

# MÁSTER UNIVERSITARIO EN SISTEMAS ELECTRÓNICOS AVANZADOS

## TRABAJO FIN DE MÁSTER

### **IMPLEMENTACIÓN, ANÁLISIS Y EVALUACIÓN DE UN SISTEMA DE COMUNICACIONES INALÁMBRICO WIFI 6E PARA APLICACIONES INDUSTRIALES**

**Estudiante:** Canto, Lorente, Martín

**Director/a:** Zuloaga, Izaguirre, Aitzol

**Instructor de la empresa:** Val, Beitia, Iñaki

**Curso académico:** 2021/2022

*Bilbao, 14 de Septiembre de 2022*

# Resumen Laburpena Abstract

En el contexto de la industria 4.0. existe el reto de sustituir los sistemas de comunicaciones cableados por inalámbricos para conseguir aumentar la flexibilidad, escalabilidad y libre movimiento de los nodos inalámbricos en los entornos de trabajo, además de reducir significativamente los costes de operación. No obstante, debido a la naturaleza de la propagación inalámbrica, es todavía un desafío cumplir los requisitos de alta fiabilidad, baja latencia y determinismo de la industria mediante soluciones inalámbricas. Este Trabajo Fin de Máster consiste en la implementación, análisis y evaluación de una red que utiliza la tecnología inalámbrica WiFi 6E. Esta tecnología comercial se pone a prueba, en términos de latencia y fiabilidad, para el cumplimiento los requisitos que establece la industria. Se realizan evaluaciones para cuantificar la mejora, en estos términos, que conlleva el uso de la recién habilitada banda de 6 GHz, así como el resto de funcionalidades de la versión del estándar IEEE 802.11ax.

**Palabras Clave:** Comunicaciones Inalámbricas, IEEE 802.11, Industria 4.0.

4.0 Industriaren testuinguruan, komunikazio-sistema kableatuak haririk gabeko komunikazio sistemekin ordezkatzeko nahia dago, hari gabeko nodoen malgutasuna eta mugimendu askea areagotzeko. Hala ere, haririk gabeko hedapenaren izaera dela eta, oraindik zaila da fidagarritasun handiko eta latentzia txikiko industriaren baldintzak haririk gabeko soluzioen bidez betetzea. Master bukaerako lan hau, WiFi 6E teknologia erabiltzen duen sare bat inplementatzean, aztertzean eta ebaluatzean datza. Industriak ezartzen dituen baldintzak bete ahal izateko, teknologia komertzial honen latentzia eta fidagarritasuna aztertzen da. 6GHz-ko banda berriak dituen hoberakuntzak eta IEEE 802.11ax estandarraren bertsioaren gainerako funtzionalitateak aztertzeke ebaluazio bat egin da.

**Gako-hitzak:** Haririk gabeko komunikazioak, IEEE 802.11, Industria 4.0.

In the scope of Industry 4.0, exist the challenge of replacing wired communications systems with wireless ones in the factory workcell. Wireless networks provide a significant cost reduction, flexibility and free movement of the wireless nodes. However, due to the nature of wireless propagation, it's still a challenge to cope with the high reliability, low latency and determinism requirements of industry through wireless solutions. This Master Thesis present the implementation, analysis and evaluation of a WiFi 6E network. This wireless technology is evaluated for fulfil the industry requirements of latency and reliability. Evaluations are carried out to quantify the improvement, in these terms, brought about by the use of the recently enabled 6 GHz band, as well as the rest of the features of the IEEE 802.11ax standard version.

**Keywords:** Wireless communications, IEEE 802.11, Industry 4.0.

# Índice

<b>Resumen Laburpena Abstract</b>	<b>I</b>
<b>Lista de figuras</b>	<b>IV</b>
<b>Lista de tablas</b>	<b>VII</b>
<b>Lista de acrónimos</b>	<b>VIII</b>
<b>1. Introducción</b>	<b>1</b>
<b>2. Contexto</b>	<b>2</b>
2.1. Sobre Ikerlan . . . . .	2
2.2. Comunicaciones Industriales . . . . .	3
<b>3. Objetivos y alcance</b>	<b>4</b>
<b>4. Estado del arte</b>	<b>5</b>
4.1. Comunicaciones industriales . . . . .	5
4.2. Comunicaciones inalámbricas industriales . . . . .	7
<b>5. Descripción de la tecnología IEEE 802.11ax</b>	<b>13</b>
5.1. Introduccion . . . . .	13
5.2. PHY . . . . .	16
5.3. OFDMA . . . . .	18
5.4. MU-MIMO . . . . .	23
5.5. BSS . . . . .	25
5.6. WiFi 6E . . . . .	27
<b>6. Plataforma de experimentación</b>	<b>30</b>

6.1. Implementación de red . . . . .	30
6.2. Setup de red para análisis . . . . .	35
6.3. Desarrollo para evaluación de latencia . . . . .	39
<b>7. Análisis de capturas de la red</b>	<b>54</b>
7.1. Downlink . . . . .	54
7.2. Uplink . . . . .	57
7.3. Control . . . . .	60
<b>8. Evaluación de requisitos</b>	<b>69</b>
8.1. Parámetros de la implementación . . . . .	69
8.2. Caracterización del rendimiento . . . . .	78
8.3. Descripción de evaluaciones . . . . .	83
8.4. Resultados . . . . .	86
<b>9. Conclusiones</b>	<b>94</b>
<b>10.Líneas futuras</b>	<b>96</b>
<b>11.Referencias</b>	<b>97</b>

# Lista de figuras

1.	Jerarquía de los 4 niveles de los procesos industriales . . . . .	6
2.	Requisitos industriales para las comunicaciones inalámbricas establecidos por el NIST . . . . .	8
3.	Arquitectura de red de la tecnología WIA-FA . . . . .	9
4.	Arquitectura de red propuesta por 3GPP para la integración de 5G-TSN . . . . .	12
5.	Red de área local inalámbrica (WLAN) . . . . .	14
6.	Niveles del modelo OSI . . . . .	15
7.	Formato de paquetes HE . . . . .	17
8.	Representación de portadoras en OFDM . . . . .	19
9.	Transmisión OFDM en el tiempo . . . . .	19
10.	Transmisión OFDMA en el tiempo . . . . .	20
11.	Secuencia Downlink OFDMA . . . . .	22
12.	Secuencia Uplink OFDMA . . . . .	23
13.	Ejemplo de MU-MIMO 4x4:4:4:4 entre un AP y 4 clientes . . . . .	24
14.	Esquema de la secuencia HE sounding en el estándar 802.11ax . . . . .	25
15.	OBSS, overlapping basic service set . . . . .	26
16.	Canales en la banda de 6GHz en Estados Unidos y en Europa . . . . .	27
17.	Captura de la interfaz Web de configuración del router Aruba. . . . .	33
18.	Captura del terminal de comandos Aruba CLI desactivando el uso de HE en la red. . . . .	34
19.	Captura del terminal de comandos Aruba CLI mostrando estadísticas de uno de los clientes de la red. . . . .	34
20.	Setup de red para el análisis del estándar IEEE 802.11ax . . . . .	35
21.	Captura de Wireshark mostrando los paquetes capturados por el sniffer. . . . .	36
22.	Captura del tráfico en el dominio temporal realizando un análisis real y complejo del VSA. . . . .	37

23.	Resumen de las tramas identificadas por la función <i>WaveformAnalyzer</i> del ToolBox WLAN de MATLAB. . . . .	38
24.	Setup 1 para la medida de latencia entre TX y RX . . . . .	39
25.	Setup 2 para la medida de latencia entre Tx y Rx . . . . .	40
26.	Captura de la herramienta Wavemon mostrando información acerca del driver WiFi. . . . .	41
27.	Diagrama de flujo de los programas diseñados . . . . .	43
28.	Diagrama de la sincronización de relojes implementada mediante PTP . . . .	49
29.	Salida del comando <code>ptp4l</code> para el maestro. . . . .	49
30.	Salida del comando <code>ptp4l</code> para el esclavo. . . . .	50
31.	Salida del comando <code>phc2sys</code> para el maestro. . . . .	51
32.	Salida del comando <code>phc2sys</code> para el esclavo. . . . .	51
33.	Ejemplo de la representación gráfica de un histograma de latencias. . . . .	52
34.	Ejemplo de una representación gráfica de la función de distribución acumulada (cdf). . . . .	53
35.	Captura de una secuencia de envío de datos Downlink. . . . .	54
36.	Captura de la información común de un Trigger Frame. . . . .	55
37.	Captura de la información de usuario de un Trigger Frame. . . . .	56
38.	Captura de la información MAC de la trama HE-TB Block ACK. . . . .	56
39.	Captura de la información PHY de la trama HE-TB. . . . .	57
40.	Captura de la secuencia de envío de datos UL. . . . .	58
41.	Captura de la información MAC de la trama Multi STA Block ACK. . . . .	58
42.	Captura de tramas HE-SU. . . . .	59
43.	Captura de una secuencia de Trigger BSRP y Trigger Basic. . . . .	59
44.	Captura de una secuencia del Trigger BSRP. . . . .	60
45.	Captura de la secuencia HE sounding . . . . .	61
46.	Datos de la trama HE NDP Announcement. . . . .	61
47.	Datos de la trama HE Compressed Beamforming/CQI. . . . .	62
48.	Captura en Wireshark filtrando las tramas de HE sounding. . . . .	63
49.	Captura de la información obligatoria del Beacon. . . . .	64
50.	Captura de la información común del Beacon. . . . .	65
51.	Captura de la información MAC del Beacon. . . . .	66
52.	Captura de la información PHY del Beacon. . . . .	67

53.	Cambio de duración de las tramas de 100 bytes al duplicar el tamaño del canal. . . . .	71
54.	Cambio de duración de las tramas de 1500 bytes al duplicar el tamaño del canal. . . . .	72
55.	Captura del analizador de espectros en tiempo real mostrando los canales vecinos. . . . .	75
56.	Captura del Sniffer para el intercambio de tramas en el Setup 1. . . . .	77
57.	Captura del Sniffer para el intercambio de tramas en el Setup 2. . . . .	77
58.	Representación de los histograma de latencias para diferentes intervalos de transmisión. . . . .	79
59.	Representación del histograma de latencias al cambiar la configuración de power_management. . . . .	80
60.	Captura del Sniffer para el intercambio de tramas utilizando método de power_management. . . . .	81
61.	Captura del Sniffer para el intercambio de tramas desactivando el método de power_management. . . . .	81
62.	Representación del histograma de latencias al cambiar la configuración de retransmisiones. . . . .	82
63.	Representación de las curvas CDF de latencias al cambiar la configuración de retransmisiones. . . . .	83
64.	Representación del histograma para 20 MHz de la primera evaluación. . . .	86
65.	Representación del histograma para 40 MHz de la primera evaluación. . . .	87
66.	Representación del histograma para 80 MHz de la primera evaluación. . . .	87
67.	Representación del histograma para 160 MHz de la primera evaluación. . .	88
68.	Representación de las curvas CDF de los resultados de la primera evaluación. .	89
69.	Representación del histograma para 20 MHz de la segunda evaluación. . . .	90
70.	Representación del histograma para 40 MHz de la segunda evaluación. . . .	91
71.	Representación del histograma para 80 MHz de la segunda evaluación. . . .	91
72.	Representación de las curvas CDF de los resultados de la segunda evaluación. .	92

# Lista de tablas

1.	Resumen de las principales características de todas las versiones del estándar IEEE 802.11 . . . . .	15
2.	Tamaños de las RU en WiFi6 . . . . .	20
3.	Nueva normativa de la FCC acerca de la densidad espectral de potencia para diferentes tamaños de canal. . . . .	28
4.	Ejemplo de los resultados obtenidos en el fichero de salida del SW. . . . .	70
5.	Canales de 5GHz permitidos por el router (Unidades en MHz). . . . .	76
6.	Resultados obtenidos al activar y desactivar las retransmisiones del driver WiFi. . . . .	83
7.	Resultados obtenidos en la banda de 6 GHz para las pruebas de la primera evaluación. . . . .	89
8.	Resultados obtenidos en la banda de 5 GHz para las pruebas de la primera evaluación. . . . .	90
9.	Resultados obtenidos en las pruebas de la tercera evaluación. . . . .	93

# Lista de acrónimos

**ACK** Acknowledgement

**AMPDU** Aggregate MAC Protocol Data Unit

**AMSDU** Aggregate MAC Service Data Unit

**AP** Access Point

**BIOS** Basic Input Output System

**BPSK** Binary Phase-shift Keying

**BSS** Basic Service Set

**CCA** Clear Channel Assesment

**CDF** Cumulative Distribution Function

**COTS** Commercial off the self

**CSMA/CA** Carrier Sense Multiple Access with Collision Avoidance

**DSSS** Direct-sequence Spread Spectrum

**ETSI** European Telecommunications Standards Institute

**FCC** Federal Communications Commission

**FCS** Frame Check Sequence

**FW** Firmware

**GRUB** Grand Unified Bootloader

**HW** Hardware

**IEEE** Institute of Electrical and Electronics Engineers

**IoT** Internet of Things

**ITU** International Telecommunication Union

**LLC** Logical Link Control

**MAC** Media Access Control

**NIST** National Institute of Standars and Tecnhology

**OFDM** Orthogonal Frequency Division Multiplexing

**OFDMA** Orthogonal Frequency-Division Multiple Access

**PER** Packet Error Rate

**PPDU** Physical Layer Protocol Data Unit

**RSSI** Received Signal Strength Indicator

**RX** Receptor

**SDR** Software-defined Radio

**SHARP** Synchronous and Hybrid Architecture for Real-time Performance

**SPI** Serial Peripheral Interface

**SRO** Spatial Reuse Operation

**SSID** Service Set Identifier

**STA** Station

**SW** Software

**TCP** Transmission Control Protocol

**TF** Trigger Frame

**TX** Transmitter

**UDP** User Datagram Protocol

**USB** Universal Serial Bus

**UWB** Ultra Wide-Band

**WIA-FA** Wireless networks for Industrial Automation-Factory Automation

**WLAN** Wireless Local Area Network

**WPA** Wi-Fi Protected Access

**WPAN** Wireless Personal Area Network

# 1. Introducción

La creciente digitalización de procesos en el contexto de la industria 4.0 ha supuesto el uso de más dispositivos digitales en los entornos de trabajo. Estos dispositivos requieren el intercambio constante de información para su control y configuración y en muchos casos de manera rápida y fiable. Hasta ahora, la interconexión entre ellos se ha implementado mediante soluciones cableadas. No obstante, las comunicaciones inalámbricas ofrecen una nueva posibilidad de comunicación en este tipo de escenarios, ofreciendo mayor flexibilidad y escalabilidad con un coste operacional notablemente menor.

Para ello, estos nuevos sistemas de comunicaciones inalámbricos deben ser capaces de cumplir los requisitos de baja latencia, alta fiabilidad y determinismo que tienen las comunicaciones en la industria. Estos requisitos, hasta ahora, no se cumplen mediante las tecnologías inalámbricas tradicionales y es necesario el diseño de tecnologías y soluciones específicas para alcanzarlos.

No obstante las últimas versiones de los estándares tecnológicos pueden suponer un acercamiento hacia el cumplimiento de estos requisitos. Concretamente, en este proyecto se pretende realizar una evaluación sobre la última versión del estándar IEEE 802.11, IEEE 802.11ax (WiFi 6). Recientemente se ha habilitado el uso de la banda de 6 GHz para esta tecnología inalámbrica, conociéndose esta versión como WiFi 6E.

En este proyecto se va a realizar una evaluación de fiabilidad y latencia de esta tecnología, particularmente se va a evaluar el término conocido como *bounded latency* (latencia limitada). Este término se refiere a que todos los envíos de un sistema no superen una latencia máxima. En función de la aplicación industrial se establece una latencia y tasa de error concretas, de forma que los paquetes que superen este límite de latencia son considerados como erróneos.

## 2. Contexto

Este Trabajo Fin de Máster (TFM) se lleva a cabo durante una cooperación educativa con la empresa Ikerlan, S. Coop. Es por ello que, en este apartado, se da información sobre Ikerlan y el equipo de investigación que ha identificado la necesidad de este proyecto.

### 2.1. Sobre Ikerlan

Ikerlan es un centro tecnológico fundado en 1974, cuya sede principal está situada en Mondragón, Guipúzcoa. Pertenece a una de las cooperativas miembro de la Corporación Mondragón, que es el segundo grupo empresarial de economía social en España. También, Ikerlan es miembro del Basque Research and Technology Alliance (BRTA). Es líder en la transferencia de conocimiento y en la aportación de valor competitivo a las empresas.

Ikerlan sigue un modelo único de colaboración con distintas universidades como la UPV/EHU que combina actividades de transferencia tecnológica, investigación propia y formación de personal especializado. Se divide principalmente en tres unidades de especialización tecnológicas, para las cuales las líneas de investigación son las siguientes:

- Tecnologías de Electrónica, Información y Comunicación: desarrollo de productos electrónicos confiables, ciberseguridad industrial y digitalización industrial.
- Energía y Electrónica de Potencia: tecnologías de almacenamiento, gestión energética y electrónica de potencia para aplicaciones de e-movilidad (vehículos, transporte ferroviario, aeronáutica, ascensores...) y estacionarias (energías renovables, redes eléctricas...), orientadas a obtener soluciones energéticamente más eficientes, más fiables, más compactas y de menor coste.
- Mecatrónica y automatización: integración de tecnologías de mecánica aplicada y de control inteligente y monitorización para mejorar la fiabilidad durante todo el ciclo de vida de los productos.

Este proyecto está desarrollado en la unidad de especialización de Tecnologías de Electrónica, Informática y Comunicación. Dentro de la línea de investigación acerca de la digitalización industrial, existe la tarea de investigar acerca de la integración de comunicaciones inalámbricas en la industria. Esta, se lleva a cabo en el equipo de Sistemas de Comunicaciones, liderado por Aitor Arriola.

## 2.2. Comunicaciones Industriales

En el equipo de Sistemas de Comunicaciones de Ikerlan llevan años investigando acerca de la integración de comunicaciones inalámbricas en la industria. Debido a la naturaleza de la propagación inalámbrica, alcanzar la fiabilidad requerida en los entornos de trabajo es todavía un reto.

Dentro de este equipo, se ha llevado a cabo una investigación muy amplia en esta línea. Por ejemplo, recientemente, se ha investigado acerca de la integración de la tecnología 5G para la industria 4.0 [1], también acerca de la viabilidad de sistemas inalámbricos redundados para aplicaciones safety [2] e incluso se han implementado soluciones que cumplen los requisitos de alta fiabilidad y latencia de las aplicaciones industriales, en el caso del trabajo realizado en [3] mediante la tecnología SHARP (Synchronous and Hybrid Architecture for Real-time Performance).

Este proyecto en concreto se enmarca en el contexto de la evaluación de las últimas tecnologías *commercial off the shelf* (COTS) de cara a poder ser utilizadas en aplicaciones industriales. Específicamente en WiFi 6E, para la cual en el equipo no se había llevado a cabo ningún desarrollo o implementación hasta la fecha.

### 3. Objetivos y alcance

Antes del comienzo del proyecto, el objetivo de este era desarrollar un sistema de comunicaciones inalámbrico para evaluar el rendimiento de los últimos estándares de las tecnologías de WiFi y UWB de manera redundada e individual de cara a utilizarlos en aplicaciones industriales.

No obstante, debido a las últimas tendencias de estas tecnologías y la reestructuración de proyectos dentro del grupo de investigación, se decidió darle al proyecto un enfoque más centrado en la tecnología de WiFi, dejando la tecnología de UWB para que sea analizada en otro proyecto aparte.

Por tanto, el objetivo principal de este proyecto es **implementar, analizar y evaluar un sistema de comunicaciones WiFi 6E para el cumplimiento de requisitos industriales**. Al analizar y comprobar el alcance de esta tecnología, este proyecto servirá para considerar la alternativa de WiFi en futuros desarrollos inalámbricos dentro del grupo de investigación de Ikerlan.

Los objetivos secundarios de este proyecto son:

- **Analizar el estado del arte:** Estudiar las características de las comunicaciones en la industria, los requisitos para las soluciones inalámbricas y tecnologías que cumplen estos requisitos.
- **Estudiar las mejoras introducidas en la última versión de estándar IEEE 802.11ax.**
- **Implementar una red WiFi 6E.** Se pretende lograr el funcionamiento de un sistema de comunicaciones inalámbrico en la banda de 6 GHz mediante los módulos WiFi y plataformas proporcionadas por Ikerlan.
- **Analizar mediante capturas el uso del estándar IEEE 802.11ax en la red implementada.** Para comprobar que la red implementada esté utilizando y aprovechándose de las mejoras introducidas en el último estándar WiFi, se pretenden capturar y analizar los intercambios de tramas entre dispositivos de la red.
- **Evaluación de parámetros críticos asociados a redes industriales.** Como último objetivo del proyecto se pretende evaluar la latencia y fiabilidad entre los dispositivos del sistema de comunicaciones. Para ello, primero se deberán analizar las configuraciones de estos de cara a maximizar el rendimiento y, después de la evaluación, comprobar si se logran alcanzar los requisitos industriales. Dentro de este objetivo se pretende también cuantificar las mejoras que introduce el uso de la nueva banda de 6 GHz respecto a la de 5GHz, además de comparar el rendimiento del estándar IEEE 802.11ax respecto al anterior IEEE 802.11ac.

## 4. Estado del arte

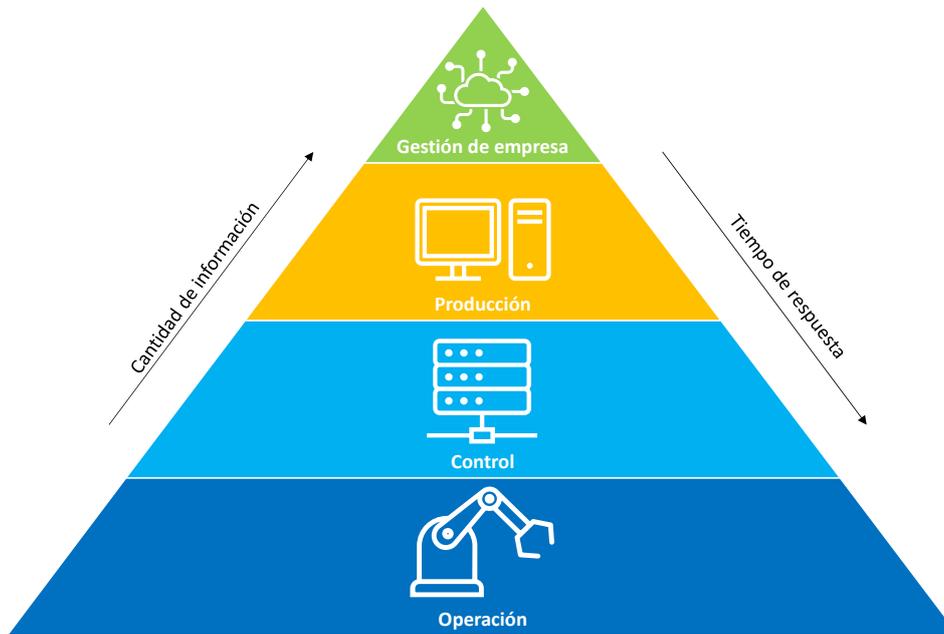
Este proyecto se enmarca en la línea de investigación de las comunicaciones inalámbricas para aplicaciones industriales. Por ello, primero se van a mencionar las características de las comunicaciones en la industria, así como las soluciones cableadas actuales. Después, se mencionan los requisitos que tienen las comunicaciones inalámbricas para sustituir a las soluciones cableadas. Más tarde, se realiza un estado del arte de soluciones inalámbricas que cumplen estos requisitos.

Por último, debido a que en este proyecto se realiza una evaluación de una tecnología inalámbrica COTS, se describe el estado del arte de las dos opciones más prometedoras para los entornos industriales: WiFi y 5G.

### 4.1. Comunicaciones industriales

En los últimos años, debido a la digitalización de la industria, cada vez hay más dispositivos electrónicos en los entornos de trabajo. Desde que se comenzaron a automatizar los procesos industriales en la década de los 1950, se han utilizado circuitos electrónicos para el control de estos procesos. Con el paso del tiempo, la tecnología de estos sistemas de control ha ido evolucionando al mismo tiempo que el sector electrónico en general. Cada vez, estos sistemas realizan tareas más complejas y, debido a lo catastrófico que puede ser un error en el sistema de control de procesos industriales, requieren mayor fiabilidad.

En los entornos de trabajo, no sólo se requieren sistemas de comunicaciones para el intercambio de tramas en los procesos de control. Sino para todas las partes de un proceso industrial, en donde no todas tienen los mismos requerimientos.



**Figura 1:** Jerarquía de los 4 niveles de los procesos industriales.  
**Fuente:** Elaboración propia.

En la Figura 1 se muestra la pirámide que distingue en 4 niveles las partes de un proceso industrial.

Los niveles altos de esta pirámide, gestión de empresa y producción, se encargan de la gestión de los procesos industriales como aplicaciones en red o procesos de supervisión del producto. Estos dispositivos requieren comunicaciones de grandes cantidades de datos, pero no de baja latencia.

Los niveles bajos de esta jerarquía no envían tanta información y suelen transmitir paquetes más pequeños. Estos en cambio, tienen el estricto requisito de respuesta rápida, alrededor del milisegundo. Las comunicaciones entre estos niveles suelen ser entre controladores (PLCs - Programmable Logic Controllers) y sensores más actuadores. Los sensores informan al controlador sobre variables que se desean analizar como temperatura, posición o material de una pieza (por ejemplo, para distinguir piezas de metal y de plástico). Los actuadores, en cambio, ejecutan las órdenes del controlador.

El tiempo de respuesta es el tiempo en el que el sensor detecta una anomalía y el controlador indica al actuador la detención del proceso. Exceder dicho tiempo puede tener consecuencias catastróficas. Por ejemplo, en el caso de las líneas de montaje puede ser crucial que las ordenes de la maquinaria se ejecuten en tiempo y forma, evitando así ocasionar daños logísticos e incluso humanos para la empresa. Las comunicaciones de estos dos niveles son las que necesitan cumplir los requisitos industriales mencionados en este proyecto. Estos son principalmente baja latencia, alta fiabilidad y determinismo.

#### 4.1.1. Soluciones actuales

Para cumplir estos requisitos, a lo largo de los años se han utilizado diferentes protocolos y tecnologías cableadas.

Estos primeros protocolos estaban basados en buses de campo como Profibus o Modbus. Los buses de campo, hoy en día, requieren de una arquitectura compleja y un precio elevado, debido a la incompatibilidad que existe entre los diferentes estándares. Aun así, con los buses de campo se pueden conseguir comunicaciones muy seguras y con altas tasas de datos.

Más adelante, gracias a la versión del estándar IEEE 802.3 utilizada en industria, llamada Industrial Ethernet [4], se dio un salto importante en los sistemas cableados. Con Industrial Ethernet se consiguen redes de comunicaciones industriales de menor complejidad y menor coste, a la vez que se incrementa la velocidad de transmisión de datos. A parte de mejorar frente a los buses de campo en este aspecto, tienen la ventaja de poder transmitir información en tiempo real. Por ello, en la industria se han ido reemplazando los buses de campo por tecnologías basadas en Industrial Ethernet.

Las alternativas más utilizadas de Industrial Ethernet son: EtherCAT [5], SERCOS III [6] y Profinet IO [7] que, en función de necesidades de la aplicación, tienen sus ventajas y desventajas.

Por otro lado, hay redes de comunicaciones que requieren de requisitos temporales todavía más precisos. En esta línea, una de las tareas principales del grupo de trabajo IEEE 802.1, denominada Time Sensitive Networking (TSN) [8], está centrada en lograr comunicaciones deterministas en tiempo real mediante Ethernet. Esta tecnología está centrada en la capa MAC del modelo OSI y no pretende sustituir los protocolos como Profinet, ya que estos operan en las capas de más arriba. Pretende, sin embargo, establecer mecanismos que puedan ser utilizados en estos protocolos para lograr determinismo en tiempo real.

## **4.2. Comunicaciones inalámbricas industriales**

Debido a la industria 4.0, están creciendo de manera significativa los procesos de automatización en los entornos de trabajo. Esto está afectando a las instalaciones industriales, ya que se están saturando de dispositivos heterogéneos interconectados entre sí mediante cables. Por ello, para facilitar la instalación y mantenimiento de estos nuevos procesos en la industria, existe el reto de sustituir los sistemas cableados por inalámbricos [9]. Las redes inalámbricas reducirían los costos de operación e instalación de los sistemas de comunicaciones entre estos nuevos dispositivos. Además, aumentarían la escalabilidad y flexibilidad de estas redes, logrando el libre movimiento de los nodos.

No obstante, las comunicaciones inalámbricas son más vulnerables que las cableadas, debido principalmente a la naturaleza de la propagación inalámbrica. Las señales inalámbricas se atenúan a lo largo del trayecto y hay objetos que interfieren en la propagación de la señal radio, provocando efectos como multicamino o fading. Además, el medio por el que se transmite la información es compartido y puede producir interferencias que afectan a la fiabilidad. Por ello, es más difícil desarrollar sistemas que cumplan los requisitos de fiabilidad y latencia mediante soluciones inalámbricas.

### **4.2.1. Requisitos**

En estas aplicaciones industriales se utilizan los siguientes parámetros para establecer los requisitos de las soluciones inalámbricas:

- **Latencia:** es el tiempo que tarda un paquete en llegar al receptor desde que se transmite del origen. Es un factor crítico, debido al tiempo máximo de respuesta de estas aplicaciones. Un paquete que supera este parámetro es considerado como erróneo y se contabiliza mediante el parámetro de fiabilidad.
- **Fiabilidad:** aplicaciones industriales como transmisiones safety y procesos críticos son muy sensibles a la pérdida de paquetes. La fiabilidad se mide mediante la tasa de paquetes erróneos (PER), cuyo valor indica el número de errores entre el número de paquetes totales.
- **Escalabilidad:** son el número de dispositivos que se pueden integrar en el sistema de comunicaciones, cumpliendo todos ellos los demás requisitos exigidos.
- **Rango:** es la distancia máxima en la que una comunicación wireless puede funcionar cumpliendo los demás requisitos.
- **Tamaño del payload:** el payload es la información útil que se transmite, los bytes de información que la aplicación desea transmitir. En función de la aplicación industrial, se requiere de un tamaño de payload distinto. Por ejemplo, para aplicaciones safety se requiere un payload pequeño.
- **Tasa de actualización:** o intervalo de transmisión, es la frecuencia con la que un sistema de comunicaciones envía información.

En base a estos parámetros, un trabajo del NIST (National Institute of Standards and Technology) [10] recoge en base a diferentes proyectos industriales reales una serie de requisitos, divididos en 5 clases de aplicaciones industriales diferentes:

User Requirement		Class 0: Safety	Class 1: Closed Loop Regulatory Control	Class 2: Closed Loop Supervisory Control	Class 3: Open Loop Regulatory Control	Class 4: Alerting Monitoring
Latency (ms)	Typical	4	4	20	4	50
	Minimum	0.5	0.25	4	0.5	4
Reliability (Pr. of Loss)	Typical	$10^{-7}$	$10^{-7}$	$10^{-7}$	$10^{-7}$	$10^{-6}$
	Minimum	$10^{-7}$	$10^{-7}$	$10^{-7}$	$10^{-7}$	$10^{-7}$
Scale (# of links)	Typical	8	10	10	1	100
	Maximum	16	30	30	4	300
Range (m)	Typical	10	10	10	10	10
	Maximum	30	30	30	30	30
Payload (B)	Minimum	6	8	8	8	12
	Maximum	24	1024	1024	1024	33K
Update Rate (Hz)	Typical	125	125	25	125	10
	Maximum	1000	2000	125	1000	125

**Figura 2:** Requisitos industriales para las comunicaciones inalámbricas establecidos por el NIST.

**Fuente:** [10]. Extraído de la definición del estándar.

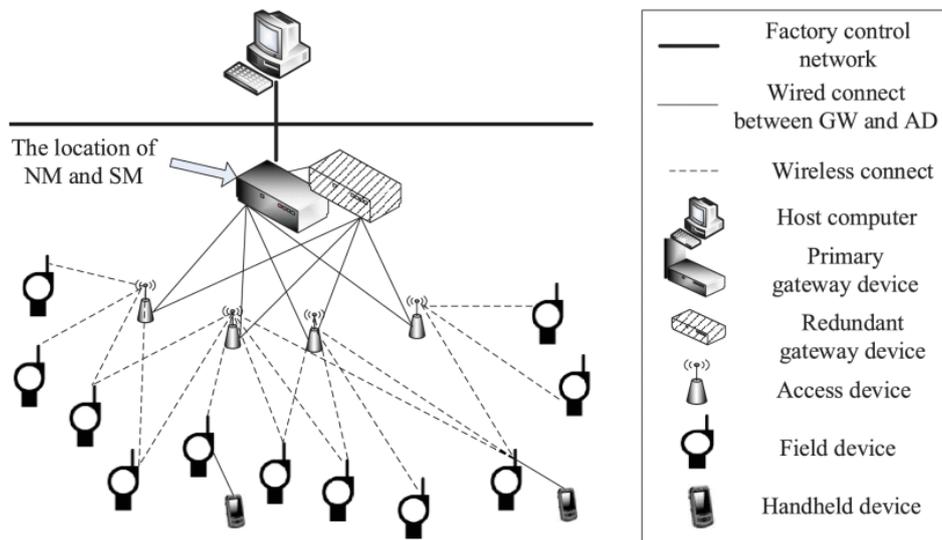
Estos requisitos sirven como referencia para la evaluación de este proyecto, en el que se evalúa la combinación de latencia y fiabilidad, también conocida como bounded latency, además de los paquetes perdidos. Se requieren tasas de error de entre  $[10^{-6}, 10^{-7}]$  para latencias de 4, 20 y 50 ms.

#### 4.2.2. Soluciones inalámbricas

Un aspecto clave a tener en cuenta es que la mayoría de tecnologías inalámbricas hasta la fecha han sido desarrolladas para el mercado de consumo y, por tanto, se centran en lograr transmisiones de altas tasas de datos sin reparar en latencia y fiabilidad. Por ello, los sistemas inalámbricos actuales no cumplen estos requisitos y no están preparados para el despliegue en escenarios industriales.

No obstante, en determinados grupos de trabajo se han llevado a cabo soluciones inalámbricas capaces de cumplir estos requisitos. Todas ellas se basan en el diseño de HW específico sin ninguna estandarización. Utilizan tecnologías inalámbricas basadas en los estándares del IEEE, pero con modificaciones tanto a nivel MAC como PHY para optimizar su rendimiento aumentando su fiabilidad y reduciendo la latencia.

Una de estas tecnologías es *Wireless networks for Industrial Automation-Factory Automation* (WIA-FA). Esta tecnología, ya estandarizada [11], define una arquitectura redundante compuesta por diferentes dispositivos donde cada uno realiza una determinada función. Se trata de una topología de red de estrella, basada en la jerarquía industrial de la Figura 1, donde el nivel más bajo está conectado a los dispositivos de campo: sensores y actuadores.



**Figura 3:** Arquitectura de red de la tecnología WIA-FA.

**Fuente:** [12]. Extraído del paper original.

Esta arquitectura de red se puede ver en la Figura 3, donde se muestran todos los dispositivos que forman parte de la red. Además, se distinguen los enlaces inalámbricos y cableados.

El nivel PHY de esta tecnología está basado en el del estándar IEEE 802.11n. El

nivel MAC es definido específicamente, que ofrece funcionalidades propias para la comunicación entre los dispositivos de acceso (similares a los APs) y un sistema de retransmisiones más complejo que garantiza la robustez contra errores.

Según el trabajo de evaluación realizado en [12], se demuestra que esta tecnología cumple los requisitos de 3 casos de uso industriales distintos. Estos requisitos se centran en fiabilidad ( $10^{-4}$  y  $10^{-6}$  en el caso más restrictivo), latencia ( $<1$  ms) para transmisiones de paquetes pequeños ( $<100$  bytes) y tasa de datos baja ( $<100$  kbps). Para cada aplicación, modifican parámetros como el número de retransmisiones y velocidad para alcanzar los requisitos específicos. Además, según el número de dispositivos que necesitan interconectar y el espacio en el que se encuentran, varían el tamaño de la red.

Otro trabajo en este campo es el de *wireless high performance*, Wireless HP [13]. Esta tecnología se basa en el diseño de una capa PHY de alto rendimiento para aplicaciones industriales específicas, centrándose en el uso de paquetes pequeños. Tiene el objetivo de reducir la latencia e intervalo de transmisión de tecnologías como WIA-FA, para poder alcanzar requisitos temporales más estrictos. Según lo evaluado en el trabajo de [14], teóricamente, esta tecnología es capaz de transmitir en intervalos de menos de 100 us, obteniendo un resultado de baja latencia ( $<1$  ms) y alta fiabilidad ( $10^{-7}$ ).

