Oct. 2018

DNS usage in LoRaWAN

afnic

Overview

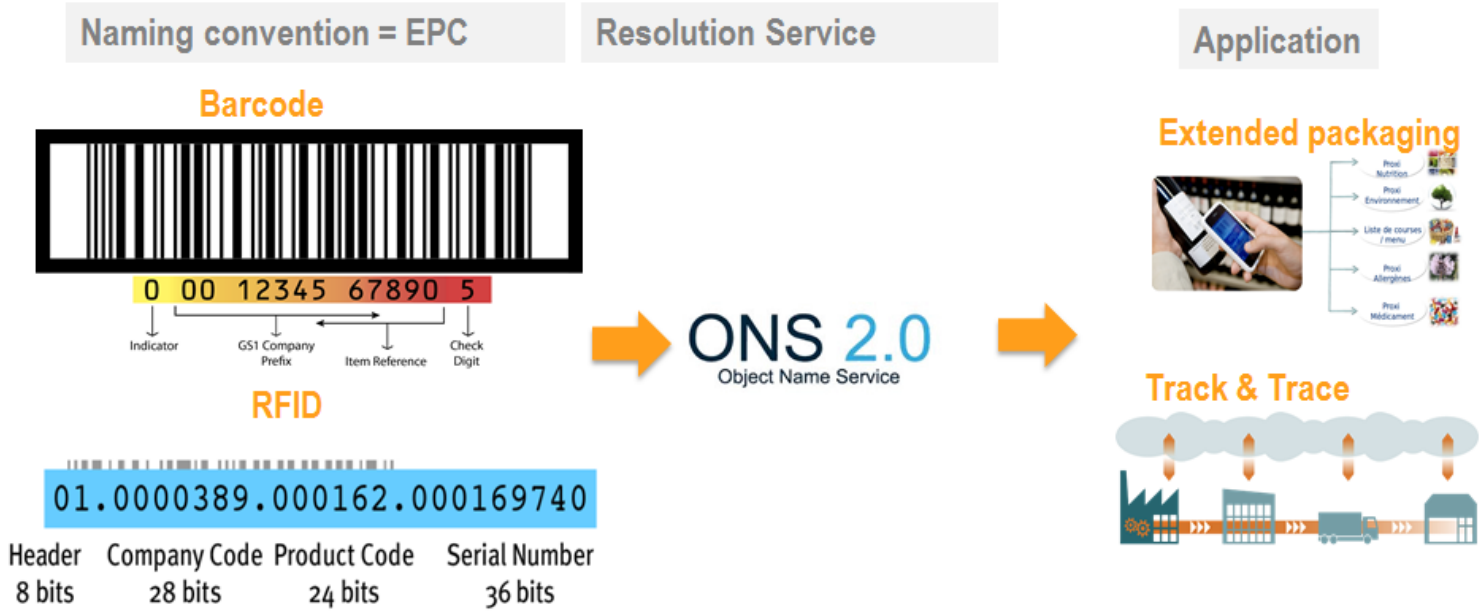
- Afnic’s past IoT activities
- Introduction to the LoRa infrastructure
- DNS present and possible future usages in LoRaWAN

Afnic’s past IoT activities

Examples of SDOs and respective naming services

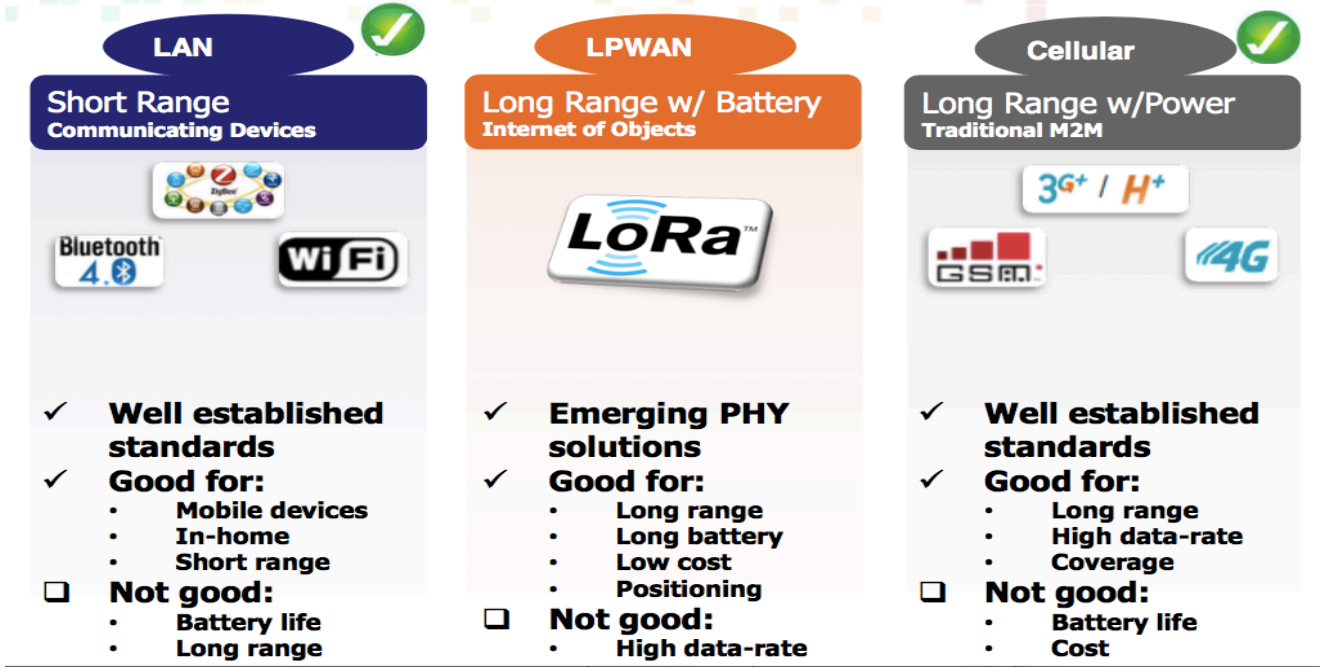
Identification Schema	SDO	Naming Service
URI (e.g. Domain names)	IETF	DNS
EPC	GS1	ONS
OID	ITU and ISO/IEC	ORS
DOI	ISO	Handle

