



UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior de Linares

Trabajo Fin de Grado

DISEÑO E IMPLEMENTACIÓN DE SISTEMA DE MONITORIZACIÓN DE RUIDO ACÚSTICO A TRAVÉS DE UNA RED LoRAWAN

Alumno: Alberto López Casanova

Tutores: Prof. D. José Ángel Fernández Prieto
Andrés del Río Tassara

Depto.: Ingeniería de Telecomunicación



UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior de Linares

Departamento de Ingeniería de Telecomunicación

Don JOSE ANGEL FERNANDEZ PRIETO y Don ANDRES DEL RIO TASSARA como tutores del Trabajo Fin de Grado titulado: DISEÑO E IMPLEMENTACION DE SISTEMA DE MONITORIZACION DE RUIDO ACUSTICO A TRAVES DE UNA RED LORAWAN; autorizan su presentación para defensa y evaluación en el Campus Científico – Tecnológico de Linares.

Linares, Junio de 2022.

El alumno:

El tutor:

El tutor:

Alberto López Casanova

Andrés del Río Tassara.

José Ángel Fernández Prieto

INDICE

1. RESUMEN	7
2. ABSTRACT	8
3. INTRODUCCIÓN	9
4. OBJETIVOS	13
5. FUNDAMENTOS LORAWAN	14
5.1 INTRODUCCIÓN AL IOT	14
5.2 REDES LPWAN	16
5.2.1 <i>LoRa y LoRaWAN</i>	18
6. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA	34
6.1 PERSPECTIVA GENERAL	35
6.1.1 <i>Arquitectura de red</i>	36
6.2 DESARROLLO DEL SISTEMA	38
6.2.1 <i>Dispositivo sensor</i>	38
6.2.2 <i>Gateway</i>	41
6.2.3 <i>Application Server / Plataforma IoT</i>	52
7. RESULTADOS	73
7.1 INSTALACIÓN DEL DISPOSITIVO SENSOR Y GATEWAY	73
7.2 GRÁFICAS DE NIVELES DE RUIDO Y NOTIFICACIONES EN AMBAS PLATAFORMAS IOT	76
8. CONCLUSIONES Y LÍNEAS DE FUTURO	79
8.1 COMPARATIVA DE LAS DOS PLATAFORMAS IOT UTILIZADAS.....	80
8.2 LÍNEAS DE FUTURO	81
9. ESTUDIO ECONÓMICO	82
10. BIBLIOGRAFÍA	83
11. ANEXOS	85
ANEXO I: HOJA DE CARACTERÍSTICAS DEL SENSOR ELSYS ERS SOUND.....	85
ANEXO II: HOJA DE CARACTERÍSTICAS DEL GATEWAY MULTITECH CONDUIT IP67.	89
ANEXO III: CÓDIGO DEL NODO ‘ARRAYBIN TO STRINGHEX’	93
ANEXO IV: CÓDIGO DEL NODO ‘ELSYS DECODER’	93
ANEXO V: MANUAL DE INSTALACIÓN DEL GATEWAY MULTITECH CONDUIT IP67	95

INDICE DE FIGURAS

Figura 1.	Salud y niveles de ruido	9
Figura 2.	Medición ruido acústico en industria con sonómetro. Fuente: Induanalisis	10
Figura 3.	Diagrama general de la red.....	12
Figura 4.	Origen IoT. Fuente: Cisco IBSG.....	15
Figura 5.	Casos de uso del IoT. Fuente: Fostec&Company	15
Figura 6.	Diferentes tecnologías inalámbricas. Fuente: Peter R.Egli 2015.	17
Figura 7.	Diferentes redes LPWAN. Fuente: Nokia White Paper, LTE-M.....	17
Figura 8.	Pila de Protocolos LoRa/LoRaWAN. Fuente: LoRa Alliance.	18
Figura 9.	Arquitectura general red LoRaWAN. Fuente: Industrial M2M by Logitek.	20
Figura 10.	Capas de seguridad en LoRaWAN. Fuente: StackExchange[10].	22
Figura 11.	Duración de chirp en función del SF. Fuente: ETSI [11].....	23
Figura 12.	DR en base al SF . Fuente: ETSI [11].	23
Figura 13.	DR en el protocolo LoRaWAN Fuente: ETSI [11].....	24
Figura 14.	Canales por defecto en LoRaWAN. Fuente: ETSI [11].	24
Figura 15.	Ejemplo de señal CSS en LoRaWAN. Fuente: ETSI [11].....	25
Figura 16.	Comunicación Clase A. .Fuente: Witekio	26
Figura 17.	Comunicación Clase B. Fuente: Witekio.	27
Figura 18.	Comunicación Clase C. Fuente: W.itekio	27
Figura 19.	Método de activación OTAA LoRaWAN. Fuente: Cisco.	30
Figura 20.	Método de activación ABP LoRaWAN. Fuente: Cisco.....	31
Figura 21.	Red LoRaWAN con Network Server dedicado. Fuente: Ursalink.....	32
Figura 22.	Red LoRaWAN con Network Server embebido en Gateway. Fuente: WoMaster.....	33
Figura 23.	Diagrama general de la red.....	37
Figura 24.	Sensor Elsys ERS Sound LoRaWAN. Fuente: Elsys.....	38
Figura 25.	App para configuración del sensor en la App Store (IOS).....	38
Figura 26.	Inicio app Elsys.	39
Figura 27.	Claves del sensor.....	40
Figura 28.	Configuración LoRaWAN en el sensor.	40
Figura 29.	Data Rate del sensor.	41
Figura 30.	Gateway Multitech Conduit IP 67 Base Station. Fuente: Multitech.....	42
Figura 31.	Cambio de IP a la interfaz ethernet	42
Figura 32.	Pantalla inicial de configuración del Gateway	43
Figura 33.	Configuración del Gateway en modo Network Server.	44
Figura 34.	Sensor Elsys añadido en el Gateway.....	44
Figura 35.	Claves del sensor añadidas en el Gateway	45
Figura 36.	Sesión OTAA entre el sensor y el Gateway	45

Figura 37.	Flujo 1 del Node-Red en el Gateway.....	46
Figura 38.	Campos trama LoRa	47
Figura 39.	Nodo LoRa flujo 1.....	47
Figura 40.	Nodo Clasifica Trama flujo 1.	48
Figura 41.	Nodo http request flujo 1	49
Figura 42.	Flujo 2 Node-Red en el Gateway	50
Figura 43.	Nodo Swith 1 flujo 2.....	51
Figura 44.	Nodo Switch 2 Flujo 2.	52
Figura 45.	Nodo para asignación de token en flujo 2	52
Figura 46.	Tabla ‘medidas’ y sus columnas en la BBDD MySQL	55
Figura 47.	Flujo Node-Red de recepción de datos en el CPD.	56
Figura 48.	Nodo servidor http en flujo de recepción en el CPD.	57
Figura 49.	Nodo conversión a JSON en flujo de recepción en el CPD.	57
Figura 50.	Nodo MySQL en flujo de recepción en Node-Red	58
Figura 51.	Registro de datos en la BBDD.	59
Figura 52.	Inclusión de repositorio Grafana.	60
Figura 53.	Acceso a la paltforma Grafana	61
Figura 54.	Sección Añadir fuente de datos en Grafana.	61
Figura 55.	Conexión con la BBDD MySQL en Grafana.	62
Figura 56.	Creación de dashboard en Grafana.	63
Figura 57.	Query a la BD para representación de la media de ruido.....	63
Figura 58.	Configuración visualización de la media de ruido.	64
Figura 59.	Query a la BD para la representación del nivel de pico de ruido.	64
Figura 60.	Creación del canal de notificaciones Telegram en Grafana.	65
Figura 61.	Obtención del token de Telegram.	66
Figura 62.	Obtención del Chat ID de Telegram.....	66
Figura 63.	Recepción de notificación de test de Grafana.	67
Figura 64.	Configuración alerta Grafana para nivel de ruido medio.	68
Figura 65.	Configuración alerta Grafana para nivel pico de ruido.....	68
Figura 66.	Pantalla inicial de In4city.	69
Figura 67.	Creación de destinatarios en In4city.	70
Figura 68.	Creación notificaciones en In4city.	71
Figura 69.	Introducción del Gateway en In4city.	71
Figura 70.	Introducción sensor Elsys en In4city.....	72
Figura 71.	Información de dispositivos en línea en In4city	72
Figura 72.	Orificios de la tapa trasera del sensor Elsys. Fuente: Elsys.....	74
Figura 73.	Instalación tapa trasera del sensor	74

Figura 74.	Sensor Elsys instalado en la cafetería de Geolit.	74
Figura 75.	Gateway instalado en la sala Demo	75
Figura 76.	Gráficas niveles de ruido acústico presentes en la cafetería de Geolit. Grafana.	76
Figura 77.	Recepción de notificaciones vía Telegram. Grafana.....	77
Figura 78.	Gráfica del nivel de ruido acústico presente en la cafetería de Geolit. In4city.	78
Figura 79.	Recepción de notificaciones en In4city.	78

1. Resumen

La contaminación acústica es uno de los factores ambientales que más efectos perjudiciales provoca tanto en las personas como en el medio ambiente, lo que ha llevado a buscar soluciones. Existen herramientas software de simulación que permiten estimar los medir los niveles de ruido acústico en un entorno. Sin embargo, la Comisión Europea (CE) sugiere que estos niveles sean el resultado de tomar mediciones *in-situ* con sonómetros. Con el auge del *Internet of things (IoT)* o Internet de las Cosas surgen redes de sensores de largo alcance y bajo consumo con conectividad a Internet, lo cual las dota con la capacidad de monitorizar cambios en el entorno de forma remota y constante.

El presente Trabajo Fin de Grado (TFG) realizado en colaboración con la empresa Innovasur S.L, aborda el diseño e implementación de una red Long Range Wide Area Network (LoRaWAN) privada para la monitorización del nivel de ruido acústico presente en un entorno urbano. Para ello, se hace uso de un sensor que capta el nivel de presión sonora (dBSPL) y envía los datos generados mediante LoRa a una pasarela o *Gateway*. Este dispositivo se comunica mediante el protocolo de internet (IP) con los demás elementos de la red. Los datos son procesados y finalmente representados en dos plataformas en la nube, de forma que cualquier usuario con conectividad a Internet pueda visualizar dicha información en tiempo real. Además, el sistema cuenta con un servicio de notificaciones.

2. Abstract

Noise pollution is one of the environmental factors that has the most detrimental effects on both people and the environment, which has led to the search for solutions to reduce it. Simulation software tools are available to estimate and measure noise levels in an environment. However, the European Commission (EC) suggests that these levels should be the result of taking in-situ measurements with sound level meters. With the rise of the Internet of things (IoT) or Internet of Things, long-range and low-power sensor networks with Internet connectivity are emerging, which provides them with the ability to monitor changes in the environment remotely and constantly.

This Final Degree Project (FDP), carried out in collaboration with the company Innovasur S.L., deals with the design and implementation of a private Long Range Wide Area Network (LoRaWAN) for monitoring the level of acoustic noise in an urban environment. To do this, a sensor is used to capture the sound pressure level (dBSPL) and send the data generated by LoRa to a gateway. This device communicates via internet protocol (IP) with the other elements of the network. The data is processed and finally represented on two platforms in the cloud, so that any user with Internet connectivity can view this information in real time. In addition, the system has a notification service.

3. Introducción

La contaminación acústica se define como “ la presencia en el ambiente de ruidos o vibraciones, cualquiera que sea el emisor acústico que los origine, que impliquen molestia, riesgo o daño para las personas, para el desarrollo de sus actividades o que causen efectos significativos sobre el medio ambiente” [1]. Según la Organización Mundial de la Salud (OMS), es uno de los factores ambientales que más problemas de salud provoca. Sólo en Europa es el segundo factor ambiental más perjudicial, por detrás de la contaminación atmosférica; sin embargo, su impacto en la salud es similar a esta última. Cuando el ruido es de gran intensidad provoca efectos auditivos como sordera. Sin embargo, si es excesivo y mantenido en el tiempo surgen efectos de otra índole: psicológicos (estrés, depresión...), sueño y conducta (irritabilidad, agresividad...), memoria y atención (disminución de la capacidad de atención y rendimiento intelectual). Además, cabe destacar que las fuentes de las que puede proceder la contaminación acústica son variadas, destacando la procedente de la industria, tráfico automovilístico, restauración y ocio nocturno, etc.

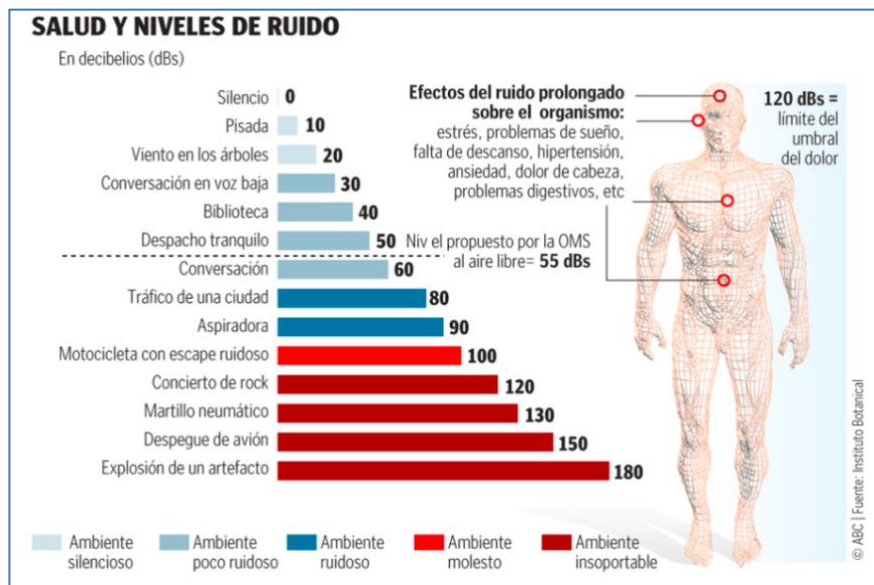


Figura 1. Salud y niveles de ruido

A pesar de ello, no es hasta principios del presente siglo que se comienza a crear políticas que regulen este fenómeno. En el año 2002 se aprueba la primera directiva europea sobre el ruido (2002/49/E) [2] la cual tiene por objeto la adopción por parte de los estados miembros de un enfoque común dirigido a reducir los efectos nocivos de la contaminación sonora. Para ello, los Estados miembros deben acordar métodos de

evaluación comunes que permitan recopilar información acerca del ruido presentada en forma de 'mapas de ruido', siendo revisados cada cinco años. En base a ello se crean planes de acción para reducir y prevenir los daños producidos por la contaminación acústica. Además, la información sobre el ruido y sus efectos deben ser puestos a disposición de la población. Un año después, en el 2003 se aprueba en España la primera Ley del ruido (37/2003) [3].

Para la elaboración de mapas de ruido existen dos métodos: simulación y muestreo. El primero consiste en la obtención de mapas de ruido mediante técnicas de cálculo y software. Los parámetros de entrada son modelos matemáticos de fuentes sonoras, obstáculos, etc.; es decir, cualquier elemento que tenga efectos en la propagación y recepción del ruido. El segundo método consiste en la realización de campañas de mediciones directas de ruido haciendo uso de sonómetros, durante al menos un año. Este método es más costoso y requiere de más tiempo, sin embargo, los niveles obtenidos son reales pues se trata de un método empírico. Cabe destacar que el nivel de ruido acústico se mide en decibelios ponderados (dBA). Esto es, el nivel de presión sonora para cuya medición se filtran las bajas y altas frecuencias, para las cuales el oído humano es menos sensible.

A pesar de arrojar datos reales sobre la contaminación acústica, la medición de ruido con sonómetros cuenta con una serie de desventajas. En primer lugar, estas deben ser realizadas por personal cualificado para ello. Sin embargo, el mayor problema es la incapacidad de monitorizar continuamente y en tiempo real los niveles de ruido; ya que como es lógico es inviable mantener un técnico con un sonómetro las 24 horas del día en un emplazamiento.



Figura 2. Medición ruido acústico en industria con sonómetro. Fuente: Induanalisis

En los últimos años se ha podido observar un crecimiento exponencial del IoT; dispositivos interconectados entre sí en tiempo real por medio de Internet. Son muchos los ámbitos de aplicación de este paradigma: logística, automatización industrial, ciudades inteligentes, etc. Esta interconexión permite que los dispositivos se comuniquen entre sí intercambiando datos y pudiendo ser estos accedidos desde cualquier parte con acceso a Internet, concepto llamado Interacción Machine to Machine (M2M). La tecnología inalámbrica es una vía fundamental por la que los dispositivos inteligentes se comunican entre sí y con Internet. En este marco cobran especial importancia las redes de sensores inalámbricos o por su siglas en inglés, WSN. Estas redes están formadas por sensores y actuadores capaces de monitorizar su entorno de forma continua y tomar decisiones respecto a los datos obtenidos [4]. La unión de estas redes de sensores y el IoT ha dado lugar a que estas tecnologías cobren especial interés en ámbitos como digitalización de hogar, industria o ciudades.

Surge en las redes de sensores inalámbricos conectados a Internet una solución a la problemática de la medición de ruido. En este ámbito, estas redes permiten la monitorización constante de los niveles de ruido ambiental a un coste relativamente bajo. Dado que una vez instalados los sensores no se hace necesario la toma de mediciones in-situ, hacen de esta una solución más cómoda y eficiente que el método tradicional. Junto a las nombradas anteriormente, cuenta con otras ventajas como: fácil escalabilidad, recopilación de datos durante largos periodos de tiempo, fácil movilidad, etc.

En este TFG se presenta el desarrollo e implementación de una red LoRaWAN privada para la monitorización del ruido acústico presente en un entorno urbano. Para el testeo del sistema, el sensor se ha instalado en la cafetería del Parque Científico y Tecnológico de Geolit con la colaboración de los técnicos instaladores de la empresa. Este trabajo ha sido realizado en colaboración con la empresa Innovasur S.L, y nace de la motivación de desarrollar una solución IoT enmarcada en el ámbito de *Smart Cities*, con el objetivo de monitorizar en tiempo real la contaminación acústica para tomar decisiones que mejoren la calidad ambiental.

Para la realización de este TFG se diseña la topología de red, se lleva a cabo la configuración de los dispositivos hardware que la componen, así como de los servicios software. Un sensor LoRa es el encargado de medir el nivel de presión sonora. Este sensor entrega como salida dos parámetros: nivel medio de ruido (*sound-average*) y

nivel de pico (*peak-sound*), ambos en decibelio del nivel de presión sonora (dB SPL). Estos datos son enviados vía LoRa a una pasarela o *Gateway*. Este último es el elemento central de la red encargado dar cobertura al nodo, y entre otras funciones, comunicar con el servidor de red y de aplicación mediante el protocolo IP. Como resultado final, los datos son representados en dos plataformas IoT: una plataforma *open-source* y otra, de la cual es propietaria de la empresa colaboradora. Además, ambas plataformas son dotadas con un servicio de notificaciones. El diagrama general de la red se presenta en la Figura 3.

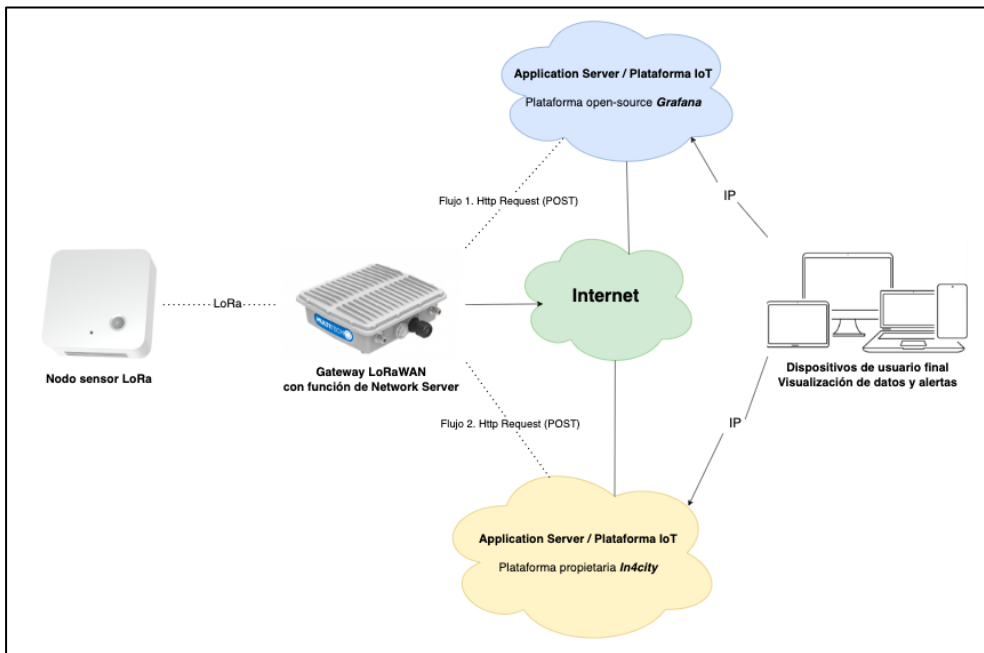


Figura 3. Diagrama general de la red.

4. Objetivos

El objeto principal de este TFG es la monitorización del ruido acústico a través de una red LoRaWAN privada. Para ello se ha de conseguir los siguientes objetivos específicos cuya consecución permita alcanzar el objetivo principal:

1. Estudiar la arquitectura y funcionamiento de una red LoRaWAN así como de los componentes que la conforman.
2. Diseñar la topología o arquitectura de red, de tal forma que queden reflejadas las interconexiones entre elementos de la red, así como las funciones de cada uno de ellos.
3. Configurar los diferentes componentes del sistema LoRaWAN tales como: sensor LoRa, Gateway Bridge, Network Sever y Application Server/ Plataforma IoT.
4. Programar los flujos de Node-Red en el Network Server y Application Server/ Plataforma IoT.
5. Representar los datos obtenidos por el sensor tanto en una plataforma IoT *Open-Source* como en una propietaria de la empresa Innovasur S.L con el fin de comparar ambas plataformas.
6. Dotar al sistema IoT con un servicio de notificaciones.
7. Instalar los elementos de la red, así como realizar la interconexión de estos con el fin de implementar el sistema en un entorno urbano real.
8. Comprobar el correcto funcionamiento del sistema. Para ello se verifica que se recogen y representan correctamente los datos además de que se reciben las notificaciones de aviso generadas en el *back-end* de la red LoRaWAN.

5. Fundamentos LoRaWAN

Este capítulo está pensado para dotar al lector de las nociones básicas relativas al funcionamiento y componentes de una red LoRaWAN. En primer lugar, se realiza una breve introducción al IoT. Tras ello, se presentan las redes LPWAN y se exponen diferentes razones para el uso de este tipo de redes frente a otras. Finalmente se describen los elementos que componen una especificación de red LPWAN, las redes LoRaWAN.

5.1 Introducción al IoT

Cada vez vivimos en un mundo y una sociedad más conectados gracias al gran auge de Internet y las tecnologías desarrolladas en torno a este. Hoy en día el mundo físico y digital van de la mano y cooperan entre sí, siendo en ciertos escenarios, dependientes el uno del otro. A pesar de suponer esto una mayor dependencia de la tecnología, lo cual tiene su parte negativa, no se puede negar la mejora que la digitalización aporta a la calidad de vida de las personas y las relaciones interpersonales. El número de dispositivos conectados a Internet ha aumentado exponencialmente en los últimos años, y sigue en aumento. Se prevé que el número de dispositivos conectados se triplique a nivel mundial durante los próximos años [5]. IoT se define como una tendencia basada en la interconexión de dispositivos y objetos a través de Internet, los cuales se encargan de medir, recopilar, enviar e intercambiar datos entre sí con el fin de ser almacenados en un servidor centralizado o en la nube para posteriormente ser representados a modo informativo (mostrar estadísticas) o bien ser procesados con algún fin.

A pesar de coger más fuerza en estos últimos años, el concepto de IoT no es nuevo. Este término fue usado públicamente por primera vez en 2009 por Kevin Ashton, experimentando desde entonces un crecimiento exponencial. Aunque él mismo ha comentado que la expresión era de uso corriente en círculos internos de investigación desde 1999, no se hizo público de forma notoria hasta entonces [6]. Sin embargo, según el Grupo de soluciones empresariales basadas en Internet (IBSG, Internet Business Solutions Group) de Cisco, IoT es sencillamente el punto en el tiempo en el que se conectaron a Internet más “cosas u objetos” que personas. Es por tanto que Cisco IBSG estima que IoT “nació” en algún punto entre 2008 y 2009 [7].

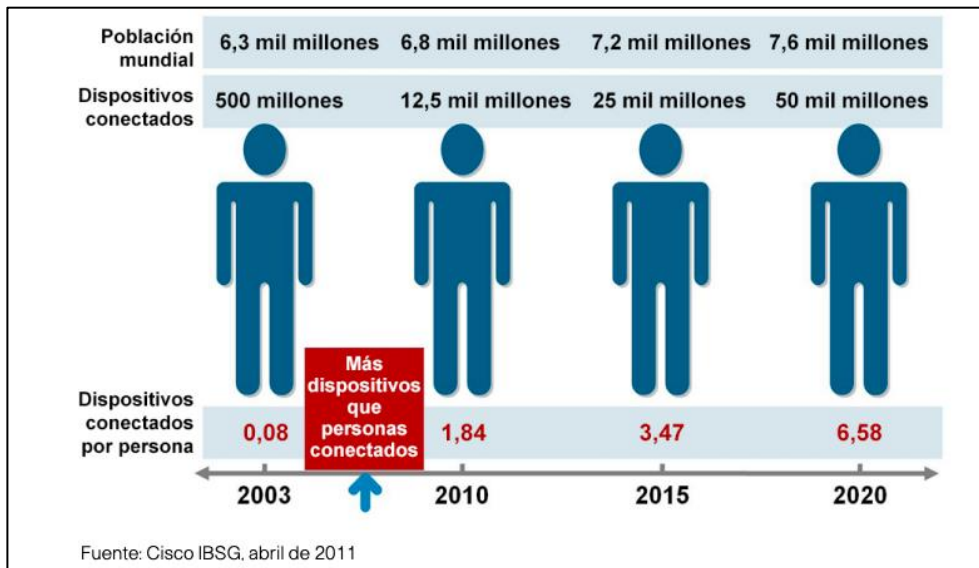


Figura 4. Origen IoT. Fuente: Cisco IBSG.

Son muchas las aplicaciones que tiene el IoT y las necesidades que busca satisfacer, pudiendo destacar entre los espacios de operación de este: edificios, empresas, espacios públicos, automóviles, agricultura y también las propias personas. A pesar de parecer a priori ámbitos de aplicación independientes, todos tienen un objetivo común. Este objetivo es la digitalización de la sociedad, la cual trae consigo una serie de beneficios como: aceleración de la productividad, automatización de procesos y el ahorro de recursos. En definitiva, la idea principal en la que se sustenta es la de mejorar la calidad de vida de quienes lo usan y aplican.

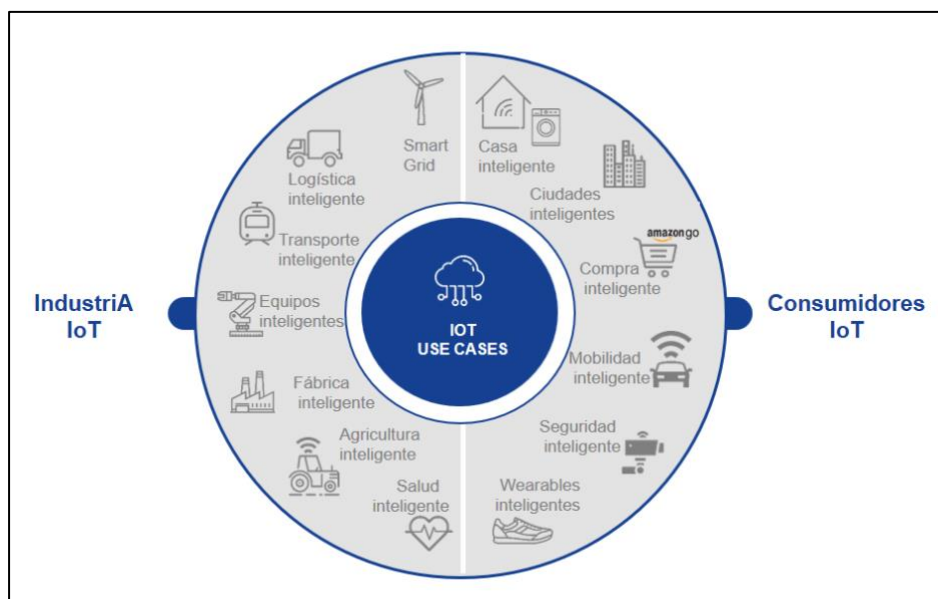


Figura 5. Casos de uso del IoT. Fuente: Fostec&Company

5.2 Redes LPWAN

Las tecnologías de comunicación son un importante componente en el IoT. Para garantizar la viabilidad económica y expansión del IoT es importante que estas redes sean económicas y los nodos finales cuenten con baterías de larga duración y bajo consumo para ello. Podemos establecer tres ejes principales cuando se habla de soluciones IoT: alcance, consumo y capacidad de transmisión; sin embargo, no existe una tecnología que consiga aunar estas características completamente de forma conjunta. Por ejemplo, las redes de comunicaciones móviles inalámbricas como el 4G a pesar de su alcance y alta capacidad de transmisión, cuentan con un alto consumo tanto a nivel de red como de dispositivos finales. En el otro lado de la balanza tenemos el ejemplo de la tecnología Bluetooth, que a pesar de tener un consumo energético bajo y una capacidad de transmisión aceptable, cuenta con un alcance muy limitado. En este ámbito, las comunicaciones cableadas quedan descartadas dado que, a pesar de ofrecer una excelente calidad, su despliegue conlleva un alto coste tanto económico como humano.

Entre las diferentes tecnologías de comunicación disponibles, cobran especial interés las redes *Low Power Wide Area Network* (LPWAN). Las redes LPWAN engloban las tecnologías y protocolos de comunicación inalámbrica que permiten el intercambio de datos entre dispositivos y Gateways separados distancias de kilómetros con un bajo consumo energético. Las principales características de estas redes son las siguientes:

- **Largo alcance:** Entre 5 km en entornos urbanos y 15 km en entornos rurales.
- **Bajo consumo:** Esto permite que los nodos finales cuenten con una vida útil de hasta 20 años .
- **Capacidad de transmisión:** Pensada para la transmisión no constante de pequeñas cantidades de datos.
- **Bajo coste:** El bajo consumo de estas redes unido al uso de banda de frecuencias *Industrial, Scientific and Medical* (ISM) de licencia libre reduce significativamente el coste de estas.