Otro desarrollo de una tecnología para aplicaciones con requisitos críticos temporales es el de [15]. En este trabajo, se presenta una solución llamada *w-SHARP*. Es una tecnología basada en los fundamentos de TSN, que ofrece sincronización temporal con planificación consciente del tiempo a la vez que alta fiabilidad y latencia controlada (bounded latency). Esta tecnología utiliza unas capas MAC y PHY propias, basadas en el estándar 802.11, pero optimizadas para tráfico industrial. En el trabajo [15] se realiza una implementación sobre FPGA basada en una plataforma SDR de esta tecnología. Mediante esta solución se demuestra que se logran cumplir los requisitos de fiabilidad ( $10^{-7}$ ) y latencia ( $<100$  us) de la Figura 2, además de un jitter menor que 1 us, requerido para la integración en TSN.

No obstante, todas estas soluciones suponen un diseño HW específico para su despliegue. En el caso de *w-SHARP* y Wireless HP, requieren una implementación mediante FPGAs de alto rendimiento. Esto supone un coste alto en comparación a las soluciones cableadas como Profinet. En estas se ofrecen módulos maestros y esclavos ya diseñados para un uso general, que se pueden integrar en el HW de los propios nodos de manera sencilla. Para llevar a cabo el mismo proceso en las soluciones inalámbricas, las últimas versiones de los estándares WiFi y 5G buscan ofrecer servicios que cumplan los requisitos temporales y de fiabilidad mencionados [16].

### 4.2.3. Tecnologías COTS

Las tecnologías inalámbricas COTS (Commercial off the shelf), tradicionalmente, han estado orientadas para mejorar la velocidad de dispositivos como smartphones o PCs en entornos domésticos.

No obstante, debido a la tendencia de reemplazar las comunicaciones cableadas por inalámbricas en la industria, las últimas versiones de WiFi (IEEE 802.11ax y IEEE 802.11be) y 5G están diseñados para, aparte de mejorar velocidad, soportar comunicaciones de baja latencia y alta fiabilidad.

#### 4.2.3.1. WiFi

La tecnología de WiFi permite la interconexión de dispositivos electrónicos de manera inalámbrica dentro de una red de área local (WLAN). Opera en las bandas sin licencia de 2.4, 5 y ahora 6 GHz.

La última versión de WiFi en el mercado es WiFi 6 [17], descrita con mayor detalle en la sección 5, introduce por primera vez en el estándar la tecnología OFDMA (Orthogonal Frequency Division Multiple Access). Esta permite la transmisión simultánea de varios usuarios mediante el reparto del espectro. Gracias a esta tecnología y otras funcionalidades, en teoría, se logra reducir la latencia respecto a la versión anterior WiFi 5. Además, permite el uso de canales de 160 MHz de ancho de banda que, utilizando la modulación para mayor velocidad (1024 QAM), logra una velocidad máxima de 2.4 Gbps.

La próxima versión del estándar es el IEEE 802.11be [18], más conocido como WiFi 7. Esta introduce el uso de canales de 320 MHz junto a la modulación 4096 QAM, con lo que se pueden alcanzar velocidades de más de 5 Gbps.

Además de mejorar en este aspecto, también se introduce la funcionalidad clave de Multi Link Operation (MLO). El término, Multi Link, se refiere al uso simultáneo de varias bandas de transmisión. Este método permite a los clientes conectarse al AP en más de una banda frecuencial, es decir, permite establecer una misma conexión a través de dos de las bandas de 2.4, 5 o 6 GHz. Al utilizar más de una banda, se mejoran las velocidades de transmisión pero, además, al poder enviar la misma información por las dos bandas de manera redundante, se logran sistemas de comunicaciones más fiables y con latencia bajas y controladas.

Mediante esta nueva funcionalidad de operación Multi-Link, OFDMA y otras características extra del 802.11be se pretende lograr latencias bajas y deterministas junto con una gran fiabilidad para poder integrar esta tecnología en redes TSN. En [19] se realiza una simulación de la funcionalidad MLO sumada al estándar 802.11ax. En esta se simula el rendimiento de esta tecnología en escenarios industriales para una latencia máxima de 1 ms con un 99.9 % de fiabilidad. Al comparar la tecnología de 802.11ax con y sin la funcionalidad de MLO, se logra alcanzar estos mismos resultados de fiabilidad y latencia en canales con una diferencia de 3 dB de SNR. Es decir, la técnica Multi Link mejora la operación de la tecnología en canales con más ruido, con una SNR 3dB menor. Esto comprueba que la técnica de Multi Link mejora el rendimiento del estándar en términos de latencia y fiabilidad, ya que funciona en escenarios con peores condiciones.

#### 4.2.3.2. 5G

La tecnología 5G es la quinta generación de tecnologías de telefonía móvil. Interconectan dispositivos en redes de área amplia (WAN, Wide Area Network) a través de distancias largas, para exteriores e interiores. Son redes de celdas, cuya área de servicio está dividida en pequeñas regiones geográficas denominadas celdas.

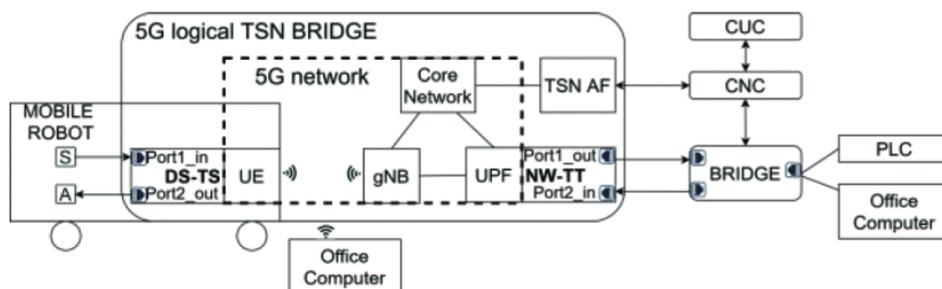
Estas redes están diseñadas para mejorar la velocidad respecto a su anterior versión, 4G, superando velocidades de 10 Gbps. Además, se presentan nuevos mecanismos para reducir la latencia entre usuarios y así poder interconectar más usuarios. Al igual que en 4G, estas tecnologías utilizan OFDMA, como las últimas versiones de WiFi.

5G opera en tres tipos de banda frecuenciales diferentes:

- Banda baja: 600 MHz, 800 MHz, 900 MHz
- Banda media: 2.5 GHz, 3.5 GHz, 3.7-4.2 GHz
- Banda alta (onda milimétrica): 24 GHz, 28 GHz, 37 GHz, 39 GHz, 47 GHz

Según aumenta la frecuencia, baja la cobertura de la red, pero se obtiene un mejor rendimiento. Las velocidades de 10 Gbps se alcanzan tan sólo en las bandas milimétricas [20], que es también en las que menor latencia se consigue.

No obstante, para integrar 5G con TSN el grupo 3GPP (3rd Generation Partnership Project) define en [21] la arquitectura y funcionalidades que se deben llevar a cabo. Esto se basa en los sistemas 5G, que están formados por un 5G Access Network (5G-AN) y un 5G Core Network (5GC). 3GPP define una arquitectura en la que este sistema 5G se integra como puente TSN en una red TSN.



**Figura 4:** Arquitectura de red propuesta por 3GPP para la integración de 5G-TSN.  
**Fuente:** [1]. Extraído del paper original.

Esta arquitectura se representa en la Figura 4 en donde se muestra un ejemplo de la conexión inalámbrica entre sensores y un PLC, a través de los componentes de este sistema. En [1] se realiza una evaluación teórica del delay que introduce este sistema 5G a la red TSN, donde se obtiene un máximo delay de 22  $\mu$ s para una aplicación de latencia máxima de 1 ms y 100 Mbps de velocidad. Esta medida sirve para evaluar el determinismo que se obtiene a la hora de integrar 5G en las redes TSN. Se trata de un resultado aceptable que acerca la integración de esta tecnología inalámbrica en aplicaciones con requisitos temporales críticos.

# 5. Descripción de la tecnología IEEE 802.11ax

En este apartado se va a hacer una descripción de la tecnología utilizada, concretamente el estándar IEEE 802.11ax. Se van a explicar las características generales del estándar así como las funcionalidades extra que ofrece respecto a versiones anteriores.

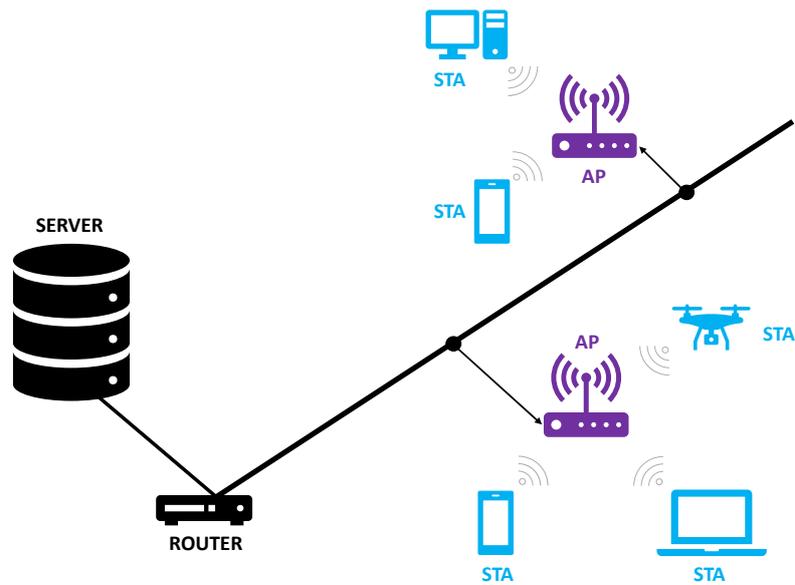
## 5.1. Introducción

WiFi es la manera establecida para la conexión a internet. Con alrededor de 18 billones de dispositivos en uso hoy en día [22], es la tecnología inalámbrica más utilizada, que permite la interconexión de dispositivos electrónicos de manera inalámbrica dentro de una red de área local.

### 5.1.1. WLAN

Una red de área local inalámbrica (WLAN - Wireless Local Area Network), es un tipo de red utilizada como alternativa de una red de área local LAN. Una LAN es básicamente un conjunto de equipos (nodos y software) conectados entre sí que envían y reciben impulsos eléctricos y ondas electromagnéticas para el transporte de datos en una determinada área (por ejemplo, en una casa, una oficina o un edificio). La única diferencia entre WLAN y LAN es el medio de transmisión, mientras que en LAN se utilizan cables de par trenzado o fibra óptica, en WLAN se usa el aire como medio de transmisión para comunicar los clientes.

La manera habitual de utilizar una WLAN es utilizar un medio cableado para la comunicación troncal del sistema y conectar la misma al punto de acceso. El AP (Access Point) es el dispositivo encargado de comunicarse con los clientes y transmitir esta información a la comunicación principal cableada. Por ello, tiene dos interfaces, una para comunicarse con la red troncal cableada y otra inalámbrica para conectar los clientes. Las estaciones de cliente (STA-Station) pueden ser cualquier tipo de dispositivo como, por ejemplo, ordenadores, portátiles o teléfonos móviles. Todas las tramas que se envían entre clientes dentro de una red pasan primero por el AP.



**Figura 5:** Red de área local inalámbrica (WLAN).  
**Fuente:** Elaboración propia.

### 5.1.2. IEEE 802.11

Un estándar define un conjunto de reglas de acceso y de transmisiones dentro de la topología de red. Es un elemento indispensable para garantizar la difusión de una tecnología, ya que permite la realización del mismo producto a diferentes fabricantes, obteniendo de esta manera competitividad para su comercialización.

El estándar WiFi (IEEE 802.11) está definido por el comité de la IEEE (Institute for Electrical and Electronics Engineers), y define la modalidad de interconexión entre estaciones en espacios limitados utilizando el aire como medio de transmisión. Es uno de los estándares de mayor interés para la evolución de las tecnologías de interconexión en áreas locales.

Hoy en día, las redes de área local inalámbricas han incrementado su popularidad, a la vez que han aumentando su tasa de datos y fiabilidad. La IEEE 802.11 WLAN se ha convertido en una tecnología complementaria a la tecnología de alta velocidad IEEE 802.3, más conocida como Ethernet, para dispositivos portátiles. Debido a la facilidad en cuanto al movimiento de los dispositivos que introduce esta tecnología inalámbrica, se ha popularizado tanto en entornos de trabajo como en los hogares. Hoy en día, es difícil encontrar un lugar en donde no se perciba ninguna señal WiFi.

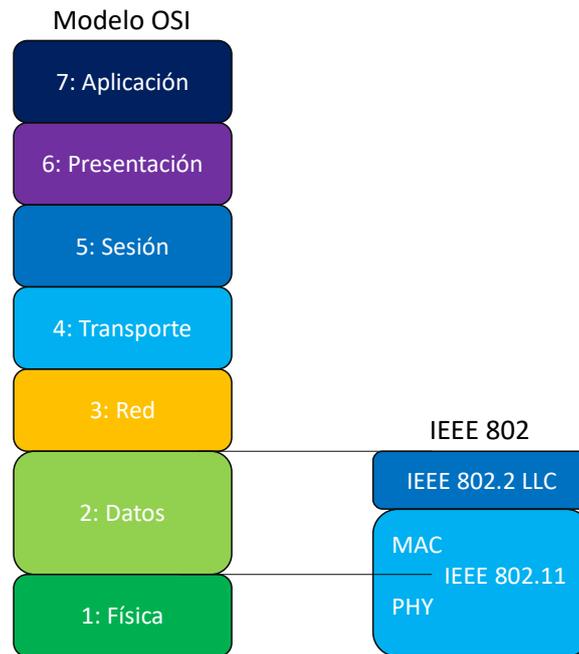
Otro de los motivos del éxito ha sido la constante mejora de la tecnología. Con el paso de los años, los nuevos estándares WiFi han conseguido mejorar la tasa de datos y fiabilidad de la comunicación, esto, sin incrementar el precio, ha hecho que cada vez se pueda utilizar WiFi en más aplicaciones diferentes como por ejemplo streaming de vídeos de alta resolución.

En la Tabla 1 se puede apreciar el crecimiento en cuanto a tasa de datos de los estándares a lo largo de los años. Ha sido la motivación principal de esta línea de investigación en las dos últimas décadas.

Estándar	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
<b>Año</b>	1997	1999	1999	2003	2009	2013	2019
<b>Nombre</b>	WiFi	WiFi 1	WiFi 2	WiFi 3	WiFi 4	WiFi 5	WiFi 6
<b>Data Rate</b>	2 Mbps	11 Mbps	54 Mbps	54 Mbps	450 Mbps	1.7 Gbps	2.4 Gbps
<b>2.4 GHz</b>	✓	✓		✓	✓	✓	✓
<b>5 GHz</b>			✓		✓	✓	✓
<b>6 GHz</b>							✓
<b>Ancho de Banda</b>	20	20	20	20	20, 40	20, 40, 80, 160	20, 40, 80, 160
<b>Tecnología RF</b>	DSSS, FHSS	DSSS	OFDM	OFDM, DSSA	OFDM	OFDM	OFDMA

**Tabla 1:** Resumen de las principales características de todas las versiones del estándar IEEE 802.11

Los estándares de las redes LAN, si nos basamos en el modelo OSI definido por la Organización Internacional de Normalización en [23], abarcan el nivel de enlace y el nivel físico.



**Figura 6:** Niveles del modelo OSI.

**Fuente:** Elaboración propia.

Como se puede ver en la Figura 6 se definen para el IEEE 802 tres capas:

- **Logical Link Control (LCC):** se encarga de gestionar los enlaces lógicos del nivel de enlace y las interfaces comunes con el nivel de red.

- **Medium Access Control (MAC):** controla el acceso al medio físico en el caso en que este esté compartido por más nodos, buscando principalmente evitar las colisiones
- **Físico (PHY):** es el encargado de proporcionar una interfaz entre las estaciones y el medio de propagación.

Dentro de estos tres niveles del IEEE 802, la arquitectura lógica del estándar 802.11 está definida por el nivel MAC y PHY del modelo OSI.

Estos sistemas diseñados a niveles están basados en que cada nivel (N) proporciona servicios a su respectivo nivel superior (N+1). Estos niveles N, menos el físico, usan para comunicarse un servicio del nivel N-1 y es el nivel físico el que se comunica mediante el medio de transmisión con el nivel físico de otro nodo, de manera que, en todos los niveles menos el PHY, no hay tráfico de información de manera directa entre estos niveles en diferentes nodos, sino a través de los niveles inferiores. El bloque de datos que se envía en estas operaciones constituye la trama, en la que se representa la unidad informativa del nivel MAC, en el cual vienen encapsulados los datos de usuario del nivel superior.

Debido al aumento del número de APs WiFi que ha habido en los últimos años, la gestión de red se ha convertido en un problema muy serio. Este tipo de escenarios pueden ser desde aeropuertos o estaciones de tren hasta universidades y colegios. Por ello, el IEEE ha tenido como objetivo mejorar el rendimiento de la tecnología en estos escenarios, en donde son notorias las limitaciones de versiones anteriores del estándar.

Otra de las aplicaciones principales de WiFi, a parte de los dispositivos comerciales que buscan tener acceso a Internet, es el IoT. IoT, Internet of Things, se refiere a la interconexión digital de objetos cotidianos mediante Internet. El mercado de sensores de IoT se está centrando últimamente en el uso de WiFi como tecnología inalámbrica de interconexión, debido a la facilidad de implementación por lo utilizada que ha sido a lo largo de los años. No obstante, los estándares anteriores no están diseñados para aplicaciones de este tipo y tienen limitaciones en cuanto al consumo de energía y alcance de la comunicación para aplicaciones de tasas de datos bajas para estos sensores. Por ello, el estándar IEEE 802.11ax tiene el objetivo de hacer un uso eficiente de los recursos frecuenciales para poder integrar en una misma red múltiples dispositivos aumentando la vida de su batería.

El estándar IEEE 802.11ax introduce mejoras tanto en la capa MAC como en la PHY respecto a versiones anteriores con el objeto de mejorar el rendimiento de la tecnología.

## 5.2. PHY

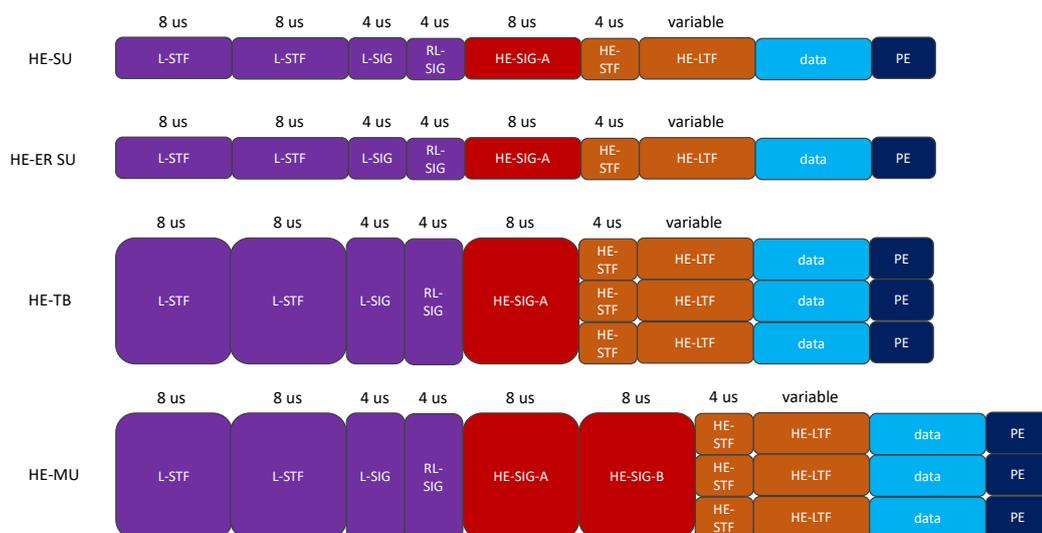
En el estándar IEEE 802.11ax se definen a nivel PHY nuevos tipos de paquetes, estos se conocen como *physical layer protocol data unit* (PPDU). En WiFi, debido a que es una tecnología inalámbrica, el comienzo de los paquetes está compuesto por un preámbulo y, por tanto, los PPDU están formados por el preámbulo más los datos. El comienzo de este debe ser igual en todos los estándares, para la compatibilidad entre ellos. Esta parte común, conocida como Legacy Preamble, se envía modulada mediante Phase-Shift Keying (BPSK), que es soportada por todos los dispositivos WiFi. Este preámbulo está formado por los campos Legacy-Short Training Field (L-STF), Legacy-Large Training Field (L-STF) y Legacy-Signal (L-SIG). Estas dos primeras están formadas por repeticiones de la misma secuencia de datos, conocidas por los receptores, que sirven para identificar

el paquete y obtener información acerca de la frecuencia, tiempo y hacer una estimación del canal. El campo L-SIG se utiliza para diferenciar el formato del paquete dentro de todos los definidos en el estándar:

- **Non-HT:** Este formato es el primero que se definió en el estándar, se utiliza en versiones anteriores a la IEEE 802.11n y en tramas de control.
- **HT:** High Throughput, este formato se definió en la versión IEEE 802.11n, a la vez que se utilizó por primera vez OFDM en WiFi.
- **VHT:** Very High Throughput, este formato se definió en la versión IEEE 802.11ac.
- **HE:** High Efficiency, este formato se definió en la versión IEEE 802.11ax, con el objetivo de dar soporte a las características multi usuario de OFDMA.

Cada formato, menos non-HT, añade preámbulos extra al Legacy antes de la trama MAC. En el caso del formato HE, este preámbulo adicional es diferente para los distintos tipos de paquete que se definen en el estándar. Estos tipos de paquete son los siguientes:

- **RL-SIG:** este campo se denomina repeated signal field, repite el contenido del campo Legacy L-SIG, sólo se utiliza en el formato HE.
- **HE-SU:** este formato se utiliza para enviar datos a un único usuario, utilizando el canal entero. Se permite utilizar tanto para Downlink (desde el AP hacia una STA) o Uplink (desde una STA hacia el AP).
- **HE-MU:** sirve para enviar datos a varios usuarios, compartiendo el canal. Solo el AP puede enviar tramas de este formato, Downlink, hacia varios usuarios.
- **HE-TB:** este es el formato de las tramas de respuesta (Trigger Frames), mencionados en la sección 5.3.2. Estas las envían las STAs hacia el AP, compartiendo el canal.
- **HE-ER SU:** Este formato está diseñado específicamente para comunicaciones con un mayor alcance, sobre todo para escenarios exteriores.



**Figura 7:** Formato de paquetes HE.  
Fuente: Elaboración propia.

El formato de estas tramas se puede ver en la Figura 7. Los diferentes campos de los preámbulos son los siguientes:

- **HE-SIG-A:** en este apartado se indica la información necesaria para decodificar el resto de la trama. Información como el intervalo de guarda (GI), identificador básico del servicio (BSS), ancho de banda o modulación (MCS) utilizada.
- **HE-SIG-B:** este campo solo se utiliza en las tramas del tipo HE-MU, en donde se indica la información acerca de la asignación de recursos de las STAs. Este proceso se explica en la sección 5.3 y en este campo se indica la información necesaria que debe saber cada estación para identificar la trama cuyo destinatario es ella misma.
- **HE-STF y HE-LTF:** estos dos campos tienen el mismo objetivo que el preámbulo Legacy además de facilitar al receptor la detección de trama y estimación de canal para operaciones multi usuario. Este preámbulo es transmitido utilizando los recursos asignados para cada usuario.

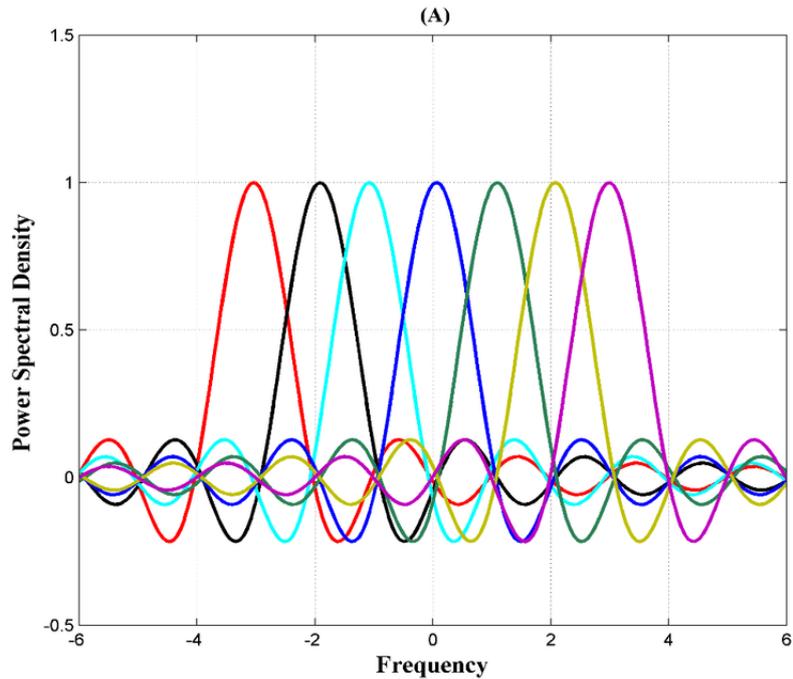
### 5.3. OFDMA

El método llamado acceso múltiple por división de frecuencias ortogonales (OFDMA, Orthogonal Frequency Division Multiple Access), es sin lugar a dudas la funcionalidad más destacada de WiFi 6 [24]. Antes del 802.11ax, las redes WLAN sólo soportaban un único dispositivo transmitiendo en cada instante, utilizando para ello la multiplexación por división de frecuencias ortogonales, OFDM [25].

#### 5.3.1. OFDM y OFDMA

Ambas son técnicas de acceso al medio multiportadora. Estas consisten en subdividir el ancho de banda del canal en un número de subcanales paralelos. Idealmente el ancho de cada subcanal está determinado para que no sean selectivos en frecuencia, es decir, que en dichos subcanales se suponga una atenuación plana para todas las frecuencias que los componen, esto supone una ventaja en el receptor ya que este puede compensar las atenuaciones de cada subcanal de manera individual.

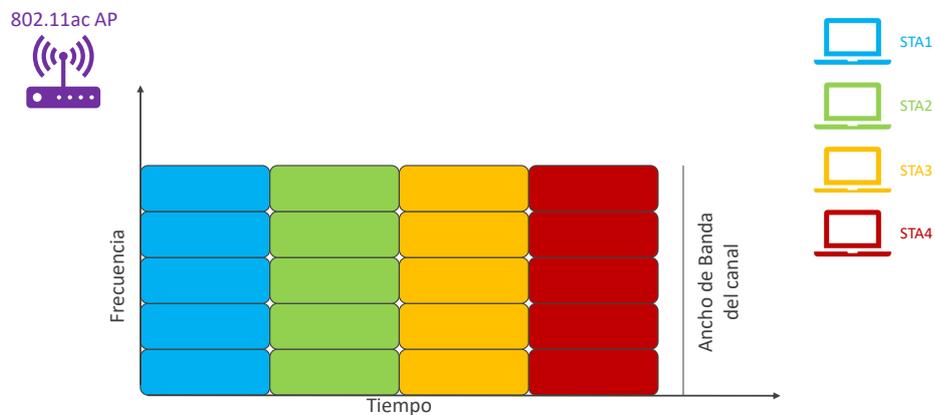
OFDM es un caso especial de transmisión multiportadora, en OFDM los subcanales paralelos se superponen los unos a los otros sin interferirse gracias a su ortogonalidad. Esto permite ahorrarse el uso de bandas de guardia (GPs) para separar los subcanales entre sí lo cual hace a OFDM una técnica espectral muy eficiente.



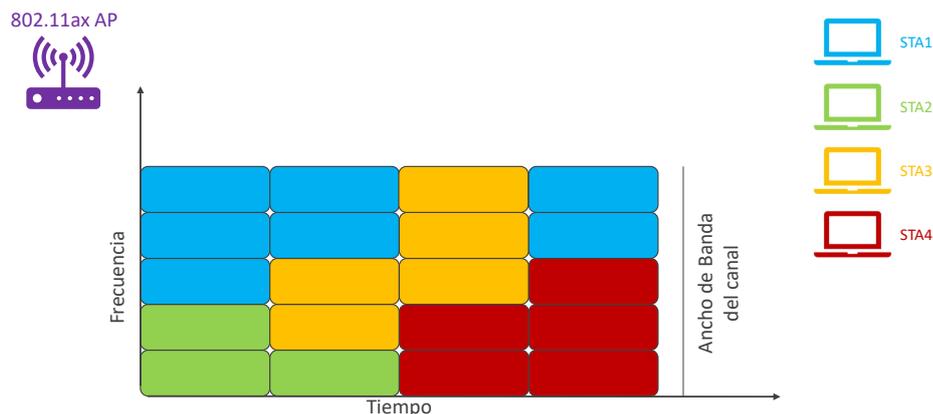
**Figura 8:** Representación de portadoras en OFDM.  
**Fuente:** [25]. Extraído del documento original.

La Figura 8 representa un símbolo OFDM, que se compone por toda la información de las portadoras. Otro concepto a tener en cuenta para la comprensión de estas técnicas es la Resource Unit (RU). El ancho de banda del canal se divide en RUs, y estas, son conjuntos de portadoras.

La diferencia entre OFDM y OFDMA es que en OFDMA cada RU es asignada a un usuario diferente, por tanto, el canal es utilizado simultáneamente por diferentes usuarios. En las figuras 9 y 10 se puede apreciar de manera gráfica esta diferencia. Cada rectángulo se representa una RU, y se aprecia como se reserva el canal entero para cada STA en distintos espacios temporales con OFDM. Con OFDMA en cambio, al separar el canal, se aprovecha de una mejor manera, ya que muchas veces los clientes no necesitan el canal entero para transmitir información.



**Figura 9:** Transmisión OFDM en el tiempo.  
**Fuente:** Elaboración propia.



**Figura 10:** Transmisión OFDMA en el tiempo.

**Fuente:** Elaboración propia.

De esta manera se permite que varios usuarios transmitan información en el mismo símbolo OFDM. Esto permite por ejemplo que, con 20 MHz de ancho de banda, se pueda dividir el canal para 9 usuarios diferentes. Por tanto, con WiFi 6, un AP podría estar enviando tramas pequeñas hacia 9 STAs a la vez. OFDMA es más eficiente al utilizar tramas cortas, ya que la transmisión simultánea, también llamada multiusuario (MU), recorta parte de las cabeceras MAC y PHY habituales ya que son compartidas por los distintos usuarios. De esta manera, se optimiza el uso de los recursos de la red, que es el objetivo principal de OFDMA.

No obstante, utilizar OFDMA no significa que siempre se esté repartiendo el canal. El AP, es capaz de asignar a una estación todo el ancho del canal si la situación de tráfico lo permite. Enviando para ello tramas de tipo único usuario (SU).

Las RU pueden estar formadas por un número variable de portadoras, este puede ir desde 26 hasta 996 según lo definido en el estándar IEEE 802.11ax [26]. La elección del tamaño de las RUs para cada usuario la realiza el AP en base a diferentes criterios acerca del estado de la red. De esta forma, en OFDMA, el canal se divide de una manera más eficiente. El número máximo de RUs por canal lo determina el ancho de banda del mismo. Teniendo en cuenta la separación entre ellas, las opciones permitidas se muestran en la Tabla 2:

RU	20 MHz	40 MHz	80 MHz	80 + 80 / 160 MHz
<b>26-tone RU</b>	9	18	37	74
<b>52-tone RU</b>	4	8	16	32
<b>106-tone RU</b>	2	4	8	16
<b>242-tone RU</b>	1	2	4	8
<b>484-tone RU</b>	0	1	2	4
<b>996-tone RU</b>	0	0	1	2
<b>2x996-tone RU</b>	0	0	0	1

**Tabla 2:** Tamaños de las RU en WiFi6.

**Fuente:** [26]. Datos obtenidos de la definición del estándar IEEE 802.11ax.

Otro cambio representativo en el estándar es el número de subportadoras. Estas se agrupan de manera diferente respecto al estándar 802.11ac en el espectro. En 802.11ac,

estaban separadas por 312.5 kHz, por lo que en 20 MHz cabían 64. En 802.11ax, en cambio, entran 4 veces más en 20 MHz, 256 en total, utilizando una separación frecuencial de 78.125 kHz. La duración de los símbolos también es 4 veces mayor en 802.11ax, pasa de ser de 3.2 a 12.8 us.

No obstante, es importante recordar que WiFi 6 sigue soportando OFDM. Se utiliza tanto para las tramas de control y organización como para comunicarse con dispositivos funcionando con estándares anteriores. OFDMA sólo se utiliza entre APs de WiFi 6 y STAs de WiFi 6.

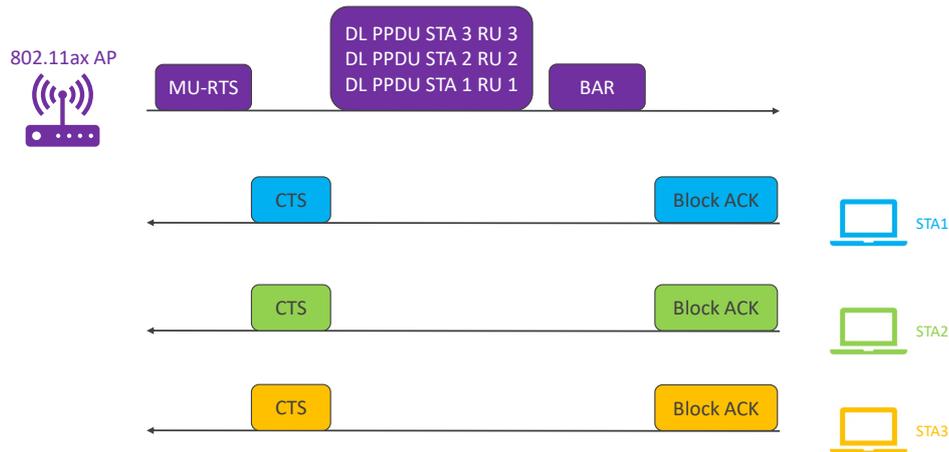
### **5.3.2. Trigger Frames**

Con el objetivo de detallar la información acerca de la asignación de recursos en comunicaciones multi usuario (MU), en el estándar se definen las tramas de tipo Trigger, Trigger Frames (TF). Diferentes tipos de tramas de control de 802.11 pueden funcionar como Trigger Frames en WiFi 6. Además de los Trigger básicos, se definen otros tipos de TF que, junto a la información acerca de la asignación de recursos, realizan funciones extra como petición de confirmación de paquetes (MU-BAR) o petición de reporte del estado del buffer (BSRP). Este tipo de tramas se envían mediante OFDM, por lo que no entran dentro de los nuevos tipos de PPDU detallados en el apartado 5.2.

En todas estas tramas se detalla la información acerca del uso de los recursos de canal en la capa MAC. Se informa acerca del reparto de las RUs, indicando tanto la información común para los usuarios acerca del número total de RUs que se van a asignar como la información de usuario acerca de que RU deberá utilizar cada uno. A parte de esta información, se indican las características en cuanto a modulación, codificación y hasta potencia que deberá utilizar cada usuario para la respuesta. Todos estos campos se muestran y estudian en el desarrollo del proyecto en la sección 7 para diferentes tipos de TF.

### **5.3.3. Downlink OFDMA**

La secuencia de intercambio de tramas en OFDMA varía en función de si se trata de Downlink o Uplink, es decir, de si es el AP el que tiene que transmitir datos a los clientes o al revés. Para DL OFDMA, el AP transmite información hacia varios usuarios a la vez, utilizando para cada uno de ellos una RU diferente. El AP debe esperar a que el canal esté libre para comenzar la secuencia para el envío de datos DL. Esta se define en el estándar de la siguiente manera:



**Figura 11:** Secuencia Downlink OFDMA .  
**Fuente:** Elaboración propia.

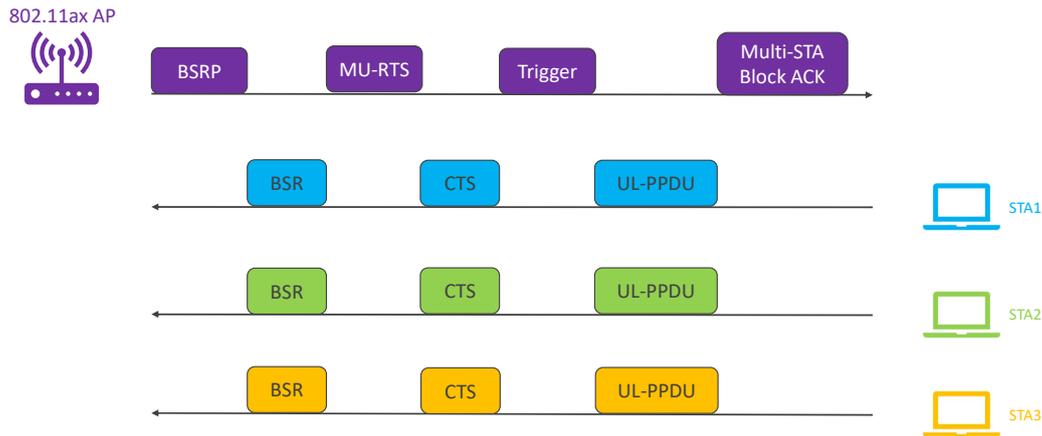
La primera trama que envía el AP es del tipo MU-RTS, que se trata de un tipo de Trigger Frame. Esta trama es enviada hacia todos los clientes y tiene el objetivo de solicitar el envío de datos. Como es un TF, los clientes deberán responder enviando la trama habitual de 802.11 CTS (Clear to Send) utilizando los recursos asignados por el AP.

