



LoRa Alliance™
Wide Area Networks for IoT



LoRaWAN™ 101

Технічне введення

Хто такі LoRa® Alliance?

- LoRa® Alliance є відкритим, некомерційним об'єднанням (<http://lora-alliance.org/>).
- Члени Alliance співпрацюють в просуванні на світовий ринок протоколу LoRaWAN™.
- **Місія:** стандартизувати енергоефективні мережі далекого радіусу дії.
- **“ДОЗВОЛЯЄМО РЕЧАМ МАТИ ГОЛОС У ВСЬОМУ СВІТІ”**

Комітет зі стратегії

Дорожня карта і безпека



Технічний комітет

Специфікації й оновлення функцій

Комітет з маркетингу

Бренд, ЗМІ, виставки-ярмарки, дні відкритих дверей

Комітет з

сертифікації

Тестування та акредитація

LoRa-Alliance.org



Оновлення специфікації

- LoraWAN™ 1.0.0 -> 1.0.1 -> 1.0.2 -> 1.1
 - 1.0.2 зараз на остаточному розгляді, реліз в цьому кварталі
 - Уточнення, що дозволяють запустити програму сертифікації NA
 - Переміщення регіональних параметрів в окремий документ
 - Набагато легше просуватися поза процесом IPR
 - Швидке збільшення числа охоплених країн
 - Додає підтримку кластеру країн ATP
 - Команди для зміни регіональних частот і потужностей передавачів
 - Специфікацію можна зараз безкоштовно завантажити
<https://www.lora-alliance.org/Contact/RequestSpecificationForm.aspx>



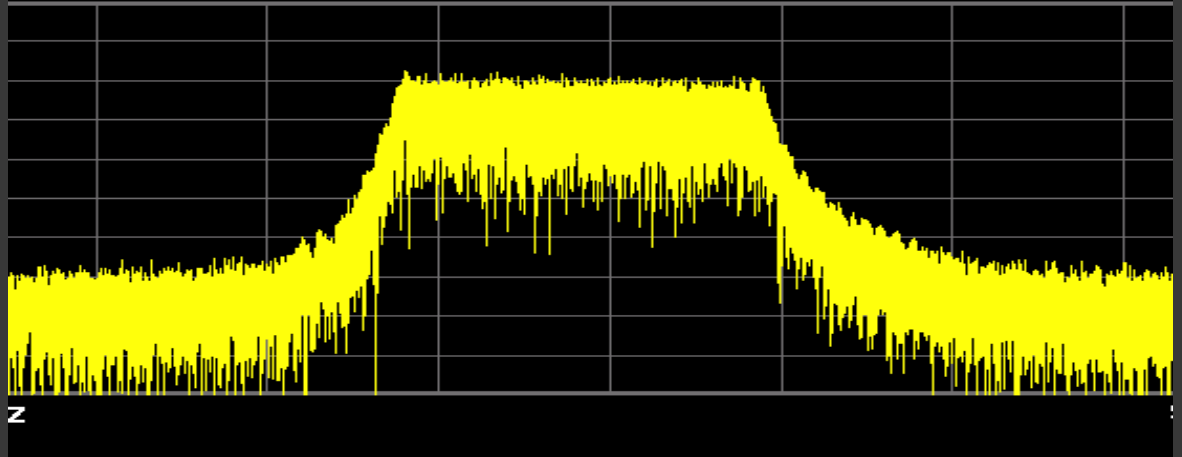
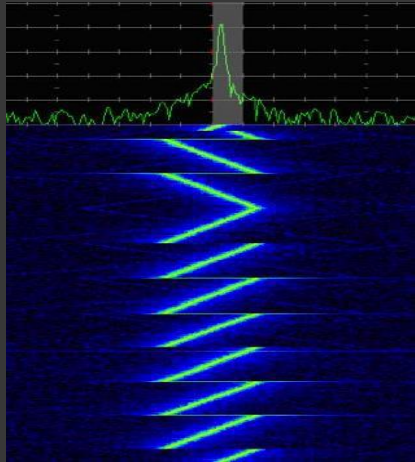
Оновлення специфікації

