



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO

EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

**“EVALUACIÓN DEL RENDIMIENTO DE LA TECNOLOGÍA 802.11 AX
MEDIANTE UN TESBED PARA EL LABORATORIO DE LA MATERIA DE
COMUNICACIÓN INALÁMBRICA”**

AUTOR: ADONIS BLADIMIR NARVÁEZ ZAMBRANO

DIRECTOR: Msc. CARLOS ALBERTO VÁSQUEZ AYALA

IBARRA- ECUADOR

2023

IDENTIFICACIÓN DE LA OBRA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Identificación de la obra

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DEL CONTACTO			
CÉDULA DE IDENTIDAD	100415333-2		
APELLIDOS Y NOMBRES	Narváez Zambrano Adonis Bladimir		
DIRECCIÓN	San Antonio		
E-MAIL	abnarvaezz@utn.edu.ec		
TELÉFONO FIJO		TELÉFONO MOVIL	0983751533

DATOS DE LA OBRA	
TÍTULO	EVALUACIÓN DEL RENDIMIENTO DE LA TECNOLOGÍA 802.11 AX MEDIANTE UN TESBED PARA EL LABORATORIO DE LA MATERIA DE COMUNICACIÓN INALÁMBRICA
AUTOR	Narváez Zambrano Adonis Bladimir
FECHA	27/02/2023
PROGRAMA	Pregrado
TÍTULO	Ingeniero en Electrónica y Redes de Comunicación
DIRECTOR	Msc. Carlos Alberto Vásquez

CONSTANCIA**UNIVERSIDAD TÉCNICA DEL NORTE****CONSTANCIAS**

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 9 días del mes de mayo del 2023

EL AUTOR:

A handwritten signature in blue ink, appearing to read "Adonis Narváez", is written over a horizontal line.

Adonis Bladimir Narváez Zambrano

C.I. 100415333-2

CERTIFICACIÓN

CERTIFICACIÓN



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Certificación

MAGISTER CARLOS ALBERTO VÁSQUEZ AYALA, DIRECTOR DEL PRESENTE
TRABAJO DE TITULACIÓN CERTIFICA:

Que, el presente trabajo de titulación “EVALUACIÓN DEL RENDIMIENTO DE LA
TECNOLOGÍA 802.11 AX MEDIANTE UN TESBED PARA EL LABORATORIO DE LA
MATERIA DE COMUNICACIÓN INALÁMBRICA”, ha sido desarrollado por el señor Adonis
Bladimir Narvárez Zambrano, bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

A handwritten signature in blue ink, appearing to read "C. Vásquez", is written over a horizontal dotted line.

Msc. Carlos Alberto Vásquez

CI:100242498-2

Director

DEDICATORIA

Este trabajo se lo dedico a mis padres,

“A mi amado padre, quien siempre fue mi modelo a seguir en la vida. Gracias por todo lo que me enseñaste, por tu amor incondicional y apoyo en cada momento de mi vida. Esta dedicatoria es en tu honor, para que sepas que siempre estarás vivo en mi corazón, siempre estarán presentes tus enseñanzas, valores y recuerdos que me darán la fuerza para seguir adelante.

Y a mi madre, quien ha sido fuente de amor y apoyo incondicional, todo lo que soy es gracias a ti, por tu entrega y por siempre estar para mí. Eres la mejor madre del mundo.”

Los amo mucho.

Adonis Narváez

AGRADECIMIENTO

Primero quiero expresar mi gratitud a Dios, gracias por todas las bendiciones que ha derramado sobre mí, por la salud y protección que me ha brindado durante toda mi vida.

Agradezco de corazón a las personas más importantes en mi vida, mi padre Segundo (†), mi madre Margarita, mis hermanos Luis, Richard y Ronald, y mi tío Washi, quienes han sido mi apoyo constante en cada paso que he dado, gracias por estar siempre ahí conmigo, con sus palabras de aliento, consejos y apoyo incondicional. ¡Gracias por ser mi familia, los amo!

Quiero expresar toda mi gratitud a mi compañera de vida Cintya, quien ha sido un pilar fundamental en el logro de esta meta, gracias por ser mi amiga, confidente y más que todo mi apoyo. Gracias por estar a mi lado en los buenos y malos momentos, por apoyarme y por darme tu amor incondicional. Eres la persona más importante en mi vida, espero poder seguir construyendo una vida llena de amor a tu lado. Te amo “A&C”.

También agradezco a mi tutor de tesis Msc. Carlos Vásquez por toda la guía en el desarrollo de este proyecto, así mismo por toda la sabiduría y consejos brindados durante la carrera, más que un docente lo considero un amigo.

Agradezco a la Sra. Guadalupe Espinosa, quien en los últimos años ha sido fundamental en mi vida, gracias por estar siempre al pendiente de mí.

Por último, agradezco a mis amigos con quienes compartí mi vida universitaria, a mi amigo Bryan Maigua, Armando Chandi, Wilmer Benavides, Axel Almeida, Freddy Chicaiza y Christofer Macas, los cuales hicieron que esta etapa universitaria sea la mejor.

ÍNDICE

IDENTIFICACIÓN DE LA OBRA.....	II
CONSTANCIA	III
CERTIFICACIÓN	IV
DEDICATORIA	V
AGRADECIMIENTO.....	VI
ÍNDICE	VII
ÍNDICE DE FIGURAS.....	XI
ÍNDICE DE TABLAS	XVII
RESUMEN.....	XIX
ABSTRACT.....	XX
1. Capítulo 1: Antecedentes	21
1.1. Tema	21
1.2. Planteamiento del problema.....	21
1.3. Objetivos.....	23
1.3.1. <i>Objetivo General</i>	23
1.3.2. <i>Objetivos específicos</i>	23
1.4. Alcance	24
1.5. Justificación	27
2. Capítulo II: Marco teórico.....	28
2.1. Redes inalámbricas.....	28
2.1.1. <i>Introducción a las redes inalámbricas</i>	28
2.1.2. <i>Tipos de redes inalámbricas</i>	29
2.1.3. <i>Redes de área Local (WLAN)</i>	30

2.2.	Estándar 802.11	31
2.2.1.	<i>Introducción</i>	31
2.2.2.	<i>Arquitectura 802.11</i>	31
2.2.2.1.	Estación (STA)	32
2.2.2.2.	Punto de acceso (AP).....	33
2.2.2.3.	Basic Service Set (BSS)	33
2.2.2.4.	Distribution System (DS)	34
2.2.2.5.	Extended service set (ESS).....	35
2.2.3.	<i>Capa física</i>	36
2.2.3.1.	Espectro radioeléctrico	36
2.2.3.2.	Tecnologías de transmisión	36
2.2.3.3.	Protocolos de capa física	42
2.2.4.	<i>Capa de enlace</i>	46
2.2.4.1.	Capa MAC (Media Access Control)	47
2.2.4.2.	Capa LLC (Logical Link Control).....	58
2.3.	IEEE 802.11 ax	58
2.3.1.	<i>1024 QAM</i>	58
2.3.2.	<i>OFDMA</i>	59
2.3.2.1.	RU (Resource Unit).....	61
2.3.3.	<i>MU-MIMO</i>	62
2.3.3.1.	DL MU-MIMO.....	63
2.3.3.2.	UP MU-MIMO	63
2.3.4.	<i>BSS Coloring</i>	64
2.3.5.	<i>TWT (Target Wake Time)</i>	65
3.	Capítulo III: Requerimientos y Diseño	69

3.1. Análisis.....	69
3.1.1. Metodología en cascada.....	69
3.1.2. Tesbed.....	70
3.1.2.1. Objetivo del tesbed.....	71
3.1.2.2. Etapas.....	71
3.1.3. Características de la tecnología.....	72
3.1.4. Requerimientos.....	73
3.1.5. Stakeholders.....	73
3.1.6. Requerimientos de stakeholders.....	74
3.1.7. Requerimientos de sistema.....	75
3.1.8. Requerimientos de arquitectura.....	76
3.2. Alcance de la propuesta.....	78
3.2.1. Restricciones.....	78
3.2.2. Riesgos.....	78
3.3. Desarrollo de la propuesta.....	79
3.3.1. Selección de hardware.....	79
3.3.2. Selección de software.....	82
4. Capítulo IV: Implementación y pruebas.....	105
4.1. Implementación de la red Ad-hoc.....	105
4.2. Implementación de la red de infraestructura.....	106
4.3. Implementación de la red mesh.....	109
4.4. Instalación y configuración de las herramientas.....	113
4.5. Implementación de pruebas.....	113
4.5.1. Red ad-hoc sin interferencia.....	113
4.5.2. Ad-hoc con interferencia.....	121

4.5.3. Infraestructura sin interferencia	125
4.5.4. Infraestructura con interferencia	131
4.5.5. Mesh sin interferencia	135
4.5.6. Mesh con interferencia	139
4.5.7. Captura de paquetes	142
4.5.8. Análisis de espectro.....	154
4.6. Guías de laboratorio.....	158
4.6.1. Guía 1: “Instalación y configuración de Raspberry PI OS”	159
4.6.2. Guía 2: “Levantamiento red en modo ad-hoc e infraestructura”	162
4.6.3. Guía 3: “Levantamiento red mesh”	166
4.6.4. Guía 4: “Instalación y configuración de D-ITG, jperf y wireshark.”	169
4.6.5. Guía 5: “Métricas de rendimiento en red de infraestructura”	174
4.6.6. Guía 6: “Captura de marcos 802.11ax”	176
CONCLUSIONES	179
RECOMENDACIONES	180
REFERENCIAS.....	181
ANEXOS.....	186

ÍNDICE DE FIGURAS

Figura 1 <i>Clasificación de las redes inalámbricas según su alcance</i>	29
Figura 2 <i>Esquema de una WLAN con AP y Estaciones</i>	30
Figura 3 <i>Estándares del grupo 802.x y en que capas del modelo OSI trabajan</i>	31
Figura 4 <i>Arquitectura IEEE 802.11 con sus componentes</i>	32
Figura 5 <i>Esquema de un BSS según IEE Std. 802.11</i>	34
Figura 6 <i>Esquema de un Distribution System con sus componentes</i>	35
Figura 7 <i>Esquema de un ESS con sus componentes principales.</i>	36
Figura 8 <i>División de canales de FHSS</i>	38
Figura 9 <i>Proceso de ensanchamiento de DSSS</i>	39
Figura 10 <i>Distribución de canales en DSSS</i>	39
Figura 11 <i>Canales que no se superponen unos a otros</i>	40
Figura 12 <i>Amplitudes de las subportadoras</i>	41
Figura 13 <i>Formato de la PPDU DSSS</i>	44
Figura 14 <i>Formato de PPDU de HR/DSSS largo y corto</i>	45
Figura 15 <i>Formato de PPDU de OFDM</i>	46
Figura 16 <i>Capas y subcapas Física y enlace de datos</i>	47
Figura 17 <i>Funciones de coordinación</i>	48
Figura 18 <i>Funcionamiento de CSMA/CA</i>	49
Figura 19 <i>Problema de estación oculta</i>	50
Figura 20 <i>Intercambio de mensajes RTS/CTS</i>	51
Figura 21 <i>Formato de la trama MAC</i>	53
Figura 22 <i>Formato del frame de control</i>	54
Figura 23 <i>Diagrama de constelaciones de 4, 16, 32 y 64 QAM</i>	59

Figura 24	<i>OFDM vs OFDMA</i>	60
Figura 25	<i>Número de RU en un canal de 20 MHz</i>	62
Figura 26	<i>Funcionamiento de MU-MIMO, operan con varios usuarios.</i>	63
Figura 27	<i>Interferencia OBSS</i>	64
Figura 28	<i>Proceso de asignación de color en un OBSS.</i>	65
Figura 29	<i>Proceso de TWT entre un AP y una estación.</i>	66
Figura 30	<i>Acuerdo TWT individual</i>	67
Figura 31	<i>Acuerdo TWT broadcast</i>	68
Figura 32	<i>Huawei AX3 Quad Core</i>	80
Figura 33	<i>Placa Raspberry Pi</i>	81
Figura 34	<i>Antena Intel AX200</i>	82
Figura 35	<i>Diagrama de bloques del tesbed.</i>	84
Figura 36	<i>Diagrama de bloques de los nodos</i>	85
Figura 37	<i>Flujograma de los nodos</i>	86
Figura 38	<i>Diagrama de bloques del sniffer</i>	87
Figura 39	<i>Diagrama de flujo del sniffer</i>	88
Figura 40	<i>Placa Raspberry</i>	89
Figura 41	<i>Deshabilitar eMMC boot</i>	90
Figura 42	<i>Instalación de rpiboot</i>	90
Figura 43	<i>Página oficial de Raspberry</i>	91
Figura 44	<i>Selección del Sistema Operativo</i>	91
Figura 45	<i>Selección del almacenamiento</i>	92
Figura 46	<i>Escritorio de Raspberry Pi OS</i>	92
Figura 47	<i>Reconocimiento del puerto PCIe</i>	93