Después de recibir los CTS, el AP, enviará mediante una trama MU los datos hacia los clientes, que irán separados en las RUs asignadas a cada uno de ellos. El preámbulo, la parte PHY del paquete completo, es común para todos ellos, y en este se indica qué RU deberá utilizar cada uno. Después de la trama MU, el AP envía un TF de tipo MU-BAR. Se trata de un paquete que solicita la confirmación de las tramas enviadas (Multi User Block ACK Request) y es común para todos los clientes. En la parte de información de usuario de la trama MAC, se indican los paquetes para los que se solicita la confirmación, además de los recursos asignados para la respuesta.

Por último, los clientes confirman los paquetes solicitados por el AP, utilizando la RU y propiedades asignadas por el AP en el último Trigger Frame. Este paquete es un Block ACK diferente a los estándares anteriores ya que es un PPDU de tipo HE-TRIG.

### 5.3.4. Uplink OFDMA

Para el envío de datos desde los clientes hacia el AP, el estándar define una secuencia más compleja, formada por tres Trigger Frames de tipos diferentes.



**Figura 12:** Secuencia Uplink OFDMA.  
**Fuente:** Elaboración propia.

Como se puede ver en la Figura 12 la secuencia para UL comienza con un TF de tipo Buffer Status Report Pull (BSRP) enviado por el AP. Este sirve para solicitar a todos los clientes información acerca de las tramas que tienen pendientes de enviar. Los clientes mediante un paquete de tipo HE-TRIG responden al AP a través de la RU asignada enviando la información solicitada en la trama MAC, Buffer Status Report (BSR).

En base a esta información, el AP decide la mejor manera para asignar las RUs del canal. Después se repite la misma secuencia de MU-RTS y CTS que en DL con el objetivo de reservar el canal para utilizar OFDMA.

Por último, el AP envía un TF básico dando permiso a los clientes para enviar los paquetes de datos pendientes a través de la RU asignada en este último TF básico. Después, el AP envía el mismo paquete a todos los clientes, Multi-STA Block ACK, el cual tiene un campo de información de usuario que indica que paquetes ha recibido correctamente el AP de cada cliente. Este último paquete, al igual que los TF, se envía utilizando todo el ancho del canal, mediante OFDM, pero con dirección MAC destino broadcast.

Tanto las secuencias DL como UL se estudian en este proyecto para un caso de funcionamiento real de WiFi 6 en la secciones 7.1 y 7.2.

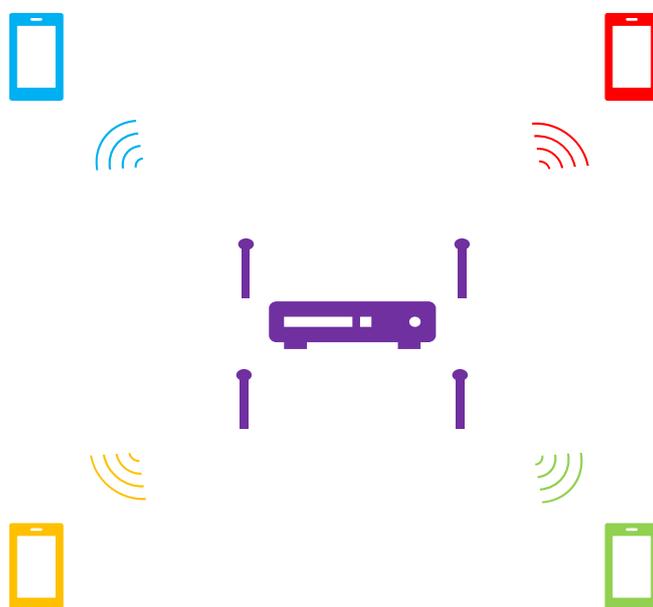
## 5.4. MU-MIMO

Los dispositivos WiFi 6 soportan también la tecnología multi-user multiple-input multiple-output (MU-MIMO). Esta tecnología permite a un router WiFi comunicarse con múltiples dispositivos de forma simultánea.

La tecnología multiple-input multiple-output (MIMO) [27] consiste en utilizar múltiples antenas para transmitir a través de varios flujos espaciales y de esta manera aprovecharse del fenómeno de propagación multipath. Este fenómeno es muy común en comunicaciones inalámbricas y consiste en que al receptor lleguen diferentes réplicas de la señal original rebotadas en obstáculos de alrededor del canal inalámbrico. MIMO permite a los dispositivos identificar los paths (caminos) que recorre la señal hacia el receptor y transmitir flujos de datos únicos a través de estos. Esta técnica se denomina SU MU-MIMO, en la que se utilizan varias antenas y flujos de datos para el mismo cliente.

Esta tecnología se contempló en la versión del estándar IEEE 802.11n, en donde se definía para un único usuario. En el IEEE 802.11ac se contempla, por primera vez, la posibilidad de que el AP transmita a través de un flujo de datos diferente para distintos clientes simultáneamente. Esto se denomina como DL MU-MIMO. Ya por último, en el estándar IEEE 802.11ax, a parte de mejorar las capacidades de esta última tecnología, se contempla el caso de UL MU-MIMO, en donde a cada cliente se le asigna un flujo espacial de datos por el que transmitir datos hacia el AP.

A diferencia de OFDMA, mediante MU-MIMO no se comparte el ancho de banda, sino que se aprovecha de que estos nuevos dispositivos tienen varias radios y antenas. El AP transmite diferentes flujos de datos hacia los clientes a través de diferentes flujos espaciales para cada usuario con el objetivo de mejorar el throughput de la red.



**Figura 13:** Ejemplo de MU-MIMO 4x4:4:4:4 entre un AP y 4 clientes.  
**Fuente:** Elaboración propia.

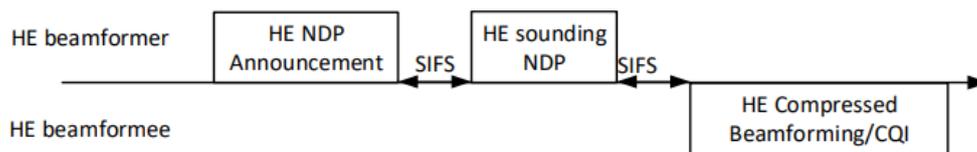
En la Figura 13 se muestra un caso en donde el AP transmite información a 4 usuarios a través de 4 flujos espaciales. Para describir las capacidades MU-MIMO de los dispositivos, se utiliza una nomenclatura de 5 números, en este caso se trata de 4x4:4:4:4. Los dos primeros valores indican el número de transmisores y receptores del sistema, el tercero el número de flujos de único usuario (SU) permitidos y el cuarto el número de flujos multiusuario (MU). El último representa el número de clientes MU-MIMO al mismo tiempo. Un AP con capacidad de 4x4:4:4:2 es capaz de destinar dos flujos de datos hacia un usuario 2x2:2 y otros dos hacia otro cliente 2x2:2.

#### 5.4.1. Sounding

Los routers de WiFi 6 son capaces de modificar el funcionamiento MU-MIMO en función del estado del canal de radio. Para conocer esto se realiza el proceso de sounding.

Sounding, sondeo en inglés, es un proceso que realiza el AP para estimar el estado del canal que está utilizando junto con una estación. Este proceso está definido en el estándar 802.11ac, el cual se permite hacer de manera unicast o multicast. Es decir, el AP puede hacer la estimación de canal hacia más de una estación a la vez, obteniendo diferentes resultados para cada una de ellas. No obstante, el estándar 802.11ax introduce cambios en el formato y secuencia de estas tramas, lo que permite conocer en menos tiempo el estado del canal y así mejorar el rendimiento de MU-MIMO. Estos se detallan a continuación.

En el estándar se define la siguiente secuencia para el tipo de sondeo single user (SU), en donde es el AP quien comienza a hacer la estimación:



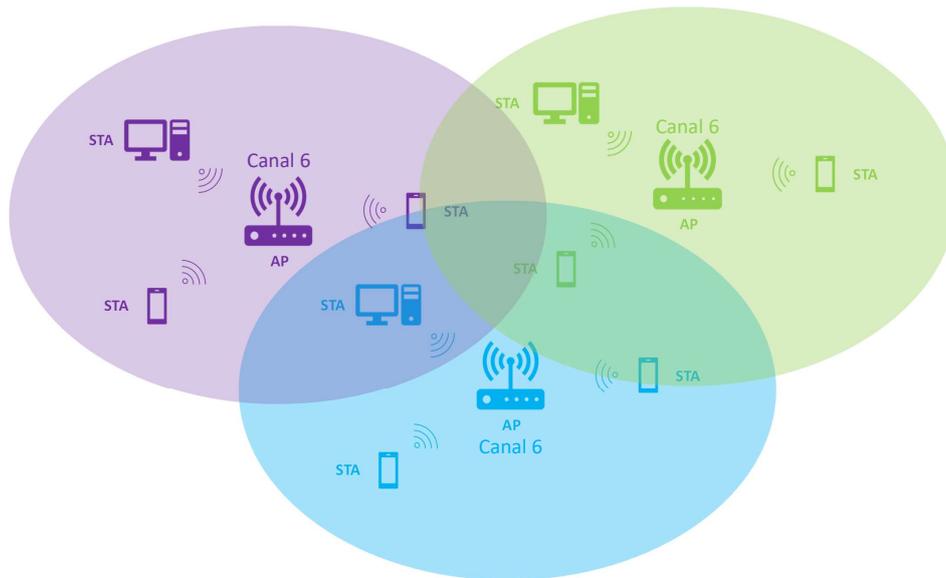
**Figura 14:** Esquema de la secuencia HE sounding en el estándar 802.11ax.

**Fuente:** [26]. Extraído de la definición del estándar.

En la Figura 14 HE beamformer representa al AP y HE beamformee a una de las estaciones. Las tramas que se muestran se han capturado en la red implementada y se describen en la sección 7.3.1. En el estándar se definen otros métodos de sondeo, mediante Trigger Frame y para varias estaciones a la vez. Sin embargo, debido a que estos no han sido capturados en la red implementada, no se analizan en esta sección.

## 5.5. BSS

WiFi, al ser una tecnología inalámbrica, utiliza como medio de transmisión el canal de radio, que es compartido por el resto de dispositivos del entorno. Esta tecnología utiliza el método *carrier sense with multiple access collision avoidance (CSMA/CA)* [28] para evitar la transmisión simultánea de diferentes dispositivos en el mismo canal. Este método sirve para evitar colisiones y hace que las radios WiFi no transmitan si a nivel PHY detectan un preámbulo 802.11 en un determinado umbral de señal. Este umbral se conoce como signal detect (SD), normalmente ubicado 4 dB por encima del ruido del canal. El problema de esta tecnología es que reduce los tiempos en los que los dispositivos pueden transmitir, obteniendo de esta manera latencias altas en entornos compartidos por más dispositivos. Este fenómeno se conoce como *contention overhead* y, en el caso que haya muchos APs y STAs en el mismo canal, se conoce como *overlapping basic service set (OBSS)*, tal y como se puede apreciar en la Figura 15.



**Figura 15:** OBSS, overlapping basic service set.  
**Fuente:** Elaboración propia.

Debido a este problema, en el estándar IEEE 802.11ax se define el método de *basic service set (BSS)* o *BSS Coloring*. Esto consiste en que cada AP es identificado por un color, y todas las tramas que manda tienen tanto en la parte PHY como MAC un campo especificando este color. Realmente es una secuencia de 6 bits, que permite diferenciar hasta 64 colores diferentes.

De esta manera, cada cliente que se quiera conectar a los APs en WiFi 6 tendrá que indicar en todas sus tramas este identificador. Así, cada nodo puede identificar rápidamente (tan sólo con detectar el preámbulo) si la trama que detecta tiene el mismo identificador BSS y, si es que no, descartarla. Los dispositivos WiFi con versiones anteriores del estándar no son capaces de detectar este campo.

Con esto lo que se consigue es detectar de una manera más rápida si el canal está ocupado por el alguien que no es de tu red, incluso si está utilizando el mismo canal.

Cuando un dispositivo quiere transmitir una trama y ha detectado un preámbulo, identifica primero el color BSS y, en caso que sea el mismo que el suyo (Intra-BSS), pospone la transmisión de la trama. En caso contrario (Inter-BSS), la trama no está en la misma red, por lo que puede no posponer la transmisión dependiendo de la configuración de red.

### 5.5.1. Spatial Reuse

Otra de las aplicaciones de BSS Coloring es conocida como *spatial reuse operation (SRO)*. Esta consiste en modificar los umbrales de recepción del dispositivo si se identifica que hay una transmisión OBSS. Esto se realiza aplicando la técnica *clear channel assessment (CCA)*. El objetivo es ignorar transmisiones de diferentes BSS y así no tener que esperar para transmitir.

CCA se utiliza en WiFi para examinar el canal radio. En función de la señal RF detectada un dispositivo puede posponer una transmisión. Para ello tiene dos umbrales: SD, para

detectar preámbulos 802.11 y *energy detect* (ED) para detectar cualquier señal. Ambos dan información acerca de si el canal está ocupado.

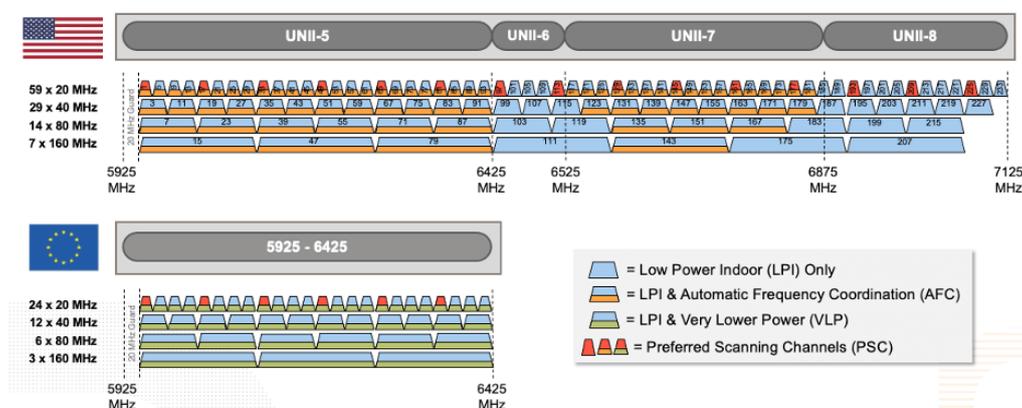
Basándose en los colores BSS de las tramas detectadas, los módulos WiFi 6 pueden utilizar CCA para adaptar el umbral SD, bajándolo para percibir sólo tramas Inter-BSS y manteniéndolo para señales Intra-BSS.

Mediante SRO y BSS se pretende conseguir reducir el problema de contención OBSS y latencia de la redes WiFi en un futuro donde la mayoría de los dispositivos soporten WiFi 6.

## 5.6. WiFi 6E

Una de las últimas novedades para el estándar IEEE 802.11 fue la decisión de permitir el uso de 1200 MHz en la banda de 6 GHz para esta tecnología en Estados Unidos por parte de la Comisión Federal de Comunicaciones (FCC). Esto ocurrió en 2020 y, en Europa, se ha aprobado el uso de esta parte del espectro a comienzos de año.

En Estados Unidos estos 1200 MHz, que van desde 5925 hasta 7125 MHz, contienen más del doble de canales que los que ya habían sumando las bandas de 2,4 y 5 GHz. En Europa, en cambio, tan sólo se han aprobado 500 MHz (5925-6425 MHz). Son, en el caso de Europa, un total de 24 canales de 20 MHz nuevos, lo que supone un salto importante para la tecnología. El uso de la banda de 6 GHz mediante al último estándar se conoce como la tecnología de WiFi 6E.



**Figura 16:** Canales en la banda de 6GHz en Estados Unidos y en Europa.

**Fuente:** [29]. Extraído de la página original.

### 5.6.1. Aumento de Espectro

Al tener más espectro disponible, se presentan nuevas oportunidades. Una de ellas es que se facilita el uso de canales grandes. El estándar introdujo canales de 80 y 160 MHz en la versión IEEE 802.11ac, la anterior a IEEE 802.11ax. No obstante, la mayoría de APs WiFi tan sólo utilizan canales de 20 o 40 MHz. Esto ocurre debido a que no hay espacio frecuencial para ello y es muy fácil encontrar situaciones de interferencia con otros canales en la banda de 5 GHz.

Por ello, se presentan situaciones en las que sí que se podría utilizar canales grandes con esta nueva banda. Por ejemplo, en Estados Unidos, ya que se disponen de 14 canales

de 80 MHz nuevos, se prevé el uso por defecto de estos canales en escenarios indoor controlados como oficinas.

Mediante la combinación de todas las bandas disponibles (especialmente las de 5GHz y 6 GHz) se mejorará el rendimiento de la tecnología en escenarios con mucha densidad de tráfico como aeropuertos, estadios o eventos grandes. Esto ocurre debido a que los APs WiFi 6E que hay en el mercado tienen 3 radios diferentes, una para cada banda, y pueden funcionar utilizando las 3 simultáneamente. La tecnología de WiFi 6 y 6E ha supuesto una mejora de la velocidad enorme en escenarios de este tipo. La empresa *Extreme Networks*, por ejemplo, ha realizado ya despliegues de redes WiFi 6 mediante sus propios APs en los mayores estadios del mundo [30], proporcionando así acceso a internet a los asistentes y otros servicios para los fans.

### 5.6.2. Ruido

Uno de los problemas del uso de canales más grandes en este nuevo espectro es el ruido. Al duplicar el canal, pasando de 20 a 40 MHz, el ruido plano aumenta 3 dB. Por tanto, la relación señal a ruido (SNR) es 3 dB peor. En el caso de 80 MHz son 6 dB menos, lo que podría ser peligroso para la señal y suponer que las radios WiFi deban bajar la modulación para poder transmitir con fiabilidad. Para las señales WiFi, la SNR por debajo de 25 dB empieza a ser considerada como mala y por debajo de 10 dB ya es difícil identificar la señal.

No obstante, para solucionar esto, la FCC ha redefinido las leyes de potencia transmitida. Para 6 GHz se limita la transmisión de las radios WiFi en términos de densidad espectral de potencia. Esto relaciona el ancho de banda (MHz) con potencia (dBm). Se permiten 5 dBm de Potencia Isotrópica Radiada Equivalente (PIRE) por cada 1 MHz en escenarios de baja potencia indoor (LPI), con un máximo de 30 dBm. El término PIRE es la potencia de transmisión de una radio más la ganancia de la antena menos las pérdidas del cable. Resumidamente, en la Tabla 3 se muestra como afecta esta nueva regla, en donde se consiguen obtener las mismas relaciones señal a ruido para los distintos anchos de banda.

Ancho de Banda	PSD	PIRE	Ruido	SNR
20 MHz	5 dBm/MHz	18 dBm		25 dBm
40 MHz	5 dBm/MHz	21 dBm	+3dBm	25 dBm
80 MHz	5 dBm/MHz	24 dBm	+6dBm	25 dBm
160 MHz	5 dBm/MHz	27 dBm	+9dBm	25 dBm

**Tabla 3:** Nueva normativa de la FCC acerca de la densidad espectral de potencia para diferentes tamaños de canal.

La fórmula para obtener las PIRE de la tabla anterior es la siguiente:

$$EIRP = PSD(dBm/MHz) + 10\log(BW(MHz))$$

### 5.6.3. Seguridad

Con el objetivo de aumentar la seguridad, para esta nueva tecnología WiFi 6E el estándar definió un nuevo protocolo de seguridad: WPA3. Este es requerido para todas las redes WiFi en la banda de 6 GHz.

### **5.6.3.1. WPA3**

Los protocolos de seguridad WPA, WiFi Protected Access, tienen el objetivo de que los datos dentro de una red WiFi sean privados y no interceptables por una tercera persona. WPA2, la anterior versión, ha estado activa durante 15 años y, para asegurar la invulnerabilidad de las redes WiFi, el estándar ha decidido renovarla.

La principal diferencia entre WPA3 y WPA2 es que se reemplaza la autenticación de tipo PSK (Preshared Key Authentication) por SAE (Simultaneous Authentication of Equals). Esta primera consiste en utilizar una clave secreta compartida con anterioridad entre las dos partes, en este caso el AP y el cliente, lo que es vulnerable a ataques de fuerza bruta utilizando diccionarios de contraseñas.

SAE, en cambio, tiene un proceso de autenticación en el que se produce un intercambio de mensajes entre el cliente y el AP en el que el cliente debe demostrar conocimiento acerca de la clave sin revelar la clave. A nivel de usuario, la contraseña de la red WiFi funciona de la misma manera que en WPA2, pero esta no es enviada desde el cliente hasta el AP durante el proceso de autenticación. El cifrado también aumenta, pasando de una clave de 128 a 192 bits.

### **5.6.3.2. OWE**

Otra característica nueva en la banda de 6 GHz es el protocolo Opportunistic Wireless Encryption (OWE). Este está diseñado para proteger la integridad de los datos de los dispositivos que se conectan a una red abierta, sin contraseña. Se basa en utilizar un cifrado único para cada cliente conectado al AP y de esta manera proteger el intercambio de datos. Este protocolo no es parte de WPA3, solo funciona en redes abiertas y no proporciona autenticación. Es requerido en la banda de 6 GHz, pero no en las de 2,4 y 5 GHz.

Estas dos características suponen una mejora de seguridad para el estándar. No obstante, no son implementadas en las bandas de 2,4 y 5 GHz, y los clientes que no son WiFi 6 no las soportan. Esto supone el uso de diferentes SSID para poder contemplar los diferentes niveles de seguridad en diferentes bandas. Esto se deba a que, si un AP quiere utilizar WPA3 y además dar servicio en la banda de 2.4 o 5 GHz, no tiene más remedio que utilizar varias SSID diferentes.

## 6. Plataforma de experimentación

El desarrollo de este proyecto tiene el objetivo de analizar y evaluar el estándar 802.11ax en la banda de 6 GHz. Para ello, primero es necesario implementar una red WiFi entre un AP y varios STAs.

### 6.1. Implementación de red

En esta sección se describen los pasos llevados a cabo para la implementación de la red WiFi 6E llevada a cabo en este proyecto. Mediante esta implementación se van a poder realizar el análisis del funcionamiento y la evaluación del rendimiento del estándar 802.11ax, objetivos principales del proyecto.

#### 6.1.1. Descripción del material proporcionado por la empresa

Para llevar a cabo la implementación de una red WiFi 6E, la empresa en donde se ha llevado a cabo este proyecto ha seleccionado para este proyecto los siguientes dispositivos:

- **GIGABYTE BRi7H-8550 [31]:** se tratan de unos miniPCs con un procesador Intel i7 para los cuales se pretende cargar un Sistema Operativo Linux y sustituir el módulo WiFi por uno WiFi 6E. En total se disponen de 4 modelos idénticos los cuales serán utilizados como STAs en la red implementada. Mediante el sistema operativo Linux, se pretende controlar las configuraciones específicas del driver WiFi de Intel (iw) así como diseñar un SW propio para el intercambio de tramas con el resto de dispositivos de la red.
- **Módulo Intel AX210 [32]:** se trata de uno de los módulos de comunicaciones comerciales más punteros del mercado. Es de los primeros que soportan WiFi 6E, con disponibilidad de las bandas de 2.4, 5 y 6 GHz y canales hasta 160 MHz. Característica imprescindible para este proyecto. Soporta las tecnologías de OFDMA, MU-MIMO con una antena 2x2 y velocidad máxima de hasta 2.4 Gbps.
- **Router Aruba 650 [33]:** es un Router WiFi 6E que dispone tres radios independientes para las bandas de 2.4, 5 y 6 GHz. Tiene una antena 4x4 en la banda de 6 GHz que es capaz de transmitir a una velocidad máxima de 4.8 Gbps. Soporta todas las tecnologías específicas del estándar IEEE 802.11ax como OFDMA (con una disponibilidad máxima de 37 RUs), TWT y MU-MIMO.

## 6.1.2. Implementación del módulo Intel WiFi 6E en miniPCs

En este apartado se van a explicar los pasos seguidos para poder utilizar el módulo Intel AX210 de WiFi 6E en los miniPCs de GIGABYTE. En total se ha seguido este proceso completo 4 veces, de manera que se ha logrado poner en marcha 4 STAs para la red WiFi implementada en este proyecto.

El primer paso de este proceso ha sido sustituir el Hardware. Para ello ha sido necesario abrir el miniPC, desmontar el módulo de red anterior y colocar la nueva tarjeta que se utiliza en este proyecto.

### 6.1.2.1. Sistema Operativo

El siguiente paso ha sido la instalación del sistema operativo en estos PCs. Se utiliza Linux, la última versión de Ubuntu, 20.04. Esto se realiza primero descargando un disco de Ubuntu (fichero ISO) desde la página oficial. Después, configurando un USB como unidad flash de arranque (bootable flash drive), que en este caso se ha utilizado la aplicación de Ubuntu Startup Disk Creator, para después cargar el disco descargado. Por último, se ha de conectar el USB al PC, abrir el menú de arranque, en la BIOS, y seleccionar la opción de disco duro USB ('hard disk/USB-HDD0').

Después del sistema operativo, es necesario configurar el kernel. En este proyecto, debido a la aplicación final, se ha utilizado una versión de baja latencia. Se trata de un kernel que aprovecha al máximo los recursos con el objetivo de reducir la latencia y el jitter del sistema. Los cambios respecto a los kernels habituales son la subida de la tasa de actualización (tick rate) de 250 a 1000 Hz y la modificación del sistema de prioridades de tareas a uno mucho más estricto. De esta manera, se permite interrumpir tareas de menor prioridad en mayor frecuencia que utilizando el kernel general, reduciendo así la latencia. Esto es útil para un posible desarrollo de un sistema de comunicaciones que utilice estos módulos, ya que el requisito de baja latencia es muy necesario.

Para la modificación del kernel, se han utilizado estos comandos:

```
~$ sudo apt-get install linux-headers-lowlatency
~$ sudo apt-get install linux-lowlatency
~$ sudo update-grub
```

Mediante estos comandos primero se descarga e instala la última versión del kernel de baja latencia disponible (en este caso el 5.17) y después se modifica de manera automática el GRUB, que es el sistema cargador de arranque, que permite elegir entre los sistemas operativos (y kernel) instalados. Después, es necesario resetear el PC.

Una vez instalado el sistema operativo y kernel, fue necesario actualizar los drivers de comunicaciones del PC, debido a que las últimas versiones del firmware de Intel no están incluidas en el sistema operativo, y son necesarias para el correcto funcionamiento del módulo. Para realizar este paso, tan solo es necesario comprobar cuál es el FW de Intel ya instalado, mediante el comando `modinfo iwlmwifi` desde el terminal, descargar el FW de Intel oficial que falta y copiarlo en el directorio `/lib/firmware`. Por último, solo queda verificar que se detectan correctamente estas últimas versiones del FW en el sistema.

### 6.1.2.2. Wpa\_Supplicant

Para poder conectarse a una red que utiliza la banda de 6 GHz, es necesario utilizar la herramienta Wpa\_supplicant. Esto ocurre debido a que en esta banda, es de obligado cumplimiento utilizar WPA3, y esta herramienta permite conectarse a una red inalámbrica utilizando las configuraciones de seguridad de WPA3. Wpa\_Supplicant implementa las negociaciones entre el cliente y autenticador WPA y el proceso de asociación IEEE 802.11.

Para utilizar esta herramienta se han llevado a cabo los siguientes pasos:

- Primero se ha instalado la última versión de wpa\_supplicant disponible desde el siguiente repositorio:

```
~$ git clone git://w1.fi/hostap.git
```

- Crear una configuración por defecto y compilar:

```
~$ cp defconfig .config
~$ make
~$ make install
```

- Copiar el programa al directorio /usr/sbin/ y configurarlo como ejecutable:

```
~$ cp -f hostap/wpa_supplicant/wpa_supplicant /usr/sbin/.
~$ chmod 755 /usr/sbin/wpa_supplicant
```

- Comprobar que se ha instalado una versión superior a la 2.11:

```
~$ wpa_supplicant -v
```

- Modificar el fichero de configuración de la herramienta para utilizar WPA3 e indicar la red y clave a la que se va a intentar conectar:

```
~$ vim /etc/wpa_supplicant/wpa_supplicant.conf
/*texto del fichero:*/
pmf=2
sae_pwe=1
network={
    scan_ssid=1
    ssid= "SSID de la red deseada"
    key_mgmt=SAE
    proto=RSN
    ieee80211w=2
    sae_password= "Contraseña de la red"
    pairwise=CCMP
    group=CCMP
}
```

- Una vez encendido el AP, el router de Aruba, se podrá intentar arrancar el programa para intentar conectarse como cliente (STA) utilizando las configuraciones indicadas y la interfaz de WiFi del pc:

```

~$ iwconfig /*para obtener el nombre de la interfaz*/
~$ wpa_supplicant -B -c /etc/wpa_supplicant/wpa_supplicant.conf
-i ${ifname}

```

- Comprobar que se ha conectado correctamente:

```

~$ route
~$ iwconfig
~$ ping 192.168.1.1

```

### 6.1.3. Router Aruba

Como se ha mencionado al comienzo de esta sección, por parte de la empresa Ikerlan se dispone de uno de los routers comerciales WiFi 6E más potentes del mercado para este proyecto, del fabricante Aruba.

Este router va a servir para crear una red WiFi en la banda de 6 GHz sobre la que se van a conectar los clientes implementados mediante los miniPCs GIGABYTE en la sección 6.1.2. Para el diseño de la red y la modificación de configuraciones acerca de esta, el fabricante proporciona dos opciones: la interfaz web habitual de un router o el terminal de comandos Aruba CLI. Ambas se acceden mediante el puerto Ethernet del router.

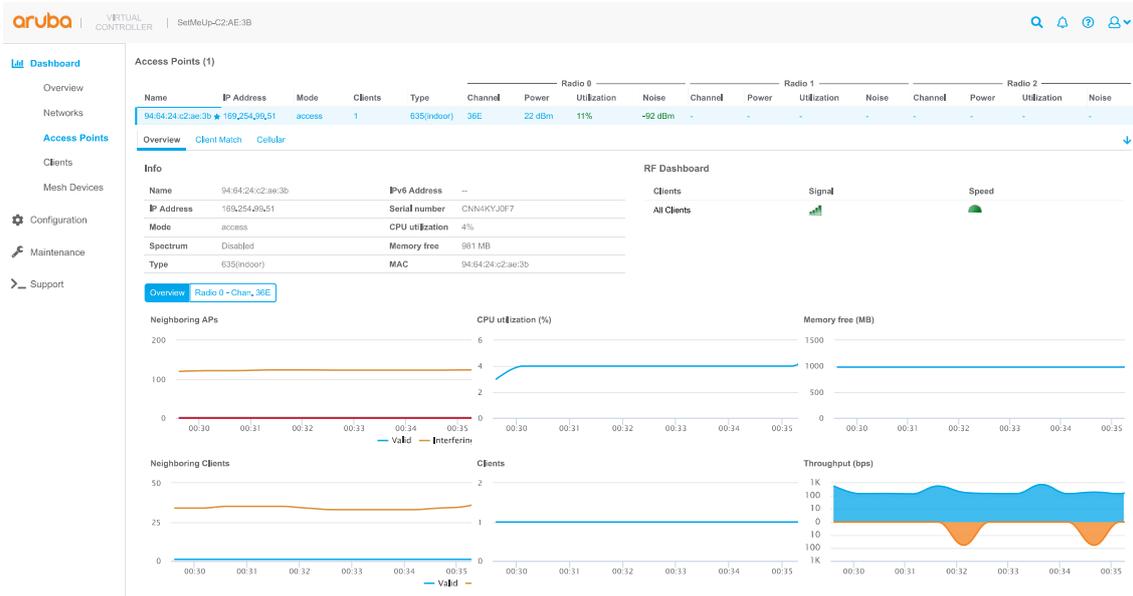


Figura 17: Captura de la interfaz Web de configuración del router Aruba.

La interfaz web sirve para diseñar la red WiFi y definir configuraciones básicas como SSID, contraseña, frecuencia, potencia, ... También, como se muestra en la Figura 17 se proporcionan datos como el número de clientes, tasa de datos de cada uno, direcciones IP o ruido. Información clave para comprobar el estado de la red al mismo tiempo que se realizan las evaluaciones de este proyecto.

Mediante el terminal de comandos en línea en cambio, se permiten modificar configuraciones más complejas acerca del router y de la tecnología IEEE 802.11ax. Estas

configuraciones son como el uso de canales de 160 MHz, OFDMA, MU-MIMO, modulación máxima (MCS). También se permite activar y desactivar el uso de las tecnologías del estándar IEEE 802.11ax (HE), que se utiliza en este proyecto para la evaluación de los estándares realizada en la sección 8.3.2.

```

169.254.99.51 - PuTTY
login as: admin
admin@169.254.99.51's password:

show tech-support and show tech-support supplemental are the two most useful out
puts to collect for any kind of troubleshooting session.

94:64:24:c2:ae:3b# config
We now support CLI commit model, please type "commit apply" for configuration to
take effect.
94:64:24:c2:ae:3b (config) # wlan ssid-profile TEST_MARTIN
94:64:24:c2:ae:3b (SSID Profile "TEST_MARTIN") # high-efficiency-enable
94:64:24:c2:ae:3b (SSID Profile "TEST_MARTIN") # end
94:64:24:c2:ae:3b# commit apply
committing configuration...
configuration committed.
94:64:24:c2:ae:3b# █
  
```

**Figura 18:** Captura del terminal de comandos Aruba CLI desactivando el uso de HE en la red.

En la Figura 18 se muestra el proceso que se sigue para desactivar esta opción. Mediante este terminal se proporcionan estadísticas en tiempo real más complejas que en la interfaz web acerca los clientes y del propio router. Se proporcionan datos acerca de las tramas enviadas y recibidas, el número de retransmisiones que hay en la red, la modulación que se está utilizando, al utilizar OFDMA las RUs que se están asignando y otras informaciones útiles para comprobar el correcto funcionamiento de la red.

```

169.254.99.51 - PuTTY
94:64:24:c2:ae:3b# show stats client 80:45:dd:05:4a:29

Name:
IP Address::169.254.99.3
MAC Address::80:45:dd:05:4a:29
AP IP Address::169.254.99.51
Access Point::94:64:24:c2:ae:3b
Channel::149
ESSID::TEST_MARTIN
Connection Time::3m:17s
Type::2-HE
OS::NOFP
CM::Disabled
stats_debug::0/0
stats_cleared::No
Swarm Client Stats
-----
Timestamp  Signal (dB)  Frames [In] (fps)  Frames [Out] (fps)  Throughput [In] (bps)  Throughput [Out] (bps)  Frames [Retries In] (fps)
-----
02:04:02   43           624                1268                489738              489788                37
3
02:03:32   43           612                1243                480132              480054                38
3
02:03:01   43           715                1450                559708              559682                40
3
02:02:31   43           748                1517                587540              587564                44
3
02:02:00   42           524                1065                410330              410437                39
  
```

**Figura 19:** Captura del terminal de comandos Aruba CLI mostrando estadísticas de uno de los clientes de la red.

En la Figura 19 se muestra un ejemplo de unas de las opciones sobre las estadísticas que proporciona este terminal para cada cliente, seleccionado mediante la dirección

MAC. En este caso se da información acerca de tramas recibidas y enviadas, retransmisiones y tasa de datos en un instante temporal (timestamp).

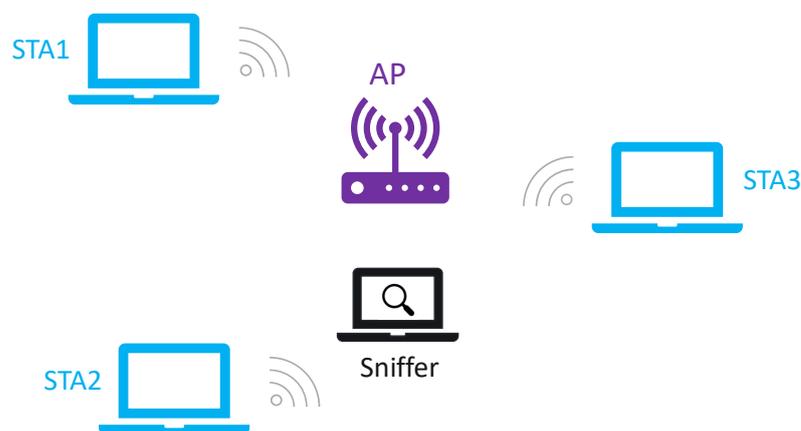
Toda esta información se ha utilizado a la hora de realizar las evaluaciones de este proyecto. Se han combinado ambos métodos de configuración del router para verificar el correcto funcionamiento de cada una de las evaluaciones.

## 6.2. Setup de red para análisis

En este apartado se va a explicar el Setup utilizado para poder realizar el análisis de las características del estándar 802.11ax, descrito en el apartado 7.

La red implementada consta de 3 STAs y un AP. Los STA son los miniPCs de GIGABYTE y el AP es el router de Aruba mencionados en la sección 6.1.