DNS in the bar code/RF-ID domain



LoRa introduction

IoT segment trade-offs



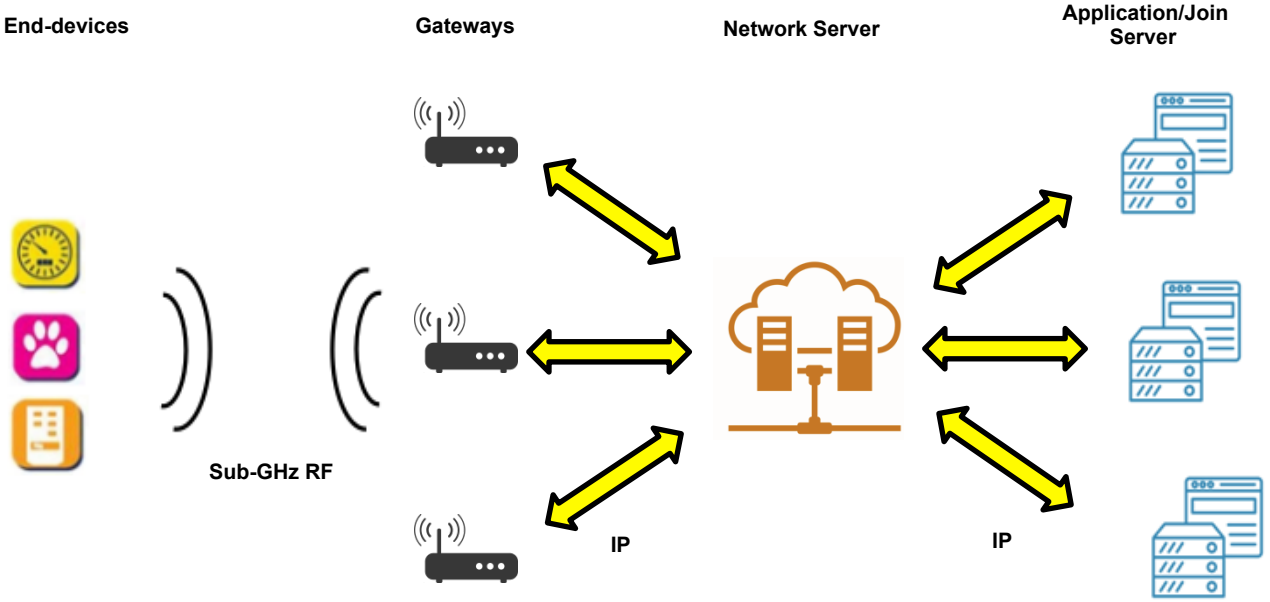
Source : Semtech

LoRa network advantages

Key Features	Attribute/Benefit
157dB to 168dB link budget	Long range 
>15 km range	
Minimal infrastructure	Ease of deployment 
Concentrator with capacity	
>10 yrs battery lifetime	Long battery life 
RX - 10 mA, sleep <200 nA	
Unlicensed spectrum	Low cost 
Low infrastructure cost	
Low end-node cost	

