Aplicaciones IoT: LoRa WAN & MQTT

Asignatura: Redes de Datos

Estudiantes: Allegrini, Tomás; Ortiz, Joaquín; Vazquez, Leonardo

Profesores: Carnagui, Marco; Cebedio, Celeste; Copolillo, Leonardo; Liberatori, Mónica

Fecha: 24/11/2022

Facultad de Ingeniería

Universidad Nacional de Mar del Plata

ÍNDICE

Introducción a Internet de las Cosas (IoT)

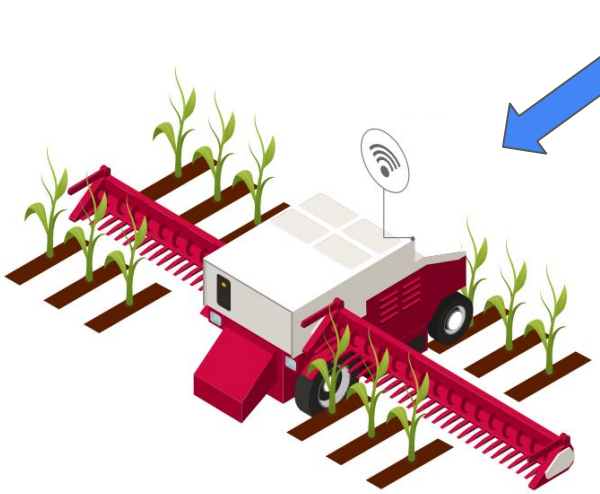
Definición:

"IoT describe la red de objetos físicos que llevan incorporados tecnología de hardware y software con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de internet"

Casos de aplicaciones IoT

- **Ganadería:** Control de temperatura de carne vacuna, monitoreo de ganado
- **Conservación de animales:** seguimiento de especies en peligro de extinción
- **Granjas inteligentes:** información en tiempo real de cultivos, optimización de riego y uso del agua, control en pulverización
- **Seguimiento en aeropuertos:** monitoreo de vehículos, personal y equipaje
- **Espacios de trabajo eficientes:** disponibilidad de estacionamiento, uso de la energía

Caso PulverizAR



Vía LoRa WAN

MQTT

LoRa/LoRa Wan - Fundamentos

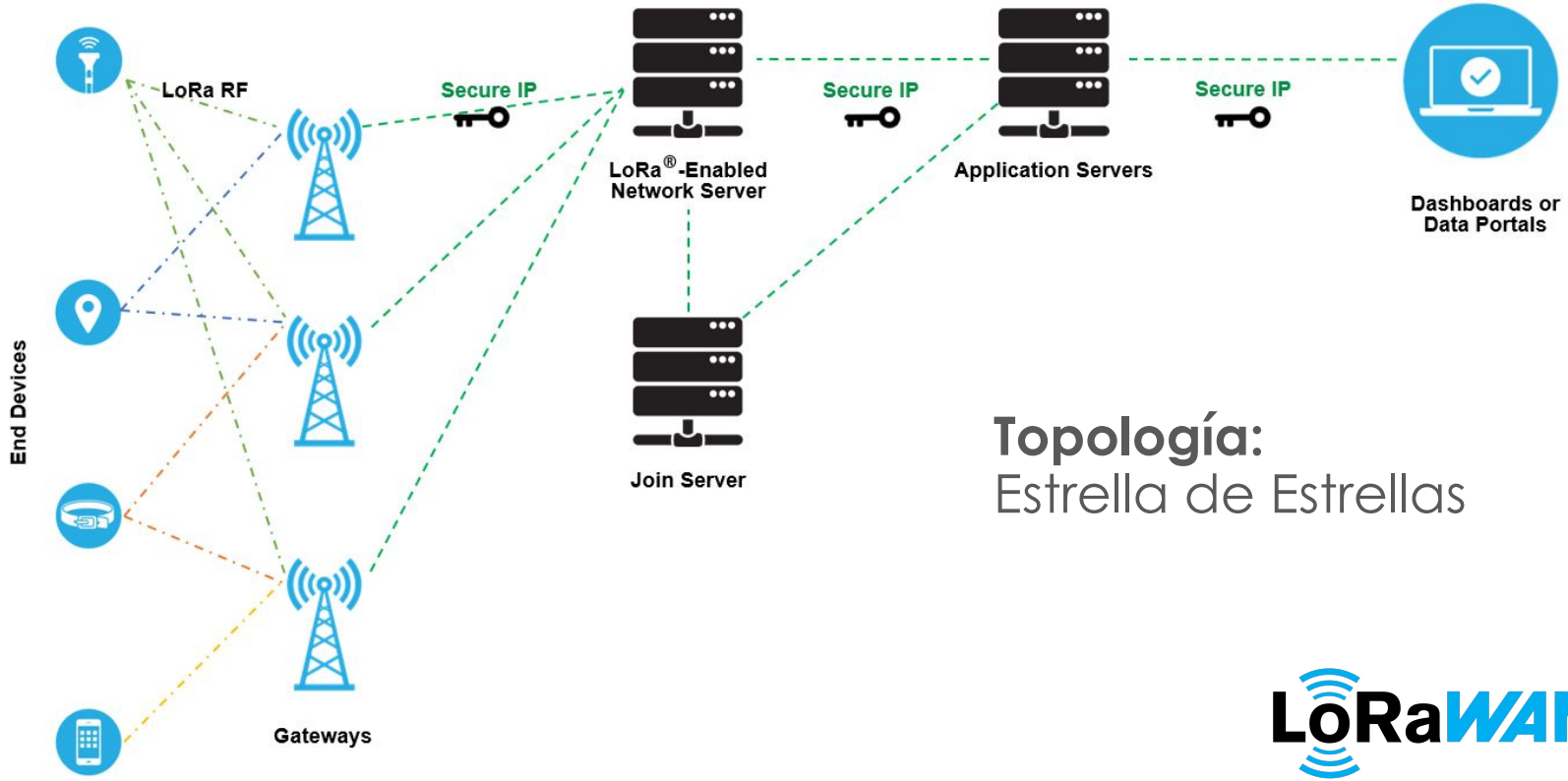
LoRa:

Técnica de modulación inalámbrica basada en dispersión de frecuencia.

LoRa WAN:

Protocolo de la capa de acceso al medio (MAC) para aplicaciones IoT. Establece el formato de mensajes para la modulación LoRa.

Arquitectura



Topología:
Estrella de Estrellas

LoRaWAN®

Arquitectura

Dispositivos finales (Nodos):

Reciben/transmiten los mensajes desde/hacía las puertas de enlace o Gateways.

Puertas de enlace (Gateways):

Reciben/transmiten los mensajes a los nodos y los reenvían al servidor de red.

Servidor de red:

Ejecuta el software que administra toda la red.

Servidor de aplicaciones:

Ejecuta el software que procesa los datos en la aplicación.

