



Master 2 SSIO

Systèmes et Services pour l'Internet des Objets



UE Technologie d'accès sans fil
Réseau LoRa®

LoRaWAN™

SOMMAIRE



1. Intro sur l'Internet des Objets

2. Les solutions de connectivités

3. Réseau LoRa®

Normes, caractéristiques, Architecture, classes, couches, provisioning, sécurité, MTypes et commandes MAC

4. Call Flows de base LoRa®

5. Fonctionnalités avancées
LoRaWAN™

Amélioration de l'ADR, Géolocalisation, Roaming, Call Flow avancés LoRaWAN™

6. Annexes



01

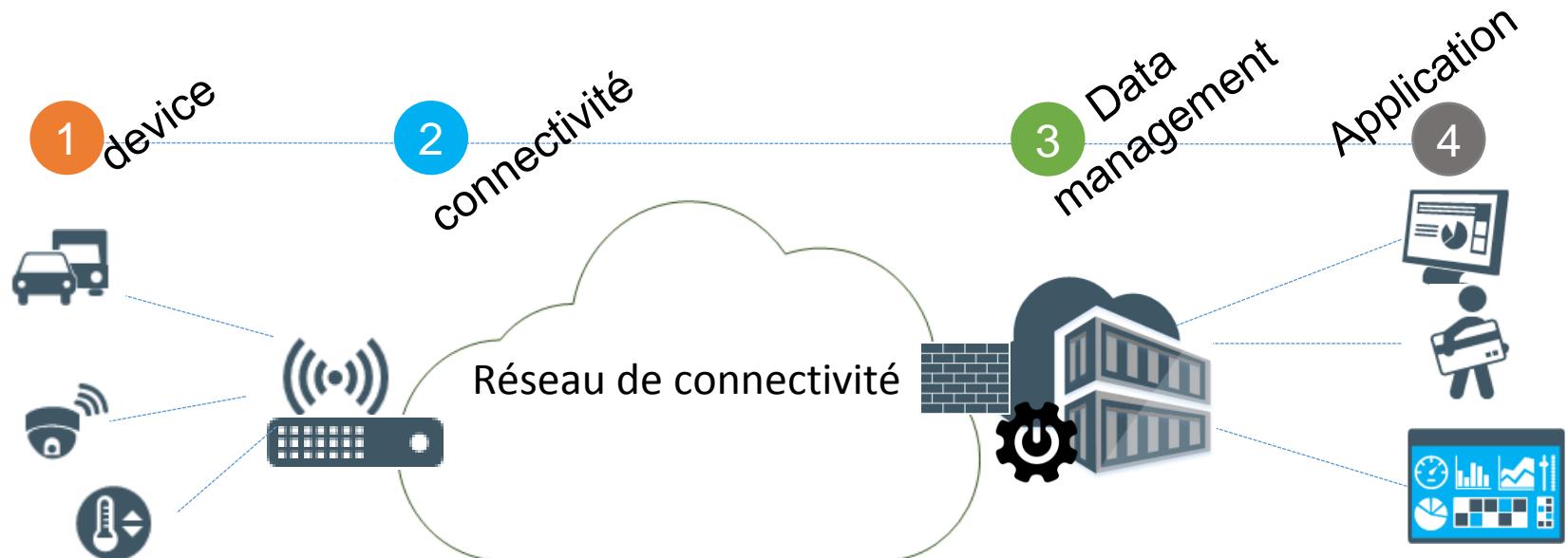
Intro sur l'Internet des Objets

- Définition M2M & IoT
- Le marché de l'IoT
- Quels domaines d'activité ?
- Quels modèles de distribution ?

Définition M2M & IoT

Machine to Machine (M2M), aussi appelé **MTC** (Machine Type Communication) dans les standards 3GPP, est un **mode de communication sans intervention humaine (ou très limitée) entre un device et une application** (SI d'une entreprise) via un réseau de communication.

L'Internet des Objets (IoT) est une **version plus étendue du Machine to Machine et surtout plus ouverte**, dans la mesure où le traitement et la transmission des informations sont dématérialisés et **sortent du cercle interne de l'usine en passant par Internet**. Les données, captées en masse, sont envoyées sur une plateforme de type Cloud.



Une machine/ un Device

1 Une machine/Device équipé d'un module qui permet de remonter des données d'informations issue de capteurs et aussi de réceptionner des messages, équipé ou non d'une carte SIM.

Connectivité réseau

2 Réseau fixe
Réseau cellulaire: 2G/3G/4G/5G
Réseau LPWA
Réseau cellulaire Wifi, NFC, Bluetooth
...

Plateforme de données

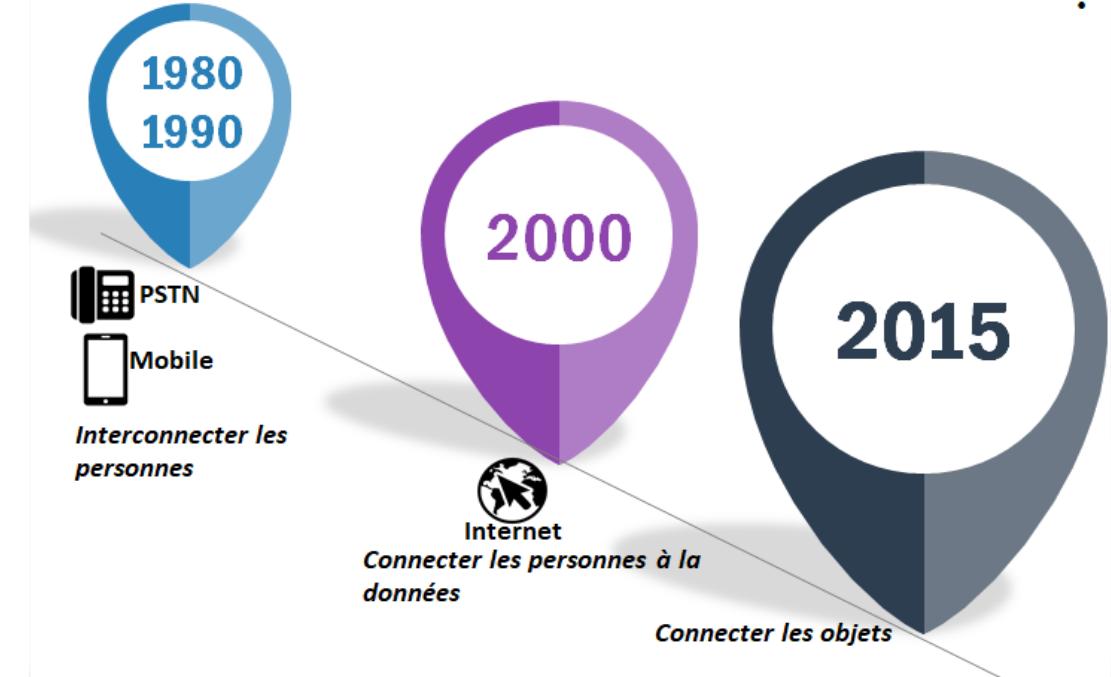
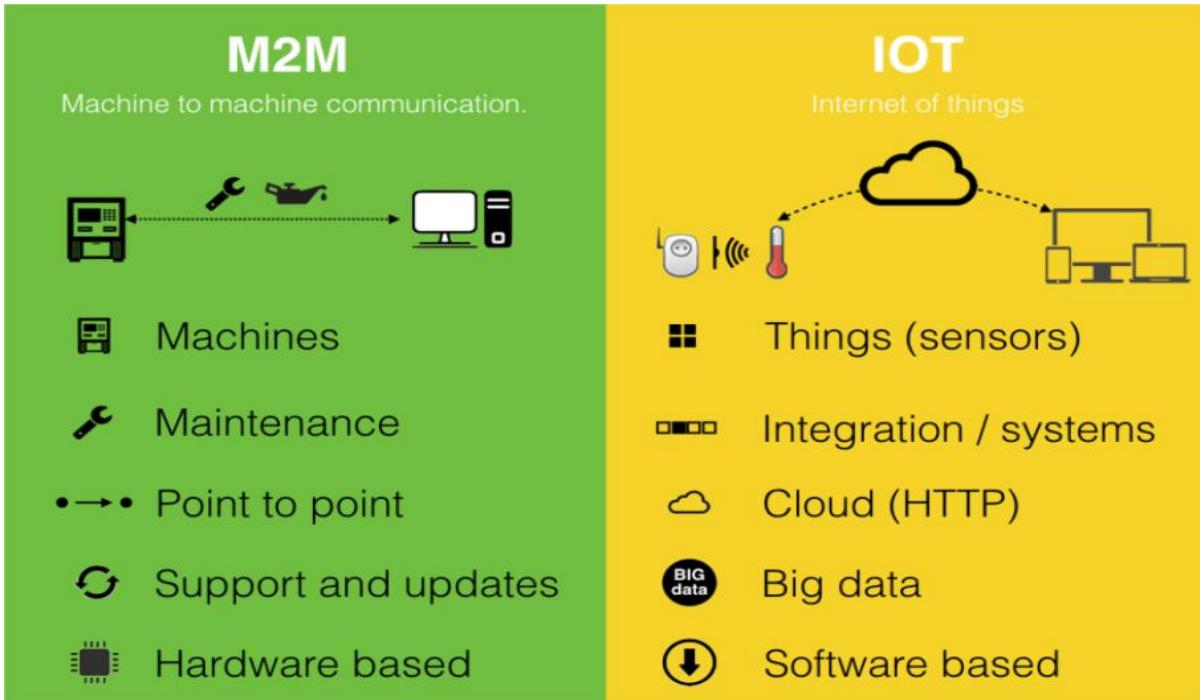
3 Plateforme de gestion des données.
Gestion des devices.
Sécurité.
...

Application métier

4 Une application ou programme logiciel qui traduit l'évènement capturé en information significative.

Différence entre M2M & IoT

L'internet des objets est vue comme une 3^{ème} révolution



Les domaines d'activités ou verticaux



Automotive

- Services et info-divertissement embarqués
- Assurance à l'usage
- Sécurité télématique
- Gestion des flottes
- Télé maintenance des véhicules



Industrie

- Maintenance préventive
- Sécurité du travailleur
- Optimisation des stocks
- Réassort automatique
- Supervision des zones critiques

Santé & humains

- Monitoring des patients chroniques et des patients en sortie d'hospitalisation
- Sérénité des proches
- Suivi des personnes âgées
- Boutons satisfaction



Smart Cities

- Contrôle d'accès au bâtiment
- Éclairage intelligent
- Optimisation du remplissage des parkings
- Optimisation de gestion du trafic

Smart Home

- Télésurveillance et sécurité à domicile
- Domotique
- Gestion de l'énergie
- Smart Office

Smart Agri

- Suivi de la récolte et des champs.
- Vaches Connectées
- Suivi des ruches
- Pet tracking

Les différents modèles de distribution

- Marketing **B2C**: Business to Consumer

Du professionnel au consommateur final.



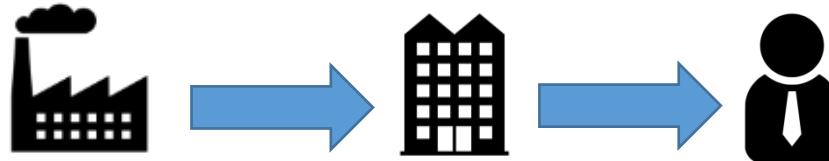
- Marketing **B2B**: Business to Business

Des sociétés vendent des produits à d'autres sociétés qui les utilisent.



- Marketing **B2B2C**: Business to Business to Consumer

Des professionnels vendent leurs produits à d'autres qui vont se charger de les vendre aux consommateurs finaux.

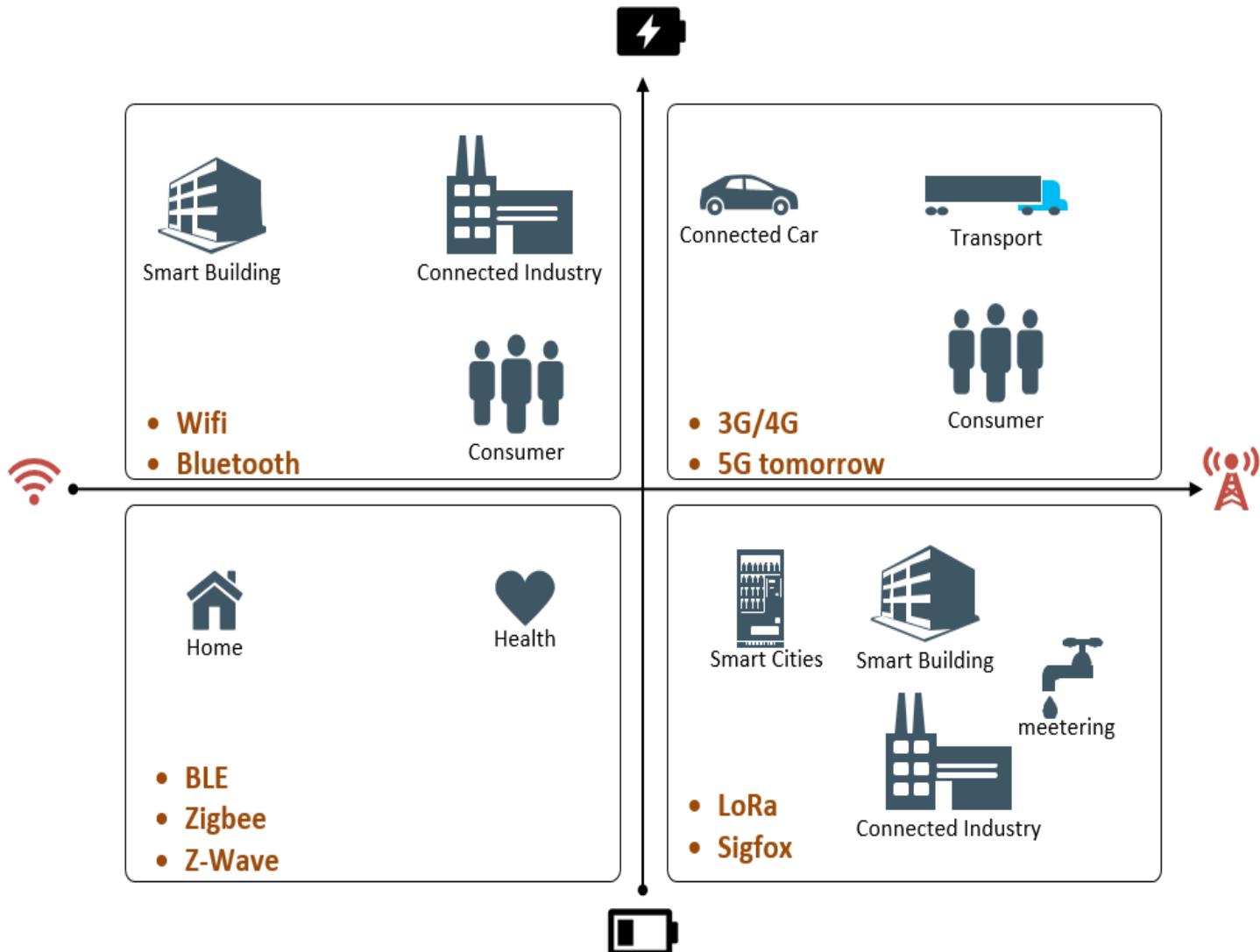




02

Les solutions de connectivités

Les solutions de connectivité



Les solutions répondent à une ou plusieurs problématiques différentes.

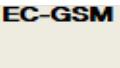
Cela va dépendre du cas d'usage (ou Use Case) applicatif et des contraintes liées :

- De débits.
- De latente.
- De consommation d'énergie.
- De couverture.
- Du coût.
- De sécurité.
- De mobilité.
- ...

Il existe différentes solutions de connectivité IoT, 3GPP* ou non 3GPP*

*3GPP : 3rd Generation Partnership Project → coopération de normalisation de réseaux mobiles 2G, 3G, 4G et 5G

Comparaison des technologies

	 LoRa	 SigFox	 CategM1	 NB_IoT	 EC-GSM	 LTE Cat1	 LTE Rel8 Categ4
Technology	non 3GPP	non 3GPP	3GPP Rel13	3GPP Rel13	3GPP Rel13	3GPP Rel8	3GPP Rel8
Bandwidth	125Khz GW v1: 8 canaux GW v2: 16 canaux	100Hz	1.4Mhz (1.08MHz)	200Khz (180KHz)	200Khz	5/10/1520Mhz	5/10/1520Mhz
Spectrum	no license ISM Band: 868MHz	no license ISM Band: 868MHz	license, In-band LTE	license, In-band & Guard-band LTE, StandAlone	Licensed Inband GSM	license	license
Downlink	Proprietary Semtech LoRa (CSS =Chirp Spread Spectrum)	Proprietary SigFox UNB (Ultra Narrow Band)	OFDMA, 15Khz tone spacing, Turbo code, 16QAM, 1Rx	OFDMA, 15Khz tone spacing, 1Rx	384Kbps	OFDMA	OFDMA
Uplink	Proprietary Semtech LoRa (CSS =Chirp Spread Spectrum)	Proprietary SigFox UNB (Ultra Narrow Band)	SC-FDMA, 15Khz tone spacing, Turbo code, 16QAM, 1Rx	Single tone, 15KHz & 3.75KHz spacing SC-FDMA, 15KHz tone spacing, Turbo code	60Kbps	SC-FDMA	SC-FDMA
Battery Lifetime	10+ Year	10+ Year	10+ Year	10+ Year	10+ Year		
Power Class	14dBm / 20dBm	14dBm / 20dBm	23dBm, 20dBm	23dBm	23dBm / 33dBm	23dBm	23dBm
Power saving			Mode PSM, eDRX	Mode PSM, eDRX			
Duplex Mode	Asynchrone	Asynchrone	Half Duplex (HD-FDD) Full Duplex (FD-FDD)	Half Duplex (HD-FDD)	HD;FDD	Full Duplex (FD-HDD)	Full Duplex (FD-HDD)
UE Receiver chain	1	1	1	1		2	2
Coverage MCL	154dB	151dB	160.7dB 155.7dB	164dB	164dBm	130dB	130dB
Enhance coverage	-	-	CE Mode A (5dB) CE Mode B (10,15 dB) +15dB	Normal/ Robust +10dB/ Extreme +20dB		-	-
Outdoor coverage	<10km	<13km	<10km	<15km	>15km		
Interference	High	High	Low	Low		Low	Low
Voice	NO	NO	YES	NO	NO	YES	YES
SMS	NO	NO	YES	OPTION	YES	YES	YES
Cell capacity	40 000	50 000	1M+ per cell (E//)	200000 (E//)			
Throughput	<5kbps Payload depend on SF (51 to 221bytes)	<100bps Payload 12/8 Bytes Max	DL Max 1Mbps UL Max 1Mbps	DL 250Kbps UL 20Kbps Single tone; 250Kbps Multi one.		DL 10Mbps UL 5Mbps	DL 150Mbps UL 50Mbps
Number of message	limited by duty cycle	limited by duty cycle	Unlimited	Unlimited		Unlimited	Unlimited
Handover	No Handover	No Handover	Support Cell Reselection (First) Support Handover (Next)	Support Cell Reselection	Support Cell Reselection	Handover	Handover
Roaming	yes	yes(SNO)	yes	yes		yes	yes
Fast Moving	Tested mobility 80km/h		+ 300Km/h	240km/h		+ 300Km/h	+ 300Km/h
Localisation	yes	no	yes	yes		yes	yes
Latency	ex: SF12, 51bytes->2.5s	ex: 192 bits -> 1.92s	From 200ms			From 10ms	From 10ms
Rollout	new network	new network	Software + Hardware?	Software + Hardware?		-	10 -
Module Cost	\$8 and 2017 3.5\$?	as	as			



03

Le réseau LoRa®

- Normes, caractéristiques, Architecture, classes, couches, provisioning, sécurité, MTypes et commandes MAC

Définition d'un réseau LPWAN

Low Power Wide Area Network

Un réseau LPWAN offre la possibilité de communiquer sur une longue distance avec une consommation modérée.

On parle aussi de réseau 4L (rien à voir avec la voiture ☺), car il répond à 4 critères (commençant par la lettre 'L') :

 Low Power

 Long Range

 Low Cost

 Low Data Rate

2 familles de réseaux : Propriétaires et Licenciés

Utilisations de solutions propriétaires

- usage de bandes de fréquences libres
- bandes gratuites mais notion de Duty Cycle

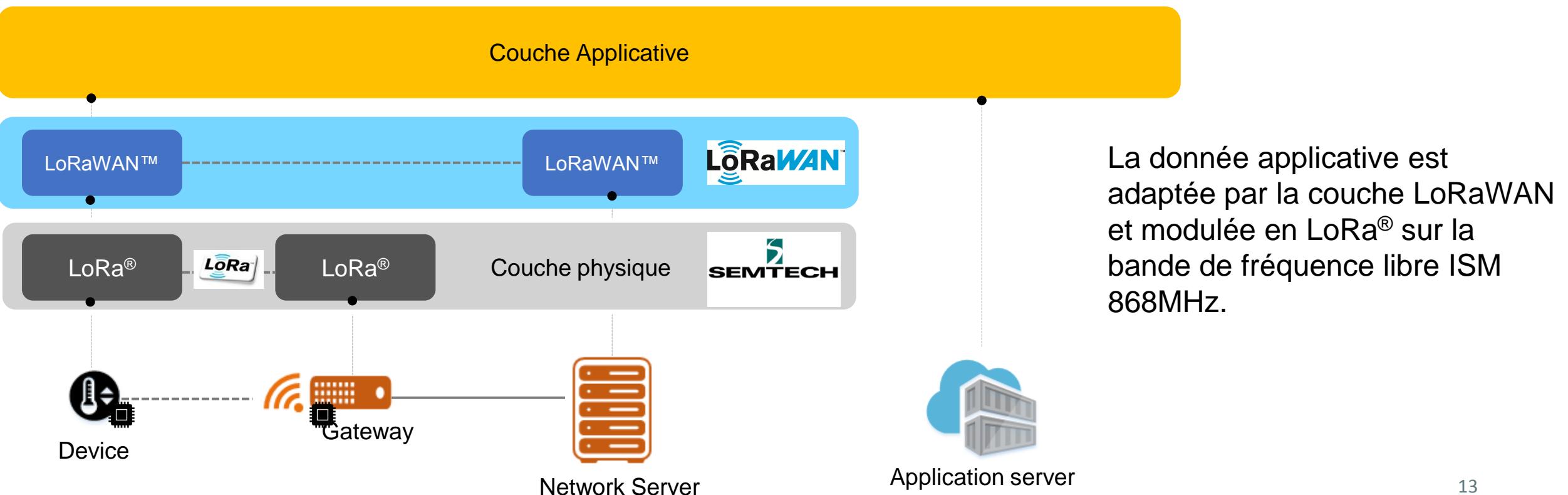
Utilisation de solutions 3GPP

- Usage de bandes de fréquences licenciées
- coûteuses mais sans contrainte d'interférence



LoRa® et LoRaWAN™

- **LoRa®** est une **modulation radio propriétaire à étalement de spectre** développée par une société grenobloise appelée CYCLEO, qui fut rachetée en 2012 par Semtech.
- **LoRa® signifie Long Range.**
- Modulation LoRa® utilisée entre le device et la gateway sur l'interface radio dans une bande de fréquence publique. Pour ce faire, **le device et la gateway embarquent un chipset Semtech de type SX1272 / SX1273.**
- **La couche LoRaWAN™** est une couche protocolaire Open Source développée au sein de la **LoRa Alliance** permettant la communication bas débits, **s'appuyant sur la couche radio physique LoRa®**.



- La LoRa® Alliance est une association ouverte à but non lucratif qui compte aujourd'hui plus de 500 membres depuis sa création en mars 2015.
- Membres : Opérateurs et fournisseurs de solution : chipsets, modules, devices, gateways, cœurs de réseau et Application Server

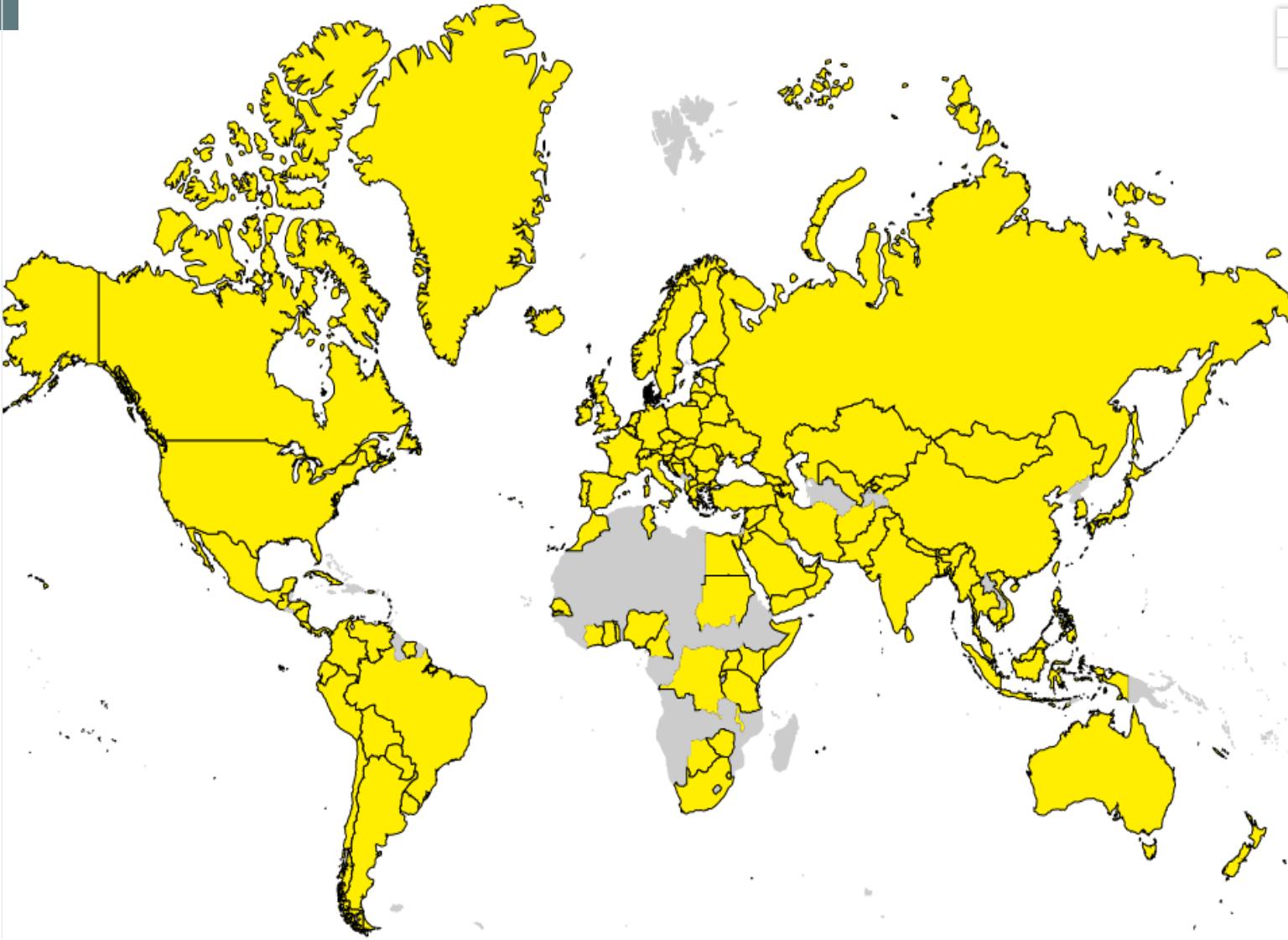


- Objectif : partager les expériences afin de promouvoir et de garantir le succès du protocole LoRaWAN en tant que norme mondiale ouverte et leader en matière de connectivité LPWAN pour l'IoT
➔ Rédaction de normes, plans de test et autres documents de recommandations techniques pour garantir le bon fonctionnement des réseaux et des devices sur ces mêmes réseaux

Les Opérateurs réseaux de norme LoRaWAN™

Dans le monde: **173**

LoRaWAN Network Operators globally.