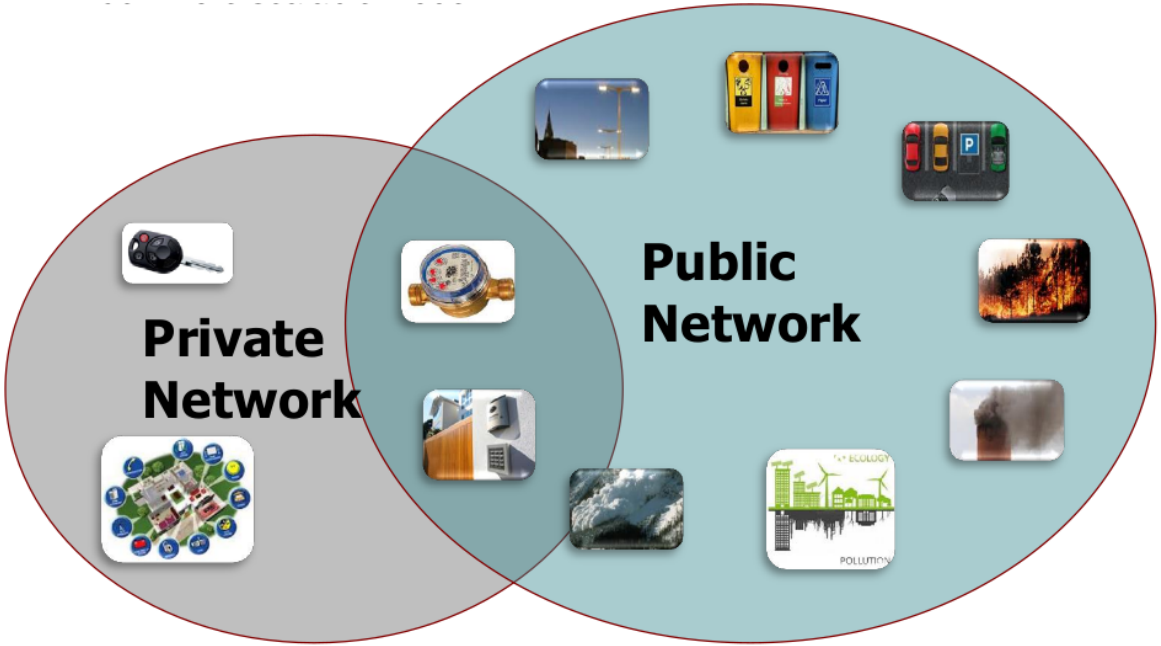
Source : Semtech

LoRa network topology



Why LoRa-alliance chose DNS?