Modelo de Capas

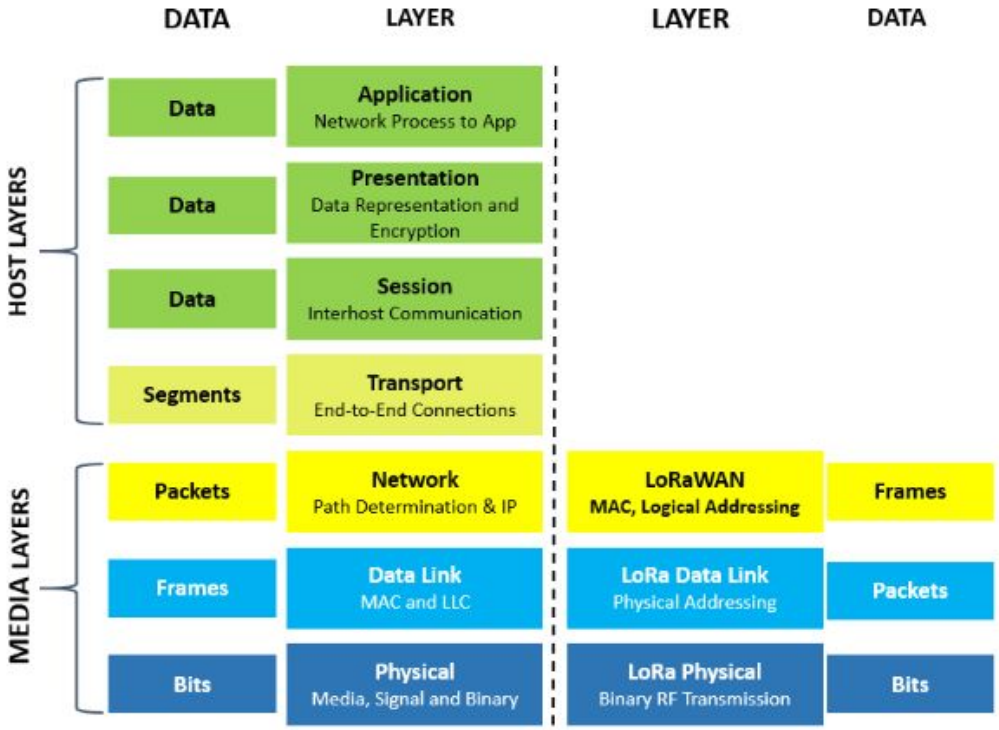
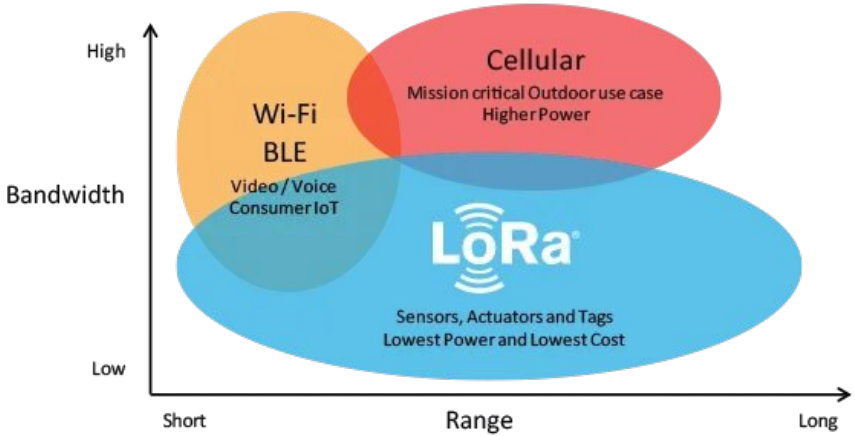


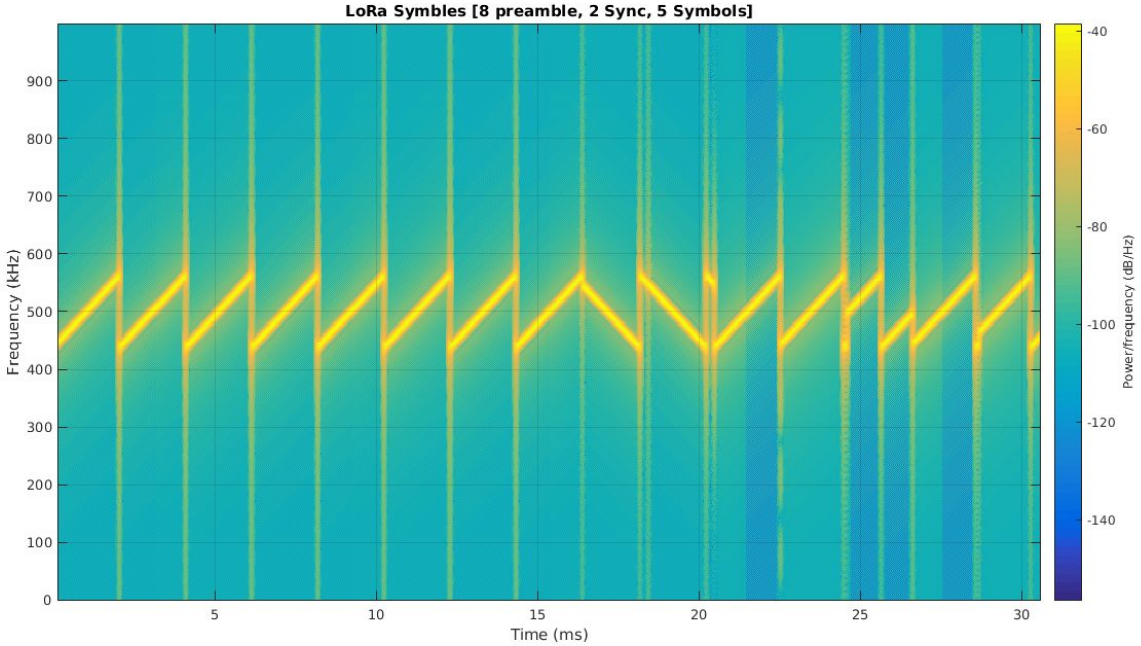
Figura 3: Modelo de red OSI de siete capas

Capa física: características

- Modulación inalámbrica basada en CSS (Chirp Spread Spectrum)
- Alta sensibilidad
- Redes de área amplia (5 a 15 km)
- Baja potencia
- Bandas ISM: 915, 868, 433 MHz
- BW: 125, 250, 500 kHz



Capa física: parámetros



Espectrograma

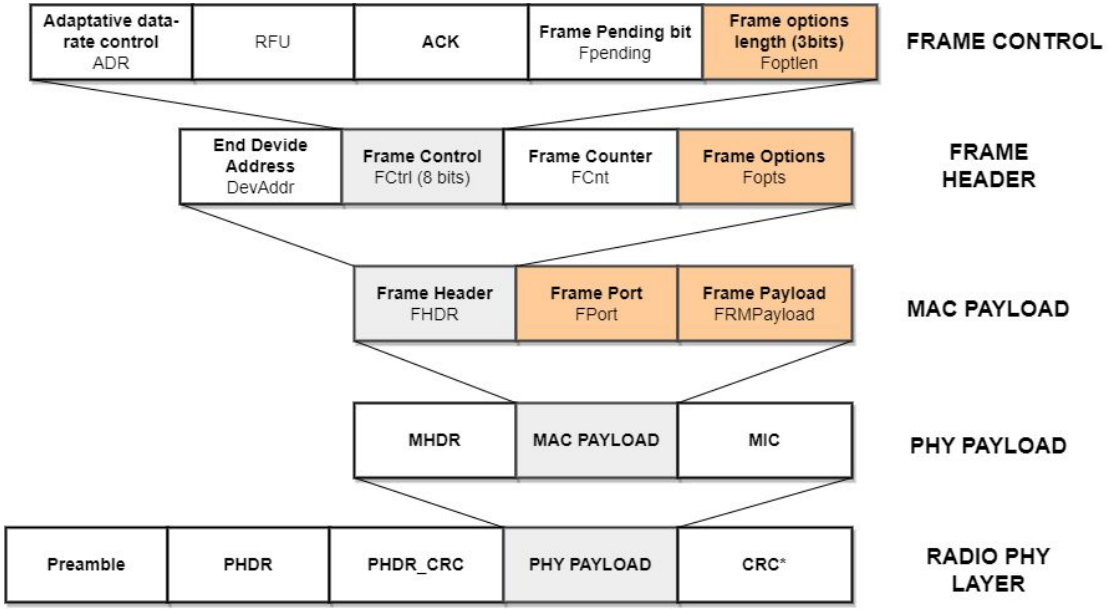
- Bandwidth
- **Spreading Factor**
- Coding Rate (FEC)
- Bit Rate
- SNR
- Air Rate

Capa MAC: características

- Establece conexión virtual entre servidor de red y Nodos LoRa WAN (enlaces descendente y ascendente)
- Consulta y define el estado de los nodos finales
- Posee opciones para configurar parámetros de la capa física, tanto en transmisión como en recepción
- Recibe parámetros de Windows desde el servidor de red para modificar la velocidad de los datos
- Emplea método ALOHA

LoRaWAN® L2 1.0.4 Specification (TS001-1.0.4)