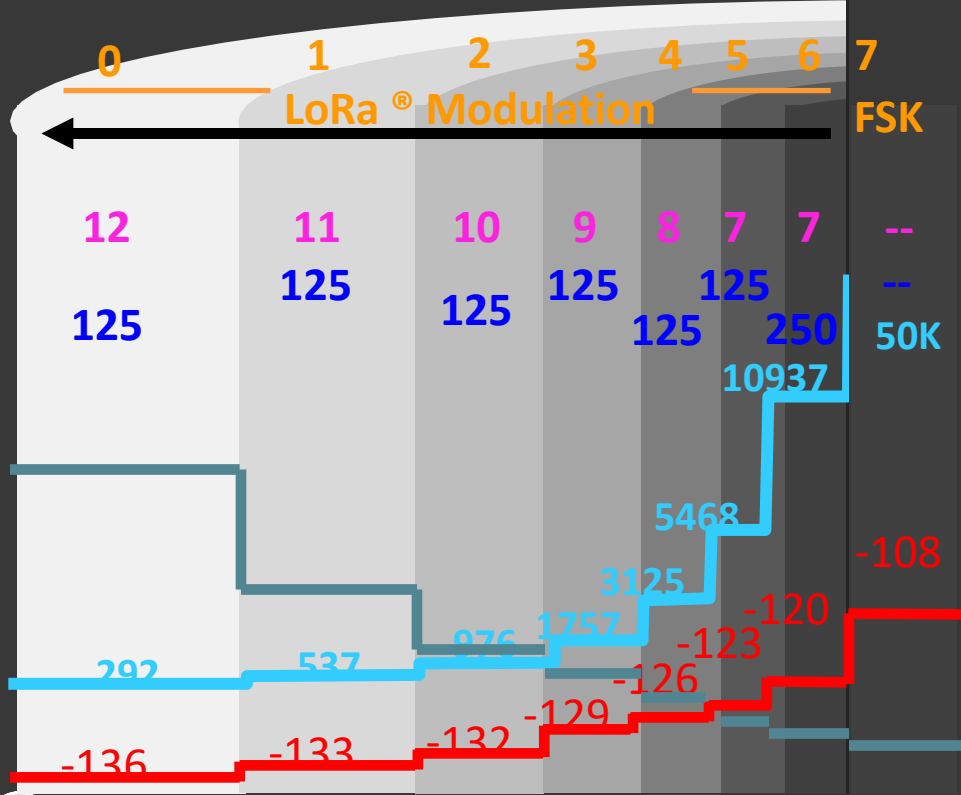
- LoraWAN™ 1.0.0 -> 1.0.1 -> 1.0.2 -> 1.1
- 1.1 в розробці, термін виконання - середина 2017 р.
- Доповнення:
 - Можливості роумінгу пасивного і через хендовер
 - Роз'яснення щодо класу B
 - Тимчасове перемикання класу A/C
- Необхідність стандартизації внутрішніх інтерфейсів
- Alliance дотримується принципу сумісності з попередніми версіями.



- **Технологія розширеного спектру**

- Розробка Semtech Corporation (<http://www.semtech.com/>)
- Лінійна частотна модуляція, символи частоти, що лінійно змінюється
- Виграш від обробки = збільшена чутливість при прийомі
- Більший діапазон за рахунок зниження швидкості передачі даних





Швидкість передачі даних (DR)

Діапазон

Коефіцієнт розширення (SF)

Смуга пропускання (BW) (кГц)

Швидкість передачі бітів (BR) (біт/с)

Чутливість при прийомі (дБм)

Час в ефірі та споживання



ADR = Адаптивна швидкість передачі даних

- LoRaWAN може автоматично керувати коефіцієнтом **SF** для кожного кінцевого пристрою:
 - Для оптимізації для отримання максимальної швидкості передачі даних в порівнянні з діапазоном
 - Для збільшення до максимуму терміну служби батареї і
 - Для досягнення максимальної місткості мережі



