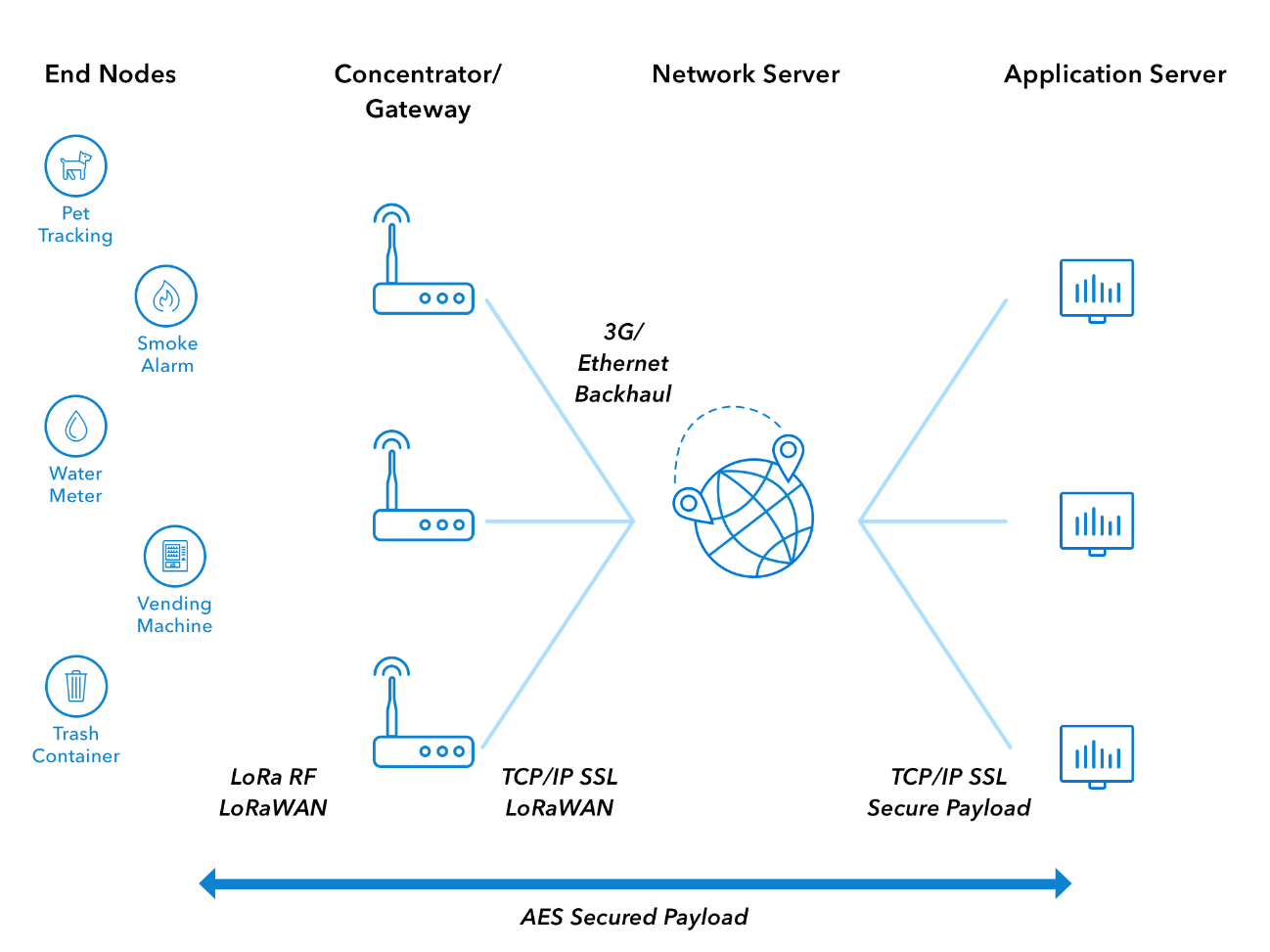
Background information about LoRaWAN

LoRaWAN Overview

LoRaWAN is a media access control (MAC) protocol for wide area networks. It is designed to allow low-powered devices to communicate with Internet-connected applications over long range wireless connections. LoRaWAN can be mapped to the second and third layer of the OSI model. It is implemented on top of LoRa or FSK modulation in industrial, scientific and medical (ISM) radio bands. The LoRaWAN protocols are defined by the [LoRa Alliance](https://www.lora-alliance.org/) and formalized in the LoRaWAN Specification which can be [downloaded](https://www.lora-alliance.org/lorawan-for-developers) on the LoRa Alliance website.

