LoRa

LoRa

- LoRa is a wireless modulation technique derived from Chirp Spread Spectrum (CSS) technology.

- It encodes information on radio waves using chirp pulses - similar to the way dolphins and bats communicate! LoRa modulated transmission is robust against disturbances and can be received across great distances.

- LoRa is ideal for applications that transmit small chunks of data with low bit rates. Data can be transmitted at a longer range compared to technologies like WiFi, Bluetooth or ZigBee. These features make LoRa well suited for sensors and actuators that operate in low power mode.

- LoRa can be operated on the license free sub-gigahertz bands, for example, 915 MHz, 868 MHz, and 433 MHz. It also can be operated on 2.4 GHz to achieve higher data rates compared to sub-gigahertz bands, at the cost of range. These frequencies fall into ISM bands that are reserved internationally for industrial, scientific, and medical purposes.

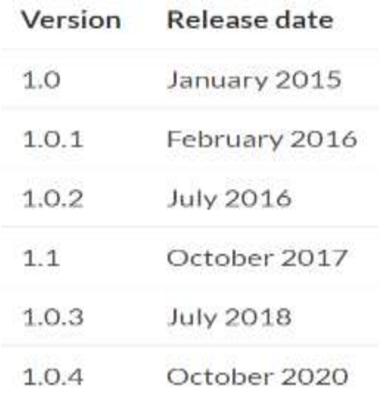
- LoRa devices enable smart IoT applications that solve some of the biggest challenges facing our planet: energy management, natural resource reduction, pollution control, and infrastructure efficiency.

LoRaWAN

- LoRaWAN is a Media Access Control (MAC) layer protocol built on top of LoRa modulation. It is a software layer which defines how devices use the LoRa hardware, for example when they transmit, and the format of messages.

- LoRaWAN is an open networking protocol that delivers secure bi-directional communication, mobility, and localization services standardized and maintained by the LoRa Alliance.

- The first LoRaWAN specification was released in January 2015.

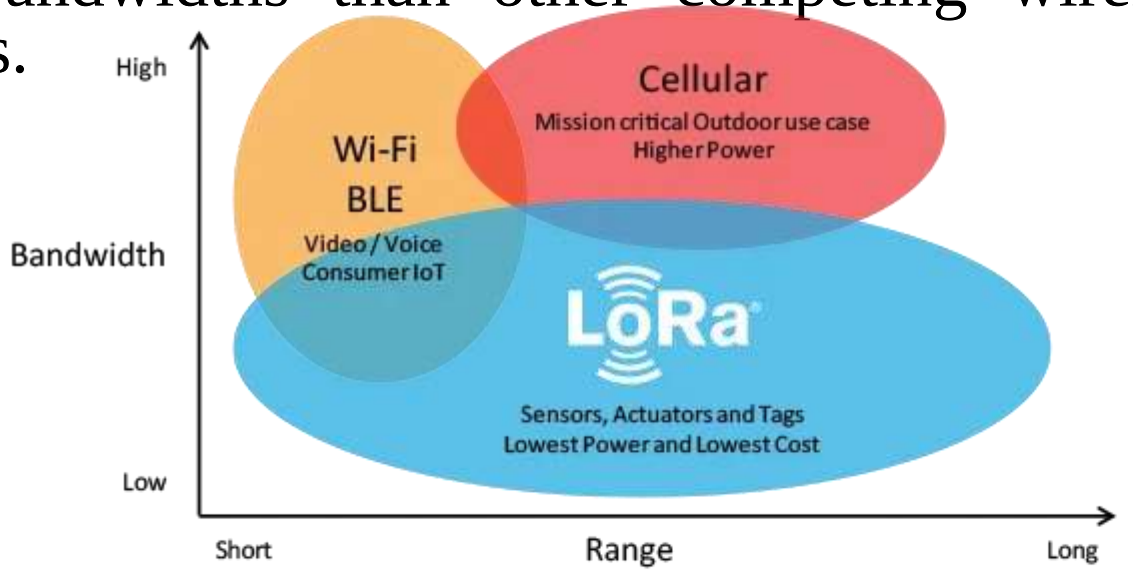


Version	Release date
1.0	January 2015
1.0.1	February 2016
1.0.2	July 2016
1.1	October 2017
1.0.3	July 2018
1.0.4	October 2020

- The table above shows the version history of the LoRaWAN specifications. At the time of this writing the latest specifications are 1.0.4 (in 1.0 series) and 1.1 (1.1 series).

Bandwidth vs. Range

- LoRaWAN is suitable for transmitting small size payloads (like sensor data) over long distances.
- LoRa modulation provides a significantly greater communication range with low bandwidths than other competing wireless data transmission technologies.


High
Bandwidth
Low
Wi-Fi
BLE
Video / Voice
Consumer IoT
Cellular
Mission critical Outdoor use case
Higher Power
LoRa
Sensors, Actuators and Tags
Lowest Power and Lowest Cost
Short
Range
Long

- The figure shows some access technologies that can be used for wireless data transmission and their expected transmission ranges vs. bandwidth.

Why LoRaWAN ?

Accura Tequipment

- **Ultra low power** - LoRaWAN end devices are optimized to operate in low power mode and can last up to 10 years on a single coin cell battery.
- **Long range** - LoRaWAN gateways can transmit and receive signals over a distance of over 10 kilometers in rural areas and up to 3 kilometers in dense urban areas.
- **Deep indoor penetration** - LoRaWAN networks can provide deep indoor coverage, and easily cover multi floor buildings.
- **License free spectrum** - You don’t have to pay expensive frequency spectrum license fees to deploy a LoRaWAN network.
- **Geolocation**- A LoRaWAN network can determine the location of end devices using triangulation without the need for GPS. A LoRa end device can be located if at least three gateways pick up its signal.
- **High capacity** - LoRaWAN Network Servers handle millions of messages from thousands of gateways.

Accura Tequipment

- **Public and private deployments -** It is easy to deploy public and private LoRaWAN networks using the same hardware (gateways, end devices, antennas) and software (UDP packet forwarders, Basic Station software, LoRaWAN stacks for end devices).
- **End-to-end security-** LoRaWAN ensures secure communication between the end device and the application server using AES-128 encryption.
- **Firmware updates over the air -** You can remotely update firmware (applications and the LoRaWAN stack) for a single end device or group of end devices.
- **Roaming-** LoRaWAN end devices can perform seamless handovers from one network to another.
- **Low cost -** Minimal infrastructure, low-cost end nodes and open source software.
- **Certification program-** The LoRa Alliance certification program certifies end devices and provides end-users with confidence that the devices are reliable and compliant with the LoRaWAN specification.
- **Ecosystem-** LoRaWAN has a very large ecosystem of device makers, gateway makers, antenna makers, network service providers, and application developers.

LoRaWAN use cases

Accura Tequipment

LoRaWAN can be applied:

- **Vaccine cold chain monitoring** - LoRaWAN sensors are used to ensure vaccines are kept at appropriate temperatures in transit.
- **Animal conservation** - Tracking sensors manage endangered species such as Black Rhinos and Amur Leopards.
- **Dementia patients** - Wristband sensors provide fall detection and medication tracking.
- **Smart farms-** Real time insights into crop soil moisture and optimized irrigation schedule reduce water use up to 30%.
- **Water conservation-** Identification and faster repair of leaks in a city's water network.

Accura Tequipment

- **Food safety**- Temperature monitoring ensures food quality maintenance.
- **Smart waste bins** - Waste bin level alerts sent to staff optimize the pickup schedule.
- **Smart bikes**- Bike trackers track bikes in remote areas and dense buildings.
- **Airport tracking** - GPS-free tracking monitors vehicles, personnel, and luggage.
- **Efficient workspaces** - Room occupancy, temperature, energy usage and parking availability monitoring.
- **Cattle health** - Sensors monitor cattle health, detect diseases and forecast calves delivery time.
- **LoRa in space** - Satellites to provide LoRaWAN-based coverage worldwide.