Figura 48 <i>Asignación de espacio</i>	93
Figura 49 <i>Escenario 1 Modo Ad-hoc</i>	96
Figura 50 <i>Topología de la red Ad-hoc</i>	97
Figura 51 <i>Escenario 2 Modo Infraestructura sin interferencia</i>	97
Figura 52 <i>Topología de la red en modo infraestructura</i>	98
Figura 53 <i>Escenario 3 Modo ad-hoc con interferencia</i>	99
Figura 54 <i>Escenario 4 Modo Infraestructura con interferencia</i>	99
Figura 55 <i>Escenario 5 Red mesh sin interferencia</i>	100
Figura 56 <i>Topología de la red mesh</i>	101
Figura 57 <i>Escenario 6 Red mesh con interferencia</i>	101
Figura 58 <i>Conexión Ad-Hoc</i>	106
Figura 59 <i>Configuración del AP</i>	107
Figura 60 <i>Configuración de la red Wifi</i>	107
Figura 61 <i>Redes disponibles</i>	108
Figura 62 <i>Conexión de clientes al AP</i>	108
Figura 63 <i>Configuración de MESH</i>	112
Figura 64 <i>Asignación de IP a la interfaz bat0</i>	112
Figura 65 <i>Vecinos de la red mesh</i>	112
Figura 66 <i>Verificación de la comunicación entre nodos</i>	113
Figura 67 <i>Configuración del nodo 1</i>	114
Figura 68 <i>Configuración del nodo 3</i>	115
Figura 69 <i>Ping del nodo 1 al nodo 3</i>	115
Figura 70 <i>Información de la interfaz wlan0</i>	116
Figura 71 <i>Configuración del servidor con iperf</i>	116

Figura 72 <i>Configuración del cliente con iperf</i>	117
Figura 73 <i>Informe de ancho de banda</i>	118
Figura 74 <i>Gráfico de ancho de banda</i>	118
Figura 75 <i>Bitrate modo ad-hoc sin interferencia</i>	119
Figura 76 <i>Jitter en modo ad-hoc sin interferencia</i>	119
Figura 77 <i>Delay en modo ad-hoc son interferencia</i>	120
Figura 78 <i>Paquetes perdidos en modo ad-hoc</i>	121
Figura 79 <i>Ancho de banda modo ad-hoc con interferencia</i>	122
Figura 80 <i>Variaciones del ancho de banda</i>	122
Figura 81 <i>Bitrate en un entorno con interferencia</i>	123
Figura 82 <i>Jitter en modo ad-hoc con interferencia</i>	124
Figura 83 <i>Delay en modo ad-hoc con interferencia</i>	124
Figura 84 <i>Conexión en modo infraestructura</i>	126
Figura 85 <i>Verificación de la comunicación</i>	126
Figura 86 <i>Ancho de banda modo infraestructura</i>	127
Figura 87 <i>Variación del ancho de banda</i>	127
Figura 88 <i>Bitrate en modo infraestructura sin interferencia</i>	128
Figura 89 <i>Jitter en modo infraestructura sin interferencia</i>	129
Figura 90 <i>Delay en modo infraestructura sin interferencia</i>	129
Figura 91 <i>Pérdida de paquetes</i>	130
Figura 92 <i>Ancho de banda en infraestructura con interferencia</i>	131
Figura 93 <i>Bitrate en infraestructura con interferencia</i>	132
Figura 94 <i>Jitter en infraestructura con interferencia</i>	133
Figura 95 <i>Delay en infraestructura con interferencia</i>	134

Figura 96	<i>Pérdida de paquetes en infraestructura con interferencia</i>	135
Figura 97	<i>Variación del ancho de banda</i>	136
Figura 98	<i>Bitrate en red mesh sin interferencia</i>	137
Figura 99	<i>Jitter en una red mesh sin interferencia</i>	138
Figura 100	<i>Delay en una red mesh sin interferencia</i>	138
Figura 101	<i>Ancho de banda en red mesh con interferencia</i>	139
Figura 102	<i>Bitrate en red mesh con interferencia</i>	140
Figura 103	<i>Jitter en red mesh con interferencia</i>	141
Figura 104	<i>Delay en red mesh con interferencia</i>	141
Figura 105	<i>Beacon frame</i>	143
Figura 106	<i>HE Capabilities</i>	143
Figura 107	<i>HE MAC Capabilities</i>	144
Figura 108	<i>Ancho del canal soportado</i>	145
Figura 109	<i>HE Operation - BSS Color</i>	145
Figura 110	<i>Variables para MSC con OFDM</i>	146
Figura 111	<i>Variables para MSC con OFDMA</i>	147
Figura 112	<i>Información de marcos 802.11ax</i>	148
Figura 113	<i>Índice MSC</i>	149
Figura 114	<i>Intervalo de guarda y Ancho de canal</i>	150
Figura 115	<i>Número de flujos espaciales</i>	151
Figura 116	<i>Modulación en la transmisión</i>	151
Figura 117	<i>Valor de la velocidad de datos.</i>	152
Figura 118	<i>Información del beacon</i>	153
Figura 119	<i>Auth AKM Management</i>	154

Figura 120 Análisis del espectro Wifi.	155
Figura 121 <i>Mapa de calor</i>	155
Figura 122 <i>Señal del canal 1</i>	156
Figura 123 <i>Análisis del canal 11</i>	157
Figura 124 <i>Mapa de calor canal 11</i>	157
Figura 125 <i>Señal del canal 11</i>	158
Figura 126 <i>Página para descargar D-ITG</i>	186
Figura 127 <i>Descarga de la GUI de D-ITG</i>	187
Figura 128 <i>Configuración de transmisor</i>	188
Figura 129 <i>Configuración del receptor</i>	188
Figura 130 <i>Pantalla principal de jPerf</i>	189
Figura 131 <i>Verificar conexión a Adalm-Pluto SDR</i>	190
Figura 132 <i>Pantalla de GNU Radio Companion</i>	190
Figura 133 <i>Parámetros para el análisis espectral</i>	191
Figura 134 <i>Graficas de las señales obtenidas(FFT y mapa de calor)</i>	191
Figura 135 <i>Tabla MCS con OFDM</i>	194

ÍNDICE DE TABLAS

Tabla 1 <i>Tipo, subtipo y descripción de la trama de datos</i>	55
Tabla 2 <i>Tipo, subtipo y descripción de la trama de control</i>	56
Tabla 3 <i>Tipo, subtipo y descripción de la trama de gestión</i>	57
Tabla 4 <i>Número de RU soportados por diferentes anchos de banda</i>	61
Tabla 5 <i>Características de 802.11 ac y ax</i>	72
Tabla 6 <i>Lista de stakeholders</i>	74
Tabla 7 <i>Requerimientos operacionales</i>	74
Tabla 8 <i>Requerimientos del sistema</i>	75
Tabla 9 <i>Requerimientos de arquitectura</i>	77
Tabla 10 <i>Nomenclatura para selección de hardware y software</i>	79
Tabla 11 <i>Análisis comparativo de APs</i>	80
Tabla 12 <i>Análisis comparativo de placas SBC</i>	80
Tabla 13 <i>Análisis comparativo de antenas PCIe</i>	81
Tabla 14 <i>Análisis comparativo de SO</i>	82
Tabla 15 <i>Análisis comparativo de sniffers</i>	83
Tabla 16 <i>Direccionamiento para la red ad-hoc</i>	104
Tabla 17 <i>Direccionamiento para la red de infraestructura</i>	104
Tabla 18 <i>Direccionamiento para la red mesh</i>	104
Tabla 19 <i>Condiciones para la red ad-hoc</i>	114
Tabla 20 <i>Resultados en modo ad-hoc</i>	121
Tabla 21 <i>Resultados modo ad-hoc con interferencia</i>	125
Tabla 22 <i>Condiciones para la red</i>	125
Tabla 23 <i>Resultados de la red en modo infraestructura sin interferencia</i>	130

Tabla 24	<i>Resultados de la red en modo infraestructura con interferencia</i>	135
Tabla 25	<i>Condiciones para red Mesh</i>	136
Tabla 26	<i>Resultados de la red mesh sin interferencia</i>	139
Tabla 27	<i>Resultados de la red mesh con interferencia</i>	142
Tabla 28	<i>Valores obtenidos en la captura de marcos 802.11ax</i>	152

RESUMEN

El presente trabajo de titulación muestra un tesbed para la tecnología 802.11ax, que es una tecnología inalámbrica que se encuentra en crecimiento, siendo esta la sexta generación de wifi según la Wifi Alliance. Esta tecnología trae consigo nuevas características en comparación a su antecesor (802.11ac), entre las que se puede mencionar la modulación OFDMA, TWT, 1024-QAM, WPA3 entre otros.

Es así como, para esta investigación se utiliza la tecnología 802.11ax en combinación con placas SBC como son las Raspberry Pi en su versión CM4, permitiendo así crear redes en varios modos como ad-hoc, infraestructura y mallada, permitiendo el análisis en campos relacionados al proceso de acceso, gestión y transmisión de datos.

Para el desarrollo de la solución se debe recopilar información teórica que permitirá sustentar los objetivos de la investigación, es importante entender que es la tecnología, que características tiene, cuáles son sus ventajas y desventajas, cómo funciona la tecnología a nivel de capas, entender todos los parámetros necesarios para medir su rendimiento y por último como se lo implementaría en un banco de pruebas, toda esta investigación se basa en la metodología en cascada.

El desarrollo del proyecto será de ayuda para los estudiantes de la carrera, ya que se tendrá beneficios académicos, tecnológicos y económicos, además de ser un gran avance para la Universidad y la carrera de telecomunicaciones.

ABSTRACT

The present degree work shows a testbed for the 802.11ax technology, which is a wireless technology that is currently growing and is the sixth generation of WiFi according to the Wifi Alliance. This technology brings new features compared to its predecessor (802.11ac), such as OFDMA modulation, TWT, 1024-QAM, WPA3, among others.

For this research, the 802.11ax technology is used in combination with SBC boards such as the Raspberry Pi in its CM4 version, allowing the creation of networks in various modes such as ad-hoc, infrastructure, and mesh, allowing the analysis in fields related to access, management and data transmission process.

For the development of the solution, theoretical information must be collected to support the research objectives. It is important to understand what the technology is, what its characteristics are, what its advantages and disadvantages are, how the technology works at the layer level, understand all the parameters necessary to measure its performance, and finally how it would be implemented in a testbed. All this research is based on the waterfall methodology.

The project's development will be helpful for students in the field, as it will provide academic, technological, and economic benefits, in addition to being a great advancement for the university and the telecommunications career.

1. Capítulo 1: Antecedentes

El capítulo I de antecedentes permite dar a conocer al lector las razones por las que se realiza el desarrollo del proyecto. En este capítulo se presenta la problemática, el objetivo general y específicos, el alcance y la justificación que sustenta el desarrollo del proyecto.

1.1.Tema

Evaluación del rendimiento de la tecnología 802.11 ax mediante una tesbed para el laboratorio de la materia de Comunicación Inalámbrica

1.2.Planteamiento del problema

Las comunicaciones inalámbricas se han convertido en un pilar fundamental en la actualidad, y es importante conocer como estas tecnologías estan evolucionando y que características nuevas se van implementando, una de las tecnologías más utilizadas es Wi-Fi, impulsado por Wi-Fi Alliance(*Quiénes Somos / Alianza Wi-Fi*, n.d.). Esta es una solución que comprende un conjunto de estándares basados en las especificaciones del estándar IEEE 802.11(“IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2021), con la finalidad de establecer normas y estatutos para asegurar la interoperabilidad con los equipos certificados bajo esta denominación. El estándar fue lanzado en 1997, a lo largo de los años este estándar ha ido cambiando y mejorando sus prestaciones, hasta llegar al punto de que existen varias versiones como son 802.11 a/b/g/n/ac/ax(Grupo de Nuevas Actividades Profesionales (NAP) del COIT, 2004). La comunidad IEEE 802.11 creo el grupo TGax(Task Group ax) con el objetivo de desarrollar nuevas especificaciones de capa física (PHY) y capa de control de acceso

al medio (MAC), para ofrecer un mejor rendimiento en escenarios con alta densidad de puntos de acceso (AP) y estaciones de usuarios (STA) (Bellalta & Kosek-Szott, 2019). Esta nueva enmienda también denominada WLAN de alta eficiencia (High-Efficiency WLAN), se encuentra disponible en su versión 2021 (“IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment,” 2021). Esta enmienda se basa en IEEE 802.11 ac (“IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks--Specific Requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--A,” 2013), ya que amplía capacidades de comunicación multiusuario (MU) al incluir UL-MU-MIMO (Uplink Multi-user Multiple Input, Multiple Output) y acceso múltiple por división de frecuencia ortogonal (OFDMA), además de mejoras como la utilización de BSS coloring, rendimiento de Single-User (SU), mejora de consumo de energía con la implementación de TWT (Target Wake Up Time) entre otras mejoras de la tecnología (Bellalta & Kosek-Szott, 2019).

