SORBONNE UNIVERSITÉ

CRÉATEURS DE FUTURS
DEPUIS 1257

Yann DOUZE
Twitter : @yann_douze
Linkedin :
https://www.linkedin.com/in/yanndouze/

The Internet Of Things
C8 : LoRaWAN Protocol

Introduction to what is the Internet of Things, why does it change the world where we live, what are the technologies behind the scene ?
How des it apply to your domain ?

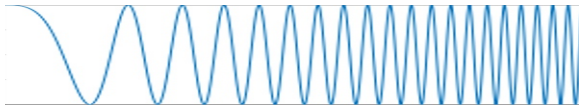
The LoRaWAN protocol

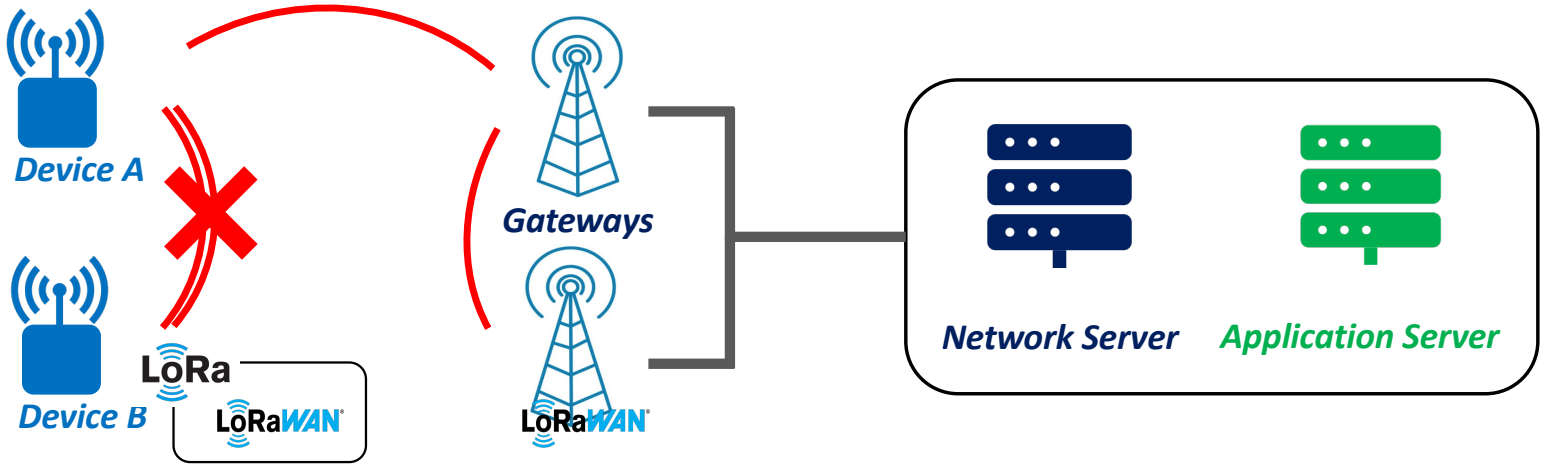
- ✓ LoRaWAN ecosystem
  - Specification
  - LoRa vs LoRaWAN
- ✓ LoRaWAN infrastructure
  - Device
  - Gateway
  - LoRaWAN Server
- ✓ LoRaWAN Security
- ✓ Device classes
- ✓ Activation methods: ABP or OTAA
- ✓ How to …
  - … prevent replay attack?
  - … change the communication parameters?
  - … change Network operator?
- ✓ Optimization of the communication: ADR

LoRa vs LoRaWAN

LoRa vs LoRaWAN

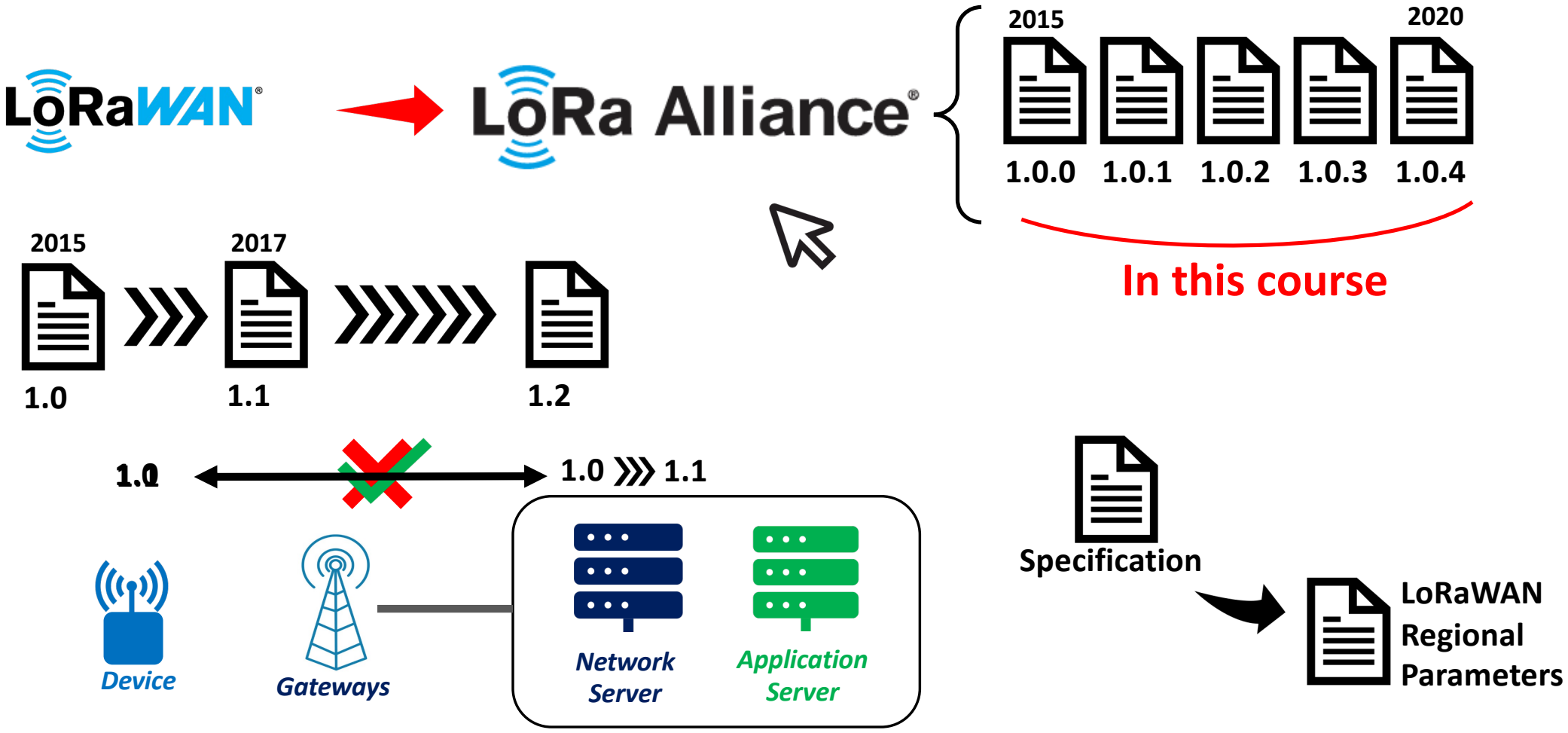
LoRa → **Type of modulation** (Chirp)





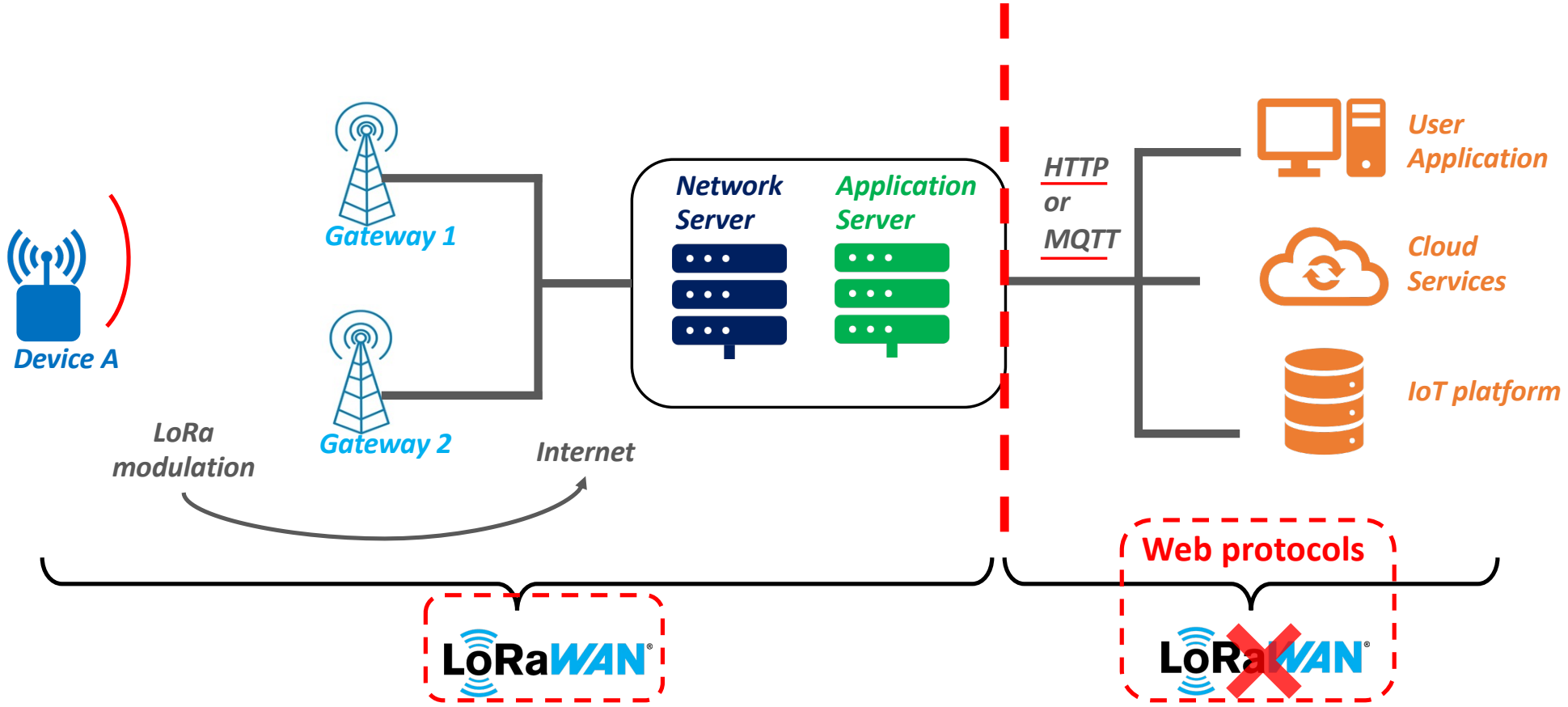
LoRaWAN → **Secured and standardized protocol**