Estas características hacen las redes LPWAN se entiendan como básicas hoy en día para la implementación de soluciones IoT de banda estrecha, bajo consumo y largo alcance.

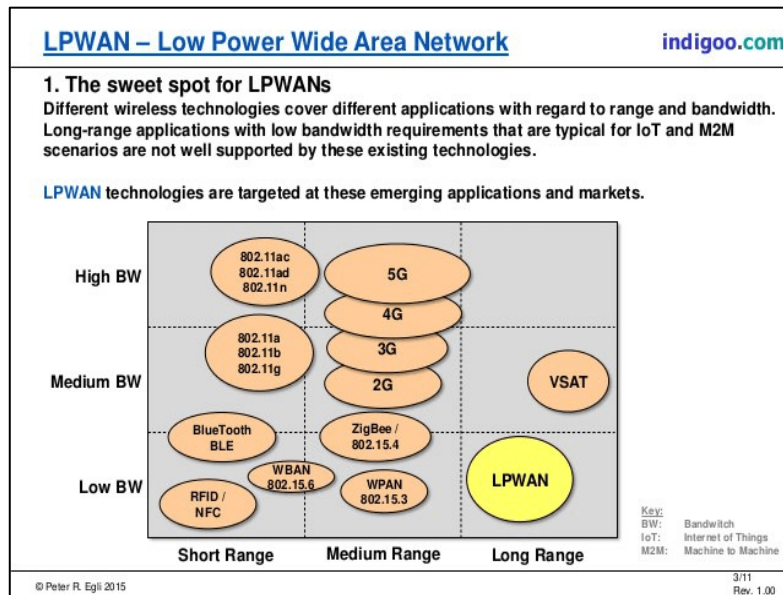


Figura 6. Diferentes tecnologías inalámbricas. Fuente: Peter R.Egli 2015.

En la Figura 6, se observa como LPWAN sacrifica la capacidad de transmisión con el fin de tener un largo alcance y bajo consumo de red. Esto es precisamente lo que la diferencia de una red WAN inalámbrica la cual está pensada para conectar usuarios/empresas con un ancho de banda mayor. En base a LPWAN podemos encontrar diferentes estándares y proveedores entre los que destacan Sigfox, LoRaWAN y NB-IoT entre otros.

	SIGFOX	LoRa	clean slate cloT	NB LTE-M Rel. 13 lte	LTE-M Rel. 12/13 lte	EC-GSM Rel. 13 GSM	5G (targets) 5G
Range (outdoor) MCL	<13km 160 dB	<11km 157 dB	<15km 164 dB	<15km 164 dB	<11km 156 dB	<15km 164 dB	<15km 164 dB
Spectrum Bandwidth	Unlicensed 900MHz 100Hz	Unlicensed 900MHz <500kHz	Licensed 7-900MHz 200kHz or dedicated	Licensed 7-900MHz 200kHz or shared	Licensed 7-900MHz 1.4 MHz or shared	Licensed 8-900MHz 2.4 MHz or shared	Licensed 7-900MHz shared
Data rate	<100bps	<10 kbps	<50kbps	<150kbps	<1 Mbps	10kbps	<1 Mbps
Battery life	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years
Availability	Today	Today	2016	2016	2016	2016	beyond 2020

Figure 3. LPWA IoT connectivity overview

Figura 7. Diferentes redes LPWAN. Fuente: Nokia White Paper, LTE-M.

Cada uno de estos estándares tiene distintos modos de funcionamiento, estructura de red, estrategias de negocio y limitaciones. LoRaWAN es una especificación de LPWAN que hace uso a nivel físico de la técnica de modulación LoRa.

Estas redes son ideales para la creación de redes privadas ya que con la configuración de un Gateway propio se crea una red única y segura. Esto es especial interés para empresas tecnológica que no quieran añadir dispositivos de terceros en sus propias redes para salvaguardar su seguridad. Es por ello que este TFG se desarrolla en base a una red LoRaWAN.

5.2.1 LoRa y LoRaWAN

En primer lugar, es importante diferenciar de forma clara LoRa y LoRaWAN , ya que son términos habitualmente usados erróneamente de manera ambigua debido en la mayoría de veces al nombre. Esta diferenciación es importante puesto que ocupan diferentes roles dentro de la jerarquía de capas de esta tecnología. LoRaWAN es un protocolo de red que usa la tecnología de modulación LoRa para comunicar y administrar nodos LoRa para redes de baja potencia y largo alcance. LoRa en cambio es una tecnología de modulación inalámbrica de radiofrecuencia la cual define la capa física dentro de la jerarquía de capas de la arquitectura LoRaWAN, responsable de permitir el envío y recepción punto a punto entre nodo final y Gateway. En pocas palabras y a grandes rasgos, “LoRa es la modulación que emplean los dispositivos para lograr una alta cobertura con baja potencia. LoRaWAN es el protocolo que dicta como se envían los paquetes” [8].

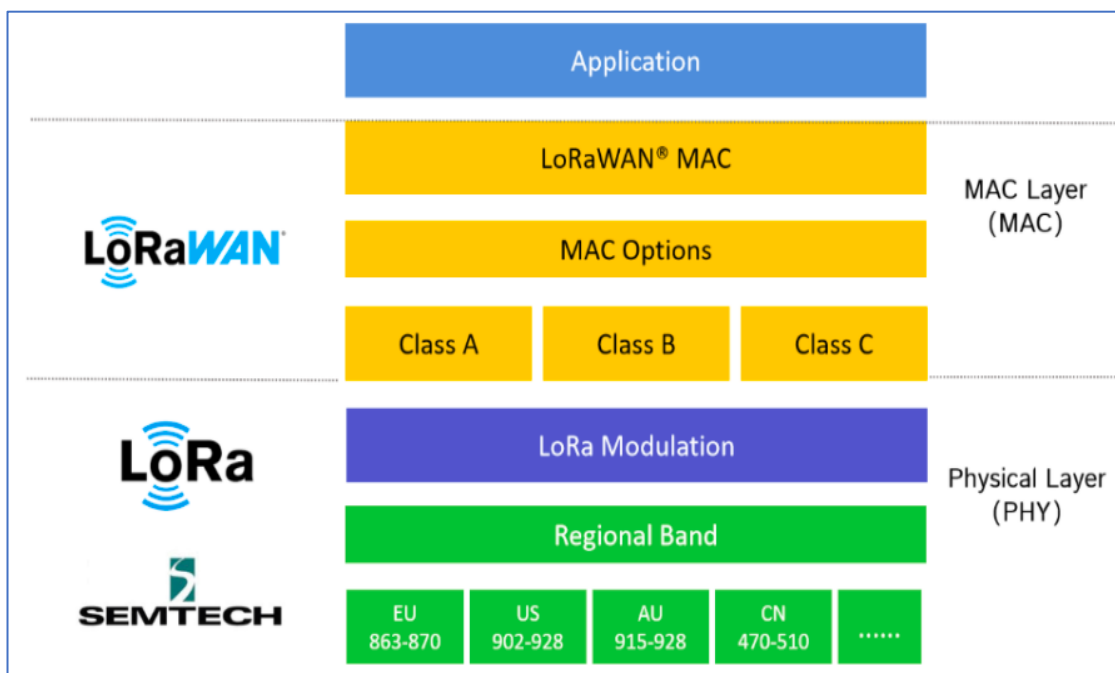


Figura 8. Pila de Protocolos LoRa/LoRaWAN. Fuente: LoRa Alliance.

5.2.1.1 Características LoRa

La tecnología LoRa es propiedad de la empresa Semtech, fundadora de la LoRa Alliance compuesta entre otros por Cisco, IBM y Orange. Además diseña y produce los chips LoRa, utilizados como base física en redes LoRaWAN. Se trata de una modulación inalámbrica de radiofrecuencia la cual define la capa física de una red LoRaWAN, tal y como se ha expuesto anteriormente. Puede operar en cualquier frecuencia por debajo de 1 GHz, sin embargo, su uso se centra principalmente en las correspondientes a la banda ISM, por ser esta una banda sin licencia, siempre y cuando se respeten unos valores de potencia de emisión. Según el país existen frecuencias restringidas dentro de esta banda, en el caso de Europa se usa la banda de 868 MHz.

LoRa se basa en la modulación Chirp Spread Spectrum (CSS), la cual a su vez está basada en las técnicas de espectro ensanchado. Esto consiste en usar un ancho de banda en la comunicación mucho mayor que el necesario teórico. Esto permite aumentar la seguridad de las comunicaciones y reducir las interferencias considerablemente en un espectro electromagnético el cual a priori puede estar saturado al tratarse de bandas de frecuencias de uso libre. Con ello, LoRa alcanza una velocidad o capacidad de transmisión de datos varía en un rango de 0.4 kbps a 50 kbps.

Como curiosidad cabe destacar que las técnicas de espectro ensanchado son una importante tecnología en el ámbito de las telecomunicaciones, coinventada su primera versión por la actriz de Hollywood e ingeniera Hedy Lamarr, con el fin de vencer la amenaza de interferencias por parte de las potencias del Eje durante la Segunda Guerra Mundial [9].

Se puede resumir esta tecnología en que es la encargada dentro del protocolo LoRaWAN de realizar la conexión física entre los nodos y dispositivos de la red, estableciendo los diferentes parámetros de la conexión como son: bandas de frecuencias, canales y cifrado.

5.2.1.2 Características LoRaWAN

LoRaWAN en cambio es el protocolo de red que define la capa de control de acceso al medio (MAC) en la jerarquía de capas de la tecnología. Comunica los dispositivos sensores de baja potencia con aplicaciones conectadas a internet,

definiendo el formato de los mensajes y gestionando la comunicación entre los Gateways LoRaWAN y los nodos finales, así como los canales LoRa.

Las comunicaciones entre dispositivos de la red pueden ser tanto unidireccionales como bidireccionales, soportando también multidifusión. Además, estas comunicaciones se realizan a diferentes frecuencias y velocidades de transmisión según los datos a transmitir y el alcance.

La arquitectura de red típica de LoRaWAN es una red de redes en estrella, donde la primera estrella está formada por los dispositivos finales y los Gateways, mientras que la segunda estrella está formada por los Gateways y un servidor de red central o también llamado *Network Server*. Sin embargo, en el caso que nos ocupa en este trabajo, al tratarse de una red formada por un único sensor y Gateway, esta comunicación es punto a punto. Por otra parte, el Gateway es el que proporciona al *Network Server* todos los datos recibidos desde los dispositivos sensores, y es allí donde son procesados para enviarse a la nube o plataforma IoT a través del servidor de aplicaciones o *Application Server*. La comunicación a partir del Gateway hacia delante no se realiza bajo la comunicación LoRa/LoRaWAN, siendo lo normal basar las comunicaciones en el modelo TCP/IP.

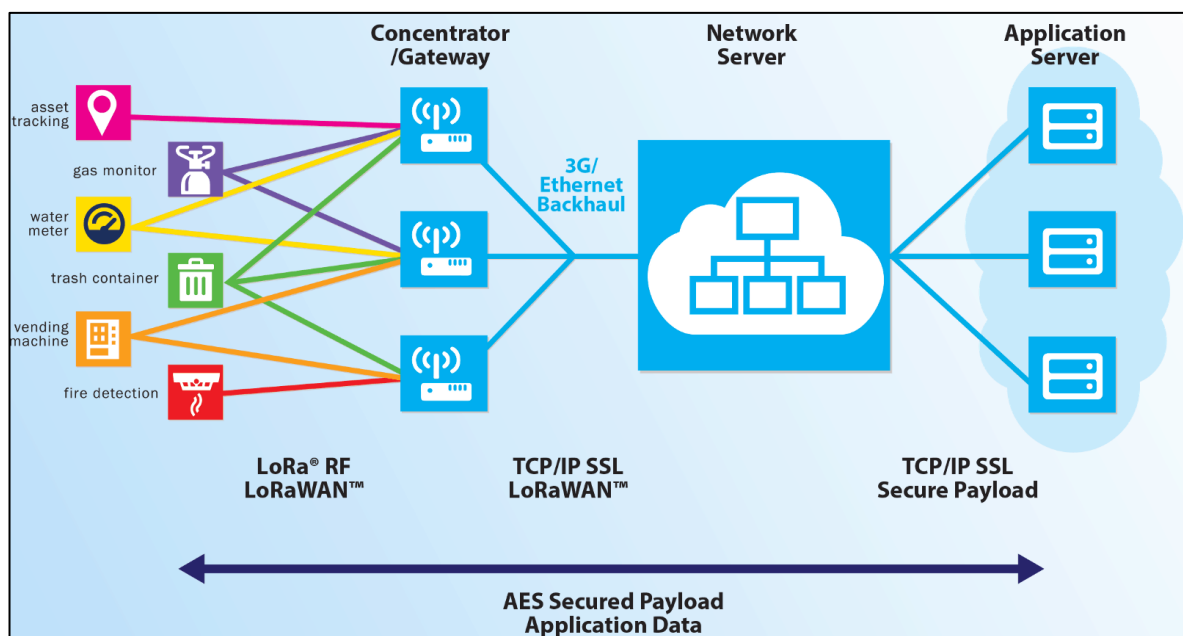


Figura 9. Arquitectura general red LoRaWAN. Fuente: Industrial M2M by Logitek.

5.2.1.2.1 Seguridad en LoRaWAN

En las redes IoT enmarcadas dentro de las redes WSN, donde las comunicaciones entre sensor y Gateway se realizan de forma inalámbrica, es importante contar con una sólida capa de seguridad extremo a extremo, puesto que la información a transmitir podría ser sensible, y las comunicaciones inalámbricas son más susceptibles a ser corrompidas que las comunicaciones que usan medios guiados, como puede ser la fibra óptica. Es por ello, que es importante presentar la forma en que LoRaWAN mantiene sus comunicaciones seguras. Se resumen en tres las propiedades fundamentales relativas a seguridad de este protocolo:

- **Autenticación mutua** entre un dispositivo sensor y la red LoRaWAN durante el proceso de unión a la red. Con esto se consigue que sólo dispositivos autorizados se unan a la red.
- **Integridad** de los datos, los cuales no pueden ser modificados por terceros sin autorización.
- **Confidencialidad** de las comunicaciones, gracias al cifrado extremo a extremo implementado entre el dispositivo sensor y el Application Server.

Gracias a este cifrado, se evita que el tráfico no sea alterado, se asegura este tenga como origen un dispositivo autorizado y se evita que sea comprensible para posibles atacantes.

Para conseguir estas características, en primer lugar LoRaWAN implementa dos capas de seguridad haciendo uso de la encriptación *Advanced Encryption Standard* (AES):

- **Capa de red:** se hace uso una clave AES de 128 bits única conocida como *Network Session Key* (NwkSKey), que es compartida entre el dispositivo sensor y el Network Server.
- **Capa de aplicación:** se hace uso una clave AES de 128 bits única conocida como *Application Session Key* (AppSKey), que es compartida entre el dispositivo sensor y el Application Server.

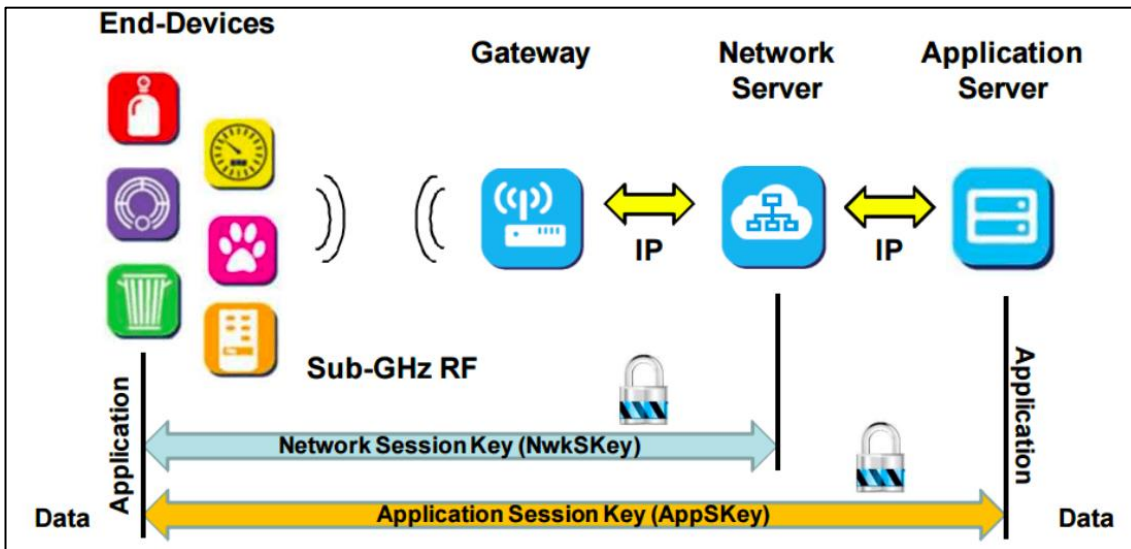


Figura 10. Capas de seguridad en LoRaWAN. Fuente: StackExchange[10].

Para conseguir la autenticación del dispositivo sensor, cada uno de ellos cuenta con un identificador único llamado *Device Extended Unique Identifier* (DevEUI), que es el equivalente a la dirección MAC de los dispositivos electrónicos y con otra clave AES de 128 bits, llamada *Application Key* (AppKey).

Existen dos métodos de activación de los dispositivos sensores, es decir, dos métodos a partir de los cuales estos dispositivos pueden unirse a la red. Según el método utilizado se hará uso de las claves mencionadas anteriormente de una forma u otra.

5.2.1.3 Parámetros regionales LoRa y LoRaWAN

En cada zona donde operan estas tecnologías, se deben cumplir ciertos estándares, tanto por parte de los fabricantes como de los usuarios. En estos estándares se especifica según regiones, los valores entre los que deben estar los parámetros de la red. Entre estos parámetros se encuentran la potencia de emisión tanto del sensor como del Gateway, la Potencia Isótropa Radiada Equivalentemente (PIRE), el ancho de banda o los canales de frecuencias utilizados. El objetivo de estas especificaciones es, dado que el espectro electromagnético es un recurso compartido y limitado, evitar en la medida de lo posible las interferencias entre señales de diferentes comunicaciones. Con ello se consigue una buena calidad en las comunicaciones y garantizar la fiabilidad de estas. Por tanto, a continuación se describen los parámetros regionales LoRaWAN correspondientes a la banda europea, llamada EU863-870 o EU868.

A nivel de señal, cabe destacar el factor de esparcimiento o *Spreading Factor* (SF). Esto es una medida del ensanchamiento en el tiempo de la señal. Este parámetro define la cantidad de bits con la que se codifica un chirp, el cual es un símbolo transmitido referido a la técnica de CSS. A mayor SF, mayor número de bits por chirp. Esto hace que un chirp tenga una duración temporal mayor, pero a su vez lo hace más inmune a interferencias, por lo que el alcance de la comunicación aumenta. Este parámetro tiene valores de 7 a 12.

Spreading Factor index	7	8	9	10	11	12
Chirp duration	1 ms	2 ms	4 ms	8 ms	16 ms	32 ms

Figura 11. Duración de chirp en función del SF. Fuente: ETSI [11].

La longitud mínima de un payload a nivel físico en LoRaWAN es de 13 bytes. Se le añade una cabecera PHY (capa física) para describir la longitud del payload, contando este campo con una longitud de 13 a 255 bytes. Además, se añade un código de verificación de redundancia cíclica (CRC) de 16 bits. Finalmente se aplica como codificación de canal un código de chequeo de paridad. Esta codificación varía según un parámetro conocido como *Code Rate* (CR). En LoRaWAN se aplica una codificación de canal resultante de la siguiente expresión: $\frac{4}{(CR+4)} CR \in [1,4]$. La codificación de canal aplicada por defecto es de (4,5), es decir, cada 4 bits de datos se añade 1 adicional de protección contra errores. Así se obtiene la relación entre régimen binario del payload y la duración temporal de los bits no correspondientes al payload en base al SF.

SF index	Payload Data rate	Time overhead
7	5,5 kbps	40 ms
8	3,1 kbps	80 ms
9	1,8 kbps	150 ms
10	0,98 kbps	280 ms
11	0,44 kbps	570 ms
12	0,25 kbps	1 100 ms

Figura 12. DR en base al SF . Fuente: ETSI [11].

En la implementación de redes LoRaWAN en Europa, se define en el protocolo una serie de canales a utilizar tanto por los sensores como por gateways. Cabe destacar que en LoRaWAN, un canal se define como el conjunto formado por tres parámetros: frecuencia central, ancho de banda ocupado y SF aplicado. Por otra parte, un Data Rate (DR) se define como la combinación de dos parámetros: SF aplicado y ancho de banda ocupado. Además, este protocolo permite el uso de modulación FSK a un régimen binario de 50 kbps. El ancho de banda disponible para la transmisión de datos en una red LoRaWAN es de 125 o 250 KHz, siendo el primero el más utilizado.

DR	Configuration (SF for LPWAN-CSS or FSK, occupied bandwidth)	bit rate (bit/s)
0	LPWAN-CSS: SF12 / 125 kHz	250
1	LPWAN-CSS: SF11 / 125 kHz	440
2	LPWAN-CSS: SF10 / 125 kHz	980
3	LPWAN-CSS: SF9 / 125 kHz	1 760
4	LPWAN-CSS: SF8 / 125 kHz	3 125
5	LPWAN-CSS: SF7 / 125 kHz	5 470
6	LPWAN-CSS: SF7 / 250 kHz	11 000
7	FSK	50 000

Figura 13. DR en el protocolo LoRaWAN Fuente: ETSI [11].

Para un ancho de banda ocupado de 125 KHz, los canales tienen una separación de 200 KHz. Durante la transmisión, la señal varía de frecuencia en el tiempo dentro del ancho de banda ocupado, siendo esta la característica principal de la técnica CSS. Todo sensor o nodo final debe soportar tres canales, llamados 'canales por defecto'. Por tanto, también todo Gateway debe escuchar en estos canales. Estos canales tienen un ancho de banda de 125 KHz y sus frecuencias centrales son de 868.1, 868.3 y 868.5 (MHz), soportando los DR0 a DR5. Tienen todos un *Duty Cycle* o ciclo de trabajo menor al 1%. Este parámetro indica el tiempo que un dispositivo está comunicando. Como ejemplo, cada 200 segundos (s) se podría transmitir durante 2s. Cabe destacar que el tiempo de comunicación de 2 s está referido al tiempo total de transmisión, no a una única transmisión. Respecto a la transmisión de downlink, el canal utilizado tiene una frecuencia central de 869.525 MHz.

Modulation	Bandwidth [kHz]	Central Channel Frequency [MHz]	LPWAN-CSS DR/Bitrate
LPWAN-CSS	125	868,10 868,30 868,50	DR0 - DR5 / 0,3 - 5 kbps

Figura 14. Canales por defecto en LoRaWAN. Fuente: ETSI [11].

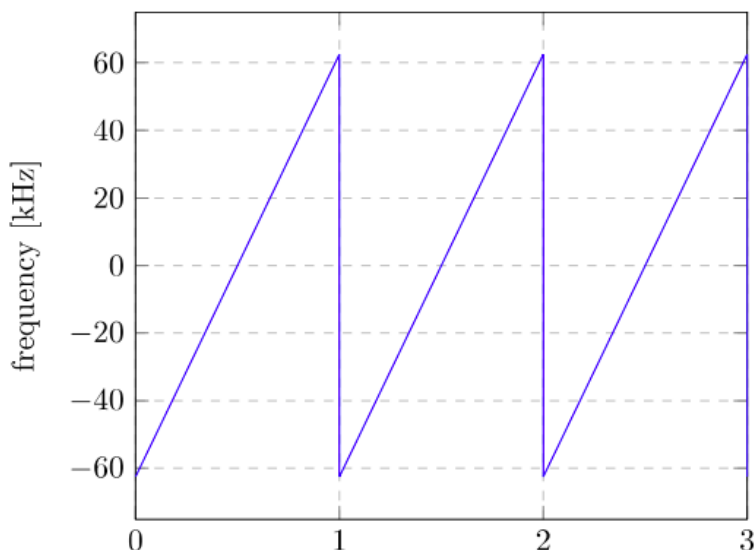


Figura 15. Ejemplo de señal CSS en LoRaWAN. Fuente: ETSI [11].

5.2.2 Componentes de una red LoRaWAN

Hasta ahora se ha hablado de LoRa y LoRaWAN y de sus principales características. En esta sección se describen los distintos elementos que componen una red LoRaWAN. El orden seguido para ello es en sentido ascendente de los datos. Como aclaración, el sentido ascendente es el que siguen los datos desde que son generados por el sensor hasta que son representados. Se explican los elementos que intervienen en la comunicación.

5.2.2.1 Dispositivo sensor

El dispositivo sensor es el elemento de la red encargado de captar las variaciones del entorno, recoger las métricas correspondientes y enviar dichos datos mediante ondas de radio hacia el Gateway. Son los elementos de la red que se encuentran “a pie de campo” por lo que deben ser resistentes diferentes factores tales como la meteorología, además de tener un bajo consumo puesto que por lo general se alimentan mediante baterías. Las redes IoT tienen como objetivo principal la recolección de datos a partir de la observación y monitorización del entorno; es por ello que este elemento es imprescindible en el desarrollo de cualquier solución IoT. Por tanto, aquí se describen los diferentes tipos de nodos finales que existen en una red LoRaWAN así como la forma en que interactúan con esta.

Los nodos se comunican con el Gateway de forma bidireccional (el sensor le “habla” al Gateway y viceversa), pero los nodos no se comunican entre ellos; es por ello que se describe la red entre los dispositivos sensores y Gateway como una red con topología de estrella. A priori podría parecer no tener importancia, pero sin embargo es un detalle importante puesto que esta topología permite un mejor aprovechamiento de las baterías de los dispositivos sensores.

En una red LoRaWAN podemos encontrar 3 clases de sensores según realizan la comunicación con el Gateway y la forma en que son alimentados:

5.2.2.1.1 Clase A (“All”)

Los dispositivos sensores incluidos en esta clase se caracterizan por estar alimentados por baterías, su estado normal es de hibernación y se activan ante un evento o cada cierto tiempo para enviar una trama de datos. Con el fin de optimizar el consumo, se quedan a la escucha tras enviar una trama, es decir, el *downlink* (datos desde el Gateway al sensor) sólo está disponible tras enviar el dispositivo el mensaje de *uplink* (datos desde el sensor al Gateway).

Para ser más específicos, tras la transmisión de enlace ascendente, el dispositivo sigue dos ventanas de recepción; una de ellas se da un (1) segundo después del envío del mensaje de uplink, mientras que la otra lo hace 1 segundo después de la primera ventana. Tras estas ventanas de recepción tal y como se ha dicho antes, no podrá volver a recibir datos hasta que estas se abran de nuevo tras producirse de nuevo un mensaje de uplink.

Por sus características descritas anteriormente, esta clase de sensores son los más eficientes desde el punto de vista energético, pudiendo ser la duración de su batería de años. Además, es importante destacar que todos los dispositivos de la red LoRaWAN deben admitir los dispositivos sensores de esta clase.

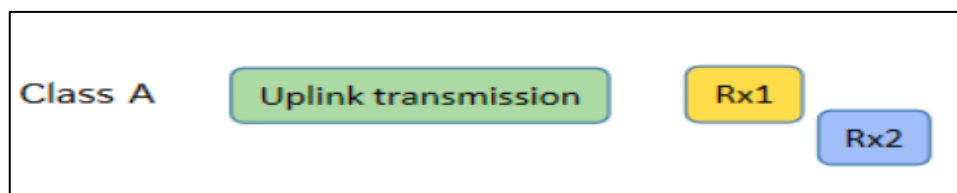


Figura 16. Comunicación Clase A. Fuente: Witekio

5.2.2.1.2 Clase B (“Ballice” -> Baliza)

Los dispositivos sensores de esta clase, al igual que los de clase A se caracterizan por estar alimentados por baterías. La diferencia más notable con respecto a la clase anterior es que se encuentran en modo de ‘hibernación profunda’. Esto es, que se activan periódicamente durante un intervalo de tiempo para recibir mensajes de downlink gracias a que la segunda ventana de recepción se repite durante un intervalo de tiempo determinado. Esto permite que la red envíe mensajes al sensor durante un intervalo de tiempo fijo, lo que hace que la latencia de los mensajes descendentes sea notablemente más pequeña. Sin embargo, el consumo energético se ve incrementado.

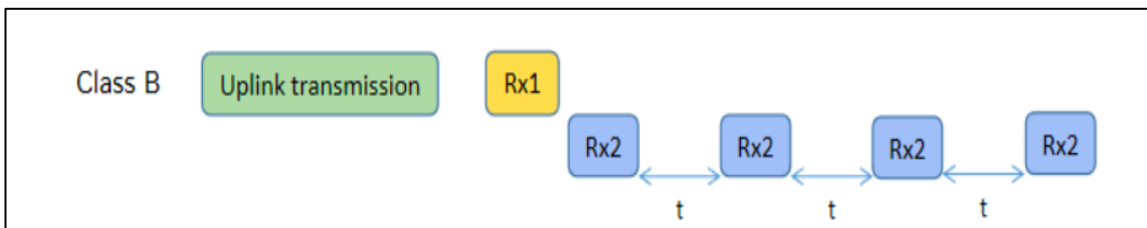


Figura 17. Comunicación Clase B. Fuente: Witekio.

5.2.2.1.3 Clase C (“Continous” -> Continuo)

Esta clase de sensores se caracteriza por contar con una fuente externa de alimentación. Esto se debe a que son la clase de dispositivos menos eficientes por estar constantemente a la escucha para recibir mensajes de downlink cuando lo requiera. En resumen, tienen la ventana de recepción siempre abierta. Únicamente pasa a modo transmisión cuando necesita enviar un mensaje de uplink.