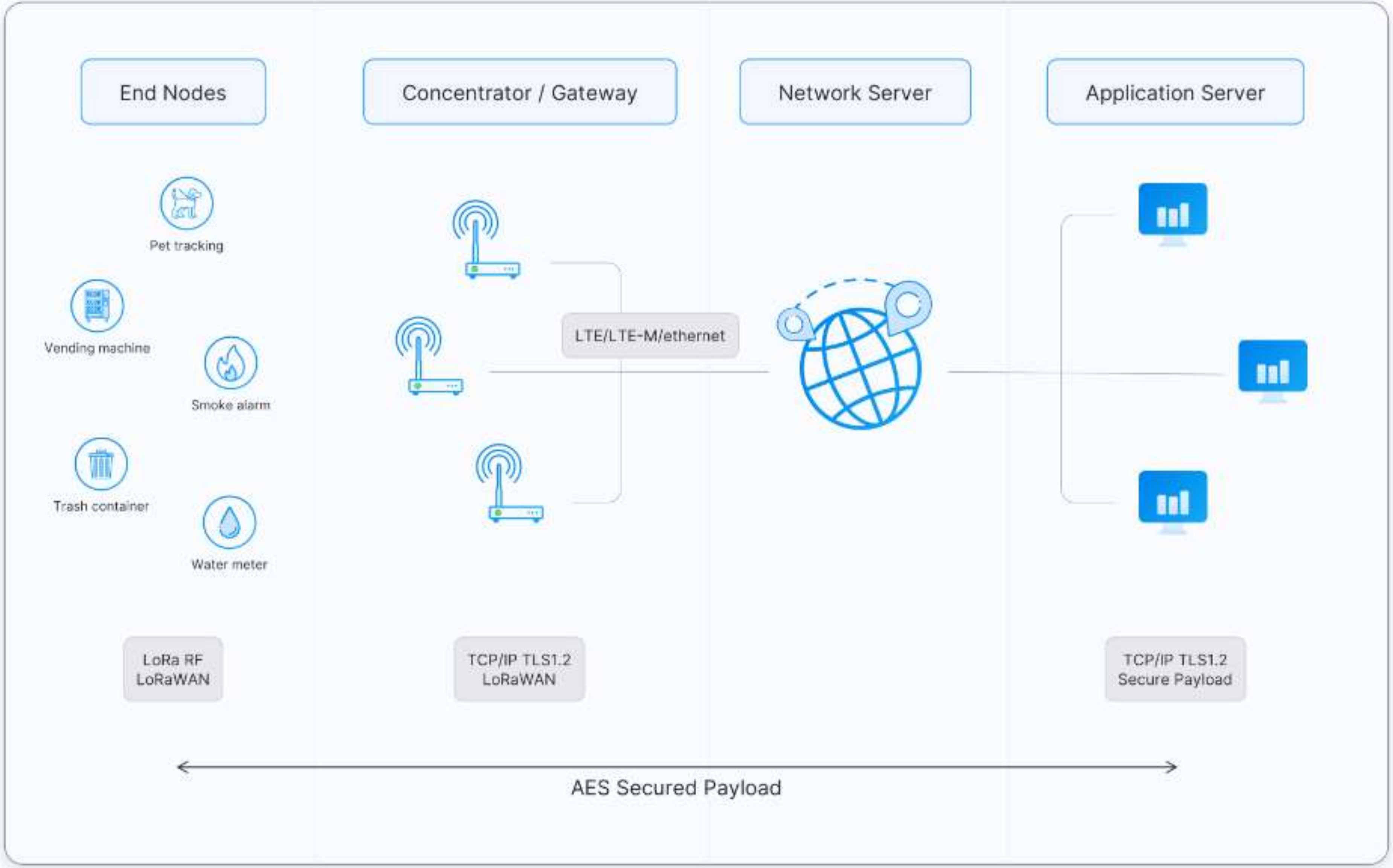
LoRa Alliance

Accura
Tequipment

- The LoRa Alliance® is an open, non-profit association established in 2015. It supports development of the LoRaWAN protocol and ensures interoperability of all LoRaWAN products and technologies.
- Today, the LoRa Alliance has over 500 members around the globe.
- The LoRa Alliance provides LoRaWAN certification for end devices. Certified end devices provide users with confidence that the end device is reliable and compliant with the LoRaWAN specification.
- Certification is only available for device manufacturers that are members of the LoRa Alliance. Once certified, the manufacturer can use the LoRaWAN Certified mark with the product.
- As announced by the LoRa Alliance® on December 7, 2021, LoRaWAN® is officially approved as a standard for Low Power Wide Area Networking (LPWAN) by the International Telecommunication Union (ITU).

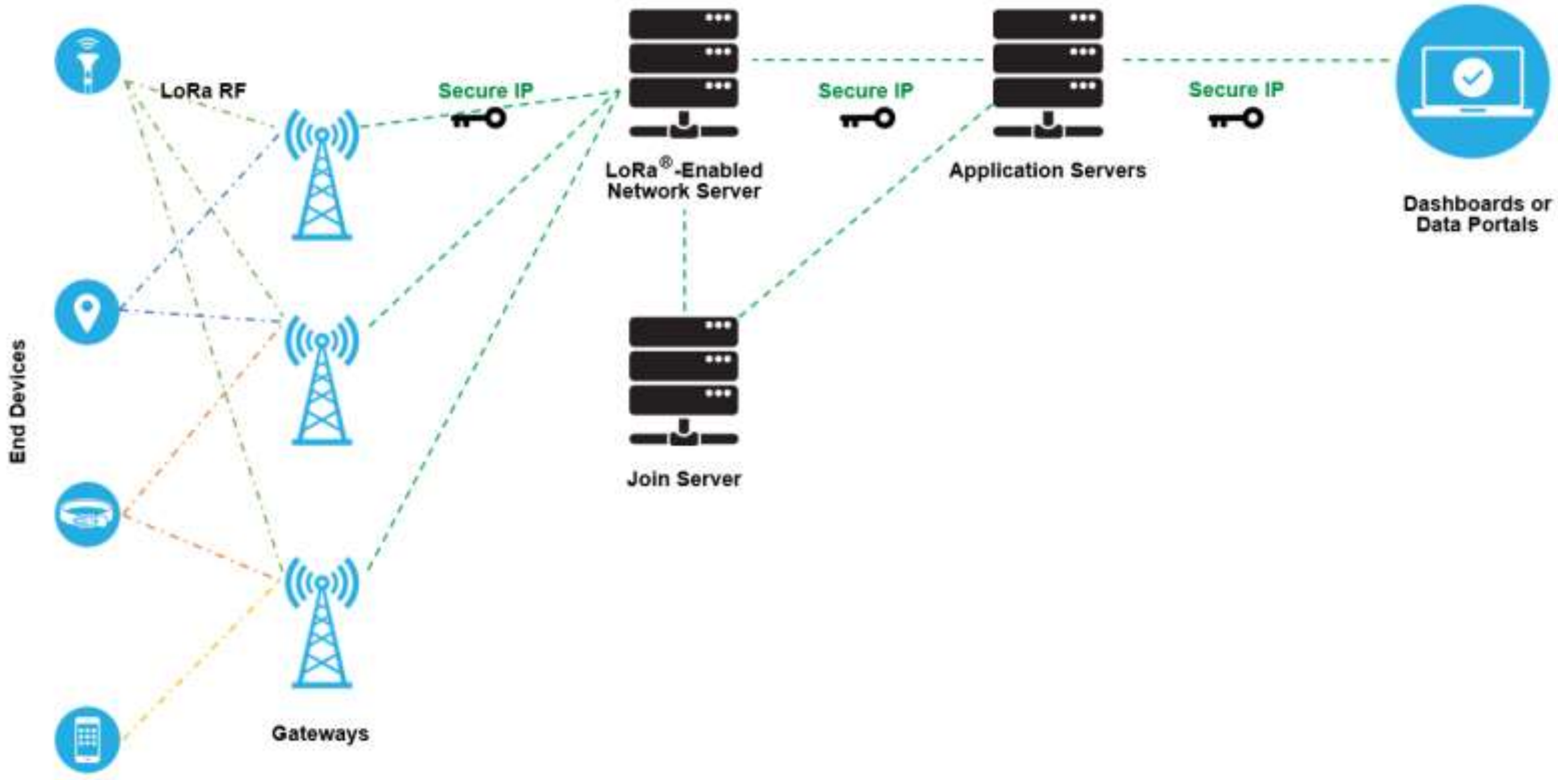
LoRaWAN Architecture

Accura Tequipment

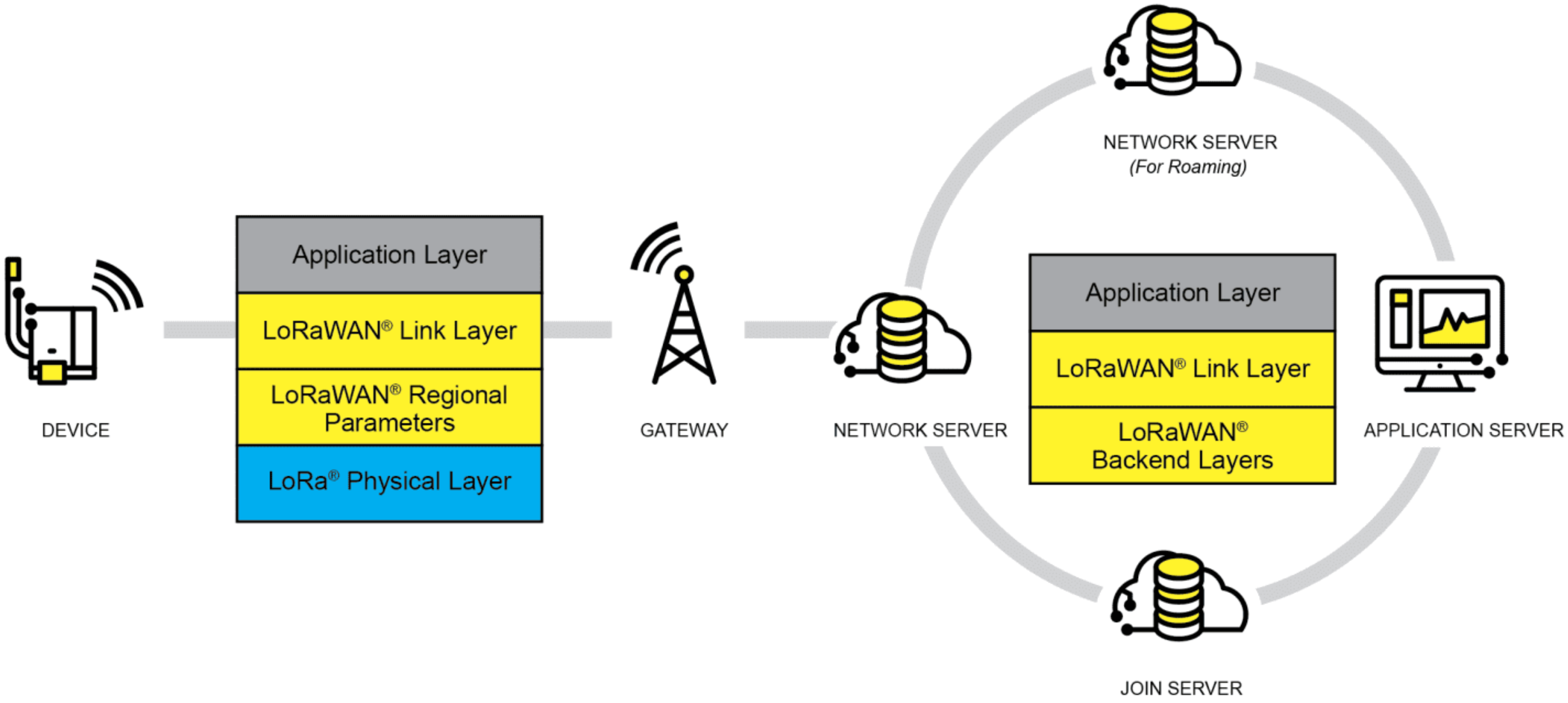


LoRaWAN Network Elements

Accura Tequipment



LoRaWAN® Network Architecture



- LoRaWAN networks are deployed in a **star-of-stars** topology in which gateways relay messages between end-devices and a central network server.

- The gateways are connected to the network server via standard IP connections and act as a transparent bridge, simply converting RF packets to IP packets and vice versa.

- The wireless communication takes advantage of the Long Range characteristics of the LoRa physical layer, allowing a single-hop link between the end-device and one or many gateways.

- All modes are capable of bi-directional communication, and there is support for multicast addressing groups to make efficient use of spectrum during tasks such as Firmware Over-The-Air (FOTA) upgrades or other mass distribution messages.

- The specification defines the device-to-infrastructure (LoRa®) physical layer parameters & (LoRaWAN®) protocol and so provides seamless interoperability between manufacturers, as demonstrated via the device certification program.

