

Table of Contents

| | |
|--|---|
| Спецификация LoRaWAN. Активация оконечных устройств | 3 |
| Процедура присоединения при активации OTAA - Over-The-Air Activation | 4 |
| Активация путем персонализации ABP - Activation By Personalization | 5 |

Спецификация LoRaWAN. Активация оконечных устройств

Чтобы присоединиться к сети LoRaWAN, оконечное устройство должно пройти процедуру активации (End-Device Activation). Спецификация предусматривает два варианта активации устройств:

- **ОТАА, Over-The-Air Activation** (требуется пройти процедуру присоединения (join procedure), во время которой вырабатываются сессионные ключи шифрования и адрес DevAddr).
- **АВР, Activation By Personalization** (не требуется проходить процедуру присоединения, ключи шифрования и адрес DevAddr записываются в устройство заранее (персонализация устройства))

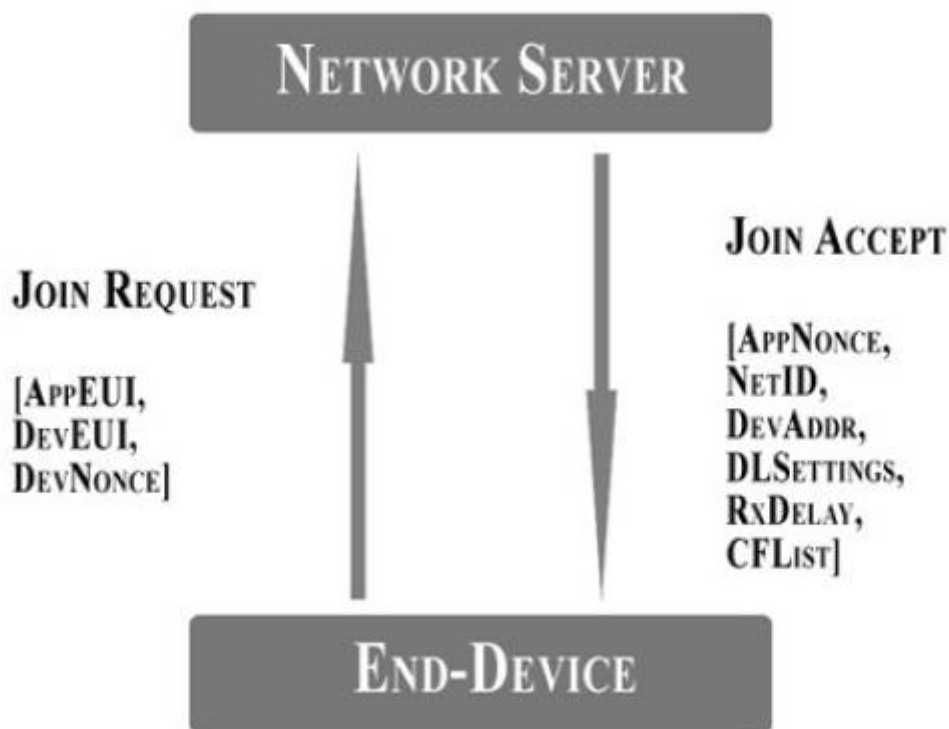
После активации устройство должно содержать следующие значения:

- **End-device address (DevAddr)** — локальный адрес устройства в данной сети [32 бита]. DevAddr состоит из двух полей: NwkID (идентификатор сети, биты 31...25) и NwkAddr (сетевой адрес, биты 24...0).
- **Network session key (NwkSKey)** — сетевой сессионный ключ [128 бит], используемый для расчета и проверки поля MIC (message integrity code) сообщений при обмене между оконечным устройством и сетевым сервером (Network Server), а также шифрования сообщений MAC-уровня.
- **Application session key (AppSKey)** — сессионный ключ [128 бит], используемый для шифрования данных на уровне приложения (между оконечным устройством и сервером приложения).
- Также устройство должно иметь идентификатор приложения [64 бита], который записывается заранее — **Application identifier (AppEUI)**



Процедура присоединения при активации OTAA - Over-The-Air Activation

Процедура присоединения всегда инициируется оконечным устройством и состоит из двух сообщений, которыми обмениваются оконечное устройство и сетевой сервер: **join request** (устройство → сервер) и **join accept** (сервер → устройство).



Сообщение join request содержит AppEUI, DevEUI и случайное число DevNonce:

| Join Request | | | | | |
|--------------|---------|---------|------------|---------|---------|
| 3 байта | 3 байта | 4 байта | 1 байт | 1 байт | 16 байт |
| AppNonce | NetID | DevAddr | DLSettings | RxDelay | CFList |

Для каждого оконечного устройства сетевой сервер запоминает значения DevNonce, которые использовались раньше, и игнорирует запросы, содержащие повторяющиеся значения DevNonce. В ответ на join request сервер посылает сообщение join accept.

| Join Accept | | | | | |
|-------------|---------|---------|------------|---------|---------|
| 3 байта | 3 байта | 4 байта | 1 байт | 1 байт | 16 байт |
| AppNonce | NetID | DevAddr | DLSettings | RxDelay | CFList |

где:

- **AppNonce** — случайное число.
- **NetID** — идентификатор сети.
- **DevAddr** — адрес устройства в сети.
- **DLSettings** — параметры, используемые для нисходящих сообщений (сервер →

устройство).

- **RxDelay** — задержка между окончанием передачи оконечного устройства и началом окна приема Rx1 (что такое окна приема — см. [Спецификация LoRaWAN. Введение. Основные понятия и классы оконечных устройств](#)).
- **CFList** — список дополнительных частотных каналов, которые могут использоваться оконечным устройством.

Поле **DLSettings** [8 бит] имеет следующий формат:

| DLSettings | | |
|-------------------|-------------|---------------|
| 7-й бит | биты 6...4 | биты 3...0 |
| RFU | RX1DRoffset | RX2 Data rate |

где:

- **RFU** — Reserved for Future Use, не используется.
- **RX1DRoffset** — разница между скоростями (data rates) на восходящей и нисходящей линиях, используемая для первого окна приема Rx1. По умолчанию равна 0.
- **RX2 Data rate** — скорость, используемая для второго окна приема Rx2.

Случайные числа **DevNonce** и **AppNonce** используются при вычислении сессионных ключей **NwkSKey** и **AppSKey**.

Активация путем персонализации ABP - Activation By Personalization

«Активация путем персонализации» означает, что в устройство напрямую записываются значения **DevAddr**, **NwkSKey** и **AppSKey** (происходит персонализация устройства). Согласно спецификации, каждое устройство должно содержать уникальные значения сессионных ключей NwkSKey и AppSKey, чтобы компрометация этих значений, содержащихся в одном устройстве, не приводила к компрометации других устройств сети.

При таком способе активации оконечному устройству не нужно проходить процедуру присоединения к сети, сразу после включения устройство готово к передаче данных.

Ссылка на оригинал статьи <https://habr.com/ru/post/317218/>

From:

<https://wiki.jooby.eu/> -

Permanent link:

https://wiki.jooby.eu/playground/ru/lorawan_spec_device_activation

Last update: **2023/04/14 18:33**