LoRaWAN protocol versions

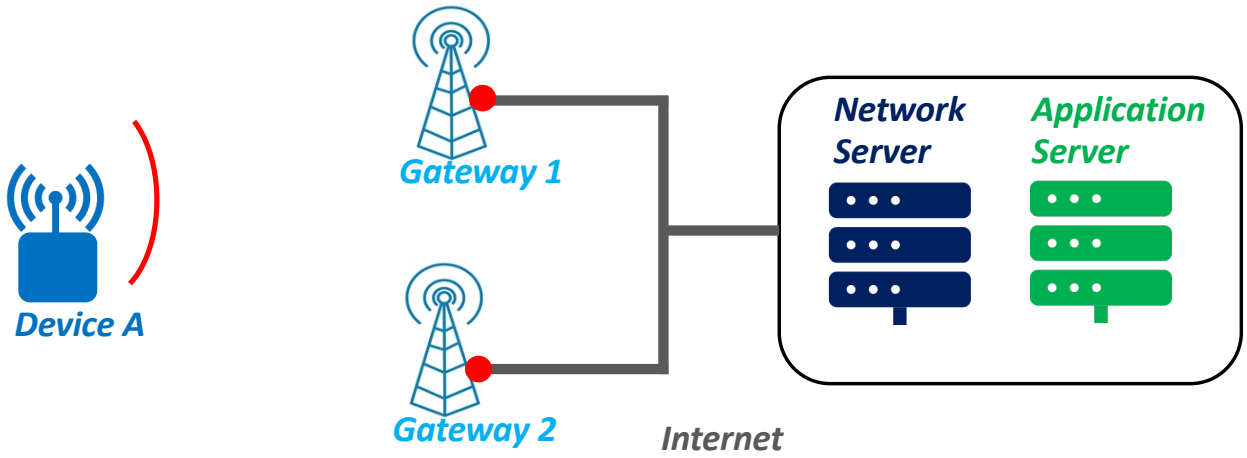


LoRaWAN network infrastructure

LoRaWAN frame = User Payload + Security information



LoRaWAN network infrastructure



LoRaWAN Network Server and Application Server

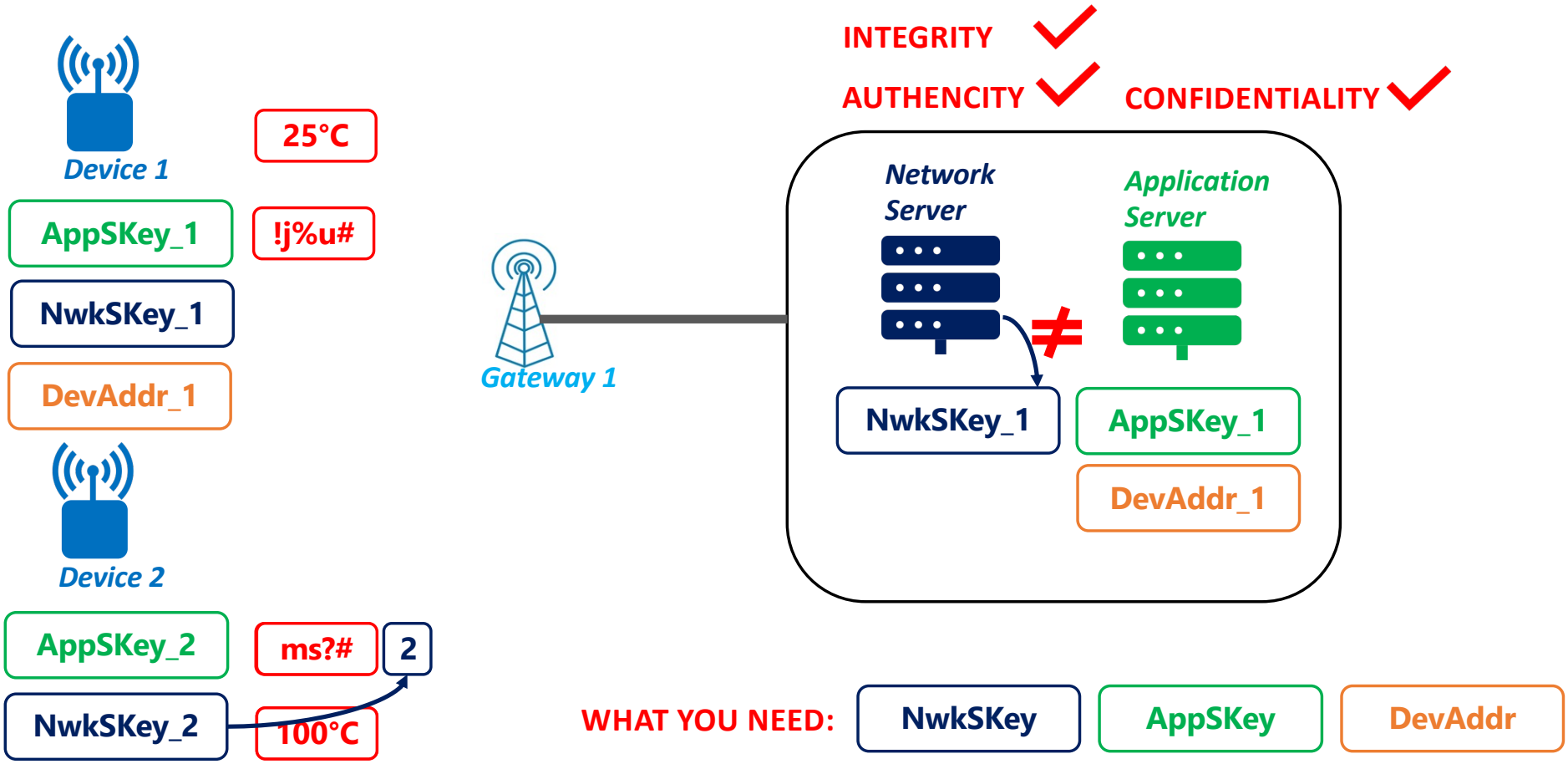
SECURITY

→ **CONFIDENTIALITY**
Nobody can understand what the end-device says

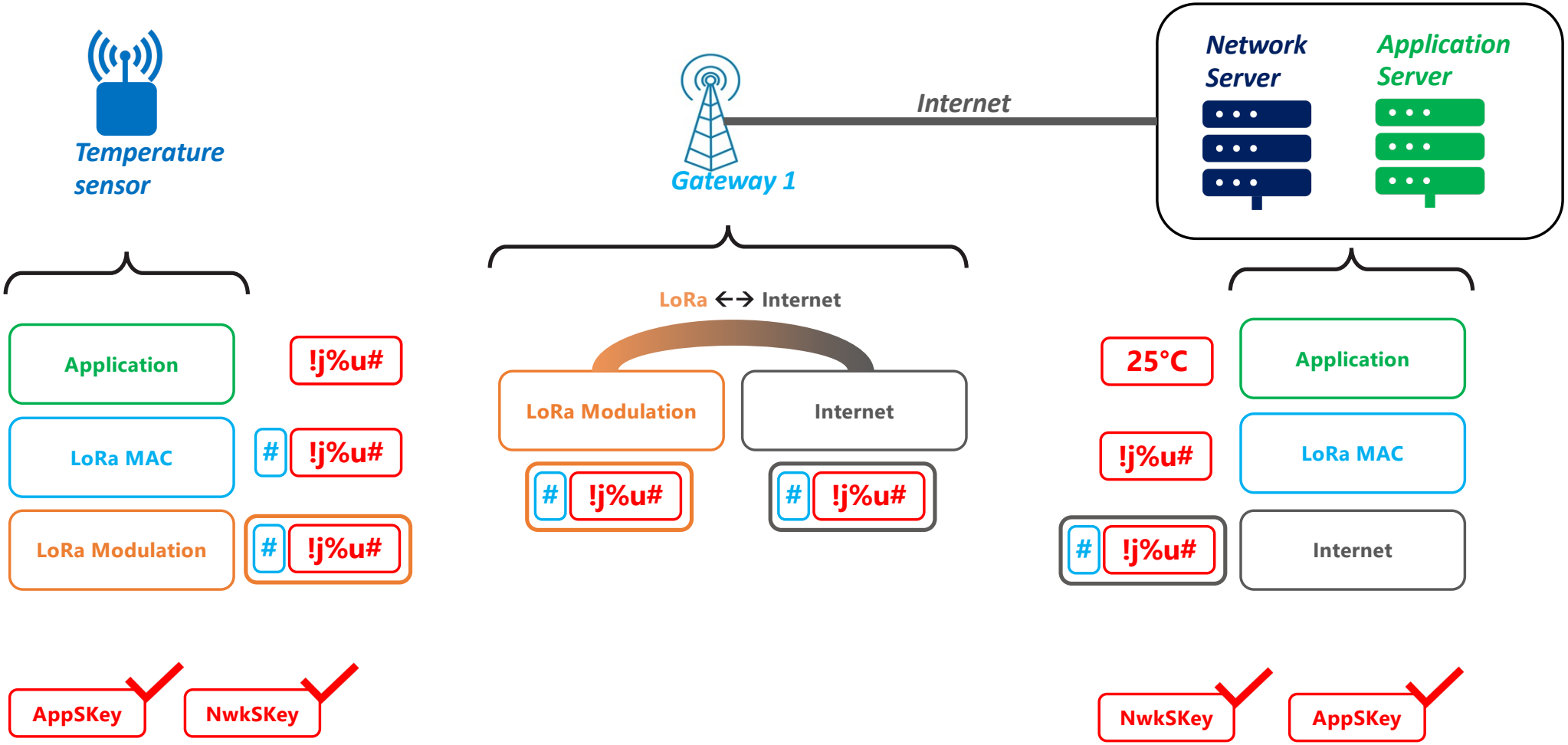
→ **INTEGRITY**
Nobody can change the transmitted frame