- While the specification defines the technical implementation, it does not define any commercial model or type of deployment (public, shared, private, enterprise) and so offers the industry the freedom to innovate and differentiate how it is used.

- A typical LoRaWAN network consists of the following elements.
  - **End Devices** - sensors or actuators send LoRa modulated wireless messages to the gateways or receive messages wirelessly back from the gateways.
  - **Gateways** - receive messages from end devices and forward them to the Network Server.
  - **Network Server** - a piece of software running on a server that manages the entire network.
  - Application servers - a piece of software running on a server that is responsible for securely processing application data.
  - **Join Server** - a piece of software running on a server that processes join-request messages sent by end devices.
- End devices communicate with nearby gateways and each gateway is connected to the network server.
- LoRaWAN networks use an ALOHA based protocol, so end devices don’t need to peer with specific gateways. Messages sent from end devices travel through all gateways within range. These messages are received by the Network Server. If the Network Server has received multiple copies of the same message, it keeps a single copy of the message and discards others. This is known as message deduplication.

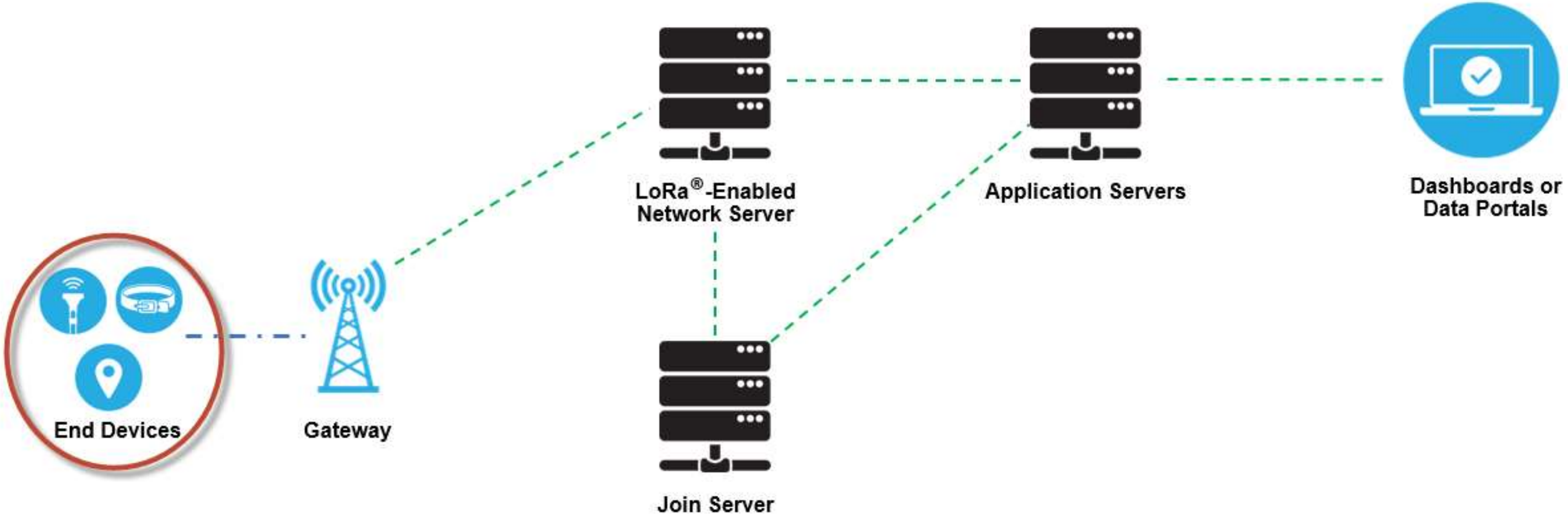
LoRa-based End Devices

- A LoRaWAN end device can be a sensor, an actuator, or both. They are often battery operated. These end devices are wirelessly connected to the LoRaWAN network through gateways using LoRa RF modulation.

- In the majority of applications, an end device is an autonomous, often battery-operated sensor that digitizes physical conditions and environmental events. Typical use cases for an actuator include: street lighting, wireless locks, water valve shut off, leak prevention, among others.

- When they are being manufactured, LoRa-based devices are assigned several unique identifiers. These identifiers are used to securely activate and administer the device, to ensure the safe transport of packets over a private or public network and to deliver encrypted data to the Cloud.

End devices in a typical LoRaWAN network deployment



LoRaWAN Gateways

- Each gateway is registered (using configuration settings) to a LoRaWAN network server.

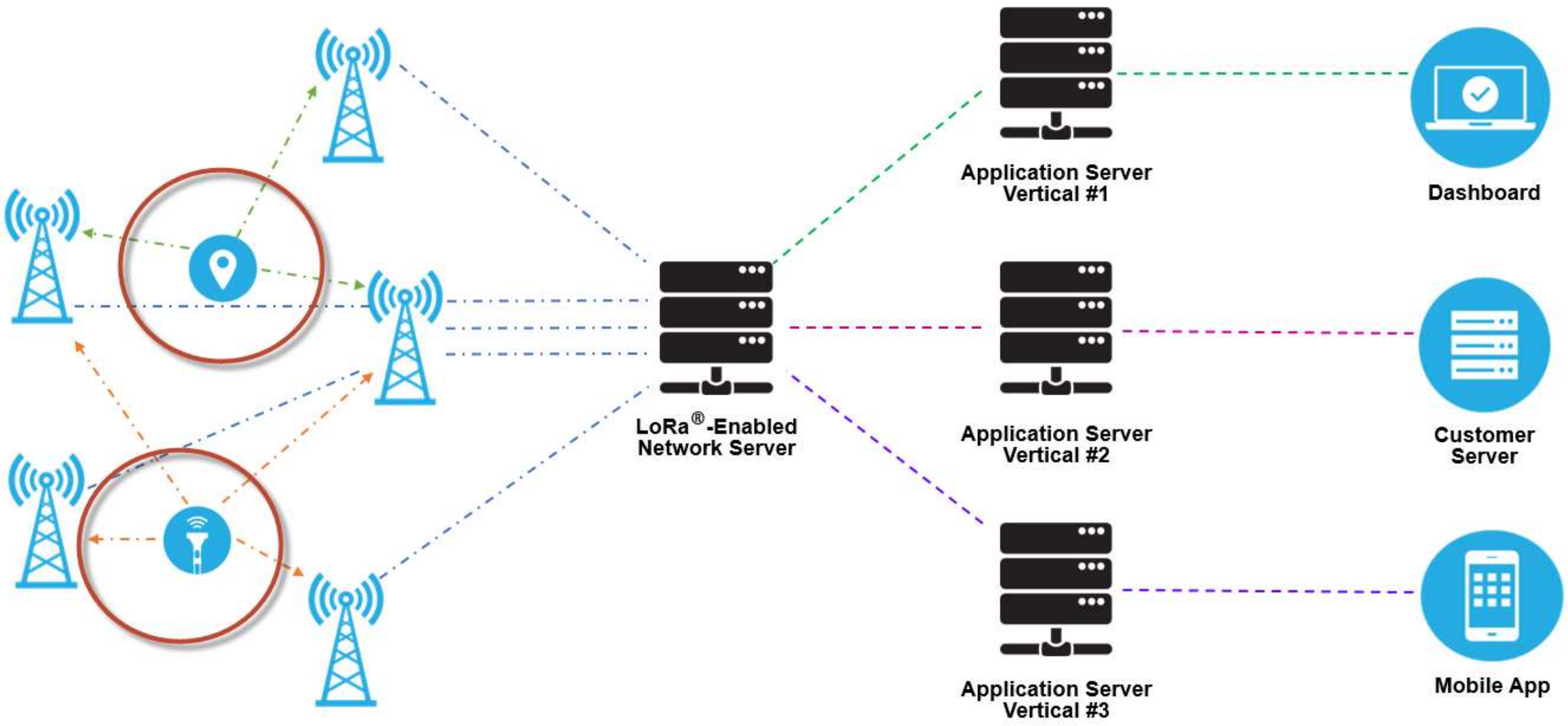
- A gateway receives LoRa messages from end devices and simply forwards them to the LoRaWAN network server (LNS).

- There is no fixed association between an end device and a specific gateway. Instead, the same sensor can be served by multiple gateways in the area. With LoRaWAN, each uplink packet sent by the end-device will be received by all gateways within reach. This arrangement significantly reduces packet error rate significantly reduces battery overhead for mobile/nomadic sensors, and allows for low-cost geolocation.

- Gateways are connected to the Network Server using a backhaul like Cellular (3G/4G/5G), WiFi, Ethernet, fiber-optic or 2.4 GHz radio links.

Gateways receiving and transmitting messages from end devices

Accura Tequipment


Application Server Vertical #1
Dashboard
LoRa®-Enabled Network Server
Application Server Vertical #2
Customer Server
Application Server Vertical #3
Mobile App

- LoRaWAN gateways operate entirely at the physical layer and, in essence, are nothing but LoRa radio message forwarders. They only check the data integrity of each incoming LoRa RF message. If the integrity is not intact, that is, if the CRC(Cyclic redundancy check) is incorrect, the message will be dropped. If correct the gateway will forward it to the LNS, together with some metadata that includes the receive RSSI(Received signal strength indicator) level of the message as well as an optional timestamp.

- For LoRaWAN downlinks, a gateway executes transmission requests coming from the LNS without any interpretation of the payload. Since multiple gateways can receive the same LoRa RF message from a single end device, the LNS performs data de-duplication and deletes all copies.

- Based on the RSSI levels of the identical messages, the network server typically selects the gateway that received the message with the best RSSI when transmitting a downlink message because that gateway is the one closest to the end device in question.

- LoRa allows for scalable, cost-optimized gateway implementation, depending on deployment objectives. For example, in North America, 8-, 16-, and 64-channel gateways are available.

- The 8-channel gateways are the least expensive. The type of gateway needed will depend on the use case. Eight- and 16-channel gateways are available for both indoor and outdoor use. Sixty-four channel gateways are only available in a carrier-grade variant. This type of gateway is intended for deployment in such places as cell towers, the rooftops of very tall buildings, etc.

Types of LoRaWAN Gateways

LoRaWAN gateways can be categorized into indoor (picocell) and outdoor (macrocell) gateways.

