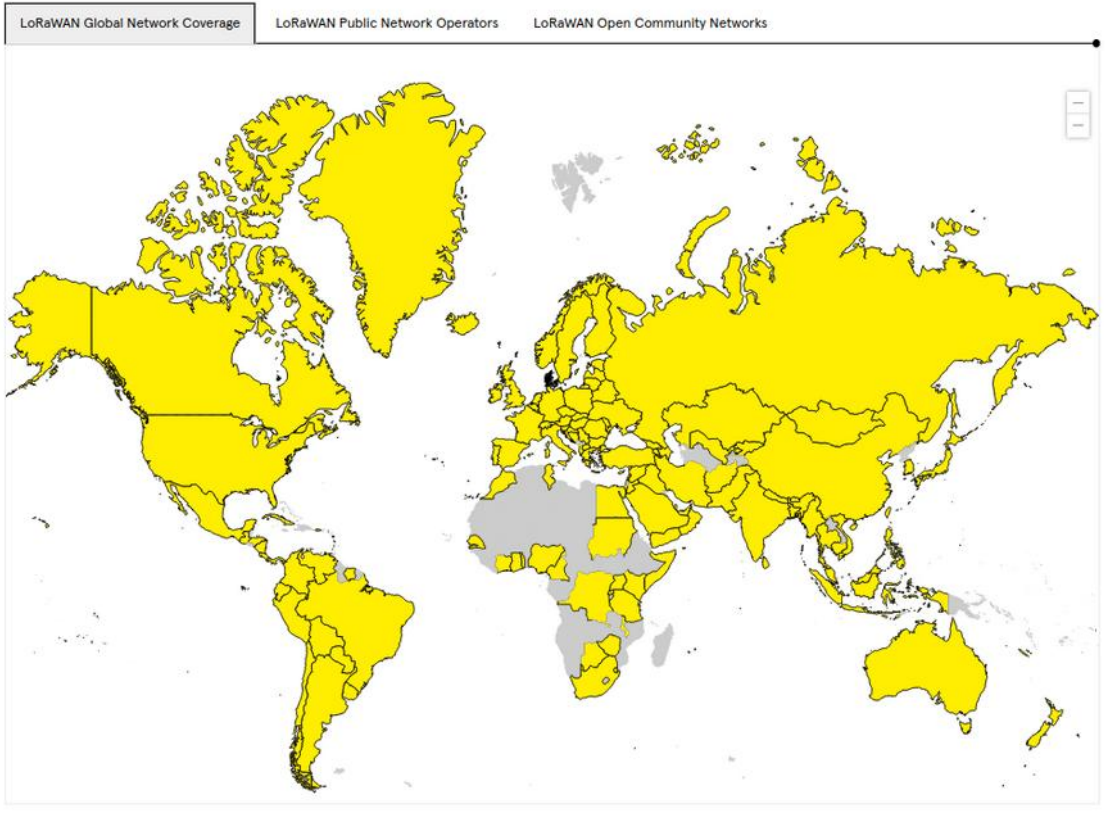
LoRaWan / 1

- LoRaWan is an open LPWAN standard building on top of LoRa
- https://www.lora-alliance.org/