Formato de Mensajes

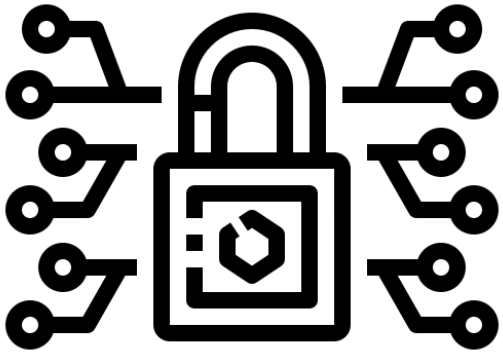


CID	Command	Transmitted by: End-device	Transmitted by: Gateway	Short Description
0x02	***LinkCheckReq***	x		Used by an end-device to validate its connectivity to a network.
0x02	***LinkCheckAns***		x	Answer to LinkCheckReq command. Contains the received signal power estimation indicating to the end-device the quality of reception (link margin).
0x03	***LinkADRReq***		x	Requests the end-device to change data rate, transmit power, repetition rate or channel.
0x03	***LinkADRAns***	x		Acknowledges the LinkRateReq.
0x04	***DutyCycleReq***		x	Sets the maximum aggregated transmit duty-cycle of a device
0x04	***DutyCycleAns***	x		Acknowledges a DutyCycleReq command
0x05	***RXParamSetupReq***		x	Sets the reception slots parameters
0x05	***RXParamSetupAns***	x		Acknowledges a RXSetupReq command
0x06	***DevStatusReq***		x	Requests the status of the end-device
0x06	***DevStatusAns***	x		Returns the status of the end-device, namely its battery level and its demodulation margin
0x07	***NewChannelReq***		x	Creates or modifies the definition of a radio channel
0x07	***NewChannelAns***	x		Acknowledges a NewChannelReq command
0x08	***RXTimingSetupReq***		x	Sets the timing of the of the reception slots
0x08	***RXTimingSetupAns***	x		Acknowledges RXTimingSetupReq command
0x09	***TxParamSetupReq***		x	Used by the network server to set the maximum allowed dwell time and Max EIRP of end-device, based on local regulations
0x09	***TxParamSetupAns***	x		Acknowledges TxParamSetupReq command
0x0A	***DlChannelReq***		x	Modifies the definition of a downlink RX1 radio channel by shifting the downlink frequency from the uplink frequencies (i.e. creating an asymmetric channel)
0x0A	***DlChannelAns***	x		Acknowledges DlChannelReq command
0x0B to 0x0C	***RFU***			
0x0D	***DeviceTimeReq***	x		Used by an end-device to request the current date and time
0x0D	***DeviceTimeAns***		x	Sent by the network, answer to the DeviceTimeReq request
0X0E to 0x7F	RFU			
0x80 to 0xFF	Proprietary	x	x	Reserved for proprietary network command extensions

Seguridad

Temas a tratar:

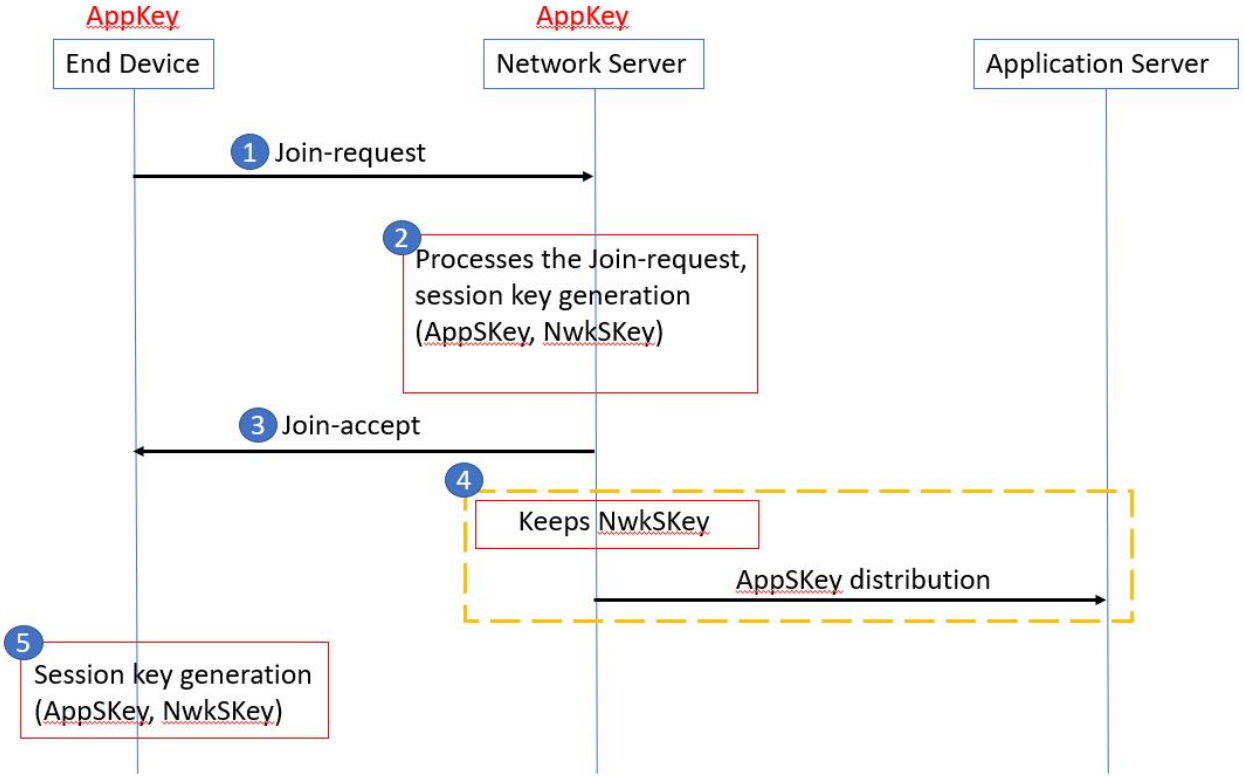
- Activación/vinculación de un Nodo a una Red LoRa Wan
  - ABP
  - OTAA
- Aspectos de seguridad en el protocolo



Incorporación de Nodo a una red LoRa Wan OTAA vs ABP

- Existen 2 metodos de activacion de un “nodo” o “end-device”:
  - **OTAA** - Over-The-Air-Activation
  - **ABP** - Activation-By-Personalization
- En LoRa Wan contamos con 1 llave y 2 ID “unívocos”:
  - DevEUI: identifica de forma unívoca al nodo (análogo a una MAC). Los dispositivos se programan con una determinada llave.
  - AppEUI: identifica al Aplication Server (podemos pensarlo como un número de puerto).
  - AppKey: llave AES de 128 bits (llave simétrica, implica que tanto el nodo como el network server deben conocerla). Es utilizada además para asegurar integridad en el mensaje a través del mecanismo MIC (Message Integrity Code).
- OTAA es el método de activación más utilizado, debido a la flexibilidad de poder migrar un nodo de una red a otra, y además de proveer mayor seguridad durante el proceso de “conexión” a la red.

OTAA - LoRa Wan v1.0.2



OTAA - LoRa Wan v1.0.2

1) Se envía un JoinRequest compuesto por Nonce/AppEui/DevEui + MIC (3 valores anteriores encriptados con la AppKey)
2) NetworkServer chequea si el nonce no fue utilizado anteriormente usando su AppKey (Replay-Attack). Auténtica además usando el MIC. Generamos 2 llaves (AppSKey, NwkSKey).
3) Enviamos cómo Join-Accept el mensaje

3 bytes	3 bytes	4 bytes	1 bytes	1 bytes	16 bytes (optional)
AppNonce	NetID	DevAddr	DLSettings	RXDelay	CFList

- Nonce generado por Network Server
- Nuevo DeviceAddress generado por NetworkServer
- Opciones

Estos parámetros son encriptados y enviados en el campo MIC para que el End-Device autentique el mensaje.