Indoor gateways

- Indoor gateways are cost-effective and suitable for providing coverage in places like deep-indoor locations (spaces covered by multiple walls), basements, and multi-floor buildings.
- These gateways have internal antennas or external ‘pigtail’ antennas. However depending on the indoor physical environment some indoor gateways can receive messages from sensors located several kilometers away.

Outdoor gateways

- Outdoor gateways provide a larger coverage than the indoor gateways. They are suitable for providing coverage in both rural and urban areas.
- These gateways can be mounted on cellular towers, the rooftops of very tall buildings, metal pipes (masts) etc. Usually an outdoor gateway has an external antenna (i.e. Fiberglass antenna) connected using a coaxial cable.

Usually, the receiver sensitivity of an outdoor gateway is higher than the receiver sensitivity of an indoor gateway.

Network Server

The Network Server manages gateways, end-devices, applications, and users in the entire LoRaWAN network.

A typical LoRaWAN Network Server has the following features.

- Establishing secure 128-bit AES connections for the transport of messages between end-devices and the Application Server (end-to-end security).
- Validating the authenticity of end devices and integrity of messages.
- Deduplicating uplink messages.
- Selecting the best gateway for routing downlink messages.
- Sending ADR(Adaptive Data Rate) commands to optimize the data rate of devices.
- Device address checking.
- Providing acknowledgements of confirmed uplink data messages.
- Forwarding uplink application payloads to the appropriate application servers
- Routing uplink application payloads to the appropriate Application Server.
- Forwarding Join-request and Join-accept messages between the devices and the join server
- Responding to all MAC layer commands.

Application Server

- The Application Server processes application-specific data messages received from end devices.

- It also generates all the application-layer downlink payloads and sends them to the connected end devices through the Network Server.

- A LoRaWAN network can have more than one Application Server.

- The collected data can be interpreted by applying techniques like machine learning and artificial intelligence to solve business problems.

Join Server

Accura Tequipment

- The join server manages the over-the-air activation process for end devices to be added to the network.
- The Join Server assists in secure device activation, root key storage, and session key generation. The join procedure is initiated by the end device by sending the Join-request message to the Join Server through the Network Server.
- The Join-server processes the Join-request message, generates session keys, and transfers NwkSKey and AppSKey to the Network server and the Application server respectively.
- The Join Server was first introduced with LoRaWAN v1.1. It is also availabe in LoRaWAN v1.0.4.

Message Types

Accura Tequipment

The different message types used in LoRaWAN 1.0.x and 1.1. These message types are used to transport MAC commands and application data.

- Uplink and downlink messages.
- MAC Message types and their uses.
- Sending MAC commands in the FOpts field.
- Sending MAC commands and application data in the FRMPayload field.
- Keys used to encrypt each field that carries MAC Commands and application data.
- Keys used to calculate the Message Integrity Code (MIC) of each message.

Uplink and Downlink Messages

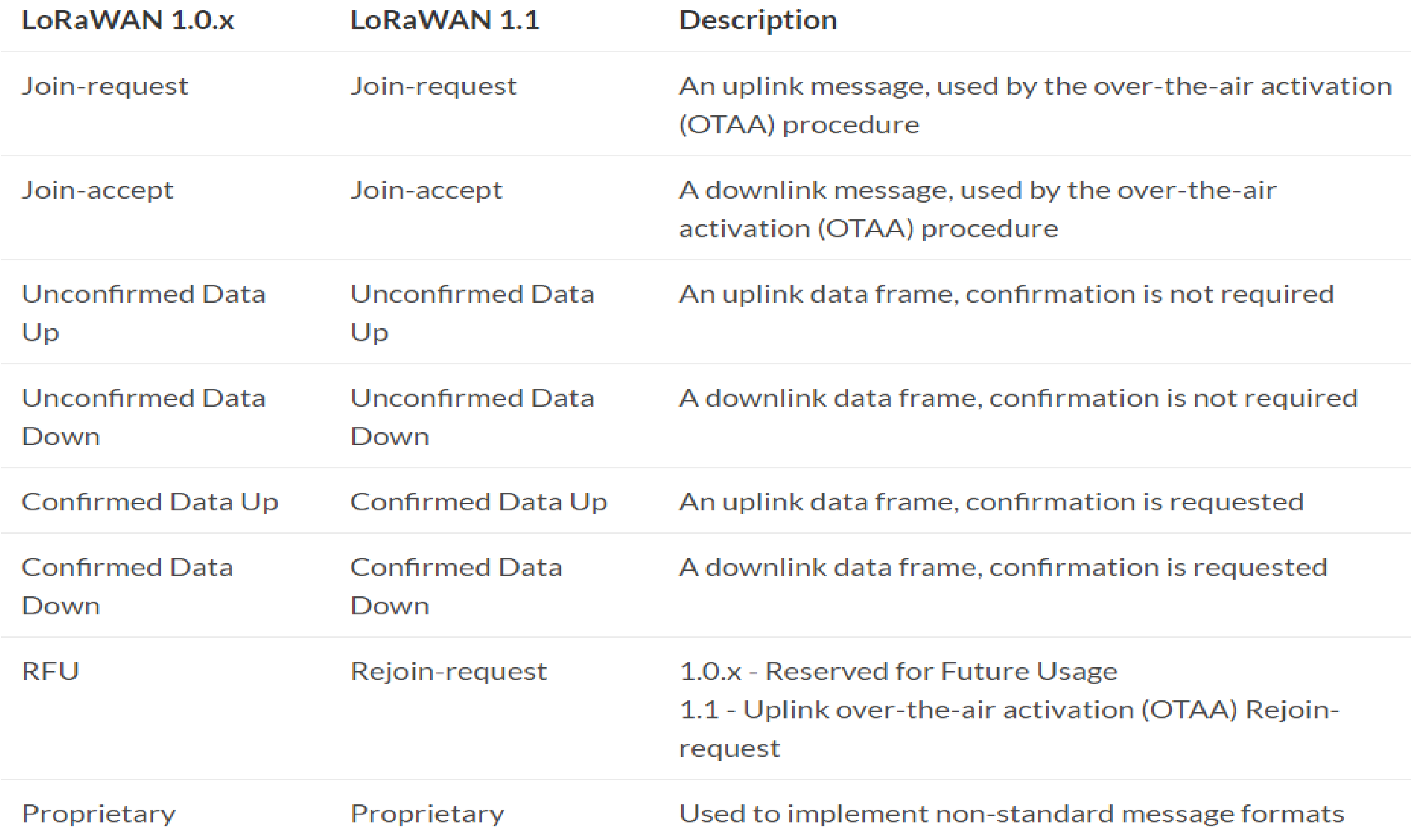
LoRa messages can be divided into uplink and downlink messages based on the direction they travel.

- **Uplink messages -** Uplink messages are sent by end devices to the Network Server relayed by one or many gateways. If the uplink message belongs to the Application Server or the Join Server, the Network server forwards it to the correct receiver.

- **Downlink messages -** Each downlink message is sent by the Network Server to only one end device and is relayed by a single gateway. This includes some messages initiated by the Application Server and the Join Server too

MAC Message Types

- LoRaWAN defines several MAC message types.
- The following table presents MAC message types that can be found in LoRaWAN 1.0.x and 1.1.



LoRaWAN 1.0.x	LoRaWAN 1.1	Description
Join-request	Join-request	An uplink message, used by the over-the-air activation (OTAA) procedure
Join-accept	Join-accept	A downlink message, used by the over-the-air activation (OTAA) procedure
Unconfirmed Data Up	Unconfirmed Data Up	An uplink data frame, confirmation is not required
Unconfirmed Data Down	Unconfirmed Data Down	A downlink data frame, confirmation is not required
Confirmed Data Up	Confirmed Data Up	An uplink data frame, confirmation is requested
Confirmed Data Down	Confirmed Data Down	A downlink data frame, confirmation is requested
RFU	Rejoin-request	1.0.x - Reserved for Future Usage 1.1 - Uplink over-the-air activation (OTAA) Rejoin-request
Proprietary	Proprietary	Used to implement non-standard message formats

Join-request

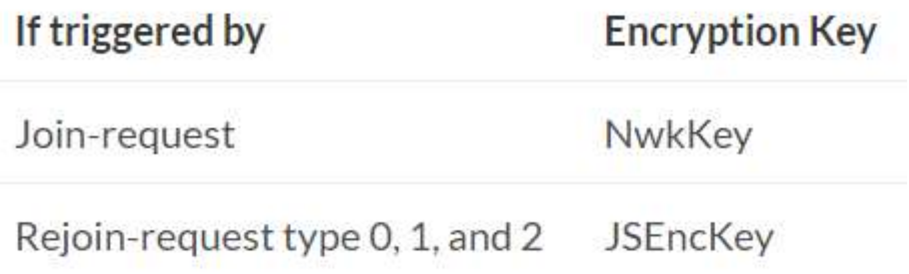
- The Join-request message is always initiated by an end device and sent to the Network Server.

- In LoRaWAN versions earlier than 1.0.4 the Join-request message is forwarded by the Network Server to the Application Server. In LoRaWAN 1.1 and 1.0.4+, the Network Server forwards the Join-request message to the device’s Join Server.

- The Join-request message is not encrypted.

Join-accept

- In LoRaWAN versions **earlier** than 1.0.4 the Join-accept message is generated by the Application Server. In LoRaWAN 1.1 and 1.0.4+ the Join-accept message is generated by the Join Server. In both cases the message passes through the Network Server. Then the Network Server routes the Join-accept message to the correct end-device.
- The Join-accept message is encrypted as follows.
    - In LoRaWAN 1.0, the Join-accept message is encrypted with the AppKey.
    - In LoRaWAN 1.1, the Join-accept message is encrypted with different keys as shown in the table below.



If triggered by	Encryption Key
Join-request	NwkKey
Rejoin-request type 0, 1, and 2	JSEncKey

Rejoin-request

- The Rejoin-request message is always initiated by an end device and sent to the Network Server.

- There are three types of Rejoin-request messages: Type 0, 1, and 2.

- These message types are used to initialize the new session context for the end device. For the Rejoin-request message, the network replies with a Join-accept message.