LoRaWAN

An open specification, maintained by the LoRa-Alliance

181 LoRaWAN Network Operators globally.

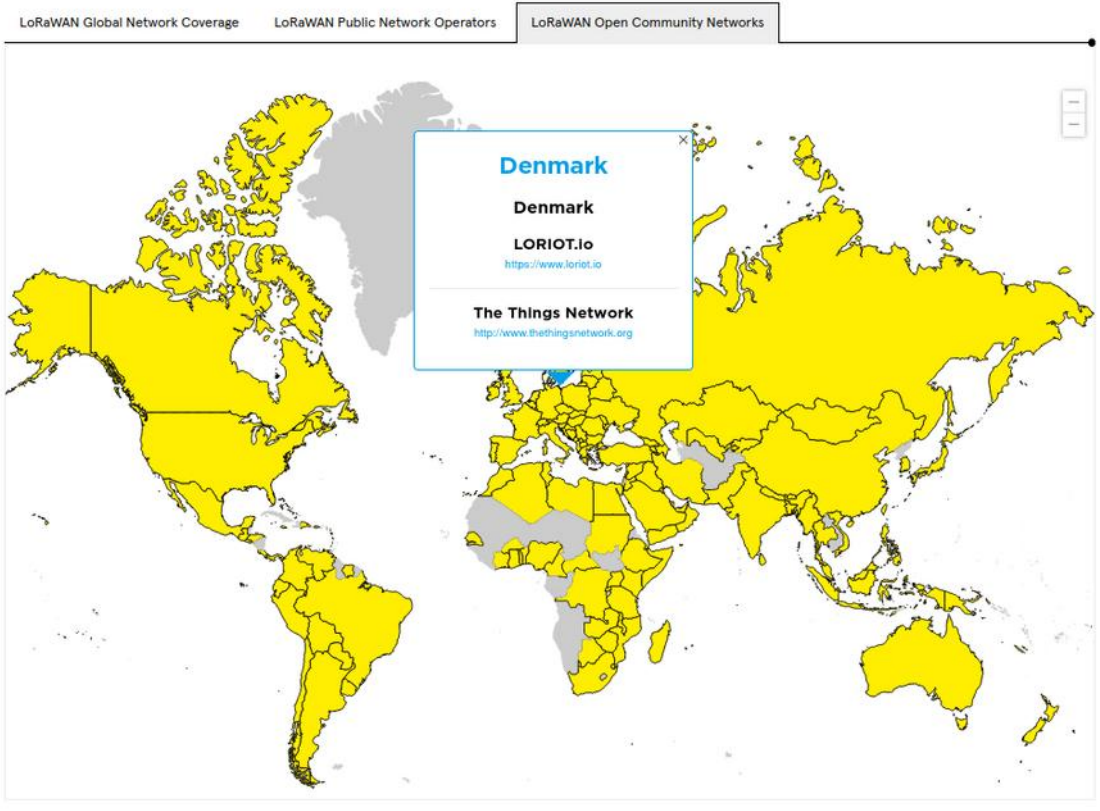


THE THINGS NETWORK

LoRaWAN

A variety of commercial and community operators

181 LoRaWAN Network Operators globally.

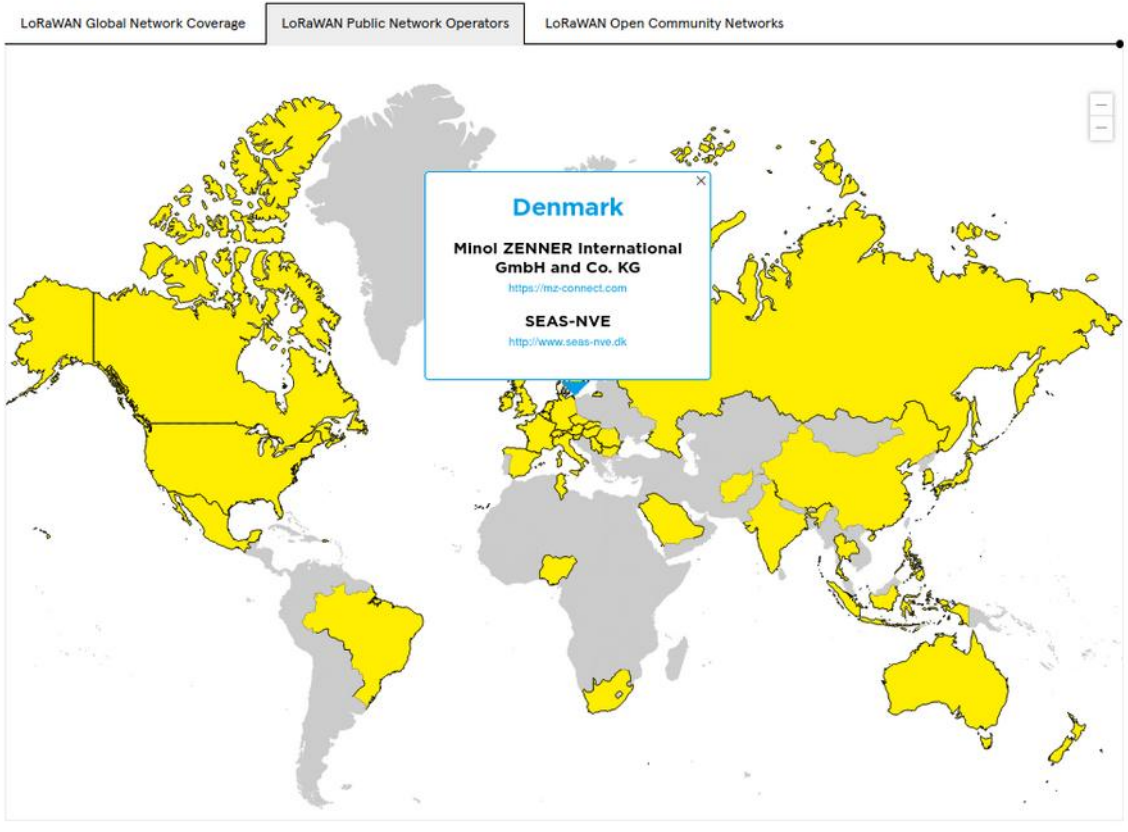


THE THINGS NETWORK

LoRaWAN

A variety of commercial and community operators

181 LoRaWAN Network Operators globally.

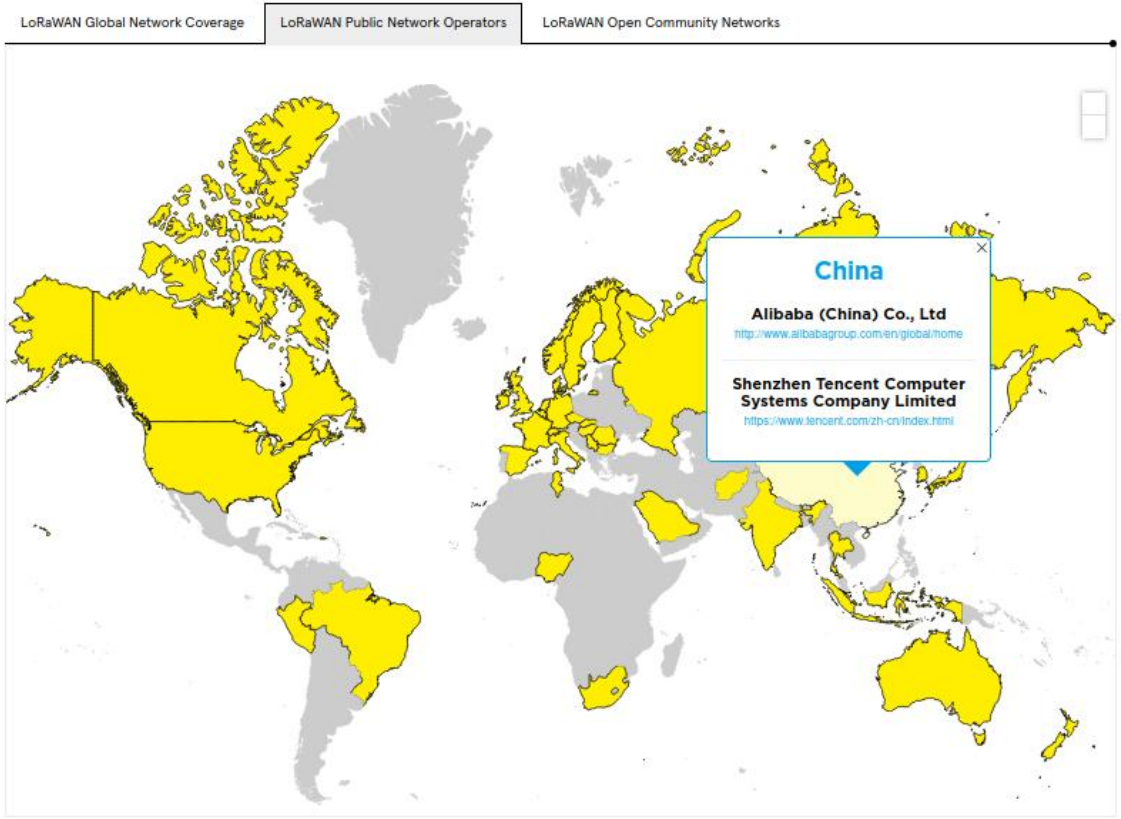


THE THINGS NETWORK

LoRaWAN

Commercial operators / China

166 LoRaWAN Network Operators globally.



THE THINGS NETWORK

LoRaWan / 3 / scope

LoRaWAN™ addresses:

architecture
topology
entities
addressing
data rates
mobility
localization
security

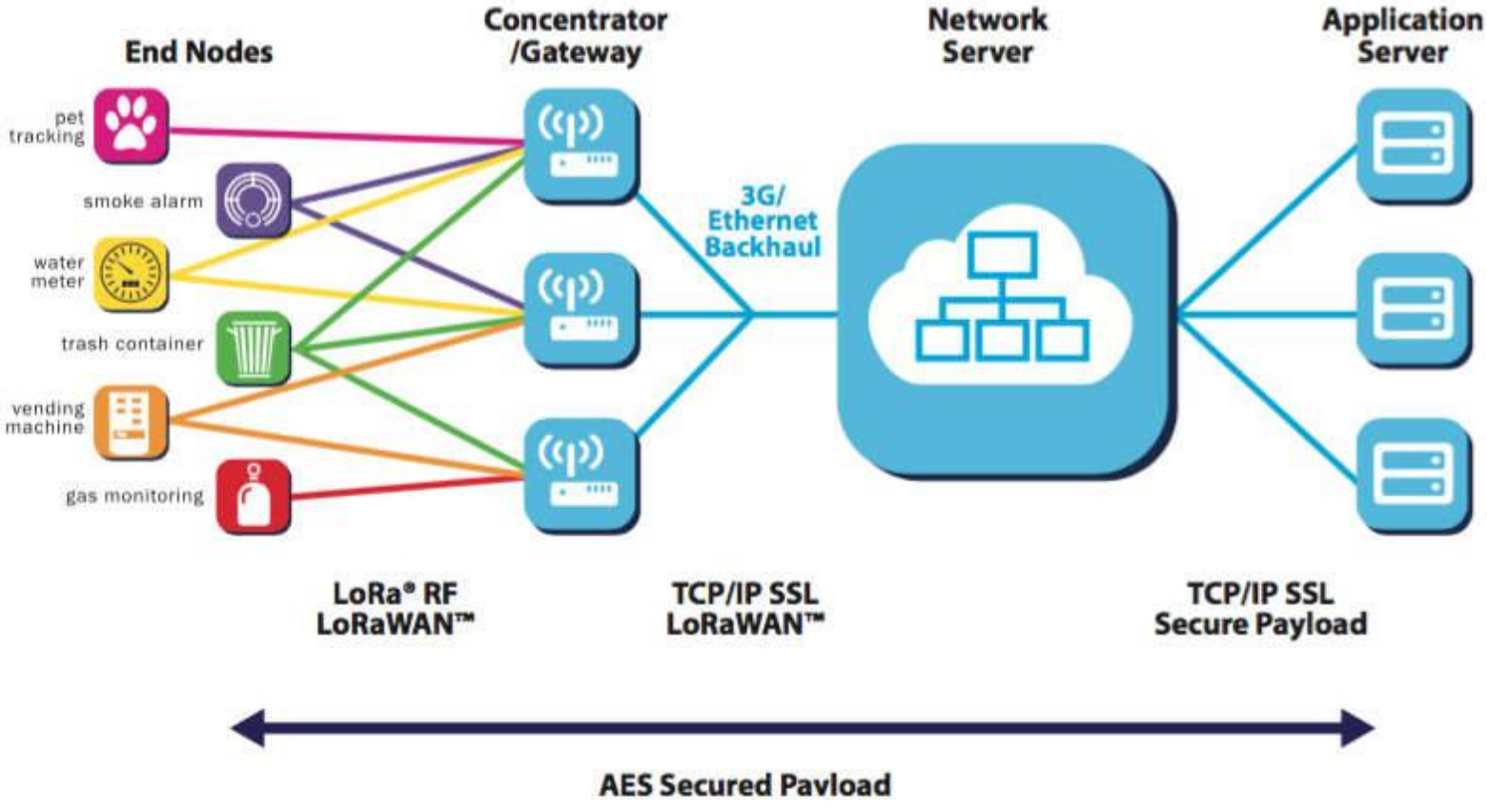
Details:

https://www.lora-alliance.org/What-Is-LoRa/Technology

LoRaWan / 4 / topologies & entities

- **Star-of-stars topology**
- **Gateways** are transparent bridges relaying messages between **end-devices** and a central **network server** in the backend.
- **Gateways are connected** to the network server via **standard IP connections** while end-devices use single-hop wireless communication to one or many gateways.
- All end-point communication generally **bi-directional**, supports **multicast** enabling **software upgrade over the air** or other mass distribution messages