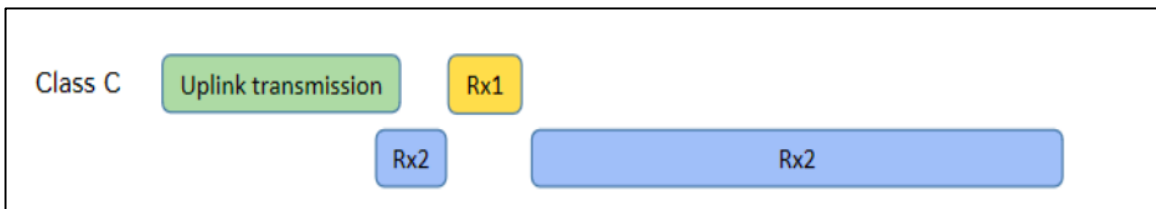


Figura 18. Comunicación Clase C. Fuente: Witekio.

5.2.2.1.4 Métodos de activación del nodo

Una vez presentadas las clases de dispositivos sensores es importante destacar que estos tienen dos formas de unirse a la red LoRaWAN.

Los datos de enviados a través de la red LoRaWAN comienzan su camino como una secuencia de datos modulados mediante la tecnología de radio LoRa inalámbrica desde el dispositivo sensor hacia el Gateway. Desde aquí, en un esquema general, son enviados al Network Server. Este puede encontrarse o bien alojado en la nube, en la red local o embebido en el propio Gateway, siendo este último el caso del presente TFG, tal y como se verá más adelante. Este dispositivo hardware o software realiza una serie de funciones previas al envío de los datos hacia el Application Server donde serán procesados y finalmente representados en una plataforma.

Los datos son cifrados durante todo el camino, primero mediante una clave de sesión de red (NwkSKey), y después con una clave de sesión de aplicación (AppSKey). La obtención de estas dos claves depende del método de activación (unión a la red) escogido por el diseñador de la red LoRaWAN. Son dos los métodos mediante los cuales los nodos pueden unirse a la red:

5.2.2.1.4.1 OTAA: 'Over The Air Activation'

En este método las claves de cifrado de la conexión surgen de la negociación entre dispositivo sensor y Gateway al conectarse el primero el nodo a la red para enviar o recibir datos. Estas claves son temporales, ya que son únicas para cada sesión, siendo renovadas cada vez que se pierde la conexión o el dispositivo sensor se apaga o reinicia.

Esta actualización de claves de cifrado cada vez que se realiza una nueva conexión es la característica que da nombre a este método, ya que se dice que la sesión "se crea en el aire".

La renovación de claves añade una capa importante de seguridad siendo esta su principal ventaja. Sin embargo, de aquí parte también su desventaja, puesto que este proceso de negociación ocupa una ventana temporal haciendo que no sea el método más rápido. Es decir, una mayor seguridad en las comunicaciones se paga con una velocidad de conexión algo más lenta que en el otro método de activación. Al ser la

seguridad una prioridad, puesto que la cantidad de datos a enviar es reducida (orden de Kbps) y tratarse de una comunicación asíncrona, este es el método más recomendado.

Al realizar la conexión con este modo, son necesarios los siguientes parámetros en el dispositivo sensor:

- **DevEUI:** Identificador único preestablecido de fábrica. Tiene una longitud de 16 en formato hexadecimal lo que equivale a una longitud de 64 bits (Cada dígito hexadecimal puede representar 4 bits).
- **AppEUI:** Identificador único de aplicación similar a un número de puerto. Tiene la misma longitud que el DevEUI. Este parámetro es ajustable.
- **AppKEY:** Clave AES-128 bits (longitud de 32 en formato hexadecimal) entre el dispositivo sensor y la red. Este parámetro es ajustable.

Una vez han sido establecidos estos parámetros en el dispositivo sensor, se siguen los siguientes pasos para realizar la conexión:

1. El dispositivo sensor envía una solicitud de conexión o *join-request* con los parámetros descritos anteriormente junto un *DevNonce* con destino hacia el Network Server pasando por el Gateway. El *DevNonce* es un número generado aleatoriamente cuyo fin es el de evitar que el *join-request* sea replicado.
2. Al recibir el Network Server la petición, verifica que el sensor esté dado de alta en un servidor de unión o *Join Server* y que las claves sean correctas. Si no son correctas rechaza la conexión, mientras que si son correctas responde con una aceptación de conexión o *join-accept*.
3. El *join-accept* es enviado hacia el dispositivo sensor conteniendo varios parámetros de la sesión temporal creada, siendo los más relevantes: *Network ID* (NetID), *Device Address* (DevAddr) y un *AppNonce*.
4. Una vez el sensor recibe dichos parámetros, almacena la configuración de red y utiliza el *AppNonce* y *NetID*, para junto al *DevNonce* y *AppKey*, generar las dos

claves que brindan seguridad a nivel de capa de red y aplicación a la sesión: el NwkSKey y el AppSKey.

Una vez obtenidas las llaves de encriptación, el sensor puede enviar datos a través de la red. En la Figura 19 queda representado gráficamente el proceso.

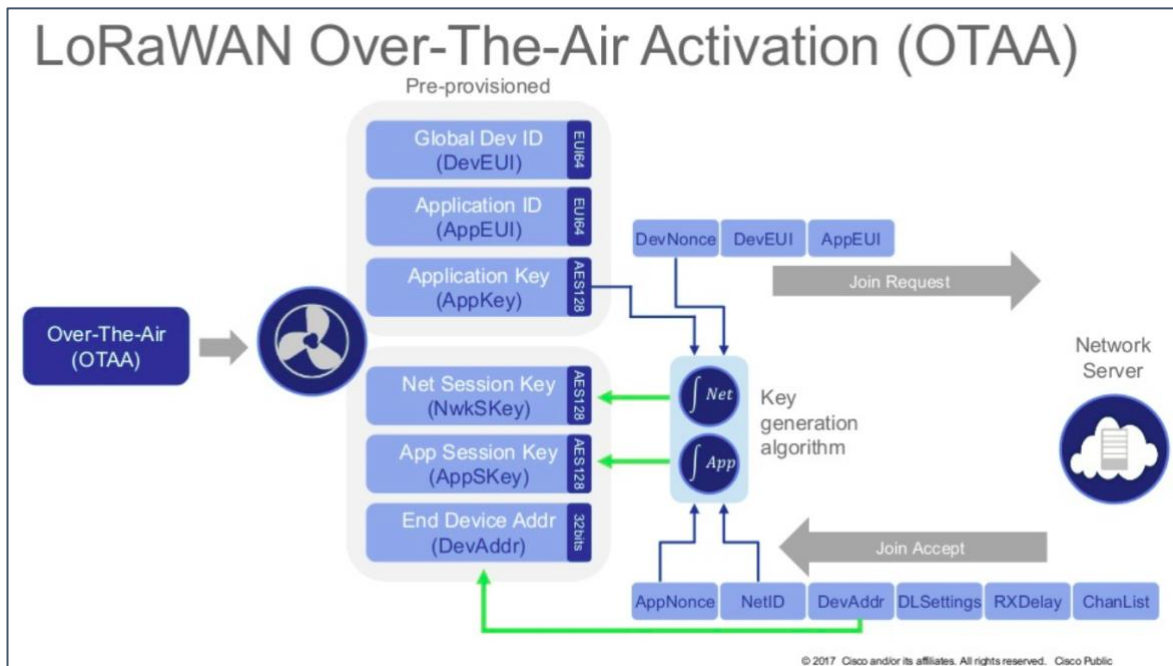


Figura 19. Método de activación OTAA LoRaWAN. Fuente: Cisco.

5.2.2.1.4.2 ABP: 'Activation By Personalization'

A diferencia de OTAA, este método es más sencillo y rápido, puesto que al estar las claves NwkSKey, DevAddr y AppSKey preestablecidas en el dispositivo sensor, no se da el proceso de negociación de estos parámetros, tal y como se vio en la descripción de OTAA, ya que la sesión se asigna manualmente. Sin embargo, esto hace que sea el método menos seguro, ya que las llaves de encriptación se encuentran almacenadas en el propio dispositivo, siendo susceptibles a ser extraídas por atacantes.

Partiendo de los tres parámetros preestablecidos en el dispositivo, se realizan los siguientes pasos para realizar la conexión:

1. El dispositivo sensor envía datos hacia el Network Server pasando por el Gateway. No es necesario ningún proceso de join-request.

2. El Network Server está también preconfigurado de manera que contiene los tres parámetros de cada sensor necesarios para la conexión. Así, este se encarga de validar los parámetros del sensor que está enviando datos.
3. Si el Network Server verifica la sesión, los datos son procesados; si no, son rechazados.

En la figura 20 queda representado el proceso.

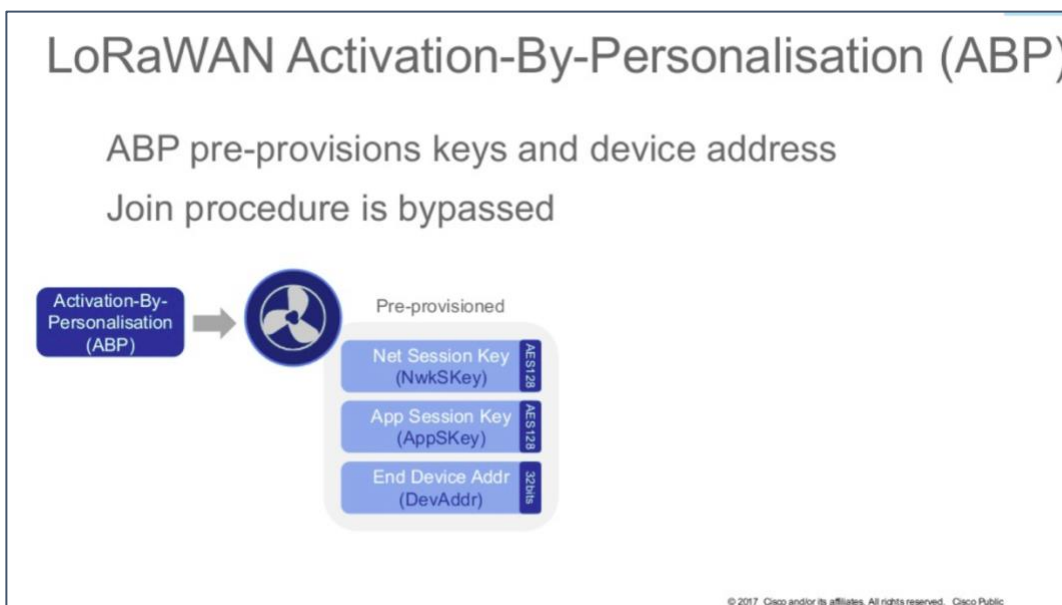


Figura 20. Método de activación ABP LoRaWAN. Fuente: Cisco.

5.2.2.2 Gateway

Un Gateway o pasarela se define como un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes. Se encarga de traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino [12].

En una red LoRaWAN, este dispositivo es el encargado de recibir los datos enviados por los nodos a través de señales radioeléctricas bajo la tecnología LoRa y enviarlos al Network server vía internet bajo el modelo TCP/IP mediante medios físicos como Ethernet, Wifi o 4G, entre otros. Además, envía los mensajes que el Network Server envía a los dispositivos sensores, tales como los generados durante el proceso de conexión a la red de estos.

En definitiva, es el dispositivo responsable de crear la red inalámbrica LoRa que conecta los dispositivos sensores y de recibir los mensajes generados por estos para enviarlos hacia el Network Server, el cual se encarga de la gestión de la red y envío de los datos a las aplicaciones superiores.

Los Gateways en una red IoT tiene dos posibles modos de funcionamiento dentro de la red LoRaWAN según las funciones a realizar: Packet Forwarder o Network Server. Para redes LoRaWAN compuestas por más de un Gateway, dado que se debe cubrir un área de cobertura grande como una ciudad y/o dar conectividad a un número elevado de sensores, se hace necesario un Network Server dedicado. En este caso, el Gateway se encarga de pasar al Network Server los datos para que este los gestione; por ello el modo de funcionamiento es 'Packet Forwarder' o reenviador de paquetes.

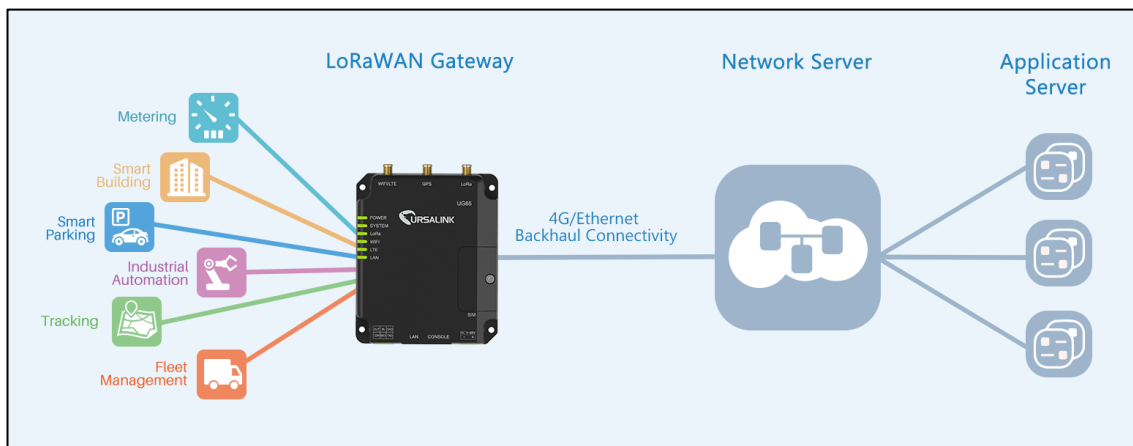


Figura 21. Red LoRaWAN con Network Server dedicado. Fuente: Ursalink.

En redes más pequeñas, como pueden ser redes privadas donde el área a cubrir es de centenares de metros a unos pocos kilómetros y el número de sensores es reducido, un único Gateway es suficiente para dar cobertura. En este caso, existen Gateways capaces de realizar a su vez las funciones de Network Server, de aquí el nombre de este segundo modo de funcionamiento. Con esta función, no se hace necesario un Network Server dedicado en la red, ya que el propio Gateway realiza las funciones propias de este como la traducción de los mensajes o *payloads* y la verificación de credenciales del nodo.

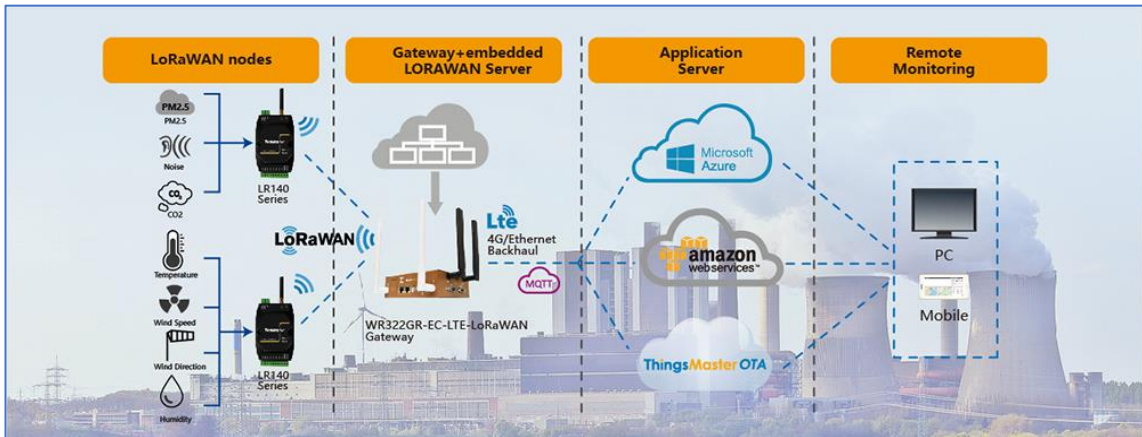


Figura 22. Red LoRaWAN con Network Server embebido en Gateway. Fuente: WoMaster.

5.2.2.3 Network Server

El LoRaWAN Network Server o Servidor de Red es el dispositivo hardware o software encargado de la administración de la red. Conecta los Gateways y por tanto también sensores con las aplicaciones superiores, manteniendo la seguridad en las comunicaciones y la fiabilidad de los datos de la red.

Se pueden resumir sus principales funciones en las siguientes:

- Comprobación de las credenciales y direcciones de los dispositivos. Es el encargado del proceso de autenticación de los sensores para su unión a la red.
- Envío de los datos al Application Server, así como de los que este envía hacia los sensores, gestionando la comunicación durante el proceso.
- Evitar el duplicado y pérdida de mensajes seleccionando el Gateway más conveniente para cada nodo aplicando el mecanismo *Adaptive Data Rate* (ADR).

En las soluciones IoT donde se hace necesario el uso de más de un Gateway, los datos enviados por los sensores pueden ser recibidos por más de un Gateway. En este caso, el Network Server se encarga de seleccionar uno de ellos y eliminar el resto de copias para evitar el duplicado. De igual forma ocurre con los mensajes de downlink, donde el Network Server selecciona el Gateway que enviará los datos al dispositivo sensor correspondiente; para ello compara el *Received Signal Strength Indicator* (RSSI) de los mensajes de uplink de los nodos para así tener constancia de qué Gateway es el que tiene mejor conexión con el nodo destinatario. Como es lógico, este proceso de

selección por parte del Network Server no es necesario en redes donde únicamente existe un Gateway.

En resumen, se dice que es el “cerebro” de una red LoRaWAN ya que es el responsable de la centralización, control y supervisión de la red, gestionando los dispositivos sensores y Gateways para enviar los mensajes de forma segura y fiable al Application Server.

5.2.2.4 Application Server

El Application Server o servidor de aplicaciones es el elemento de una red LoRaWAN previo a la representación de los datos. Realiza las funciones de descifrar y decodificar los mensajes recibidos desde el Network Server para que estos puedan ser usados por las aplicaciones superiores para su representación.

6. Diseño e implementación del sistema

El presente TFG consiste en el diseño e implementación de los componentes de una red LoRaWAN con el fin de monitorizar los niveles de ruido acústico presentes en un entorno urbano real y notificar al usuario cuando los niveles de ruido superen cierto umbral. Para comprobación del funcionamiento del sistema, el sensor se ha instalado en la cafetería del Parque Científico y Tecnológico de Geolit (Mengíbar) mientras que el Gateway se ha instalado en la sala Demo de la empresa. La instalación de estos elementos se ha llevado a cabo con la colaboración de los instaladores de la empresa. Cabe destacar que este sistema se encuentra dentro del catálogo de proyectos de la empresa colaboradora Innovasur S.L. Por tanto, durante mi periodo de prácticas en el departamento de IoT, he formado parte en algunos de estos proyectos de sensórica LoRa, en los cuales se han implementado en distintas localidades españolas diferentes tipos de sensores LoRa tales como sensores de CO₂, humedad, calidad del aire, etc. Gracias a ello he obtenido una visión más amplia y unos conocimientos más consolidados acerca de la configuración, funcionamiento y soporte de redes LoRaWAN, así como de su instalación y mantenimiento.

Tras presentar en el capítulo 5 la estructura y funcionamiento de una red LoRaWAN, en este capítulo se describe la configuración e implementación del sistema

desarrollado. Para ello, primero se da una perspectiva general donde se presenta una descripción más detallada de la arquitectura de red. Posteriormente se describe uno a uno cada elemento hardware y software, así como su configuración y programación, estando la disposición de las distintas secciones y subsecciones determinada por el orden seguido a la hora de ir ensamblando la red. Estos elementos conforman tanto el *back-end* como el *front-end* del sistema. Finalmente se instalan los componentes de la red, se interconectan entre sí y se verifica el funcionamiento del sistema mediante la representación de los datos y la recepción de alertas.

6.1 Perspectiva general

La presente sección tiene como fin realizar el planteamiento de la red y de los elementos que la conforman, así como de las comunicaciones realizadas entre estos. Para el desarrollo e implementación del sistema se hace uso de la red, materiales y software propietarios de la empresa. Además, se hace uso de software de código abierto u *open source* como es Grafana y Node-Red.

Los siguientes pasos describen forma general de los diferentes dispositivos junto con el flujo de comunicación:

1. Dado que el factor a monitorizar es el nivel de ruido acústico, como es lógico se parte del uso de un sensor LoRa con capacidad de medir las variaciones de presión sonora del establecimiento. Al tratarse de una red LoRaWAN, la comunicación es bidireccional y por tanto el sensor también recibirá datos de la red tales como los mensajes respectivos al proceso de activación y autenticación.
2. Los datos generados por el sensor son recibidos por el Gateway en su interfaz LoRa. Este dispositivo es el encargado de realizar la conversión de los datos al protocolo TCP/IP bajo el que trabajará el sistema a partir de este punto. Este Gateway se ha instalado en la Sala Demo y está conectado a la red local de esta sala por medio de un router Mikrotik.
3. El Network Server del sistema se encuentra embebido en el propio Gateway, realizando este por tanto la función de autenticación.

4. El Gateway además cuenta con una aplicación de Node-Red, que junto con otra instancia de este que se ejecuta en el Centro de Procesamiento de Datos (CPD) y con las plataformas de representación, forman el Application Server del sistema.
5. En el Node-Red del Gateway se programan dos flujos; uno de ellos decodifica y envía los datos a través del protocolo *HyperText Transfer Protocol Secure* (HTTP) a otra instancia de Node-Red mediante un túnel *Open Virtual Private Network* (OVPN) que se encuentra en el CPD. En el CPD corre una instancia de máquina virtual y la base de datos que almacena la información generada por el sensor, para posteriormente ser representados en la plataforma open-source Grafana. El otro flujo sirve para enviar los datos hacia una *Uniform Resource Locator* (URL) donde se encuentra una *Application Programming Interface* (API) gestionada por el departamento de desarrollo. Esta API decodifica y almacena los datos en otra base de datos. Finalmente, los datos son representados en la plataforma propietaria de la empresa In4city.
6. En último lugar se verifica el funcionamiento del sistema mediante la visualización de los datos en ambas plataformas y la recepción de alertas. Además, se comparan ambas plataformas con el fin de estudiar las ventajas y desventajas del uso de una plataforma open-source frente a una propietaria.

6.1.1 Arquitectura de red

A continuación, se presenta una descripción gráfica del sistema y de los distintos elementos y servicios implicados en este mediante el diseño del diagrama general de red.

En la red se incluyen elementos externos al TFG en sí, pero necesarios puesto que son los responsables de crear las redes utilizadas para interconectar los elementos de esta y albergar los diferentes servicios. Estos elementos se encuentran instalados antes del inicio del presente TFG y por tanto la configuración de red de dispositivos como el Gateway se ajusta a la red existente. Más específicamente, los routers empleados para este TFG son del fabricante Mikrotik. Mediante estos dispositivos se crea el túnel OVPN que permite conectar el Gateway con el CPD, de manera que toda la información viaja cifrada, consiguiendo así agregar una capa de seguridad. Para ello,

cada uno de los routers mikrotik cuenta con un cliente OVPN que cuelgan de un mismo servidor, lo que permite la conexión entre clientes.

De cara a la representación final de los datos, tal y como se ha indicado anteriormente, se cuenta con dos plataformas. Una de ellas Grafana, que, al ser un servicio instalado en la máquina virtual, la cual se ejecuta en el CPD, es únicamente accesible mediante un cliente OVPN. Por tanto, para acceder a este servicio local se precisa de tener instalado en el ordenador del usuario el programa GlobalProtect para poder acceder al portal de la empresa. La otra plataforma, In4city, es la plataforma propietaria de la empresa, y dado que es la ofrecida como servicio a los clientes, cuenta con un dominio web. Esto hace que sea accesible desde cualquier navegador con acceso a Internet.

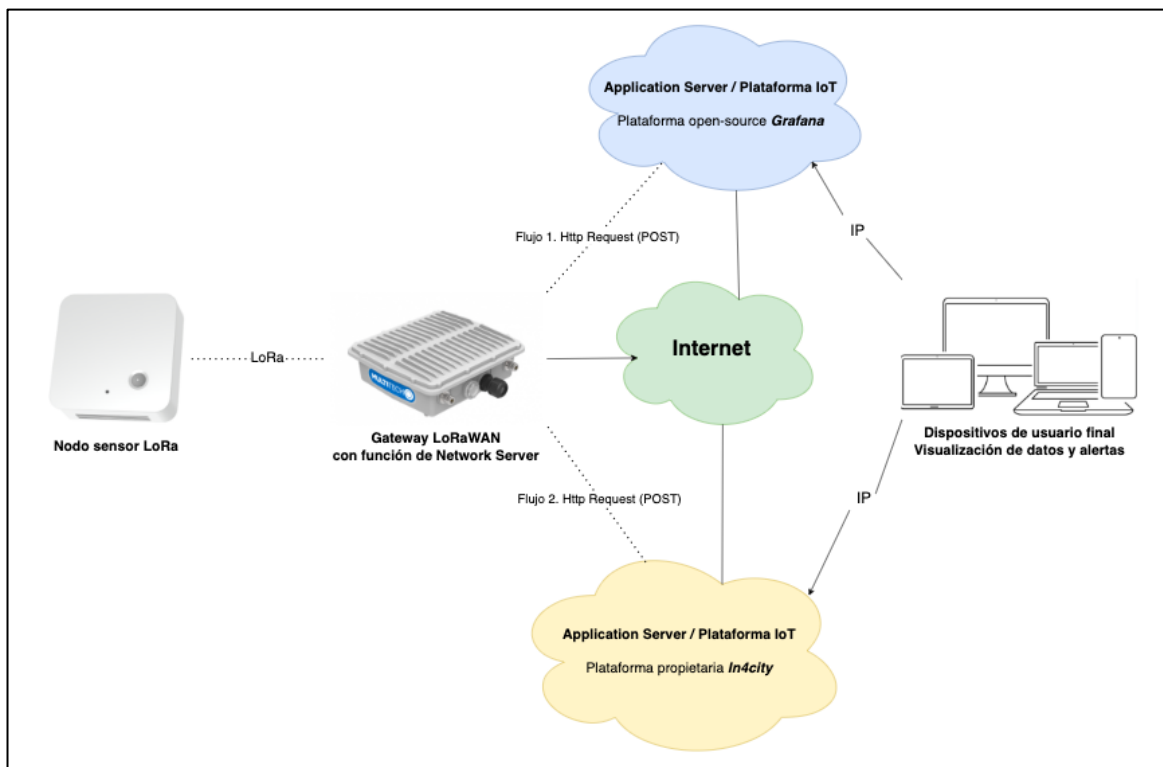


Figura 23. Diagrama general de la red

6.2 Desarrollo del sistema

En la presente sección se describe la configuración y programación cuando procede de los elementos que conforman la red LoRaWAN.

6.2.1 Dispositivo sensor

Para la monitorización del nivel de ruido acústico se hace uso de un sensor del fabricante ELSYS.se, específicamente se trata del modelo ERS Sound. Este sensor LoRa está diseñado para mediciones en interiores. Cuenta con sensores internos para la medición de: temperatura, humedad, luminosidad, movimiento y sonido. Las características técnicas se describen en el Anexo I .



Figura 24. Sensor Elsys ERS Sound LoRaWAN. Fuente: Elsys.

Este sensor no es programable a nivel de código, su configuración es realizada mediante una aplicación móvil. Es necesario un smartphone Android o IOS para descargar la aplicación 'Sensor Settings', a través de la cual se realiza la configuración. La app cuenta con tres modos de configuración: Wizard mode, Normal mode o Advanced mode siendo el primero el modo más básico y el último el más completo. [13]



Figura 25. App para configuración del sensor en la App Store (IOS)

La configuración realizada en el sensor es la siguiente:

1. Para leer el sensor, se debe pulsar el botón de 'read' y acercar el teléfono móvil a la parte delantera del sensor. Una vez reconocido, en la pantalla inicial se muestra el DevEUI del sensor, tal y como se aprecia en la figura 26. Para la configuración del sensor se ha escogido el modo avanzado, ya que es el único que permite la modificación de parámetros LoRa, tales como el DR. Se establece un 'timebase' de 600s, lo cual son 10 minutos. Esto indica el intervalo de tiempo para que el sensor se active y envíe datos hacia el Gateway.

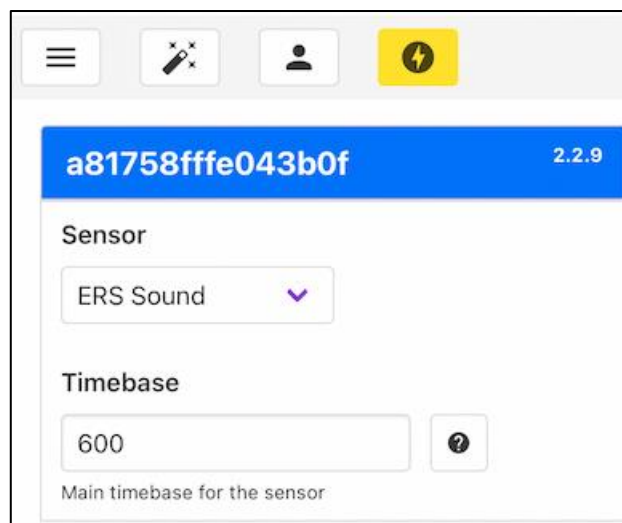


Figura 26. Inicio app Elsys.

2. El primer paso consiste en fijar las claves en el sensor necesarias para que se una al Gateway vía OTAA. Esto se realiza en el apartado 'Sensor Keys'. Las claves a establecer son el AppEUI y AppKey. Dado que tienen formato hexadecimal, se hace uso de un generador aleatorio de números hexadecimales (<https://www.browserling.com/tools/random-hex>). Es importante recordar que la longitud de estas claves es 16 y 32 respectivamente.

Sensor keys

AppEui

ee9e4e81ddb3a92b

16 hex digits (8 bytes)

AppKey

c55798f3589aa8a4ef41d1dc38de5ca8

32 hex digits (16 bytes)

Figura 27. Claves del sensor

3. En el apartado 'LoRaWAN configuration' se escoge el modo de activación, siendo OTAA el configurado por defecto. También es importante escoger la banda de frecuencias de operación. Dado que nos encontramos en Europa, se debe escoger la banda EU868. El canal LoRa es escogido automáticamente por el sensor entre los tres canales 'por defecto' que todo sensor LoRa debe implementar.

LoRaWAN configuration

OTAA

Enabled ⓘ

Over the air activation

Confirmed message

On ⓘ

Request acknowledge from server every message (use with care)

Frequency plan

EU868 ▼ ⓘ

LoRaWAN frequency plan

Sub-band

Band0 Ch:0-7 ▼ ⓘ

Only in combination with hybrid mode

Figura 28. Configuración LoRaWAN en el sensor.