- A scalable model



DNS usage in LoRaWAN Specs

- OTA activation
- Roaming – either passive or handover roaming

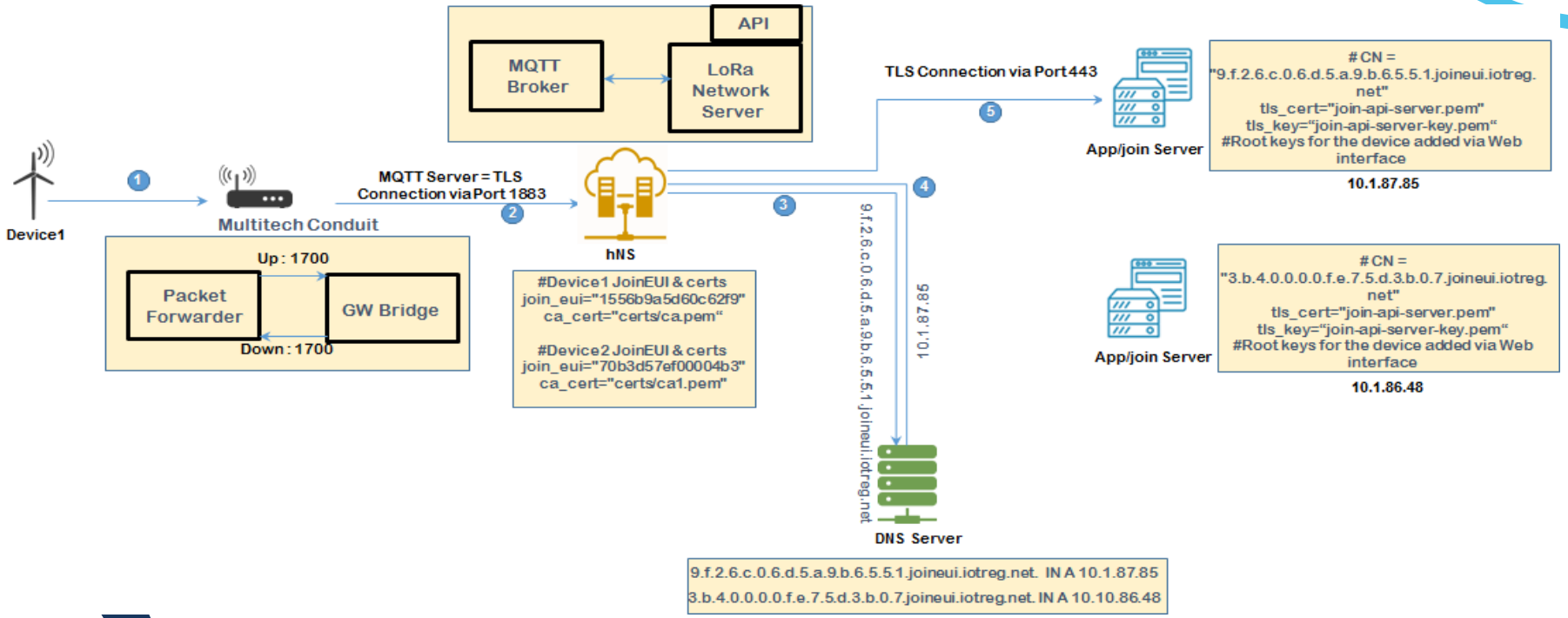
Pre-provisioning needed before OTAA

Device contains the DevEUI, NwkKey, AppKey, JoinEUI

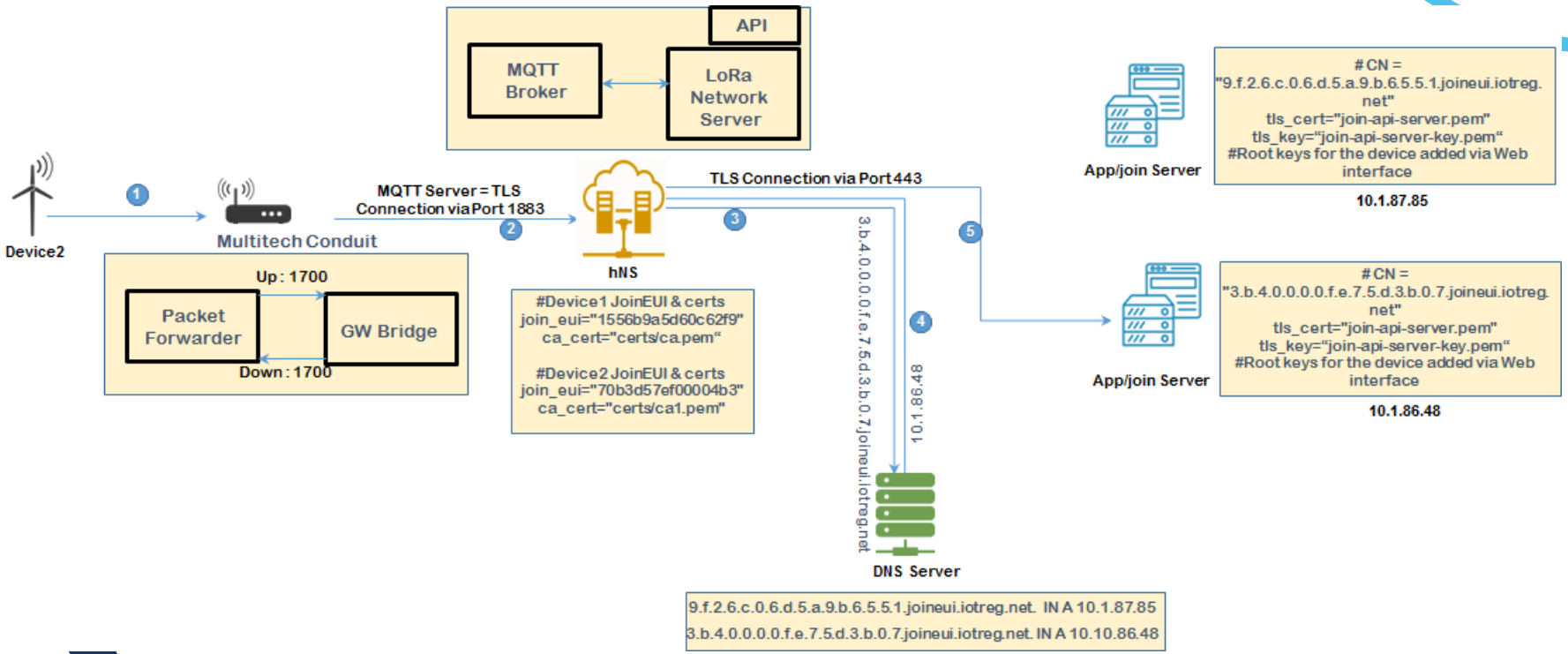
Network server contains the DevEUI, NwkKey

Appserver contains the DevEUI, AppKey

OTAA via DNS for device ‘1’