OTAA - LoRa Wan v1.0.2

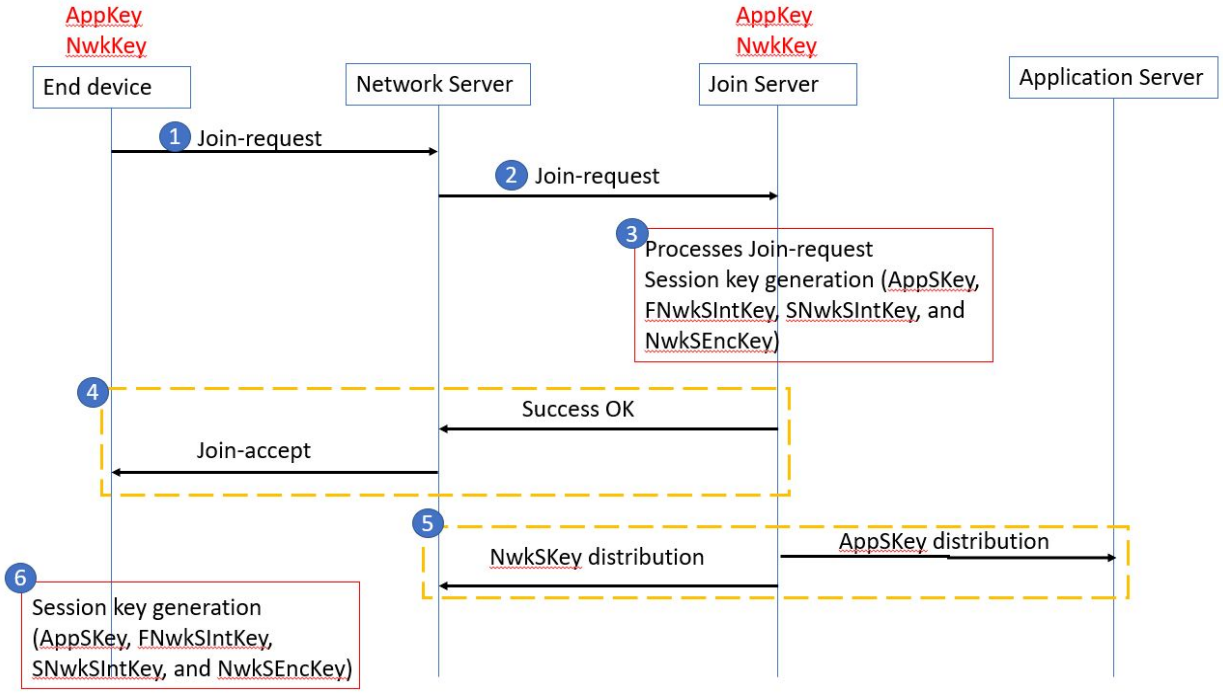
4) El network Server distribuye la AppSKey al Aplication-Server.

5) El End-Device desencripta el Join-Accept que recibio con la AppKey y el AppNonce para obtener la Network-Session-Key y la Application-Session-Key.

Luego de la activación, el end-device usa la Network-Session-Key para calcular y verificar el MIC de todos los mensajes que reciba (**integridad**).

AppSKey es usada como la nueva llave para encriptar/desencriptar los payloads de los mensajes.

OTAA - LoRa Wan v1.0.0



OTAA - LoRa Wan v1.0.0

- Esquema que provee mayor seguridad que el anterior.
- Se hace uso de 2 llaves AES, y se agrega un nuevo actor, el **Join-Server**.
- JoinEUI identifica al JoinServer.

1) Análogo a v1.0.2, se envía un Join-Request con **JoinEUI/DevEUI/DevNonce + MIC.**
2) NetworkServer forwarded el mensaje al Join-Server
3) Procesa el mensaje, y genera las llaves **AppSKey, FNwkSIntKey, SNwkIntKey y NwkSEncKey** si se verificó correctamente el Join-request.
4) El Network-Server genera el Join-Accept enviando

1 byte	3 bytes	4 bytes	1 bytes	1 bytes	16 bytes
JoinNonce	NetID	DevAddr	DLSettings	RXDelay	CFList

OTAA - LoRa Wan v1.0.0

5) El Join Server envia el AppSKEy al **Application-Server** y las otras 3 llaves de sesion (FWwkSIntKey, SNwkSIntKey y NwkSEncKey) al **Network-Server**

6) El End-device verifica el JoinAccept, y si es valido deriva el AppSKey usando el AppKey, y las llaves FNwkSIntKey, SNwkIntKey y NwkSEncKey de la NwkKey.

Estas llaves se usan para:

- **FNwkSIntKey:** usada para calcular el MIC parcial de los mensajes de UpLink.
- **SNwkSIntKey:** Calcular parcialmente el MIC de los mensajes de uplink y downlink.
- **NwkSEncKey:** encriptar/desencriptar payloads con comandos MAC para garantizar confidencialidad.
- **AppSKey:** Usado para desencriptar los payloads que recibe, aportando a la confidencialidad

ABP (Activation by Personalization)

Tanto para el estandar v1.0.2 y v1.1, todas las llaves son hardcodeadas en el dispositivo. Esto impide que sea reutilizable en otra red.

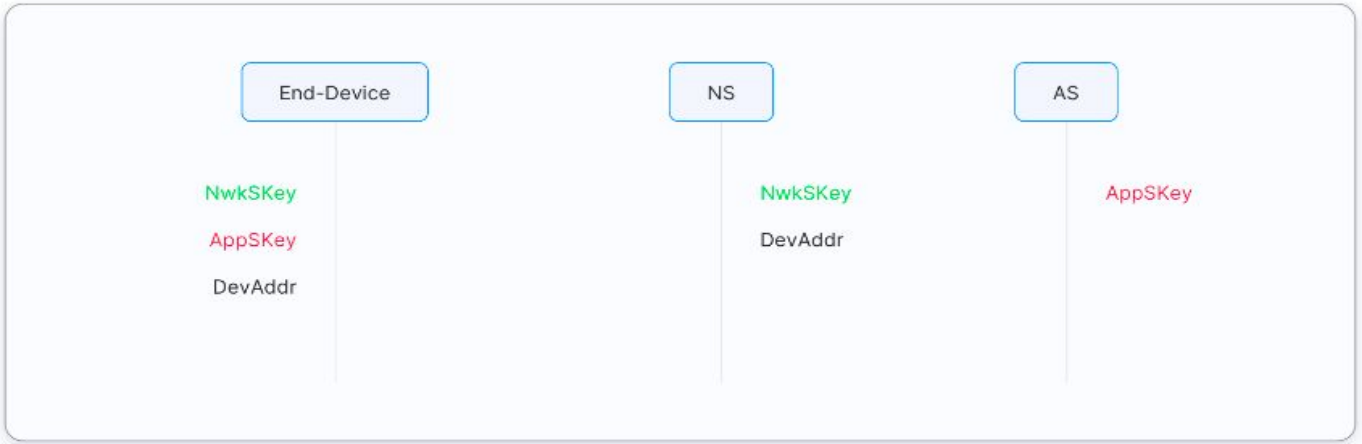


Figure: Pre-sharing DevAddr and session keys for ABP in LoRaWAN 1.0

Figure: Pre-sharing DevAddr and session keys for ABP in LoRaWAN 1.1

¿Cómo podemos implementar una red LoRa Wan?

- HWD mínimo necesario:
  - Gateway LoRa Wan
  - Sistema de computación para alojar el servidor (puede ser montado localmente, o alguna solución en la nube).

Outdoor Gateway

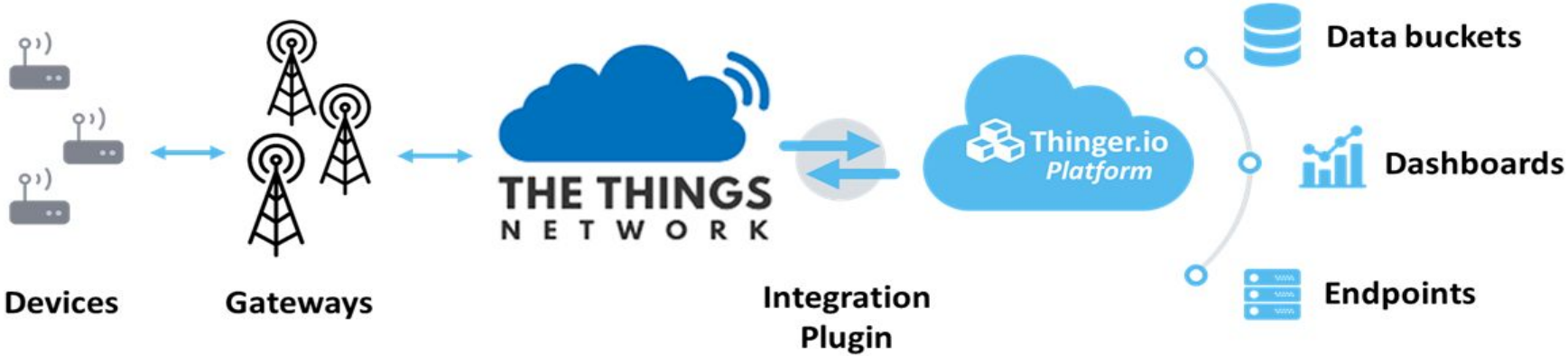
Indoor Gateway

¿Cómo podemos implementar una red LoRa Wan?