En France il existe :



- 2 réseaux publics avec couverture nationale



- Des réseaux privés LoRaWAN™
Réalisation de son propre réseau privé en implémentant ses propres équipements gateway et antennes.

Ex : la ville de Rennes a annoncé en 2019 le déploiement d'un réseau LoRa® privé.

Caractéristiques d'un réseau LPWAN LoRaWAN™

Les réseaux LPWA sans licence sont une alternative aux réseaux cellulaires pour la transmission de petits paquets de données à longue portée, à partir de capteurs ou d'objets alimentés par batterie et à haute efficacité énergétique.



Technologie propriétaire
Modulation LoRa®



Spécification LoRaWAN™
LoRa Alliance



Construction d'un nouveau
réseau dédié



Fréquence libre (868MHz en EU)



Très faible consommation
d'énergie



Modules à bas coûts



Couverture longue portée et
indoor
Couverture indoor profond via
des nano GW.



Bidirectionnel



Faibles débits
250 bps à 5 Kbps

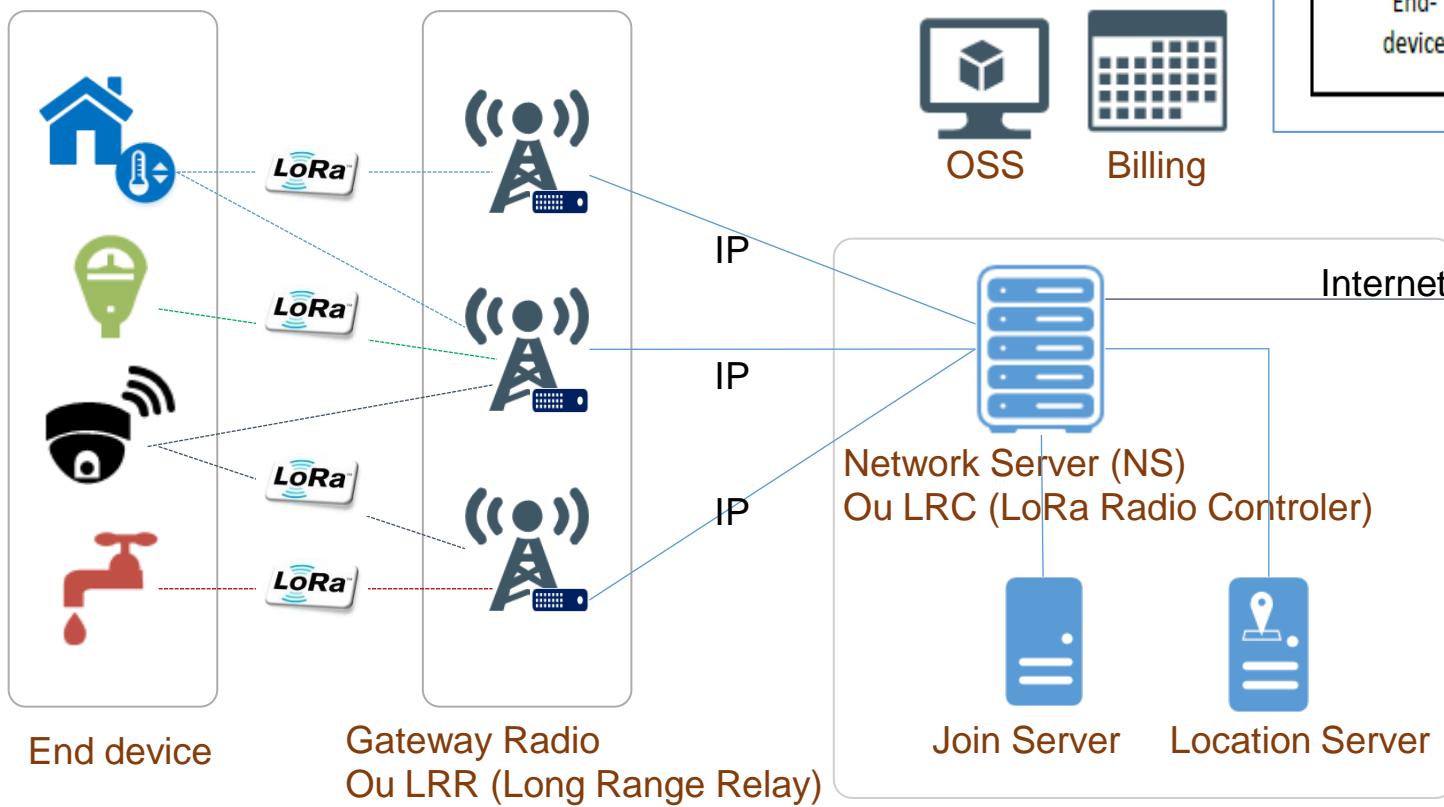


Aucune mobilité

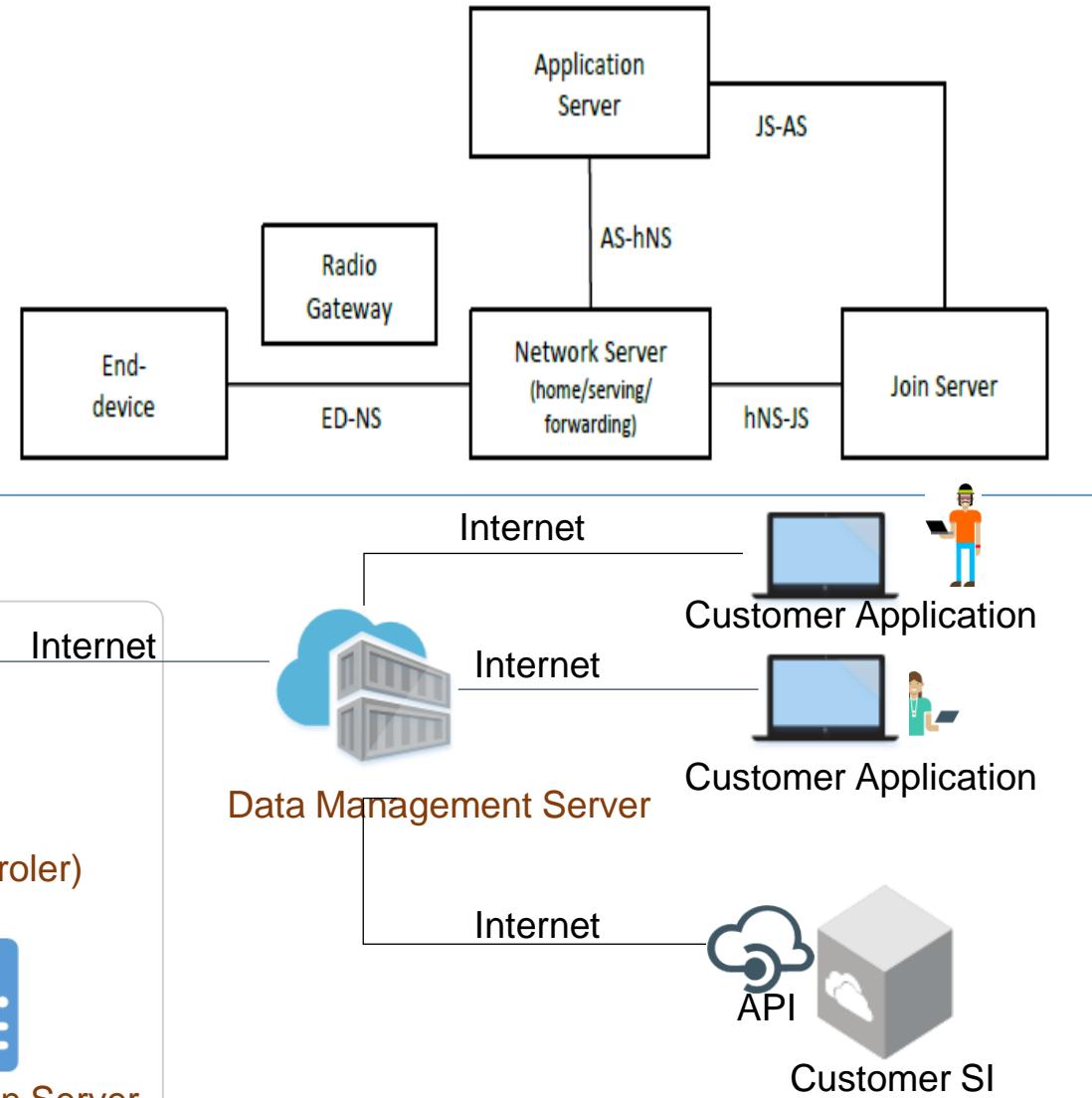
Architecture d'un réseau LoRaWAN™

Un réseau LoRa® est composé de :

- ❖ Devices correspondant aux capteurs.
- ❖ Gateways (GW) qui représentent l'émetteur/récepteur, déployées sur le territoire. Elles sont aussi appelées LRR (Long Range Relay)
- ❖ Un Network serveur (NS) ou LRC (Long Range Controller) qui réalise les fonctions de contrôleur et de gestion des devices.
- ❖ Un plateforme de post-traitement des données appelée « Data Management Plateforme » (DMP) assimilée à un cloud data.
- ❖ Une solution de supervision (OSS) et de facturation (billing).



Spécification: LoRaWAN Network Reference Model (NRM)



Les devices d'un réseau LoRa®

3 couches :

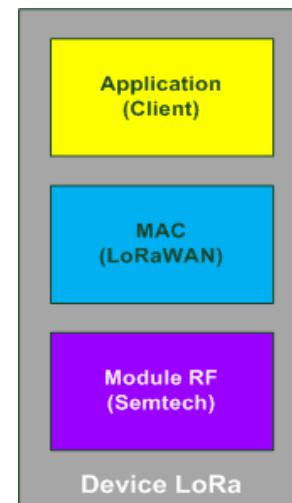
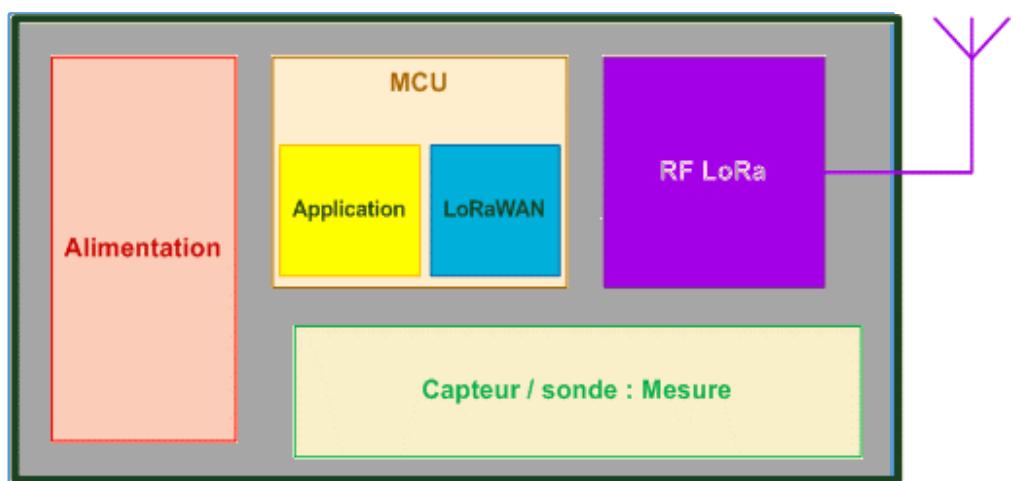
- **Applicative**
- **LoRaWAN**
- **Physique**

2 modes d'activation :

- **ABP (Activation By Personalization)** → clés de session fixes définies en dur sur le device
- **OTAA (Over The Air Activation)** → clés de session dynamiques calculées lors de la procédure JOIN (première communication entre le device et le réseau).

1 identifiant unique : **DevEUI**

Les devices LoRa® peuvent être certifiés au sein de la LoRa Alliance et/ou chez les opérateurs



Bouton de satisfaction



Télérelève de compteur d'eau



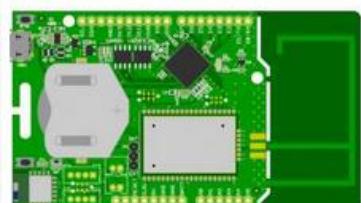
Traqueur industriel



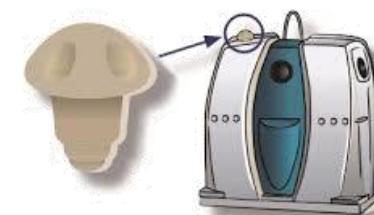
Micro tracker



Field test



Kit de développement



Taux de remplissage de conteneurs



Capteur de température

Les devices d'un réseau LoRa®

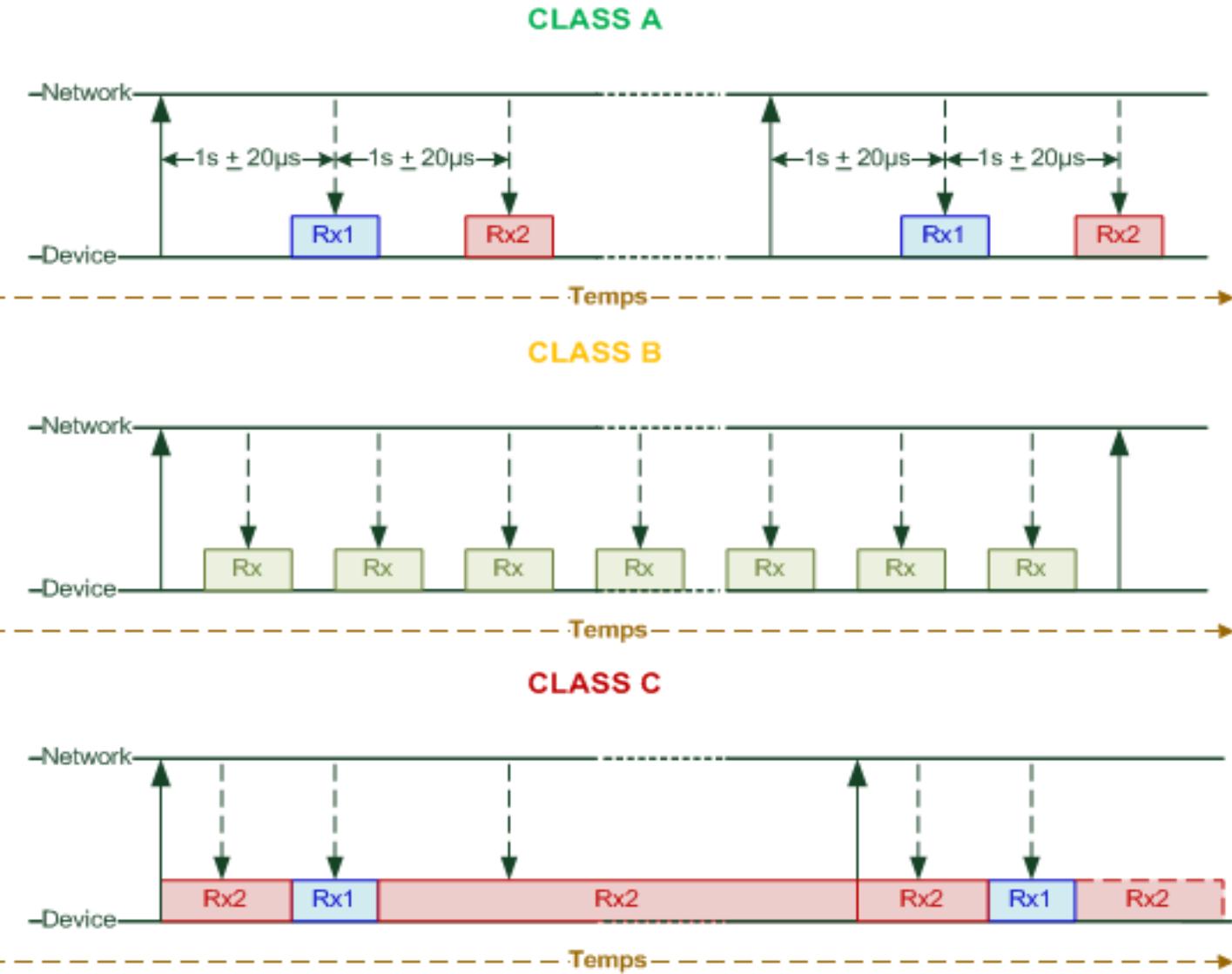
3 classes :

- **Class A (All)**
- **Class B (Beacon)**
- **Class C (Continuous)**

La classe A est la moins énergivore, car le device passera la plupart de son temps en mode dormant, ne possédant que **deux fenêtres de réceptions Rx1 et Rx2**). Elle demeure à ce jour la classe privilégiée (99% des devices déployés sur les réseaux LoRa mondiaux) du fait de **sa faible consommation de batterie qui permet une durée de vie importante du device**

La classe B l'est davantage, avec des fenêtres de réception Rx régulières. Elle **nécessite une synchronisation d'horloge régulière entre le device et le réseau (gateway qui envoie des trames balises)**, ce qui permet notamment **la possibilité de faire du FUOTA (Firmware Upgrade Over The Air)**.

Un device en classe C est au contraire assez énergivore puisqu'il sera toujours à l'écoute en dehors de ses **périodes de transmissions**. Cette classe nécessite donc un device avec une grosse batterie ou alimenté en permanence, et est utile pour des cas d'usage nécessitant une réactivité rapide du device côté applicatif.



Les gateways d'un réseau LoRa®

Partie Hardware : connectivité, fonction RF, fonction de routage.

Partie Software : appelée Long Range Router (LRR) sur laquelle est implémentée le logiciel open source LoRaWAN™ MAC.

Macro Gateway: Cisco, Kerlink, Tektelit....
Couverture outdoor.



Nano Gateway: Multitech, Kerlink...
Couverture indoor.

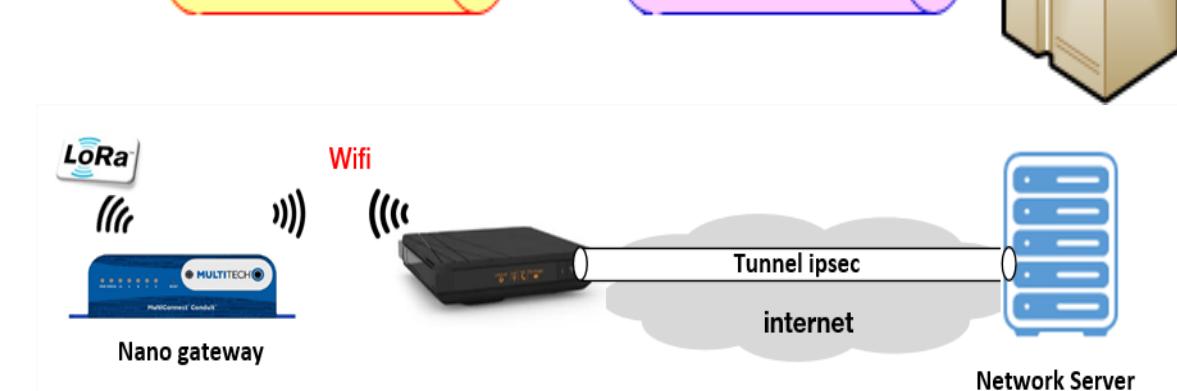
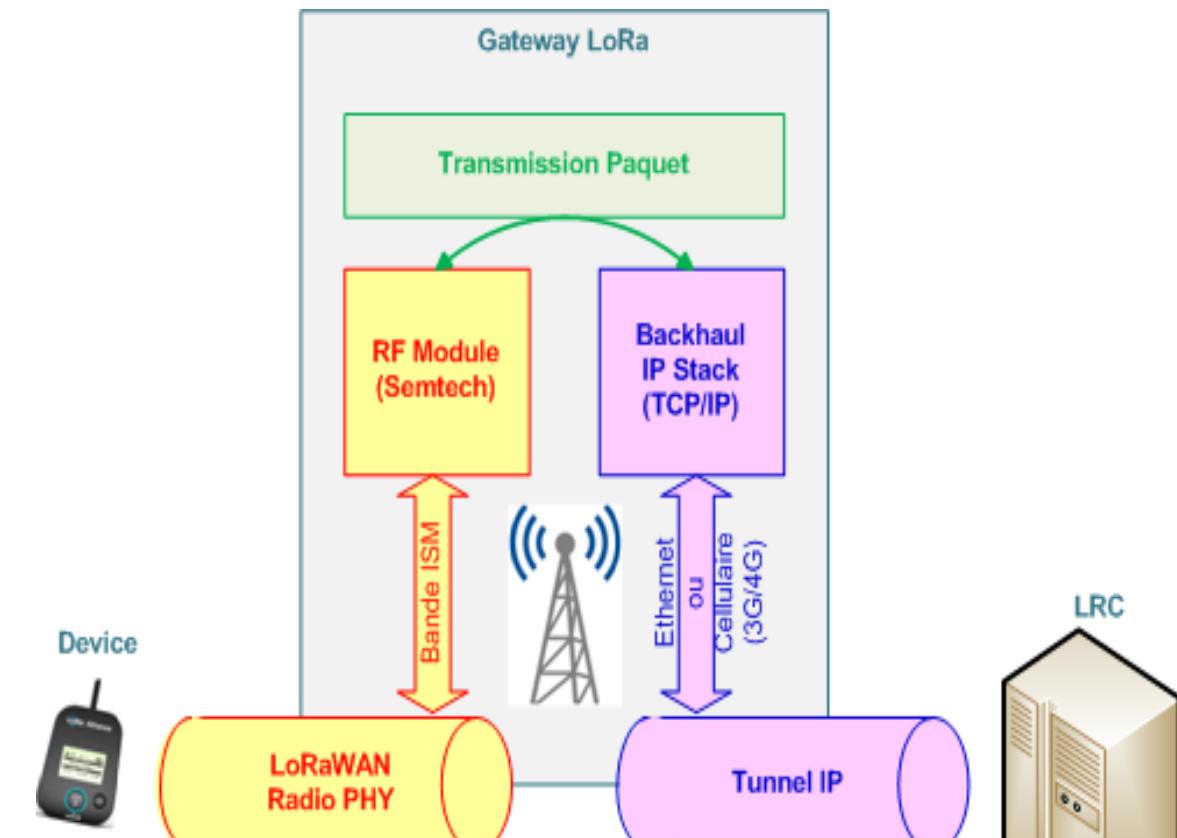


Les macro et nano gateway sont connectées au network serveur via :

- › **Un backhaul Intranet** (backbone privé utilisant ou non IPSEC)
- › **Un backhaul Internet** (utilisant le réseau public – IPSEC devient alors obligatoire pour la sécurité)

Dans le cas d'un backhaul Internet, il existe différentes connexions possibles entre la gateway et Internet :

- › **Un backhaul Wi-Fi ou Ethernet** via une box, qui donne l'accès à Internet
- › **Un backhaul cellulaire** : usage d'une carte SIM avec accès Internet en passant par le réseau d'accès et cœur mobile (2G/3G/4G)
- › **Un backhaul satellitaire** : communication de la gateway avec un satellite qui renvoie l'information au cœur de réseau NS via Internet



Les éléments d'un réseau LoRa®

Network serveur

Fonction LRC: LoRa Radio Controller.

Gestion de la couche LoRaWAN™, software Open Source.



- Gestion de la couche MAC.
- Gestion des messages montant & descendant.
- Sélection de la meilleure gateway dans le sens descendant.
- Gestion de l'algorithme ADR (Adaptive Data Rate).
- Gestion des devices (provisionning, supervision...).
- Gestion des gateways (provisionning, supervision...).
- Routage des données (MQTT, HTTP Push, HTTP...)
- Gestion des API

Rôle du JOIN SERVER:

Gestion des clés AES 128 pour la procédure JOIN.

Rôle du Serveur de localisation:

Calcul la localisation des devices à partir des différentes données.