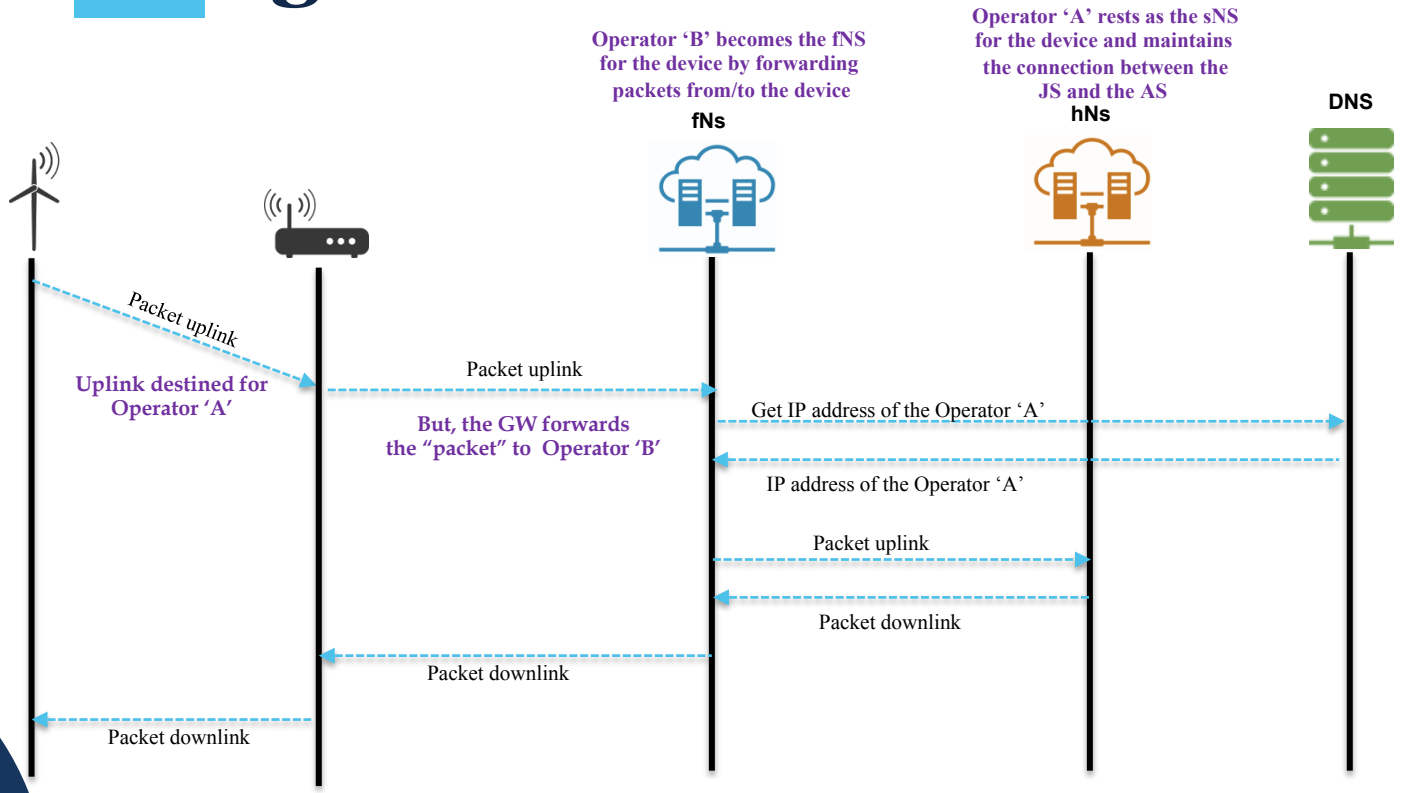
OTAA via DNS for device ‘2’



