Table of Contents

LoRaWAN specification. The end-devices activation

To join the LoRaWAN network, the end-device must go through the activation procedure (End-Device Activation). The specification provides for two options for activating devices:

- **OTAA, Over-The-Air Activation** (you need to go through the join procedure, during which session encryption keys and the DevAddr address are generated).
- **ABP, Activation By Personalization** (there is no need to go through the join procedure, encryption keys and the DevAddr address are written to the device in advance (device personalization))

The device must contain the following values after activation:

- **End-device address (DevAddr)** — local address of the device on the given network [32 bits]. DevAddr consists of two fields: NwkID (network identifier, bits 31…25) and NwkAddr (network address, bits 24…0).
- **Network session key (NwkSKey)** — network session key [128 bits] used to calculate and check the MIC (message integrity code) field of messages in the exchange between the end-device and the network server (Network Server), as well as encrypt MAC-level messages.
- **Application session key (AppSKey)** — session key [128 bits] used to encrypt data at the application level (between the end-device and the application server).
- Also, the device must have an application ID [64 bits], which is written in advance — **Application identifier (AppEUI)**

OTAA - Over-The-Air Activation join procedure

The join procedure is always initiated by the end-device and consists of two messages exchanged between the end-device and the network server: **join request** (device → server) and **join accept** (server → device).
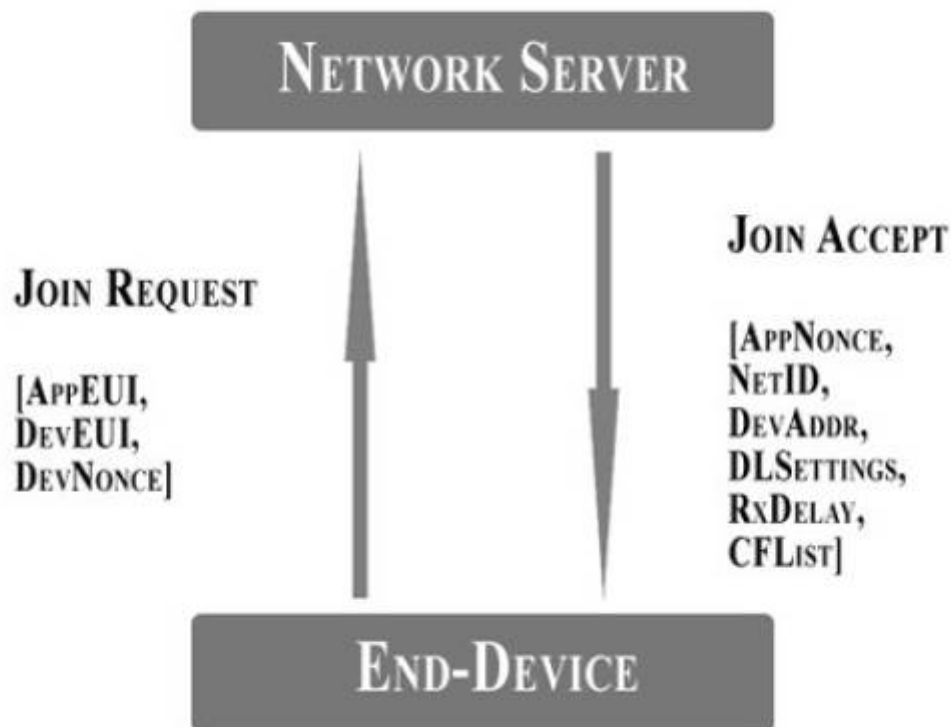
The join request message contains AppEUI, DevEUI, and a random DevNonce:

Join Request					
3 bytes	3 bytes	4 bytes	1 byte	1 byte	16 bytes
AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

For each end-device, the network server remembers the DevNonce values that were used before and ignores requests containing duplicate DevNonce values. In response to a join request, the server sends a join accept message.

Join Accept					
3 bytes	3 bytes	4 bytes	1 byte	1 byte	16 bytes
AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

where:

- **AppNonce** — rundom number.
- **NetID** — network identificator.
- **DevAddr** — device address in the network.
- **DLSettings** — parameters used for outgoing messages (server → device).
- **RxDelay** — delay between end of end-device transmission and start of Rx1 receive window (what are reception windows — LoRaWAN specification. Introduction. Basic concepts and end-device classes).
- **CFList** — list of additional frequency channels that can be used by the end-device.

The **DLSettings** field [8 bits] has the following format:

DLSettings		
7th byte	6...4 bytes	3...0 bytes
RFU	RX1DRoffset	RX2 Data rate

where:

- **RFU** — Reserved for Future Use, not used.
- **RX1DRoffset** — difference between uplink and downlink data rates used for the first Rx1 receive window. The default is 0.
- **RX2 Data rate** — the rate used for the second Rx2 receive window.

Random numbers **DevNonce** and **AppNonce** are used to calculate session keys **NwkSKey** and **AppSKey**.

ABP - Activation By Personalization

"Activation by Personalization" means that the **DevAddr**, **NwkSKey** and **AppSKey** values are directly written to the device (the device is personalized). According to the specification, each device must contain unique NwkSKey and AppSKey session key values so that the compromise of these values contained in one device does not lead to the compromise of other network devices.

With this activation method, the end-device does not need to go through the network join procedure, the device is ready for data transfer immediately after switching on.