LoRaWan / 5 / architecture



LoRaWan / 6 / device classes

Device classes

A Battery powered, small loads, long breaks, long latency, unicast

B low latency, scheduled receive slots, periodic beacon from gateway, uni/multicast, higher power, 14-30 mA

C no latency, uni/multi, constantly receiving, power hungry

Classes can be dynamically assigned / changed

Source, Details:

https://lora-alliance.org/about-lorawan/

LoRaWan / 7 / addressing

Devices and applications

have a 64 bit / 8 byte unique identifier (DevEUI and AppEUI).

When a device joins the network, it receives a dynamic (non-unique) 32-bit / 4 byte address (DevAddr).

Source, Details:

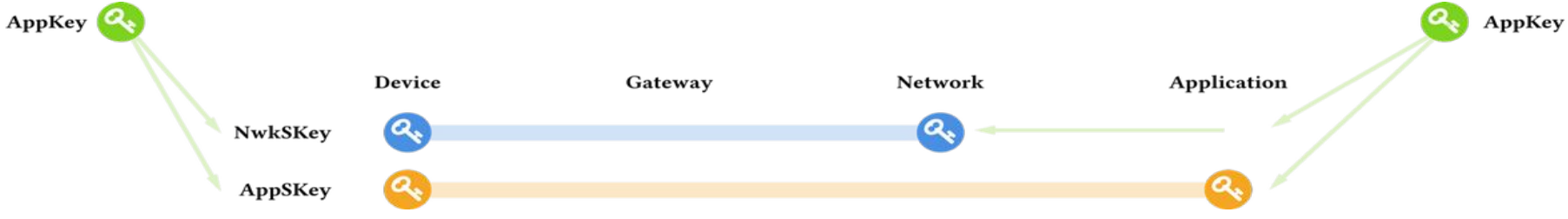
https://www.thethingsnetwork.org/docs/lorawan/

LoRaWan / 8 / Security / keys

Security measures:
three distinct 128-bit AES keys:
The **application key AppKey** is only known by the device and by the application. When a device joins the network (this is called a join or activation), an application session key **AppSKey** and a network session key **NwkSKey** are generated. The NwkSKey is shared with the network, while the AppSKey is kept private.

Source, Details:

https://www.lora-alliance.org/What-Is-LoRa/Technology



LoRaWan / 9 / Security / frame counter

The **frame counter in LoRaWAN** messages is a security measure used to detect **replay attacks**. After validating the MIC, the Broker checks if the Frame counter is valid. As frame counters can only increase, a message with a frame counter that is lower than the last known frame counter should be dropped. Additionally, the Broker has to verify that the gap between the last known frame counter and the counter in the message is not too big. According to the LoRaWAN specification, the maximum gap is 16384.

Source, Details:

https://www.lora-alliance.org/What-Is-LoRa/Technology

LoRaWan / 10 / data rates

LoRaWAN abstracts the PHY data rates of LoRa – for EU / CN:

- EU 863-870 MHz (LoRaWAN Specification (2015), Page 35, Table 14)
- CN 779-787 MHz (LoRaWAN Specification (2015), Page 44, Table 25)
- EU 433 MHz (LoRaWAN Specification (2015), Page 48, Table 31)

DataRate	Modulation	SF	BW	bit/s
0	LoRa	12	125	250
1	LoRa	11	125	440
2	LoRa	10	125	980
3	LoRa	9	125	1'760
4	LoRa	8	125	3'125
5	LoRa	7	125	5'470
6	LoRa	7	250	11'000
7	FSK 50 kbps			50'000

https://blog.dbrgn.ch/2017/6/23/lorawan-data-rates/

LoRaWan / 11 / duty cycles

LoRaWAN implements duty cycle rules made by regulators:

In Europe, duty cycles are regulated by section 7.2.3 of the ETSI EN300.220 standard. This standard defines the following sub-bands and their duty cycles:

- **g** (863.0 – 868.0 MHz): 1%
- **g1** (868.0 – 868.6 MHz): 1%
- **g2** (868.7 – 869.2 MHz): 0.1%
- **g3** (869.4 – 869.65 MHz): 10%
- **g4** (869.7 – 870.0 MHz): 1%

+ duty cycle for join channel: 1%

On top of that, specific networks might have **fairplay rules.**

The Things Network / 1

The Things Network / 2 / Manifesto

Everything that carries power will be connected to Internet eventually.

Controlling the network that makes this possible means controlling the world. We believe that this power should not be restricted to a few people, companies or nations. Instead this should be distributed over as many people as possible without the possibility to be taken away by anyone. We therefore founded "The Things Network".

The Things Network is an open source, free initiative with the following properties:

It connects sensors and actuators, called "Things", with transceivers called "Things Gateways" to servers called "Things Access".
The first connection is "Over The Air", the second is "Over The Net". The distributed implementation of these concepts is called "The Things Network".
Anyone shall be free to set up "Things" and connect to "Things Gateways" that may or may not be their own.
Anyone shall be free to set up "Things Gateways" and connect to "Things Access" that may or may not be their own. Their "Things Gateways" will give access to all "Things" in a net neutral manner, limited by the maximum available capacity alone.
Anyone shall be free to set up "Things Access" and allow anonymous connections from the Internet. Their "Things Access" will give access to all "Things Gateways" in a net neutral manner, limited by the maximum available capacity alone. Furthermore their "Things Access" will allow connection of other "Things Access" servers for the distribution of data.
The "Over The Air" and "Over The Net" networks shall be protocol agnostic, as long as these protocols are not proprietary, open source and free of rights.
Anyone who perpetrates a "Things Access" or a "Things Gateway" will do so free of charge for all connecting devices and servers.
Anyone making use of the network is allowed to do so for any reason or cause, possibly limited by local law, fully at own risk and realizing that services are provided "as is" and may be terminated for any reason at any moment. The use may be open for anybody, limited to customers, commercial, not-for-profit, or in any other fashion. "The Things Network" providers will not pose restrictions upon its users.

We invite you to sign this Manifesto, and uphold its principles to the best of your abilities.

Source, Details:

https://github.com/TheThingsNetwork/Manifest

The Things Network

THE THINGS NETWORK

Anyone shall be free to set up "Things" and connect to "Things Gateways" that may or may not be their own.

Anyone shall be free to set up "Things Gateways" and connect to "Things Access" that may or may not be their own. Their "Things Gateways" will give [free] access to all "Things" in a net neutral manner, limited by the maximum available capacity alone.