4. En el apartado 'Extended LoRaWAN configuration' se establece el DR del sensor. Para utilizar uno fijo se da el mismo valor DR por defecto, mínimo y máximo. En este caso, se utiliza un DR5 fijo. De esta forma el mecanismo ADR no se aplica. Se escoge este DR ya que el sensor se instala cerca del Gateway de cara a la comprobación del funcionamiento del sistema. En cuanto al canal utilizado, el

sensor escoge automáticamente en cada transmisión uno de los tres canales LoRaWAN por defecto.

The image shows a configuration screen titled "Extended LoRaWan configuration". It contains several settings, each with a help icon (a question mark in a circle):

- Listen before talk:** A toggle switch is turned off.
- Link period:** A text input field contains the value "0".
- Link check period (1*x send period):** A text input field contains the value "0".
- Link threshold:** A text input field contains the value "0".
- Number of lost packets before reboot:** A text input field contains the value "0".
- Datarate default:** A dropdown menu is set to "DR5".
- Datarate max:** A dropdown menu is set to "DR5".
- Datarate min:** A dropdown menu is set to "DR5".
- Port:** A text input field contains the value "5".

At the bottom of the screen, there is a note: "LoRaWan data port (settings port:+1)".

Figura 29. Data Rate del sensor.

Una vez finalizada la configuración en la app, queda escribirla en el sensor. Para ello basta con pulsar el icono verde 'Write' y acercar de nuevo el teléfono móvil al sensor. De esta forma queda completada la configuración del sensor y listo para unirse al Gateway para enviar datos a la red.

6.2.2 Gateway

El modelo de Gateway o puerta de enlace escogido para este TFG es el Conduit IP 67 Base Station de la marca Multitech. Este dispositivo trabaja bajo la tecnología LoRaWAN y está pensado para su instalación en exteriores. Es por ello que cuenta con protección ante factores medioambientales como agua, polvo, arena, nieve y temperaturas extremas. Las características técnicas se describen en el Anexo II .



Figura 30. Gateway Multitech Conduit IP 67 Base Station. Fuente: Multitech.

Para su configuración, se accede a la interfaz web local mediante la dirección <http://192.168.2.1>, por ser esta la dirección que tiene este equipo por defecto [14]. Se configura un usuario y contraseña para el dispositivo y accedemos a la página inicial.

La configuración realizada en el Gateway es la siguiente:

1. Se le asigna la dirección IP 192.168.88.9 al interfaz ethernet0, ya que se ha establecido la red 192.168.88.0/24 en el equipo mikrotik, al cual se conecta el Gateway para las pruebas en un entorno real. Para ello, se accede al apartado: Setup -> Network Interfaces y se edita la interfaz 'eth0'.

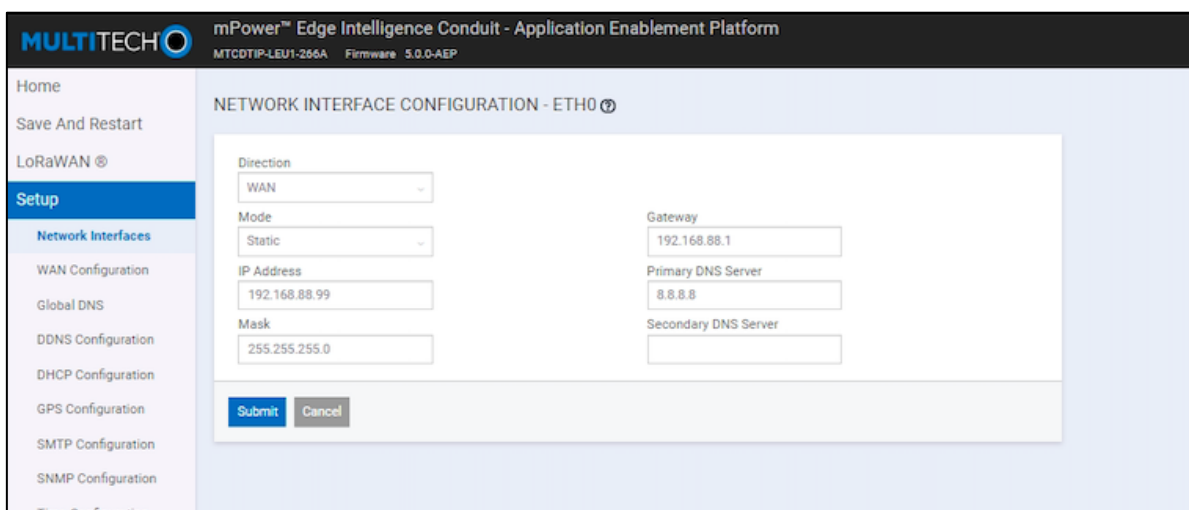


Figura 31. Cambio de IP a la interfaz ethernet

2. Se accede de nuevo al Gateway mediante la nueva IP para comprobar que la configuración se ha realizado correctamente. Se encuentra la página inicial de nuevo.

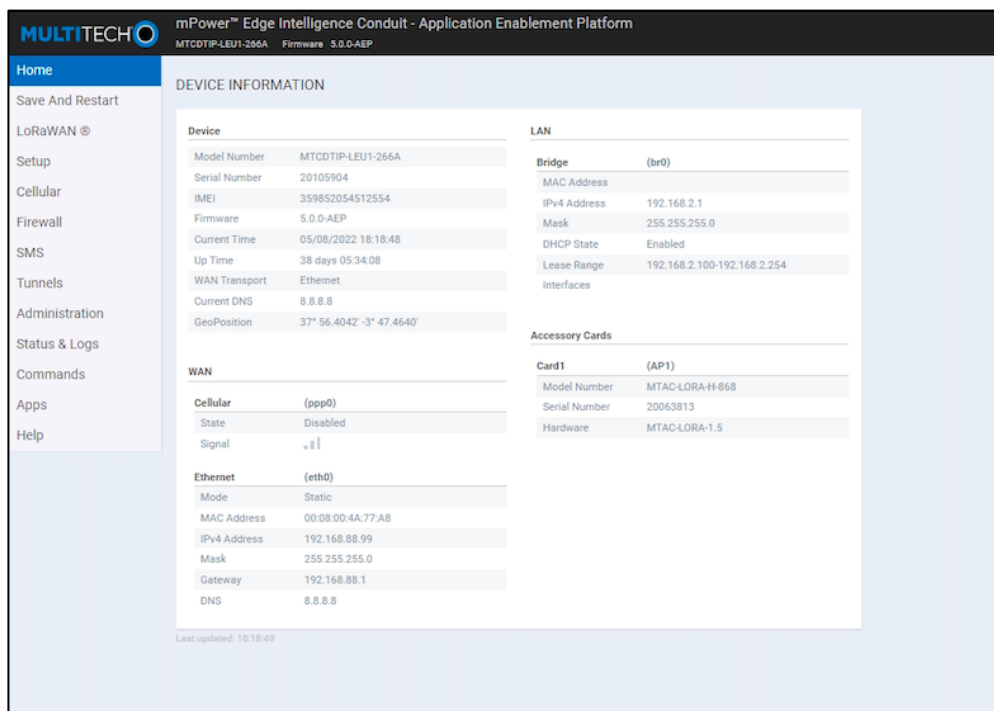


Figura 32. Pantalla inicial de configuración del Gateway

3. Se establece el modo de funcionamiento en 'Network Server'. Para ello, se accede al apartado: LoRaWAN -> Network Settings. Se hace uso de este modo de funcionamiento ya que así la verificación de las claves de activación del nodo se realiza en el propio Gateway. Así se hace un cribado de los sensores que pueden unirse a la red, lo que añade una capa extra de seguridad. En este punto también es importante establecer la banda de frecuencias LoRa, la cual es la EU868. El canal LoRa, para la transmisión en sentido descendente desde el Gateway hacia el sensor, tiene una frecuencia central de 869,525 MHz. La potencia máxima de transmisión para el Gateway es de 27 dBm por normativa; por tanto, se establece en 26 dBm para asegurar su cumplimiento.

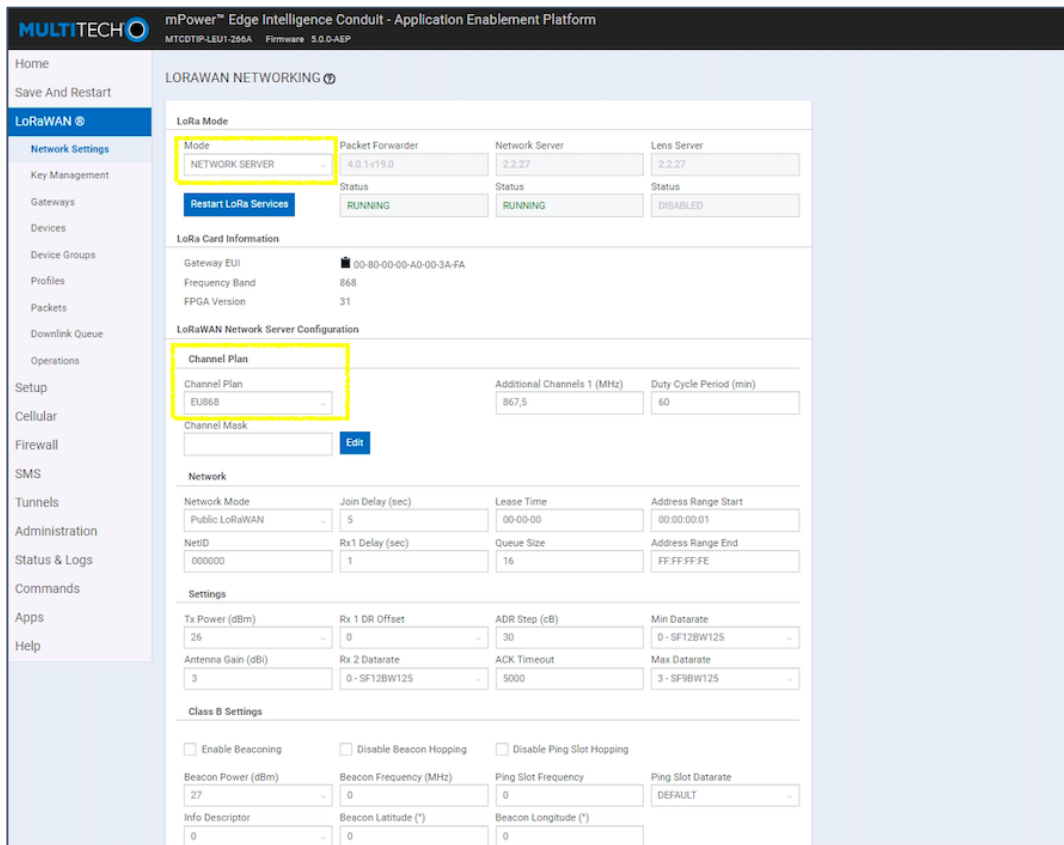


Figura 33. Configuración del Gateway en modo Network Server.

- Para añadir el sensor de ruido acústico en el Gateway, se accede al apartado: LoRaWAN -> Devices -> Add New y se introducen los campos correspondientes.

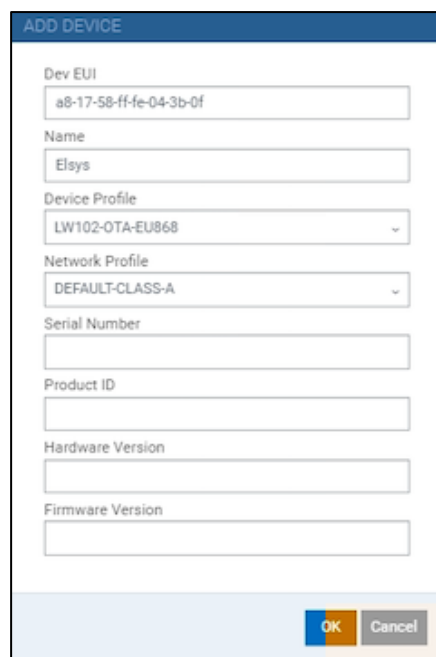


Figura 34. Sensor Elsys añadido en el Gateway

- Para que el sensor se una a la red vía OTAA, se deben introducir sus claves en el Network Server. Para ello se accede a: LoRaWAN -> Key Management -> Add New. Una vez añadidas las claves hay que esperar unos minutos para que el sensor se una a la red y comience a transmitir datos.

Figura 35. Claves del sensor añadidas en el Gateway

- Finalmente se comprueba que el sensor se ha añadido correctamente a la red LoRa y que está enviando y recibiendo datos. Para ello, en el apartado: LoRaWAN -> Devices, se pueden observar el subapartado llamado 'Sessions'. Aquí se comprueba que se están creando sesiones OTAA entre el Gateway y el sensor.

a8-17-58-ff-fe-04-3b-0f	0104c5f0	48	51	10 minutos ago	local	👁️ 🗑️
-------------------------	----------	----	----	----------------	-------	-------

Figura 36. Sesión OTAA entre el sensor y el Gateway

6.2.2.1 Programación de flujos Node-Red

Node-Red es una interfaz de programación visual desarrollada por International Business Machines (IBM). En esta herramienta se pueden crear flujos, dentro de los cuales se añaden o eliminan nodos que se conectan entre sí para comunicarse. Se puede hacer uso de Node-Red para conectar hardware, interfaces y servicios IoT.

El Gateway tiene instalada una aplicación Node-Red, dentro de la misma se crean dos flujos de comunicación mediante los cuales los datos son enviados a dos Application Server/Plataforma IoT. El primer flujo sirve para enviar los datos hacia el CPD, donde se encuentra otra aplicación de Node-Red que almacena los datos en una BBDD MySQL. Para alojar los diferentes servicios se hace uso de una instancia de una máquina virtual instalada en el CPD. Esta máquina virtual contiene el sistema operativo (SO) Ubuntu 14.04 LTS. El segundo flujo envía los datos a una API encargada de almacenarlos en otra BBDD. Cabe destacar que para inicial la aplicación Node-Red se accede al apartado 'Apps' y se pulsa en 'Launch Node-Red'.

6.2.2.1.1 Flujo 1. Plataforma open-source Grafana

En esta subsección se describe la programación del primer flujo del Node-Red que se ejecuta en el Gateway. Como se ha descrito en el desarrollo del presente documento, el fin de este flujo es la representación de los niveles de ruido acústico en la plataforma open-source Grafana. En la Figura 37 se muestra el flujo completo.

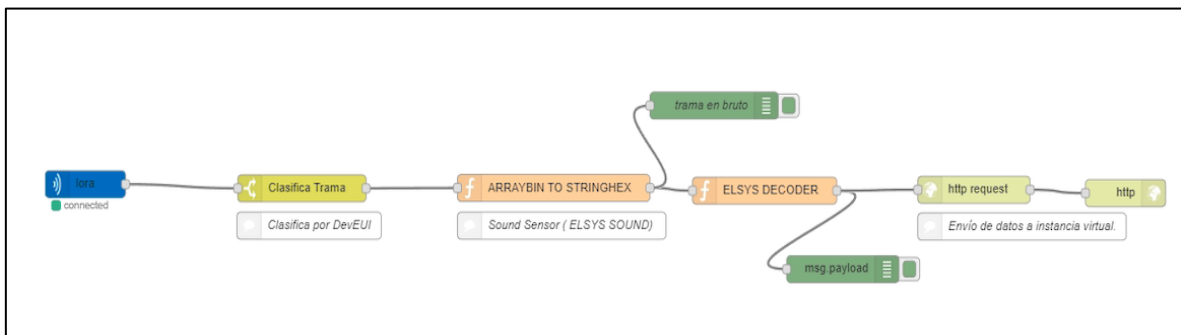


Figura 37. Flujo 1 del Node-Red en el Gateway

Se describe seguidamente la programación realizada en cada uno de los nodos la cual permite: decodificar los datos recibidos por el sensor y su envío hacia otra aplicación de Node-Red.

1. El primer nodo 'lora' recibe mensajes LoRa de la tarjeta LoRa del Gateway (MTAC-LoRA). Las tramas LoRa recibidas contienen campos como: canal usado para la recepción, DevEUI, CR, etc, tal y como se muestra en la Figura 38.

Variable	Type	Description
chan	Number	Channel used for RX
codr	String	LoRa ECC coding rate identifier
datr	String	LoRa datarate identifier
freq	String	RX central frequency in MHz (unsigned float, Hz precision)
lsnr	String	Lora SNR ratio in dB
modu	String	Modulation identifier "LORA" or "FSK"
rfch	Number	"RF chain" used for RX (will be 0 or 1)
rssi	Number	RSSI in dBm
size	Number	RF packet payload size in bytes
timestamp	String	Time of packet RX
tmst	String	Internal timestamp of "RX finished" event (32b unsigned)
payload	String or Buffer	The message data.
eui	String	The device EUI. This is a unique identifier for the mDot.

Figura 38. Campos trama LoRa.

La configuración del nodo es tan simple como escoger el formato en el que se desea que se reciban los mensajes: UTF-8 o Bytes. Se escoge la recepción de las tramas LoRa en Bytes, formato binario.

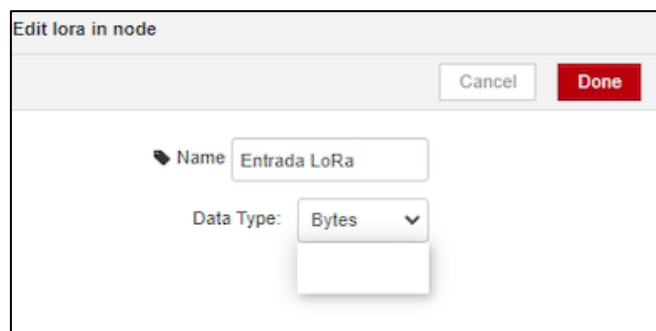


Figura 39. Nodo LoRa flujo 1.

2. El nodo titulado 'Clasifica Trama' tiene la función de filtrar las tramas LoRa según su campo DevEUI. Este nodo es de especial utilidad en flujos donde las tramas LoRa son recibidas en el Network Server desde varios sensores. En este caso se filtran las tramas para eliminar aquellas que no correspondan a las enviadas por el sensor de ruido. A pesar de no existir más sensores en la red, se introduce este nodo de cara a una ampliación futura.



Figura 40. Nodo Clasifica Trama flujo 1.

3. El siguiente nodo titulado 'ARRAYBIN TO STRINGHEX' es el nodo previo a la decodificación de los datos. Las tramas LoRa son recibidas en formato binario y en este nodo se cambian a cadenas con formato hexadecimal. Este nodo se programa con un código JavaScript para el cambio de formato del payload (datos útiles). El código se presenta en el Anexo III.
4. El nodo 'ELSYS DECODER' es el encargado de la decodificación del payload. A este nodo entra el mensaje LoRa en formato hexadecimal. A la salida se obtiene un objeto en formato *JavaScript Object Notation* (JSON), el cual es un formato de texto sencillo para el intercambio de datos. El JSON contiene los datos del payload decodificados. El código implementado para ello se presenta en el Anexo IV [15]. Tras la decodificación del payload se obtiene un JSON del siguiente tipo:

```

1 {
2   "temperature": 26.3,
3   "humidity": 46,
4   "light": 1,
5   "motion": 0,
6   "vdd": 3630,
7   "soundPeak": 64,
8   "soundAvg": 48
9 }

```

Cabe destacar que se obtienen los datos recogidos por todos los sensores internos, sin embargo, en este TFG se hace uso únicamente de los parámetros 'soundPeak' y 'soundAvg' ya que son los correspondientes al ruido acústico.

5. El Gateway cuenta con un cliente http. Esto hace posible que se puedan enviar los datos decodificados hacia un servidor http. Los datos son enviados al servidor

http, el cual se aloja en la instancia virtual del CPD. Se hace uso del método POST para el envío de los datos al servidor. Se hace uso del certificado SSL/TLS para realizar el envío mediante una conexión segura y cifrada (HTTPS). La URL a la cual se realiza el envío es la correspondiente a la dirección de red de la instancia Node-Red alojada en el CPD. El nodo 'http request' es el encargado de esta tarea. Su configuración queda reflejada en la Figura 41.

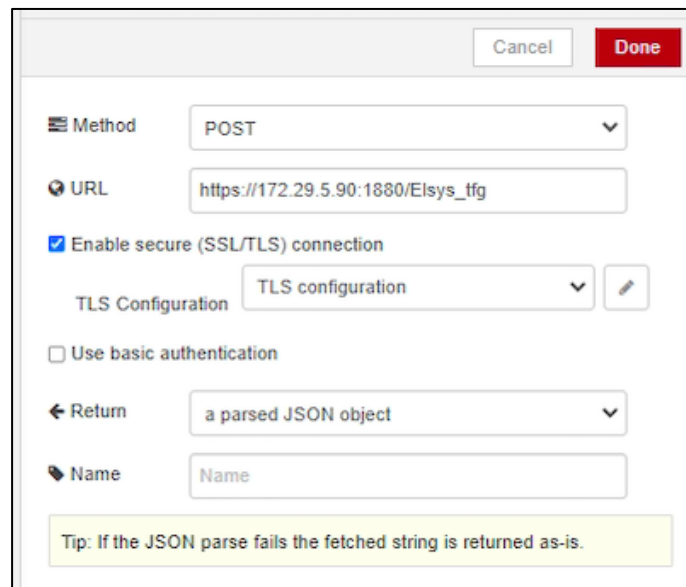


Figura 41. Nodo http request flujo 1

Una vez realizada la configuración y programación de los nodos, queda completado el primer flujo Node-Red del Gateway. En la sección relativa a la descripción del Application Server / Plataforma IoT se describe la configuración de la instancia de Node-Red alojada en el CPD, la cual es la encargada de almacenar los datos en una BBDD. A partir de esta, Grafana representan los datos al usuario final.

6.2.2.1.2 Flujo 2. Plataforma propietaria In4city

En la presente subsección se describe la programación del segundo flujo del Node-Red que se ejecuta en el Gateway. La función de este flujo es enviar las tramas LoRa recibidas en el Network Server hacia una API propietaria de la empresa. Una vez recibidos los datos, esta API realiza la conversión y decodificación de los datos y su almacenamiento en una base de datos (BD). Finalmente, la plataforma propietaria In4city hace uso de esta BD para representar la información.

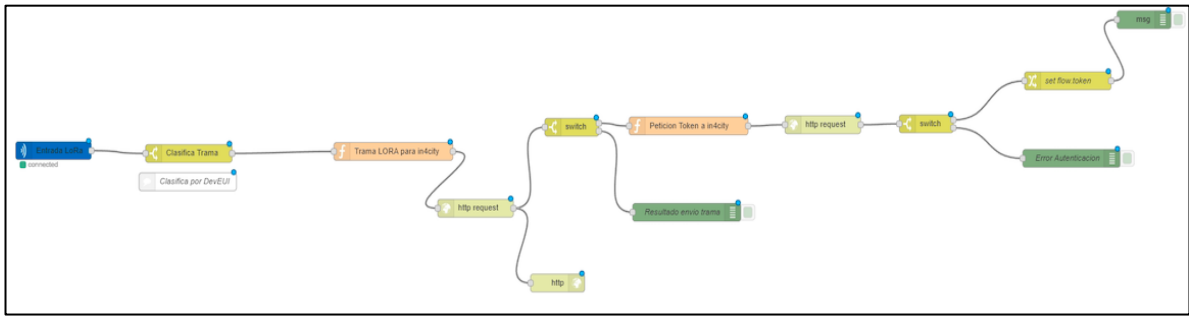


Figura 42. Flujo 2 Node-Red en el Gateway

A continuación, se describe la función de cada uno de los nodos que componen el presente flujo. Sin embargo, por razones de confidencialidad no se muestra el código implementado en los nodos.

1. El nodo titulado 'Trama LORA para in4city' se encarga de crear el mensaje que será enviado al back-end de la plataforma In4city donde son decodificados los datos. Para ello, este nodo se programa de forma que se crea un mensaje con método de envío POST, la URL de la API y un payload que contiene la trama LoRa recibida en el Network Server.
2. El primer nodo 'http request' realiza el envío del mensaje creado en el anterior nodo a la API, mediante un POST y haciendo uso de https.
3. Cuando se crea un nuevo usuario en la plataforma In4city, es necesaria su validación mediante un token. Sin este token, no se pueden enviar datos hacia el back-end de In4city. Por tanto, el nodo 'switch' sirve para escoger un camino del flujo según los mensajes de respuesta enviados por el servidor http tras la petición POST. Cuando el usuario de in4city no dispone del token, se produce un error (código de error http 401) al no disponer el usuario de un token. Entonces se hace necesaria su petición. En caso de disponer el usuario de un token, la petición se realizará correctamente (código http 200).

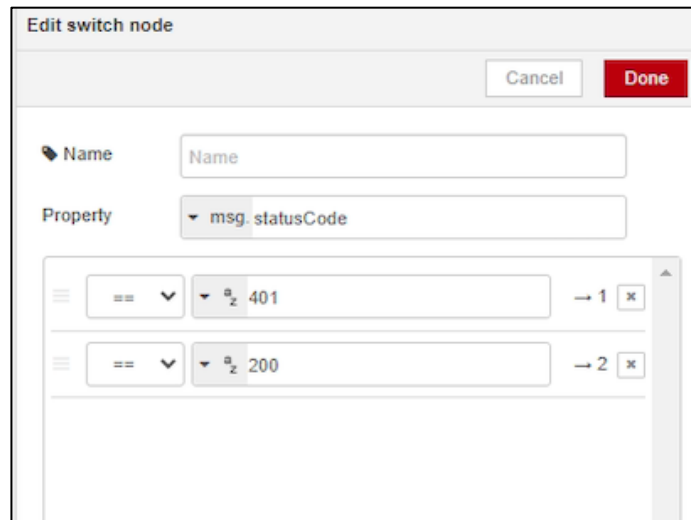


Figura 43. Nodo Switch 1 flujo 2.

4. Cuando se necesita de la petición de token, el camino que sigue el flujo tras el nodo 'switch' es el camino 1 (superior). En este camino, el primer nodo llamado 'Petición Token a in4city' crea el mensaje que será enviado mediante https con el método POST para la petición del token. En la programación de este nodo se debe incluir el nombre de usuario de In4city y su contraseña.
5. El nodo 'http request' es el encargado de realizar la petición POST al servidor, enviando en esta la petición del token.
6. Una vez la petición es enviada, el servidor responde con un mensaje de aceptación (código 200) en el caso de que la petición se realice correctamente. En este caso el servidor envía el token hacia el cliente para que finalmente se pueda realizar el envío de los datos hacia la API. Si la petición es errónea, se recibe un mensaje de error por parte del servidor (código distinto a 200). En este caso se muestra un mensaje de debug mostrando el error. El proceso de selección del camino a seguir según el código de estado http recibido es realizado por el nodo 'switch'.

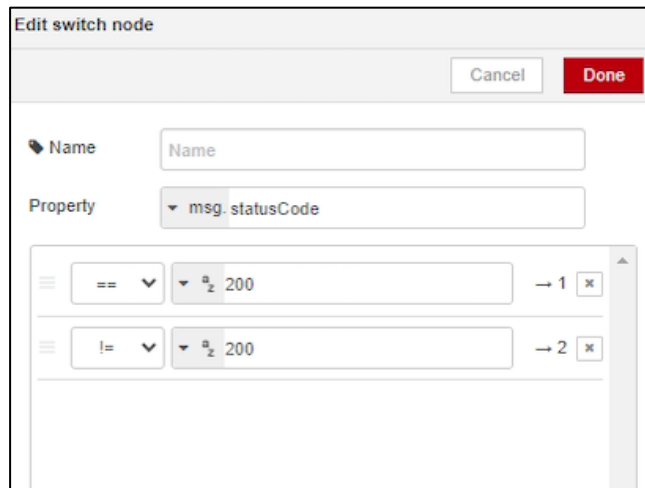


Figura 44. Nodo Switch 2 Flujo 2.

7. Cuando la petición del token se realiza correctamente, se asigna el token al mensaje que será enviado hacia la API. Para ello se implementa el nodo 'set Flow.token'. Cabe destacar que los token tienen un periodo de expiración de un (1) día, por lo que se solicitan una vez al día aproximadamente.

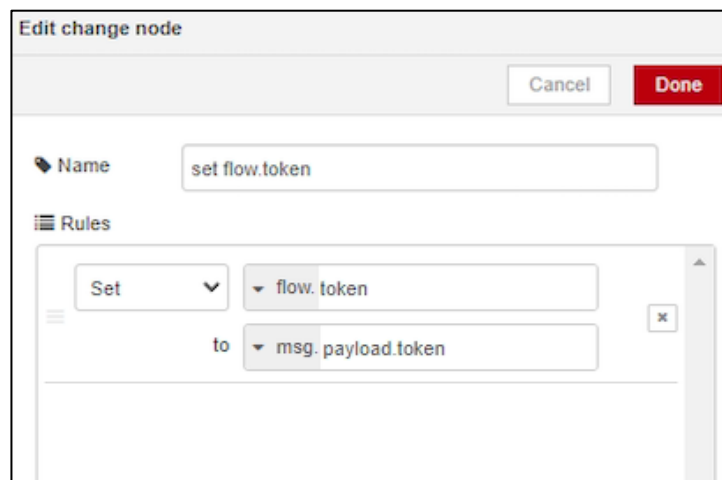


Figura 45. Nodo para asignación de token en flujo 2

De esta forma queda finalizada la configuración y programación de los nodos que componen el presente flujo.

6.2.3 Application Server / Plataforma IoT

En las secciones anteriores se ha descrito la configuración del sensor y el Gateway. Además, se ha configurado el Network Server el cual se encuentra embebido en el propio Gateway. Finalmente se ha realizado la configuración y programación de

los nodos que componen los dos flujos del Node-Red ejecutado en el Gateway. En la presente sección se describe la configuración y programación cuando procede del Application Server y plataforma IoT. Para la descripción, se divide esta sección en dos subsecciones correspondientes a cada uno de los flujos que sirven para la representación de los datos en dos plataformas distintas.

6.2.3.1 Plataforma open-source Grafana

Una vez los datos decodificados son enviados desde el Network Server hacia la instancia virtual alojada en el CPD, estos son recibidos en una aplicación Node-Red. Aquí, se crea un flujo cuyo fin es el almacenamiento de los datos en una BD MySQL. Para la representación de los niveles de ruido acústico se crea un tablero o dashboard en la plataforma open-source Grafana. Cabe destacar que la máquina virtual de la que se hace uso es propietaria de la empresa y fue implementada anteriormente por el departamento de desarrollo. Se trata de una máquina virtual VMware ESXi con SO Ubuntu 14.04 LTS. Para el acceso a esta es necesario disponer de un cliente VPN conectado al portal de la empresa. Para ello se hace uso de la tecnología Global Protect.