→ **AUTHENCITY**
Only allowed end-device can send on the Network Server

LoRaWAN Network Server and Application Server



The LoRaWAN Gateways



LoRa end-device Classes

Packet transmission time

= TIME ON AIR

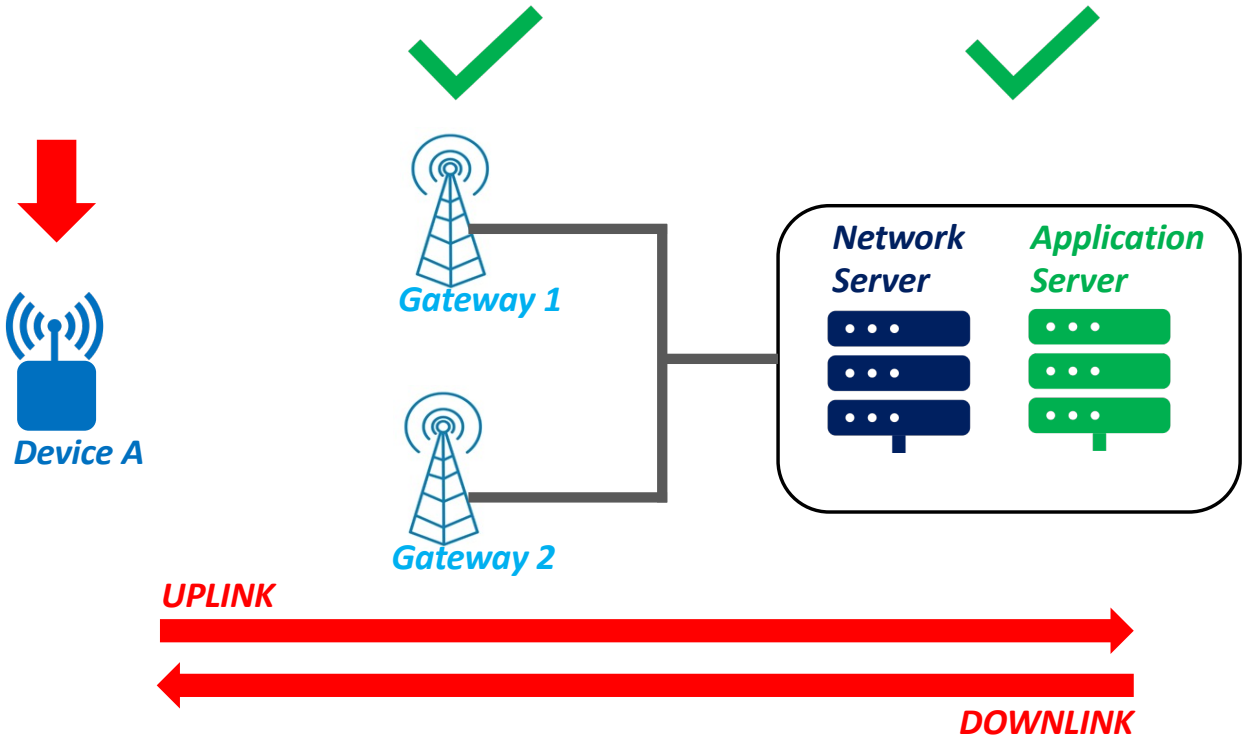
1% Time duration

= DUTY CYCLE

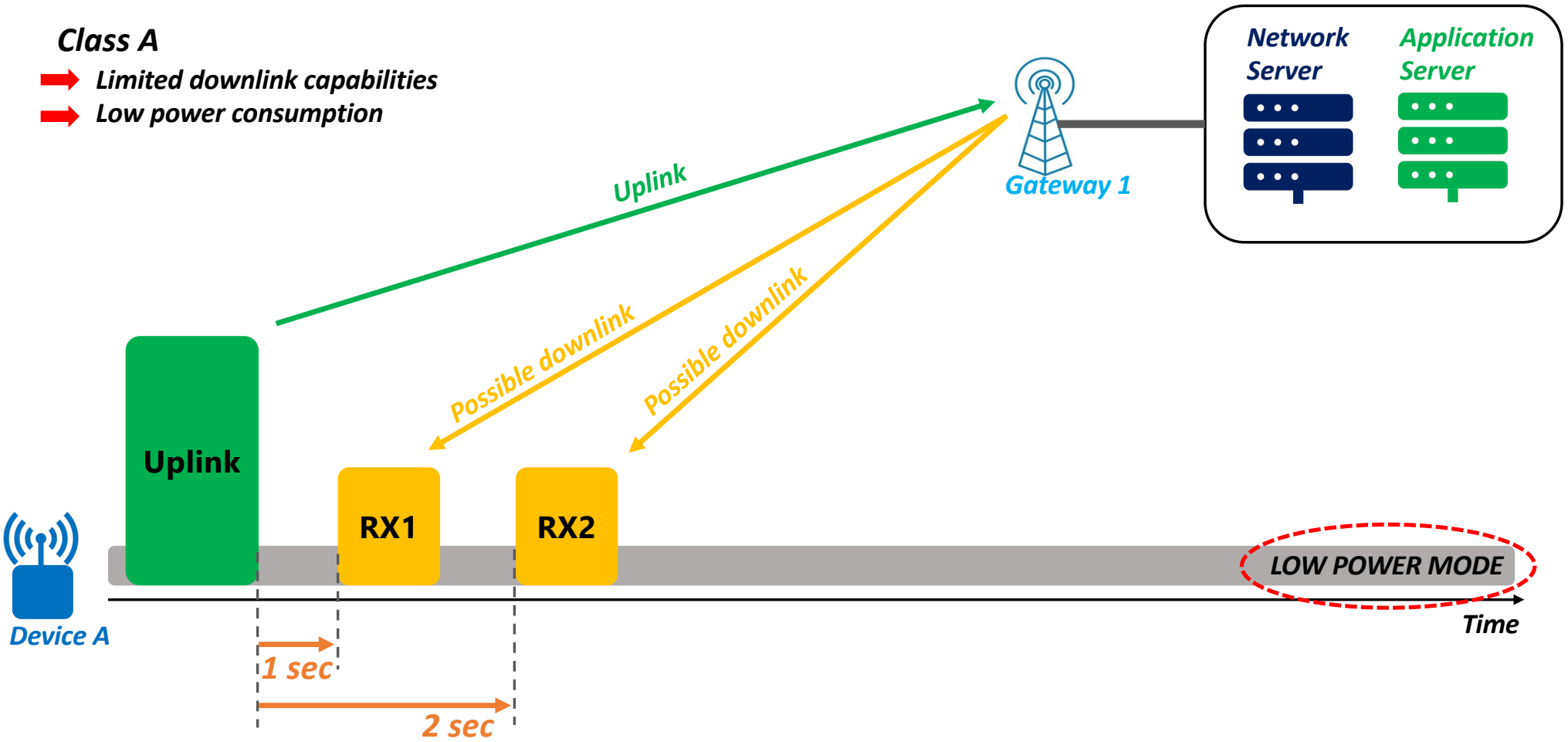
Downlink ?