Application Server:

Service managé pour permettre une communication bidirectionnelle entre les appareils IoT et l'application server

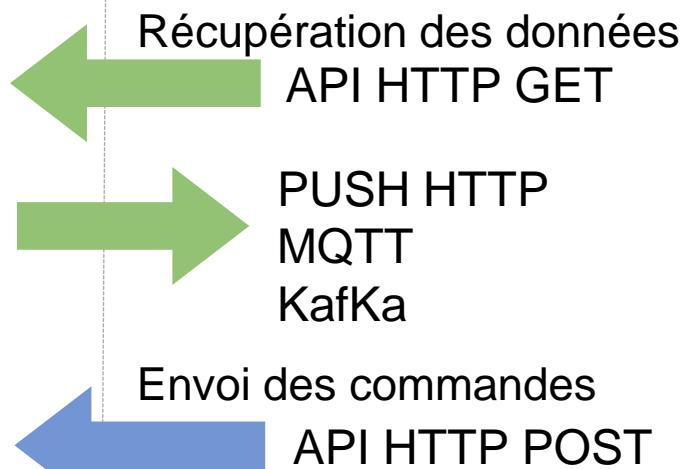
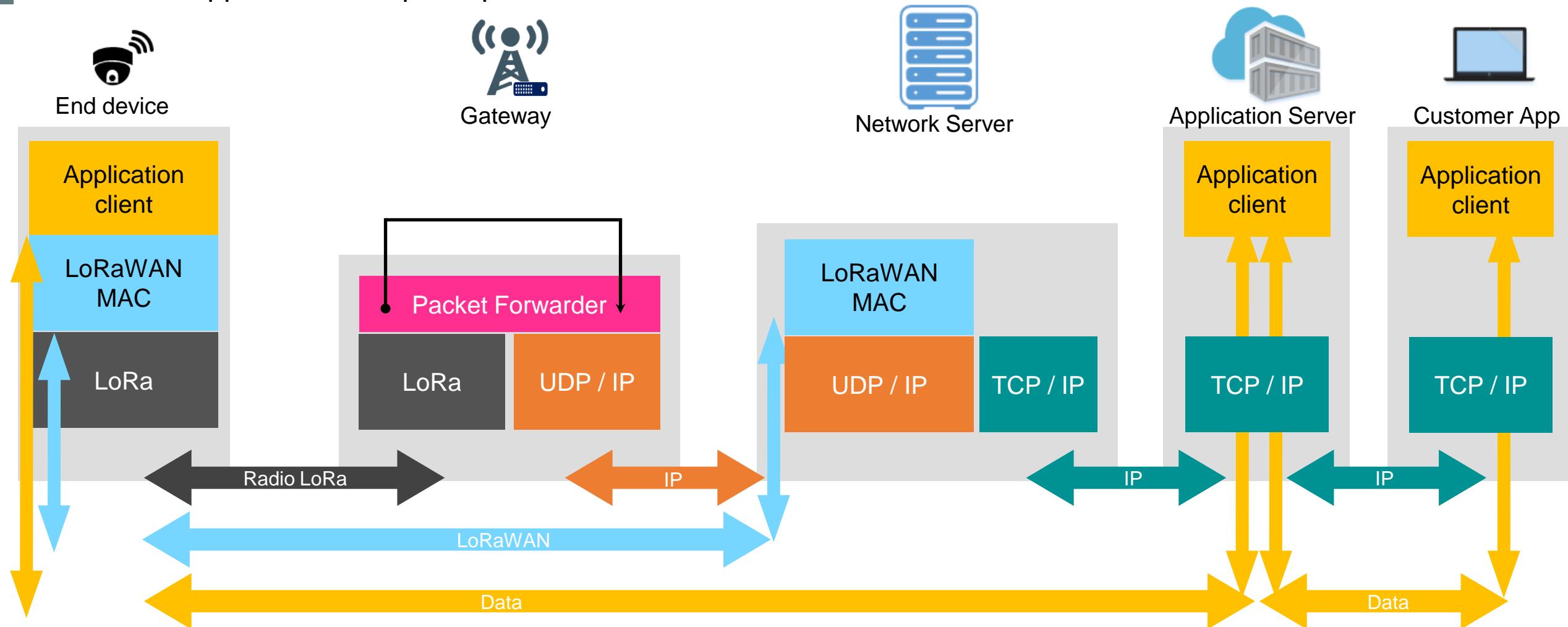


Schéma protocolaire

La couche physique est propriété de Semtech.

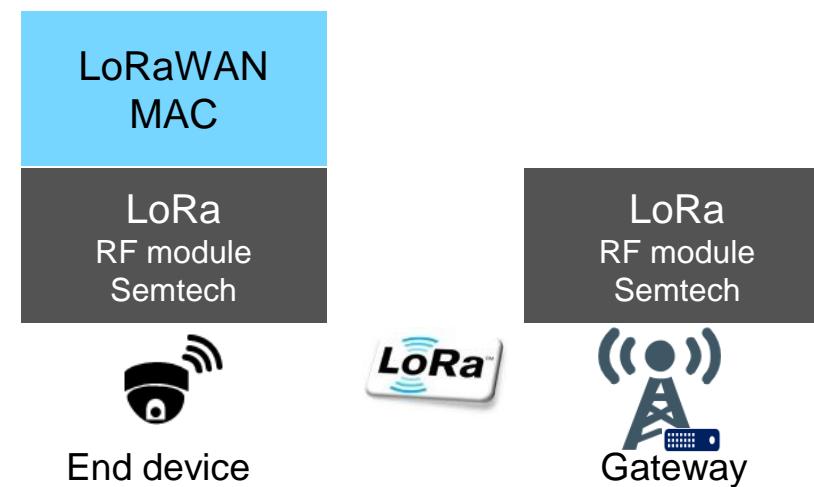
La couche LoRaWAN est spécifiée par la LoRa Alliance et est Open Source.

La couche applicative est spécifique au client et au device.



Couche Physique LoRa® - End Device <> Gateway

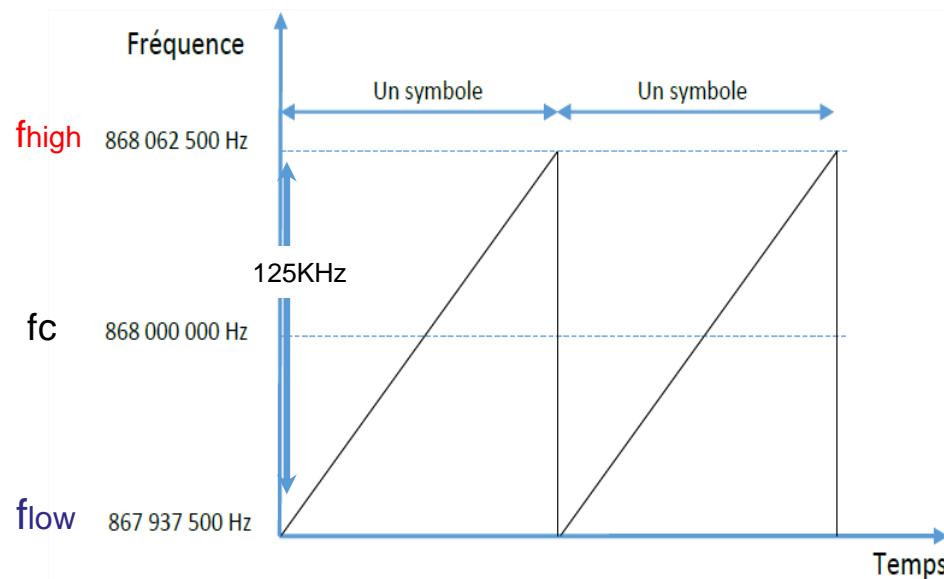
- Permet de « moduler » la donnée issue de la couche MAC sur le lien radio du device à la gateway, et de « démoduler » le signal de la gateway au Device.
- Utilisation d'une modulation propriétaire Semtech, appelée LoRa® de type FSK (frequency-shift keying).
- Dans chaque device et chaque gateway, un chipset LoRa® construit par Semtech (SX1272, SX1273) dont les principales caractéristiques radios sont les suivantes :



La modulation LoRa®

- Pour transmettre les informations la **modulation LoRa® utilise la méthode CSS (Chirp Spread Spectrum)** basée sur le principe d'étalement de spectre sur une large bande, ce qui en fait un système robuste contre le bruit et le multi-path fading.

La modulation LoRa® utilise le mode FSK (Frequency Shift Keying). Le principe est de faire varier la fréquence pour transmettre les informations. Le signal émis en LoRa® est un symbole dont la forme de base appelé Chirp est représentée ci-dessous :



La fréquence de départ est la fréquence centrale du canal moins la bande passante divisée par deux (**125KHz/2**), représentée par **flow**. La fréquence de fin est la fréquence centrale plus la bande passante divisée par deux, représentée par **fhigh**.

- La fréquence centrale est appelée **canal** (canal sur la bande 868MHz).
- La bande passante est la largeur de bande occupée autour du canal fixé à 125KHz dans le cadre d'un réseau LoRaWAN.

En LoRa®, chaque symbole représente un certain nombre de bits transmis. Ce nombre de bits est identifié par le **Spreading Factor SF qui représente le facteur d'étalement et qui varie de 7 à 12**.

Nombre de bits transmis dans un symbole = SF

Exemple: SF=7 ► 1 symbole est composé de 7 bits ► soit 2^7 combinaisons soit 128 combinaisons possibles (soit 128 chips) (0 à 127).

La modulation LoRa®

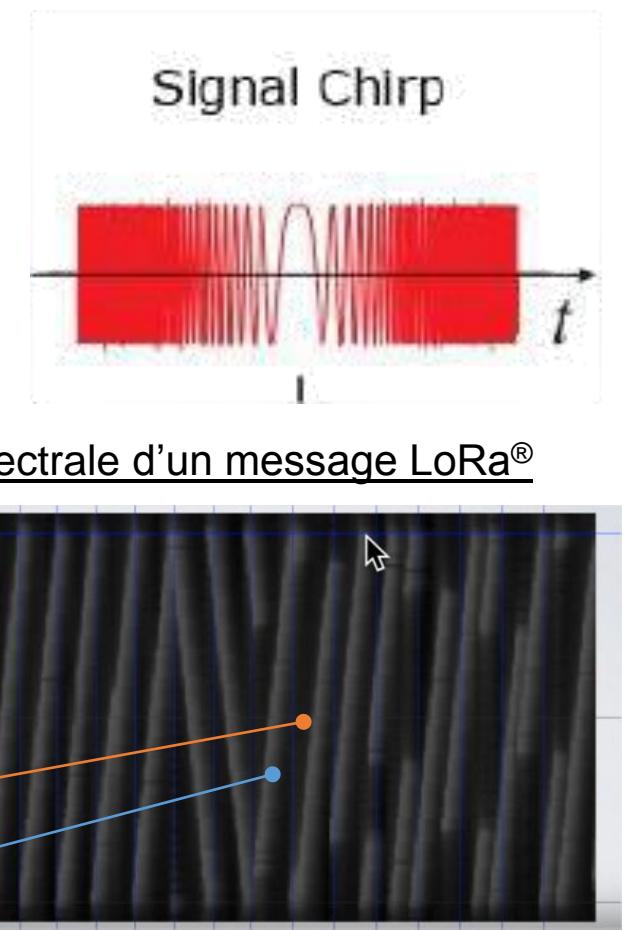
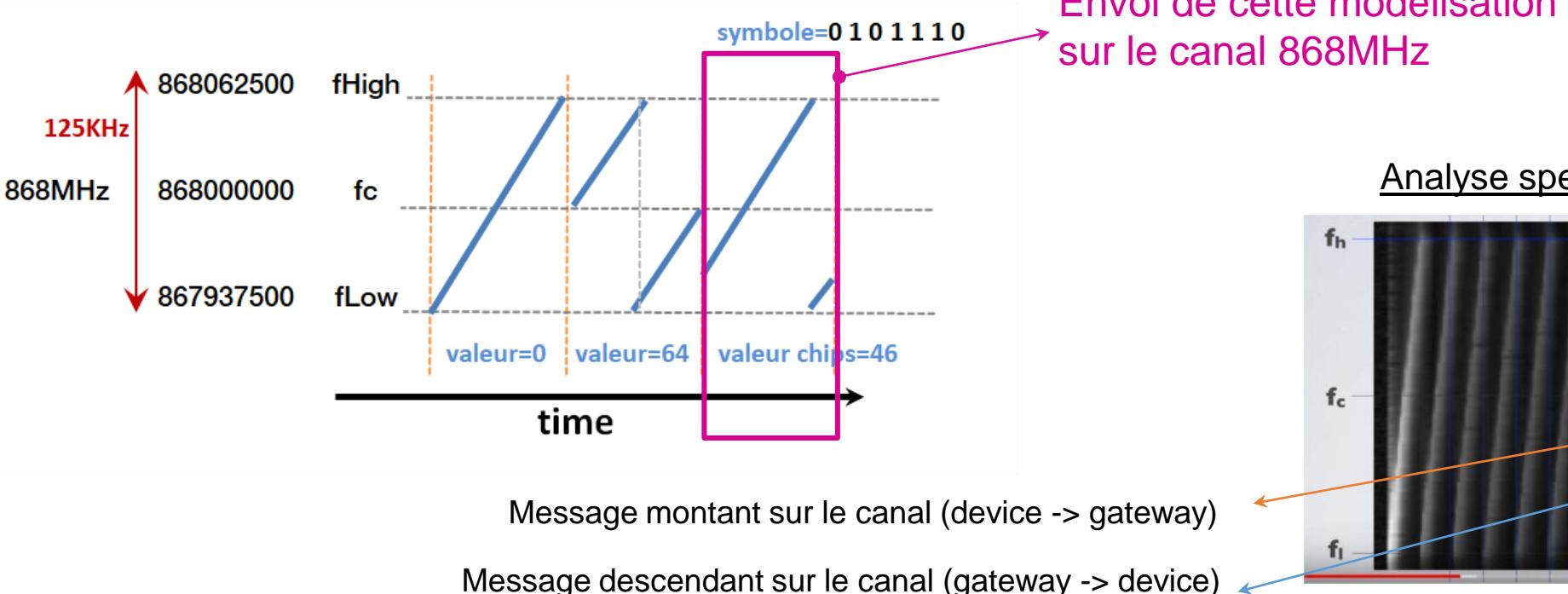
Ex : Utilisation du SF7 → On en déduit 1 symbole = 7 bits et 2^7 soit 128 combinaisons possibles.

La valeur d'entrée est la suivante: 0 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 0 1 1 0 1

On découpe ce message en paquets de 7 bits. 0 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 0 1 1 0 1

symbole1= 0 1 0 1 1 1 0 ► 46 en décimal.

La modélisation est la suivante: Quel est le modèle parmi les 128 correspondant à la valeur 46.



La modulation LoRa® - calcul des débits

- Coding Rate: ratio qui augmente le nombre de bits à transmettre afin de réaliser de la détection/correction d'erreur.

En LoRa® on utilise un coding rate CR=4/5 ► il y aura 5 bits de transmis réellement lorsqu'on transmet initialement 4 bits.

- Symbol Rate: R_s

$$R_s \text{ (symbols/sec)} = \text{BW} / 2^{\text{SF}} = R_c / 2^{\text{SF}}$$

- Data Rate: R_b

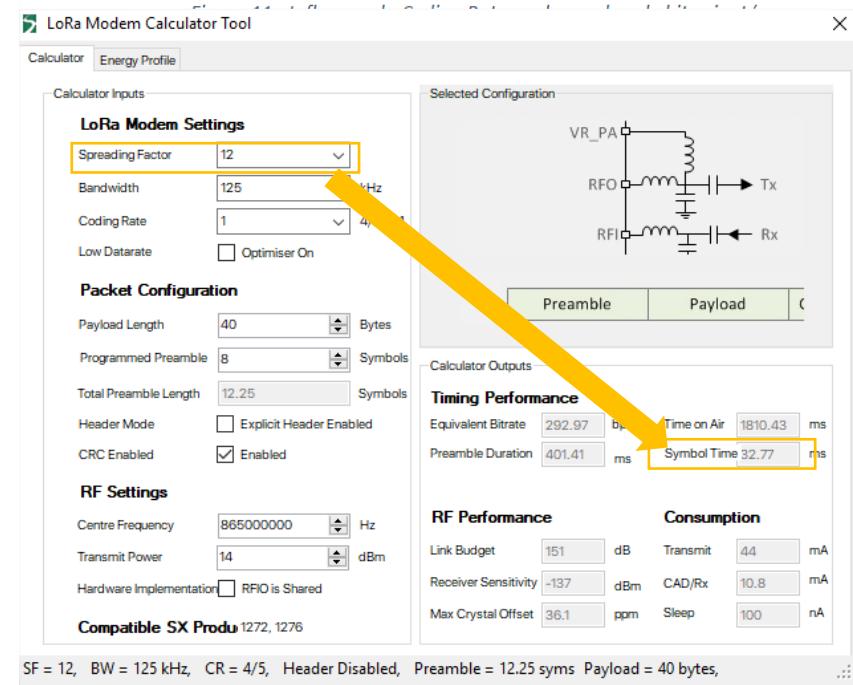
$$R_b \text{ (bits/sec)} = \text{SF} \times \frac{\text{BW}}{2^{\text{SF}}} \times \frac{4}{(4 + \text{CR})}$$

- Symbol Duration T_s

$$T_s \text{ (sec)} = 2^{\text{SF}} / \text{BW}$$

- Evaluation des résultats via l'outil Semtech: LoRa Calculator.
<https://bit.ly/2TyloAh>
- [https://www.loratools.nl/#/airtime \(Air time calculator\)](https://www.loratools.nl/#/airtime (Air time calculator))

CodingRate (RegModemConfig1)	Cyclic Coding Rate	Overhead Ratio
1	4/5	1.25
2	4/6	1.5
3	4/7	1.75
4	4/8	2



Exemple:

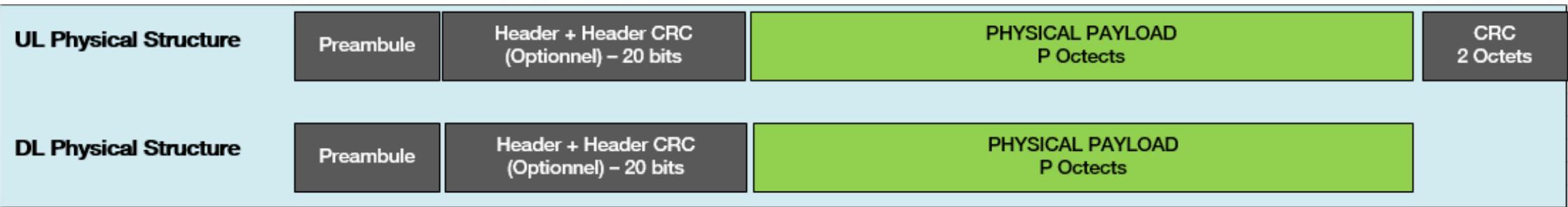
40 Octets transmis en SF12 dure 1.8s
 40 Octets transmis en SF7 dure 80ms.

La modulation LoRa® - conclusion

Data Rate	SF	Chips/ symbol	Symbol Rate Rs	Data Rate DR (Rb) Bits/s	Symbol Duration Ts en ms	LoRa demodulator SNR (SX1272/73)	Sensitivity (SX1272/73)
5	7	128	977	5469	1.024	-7.5 dB	-124 dBm
4	8	256	488	3125	2.048	-10 dB	-127 dBm
3	9	512	244	1758	4.096	-12.5 dB	-130 dBm
2	10	1024	122	977	8.192	-15 dB	-133 dBm
1	11	2048	61	537	16.384	-17.5dB	-135 dBm
0	12	4096	31	293	32.768	-20dB	-137 dBm

- Plus le Spreading Factor est élevé (SF12), utilisation en mauvaise condition radio (SNR=-20dB), plus le débit sera faible, et plus la portée de transmission sera longue
- Plus le Spreading Factor est faible (SF7), utilisation en très bonne condition radio (SNR=-7.5dB), plus le débit sera élevé, et plus le temps de transmission sera court.
- L'algorithme permettant d'adapter le débit en fonction des conditions radio du device s'appelle l'**ADR (Adaptive Data Rate)**.

La couche Physique LoRa® - Header



- Preamble: permet la synchronisation entre l'émetteur et le récepteur. Il est composé de 8 symboles, il indique quand commence la trame reçue.
- Header (Optionnel): contient les informations Coding Rate (CR), taille du message, et indique la présence ou non d'un contrôle CRC.
- Physical Payload: contient toutes les informations de la couche LoRaWAN.
- Le CRC sert à la détection d'erreur de la trame LoRa®.

Band 868MHz ISM

- LoRa est utilisée sur des bandes de fréquence ISM, dites libres, qui ne sont soumises à aucune licence.

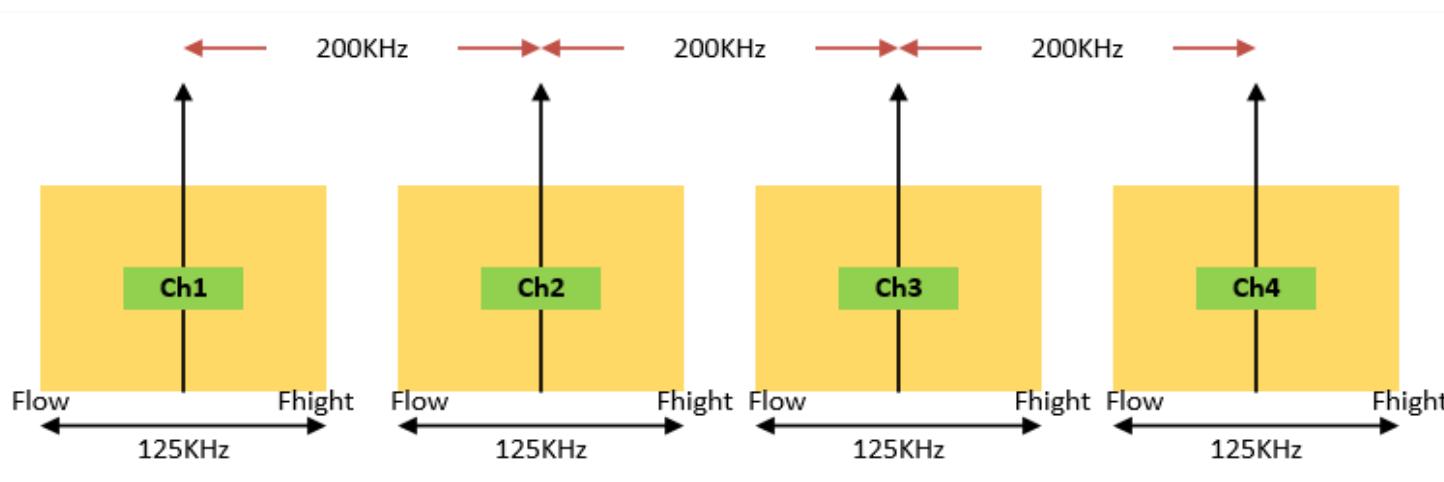
Exemples de bandes de fréquences ISM utilisées dans le monde sont les suivantes :

EU	863 – 870Mhz ISM Band
US	902 – 928Mhz ISM Band
China	779 – 787Mhz ISM Band
EU	433Mhz ISM Band

Un chipset Semtech fonctionne sur une seule bande de fréquence.
Exemple: un objet LoRa® fonctionnant en France ne fonctionnera pas au US.

- L'ETSI (Spec [ETSI EN 300 220-1 V2.4.1 \(2012-05\)](#) 7.10.1) a spécifié un paramètre appelé « **duty cycle** » qui définit la portion de temps pendant laquelle un dispositif peut émettre sur une fréquence donnée.

En LoRa® il est calculé sur une heure glissante et exprime un pourcentage qui varie suivant la bande utilisée (**0.1%, 1%, 10%**).

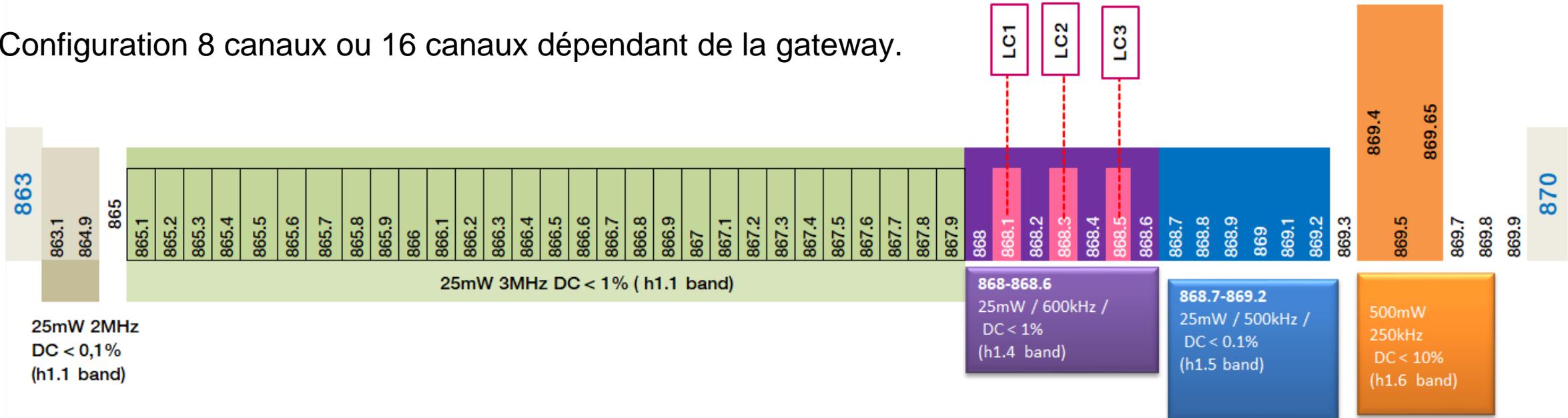


Largeur de bande d'un canal: 125KHz
Recommandation: espace entre 2 canaux: 200KHz

Band ISM 868MHz

Répartition des canaux de fréquences LoRa® sur la bande ISM 868MHz.

Configuration 8 canaux ou 16 canaux dépendant de la gateway.



Les canaux LC1 (868.1MHz), LC2 (868.3MHz), LC3 (868.5MHz) sont les canaux configurés par défaut sur tous les équipements LoRa®, représentant **les canaux obligatoires**.

Un device LoRa® établit une session avec le réseau pour la 1^{ère} fois via l'un de ces 3 canaux.