El AP se configura en la banda de 6 GHz y los 3 STAs se conectan a él utilizando la herramienta wpa\_supplicant.



**Figura 20:** Setup de red para el análisis del estándar IEEE 802.11ax.

**Fuente:** Elaboración propia.

### 6.2.1. Sniffer

Además de los 3 miniPCs utilizados como clientes, se ha utilizado un cuarto en modo sniffer para poder obtener la información de las tramas intercambiadas entre los STAs y el AP. Para ello, se ha utilizado la herramienta air-crack de Linux, configurándola en el canal utilizado por el AP. Para la interpretación de las tramas capturadas se ha utilizado Wireshark. Air-crack configura la interfaz de red inalámbrica del PC en modo monitor, lo que permite leer las tramas que captura el módulo de WiFi. De las tramas capturadas solo puede interpretar la parte PHY y MAC, debido a que los datos de las tramas MAC están encriptadas.

No.	Source	Destination	PPDU	Info
93	ArubaaHe_c2:ae:3b	IntelCor_00:22:e2	HE_MU	QoS Data, SN=1496, FN=0, Flags=.p....F.C
94	ArubaaHe_c2:ae:3b	IntelCor_00:22:e2	HE_MU	QoS Data, SN=1497, FN=0, Flags=.p....F.C
95	ArubaaHe_c2:ae:3b	IntelCor_00:22:e2	HE_MU	QoS Data, SN=1498, FN=0, Flags=.p....F.C
96	ArubaaHe_c2:ae:3b	IntelCor_00:22:e2	HE_MU	QoS Data, SN=1499, FN=0, Flags=.p....F.C
97	ArubaaHe_aa:e3:d0 ...	Broadcast (ff:ff:ff...		Trigger MU-BAR, Flags=.....C
98	IntelCor_00:22:e2 ...	ArubaaHe_aa:e3:d0 (...	HE_TRIG	802.11 Block Ack, Flags=.....C
99	IntelCor_04:b2:58 ...	ArubaaHe_aa:e3:d0 (...		Request-to-send, Flags=.....C
1...		IntelCor_04:b2:58 (...		Clear-to-send, Flags=.....C
1...	IntelCor_04:b2:58	ArubaaHe_c2:ae:3b	HE_SU	QoS Data, SN=136, FN=0, Flags=.p....TC
1...	IntelCor_04:b2:58	ArubaaHe_c2:ae:3b	HE_SU	QoS Data, SN=138, FN=0, Flags=.p....TC
1...	IntelCor_04:b2:58	ArubaaHe_c2:ae:3b	HE_SU	QoS Data, SN=139, FN=0, Flags=.p....TC
1...	ArubaaHe_aa:e3:d0 ...	IntelCor_04:b2:58 (...		802.11 Block Ack, Flags=.....C

**Figura 21:** Captura de Wireshark mostrando los paquetes capturados por el sniffer.

Como se puede apreciar en la Figura 21, el sniffer sólo captura tramas del protocolo 802.11, debido a que los niveles superiores están encriptados. El router utilizado en el desarrollo aparece en las capturas como ArubaaHe, y las STAs como IntelCor, diferenciadas por la dirección MAC.

Otro aspecto para considerar del capturador de tramas, son las tramas multiuser que se utilizan en el estándar. Estas tramas, tienen un preámbulo y nivel físico común para todos los usuarios a los que está dirigida la trama, pero, tienen una parte MAC diferente. Esto ocurre debido a que el estándar, permite utilizar este tipo de tramas para enviar a cada destino una información diferente. Estas tramas no se pueden capturar completas utilizando el sniffer, debido a que todavía el software del analizador de paquetes no es capaz de mostrar varios payload en paralelo. Por ello, se consigue obtener la información MAC de las tramas de manera individual, seleccionando para cada AID por separado. Esto se realiza mediante un comando echo en el terminal de Linux:

```
~$ echo 0 00:00:00:00:00:00 >
/sys/kernel/debug/iwlwifi/0000:03:00.0/iwlmvm/he_sniffer_params
```

El primer parámetro es el número de asociación (AID) y el segundo será la dirección MAC del AP. De esta manera se está indicando al sniffer el número de asociación específico sobre el que tiene que capturar los paquetes, lo que este utiliza para extraer la información del preámbulo HE-SIG-B (que es común para todos los usuarios) que indica la RU asignada para esta asociación. Antes de este comando, es necesario dar permisos de ejecución y escritura en el directorio de las configuraciones del sniffer:

```
~$ sudo chmod a+rx /sys/kernel/debug
~$ sudo chmod a+rx /sys/kernel/debug/iwlwifi
~$ sudo chmod a+rx /sys/kernel/debug/iwlwifi/0000:03:00.0
~$ sudo chmod a+rx /sys/kernel/debug/iwlwifi/0000:03:00.0/iwlmvm
~$ sudo chmod a+rxw
/sys/kernel/debug/iwlwifi/0000:03:00.0/iwlmvm/he_sniffer_params
```

### 6.2.2. VSA-Matlab

Otra herramienta clave para este análisis ha sido el VSA (Vector Signal Analyzer). Este aparato, del fabricante Keysight y ya incluido en el equipo de Ikerlan, sirve para medir las

señales de RF. Es un instrumento muy potente que realiza las tareas de medida y caracterización que realiza un analizador de espectros habitual implementando funciones digitales de demodulación extra. Se puede utilizar para mostrar simultáneamente el análisis de frecuencia y tiempo. En este caso se ha utilizado de manera mayoritaria para obtener información sobre la modulación I/Q.



**Figura 22:** Captura del tráfico en el dominio temporal realizando un análisis real y complejo del VSA.

Mediante este instrumento se han conseguido capturar las tramas de la red y obtenido los bits de estas a través de la señal eléctrica. Para ello, el propio VSA permite guardar la parte real e imaginaria de la modulación I/Q en un determinado espacio temporal en formato .mat.

Los ficheros que genera el VSA después se cargan en Matlab y utilizando el Toolbox WLAN se han logrado interpretar las tramas capturadas, tanto a nivel PHY como MAC.

Mediante el diseño de un pequeño script que utiliza las funciones del Toolbox WLAN *wlanSampleRate*, *resample* y *WaveformAnalyzer* se han logrado demodular las cabeceras de las tramas capturadas por el VSA. Una captura de la situación de intercambio de tramas en la red como podría como la del ejemplo de la Figura 22 se logra resumir en MATLAB de la siguiente manera:

```
>> m_resumen
```

Summary of ↵

the Detected Packets

detSummary =

56×9 table

Number (samples)	Format MAC Contents	PHY Status RMS EVM (dB)	Power (dBm) Max EVM (dB)	CFO (Hz)	Offset ↵
1	"Non-HT"	"Success"	-30.81	-2807.2	↵
21599	"RTS"	-17.299	-3.265		
2	"Non-HT"	"Success"	-44.71	-5252.2	↵
22497	"CTS"	-12.509	-4.0932		
3	"HE-SU"	"Success"	-44.85	-1887.8	↵
23379	"Unknown"	-25.654	-6.3417		
4	"Non-HT"	"Success"	-44.69	-4548.1	↵
25429	"ACK"	-12.202	-5.2278		
5	"HE-MU"	"Success"	-46.88	-3624.9	↵
28842	"Unknown"	-20.386	-1.0459		
6	"Non-HT"	"Success"	-44.46	-3452.2	↵
34531	"Trigger"	-12.216	-3.008		
7	"HE-TB"	"Unsupported format"	-30.51	-4712.7	↵
35971	"Unknown"	NaN	NaN		
8	"Non-HT"	"Success"	-27.72	-3754.7	↵
42325	"RTS"	-15.668	-8.8657		
9	"Non-HT"	"Success"	-44.79	-4244.4	↵
43223	"CTS"	-11.342	-3.6651		
10	"HE-SU"	"Success"	-41.42	-4921.5	↵
44100	"Unknown"	-22.765	-9.5414		
11	"Non-HT"	"Success"	-44.85	-6787	↵
46150	"ACK"	-12.106	-4.4024		
12	"Non-HT"	"Success"	-31.44	-89427	↵
52489	"RTS"	-17.176	-11.68		
13	"Non-HT"	"Success"	-44.7	-4677.7	↵
53387	"CTS"	-11.988	-1.9884		
14	"HE-SU"	"Success"	-34.71	-88326	↵
54265	"Unknown"	-28.512	-13.58		
15	"Non-HT"	"Success"	-44.76	-5364.2	↵
56863	"ACK"	-12.866	-6.5719		
16	"Non-HT"	"Success"	-33.02	-7863.5	↵
60761	"RTS"	-17.542	-9.9146		
17	"Non-HT"	"Success"	-44.73	-3323.4	↵
61659	"CTS"	-11.776	-5.3601		
18	"HE-SU"	"Success"	-44.04	-7101.5	↵
62541	"Unknown"	-22.82	-3.2846		
19	"Non-HT"	"Success"	-44.81	-4064.3	↵
64590	"ACK"	-12.02	-2.7461		
20	"HE-MU"	"Success"	-44.3	-4603.6	↵
83682	"Unknown"	-20.112	-2.149		
21	"Non-HT"	"Success"	-44.42	-4190.7	↵

**Figura 23:** Resumen de las tramas identificadas por la función *WaveformAnalyzer* del ToolBox WLAN de MATLAB.

En la Figura 23 se muestra el resumen del resultado de la función *WaveformAnalyzer*, en donde se consiguen identificar las cabeceras MAC y PHY de las tramas en la red. De esta manera, se logra capturar el tráfico de la red de una manera similar al Sniffer. Utilizando el resto de funciones de este Toolbox se pueden demodular estas tramas completas, pero, debido a que el Sniffer de la sección 6.2.1 es más rápido y sencillo de utilizar se ha priorizado su uso frente a la demodulación de las tramas.

También, el VSA se ha usado para analizar el espectro de la red, limitado hasta 6 GHz. Por tanto, tan sólo se logran capturar señales de los primeros canales de la banda de 6 GHz.

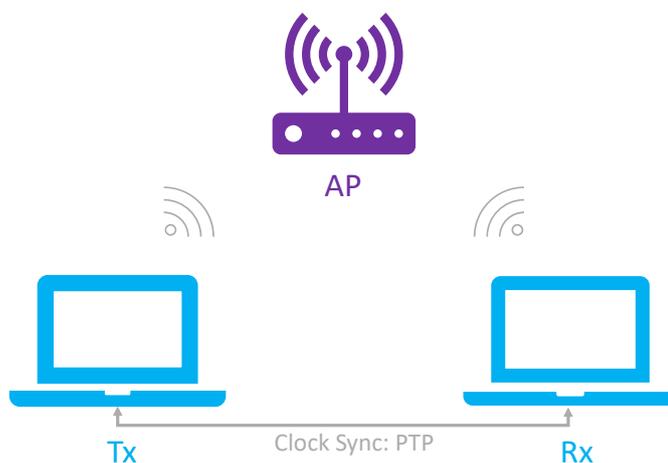
### 6.3. Desarrollo para evaluación de latencia

En este apartado se va a describir la parte del desarrollo del proyecto orientada a la evaluación de la latencia.

Se han desarrollado dos Setups para la medida de latencias sobre la red WiFi 6E implementada en este proyecto. Como se ha comentado anteriormente, se disponen de 4 STAs y un AP en esta red, y las medidas de latencia se realizarán entre dos de las STAs de la red.

La diferencia principal entre estos dos Setups es que en uno los paquetes se envían desde un STA hacia otra, pasando por el AP, y en el otro los paquetes se transmiten directamente desde el AP hacia una STA. Es decir, en el primero hay dos saltos inalámbricos y en el segundo solo uno.

#### 6.3.1. Setup 1

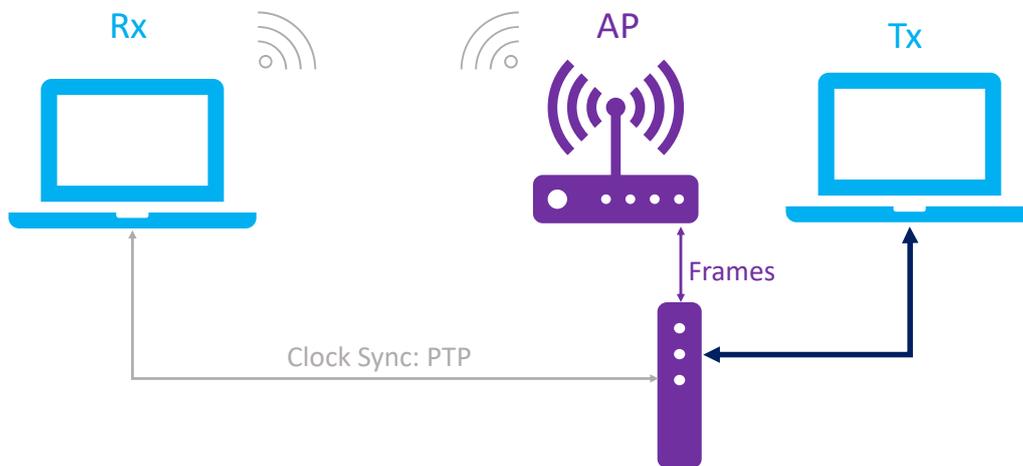


**Figura 24:** Setup 1 para la medida de latencia entre TX y RX.

**Fuente:** Elaboración propia.

En este Setup, las dos estaciones están conectadas a la red del AP. Las tramas sobre las que se van a medir la latencia van desde una estación hacia el AP, y, desde el AP hacia la segunda STA de manera inalámbrica. Los relojes de las estaciones están sincronizados mediante Ethernet. Esto se detalla en la sección 6.3.5.

### 6.3.2. Setup 2



**Figura 25:** Setup 2 para la medida de latencia entre Tx y Rx.  
**Fuente:** Elaboración propia.

En este segundo Setup tan sólo un miniPC está conectado a la red WiFi del AP. Las tramas siguen el camino desde el TX hacia el RX, salen por la interfaz Ethernet del TX, con dirección IP destino la del RX, ya que esta interfaz tiene una IP dentro del rango de direcciones del AP. Después, atraviesan un switch y son transmitidas por la interfaz inalámbrica del AP. Por último, se reciben en la interfaz inalámbrica del RX. Los relojes de TX y RX están sincronizados mediante PTP, utilizando para ello el switch que interconecta tanto el proceso del intercambio de tramas como el de sincronización.

Para la comprobación de que las tramas siguen el camino inalámbrico y no el *fácil* mediante el cable, se utiliza la herramienta *Wavemon* de Linux, que da información en tiempo real acerca de las tramas que envía y recibe el driver WiFi. Y, en caso de que se envíen por cable, no se contabilizan en esta herramienta.

```
user@user-nodo4: ~  
-Interface-  
wlp2s0 (IEEE 802.11), phy 0, reg: n/a, SSID: TEST_MARTIN  
-Levels-  
link quality: 97% (68/70)  
=====  
signal level: -42 dBm (0,06 uW)  
=====  
-Statistics-  
RX: 1.717.868 (2,30 GiB), drop: 2.149 (0,1%)  
TX: 27 (4,27 KiB)  
-Info-  
mode: Managed, connected to: 94:64:24:AA:E3:C0, time: 36:19m, inactive: 0,0s  
freq: 5975 MHz, channel: 195 (width: 20 MHz)  
rx rate: 143.3 Mbit/s, tx rate: 58.5 Mbit/s  
beacons: 19.534, lost: 9, avg sig: -42 dBm, interval: 0,1s, DTIM: 1  
power mgt: off, tx-power: 22 dBm (158,49 mW)  
retry: short long limit 1, rts/cts: off, frag: off  
-Network-  
wlp2s0 (UP RUNNING BROADCAST MULTICAST)  
mac: 80:45:DD:00:2C:2F, qlen: 1000  
ip: 169.254.99.5/16
```

Figura 26: Captura de la herramienta Wavemon mostrando información acerca del driver WiFi.

Como se aprecia en la Figura 26, esta herramienta también da información acerca del nivel de la señal WiFi, características de la red, y propiedades del propio driver.

### 6.3.3. Iperf

Para realizar las medidas de latencia se ha probado a utilizar la herramienta Iperf, en donde una estación actuará como cliente y una como servidor. Para el cálculo de la latencia, el cliente envía un paquete UDP indicando el timestamp de salida. El servidor resta el tiempo de recepción del paquete a este timestamp y así obtiene el resultado de latencia final.

Por ello, se han realizado estas pruebas enviando tramas pequeñas, de 100 Bytes, para que esta incertidumbre no sea determinante en las medidas. También, al utilizar tramas más pequeñas, el aumento del ancho de banda del canal afecta más a la latencia final. Esto ocurre debido a que al aumentar el ancho de banda se disminuye la MCS utilizada, siempre y cuando se envíe la misma información, y esto es más representativo en tramas cortas, ya que la modulación se reduce de una manera más significativa, lo que mejora la robustez de la comunicación, reduciendo el número de retransmisiones.

La herramienta Iperf da como resultado un histograma de latencias, en el que se muestra el número de paquetes que han tenido una latencia comprendida en un rango de 10 us. Este resultado solo se obtiene si se utiliza UDP, por lo que en estas pruebas se va a utilizar este protocolo.

El comando para el servidor es el siguiente:

```
~$ iperf -s -u -e -i 1 -udp-histogram=10u,1000 -l 100
```

Para el cliente:

```
~$ iperf -c IP_SERVER -u -t 600 -l 100
```

Mediante la opción `-t` se especifica el tiempo de la prueba en segundos, que en este caso se realizan pruebas de 10 minutos. La opción `-l` es el tamaño en bytes de las tramas que se envían para medir la latencia.

El cliente enviará tramas hacia el servidor mediante Socket UDP, por lo que es necesario especificar la dirección IP del servidor. Antes es necesario asignar una dirección IP dentro de la red del AP a cada uno de los dispositivos en la interfaz inalámbrica, que se realiza utilizando `ifconfig`, en este caso:

```
#sudo ifconfig wlan0 169.254.99.1
```

Wlan0 es la interfaz inalámbrica del PC, y se le asigna la dirección IP 169.254.99.1 que está dentro del rango de direcciones del AP(169.254.99.51/24).

#### 6.3.4. Software

Uno de los problemas que tiene utilizar una aplicación como Iperf son las incertidumbres que genera. No se puede conocer con exactitud el intervalo entre los paquetes transmitidos, ya que varía a lo largo del transcurso de la prueba. Tampoco se puede enviar un paquete concreto, y de esta manera en recepción poder observar si ha sido retransmitido o perdido.

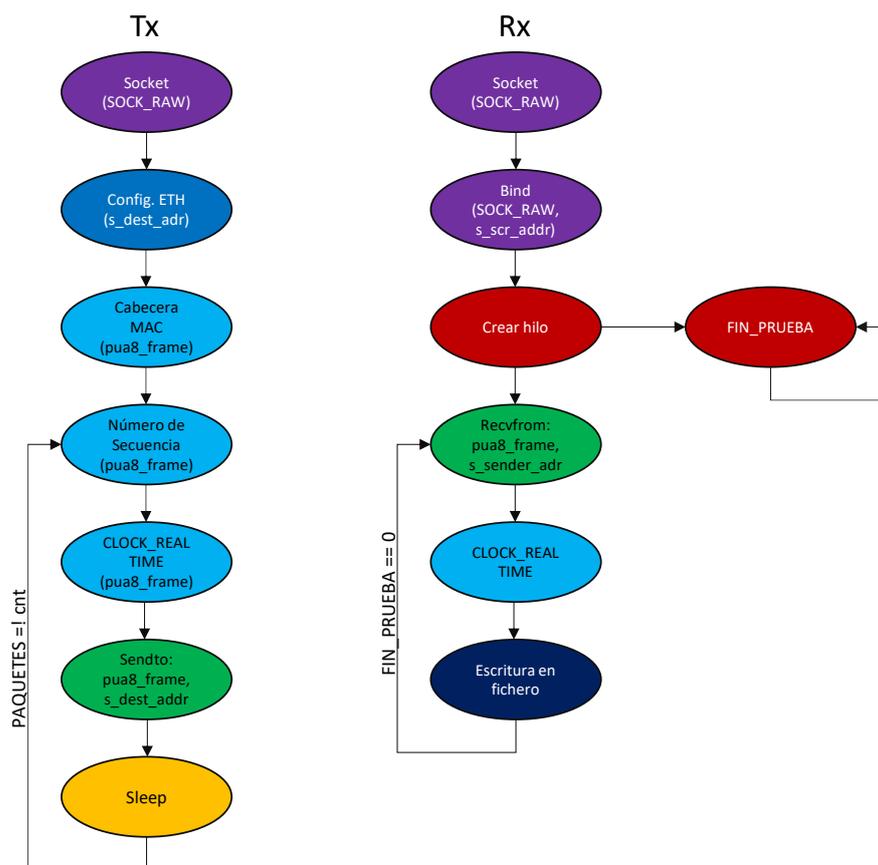
Como se pretende hacer un análisis más en detalle de lo que ocurre en la red: en qué momento se pierden los paquetes, si al perderse un paquete llegan con latencias altas los siguientes, o casuísticas de este estilo, se ha desarrollado un SW propio basado en *Sockets Raw* para poder controlar con exactitud el intervalo de transmisión de todos los paquetes como el contenido y tamaño de los mismos. De esta manera, se puede obtener información detallada de cómo ha sido el transcurso de una prueba además de evaluar la fiabilidad de la misma.

Además, mediante Iperf no se obtiene información clara acerca de los paquetes fuera del rango del histograma, para los que se obtiene un resultado como Outliers, aquellos paquetes cuya latencia es muy superior a la del resto.

A continuación se detalla el funcionamiento del programa, así como la manera en la que se realiza el cálculo de latencia y se podrá obtener la tasa de paquetes erróneos.

Para la esta medida de latencia entre el transmisor y el receptor de los Setups descritos en la sección 6.3.1 se han diseñado dos programas basados en Sockets, uno para el receptor y otro para el transmisor. Socket es un concepto abstracto por el que dos procesos pueden intercambiar un flujo de datos y además establece el mecanismo para la entrega de datos que provienen de la tarjeta de red a los procesos apropiados.

El diagrama de flujo que siguen estos programas se muestra en la Figura 27.



**Figura 27:** Diagrama de flujo de los programas diseñados.  
**Fuente:** Elaboración propia.

Para este diseño se han utilizado *Sockets Raw*, esto quiere decir que no se utiliza ningún protocolo por encima de Ethernet, no se utilizan los protocolos de transporte TCP ni UDP de los Sockets habituales, como utiliza la herramienta Iperf. De esta manera tampoco se crea una comunicación orientada a conexión, por lo que no es necesario conectar el cliente al servidor antes del envío de datos.

Al usar *Sockets Raw*, desde el SW diseñado, se pasan los paquetes definidos sin ningún tipo de modificación hacia el driver. Para ello, desde el código se definen las direcciones origen y destino MAC y la interfaz del ordenador que se va a utilizar para la transmisión. Para ello se utilizan Sockets de tipo *SOCK\_RAW* y el dominio *AF\_PACKET*, que especifica la familia de protocolos de la comunicación, en este caso de bajo nivel. Se indica la opción de *ETH\_P\_ALL* para aceptar paquetes de todos los protocolos.

### 6.3.4.1. Transmisor

En el transmisor, antes de comenzar con el diagrama de flujo, se definen primero las siguientes características:

```

#define NIC_NAME "wlp2s0" //interfaz por la que enviar los paquetes
#define PAQUETES 1000000 //número de paquetes de la prueba
#define ETH_DATA_LEN_MARTIN 100 //tamaño de los paquetes
  
```

```

/*Direccion MAC del TX*/
static uint8_t gu8a_src_mac[6] = {0x80, 0x45, 0xdd, 0x00, 0x2c, 0x2f};
/*Direccion MAC del RX*/
static uint8_t gu8a_dest_mac[6] = {0x80, 0x45, 0xdd, 0x00, 0x22, 0xe3};

```

El primer paso del diagrama es crear el Socket con las configuraciones mencionadas:

```

s32_sock = socket (AF_PACKET, SOCK_RAW, htons (ETH_P_ALL));
if( -1 == s32_sock )
{
    perror ("Could not create the socket");
    goto LABEL_CLEAN_EXIT;
}

printf ("Socket created\n");

```

El segundo es configurar la dirección Ethernet de la trama que se va a enviar, sólo es necesario configurar la interfaz y la dirección MAC ya que no se usan protocolos por encima:

```

/*no se usan protocolos por encima de ETH*/
s_dest_addr.sll_family = AF_PACKET;
s_dest_addr.sll_protocol = htons(ETH_P_ALL);
/*Interfaz del dispositivo*/
s_dest_addr.sll_ifindex = get_nic_index ((uint8_t *) NIC_NAME);
s_dest_addr.sll_hatype = ARPHRD_ETHER;
s_dest_addr.sll_pkttype = PACKET_OTHERHOST;
s_dest_addr.sll_halen = ETH_ALEN;
/*Comienzo MAC*/
s_dest_addr.sll_addr[0] = gu8a_dest_mac[0];
s_dest_addr.sll_addr[1] = gu8a_dest_mac[1];
s_dest_addr.sll_addr[2] = gu8a_dest_mac[2];
s_dest_addr.sll_addr[3] = gu8a_dest_mac[3];
s_dest_addr.sll_addr[4] = gu8a_dest_mac[4];
s_dest_addr.sll_addr[5] = gu8a_dest_mac[5];
/*Fin MAC*/

```

Después, se configura la cabecera de la trama que se va a enviar, se añaden primero las direcciones origen y destino MAC:

```

/*Cabeceras*/
(void) memcpy (pu8a_frame, gu8a_dest_mac, ETH_ALEN);
(void) memcpy (pu8a_frame+ETH_ALEN, gu8a_src_mac, ETH_ALEN);

```

Más tarde comienza el bucle, que finalizará cuando se envíe el número de paquetes totales definido. El primer paso del bucle es sacar el tiempo del clock de Linux y escribirlo en la trama que se va a mandar además del contador de número de secuencia:

```

while( cnt < PAQUETES )
{
    (void) memset (&pu8a_data[u16_data_off],
        '\0', ETH_DATA_LEN_MARTIN);

```

```

clock_gettime(CLOCK_REALTIME, &logtime);

long int * ntiempo_32 = &logtime.tv_nsec;
uint8_t* ntiempo_8 = (uint8_t*)ntiempo_32;
pu8a_data[0] = *(ntiempo_8);
pu8a_data[1] = *(ntiempo_8+1);
pu8a_data[2] = *(ntiempo_8+2);
pu8a_data[3] = *(ntiempo_8+3);

long int * tiempo_32 = &logtime.tv_sec;
uint8_t* tiempo_8 = (uint8_t*)tiempo_32;
pu8a_data[4] = *(tiempo_8);
pu8a_data[5] = *(tiempo_8+1);
pu8a_data[6] = *(tiempo_8+2);
pu8a_data[7] = *(tiempo_8+3);
pu8a_data[8] = *(tiempo_8+4);

long int * cnt_32 = &cnt;
uint8_t* cnt_8 = (uint8_t*)cnt_32;
pu8a_data[9] = *(cnt_8);
pu8a_data[10] = *(cnt_8+1);
pu8a_data[11] = *(cnt_8+2);
pu8a_data[12] = *(cnt_8+3);
pu8a_data[13] = *(cnt_8+4);

```

Después de esto, la trama ya lista para enviar se envía de manera no bloqueante utilizando las configuraciones definidas:

```

s32_res = sendto (s32_sock, pu8a_frame, ETH_FRAME_LEN, 0,
(struct sockaddr*)&s_dest_addr, sizeof(s_dest_addr));
if( -1 == s32_res )
{
    perror ("Socket send failed"); goto LABEL_CLEAN_EXIT;
}

```

Por último, se bloquea el programa durante el intervalo definido, y se incrementa el contador de número de secuencia, después el programa vuelve al comienzo del bucle:

```

usleep(INTERVALO);
cnt++;

```

### 6.3.4.2. Receptor

Al igual que en el transmisor, en el receptor, antes del comienzo del programa se definen las siguientes configuraciones:

```

#define NIC_NAME "wlp2s0"
#define PAQUETES 1000000
#define ETH_DATA_LEN_MARTIN 100
char *nombre_fichero = "LatWiFi6E_mcs7_oneway/Canal36E_escenario1_100bytes.dat";

```

El primer paso es crear el socket:

```

s32_sock = socket (AF_PACKET, SOCK_RAW, htons (ETH_P_ALL));
if( -1 == s32_sock )
{
perror ("Could not create the socket");
goto LABEL_CLEAN_EXIT;
}

```

Después, configurar la dirección Ethernet de origen junto a la interfaz del dispositivo para poder realizar un bind del Socket:

```

(void) memset (&s_src_addr, 0, sizeof (s_src_addr));
s_src_addr.sll_family = AF_PACKET; /*we don't use a protocol above ethernet layer, just ethernet layer*/
s_src_addr.sll_protocol = htons(ETH_P_ALL);
s_src_addr.sll_ifindex = get_nic_index ((uint8_t *) NIC_NAME);
s_src_addr.sll_hatype = ARPHRD_ETHER;
s_src_addr.sll_pkttype = PACKET_HOST;
s_src_addr.sll_halen = ETH_ALEN;

s32_res = bind (s32_sock, (struct sockaddr *) &s_src_addr,
sizeof(s_src_addr));
if( -1 == s32_res )
{
    perror ("Could not bind to the socket");
    goto LABEL_CLEAN_EXIT;
}
printf ("Socket bind successful\n");

```

El siguiente paso es abrir el fichero y crear el hilo encargado de controlar el final de la prueba:

```

fichero = fopen(nombre_fichero,"w");
if(fichero == NULL)
{
printf("\n Error al abrir el fichero");
}
else
{
printf("\n Fichero %s abierto",nombre_fichero);
}
printf("\nRecibiendo %d paquetes por %s\n",PAQUETES,NIC_NAME);
logtime.tv_sec = 999999999;
err = pthread_create(&(tid),NULL,&final_prueba,NULL);
if(err ==0){ printf ("hilo creado\n");
}
else
{
printf ("hilo error\n");
return 0;
}

```

El hilo encargado de controlar el final de la prueba comprueba cada segundo si se ha recibido el último paquete, en caso de que este se perdiera, se tiene en cuenta el último tiempo de transmisión recibido:

```

void * final_prueba(void *arg){ printf("HILO\n");
while(1)
{
    clock_gettime(CLOCK_REALTIME, &tiempo_actual);
    if(tiempo_actual.tv_sec > logtime.tv_sec + 10)
    {
        fin_prueba = 0;
    }
    else if(tx_sec == PAQUETES -1)
    {
        fin_prueba = 0;
    }
    sleep(1);
}
}

```

Una vez teniendo el hilo funcionando en paralelo, comienza el bucle del main, en donde primero se inicializa la dirección del posible transmisor y se utiliza la función `recvfrom` para recibir tramas. También, se guarda el tiempo de recepción en el momento justo después de recibir la trama:

```

while(fin_prueba)
{
    struct sockaddr_ll s_sender_addr;
    socklen_t u32_sender_addr_len = sizeof (s_sender_addr);
    (void) memset (&s_sender_addr, 0, sizeof (s_sender_addr));
    s32_res = recvfrom (s32_sock, pu8a_frame,
    ETH_FRAME_LEN, 0, (struct sockaddr *) &s_sender_addr, &u32_sender_addr_len);
    clock_gettime(CLOCK_REALTIME, &logtime);
    if( -1 == s32_res )
    {
        perror ("Socket receive failed");
        break;
    }
    else if( s32_res < 0 )
    {
        perror ("Socket receive, error ");
    }
}

```

Una vez recibida una trama sin errores, se parsean sus datos y se separan el número de secuencia, tiempo de tx en segundos y parte decimal en nanosegundos:

```

cnt++;
for( u16_i=0; u16_i<ETH_DATA_LEN_MARTIN; u16_i++ )
{
    data8[u16_i] = pu8a_frame[u16_data_off+u16_i];
}
long int * tx_ntime_32 = &tx_ntime;
uint8_t* tx_ntime_8 = (uint8_t*)tx_ntime_32;
*(tx_ntime_8) = data8[0];
*(tx_ntime_8+1) = data8[1];
*(tx_ntime_8+2) = data8[2];
*(tx_ntime_8+3) = data8[3];

long int * tx_time_32 = &tx_time;
uint8_t* tx_time_8 = (uint8_t*)tx_time_32;

```

```

*(tx_time_8) = data8[4];
*(tx_time_8+1) = data8[5];
*(tx_time_8+2) = data8[6];
*(tx_time_8+3) = data8[7];
*(tx_time_8+4) = data8[8];

long int * tx_sec_32 = &tx_sec;
uint8_t* tx_sec_8 = (uint8_t*)tx_sec_32;
*(tx_sec_8) = data8[9];
*(tx_sec_8+1) = data8[10];
*(tx_sec_8+2) = data8[11];
*(tx_sec_8+3) = data8[12];
*(tx_sec_8+4) = data8[13];

```

Por último, se calcula la latencia, comprobando que estén dentro del mismo segundo (número entero) y junto al número de secuencia se escribe en el fichero antes creado:

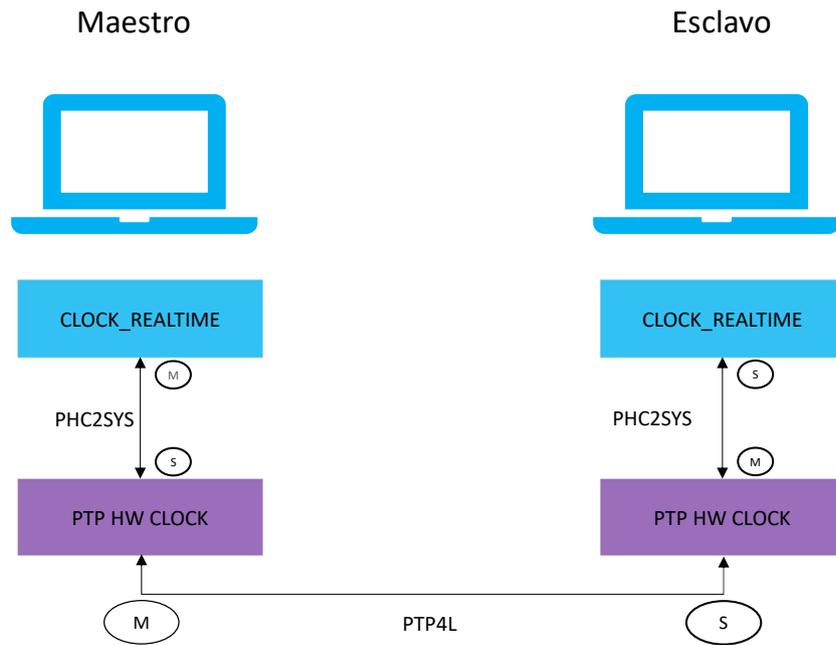
```

results = logtime.tv_sec - tx_time; if (results>0)
{
logtime.tv_nsec = logtime.tv_nsec + 1000000000;
}
resultn = logtime.tv_nsec - tx_ntime;
//Escritura del número de secuencia + latencia en el fichero
fprintf(fichero, "%ld %d\n",tx_sec, resultn);

```

### 6.3.5. Sincronización

Para la correcta medida de latencia entre el Transmisor y el Receptor es necesario que los relojes de ambos dispositivos estén sincronizados. Estos relojes, en Linux tienen el nombre de *CLOCK\_REALTIME* y son el reloj del sistema general. Para sincronizarlos, se ha utilizado *precision time protocol, PTP*. Este protocolo se define en el estándar IEEE 1588 [34] para la sincronización de reloj de alta precisión. En Linux, se utilizan las aplicaciones *phc2sys* y *ptp4l* basadas en este protocolo para llevar a cabo la sincronización.



**Figura 28:** Diagrama de la sincronización de relojes implementada mediante PTP.  
**Fuente:** Elaboración propia.

Como se muestra en la Figura 28, se llevan a cabo en total 3 procesos para sincronización. Primero, a más bajo nivel, es necesario sincronizar los relojes de las interfaces Ethernet de los PCs, esto se realiza mediante *ptp4l*, configurando un dispositivo como maestro y otro como esclavo:

```

user@user-nodo3:~$ sudo ptp4l -i enp0s31f6 -m -2 -H
ptp4l[628548.992]: selected /dev/ptp0 as PTP clock
ptp4l[628549.056]: port 1: INITIALIZING to LISTENING on INIT_COMPLETE
ptp4l[628549.056]: port 0: INITIALIZING to LISTENING on INIT_COMPLETE
ptp4l[628556.829]: port 1: LISTENING to MASTER on ANNOUNCE_RECEIPT_TIMEOUT_EXPIRES
ptp4l[628556.829]: selected local clock b42e99.ffff.72d8bf as best master
ptp4l[628556.829]: assuming the grand master role

```

**Figura 29:** Salida del comando *ptp4l* para el maestro.

```
user@user-nodo4:~$ sudo ptp4l -i enp0s31f6 -m -2 -H -s
ptp4l[1137280.944]: selected /dev/ptp0 as PTP clock
ptp4l[1137281.018]: port 1: INITIALIZING to LISTENING on INIT_COMPLETE
ptp4l[1137281.018]: port 0: INITIALIZING to LISTENING on INIT_COMPLETE
ptp4l[1137284.602]: port 1: new foreign master b42e99.ffffe.72d8bf-1
ptp4l[1137288.642]: selected local clock b42e99.ffffe.ddd373 as best master
ptp4l[1137290.603]: selected best master clock b42e99.ffffe.72d8bf
ptp4l[1137290.603]: port 1: LISTENING to UNCALIBRATED on RS_SLAVE
ptp4l[1137292.602]: master offset 196163819 s0 freq -3871 path delay 1017
2
ptp4l[1137293.602]: master offset 196164988 s1 freq -2702 path delay 1017
2
ptp4l[1137294.603]: master offset 192 s2 freq -2510 path delay 1017
2
ptp4l[1137294.603]: port 1: UNCALIBRATED to SLAVE on MASTER_CLOCK_SELECTED
ptp4l[1137295.603]: master offset 384 s2 freq -2261 path delay 1017
2
ptp4l[1137296.603]: master offset -7096 s2 freq -9625 path delay 1023
0
ptp4l[1137297.603]: master offset 7112 s2 freq +2454 path delay 1017
2
ptp4l[1137298.603]: master offset -4758 s2 freq -7283 path delay 1023
0
ptp4l[1137299.603]: master offset 6951 s2 freq +2999 path delay 1023
0
```

Figura 30: Salida del comando ptp4l para el esclavo.