 *Image: LoRaWAN Architecture*

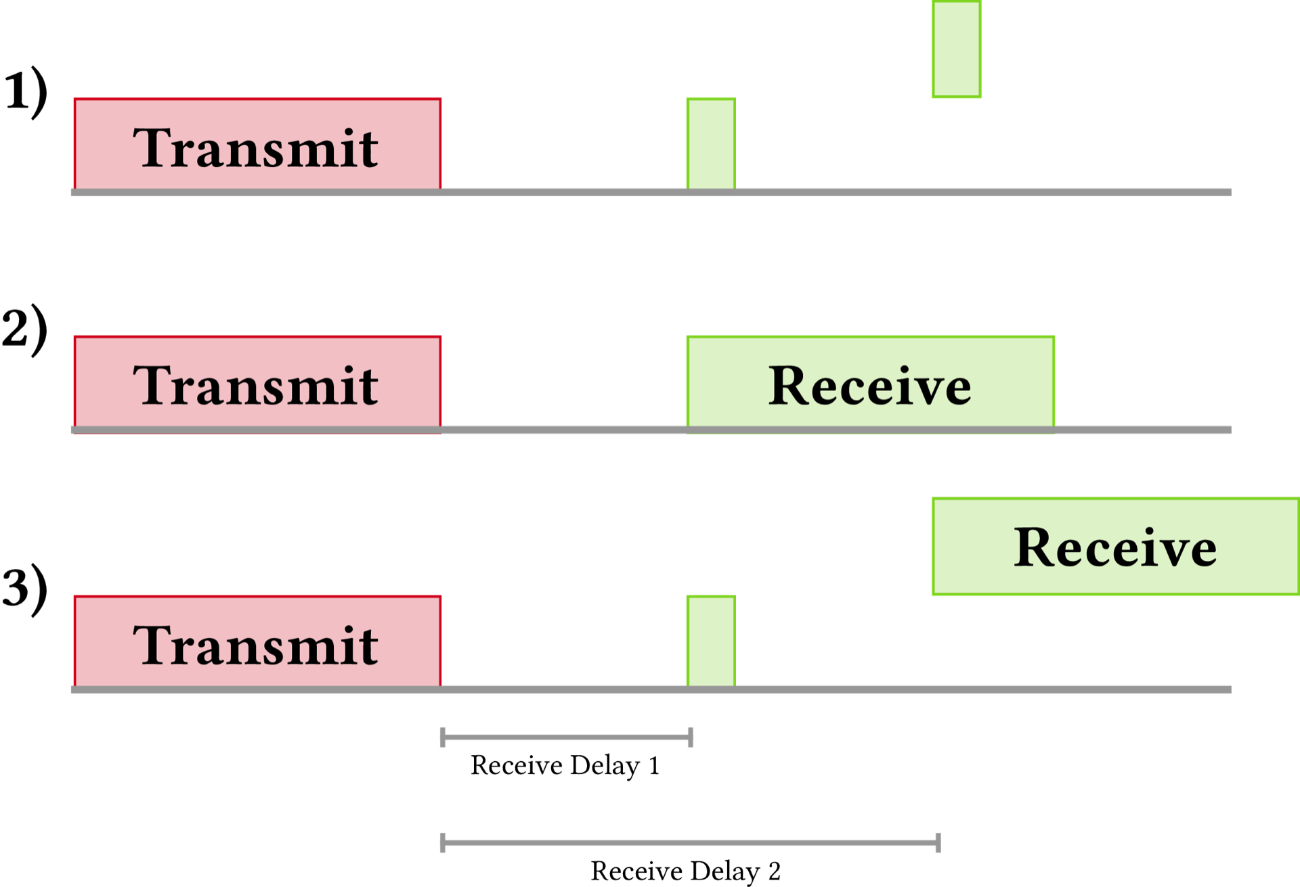
Terminology

* [**End Device, Node, Mote**](https://www.thethingsnetwork.org/docs/devices/) - an object with an embedded low-power communication device.
* [**Gateway**](https://www.thethingsnetwork.org/docs/gateways/) - antennas that receive broadcasts from End Devices and send data back to End Devices.
* [**Network Server**](https://www.thethingsnetwork.org/docs/network/) - servers that route messages from End Devices to the right Application, and back.
* **Application** - a piece of software, running on a server.
* **Uplink Message** - a message from a Device to an Application.
* **Downlink Message** - a message from an Application to a Device.

End Devices

The LoRaWAN specification defines three device types. All LoRaWAN devices must implement Class A, whereas Class B and Class C are extensions to the specification of Class A devices.

**Class A** devices support bi-directional communication between a device and a gateway. Uplink messages (from the device to the server) can be sent at any time (randomly). The device then opens two receive windows at specified times (1s and 2s) after an uplink transmission. If the server does not respond in either of these receive windows (situation 1 in the figure), the next opportunity will be after the next uplink transmission from the device. The server can respond either in the first receive window, or in the second receive window, but should not use both windows.



**Class B** devices extend Class A by adding scheduled receive windows for downlink messages from the server. Using time-synchronized beacons transmitted by the gateway, the devices periodically open receive windows.

**Class C** devices extend Class A by keeping the receive windows open unless they are transmitting, as shown in the figure below. This allows for low-latency communication but is many times more energy consuming than Class A devices.



Frequency Bands