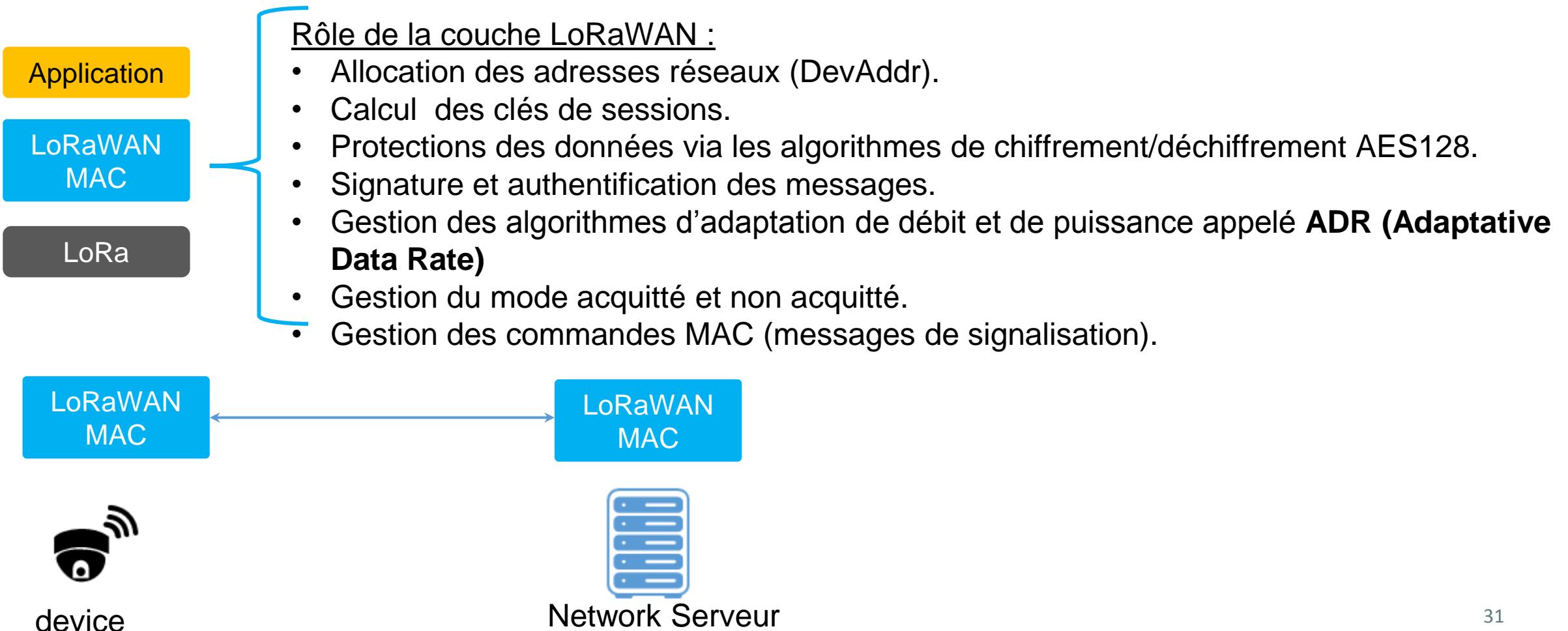
Ensuite il va utiliser un canal choisi aléatoirement et changer de canal à chaque transmission de données.

Le plan de fréquence (8 ou 16 canaux) choisi par l'opérateur, configuré dans le cœur de réseau (NS) est transmis au device soit lors de la procédure JOIN (OTAA), soit dans des commandes MAC dédiées définies dans les normes.

On note que sur la bande 865.1 à 867.9 le duty Cycle est de 1%, ce qui veut dire que pendant la dernière heure (soit 3600 secondes), un dispositif ne doit jamais avoir émis pendant plus de 36 secondes au total.

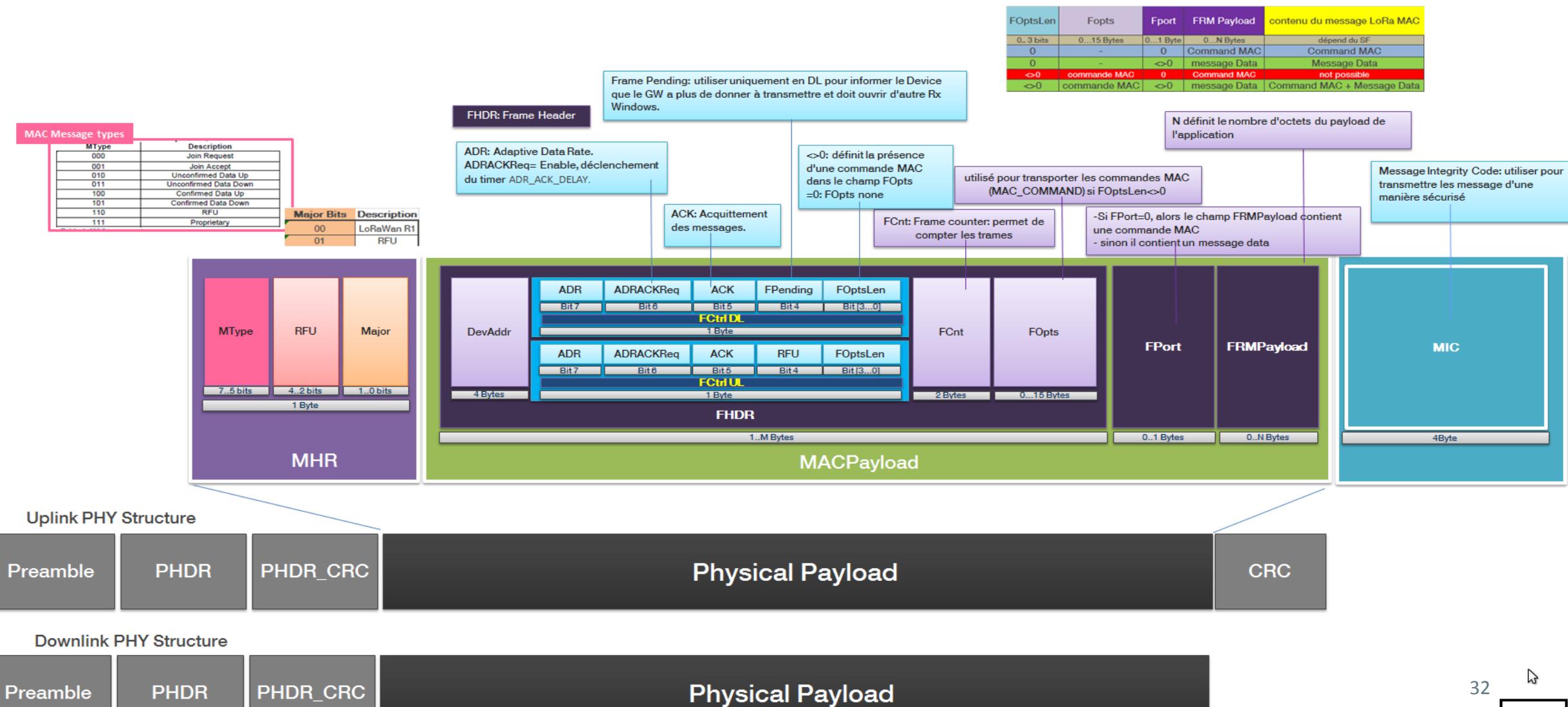
Couche LoRaWAN™

- La couche LoRaWAN est une couche d'adaptation open source, spécifiée par la LoRa Alliance.
La spécification 1.0 explique le fonctionnement de la couche LoRaWAN.
La spécification 1.1 finalisée en 2018 apporte les évolutions liées au roaming (passive & handover).
La couche LoRaWAN est gérée au niveau du network serveur.



Couche LoRaWAN™ - protocoles

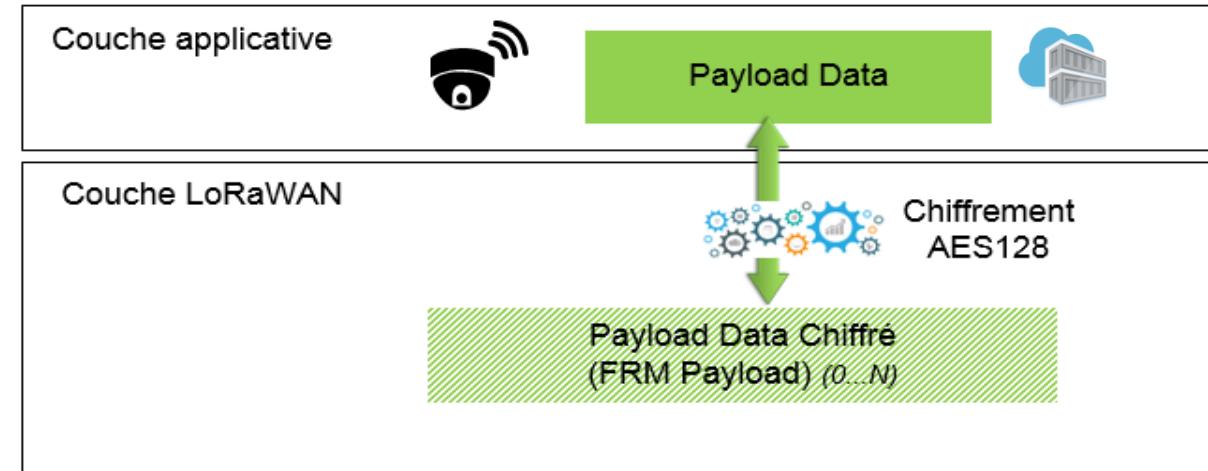
Elle contient les informations de signature, d'authentification (MIC), relatives à l'ADR, sur le type de message (signalisation, data ou signalisation + data), si le message doit être acquitté, ou encore le numéro de trame (FCnt)...



La couche applicative

La couche Applicative est définie par le champ « Frame Payload Data » dont la taille N dépend du spreading factor SF

Data Rate	Spreading Factor	Bandwidth	Max Frame Payload (Nombre N)
DR 0	SF12	125 KHz	51 octets
DR 1	SF11	125 KHz	51 octets
DR 2	SF10	125 KHz	51 octets
DR 3	SF9	125 KHz	115 octets
DR 4	SF8	125 KHz	222 octets
DR 5	SF7	125 KHz	222 octets

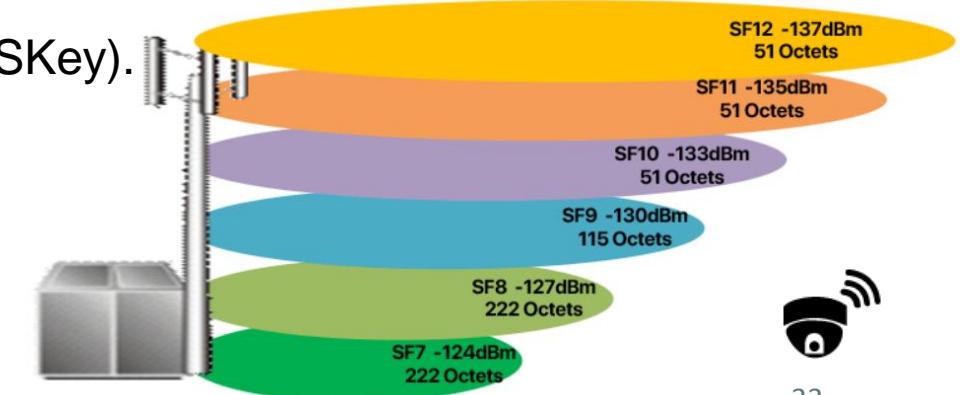


Si l'on se place en bordure de cellule, on utilise le spreading factor 12 qui délimite la taille maximale de la « payload data » à 51 octets (valeur N).

Cette valeur de 51 octets représente la valeur max d'une payload data à utiliser sur un réseau LoRa®.

La payload data est chiffrée avec une clé de session applicative (AppSKey).

L'algorithme permettant de changer de Spreading Factor s'appelle l'ADR (Adaptive Data Rate).



Clés et identifiants LoRaWAN™

LoRaWAN 1.0

■ **DevEUI**: Device ID – Identification du device. Format normalisé IEEE EU64 unique (\Leftrightarrow adresse MAC). Exemple: 0018B200000000216

■ **AppEUI**: Application ID – Identifiant de l'application. Identifie l'application utilisée par le device et est spécifiée par le constructeur. Exemple: 0018B24441524631

Note : Les compteurs d'eau appartenant à un même modèle auront le même identifiant AppEUI.

■ **AppKey**: clé racine applicative, clé AES 128 unique. Clé racine unique utilisée pour calculer les clés de session réseau et applicative dans le mode de provisioning OTAA. Clé non visible du réseau. Exemple: 0018B244415246310018B20000000216.

■ **AppSKey**: Application Session Key.

Clé de session applicative utilisé pour le chiffrement des données (AES 128). Calculée durant la procédure JOIN en OTAA et définie manuellement en ABP.

■ **NwkSKey**: Network Session Key.

Clé de session réseau utilisée pour l'authentification des messages (AES 128). Calculée durant la procédure JOIN en OTAA et définie manuellement en ABP.

`NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16)`

`AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16)`

■ **DevAddr**: Device Address.

Adresse du device allouée par le network serveur (mode OTAA) (\Leftrightarrow adresse IP)

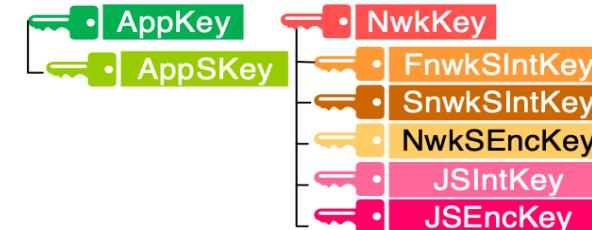
NwKID: Network ID: identifiant du réseau LoRa® alloué par la LoRaAlliance.

NwkAddr: Network Address: adresse allouée par le réseau au device sur le NetID.

LoRaWAN 1.1

D'autres identifiants ont été ajoutés pour les use case roaming et les devices en version 1.1.

- **JoinEUI** : remplace l'**AppEUI**. Permet d'identifier le Join Serveur
- **NwkKey**: Network Key (clé racine réseau)
- **FNwkSIntKey**: Forwarding Network Session Integrity Key : clé d'intégrité de session du fNS (forwarding Network Server).
- **SNwkSIntKey**: Serving Network Session Integrity Key : clé d'intégrité de session du sNS (Serving Network Server).
- **NwkSEncKey**: Network Session Encryption Key (clé de chiffrement de session réseau LW1.1)
- **JSEncKey**: Clé de chiffrement du Join Serveur.
- **JSIntKey**: Clé d'intégrité du Join Serveur.



AppSKey à partir d'AppKey

`AppSKey = aes128_encrypt(AppKey, 0x02 | JoinNonce | JoinEUI | DevNonce | pad16)`

FNwkSIntKey, SNwkSIntKey, NwkSEncKey à partir de NwkKey.

`FNwkSIntKey = aes128_encrypt(NwkKey, 0x01 | JoinNonce | JoinEUI | DevNonce | pad16)`

`SNwkSIntKey = aes128_encrypt(NwkKey, 0x03 | JoinNonce | JoinEUI | DevNonce | pad16)`

`NwkSEncKey = aes128_encrypt(NwkKey, 0x04 | JoinNonce | JoinEUI | DevNonce | pad16)`

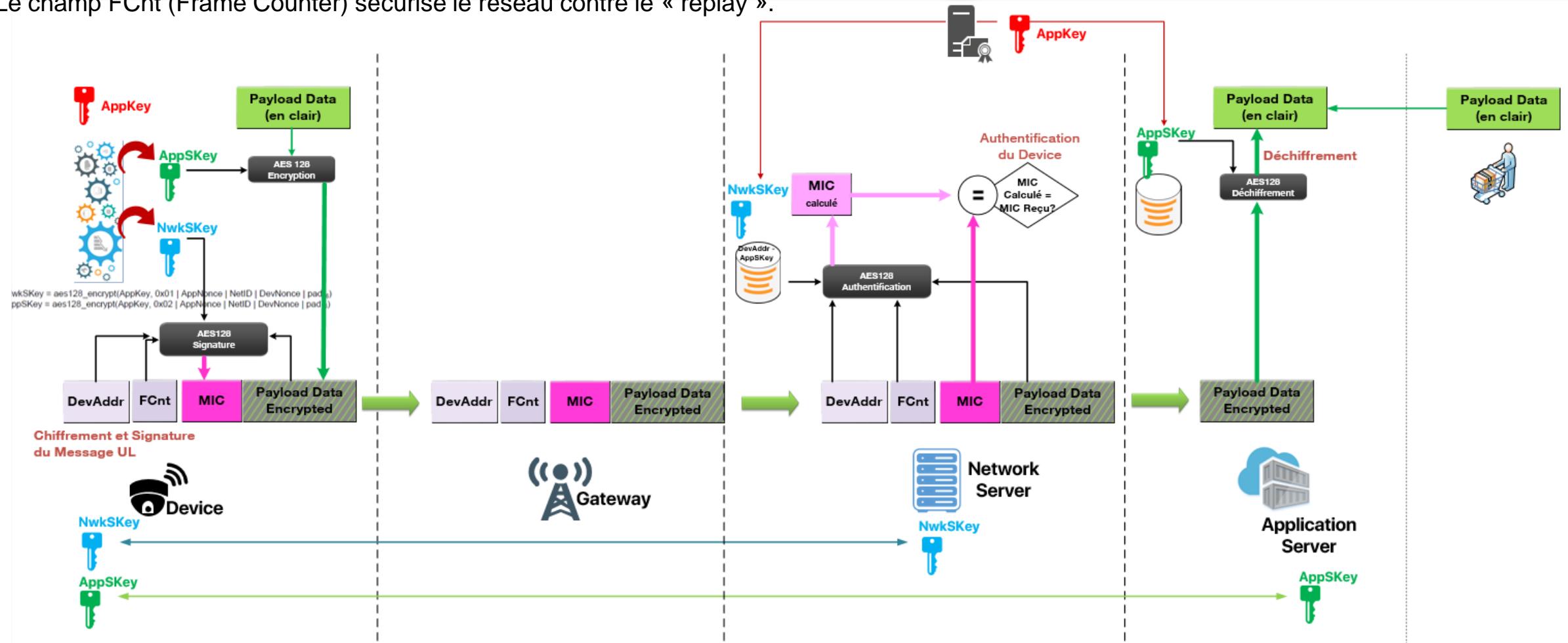
`JSIntKey = aes128_encrypt(NwkKey, 0x06 | DevEUI | pad16)`

`JSEncKey = aes128_encrypt(NwkKey, 0x05 | DevEUI | pad16)`

Authentification & Chiffrement

La clé **AppSKey** (clé de session applicative) localisée dans le device permet de chiffrer la donnée applicative, et de la déchiffrer dans l'application server.

La clé **NwkSKey** (clé de session réseau) localisée dans le device permet de signer le message et de l'authentifier dans le network serveur.
Le champ FCnt (Frame Counter) sécurise le réseau contre le « replay ».



Modes d'activation des devices LoRa® - Mode ABP

Activation By Personalisation

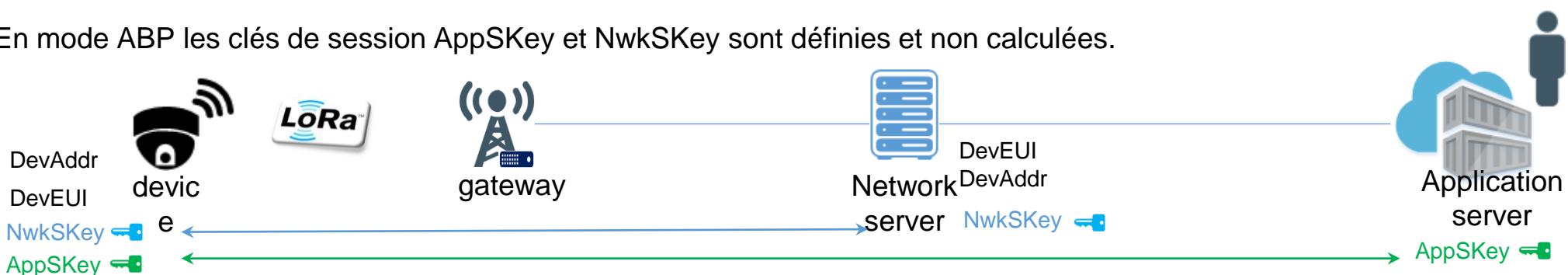
Méthode simple utilisée lors des tests de développement de prototype, très peu utilisée car peu sécurisée.

Fournis la clé de session réseau **NwkSKey** et l'adresse du device **DevAddr** au client pour chacun des devices DevEUI.

Demande la production du device (DevEUI) avec les informations **DevAddr**, **NwkSKey**, **AppSKey**



En mode ABP les clés de session AppSKey et NwkSKey sont définies et non calculées.

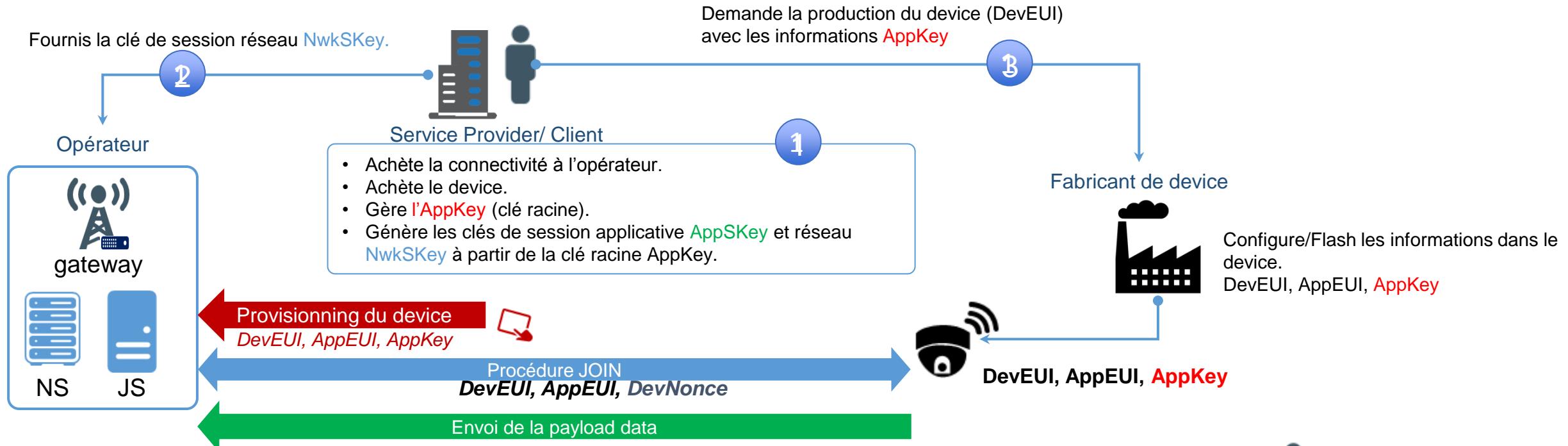


Mode d'activation des devices LoRa® - Mode OTAA

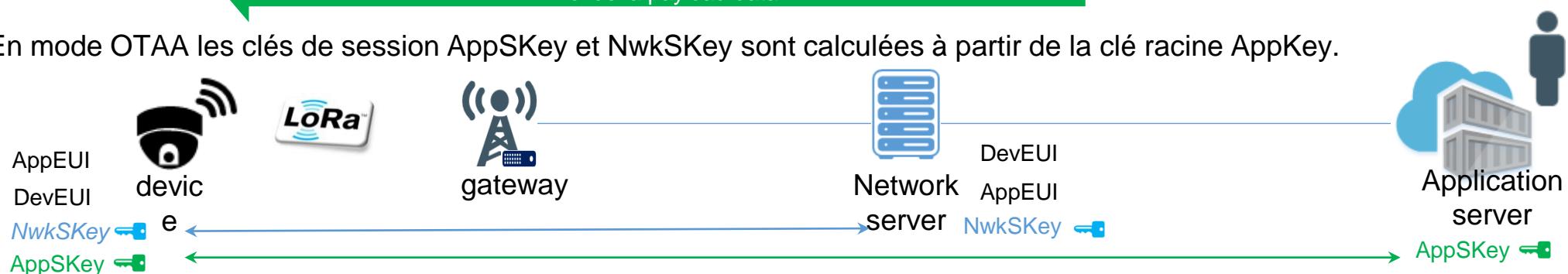
Over the Air Activation

Méthode sécurisée à privilégier, majoritairement utilisée

Authentification à chaque nouvelle session, clés de sessions dynamiquement calculées avec un Join Server



En mode OTAA les clés de session AppSKey et NwkSKey sont calculées à partir de la clé racine AppKey.



Mode OTAA – Calcul des clés de session



AppKey: clé racine AES 128.

Extrémité A: La clé AppKey est « flashée » dans le device.

Extrémité B: La LoRa Alliance ne spécifie rien à ce sujet.

- Soit provisionnée dans le network serveur de manière chiffrée dans un espace sécurisé.
- Soit provisionnée dans une entité tiers de type HSM (High Security Module) ou autre.

A partir de la clé racine AppKey, deux clés de sessions sont calculées au niveau du device et au niveau network serveur ou d'une entité tiers.

→ **AppSKey:** Application Session Key – AES 128.

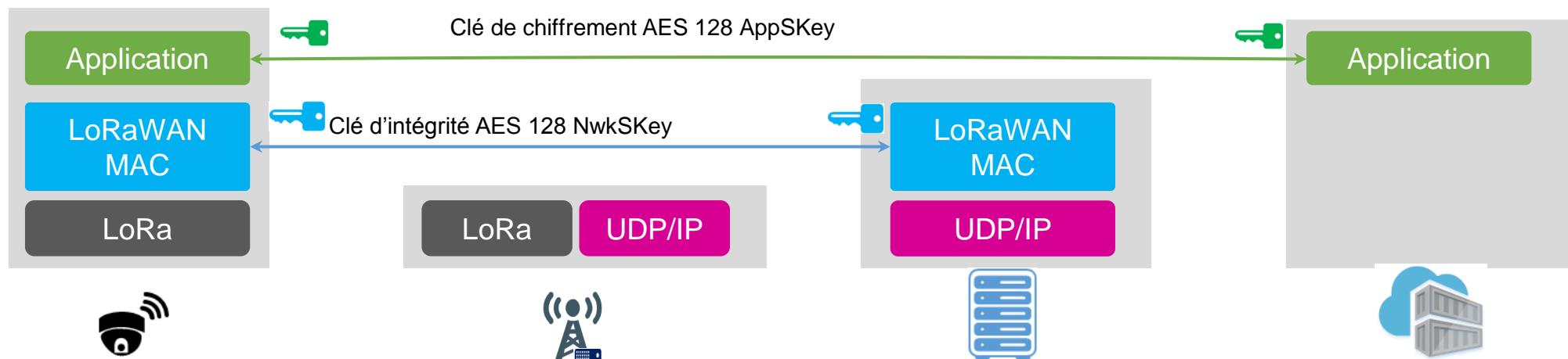
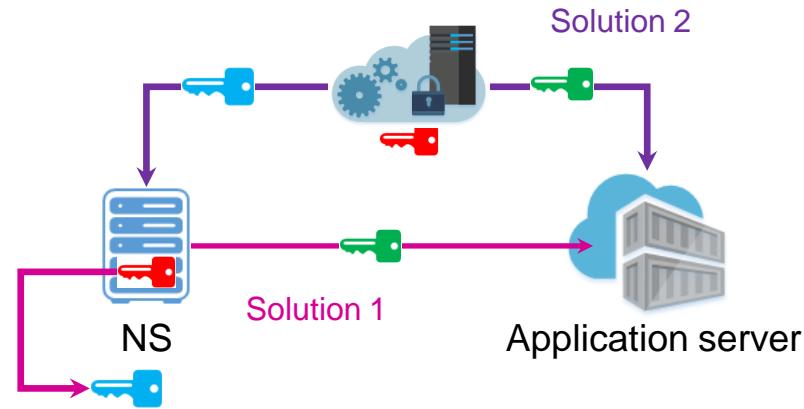
Clé de session applicative utilisée pour le chiffrement des données (AES 128).

$$\text{AppSKey} = \text{aes128_encrypt}(\text{AppKey}, 0x02 \mid \text{AppNonce} \mid \text{NetID} \mid \text{DevNonce} \mid \text{pad}_{16})$$

→ **NwKskey:** Network Session Key – AES 128.