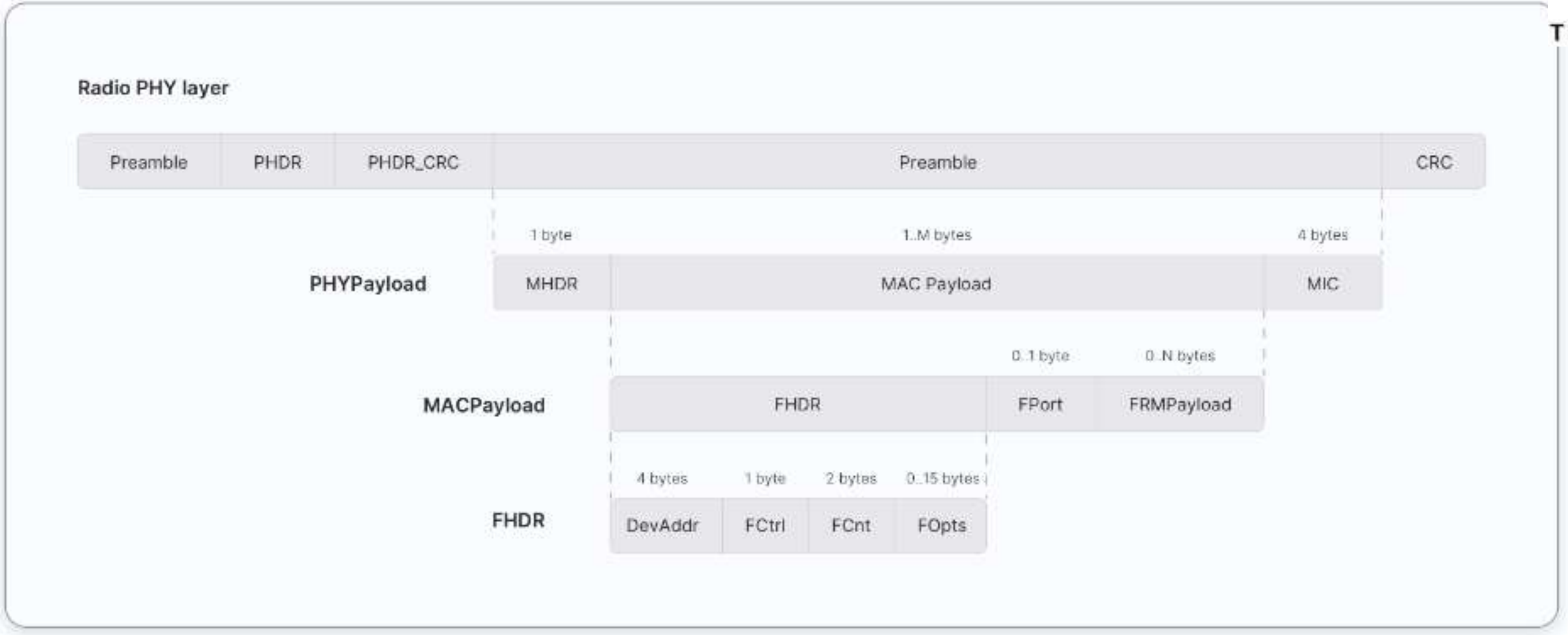
Accura Tequipment

Data Messages

- There are 4 data message types used in both LoRaWAN 1.0.x and 1.1. These data message types are used to transport both MAC commands and application data which can be combined together in a single message.

- Data messages can be confirmed or unconfirmed. Confirmed data messages must be acknowledged by the receiver whereas unconfirmed data messages do not need to be acknowledged by the receiver.

A data message is constructed as shown below:



Radio PHY layer

Preamble	PHDR	PHDR_CRC	Preamble	CRC

PHYPayload

1 byte	1..M bytes	4 bytes
MHDR	MAC Payload	MIC

MACPayload

	0..1 byte	0..N bytes
FHDR	FPort	FRMPayload

FHDR

4 bytes	1 byte	2 bytes	0..15 bytes
DevAddr	FCtrl	FCnt	FOpts

MAC payload of the data messages consists of a frame header (FHDR) followed by an optional port field (FPort) and an optional frame payload (FRMPayload)

Sending MAC Commands and Application-Specific Data

- A data message can contain any sequence of MAC commands. A data message can carry both MAC commands and application data simultaneously in separate fields.

- MAC commands can be sent either in the frame options field (FOpts) field or frame payload field (FRMPayload) field of a data message, but not both simultaneously.

- Application data can be sent in the frame payload (FRMPayload) field of a data message. The FRMPayload field CAN NOT contain MAC commands and application data simultaneously.

Sending MAC Commands in FOpts Field

- MAC commands can be piggybacked in the FOpts field of a data message for sending. The total length of the MAC commands MUST NOT exceed 15 bytes.
  - In LoRaWAN 1.0.x, these piggybacked MAC commands are always sent unencrypted.
  - In LoRaWAN 1.1, these piggybacked MAC commands are always sent encrypted using the NwkSEncKey.

Sending MAC Commands and Application-specific data in the FRMPayload field

- The FRMPayload field can contain MAC Commands or application data. If the FRMPayload field is not empty, the FPort field must be present. If the FPort field is present,
  - FPort value 0 indicates that the FRMPayload field contains only MAC commands. The total length of the MAC commands MUST NOT exceed the maximum FRMPayload length (region-specific).
  - FPort value 1-223 indicates that the FRMPayload field contains application data.

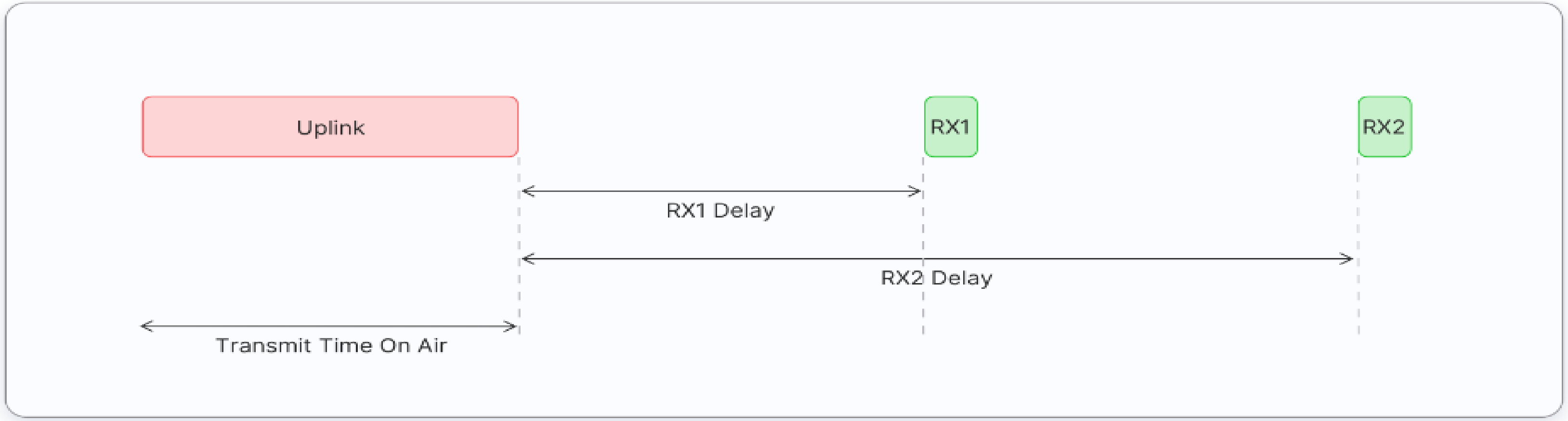
Device Classes

- The LoRaWAN specification defines three device types: **Class A**, **Class B**, and **Class C**.
- All LoRaWAN devices must implement Class A, whereas Class B and Class C are extensions to the specification of Class A devices.
- All device classes support bi-directional communication (uplink and downlink).
- During firmware upgrades over-the-air (FUOTA), a device must be switched to Class B or Class C
- End devices can’t send uplink messages while they receive downlink messages.

Class A

Accura Tequipment

- All LoRaWAN end-devices must support Class A implementation.
- A Class A device can send an uplink message at any time.
- Once the uplink transmission is completed, the device opens two short receive windows for receiving downlink messages from the network.
- There is a delay between the end of the uplink transmission and the start of each receive window, known as RX1 Delay and RX2 Delay, respectively.



- If the network server does not respond during these two receive windows, the next downlink will be scheduled immediately after the next uplink transmission.

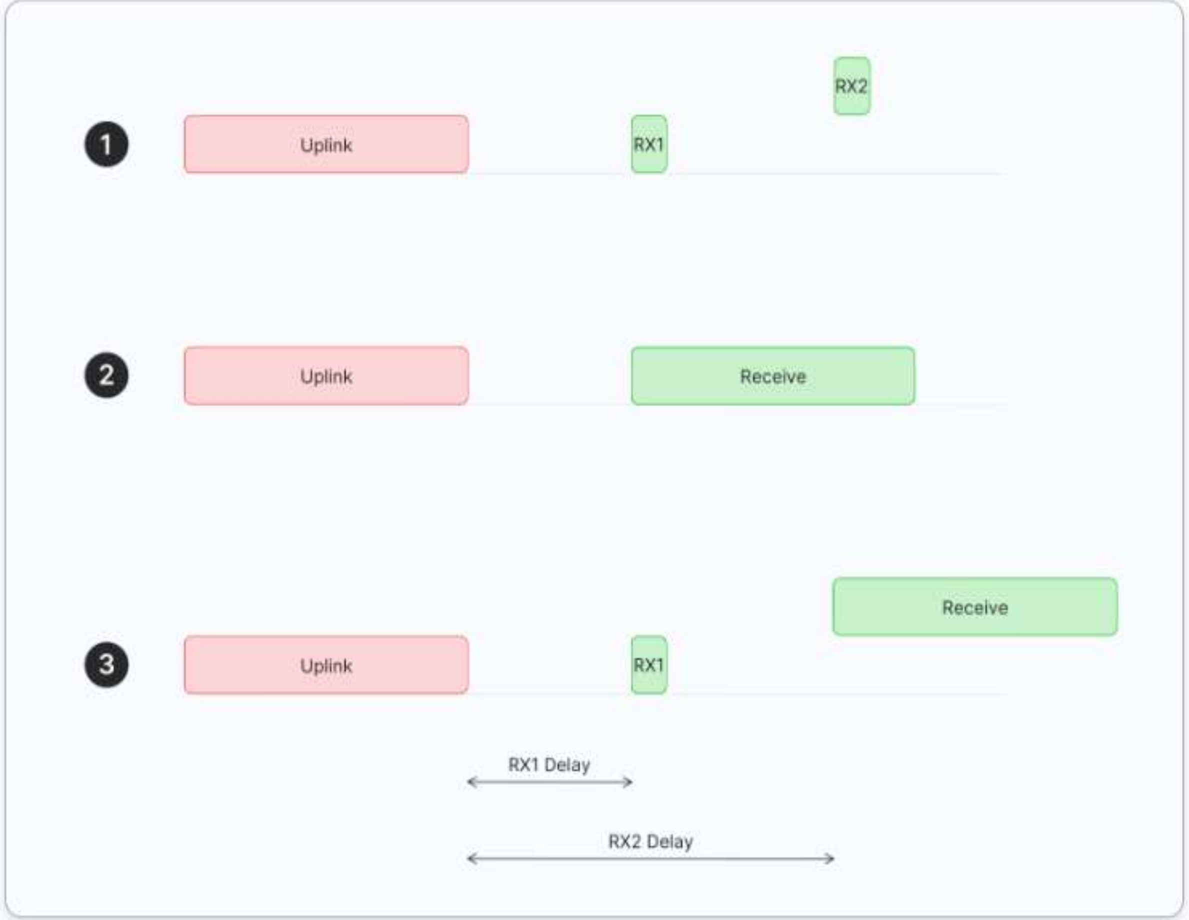
The network server can respond during the first receive window (RX1) or the second receive window (RX2), but does not use both windows.