Con la implementación de estas nuevas características tanto en capa PHY como en capa MAC es necesario comprender el comportamiento de la tecnología, entender cómo se diferencia del estándar anterior (802.11 ac), identificar las ventajas y desventajas de la tecnología, y evaluar el rendimiento en entornos reales y teóricos de como esta tecnología es una mejor opción para ser implementada.

En base a lo mencionado se pretende realizar un estudio de la tecnología en sus capas física y enlace de datos, determinando las características y ventajas que tiene sobre otras tecnologías,

evaluar el rendimiento en diversos escenarios de pruebas, además desarrollar una guía de prácticas de laboratorio para complementar la educación de los estudiantes sobre esta tecnología y evaluar el rendimiento mediante el diseño de una red con la tecnología 802.11ax, y la implementación de un tesbed conformado de placas SBC, tarjetas inalámbricas, y un sniffer para la captura de paquetes, en estas prácticas se abordará temas relacionados con el proceso de acceso, gestión, y transmisión de datos, en donde se comprenderá como opera la tecnología a nivel de tramas. Esto permitirá a los estudiantes tener un mejor entendimiento de la tecnología y desenvolverse mejor en este tipo de entornos.

1.3.Objetivos

1.3.1. Objetivo General

Implementar un banco de pruebas(tesbed) basado en la tecnología 802.11ax para estudiar el comportamiento y características en las capas física y enlace de datos según el modelo OSI.

1.3.2. Objetivos específicos

- Recopilar fundamentación teórica de 802.11ax, entendiendo el funcionamiento y sus características, las mismas que permitirán realizar el análisis, diseño y desarrollo del proyecto.
- Identificar las características y requerimientos para el diseño e implementación del banco de pruebas.
- Evaluar el rendimiento de la tecnología basado en métricas de comportamiento en las capas física y capa de enlace.
- Desarrollar guías de laboratorio prácticas para complementar el aprendizaje en la materia de comunicación inalámbrica.

1.4.Alcance

Es proyecto está enfocado en el desarrollo de un banco de pruebas basado en la tecnología 802.11ax para el estudio de su comportamiento y rendimiento acorde a las capas física y enlace de datos, además del desarrollo de guías de laboratorio para la materia de Comunicación Inalámbrica.

El proyecto estará basado en la metodología en cascada, este modelo sigue una secuencia lineal permitiendo identificar etapas específicas las cuales se deben dar cumplimiento(González González et al., 2019).

Para el desarrollo de la solución se debe recopilar información teórica que permitirá sustentar los objetivos de la investigación, es importante entender que es la tecnología, que características tiene, cuáles son sus ventajas y desventajas, cómo funciona la tecnología a nivel de capas, entender todos los parámetros necesarios para medir su rendimiento y por último como se lo implementaría en un banco de pruebas.

En la primera etapa (Análisis) se identifican y evalúan las necesidades y restricciones para el proyecto, con lo cual, si hay dudas en los requisitos, poder mitigarlos mediante el análisis de características y requerimientos planteados, para posteriormente determinar las mejores alternativas y darle viabilidad al proyecto.

En la segunda etapa (Diseño) se tiene el estudio de las alternativas y restricciones que puede generar el proyecto, aquí se identifican y especifican las condiciones para el desarrollo del proyecto como son: sistemas operativos de código abierto(Linux), entornos de desarrollo(Visual Studio, Pydev), lenguajes de programación(Phyton, Java, C), dispositivos necesarios para la infraestructura(concentradores, placas Raspberry, puntos de acceso entre otros), además permite

identificar las características y requerimientos necesarios para la infraestructura inalámbrica en diferentes entornos, como son número de dispositivos, marcas, tipo de topología a utilizar para un correcto diseño del banco de pruebas.

En la tercera etapa (Implementación). En esta etapa se realiza la implementación del banco de pruebas, este estará compuesto de dispositivos basados en tecnología 802.11ax que es tecnología que está en apogeo y crecimiento, con estos dispositivos se crearan cuatro modos de comunicación (Infraestructura, ad-hoc, infraestructura mesh) con la finalidad de probar diferentes entornos y requerimientos. Cada uno de los modos propuestos estarán conformados por varios dispositivos que serán placas Raspberry CM4 IO Board(*Buy a Compute Module 4 IO Board – Raspberry Pi*, n.d.) cada uno con interfaces 802.11ax, que conformarán los AP en los modo infraestructura y las estaciones en los modo Ad-Hoc. En cada uno de los modos propuesto se analizará las capas física y enlace de datos; en la capa física se tomará en cuenta las bandas de operación de 802.11 ax, verificando su rendimiento en entornos donde exista interferencia. También se analizará la tecnología de transmisión como es OFDMA, indicando sus ventajas, desventajas, características y modo de operación en donde agrupa subportadoras hasta formar Unidades de Recursos(RU) y luego asignará estas unidades para implementar la transmisión concurrente para varios usuarios en varias direcciones(*Wi-Fi 6 Technology and Evolution White Paper*, 2020a), en donde se tiene OFDMA uplink y downlink.

Otra de las características en capa física que se evaluara es la modulación 1024 QAM la cual es un esquema de orden superior más eficiente que los utilizados en otras versiones.

Además, se evaluara las nuevas características implementadas en esta tecnología que son BSS coloring y el Target Wake Time(TWT), el primero es un método para identificar conjuntos de servicios básicos superpuestos, este identificador permite conocer si el dispositivo pertenece al

mismo BSS(Basic Service Set) o a otro BSS superpuesto esto dependiendo del color(*What Is BSS Color in 802.11ax? Background, Definition, Set-Up*, n.d.), mientras que el segundo es un mecanismo que permite tener un mayor periodo de programación de sueño en múltiples estaciones, lo que mejora de gran manera la duración de las baterías en los dispositivos IoT(*Wi-Fi 6 Technology and Evolution White Paper*, 2020a).

Una parte importante es el análisis de las tramas en cada capa, esto se realizará mediante la captura con el sniffer, aquí se evaluará el comportamiento de la tecnología a nivel de tramas, que nuevas cabeceras se agregan y como estas interactúan en los diferentes entornos.

En el dimensionamiento de los parámetros se especifican todos los requerimientos que el estudiante necesita para realizar la practica correctamente, es aquí en donde se realizan guías de laboratorio para que el estudiante sepa como operar en el banco de pruebas y de la misma manera pueda cumplir con los objetivos de la práctica, estas estarán enfocadas en el comportamiento y rendimiento de la tecnología.

En la cuarta etapa (Verificación) se debe poner a prueba la red y verificar su funcionamiento, aquí en esta etapa se compara los resultados obtenidos con los resultados teóricos, se debe verificar si los objetivos del proyecto fueron cumplidos.

En la quinta etapa (Mantenimiento) se planifica al final del proyecto, si se producen errores, existen inconvenientes o los resultados no son los esperados, se busca soluciones en las alternativas planteadas, en donde si existe una mejor solución, se la aplicará hasta tener la solución terminada y con la calidad requerida.

1.5. Justificación

En la Universidad Técnica del Norte existe la carrera de Telecomunicaciones(CITEL) perteneciente a la Facultad de Ingeniería en Ciencias Aplicadas, la cual forma gran cantidad de profesionales en el área de las comunicaciones, esta carrera con el pasar de los años ha ido mejorando en cuanto a implementación de tecnología se refiere, tanto para uso general como uso en la formación de los estudiantes, por tal motivo esta carrera debe contar con los recursos necesarios para que los estudiantes adquieran la mayor cantidad de conocimiento de manera práctica.

Una de las tecnologías que se encuentra en crecimiento son las inalámbricas específicamente las del estándar IEEE 802.11 en su versión ax, además de tener una gran acogida en los últimos meses, por tal razón al ser una nueva tecnología el estudio del comportamiento en diferentes entornos es fundamental, además los estudiantes deben conocer sobre esta tecnología, deben conocer cómo opera a nivel de capas física y enlace de datos.

Para realizar este proyecto se toma en cuenta el análisis de la situación actual de la carrera, así como el análisis de alternativas y restricciones para determinar los riesgos más potenciales y poder mitigarlos según la metodología en cascada. El desarrollo del proyecto será de ayuda para los estudiantes de la carrera, ya que se tendrá beneficios académicos, tecnológicos y económicos, además de ser un gran avance para la Universidad y la carrera de telecomunicaciones

2. Capítulo II: Marco teórico

2.1. Redes inalámbricas

2.1.1. *Introducción a las redes inalámbricas*

Las redes inalámbricas son aquellas en la que dos dispositivos pueden comunicarse sin la necesidad de utilizar cable, esto a través de un enlace que utiliza ondas electromagnéticas, infrarrojas, microondas o de radio(Lederkremer, 2019), facilitando la conexión entre puntos remotos, que se pueden encontrar a metros o kilómetros de distancia.

2.1.1.1. **Ventajas de las redes inalámbricas.**

Como ventajas de las redes inalámbricas se pueden mencionar las siguientes:

- **Comunicación punto a punto sencilla:** se puede comunicar varios dispositivos sin la necesidad de utilizar cables.
- **Instalación rápida y costo mínimo:** levantar una red inalámbrica es mucho más económica que una cableada, además el procedimiento de instalación y configuración es más rápido que las cableadas.
- **Excelente reubicación:** las redes inalámbricas permiten desplazarse sin tener que preocuparse por el cableado, así la ausencia de cable permite facilidad en reubicación de estaciones de trabajo en áreas limitadas (Gutierrez, 2020).

2.1.1.2. **Desventajas de las redes inalámbricas.**

Como desventajas se pueden mencionar las siguientes:

- **Alcance limitado:** las ondas de radio están limitadas a un área específica, dependerá de la potencia de transmisión, ganancia de las antenas y la sensibilidad de los receptores.
- **Apantallamiento de la señal:** este parámetro dependerá de lo que obstaculice la señal de emisión, puede ser puertas, muebles, paredes, árboles entre otros.

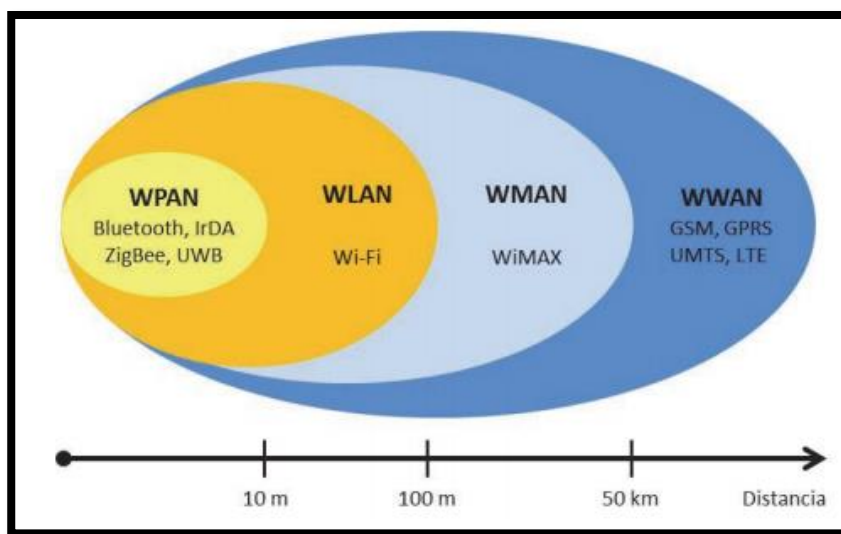
- **Interferencias:** se puede dar problemas en la conexión, donde se utiliza tecnología que trabaja en la misma frecuencia.
- **Seguridad:** es un parámetro muy importante, ya que se transmite por medio de ondas, estas pueden ser interceptadas poniendo en riesgo la información.
- **Velocidades limitadas:** si se compara con medios como el cobre o la fibra óptica, la velocidad es limitada, puesto que algunas tecnologías no alcanzan los 100 Mbps o 1 Gbps.(Gutierrez, 2020)

2.1.2. Tipos de redes inalámbricas

Según (Salazar, n.d.) las redes inalámbricas al igual que las alámbricas se las puede clasificar por el alcance, en la Figura 1 se puede observar que rangos de alcance tiene cada una, así de manera general se puede encontrar las siguientes(CAPÍTULO 1: INTRODUCCIÓN A LAS REDES INALÁMBRICAS 1.1 Introducción, n.d.):

Figura 1

Clasificación de las redes inalámbricas según su alcance



Nota: Adaptado de Redes Inalámbricas (p. 7), por J. Salazar, TechPedia.