Clé de session réseau utilisée pour l'authentification des données (AES 128)

$$\text{NwkSKey} = \text{aes128_encrypt}(\text{AppKey}, 0x01 \mid \text{AppNonce} \mid \text{NetID} \mid \text{DevNonce} \mid \text{pad16})$$



Types de message (et non MType !)

3 types de messages échangés entre les éléments d'un réseau LoRa®:

- Message data : message applicatif échangé entre le device et le serveur applicatif dans le sens montant et descendant.
- Message MAC : message contenant une ou plusieurs commandes MAC échangé entre le device et le network serveur dans le sens montant et descendant.
- Message MAC + data : message contenant une ou plusieurs commandes MAC ainsi qu'un message applicatif

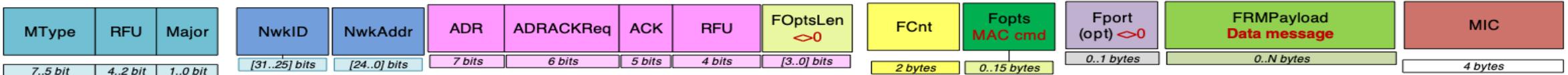
Commande MAC



Message Data



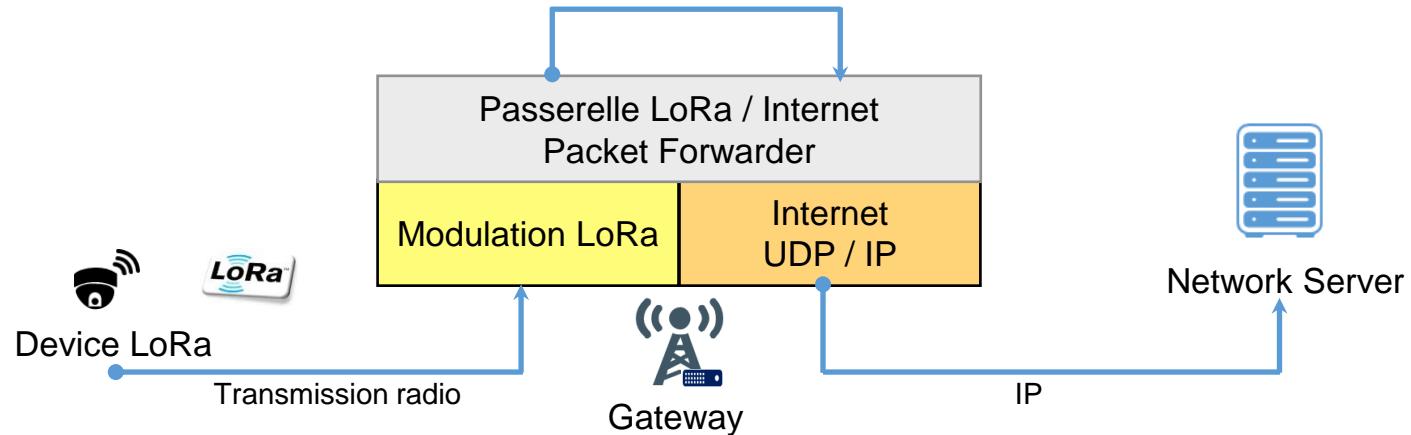
Commande MAC + Message Data



DR	Configuration	indicative physical bit rate(bits/s)	N
0	SF12 / 125Khz	250	51
1	SF11 / 125Khz	440	51
2	SF10 / 125Khz	980	51
3	SF9 / 125Khz	1760	115
4	SF8 / 125Khz	3125	222
5	SF7 / 125Khz	5470	222
6	SF6 / 125Khz	11000	222

La longueur du champ FRMPayload est fonction du Spreading Factor

Message Data



La Gateway a un rôle de passerelle entre le protocole LoRa d'un côté et un réseau IP de l'autre.

Coté interface Radio :

- La Gateway réceptionne la trame LoRaWAN et extrait le PHYSICAL Payload.
- La Gateway extrait aussi toutes les informations utiles sur les caractéristiques de la réception SF, RSSI, SNR...

Coté interface réseau IP :

La Gateway transmet l'ensemble des informations dans paquet IP (UDP) au Network Server.
Les données transmises sont du texte en format JSON.

Exemple de fichier JSON

```
, "encoding": "Adeunis-LoRaWanDemonstrator",  
"connector": "lora",  
"network": {  
    "lora": {  
        "devEUI": "0018B20000004F5",  
        "port": 1,  
        "fcnt": 121230,  
        "rssi": -115,  
        "snr": -13,  
        "esp": -128.21,  
        "sf": 12,  
        "signalLevel": 2,  
        "ack": false,  
        "messageType": "UNCONFIRMED_DATA_UP",  
        "location": {},  
        "gatewayCnt": 2,  
        "bestGatewayId": "FF010972",  
        "gateways": [  
            {  
                "id": "FF010972",  
                "rssi": -115,  
                "snr": -13,  
                "esp": -128.21  
            },  
            {  
                "id": "FF010B70",  
                "rssi": -116,  
                "snr": -17,  
                "esp": -133.09  
            }  
        ]  
    }  
}
```

Les commandes MAC LW 1.0

Les commandes MAC permettent au réseau cœur et au device de communiquer via la couche MAC LoRa.

Généralement émises par le réseau, elles peuvent aussi l'être par le device, exceptée la commande LinkCheckReq (équivalent à un ping émis par le device pour s'assurer que le réseau répond toujours).

Les autres commandes MAC permettent pour la plupart de modifier le paramétrage radio du device pour que ce dernier s'adapte à son environnement.

CID	Command	Direction
0x02	LinkCheckReq	UL
0x02	LinkCheckAns	DL
0x03	LinkADRReq	DL
0x03	LinkADRAbs	UL
0x04	DutyCycleReq	DL
0x04	DutyCycleAns	UL
0x05	RXParamSetupReq	DL
0x05	RXParamSetupRAns	UL
0x06	DevStatusReq	DL
0x06	DevStatusAns	UL
0x07	NewChannelReq	DL
0x07	NewChannelAns	UL
0x08	RXTimingSetupReq	DL
0x08	RXTimingSetupAns	UL

MType

- Tout message LoRa est défini par un MType
- Mtype : champ défini sur 3 bits

MType	Correspondance	Direction	Norme LoRaWAN
000 (0)	Join Request	UL	LW1.0
001 (1)	Join Accept	DL	LW1.0
010 (2)	Unconfirmed Data UL	UL	LW1.0
011 (3)	Unconfirmed Data DL	DL	LW1.0
100 (4)	Confirmed Data UL	UL	LW1.0
101 (5)	Confirmed Data DL	DL	LW1.0
110 (6)	Rejoin Request	UL	LW1.1
111 (7)	Propriétaire	-	LW1.0

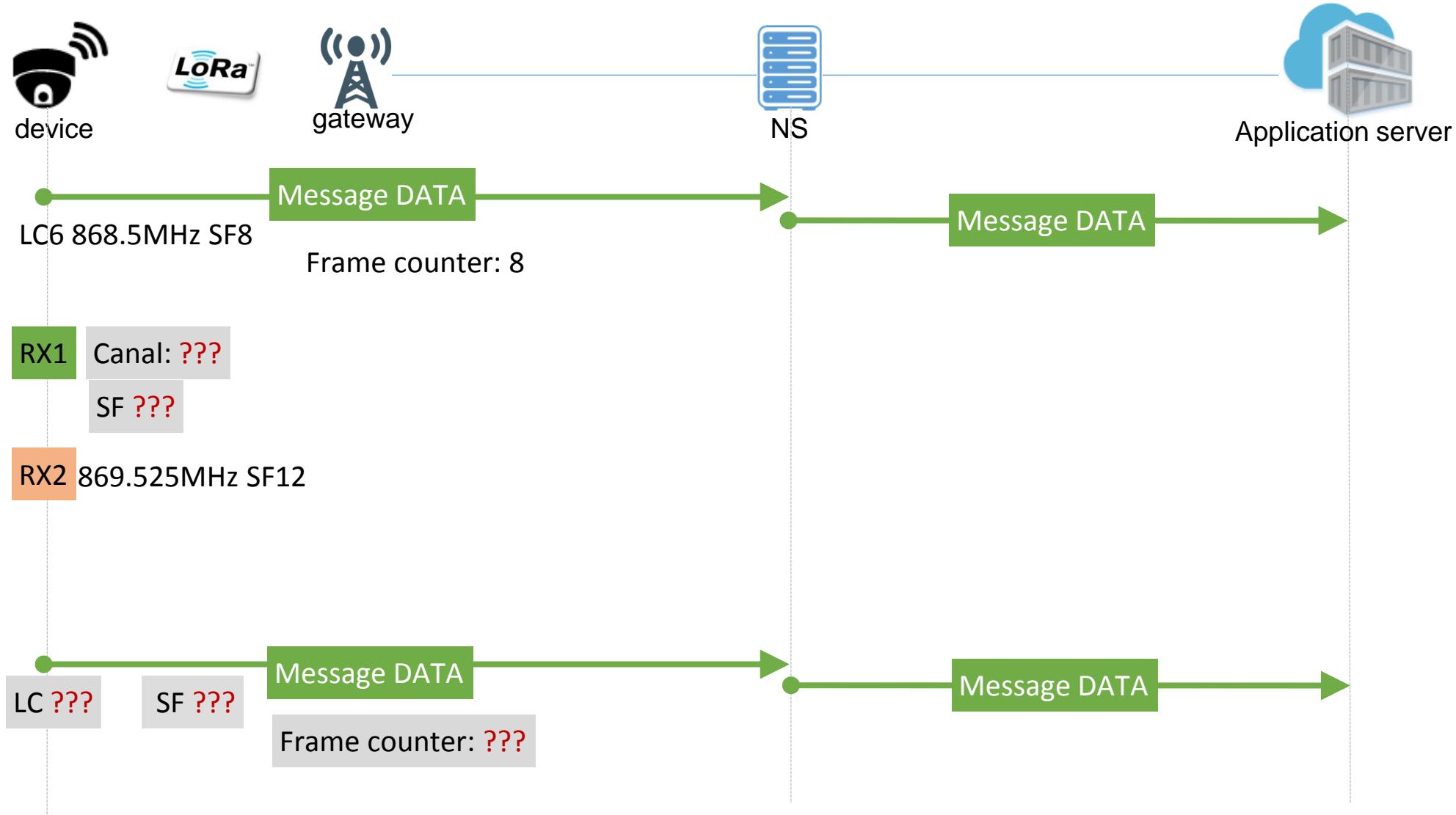


04

Call Flow de base

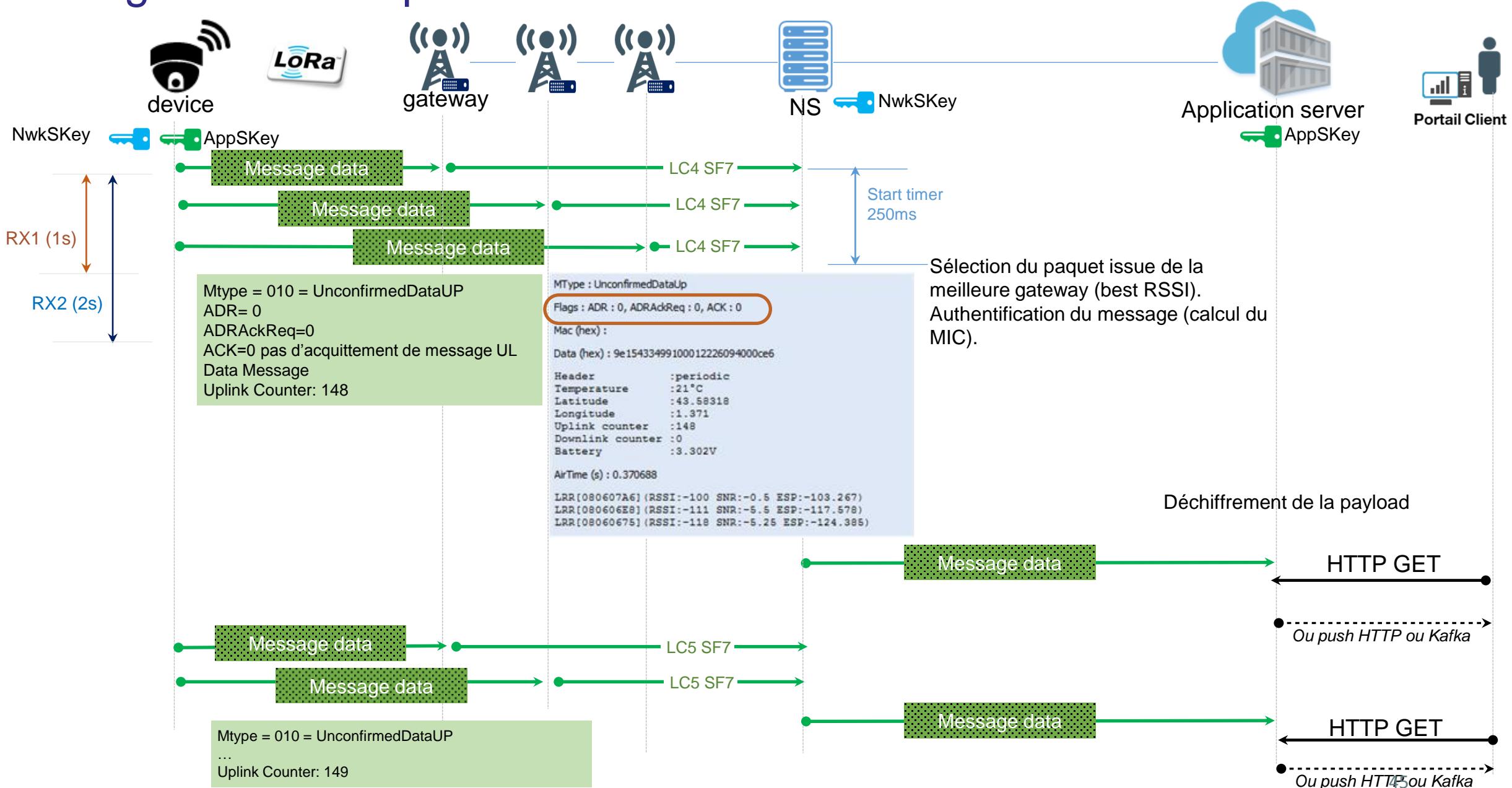
- Trame Class A
- Procédure JOIN
- Transmission d'un message data UL
- Procédure de changement de Spreading Factor
- Message nécessitant un acquittement

Trafic UL de base – classe A

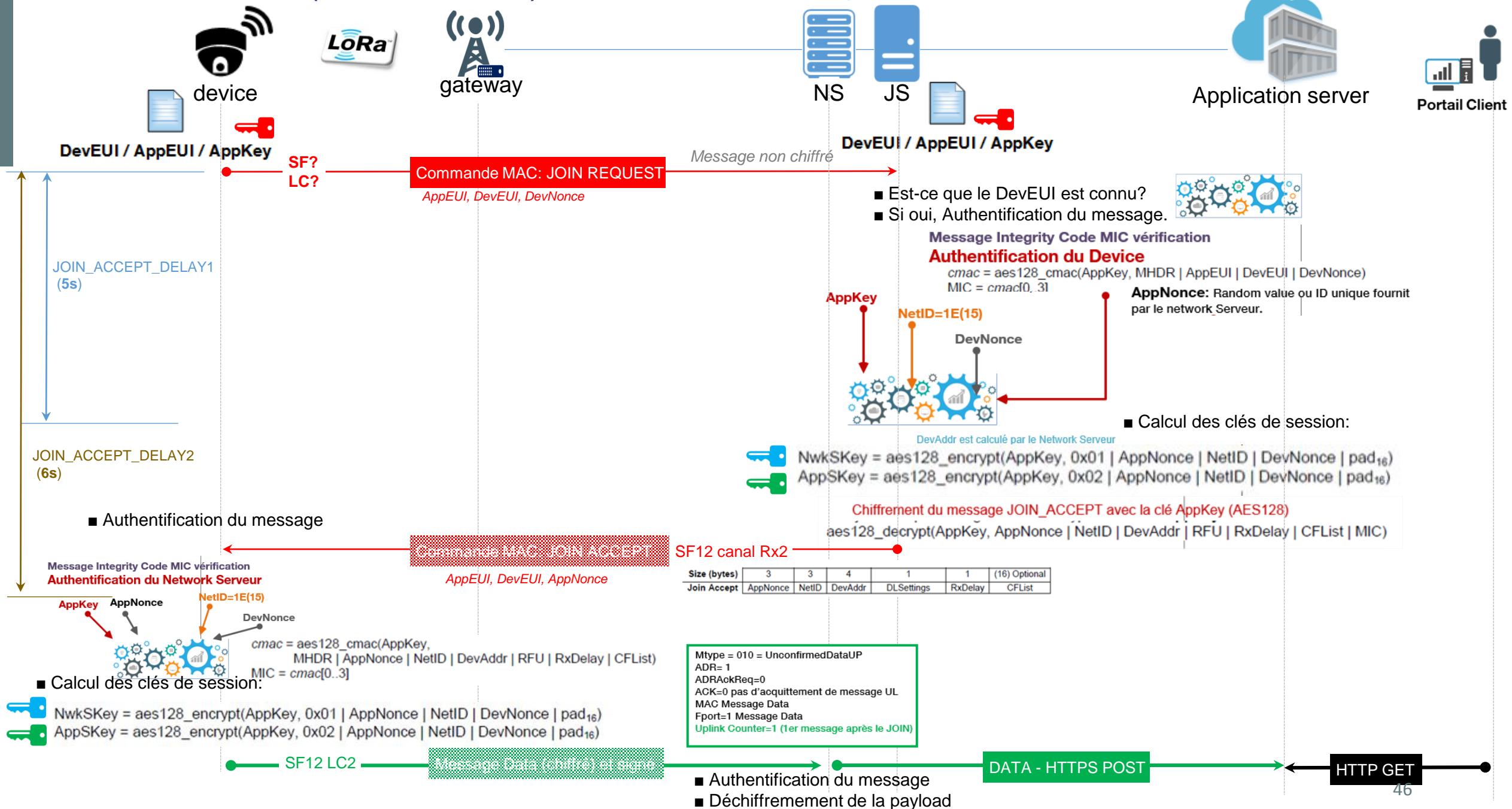


Quel Mtype ?

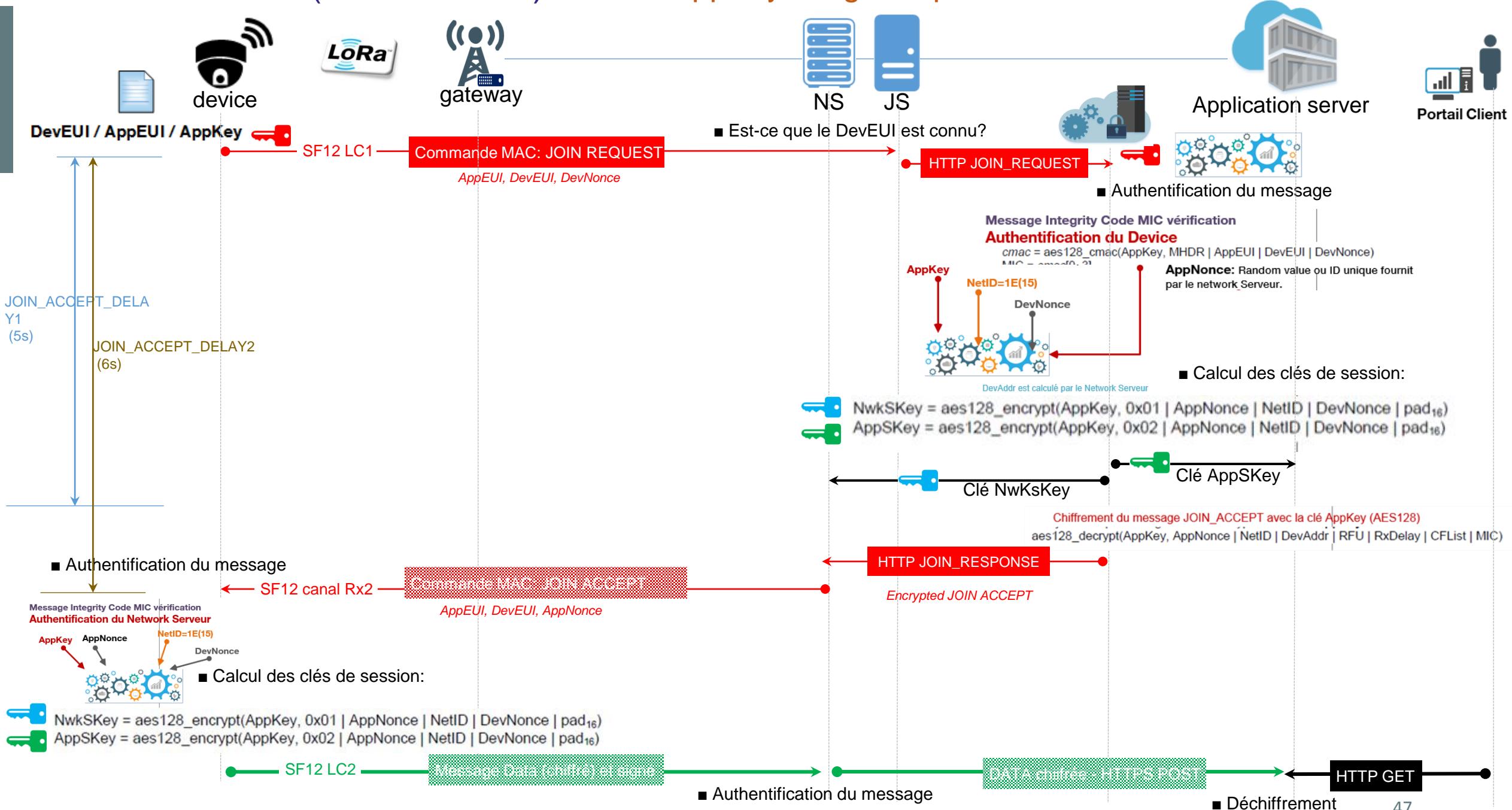
Message data UL – plusieurs GWs



Procédure JOIN (mode OTAA) – la clé AppKey est gérée dans le Network Serveur

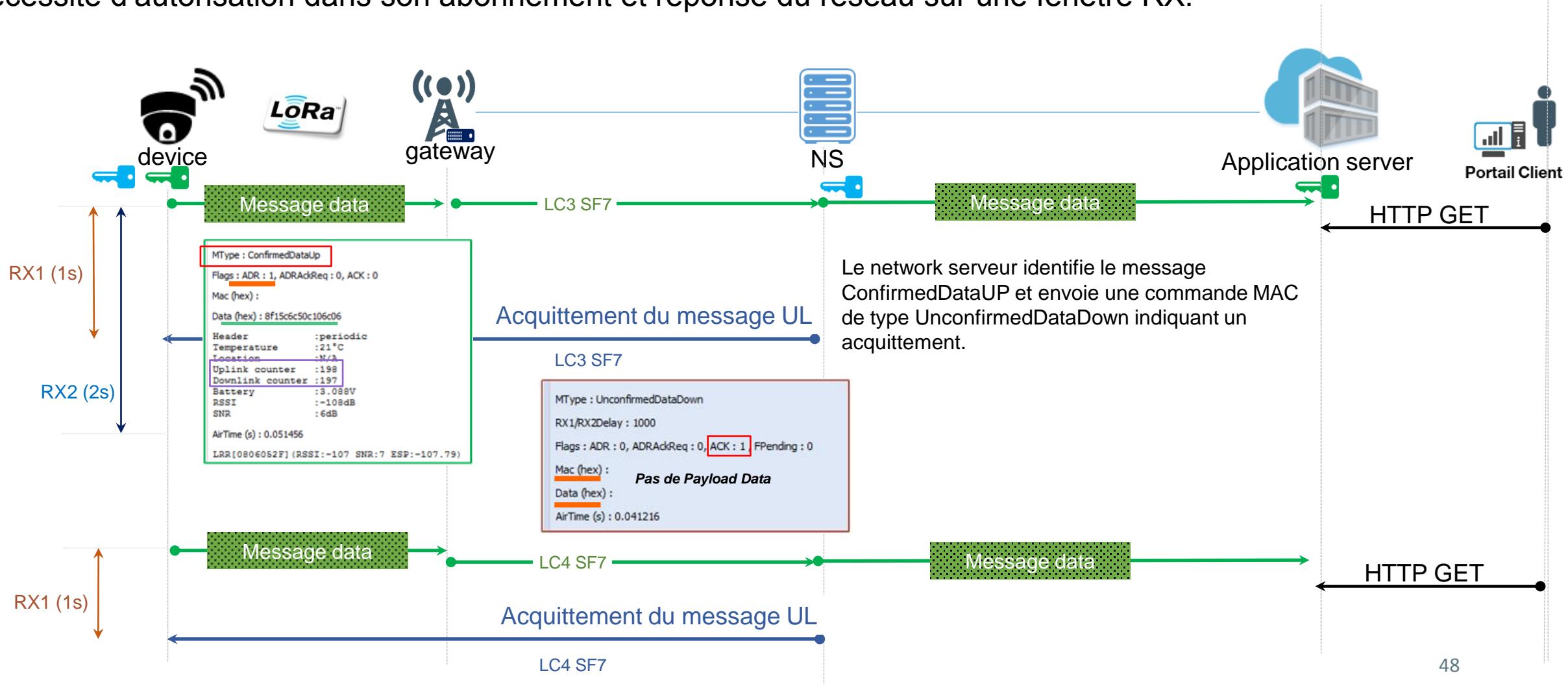


Procédure JOIN (mode OTAA) – la clé AppKey est gérée par une entité tierce.



Message data UL - Acquittement des messages UL

L'envoi des messages data UL demandant un acquittement est un choix client et est implémenté au sein du device. Le device enverra un message de **MType « ConfirmedDataUP »**. Il y a demande implicite d'acquittement : nécessité d'autorisation dans son abonnement et réponse du réseau sur une fenêtre RX.