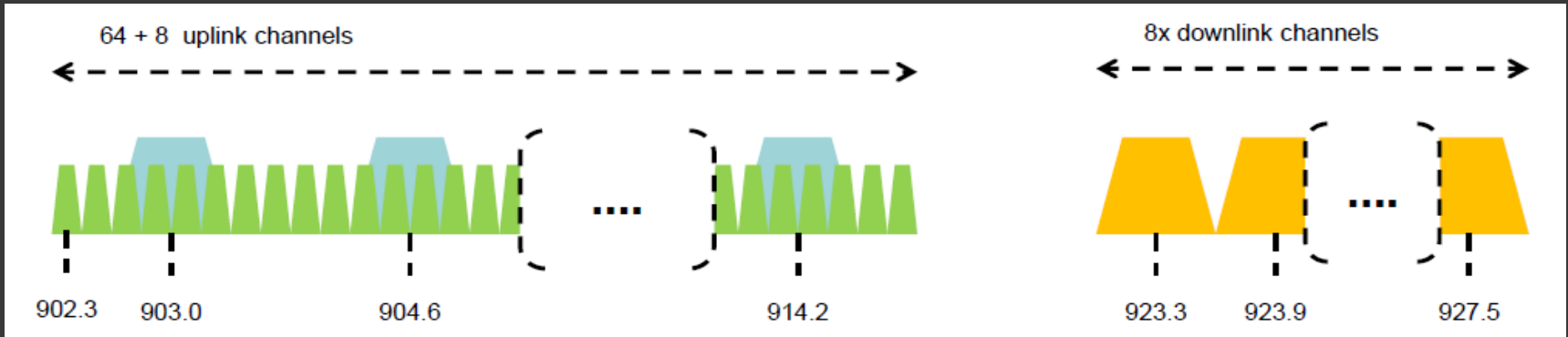
- Неліцензовані частоти субгігагерцового діапазону
 - Європа: 868 МГц
 - Канали мережі можуть вільно присвоюватися оператором мережі
 - 3 обов'язкові канали, які повинні постійно отримувати всі шлюзи:

Modulation	Bandwidth [kHz]	Channel Frequency [MHz]	FSK Bitrate or LoRa DR / Bitrate	Nb Channels	Duty cycle
LoRa	125	868.10 868.30 868.50	DR0 to DR5 / 0.3-5 kbps	3	<1%

- Шлюзи ЄС зазвичай використовують 8 каналів
- Кінцеві пристрої повинні мати не менше 16 каналів



- Неліцензовані частоти субгігагерцового діапазону
 - Північна Америка: 915 МГц
 - Висхідні: 64 канали з номерами від 0 до 63, DR0-DR3
 - Висхідні: 8 каналів з номерами від 64 до 71, DR4
 - Низхідні: 8 каналів з номерами від 0 до 7, DR8-DR13





- **Енергоефективна мережа далекого радіусу дії (LPWAN)**

- **Двонаправлена**, визнана
- **Проста** топологія мережі «зірка»
- Низька швидкість передачі даних
- Низька вартість
- Тривалий термін служби батареї
- Далекий діапазон дії (**Long Range**)

Проста архітектура мережі:

- **Без ретрансляторів**
- **Без комірчастої топології**

- **Області застосування:**

- Інтернет речей (**IoT**) і міжмашинна взаємодія (**M2M**)
- Промислова автоматизація
- Застосунки з низьким енергоспоживанням
- Батарейні давачі
- Розумне місто, сільське господарство, облік, вуличне освітлення

Топологія мережі LoRaWAN™





Безпека мережевого протоколу LoRaWAN™

- На основі стандарту безпеки 802.15.4
 - AES-128
- Удосконалення:
 - Сеансовий ключ мережі (NwkSKey)
 - Сеансовий ключ застосунку (AppSKey)

Логічна модель даних (Модель програміста)

Кінцеві пристрої



Радіочастоти
субгігагерцового діапазону

Мережевий
сервер



Сервер
застосунків



IP



IP

Керуючі
дані

Сеансовий ключ мережі (NwkSKey)



Сеансовий ключ застосунку (AppSKey)



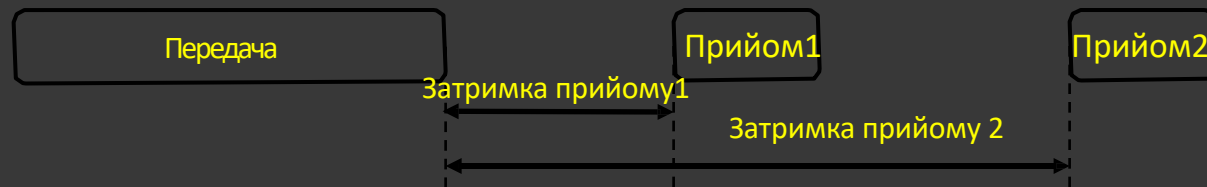
Керуючі
дані



- Кожен клас кінцевого пристрою має різні особливості в залежності від вибору оптимізації:
 - Живлення від батареї – Клас **A**
 - Мала затримка – Клас **B**
 - Без затримки – Клас **C**

• Живлення від батареї – Клас А

- Двонаправлена передача даних
- Одноадресні повідомлення
- Малий обсяг корисних даних, тривалі інтервали
- Кінцевий пристрій ініціює передачу даних (висхідний канал)
- Сервер взаємодіє з кінцевим пристроєм (низхідний канал) в заздалегідь визначені моменти часу:





• Мала затримка – Клас В

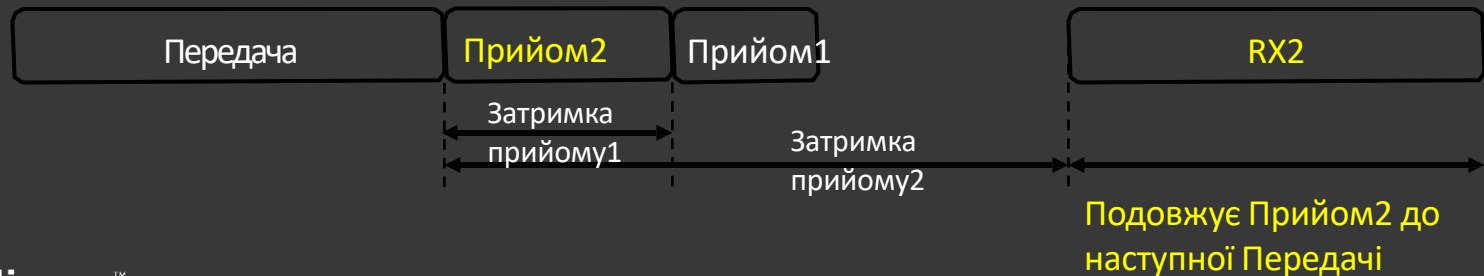
- Двонаправлена передача даних з часом прийому, передбаченим графіком
- Одноадресні й **багатоадресні** повідомлення
- Малий обсяг корисних даних, тривалі інтервали
- **Періодичні маяки** від шлюзу
- Додаткове вікно прийому (ping slot)
- Сервер може ініціювати передачу даних у визначені інтервали часу





- Без затримки – **Клас С**

- Двонаправлена передача даних
- Одноадресні й **багатоадресні** повідомлення
- Малий обсяг корисних даних
- **Сервер може ініціювати передачу даних у будь-який момент часу**
- Кінцевий пристрій завжди перебуває у Прийомі





- Перш ніж кінцевий пристрій зможе здійснювати передачу даних у мережі LoRaWAN, він повинен бути **активованим**.
- Потрібна наступна інформація:
 - Адреса пристрою (**DevAddr**)
 - Сеансовий ключ мережі (**NwkSKey**)
 - Сеансовий ключ застосунку (**AppSKey**)

Зупинимося на кожному з них детально...



- Адреса пристрою (**DevAddr**)
 - 32-бітний ідентифікатор
 - Унікальна в межах мережі
 - Присутня в кожному кадрі даних
 - Загальнодоступна для кінцевого пристрою, мережевого сервера і сервера застосунків
- Відрізняє вузли в мережі, дозволяючи мережі використовувати правильні ключі шифрування і правильно інтерпретувати дані



- Сеансовий ключ мережі (**NwkSKey**)
 - **128-бітний** ключ шифрування **AES**
 - **Унікальний для кожного кінцевого пристрою**
 - **Загальнодоступний для кінцевого пристрою і мережевого сервера**
- **Забезпечує цілісність повідомлень під час передачі даних**
- **Забезпечує безпеку передачі даних на рівні Кінцевий пристрій <-> Мережевий сервер**



- Сеансовий ключ застосунку (**AppSKey**)
 - **128-бітний** ключ шифрування **AES**
 - **Унікальний для кожного кінцевого пристрою**
 - **Загальнодоступний для кінцевого пристрою і сервера застосунків**
 - Використовується для шифрування/дешифрування інформаційних повідомлень застосунку
- **Забезпечує безпеку корисних даних застосунку**



- Для обміну цією інформацією доступні **два способи активації**:

Активация бездротовим способом (ОТАА)

- На основі глобально унікального ідентифікатора
- Квитування повідомлення по бездротовій мережі



Активация шляхом персоналізації (АВР)

- Загальнодоступні ключі прошиваються на етапі виробництва
- Прив'язка до певної мережі





Активація бездротовим способом (ОТАА)

- Кінцевий пристрій передає на сервер застосунків **Запит на підключення**, який містить:
 - Глобально унікальний ідентифікатор кінцевого пристрою (**DevEUI**)
 - Ідентифікатор застосунку (**AppEUI**)
 - Аутентифікацію за допомогою ключа застосунку (**AppKey**)
- Сервер застосунків відправляє кінцевому пристрою **Дозвіл на підключення**

(продовження...)