End-device classes

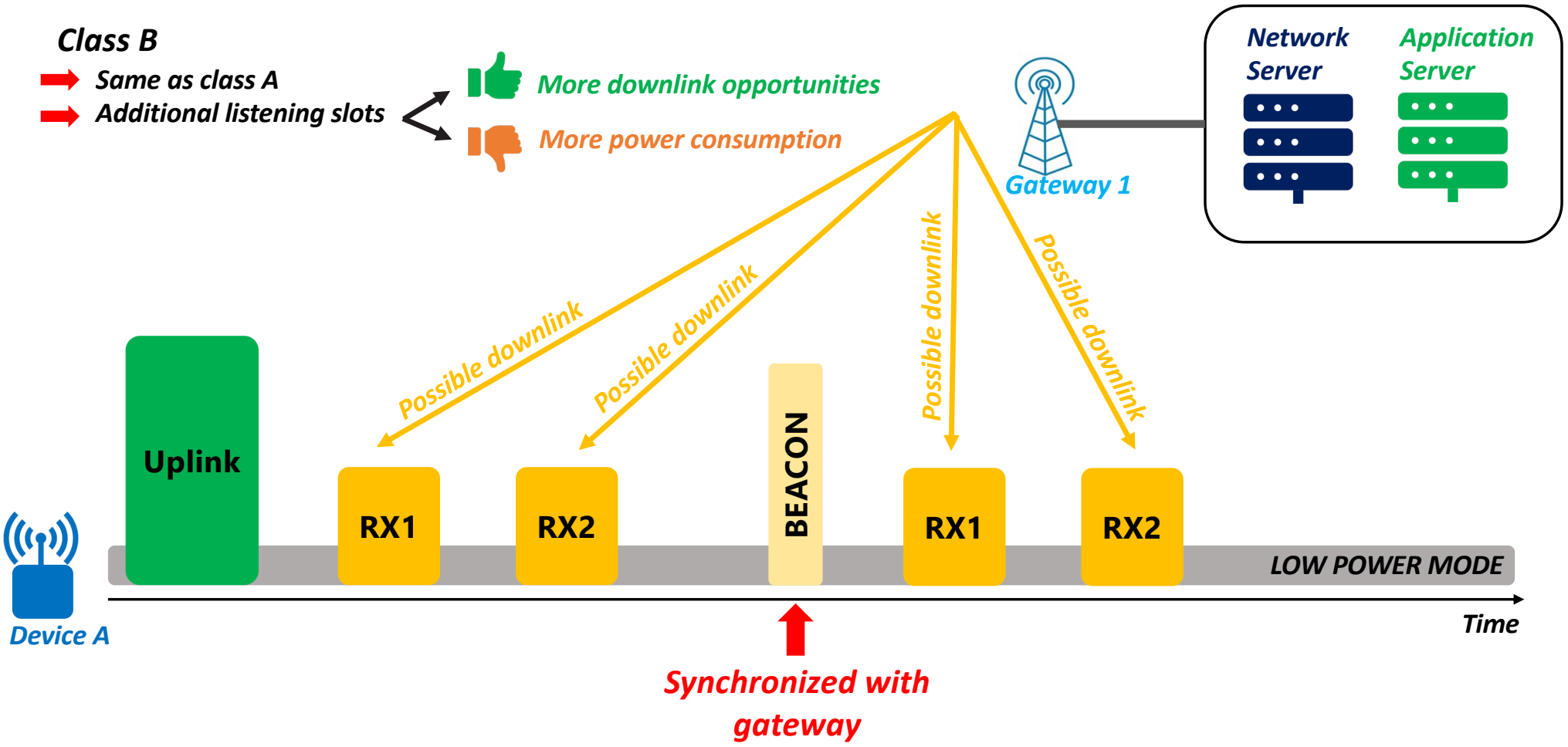
A or B or C



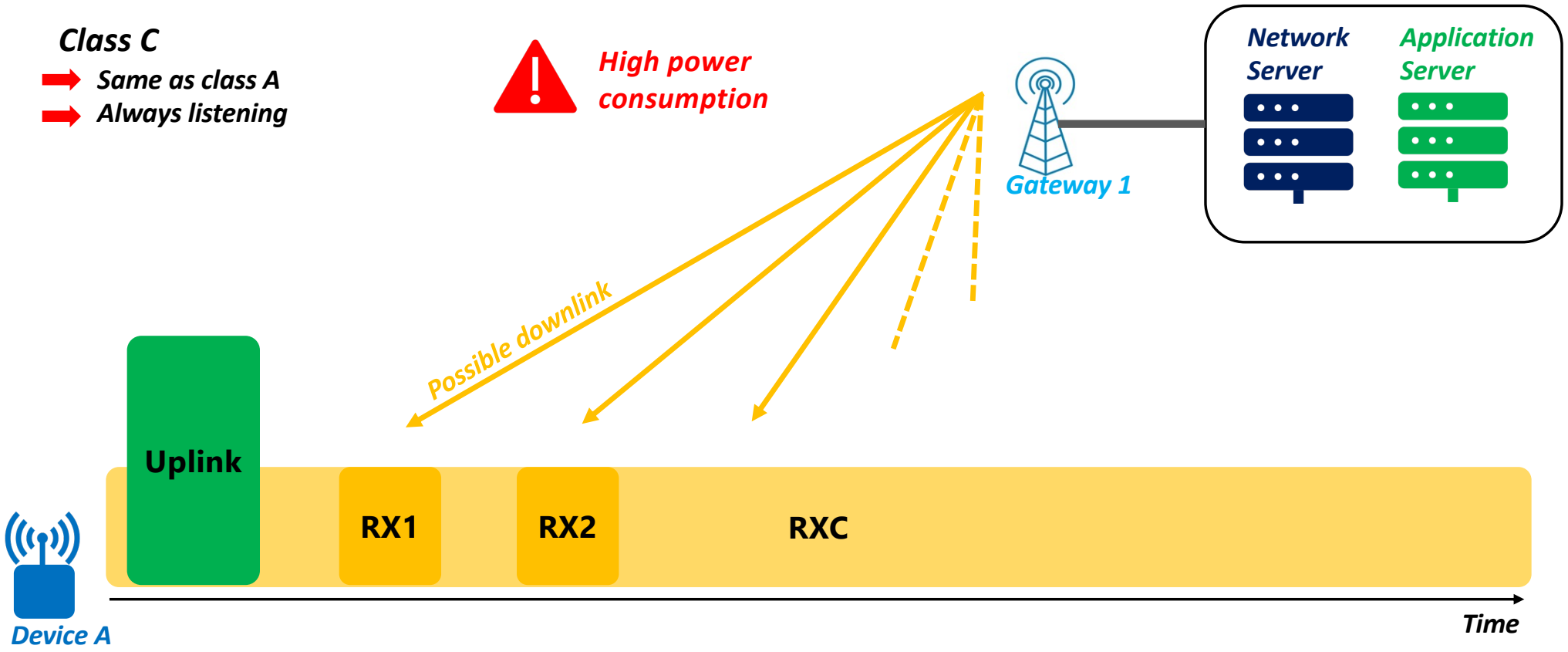
Class A end-devices



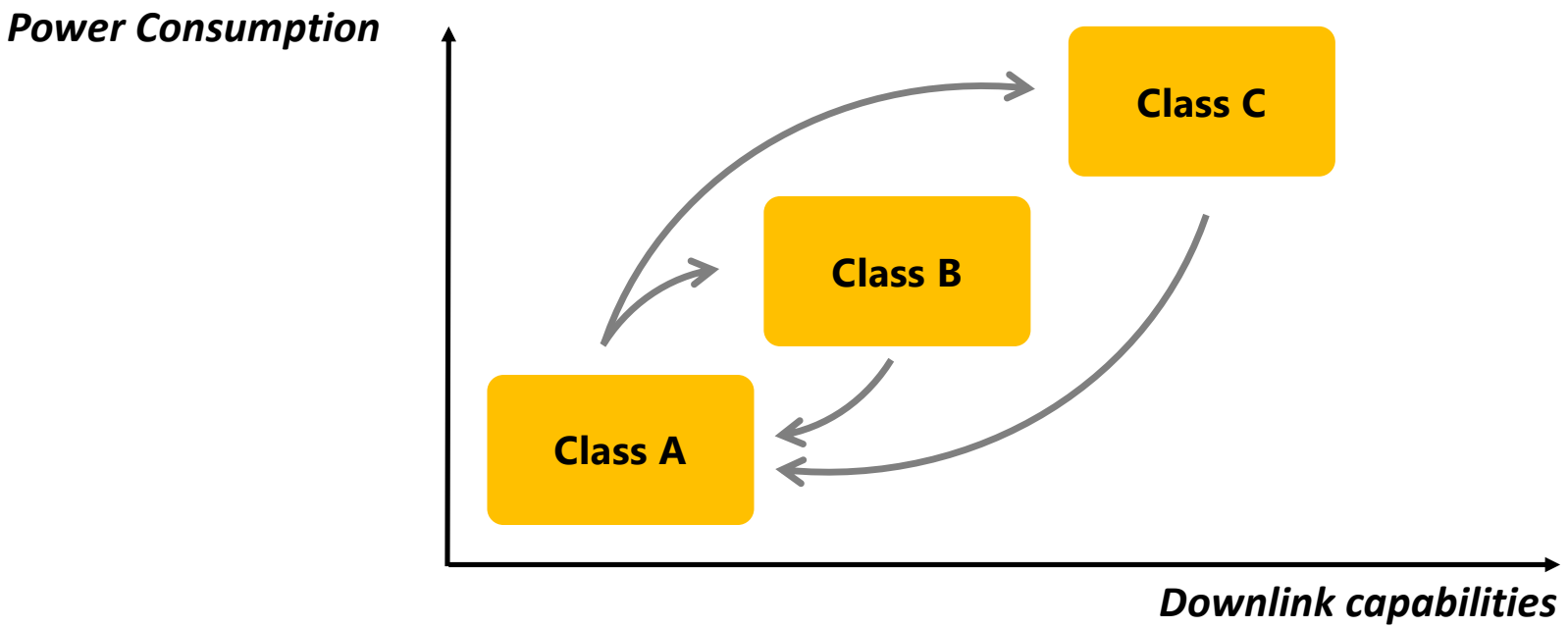
Class B end-devices



Class C end-devices



LoRa end-device Classes



LoRa end-device Classes

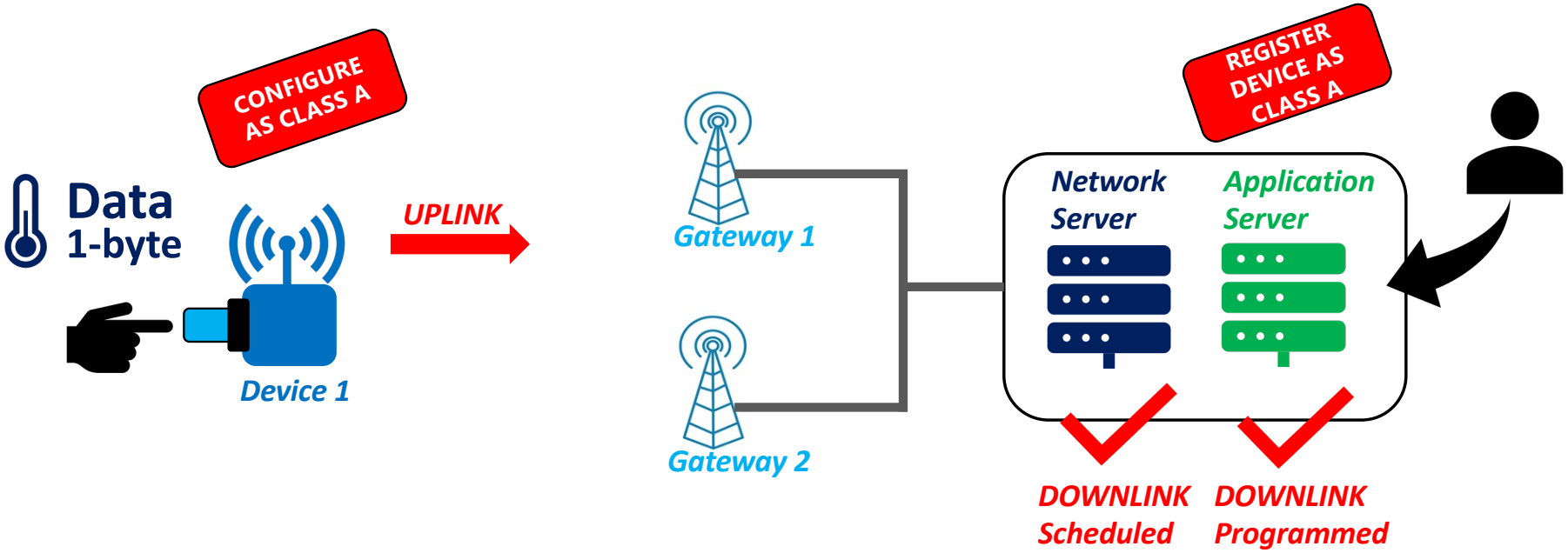
Class A → **All devices, Gateways and Network Server support class A**