Algorithme ADR (Adaptive Data Rate)

L'algorithme ADR (Adaptive Data Rate) permet d'adapter le débit (changement de Spreading Factor) ainsi que la puissance en fonction des conditions radio.

Cet algorithme est géré par la couche LoRaWAN™ et le fonctionnement est dépendant du network serveur.

L'adaptation de puissance a lieu en SF7.

L'ADR est géré via les commandes MAC *LinkADRReq*, *LinkADRAns*.

Le Network Serveur à partir d'un certain nombre de mesure en entrée dont le SNR va identifier le Spreading Factor à utiliser.

L'utilisation de l'ADR est un choix client, le device via le message UL envoyé spécifie s'il utilise ou non l'ADR.

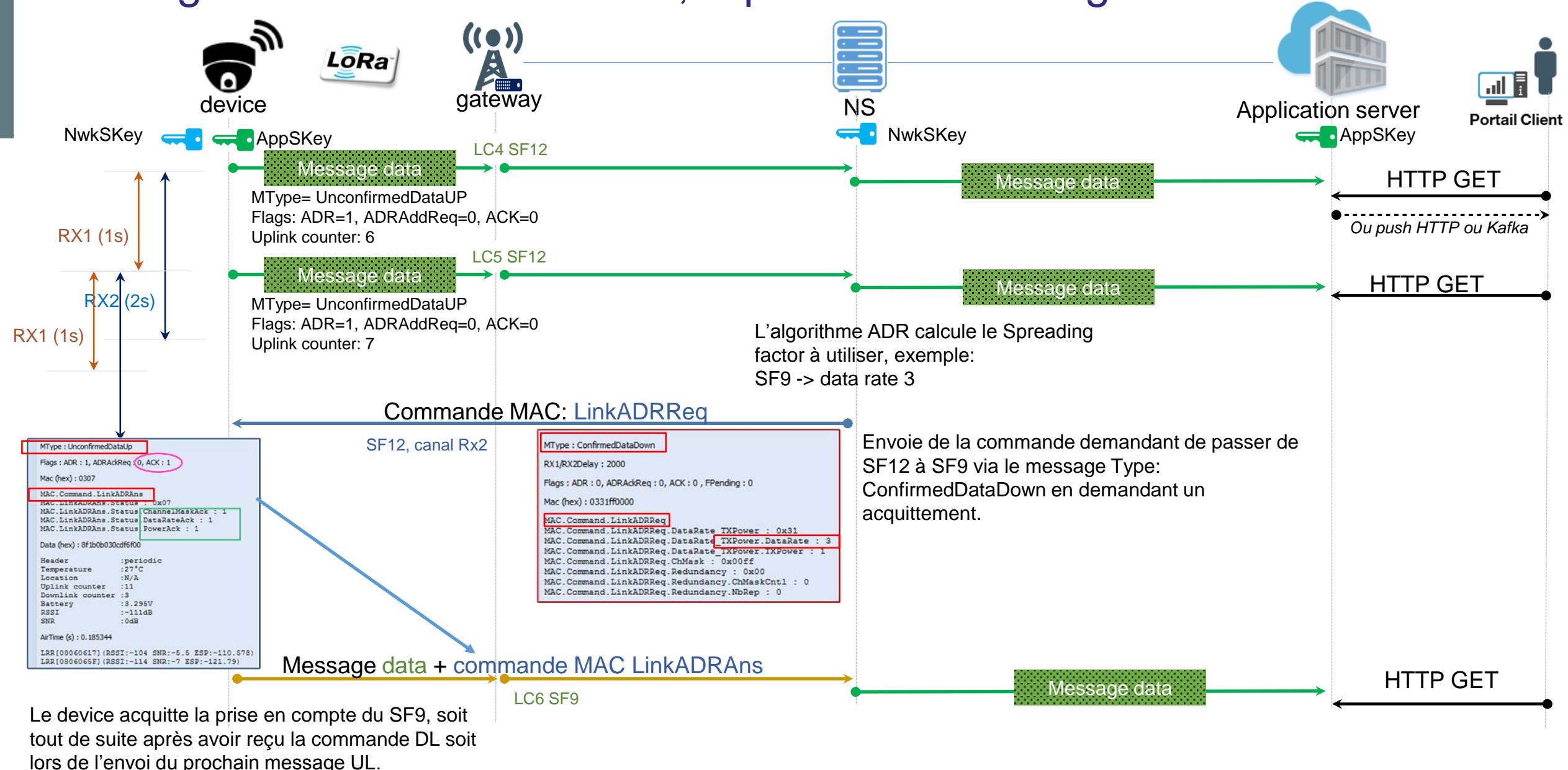
L'ADR est utile pour les devices dit « statique » et potentiellement problématique pour les devices en mobilité.

DataRate	Configuration	Indicative physical bit rate [bit/s]	TXPower	Configuration
0	LoRa: SF12 / 125 kHz	250	0	20 dBm (if supported)
1	LoRa: SF11 / 125 kHz	440	1	14 dBm
2	LoRa: SF10 / 125 kHz	980	2	11 dBm
3	LoRa: SF9 / 125 kHz	1760	3	8 dBm
4	LoRa: SF8 / 125 kHz	3125	4	5 dBm
5	LoRa: SF7 / 125 kHz	5470	5	2 dBm
6	LoRa: SF7 / 250 kHz	11000	6..15	RFU
7	FSK: 50 kbps	50000		
8..15	RFU			

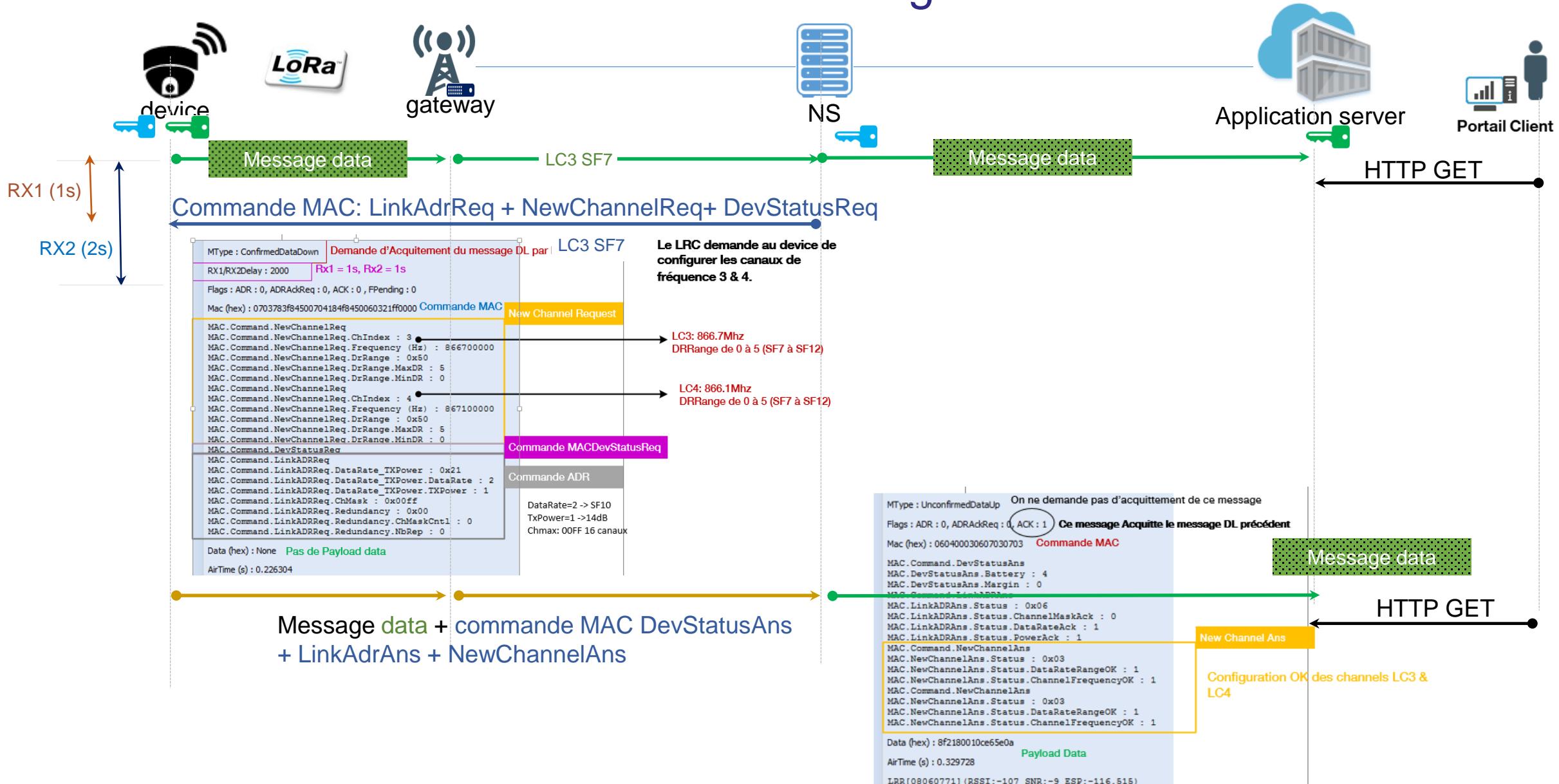
Table 14: Data rate and TX power table

Data Rate	SF	Chips/ symbol	Symbol Rate Rs	Data Rate DR (Rb) Bits/s	Symbol Duration Ts en ms	LoRa demodulator SNR (SX1272/73)	Sensitivity (SX1272/73)
5	7	128	977	5469	1.024	-7.5 dB	-124 dBm
4	8	256	488	3125	2.048	-10 dB	-127 dBm
3	9	512	244	1758	4.096	-12.5 dB	-130 dBm
2	10	1024	122	977	8.192	-15 dB	-133 dBm
1	11	2048	61	537	16.384	-17.5dB	-135 dBm
0	12	4096	31	293	32.768	-20dB	-137 dBm

Message data UL - ADR activé, réponse au message DL



Plusieurs commandes MAC dans un message





05

Fonctionnalités avancées LoRaWAN™

- Géolocalisation
- Roaming
- Call Flow LoRaWAN™ 1.1
- HSM / SSM

Géolocalisation

L'une des promesses de la technologie LoRa® est de géolocaliser des objets avec une précision de l'ordre de 100m sans implémenter de GPS sur ces devices d'où un gain fort en terme de consommation de batterie.

Il existe deux types de géolocalisation en LoRa® : la macrogéolocalisation et la TDoA (Time Difference of Arrival).

Macrogéolocalisation

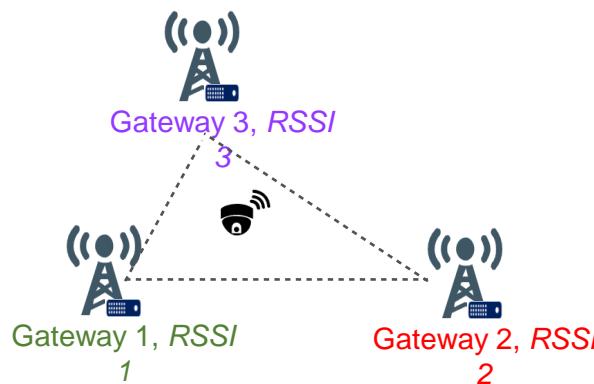
Pour obtenir une macrogéolocalisation d'un device LoRa® il faut :

- La réception d'une trame UL par **au moins une gateway** (avec horodatage)
- Obtenir la position de la (ou des) gateway(s) réceptrice(s) (de manière statique/manuelle ou dynamique avec un GPS)
- Avoir l'option activée dans le plan de connectivité du device
- Avoir une entité solveur de localisation pour en déduire une position estimée du device

Ainsi, le solveur de localisation va estimer la position du device en se basant sur ses mesures radio : RSSI, SNR, Spreading Factor.

- Si le device est reçu par une seule gateway, l'estimation sera la position de la GW elle-même.
- Si le device est reçu par deux gateways ou plus, le solveur calculera un barycentre pondéré (en tenant compte des niveaux RSSI) pour estimer la position du device.

L'ordre de précision (~1 km) n'est toutefois pas idéal, même s'il peut suffire pour certains types d'usage / besoins clients.



Notes :

- **le solveur de localisation est relié dans l'architecture au LRC de l'opérateur. Il est indépendant du LRC**, ce qui signifie que l'opérateur n'est pas contraint d'utiliser le solveur de son fournisseur LRC.
- **Les positions des gateways** (statiques ou dynamiques) **sont stockées dans le LRC dans des tables spécifiques appelées tables L**

Géolocalisation

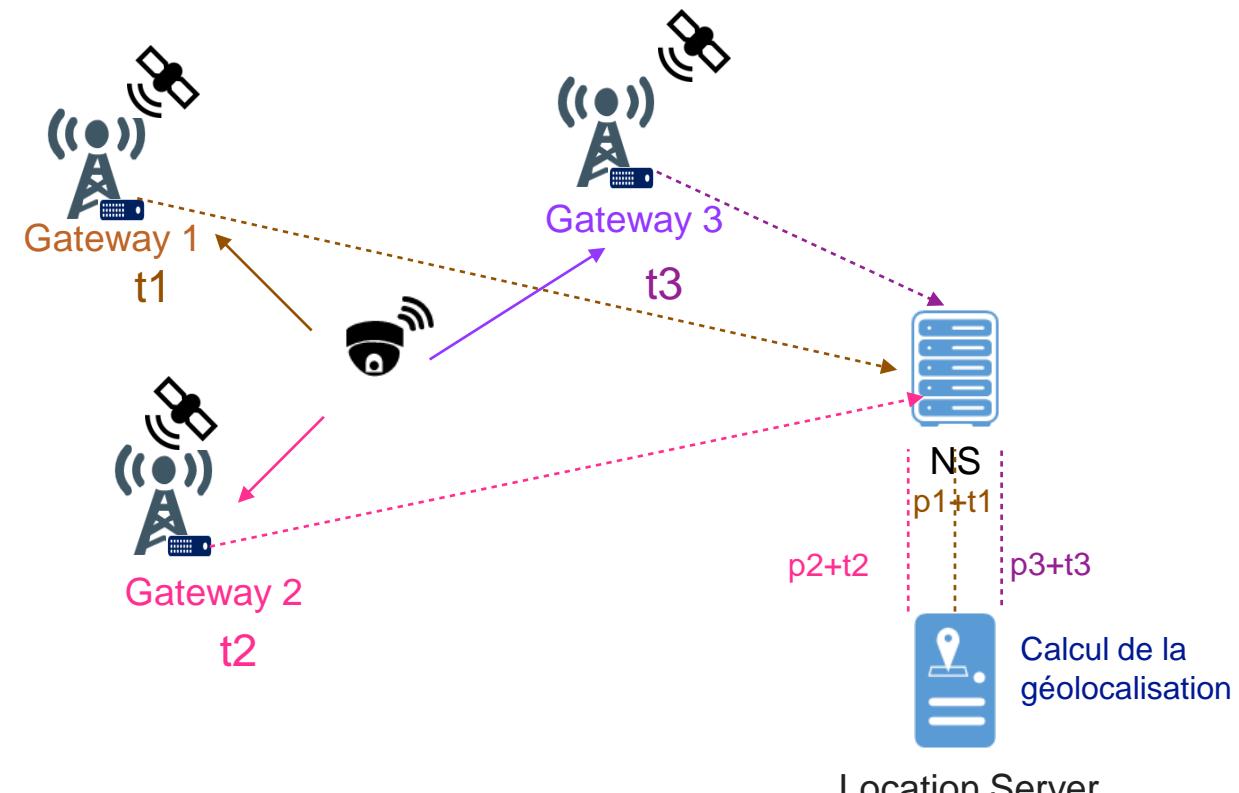
TDoA (Time Difference of Arrival) :

Meilleure précision : ~100m

Peut répondre à des use cases type géofencing

Pour pouvoir faire de la géolocalisation par TDoA, les critères à respecter sont plus contraignants qu'en macrogéolocalisation :

- La réception d'une trame UL par **au moins TROIS (voire quatre) gateways** (**minimum macrodiversité = 3 ou 4**)
- **Gateways capables de faire un horodatage fin (Finetimestamping, précision à 10^{-9} s)** de la trame UL reçue
- Gateways qui embarquent des **clés de géolocalisation (licences Semtech obligatoires) et un GPS**
- Connaître la position des gateways réceptrices avec un GPS
- **Paramétrage GDOP** (Geometric Dilution Of Precision) : calcul possible et plus précis si le device se trouve dans un polygone délimité par les gateways → **nécessité d'une bonne topographie !**
- Avoir l'option activée dans le plan de connectivité du device
- Avoir une entité solveur de localisation pour en déduire une position estimée du device
- Paramétrage HTOL : cercle de précision calculé



Location Server

Géolocalisation

Globalement, les mesures de géolocalisation peuvent être moins bonnes lorsqu'un device n'est pas en vision directe avec les antennes (LOS – Line Of Sight). En effet, les devices sont plus généralement en configuration NLOS (Non-Line Of Sight) avec les gateways qui les couvrent. Cela engendre donc des transmissions radios non-directes, biaisées ou polluées (path fading, réflexion de l'onde, etc...)

Macrogéolocalisation		Géoloc TDoA
Pécision de la localisation	> 1 km	~ 100 m
Contraintes techniques	<ul style="list-style-type: none">• Minimum macrodiversité = 1• Disponibilité de la (ou des) gateway(s)	<ul style="list-style-type: none">• Minimum macrodiversité = 4• Disponibilité des gateways• Gateways équipées d'un FPGA V61• Intégration de clés de géoloc (licences Semtech) nécessaires au Fine Timestamping• Nécessité du GPS et du bon fonctionnement de l'horodatage fin• Design (impacts GDOP & NLOS)

Autres évolutions en géolocalisation

Semtech propose une solution multi-technologies pour améliorer la géolocalisation en LoRa.

Utilisation de GPS, Wi-Fi ou Bluetooth pour des cas d'usage nécessaire (utilisation très courte d'une de ces technologies le temps de la mesure) → impact sur la batterie moindre

Roaming LoRa®

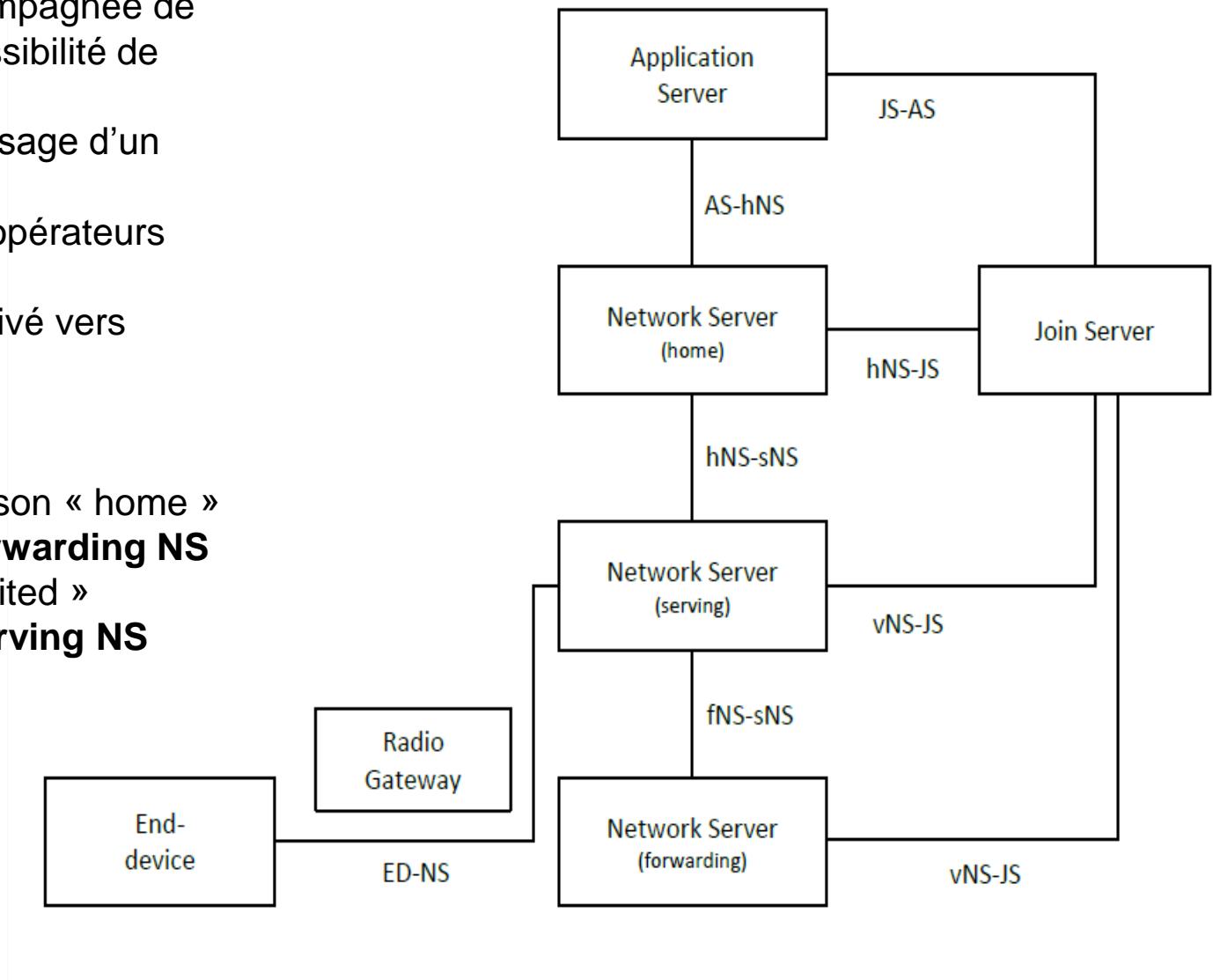
L'une des évolutions majeures de la release 1.1 accompagnée de la spécification backend interface 1.0 est d'offrir la possibilité de faire du roaming entre 2 réseaux.

On parle de roaming (ou d'itinérance) pour les cas d'usage d'un device LoRa® mobile :

- entre deux réseaux différents appartenant à deux opérateurs différents de deux pays différents
- ou entre deux réseaux différents de type réseau privé vers réseau public.

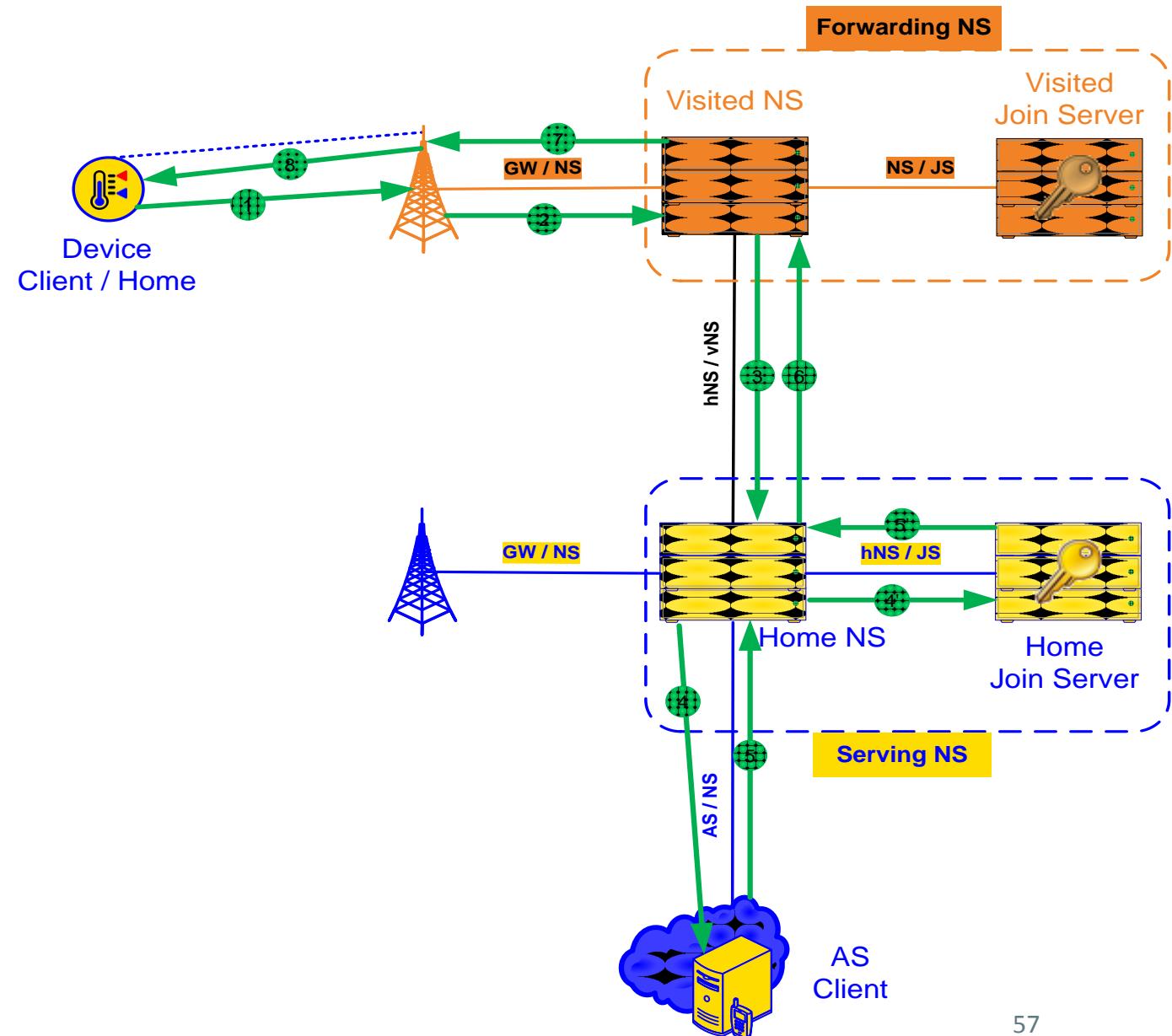
Il existe 2 types de Roaming en LoRa®

- **Passive Roaming** : le device est toujours servi par son « home » network serveur. Le réseau visité joue un rôle de **forwarding NS**
- **Handover Roaming** : le device est servi par le « visited » network serveur. Le réseau visité joue un rôle de **serving NS**