1. The end device opens both receive windows but it doesn't receive an downlink message during either receive window.

2. The end device receives a downlink during the first receive window and therefore it does not open the second receive window.

3. The end device opens the first receive window but it does not receive a downlink. Therefore it opens the second receive window and it receives a downlink during the second receive window.

Let's consider three situations for downlink messages as illustrated below.



- Class A end devices have very low power consumption. Therefore, they can operate with battery power. They spend most of their time in sleep mode and usually have long intervals between uplinks.

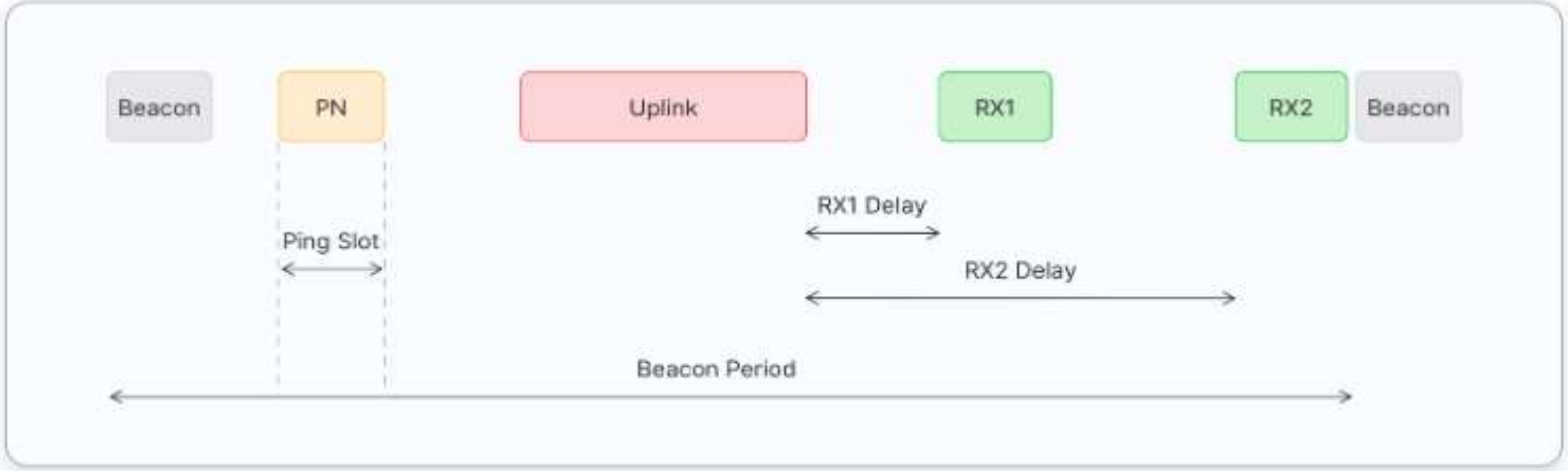
- Class A devices have high downlink latency, as they require sending an uplink to receive a downlink.

- The use cases for Class A end devices are:
  - Environmental monitoring
  - Animal tracking
  - Forest fire detection
  - Water leakage detection
  - Smart parking
  - Asset tracking
  - Waste management

Class B

- Class B devices extend Class A capabilities by periodically opening receive windows called **ping slots** to receive downlink messages.

- The network broadcasts a time-synchronized beacon (unicast and multicast) periodically through the gateways, which is received by the end devices. These beacons provide a timing reference for the end devices, allowing them to align their internal clocks with the network. This allows the network server to know when to send a downlink to a specific device or a group of devices. The time between two beacons is known as the **beacon period**.



- After an uplink, the two short receive windows, RX1 and RX2 will open similar to Class A devices.

- Class B end devices have low latency for downlinks compared to Class A end devices because they periodically open ping slots. However, they have much higher latency than the Class C end devices.

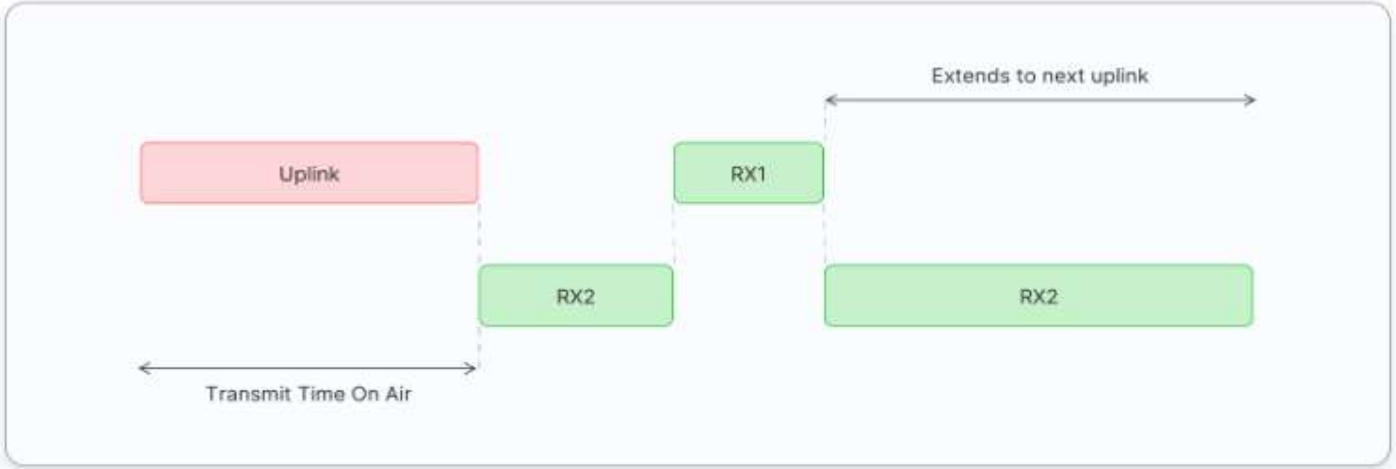
- Class B devices are often battery powered. The battery life is shorter in Class B compared to Class A because the devices spend more time in active mode due to receiving beacons and having open ping slots. Because of the low latency for downlinks, Class B mode can be used in devices that require medium-level critical actuation, such as utility meters.

- The following are some of the use cases for Class B end devices:
  - Utility meters (electrical meters, water meters, etc)
  - Street lights

- Class B devices can also operate in Class A mode.

Class C

- Class C devices extend Class A capabilities by keeping the receive windows open unless transmitting an uplink, as shown in the figure below.



- Class C devices can receive downlink messages at almost any time, thus having very low latency for downlinks. These downlink messages can be used to activate certain functions of a device, such as reducing the brightness of a street light or turning on the cut-off valve of a water meter.

- Class C devices open two receive windows, RX1 and RX2, similar to Class A. However, the RX2 receive window remains open until the next uplink transmission.

- After the device sends an uplink, a short RX2 receive window opens, followed by a short RX1 receive window, and then the continuous RX2 receive window opens.

- This RX2 receive window remains open until the next uplink is scheduled. Uplinks are sent when there is no downlink in progress.

- Compared to Class A and Class B devices, Class C devices have the lowest latency. However, they consume more power due to the need for opening continuous receive slots. As a result, these devices cannot be operated with batteries for long time therefore they are often mains powered.
- The following are some of the use cases for Class C end devices:
  - Utility meters (electrical meters, water meters, etc)
  - Street lights
  - Beacon lights
  - Alarms
  - Class C devices can also operate in Class A mode.

Security Keys

Accura Tequipment

- Security keys are the basis of maintaining data and device integrity.
- LoRaWAN relies on a unique security key for each end-device to minimize the damage of a stolen key. Therefore, it is not acceptable to use the same root key on multiple devices. Additionally, root keys cannot be based on DevEUI or any other easily-guessed scheme.
- Keys should not be all zeros or all ones.
- To obtain security keys, use a state-of-the-art cryptographic process that allows minimal transport of keys in plain text.
- Nonces and other methods used to generate keys should vary based on blocks of devices.
- For example, you can change the inputs, such as nonce values, for key generation every 64,000 devices. You can also use an alternate JoinEUI to ease the burden of looking up the exact input needed to regenerate the key, if required.

- LoRaWAN 1.0 specifies a number of security keys: NwkSKey, AppSKey and AppKey.

- All keys have a length of 128 bits.

- The algorithm used for this is AES-128, similar to the algorithm used in the 802.15.4 standard.

Session Keys

- 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.

Accura Tequipment

Network Session Key

- The Network Session Key (NwkSKey) is used for interaction between the Node and the Network Server.
- This key is used to validate the integrity of each message by its Message Integrity Code (MIC check). This MIC is similar to a checksum, except that it prevents intentional tampering with a message. For this, LoRaWAN uses AES-CMAC.
- In the backend of The Things Network this validation is also used to map a non-unique device address (DevAddr) to a unique DevEUI and AppEUI.

Application Session Key

- The Application Session Key (AppSKey) is used for encryption and decryption of the payload.
- The payload is fully encrypted between the Node and the Handler/Application Server component of The Things Network (which you will be able to run on your own server). This means that nobody except you is able to read the contents of messages you send or receive.