- Montar un gateway propio
  - Tiene la ventaja de asegurar una zona con conectividad
  - Tiene la desventaja del costo de compra del equipo, sumado al costo operativo (instalación, roturas, soporte, plan de datos para conexión a internet).
- Usar una Red LoRa Wan Pública de un tercero
  - Suele haber para fines educativos.
- Usar una Red LoRa Wan Privada de un tercero
  - Hay un proyecto de "democratizar" y escalar LoRa Wan a través de sistema de pago por mensaje, llamado Helium-Network

Montando una red… TTN (The things Network)

- Server más utilizado (planes libre de costo, o con mayores prestaciones para uso industrial). Basado en Cloud o con opción local para linux.



We are a global collaborative Internet of Things ecosystem that creates networks, devices and solutions using LoRaWAN®.

Start building Learn more

60.5M	152	1.2K	180.5K	20.8K	1.4M	15.8K	763	14.7
Messages today	Countries	Certified developers	Members	Gateways	YouTube views	YouTube subscribers	GitHub stars	GitHub co

ChirpStack

ChirpStack

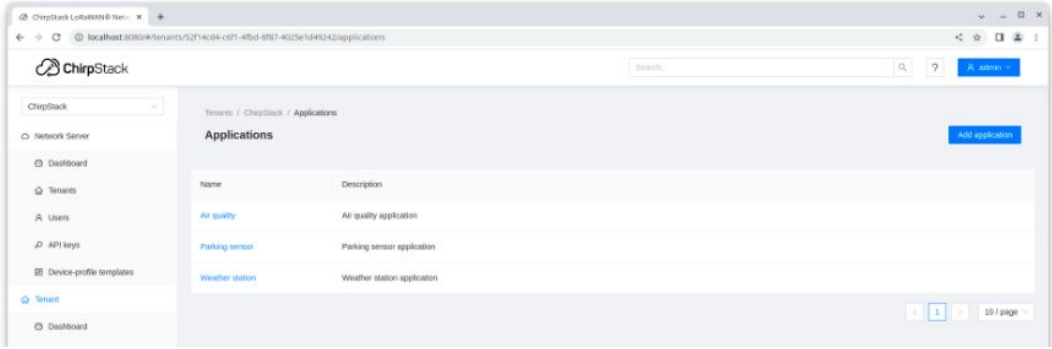
Home | Documentation (v4) | Documentation (v3) | Community forum

Chirpstack v4 is out and brings many improvements! **Read the announcement on the forum**.

ChirpStack, open-source LoRaWAN® Network Server

ChirpStack is an open-source LoRaWAN Network Server which can be used to to setup LoRaWAN networks. ChirpStack provides a web-interface for the management of gateways, devices and tenants as well to setup data integrations with the major cloud providers, databases and services commonly used for handling device data. ChirpStack provides a gRPC based API that can be used to integrate or extend ChirpStack.

Documentation



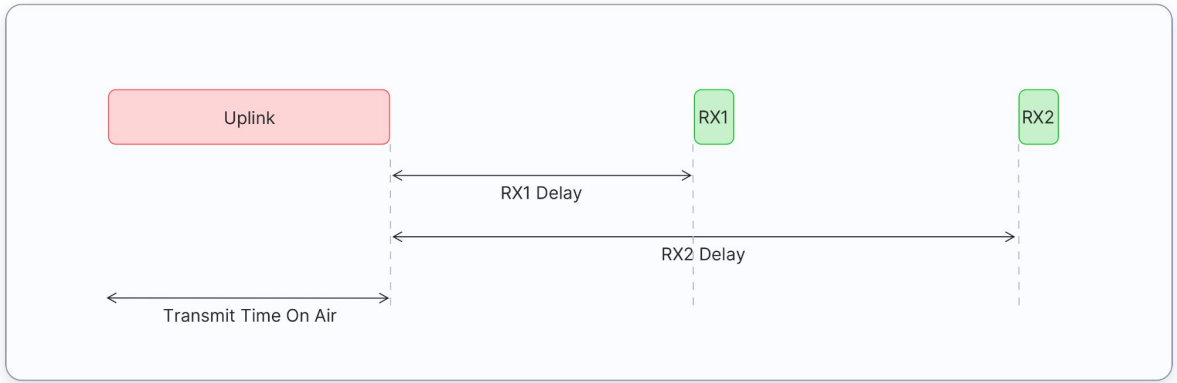
Nodos / End-Devices LoRa Wan

- Nodos de uso industrial, certificados y listos para ser incorporados en una red LoRaWan como los SenseCap de seeedstudio.
- Nodos DIY creados para cumplir con algún uso específico.
- Estos nodos se clasifican en 3 tipos, donde se define su comportamiento y escenario de uso:
  - Clase A
  - Clase B
  - Clase C

Nodo LoRa Wan - Clase A

Características principales:

- Puede enviar un mensaje de Uplink en cualquier momento, luego de cada TX, abre 2 ventanas de escucha para recibir un downlink. El server puede responder en RX1 o RX2.



Nodo LoRa Wan - Clase A

Características principales:

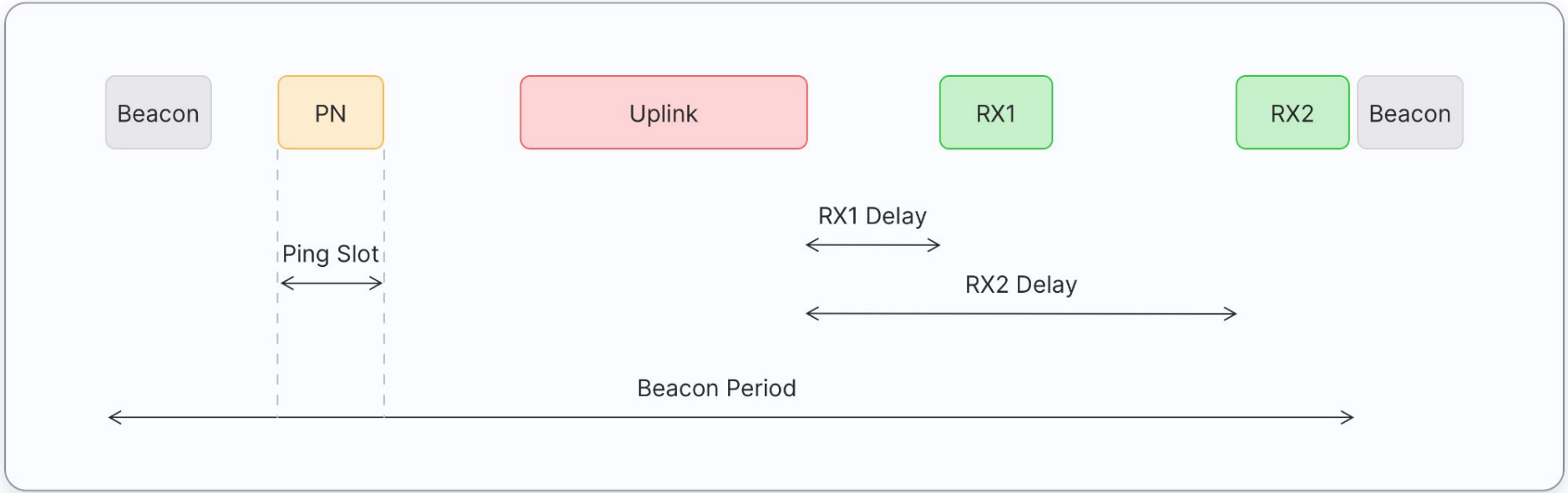
- Pensado para dispositivos a batería (se busca minimizar el consumo al apagar el transceptor y reducir el tiempo en modo RX).
- Permite que el sensor pase mayor parte del tiempo en modo sleep.
- Generalmente, usado para sensores que envían datos con poca frecuencia.