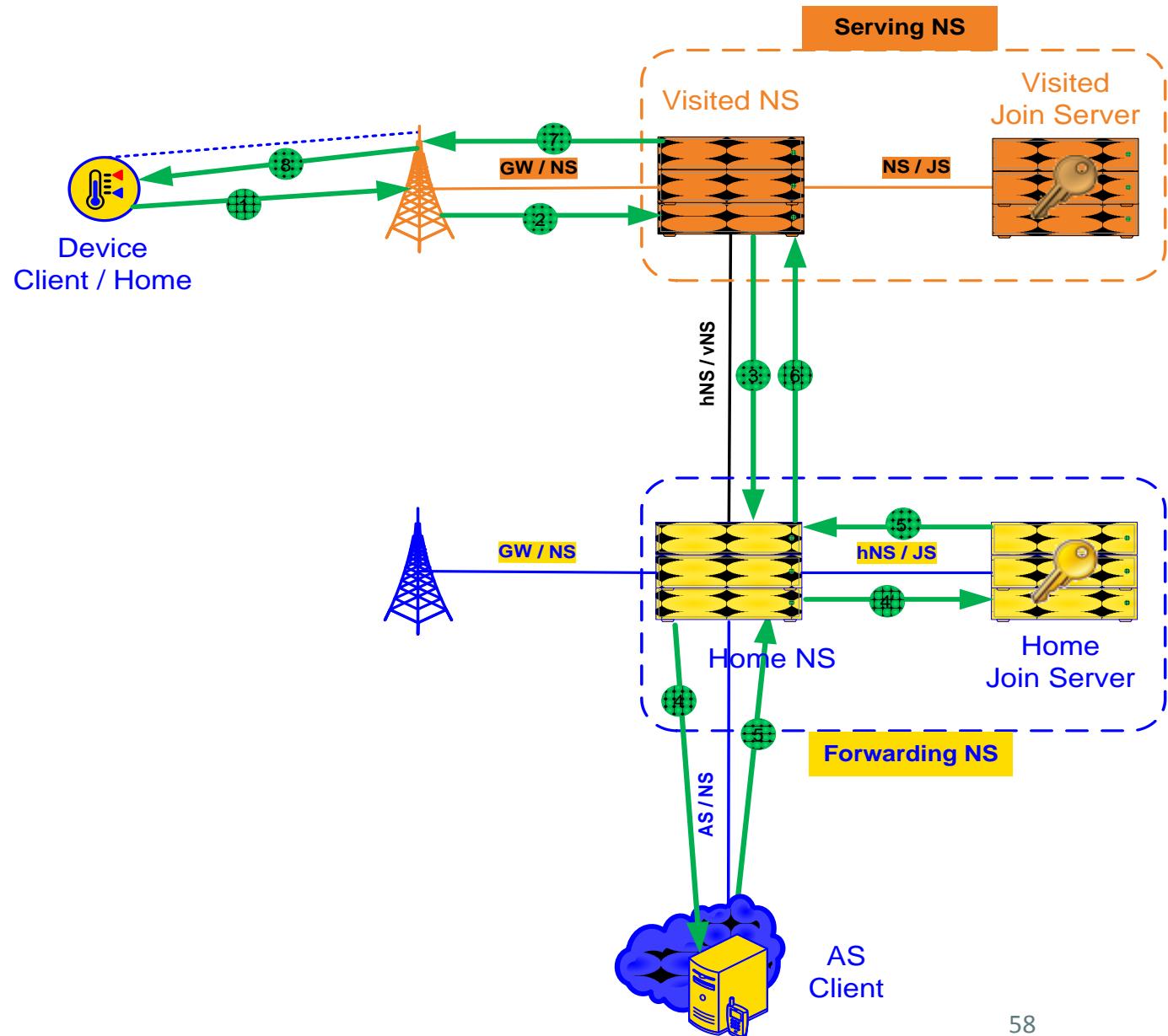
Roaming LoRa® - Passive Roaming

- **1 et 2** : trame UL du device reçu par le réseau visité
- **3** : vérification des accords de Roaming et de l'abonnement du device. Si accord et abonnement OK, alors établissement d'une session roaming : **PRStartReq / PRStartAns** (**2 modes possibles : stateless et stateful**), puis transmission de la trame vers le NS Home.
- **4** : S'il s'agit d'une trame data, la donnée applicative est transmise à l'AS
- **4' et 5'** : S'il s'agit un message Join Request destiné au JS Home (phase d'activation), alors la trame est transmise au Join Server visité qui produira un Join Accept (si tous les voyants sont au vert) qui arrivera ensuite jusqu'au device via le réseau visité (6 à 8)
- **5** : avant ou après la trame UL du device, l'AS peut envoyer au NS Home une commande applicative (Data)
- **6 à 8** : Envoi possible d'une **commande DL initiée par le Home NS** (MAC) ou l'AS client (Data) ou les deux (MAC + Data) vers le device



Roaming LoRa® - Handover Roaming

- Pour la partie Join, cela se passe de la même manière que Passive Roaming (**4' et 5'**)
- Pour des trames UL « classiques », le processus diffère légèrement :
- **1 et 2** : Trame UL du device reçu par le réseau visité
- **3** : Vérification des accords de Roaming et de l'abonnement du device. Si accord et abonnement OK, alors établissement d'une session roaming : **HRStartReq / HRStartAns**, puis transmission de la trame vers le NS Home.
- **4** : S'il s'agit d'une trame data, la donnée applicative est transmise à l'AS
- **5** : Avant ou après la trame UL du device, l'AS peut envoyer au NS Home une commande applicative (Data)
- **6** : Si une trame DL applicative est en attente durant la session HR, le hNS peut transmettre la trame applicative au vNS
- **7 et 8** : Envoi possible d'une **commande DL initiée par le Visited NS (MAC)** ou l'AS client (Data) ou les deux (MAC + Data) vers le device



Roaming LoRa®

Comparatif des deux solutions

Passive Roaming

Visited NS = fNS (forwarding Network Server)

Le réseau Home reste maître

- 😊 Compatible tous devices (dont LW1.0)
- 😊 Pas de procédure de Rejoin nécessaire
- 😢 Alignement du paramétrage radio des deux opérateurs obligatoire
- 😢 Plus de trafic inter-NS, et donc plus de latence

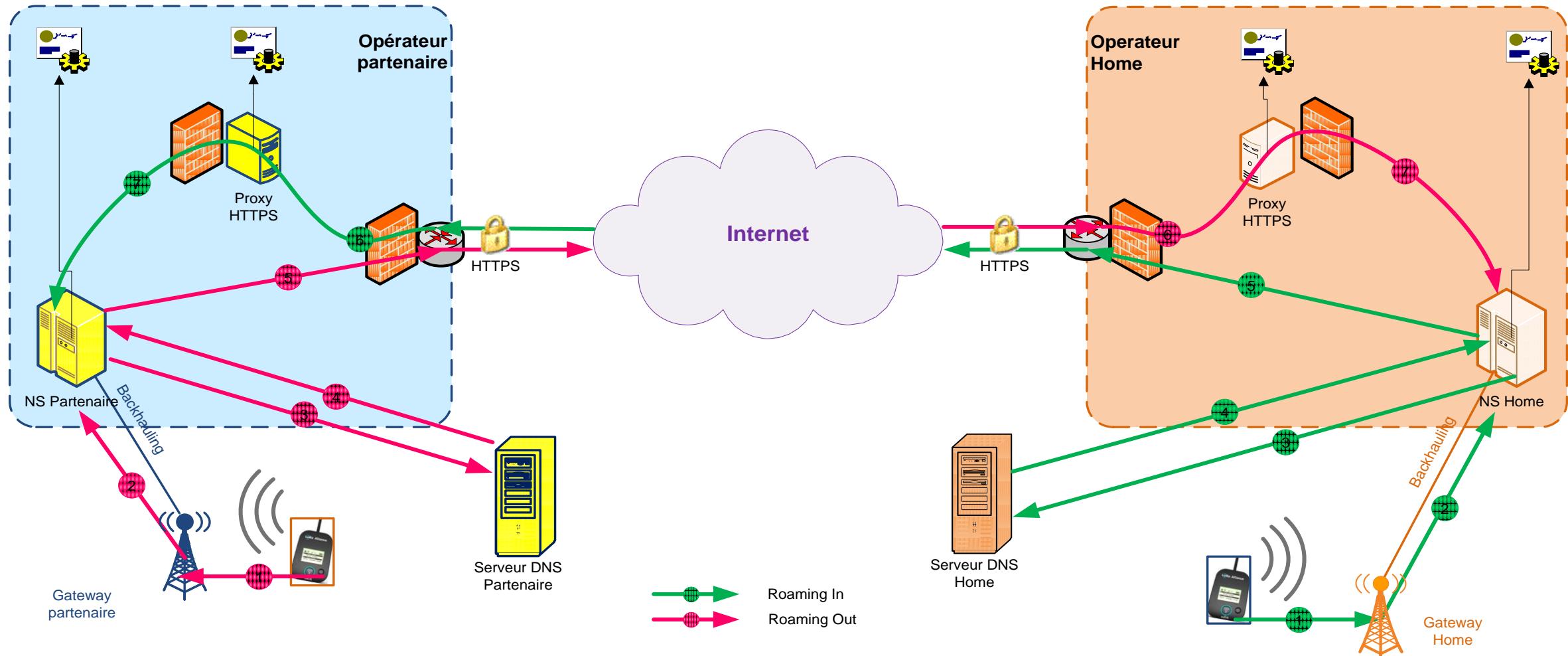
Handover Roaming

Visited NS = sNS (serving Network Server)
Le réseau visité devient maître

- 😊 Adaptation automatique du paramétrage radio du device par le vNS
- 😊 Limitation de trafic inter-NS et latence réduite
- 😢 Devices OTAA LW1.1 nécessaire
- 😢 Procédure lourde (Rejoin Request nécessaire)

Roaming LoRa® - Interconnexions entre opérateurs

Lien direct (sécurisé avec contrôle par certificats et résolutions DNS)

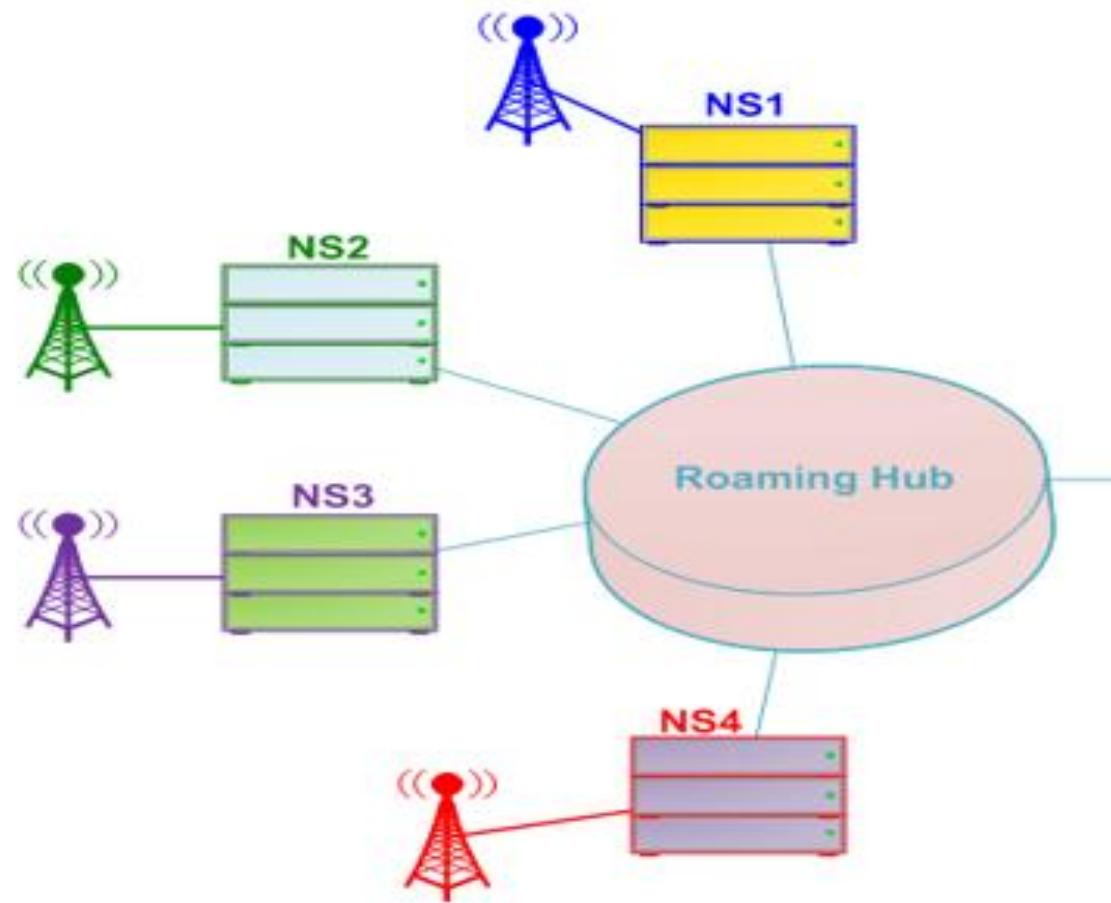


Note : il est possible de gérer le roaming de façon unilatérale (dans un seul sens)

Roaming LoRa® - Interconnexions entre opérateurs

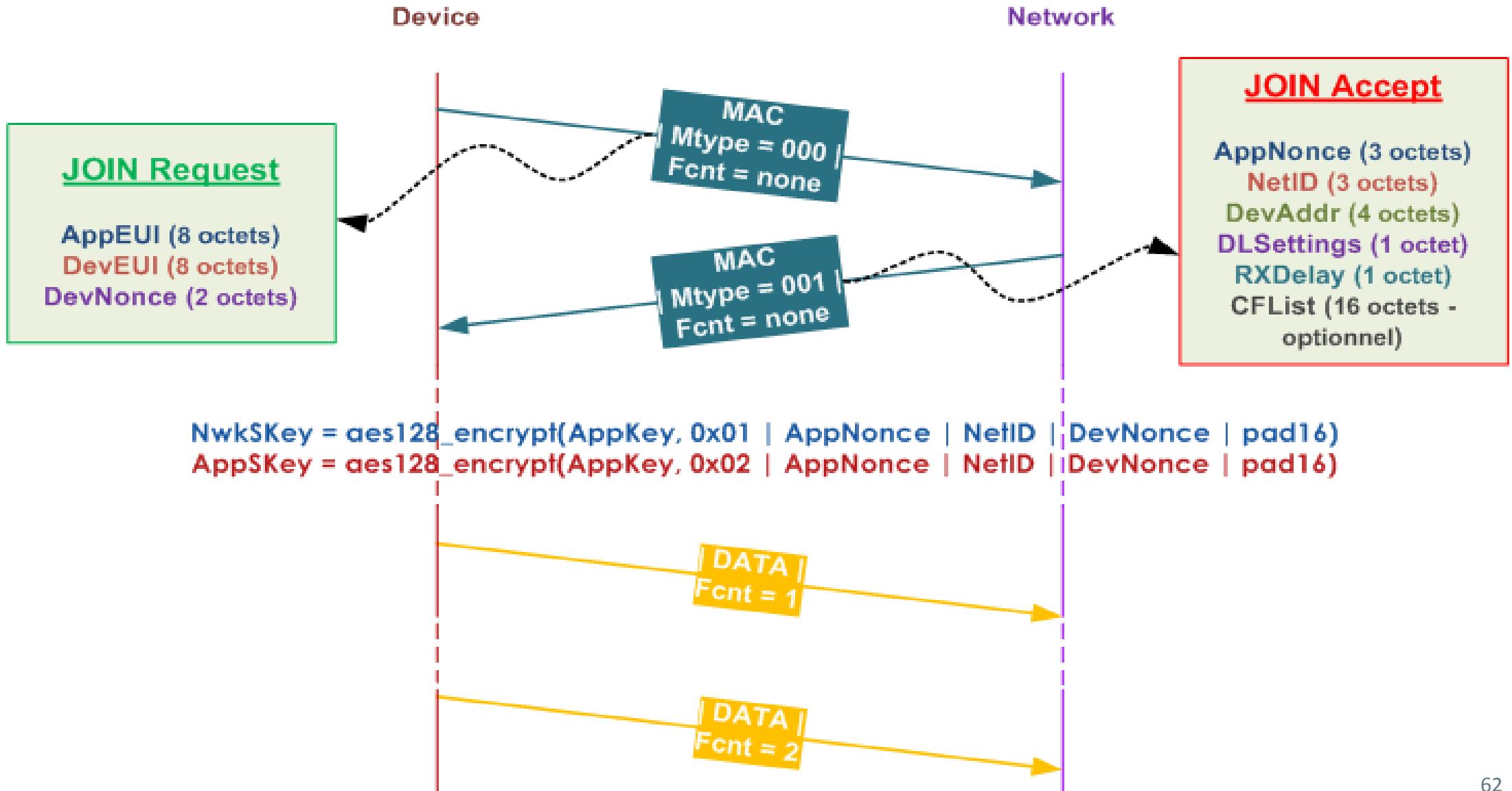
Lien via HUB Roaming

Permet de limiter les interconnexions point à point entre opérateurs



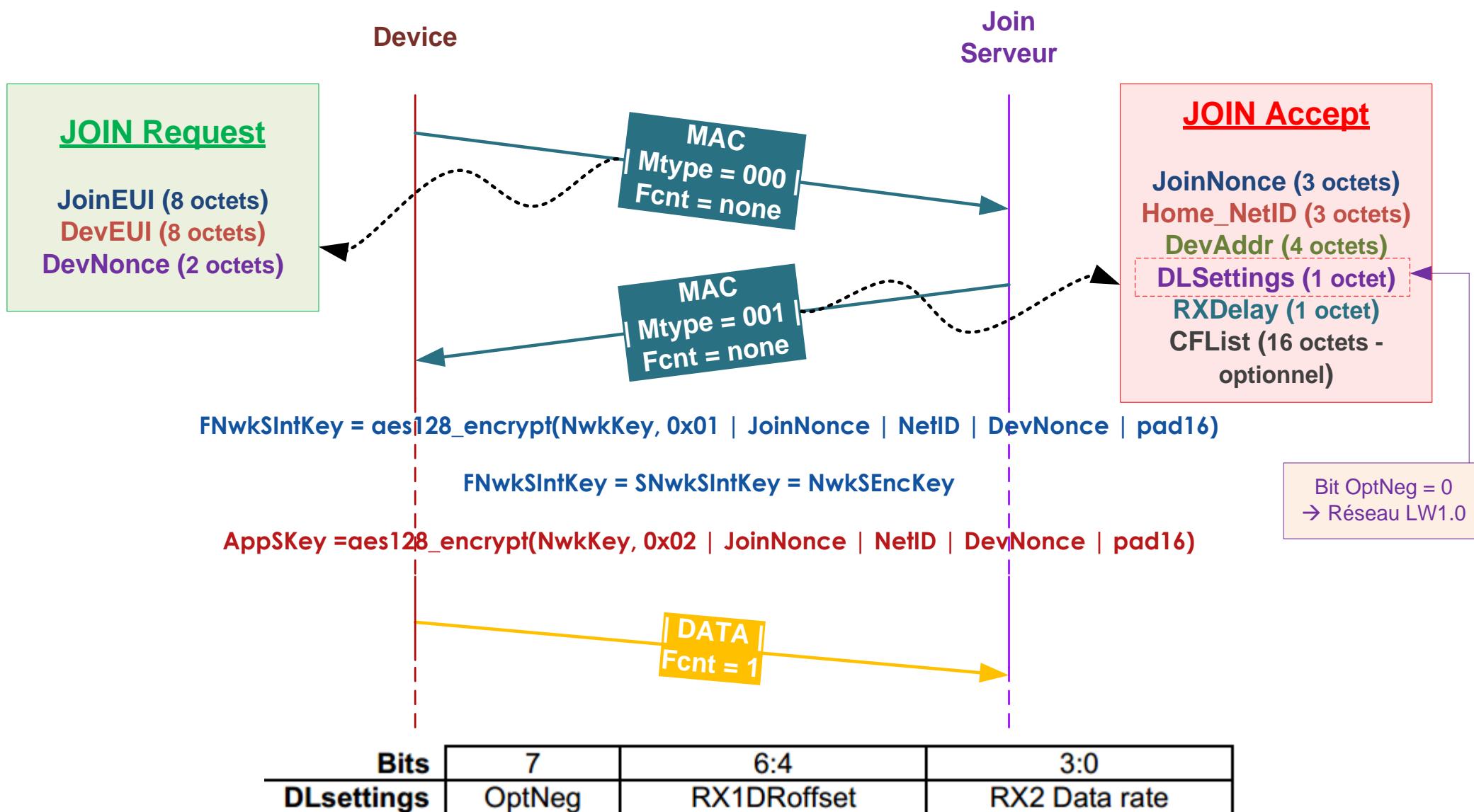
Call Flow LoRaWAN™ 1.1

Procédure JOIN en LW1.0 (Rappel)



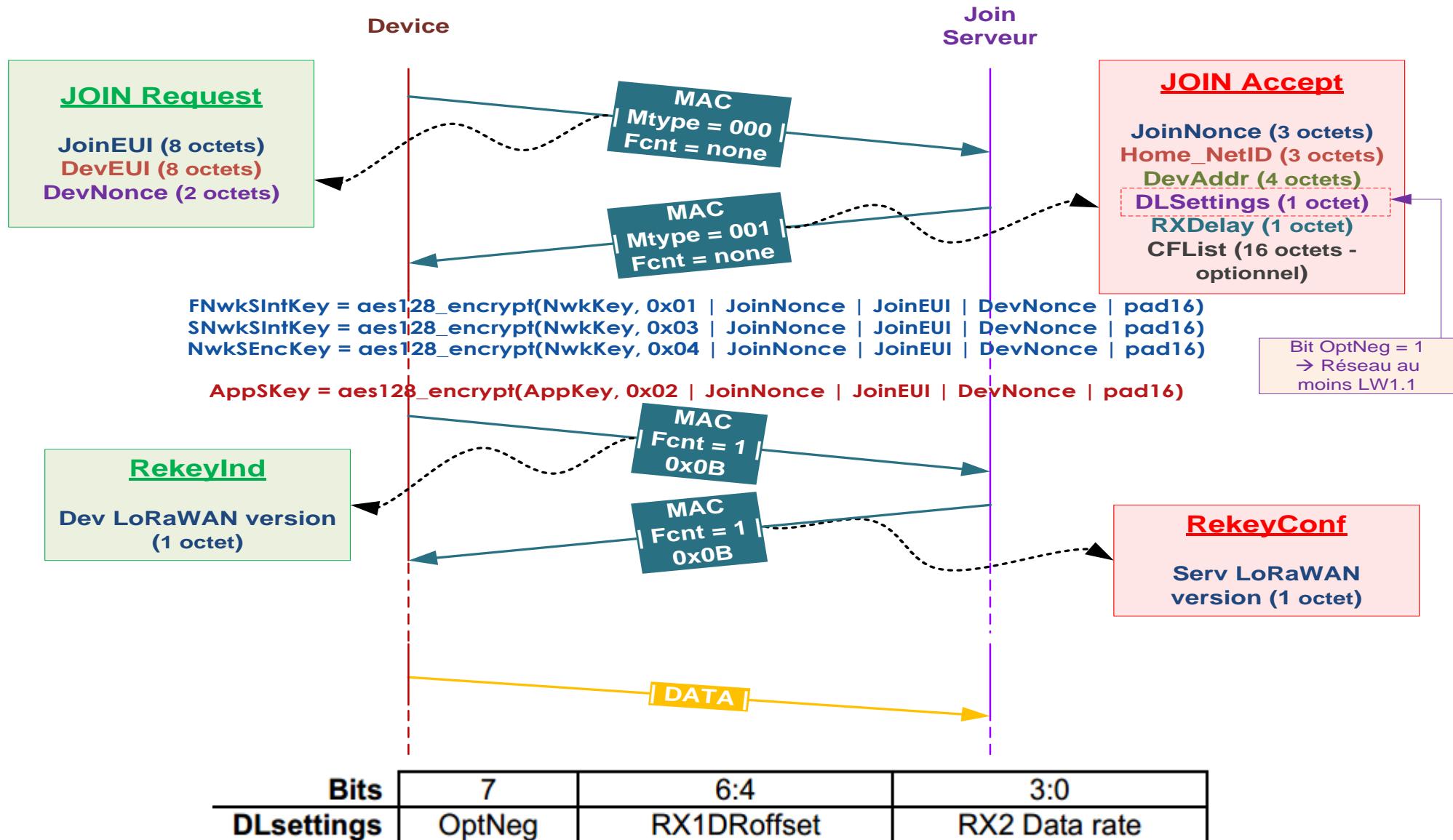
Call Flow LoRaWAN™ 1.1

Procédure JOIN en LW1.1 (cas OptNeg = 0)



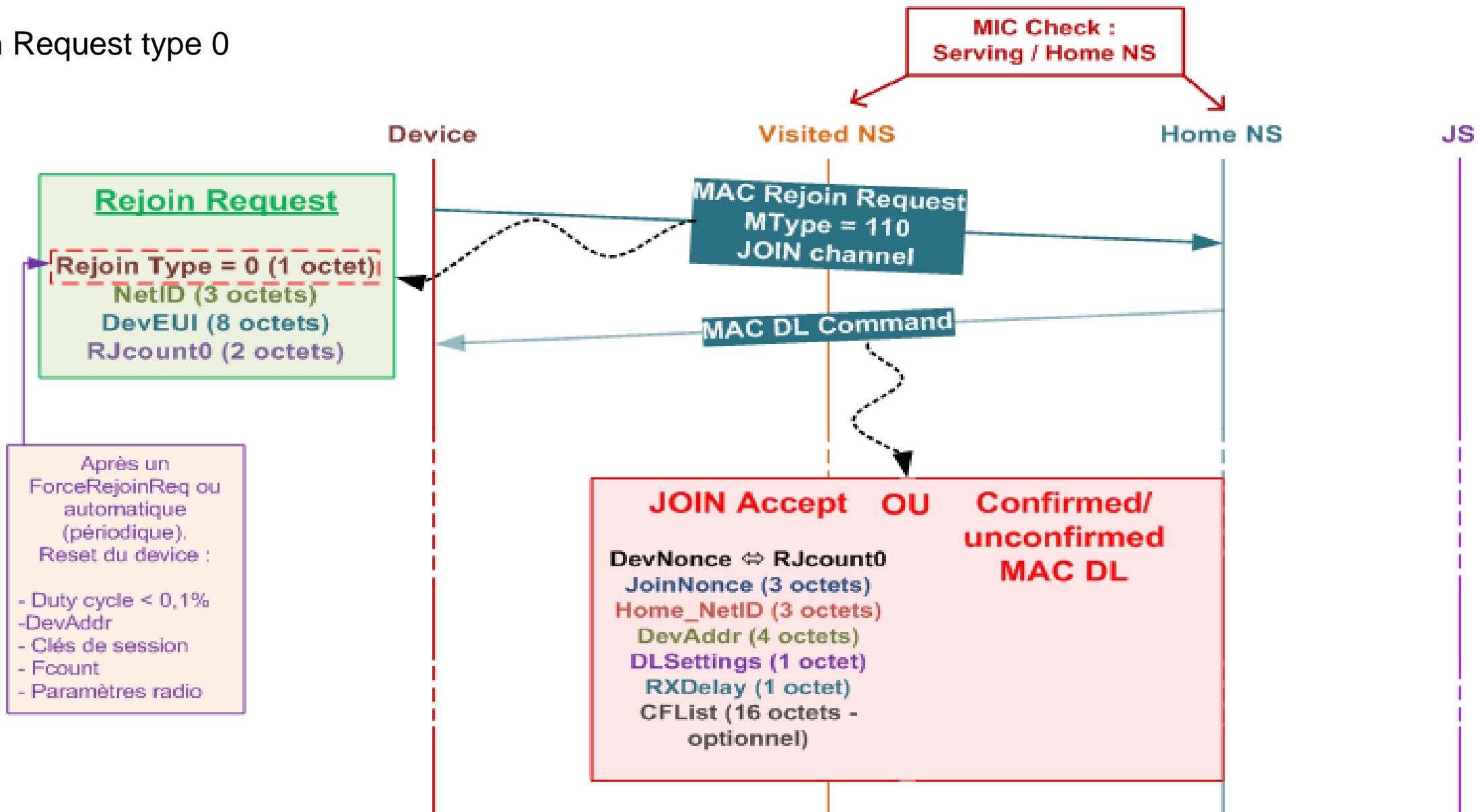
Call Flow LoRaWAN™ 1.1

Procédure JOIN en LW1.1 (cas OptNeg = 1)