The Things Network / 3 / Essentials

- Open source - The Things Stack
- Free ... to set up and run their own, in particular:

  Anyone who perpetrates a "Things Access" or a "Things Gateway" will do so **free of charge for all connecting devices and servers** and **without traffic prioritization other than governed by capacity**

  (-> network neutrality)

Source, Details:

https://github.com/TheThingsNetwork/Manifest

The Things Network / 3a / Essentials

- Community project started in Netherlands, 2015
- Commercial side: The Things Industries
- Open source

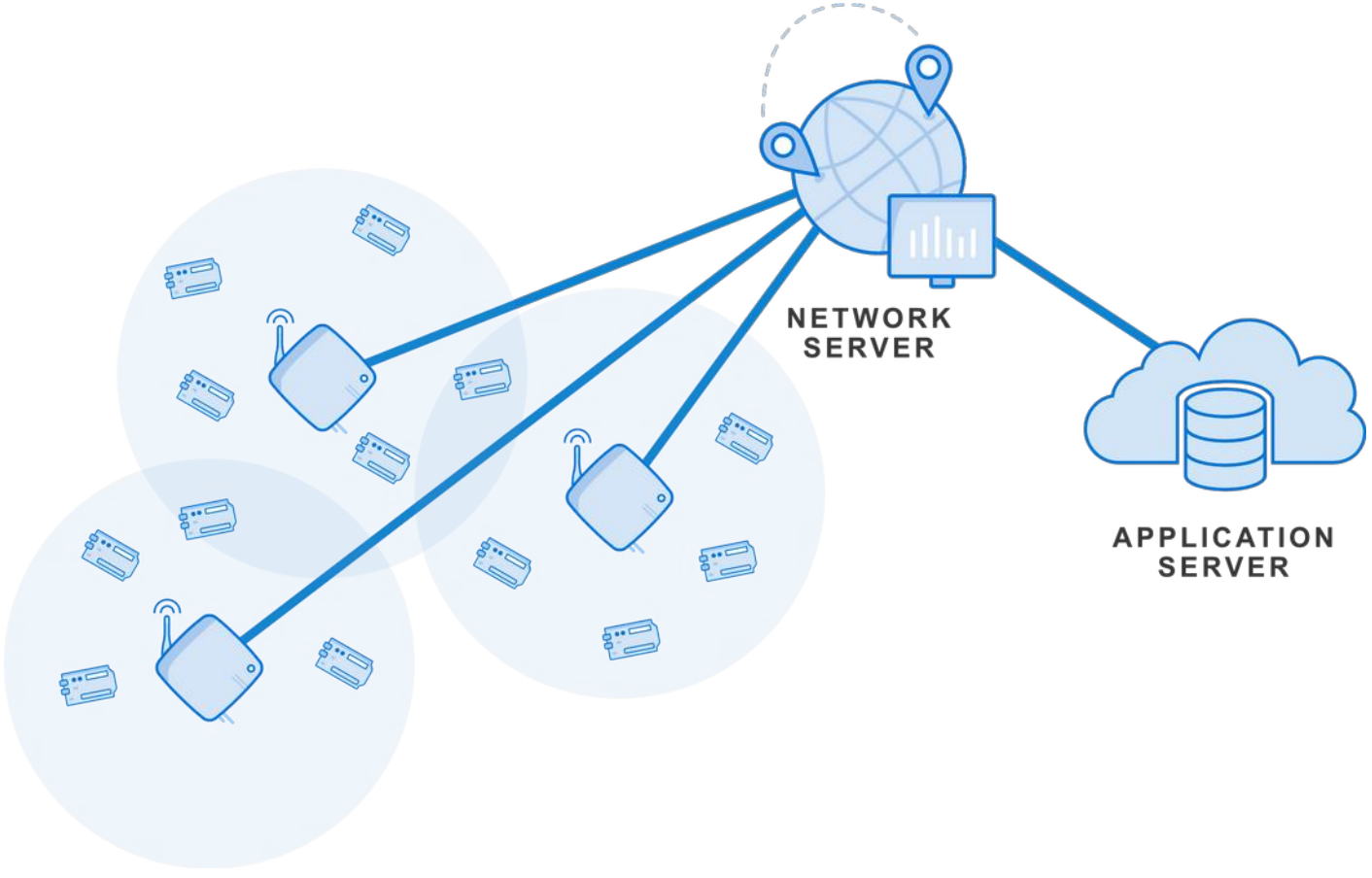
TheThingsNetwork/lorawan-stack is licensed under the **Apache License 2.0**

- *This to some degree explains our current interest in TTN, in an educational context*
- **Great Learning resource: https://www.thethingsnetwork.org/docs/**

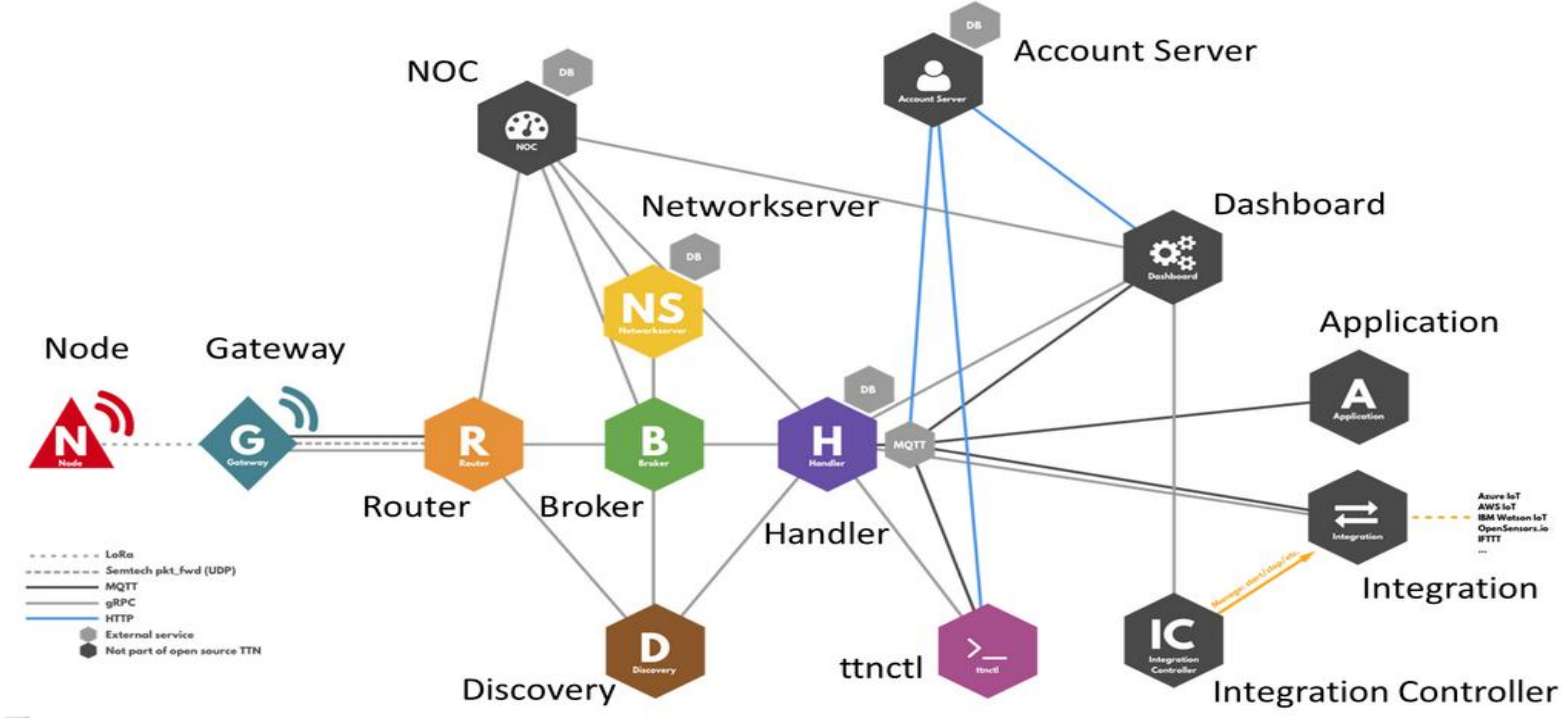
The Things Network / 3b / Context

- The Things Network is both a community movement and platform (with a commercial stakeholder (The Things Industries) as driver – *compare to related models in FLOSS Free and Open Software area – e.g. Ubuntu/Canonical*)
- and provider of a LoRaWAN Software Stack – of which there are many others, e.g.
  - free ones like Chirpstack,
  - commercial ones like LORIOT, Thingpark/Actility, ...