- **WPAN (Wireless Personal Area Network):** Estas redes cubren distancias inferiores a los 10 metros, por ejemplo Bluetooth o IEEE 802.15.

- **WLAN (Wireless Local Area Network):** Estas redes cubren distancias de cientos de metros, por ejemplo Wi-Fi o IEEE 802.11
- **WMAN (Wireless Metropolitan Area Network):** Estas redes pretenden cubrir áreas de ciudad o entornos metropolitanos, aquí se tiene Wi-Max o IEEE 802.16
- **WWAN (Wireless Wide Area Network):** Estas redes pueden alcanzar a cubrir toda una región o país, estas redes se basan en la tecnología celular.

2.1.3. Redes de área Local (WLAN)

Las WLAN son redes diseñadas para proporcionar acceso a zonas en rangos de cobertura alrededor de 100 metros, son utilizadas en el hogar, la escuela, en laboratorios de cómputo o entornos de oficina. Esto permite a los usuarios moverse en el área de cobertura y permanecer conectado(Salazar, n.d.), en la Figura 2 se puede observar un esquema de una WLAN.

Figura 2

Esquema de una WLAN con AP y Estaciones



Nota: Adaptado de Redes Inalámbricas (p. 7), por J. Salazar, TechPedia.

Las WLAN se basan en el estándar de IEEE 802.11 y son comercializados bajo la denominación de Wi-Fi (Wireless Fidelity) impulsado por Wi-Fi Alliance(*Quiénes Somos /*

Alianza Wi-Fi, n.d.), existen otros estándares como HIPERLAN que nunca recibió tanta aceptación comercial como Wi-Fi, ya que este es más sencillo de implementar.

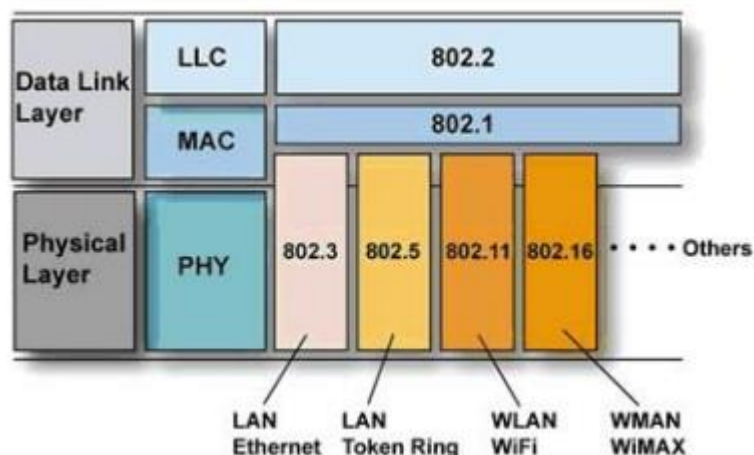
2.2. Estándar 802.11

2.2.1. Introducción

IEEE (Institute of Electrical and Electronics Engineers) define un estándar para el entorno de las redes inalámbricas 802.11, según (Horno Anguís, 2008) este está centrado en los dos niveles más bajos del modelo OSI, capa física y capa enlace, en la Figura 3 se puede observar en que capas opera este estándar, tomando en cuenta que opera en capa PHY y MAC.

Figura 3

Estándares del grupo 802.x y en que capas del modelo OSI trabajan.



Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage (p. 26), J. Honor, 2008, Universidad de Sevilla.

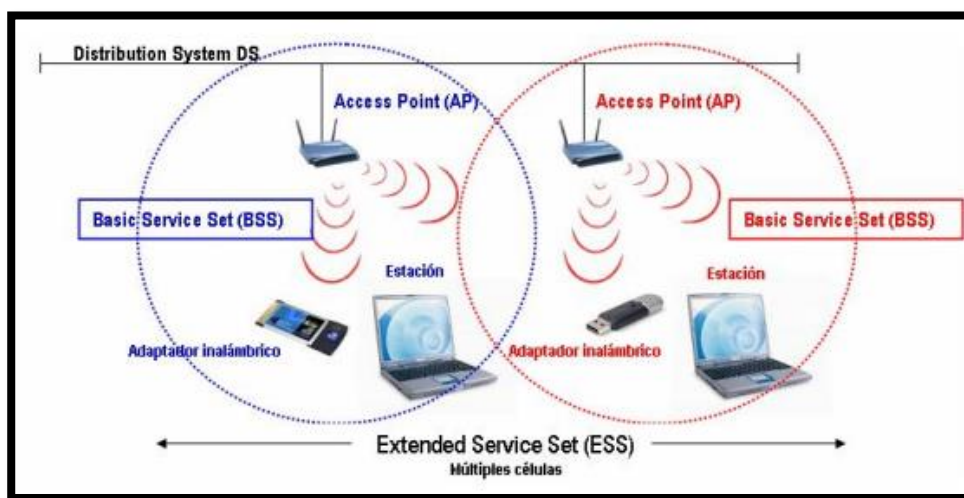
2.2.2. Arquitectura 802.11

La arquitectura de IEEE 802.11 consta de varios componentes que interactúan para proporcionar una WLAN que admite la movilidad de la estación (STA) de forma transparente a las capas superiores ("IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific

Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2021).

Figura 4

Arquitectura IEEE 802.11 con sus componentes



Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage (p. 26), J. Honor, 2008, Universidad de Sevilla.

La arquitectura del estándar IEEE 802.11 como se observa en la Figura 4 contiene varios componentes: la estación (STA), access point (AP), Independent Basic Service Set (IBSS), Basic Service Set (BSS), distribution System (DS), y el extended Service Set (ESS).

2.2.2.1. Estación (STA)

Es una instancia direccionable individualmente de un control de acceso al medio (MAC) y una interfaz de capa física (PHY) al medio inalámbrico. En IEEE Std 802.11 (“IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2021), la unidad direccionable es una estación (STA). Las características físicas y operativas se definen mediante

modificadores que se colocan delante del término STA. Por ejemplo, en el caso de ubicación y movilidad, STA portátil y STA móvil. La STA es un destino direccionable, pero no (en general) una ubicación fija.

De acuerdo con (Salazar, n.d.) una estación podría ser un PC, un ordenador portátil, un smartphone o cualquier dispositivo que tenga una tarjeta para acceder al medio inalámbrico.

Uno de los requisitos de IEEE Std 802.11 es manejar STA móviles y portátiles. Un STA portátil es uno que se mueve de un lugar a otro, pero que se usa solo mientras se encuentra en un lugar fijo, mientras que STA móvil: acceda a la LAN mientras está en movimiento.

2.2.2.2. Punto de acceso (AP)

En estándar 802.11 (“IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2021) define al AP como una entidad que contiene una estación y proporciona acceso a los servicios del sistema distribuido, a través del medio inalámbrico para las estaciones asociadas.

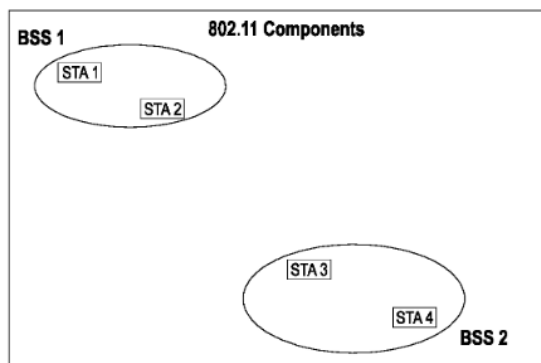
Es un dispositivo que permite a los dispositivos inalámbricos que se conecten a una red cableada mediante Wi-Fi, o estándares relacionados

2.2.2.3. Basic Service Set (BSS)

Consiste en un AP, junto con todas las STA. El AP actúa como un punto central para manejar las STA dentro de ese BSS. El BSS más simple se compone de un AP y una STA.

Figura 5

Esquema de un BSS según IEE Std. 802.11



Nota: Adaptado de IEEE Std. 802.11 (p. 220).

En la figura 5 se puede observar cómo se conforma dos BSS cada una con STA asociadas a él. Es útil pensar en cada óvalo que representa un BSS como el área de cobertura dentro de la cual las STA miembros del BSS pueden permanecer en comunicación.

También se debe mencionar un IBSS que es un Independent Basic Service Set, este tiene la misma funcionalidad que un BSS con la diferencia que no está conectado a un sistema distribuido ("IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2021).

2.2.2.4. Distribution System (DS)

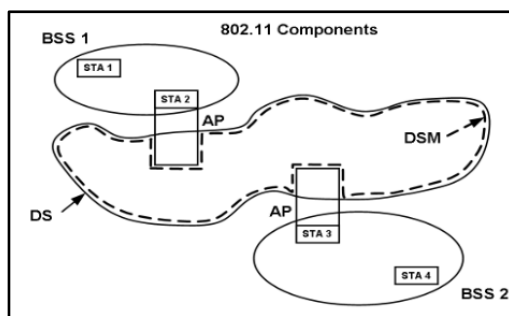
Es un sistema que se utiliza para interconectar un conjunto de BSS y redes de área local integradas (LAN) para crear un conjunto de servicios extendidos (ESS).

Es el mecanismo donde diferentes AP pueden intercambiar datos entre sí o bien con las redes cableadas. El DS no es necesariamente una red y IEEE 802.11 no especifica ninguna tecnología en particular para el DS.

IEEE Std 802.11 (“IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2021) separa lógicamente el WM del medio del sistema de distribución (DSM). Cada medio lógico se utiliza para diferentes propósitos, por un componente diferente de la arquitectura.

Figura 6

Esquema de un Distribution System con sus componentes



Nota: Adaptado de IEEE Std. 802.11 (p. 221).

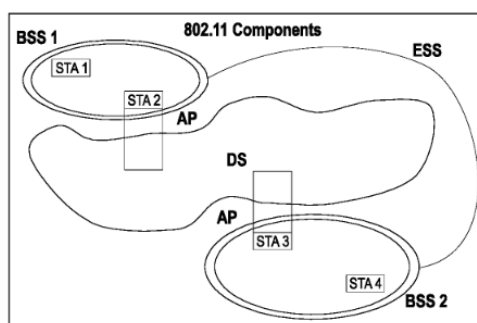
En la figura 6 se observa cómo se añade estos nuevos componentes a la arquitectura inicial, en donde se aprecia que los dos BSS se encuentran conectados mediante un DS.

2.2.2.5. Extended service set (ESS)

Es un conjunto de uno o más BSS que aparece como un único BSS para la capa de control de enlace lógico (LLC) en cualquier estación (STA) asociada con uno de esos BSS.

Figura 7

Esquema de un ESS con sus componentes principales.



Nota: Adaptado de IEEE Std. 802.11 (p. 222).

En la figura 7 se observa cómo se conforma un ESS, el cual es la unión de los BSS de infraestructura con el mismo SSID (Service Set Identifier) conectado por un DS. El ESS no incluye el DS.

2.2.3. Capa física

La capa física (PHY) determina el modo de la codificación y transmisión para las comunicaciones inalámbricas. Esta capa es la encargada de transmitir y recibir los datos por el medio físico en este caso el aire.

2.2.3.1. Espectro radioeléctrico

El estándar 802.11 utiliza las bandas de 2.4GHz y 5GHz, estas bandas no son reguladas ya que pertenecen a las bandas ISM (Industrial-Científica-Médica) y se encuentran disponibles en todo el mundo. Al estar disponibles de manera libre quien desee transmitir en ella debe evitar que exista una excesiva interferencia entre las emisiones por lo cual la potencia debe ser igual o menor a 1mW y en espectro disperso(Horno Anguís, 2008).

2.2.3.2. Tecnologías de transmisión

Las tecnologías de transmisión permitirán tener vario beneficios, además su uso dependerá de las necesidades y de la variante del estándar que se esté utilizando.

A estas tecnologías se las puede dividir en tecnologías de transmisión por infrarrojos y por ondas de radio, pero para 802.11 solo se utilizará por ondas de radio, aquí se estudiará tres técnicas de propagación FHSS, DSS y OFDM.

2.2.3.2.1. Espectro ensanchado

Esta técnica se caracteriza por distribuir la energía media de la señal transmitida, dentro de un ancho de banda mucho mayor que el de los datos(Unda & Jaramillo, 2004).

El ancho de banda es mucho mayor que el de una transmisión normal, este ensanchamiento se lo realiza a partir de una señal pseudoaleatoria, esta señal transmitida solo se la podrá demodular si el receptor puede generar la misma señal.