En la presente subsección se describe la configuración y programación de los diferentes servicios necesarios para la representación final de los datos.

6.2.3.1.1 Base de datos MySQL

Para la recepción de los datos en el CPD se hace necesaria la creación de una BD en la cual se almacenen los parámetros recogidos por el sensor. Se instala en la máquina virtual del CPD una BD MySQL para este fin. Para la representación, Grafana lee esta BD en local. La presente subsección describe la instalación del servicio y la creación de la BD, usuario para acceder a esta y finalmente la tabla con sus correspondientes columnas.

1. Para la instalación del servicio se accede a la máquina virtual mediante Secure Shell (SSH) con las credenciales del usuario root, proporcionadas por la empresa.

```
1 ssh usuario@172.29.5.90
```

2. Para la instalación de MySQL, primero se actualiza la lista de paquetes.

```
1 sudo apt update
```

3. Se instala el servidor MySQL.

```
1 sudo apt install mysql-server
```

4. En el primer inicio, al no haber establecido una contraseña se inicia el servicio con usuario 'root' y campo de contraseña vacío.

```
1 mysql -u root -p
```

6. Se crea la BD a la cual Grafana accede en local para la representación de los datos.

```
1 create database LoRaTFG character set utf8;
```

7. Para el acceso a la BD creada, se crea un nuevo usuario.

```
1 create user alc00101@'localhost' identified by 'Loratfgl!';
```

8. Es necesario asignar privilegios al usuario creado para poder acceder y modificar la BD creada.

```
1 grant all on LoRaTFG.* to 'alc00101'@'localhost';
```

9. Para asegurar que se asignan los privilegios, se debe reiniciar la caché para que todo funcione como se espera.

```
1 flush privileges;
```

10. Para entrar al servidor MySQL con el nuevo usuario se debe salir del servicio y entrar de nuevo con las credenciales del nuevo usuario.

```
1 mysql -ualc00101 -pLoratfgl!
```

11. Una vez se accede con el usuario creado, queda crear la tabla con sus respectivas columnas para el almacenamiento de los datos enviados por el sensor de ruido. Para ello en primer lugar se accede a la BD.

```
1 use LoRaTFG
```

12. Se crea una tabla en la BD con el nombre 'medidas'. En ella, las columnas o entradas creadas son: id, DevEUI, soundAvg, soundPeak y timestamp. La clave primaria es el 'id'. Es muy importante introducir la columna 'timestamp' para la situar temporalmente los datos en la representación.

```
1 CREATE TABLE medidas( id BIGINT UNSIGNED AUTO INCREMENT
PRIMARY KEY, DevEUI VARCHAR(255), soundAvg INT(11), soundPeak
INT(11), TIMESTAMP DEFAULT CURRENT_TIMESTAMP );
```

13. Finalmente queda realizada la instalación y creación de la BD. Se comprueba la creación de la tabla con sus columnas.

```
mysql> show tables;
+-----+
| Tables_in_LoRaTFG |
+-----+
| medidas           |
+-----+
1 row in set (0,01 sec)

mysql> show columns from medidas;
+-----+-----+-----+-----+-----+-----+
| Field      | Type                | Null | Key | Default        | Extra          |
+-----+-----+-----+-----+-----+-----+
| id         | bigint(20) unsigned | NO   | PRI | NULL           | auto_increment |
| DevEUI     | varchar(255)        | YES  |     | NULL           |                |
| soundAvg   | int(11)             | YES  |     | NULL           |                |
| soundPeak  | int(11)             | YES  |     | NULL           |                |
| timestamp  | timestamp           | NO   |     | CURRENT_TIMESTAMP |                |
+-----+-----+-----+-----+-----+-----+
5 rows in set (0,05 sec)

mysql> █
```

Figura 46. Tabla 'medidas' y sus columnas en la BBDD MySQL

6.2.3.1.2 Flujo Node-Red para la recepción y almacenamiento de datos

Este flujo sirve como back-end de la plataforma IoT para la representación de los datos. En primer lugar, es necesaria la instalación de este servicio en la máquina virtual. Para ello se describe a continuación los comandos de consola necesarios para ello [16].

1. En primer lugar, se actualizan los repositorios.

```
1 sudo apt-get update
```

2. Instalación de git.

```
1 sudo apt-get install git
```

3. Instalación de cURL, la cual es una herramienta de línea de comandos que sirve para enviar o recibir datos con la sintaxis URL.

```
1 sudo apt-get install curl
```

4. Instalación de Node JS.

```
1 curl -sL https://deb.nodesource.com/setup_6.x | sudo -E bash
```

5. Instalación de Node-Red.

```
1 sudo npm install -g --unsafe -perm node-red
```

6. Inicio de Node-Red.

```
1 sudo node-red
```

Una vez instalado e iniciado el servicio, este comenzará su ejecución en el puerto 1880. Para acceder a este, se introduce en un navegador la URL con la dirección IP de la máquina virtual y el puerto correspondiente: <https://172.29.5.90:1880>. Una vez dentro, se procede a la creación del flujo.

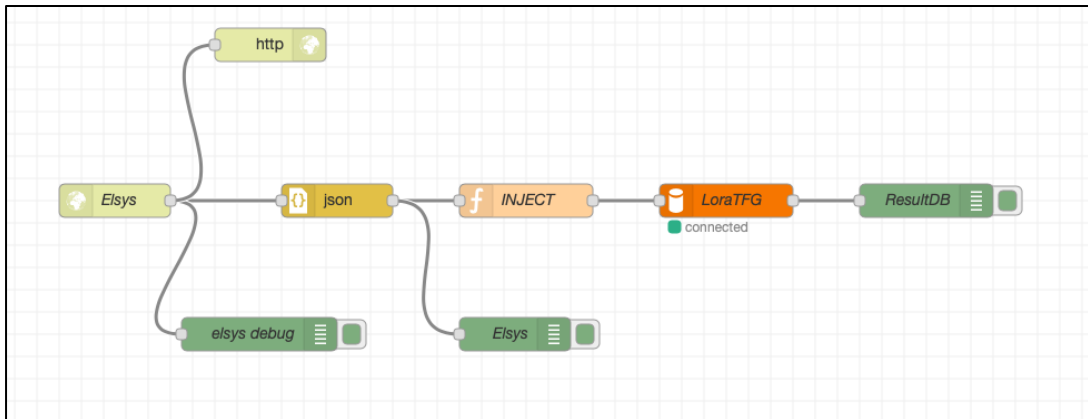


Figura 47. Flujo Node-Red de recepción de datos en el CPD.

La configuración y programación de los diferentes nodos que lo componen es la que sigue:

1. La comunicación entre el Network Server y el CPD se realiza mediante el protocolo http(s). Tal y como se describió anteriormente, el Gateway cuenta con un cliente http que envía los datos hacia el servidor. El servidor corre en la instancia virtual del CPD y es el que recibe dichos datos. Para la recepción y procesamiento de estos, se crea un nodo en el presente flujo con la función de servidor http. El nodo titulado 'Elsys' sirve para la recepción de la petición POST enviada desde el Node-Red del Network Server. En este nodo se crea un directorio para la recepción de la petición.

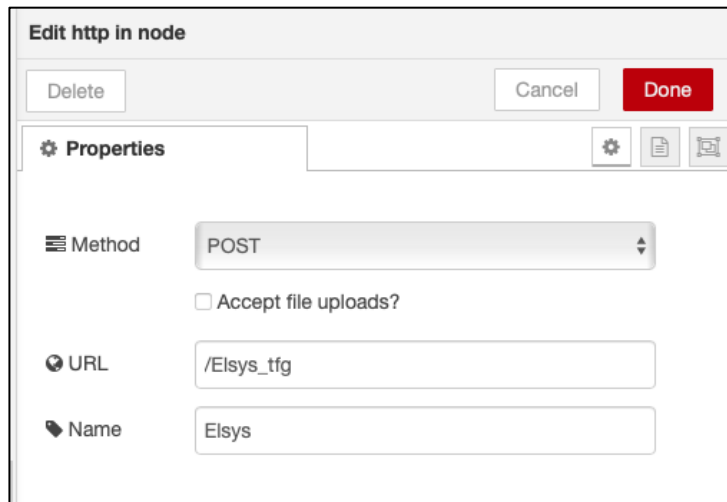


Figura 48. Nodo servidor http en flujo de recepción en el CPD.

2. Los datos son recibidos en el servidor en formato JSON. Al tratarse este de un formato de texto plano para el intercambio de datos, se hace necesaria su conversión a objeto JS para su manipulación. El nodo titulado 'json' es el encargado de realizar dicha conversión.

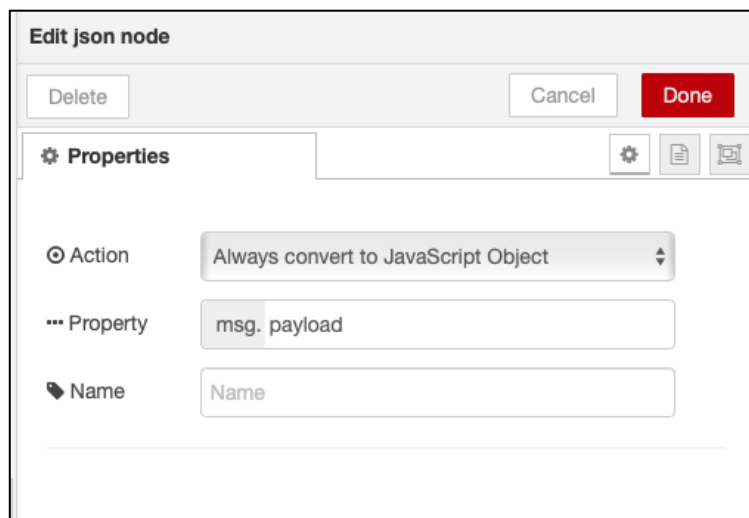


Figura 49. Nodo conversión a JSON en flujo de recepción en el CPD.

3. Una vez se obtiene un objeto JS, sus campos son accesibles. Esto es necesario para la creación de la consulta o *query* a la BD. El nodo 'INJECT' se programa para montar la *query* en base a las columnas de la tabla que se creó en el apartado anterior. Cabe destacar que únicamente se almacenan las medidas relativas al ruido acústico.

```

1 msg.topic = "INSERT INTO medidas (DevEUI, soundAvg, soundPeak)
2 VALUES ('a8-17-58-ff-fe-04-3b-0f', "+msg.payload.soundAvg+",
3 "+msg.payload.soundPeak+")";
4 return msg;

```

- Tras la creación de la query para la inyección en la BD, únicamente queda conectar con la BD. El nodo 'LoraTFG' realiza esta conexión. Para ello se debe configurar introduciendo como dirección de host la de *loopback*, ya que es un proceso local. Además, se especifica el puerto de MySQL 3306 (puerto por defecto).

The image shows a configuration window titled 'Edit mysql node > Edit MySQLdatabase node'. At the top, there are three buttons: 'Delete', 'Cancel', and 'Update'. Below the buttons is a 'Properties' section with several input fields:

- Host:** 127.0.0.1
- Port:** 3306
- User:** alc00101
- Password:**
- Database:** LoRaTFG
- Timezone:** (empty field)

Figura 50. Nodo MySQL en flujo de recepción en Node-Red

De esta forma queda finalizada la configuración y programación de los nodos que componen el presente flujo de Node-Red. Se comprueba que los datos se almacenan correctamente en la BD. Para ello se realiza la siguiente consulta.

```

1 select * from medidas;

```

```
mysql> select * from medidas;
```

id	DevEUI	soundAvg	soundPeak	timestamp
1	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 17:39:00
2	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 17:49:04
3	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 17:59:00
4	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 18:09:04
5	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 18:19:04
6	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 18:29:03
7	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 18:39:01
8	a8-17-58-ff-fe-04-3b-0f	43	64	2022-06-06 18:49:03
9	a8-17-58-ff-fe-04-3b-0f	42	64	2022-06-06 18:59:00
10	a8-17-58-ff-fe-04-3b-0f	48	64	2022-06-06 19:09:04
11	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 19:19:05
12	a8-17-58-ff-fe-04-3b-0f	48	64	2022-06-06 19:29:04
13	a8-17-58-ff-fe-04-3b-0f	48	64	2022-06-06 19:39:03
14	a8-17-58-ff-fe-04-3b-0f	48	64	2022-06-06 19:49:03
15	a8-17-58-ff-fe-04-3b-0f	48	64	2022-06-06 19:59:03
16	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 20:09:01
17	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 20:19:00
18	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 20:29:00
19	a8-17-58-ff-fe-04-3b-0f	49	64	2022-06-06 20:39:01
20	a8-17-58-ff-fe-04-3b-0f	48	64	2022-06-06 20:49:03

Figura 51. Registro de datos en la BBDD.

6.2.3.1.3 Creación dashboard de Grafana e implementación de notificaciones

Grafana es un software open-source que permite ejecutar análisis de datos, extraer métricas significativas en grandes volúmenes de datos y monitorear recursos de aplicaciones y hardware con tableros personalizables. Para la lectura de datos, se conecta con diferentes BBDD tales como MySQL, Influx DB o PostgreSQL.

En la presente subsección se describe en primer lugar la instalación de Grafana en la máquina virtual del CPD. Tras ello se configura para que lea la BD en local. Se crea un tablero con dos paneles, uno para la representación del nivel medio de ruido acústico y otro para el nivel de pico recogidos por el sensor. Finalmente se dota a la plataforma de un servicio de notificaciones vía Telegram.

Para la instalación de Grafana se realizan los pasos que se detallan a continuación [17]. Los comandos son introducidos en la máquina virtual mediante la conexión a esta por SSH.

1. Por defecto Grafana no se encuentra disponible en el repositorio de Ubuntu 18.04 LTS. Por ello es necesario añadirlo, para ello se introduce el siguiente comando:

```
1 sudo nano /etc/apt/sources.list
```

2. Se añade la siguiente línea al final del archivo.

```
1 deb https://packagecloud.io/grafana/stable/debian/ stretch main
```



```
albertlopezcasanova — usuario@nodered1: ~ — ssh usuario@172.29.5.9...
GNU nano 2.9.3 /etc/apt/sources.list

# deb http://archive.canonical.com/ubuntu bionic partner
# deb-src http://archive.canonical.com/ubuntu bionic partner

deb http://archive.ubuntu.com/ubuntu bionic-security main restricted
# deb-src http://archive.ubuntu.com/ubuntu bionic-security main restricted
deb http://archive.ubuntu.com/ubuntu bionic-security universe
# deb-src http://archive.ubuntu.com/ubuntu bionic-security universe
deb http://archive.ubuntu.com/ubuntu bionic-security multiverse
# deb-src http://archive.ubuntu.com/ubuntu bionic-security multiverse
deb https://artifacts.elastic.co/packages/7.x/apt stable main
# deb-src https://artifacts.elastic.co/packages/7.x/apt stable main
deb https://packagecloud.io/grafana/stable/debian/ stretch main

[ Wrote 53 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Figura 52. Inclusión de repositorio Grafana.

3. Una vez guardado el archivo, se añade la clave pública mediante el siguiente comando:

```
1 sudo curl https://packagecloud.io/gpg.key | sudo apt-key add -
```

4. Se actualiza el repositorio.

```
1 sudo apt-get update -y
```

5. Finalmente se realiza la instalación de Grafana con el siguiente comando:

```
1 sudo apt-get install grafana -y
```

6. Una finalizada la instalación, se inicia el servicio y se permite a Grafana iniciarse a la vez que el sistema. Todo ello se realiza introduciendo los siguientes comandos:

```
1 sudo systemctl daemon-reload
2 sudo systemctl enable grafana-server
3 sudo systemctl start grafana-server
```

7. De esta forma queda instalado e iniciado el servicio. Para acceder a Grafana se introduce en un navegador la URL con la dirección IP de la máquina y el puerto por defecto de Grafana, el cual es el 3000.

URL : <http://172.29.5.90:3000>.



Figura 53. Acceso a la plataforma Grafana

En el primer inicio de Grafana se debe crear un usuario, el creado en este TFG es el siguiente: username: admin / password: Innovasur1!.

Una vez instalada la herramienta Grafana, se procede a la creación del dashboard para la visualización de los datos almacenados en la BD. Para ello en primer lugar se realiza la conexión con la BD y en segundo lugar se crea el dashboard. A continuación se describe el procedimiento seguido para ello.

1. El primer paso es la conexión local de Grafana con la BD. Para ello se accede al apartado 'configuration' -> 'Data Sources' -> 'Add data source'.

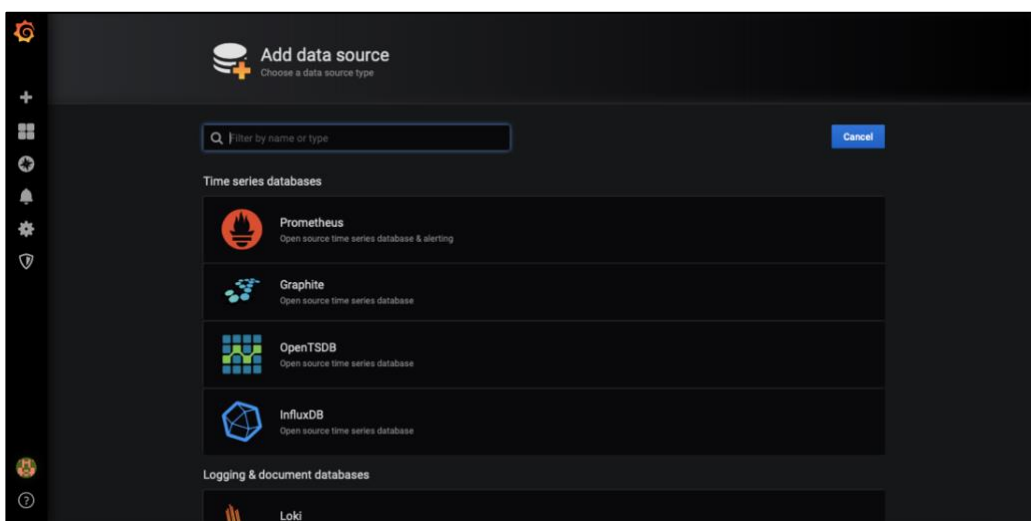


Figura 54. Sección Añadir fuente de datos en Grafana.

A continuación, se busca la BD con la que se desea conectar Grafana, en el caso del presente TFG se selecciona la BD MySQL. Una vez seleccionada queda rellenar los campos descritos con la configuración realizada en la BD creada para el presente TFG.

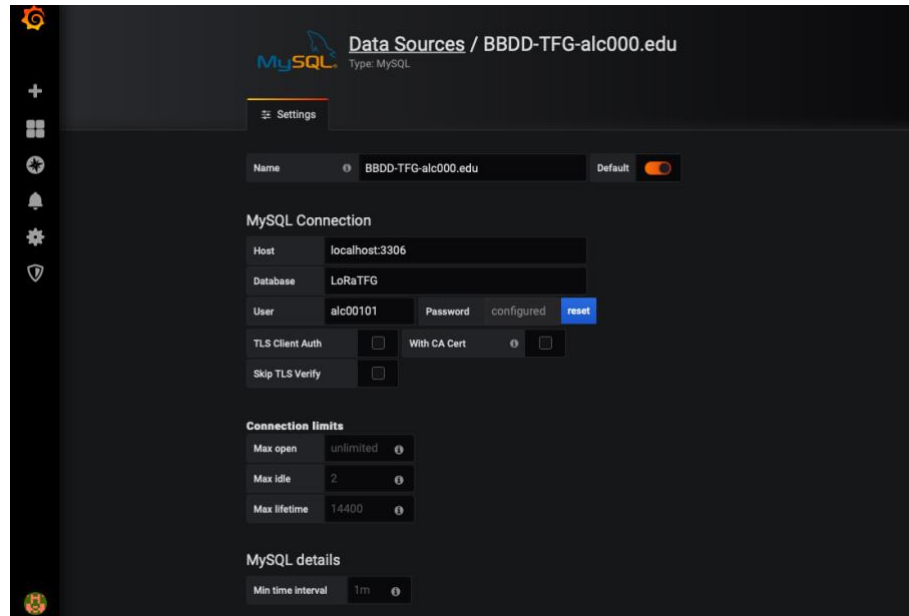


Figura 55. Conexión con la BBDD MySQL en Grafana.

2. Una vez realizada exitosamente la conexión con la BD se procede a la creación del dashboard para la representación y visualización de los niveles de ruido acústico. El dashboard cuenta con dos paneles: uno para representar la medida 'soundAvg' y otro para 'soundPeak'. Para la creación del dashboard se parte de la ventana inicial de Grafana y se accede a 'create (+)' -> 'Dashboard'.

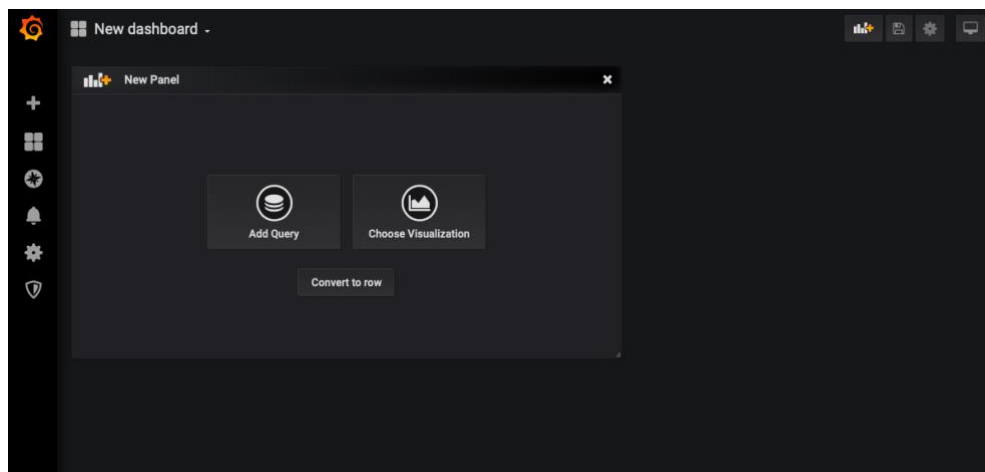


Figura 56. Creación de dashboard en Grafana.

Se procede a la creación del primer panel pulsando en el icono 'Add Query'. Tras ello, el primer paso es crear la query a la BD para la lectura de datos. En primer lugar, se crea el panel para representar la medida 'soundAvg'. La consulta realizada es la siguiente:

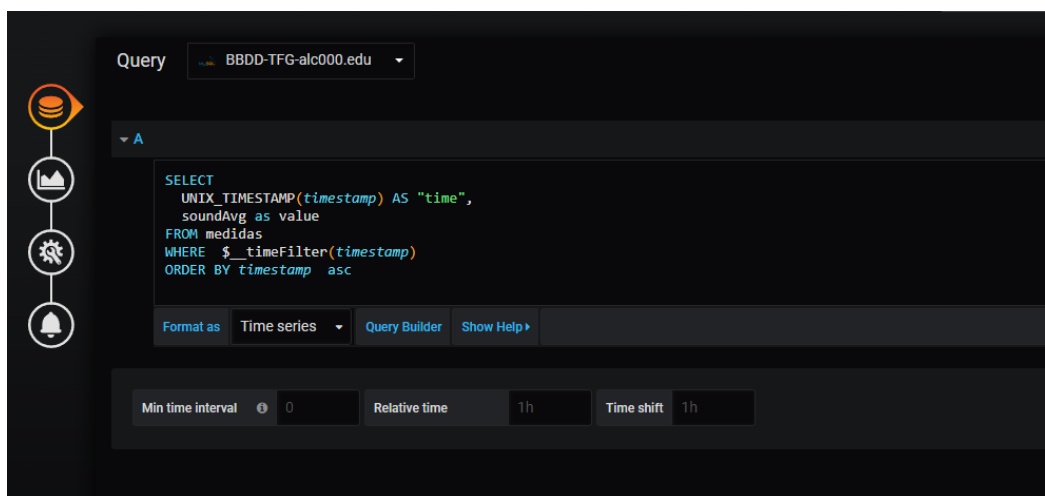


Figura 57. Query a la BD para representación de la media de ruido.

En segundo lugar, se escoge el gráfico de visualización. Se ha escogido una gráfica con líneas y puntos. El eje 'x' representa la línea temporal mientras que el eje 'y' representa el nivel de ruido acústico en DbSPL.

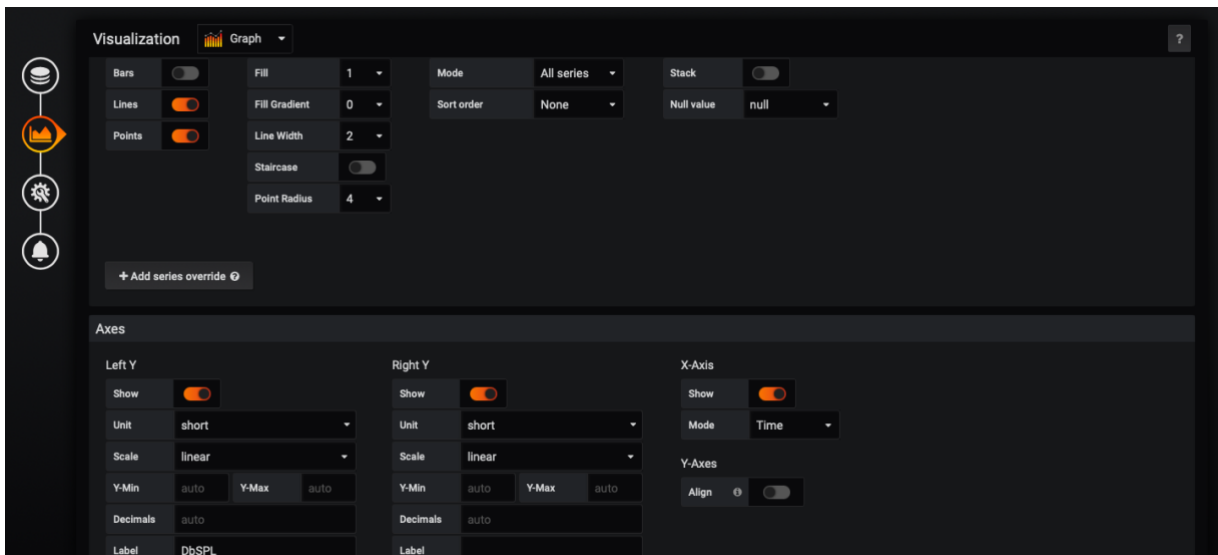


Figura 58. Configuración visualización de la media de ruido.

Finalmente se añade el título 'Sound Average' al panel. De esta forma queda finalizada la creación del presente panel. Para la creación del panel 'Sound Peak' se accede al dashboard -> 'Add new Panel' y se repite el proceso de creación de panel. En este caso la query realizada es la siguiente:

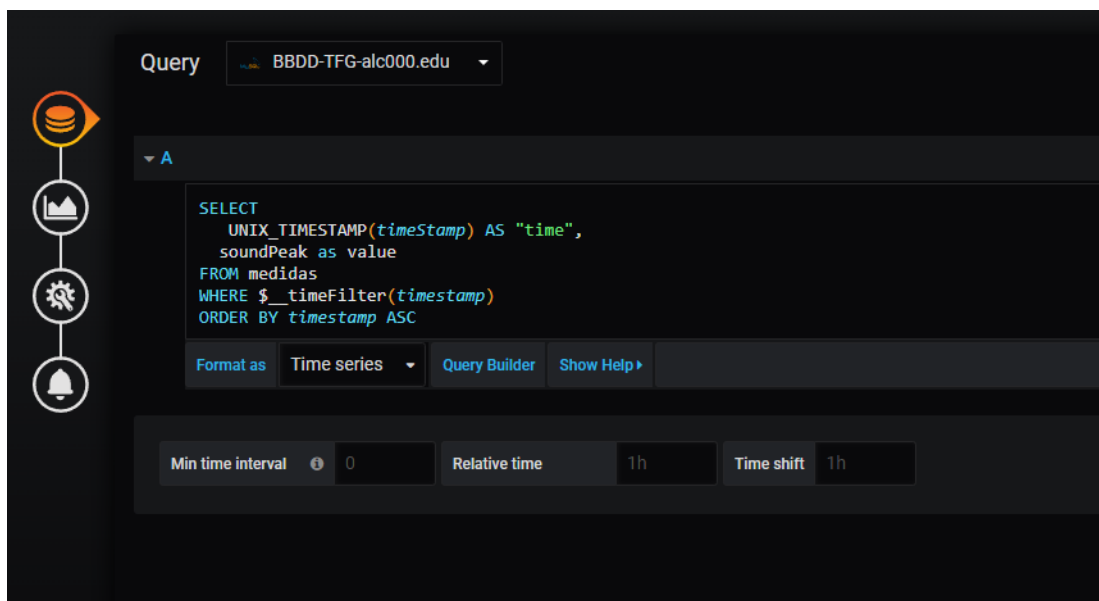


Figura 59. Query a la BD para la representación del nivel de pico de ruido.

Con el fin de que el usuario no necesite consultar constantemente el dashboard para saber cuándo se supera cierto nivel de ruido acústico, se ha dotado al sistema con un servicio de notificaciones. Grafana dispone de servicio de notificaciones a través de diferentes canales tales como: correo electrónico, Telegram o Discord entre otros. En el

presente TFG se ha implementado el servicio de notificaciones a través de la aplicación de mensajería instantánea Telegram. Los pasos realizados para ello son los que siguen [18]:

1. En primer lugar, se añade un nuevo canal de notificaciones. Para ello se accede desde la ventana inicial de Grafana a 'Alerting' -> 'Notification channels' -> 'Add channel'. A continuación, se rellenan los campos escogiendo Telegram como el canal de notificaciones.

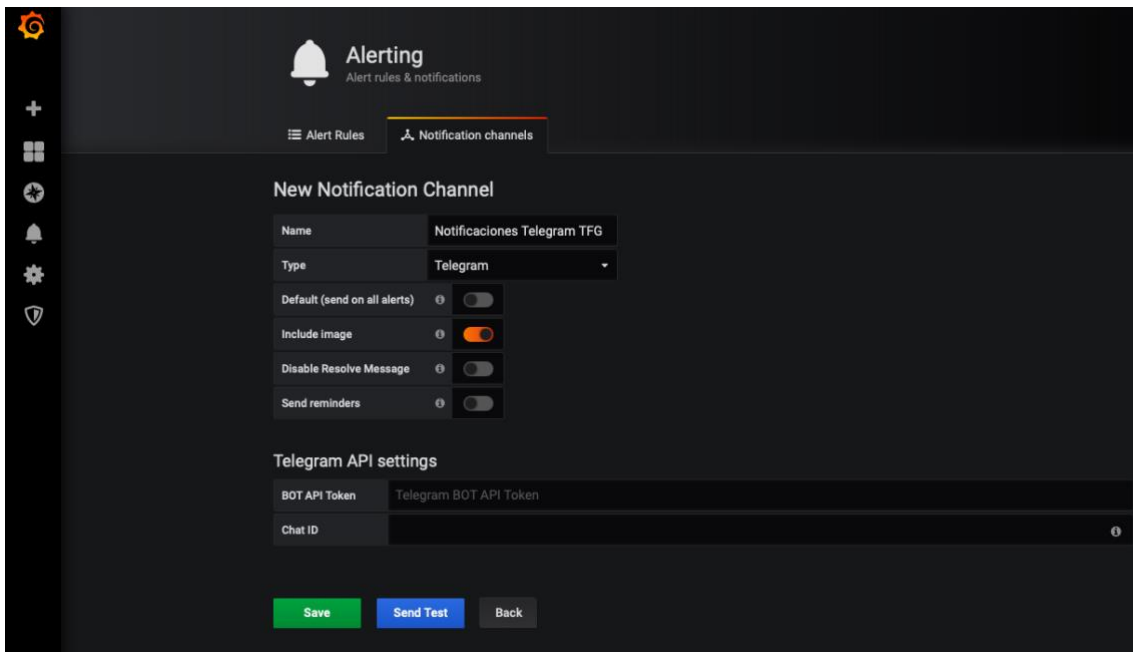


Figura 60. Creación del canal de notificaciones Telegram en Grafana.

Para finalizar este paso es necesario introducir los campos 'BOT API Token' y 'Chat ID', necesarios para la recepción de las alertas. Para ello en primer lugar se debe iniciar una conversación en Telegram con *@BotFather*. Una vez iniciada la conversación, se escribe el comando */newbot*. El bot responde preguntando por el nombre que se desea que tenga y el nombre de usuario. Cabe destacar que el nombre de usuario debe acabar en *bot*. Una vez se ha respondido al bot, este envía un mensaje con el token para poder usar la API de notificaciones. Este token es el que se debe introducir en la creación del canal de notificaciones en Grafana. El token obtenido es el siguiente: **5382912909:AAFy9kec6vvoIQZ7xonjWe-dX45fiqqSXIE**. La conversación completa con *@BotFather* se muestra a continuación en la Figura 61.

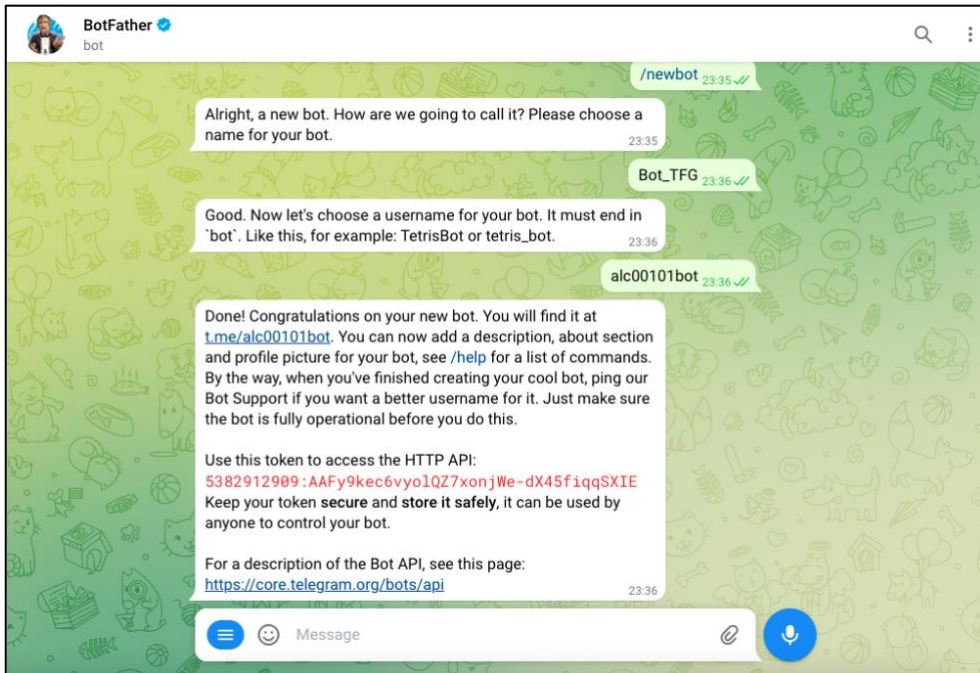


Figura 61. Obtención del token de Telegram.

Por último, es necesario obtener el 'Chat ID', el cual es un identificador único del usuario de Telegram creado. Se accede a Telegram y se inicia una conversación con @IDBot. Para obtener el ID basta con enviar el comando /getid. El ID obtenido es el siguiente: **1285963877**.

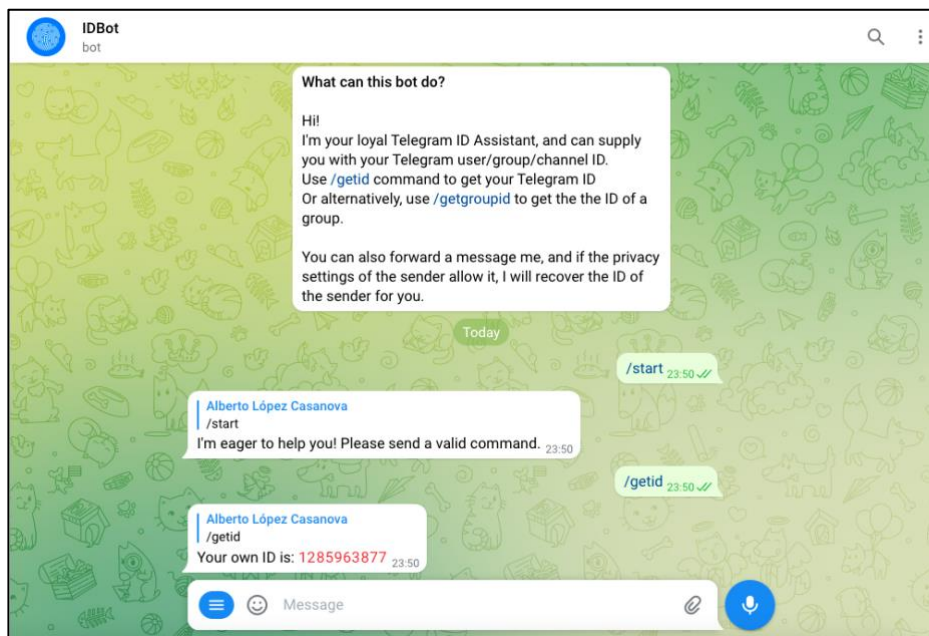


Figura 62. Obtención del Chat ID de Telegram

Obtenidos el token y el ID, se introducen en los campos correspondientes en la creación del canal de notificaciones de Grafana. Para comprobar el funcionamiento, se pulsa en 'Send test'. De esta forma se recibe un mensaje de Telegram de prueba tal y como se puede observar en la Figura 63.

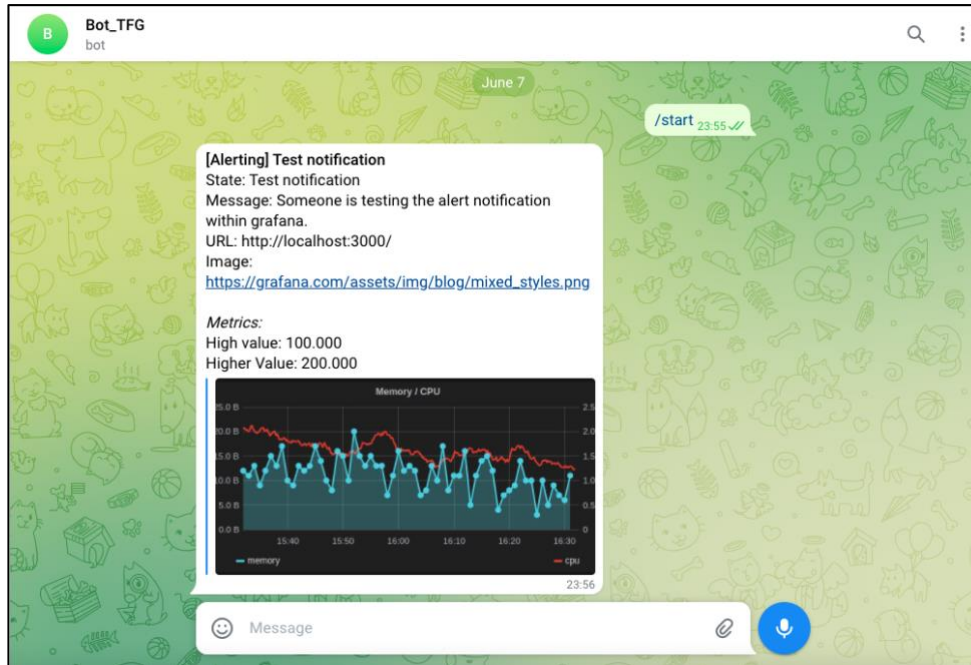


Figura 63. Recepción de notificación de test de Grafana.

2. Finalmente se crean las alertas que se desean recibir. Se han creado dos alertas, una por cada panel del dashboard. Para configuración hay que entrar en el panel al que se le desea aplicar la alerta. Una vez dentro se accede al apartado 'alertas'. Se rellenan los campos y se asigna el canal de notificaciones creado en el anterior paso. En el caso del panel correspondiente a la media de ruido acústico, se ha configurado para que se active la alerta cuando se superen los 60 Db(A), tal y como se observa en la Figura 64. Para el nivel de ruido de pico, en la Figura 65 se observa que la alerta se activa cuando se superan los 85 Db(A).

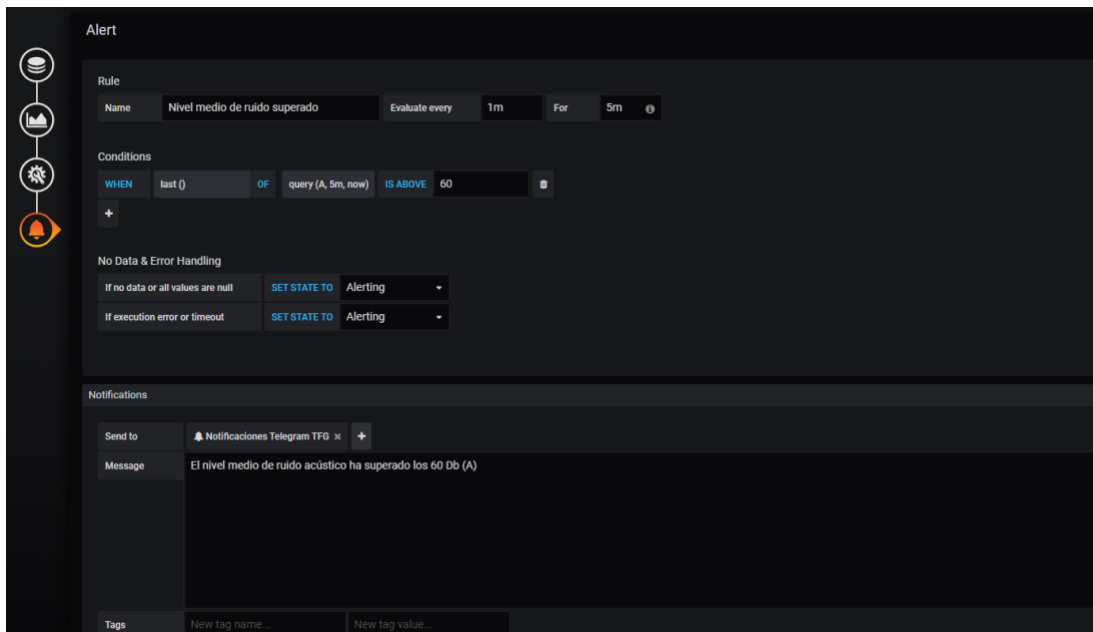


Figura 64. Configuración alerta Grafana para nivel de ruido medio.

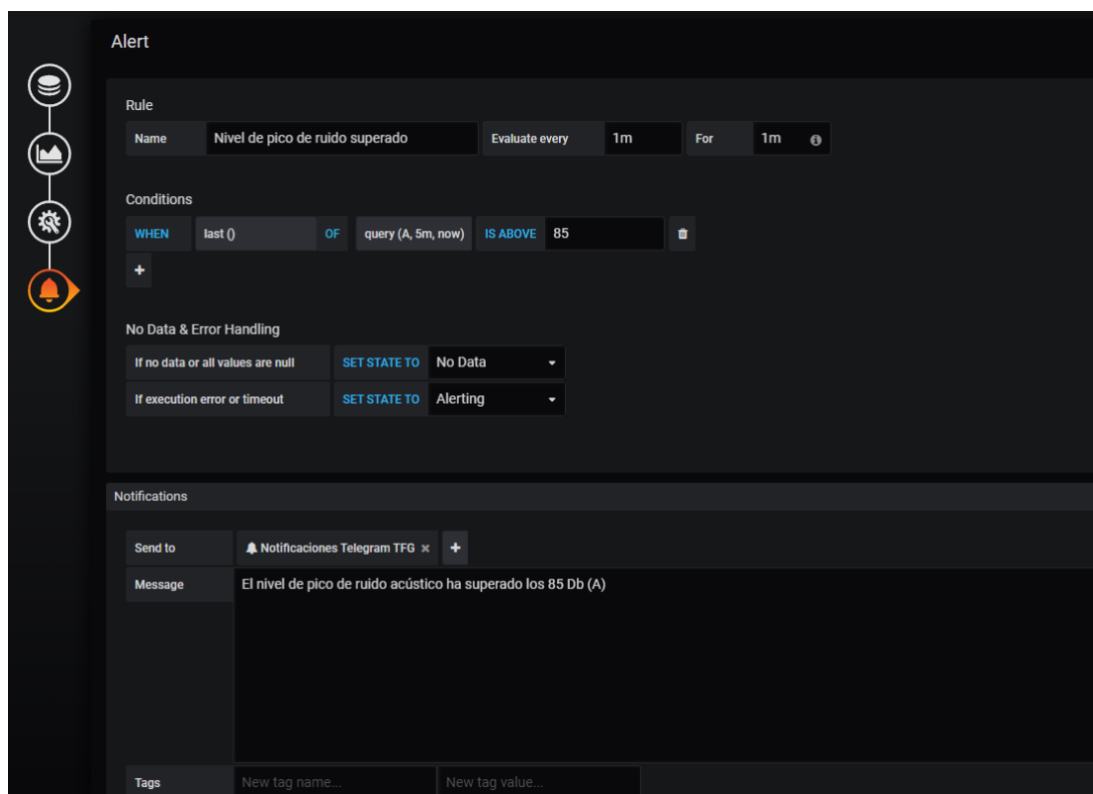


Figura 65. Configuración alerta Grafana para nivel pico de ruido.

De esta forma queda realizada la instalación y configuración de Grafana para la representación de los datos y la recepción de notificaciones.

6.2.3.2 Plataforma propietaria In4city

In4city es una plataforma urbana inteligente desarrollada por la empresa Innovasur S.L.. In4city ofrece una gestión integral de soluciones inteligentes y tecnologías vanguardistas con el objetivo de optimizar los servicios y recursos públicos [19]. En ella se integran las diferentes verticales implementadas por la empresa tales como: sistema de Circuito Cerrado de Televisión (CCTV) con analítica de vídeo o sensórica LoRa. En el presente TFG se hace uso de la vertical de sensórica LoRa. Además, la parte del presente TFG correspondiente a la plataforma In4city sirve como muestra del servicio ofrecido a los clientes.

En la presente subsección se detalla el procedimiento realizado para representar los niveles de ruido acústico del sensor LoRa en esta plataforma. Cabe destacar que por motivos de confidencialidad no se muestran contraseñas.

En primer lugar, se debe crear un usuario de In4city, para ello se accede al usuario con privilegios de administración de la plataforma y se crea un usuario llamado 'LoraTFG' con su respectiva contraseña.

Los pasos realizados para la representación de los niveles de ruido acústico en In4city además de la recepción de notificaciones son los siguientes:

1. Una vez creado el usuario, se accede a <https://mi.in4city.es> y se entra a la plataforma con las credenciales del usuario creado. La pantalla principal se muestra en la Figura 66.

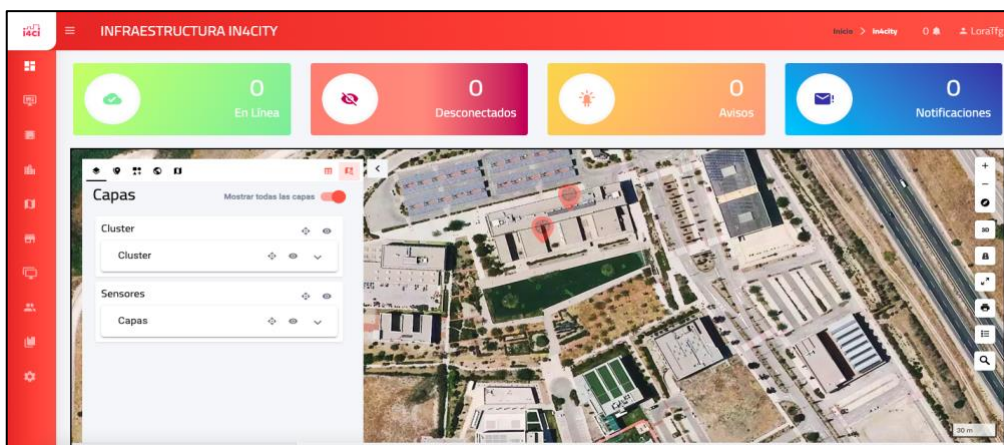
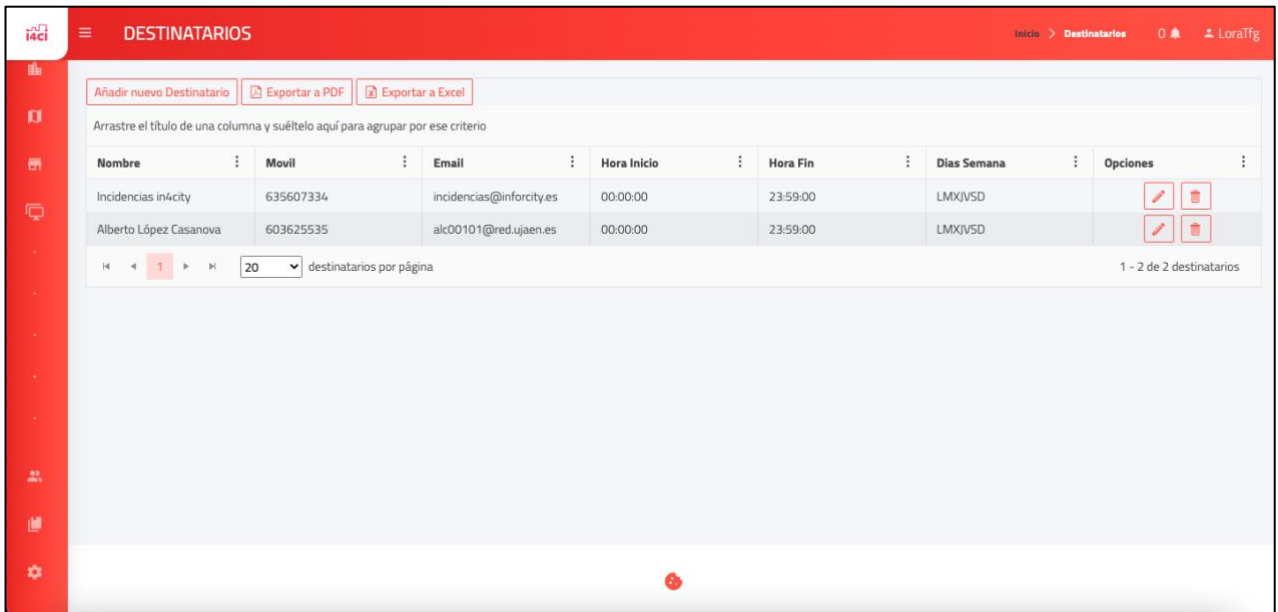


Figura 66. Pantalla inicial de In4city.

2. Previamente a introducir el Gateway y el sensor, se añaden dos destinatarios para notificaciones. El primero corresponde a soporte e incidencias y sirve para la monitorización del sistema y solución de posibles errores por parte de la empresa. El segundo corresponde al usuario de la plataforma y está destinado a la recepción de notificaciones respectivas a control de valores. Para ello se accede desde el menú lateral a 'Monitorización' -> 'Destinatarios' -> 'Añadir nuevo destinatario'. Tras la creación de los destinatarios el resultado se observa en la Figura 67.







Nombre	Movil	Email	Hora Inicio	Hora Fin	Dias Semana	Opciones
Incidencias in4city	635607334	incidencias@inforcity.es	00:00:00	23:59:00	LMXIVSD	 
Alberto López Casanova	603625535	alc00101@red.ujaen.es	00:00:00	23:59:00	LMXIVSD	 

Figura 67. Creación de destinatarios en In4city.

3. El siguiente paso es la creación las notificaciones. Este paso es necesario hacerlo previamente a la introducción del Gateway en la plataforma ya que es un campo obligatorio en el proceso. Se accede desde el menú de navegación

lateral a 'Monotorización' -> 'Notificaciones' -> 'Añadir nueva notificación'. Las notificaciones creadas se muestran en la Figura 68.

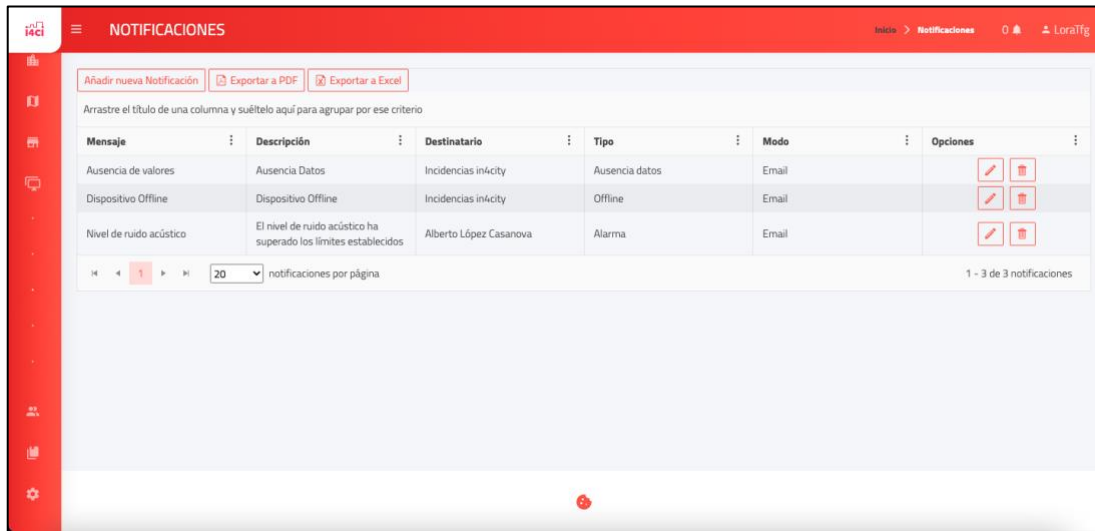


Figura 68. Creación notificaciones en In4city.

4. Creadas las notificaciones, se procede a introducir el Gateway en la plataforma. Se accede desde el menú de navegación lateral a 'Inventario IoT' -> 'Dispositivos' -> 'Añadir nuevo dispositivo'. Dentro de esta sección se rellenan los diferentes campos tales como: credenciales del Gateway, dirección IP (OVPN) y puerto, etc. Tras finalizar, el resultado es mostrado en la Figura 69.

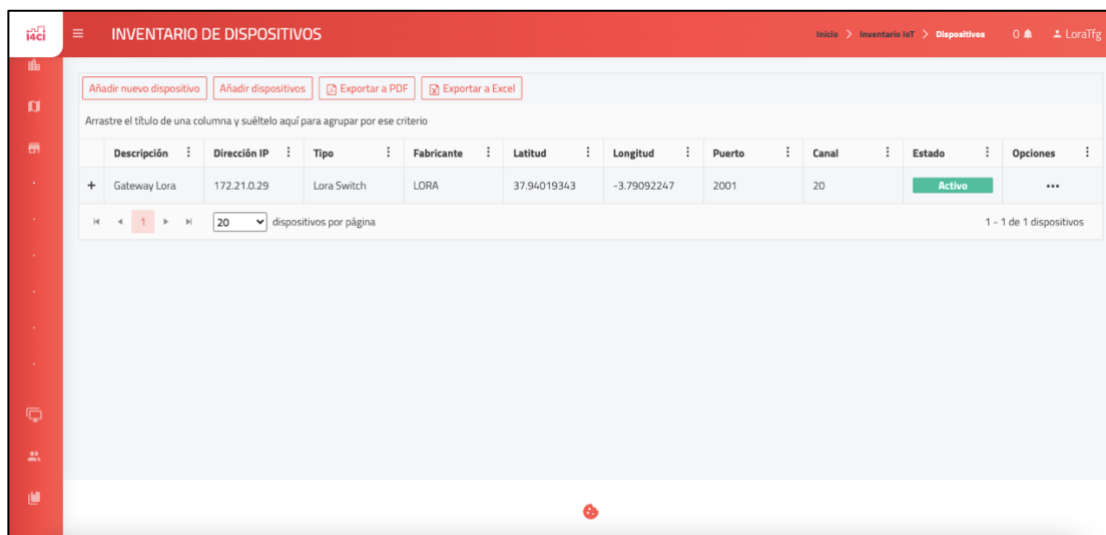


Figura 69. Introducción del Gateway en In4city.

5. Una vez se ha añadido el Gateway, queda por introducir el sensor de ruido Elsys ERS Sound y asociarlo al Gateway. Se accede desde el menú lateral a

'Inventario IoT' -> 'Sensores' -> 'Añadir nuevo sensor'. Tras ello se rellenan los campos correspondientes y queda el sensor añadido.

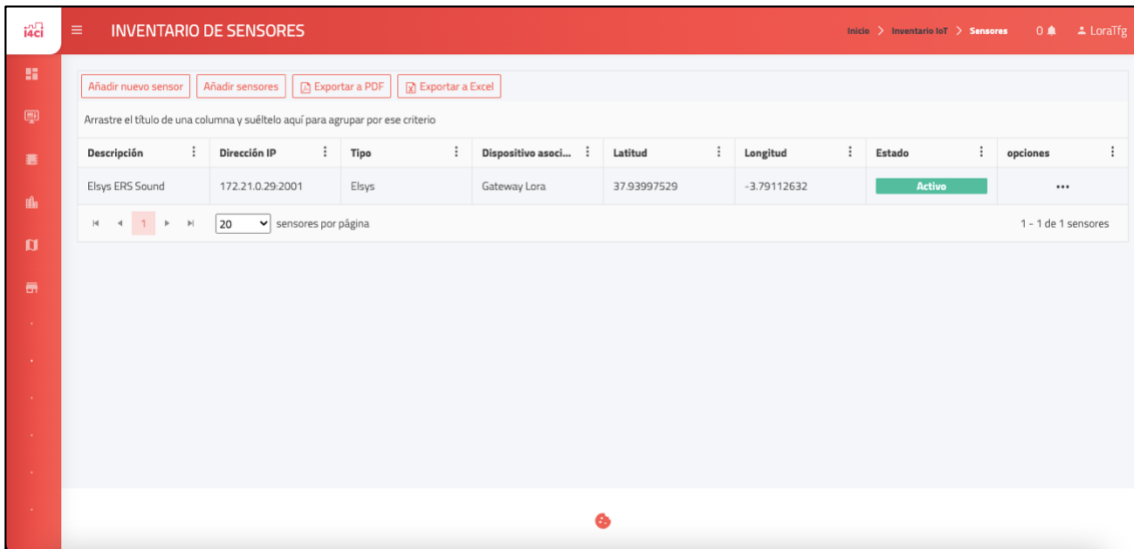


Figura 70. Introducción sensor Elsys en In4city.

- Tras añadir el Gateway y sensor en la plataforma, hay que esperar unos minutos para que estos se conecten. Una vez estén activos en In4city, desde la pantalla inicial se puede observar en el mapa la situación de ambos dispositivos. Además, en la sección 'En línea' se observa que hay un dispositivo conectado, el cual es el Gateway. Los sensores no se muestran en esta sección ya que In4city los toma como parte del Gateway.

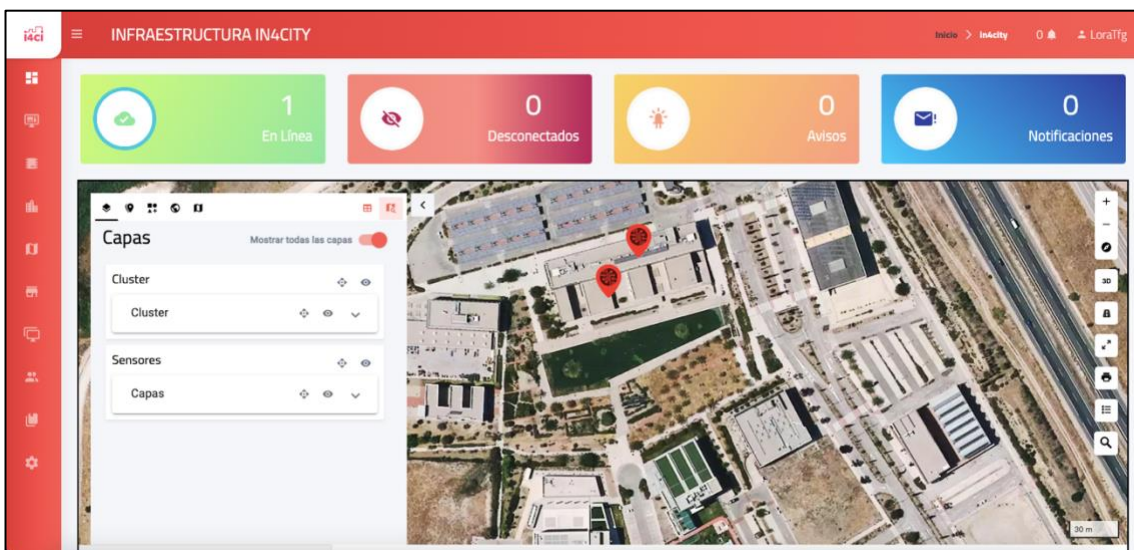


Figura 71. Información de dispositivos en línea en In4city

La plataforma cuenta con un sistema de notificaciones, para este TFG se ha establecido una alerta de control de niveles permitidos. Esta avisa cuando el nivel de ruido es menor que 40 DbSPL o mayor que 60 DbSPL.

7. Resultados

El presente capítulo sirve para presentar los resultados obtenidos tras la instalación del sistema en un entorno urbano real de cara a la comprobación y verificación del funcionamiento del mismo. En primer lugar se muestra la instalación de los dispositivos físicos que forman parte del sistema: dispositivo sensor y Gateway. Tras ello, se muestran y analizan las gráficas obtenidas en ambas plataformas IoT configuradas para ello: Grafana e In4city. Para finalizar se comprueba la recepción de las notificaciones generadas en el back-end de ambas plataformas.

7.1 Instalación del dispositivo sensor y Gateway

Una vez descrita la configuración de los elementos que conforman el sistema desarrollado en el presente TFG, este se ha instalado en un entorno urbano real de cara a analizar su correcto funcionamiento. Para ello, se ha instalado el sensor en la cafetería de Geolit y el Gateway en la sala Demo de la empresa. Cabe destacar que la instalación se ha llevado a cabo con la colaboración de los instaladores de la empresa.

La instalación se debe llevar a cabo en un lugar donde no se encuentren ventanas o puertas muy cerca ya que esto podría afectar a su correcto funcionamiento. Para su alimentación, se hace uso de dos pilas de litio 3,6 Voltios (V); aunque sólo necesita una para funcionar, el fabricante recomienda usar las dos para un mejor rendimiento y duración de la batería. Para llevar a cabo la instalación se debe atornillar la tapa trasera del sensor a la superficie escogida con al menos dos tornillos haciendo uso de alguno de los seis orificios disponibles, tal y como se muestra en la figura 72. Una vez instalada la tapa trasera basta con colocar la otra parte del sensor en la tapa trasera instalada.

En el caso de este TFG, el sensor se ha instalado en una pared de la cafetería cerca de la barra y sin puertas o ventanas muy cerca. En la figura 73 se muestra la instalación de la tapa trasera en la pared. Finalmente se muestra en la figura 74 la instalación del sensor completada.

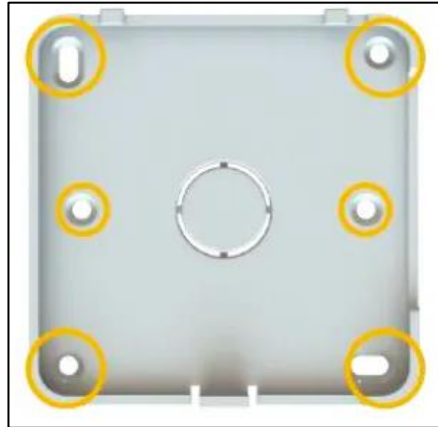


Figura 72. Orificios de la tapa trasera del sensor Elsys. Fuente: Elsys.



Figura 73. Instalación tapa trasera del sensor

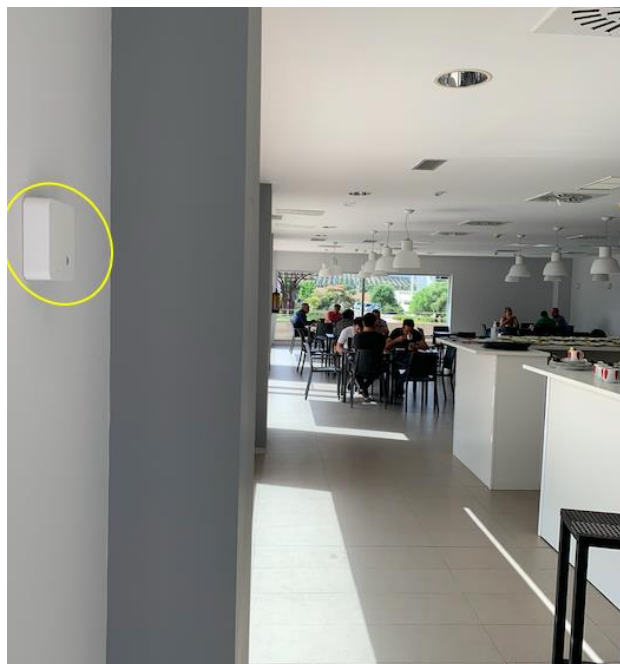


Figura 74. Sensor Elsys instalado en la cafetería de Geolit.

El Gateway cuenta con un soporte de montaje y una abrazadera mediante los cuales se realiza la instalación en pared o poste. En primer lugar se deben instalar las antenas del dispositivo ya que son la parte más importante de cara al funcionamiento del mismo. La alimentación del dispositivo se lleva a cabo mediante la tecnología Power over Ethernet (PoE), la cual permite darle alimentación y conectividad mediante un único cable de red. Cabe destacar que para hacer uso del PoE, es necesario que el elemento de red al que el Gateway vaya conectado ya sea un switch o router, cuente con salida PoE. En caso de no contar con ello, se debe hacer uso de un inyector PoE. El manual de instalación de este dispositivo se encuentra disponible en el Anexo V.

Para el presente TFG, se hace uso de la sala Demo de la empresa colaboradora Innovasur para llevar a cabo el montaje del Gateway. Este ha sido instalado en un montaje de poste. En cuanto a la alimentación, el Gateway es conectado mediante cable de red Unshielded twisted pair (UTP) directamente a un router mikrotik HeX PoE situado en la sala Demo. Dado que este router cuenta con salidas PoE, no se hace necesario un inyector PoE. El Gateway finalmente instalado se muestra en la figura 75.



Figura 75. Gateway instalado en la sala Demo

7.2 Gráficas de niveles de ruido y notificaciones en ambas plataformas IoT

En el capítulo 6 se ha realizado la configuración de ambas plataformas donde son representados los datos al usuario: Grafana e In4city. En la primera se han creado dos paneles dentro de un dashboard mientras que en la segunda, la representación es realizada automáticamente por la plataforma una vez esta está correctamente configurada.

En la figura 76 se muestran los dos paneles creados en Grafana. El panel superior representa el nivel medio de ruido acústico presente en la cafetería (SoundAvg), mientras que el inferior representa el nivel de pico de ruido (SoundPeak). Cabe destacar que la plataforma Grafana cuenta con un filtro temporal que permite consultar los niveles de ruido en diferentes franjas horarias y en diferentes días. En el caso de la figura 76, se muestran los niveles de ruido recogidos durante una semana. A partir de estas gráficas, se puede hacer una estimación del horario de apertura y cierre del local, conocer las horas con más afluencia de gente, etc.



Figura 76. Gráficas niveles de ruido acústico presentes en la cafetería de Geolit. Grafana.

Las líneas rojas que se observan en la figura anterior muestran los niveles límite establecidos los cuales una vez son superados, activan las alarmas creadas. Al

activarse las alarmas se reciben las notificaciones vía Telegram tal y como se observa en la figura 77. Cuando el nivel de ruido supera el establecido, se envía una notificación de alerta, junto una imagen de la gráfica en el instante en que el que la alerta ha sido activada. Una vez el nivel de ruido vuelve a ser inferior al límite, se envía una notificación de OK para avisar al usuario de que los niveles están por debajo del límite.



Figura 77. Recepción de notificaciones vía Telegram. Grafana.

En cuanto a la plataforma propietaria In4city, en la figura 78 se muestra la gráfica que representa el nivel ruido acústico presente en la cafetería. Cabe destacar que esta gráfica viene preestablecida en el propio desarrollo de la plataforma. Dado que es una plataforma propietaria y es desarrollada por el departamento de desarrollo de la misma, no es posible modificarla. El nivel de ruido acústico representado en la gráfica de la figura 78 es el resultado de hacer la media de los niveles de ruido recogidos durante una hora (SoundAvg y SoundPeak de forma conjunta). Para consultar esta gráfica dentro de la plataforma se accede desde el menú de navegación lateral a la sección 'Sensórica LoRa' -> 'Cuadros de mandos' -> 'Elsys ERS Sound'.

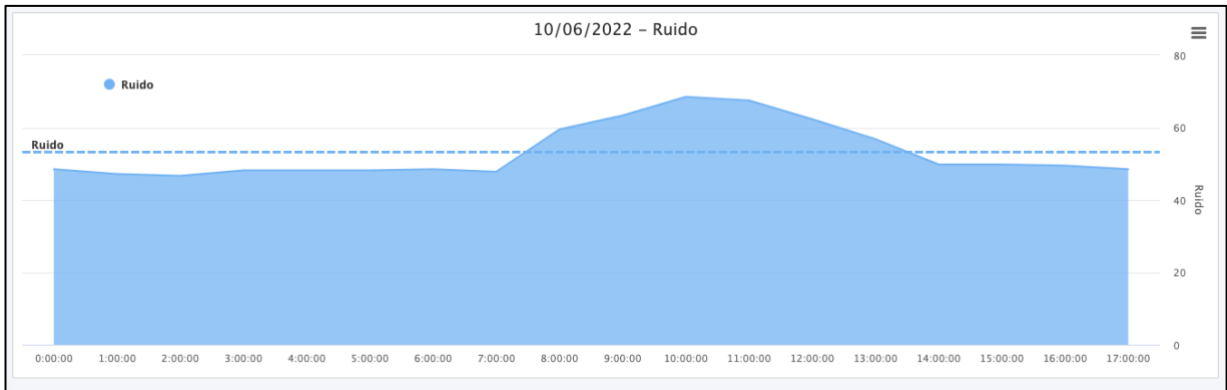


Figura 78. Gráfica del nivel de ruido acústico presente en la cafetería de Geolit. In4city.

En la figura 79 se muestra la recepción de notificaciones vía email una vez la alerta creada se activa. La alarma es activada cuando el nivel de ruido acústico representado es menor que 40 DbSPL o mayor que 60 DbSPL.

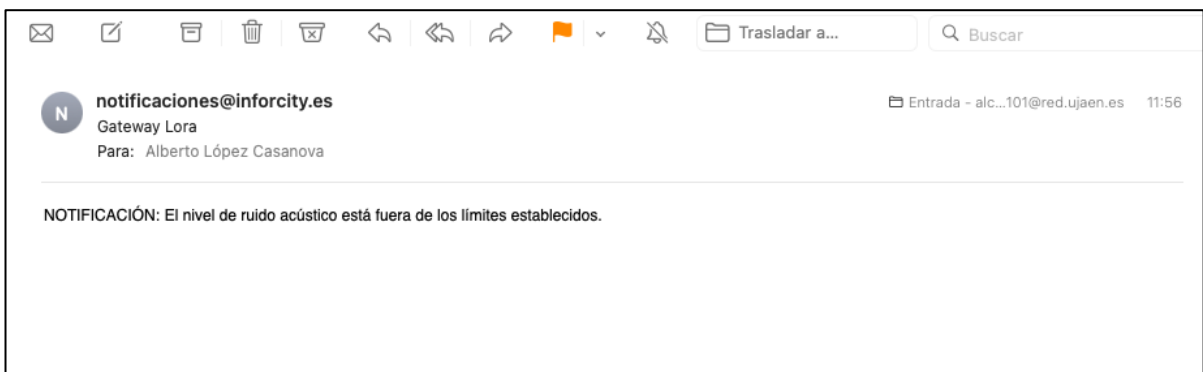


Figura 79. Recepción de notificaciones en In4city.

8. Conclusiones y líneas de futuro

Se proponía al comienzo de este TFG como objetivo principal el diseño e implementación de un sistema de monitorización de ruido acústico a través de una red LoRaWAN. Surge de la motivación de desarrollar un sistema que permita monitorizar los niveles de ruido acústicos presentes en un entorno urbano real de forma constante y remota a través de Internet. Durante el desarrollo del presente TFG se han ido cumpliendo los diferentes objetivos que han permitido llevar a cabo de forma exitosa el objetivo principal.

En primer lugar se han estudiado las bases de una red LoRaWAN relativas a su arquitectura de red y funcionamiento. Con ello se ha conseguido obtener los conocimientos teóricos necesarios para el posterior diseño e implementación de una red LoRaWAN privada. De cara al desarrollo del sistema presentado en este TFG, se ha diseñado la arquitectura de red con el fin de reflejar gráficamente las interconexiones entre los distintos elementos hardware y software que la componen. Tras ello, se han configurado los elementos hardware: dispositivo sensor y Gateway para así pasar a la configuración y programación de los elementos software. Dentro de estos, se ha configurado el Network Server el cual se encuentra dentro del mismo Gateway. Para la conexión con el back-end de las plataformas IoT utilizadas se han programado los flujos de Node-Red necesarios para ello. En primer lugar se han programado dos flujos en el Node-Red instalado en el Gateway: el primero permite la conexión con el CPD donde se encuentra la primera plataforma IoT Grafana, mientras que el segundo sirve para la conexión con una API que hace las veces de back-end de la plataforma propietaria de la empresa colaboradora Innovasur llamada In4city. En segundo lugar se ha programado un flujo de la aplicación Node-Red instalada en una Máquina virtual alojada en el CPD, el cual hace las veces de back-end de la plataforma IoT open-source Grafana. Para finalizar, se han configurado ambas plataformas así como otros servicios necesarios cuando procede tales como una BD MySQL. Además ambas plataformas han sido dotadas con un sistema de notificaciones. Una vez finalizada la configuración del sistema completo, se ha llevado a cabo la instalación del sistema en un entorno urbano real con la colaboración de los técnicos instaladores de la empresa. Para ello se ha escogido la cafetería del Parque Tecnológico y Científico de Geolit como el lugar para instalar el dispositivo sensor, mientras que el Gateway ha sido instalado en la Sala

Demo de la empresa colaboradora. De esta forma se ha alcanzado con éxito el objetivo principal del presente TFG.

La instalación del sistema en un entorno urbano real ha permitido verificar el correcto funcionamiento del sistema al obtener la representación de los niveles de ruido acústico presentes en la cafetería, así como verificar la recepción de notificaciones. En la plataforma open-source Grafana se han obtenido dos gráficas relativas al ruido: una muestra el nivel medio de ruido y otra el nivel de pico. En cambio, en la plataforma propietaria In4city se obtiene una única gráfica donde se muestra la media de los niveles de ruido medio y de pico recogidos por el sensor durante una hora.

8.1 Comparativa de las dos plataformas IoT utilizadas

En el presente TFG se ha hecho uso de dos plataformas IoT para la representación de los datos con el objetivo de compararlas. Durante el desarrollo del presente TFG se han podido observar las ventajas e inconvenientes de cada una de ellas.

En primer lugar, cabe destacar que Grafana es un software open-source que sirve para la representación y visualización de datos métricos. Por tanto su propósito no es servir como plataforma IoT específicamente ya que puede ser utilizada para la representación de datos provenientes de tecnologías no enmarcadas en el ámbito del IoT. Sin embargo, su sencilla instalación y configuración, su amplio catálogo de herramientas para la creación de gráficas y su sistema de notificaciones hacen que sea una herramienta ideal para los proyectos IoT. Además, al ser un software de código libre cuenta con soporte y actualizaciones constantes por parte de la comunidad de desarrolladores. Esto hace que sea un software consolidado y cada vez más usado en el ámbito del IoT. Para soluciones IoT donde se desarrolla una red privada como es el caso del presente TFG es una solución idónea como plataforma IoT para representar los datos generados por el sensor. Al permitir realizar consultas personalizadas a la BD, el usuario es capaz de conseguir representar los datos ajustándose a sus necesidades y gustos.