Nodo LoRa Wan - Clase B

Características Principales:

- Similar al Clase A, pero abre de forma periódica ventanas de escucha. Esto requiere de mayor sincronismo con el Network-Server.
- El Gateway envía periódicamente beacons, que son usados por el Nodo para sincronizarse cuando esté en una ventana de escucha.
- El nodo abre ventanas de escucha llamadas “ping slots” en tiempos determinados para poder escuchar estos mensajes de downlink y sincronizarse.
- Al igual que en Clase A, también abrirá ventanas RX1 y RX2 luego de un uplink.
- Mayor consumo que Clase A.
- Común para sensores que deban enviar datos de forma periódica con mayor precisión

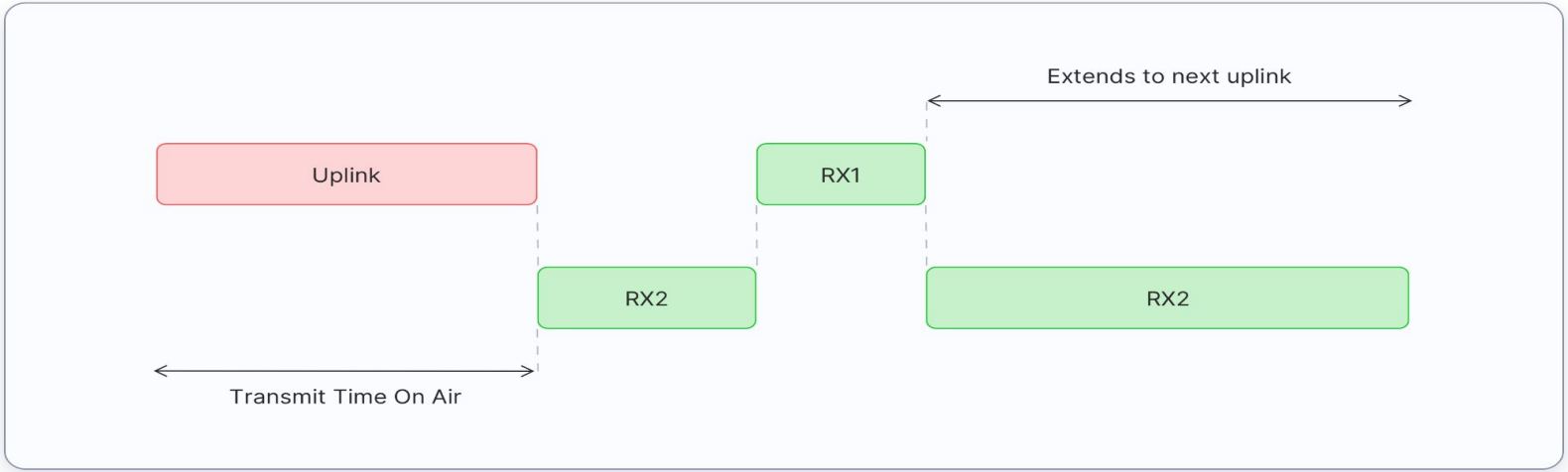
Nodo LoRa Wan - Clase B



Nodo LoRa Wan - Clase C

Característica Principal:

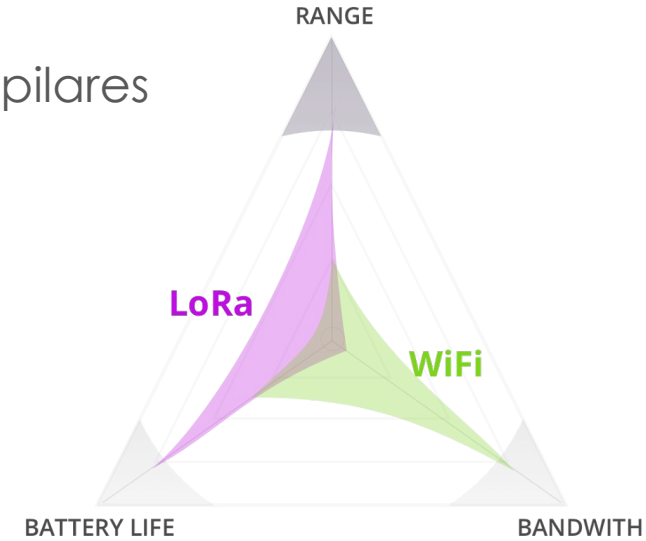
- Si no está transmitiendo, siempre está en modo RX.
- Consumo elevado de batería
- Pensado para sensores que cuentan con alimentación externa.



Comparación de Tecnologías: LoRa WAN vs WiFi

Las diferencias radican en tres pilares fundamentales:

- Rango de cobertura
- Potencia utilizada
- Ancho de banda



Power vs. bandwidth vs. range for wireless communication

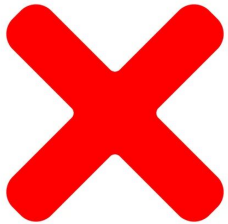
Rango de cobertura:

LoRa Wan:

- Extenso rango de cobertura con un gateway.
- Hasta 10/15 km de distancia en zonas rurales.
- Hasta ~5km en zonas urbanas.

WiFi:

- Poco rango de cobertura.
- Menos de 100 metros.



LoRaWAN

Wi Fi™

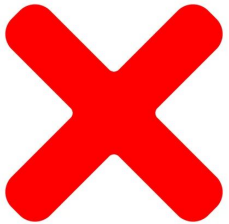
Potencia

LoRaWan:

- Bajo consumo de potencia.
- Larga duración de baterías (5-10 años).
- Modulación de espectro esparcido Chirp (CSS), permite SNR de hasta -20dB(según SF).

WiFi:

- Alto consumo de potencia.
- Poca duración de batería.
- No es un problema.



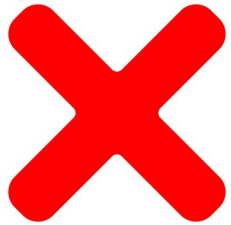
LoRaWAN

Wi Fi

Ancho de banda

LoRa Wan:

- Banda de frecuencias libre (433MHz hasta los 928MHz segun el pais).
- Ancho de banda de 125 kHz, 250 kHz o 500 kHz.
- Según la frecuencia central, cada gateway opera hasta 8 canales simultáneamente.
- Velocidad de transferencia <50kbits/s.
- Capacidad máxima de carga de 242 bytes.



WiFi:

- Banda ISM 2.4GHz y banda no licenciada (U-NII) 5GHz.
- Canales de 20 a 160MHz.
- En 2.4GHz existen hasta 13 canales disponibles (solo 3 simultáneamente).
- Velocidades desde 1Mbit/s hasta +10Gbits/s.

Modelo OSI

Arquitectura de 7 capas en la cual se modela la comunicación de una red.

Beacon

WiFi: los routers avisan la existencia y parámetros de la red mediante esta trama periódica. Mediante ellos, los dispositivos pueden saber de la existencia de la red, sus características, y decidir si ingresar a ella o no.

LoRa: los gateway envían esta trama hacia todos los dispositivos clase B de la red periódicamente. Los nodos usan los beacon para alinear su reloj interno con la red y abrir ventanas de recepción periódicamente.

Método de Acceso al Medio

¿Qué pasa si varios nodos envían datos al mismo tiempo?**Colisión=Error**

Solución: se plantea un modelo para disminuir la probabilidad de colisión.

LoRa Wan utiliza Aloha

- Cuando se tienen datos para enviar, se envían directamente.
- El dispositivo cambia de canal de manera pseudoaleatoria.
- Se debe respetar el ciclo de trabajo del 1%.