Активація бездротовим способом (ОТАА)

- Кінцевий пристрій аутентифікує **Дозвіл на підключення**
- Кінцевий пристрій **розшифровує** Дозвіл на підключення
- Кінцевий пристрій витягує і запам'ятовує Адресу пристрою (**DevAddr**)
- Кінцевий пристрій **витагує**:
 - Сеансовий ключ мережі (**NwkSKey**)
 - Сеансовий ключ застосунку (**AppSKey**)

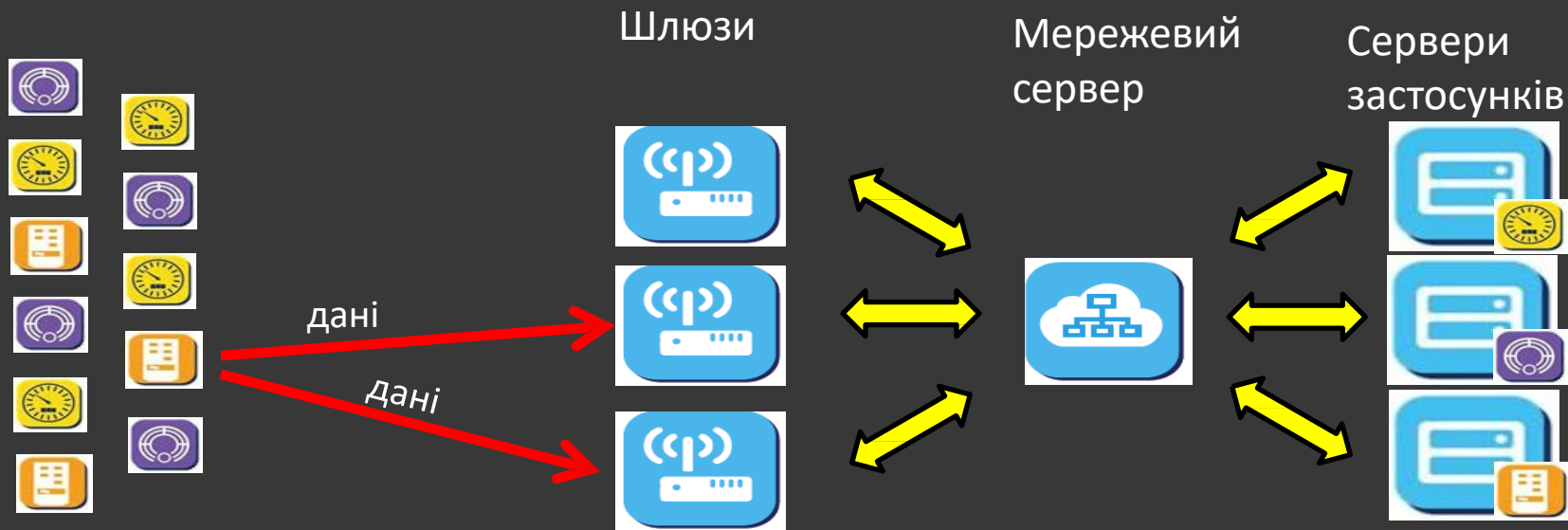
Ключі безпеки



Активація шляхом персоналізації (ABP)