The Things Network / 4 / Architecture



The Things Network / 5 / Architecture



The Things Network / 6 / Security

= LoRaWan defined

NwkSKey, AppSKey and AppKey

Challenge of key provision:

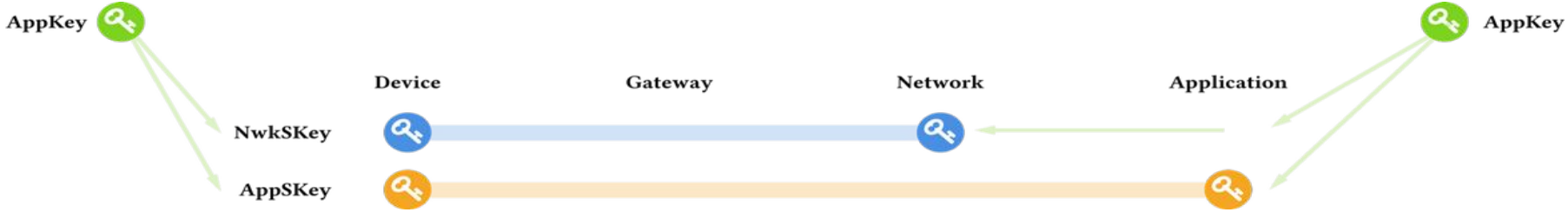
how to get a key to a customer and into a deployment?

LoRaWan / Security / keys

Security measures:
three distinct 128-bit AES keys:
The **application key AppKey** is only known by the device and by the application. When a device joins the network (this is called a join or activation), an application session key **AppSKey** and a network session key **NwkSKey** are generated. The NwkSKey is shared with the network, while the AppSKey is kept private.

Source, Details:

https://www.lora-alliance.org/What-Is-LoRa/Technology



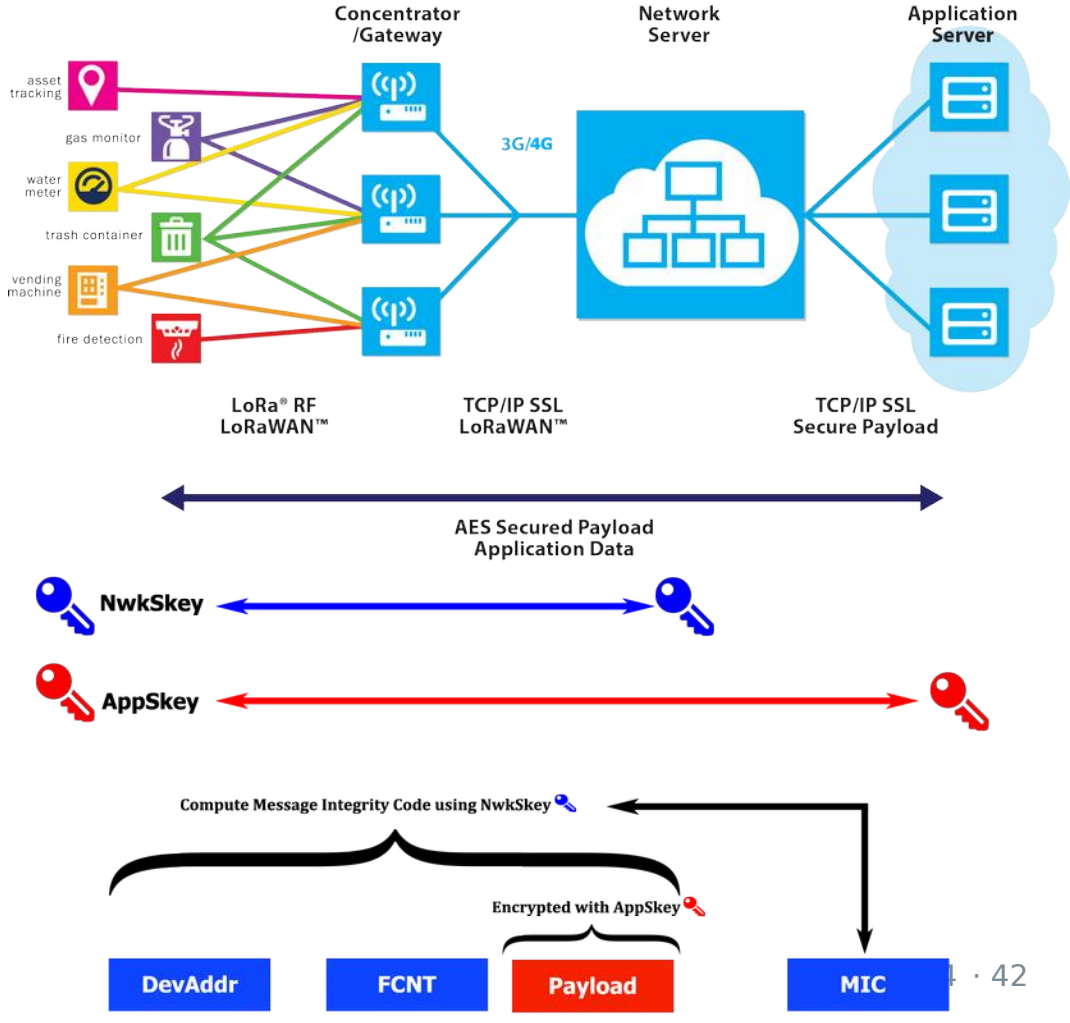
The Things Network / Security, cntd

LoRaWAN 1.0 specifies a number of security keys: `NwkSKey`, `AppSKey` and `AppKey`. All keys have a length of 128 bits.

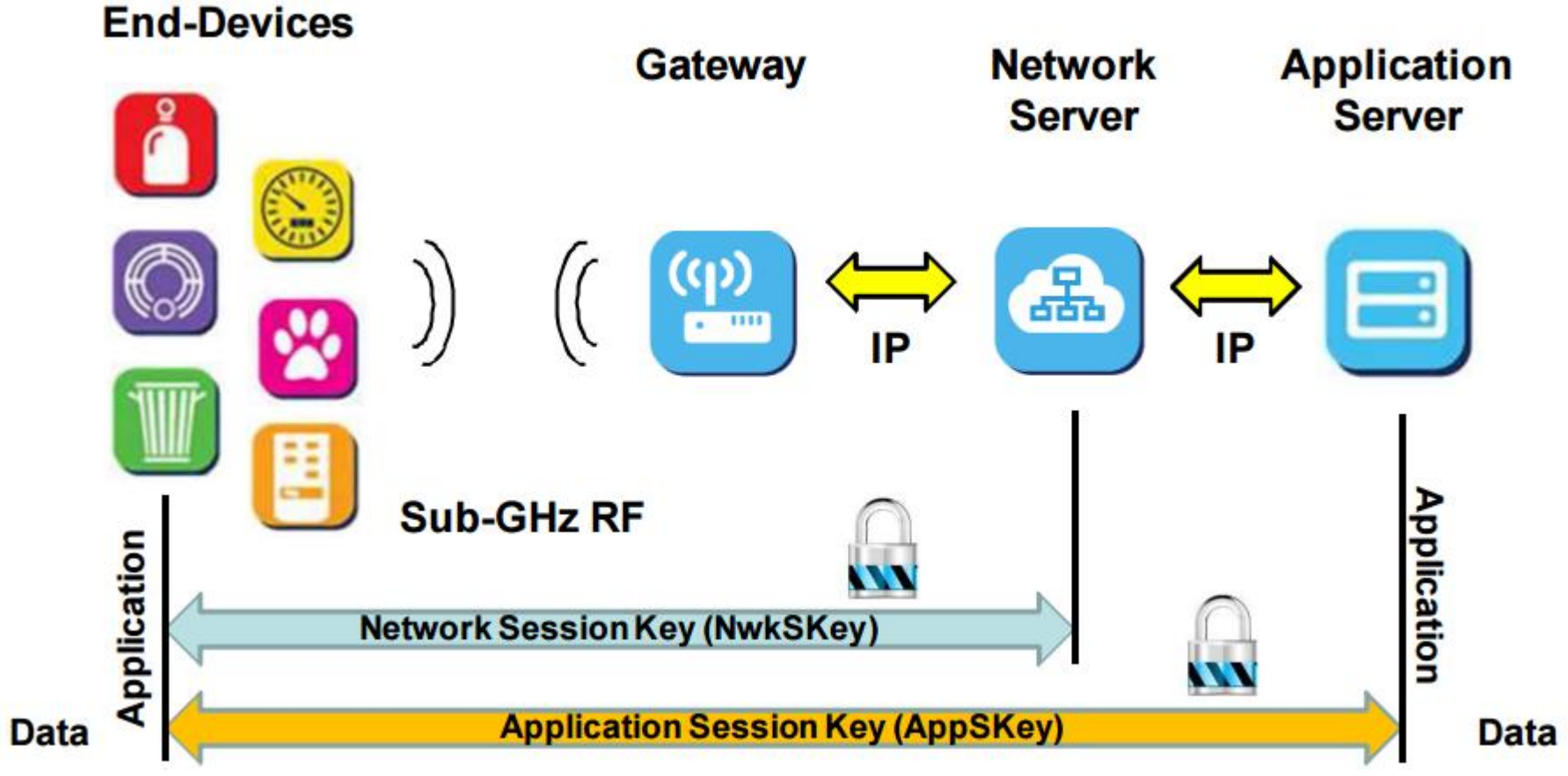
The **Network Session Key** (`NwkSKey`) is used for interaction between the Node and the Network Server. This key is used to check the validity of messages (MIC check). In the backend of The Things Network this validation is also used to map a non-unique device address (`DevAddr`) to a unique `DevEUI` and `AppEUI`.