Se han utilizado los siguientes parámetros de la aplicación:

- **-i**: interfaz del dispositivo, en este caso la de Ethernet.
- **-H**: timestamping mediante Hardware, es decir, que el tiempo de transmisión de los paquetes se obtenga a través del reloj del Driver Ethernet, y no a través del Software del sistema operativo. Lo que supone mayor precisión para la sincronización, ya que se está más cerca de donde salen los paquetes.
- **-2**: protocolo de red, en este caso IEEE 802.3, Ethernet.
- **-s**: en el caso del esclavo, esta opción permite forzar a que el dispositivo funcione como esclavo.
- **m**: mostrar mensajes de salida por pantalla.

Como se aprecia en la Figura 29, se obtiene una precisión menor que 1 us, ya que la columna de master offset indica la diferencia en nanosegundos entre el reloj del maestro y del esclavo.

Una vez sincronizados los relojes PTP, para sincronizar los del sistema operativo se siguen los siguientes procesos mediante phc2sys, cada uno en un dispositivo. Esta aplicación sincroniza dos relojes de un mismo dispositivo, en este caso se pretenden sincronizar el reloj HW de PTP (/dev/ptp0) con el del sistema (CLOCKREALTIME).

```

user@user-nodo3:~$ sudo phc2sys -c /dev/ptp0 -s CLOCK_REALTIME -w -E linreg -R 100
-m
[sudo] password for user:
phc2sys[628654.957]: /dev/ptp0 sys offset -175861385 s0 freq -113 delay 5000
phc2sys[628654.967]: /dev/ptp0 sys offset -175861400 s0 freq -113 delay 4875
phc2sys[628654.977]: /dev/ptp0 sys offset -175861349 s0 freq -113 delay 4875
phc2sys[628654.988]: /dev/ptp0 sys offset -175861383 s1 freq +1632 delay 4875
phc2sys[628654.998]: /dev/ptp0 sys offset 3 s2 freq +1032 delay 4750
phc2sys[628655.008]: /dev/ptp0 sys offset -29 s2 freq -3621 delay 5000
phc2sys[628655.019]: /dev/ptp0 sys offset -56 s2 freq -5639 delay 5000
phc2sys[628655.029]: /dev/ptp0 sys offset 392 s2 freq +34650 delay 3000
phc2sys[628655.039]: /dev/ptp0 sys offset 40 s2 freq +19854 delay 3125
phc2sys[628655.049]: /dev/ptp0 sys offset -428 s2 freq -23279 delay 4000
phc2sys[628655.060]: /dev/ptp0 sys offset -296 s2 freq -42378 delay 4751
phc2sys[628655.070]: /dev/ptp0 sys offset 93 s2 freq -8899 delay 5000
phc2sys[628655.080]: /dev/ptp0 sys offset 180 s2 freq +10449 delay 5000
phc2sys[628655.091]: /dev/ptp0 sys offset 94 s2 freq +6880 delay 5000
phc2sys[628655.101]: /dev/ptp0 sys offset 55 s2 freq +6250 delay 4875
phc2sys[628655.111]: /dev/ptp0 sys offset -151 s2 freq -12403 delay 5000
phc2sys[628655.122]: /dev/ptp0 sys offset -73 s2 freq -12554 delay 5250
phc2sys[628655.132]: /dev/ptp0 sys offset 160 s2 freq +9612 delay 4750

```

Figura 31: Salida del comando phc2sys para el maestro.

En el dispositivo maestro se escoge como maestro el reloj del sistema y como esclavo el de PTP. Así al terminar todos los procesos el reloj maestro de phc2sys es el que indicará el tiempo al resto. Se han utilizado los siguientes parámetros de la aplicación:

- **-s:** reloj maestro.
- **-c:** reloj esclavo sincronización, ya que se está más cerca de donde salen los paquetes.
- **-E:** utilizar regresión lineal.
- **-R:** frecuencia en Hz de actualización del reloj. En este caso se realizará cada 10 ms (100Hz).
- **-m:** mostrar mensajes por pantalla.

```

user@user-nodo4:~$ sudo phc2sys -s /dev/ptp0 -c CLOCK_REALTIME -w -E linreg -m -R 100
phc2sys[1137419.339]: CLOCK_REALTIME phc offset -16 s0 freq -2140 delay 2191
phc2sys[1137419.349]: CLOCK_REALTIME phc offset 160 s0 freq -2140 delay 2540
phc2sys[1137419.359]: CLOCK_REALTIME phc offset 74 s0 freq -2140 delay 2769
phc2sys[1137419.370]: CLOCK_REALTIME phc offset 81 s2 freq +10396 delay 2911
phc2sys[1137419.380]: CLOCK_REALTIME phc offset 13 s2 freq -4805 delay 2896
phc2sys[1137419.390]: CLOCK_REALTIME phc offset 58 s2 freq +6966 delay 2777
phc2sys[1137419.400]: CLOCK_REALTIME phc offset -41 s2 freq -2308 delay 2913
phc2sys[1137419.411]: CLOCK_REALTIME phc offset -2 s2 freq -1729 delay 2885
phc2sys[1137419.421]: CLOCK_REALTIME phc offset 2 s2 freq -381 delay 2883
phc2sys[1137419.431]: CLOCK_REALTIME phc offset -96 s2 freq -9454 delay 2841

```

Figura 32: Salida del comando phc2sys para el esclavo.

En el caso del dispositivo esclavo se indica lo mismo cambiando el maestro por el esclavo. Como se aprecia en las Figuras 32 y 31 se consigue una sincronización de menos de 100 ns, indicada en el campo de offset. Por tanto, en total se consigue que el reloj de Linux del maestro esté sincronizado con menos de 2 us del esclavo, lo que es aceptable si las latencias son en el orden de los milisegundos.

### 6.3.6. Procesamiento de resultados mediante MATLAB:

Como se ha mencionado en la sección 6.3.4 desde la aplicación desarrollada se guardan en un fichero el número de secuencia y latencia (en nanosegundos) de todos los paquetes recibidos en el receptor. Estos datos, se cargan fácilmente en MATLAB mediante la función *load*, ya que el fichero creado por SW es en formato .dat. Antes del análisis, se eliminan los paquetes cuyo número de secuencia no entra dentro del rango de los paquetes enviados, para evitar mal interpretaciones.

Para la correcta interpretación de las latencias obtenidas se han realizado dos análisis.

#### 6.3.6.1. Histograma

El primero sirve para poder ver a simple vista las latencias de la gran mayoría de paquetes de una prueba. Se representa el histograma de latencias, recortado para poder apreciar los intervalos con más paquetes. Mediante este análisis, se puede apreciar si la latencia de la red es constante lo que ocurre si todos los paquetes llegan en un intervalo pequeño de tiempo. Por tanto, se puede apreciar a simple vista el determinismo del sistema. También sirve por si no lo es, lo que ocurre cuando en vez de obtener picos en intervalos pequeños se obtienen cantidades de paquetes con latencias similares a lo largo del tiempo.

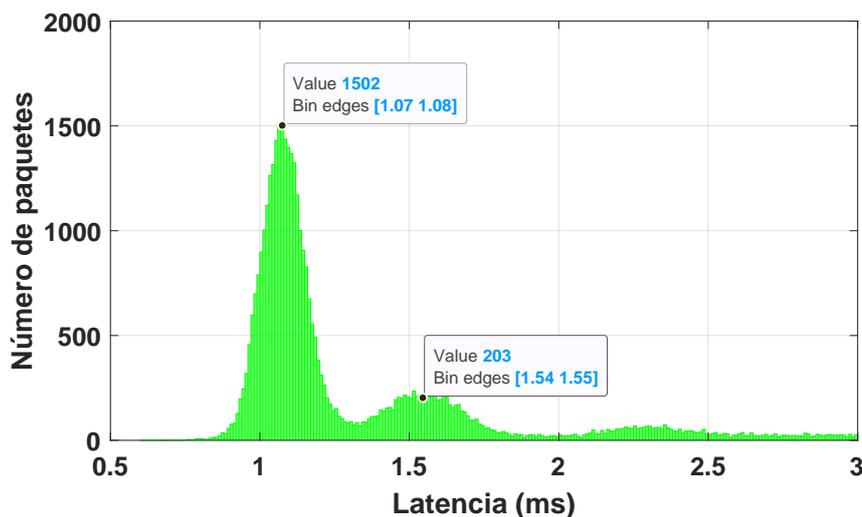


Figura 33: Ejemplo de la representación gráfica de un histograma de latencias.

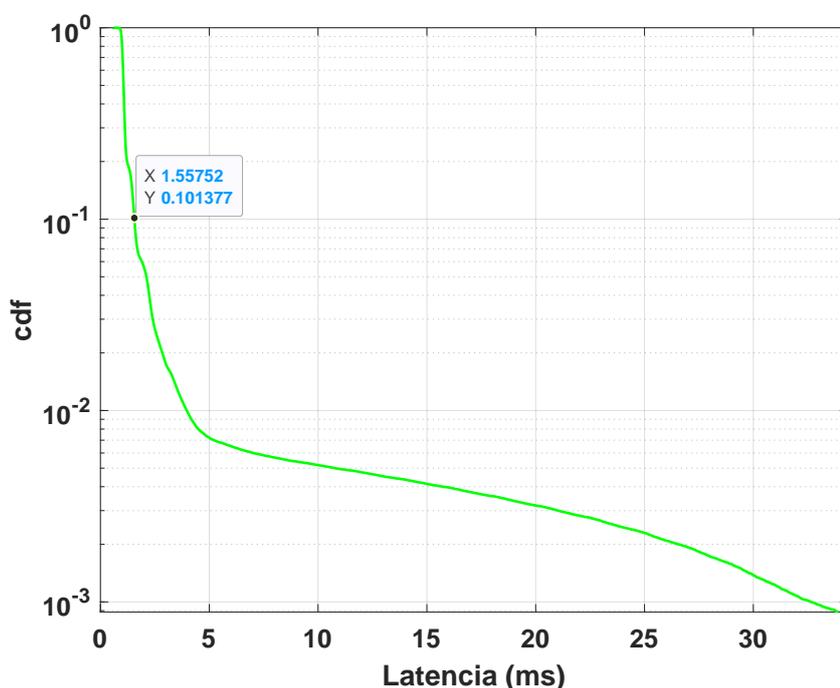
En la Figura 33 se puede ver un ejemplo de este tipo de representación. Como se puede apreciar, el eje vertical representa el número de paquetes, y el horizontal la latencia, separada por intervalos de 100 us en este caso. Este se trata de un caso en donde hay retransmisiones en la red, y el primer pico representa los paquetes que llegan sin

haberse retransmitido y el segundo los que se han mandando una segunda vez. Este es un caso en el que se obtienen menos de un 10 % de retransmisiones, y para el cual la mayoría de los paquetes llegan con un margen bastante reducido de latencia, menor que 300 us.

Para esta representación gráfica se utiliza la función *histogram* de MATLAB.

### 6.3.6.2. Representación acumulada

El segundo análisis para interpretar los resultados de las pruebas se ha realizado representando la función de distribución acumulada con el eje vertical en logarítmico. Esta función representa la probabilidad de que un valor del destino supere un valor especificado.



**Figura 34:** Ejemplo de una representación gráfica de la función de distribución acumulada (cdf).

El eje horizontal vuelve a representar la latencia en milisegundos, y el vertical la función CDF. En el caso de la Figura 34 el valor marcado representa que el 90 % de los paquetes tienen una latencia menor que 1.5572 ms, y el resto por tanto mayor. Mediante esta representación se pueden ver los límites de la tecnología, se examina en términos de bounded latency. En ciertas aplicaciones industriales, los paquetes que superan una determinada latencia se pueden considerar como erróneos, y mediante esta representación, se pueden definir estos límites.

Esta representación se realiza mediante las funciones *ecdf* y *semilogy* de MATLAB.

# 7. Análisis de capturas de la red

En este apartado se pretende comprobar el uso de las nuevas mejoras que incorpora el estándar 802.11ax en la red WiFi que se ha implementado. Se ha realizado un análisis del intercambio de tramas entre el AP y los STA, con el objetivo de verificar el uso de OFDMA y el formato de intercambio de mensajes mediante Trigger Frames definido en el estándar. Como se ha mencionado en el apartado anterior, el análisis se ha realizado a partir de dos fuentes de captura de tráfico de la red distintas. Estas son:

- Captura de las señales eléctricas con su posterior decodificación en MATLAB.
- Captura de tramas desde un módulo ajeno (Sniffer) a la red.

El análisis se divide en 3 partes: Intercambio de tramas Downlink, Uplink, y tramas de control.

## 7.1. Downlink

Como ya se ha comentado en el apartado 5.3.3, para el envío de datos desde el AP hacia los STAs el estándar define la siguiente secuencia:

- Una secuencia RTS-CTS antes del envío de tramas de datos, siendo el RTS de tipo Multi User.
- Envío de datos Multi User por parte del AP.
- Trigger Frame de tipo BAR hacia todos los STAs
- Respuesta de los clientes con el BA requerido

De lo definido en el estándar, (ver Figura 11 el AP de la red implementada, omite la secuencia RTS-CTS inicial, respetando el resto de las tramas definidas en el estándar. Esto se concluye después de haber capturado numerosas secuencias de envío de datos DL mediante el sniffer. La secuencia que se observa de manera repetitiva es la siguiente:

No.	Source	Destination	PHY type	BW/RU	RUs	PPDU Format	Info
1	ArubaaHe...	IntelCor...	802.11ax (HE)	106-tone RU		HE_MU	QoS Data, SN=3773,
2	ArubaaHe...	IntelCor...	802.11ax (HE)	106-tone RU		HE_MU	QoS Data, SN=3774,
3	ArubaaHe...	IntelCor...	802.11ax (HE)	106-tone RU		HE_MU	QoS Data, SN=3775,
4	ArubaaHe...	IntelCor...	802.11ax (HE)	106-tone RU		HE_MU	QoS Data, SN=3776,
5	ArubaaHe...	Broadcast...	802.11a (OFDM)		54 (106 tones),53 (106 tones)		Trigger MU-BAR, Fl
6	IntelCor...	ArubaaHe...	802.11ax (HE)	106-tone RU		HE_TRIG	802.11 Block Ack,

Figura 35: Captura de una secuencia de envío de datos Downlink.

En esta secuencia se puede apreciar primero una trama multi user del AP, que envía hacia todos los STAs conectados en la red. Se trata de una trama de datos que se envía utilizando a nivel PHY una RU de 106 portadoras. Como se ha mencionado anteriormente, para cada usuario la parte MAC es distinta, por tanto, los datos que se envían a cada usuario son diferentes.

Después, el AP envía un Trigger Frame, trama característica del estándar 802.11ax, de tipo MU-BAR, que solicita a los STAs la confirmación de determinados paquetes (diferentes para cada usuario). Además de esta información, el AP, especifica el reparto del canal para las respuestas. Esto es indicado en el campo de información de usuario de la trama, que se muestra más adelante en la Figura 37.

Por último, el STA le contesta con un Block ACK, confirmando los paquetes que ha solicitado el AP, utilizando los recursos frecuenciales asignados.

A nivel PHY, se aprecian dos de las nuevas tramas definidas en el estándar 802.11ax, tramas multi user (HE-MU) y tramas basadas en un Trigger Frame (HE-TB). El Trigger Frame lleva el mismo nivel físico que los estándares anteriores (nonHT), utilizado habitualmente para las tramas de control.

```
IEEE 802.11 Trigger, Flags: .....C
Type/Subtype: Trigger (0x0012)
> Frame Control Field: 0x2400
.000 0000 1000 1000 = Duration: 136 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: ArubaaHe_aa:e3:d0 (94:64:24:aa:e3:d0)
Common Info
  HE Trigger Common Info: 0x7fc0001248200462
    .....0010 = Trigger Type: MU-BAR (2)
    .....0000 0100 0110 = UL Length: 70
    .....0 = More TF: False
    .....0 = CS Required: False
    .....00 = UL BW: 20 MHz (0)
    .....10 = GI And LTF Type: 4x LTF + 3.2 us GI (2)
    .....0 = MU-MIMO LTF Mode: HE single stream pilot HE LTF mode
    .....00 0 = Number of HE-LTF Symbols and Midamble Periodicity: 0x0
    .....0 = UL STBC: False
    .....1 = LDPC Extra Symbol Segment: True
    .....10 0100 = AP Tx Power: 16 dBm
    .....1 00 = Packet Extension: PE disambiguity & pre-FEC padding factor of 4
    .....0 0000 0000 0000 000 = Spatial Reuse: 0x0000
    .....0 = Doppler: False
    .....111 1111 11 = UL HE-SIG-A2 Reserved: 0x1fff
    .....0 = Reserved: 0x0
  > User Info
    Padding: ffffffff...
    Frame check sequence: 0x4bd2d0ed [unverified]
    [FCS Status: Unverified]
```

Figura 36: Captura de la información común de un Trigger Frame.

En la Figura 36 se puede apreciar la información a nivel MAC de un Trigger Frame. Primero, se especifica el tipo de trama y las direcciones, que para este caso el destino es Broadcast y transmisor el AP. Después, se indica la información común para todos los usuarios acerca de la respuesta que el AP espera. Los campos más relevantes son:

- Tamaño (**UL Length**): 70 bytes.
- Ancho de banda (**UL BW**): 20 MHz.
- Intervalo de guarda (**GI**) y duración **LTF**: 3.2 us y 4xLTF (12.8 us).
- Modo de **MU-MIMO LTF**: He single stream pilot. Consiste básicamente en utilizar el mismo símbolo LTF para los diferentes flujos espaciales.
- Uso de codificación **LDPC**.
- Técnica reutilización espacial utilizada (**Spatial Reuse**): en este caso ninguna, en el caso de utilizarse, este campo sirve para que los usuarios utilicen la misma para la respuesta HE-TB, que se deberá indicar en el campo HE-SIG-A.



En esta captura se observa la respuesta a este TF por parte de uno de los usuarios, que es un Block ACK. En la captura se muestra la trama MAC, donde se puede ver cómo las direcciones en este caso son las opuestas a la trama de datos, ya que el STA le está confirmando al AP los paquetes que ha recibido y de los que ha solicitado la confirmación mediante el TF. Los paquetes confirmados son desde el **3773** hasta el **3776**, que coinciden con los paquetes de datos que se ven en la Figura 35.

```

HE information
> HE Data 1: 0xffe7, PPDU Format: HE_TRIG, BSS Color known, data MCS known, data DCM known, Coding known, LDPC extra
> HE Data 2: 0x417f, pri/sec 80 MHz known, GI known, LTF symbols known, Pre-FEC Padding Factor known, TxBF known, PE
v HE Data 3: 0x6305, Coding: LDPC
  .... ..00 0101 = BSS Color: 0x05
  .... ..0.. .... = Beam Change unknown: 0x0
  .... ..0... .... = UL/DL unknown: 0x0
  .... 0011 .... = data MCS: 0x3
  ...0 .... .... = data DCM: 0x0
  ..1. .... .... = Coding: LDPC (0x1)
  .1.. .... .... = LDPC extra symbol segment: 0x1
  0... .... .... = STBC: 0x0
> HE Data 4: 0x0000
v HE Data 5: 0x80e6, data Bandwidth/RU allocation: 106-tone RU, GI: 3.2us, LTF symbol size: 4x, LTF symbols: 1x
  .... ..0110 = data Bandwidth/RU allocation: 106-tone RU (0x6)
  .... ..10 .... = GI: 3.2us (0x2)
  .... ..11.. .... = LTF symbol size: 4x (0x3)
  .... .000 .... = LTF symbols: 1x (0x0)
  .... 0... .... = reserved: 0x0
  ..00 .... .... = Pre-FEC Padding Factor: 0x0
  .0.. .... .... = TxBF: 0x0
  1... .... .... = PE Disambiguity: 0x1
> HE Data 6: 0x0021, NSTS: 1 space-time stream

```

**Figura 39:** Captura de la información PHY de la trama HE-TB.

En la Figura 39 se muestra la información a nivel PHY de la trama. Como se trata de una trama HE-TB, esta información está detallada en el campo HE-SIG-A. Como se puede comprobar, se utilizan las características de la comunicación especificadas por el AP: RU asignada, MCS, DCM, intervalo de guarda y LTF.

## 7.2. Uplink

Para el envío de datos desde los usuarios hacia el AP, el estándar define una secuencia, representada en la Figura 12. En esta secuencia se utilizan tres tipos de Trigger Frame:

- **BSRP:** Buffer Status Report Pool.
- **MU-RTS:** Multi user Request to Send.
- **Basic:** Trigger Frame básico para el envío de datos.

Después del análisis de red realizado se han observado dos de ellos (BSRP y Basic) pero no de manera secuencial ni como previa al envío de datos UL.

### 7.2.1. Trigger Basic

El primer tipo de Trigger capturado es de tipo Basic, que se utiliza para desencadenar el envío de datos de las estaciones al AP. La secuencia para el intercambio de datos capturada es la siguiente:

No. ^	Source	Destination	Protocol	PPDU Format	Info
1	ArubaaHe...	Broadcast (f...	802.11		Trigger Basic, Flags=.....C
2	IntelCor...	ArubaaHe_c2:...	802.11 HE_TRIG		QoS Data, SN=231, FN=0, Flags=op....TC
3	ArubaaHe...	Broadcast (f...	802.11		802.11 Block Ack, Flags=.....C

**Figura 40:** Captura de la secuencia de envío de datos UL.

En esta captura se aprecia como uno de los STAs conectados al AP responde a un TF básico enviado desde el AP a dos STAs. Solo se ha podido capturar una de las dos respuestas al TF debido al inconveniente SW mencionado en la sección 6.2.1, que sólo permite capturar paquetes HE-MU y HE-TB de una asociación AP-STA.

En cuanto a la asignación de RUs ocurre lo mismo que en el caso de DL. El STA envía una trama, de datos en este caso, utilizando la RU asignada por el AP en el TF, además de utilizar las características a nivel PHY también mencionadas.

La respuesta a la trama de datos es un Block ACK diferente al habitual. Se trata de un paquete de tipo HE-MU (multi user) que envía el AP hacia ambos STAs (entendiendo entonces que el otro STA también ha enviado datos) confirmando los paquetes recibidos:

```
IEEE 802.11 802.11 Block Ack, Flags: .....C
  Type/Subtype: 802.11 Block Ack (0x0019)
  > Frame Control Field: 0x9400
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: ArubaaHe_aa:e3:d0 (94:64:24:aa:e3:d0)
  < Multi-STA BlockAck Response
    > Block Ack Control: 0x0016
    < Per AID TID Info: 0x3
      > AID TID Info: 0x0003
        < Block Ack Starting Sequence Control (SSC): 0xeb34
          .... .... 0100 = Fragment: 4
          1110 1011 0011 .... = Starting Sequence Number: 3763
          Block Ack Bitmap: ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
        < Per AID TID Info: 0x4
          > AID TID Info: 0x0004
            < Block Ack Starting Sequence Control (SSC): 0xfe94
              .... .... 0100 = Fragment: 4
              1111 1110 1001 .... = Starting Sequence Number: 4073
            Block Ack Bitmap: ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
          Frame check sequence: 0x51abd8b9 [unverified]
          [FCS Status: Unverified]
```

**Figura 41:** Captura de la información MAC de la trama Multi STA Block ACK.

En la Figura 41 se puede ver la trama Multi STA ACK en detalle, cómo el AP envía la confirmación de paquetes hacia dos STAs a la vez, diferenciados por el AID.

No obstante, es importante mencionar que después del análisis realizado sobre la red montada, se encuentran diferencias respecto al uso de OFDMA en UL y DL. Como se ha mencionado anteriormente, para el intercambio de datos el estándar define varios tipos de PPDU: MU, SU, TB, ... Además de este tipo de paquetes, en la red también se utilizan paquetes para las que no se realiza la asignación de recursos frecuenciales de OFDMA. Estos paquetes también se han capturado y tenido en cuenta para este análisis.

Los paquetes capturados en mayor frecuencia han sido del tipo HE-SU. Estos son de datos, tanto desde el AP hacia las STAs y viceversa. En la Figura 42 se aprecia una secuencia habitual en donde las STAs, después de hacer un intercambio RTS/CTS, envían datos al AP utilizando el formato PHY de HE-SU, utilizando todo el canal, 20 MHz.

No.	Source	Destination	PHY type	BW/RU	PPDU Format	Info
109	IntelCor_00:22:e2...	ArubaaHe_aa:e3:d0...	802.11a (OFDM)			Request-to-send, Flags=.....C
110		IntelCor_00:22:e2...	802.11a (OFDM)			Clear-to-send, Flags=.....C
111	80:47:dd:00:22:e2	94:66:24:c2:ae:3b	802.11ax (HE)	20	HE_SU	QoS Data, SN=2439, FN=0, Flags=.p....TC
112	IntelCor_00:2c:2e...	ArubaaHe_aa:e3:d0...	802.11a (OFDM)			Request-to-send, Flags=.....C
113		IntelCor_00:2c:2e...	802.11a (OFDM)			Clear-to-send, Flags=.....C
114	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	802.11ax (HE)	20	HE_SU	QoS Data, SN=1747, FN=0, Flags=.p....TC
115		IntelCor_00:2c:2e...	802.11a (OFDM)			Acknowledgement, Flags=.....C
116	IntelCor_04:b2:58...	ArubaaHe_aa:e3:d0...	802.11a (OFDM)			Request-to-send, Flags=.....C
117		IntelCor_04:b2:58...	802.11a (OFDM)			Clear-to-send, Flags=.....C
118	IntelCor_04:b2:58	ArubaaHe_c2:ae:3b	802.11ax (HE)	20	HE_SU	QoS Data, SN=840, FN=0, Flags=.p....TC
119		IntelCor_04:b2:58...	802.11a (OFDM)			Acknowledgement, Flags=.....C

Figura 42: Captura de tramas HE-SU.

En el caso de UL, se aprecian tanto esta secuencia como la de la Figura 40. Esto ocurre debido a que es desconocido el criterio por el cual el AP utiliza OFDMA, y, aun probando en diferentes escenarios, no se encuentra el motivo por el cual el AP decide utilizar o no TF para que los STAs envíen tramas de datos.

En DL en cambio, el AP envía tramas de información mediante OFDMA en mayor medida, utilizando el TF mencionado en la sección 7.1. Se ha podido observar cómo en situaciones de congestión y tráfico en la red, el AP envía las tramas de datos hacia los STAs utilizando sólo el método de la Figura 35.

### 7.2.2. Trigger BSRP

Otro de los Trigger Frame capturados es el BSRP. Según lo definido en el estándar, esta trama la envía el AP a todas las STAs a la vez (dirección destino Broadcast) preguntando sobre el estado del buffer de transmisión de cada una, es decir, preguntando si tienen información pendiente para transmitir. La respuesta de las estaciones en teoría la realizan compartiendo el canal, como en el resto de TF.

No obstante, tras realizar el análisis de esta red, se concluye con que el AP realiza esta comprobación del buffer de las estaciones de manera periódica e individual. Es decir, pregunta cada X tiempo a cada una de las estaciones por separado si tiene información para transmitir. La respuesta está separada en función del nivel de prioridad de las tramas pendientes, este nivel se indica en el campo de control del QoS de las tramas. En el caso que la STA tenga información pendiente, el AP envía un TF de tipo Basic Unicast hacia esa estación para que transmita esta información. Esta última secuencia se puede ver en las tramas 1 y 20 de la Figura 43.

No.	Source	Destination	BW/RU	RUs	PPDU	Queue Info	Preferred AC Priority
1	ArubaaHe_aa:e3:d0...	IntelCor_00:22:e...		61 (242 tones)		Trigger Buffer Status Report...	
2	IntelCor_00:22:e2	ArubaaHe_aa:e3:d0	242-tone RU		HE_TRIG	102 QoS Null function (No data),...	Best Effort (Best Effort)
3	IntelCor_00:22:e2	ArubaaHe_aa:e3:d0	242-tone RU		HE_TRIG	0 QoS Null function (No data),...	Network Control (Voice)
4	IntelCor_00:22:e2	ArubaaHe_aa:e3:d0	242-tone RU		HE_TRIG	0 QoS Null function (No data),...	Video (Video)
5	IntelCor_00:22:e2	ArubaaHe_aa:e3:d0	242-tone RU		HE_TRIG	0 QoS Null function (No data),...	Background (Background)
6	ArubaaHe_aa:e3:d0...	IntelCor_00:2c:2...				Request-to-send, Flags=.....C	
7		ArubaaHe_aa:e3:d...				Clear-to-send, Flags=.....C	
8	ArubaaHe_c2:ae:3b	IntelCor_00:2c:2e	20		HE_SU	QoS Data, SN=2823, FN=0, Fla...	Best Effort (Best Effort)
9	ArubaaHe_c2:ae:3b	IntelCor_00:2c:2e	20		HE_SU	QoS Data, SN=2824, FN=0, Fla...	Best Effort (Best Effort)
10	ArubaaHe_c2:ae:3b	IntelCor_00:2c:2e	20		HE_SU	QoS Data, SN=2825, FN=0, Fla...	Best Effort (Best Effort)
11	ArubaaHe_c2:ae:3b	IntelCor_00:2c:2e	20		HE_SU	QoS Data, SN=2826, FN=0, Fla...	Best Effort (Best Effort)
12	IntelCor_00:2c:2e...	ArubaaHe_aa:e3:d...				802.11 Block Ack, Flags=.....C	
13	IntelCor_00:2c:2e...	ArubaaHe_aa:e3:d...				Request-to-send, Flags=.....C	
14		IntelCor_00:2c:2...				Clear-to-send, Flags=.....C	
15	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	81 QoS Data, SN=751, FN=0, Flag...	Best Effort (Best Effort)
16	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	81 QoS Data, SN=752, FN=0, Flag...	Best Effort (Best Effort)
17	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	81 QoS Data, SN=753, FN=0, Flag...	Best Effort (Best Effort)
18	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	81 QoS Data, SN=754, FN=0, Flag...	Best Effort (Best Effort)
19	ArubaaHe_aa:e3:d0...	IntelCor_00:2c:2...				802.11 Block Ack, Flags=.....C	
20	ArubaaHe_aa:e3:d0...	IntelCor_00:22:e...		61 (242 tones)		Trigger Basic, Flags=..... AC_BE	
21	IntelCor_00:22:e2	ArubaaHe_c2:ae:3b	242-tone RU		HE_TRIG	90 QoS Data, SN=1650, FN=0, Fla...	Best Effort (Best Effort)
22	IntelCor_00:22:e2	ArubaaHe_c2:ae:3b	242-tone RU		HE_TRIG	90 QoS Data, SN=1651, FN=0, Fla...	Best Effort (Best Effort)
23	ArubaaHe_aa:e3:d0...	IntelCor_00:22:e...				802.11 Block Ack, Flags=.....C	

Figura 43: Captura de una secuencia de Trigger BSRP y Trigger Basic.

En esta secuencia se aprecia cómo la estación responde al Trigger Frame de tipo BSRP del AP con el tamaño de la cola para las diferentes prioridades, utilizando tramas vacías, Null Data Packet (NDP).

En el Trigger Frame (sólo en los de tipo Basic) el AP indica el tipo de prioridad de las tramas que las estaciones tienen que enviar hacia él. Esto es indicado en el campo de Preferred AC (Access Category) de la información de usuario, como se muestra en la trama número 20 de la Figura 43. Después, la estación responde al TF del AP con tramas de prioridad Best Effort.

Por parte del AP, la información obtenida sirve para modificar el tiempo de las próximas TXOP para esta estación, según lo definido en la sección 9.2.4.5 del estándar [26] acerca del servicio de calidad QoS.

Otra opción, es que antes de que el AP envíe el TF, el STA con información pendiente de transmitir lo haga antes utilizando tramas HE-SU como en la Figura 44.

No.	Source	Destination	BW/RU	RUs	PPDU	Queue Info	Priority
1	ArubaaHe_aa:e3:d0...	IntelCor_00:2c:2...		61 (242 tones)		Trigger Buffer Status Re...	
2	IntelCor_00:2c:2e	ArubaaHe_aa:e3:d0	242-tone RU		HE_TRIG	81 QoS Null function (No da...	Best Effort (Best Effort)
3	IntelCor_00:2c:2e	ArubaaHe_aa:e3:d0	242-tone RU		HE_TRIG	0 QoS Null function (No da...	Network Control (Voice)
4	IntelCor_00:2c:2e	ArubaaHe_aa:e3:d0	242-tone RU		HE_TRIG	0 QoS Null function (No da...	Video (Video)
5	IntelCor_00:2c:2e	ArubaaHe_aa:e3:d0	242-tone RU		HE_TRIG	0 QoS Null function (No da...	Background (Background)
6	IntelCor_00:2c:2e...	ArubaaHe_aa:e3:d...				Request-to-send, Flags=...	
7		IntelCor_00:2c:2...				Clear-to-send, Flags=...	
8	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	102 QoS Data, SN=4043, FN=0,...	Best Effort (Best Effort)
9	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	102 QoS Data, SN=4044, FN=0,...	Best Effort (Best Effort)
...	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	102 QoS Data, SN=4045, FN=0,...	Best Effort (Best Effort)
...	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	102 QoS Data, SN=4046, FN=0,...	Best Effort (Best Effort)
...	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	102 QoS Data, SN=4047, FN=0,...	Best Effort (Best Effort)
...	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	102 QoS Data, SN=4048, FN=0,...	Best Effort (Best Effort)
...	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	102 QoS Data, SN=4049, FN=0,...	Best Effort (Best Effort)
...	IntelCor_00:2c:2e	ArubaaHe_c2:ae:3b	20		HE_SU	102 QoS Data, SN=4050, FN=0,...	Best Effort (Best Effort)
...	ArubaaHe_aa:e3:d0...	IntelCor_00:2c:2...				802.11 Block Ack, Flags=...	

Figura 44: Captura de una secuencia del Trigger BSRP.

En este caso, el AP no envía un TF para habilitar a la estación que transmita esa información, lo requiere ella directamente. El valor de la cola no representa el número de bytes pendientes directamente, ya que sólo se utilizan 8 bits para representar este valor. Este campo representa el tamaño máximo, redondeado en exceso al múltiplo más cercano de 256. El máximo son 64768 bytes (254),y, por ejemplo 81 representa 20736 bytes.

## 7.3. Control

En este apartado se realiza una descripción de las tramas capturadas que no están orientadas hacia el envío de datos, si no que para el control de la red. Se separa este análisis en las tramas que sirven para realizar el sondeo del canal, y las que sirven para anunciar la presencia de la red.

### 7.3.1. Sounding

El primer tipo de tramas de control que se va a describir son las orientadas hacia el Sounding del canal de radio. Sounding, sondeo en inglés, es un proceso que realiza el AP para estimar el estado del canal que está utilizando junto con una estación. Este proceso está definido en el estándar IEEE 802.11ac, el cual se permite hacer de manera Unicast o Multicast. Es decir, el AP puede hacer la estimación de canal hacia más de una estación a

la vez, obteniendo diferentes resultados para cada una de ellas. No obstante, el estándar IEEE 802.11ax introduce cambios en el formato de estas tramas, los cuales se detallan a continuación.

En el estándar se define la secuencia que se muestra en la Figura 14 para el tipo de sondeo single user (SU), en donde el AP es quien comienza a hacer la estimación. En esta Figura HE beamformer representa al AP y HE beamformee a una de las estaciones. Las tramas que se muestran se han capturado en la red implementada y se describen más adelante. En el estándar se definen otros métodos de sondeo, mediante Trigger Frame y para varias estaciones a la vez, no obstante, debido a que estos no han sido capturados en la red implementada no se analizan en esta sección.