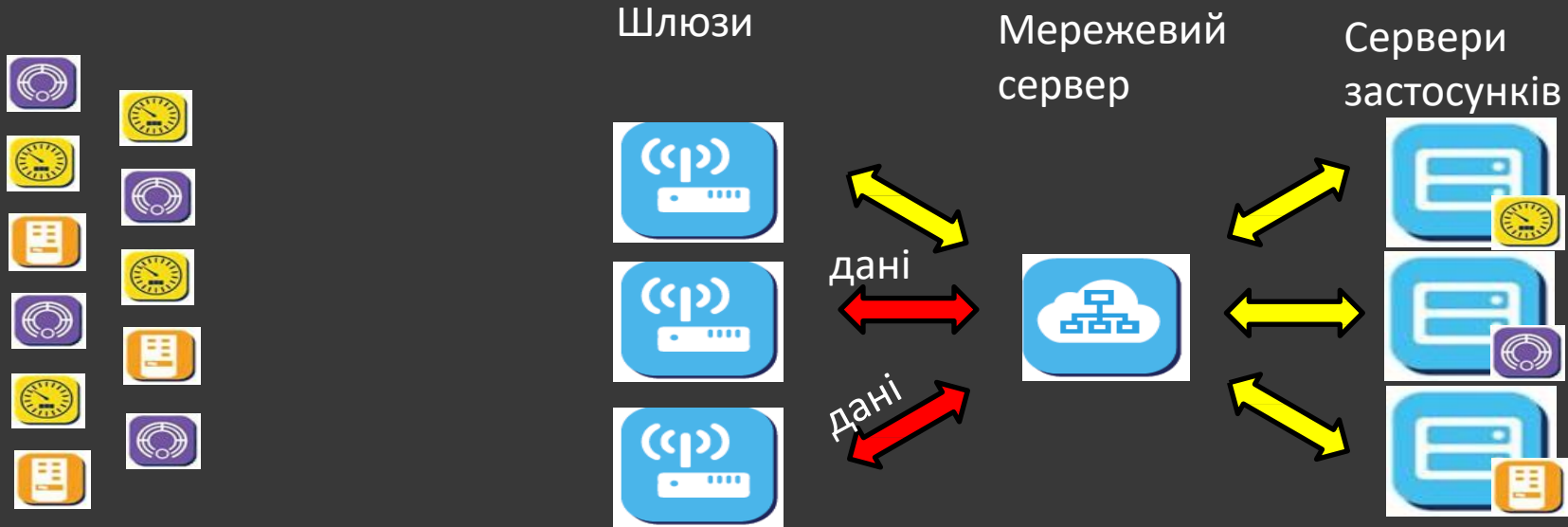
- На етапі виробництва конфігурується така інформація:
 - Адреса пристрою (**DevAddr**)
 - Сеансовий ключ мережі (**NwkSKey**)
 - Сеансовий ключ застосунку (**AppSKey**)
- **Відсутнє** квітування по бездротовій мережі
- Пристрій готовий до передачі даних в мережі без будь-якої додаткової процедури.

Повідомлення з підтвердженням



1. Торговий апарат передає дані, які приймаються двома шлюзами.

Повідомлення з підтвердженням



2. Обидва шлюзи пересилають дані на мережевий сервер.

Повідомлення з підтвердженням



3. Мережевий сервер пересилає дані серверу застосунків торгового апарата.

Повідомлення з підтвердженням



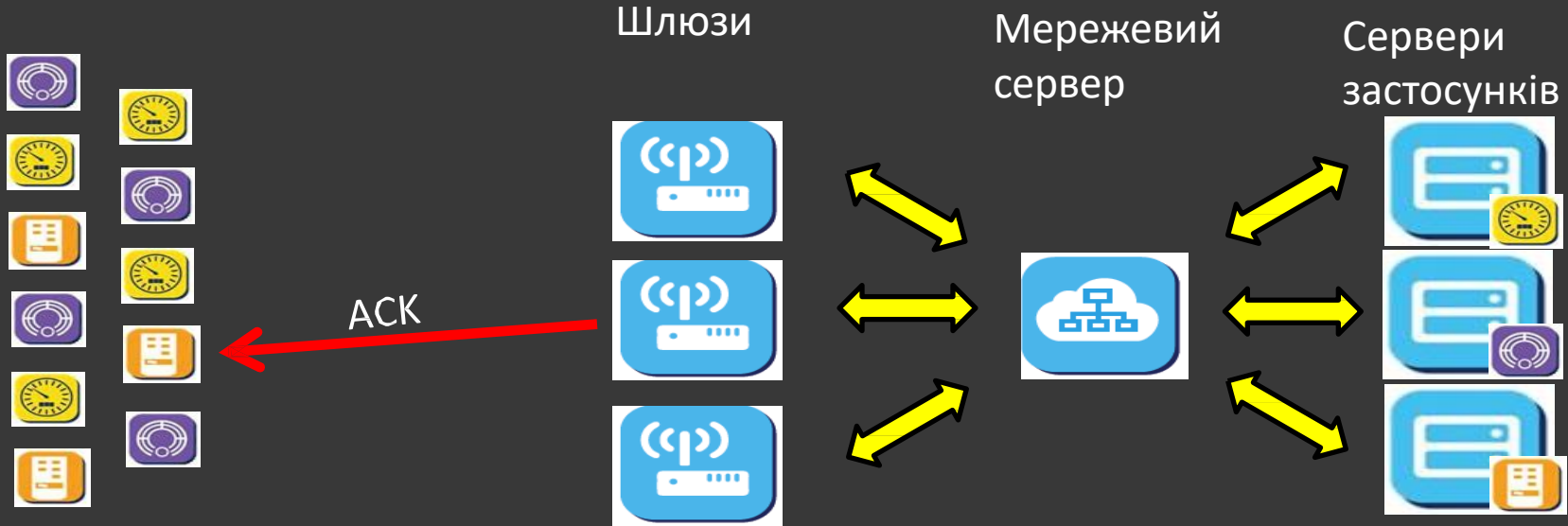
4. Сервер застосунків торгового апарата відправляє підтвердження.