Class B → **Device, Gateway, and Network Server must support class B**

⚠ **Specific gateway with absolute timestamp**

Class C → **Device, Gateway, and Network Server must support class C**

LoRa classes – Demonstration



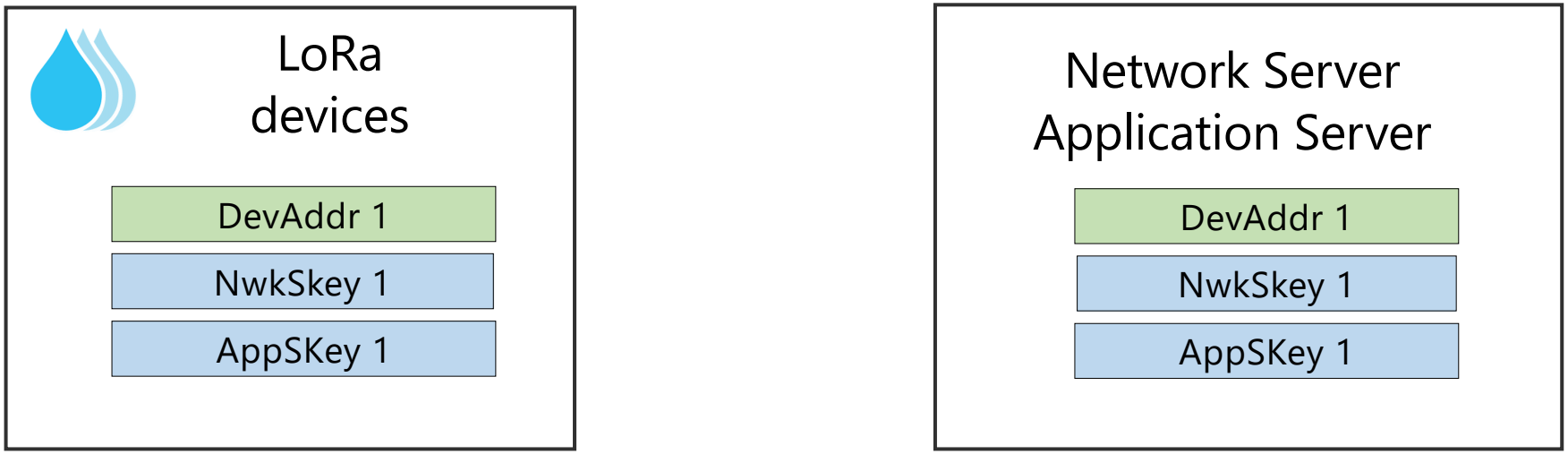
WHEN WILL THE DONWLINK FRAME BE SENT ?

CLASS A
RX1 or RX2

or

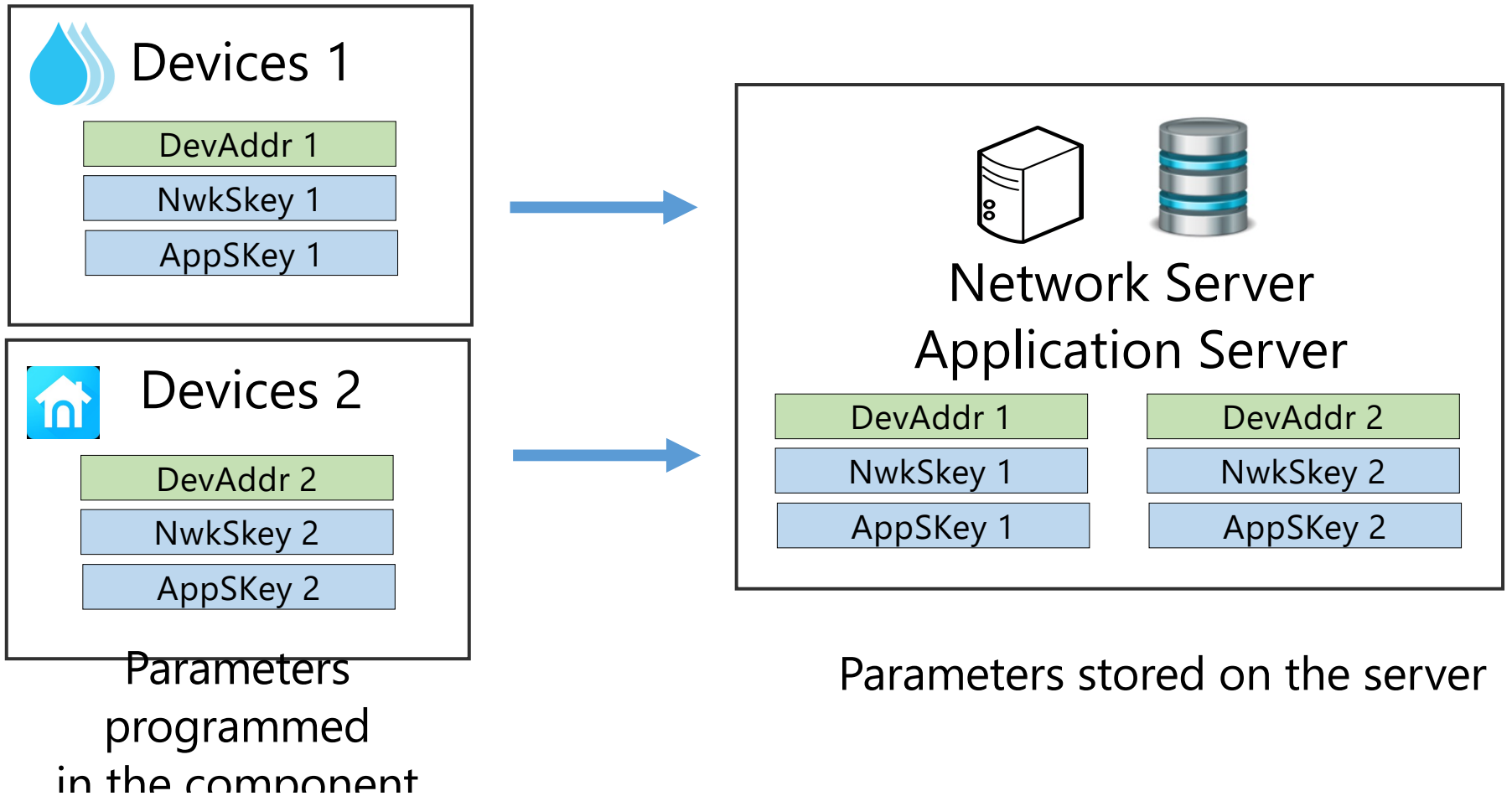
CLASS C
Whenever

Activation of LoRa Devices



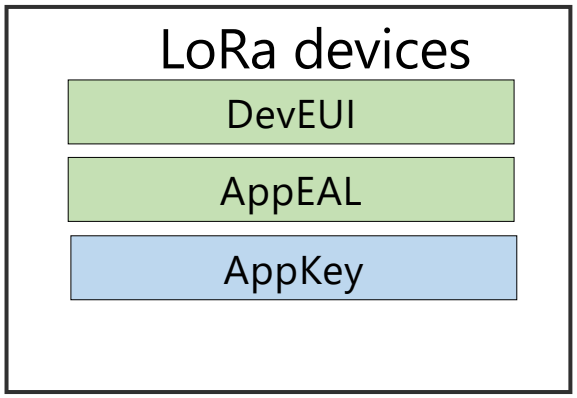
- ❑ Activation By Personalization (ABP)
- ❑ Over The Air Activation (OTAA)

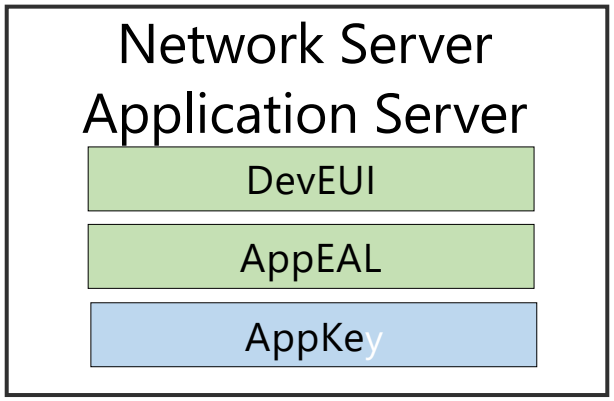
Activation By Personalization (ABP)