Una ventaja de la transmisión por espectro ensanchado es que es más resistente contra las interferencias, además la señal es difícil de detectar por el nivel bajo de potencia que tiene.

Esta señal se la puede obtener de dos formas:

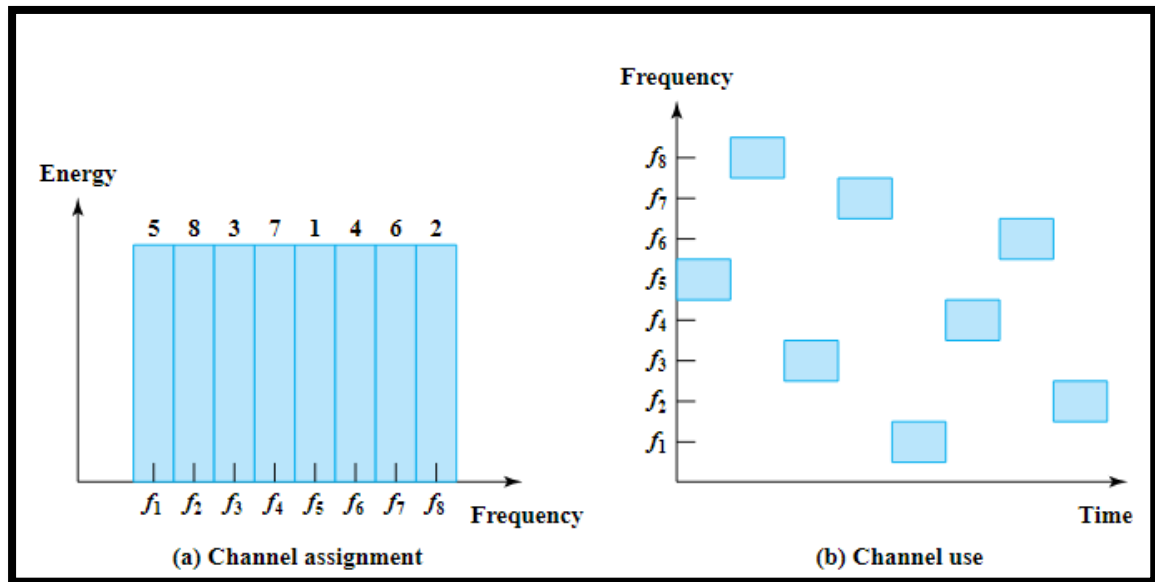
FHSS o Espectro Ensanchado por Salto de Frecuencia

Esta técnica consiste en que la señal que se emite en un conjunto de frecuencias y estas van saltando de una a otra de forma periódica y rápida, permitiendo así que solo el dispositivo que conozca la secuencia de salto puede descifrar la información(Martínez et al., n.d.).

Esta técnica es más resistente a interferencias ya que el cambio de frecuencias es constante, haciendo que la interferencia se produzca en un periodo de tiempo muy corto.

Figura 8

División de canales de FHSS



Nota: Adaptado de Frequency hopping spread spectrum, por Fraida Fund, 2017, WitesLab (<https://witestlab.poly.edu/blog/frequency-hopping-spread-spectrum/>). CC Attribution-Non Commercial 4.0 International License.

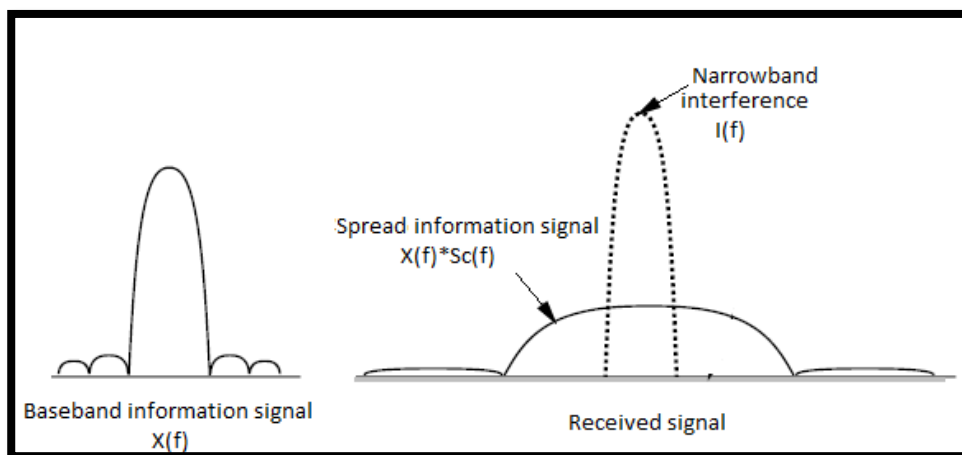
En un sistema FHSS la señal transmitida se distribuye a través de múltiples canales, como se muestra en la Figura 8a, y van saltando como se muestra en la figura 8b.

DSSS o Espectro Ensanchado por Secuencia Directa

La información se codifica con un código de falso ruido, como consecuencia se obtiene una secuencia de símbolos casi igual al ruido, ya que el número de bits enviados es muy superior a la de bits transmitidos, esto se hace para que el receptor sea capaz de reconstruir los datos originales aun existiendo una interferencia en el canal, pero siempre que no sea muy grande. En la figura 9 se observa el proceso de ensanchado de la señal.

Figura 9

Proceso de ensanchamiento de DSSS

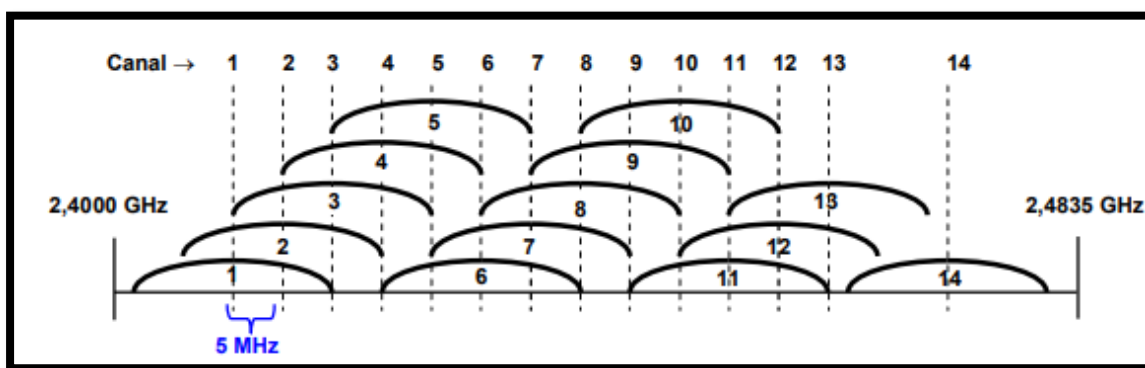


Nota: Adaptado de behindthesciences (<https://behindthesciences.com/category/signal-processing/>)

DSSS trabaja en la banda de 2,4GHz con un ancho de banda total de 83,5 MHz, este ancho de banda se divide en 14 canales con un ancho de banda de 22 MHz, estos canales están desplazados 5MHz con respecto al anterior, con lo cual los canales adyacentes se superponen.

Figura 10

Distribución de canales en DSSS

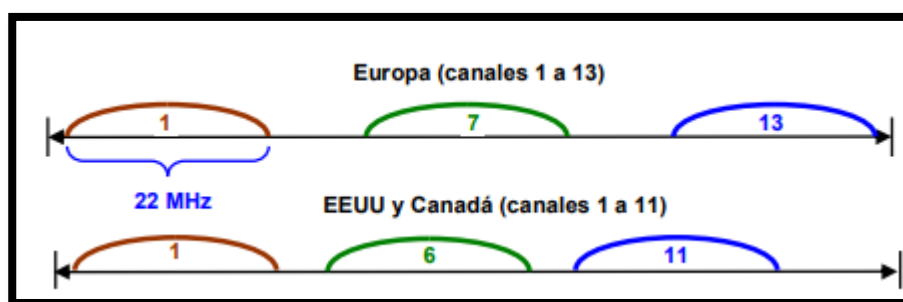


Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage (p. 44), J. Honor, 2008, Universidad de Sevilla.

En la figura 10 se observa cómo es la distribución de los canales con DSSS, se observa que los canales se van sobreponiendo unos a otros, pero se puede tener tres canales disponibles que pueden operar simultáneamente. En EEUU la FCC (Comisión Federal de Comunicaciones) define 11 canales de los cuales el canal 1, 6 y 11 no se solapan, mientras que Europa la ETSI (European Telecommunications Standards Institute) define 13 de los cuales el 1, 7 y 13 no se sobreponen como se indica en la figura 11.

Figura 11

Canales que no se sobreponen unos a otros



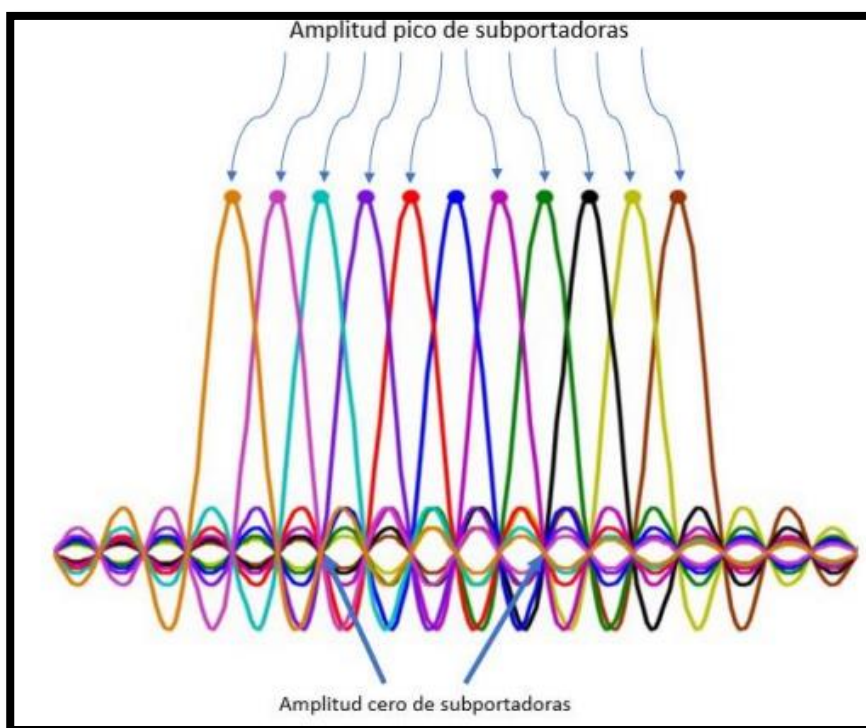
Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage (p. 44), J. Honor, 2008, Universidad de Sevilla.

2.2.3.2.2. OFDM o multiplexación por división de frecuencias ortogonales

Es una técnica de transmisión multiportadora, es decir transporta los datos o información sobre varias portadoras de datos separadas ortogonalmente, OFDM utiliza la transformada rápida de Fourier que le permite llevar una transmisión por subportadoras paralelas y así evita las interferencias ISI e ICI (Eduardo & Rodríguez, 2018).

Figura 12

Amplitudes de las subportadoras



Nota: Adaptado de Diseño y simulación de la técnica OFDM para redes inalámbricas móviles sobre Simulink y tarjeta FPGA (p. 28), C. Chicaiza, 2020, Universidad Católica de Santiago de Guayaquil.

Una característica importante en OFDM es el uso de frecuencias ortogonales, la cual hace posible mejorar la eficiencia espectral. Para conseguir frecuencias ortogonales se coloca el pico de un pulso sinc sobre los 0 de las funciones sinc adyacentes, al hacer esto no se produce una mezcla de componentes de interferencia desde una frecuencia central en el pico de una función sinc, hacia otra frecuencia, en la figura 12 se puede observar la amplitud cero de subportadoras y la amplitud pico de subportadoras.

OFDM puede enviar datos a varias velocidades de hasta 54 Mbps utilizando distintas técnicas de modulación como son BPSK, QPSK o QAM.

OFDM presenta las siguientes ventajas:

- OFDM es más resistente y robusto al desvanecimiento selectivo de frecuencia que el mono portador.
- Elimina el ISI e ICI a través del prefijo cíclico.
- La ecualización del canal es más sencilla a diferencia de las técnicas de ecualización adaptativas.
- OFDM es más eficiente en procesamiento al utilizar dos técnicas de FFT para realizar la modulación y demodulación(Jiménez et al., 2001).

También OFDM presenta ciertas desventajas o inconvenientes como son:

- OFDM es altamente sensitivo a errores por sincronización.
- También es más sensible al desplazamiento y fluctuación de la frecuencia portadora(Jiménez et al., 2001).