WiFi: utiliza CSMA/CA

- Detecta el medio antes de transmitir¿Ocupado? Difiere.
- ¿Libre? Algoritmo back-off aleatorio

Beneficios

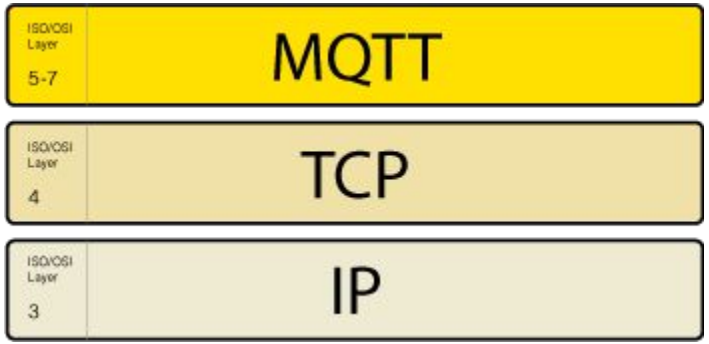
- Bajo consumo y largo alcance
- Bandas sin licencia
- Alta capacidad
- Geolocalización sin GPS (3 gateways)
- Bajo costo y gran ecosistema
- Actualizaciones inalámbricas
- Seguridad de extremo a extremo

LoRaWAN®

Protocolo MQTT

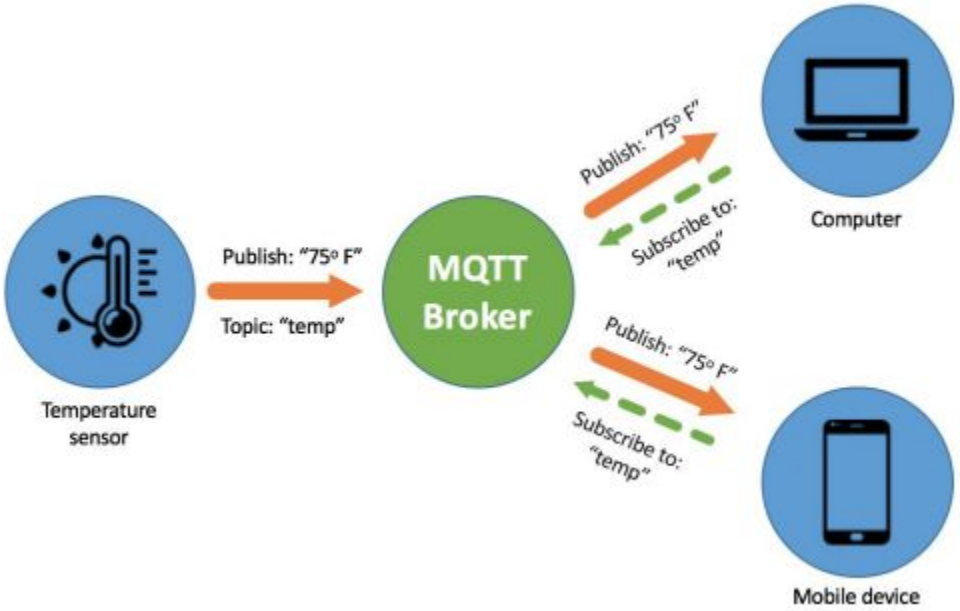
Definición:

"Es un protocolo de transporte de mensajería (de la capa de aplicación) de publicación/suscripción del servidor del cliente. Es liviano, abierto, simple y diseñado para que sea fácil de implementar. Ideal para aplicaciones IoT donde se requiere código de tamaño reducido y/o donde el ancho de banda de la red es un bien escaso "



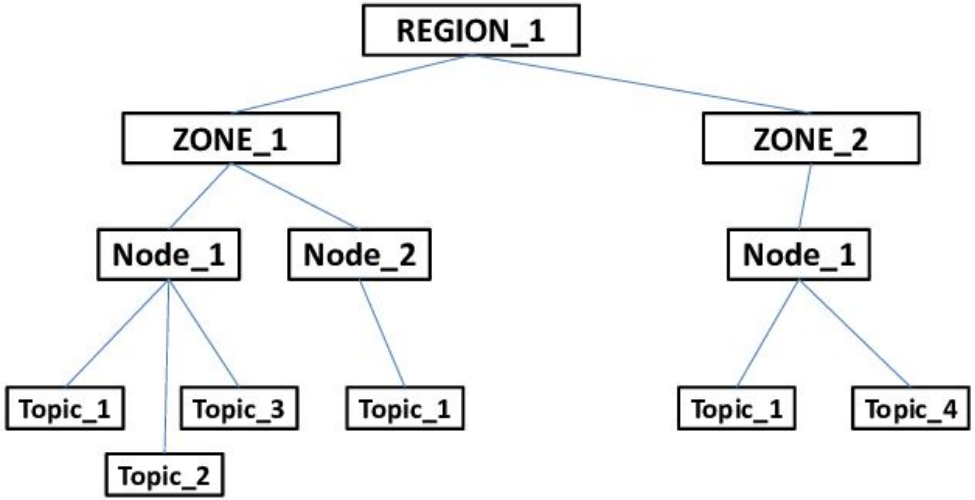
Arquitectura MQTT: publicación y suscripción

- **Broker MQTT:** Este servidor se encarga de desacoplar la comunicación y distribuir la información entre los clientes
- **Cliente:** Es quien publica o se suscribe a un Topic (tópico) pidiéndole al Broker
- **Topic:** Identificación de la información



Jerarquía de Tópicos

El uso de jerarquía permite que el cliente pueda suscribirse a la información de interés.



Tipos y estructura del paquete

- ACK (cliente/servidor)
- Publicación del mensaje (contiene el payload) (cliente hacia servidor)
- Suscripción o dada de baja a tópico (cliente hacia servidor)
- Ping request/response (cliente/servidor)
- Desconexión (cliente hacia servidor)

Figure 2.1 – Structure of an MQTT Control Packet

Fixed header, present in all MQTT Control Packets
Variable header, present in some MQTT Control Packets
Payload, present in some MQTT Control Packets

Table 2.1 - Control packet types

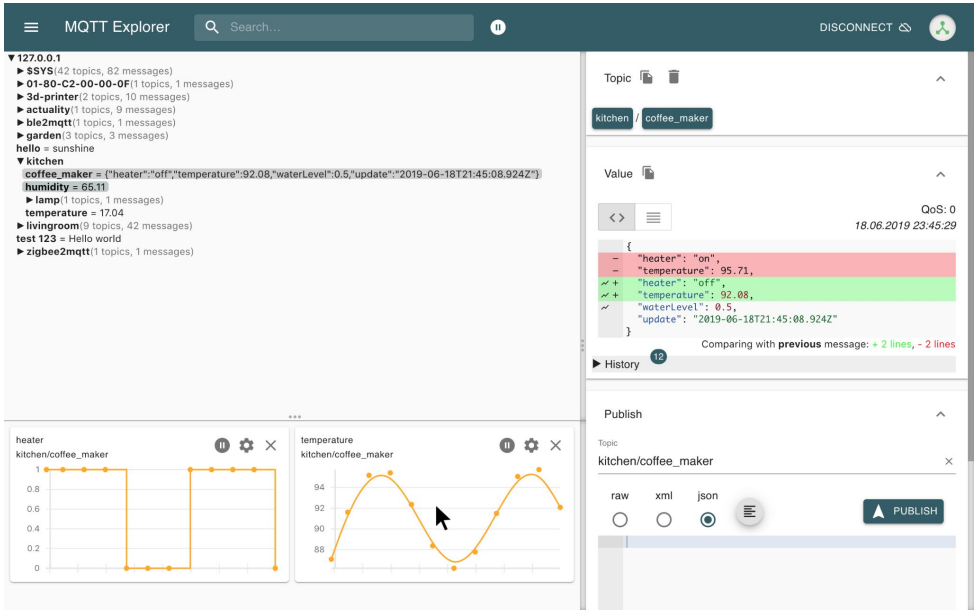
Name	Value	Direction of flow	Description
Reserved	0	Forbidden	Reserved
CONNECT	1	Client to Server	Client request to connect to Server
CONNACK	2	Server to Client	Connect acknowledgment
PUBLISH	3	Client to Server or Server to Client	Publish message
PUBACK	4	Client to Server or Server to Client	Publish acknowledgment
PUBREC	5	Client to Server or Server to Client	Publish received (assured delivery part 1)
PUBREL	6	Client to Server or Server to Client	Publish release (assured delivery part 2)
PUBCOMP	7	Client to Server or Server to Client	Publish complete (assured delivery part 3)
SUBSCRIBE	8	Client to Server	Client subscribe request
SUBACK	9	Server to Client	Subscribe acknowledgment
UNSUBSCRIBE	10	Client to Server	Unsubscribe request
UNSUBACK	11	Server to Client	Unsubscribe acknowledgment
PINGREQ	12	Client to Server	PING request
PINGRESP	13	Server to Client	PING response
DISCONNECT	14	Client to Server	Client is disconnecting
Reserved	15	Forbidden	Reserved