LoRaWAN operates in unlicensed radio spectrum. This means that anyone can use the radio frequencies without having to pay million dollar fees for transmission rights. It is similar to WiFi, which uses the 2.4GHz and 5GHz ISM bands worldwide. Anyone is allowed to set up WiFi routers and transmit WiFi signals without the need for a license or permit.

LoRaWAN uses lower radio frequencies with a longer range. The fact that frequencies have a longer range also comes with more restrictions that are often country-specific. This poses a challenge for LoRaWAN, that tries to be as uniform as possible in all different regions of the world. As a result, LoRaWAN is specified for a number of bands for these regions. These bands are similar enough to support a region-agnostic protocol, but have a number of consequences for the implementation of the backend systems.

* LoRaWAN has official regional specifications, called **Regional Parameters**, that you can download from the [LoRa Alliance website](https://lora-alliance.org/lorawan-for-developers).
* These LoRaWAN regional specifications do not specify everything either. They only cover a region by specifying the common denominator. For example, the LoRaWAN regional parameters for Asia only specify a common subset of channels - but there are variations between regulations in Asian countries. Furthermore, each network server operator is free to select additional parameters, such as additional emission channels. We call these parameters **Frequency Plans**. For The Things Network, they are defined in [this GitHub repository](https://github.com/TheThingsNetwork/gateway-conf).

EU 863-870 MHz and Duty Cycle

In Europe, LoRaWAN operates in the 863-870 MHz frequency band. European frequency regulations impose specific duty-cycles on devices for each sub-band. These apply to each device that transmits on a certain frequency, so both gateways and devices have to respect these duty-cycles. Most channels used by LoRaWAN have a duty-cycle as low as 1% or even 0.1%. As a result, the network should be smart in scheduling messages on gateways that are less busy or on channels that have a higher duty-cycle. Application developers are encouraged to keep their payloads small, do not transmit too often and avoid downlink messages if possible.