Esta misma secuencia se ha capturado de manera periódica:

No.	Source	Destination	Info	PPDU type	HE action
1	ArubaaHe_aa:e3:c0 ...	IntelCor_04:b2:58 ...	VHT/HE NDP Announcement,...		
2			Radiotap Capture v0, Len...	sounding PPDU	
3	IntelCor_04:b2:58	ArubaaHe_aa:e3:c0	Action No Ack, SN=1228, ...		HE Compressed Beamforming And CQI

**Figura 45:** Captura de la secuencia HE sounding

El segundo paquete, al ser solo del nivel físico, un preámbulo, no tiene direcciones MAC. De estas tramas, las características mas representativas son las siguientes:

- **HE NDP Announcement:** se trata del primer paquete de esta secuencia, no tiene datos (NDP, Null Data Packet) cuya única función es solicitar a la o las estaciones destino que se va a iniciar el proceso de estimación de canal.

```
IEEE 802.11 VHT/HE NDP Announcement, Flags: .....C
  Type/Subtype: VHT/HE NDP Announcement (0x0015)
  > Frame Control Field: 0x5400
    .000 0000 0110 0100 = Duration: 100 microseconds
    Receiver address: IntelCor_04:b2:58 (80:45:dd:04:b2:58)
    Transmitter address: ArubaaHe_aa:e3:c0 (95:64:24:aa:e3:c0)
  v Sounding Dialog Token: 0xde
    .... ..0 = Reserved: 0x0
    .... ..1. = HE: HE NDP Announcement frame
    1101 11.. = Sounding Dialog Token Number: 55
  v STA list
    v STA 0
      v STA Info: 0x08200012
        .... ..000 0001 0010 = AID11: 0x012
        .... ..00 0000 0... .. = RU Start Index: 0x00
        .... ..0 0010 00.. .. = RU End Index: 0x08
        .... .00. .... .. = Feedback Type and Ng: 0x0
        .... 1... .. = Disambiguation: 0x1
        .... ..0 .... .. = Codebook Size: 0x0
        000. .... .. = Nc: 0x0
    Frame check sequence: 0xb8c5d09d [unverified]
    [FCS Status: Unverified]
```

**Figura 46:** Datos de la trama HE NDP Announcement.

En cuanto al resto de campos de la trama MAC:

- **Sounding Dialog Token Number:** en este campo se detalla si la trama es del tipo VHT o HE y el número de identificación de este tipo de tramas, que usa el AP para llevar el control del número de veces que realiza este proceso.

- **STA list;** En este campo se separa para cada STA sobre las que se va a realizar el sondeo las siguientes características:
  - **AID:** mediante este campo de identidad de asociación entre un AP y una STA se diferencian el resto de características del campo.
  - **RU start y end index:** mediante esta información se detalla el comienzo y final de las RU de 26 portadoras sobre las que se solicita hacer el sondeo. Para canales de 20 MHz estos valores varían entre 0 y 8, debido a que sólo entran 8 RU en el canal. En el caso de este análisis el comienzo es 0 y el final 8. Esto indica que el AP está solicitando realizar el sondeo del canal completo.
  - **Feedback Type and Ng y Codebook size:** la combinación de estos bits dan información acerca del tipo de feedback (SU, MU o CQI) y la resolución de la misma. En este caso se trata de SU, agrupando las portadoras de 4 en 4.
  - **Disambiguation:** este campo sirve para prevenir malinterpretar el AID de estaciones que no soportan el estándar 802.11ax. Si vale indica que el AID contempla estaciones con estándares anteriores, es decir, que no existe la posibilidad de que coincidan dos STAs con AID para el sounding diferentes.
- **HE Sounding Null Data Packet:** este paquete sin datos es sobre el que la estación destino tendrá que hacer la matriz de feedback.
- **HE Compressed Beamforming/CQI:** este paquete es enviado por la estación sobre la que el AP ha solicitado el sondeo. Este, en base al preámbulo recibido, calcula la intensidad, ruido y ángulo de las portadoras de esta señal para transmitírselo al AP.

```

IEEE 802.11 Wireless Management
  v Fixed parameters
    Category code: HE (30)
    v HE Action: HE Compressed Beamforming And CQI (0)
      Total length: 89
      v HE MIMO Control: 0x0dc4008209
        .....001 = Nc Index: 2 Columns (1)
        .....00 1... = Nr Index: 2 Rows (1)
        .....00.. = BW: 0
        .....0 ..... = Grouping: Carrier Groups of 4 (0)
        .....1. .... = Codebook Information: 1
        .....00.. .... = Feedback Type: SU (0)
        .....000 ..... = Remaining Feedback Segments: 0
        .....1... .... = First Feedback Segment: 1
        .....000 0000 ..... = RU Start Index: 0x00
        .....00 0100 0... ..... = RU End Index: 0x08
        ....1101 11... ..... = Sounding Dialog Token Number: 55
        0000 ..... = Reserved: 0
      v Average Signal to Noise Ratio
        Stream 0: 34,25dB (0x31)
        Stream 1: <=-10,00dB (0x80)
      v Feedback Matrices
        SCIDX: -122, phi11:5, psi21:57
        SCIDX: -120, phi11:7, psi21:50
        SCIDX: -116, phi11:5, psi21:46
        SCIDX: -112, phi11:8, psi21:53
  
```

**Figura 47:** Datos de la trama HE Compressed Beamforming/CQI.

- **Nc y Nr:** número de columnas y filas de la matriz de feedback, en este caso 2x2.
- **BW:** Ancho de banda, 20 MHz.

- **Grouping:** Ng, número de portadoras sobre la que se agrupa cada dato de la fila de la matriz.
- **Codebook:** indica la resolución de las entradas de la matriz, en este caso como vale 1 se trata de 4 y 2 bits.
- **Feedback Type:** tipo de feedback, Single User (SU).
- **Remaining Feedback Segments:** en este caso vale 0 ya que el sondeo no se segmenta en diferentes tramas.
- **First Feedback Segment:** vale 1 si es el primer segmento. **RU Start y End Index:** igual que en la petición, hacen la referencia a las RUs sobre las que se ha realizado el sondeo.
- **Sounding Dialog Token Number:** número de identificación del sondeo.
- **Average Signal to Noise Ratio:** media de la potencia de la Señal frente al ruido para los dos flujos espaciales. Como se puede apreciar, el segundo flujo tiene un ruido gigante, por lo que el AP no lo usará para enviar datos más adelante. Esto ocurre, debido a que la antena de este flujo espacial está orientada hacia la dirección opuesta de la estación, por lo que recibe con muy poca potencia esta señal.
- **Feedback Matrices:** valores comprimidos acerca del ángulo y potencia del canal. Cada línea indica estos valores para una portadora, que se calculan cada 4 portadoras. Esto lo especifica el AP en el campo Ng, y es confirmado por el campo Grouping de esta trama. Como en este caso se realiza el sounding para 20 MHz, los índices de las portadoras van desde -122 hasta 122. (se utilizan 244 portadoras en canales de 20 MHz).

Como se puede apreciar, las características de sondeo de la respuesta coinciden con las de la petición. Después de este proceso completo, el AP es capaz de modificar el patrón de transmisión de la antena para mejorar la eficiencia y calidad de la comunicación. Después de hacer el análisis de la red, este proceso se observa de manera periódica cada 100 ms, realizándose para cada estación individualmente, como se puede apreciar en la Figura 48.

Time	Source	Destination	AID Sounding	Sounding Token	Info
0.000000000	ArubaaHe_aa:e3:c0 ...	IntelCor_00:22:e2 ...	0x010	1	VHT/HE NDP Announcement
0.001459004	ArubaaHe_aa:e3:c0 ...	IntelCor_00:2c:2e ...	0x011	2	VHT/HE NDP Announcement
0.021608791	ArubaaHe_aa:e3:c0 ...	IntelCor_04:b2:58 ...	0x012	3	VHT/HE NDP Announcement
0.103438964	ArubaaHe_aa:e3:c0 ...	IntelCor_00:22:e2 ...	0x010	4	VHT/HE NDP Announcement
0.104447390	ArubaaHe_aa:e3:c0 ...	IntelCor_00:2c:2e ...	0x011	5	VHT/HE NDP Announcement
0.125017262	ArubaaHe_aa:e3:c0 ...	IntelCor_04:b2:58 ...	0x012	6	VHT/HE NDP Announcement
0.205515589	ArubaaHe_aa:e3:c0 ...	IntelCor_00:22:e2 ...	0x010	8	VHT/HE NDP Announcement
0.206507567	ArubaaHe_aa:e3:c0 ...	IntelCor_00:2c:2e ...	0x011	9	VHT/HE NDP Announcement
0.228929402	ArubaaHe_aa:e3:c0 ...	IntelCor_04:b2:58 ...	0x012	10	VHT/HE NDP Announcement
0.307085342	ArubaaHe_aa:e3:c0 ...	IntelCor_00:22:e2 ...	0x010	11	VHT/HE NDP Announcement

**Figura 48:** Captura en Wireshark filtrando las tramas de HE sounding.

La captura de esta Figura 48 se ha obtenido después de filtrar la visualización para las tramas por del tipo VHT/HE NDP , cuyo filtro en Wireshark es:

*wlan.fc.type\_subtype == 0x0015*

Como se observa, para cada estación diferente se utiliza un distinto AID y cada proceso, estando el tiempo en segundos, se inicia cada 100 ms. También se aprecia el campo de Sounding Token, que es incrementado por el AP cada vez que inicia un sondeo.

### 7.3.2. Beacons

En este apartado se van a explicar los beacons capturados del AP de la red implementada. Estos paquetes, conocidos también como paquetes baliza, sirven para anunciar la presencia de la red y dar información acerca de las características de la misma. En el estándar IEEE 802.11ax la información que dan estos paquetes es considerablemente superior a las de estándares inferiores, ya que se informa acerca de las propiedades de todas las tecnologías nuevas que implementa este último estándar.

Estos paquetes los envía el AP con dirección destino Broadcast, con una frecuencia de 100 ms. La información de estos paquetes, contenida en la parte de datos MAC, contiene primero los datos de beacons habituales, es decir, los que también están incluidos en los estándares más antiguos y después se describen las propiedades del IEEE 802.11ax (HE) y las de la banda de 6 GHz.

La información mínima obligatoria que deben transmitir los beacons en todos los estándares es la siguiente:

```
IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
    Timestamp: 3812864054
    Beacon Interval: 0,102400 [Seconds]
  v Capabilities Information: 0x0411
    .... ..1 = ESS capabilities: Transmitter is an AP
    .... ..0. = IBSS status: Transmitter belongs to a BSS
    .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
    .... ..1 .... = Privacy: AP/STA can support WEP
    .... ..0. .... = Short Preamble: Not Allowed
    .... ..0.. .... = PBCC: Not Allowed
    .... ..0... .... = Channel Agility: Not in use
    .... ..0 .... .... = Spectrum Management: Not Implemented
    .... ..1. .... .... = Short Slot Time: In use
    .... ..0... .... .... = Automatic Power Save Delivery: Not Implemented
    .... ..0 .... .... = Radio Measurement: Not Implemented
    ..0. .... .... .... = DSSS-OFDM: Not Allowed
    .0.. .... .... .... = Delayed Block Ack: Not Implemented
    0... .... .... .... = Immediate Block Ack: Not Implemented
  v Tagged parameters (209 bytes)
    v Tag: SSID parameter set: Test
      Tag Number: SSID parameter set (0)
      Tag length: 4
      SSID: Test
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
```

Figura 49: Captura de la información obligatoria del Beacon.

- **Timestamp:** Este campo refleja el tiempo en us del AP, el tiempo que este ha estado activo. En este caso es de 3800 segundos, algo más de una hora.
- **Beacon interval:** representa el intervalo de transmisión de estos paquetes, se utiliza el valor por defecto de 100 ms.
- **SSID:** Identificador de red.
- **Capability info:** da información acerca de las capacidades opcionales de la red. En este caso el soporte de WEP, que el transmisor de los beacons es un AP y el uso de tiempos de slot cortos. Este último hace referencia al tiempo de espera para la retransmisión de un paquete después de un error, al ser corto, se incrementa el throughput de la red.

- **Supported Rates:** Refleja las tasas de datos disponibles en la red. Esto indica que los clientes deberán soportar las indicadas como básicas, en este caso 6,12 y 24 Mbps, que hacen referencia a las técnicas de modulación BPSK, QPSK y QAM.

El resto de información habitual es la siguiente:

```

  v Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    Tag Number: Traffic Indication Map (TIM) (5)
    Tag length: 4
    DTIM count: 0
    DTIM period: 1
  > Bitmap control: 0x00
    Partial Virtual Bitmap: 00
  > Tag: RSN Information
  > Tag: Extended Capabilities (11 octets)
  > Ext Tag: Multiple BSSID Configuration

```

**Figura 50:** Captura de la información común del Beacon.

- **TIM:** Da información acerca del estado del buffer del AP, sobre las tramas multicast que tiene, en este caso ninguna. También indica en el campo **Partial Virtual Bitmap** el tráfico pendiente que tiene para las estaciones que están en modo de bajo consumo.
- **RSN information:** Robust Secure Network (RSN) es el protocolo de seguridad utilizado en 802.11, aquí se especifican las características de este acerca de la autenticación y encriptación para las estaciones.
- **Extended Capabilities:** aquí se informa acerca de capacidades soportadas extra de la red, que no se comentan en el campo de capability info. Hay de muchos tipos, pero las más relevantes son:
  - **Multiple BSSID:** consiste en que el AP puede usar varias SSID, redes diferentes, mediante los mismos beacon frames.
  - **TWT:**
  - **Extended Channel Switching:** esto indica el soporte de ECSA (Extended Channel Switching Announcement), que es el mecanismo encargado de avisar a las estaciones de manera inmediata si el AP va a cambiar el canal o ancho de banda.

En cuanto a la información acerca de 802.11ax (HE) del AP, el beacon separa el nivel MAC y el PHY:

- Capacidades HE para MAC:

```

+HTC HE Support: Supported
TWT Requester Support: Not supported
TWT Responder Support: Supported
Dynamic Fragmentation Support: No support for dynamic fragmentation (0)
Reserved: 0x0
Reserved: 0x1
Trigger Frame MAC Padding Duration: 0 (0)
Multi-TID Aggregation Rx Support: 0
HE Link Adaptation Support: No feedback if the STA does not provide HE MFB (0)
All Ack Support: Not supported
TRS Support: Not supported
BSR Support: Supported
Broadcast TWT Support: Not supported
32-bit BA Bitmap Support: Not supported
MU Cascading Support: Not supported
Ack-Enabled Aggregation Support: Not supported
Reserved: 0x0
OM Control Support: Supported
OFDMA RA Support: Not supported
Maximum A-MPDU Length Exponent Extension: 3
Reserved: 0x0
Flexible TWT Schedule Support: Not supported
Rx Control Frame to MultiBSS: Supported
BSRP BQRP A-MPDU Aggregation: Not supported
QTP Support: Not supported
BQR Support: Not supported
PSR Responder: Not supported
NDP Feedback Report Support: Not supported
OPS Support: Not supported
A-MSDU Not Under BA in Ack-Enabled A-MPDU Support: Supported
Multi-TID Aggregation Tx Support: 0
HE Subchannel Selective Transmission Support: Not supported
UL 2x996-tone RU Support: Not supported
OM Control UL MU Data Disable RX Support: Supported
HE Dynamic SM Power Save: Not supported
Punctured Sounding Support: Not supported
HT And VHT Trigger Frame RX Support: Not supported

```

**Figura 51:** Captura de la información MAC del Beacon.

De toda esta información, la más relevante es:

- **TWT:** Soporta Responder pero no supporter
  - **BSR:** indica para el AP el soporte de recepción de tramas Buffer Status Report, que son la respuesta a los TF de tipo BSPR que este envía, como se aprecia en la Figura 44.
  - **OFDMA RA:** este bit indica para el AP el no soporte de envío de TF que asignan RUs de manera aleatoria (RA-RU). Este protocolo se conoce como UL OFDMA-based random access (UORA) [35] y se basa en que las STAs conectadas al AP pueden enviar datos UL utilizando una RU aleatoria, dentro de unas predeterminadas que escoge el AP.
  - **UL 2X996-tone RU:** El AP no soporta el uso de RUs de 160 MHz (2x996 portadoras) para el envío de datos UL, el máximo para cada estación es de 996, 80 MHz.
- Capacidades HE para PHY:

```

HE PHY Capabilities Information
> .... ..0 = Reserved: 0x0
√ 0000 110. = Channel Width Set: 0x06
    .... ..0. = Reserved: 0x0
    .... .1.. = 40 & 80 MHz in the 5 GHz and 6 GHz bands: Supported
    .... 1... = 160 MHz in the 5 GHz and 6 GHz bands: Supported
    ...0 .... = 160/80+80 MHz in the 5 GHz and 6 GHz bands: Not supported
    ..0. .... = Reserved: 0x0
    .0.. .... = 242 tone RUs in the 5 GHz and 6 GHz bands: Not supported
    0... .... = Reserved: 0x0
> Bits 8 to 23: 0x0860
> Bits 24 to 39: 0xfd88
> Bits 40 to 55: 0x8149
> Bits 56 to 71: 0x119c
> Bits 72 to 87: 0x0008
Supported HE-MCS and NSS Set
√ Rx and Tx MCS Maps <= 80 MHz
    √ Rx HE-MCS Map <= 80 MHz: 0xffffa
        .... ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
        .... ..10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
        .... ..11 .... = Max HE-MCS for 3 SS: Not supported for HE PPDUs (0x3)
        .... ..11.. .... = Max HE-MCS for 4 SS: Not supported for HE PPDUs (0x3)
        .... ..11 .... = Max HE-MCS for 5 SS: Not supported for HE PPDUs (0x3)
        .... 11.. .... = Max HE-MCS for 6 SS: Not supported for HE PPDUs (0x3)
        ..11 .... .... = Max HE-MCS for 7 SS: Not supported for HE PPDUs (0x3)
        11.. .... .... = Max HE-MCS for 8 SS: Not supported for HE PPDUs (0x3)
    > Tx HE-MCS Map <= 80 MHz: 0xffffa
> Rx and Tx MCS Maps 160 MHz

```

**Figura 52:** Captura de la información PHY del Beacon.

El primer campo esta captura es el ancho de banda disponible para los canales, como este paquete está capturado utilizando un canal de 160 MHz, se permiten canales de 40, 80 y 160 en las bandas de 5 y 6 GHz. El campo de AI indicar que no se pueden utilizar RUs de 242 portadoras, el máximo permitido para el envío MU de datos es de 106, esto se refiere a que los TF, en caso de tener más de una estación a la que asignar recursos, no serán capaces de asignar RUs de más de 148 portadoras. En los campos que en la Figura 52 no salen desplegados, los bits 8-87 de este campo, indican el soporte de todas las propiedades físicas de la red, los más destacados son los siguientes:

- **LDPC Coding:** indica el soporte de la codificación de las PPDUs mediante LDPC.
- **SU Beamformer, Beamformee y MU Beamformer:** mediante estos campos el AP indica que soporta el sounding de tipo SU en ambos sentidos, indicando que no lo soporta de tipo MU, por lo que el soundig se realiza de manera individual hacia las STAs.
- **Ng = 16 SU, MU Feedback:** indica la posibilidad de agrupar los portadores en grupos de 16 en el reporte del sounding. Este AP lo permite solo para SU.
- **Triggered SU, MU, CQI feedback:** no soporta realizar la secuencia de sounding mediante Trigger Frames, sólo de la manera vista en el apartado 7.3.1.
- **HE SU and MU PPDU:** mediante diferentes bits se indica la posibilidad de usar intervalos de guarda (GI) de 0.8 us para tanto 1xLTF como 4xLTF. Esto no significa que pueda utilizar intervalos de guarda más grandes, de hecho, en las tramas capturadas se usan intervalos de 3.2 us mayoritariamente.

- **HE ER SU PDU:** de la misma manera que los bits anteriores el AP indica la posibilidad de usar tramas del tipo HE ER, extended range, que sirven para distancias más largas, con intervalos de guarda de 0.8 us para 1xLTF y 4xLTF.
- **Rx 1024-QAM<242-tone RU:** el AP permite la recepción de modulación 1024-QAM para RUs de 21,52 y 106 portadoras.
- **Rx Full BW SU Using HE MU PDU:** el AP no soporta la recepción de tramas HE-MU con sólo la RU de un único usuario ocupando el ancho de banda entero. Esto, en el análisis de red realizado, en esta sección 7, no se ha podido comprobar, ya que sólo se obtenía la parte de un único usuario debido al problema mencionado con el sniffer. Por tanto, después de ver que estas tramas, Figura 35, sólo utilizan una RU de 106 portadoras sumado a la información de este campo, se puede concluir con que las tramas HE MU que envía el AP contienen datos para más de una estación.

En los campos de **HE-MCS**, se indican las modulaciones soportadas por el AP para los casos de Rx y Tx para anchos de banda menores y mayores que 80 MHz. El resultado en todos los casos es el mismo por lo que el resto de casuísticas no están desplegadas. Están separadas por el número de flujos espaciales, 2 como máximo en el caso de este AP. El cual soporta para la transmisión y recepción MCS de tipo 11 como máximo. Esta se refiere a una modulación 1024-QAM con un code rate de 5/6. Utilizando esta MCS y 160 MHz, se pueden llegar a alcanzar tasas de datos de hasta 2.4 Gbps.

## 8. Evaluación de requisitos

Uno de los objetivos de este proyecto es realizar una evaluación en términos de latencia y fiabilidad sobre una red WiFi 6E para poder comparar los resultados obtenidos con los requisitos industriales. En esta sección se describen primero los parámetros de la implementación que afectan al cumplimiento de estos requisitos en el apartado 8.1. Después, se muestra la evaluación de alguno de estos parámetros para poder maximizar el rendimiento del sistema en 8.2. Más adelante, en el apartado 8.3, se describen las diferentes evaluaciones que se van a realizar y, por último, se presentan los resultados finales en 8.4.

Estos últimos resultados se obtienen tras realizar las mismas pruebas en la banda de 5 GHz y en la de 6 GHz con el estándar 802.11ax. También se realizan pruebas con los mismos canales frecuenciales utilizando el estándar anterior IEEE 802.11ac. Por ello, se obtiene una comparación de las ventajas que introduce tanto el cambio de la banda frecuencial como de las nuevas funcionalidades del último estándar WiFi.

### 8.1. Parámetros de la implementación

En este apartado se describen los parámetros y configuraciones que se pueden modificar sobre la implementación del proyecto para variar el rendimiento en cuanto a latencia del sistema. Estos se pueden modificar tanto desde el SW desarrollado o desde los dispositivos de la red (APs y STAs) como variando la implementación física de la red.

#### 8.1.1. Parámetros del SW desarrollado

Como se menciona en la sección 6.3.4, gracias al SW desarrollado se permiten modificar configuraciones para el envío de tramas. Estas modificaciones son clave para poder evaluar el rendimiento del sistema y buscar la mejor opción para maximizarlo. Estas son las principales:

##### 8.1.1.1. Intervalo entre tramas

El intervalo entre tramas es clave para un sistema de comunicaciones es el tiempo mínimo en el que un dispositivo es capaz de transmitir información. Se trata de un requisito característico de las comunicaciones industriales, como se ha mencionado en la sección 4.2.1. Según [10], para según que clase de aplicación se define un intervalo mínimo, o tasa de actualización, de hasta 500 us (2000 Hz) en el caso más restrictivo.

Se ha comprobado el correcto funcionamiento de este parámetro debido a la

importancia que tiene. Para ello, se han almacenado los tiempos de transmisión de las tramas en el receptor, y estas se han escrito en el mismo fichero donde se escriben las latencias.

Número de secuencia	Latencia (ns)	Tiempo TX (s)	Diferencia (ms)
272761	1701700	1656947680,88537	
272762	1836380	1656947680,89696	11,59000397
272763	1540486	1656947680,90801	11,04998589
272764	1606407	1656947680,91923	11,21997833
272765	1601132	1656947680,93064	11,40999794
272766	34891222	1656947680,94214	11,50012016
272767	33815508	1656947680,95365	11,50989532
272768	32679686	1656947680,96522	11,56997681

**Tabla 4:** Ejemplo de los resultados obtenidos en el fichero de salida del SW.

En la Tabla 4 se muestra un ejemplo de los paquetes guardados en el fichero. En uno de los casos, se da la situación en la que un paquete llega más tarde de lo habitual ( $>3$ ms de latencia) debido a que ha podido ser retransmitido. Como se puede apreciar, esto no afecta a la transmisión del resto de paquetes, ya que se utiliza un sistema no bloqueante en el que no es necesario esperar a la confirmación de un paquete antes de la transmisión del siguiente. En este caso, el intervalo establecido era de 11 ms, que varía debido a que se diseña mediante la función SW *usleep* que introduce un pequeño desvío, no relevante para este sistema.

Al variar el intervalo, el funcionamiento del sistema cambia completamente. Durante el intervalo de tiempo establecido el sistema tiene que ser capaz de procesar una trama, modularla y enviarla por la radio hacia el receptor, este segundo debe realizar el mismo proceso al revés y enviar un ACK confirmando la trama recibida. Todos los sistemas de comunicaciones tienen un límite de intervalo, según las capacidades de los dispositivos, y en la sección 8.2.1 se evalúa el de este sistema.

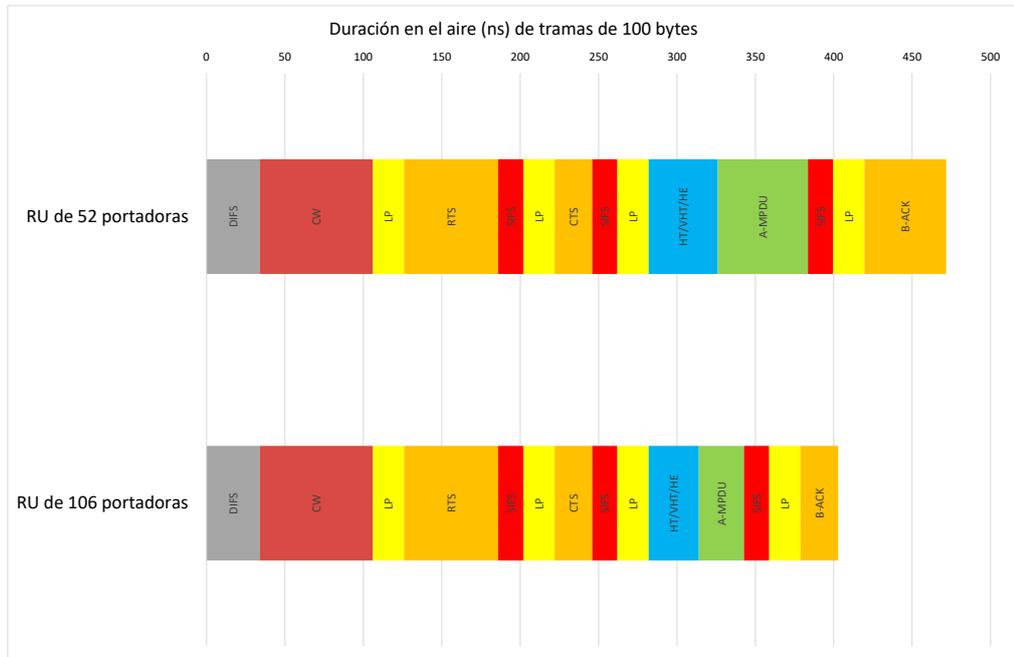
Para obtener un sistema lo más eficiente posible, en este caso, los dispositivos de la red tienen que ser capaces de transmitir un paquete antes de recibir la orden de transmisión del siguiente. De no ser así, se forman colas que con el paso del tiempo se acaban llenando y producen retrasos, además debido a la retransmisiones de WiFi estos retrasos pueden alargarse, lo que es perjudicial para aplicaciones con requisitos críticos de latencia.

### 8.1.1.2. Tamaño de trama

Otro de los parámetros relevantes en un sistema de comunicaciones es el tamaño de los paquetes que se envían. Las aplicaciones industriales no obstante, no requieren de paquetes muy grandes, según [10] el máximo que suelen requerir es de 1024 bytes.

Variar el tamaño de los paquetes afecta a la latencia, cuanto más grande sea, más tiempo está en el aire y más se tarda en procesar. Además es más probable obtener pérdidas al subir el tamaño de los paquetes, ya que las probabilidades de sufrir interferencias o pérdidas por propagación aumentan.

No obstante, teniendo en cuenta que en WiFi 6 los canales pueden ser de 20,40,80 y 160 MHz, de cara a poder apreciar las diferencias entre ellos, es interesante utilizar tramas grandes. Aumentar el tamaño del canal permite reducir el tiempo de las tramas. En WiFi 6 el preámbulo es muy grande, como se aprecia en la Figura 7, y este se envía utilizando 20 MHz. Por tanto, si la parte de datos es pequeña, hay muy poca diferencia de duración de trama entre los canales. Para demostrar esto se ha calculado la duración en el aire de tramas WiFi 6, duplicando el ancho de banda:



**Figura 53:** Cambio de duración de las tramas de 100 bytes al duplicar el tamaño del canal.



**Figura 54:** Cambio de duración de las tramas de 1500 bytes al duplicar el tamaño del canal.

Como se puede apreciar en las Figuras 53 y 54 aumentar el ancho de banda (en este caso utilizando una RU del doble de portadoras), reduce de manera significativa la duración total de las tramas si se envían más datos. En el caso de la Figura 53 la diferencia es de unos 50 ns y en la Figura 54 alrededor de 400 ns. Por ello, de cara a poder apreciar las diferencias al usar canales más grandes, característica clave de la banda de 6 GHz, es más interesante utilizar tramas grandes, de 1500 bytes.

### 8.1.1.3. Número de tramas

El número de tramas a enviar en cada prueba refleja el límite de fiabilidad del sistema. Para cumplir los requisitos de fiabilidad reflejados en [10] es necesario que el número de paquetes de la prueba sea al menos 2 órdenes de magnitud mayor que el requisito. Es decir, si se quiere comprobar que un sistema tiene un PER de  $10^{-7}$ , que como mucho se produce un error cada 10 millones de paquetes, es necesario enviar mil millones de paquetes,  $10^9$ .

El número de tramas que se envían durante una prueba, junto al intervalo entre estas, refleja la duración de una prueba. Cuanto más larga sea, más expuesta está a interferencias de otros dispositivos, así como el movimiento de obstáculos u otros fenómenos en el escenario.

### 8.1.2. Configuraciones de los dispositivos

A continuación se presentan las configuraciones tanto de las estaciones como del AP que afectan de una manera más significativa a la latencia del sistema. Durante el transcurso del proyecto se han probado la gran mayoría de configuraciones y posibilidades que

dan estos dispositivos, y se han determinado estas como las más relevantes en cuanto a latencia:

### 8.1.2.1. Power Management

Una configuración muy relevante del driver WiFi de las estaciones es el modo `power_management`, en español gestión de energía. Se trata de un modo de los componentes internos y externos de los dispositivos. Se utiliza para disminuir el tiempo de uso de ciertos componentes y conseguir así reducir el consumo de energía de los mismos. Se trata en poner en `stanby` tanto el SW como HW en momentos donde no se está usando. A parte del driver WiFi, este proceso se realiza en componentes como el disco duro, display gráfico o el periférico USB. Esto puede no ser demasiado útil para sistemas de alto rendimiento y con requisitos críticos de latencia. En [36], se realiza un estudio de las diferentes técnicas de `power_management` para aplicaciones de alto rendimiento que hay en el mercado y se discute acerca de los problemas que estas presentan.

En Linux, se definen distintos estados de ahorro de energía, que afectan de diferente manera al componente, en [37] se describen todos ellos. En la aplicación de este proyecto, no interesa el uso de este proceso debido a que no conviene poner el receptor en suspensión si se pretende alcanzar la menor latencia posible. No obstante, se ha estudiado la manera en la que esta configuración afecta al rendimiento del sistema de comunicaciones, debido al interés que genera para futuros proyectos del grupo de investigación, esto se realiza en la sección 8.2.2.

Para desactivarlo, se utiliza el siguiente comando del driver `iw`:

```
~$ iw wlan0 set power_save off
```

No obstante, esta configuración se deshace por el propio sistema operativo automáticamente pasado un tiempo. Por ello es necesario programar la ejecución periódica de un script con este comando. En este proyecto se ha creado un fichero propio que es ejecutado mediante la herramienta `crontab` para ello.

Esta configuración afecta de una muy significativa al sistema de comunicaciones, lo cual se analiza y evalúa en el apartado 8.2.2.

### 8.1.2.2. Retransmisiones

La tecnología de WiFi, en todos sus estándares, realiza por su propia cuenta retransmisiones cuando no se ha conseguido confirmar un paquete. Esto, aunque se realice a nivel MAC, se puede configurar, y el desarrollo de este proyecto permite realizarlo. Tan sólo es necesario añadir la siguiente línea al mismo script descrito en la sección anterior:

```
~$ iw phy0 set retry 1 1
```

El uso o no de retransmisiones es una incógnita clave a definir en un sistema de comunicaciones con requisitos de fiabilidad. Las retransmisiones consiguen reducir la tasa de paquetes perdidos pero a su vez pueden aumentar la latencia. Según el método que se siga para la transmisión de los paquetes es útil utilizar retransmisiones o no.

Por ejemplo, si desde la aplicación se transmiten tramas de manera consecutiva sin esperar a la confirmación de cada una de ellas, las retransmisiones a nivel MAC hacen que la latencia de los paquetes siguientes al retransmitido aumente. Esto ocurre en el sistema desarrollado. Como se muestra en la Tabla 4, al haber retransmitido el paquete 272766, los siguientes paquetes tienen también una latencia mayor. Esto ocurre debido a que mientras el driver WiFi sigue recibiendo órdenes de transmisión de paquetes está ocupado retransmitiendo el paquete 272766 y hasta que no recibe su confirmación no transmite los siguientes. Gracias a que los drivers de este sistema son capaces de transmitir los paquetes de la cola de manera inmediata, el error producido se consigue corregir, ya que la latencia se va disminuyendo de manera proporcional al intervalo de transmisión.

No obstante, antes de llegar a la conclusión de utilizar o no retransmisiones, se han realizado pruebas que cuantifican las ventajas y desventajas de este fenómeno, y se muestran en la sección 8.2.3.

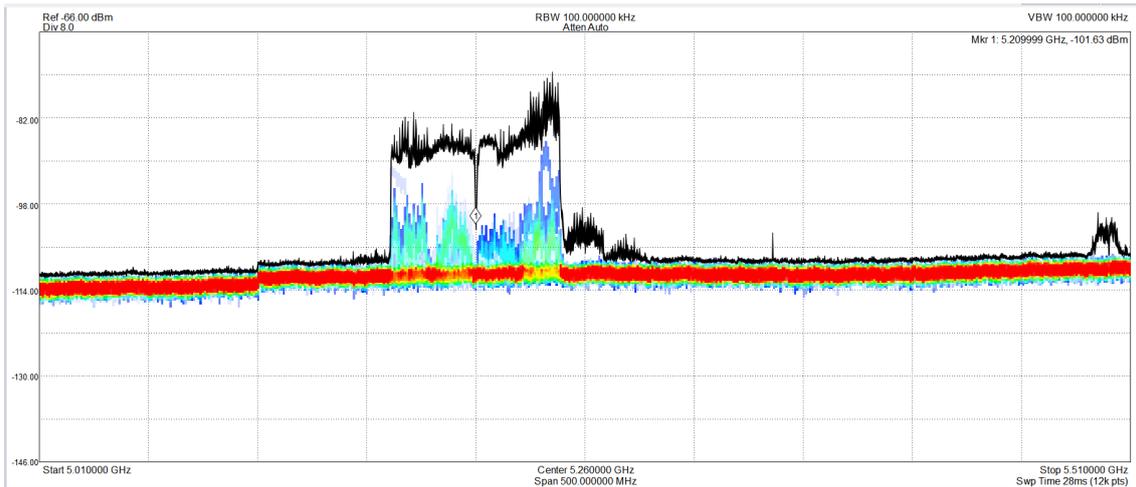
### **8.1.2.3. Canal de radio**

Un aspecto fundamental en una comunicación inalámbrica es la frecuencia utilizada, tanto la central como el ancho de banda. En este proyecto se van a utilizar las bandas de 5 y 6 GHz para canales con distintos anchos de banda, concretamente para 20, 40, 80 y 160 MHz.

El router Aruba utilizado no permite seleccionar canales de 160 MHz en la banda de 5 GHz, a diferencia de en la banda de 6 GHz, que sí que lo permite. No obstante, se añadirá el análisis de este ancho de banda para poder comparar el rendimiento respecto a tamaños más pequeños.

En cuanto a la banda de 6 GHz, ya que no hay ningún dispositivo cercano funcionando a tan alta frecuencia, la elección del canal no es determinante y se han elegido los siguientes canales: 69, 69-, 69E y 69S.

En la banda de 5 GHz, se van a utilizar canales que también los utilicen las redes vecinas a la implementada. Se pretenden analizar las ventajas que conlleva utilizar una banda "libre" respecto a una compartida, por lo que es necesario que haya interferencias de otras redes. Para ello, primero se ha realizado un análisis del canal de radio en la región del espectro donde se ha implementado esta red. Esto se ha realizado mediante un analizador de espectros en tiempo real, ya que muestra tanto la potencia como la persistencia de las señales eléctricas capturadas.



**Figura 55:** Captura del analizador de espectros en tiempo real mostrando los canales vecinos.

La Figura 55 muestra la persistencia en el espectro de las señales que captura. La intensidad de esta es representada por colores, siendo el rojo el más intenso, en este caso el nivel de ruido del canal. La línea negra indica la potencia máxima de las señales en el espectro. Como se puede apreciar, las frecuencias con mayor potencia son entre 5170 y 5250 MHz.