2.2.3.3. Protocolos de capa física

PMD (Physical Media Dependent)

Se definen todas las funciones de la capa física, aquí la función primordial es la transmisión pura de bits a través del medio. Esta subcapa también define niveles de potencia, relación S/N necesaria para un BER adecuado, banda de operación, modulación(Ricardo & Jijón, 2002).

Esta subcapa bajo la dirección de PLCP realiza la transmisión/recepción propiamente dicha, además de interactuar con el medio inalámbrico para realizar la modulación y demodulación.

PLCP (Physical Layer Convergence Procedure)

Es la cabecera que va junto a las SDU (Unidades de datos de servicio) para formar las PDU (Unidades de datos de protocolo) de la capa física(José & Torres, n.d.-a).

PLCP se comporta como un enlace entre los frames de MAC y PMD, esta subcapa añade sus encabezados y en particular los preámbulos de sincronización(Gutierrez, 2020).

La capa MAC se comunica con la PLCP mediante primitivas enviadas a través de SAP. PLCP alista las MPDU (Unidades de datos del protocolo MAC) para ser transmitidas y envía las tramas a la capa MAC(José & Torres, n.d.-a). PLCP añade algunos campos a las MPDU las cuales contienen información útil para que la capa física pueda recibirla y transmitirla, a esto se le conoce como PPDU (unidades de datos del protocolo PLCP).

PLCP se la puede dividir en preámbulo y cabecera, estas dependerán según la técnica de propagación que se utilice.

La función principal del preámbulo es sincronizar, determinar la ganancia y establecer el CCA (Clear Channel Assessment) para que la capa MAC sepa si el medio está disponible o no.

Mientras que la cabecera en la mayoría de los casos se compone de 4 campos que son:

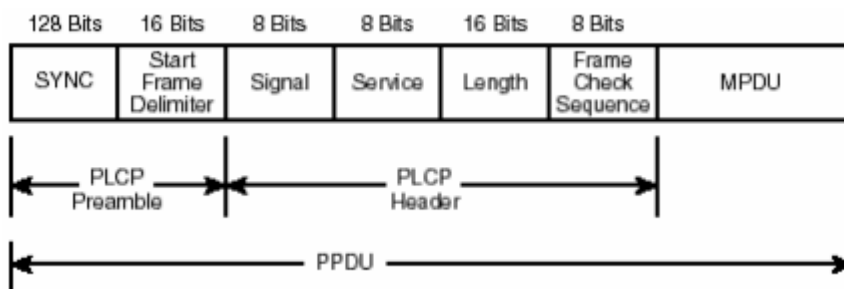
- **Señal:** Velocidad a la que se transmitan los SDU, esto variara en función del estándar en uso.
- **Servicio:** Esta reservado para usos a futuro.
- **Longitud:** Indica las longitudes de la trama.
- **HEC (Header Error Check):** Se trata de un CRC (Código de Redundancia cíclica) para el control de errores en la cabecera.

A continuación, se indica el formato de la PPDU en diferentes técnicas:

DSSS PLCP

Figura 13

Formato de la PDU DSSS



Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage, J. Honor, 2008, Universidad de Sevilla.

PLCP añade seis campos a la trama que recibe, dos de preámbulo y cuatro de cabecera como se indica en la figura 13.

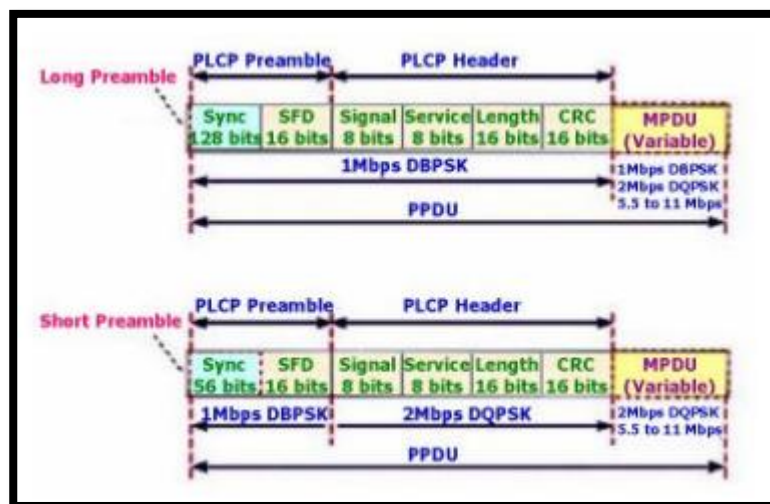
La función del preámbulo es la de sincronizar tanto al transmisor como al receptor y está compuesta de un campo de sincronismo de 128 bits, todos en uno, y un delimitador de comienzo de trama compuesto de 16 bits fijos.

Después esta la cabecera que tiene cuatro campos que son: Señal de 8 bits para identificar la velocidad, servicio de 8 bits, longitud de 16 bits que indica el tiempo en μs para transmitir la trama y el CRC que permite proteger la cabecera de posibles errores.

HR/DSSS PLCP

Figura 14

Formato de PDU de HR/DSSS largo y corto



Nota: Adaptado de Redes Inalámbricas (p. 9), C. Varela & L. Domínguez, 2002, Universidad de Valladolid.

Para HR/DSSS PLCP existen dos formatos el corto y el largo como se indica en la figura 14, en donde el formato largo es igual al usado con DSSS mientras que el corto busca mejorar el rendimiento.

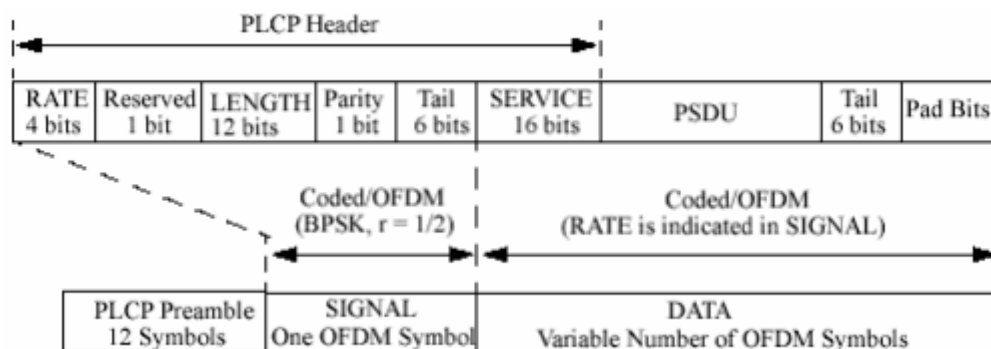
Ambos formatos están compuestos de un preámbulo y su cabecera, el preámbulo consta de dos campos que son el sincronismo en donde se especifica si es largo o corto y el SFD (Delimitador de comienzo de trama) que de igual forma se especifica si es corto o largo.

Además, se tiene la cabecera que cuenta con dos posibilidades la corta que se transmitirá a 2Mbps y la larga que se transmitirá a 1Mbps.

OFDM PLCP

Figura 15

Formato de PDU de OFDM



Nota: Adaptado de Redes Wireless Mesh (p. 13), L. Leocadia & W. Freitas, 2013, Universidad Federal Fluminense.

En este PLCP se añade además del preámbulo y la cabecera, una serie de bits para ayudar a la decodificación, como se observa en la figura 15.

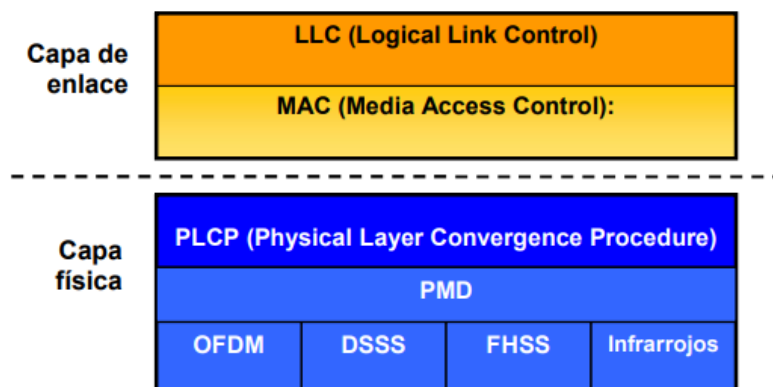
El preámbulo está compuesto de 12 símbolos OFDM y sirve para el sincronismo, la cabecera PLCP se encuentra entre el preámbulo y el campo de datos, esta cabecera está compuesta por el campo señal y el campo servicio.

2.2.4. Capa de enlace

La capa de enlace de datos da soporte y conexión a servicios de capa superior, esta proporciona un medio de intercambio de datos, permite a capas superiores acceder a los medios usando tramas, esta capa se divide a su vez en la subcapa MAC y la subcapa LLC como se indica en la figura 16.

Figura 16

Capas y subcapas Física y enlace de datos.



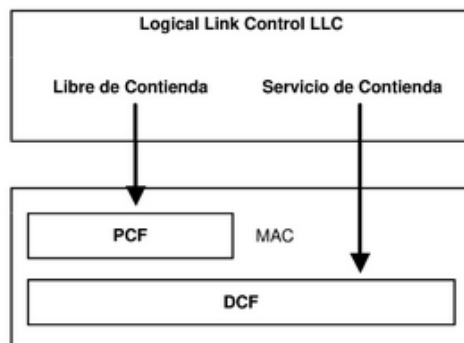
Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage (p. 26), J. Honor, 2008, Universidad de Sevilla.

2.2.4.1. Capa MAC (Media Access Control)

En esta subcapa se especifica el método de acceso al medio, como peculiaridad de 802.11 son el acuse de recibo ACK, la posibilidad de fragmentar las tramas y mecanismos de encriptación para dar seguridad a los datos. Los métodos de acceso al medio permiten la regulación del uso del canal para que este sea de la mejor manera posible (José & Torres, n.d.-b).

Figura 17

Funciones de coordinación



Nota: Adaptado de Comunicaciones móviles y redes Inalámbricas (), O. Gutiérrez, 2020, Editorial Científica Universitaria.

La subcapa MAC se compone de dos funciones que son PCF y DCF, cada una define un modo de acceso al medio para cada estación, en la figura 17 se puede observar cómo se compone en la subcapa MAC, además da otros servicios específicos de 802.11 como es la gestión de movilidad, gestión de potencia, sincronización y seguridad(Horno Anguís, 2008).

2.2.4.1.1. DFC (Función de coordinación distribuida)

Proporciona acceso al medio en base a una contienda, este utiliza el mecanismo CSMA/CA con RTS/CTS, denominado MACA(Gutierrez, 2020).

Esta funcionalidad permite determinar cuándo una estación puede transmitir o recibir datos a través del medio, esta función se basa en técnicas de acceso aleatorias de contienda por el medio(Horno Anguís, 2008).

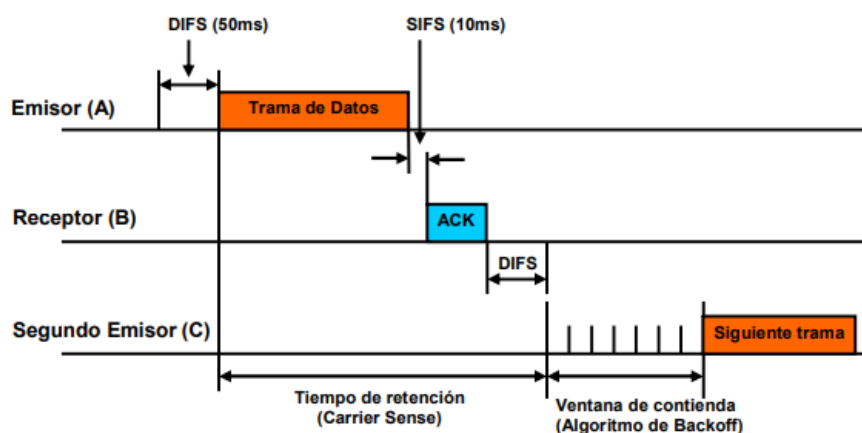
Este método utiliza ACK provocando así retransmisiones si no se reciben, además utiliza NAV (Network Allocation Vector) para que todas las estaciones que se encuentran escuchando conozcan cuando el medio vuelve a estar libre para transmitir.

CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

En redes tipo Ethernet se utiliza CSMA/CD (Carrier Sense Multiple Access / Collision Detection) como protocolo de acceso, este consiste en que las estaciones sondan el medio antes de transmitir si está libre transmiten y si no es así se quedan escuchando el medio hasta que esté libre y transmiten. En un medio inalámbrico es costoso implementar radiorreceptores que transmitan y reciban al mismo tiempo por lo cual para 802.11 se emplea CSMA/CA, la diferencia con el otro método es que este intenta evadir colisiones ya que detectarlas es difícil en el aire.