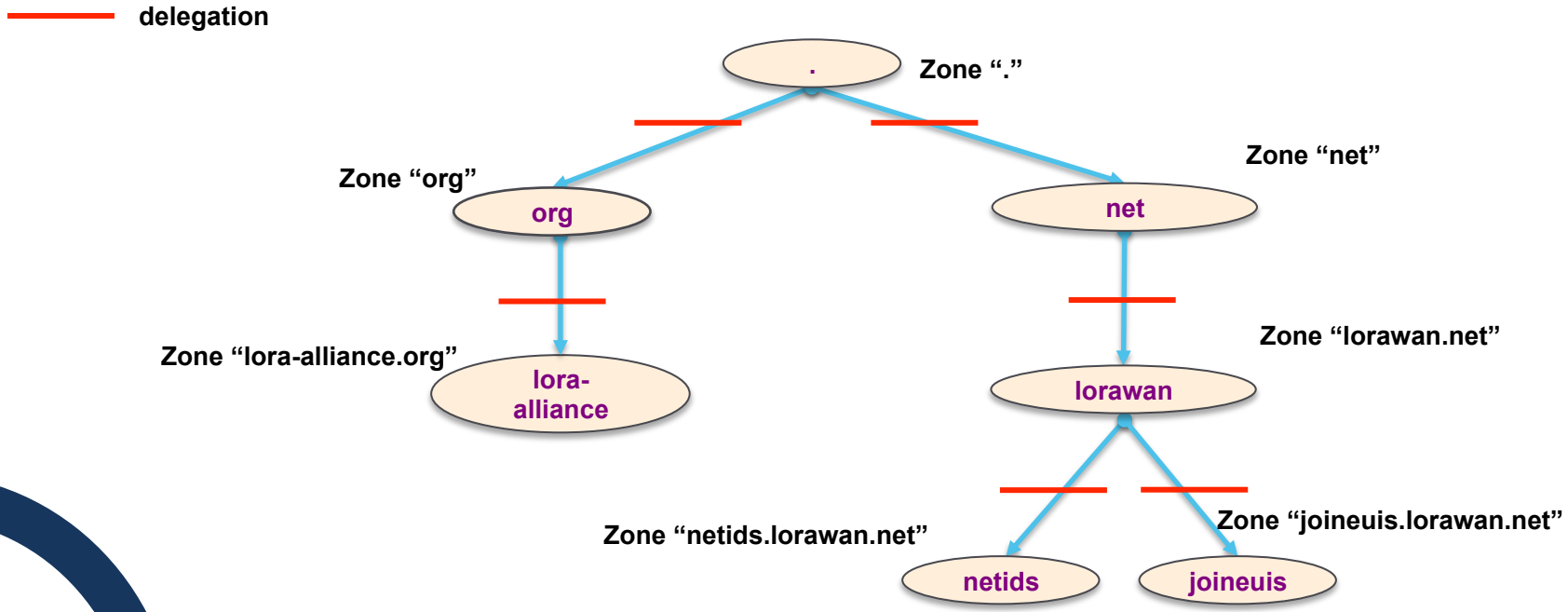
Information in the device after OTAA

Device contains the
DevEUI, NwkKey, AppKey,
JoinEUI, JoinNonce, NetID,
DevAddr , NwkSIntKeyUp,
NwkSIntKeyDwn, NwkSEncKey,
AppSKey

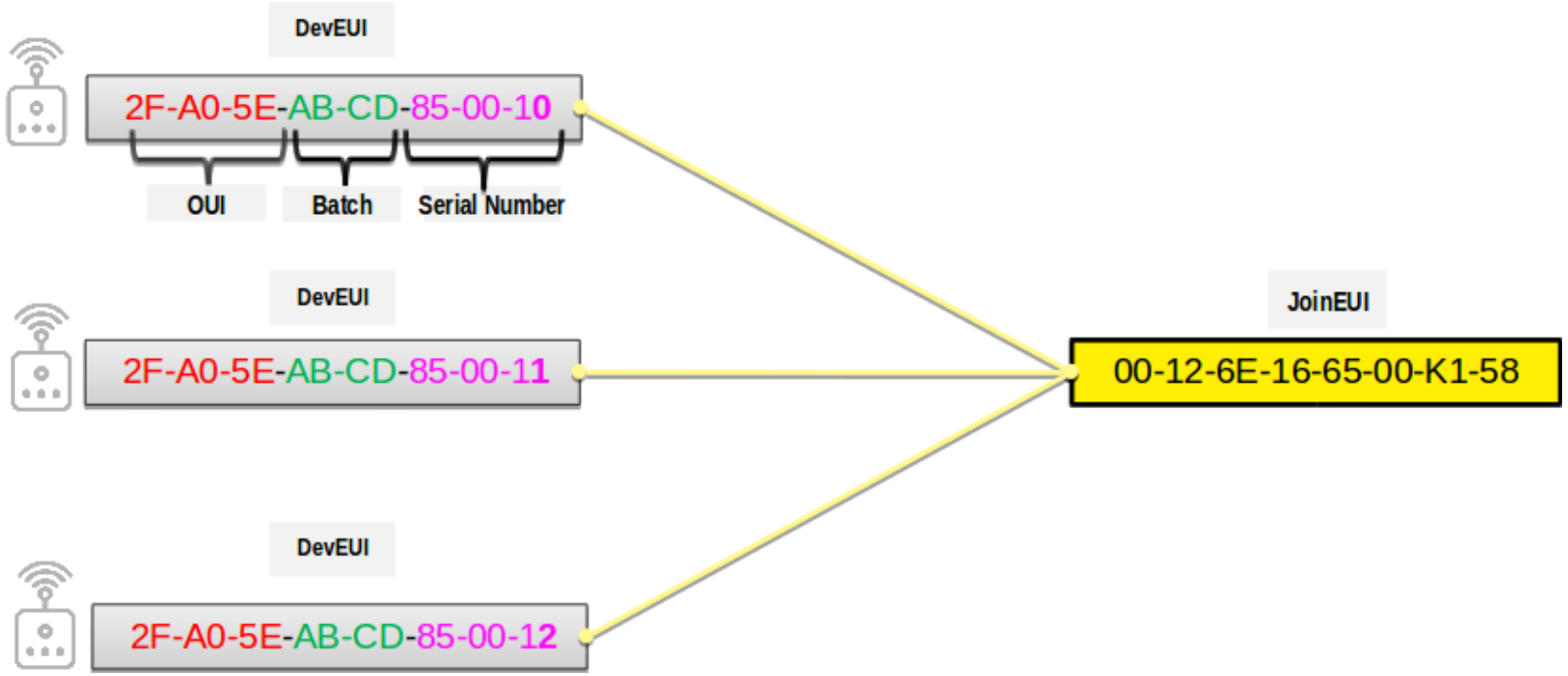
Passive roaming scenario using DNS



LoRa DNS tree



Solving device manufacturer issue using DNS



Breaking the JoinEUI dependancy

*.D.C.B.A.E.5.0.A.F.2.8.5.1.K.0.0.5.6.6.1.E.6.2.1.0.0.joineui.lora-alliance.org. IN A 1.2.3.4