Después de hacer una evaluación del escenario con este analizador de espectros, se concluye con que los canales más utilizados, ordenados por persistencia, son los siguientes:

- Canal 40: 5190–5210 MHz
- Canal 48: 5230–5250 MHz
- Canal 36: 5170–5190 MHz
- Canal 44: 5210–5230 MHz
- Canal 36 de 80 MHz: 5170–5250 MHz

Alrededor de estas frecuencias, el router permite seleccionar estos canales:

BW	Canal	F. Central	F. Inferior	F. Superior
<b>20</b>	36	5180	5170	5190
	40	5200	5190	5210
	44	5220	5210	5230
	48	5240	5230	5250
	52	5260	5250	5270
	56	5280	5270	5290
	60	5300	5290	5310
<b>40</b>	64	5320	5310	5330
	36+	5180	5170	5210
	44+	5220	5210	5250
	52+	5260	5250	5290
<b>80</b>	60+	5300	5290	5330
	36E	5180	5170	5250
	52E	5260	5250	5330

**Tabla 5:** Canales de 5GHz permitidos por el router (Unidades en MHz).

Para intentar utilizar en todas las pruebas un espectro compartido, se van a utilizar los siguientes canales: 40,36+ y 36E.

#### 8.1.2.4. Potencia de Transmisión

Otro parámetro relevante en un sistema de comunicaciones es la potencia con la que se emiten las tramas. En este caso, tanto el AP como las estaciones no permiten transmitir a más de 22 dBm, y esta, será la potencia que se va a utilizar en el proyecto.

Es importante mencionar, que al cambiar el ancho de banda de la red, no se cambia la potencia. Y por ello, se obtiene una relación señal a ruido (SNR) peor. Esto es uno de los motivos principales por los que utilizar canales grandes a día de hoy puede no ser tan eficiente, según lo mencionado en la sección 5.6.

Por tanto, aumentar el ancho de banda del sistema no sólo conlleva ventajas. Debido a la Potencia de transmisión y por lo tanto a la SNR de una comunicación, el ancho de banda seleccionado es un parámetro a tener en cuenta a la hora de definir el escenario más eficiente de un sistema de comunicaciones basado en la tecnología de WiFi 6E.

#### 8.1.3. Setup

Como se detalla en la sección 6.3.1, en este proyecto se han implementado dos setups diferentes para el envío de datos entre el Transmisor y el Receptor. Uno en el que sólo se realiza un salto inalámbrico y otro en el que se realizan dos.

El comportamiento de los dispositivos al utilizar un Setup u otro es diferente, debido a que las tramas no siguen el mismo camino. Se ha comprobado este comportamiento capturando el intercambio de tramas para ambos Setups mediante el Sniffer:

No.	Source address	Destination address	Protocol	Info
112			802.11	Request-to-send, Flags=.....C
113			802.11	Clear-to-send, Flags=.....C
114			802.11	Acknowledgement, Flags=.....C
115	80:45:dd:00:22:e3	80:45:dd:05:4a:29	802.11	QoS Data, SN=22, FN=0, Flags=.p....F.C
116			802.11	802.11 Block Ack, Flags=.....C
117			802.11	Request-to-send, Flags=.....C
118			802.11	Clear-to-send, Flags=.....C
119			802.11	Acknowledgement, Flags=.....C
120	80:45:dd:00:22:e3	80:45:dd:05:4a:29	802.11	QoS Data, SN=23, FN=0, Flags=.p....F.C
121			802.11	802.11 Block Ack, Flags=.....C
122			802.11	Request-to-send, Flags=.....C
123			802.11	Clear-to-send, Flags=.....C
124			802.11	Request-to-send, Flags=.....C
125			802.11	Clear-to-send, Flags=.....C
126			802.11	Acknowledgement, Flags=.....C
127	80:45:dd:00:22:e3	80:45:dd:05:4a:29	802.11	QoS Data, SN=24, FN=0, Flags=.p....F.C
128			802.11	802.11 Block Ack, Flags=.....C

**Figura 56:** Captura del Sniffer para el intercambio de tramas en el Setup 1.

No.	Source address	Destination address	Protocol	Info
174			802.11	Request-to-send, Flags=.....C
175			802.11	Clear-to-send, Flags=.....C
176	80:45:dd:00:2c:2e	80:45:dd:00:22:e3	802.11	QoS Data, SN=3152, FN=0, Flags=.p..R.F.C
177			802.11	802.11 Block Ack, Flags=.....C
178			802.11	Request-to-send, Flags=.....C
179			802.11	Clear-to-send, Flags=.....C
180	80:45:dd:00:2c:2e	80:45:dd:00:22:e3	802.11	QoS Data, SN=3153, FN=0, Flags=.p....F.C
181			802.11	802.11 Block Ack, Flags=.....C
182			802.11	Request-to-send, Flags=.....C
183			802.11	Clear-to-send, Flags=.....C
184	80:45:dd:00:2c:2e	80:45:dd:00:22:e3	802.11	QoS Data, SN=3154, FN=0, Flags=.p....F.C
185			802.11	802.11 Block Ack, Flags=.....C

**Figura 57:** Captura del Sniffer para el intercambio de tramas en el Setup 2.

Como se ve en las Figuras 56 y 57, la diferencia del número de tramas intercambiadas es notable. La secuencia es diferente en ambos casos. Para enviar una trama de datos desde el TX hacia el RX (ver Figura 24, primero el TX envía esta trama hacia el AP (el Sniffer no es capaz de capturarla, pero si la secuencia), además de una secuencia RTS-CTS y un posterior ACK. Después, el AP, envía esta trama hacia el RX, y, como se puede apreciar en las 4 direcciones MAC de la trama de datos, esta trama es mandada por el AP hacia el RX, pero con dirección origen del TX y destino el RX.

En el caso del Setup 2 (ver Figura 25), no se realiza el salto inalámbrico entre el TX y el AP, las tramas van por cable, utilizando Ethernet. Esto reduce el tiempo de latencia total del sistema, ya que se trata de una comunicación mucho más rápida (orden de 100 us) y constante. La secuencia de la Figura 57 muestra como el intercambio de tramas en el aire es más reducido, y el AP envía la misma trama de datos, indicando como dirección origen la del transmisor.

Para evaluar la latencia de la tecnología de WiFi 6E, es más preciso si tan sólo se evalúa un salto inalámbrico, la comunicación entre un AP y una estación, ya que es lo que se implementaría en un sistema de comunicaciones industrial, al tener menor latencia.

## 8.2. Caracterización del rendimiento

De cara a obtener el mejor rendimiento de la tecnología, con el objetivo de poder integrarla en aplicaciones con restricciones temporales críticas, se han realizado pruebas modificando los parámetros mencionados anteriormente. En esta sección se describen estas pruebas y los resultados obtenidos tras su realización. Estas pruebas han servido para conocer e identificar los errores que se producen en la red, así como para intentar definir un escenario en donde no se produzcan.

En estas pruebas, se analizan los resultados mediante el histograma de latencias, descritas en la sección 6.3.6 ya que sirven para caracterizar el comportamiento del sistema de comunicaciones.

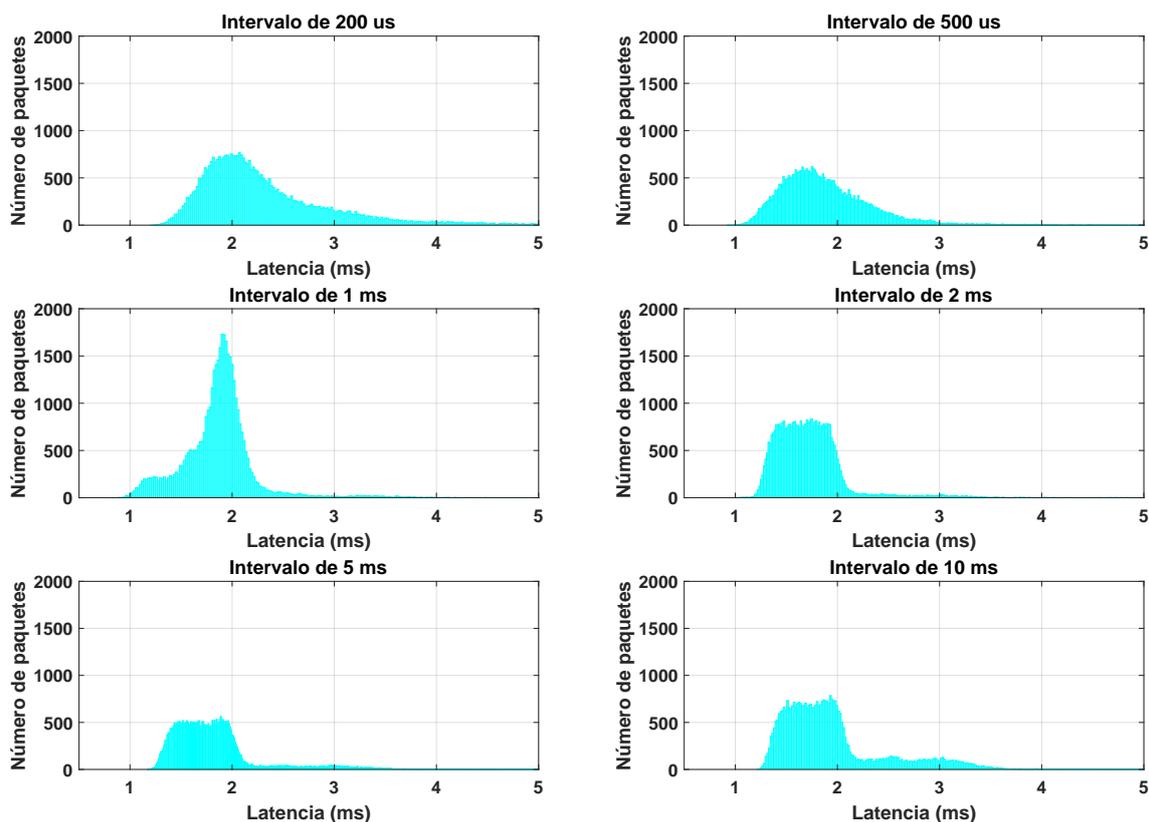
### 8.2.1. Intervalo entre tramas

Como se ha mencionado en la sección 8.1.1.1, uno de los parámetros más importantes para un sistema de comunicaciones, es el tiempo con el que es capaz de transmitir paquetes consecutivos.

En estas prueba se pretende evaluar la diferencia en cuanto a latencia que se obtiene al variar el intervalo entre paquetes transmitidos. Para ello se realiza la misma prueba, utilizando el mismo Setup, canal, tamaño de la trama y número de tramas, variando únicamente el intervalo. Concretamente se utilizan estas características:

- 50000 tramas enviadas.
- Tramas de 1500 bytes.
- Canal de 20 MHz.
- Frecuencia 6295 MHz.
- Potencia TX del AP: 22 dBm.

El histograma de latencias que se obtiene es el siguiente:



**Figura 58:** Representación de los histograma de latencias para diferentes intervalos de transmisión.

Como se aprecia en la Figura 58, el comportamiento del sistema varía según el intervalo. Para intervalos menores que 1 ms, el sistema se encuentra saturado, y se forman colas en la transmisión que retrasan los paquetes de manera progresiva.

Con 1 ms de intervalo, se logra un pico de paquetes con la misma latencia, para el cual el sistema es capaz de enviar los paquetes en el tiempo establecido, no obstante, este pico es alrededor de 2 ms, latencia mayor a la conseguida con intervalos más largos como 2,5 o 10 ms. En estos últimos se obtiene un resultado constante de latencias menores que 2 ms.

Por último, se puede concluir que el sistema de comunicaciones desarrollado se satura al utilizar intervalos menores a 1 ms, siendo este el límite. Por ello, para el resto de pruebas de este proyecto se ha utilizado un intervalo de transmisión de 2 ms.

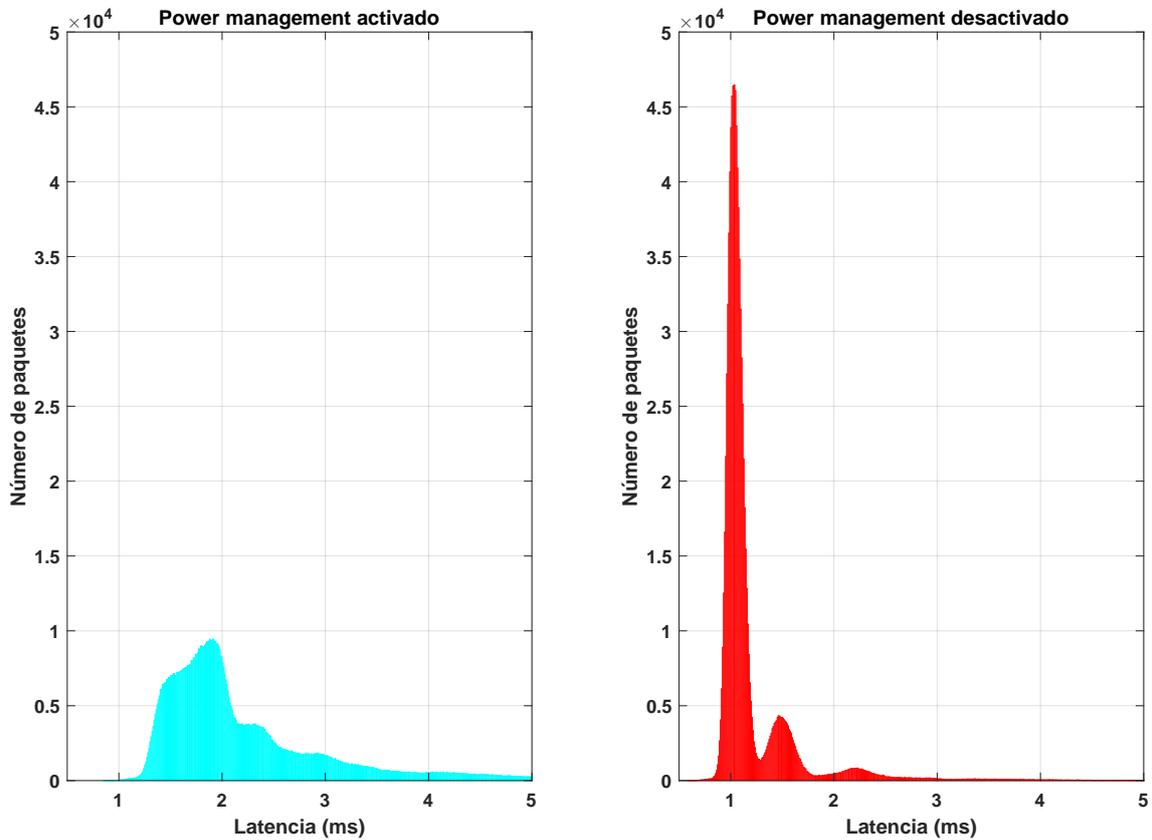
No obstante, el resultado obtenido no es el ideal, ya que este sería un pico de paquetes en la latencia final del sistema de comunicaciones y no uno en el que hay el mismo número de paquetes con latencias de 1 ms de diferencia.

### 8.2.2. Power Management

En esta sección se evalúa el uso de la configuración de `power_management` de las estaciones WiFi del sistema desarrollado. Para ello, se ha realizado la misma prueba variando únicamente esta configuración. Concretamente se utilizan estas características:

- $10^6$  tramas enviadas.
- Intervalos de 2 ms.

- Tramas de 1500 bytes.
- Canal de 20 MHz.
- Frecuencia 6295 MHz.
- Potencia TX del AP: 22 dBm.



**Figura 59:** Representación del histograma de latencias al cambiar la configuración de power\_management.

Se aprecia en la Figura 59 una gran diferencia en el histograma. Al no utilizar este método de ahorro de energía, el comportamiento del sistema es constante, se obtiene una latencia muy cercana al milisegundo en la gran mayoría de paquetes. Esto ocurre debido a que el sistema operativo de los dispositivos da mayor prioridad a las tareas del driver WiFi, y no le limita su funcionamiento. Para un sistema de comunicaciones fiable es clave desactivar el uso de este método, lo que se ha llevado a cabo en este proyecto.

Observando con mayor detalle este último histograma, se pueden ver otros dos picos de paquetes en latencias alrededor de 1.5 y 2.3 ms. Estos son los paquetes que llegan al receptor tras uno o dos intentos de transmisión, son los picos de retransmisiones.

Esta diferencia, es tan notable debido a que la desactivación de esta configuración supone un cambio drástico en el intercambio de tramas de la red. Para ver esto mejor, se han realizado capturas en el Sniffer mientras se realizaban las pruebas anteriores.

No.	Source address	Destination address	Protocol	Info
7			802.11	Request-to-send, Flags=.....C
8			802.11	Clear-to-send, Flags=.....C
9	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=813, FN=0, Flags=.p...F.C
10			802.11	802.11 Block Ack, Flags=.....C
11			802.11	Request-to-send, Flags=.....C
12			802.11	Clear-to-send, Flags=.....C
13	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=814, FN=0, Flags=.p...F.C
14			802.11	802.11 Block Ack, Flags=.....C
15			802.11	Request-to-send, Flags=.....C
16			802.11	Clear-to-send, Flags=.....C
17	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=815, FN=0, Flags=.p...F.C
18			802.11	802.11 Block Ack, Flags=.....C
19			802.11	Request-to-send, Flags=.....C
20			802.11	Clear-to-send, Flags=.....C
21	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=816, FN=0, Flags=.p...F.C
22			802.11	802.11 Block Ack, Flags=.....C
23			802.11	Request-to-send, Flags=.....C
24			802.11	Clear-to-send, Flags=.....C
25	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=817, FN=0, Flags=.p...F.C
26			802.11	802.11 Block Ack, Flags=.....C

**Figura 60:** Captura del Sniffer para el intercambio de tramas utilizando método de power\_management.

Como se puede apreciar en la Figura 60, debido a la secuencia RTS/CTS para enviar 5 tramas de datos se necesita un intercambio entre el TX y RX de 19 tramas.

No.	Source address	Destination address	Protocol	Info
10	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=1802, FN=0, Flags=.p...F.C
11			802.11	802.11 Block Ack, Flags=.....C
12	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=1803, FN=0, Flags=.p...F.C
13			802.11	802.11 Block Ack, Flags=.....C
14	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=1804, FN=0, Flags=.p...F.C
15			802.11	802.11 Block Ack, Flags=.....C
16	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=1805, FN=0, Flags=.p...F.C
17			802.11	802.11 Block Ack, Flags=.....C
18	80:45:dd:00:2c:2e	80:45:dd:00:22:e2	802.11	QoS Data, SN=1806, FN=0, Flags=.p...F.C
19			802.11	802.11 Block Ack, Flags=.....C

**Figura 61:** Captura del Sniffer para el intercambio de tramas desactivando el método de power\_management.

Como se puede apreciar en la Figura 61, se utilizan 10 tramas para enviar 5 de datos, ya que no se utilizan RTS/CTS, lo que justifica la mejora del comportamiento del sistema en cuanto a latencia que se aprecia en los histogramas de la Figura 59.

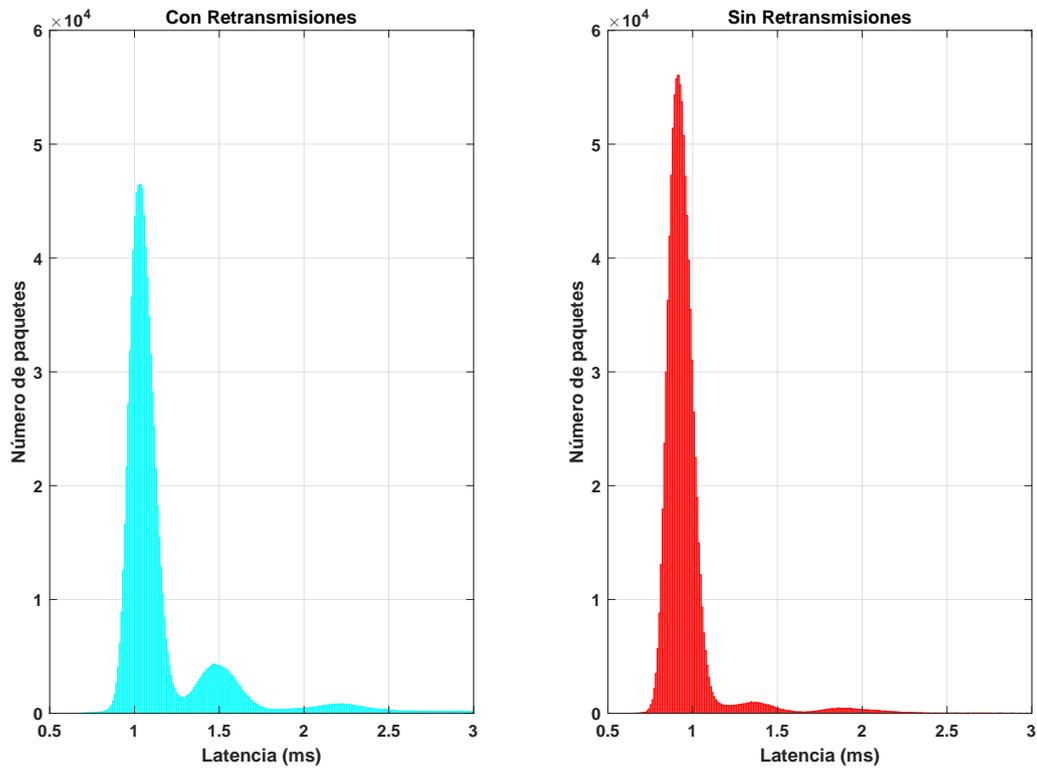
### 8.2.3. Retransmisiones

En esta sección se estudia el uso de retransmisiones en el sistema de comunicaciones. Para ello se han realizado pruebas idénticas activando y desactivando las retransmisiones como se explica en la sección 8.1.2.2. Las pruebas tienen las siguientes características:

- 10<sup>6</sup> tramas enviadas.
- Intervalos de 2 ms.
- Power Management desactivado.
- Tramas de 1500 bytes.
- Canal de 20 MHz.

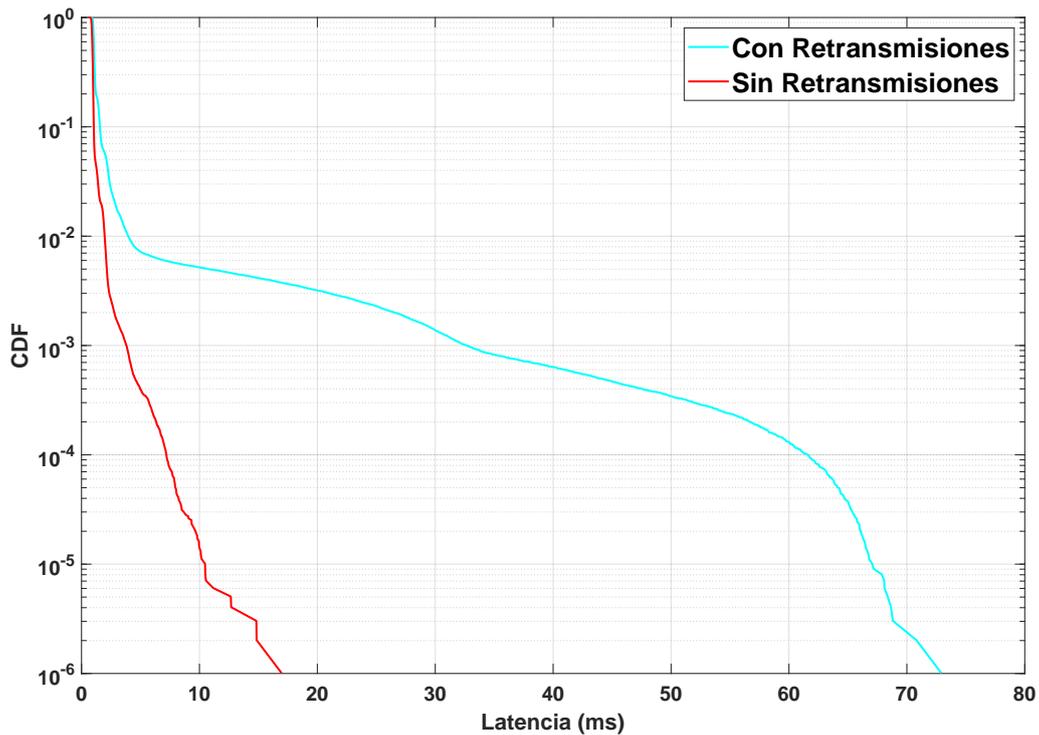
- Frecuencia 6295 MHz.
- Potencia TX del AP: 22 dBm.

En este caso se va a evaluar la fiabilidad del sistema, debido a que las retransmisiones afectan de manera determinante la pérdida de paquetes. Se van a analizar los paquetes perdidos como los que superan un cierto umbral de latencia, para ello se va a representar la curva CDF de latencias en ambos casos. Los histogramas obtenidos son los siguientes:



**Figura 62:** Representación del histograma de latencias al cambiar la configuración de retransmisiones.

En cuanto a la fiabilidad del sistema, se obtienen estos resultados:



**Figura 63:** Representación de las curvas CDF de latencias al cambiar la configuración de retransmisiones.

Como se puede observar, la diferencia es notable. Una retransmisión no sólo hace que el paquete retransmitido tenga mayor latencia, si no que afecta a los paquetes siguientes y, si se producen varias retransmisiones seguidas, la latencia cada vez es mayor.

No obstante, no todo es positivo, al utilizar retransmisiones afecta al PER del sistema. Se pierden menos paquetes al enviar varias veces los no confirmados. Mediante al sistema de procesamiento de los resultados descrito en la sección 6.3.6, se pueden contabilizar los paquetes perdidos en la transmisión, y para estas pruebas este es el resultado:

	Con Retransmisiones	Sin Retransmisiones
<b>Enviados</b>	$10^6$	$10^6$
<b>Perdidos</b>	0	$3 \rightarrow 3 \cdot 10^{-4}$
<b>&gt;50 ms</b>	$341 \rightarrow 3,41 \cdot 10^{-4}$	$3 \rightarrow 3 \cdot 10^{-6}$
<b>&gt;20 ms</b>	$5139 \rightarrow 5,139 \cdot 10^{-3}$	$17 \rightarrow 1,7 \cdot 10^{-5}$
<b>&gt;4 ms</b>	$9738 \rightarrow 9,738 \cdot 10^{-3}$	$813 \rightarrow 8,13 \cdot 10^{-4}$

**Tabla 6:** Resultados obtenidos al activar y desactivar las retransmisiones del driver WiFi.

### 8.3. Descripción de evaluaciones

En este apartado se describen las características de las pruebas que se van a realizar para evaluar la latencia de la red WiFi 6E implementada en este proyecto. Según lo establecido al comienzo del proyecto, estas pruebas tienen dos objetivos, comparar la mejora de utilizar la banda libre de 6 GHz frente a la de 5 GHz, así como los límites de esta

última mejora y comparar la mejora que supone utilizar las funcionalidades del estándar 802.11ax.

### **8.3.1. Primera evaluación, banda de 6 GHz frente a 5 GHz**

Mediante estas pruebas se pretende analizar la reducción de latencia que supone utilizar una banda libre como la de 6 GHz frente a una compartida por otras redes como es la de 5 GHz. Para ello, se han enviado paquetes desde un Transmisor hacia un Receptor utilizando el Setup 2 descrito en 6.3.1 y las siguientes configuraciones de las disponibles por la red:

- $10^6$  tramas enviadas.
- Tramas de 1500 bytes: se van a enviar tramas tan grandes para poder comparar mejor el resultado entre canales diferentes.
- Intervalo de 2 ms.
- Canales de 20,40,80 y 160 MHz.
- Frecuencia 6295 MHz.
- Escenario libre: no habrá otros dispositivos conectados al AP.
- Potencia TX del AP: 22 dBm.

En total se van a realizar 4 pruebas para la banda de 6 GHz y 3 para la de 5 GHz. Se enviarán un total de 7 millones de paquetes, para los que se obtendrán resultados de perdidos y retrasados según los límites establecidos por [10], de 4, 20 y 50 ms. Es decir, se van a obtener datos para los 3 umbrales, contabilizando como erróneos los paquetes perdidos más los que superan estos umbrales de latencia. Además se utilizarán los métodos de análisis descritos en 6.3.6 para poder obtener unas conclusiones más completas sobre los resultados.

### **8.3.2. Segunda evaluación, 802.11ax frente a 802.11ac**

Uno de los objetivos del proyecto es evaluar las nuevas funcionalidades del estándar 802.11ax. Para ello, es necesario compararlas con versiones anteriores en el mismo escenario y con las mismas facilidades. Estas pruebas en concreto tienen el objetivo de comprobar la mejora en latencia y fiabilidad que proporciona el estándar, por lo que se evaluarán el número de paquetes perdidos y que superan unos determinados umbrales de latencia.

Para hacer una evaluación del rendimiento de OFDMA, que es la principal diferencia entre el estándar 802.11ax y 802.11ac, es necesario emular una situación en donde en teoría esta tecnología es más determinante. Como se menciona en la sección 5.3 esto ocurre para transmisiones Multi User (MU). Esta situación se da cuando hay varios dispositivos en la red enviando con bastante frecuencia tramas pequeñas, ya que al compartir los recursos frecuenciales en teoría se reducen los tiempos de espera y por tanto la latencia. Por tanto, las características comunes para todas estas pruebas son las siguientes:

- $10^6$  tramas enviadas.
- Tramas de 100 bytes.
- Intervalo de 2 ms.
- Canales de 20,40,80: se utilizan exactamente los mismos canales para ambas pruebas, descritos en la sección 8.1.2.3.
- Frecuencia 5180 MHz.
- Red compartida: habrá dos estaciones conectadas al AP, transmitiendo tramas de 100 bytes cada 10 ms.
- Potencia TX del AP: 22 dBm.

La única diferencia entre las pruebas de 802.11ax y 802.11ac es la tecnología que utiliza el AP. El AP permite deshabilitar la opción de utilizar HE (High Efficiency) en la red, que es el término técnico de 802.11ax. Al deshabilitar el uso de HE, todos los dispositivos conectados al AP no podrán enviar tramas con formato HE, ya que este les indica en los beacons que no es compatible con la última versión del estándar. Por tanto, utilizan la tecnología de VHT (Very High Throughput) con OFDM para la transmisión de datos, el estándar IEEE 802.11ac.

En total se envían 6 millones de paquetes en estas pruebas, 3 para cada caso, separando pruebas de canales de 20,40 y 80 MHz. Se van a analizar tanto los histogramas como el cumplimiento de los requisitos de latencia de las aplicaciones. No obstante, mediante estas pruebas no se pretenden cumplirlos, si no comparar en cuanto se acerca esta nueva tecnología 802.11ax hacia ellos frente a la anterior 802.11ac. Para la representación de los resultados se vuelve a utilizar el método descrito en 6.3.6.

### **8.3.3. Tercera evaluación, requisitos industriales**

Por último, se ha evaluado el sistema desarrollado en este proyecto en el mejor escenario posible y utilizando las características que mejores resultados logran para poder determinar si cumple los requisitos de [10].

Para ello, se va a realizar una prueba más larga que las anteriores, en la cual se van a enviar un total de 30 millones de paquetes. Este número, para poder demostrar el cumplimiento de los límites de  $10^{-6}$  de los requisitos, debería ser de al menos de  $10^8$ , no obstante, debido al intervalo utilizado, de 2 ms, es inviable hacer esta prueba debido a la duración de este proyecto, ya que esta duraría 555 horas (más de 23 días).

En esta evaluación se van a utilizar tramas más pequeñas, de 100 bytes ya que no es necesario comparar el resultado entre diferentes canales, así como el canal de 160 MHz en la banda de 6 GHz, ya que según lo obtenido en la primera evaluación 8.4.1 es la manera de obtener el número de errores más bajo. EN resumen, las características de esta evaluación son las siguientes:

- $3 \cdot 10^7$  tramas enviadas.
- Tramas de 100 bytes.
- Intervalo de 2 ms.

- Canal de 160 MHz.
- Frecuencia 6295 MHz.
- Escenario libre.
- Potencia TX del AP: 22 dBm.

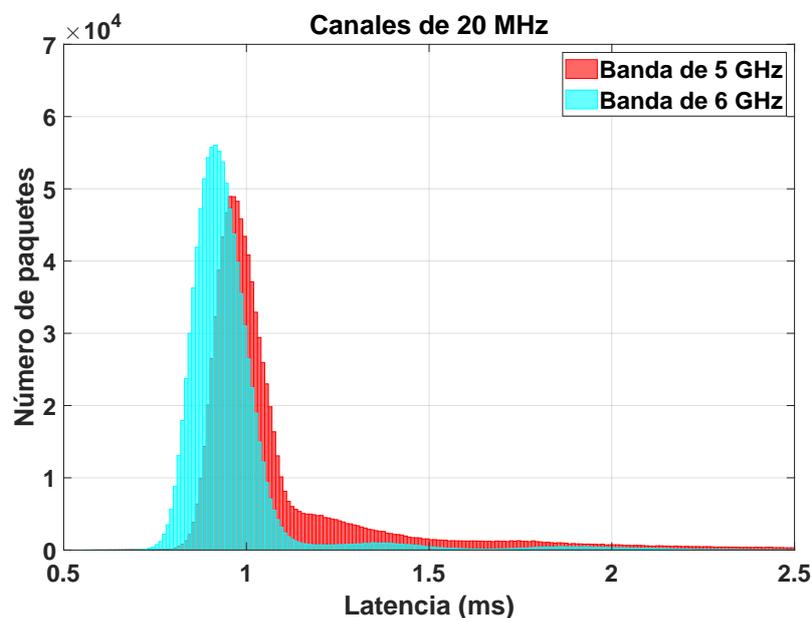
En este caso, tan solo se van a mostrar los resultados numéricos, debido a que el comportamiento es el mismo que en la primera evaluación 8.4.1 y debido a que esta evaluación está dividida en varias pruebas, debido al tiempo que se necesita para llevar a cabo esta evaluación.

## 8.4. Resultados

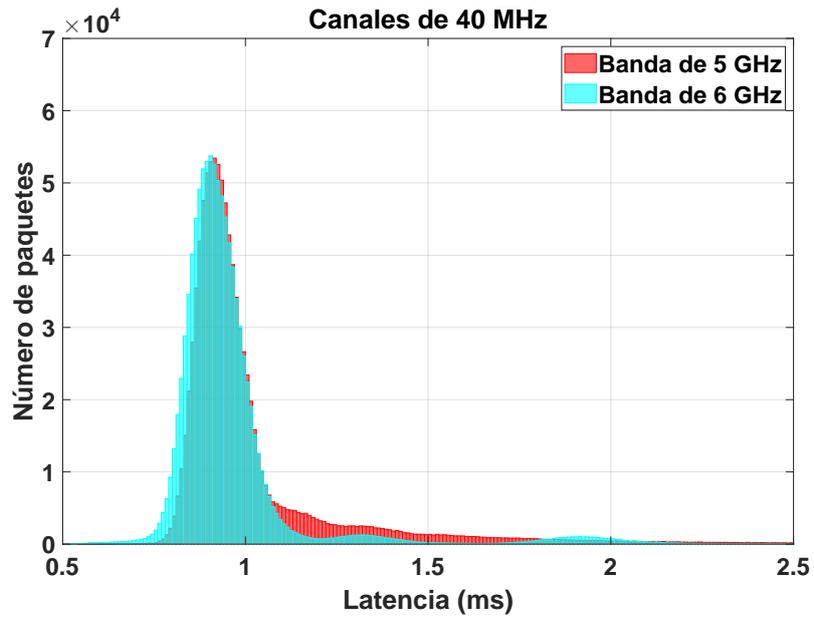
En esta sección se presentan los resultados de las pruebas descritas en la sección anterior.

### 8.4.1. Primera Evaluación, banda de 6 GHz frente a la banda de 5 GHz

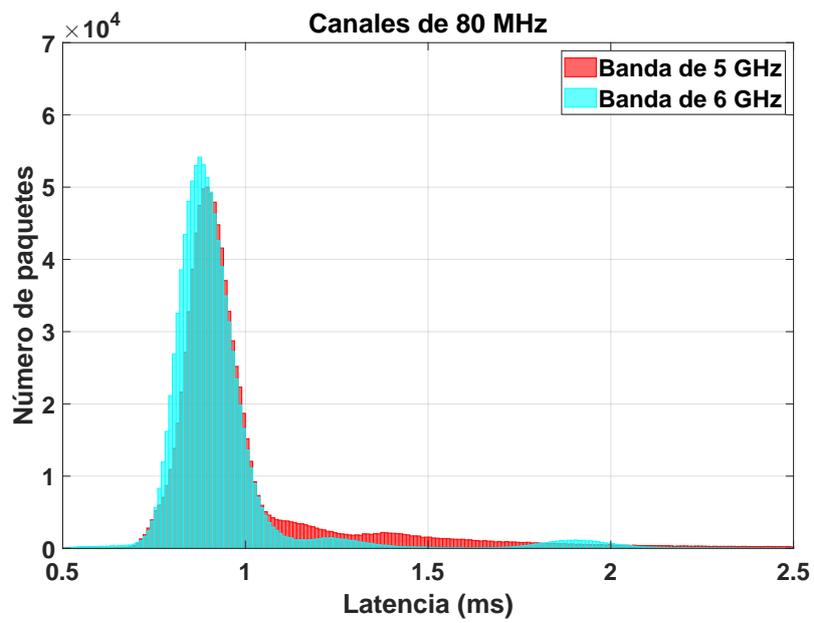
Primero se muestra el histograma de latencias menores que 2.5 ms, las que se obtienen para más del 99% de los paquetes enviados.