- These two session keys (NwkSKey and AppSKey) are unique per device, per session. If you dynamically activate your device (OTAA), these keys are re-generated on every activation. If you statically activate your device (ABP), these keys stay the same until you change them.

Accura Tequipment

Application Key

- The application key (AppKey) is only known by the device and by the application.

- Dynamically activated devices (OTAA) use the Application Key (AppKey) to derive the two session keys during the activation procedure.

- In The Things Network you can have a default AppKey which will be used to activate all devices, or customize the AppKey per device.

Frame Counters

- We’re working with a radio protocol, anyone will be able to capture and store messages. It’s not possible to read these messages without the AppSKey, because they’re encrypted. Nor is it possible to tamper with them without the NwkSKey, because this will make the MIC check fail. It is however possible to re-transmit the messages. These so-called replay attacks can be detected and blocked using frame counters.

- When a device is activated, these frame counters (FCntUp and FCntDown) are both set to 0. Every time the device transmits an uplink message, the FCntUp is incremented and every time the network sends a downlink message, the FCntDown is incremented. If either the device or the network receives a message with a frame counter that is lower than the last one, the message is ignored.

- This security measure has consequences for development devices, which often are statically activated (ABP). When you do this, you should realize that these frame counters reset to 0 every time the device restarts (when you flash the firmware or when you unplug it). As a result, The Things Network will block all messages from the device until the FCntUp becomes higher than the previous FCntUp. Therefore, you should re-register your device in the backend every time you reset it.

Spread Spectrum

- Spread Spectrum Radio Transmission was traditionally used, during WW2, to make military communications difficult to monitor - either by using a technique called ‘frequency hopping’ (FHSS) - skipping the transmission frequency around in a prearranged manner, causing the enemy to constantly retune (very rapidly) or ‘direct sequence’ (DSSS) where the digital message is added to a much higher bit-rate, pseudo random (PR) sequence.

- The code spreads the radio signal over a much wider bandwidth. In fact, so wide that the power may well be dispersed so that the total signal falls down into the background radio noise - and becomes invisible. Recovery is therefore a matter of i) knowing the original radio frequency ii) the pseudo random code and iii) and the PR code bit rate. Knowing these details means that synchronising receivers is not as difficult as may at first appear. The signal will just ‘pop up’ out of the noise when the correct values are achieved. (‘Processing Gain’)

- The technique used in LoRa is ‘CHIRP’: Compressed High Intensity Radar Pulse. It is even more complex but simple with current technology. As the name may suggest, the background design requirement, it is not used to hide the radio signal but is employed because of other factors, not just processing gain but interference immunity, channel sharing and resistance to radio reflections (amongst others). It is therefore employed as security against operating conditions not for surveillance resistance.

End Device Activation

- Every end device must be registered with a network before sending and receiving messages. This procedure is known as **activation**.

- There are two activation methods available:
  - **Over-The-Air-Activation (OTAA)** - the most secure and recommended activation method for end devices. Devices perform a join procedure with the network, during which a dynamic device address is assigned and security keys are negotiated with the device.

  - **Activation By Personalization (ABP)** - requires hardcoding the device address as well as the security keys in the device. ABP is **less secure** than OTAA and also has the downside that devices can not switch network providers without manually changing keys in the device.

- The join procedure for LoRaWAN 1.0.x and 1.1 is slightly different.

Over The Air Activation in LoRaWAN 1.0.x

- In LoRaWAN 1.0.x, the join procedure requires two MAC messages to be exchanged between the end device and the Network Server:
  - Join-request - from end device to the Network Server
  - Join-accept - from Network Server to the end device

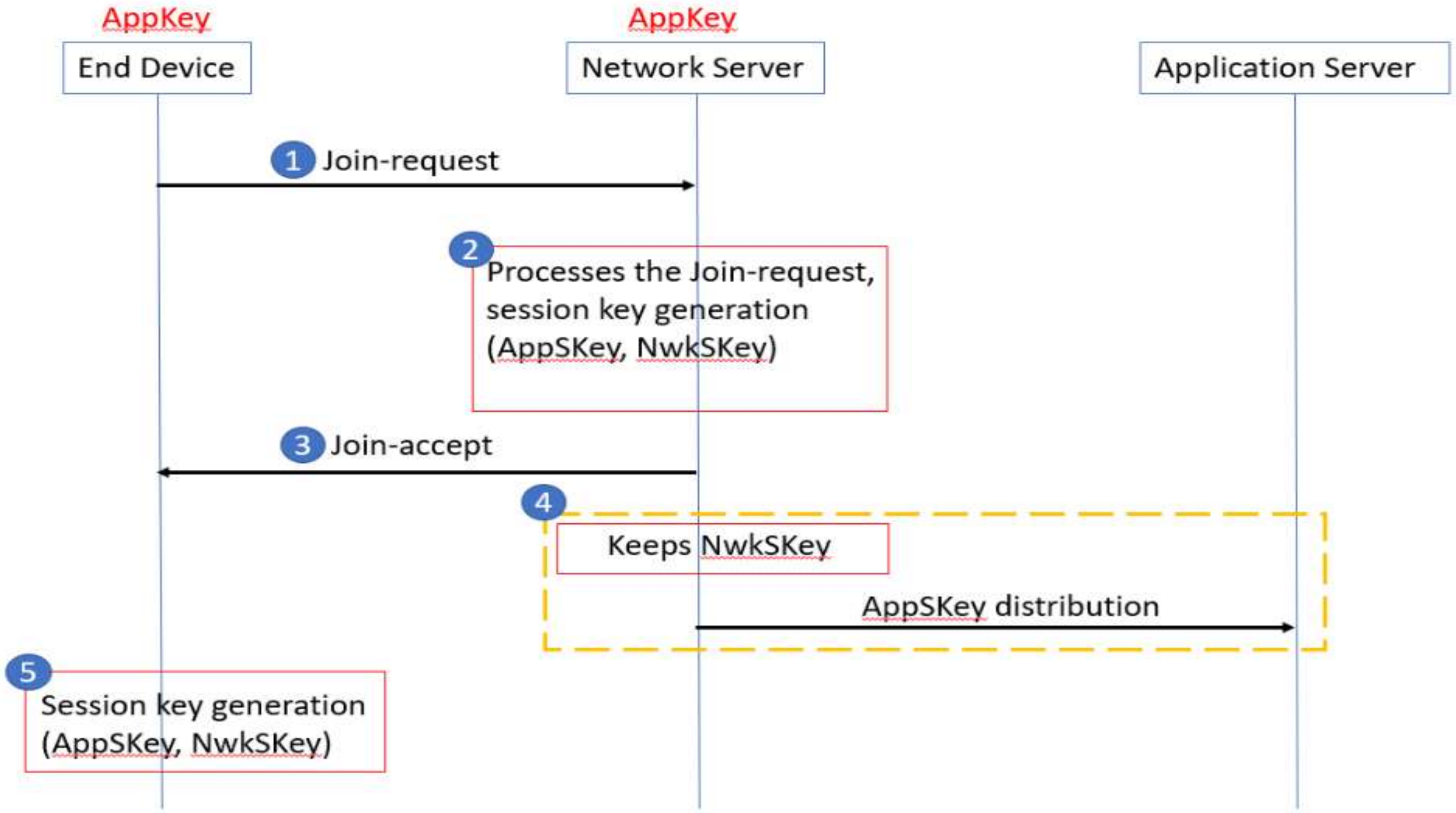
- Before activation, the AppEUI, DevEUI, and AppKey should be stored in the end device.

- The AppKey is an AES-128 bit secret key known as the root key. The same AppKey should be provisioned onto the network where the end device is going to register.

- The AppEUI and DevEUI are not secret and are visible to everyone.

- The AppKey is never sent over the network.

The following steps describe the Over-The-Air-Activation (OTAA) procedure



The Figure shows the OTAA message flow in LoRaWAN 1.0

Over-The-Air-Activation in LoRaWAN 1.1

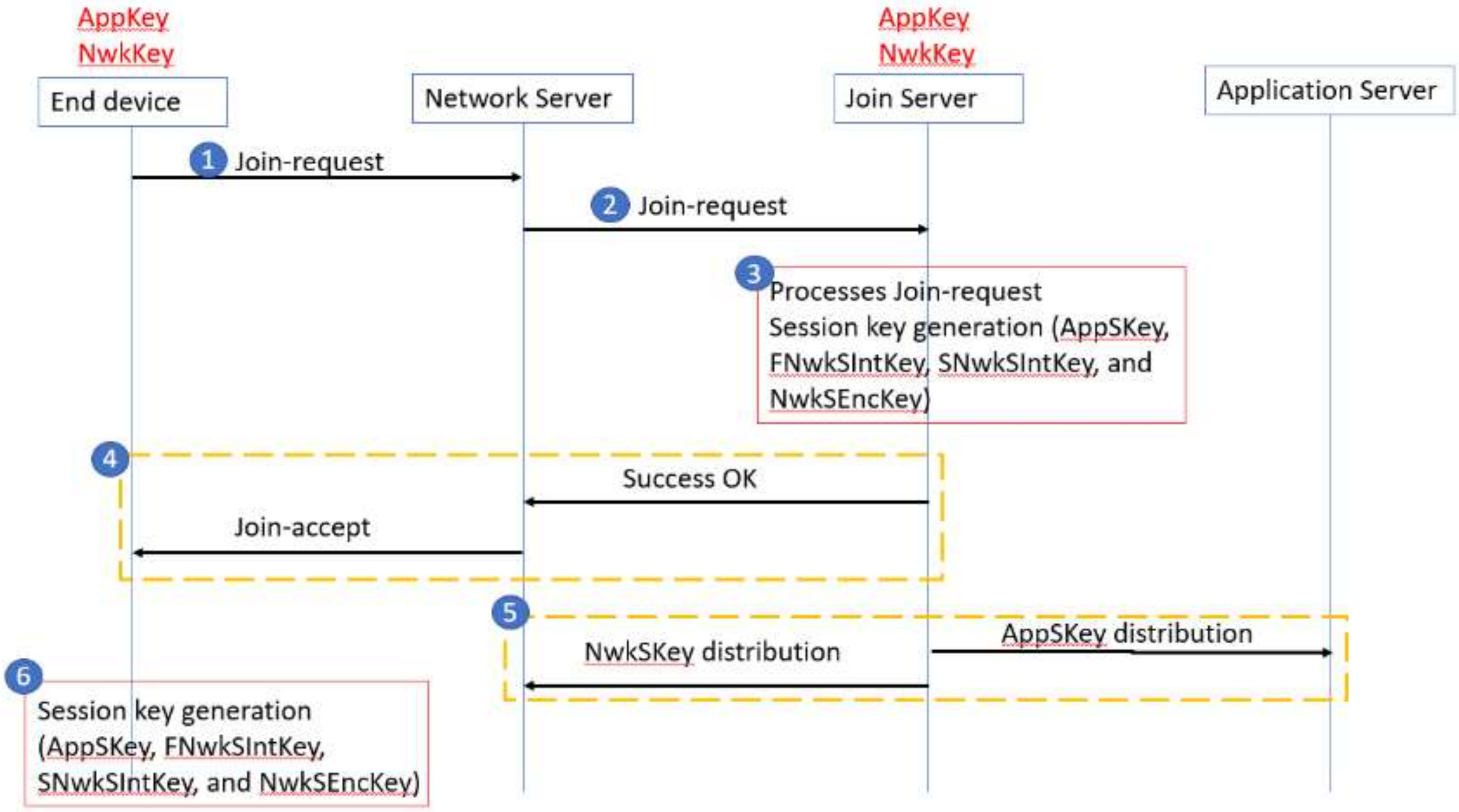
- In LoRaWAN 1.0.x, the join procedure requires two MAC messages to be exchanged between the end device and the Join Server:
  - Join-request - from end device to the Join Server
  - Join-accept - from Join Server to the end device