US 902-928 MHz

In the United States, LoRaWAN operates in the 902-928 MHz frequency band. Unlike the European band, the US band has dedicated uplink and downlink channels. The band is divided into 8 sub-bands that each have 8x125 kHz uplink channels, 1x500 kHz uplink channel and 1x500 kHz downlink channel. The Things Network uses the second sub-band (number 1 if you start counting at 0).

Australia 915-928 MHz

The specification of the Australian 915-928 MHz band is practically the same as the US 902-928 MHz, except that its uplink frequencies are on higher frequencies than in the US band. Its downlink channels are the same as in the US 902-928 MHz band. The Things Network uses the second sub-band (number 1 if you start counting at 0).

China 779-787 MHz and 470-510 MHz

The Chinese 779-787 MHz band behaves similar to the European bands. The 779-787 MHz band also has three common 125 kHz channels (779.5, 779.7 and 779.9 MHz). The Chinese 470-510 MHz band behaves similar to the US bands. There are 96 uplink channels and 48 downlink channels. In some regions, a subset of these channels is used by China Electric Power and can therefore not be used for LoRaWAN. The Things Network uses the eleventh sub-band (number 10 if you start counting at 0).

Modulation and Data Rate

In most cases LoRaWAN uses LoRa modulation. LoRa modulation is based on Chirp spread- spectrum technology, which makes it work well with channel noise, multipath fading and the Doppler effect, even at low power.

The data rate depends on the used bandwidth and spreading factor. LoRaWAN can use channels with a bandwidth of either 125 kHz, 250 kHz or 500 kHz, depending on the region or the frequency plan. The spreading factor is chosen by the end-device and influences the time it takes to transmit a frame.

**The Data Rate Story**: There are three knobs you can turn: transmission power, bandwidth and spreading factor. If you lower the tx power, you’ll save battery, but the range of the signal will obviously be shorter. The other two knobs combined form the data rate. This determines how fast bytes are transmitted. If you increase the data rate (make the bandwidth wider or the spreading factor lower) you can transmit those bytes in a shorter time. For those, the calculation is approximately as follows: Making the bandwidth 2x wider (from BW125 to BW250) allows you to send 2x more bytes in the same time. Making the spreading factor 1 step lower (from SF10 to SF9) allows you to send 2x more bytes in the same time. Lowering the spreading factor makes it more difficult for the gateway to receive a transmission, as it will be more sensitive to noise. You could compare this to two people taking in a noisy place (a bar for example). If you’re far from each other, you have to talk slow (SF10), but if you’re close, you can talk faster (SF7)

Addressing

Devices and applications have a 64 bit unique identifier (DevEUI and AppEUI). When a device joins the network, it receives a dynamic (non-unique) 32-bit address (DevAddr).

Security

LoRaWAN 1.0 knows three distinct 128-bit security keys. The application key AppKey is only known by the device and by the application. When a device joins the network (this is called a join or activation), an application session key AppSKey and a network session key NwkSKey are generated. The NwkSKey is shared with the network, while the AppSKey is kept private. These session keys will be used for the duration of the session.

The algorithm used for this is AES-128, similar to the algorithm used in the 802.15.4 standard. The NwkSKey is used to validate the integrity of each message by its Message Integrity Code (MIC). This MIC is similar to a checksum, except that it prevents intentional tampering with a message. For this, LoRaWAN uses AES-CMAC. The AppSKey is used for encryption of the application payload.

See [Security](https://www.thethingsnetwork.org/docs/lorawan/security.html) for more information.

Frame Counters

Frame Counters prevent replay attacks where an attacker re-transmits a previously recorded message. To prevent this, the network and the device must both reject messages that contain a frame counter that is lower than the expected frame counter.

MAC Commands

The network server and device can perform network-related administration and management using MAC commands. The LoRaWAN specification specifies a number of commands that can be extended in future versions of LoRaWAN or extended with proprietary commands. There are commands for checking connectivity, requesting the status of a device, adapting the data rate of a device, and modifying channel settings.