Повідомлення з підтвердженням



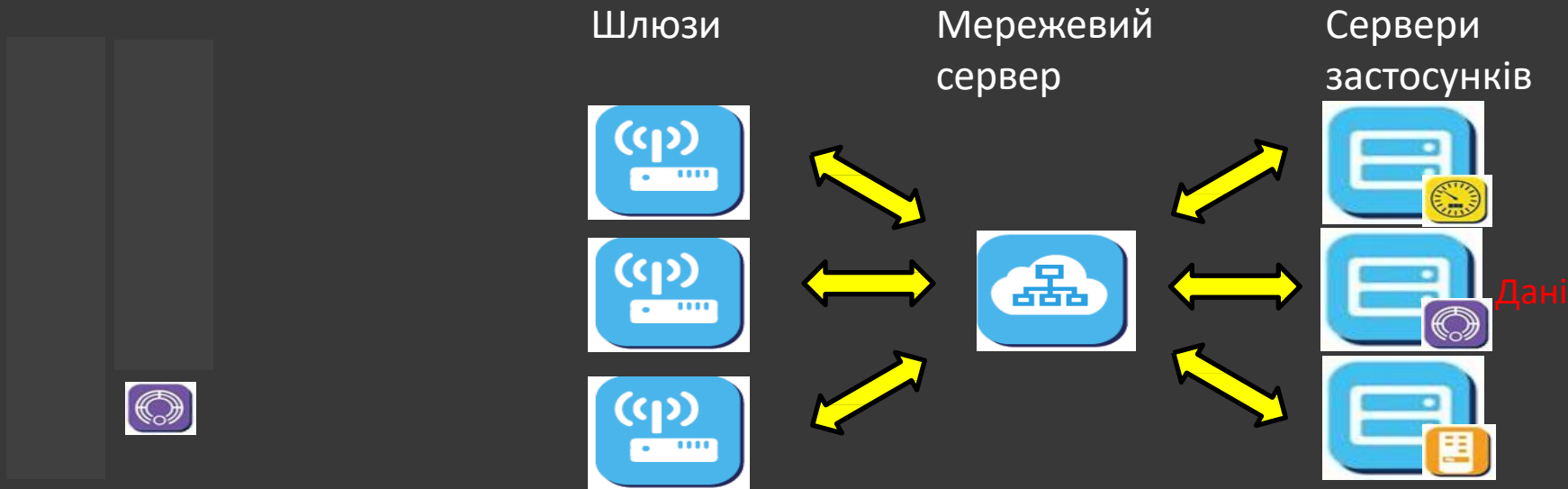
5. Мережевий сервер вибирає найкращий маршрут (шлюз) для відправлення підтвердження кінцевому пристрою.

Повідомлення з підтвердженням



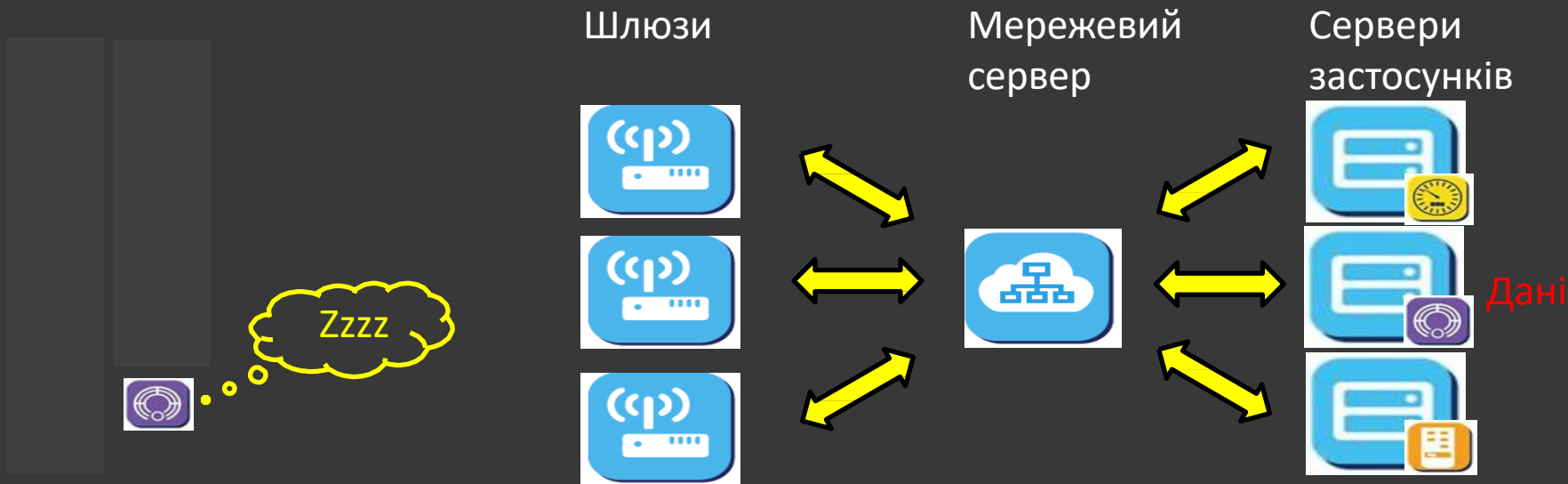
6. Шлюз пересилає підтвердження кінцевому пристрою.