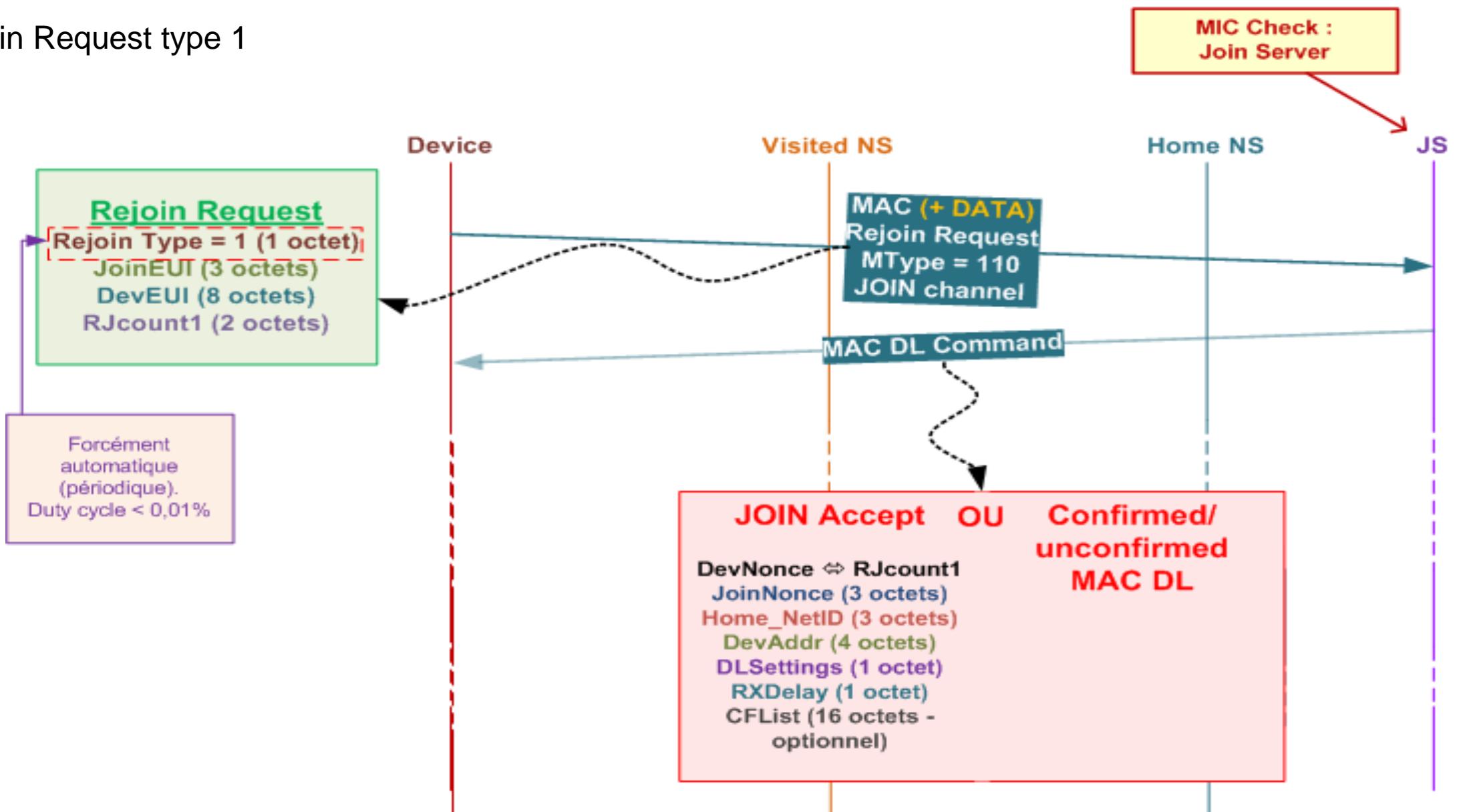
Call Flow LoRaWAN™ 1.1

Rejoin Request type 0



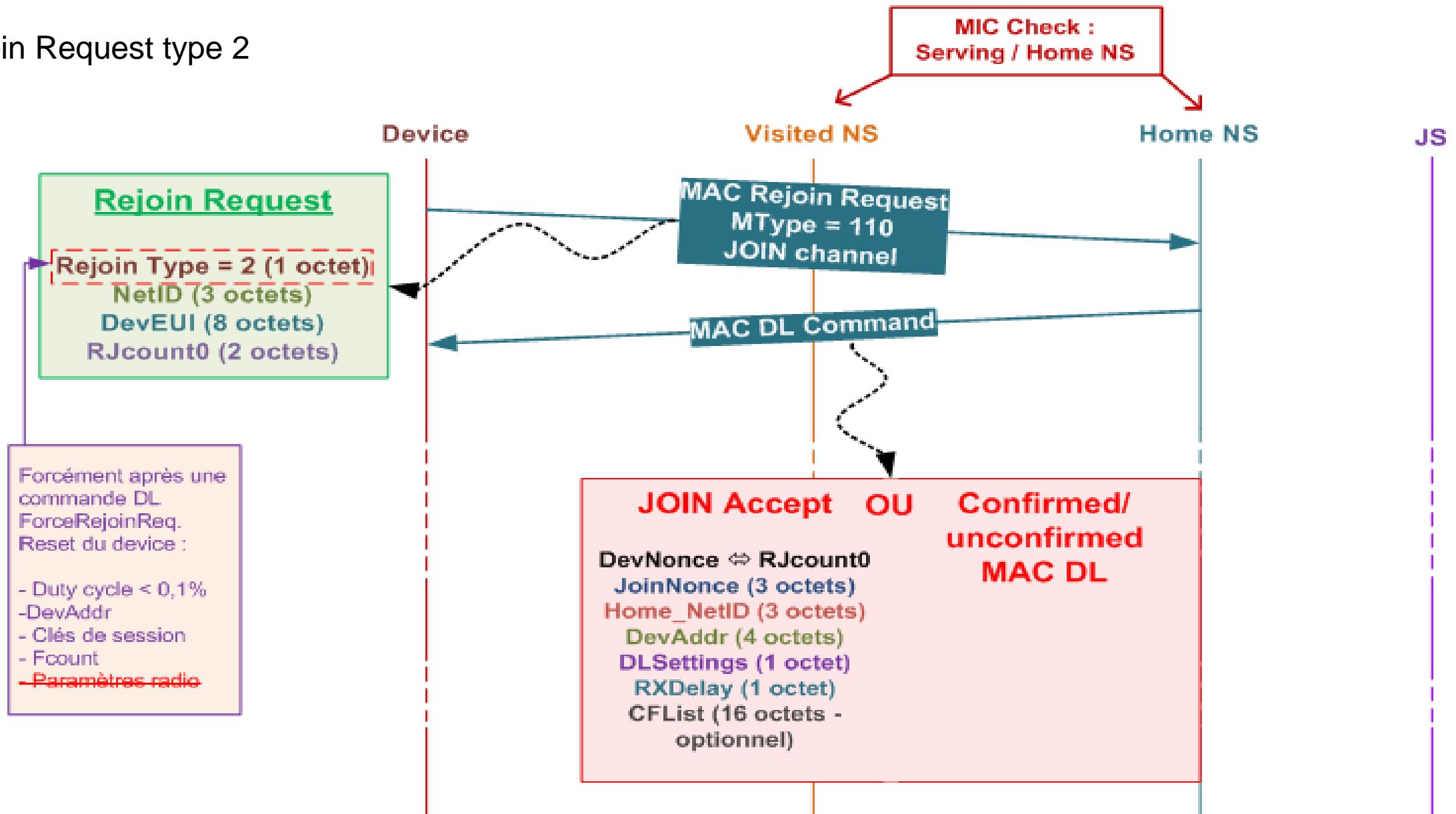
Call Flow LoRaWAN™ 1.1

Rejoin Request type 1



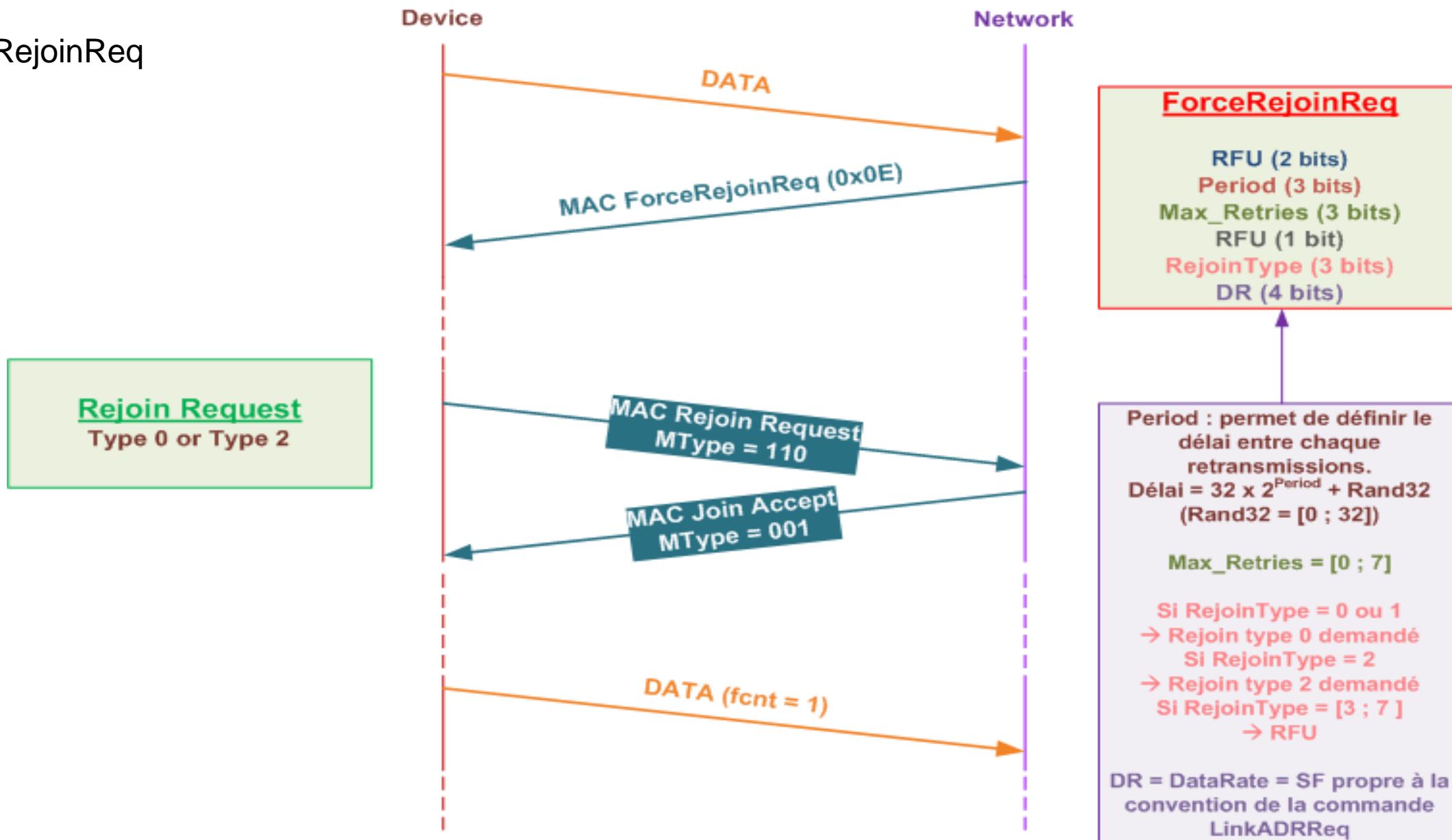
Call Flow LoRaWAN™ 1.1

Rejoin Request type 2



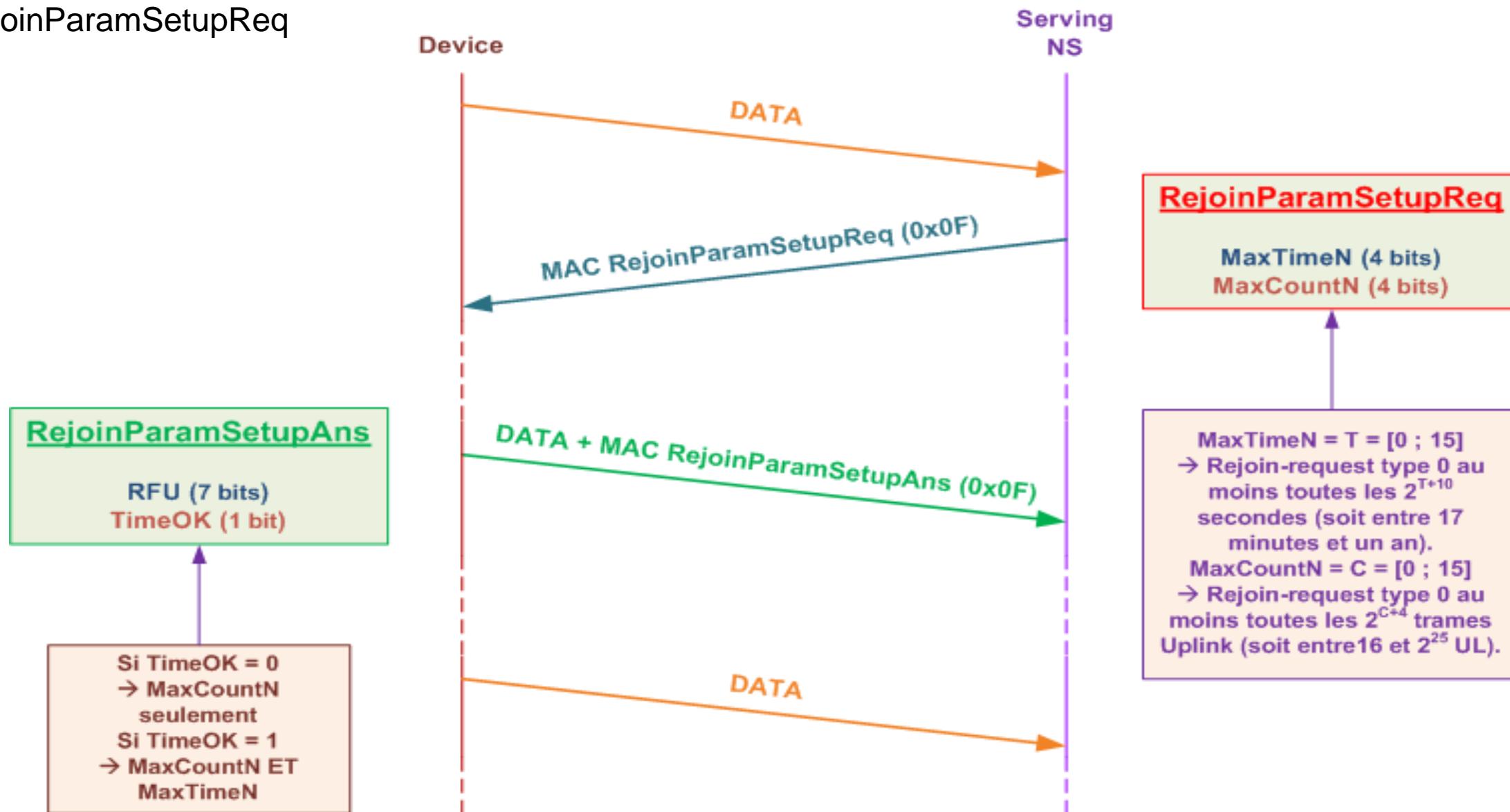
Call Flow LoRaWAN™ 1.1

ForceRejoinReq



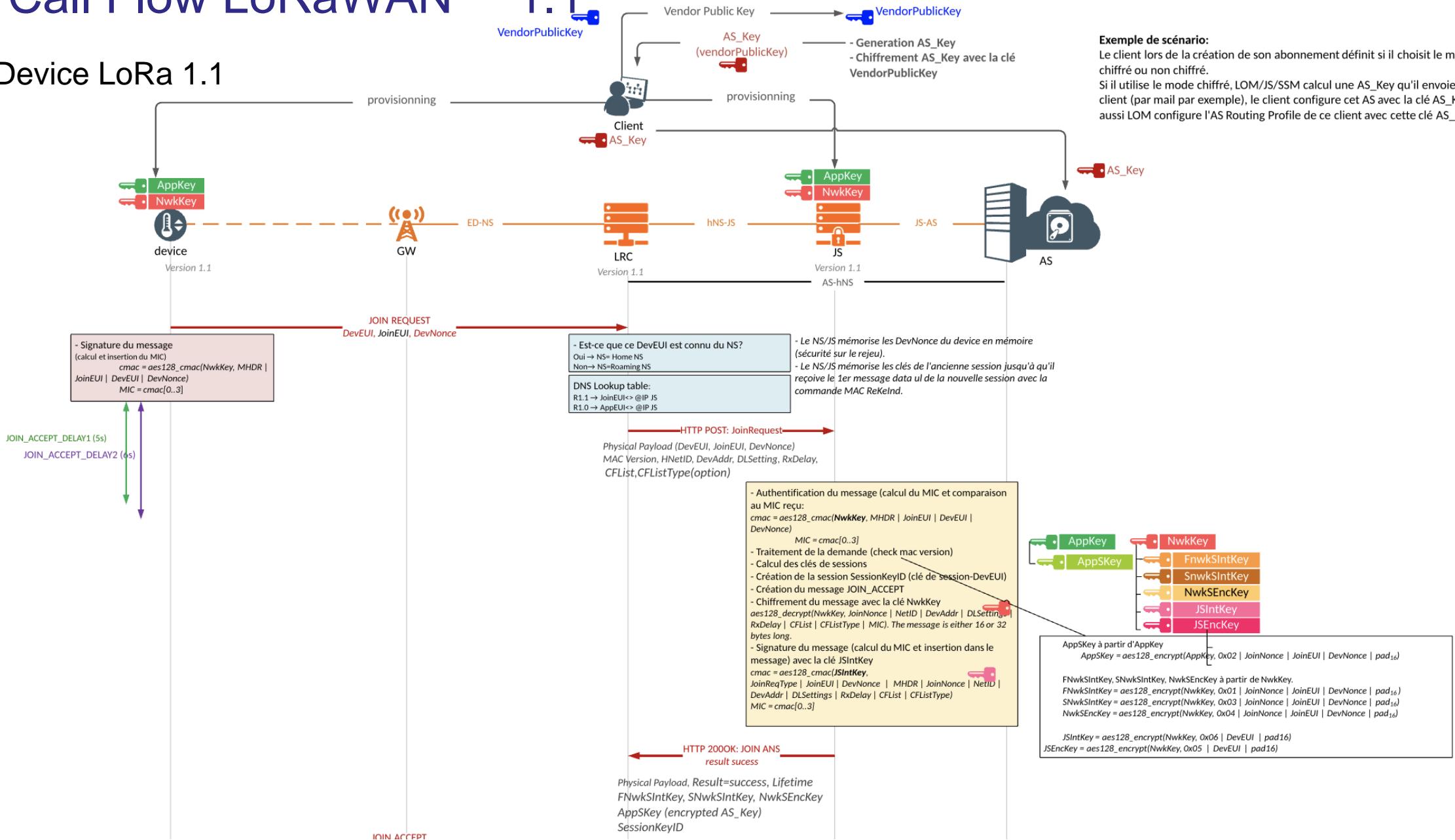
Call Flow LoRaWAN™ 1.1

RejoinParamSetupReq

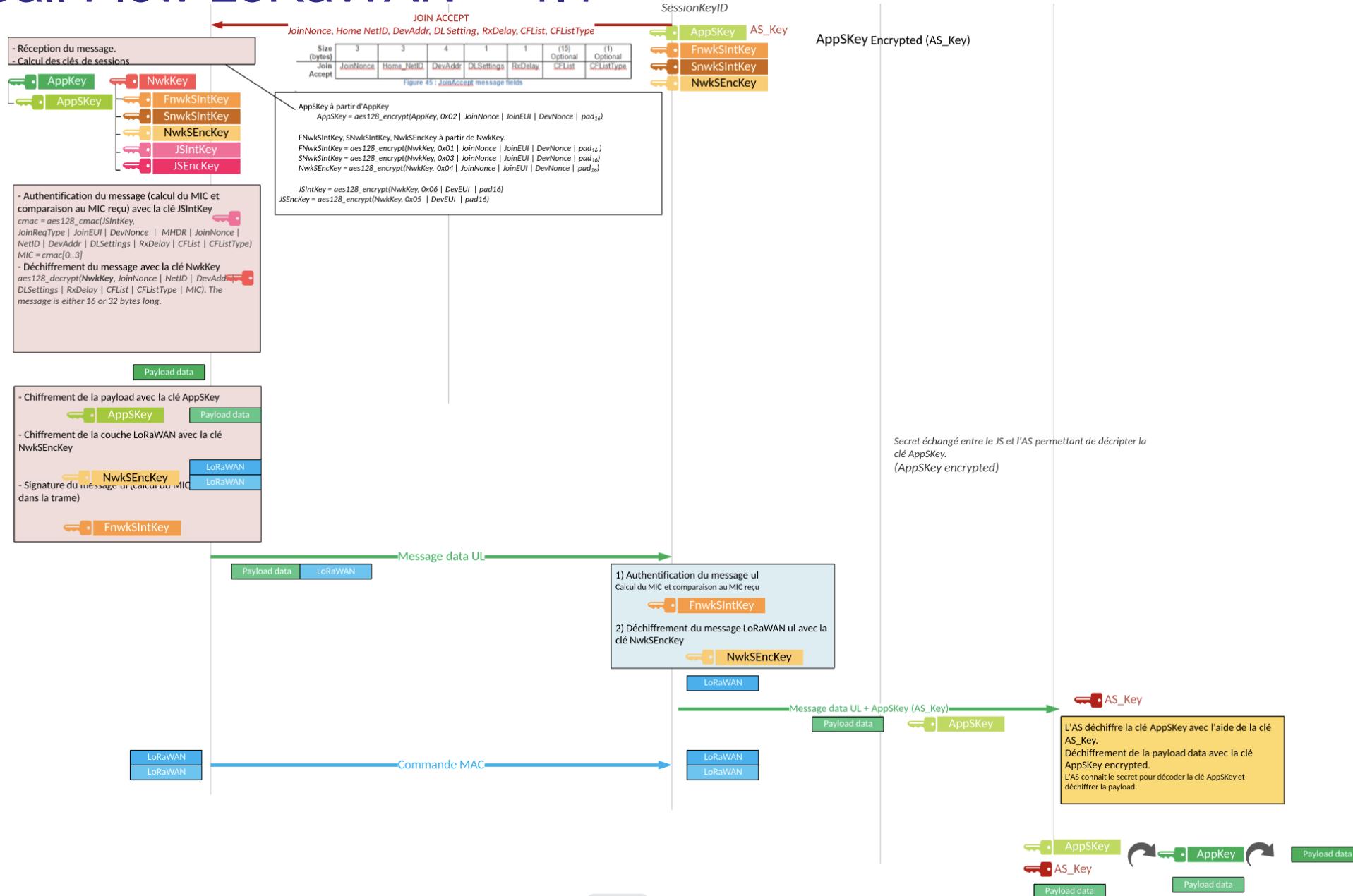


Call Flow LoRaWAN™ 1.1

Device LoRa 1.1



Call Flow LoRaWAN™ 1.1



Sécurité avancée : HSM et SSM

SSM/HSM = Software / Hardware Security Module

→ Rôle de Join Serveur indépendant

Objectif : empêcher l'opérateur de connaître la clé de session

AppSKey.

AppKey (& NwkKey dans le cas d'un device LW1.1 sur réseau
LW1.0) → AppKey_Enc_HAK (& NwkKey_Enc_HAK)



- Standard HSM
- Tamper resistant technology
- FIPS 140-2 Level 3
- Secure key storage and processing
- Cryptographic offloading/acceleration
- Key storage inside HSM or as encrypted key files
- Multiple options for user authentication and access control
- SmartCard for strong authentication
- Separation of duties
- Remote Management
- Supported OS: Windows and Linux



06

Annexes

- Sources et liens utiles

Sources et liens utiles

- LoRa Alliance™: <https://lora-alliance.org/>
- Spécification LoRa®: <https://lora-alliance.org/resource-hub>
 - Spécification 1.0: 2015_-_lorawan_specification_1r0_611_1.pdf
 - Spécification 1.03: lorawan1.0.3.pdf
 - Version 1.1:
 - Spécification 1.1: lorawantm_specification_-v1.1.pdf
 - Spécification Backend Interface 1.0:lorawantm-backend-interfaces-v1.0.pdf
- Semtech: <https://www.semtech.com/products/wireless-rf/lora-transceivers>
- GSMA : <https://www.gsma.com/iot>
- Semtech LoRa® Developers: <https://lora-developers.semtech.com>