The **Application Session Key** (`AppSKey`) is used for encryption and decryption of the payload. The payload is fully encrypted between the Node and the Handler/Application Server component of The Things Network (which you will be able to run on your own server). This means that nobody except you is able to read the contents of messages you send or receive.

The Things Network / Security, cntd



The Things Network / Security, cntd



The Things Network / Security / Activation

Two ways of activating a device:

OTAA Over the Air Activation

Interactive, Join request and answer

ABP Activation by Personalization

Hard coded credentials for session

OTAA recommended for sceurity reasons, ABP often used for ad-hoc experiments and reduction of power consumption

The Things Network / Security / OTAA

Dynamically activated devices (**OTAA**) use the application key (AppKey) to derive the two session keys during the activation procedure. In The Things Network you can have a default AppKey which will be used to activate all devices, or customize the AppKey per device.

What you will use, in your code:

DevEUI, AppEUI, AppKey

Keys will be generated on TTN server, on registration (but can be changed manually)

Source, Details: https://www.thethingsnetwork.org/wiki/LoRaWAN/Security

The Things Network / Security / ABP

ABP Activation by Personalization

What you will use, in your code:

NwkSKey, AppSKey, DevAddr

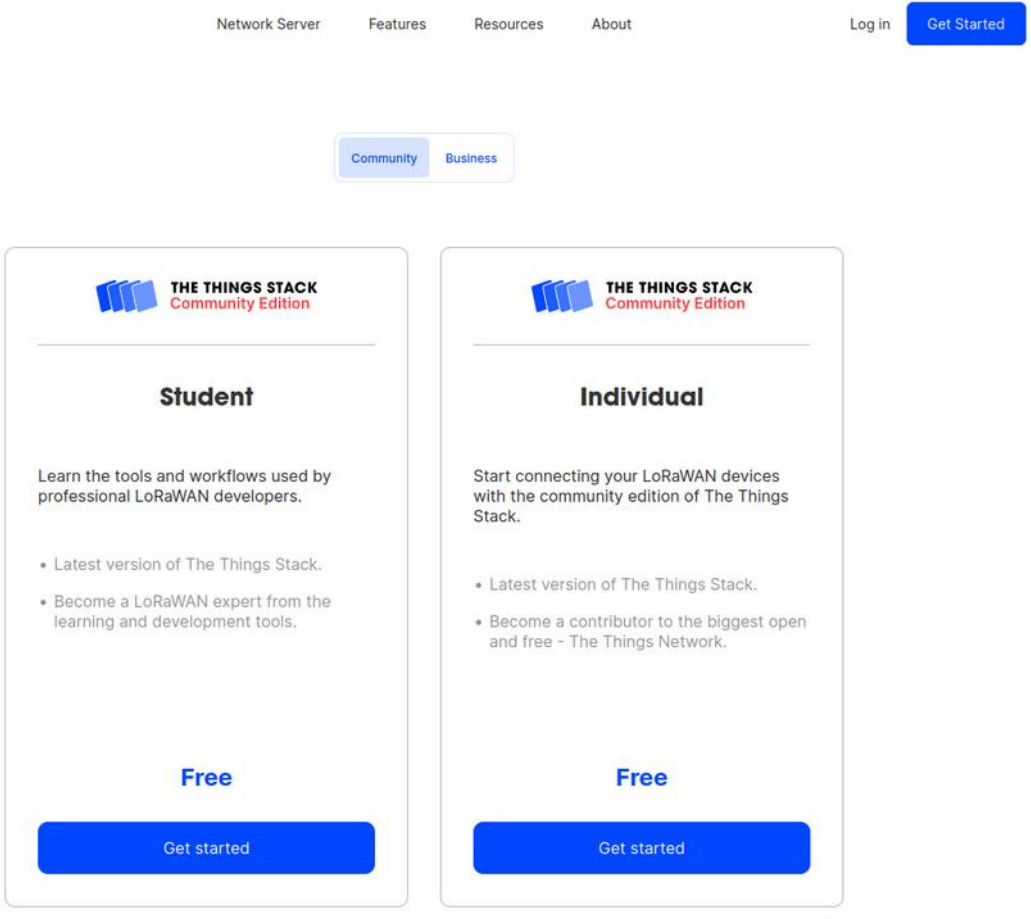
(Note the "S" here – you simply have session credentials)

Source, Details:

https://www.thethingsnetwork.org/wiki/LoRaWAN/Security

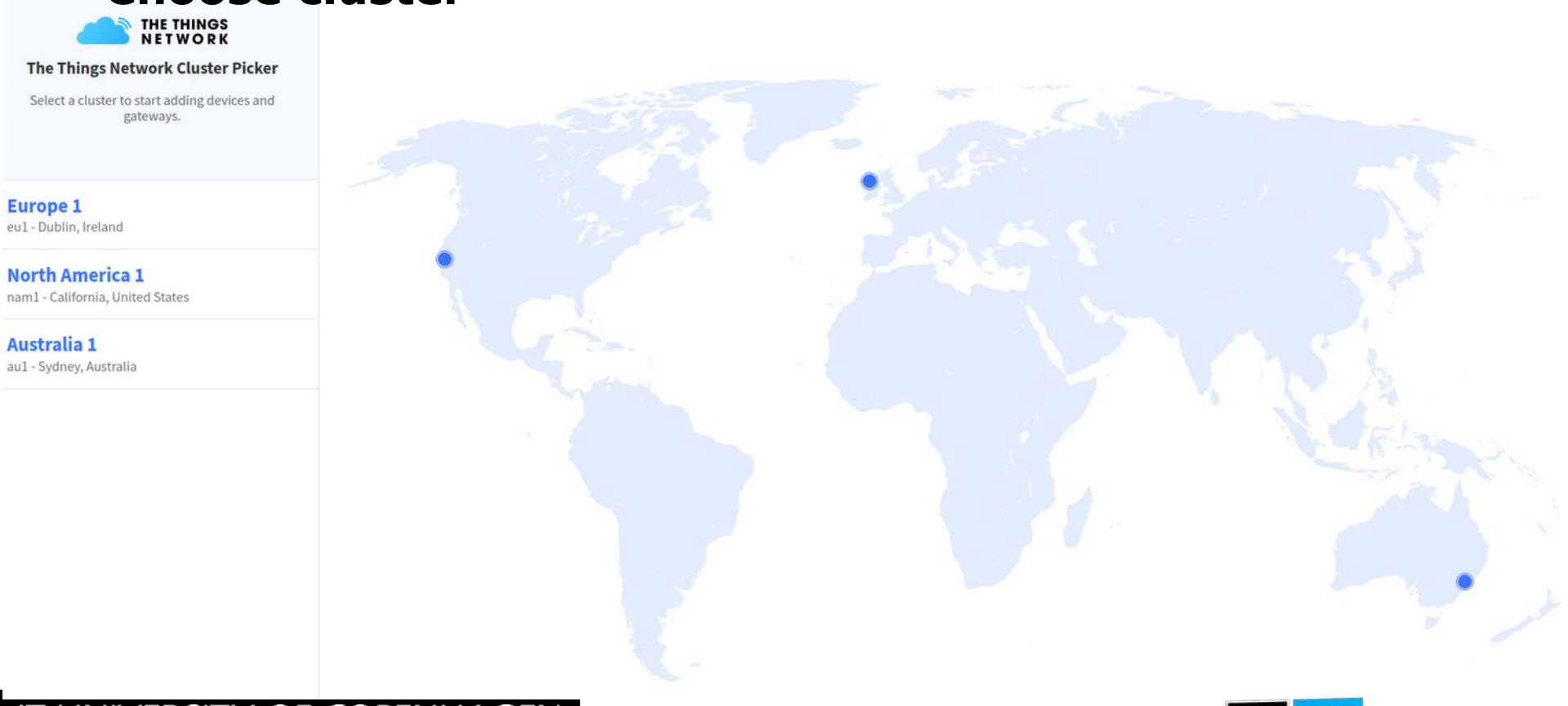
Working with The Things Network Console

Sign up!



Working with The Things Network Console

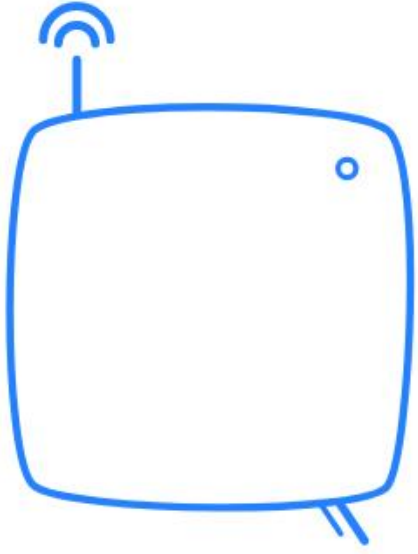
Choose cluster



Working with The Things Network Console

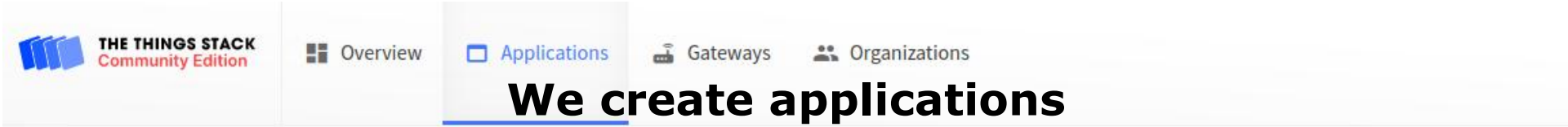
We have applications (and devices) and gateways

Go to applications



Go to gateways

Working with The Things Network Console



We create applications

Add application

Application ID *

my-new-application

Application name

My new application

Description

Description for my new application

Optional application description; can also be used to save notes about the application

Create application

Working with The Things Network Console

Applications > co2-001 > End devices > Register from The LoRaWAN Device Repository

Register end device

From The LoRaWAN Device Repository | Manually

1. Select the end device

Brand *

Type to search...

Cannot find your exact end device? Get help here and try manual device registration.