Повідомлення від сервера застосунків



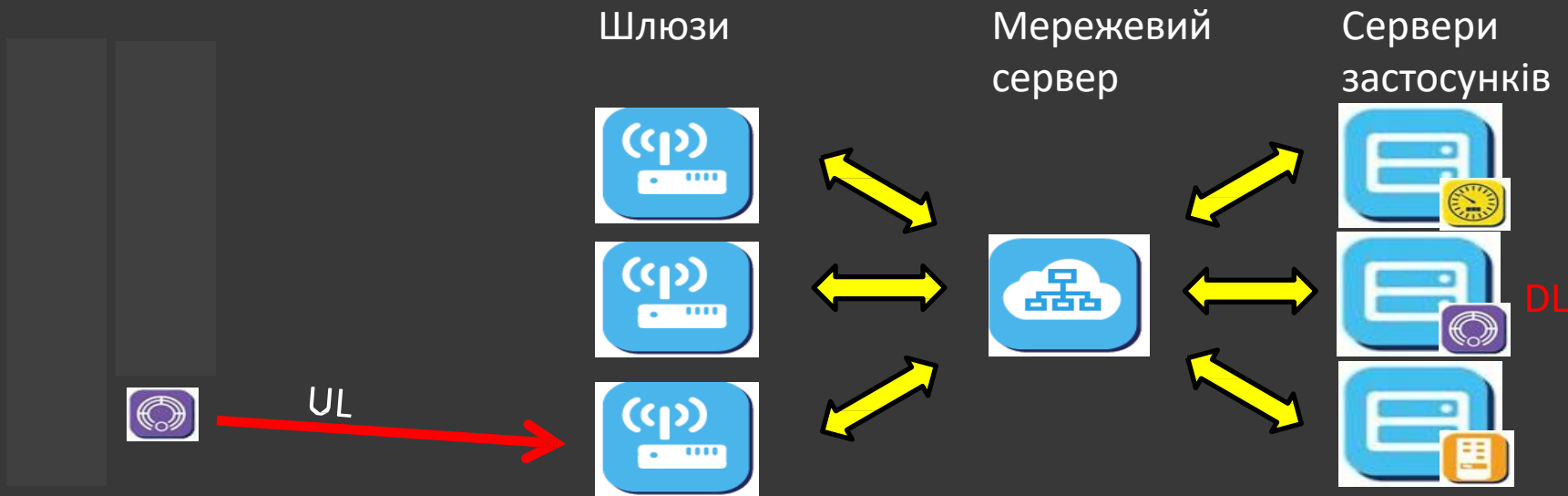
1. Сервер застосунків давача диму має дані для певного давача диму.

Повідомлення від сервера застосунків



2. Однак він повинен почекати, поки давач диму не прокинеться і не передасть повідомлення.

Повідомлення від сервера застосунків



3. При передачі датчиком диму повідомлення переміщується по висхідному каналу.

Повідомлення від сервера застосунків



4. Проходить через шлюз...

Повідомлення від сервера застосунків



5. ... і пересилається мережевим сервером серверу застосунків давача диму.

Повідомлення від сервера застосунків



6. Сервер застосунків давача диму може тепер відправити повідомлення давачу диму.

Повідомлення від сервера застосунків



7. Мережевий сервер відправляє повідомлення відповідному шлюзу.



LoRa Alliance™

Wide Area Networks for IoT



Дякуємо. Приєднуйтеся до нас...

LoRa Alliance™

“ДОЗВОЛЯЄМО РЕЧАМ МАТИ ГОЛОСУ ВСЬОМУ СВІТІ”