La plataforma propietaria In4city cuenta con desventajas frente a Grafana en cuanto a redes de sensores IoT se refiere. Esta plataforma no ha sido diseñada

únicamente para la representación de datos generados por sensores LoRa. Cuenta con diferentes verticales, siendo 'Sensórica LoRa' una de ellas, que puede ser o no utilizada. Al ser una plataforma propietaria desarrollada y mantenida por el departamento de desarrollo de la empresa, las gráficas no son configurables al antojo del usuario. Esto se hace notable en la gráfica de ruido obtenida, la cual no muestra los dos parámetros de ruido generados por el sensor de forma separada. En su lugar hace la media de ambos durante una hora, lo cual hace que los niveles representados no sean útiles a la hora de conocer el ruido ambiental presente en un entorno real.

Para finalizar cabe destacar que Grafana obtiene los datos de una BD, sin importar cual sea la fuente de estos. Por tanto no se limita su uso únicamente a redes LoRaWAN, pudiendo ser utilizada en redes basadas en otra tecnología diferente. Sin embargo, In4city se limita a redes LoRaWAN. Mientras que Grafana es una buena solución para utilizar en proyectos IoT, In4city es una solución pensada para aunar en un mismo lugar las diferentes verticales de la empresa. Por tanto, para el presente TFG basado en una red LoRaWAN privada para la monitorización de ruido acústico, la plataforma que mejores prestaciones ofrece es Grafana.

8.2 Líneas de futuro

La mejora principal, es el uso de otro tipo de sensor de ruido más preciso y homologado. El sensor utilizado en el presente TFG sirve para monitorización, pero por su tamaño y alimentación, los niveles de ruido obtenidos no pueden ser utilizados de cara a cumplir la legislación de ruido vigente.

Otra mejora a corto o medio plazo es la instalación de otro tipo de sensores de cara a monitorizar otro tipo de parámetros ambientales tales como: niveles de dióxido de carbono (Co2), localización de elementos tales como coches, luminosidad, etc. Esto es posible gracias a la escalabilidad de las redes LoRaWAN.

Finalmente, el sistema desarrollado en el presente TFG puede ser instalado en otro tipo de entornos reales. Entre ellos se puede destacar: oficinas de trabajadores, tiendas de ropa o locales de ocio.

9. Estudio económico

El presupuesto del presente TFG contempla todo el material y recursos humanos utilizados durante el desarrollo del mismo.

IT Referencia	Producto	Precio unitario	Unidades	Total
COMUNICACIONES				
48 POW	Mikrotik 48 POW 1,46 A 70W Power Adapter	12,59 €	1	12,59 €
RB960PGS	Mikrotik HeX PoE 5P PoE 1SFP Gigabit Ethernet	85,45 €	1	85,46 €
RED SENSORICA LORA				
MULTITECH67	LoRa Gateway Multitech IP 67	1.148,00 €	1	1.148,00 €
ERSSOUND	Sensor de Temperatura, Humedad, Presión Atmosférica, Luminancia, Movimiento y Ruido (AVG,PEAK) de interior, LoRa	151,00 €	1	151,00 €
CABLEADO				
UTP6	Cable UTP Cat.6 2m.	2,79 €	1	2,79 €
MANO DE OBRA				
Mano de Obra. Ingeniería.	Diseño e implementación del sistema. Graduado en Ing. Telemática	30 €	300 h	900 €
Mano de Obra. Instalación.	Instalación física. Técnico.	15 €	2 h	30 €
TOTAL				2.329,84 €
I.V.A 21%				489,26 €
TOTAL I.V.A INCLUIDO				2.819,10 €

El presupuesto del presente TFG hace un total de DOS MIL OCHO CIENTOS DIECINUEVE EUROS CON DIEZ CENTIMOS .

10. Bibliografía

- [1] «Contaminación acústica». <https://www.miteco.gob.es/es/calidad-y-evaluacion-ambiental/temas/atmosfera-y-calidad-del-aire/contaminacion-acustica/>. Accedido: 11/05/2022.
- [2] «L00012-00025.pdf». Disponible en: <https://www.boe.es/doue/2002/189/L00012-00025.pdf>. Accedido: 11/05/2022.
- [3] «A40494-40505.pdf». Disponible en: <https://www.boe.es/boe/dias/2003/11/18/pdfs/A40494-40505.pdf>. Accedido: 15/05/2022.
- [4] A. C. Pinto, E. D. la H. Franco, y D. C. Pinto, «Las redes de sensores inalámbricos y el internet de las cosas», *INGE CUC*, vol. 8, n.º 1, Art. n.º 1, oct. 2012.
- [5] «El WiFi cumple 22 años», *Telefónica*, 10 de noviembre de 2021. <https://www.telefonica.com/es/sala-comunicacion/el-wifi-cumple-22-anos-y-albergados-tercios-del-trafico-de-internet-en-espana/>. Accedido: 16/05/2022.
- [6] «La historia del Internet de las Cosas (IoT)», *Bruno Cendón*, 16 de enero de 2017. <https://www.bcendon.com/el-origen-del-iot/>. Accedido: 04/04/2022.
- [7] A. de, «Cómo la próxima evolución de Internet lo cambia todo», p. 12, 2011.
- [8] A. Camarillo, «¿Qué es LoRa y LoRaWAN?», *330ohms*, 29 de junio de 2020. <https://blog.330ohms.com/2020/06/29/que-es-lora-y-lorawan/>. Accedido: 19/04/2022.
- [9] «Hedy Lamarr», *Wikipedia, la enciclopedia libre*. 30 de marzo de 2022. Disponible en: https://es.wikipedia.org/w/index.php?title=Hedy_Lamarr&oldid=142595649. Accedido: 12/04/2022.
- [10] «Conceptos de actualidad: LoRa y LoRaWan - 2cigroup». <https://www.2cigroup.com/es/conceptos-de-actualidad-lora-y-lorawan/> Accedido: 18/04/2022.
- [11] «tr_103526v010101p.pdf». Disponible en: https://www.etsi.org/deliver/etsi_tr/103500_103599/103526/01.01.01_60/tr_103526v010101p.pdf. Accedido: 23/05/2022.
- [12] «¿Qué es una puerta de enlace (Gateway)?» <https://www.puertadeenlace.com/faq/general/46-que-es-una-puerta-de-enlace-gateway>. Accedido: 20/04/2022.
- [13] «Application Settings – en». <https://www.elsys.se/en/application-settings/>. Accedido: 03/06/2022.
- [14] «MultiConnect® Conduit™ Base Station IP67», p. 30.

- [15] «Elsys Payload – en». <https://www.elsys.se/en/elsys-payload/>. Accedido: 02/06/2022.
- [16] «Instalacion de Plataforma Node-Red», *PDAControl*, 17 de octubre de 2016. <http://pdacontroles.com/instalacion-de-plataforma-node-red/>. Accedido: 05/06/2022.
- [17] «Cómo instalar la herramienta de monitorización Grafana en Ubuntu 18.04 LTS», *HowtoForge*. <https://howtoforge.es/como-instalar-la-herramienta-de-monitorizacion-grafana-en-ubuntu-18-04-lts/>. Accedido: 07/06/2022.
- [18] C. M, «Configurar alarmas Telegram en Grafana», 16 de mayo de 2021. <https://elblogdelazaro.org/posts/2021-09-20-configurar-alarmas-telegram-en-grafana/>. Accedido: 07/06/2022.
- [19] «in4city | Web oficial de In4City». <https://inforcity.es/>. Accedido: 08/06/2022.
- [20] «Investigadores de la Universidad de Jaén diseñan e implementan un sistema completo, de bajo coste, para la monitorización del ruido acústico en tiempo real en un entorno urbano | Diario Digital de la UJA | Compromiso con la sociedad». <https://diariodigital.ujaen.es/investigacion-y-transferencia/investigadores-de-la-universidad-de-jaen-disenan-e-implementan-un>. Accedido: 21/04/2022.
- [21] «Fernandez-Prieto, J.-A.; Cañada-Bago, J.; Gadeo-Martos, M.-A. Wireless Acoustic Sensor Nodes for Noise Monitoring in the City of Linares (Jaén). *Sensors* 2020, 20, 124. <https://doi.org/10.3390/s20010124>».

11. ANEXOS

ANEXO I: Hoja de características del sensor Elsys ERS Sound.

Datasheet
Publish Date: 21.08.2019



ERS Sound

LoRaWAN Wireless Sensor

Description

ERS Sound is an advanced indoor environment sensor. It is enclosed in a room sensor box and is designed to be wall mounted. ERS Sound is completely wireless and powered by two 3.6V AA lithium batteries. Inside you will find internal sensors for measuring sound level, temperature, humidity, light, and motion. The sound module is always on and will detect every sound event.



Applications

- Indoor environment measuring
- Smart buildings
- Workplace management
- Room occupancy
- Sound level control in public spaces, schools, libraries etc.

Product features

- LoRaWAN Certified ^{CM}
- Sound sensor / Peak + Average
- Always on – no missed sound events
- dBA filtering
- Temperature sensor
- Humidity sensor
- Light sensor
- Motion detection sensor (PIR)
- NFC for configuration
- Configuration over the air
- Discrete and minimalistic design

Device Specifications

Mechanical specifications	
Weight	60 g excluding batteries / 100 g including batteries
Dimensions	86 x 86 x 27 mm
Enclosure	Plastic, PC/ABS

Operating conditions	
Temperature	0 to 50 °C
Humidity	0 to 85 % RH (non-condensing)

Device Logging Function	
Sampling Interval	Configurable via NFC and downlink configuration
Data Upload Interval	Configurable via NFC and downlink configuration

Device Power Supply	
Battery Type	2 x 3.6V AA Lithium Batteries
Expected Battery Life	< 2 years (Depending on configurations and environment)

Elektroniksystem i Umeå AB Industrivägen 12, 901 30 Umeå, Sweden
E-mail: support@elsys.se | Web: www.elsys.se

Specifications in this document are subject to change without notice.
©Elektroniksystem i Umeå AB 2019

Radio / Wireless	
Wireless Technology	LoRaWAN® 1.0.3 rev B
Wireless Security	LoRaWAN® End-to-End encryption (AES-CTR), Data Integrity Protection (AES-CMAC)
LoRaWAN Device Type	Class A/B/C (configurable) End-device
Supported LoRaWAN® features	OTAA, ABP, ADR, Adaptive Channel Setup
Supported LoRaWAN® regions	US902 – 928, EU863 – 870, AS923, AU915 – 928, KR920 – 923, RU864, IN865
Link Budget	137 dB (SF7) to 151 dB (SF12)
RF Transmit Power	14 dB / 20 dB (Region specific)

Data types			
Type value	Type	Data size	Comment
0x01	Temperature	2	-3276.5 °C → 3276.5 °C (Value of: 100 → 10.0 °C)
0x02	Humidity	1	0 – 100 %
0x04	Light	2	0 – 65535 Lux
0x05	Motion (PIR)	1	0 – 255 (Number of motion counts)
0x07	VDD (Battery voltage)	2	0 – 65535 mV
0x15	Sound	2	Sound data, 1 byte peak / 1 byte average dB
0x3D	Debug information	4	Data depends on debug information
0x3E	Sensor settings	n	Sensor setting sent to server at startup (first package). Sent on Port+1.

Sensors

Temperature

Resolution: 0.1 °C

Accuracy: ±0.2 °C (See figure 1)

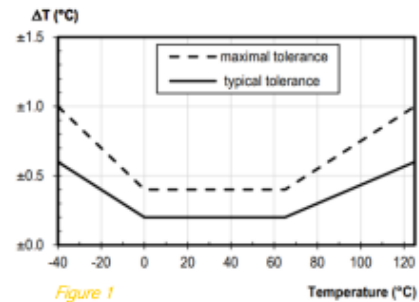


Figure 1

Humidity

Resolution: 0.1 % RH

Accuracy at 25 °C: ± 2 % RH (See figure 2)

Accuracy of humidity over temperature: See figure 3

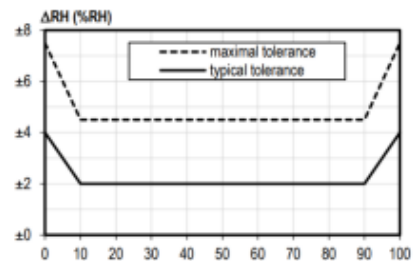


Figure 2

Light

Range: 4 – 2000 LUX

Resolution: 1 LUX

Accuracy: ± 10 LUX

Motion (PIR)

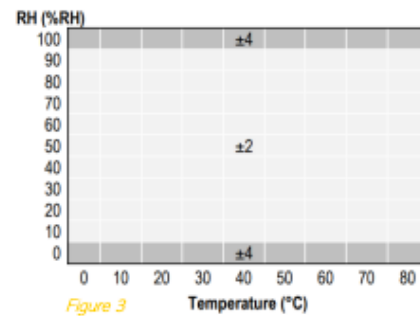
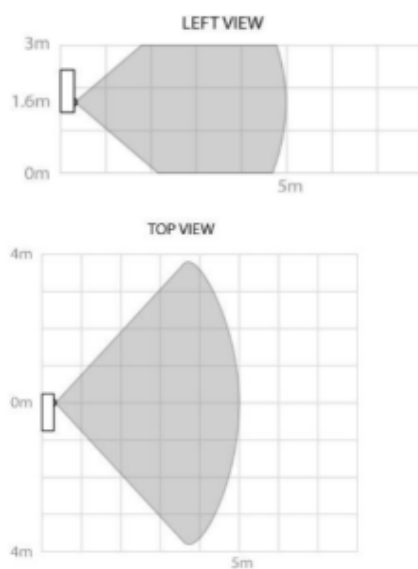


Figure 3

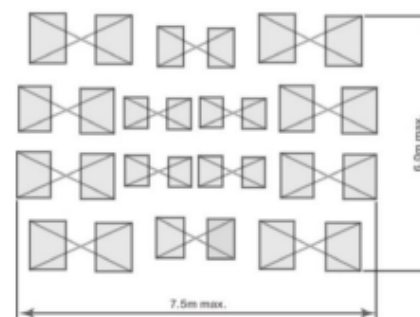


Figure 4 - Detection pattern

Note:

There is a blanking time of 30 seconds of the PIR triggering after each PIR trig and after each transmission. This is to reduce the risk of self-triggering from internal events that could disturb the high sensitivity PIR circuits.

Sound

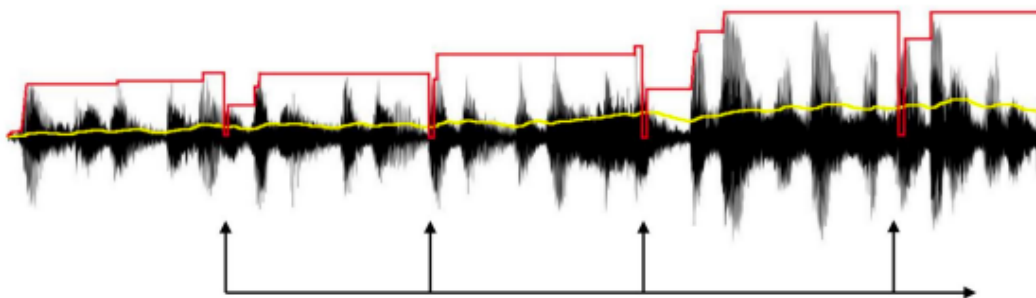
The sound sensor measures the average and peak sound pressure level with dBa filtering. It wakes and samples both signals every 10s, and does the final calculation before sending the data at the desired send interval. For large orders, sensitivity and filtering can be changed.

Average value range: 35 – 70 dBspl

Peak value range: 65 – 99 dBspl

Sound resolution: 1 dB

Sound accuracy: ± 5 dB



*10s sample and peak reset. For every send interval,
the ERSound calculates total peak and average for all samples.*

ANEXO II: Hoja de características del Gateway Multitech Conduit IP67.



MULTITECH[®]
CREATE • CONNECT • COMMUNICATE

MultiTech Conduit[®] IP67 Base Station

IP67 Conduit for Outdoor LoRa[®] Deployments
EU868 for Europe

LoRa Alliance[®]

MultiTech Conduit[®] IP67 Base Station is a ruggedized IoT gateway solution, specifically designed for outdoor LoRa[®] public or private network deployments. This highly scalable and certified IP67 solution is capable of resisting the harshest environmental factors including moisture, dust, wind, rain, snow and extreme heat, supporting LoRaWAN[®] applications in virtually any environment. The enhanced Conduit IP67 solution can support thousands of LoRaWAN certified end nodes, including the MultiTech mDot[™]* and xDot[™]. This flexible solution provides durable, low-power, wide area connectivity in support of M2M and IoT applications for both LoRa service providers and individual enterprises wanting to expand their LoRa network coverage.

Designed for easy deployment, the solution includes a MultiTech Conduit with a LoRa MultiTech mCard[™], IP67 enclosure, LoRa antenna to improve outdoor range and Ethernet or optional 4G-LTE backhaul. It can be deployed as part of an existing telecommunications tower, individual stand or wall mount.

*Represents ideal network configuration and equipment set up. Results vary depending on payload amount, transmission frequency, spreading factor used, as well as terrain, RF interference and obstruction type (e.g., metal, cement, etc.)

BENEFITS

- Greatly expands LoRa network coverage
- External antenna increases LoRa connectivity to remote assets
- Improved design enhancing thermal performance and easy external port access to SIM and USB connectors

FEATURES

- 14 dBm support for European region
- Certified for Europe 868 MHz ISM bands
- ISM band scanning for optimum LoRa performance
- Listen Before Talk operating protocol
- GNSS for location coordinate information

www.multitech.com/IP67

mPower™

EDGE INTELLIGENCE

Programmable embedded software provides enhanced security and enables task execution at the edge for reduced latency and cost optimization.

mPower™ Edge Intelligence embedded software delivers programmability, network flexibility, enhanced security and manageability for scalable Industrial Internet of Things (IIoT) solutions.

mPower simplifies integration with a variety of popular upstream IoT platforms to streamline edge-to-cloud data management and analytics, while also providing the programmability and processing capability to execute critical tasks at the edge of the network to reduce latency; control network and cloud services costs, and ensure core functionality – even in instances when network connectivity may not be available.

mPower software specifications can be found [here](#).

LENS™ Embedded Network Server & Key Management Toolset for LoRaWAN™ Networks

LENS is a hybrid LoRaWAN™ network management platform that enables deployment and management of LoRaWAN networks at scale. Designed for private and enterprise networks, LENS provides a site-by-site user account and centralized management for LoRa™ end devices, as well as configuration and control of Conduit™ gateways. LENS has the capability to assign unique access rights to individual users, add gateways and LoRa end nodes in bulk, or create separate organizations and network segmentation to support different IoT use cases or applications.



Cloud-based Application Store and IoT Device Management

MultiTech DeviceHQ™ is cloud-based tool set for managing the latest generation of MultiTech devices. It incorporates all the functionality of MultiTech Device Manager, on which so many M2M and IoT applications already rely for remote monitoring, upgrades and configuration of entire device populations – whether one or 1 million. DeviceHQ takes remote device management and maintenance to a new level, by providing an application marketplace, allowing users to browse applications or build their own then easily deploy them to and customize them for remote devices from anywhere.

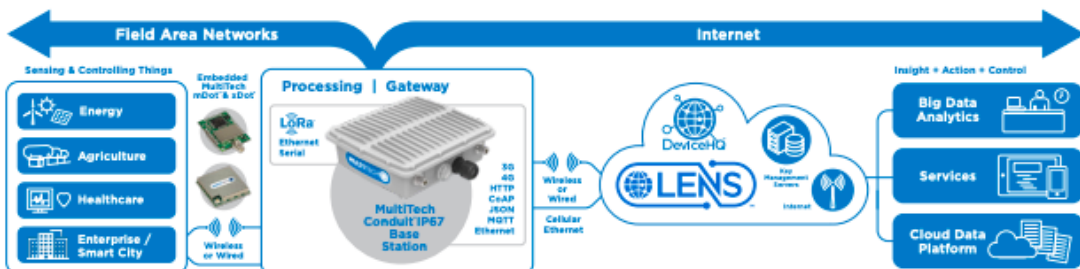


SPECIFICATIONS

Models	MTCDTIP-L4E1	MTCDTIP-868
Mobile Network Operator	European Network Operators	non-Cellular
Cellular Performance	4G - LTE Category 4	
Cellular Fallback	3G - HSPA+, 2G - GPRS	
Frequency Band (MHz)	4G: B1(2100), B3(1800), B7(2600), B8(900), B20(800), B28A(700) 3G: B1(2100), B3(1800), B8(900) 2G: B3(1800), B8(900)	
Packet Data (LTE FDD)	Up to 150 Mbps peak downlink Up to 50 Mbps peak uplink	
Input Voltage	Ethernet Input Power: 37 - 57 VDC. POE Standard: IEEE 802.3at, provided by PSE injector with power rating of 25W or greater	
Processor & Memory	ARM9 processor with 32-Bit ARM & 16-Bit Thumb instruction sets • 400 MHz • 16K Data Cache • 16K Instruction Cache • 128X16 MB DDR RAM • 256 MB Flash Memory	
Wi-Fi/Bluetooth (-267 models)	Wi-Fi: 802.11abgn (2.4 & 5 GHz) / Bluetooth: Classic 4.1 and BLE	
GPS/GNSS	GNSS for LoRa Packet Time Stamping Concurrent GNSS connections: 3 GNSS Systems Supported: (default: concurrent GPS/QZSS/SBAS and GLONASS)	
LEDs*	PR (Power), ST (Status), L1, L2	
LoRa Specifications		
LoRa Frequency Band	868 MHz	
LoRa Channel Plan	EU868 (EU863 - 870)	
Channel Capacity	8-channels (half-duplex)	
LoRa Maximum Output Power	Maximum EIRP: 14 dBm - 27 dBm**	
Connectors		
E-NET	RJ45 Ethernet jack (10/100 port) (PoE)	
USB HOST*	USB 2.0 Type A connector	
SIM*	3FF Micro SIM	None
Antennas	Cellular, LoRa, GPS: N-Type Female	
Physical Description		
Dimensions (LxWxH)	262 mm x 91 mm x 257 mm	
Weight	2.75 kg	
Chassis Type	IP67 Rated, Aluminum	
Environmental		
Operating Temperature	-40° to +70° C	
Storage Temperature	-40° to +85° C	
Certifications		
EMC Compliance	EN 55023 Class A EN 301 489-3 V2.1.1 EN 301 489-1 V2.2.0 EN 301-489-52 V1.1.0	
Radio Compliance	EN 300 220-1 V3.1.1 EN 300 220-2 V3.1.1 EN 300 328 V2.2.2 EN 301 511 V9.0.2 EN 301 893 V2.1.1 EN 301 908-1 V11.1.1 EN 301 902-2 V11.1.1 EN 301 908-13 V11.1.1 EN 62311-2008	
Safety	IEC 60950-1 IEC 62368-1	
Quality	MIL-STD-810G: High Temp, Low Temp, Random Vibration, SAE J1455; Transit Drop & Handling Drop, Random Vibration, Swept-Sine Vibration. IEC68-2-1: Cold Temp. IEC68-2-2: Dry Heat	
Warranty	2-Years - www.multitech.com/legal/warranty	

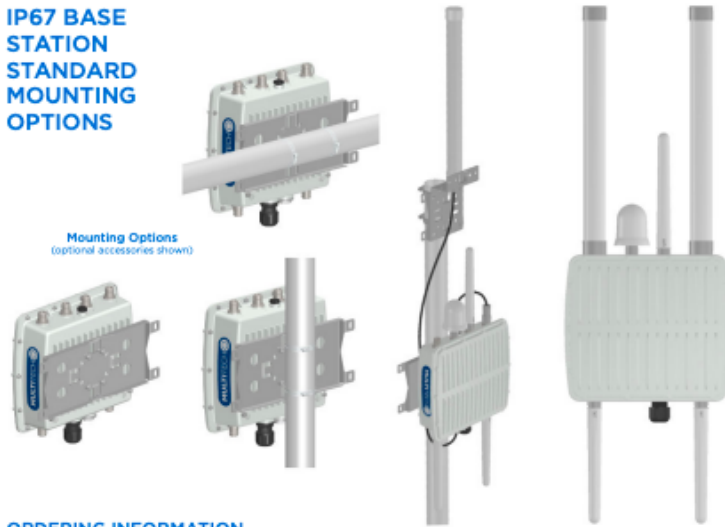
* SIM, LEDs, and USB port accessible under IP67-rated bottom cap cover

** Maximum EIRP is 14 dBm for most of the band, except 27 dBm at 869.4 - 869.65



IP67 BASE STATION STANDARD MOUNTING OPTIONS

Mounting Options
(optional accessories shown)



ORDERING INFORMATION

MultiTech Conduit* IP67 Base Station

Model	Description	Region
MTCDTIP-L4E1-267A-868	LTE Cat 4 mPower Conduit IP67 Base Station 8-channel, 868 MHz, w/ GNSS+Wi-Fi/BT and Accessory Kit (Europe) - Accessory Kit: Mounting bracket kit, 1 LoRa antenna, 2 cellular antennas, 1 GNSS antenna, 1 Wi-Fi/BT antenna	Europe
MTCDTIP-L4E1-266A-868	LTE Cat 4 mPower Conduit IP67 Base Station 8-channel, 868 MHz, w/ GNSS and Accessory Kit (Europe) - Accessory Kit: Mounting bracket kit, 1 LoRa antenna, 2 cellular antennas, 1 GNSS antenna	Europe
MTCDTIP-267A-868	Ethernet only mPower Conduit IP67 Base Station 8-channel, 868 MHz, w/ GNSS+Wi-Fi/BT and Accessory Kit (Europe) - Accessory Kit: Mounting bracket kit, 1 LoRa antenna, 1 GNSS antenna, 1 Wi-Fi/BT antenna	Europe
MTCDTIP-266A-868	Ethernet only mPower Conduit IP67 Base Station 8-channel, 868 MHz, w/ GNSS and Accessory Kit (Europe) - Accessory Kit: Mounting bracket kit, 1 LoRa antenna, 1 GNSS antenna	Europe

RECOMMENDED ACCESSORIES

MultiTech mDot™

Model	Description	Region
MTDOT-868-XI-SMA	868 MHz XI LoRa SMA	Euro
MTDOT-868-XIP-SMA	868 MHz XI LoRa SMA w/Programming Header	Euro
MTDOT-868-XI-UFL	868 MHz XI LoRa UFL	Euro
MTDOT-868-MI-UFL	868 MHz SMT LoRa UFL	Euro
MTDOT-868-MI-TRC	868 MHz SMT LoRa RF Pad	Euro

MultiTech xDot*

Model	Description	Region
MTXDOT-EU1-A00-1	868 MHz LoRa Module UFL/TRC (Single Pack)	EMEA

Developer Kit & Accessories

Model	Description	Region
PS-56V-PoE-EU-1	Single Port 30W Power over Ethernet Transformer with European Power Cord (1 Pack)	Europe
PS-56V-PoE-EU-5	Single Port 30W Power over Ethernet Transformer with European Power Cord (5 Pack)	Europe
PS-56V-PoE-GB-1	Single Port 30W Power over Ethernet Transformer with UK Power Cord (1 Pack)	Europe
PS-56V-PoE-GB-5	Single Port 30W Power over Ethernet Transformer with UK Power Cord (5 Pack)	Europe
MTKIT-IP67-MF	IP67 Accessory Kit w/ Mounting Bracket, 5' Coax Cable N Type, Male/Female Connectors & Lightning Arrester	Global
LGT-ARRST-1	Conduit IP67 Base Station Lightning Arrester (1 Pack)	Global
LGT-ARRST-5	Conduit IP67 Base Station Lightning Arrester (5 Pack)	Global
CA-NTYPE-MF-1	Outdoor Coax Cable, N Type Male & Female connectors, 5 feet (1 Pack)	Global
CA-NTYPE-MF-5	Outdoor Coax Cable, N Type Male & Female connectors, 5 feet (5 Pack)	Global
MB-ANT-IP67-1	Conduit IP67 Antenna Mounting Bracket, Mounts One Antenna (1 Pack)	Global
MB-ANT-IP67-5	Conduit IP67 Antenna Mounting Bracket, Mounts 1 Antenna (5 Pack)	Global
ANB68-915A-I-IP67	IP67 LoRa Antenna, 15.3" (4.5 dB) (1 Pack)	Global
ANB68-915A-S-IP67	IP67 LoRa Antenna, 15.3" (4.5 dB) (5 Pack)	Global
ANL7E5-I-IP67	IP67 LTE Antenna, 7" (3.5 dB) (1 Pack)	Global
ANL7E5-S-IP67	IP67 LTE Antenna, 7" (3.5 dB) (5 Pack)	Global

Go to www.multitech.com for detailed product model numbers.

Produced in the U.S. of U.S. and non-U.S. components. Features and specifications are subject to change without notice.

The LoRa® name and associated logo are trademarks of Semtech Corporation or its subsidiaries. Trademarks and Registered Trademarks: MultiTech and the MultiTech logo, MultiConnect, Conduit, mDot, xDot, mPower, DeviceHQ. MultiTech Systems, Inc. All other products and technologies are the trademarks or registered trademarks of their respective holders.

2022-02 • 86002215 • © 2022 Multi-Tech Systems, Inc. All rights reserved.

Services & Warranty

MultiTech's comprehensive Support Services programs offer a full array of options to suit your specific needs. These services are aimed at protecting your investment, extending the life of your solution or product, and reducing total cost of ownership. Our seasoned technical experts, with an average tenure of more than 10 years, can walk you through smooth installations, troubleshooting issues and help you with configurations.

Technical Support Services

At MultiTech, we're committed to providing you personalized attention and quality service while providing you a quick response to your product support needs. We have several options of support for you to choose from.

For additional information on Support Services as well as other service offerings, please contact your MultiTech representative or visit www.multitech.com/support-go

World Headquarters

Multi-Tech Systems, Inc.
2205 Wooddale Drive
Mounds View, MN 55112 U.S.A.
Tel: 763-785-3500
Toll-Free: 800-328-9717
Email: sales@multitech.com
www.multitech.com

EMEA Headquarters

Multi-Tech Systems (EMEA)
Strata House
264-270 Bath Road
Harlington UB3 5JJ
United Kingdom
Tel: +(44) 118 959 7774
Email: sales@multitech.co.uk
www.multitech.co.uk

MULTITECH

ANEXO III: Código del nodo 'ARRAYBIN TO STRINGHEX'.