In our applications, we create devices

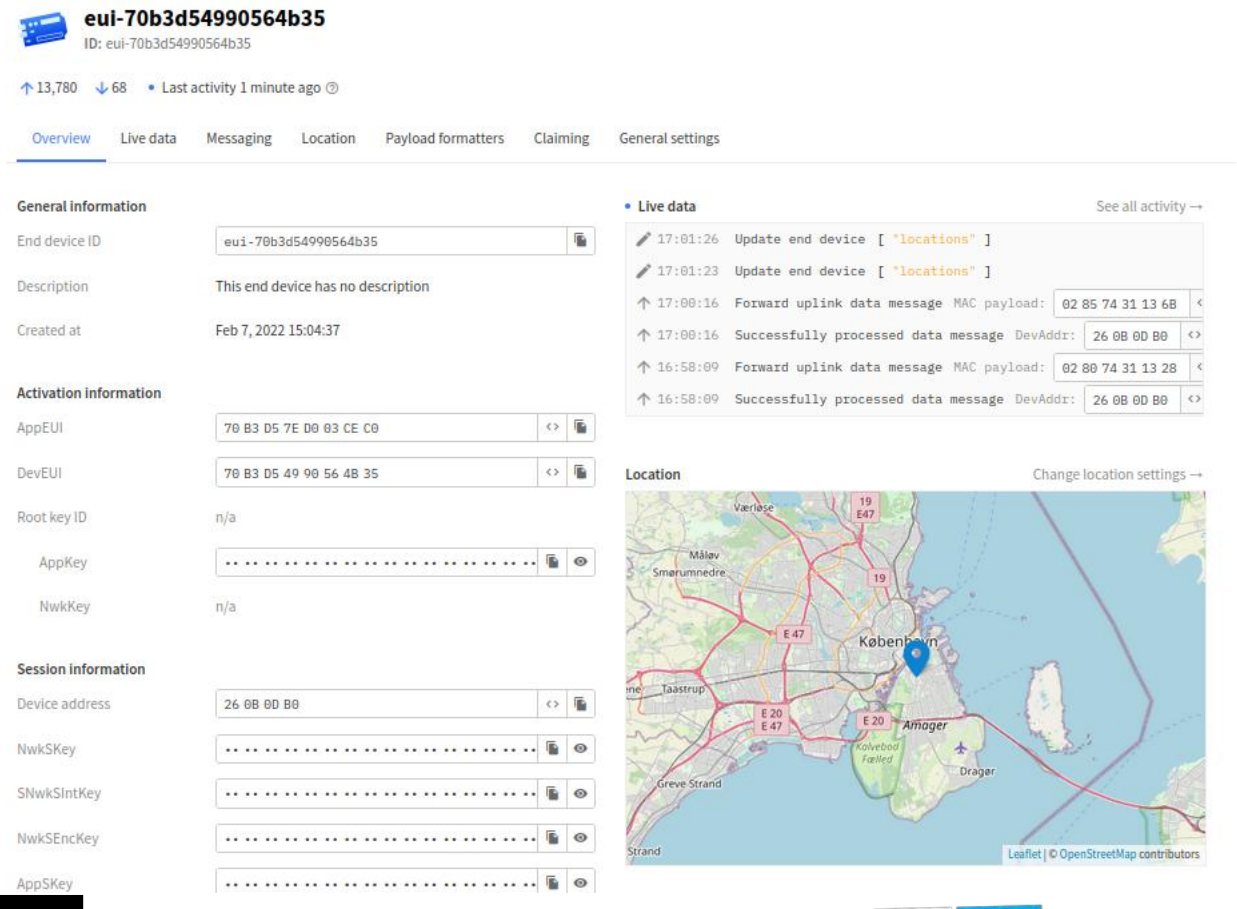
2. Enter registration data

Please choose an end device first to proceed with entering registration data

Register end device

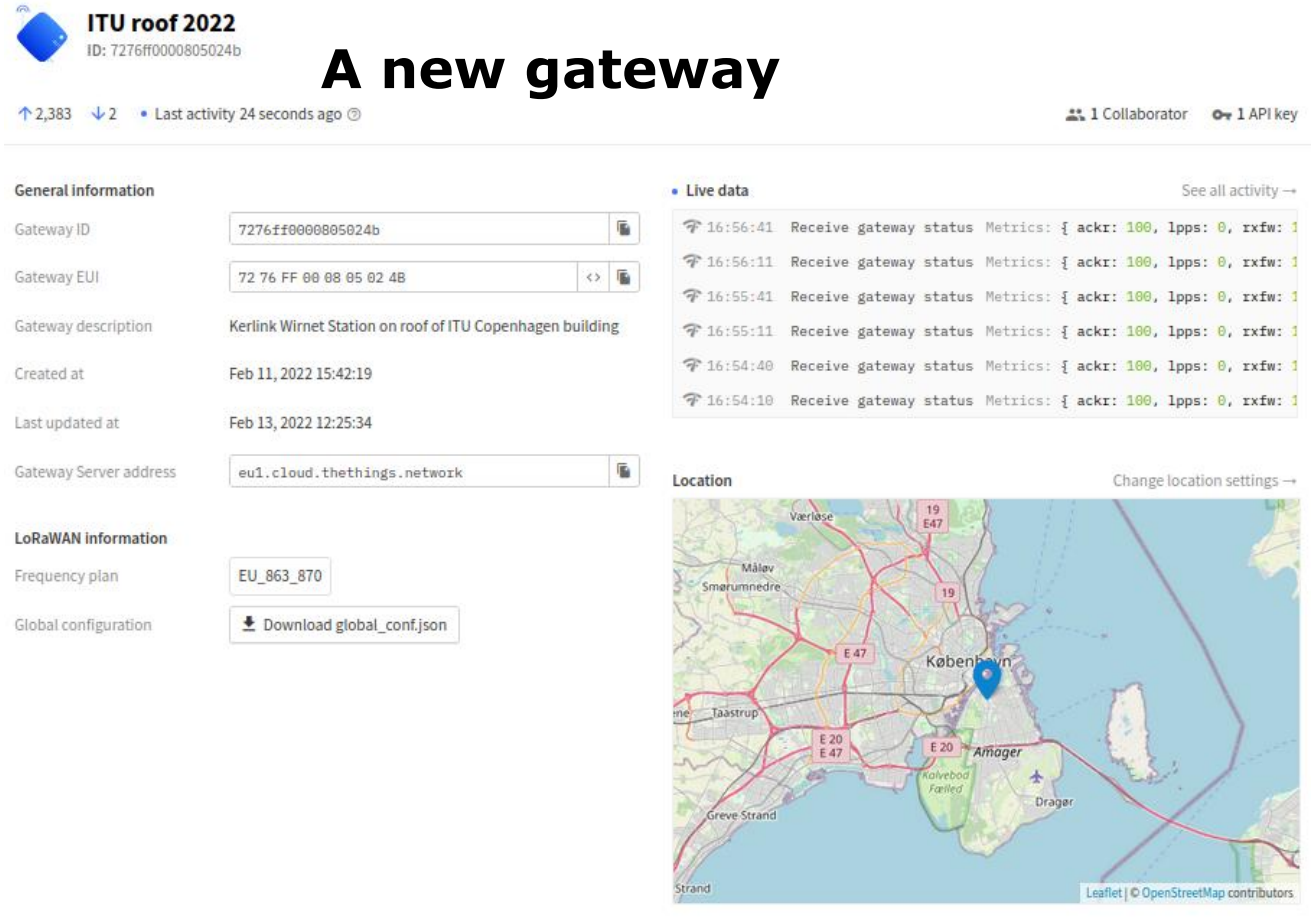
Working with The Things Network Console

A new device



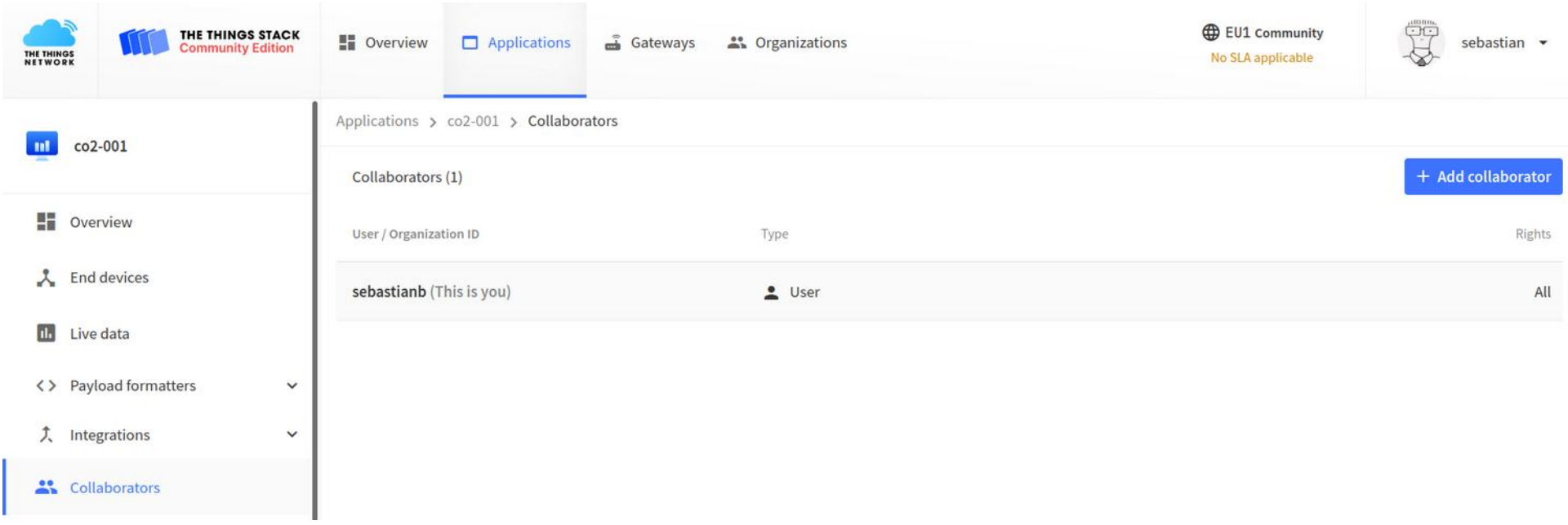
Working with The Things Network Console

A new gateway

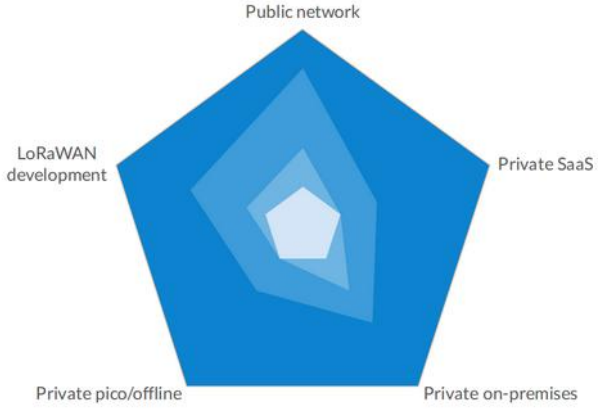


Working with The Things Network Console

Share, collaborate



V3 stack



Source, Johan Stokking, https://www.thethingsnetwork.org

V3 stack

DEPLOYMENT SCENARIOS

Public networks

Public community network and operated public networks

Private networks

Software-as-a-service, on-premises, pico and offline networks

LoRaWAN development

For device makers, application developers and prototype development

THE THINGS NETWORK

Source, Johan Stokking, https://www.thethingsnetwork.org

Recent Developments (update 2022/23)

- **Interoperation/Integration between LoRaWAN stacks and providers:**

  LoRaWAN® Roaming
  Things Network Packetbroker
  Actility ThingPark Exchange
  AWS IoT Core

- **TOF (Time of Flight) based location services based on LoRaWAN signals**

- **LoRa 2.4 Ghz – global harmonization a big advantage**

- **Additional Standard: LR-FHSS Long Range Frequency Hopping**

- **Satellite LoRa**

Take-Aways, Networking 2

- Be able to name protocols and standards on

  PHY, MAC and higher layers -
  Know which protocol belongs where

- Be able to describe the architecture
  and main features of

  LoRa
  LoRaWan

- Be able to explain security measures for these