DevEUI reversed until the batch number

JoinEUI reversed

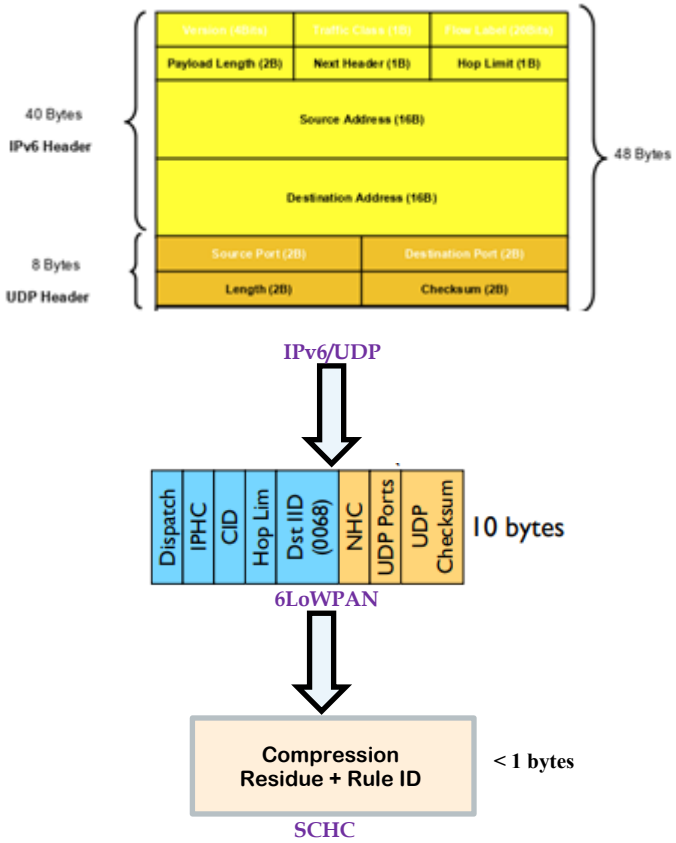
Breaking the JoinEUI dependancy of the JS:

*.4.5.D.C.B.A.E.5.0.A.F.2.8.5.1.K.0.0.5.6.6.1.E.6.2.1.0.0.joineui.lora-alliance.org. IN A 1.1.1.1

To use IP or not in IoT

- IoT is about connecting « things » to the Internet
- Non IP devices connect to the Internet through an Internet gateway
  - The gateway is an application layer gateway – Needs to strip the data and restructure it with a TCP/IP stack in order to enable communication with an Internet service
  - Packets encrypted at the IoT network must be decrypted and re-secured in the IP datagram at the Internet gateway
- IP based IoT devices can route and forward data without much intervention