- Before activation, the **JoinEUI**, **DevEUI**, **AppKey**, and **NwkKey** should be stored in the end device. The **AppKey** and **NwkKey** are AES-128 bit secret keys known as **root keys**.

- The matching **AppKey**, **NwkKey**, and **DevEUI** should be provisioned onto the Join Server that will assist in the processing of the join procedure and session key derivation. The **JoinEUI** and **DevEUI** are **not secret** and visible to everyone.

- The **AppKey** and **NwkKey** are never sent over the network.

The Figure shows OTAA message flow in LoRaWAN 1.1



Activation By Personalization

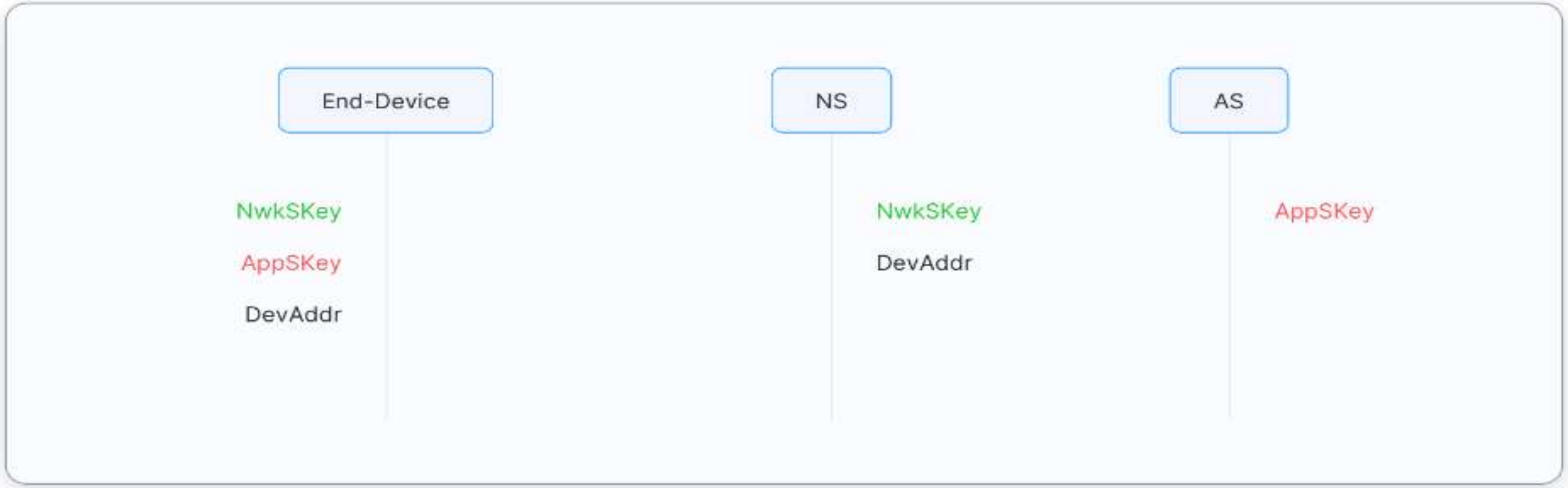
- Activation By Personalization (ABP) directly ties an end-device to a pre-selected network, bypassing the over-the-air-activation procedure.

- Activation by Personalization is the less secure activation method, and also has the downside that devices can not switch network providers without manually changing keys in the device. A Join Server is not involved in the ABP process.

- An end device activated using the ABP method can only work with a single network and keeps the same security session for its entire lifetime.

Activation By Personalisation in LoRaWAN 1.0.x

The **DevAddr** and the two session keys **NwkSKey** and **AppSKey** are directly stored into the end-device instead of the DevEUI, AppEUI, and the AppKey. Each end device should have a unique set of NwkSKey and AppSkey. The same **DevAddr** and **NwkSKey** should be stored in the Network Server and the **AppSKey** should be stored in the Application Server

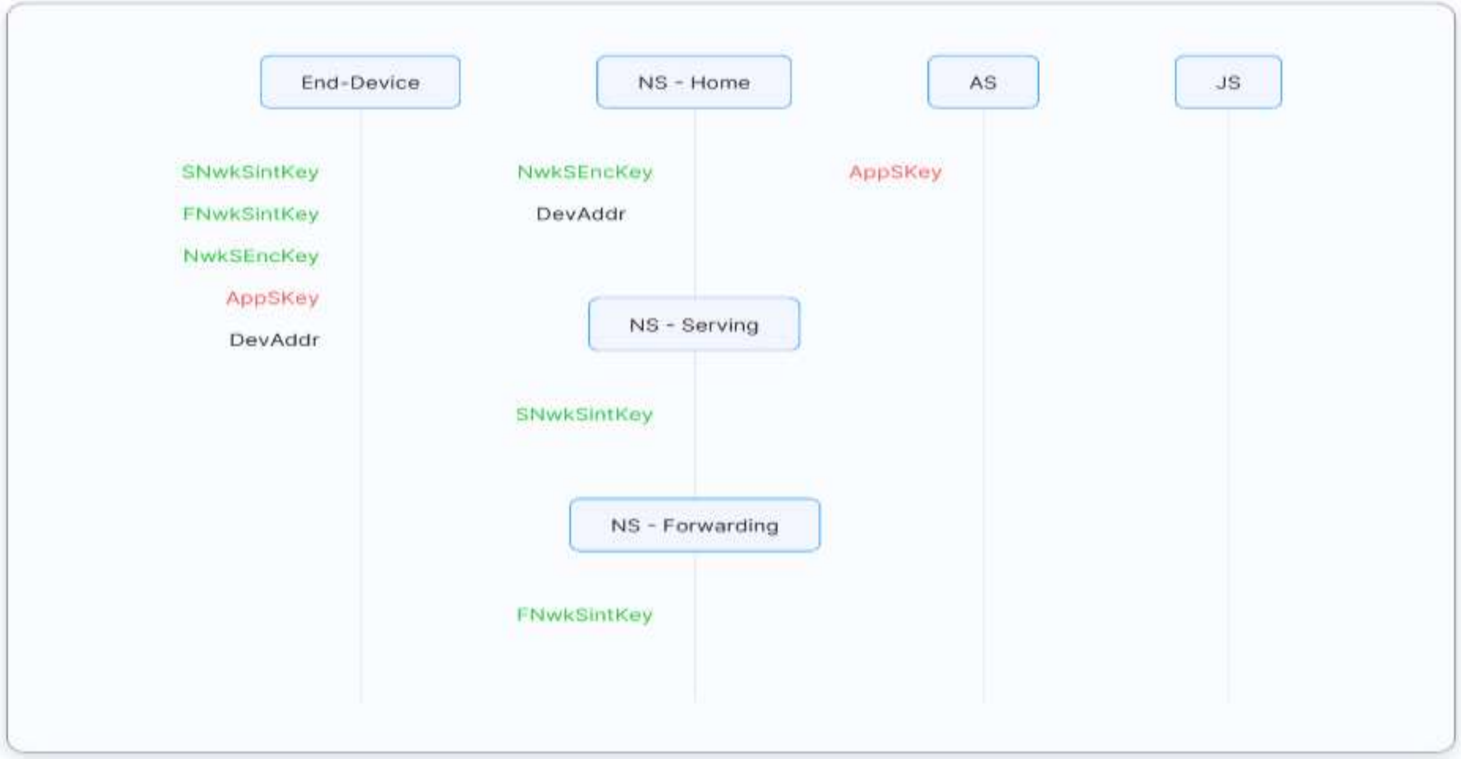


The Figure shows Pre-sharing DevAddr and session keys for ABP in LoRaWAN 1.0

Activation By Personalisation in LoRaWAN 1.1

The DevAddr and the four-sessionkeys

FNwkSIntKey, SNwkSIntKey, NwkSEncKey, and AppSKey are directly stored into the end device instead of the DevEUI, JoinEUI, AppKey, and NwkKey. The same DevAddr, FNwkSIntKey, SNwkSIntKey, and NwkSEncKey should be stored in the Network Server and the and AppSKey should be stored in the Application Server.



Limitations of LoRaWAN

LoRaWAN is not suitable for every use-case, so it is important that you understand the limitations.

Suitable use-cases for LoRaWAN:

- **Long range** - multiple kilometers
- **Low power** - can last years on a battery
- **Low cost** - less than 20€ CAPEX per node, almost no OPEX
- **Low bandwidth** - between 250bit/s and 11kbit/s in Europe using LoRa modulation (depending on the spreading factor)
- **Coverage everywhere** - you are the network! Just install your own gateways
- **Secure** - 128bit end-to-end encrypted

Not Suitable for LoRaWAN:

- **Realtime data** - you can only send small packets every couple of minutes
- **Phone calls** - you can do that with GPRS/3G/LTE
- **Controlling lights in your house** - check out ZigBee or BlueTooth
- **Sending photos, watching Netflix** - check out WiFi