Over The Air Activation (OTAA) - 1

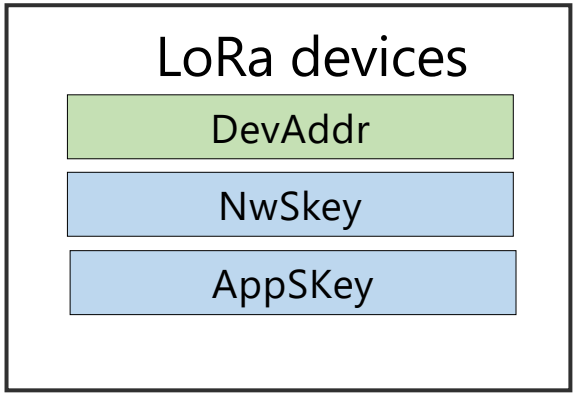
Programmed parameters **before** the "Join Request", in the component

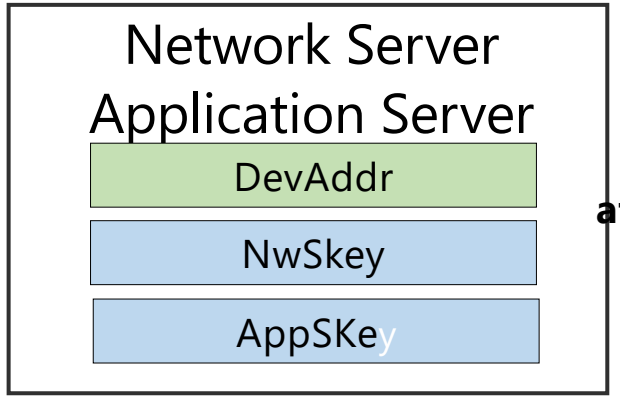




Stored parameters **before** the "Join Request in the server

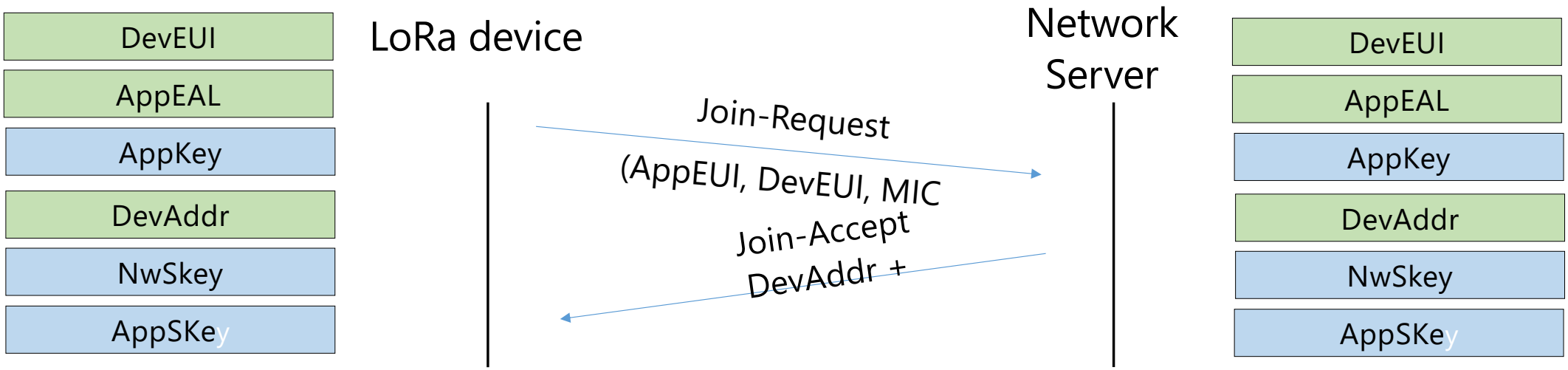
Parameters generated **after** the "Join Request", in the





Parameters generated **after** the "Join Request", in the server

Over The Air Activation (OTAA) - 2



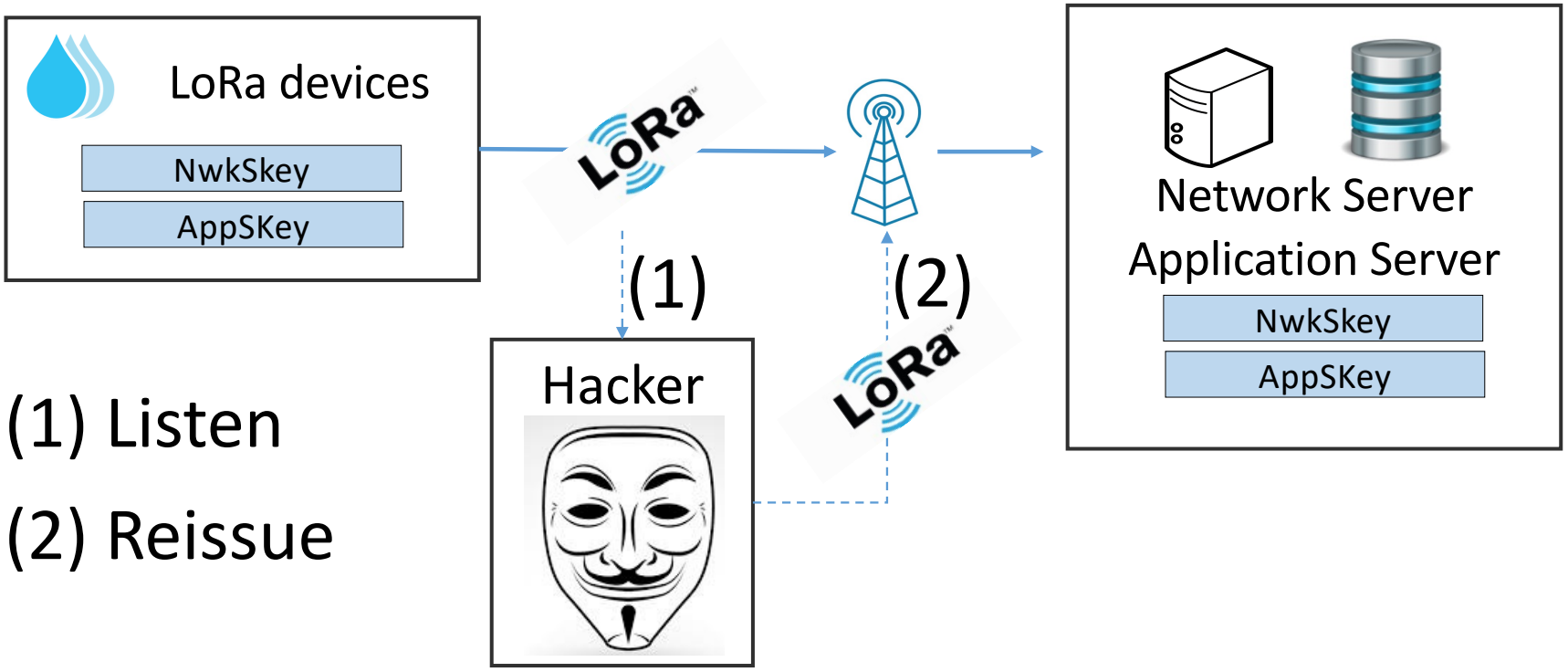
1. The LoRa Device issues a Join-Request using the **DevEUI**, **AppEUI**, and **AppKey** information it has.
2. The Network Server authenticates the Join Request and validates it. It then generates a **NwkSKey,** an **AppSKey**, and a **DevAddr**.
3. The Network Server returns the **DevAddr**, along with a series of **parameters**.
4. The **parameters** provided during the Join-Accept, associated with **the AppKey**, allow the LoRa Device to generate the same **NwkSKey** and **AppSKey** that were initially generated on the Network Server.

Choice between ABP or OTAA?

- Global security

- Frame Counter Management: Protection against replay attacks
- Change of network and server
- Modification of LoRa device parameters