Issue - IPv6/UDP Header Size



SCHC Context

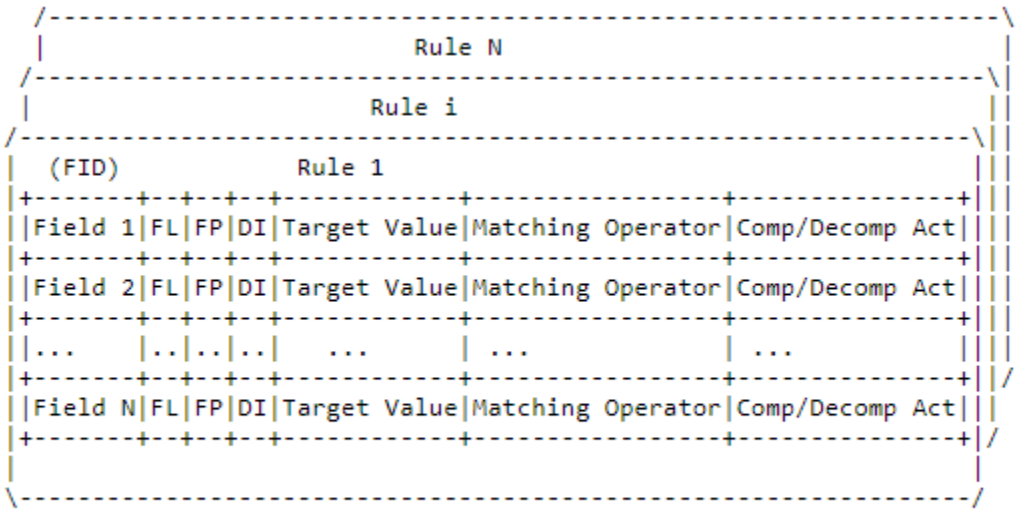
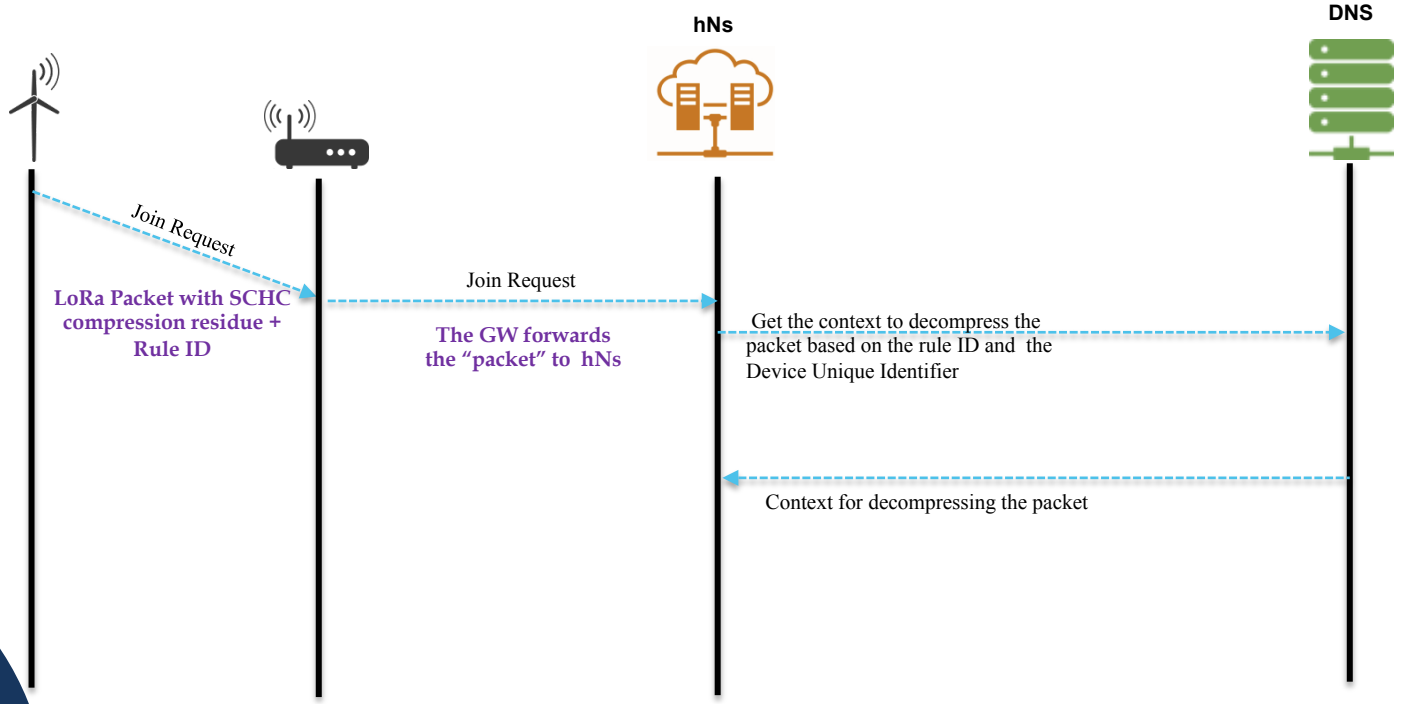
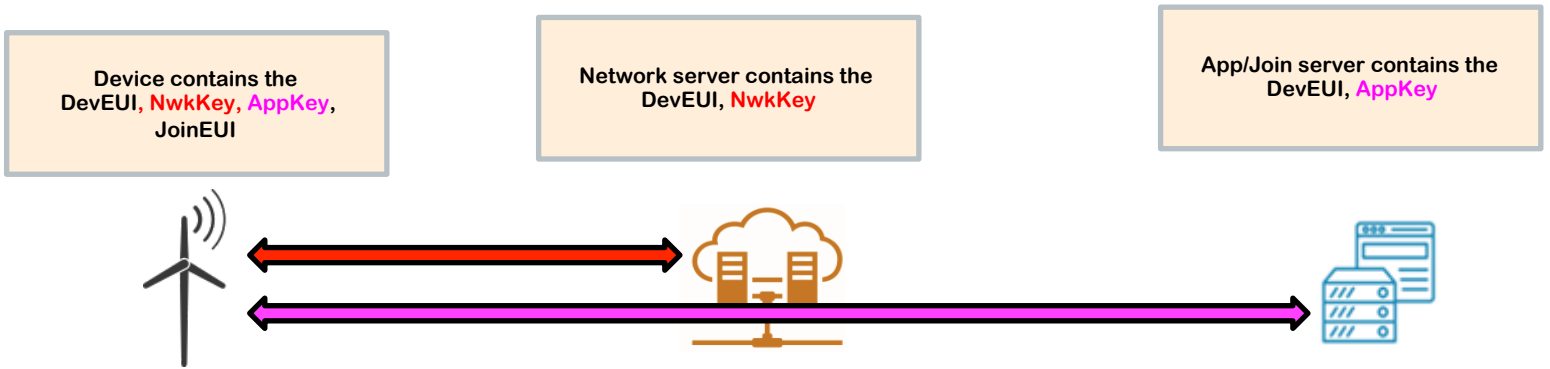


Figure 8: Compression/Decompression Context

Resolving the context from the DNS

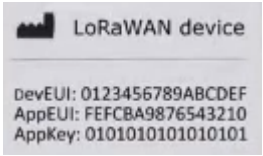


Issue : Shared Secret Key need to be pre-provisioned manually



Key distribution Challenges

- Device manufacturer adds the Key in the device
- Keys are shared with device owner:
  - Written in the back of the device
  - By files, mails etc..



- The Keys then have to be shared with the Network Operator, Join Server operator, App server operator

Looking at : DNSSEC, DANE, DoT