Figura 18

Funcionamiento de CSMA/CA



Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage (p. 53), J. Honor, 2008, Universidad de Sevilla.

Para ver como es el funcionamiento de CSMA/CA se tiene la figura 18, en donde se muestra como un emisor A envía datos a un Receptor B, mientras un emisor C espera para el envío. Una estación A desea transmitir hacia B y detecta que el canal esta libre, A espera un tiempo de DIFS y empieza a transmitir, asegurándose que cualquier trama emitida ira separada al menos ese tiempo.

Una vez que termina de transmitir espera la confirmación ACK desde B, esta trama es de suma importancia por lo que el tiempo de espera se reduce a un tiempo de SIFS.

A su vez un emisor C desea transmitir, pero observa que el medio está ocupado por lo cual espera que termine el envío actual.

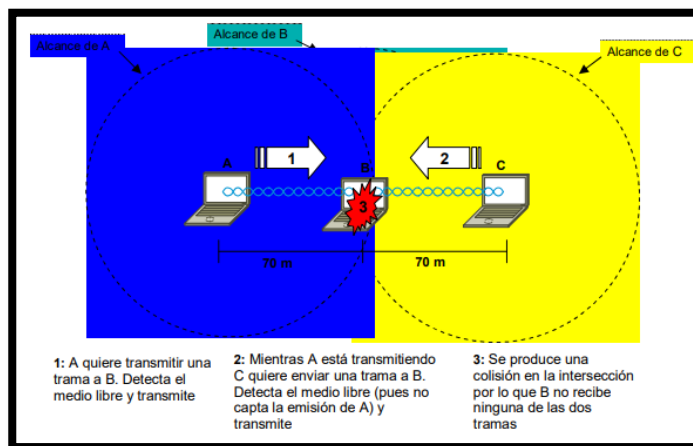
Una vez que la transmisión de A hacia B concluye, la estación C ejecuta el llamado algoritmo de backoff, el cual da un número aleatorio cuya función es la de reducir la probabilidad de colisión en el medio.

CSMA/CA presenta dos problemas principalmente:

Estación oculta: Una STA cree que el canal esta libre, pero en realidad está ocupada por otro nodo al que no se le oye.

Figura 19

Problema de estación oculta

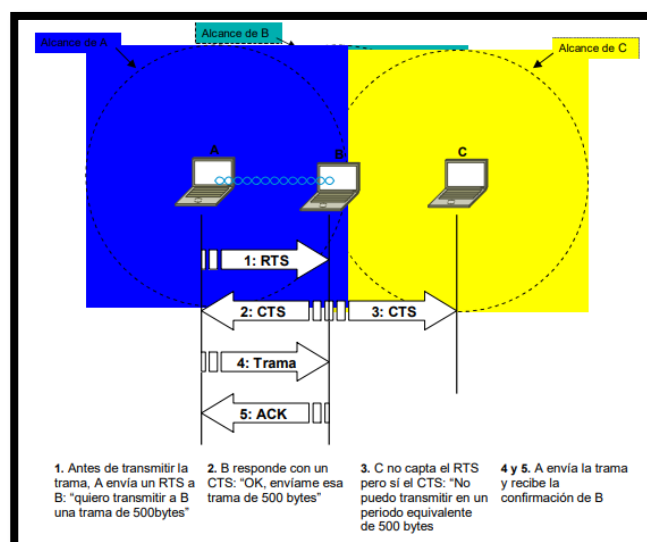


Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage (p. 56), J. Honor, 2008, Universidad de Sevilla.

Estación expuesta: la STA cree que el medio está ocupado, pero esta libre pues otra estación al que oye no le interferiría para transmitir.

Figura 20

Intercambio de mensajes RTS/CTS



Nota: Adaptado de Redes de Área Local Inalámbricas. Diseño de la WLAN de Wheelers Lane Technology Collage (p. 57), J. Honor, 2008, Universidad de Sevilla.

La solución que propone 802.11, es el intercambio de mensajes RTS/CTS que juntamente con CSMA/CA se denomina MACA (MultiAccess Collision Avoidance), en la figura 20 se indica como es el intercambio de mensaje RTS y CTS.

2.2.4.1.2. PFC (Función de coordinación puntual)

Esta función puede acceder de manera libre a la contienda, esta función se sitúa encima de la función DCF, operando conjuntamente dentro de un mismo BSS con una estructura llamada supertrama.

Con este método se pueden transmitir tramas sin la necesidad de pasar por una contienda para ganar el medio, esto está pensado para servicios de tipo síncrono que no toleran retardos en el acceso al medio.

Existe un nodo organizador o director, llamado punto de coordinación o PC. El punto de coordinación se encuentra ubicado en el punto de acceso y controla las transmisiones de tramas por parte de las estaciones. Al principio de un periodo libre de contienda, PC gana el control del medio dado que sólo espera un intervalo PIFS, intervalo menor que el del resto de las estaciones que operan bajo DFC. Entonces enviará una trama de configuración CF-Poll (trama Beacon) a cada estación que pueda transmitir en PFC, concediéndole el poder de transmisión. Esta trama incluye el campo CF (Contention Free) con los parámetros establecidos para el periodo libre de contienda, y cuando las estaciones la reciban, actualizarán su NAV al valor que se indique. El PC mantendrá una lista con todos los datos de las estaciones que se han asociado al modo PFC. La concesión de transmisiones será por riguroso listado y no permitirá que una estación envíe dos tramas hasta que la lista se haya completado.

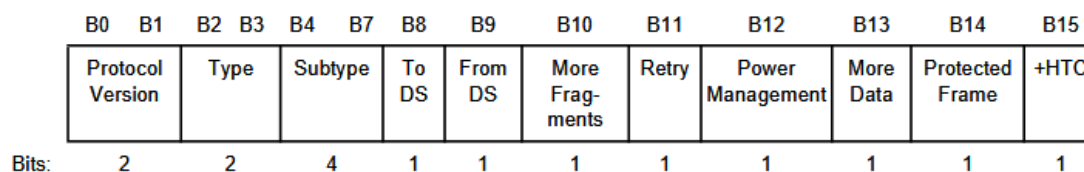
2.2.4.1.3. Formatos de trama MAC

La trama general MAC tiene los siguientes campos (“IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2021) y está formada como se indica en la figura 21.

Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 2021), se lo puede observar en la figura 22.

Figura 22

Formato del frame de control



Nota: Adaptado de Std. IEEE 802.11(p. 757)

Protocol Version: Indica la versión del protocolo que se esté utilizando

Type/Subtype: Type identifica si la trama es del tipo de datos, control o gestión; y subtype identifica el subtipo dentro de cada uno de estos tipos.

ToDS/FromDS: Indica si la trama se envía, recibe hacia o desde el sistema de distribución.

More Fragments: Se activa si se usa fragmentación.

Retry: Se activa si la trama es una retransmisión.

Power Management: Se activa si se utiliza el modo ahorro de energía

More Data: Se activa si la estación tiene tramas pendientes en un punto de acceso.

Protected Frame: Se activa si se usa el mecanismo de autenticación y encriptado.

+HTC: Se utiliza con el servicio de ordenamiento estricto

Trama de datos

Estas tramas como lo indica su nombre contienen los datos, estas tramas transportan información a capas superiores, está compuesta como lo indica la tabla 1.

Tabla 1

Tipo, subtipo y descripción de la trama de datos

Type Value	Subtype value	Description
10	0000	Data
10	0001	Reserved
10	0010	Reserved
10	0011	Reserved
10	0100	Null
10	0101	Reserved
10	0110	Reserved
10	0111	Reserved
10	1000	QoS Data
10	1001	QoS Data + CF-ACK
10	1010	QoS Data+CF-Poll
10	1011	QoS Data+ CF-ACK+CF-Poll
10	1100	QoS Null
10	1101	Reserved
10	1110	QoS +CF-Poll
10	1111	QoS + CF-ACK+CF-Poll

Nota: La tabla presenta la información de cómo se determina el tipo de trama con bits, además del subtipo y la descripción de que tipo de datos contiene.

Trama de control

Se usan para la reserva del medio y reconocimiento, tienen que ver con la preparación para enviar los datos y luego reconocer que se ha recibido los mismos (CTS, ACK, QoS, Power Save Poll etc.) estas tramas se utilizan para solicitud de envío, sobre todo cuando el AP ha tomado el control del medio, especificando cuando es el turno de una estación para enviar datos, en la tabla 2 se indica los subtipos de esta trama.

Tabla 2

Tipo, subtipo y descripción de la trama de control

Type Value	Subtype value	Description
01	0000-0010	Reserved
01	0011	TACK
01	0100	Beamforming Report Poll
01	0101	VHT NDP Announcement
01	0110	Control Frame Extension
01	0111	Control Wrapper
01	1000	Block Ack Request (BlockAckReq)
01	1001	Block Ack (BlockAck)
01	1010	PS-Poll
01	1011	RTS
01	1100	CTS
01	1101	ACK

01	1110	CF-End
01	1111	Reserved

Nota: La tabla presenta la información de cómo se determina el tipo de trama con bits, además del subtipo y la descripción de que tipo de datos contiene.

Trama de gestión

Sirven para gestionar el enlace, en la tabla 3 se encuentra los subtipos de mensajes en esta trama.

Tabla 3

Tipo, subtipo y descripción de la trama de gestión

Type Value	Subtype value	Description
00	0111	Reserved
00	1000	Beacon
00	1001	ATIM
00	1010	Disassociation
00	1011	Authentication
00	1100	Deauthentication
00	1101	Action
00	1110	Action No Ack
00	1111	Resrved

Nota: La tabla presenta la información de cómo se determina el tipo de trama con bits, además del subtipo y la descripción de que tipo de datos contiene.

2.2.4.2. Capa LLC (Logical Link Control)

La capa LLC ofrece un servicio de transporte único para todas las tecnologías.

Especifica los servicios que la subcapa LLC requiere de la subcapa MAC, independiente de la topología y del tipo de acceso al medio.

También especifica los servicios que la capa de red obtendrá de la capa de enlace.

2.3. IEEE 802.11 ax

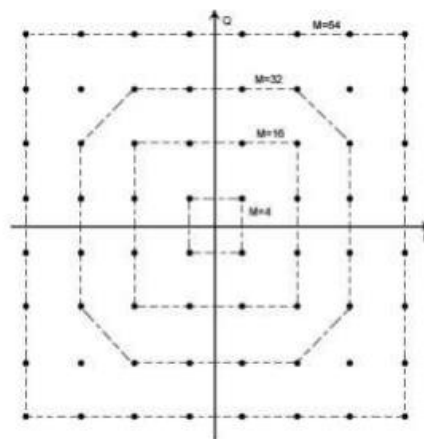
El crecimiento de la demanda de redes inalámbricas de alta velocidad ha impulsado la investigación para mejorar el rendimiento mediante la implementación de una variedad de mecanismos que se abordaran a continuación. Estos mecanismos permiten mejorar el rendimiento de la tecnología inalámbrica 802.11 en capa física y capa MAC.

2.3.1. 1024 QAM

QAM(Quadrature Amplitude Modulation) o modulación de amplitud en cuadratura, como expresa (Guayaquil, 2018) es una técnica de modulación digital donde los datos estan contenidos en la portadora tanto en amplitud como en fase, esta portadora esta desfasada 90° entre sí pero tiene la misma frecuencia.

Figura 23

Diagrama de constelaciones de 4, 16, 32 y 64 QAM



Nota: Adaptado de Diseño de una GUI en MATLAB para evaluar técnicas de modulación de amplitud en cuadratura (QAM) (p.15), R. Guayaquil, 2018, Universidad Católica de Santiago de Guayaquil.

La modulación QAM es conveniente representarla en una constelación, la cual es una representación gráfica de las señales, en donde se observa todos los símbolos que puede generar el modulador. Cada símbolo tiene asociado un valor de fase y magnitud lo cual permite representarlos en un plano de dos dimensiones, se puede observar en la figura 23 varios tipos de constelaciones dependiendo del nivel.

En 802.11 ax se integra una modulación más alta de 1024-QAM, esta modulación una gran variedad de velocidades alcanzando como un máximo teórico de 9.6 Gbps, esto mediante la transmisión sobre MSC (Modulation Coding Scheme) sobre los canales de 160 MHz 0 80 + 80 Mhz y un GI (Intervalo de guarda) de 0.8 μ s (Torres, 2021).