The REPLAY attack



(1) Listen

(2) Reissue

The Frame Counter

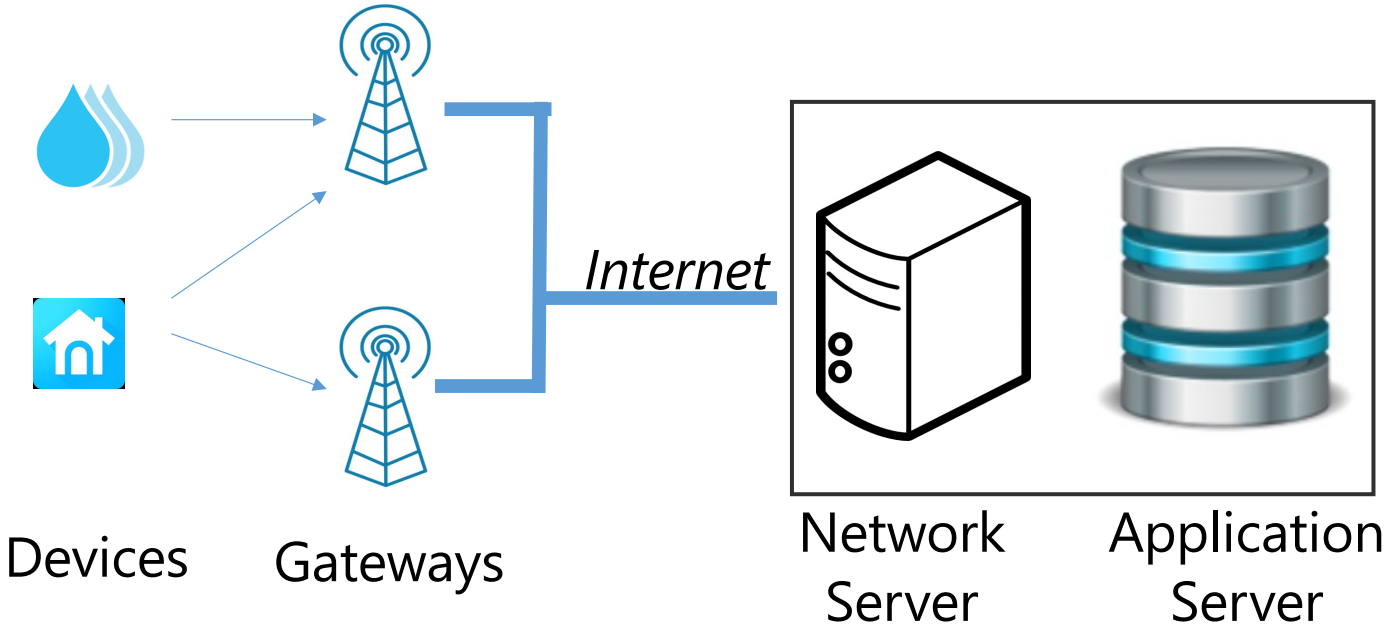
Valid reception only if X ≥ Y

1. Deactivation of the " Frame Counter Check ".

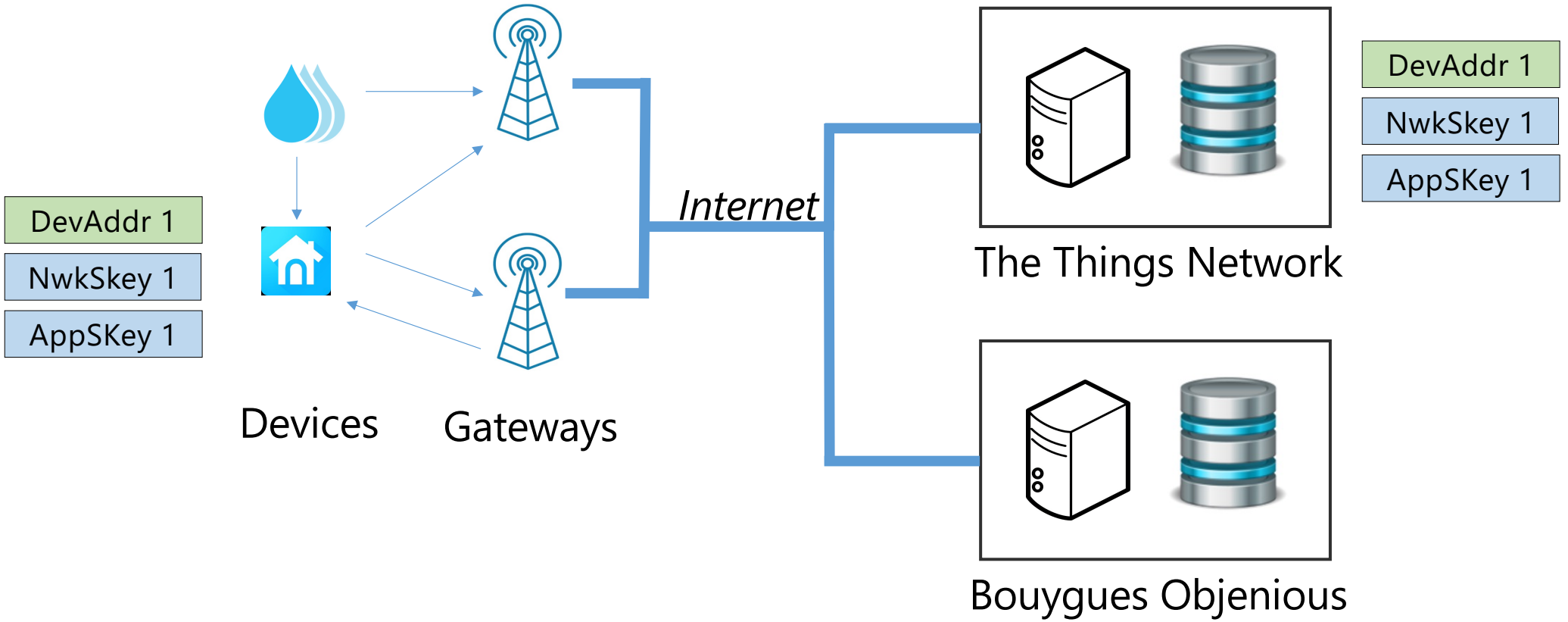
2. Use OTAA activation instead of ABP

3. Keep the value of the " Frame Counter " in a non volatile memory and retrieve its value at the start of the LoRa Device.

The Frame Counter - Demonstration

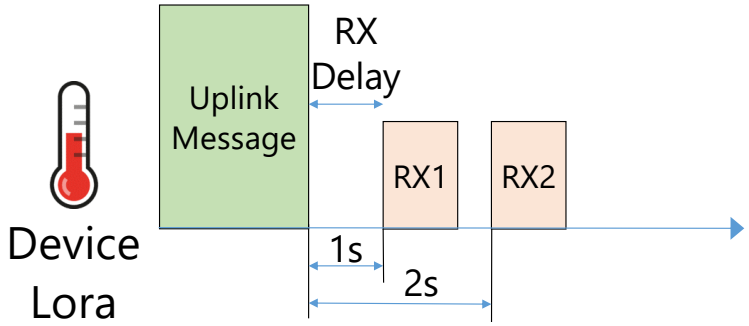


Change of network



RX Delay and CFList

The RX Delay

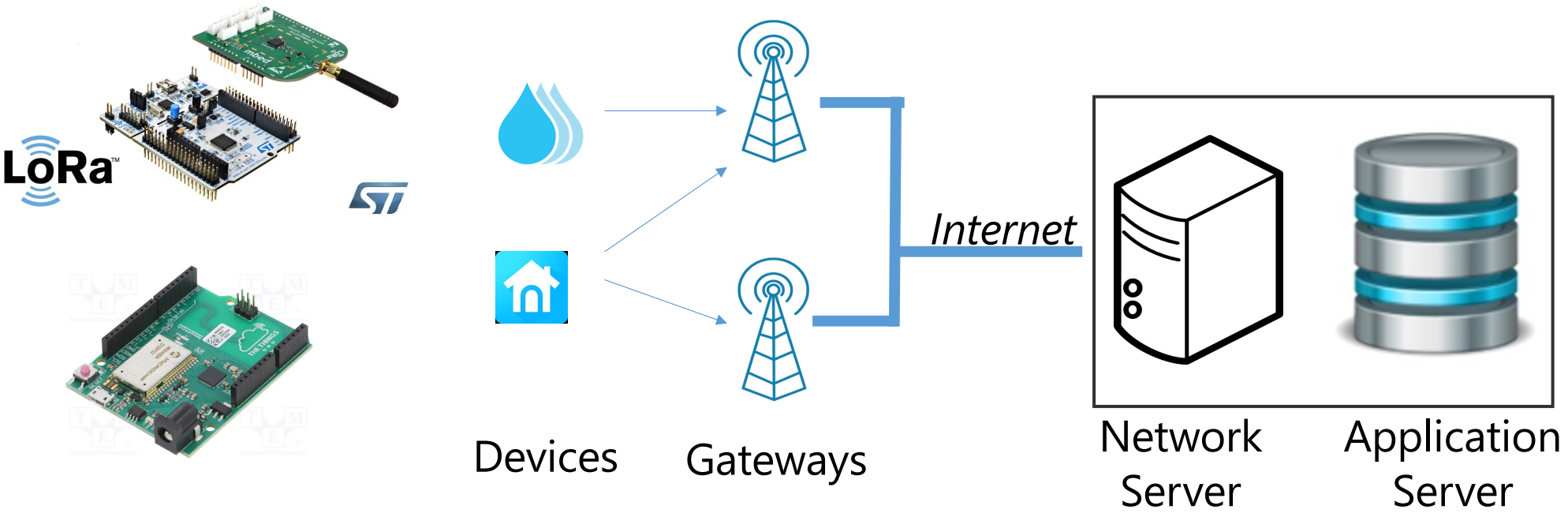


Channels
868.1 Mhz
868.3 Mhz
868.5 Mhz
867.1 Mhz
867.3 Mhz
867.5 Mhz
867.7 Mhz
867.9 Mhz

The CFList

Size (bytes)	3	3	3	3	3	1
CFList	Freq Ch3	Freq Ch4	Freq Ch5	Freq Ch6	Freq Ch7	CFListType

CFList - Demonstration



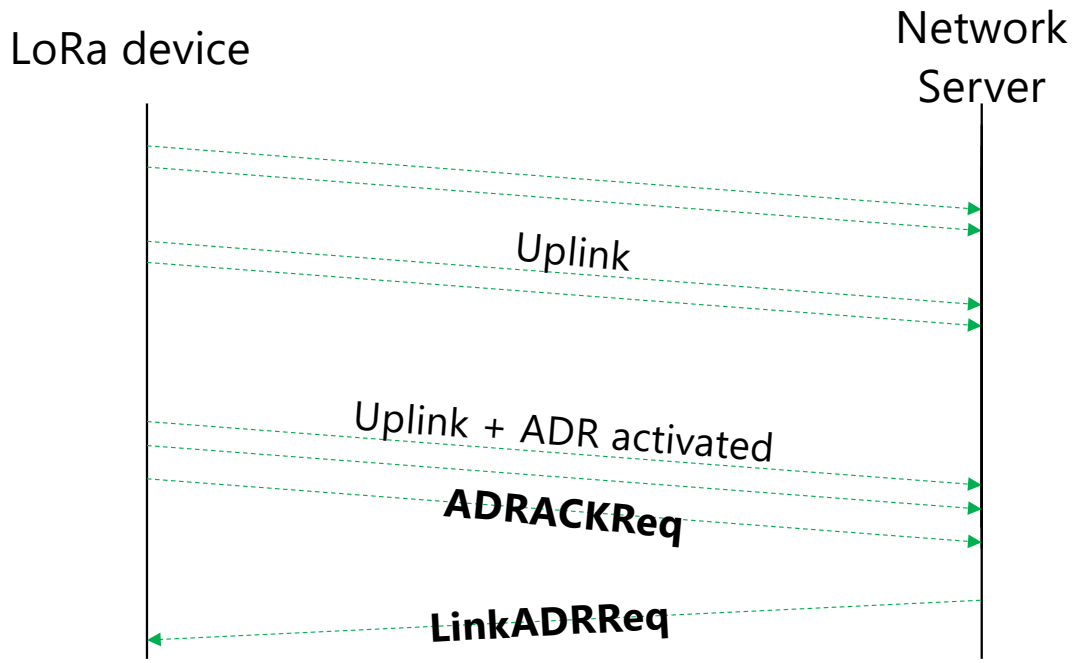
ABP - OTAA Choice: Summary

	ABP	OTAA
Global security	Secure memory storage: **NwSkey** and **AppSKey**	Secure memory storage: **AppKey**
Management of the Frame Counter	Backup in non-volatile memory is mandatory Possibility to disable the counter check by risking replay attacks	Supported by the OTAA
Change of Network	Not possible	Supported by the OTAA
Modification of the RX Delay	Not possible	Supported by the OTAA
Adding channels	Not possible	Supported by the OTAA