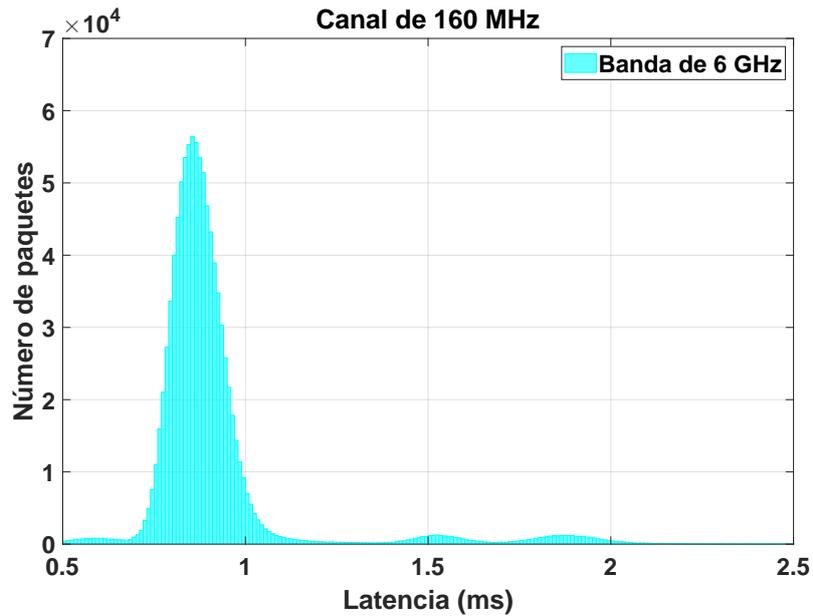
**Figura 64:** Representación del histograma para 20 MHz de la primera evaluación.



**Figura 65:** Representación del histograma para 40 MHz de la primera evaluación.



**Figura 66:** Representación del histograma para 80 MHz de la primera evaluación.



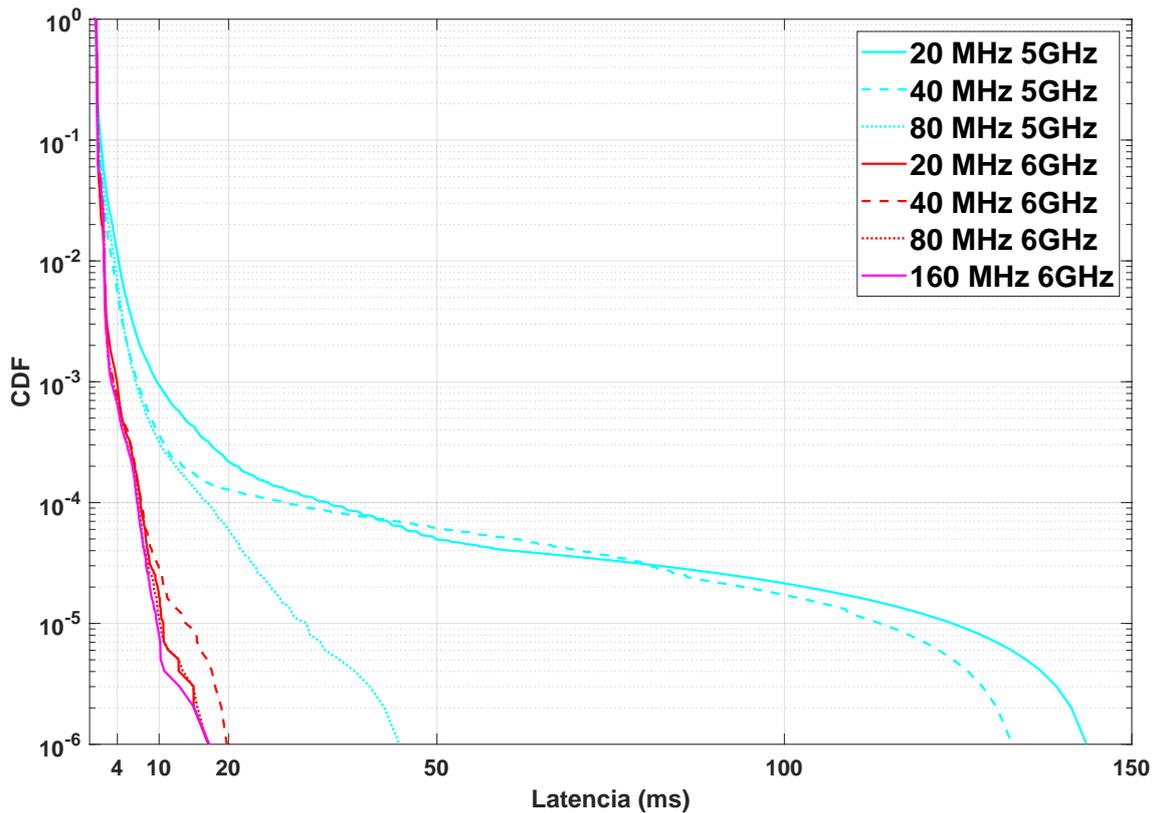
**Figura 67:** Representación del histograma para 160 MHz de la primera evaluación.

Como se puede apreciar, se observa un comportamiento parecido en ambas bandas. Una pequeña diferencia, son los picos de paquetes, en donde son ligeramente más altos en la banda de 6 GHz. El número de paquetes que tienen la misma latencia, alrededor de 1 ms, es mayor en el caso de 6 GHz. Esto significa que se obtiene un resultado más uniforme al utilizar un banda libre. Esto se aprecia también en latencias mayores que el "pico", ya que en el caso de 5 GHz se obtienen más paquetes fuera de esta mayoría que en el de 6 GHz. Esto supone una mejora en cuanto al determinismo del sistema al utilizar la banda de 6 GHz.

Además, estos picos de paquetes son ligeramente más rápidos en la banda de 6 GHz que en la de 5 GHz, lo que supone que los paquetes que se muestran en estas capturas tienen menor latencia en la banda de 6 GHz.

A la hora de diferenciar entre los anchos de banda evaluados, no se aprecia gran diferencia entre ellos, tan sólo para el canal de 20 MHz en la banda de 5 GHz se representa un resultado notablemente menos determinista. Debido a que hay más paquetes que superan la latencia del milisegundo.

Para poder ver los límites de latencia más estrictos, se utiliza la representación acumulada. De esta manera se pueden apreciar las diferencias que no se notan al representar el histograma.



**Figura 68:** Representación de las curvas CDF de los resultados de la primera evaluación.

Como se observa en la Figura 68 se obtienen unos resultados significativamente mejores en la banda de 6 GHz. Esta diferencia es más representativa en los límites inferiores, a partir del 99.9% de los paquetes ( $10^{-3}$ ).

Al estar compartiendo el espectro por dispositivos ajenos a la red, existe la posibilidad de que no se logre transmitir en el instante ordenado. Esto puede provocar colas en la transmisión del driver WiFi de los dispositivos, ya que las órdenes de transmisión las realiza el nivel de aplicación. Esto tan sólo ocurre en el caso de la banda de 5 GHz, y se puede apreciar mediante la gráfica de la Figura 64 la mejora que supone dejar de compartir el espectro.

Para cuantificar estas diferencias se obtienen los siguiente resultados numéricos, en los que se muestran tanto el número de errores como la tasa de errores para cada caso:

Banda de 6 GHz				
Canal	20 MHz	40 MHz	80 MHz	160 MHz
Enviados	$10^6$	$10^6$	$10^6$	$10^6$
Perdidos	13 $\rightarrow$ $1,3 \cdot 10^{-5}$	12 $\rightarrow$ $1,2 \cdot 10^{-5}$	19 $\rightarrow$ $1,9 \cdot 10^{-5}$	12 $\rightarrow$ $1,2 \cdot 10^{-5}$
>50 ms	13 $\rightarrow$ $1,3 \cdot 10^{-5}$	12 $\rightarrow$ $1,2 \cdot 10^{-5}$	19 $\rightarrow$ $1,9 \cdot 10^{-5}$	12 $\rightarrow$ $1,2 \cdot 10^{-5}$
>20 ms	13 $\rightarrow$ $1,3 \cdot 10^{-5}$	13 $\rightarrow$ $1,3 \cdot 10^{-5}$	19 $\rightarrow$ $1,9 \cdot 10^{-5}$	12 $\rightarrow$ $1,2 \cdot 10^{-5}$
>4 ms	936 $\rightarrow$ $9,36 \cdot 10^{-4}$	747 $\rightarrow$ $7,47 \cdot 10^{-4}$	661 $\rightarrow$ $6,61 \cdot 10^{-4}$	639 $\rightarrow$ $6,39 \cdot 10^{-4}$

**Tabla 7:** Resultados obtenidos en la banda de 6 GHz para las pruebas de la primera evaluación.

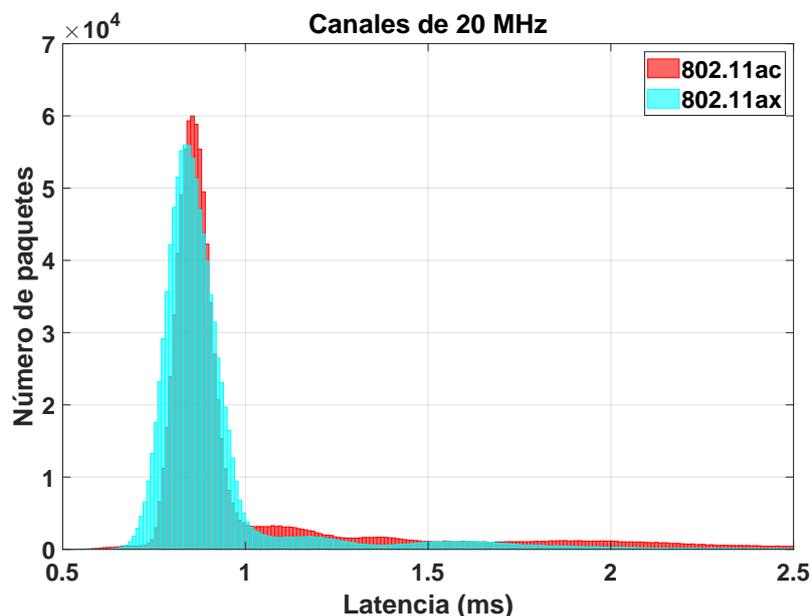
Banda de 5 GHz			
Canal	20 MHz	40 MHz	80 MHz
Enviados	$10^6$	$10^6$	$10^6$
Perdidos	$41 \rightarrow 4,1 \cdot 10^{-5}$	$16 \rightarrow 1,6 \cdot 10^{-5}$	$18 \rightarrow 1,8 \cdot 10^{-5}$
>50 ms	$90 \rightarrow 9 \cdot 10^{-5}$	$77 \rightarrow 7,7 \cdot 10^{-5}$	$18 \rightarrow 1,8 \cdot 10^{-5}$
>20 ms	$262 \rightarrow 2,62 \cdot 10^{-4}$	$305 \rightarrow 2,05 \cdot 10^{-4}$	$77 \rightarrow 7,7 \cdot 10^{-5}$
>4 ms	$11543 \rightarrow 1,15 \cdot 10^{-2}$	$5546 \rightarrow 5,55 \cdot 10^{-3}$	$6661 \rightarrow 6,67 \cdot 10^{-3}$

**Tabla 8:** Resultados obtenidos en la banda de 5 GHz para las pruebas de la primera evaluación.

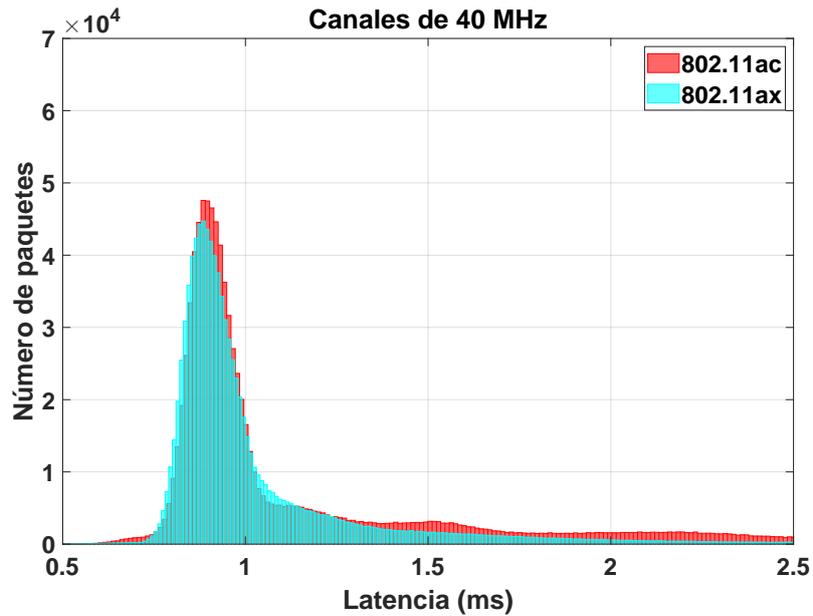
Estos resultados se obtienen sumando los perdidos con los que superan los umbrales establecido por las aplicaciones industriales (4,20 y 50 ms). Como se puede apreciar, en ninguno de los casos se pueden cumplir los requisitos de  $10^{-6}$  o  $10^{-7}$  establecidos por [10]. No obstante, se confirma la mejora que supone utilizar la banda de 6 GHz en cuanto a robustez de un sistema de comunicaciones. Esta tecnología (WiFi 6 E) no cumple los requisitos generales de la industria, pero supone una aproximación hacia ellos.

#### 8.4.2. Segunda Evaluación, 802.11ax vs 802.11ac

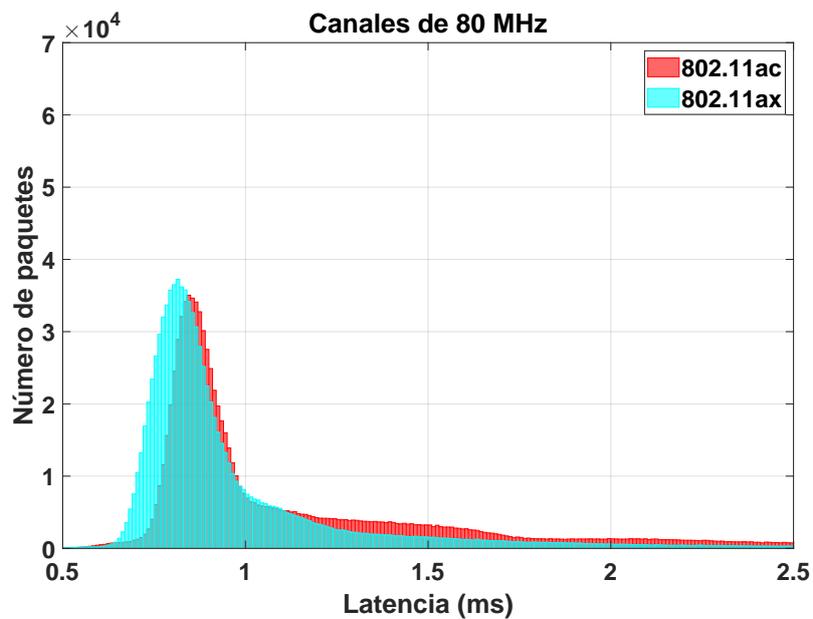
Primero se muestra el histograma de latencias menores que 2.5 ms, las que se obtienen para más del 99 % de los paquetes enviados.



**Figura 69:** Representación del histograma para 20 MHz de la segunda evaluación.



**Figura 70:** Representación del histograma para 40 MHz de la segunda evaluación.



**Figura 71:** Representación del histograma para 80 MHz de la segunda evaluación.

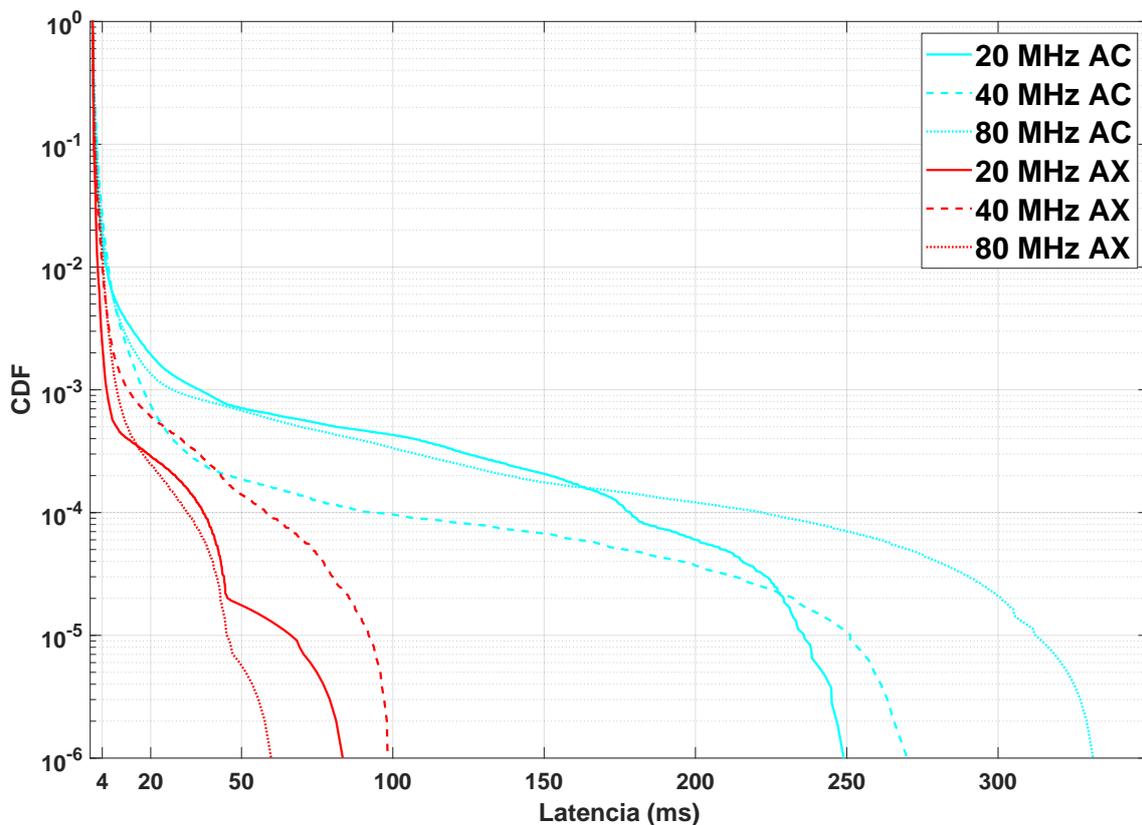
En las Figuras anteriores no se aprecia apenas diferencia entre los resultados de las tecnologías evaluadas. El pico del histograma en el caso del 802.11ac está ligeramente desplazado hacia la derecha, y hay más paquetes en las latencias que se alejan de este pico, pero con muy poca diferencia. Lo que supone que el comportamiento de la red es similar utilizando ambas tecnologías. Se esperaba una mejora en el comportamiento de la red más representativa, debido al uso de OFDMA frente a OFDM en situaciones de 4 clientes.

Lo que si que se puede apreciar en este caso, es la diferencia entre usar canales grandes de 80 MHz frente a los de 40 y 20 MHz. El resultado obtenido en el caso de 80 MHz es menos determinista, el pico de paquetes en el intervalo de latencias es menor, es decir, hay más paquetes con latencia superior a la habitual, lo que implica que el

comportamiento de la red es diferente.

Como se menciona en la sección 5.6, utilizar un canal más grande puede ser perjudicial. En la banda de 5 GHz, los routers comerciales no utilizan canales superiores a 40 MHz, ya que es más complicado encontrar el espectro libre para transmitir. En esta evaluación, hay 4 clientes WiFi intentando transmitir información constantemente, y, al utilizar canales más grandes, al AP le resulta más complicado encontrar el canal libre para hacerlo. Esto justifica por qué en los histogramas de la primera evaluación 8.4.1 no se encuentran apenas diferencias entre los canales, ya que tan sólo hay un dispositivo (el Transmisor de la prueba) transmitiendo en la red.

Analizando las latencias mediante la representación acumulada de manera logarítmica, obtenemos lo siguiente:



**Figura 72:** Representación de las curvas CDF de los resultados de la segunda evaluación.

Como se muestra en la Figura 72 en este caso sí que son notorias las diferencias entre las tecnologías. En ninguna de los se acercan a cumplir los requisitos industriales, ya que todas superan los 50 ms para  $10^{-6}$ . La diferencia se aprecia sobre todo en el 1% de los paquetes ( $10^{-6}$ ), en donde en las pruebas de la tecnología 802.11ac empiezan a aparecer latencias que superan ya los umbrales de estas aplicaciones industriales.

Por tanto, según lo evaluado en este proyecto se puede afirmar que en las mismas condiciones, la nueva versión del estándar IEEE 802.11ax supera al estándar IEEE 802.11ac en términos de bounded latency.

### 8.4.3. Tercera Evaluación, 802.11ax vs 802.11ac

Según lo explicado en la sección 8.3.3, esta tercera evaluación tiene una duración muy superior al resto, y, para la cual, tan sólo se muestra el resultado obtenido en cuanto a latencia y fiabilidad de manera numérica. Los resultados son los siguientes:

Tercera Evaluación	
Enviados	$3 \cdot 10^7$
Perdidos	$233 \rightarrow 7,767 \cdot 10^{-6}$
>50 ms	$233 \rightarrow 7,767 \cdot 10^{-6}$
>20 ms	$410 \rightarrow 1,367 \cdot 10^{-5}$
>4 ms	$18209 \rightarrow 6,07 \cdot 10^{-4}$

**Tabla 9:** Resultados obtenidos en las pruebas de la tercera evaluación.

Como se puede apreciar, no se cumplen los requisitos de la industria de  $10^{-6}$  o  $10^{-7}$  en ninguno de los umbrales. No obstante, el sistema de comunicaciones desarrollado en este proyecto, cumple el requisito de tasa de errores (PER) del  $10^{-5}$  considerando como erróneos los paquetes perdidos y los que superan la latencia de 50 ms. Esto supone una mejora circunstancial en la tecnología WiFi, y por tanto se puede concluir con el que el uso de una banda libre como es la de 6 GHz, la tecnología WiFi 6E, supone un acercamiento del estándar IEEE 802.11 para ser utilizado en aplicaciones con requisitos estrictos de latencia y fiabilidad.

## 9. Conclusiones

En este proyecto se ha logrado implementar una red que utiliza la tecnología IEEE 802.11ax en la banda de 6 GHz. El objetivo del proyecto ha sido evaluar esta tecnología para el cumplimiento de requisitos industriales de latencia y fiabilidad. Para ello, se han seguido los siguientes pasos, cumpliendo los objetivos establecidos en el apartado 3:

- **Analizar el estado del arte:** se han estudiado las propiedades de las comunicaciones en la industria, así como las soluciones cableadas actuales. De cara a las comunicaciones inalámbricas, se han estudiado los requisitos que establece el NIST [10] y se han encontrado 3 soluciones que cumplen estos requisitos: w-SHARP, Wireless HP y WIA-FA. Por último, se han detallado los últimos avances en la línea de investigación referente a la integración de las tecnologías comerciales WiFi y 5G en la industria.
- **Estudiar las mejoras del IEEE 802.11ax:** se han explicado las mejoras tanto en la capa MAC como PHY de la última versión del estándar IEEE 802.11.
- **Implementar una red WiFi 6E:** se ha logrado implementar mediante el material proporcionado por la empresa Ikerlan una red WiFi 6 en la banda de 6 GHz con 4 clientes.
- **Analizar mediante capturas el uso del estándar IEEE 802.11ax:** se ha comprobado y analizado el uso de la tecnología de OFDMA (única en 802.11ax dentro del estándar 802.11) tanto en Uplink como Downlink en la red implementada. También se han analizado los procesos de Sounding y envío de Beacons con las nuevas funcionalidades de WiFi 6E.
- **Evaluación de parámetros críticos asociados a redes industriales:** se han llevado a cabo pruebas sobre la implementación para maximizar el rendimiento en cuanto a latencia y fiabilidad de la red. Por último, se han realizado evaluaciones que han servido para cuantificar la mejora de a estos parámetros críticos que proporciona el uso de la banda libre de 6 GHz frente a la de 5 GHz, mostrada en las Tablas 7 y 8, en las que para el umbral de latencia de 4 ms se mejora en dos órdenes de magnitud (de  $10^{-2}$  a  $10^{-4}$ ) la tasa de errores. Además, en el apartado 8.4.2 se representan el resultado del uso de las nuevas características del estándar IEEE 802.11ax frente al anterior IEEE 802.11ac. En este caso, se ha obtenido una mejora notable en cuanto a bounded latency, de  $10^{-3}$  a  $10^{-5}$  para el umbral de 50 ms.

Comparando el resultado obtenido en el mejor escenario de la implementación con los requisitos industriales establecidos por el NIST [10] se concluye que esta tecnología, en su máximo rendimiento, no es capaz de lograr tasas de errores de  $[10^{-6}, 10^{-7}]$  para los umbrales de latencia 4,20 y 50 ms. No obstante, en este proyecto se demuestra cómo

esta tecnología logra cumplir una tasa de errores de  $10^{-5}$  para el umbral de latencia de 50 ms.

Esta tecnología, a diferencia de las mencionadas en el estado del arte como w-SHARP[15], no está orientada al tráfico industrial, en donde se priorizan el uso de paquetes pequeños con muy baja latencia y sin errores. Por ello, es más difícil alcanzar estos requisitos. No obstante, el resultado obtenido supone una aproximación hacia el cumplimiento de estos requisitos, ya que el uso de la banda de 6 GHz ha aportado un salto a esta tecnología como se demuestra en este trabajo.

WiFi en la banda de 6GHz parte con ventaja ante tecnologías específicas como w-SHARP. Hay cientos de fabricantes y 18 billones de dispositivos [22] actualmente, es una tecnología asimilada por el mercado que ofrecerá unos precios y un acceso con el que las tecnologías específicas como w-SHARP no podrán competir. El coste de implementación de soluciones inalámbricas en la industria será considerablemente menor utilizando WiFi.

Para la realización con éxito de este proyecto, han sido clave los conocimientos adquiridos en algunas de las asignaturas del máster de Sistemas Electrónicos Avanzados. Han sido tales como la metodología en formación e investigación, programación en C, Linux y cifrado de comunicaciones. Además, la formación acerca de conceptos como latencia, determinismo y TSN adquiridos en la especialidad de comunicaciones han servido para comprender de una manera más sencilla las propiedades de las comunicaciones industriales. De esto se concluye que después de realizar este proyecto se ha logrado profundizar en todas estas líneas de aprendizaje.

## 10. Líneas futuras

De la manera en la que se ha concluido este proyecto, se puede decir que la tecnología de WiFi 6E no es capaz de cumplir el requisito de bounded latency de las aplicaciones industriales. No obstante, se ha comprobado que el uso de la banda de 6 GHz y de las capacidades de la última versión del estándar IEEE 802.11ax suponen un primer paso hacia ello.

La siguiente versión del estándar IEEE 802.11 es IEEE 802.11be, más conocido como WiFi 7. Esta, como se menciona en la sección 4.2.3.1, a parte de aumentar la tasa de datos, pretende reducir la latencia y aumentar determinismo en las redes WiFi. Por ello, la línea futura natural de este proyecto es la evaluación de redes WiFi 7, ya que sobre esta tecnología se permite también el uso de los canales de la banda de 6 GHz, mejorando, en teoría, los resultados de este proyecto. No obstante, no se espera que se complete este protocolo hasta 2024 y, por tanto, el trabajo actual sobre esta tecnología está en las simulaciones de estas nuevas funcionalidades como Multi-Link, y su posterior análisis en cuanto a fiabilidad y latencia como se realiza en el trabajo de [19].

No obstante, existen más líneas de investigación y desarrollo a partir de este proyecto. Una de ellas es el uso de sistemas redundados para cumplir los requisitos de la industria, tal y como se puede apreciar en [38] y [39]. Las redundancias permiten desarrollar sistemas más seguros, ya sea mediante redundancias de diferentes tecnologías (utilizar WiFi y otra tecnología como, por ejemplo, 5G) o mediante diferentes frecuencias (utilizar diferentes canales al mismo tiempo). Gracias al desarrollo de este proyecto, se podría integrar el mismo en otro sistema de comunicaciones logrando así un sistema redundado capaz de superar los resultados de latencia y fiabilidad este proyecto.

Además, debido a que el desarrollo de la red y de la plataforma se han llevado a cabo con el material proporcionado por el equipo de investigación de Ikerlan, este proyecto servirá como punto de partida para futuros desarrollos de esta tecnología en el equipo.

# 11. Referencias

- [1] A. Larrañaga, M. C. Lucas-Estañ, I. Martinez, I. Val, and J. Gozalvez, "Analysis of 5G-TSN Integration to Support Industry 4.0," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, pp. 1111–1114, 2020.
- [2] P. Sanz, O. Seijo, M. C. Llorente, J. Montalban, P. Angueira, and I. Val, "On the Feasibility of Wireless Communications for Safety Applications in Industry," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2022.
- [3] O. Seijo, X. Iturbe, and I. Val, "SHARP: Implementation of a Hybrid Wired-Wireless TSN Network to Enable Flexible Smart Factories," in *2021 17th IEEE International Conference on Factory Communication Systems (WFCS)*, pp. 95–98, 2021.
- [4] Z. Lin and S. Pearson, "An inside look at industrial Ethernet communication protocols," p. 7, 2018.
- [5] D. B. Mateu, D. Hallmans, M. Ashjaei, A. V. Papadopoulos, J. Proenza, and T. Nolte, "Clock Synchronization in Integrated TSN-EtherCAT Networks," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, pp. 214–221, 2020.
- [6] G. S. Sestito, A. C. Turcato, A. L. Dias, P. Ferrari, and M. M. da Silva, "Evaluating Real-Time Ethernet performance indicators for SERCOS III networks," in *2021 14th IEEE International Conference on Industry Applications (INDUSCON)*, pp. 1191–1197, 2021.
- [7] T. Müller and H. D. Doran, "PROFINET Real-Time Protection Layer: Performance Analysis of Cryptographic and Protocol Processing Overhead," in *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, pp. 258–265, 2018.
- [8] "IEEE 802.1 Time-Sensitive Networking Task Group." <https://www.ieee802.org/1/pages/tsn.html>.
- [9] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, 2017.
- [10] K. Montgomery, R. Candell, Y. Liu, and M. Hany, "Wireless User Requirements for the Factory Workcell," 2019-10-02 2019.
- [11] "IEC 62948:2017 - Industrial networks - Wireless communication network and communication profiles - WIA-FA."

- [12] W. Liang, M. Zheng, J. Zhang, H. Shi, H. Yu, Y. Yang, S. Liu, W. Yang, and X. Zhao, "WIA-FA and Its Applications to Digital Factory: A Wireless Network Solution for Factory Automation," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 1053–1073, 2019.
- [13] Z. Pang, M. Luvisotto, and D. Dzung, "Wireless High-Performance Communications: The Challenges and Opportunities of a New Target," *IEEE Industrial Electronics Magazine*, vol. 11, no. 3, pp. 20–25, 2017.
- [14] M. Luvisotto, Z. Pang, and D. Dzung, "High-Performance Wireless Networks for Industrial Control Applications: New Targets and Feasibility," *Proceedings of the IEEE*, vol. 107, no. 6, pp. 1074–1093, 2019.
- [15] O. Seijo, J. A. López-Fernández, and I. Val, "w-SHARP: Implementation of a High-Performance Wireless Time-Sensitive Network for Low Latency and Ultra-low Cycle Time Industrial Applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3651–3662, 2021.
- [16] M. K. Atiq, R. Muzaffar, O. Seijo, I. Val, and H.-P. Bernhard, "When ieee 802.11 and 5g meet time-sensitive networking," *IEEE Open Journal of the Industrial Electronics Society*, vol. 3, pp. 14–36, 2022.
- [17] D.-J. Deng, Y.-P. Lin, X. Yang, J. Zhu, Y.-B. Li, J. Luo, and K.-C. Chen, "IEEE 802.11ax: Highly Efficient WLANs for Intelligent Information Infrastructure," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 52–59, 2017.
- [18] D. Lopez-Perez, A. Garcia-Rodriguez, L. Galati-Giordano, M. Kasslin, and K. Doppler, "IEEE 802.11be Extremely High Throughput: The Next Generation of Wi-Fi Technology Beyond 802.11ax," *IEEE Communications Magazine*, vol. 57, no. 9, pp. 113–119, 2019.
- [19] G. Lacalle, I. Val, O. Seijo, M. Mendicute, D. Cavalcanti, and J. Perez-Ramirez, "Analysis of Latency and Reliability Improvement with Multi-Link Operation over 802.11," in *2021 IEEE 19th International Conference on Industrial Informatics (INDIN)*, pp. 1–7, 2021.
- [20] "What Is 5G, and How Fast Will It Be?" <https://web.archive.org/web/20190124041504/https://www.howtogeek.com/340002/what-is-5g-and-how-fast-will-it-be/>.
- [21] "System architecture for the 5G System (5GS) Stage 2 (Release 16) 3GPP TS 23.501 V16.4.0," *Technical Specification Group Services and System Aspects*, March 2020.
- [22] "Wi-Fi Alliance® 2022 Wi-Fi® trends | Wi-Fi Alliance." <https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-2022-wi-fi-trends>.
- [23] H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," *IEEE Transactions on Communications*, vol. 28, no. 4, pp. 425–432, 1980.
- [24] S. Brahmi, M. Yazid, and M. Omar, "Multiuser Access via OFDMA Technology in High Density IEEE 802.11ax WLANs: A Survey," in *2020 Second International Conference on Embedded and Distributed Systems (EDiS)*, pp. 105–110, 2020.
- [25] Y. Al-jawhar, *An implementation of peak to average power ratio reduction for multicarrier system (orthogonal frequency division multiplexing)*. PhD thesis, 11 2017.

- [26] IEEE Standards Association, "IEEE 802.11ax-2021: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN," 2021.
- [27] H. Bolcskei, "MIMO-OFDM wireless systems: basics, perspectives, and challenges," *IEEE Wireless Communications*, vol. 13, no. 4, pp. 31–37, 2006.
- [28] X. Guo, S. Wang, H. Zhou, J. Xu, Y. Ling, and J. Cui, "Performance Evaluation of the Networks with Wi-Fi based TDMA Coexisting with CSMA/CA," *Wireless Personal Communications*, vol. 114, 09 2020.
- [29] D. Van Ingen, "Wi-Fi 6E in Europe: Frequently Asked Questions | Aruba Blogs." <https://blogs.arubanetworks.com/solutions/wi-fi-6e-in-europe-frequently-asked-questions/>, Jan. 2021.
- [30] Extreme Networks, "Liverpool Football Club Selects Extreme to Kick Up Fan Experiences at Historic Anfield Stadium." <https://www.extremenetworks.com/liverpool/>, 2022.
- [31] "GB-BRi7H-8550 (rev. 1.0) Overview | Mini-PC Barebone (BRiX) - GIGABYTE Global." <https://www.gigabyte.com/Mini-PcBarebone/GB-BRi7H-8550-rev-10>.
- [32] "Intel® Wi-Fi 6E AX210 (Gig+) Especificaciones de productos." <https://www.intel.es/content/www/es/es/products/sku/204836/intel-wifi-6e-ax210-gig/specifications.html>.
- [33] "Aruba 650 Series Wi-Fi 6E APs." <https://www.arubanetworks.com/products/wireless/access-points/indoor-access-points/650-series/>.
- [34] Institute of Electrical and Electronics Engineers, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," *IEEE Std 1588-2019 (Revision of IEEE Std 1588-2008)*, pp. 1–499, 2020.
- [35] H. Yang, D.-J. Deng, and K.-C. Chen, "Performance analysis of ieee 802.11ax ul ofdma-based random access mechanism," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1–6, 2017.
- [36] Y. Liu and H. Zhu, "A survey of the research on power management techniques for high-performance systems," *Software: Practice and Experience*, vol. 40, no. 11, pp. 943–964, 2010.
- [37] "Power Management in Linux-Based Systems | Linux Journal." <https://www.linuxjournal.com/article/6699>.
- [38] M. Lucas-Estañ, J. Maestre, B. Coll-Perales, J. Gozalvez, and I. Lluvia, "An Experimental Evaluation of Redundancy in Industrial Wireless Communications," in *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, pp. 1075–1078, 2018.
- [39] M. C. Lucas-Estañ, B. Coll-Perales, and J. Gozalvez, "Redundancy and Diversity in Wireless Networks to Support Mobile Industrial Applications in Industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 311–320, 2021.