```
1 msg.payload = array2hex(msg.payload);
2 return msg;
3
4 function elem_array_to_hexstring(value) {
5     byte = value.toString(16).toUpperCase();
6     if (byte.length < 2) byte = "0" + byte;
7     return byte;
8 }
9
10 function array2hex(miArray) {
11     var resul="";
12     for(i=0;i<miArray.length;i++){
13         resul += elem_array_to_hexstring(miArray[i]);
14     }
15     return resul;
16 }
17 }
```

ANEXO IV: Código del nodo 'ELSYS DECODER'.

```
1 const TYPE_TEMP           =0x01; //temp 2 bytes -3276.8°C -->3276.7°C
2 const TYPE_RH             =0x02; //Humidity 1 byte 0-100%
3 const TYPE_ACC            =0x03; //acceleration 3 bytes X,Y,Z -128 -->
4 127 +/-63=1G
5 const TYPE_LIGHT          =0x04; //Light 2 bytes 0-->65535 Lux
6 const TYPE_MOTION         =0x05; //No of motion 1 byte 0-255
7 const TYPE_CO2            =0x06; //Co2 2 bytes 0-65535 ppm
8 const TYPE_VDD            =0x07; //VDD 2byte 0-65535mV
9 const TYPE_ANALOG1        =0x08; //VDD 2byte 0-65535mV
10 const TYPE_GPS            =0x09; //3bytes lat 3bytes long binary
11 const TYPE_PULSE1         =0x0A; //2bytes relative pulse count
12 const TYPE_SOUND          = 0x15; //2byte sound data (peak/avg)
13
14 function bin16dec(bin) {
15     var num=bin&0xFFFF;
16     if (0x8000 & num)
17         num = - (0x010000 - num);
18     return num;
19 }
20 function bin8dec(bin) {
21     var num=bin&0xFF;
22     if (0x80 & num)
23         num = - (0x0100 - num);
24     return num;
25 }
26 function hexToBytes(hex) {
27     for (var bytes = [], c = 0; c < hex.length; c += 2)
28         bytes.push(parseInt(hex.substr(c, 2), 16));
29     return bytes;
30 }
```

```

30 }
31
32 function DecodeElsysPayload(data) {
33     var obj ={};
34     for (i=0;i<data.length;i++){
35         switch(data[i]){
36             case TYPE_TEMP: //Temperature
37                 var temp=(data[i+1]<<8) | (data[i+2]);
38                 temp=bin16dec(temp);
39                 obj.temperature=temp/10;
40                 i+=2;
41             break;
42             case TYPE_RH: //Humidity
43                 var rh=(data[i+1]);
44                 obj.humidity=rh;
45                 i+=1;
46             break;
47             case TYPE_ACC: //Acceleration
48                 obj.x=bin8dec(data[i+1]);
49                 obj.y=bin8dec(data[i+2]);
50                 obj.z=bin8dec(data[i+3]);
51                 i+=3;
52             break;
53             case TYPE_LIGHT: //Light
54                 var light=(data[i+1]<<8) | (data[i+2]);
55                 obj.light=light;
56                 i+=2;
57             break;
58             case TYPE_MOTION: //Motion sensor(PIR)
59                 var motion=(data[i+1]);
60                 obj.motion=motion;
61                 i+=1;
62             break;
63             case TYPE_CO2: //CO2
64                 var co2=(data[i+1]<<8) | (data[i+2]);
65                 obj.co2=co2;
66                 i+=2;
67             break;
68             case TYPE_VDD: //Battery level
69                 var vdd=(data[i+1]<<8) | (data[i+2]);
70                 obj.vdd=vdd;
71                 i+=2;
72             break;
73             case TYPE_SOUND: //Sound
74                 obj.soundPeak=data[i+1];
75                 obj.soundAvg=data[i+2];
76                 i+=2;
77             break;
78             case TYPE_ANALOG1: //Analog input 1
79                 var analog1=(data[i+1]<<8) | (data[i+2]);
80                 obj.analog1=analog1;
81                 i+=2;
82             break;
83             case TYPE_GPS: //gps
84                 obj.lat=(data[i+1]<<16) | (data[i+2]<<8) | (data[i+3]);


```

```


85
86 obj.long=(data[i+4]<<16)|(data[i+5]<<8)|(data[i+6]);
87     i+=6;
88     break;
89     case TYPE_PULSE1://Pulse input 1
90         var pulse1=(data[i+1]<<8)|(data[i+2]);
91         obj.pulse1=pulse1;
92         i+=2;
93         break;
94     }
95 }
96 return obj;
97 }
98 var res=DecodeElsysPayload(hexToBytes(msg.payload))
99 var json=JSON.stringify(res,null,4);
    msg.payload = json;
    return msg;

```

ANEXO V: Manual de instalación del Gateway Multitech Conduit IP67.



Conduit[®] IP67 Base Station MTC DTIP Hardware Installation Guide



WWW.MULTITECH.COM

Warning and Caution
Warning and Caution symbols mean potential danger. You are in a situation that could cause bodily injury. Before working on any equipment, be aware of hazards in the installation area and be knowledgeable about electrical circuitry. Be familiar with standard practices for preventing accidents.

For translations of key cautions and warnings, go to <http://www.multitech.net/developer/basestation>.

WARNING: Only trained and qualified personnel should install, replace, or service this equipment. Installation must comply with local and national electrical codes.

- When installing or replacing the unit, the ground connection must always be made first and disconnected last.
- Disconnect PoE power (Ethernet PoE port) before servicing IP67 Base Station.
- Do not work on the system or connect or disconnect cables during periods of lightning activity.
- This device **is not** designed or approved to be used in any Hazardous Locations. Do not install or operate device if area is known to be an explosive environment.
- Externally ground this equipment using a customer-supplied ground wire before applying power. Contact an electrician if you are uncertain that suitable grounding is available. Refer to installing the Ground Wire instructions.
- All wall mounting installations are subject to the acceptance of local jurisdiction.
- Do not locate antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, because they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes.

CAUTION:

- Power over Ethernet (PoE) Certification does not apply or extend to voltages outside of standard PoE range. Any PoE voltages beyond 0vdc to 80Vdc have not been evaluated by UL or M.U.L.T.I.T.E.C.H. Nominal PoE voltage is 48Vdc. The end user supplies the PoE cable. This cable must be suitable for outdoor location. This is an 802.3at Type 2 device. For more information, refer to the Conduit IP67 Base Station PoE Application Note (S000075).
- Ethernet port **is not** designed to be connected to a public Telecommunication (PSTN) or any other connection other than IEEE 802.3-2012 power over Ethernet devices.
- Do not remove product labels.

WARNING! HOT SURFACE DO NOT TOUCH

Note: This symbol is included on the serial label. UL evaluated this device to a safety and outdoor certification temperature of -30c to +85c.

Operating temperature is -40c to +70c.

Conduit IP67 Base Station
Part Number: 82102803L
Copyright © 2020 by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc.
2220 Woodloch Drive
Mounds View, Minnesota 55112
Phone: 763-785-3500 or 800-326-9717

MULTITECH

Support
Portal: support.multitech.com
Knowledge Base: multitech.com/kb

Europe, Middle East, Africa:
support@multitech.co.uk
+44) 118 959 7774

U.S. Canada, all others:
support@multitech.com
(800) 972-2439 or (763) 717-5883

Conduit IP67 Base Station

CAUTION: Read installation instructions and safety information before starting Base Station installation. Do not connect power until directed to do so. If you do not install the accessories when you install the Base Station, cover the LoRa connectors to keep them dry.

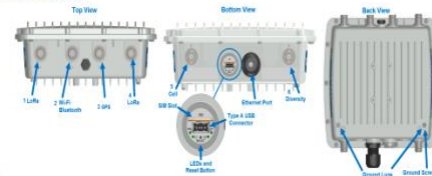
IMPORTANT: Do not attempt to disassemble the Base Station. There are no serviceable parts. Opening the enclosure without authorization may void the warranty.

Package Contents

Note: Package contents vary by model.

Item	Description	Quantity
1	MTC DTIP Base Station	1
	Mounting bracket	1
2	M5 x 10mm screws, washers and split washers (shown in the mounting bracket)	4 each
3	1/4 x 1 inch screws and anchors	4 each
4	Hose clamps	2
5	GNSS antenna	1 with GNSS models only
6	LoRa antennas	1 or 2 depending on the model
7	LTE antennas	2 with LTE models only
8	Wi-Fi antenna	1 with Wi-Fi/Bluetooth models only
9	Installation Guide	1

Connector Locations



LEDs

Label	LED	Description	Label	LED	Description
PR	Power	Green when powered up.	L1	LoRa 1	These are user-defined. Red or green.
ST	Status	Red with blinking green. These are user programmable.	L2	LoRa 2	

Additional Documentation

For additional documentation including hardware specifications, PoE application notes, and steps for using AEP, mLinux, and LoRa, go to www.multitech.net/developer/basestation. If this document has been updated, the update will be available at that location.

Safety Instructions

For safety and to achieve a good installation, please follow these safety precautions:

- Consider safety and performance when selecting an installation site. Remember electric power lines and phone lines look alike. Assume that any overhead line can cause bodily harm or death.
- Call your power company and ask them to look at your proposed installation. This is important if raising a mast or tower.
- When installing the device:
 - Do not use a metal ladder.
 - Do not work on a wet or windy day.
 - Dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
- If any part of the antenna system comes in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely. If an accident occurs, call for emergency help immediately.

IMPORTANT: Refer to Warnings and Cautions on the back page for additional information.

Requirements

In addition to the Base Station and included accessories, you will need:

- 1 - PoE injector. For requirements, refer to [Conduit IP67 Base Station PoE Application Note \(S000678\)](#).
- 1 - Cat 5 or greater Ethernet cable rated for outdoor use.
- 1 - Micro SIM (3FF) card for LTE models. MultiTech recommends using a SIM card rated for the climate where the device will be installed.
- 1 - 14awg or larger ground wire with a closed loop terminal. For details, go to [Installing a Ground Wire](#) in this document.
- 1 - Phillips screwdriver.

Related Accessories

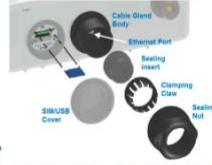
PoE injectors, higher gain LoRa antennas, lightning arrestors, and antenna accessories are available through www.multitech.com/jd07.

Note: All antennas can be directly mounted on the Base Station; however, you can mount LoRa antenna(s) up to 5 feet away from the Base Station if necessary for your location.

Installing a Micro SIM Card

To install a SIM card:

1. Remove the SIM/USB cover. The SIM holder is above the USB port.
2. Gently push the micro SIM card into the holder with the cut corner to the left and the SIM contacts facing towards the USB port as shown.
3. Reattach the plastic cover and tighten to 10.5 lbf.in (12 kgf.cm).



Installing a Ground Wire

Proper grounding of the metal enclosure is required to ensure safety. There are two ground lugs and one ground screw located on the enclosure back as shown in the [Back](#) image (under [Connector Locations](#)). Connecting a ground lug to an earth ground is the recommended method. Refer to the National Electric Code or your local codes for additional information or contact a licensed electrician for assistance in grounding an installation.

Ground wire (not provided) must be suitable for outdoor location and meet a minimum wire gauge of 14awg or larger. Use the supplied ground screw to fasten wire.

Ground wire terminal (not provided) must be closed loop (ring type, see image right) and corrosion free in design. Insert screw through loop terminal and fasten to 15 lbf.in (17.28 kgf.cm).

You can use either ground lug with the ground screw to connect the ground wire to the enclosure.

Attaching the Mounting Bracket

To attach the mounting bracket to the Base Station:

- Attach the bracket to the back of the Base Station using the supplied screws and washers as shown (right).



Mounting on a Pole

To attach the Base Station to a pole:

- Attach the Base Station to the pole using the supplied hose clamps as shown below.



Mounting on a Wall

To mount the device on a wall:

- Use the four bracket tabs to attach the Base Station to the wall with the supplied screws and anchors as shown below.



Attaching Antennas

After mounting the Base Station:

Note: All antennas should be finger-tightened plus a quarter turn.

1. For LTE models, attach the LTE cellular antennas to the Cell (5) and Diversity (6) connectors on the bottom of the Base Station.
2. Attach the GPS antenna to the GPS (3) connector on the top of the Base Station.
3. For Wi-Fi/Bluetooth models, attach the Wi-Fi antenna to the Wi-Fi (2) connector on the top of the Base Station.
4. Attach the LoRa antenna(s) to the LoRa (1) and (4) connectors at the top of the Base Station. If only one LoRa antenna, install on LoRa (1) connector.

If attaching LoRa antennas away from the Base Station, go to [Attaching LoRa Antennas via Cable](#).

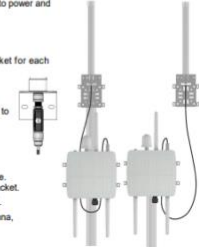
5. Go to [Connecting Ethernet](#) for steps on connecting the Base Station to power and Ethernet.

Attaching LoRa Antennas via Cable

Recommended for this option: Lightning arrestor, coaxial cable, and mounting bracket for each LoRa antenna. Refer to [Related Accessories](#) for details.

After attaching other antennas:

1. Use an antenna hose clamp to attach the antenna bracket to a LoRa antenna.
2. Attach the lightning arrestor (optional) to the antenna as shown (right).
3. Attach coaxial antenna cable to the lightning arrestor.
4. For a pole mount, use hose clamps to mount the antenna mounting bracket to the pole. For a wall mount, attach the antenna bracket to the wall using the four tabs on the bracket.
5. If you have a second LoRa antenna, repeat Steps 1 – 4 for the second LoRa antenna.
6. Attach the antenna cable to the LoRa (1) connector. If you have a second LoRa antenna, connect to the second LoRa (4) connector.



Connecting Ethernet

Note: This is an 802.3at Type 2 device. It needs a power input of at least 25W from standard 802.3at PoE input. For more information refer to the [Conduit PoE Application Note \(S000678\)](#) available at www.multitech.net/developer/basestation.

To connect your Ethernet cable and PoE injector:

1. Remove the sealing nut, clamping claw, and sealing insert.
2. Thread the Ethernet cable (not provided) through the sealing nut.
3. Wrap the sealing insert around the cable and the clamping claw over the sealing nut.
4. Plug the Ethernet cable into the Ethernet port.
5. Push the seal and clamping claw into the cable gland body.
6. Push the sealing nut over the insert and clamping claw and tighten on the cable gland body to 10.5 lbf.in (12.0 kgf.cm).

Best Practices

We recommend covering all connections with a rubber insulating tape, such as 3M's130C. Although the Base Station is rated IP67, taping provides additional protection against environmental particulates.

Next Steps

After connecting and powering up the Base Station, refer the [Conduit Base Station IP67 Getting Started Guide \(S000665\)](#) and related documentation available at www.multitech.net/developer/basestation.

Regulatory Information

This device complies with Part 15 of the FCC rules and with ICES-003 of Industry Canada for a Class A digital apparatus. Operation of this device is subject to the following conditions: (1) This device may not cause harmful interference and (2) This device must accept any interference that may cause undesired operation.

MultiTech declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The declaration of conformity may be requested at htts@support.multitech.com.