Adaptive Data Rate - 1

Parameters to adjust to reduce consumption:

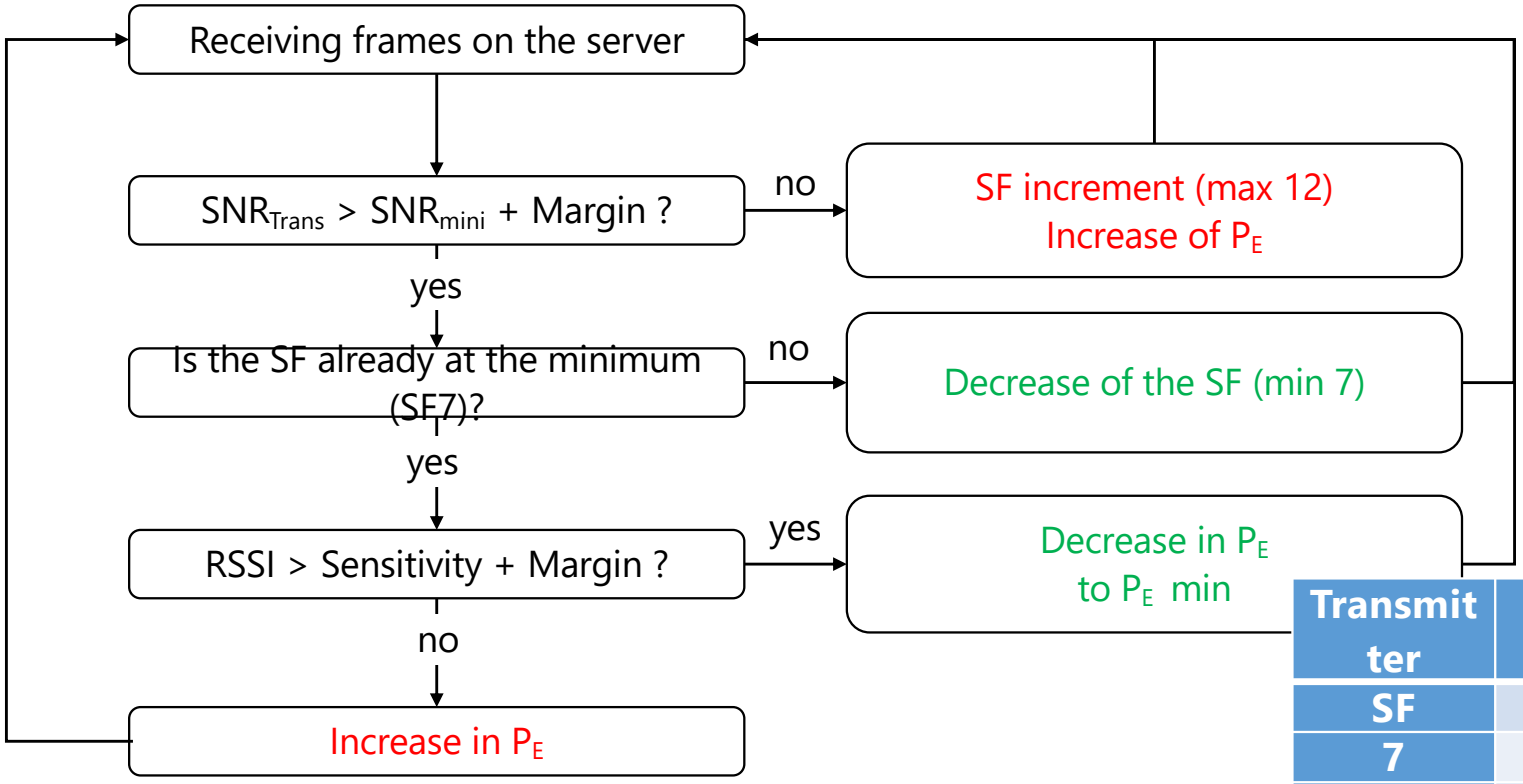
- ✓ The Spreading Factor (SF)
- ✓ Transmitter power (P_E) of the transceiver (in dBm)



Sensitivity

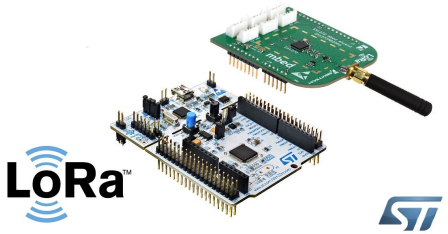
SNR mini

Adaptive Data Rate - 2



Transmitter	Receiver	
SF	Sensitivity	Minimum SNR
7	-123 dBm	-7.5 dB
8	-126 dBm	-10 dB
9	-129 dBm	-12.5 dB
10	-132 dBm	-15 dB
11	-134.5 dBm	-17.5 dB

Adaptive Data Rate - Demo 1



LoRa device

Network Server

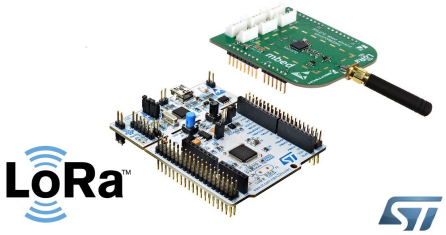
Uplink SF10 + ADR activated

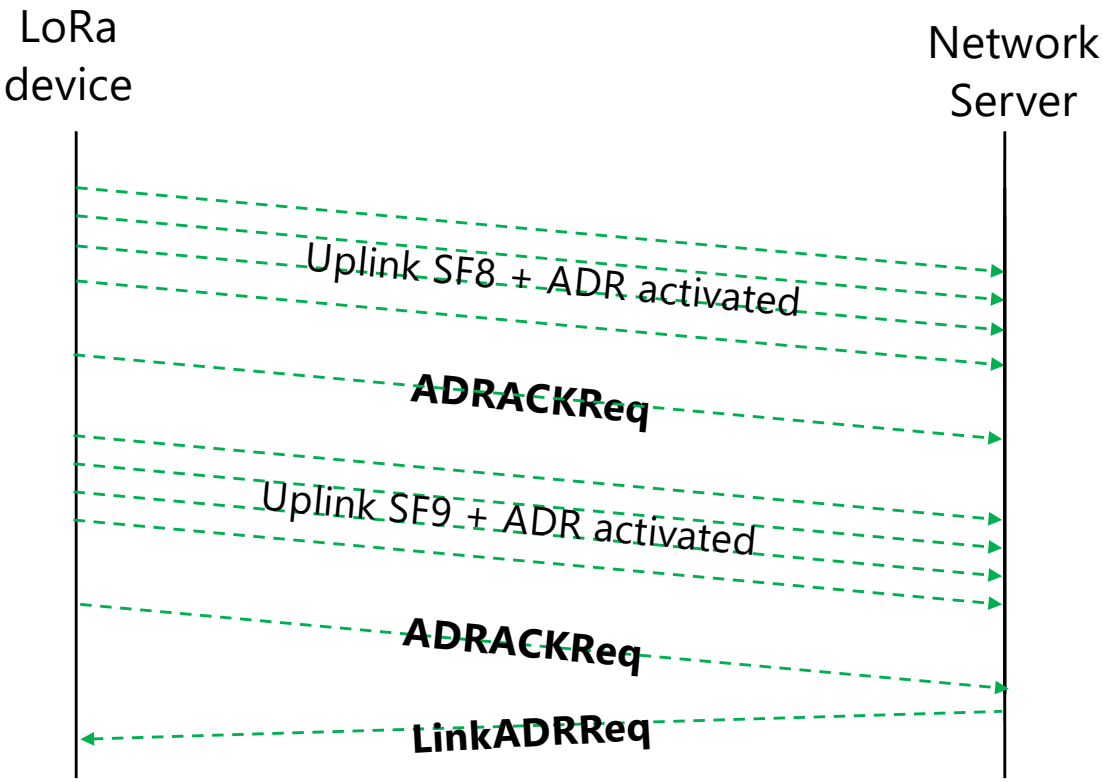
Downlink + **LinkADRReq**

Uplink SF9 + ADR activated

Downlink + **LinkADRReq**

Adaptive Data Rate - Demo 2





THE THINGS NETWORK

Channels, Frequency Bands, Data Rate and TX Power

Channels	Spreading Factor	Bandwidth
868.1 Mhz	From SF7 to SF12	125 kHz
868.3 Mhz	From SF7 to SF12	125 kHz
868.3 Mhz	SF7	250 kHz
868.5 Mhz	From SF7 to SF12	125 kHz
867.1 Mhz	From SF7 to SF12	125 kHz
867.3 Mhz	From SF7 to SF12	125 kHz
867.5 Mhz	From SF7 to SF12	125 kHz
867.7 Mhz	From SF7 to SF12	125 kHz
867.9 Mhz	From SF7 to SF12	125 kHz

Data Rate	Spreading Factor	Bandwidth
DR 0	SF12	125 KHz
DR 1	SF11	125 KHz
DR 2	SF10	125 KHz
DR 3	SF9	125 KHz
DR 4	SF8	125 KHz
DR 5	SF7	125 KHz
DR 6	SF7	250 KHz

TX Power Index	Value in dBm
1	14 dBm
2	11 dBm
3	8 dBm
4	5 dBm
5	2 dBm