Tipos de paquete de control

Figure 2.1 – Structure of an MQTT Control Packet

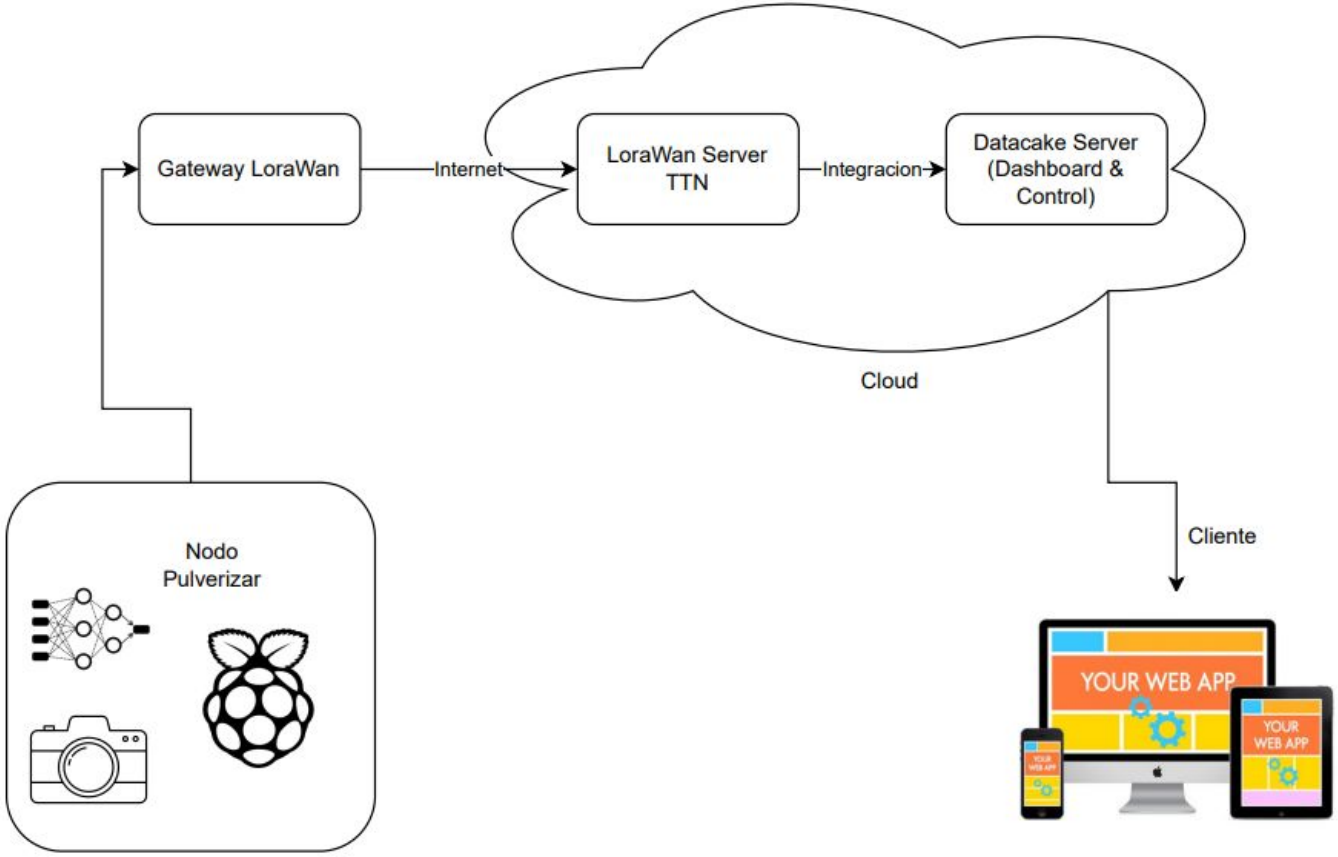
Fixed header, present in all MQTT Control Packets
Variable header, present in some MQTT Control Packets
Payload, present in some MQTT Control Packets

Implementación de sistema IoT con broker MQTT

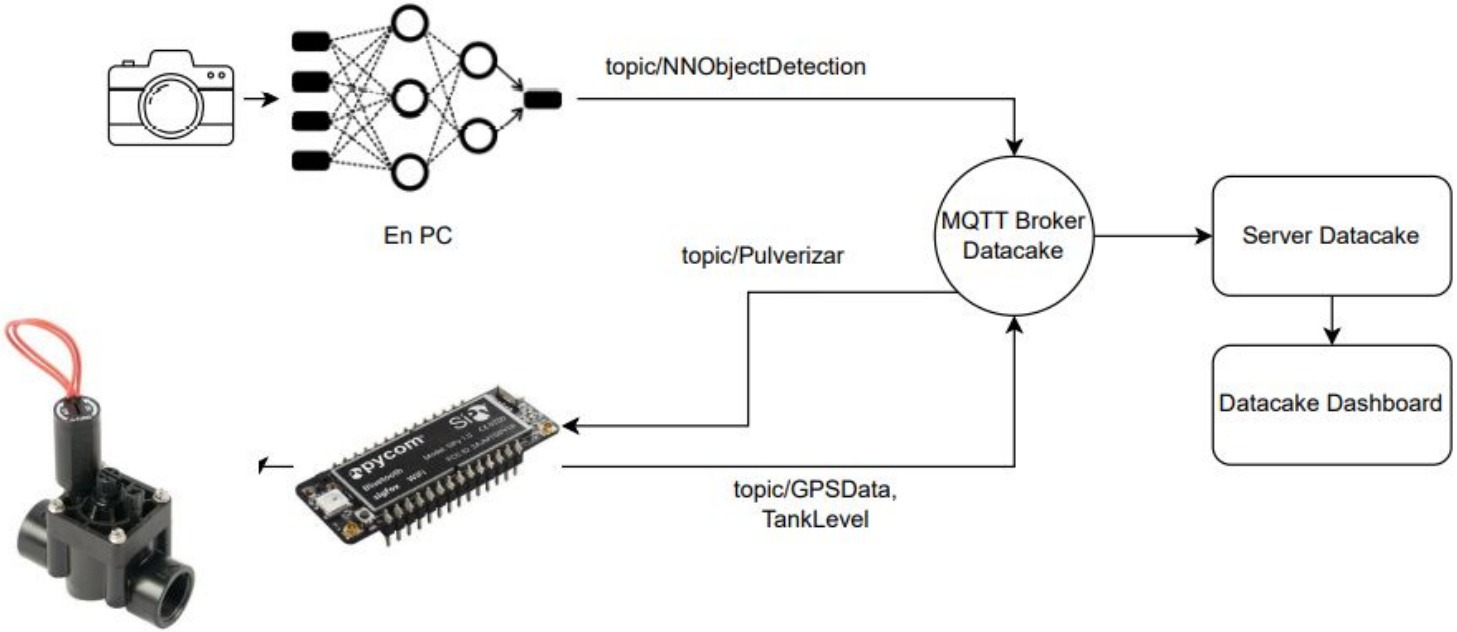


MQTT Explorer es un software que se utiliza como cliente para realizar pruebas de un sistema IoT

Solución PulverizAR



Solución PulverizAR



PulverizAR: Dashboard - WebAPP (LoRa WAN + MQTT)

Conclusiones

- Revisión de conceptos de redes en LoRa WAN
- Comparación de WiFi vs LoRa WAN
- Aplicaciones MQTT en IoT

Links de Referencia

- https://www.oracle.com/ar/internet-of-things/what-is-iot/
- https://www.thethingsnetwork.org/docs/lorawan/
- https://lora-developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/
- https://www.rfwireless-world.com/Tutorials/LoRaWAN-MAC-layer-inside.html
- https://www.thethingsnetwork.org/docs/lorawan/security
- https://www.mokolora.com/es/lora-and-wireless-thecnologies/
- https://lora-alliance.org/
- http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html
- https://www.helium.com/lorawan

MUCHAS GRACIAS

Tomás Allegrini
tallegrini74@gmail.com

Joaquín Ortíz
joaco.ortiz00@gmail.com

Leonardo David Vazquez
vazquezleonardodavid@outlook.com