2.3.2. OFDMA

Mediante la adopción de una variedad de mecanismos de control de acceso al medio (MAC). La eficiencia de MAC contribuye a mejorar el rendimiento de una WLAN. Uno de los

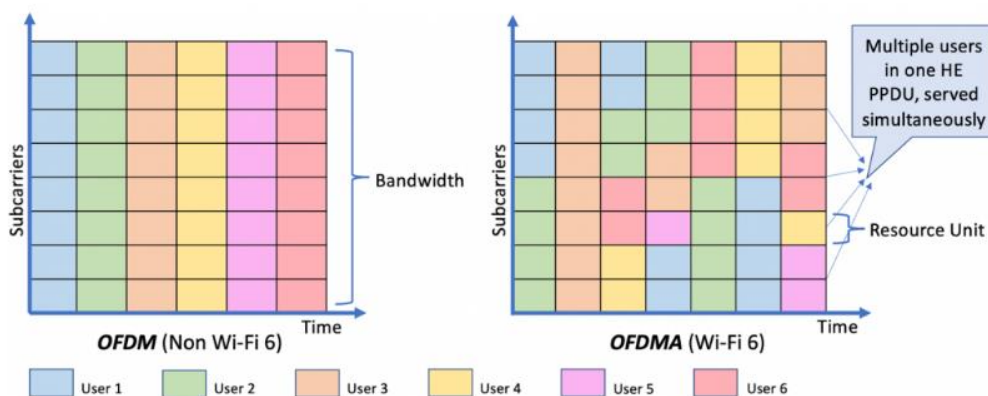
mecanismos es el acceso múltiple por división de frecuencia ortogonal (OFDMA) que originalmente se derivaba de la multiplexación por división de frecuencia ortogonal (OFDM).

Con base en (Lee, 2019) , OFDMA consiste en dividir una transmisión a través de varios subcanales, estos se denominan unidades de recursos (RU). En 802.11 ax los canales de 20, 40, 80 y 160 MHz se pueden dividir en subcanales de 9, 18, 37 y 74 RU.

Y de acuerdo con (islam & Kashem, 2018), un sistema OFDMA utiliza un grupo de subportadoras no superpuestas y formar un subcanal, este puede asignarse a cada estación transmisora. Por lo tanto, varias estaciones pueden enviar datos simultáneamente sin colisión.

Figura 24

OFDM vs OFDMA



Nota: Adaptado de Wi-Fi 6 OFDMA: Resource unit (RU) allocations and mappings, S. Trivedi, 2020, Cisco Blogs(<https://blogs.cisco.com/networking/wi-fi-6-ofdma-resource-unit-ru-allocations-and-mappings>).

En la figura 24 se observa la diferencia entre OFDM y OFDMA, en donde muestra cómo se asigna a cada usuario un subcanal, mientras en OFDM se le asigna todo el ancho de banda en un instante de tiempo en OFDMA se asigna varios RU.

2.3.2.1. RU (Resource Unit)

En un entorno denso de múltiples usuarios, un canal Wi-Fi se puede dividir en subcanales dedicados para permitir que varios usuarios de OFDMA compartan un canal 802.11ax.

Tabla 4

Número de RU soportados por diferentes anchos de banda

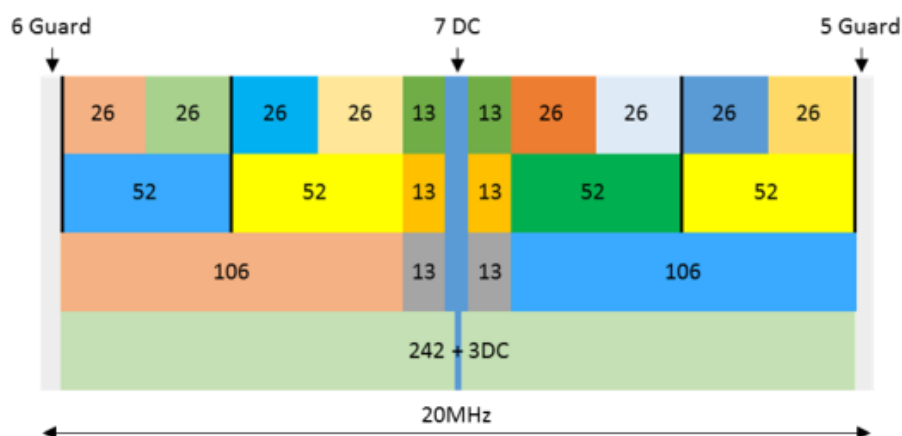
Tamaño de RU	20 MHz	40 MHz	80 MHz	160 MHz
26 subportadoras	9	18	37	74
52 subportadoras	4	8	16	32
106 subportadoras	2	4	8	16
242 subportadoras	1	2	4	8
484 subportadoras	-	1	2	4
996 subportadoras	-	-	1	2
2*996 subportadoras	-	-	-	1

Nota: La tabla muestra la información de RU que soporta cada ancho de banda dependiendo del tamaño de RUs.

La RU más pequeña consta de 26 subportadoras. 802.11ax especifica el número de subportadoras contenidas en RU de diferentes tamaños. Una RU puede contener subportadoras 26/52/106/242/484/996/2*996 (*Wi-Fi 6 Technology and Evolution White Paper*, 2020b). En la tabla 4 se observa cuantos RU soporta en cada ancho de banda. Por ejemplo, en un ancho de banda de 20 MHz se puede albergar hasta 9 RU de 26 subportadoras, es decir conectar hasta 9 usuarios simultáneos.

Figura 25

Número de RU en un canal de 20 MHz



Nota: Adaptado de Wi-Fi 6 Technology and Evolution White Paper (p. 15), ZTE(https://res-www.zte.com.cn/mediare/zte/Files/PDF/white_book/Wi-Fi_6_Technology_and_Evolution_White_Paper-20200923.pdf?la=en), 2020, Copyright © 2020 ZTE Corporation.

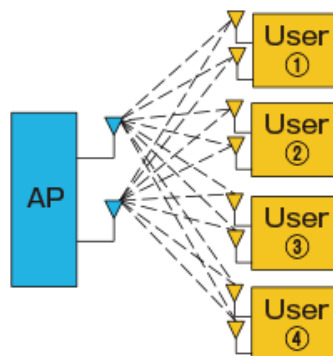
En la figura 25 se observa cómo se distribuye los RU en un canal de 20 MHz. No todas las subportadoras del canal se utilizan para datos, algunas se utilizan como intervalos de guarda (GI) para evitar interferencia como otros canales o subportadoras, mientras otras se utilizan como subportadoras piloto para la sincronización entre el AP y la estación (*Wi-Fi 6 Technology and Evolution White Paper*, 2020b).

2.3.3. MU-MIMO

MU-MIMO (Multi-usuario de múltiples entradas y múltiples salidas), es una tecnología de varias antenas que se basa en la técnica de beamforming (formación de haces). Esta tecnología mejora el rendimiento de un sistema al transmitir flujos de datos a varios usuarios en paralelo (Nayak, 2021), en la figura 26 se aprecia como un AP transmite y recibe información de varios usuarios, permitiendo así demostrar como es el funcionamiento de esta tecnología.

Figura 26

Funcionamiento de MU-MIMO, operan con varios usuarios.



Nota: Adaptado de ¿Qué es Wi-Fi 6?, 2021, Marubun, (<https://www.marubun.co.jp/service/technicalsquare/a7ijkd000000ouie.html>), Copyright©2002-2021 MARUBUN CORPORATION

802.11 ax hereda lo que se conoce como DL MU-MIMO (Downlink MU-MIMO) de 802.11ac, pero agrega UL MU-MIMO (Uplink MU-MIMO) permitiendo hasta 8 antenas, es decir puede transmitir simultáneamente los datos hasta un máximo de ocho usuarios (*Wi-Fi 6 Technology and Evolution White Paper*, 2020b).

2.3.3.1. DL MU-MIMO

DL MU-MIMO opera bajo las mismas condiciones que 802.11ac, es decir según (*Wi-Fi 6 Technology and Evolution White Paper*, 2020b) para realizar el envío de paquetes a las diferentes estaciones, detecta con las diferentes antenas y envía una sonda vacía. Las estaciones reconocen la información recibida del AP. A partir de aquí el AP calcula una matriz de canal para cada STA y luego dirige los haces para transportar la información a cada estación (*¿Qué Es Wi-Fi 6? [Básico] | Cuadrado Técnico | Marubun*, n.d.).

2.3.3.2. UP MU-MIMO

Esta es una nueva tecnología que se introduce en 802.11 ax, permite la recepción de información al AP desde varias estaciones. El proceso para la recepción de información consiste

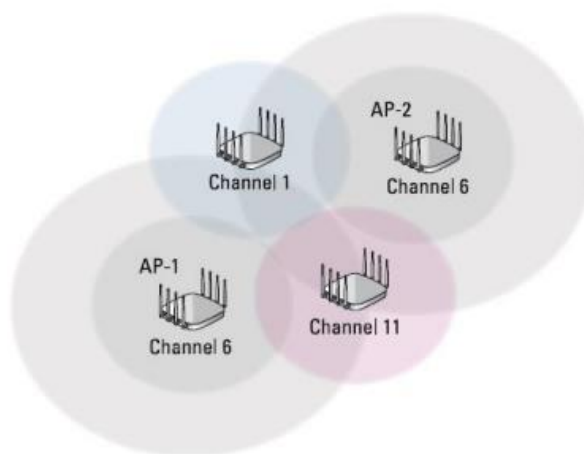
en que el AP inicia un sondeo para conocer el estado del almacenamiento cache y las características del tráfico de las estaciones. Después realiza un cálculo para determinar cómo se debe asignar los flujos espaciales y así realizar una sincronización de transmisión. Luego, utiliza una trama de activación para activar la transmisión, notifica y organiza para que múltiples estaciones realicen el envío de información en enlace ascendente para finalizar con un mensaje de ACK (*Wi-Fi 6 Technology and Evolution White Paper*, 2020b).

2.3.4. BSS Coloring

En una red Wi-Fi en donde existen demasiados AP y estaciones escuchándose entre si se produce lo que se denomina conjunto de servicios básicos superpuestos (OBSS) o interferencia cocanal, este fenómeno se puede observar en la figura 27.

Figura 27

Interferencia OBSS



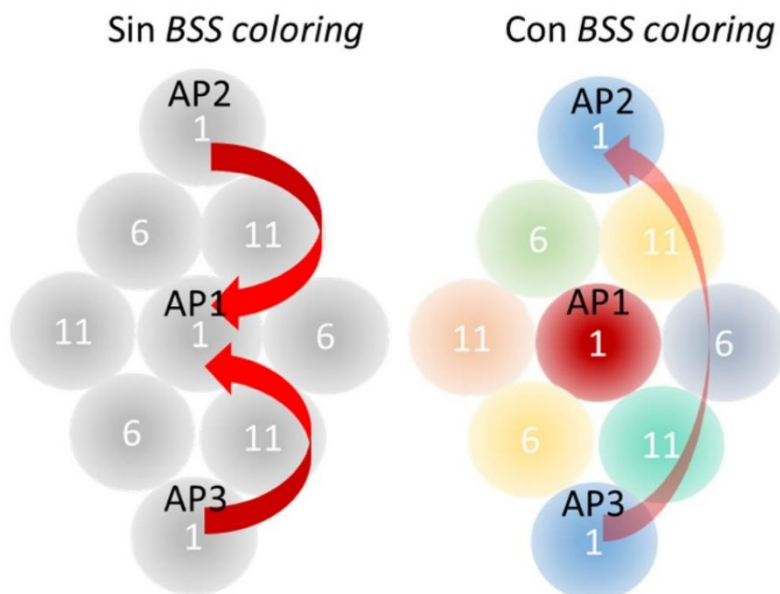
Nota: Adaptado de Estudio Y Análisis de las nuevas tecnologías 802.11ax Y 5G para el desarrollo del Internet de las Cosas (p. 26), A. Mosquera, 2019, Universidad Católica de Santiago de Guayaquil.

Para resolver este inconveniente 802.11 ax mejora la reutilización espacial con la coloración BSS. Este mecanismo aborda la sobrecarga OBSS mediante la asignación de una “color” diferente, para esto se agrega un valor entre 0 y 7 en el encabezado PHY (Mosquera Chica,

2019), en la figura 28 se puede observar cómo se representa este mecanismo y como es la asignación de color, a diferencia que no tenga BSS coloring.

Figura 28

Proceso de asignación de color en un OBSS.



Nota: Adaptado de Así es WiFi 6, el WiFi que viene para revolucionar la conexión en casa, Editorial Nobbyt, Nobbyt(<https://www.nobbyt.com/redes/wifi-6-el-mejor-wifi/>), 2019.

El procedimiento de escucha de 802.11 ax es el siguiente:

- Si el bit es del mismo color o valor, la trama se considerará para una transmisión intra-BSS y la radio que escucha se aplaza.
- Si el bit es de diferente color o valor, la radio considerara que la trama es una transmisión BSS de un OBSS y comprende que el medio está ocupado.

2.3.5. TWT (Target Wake Time)

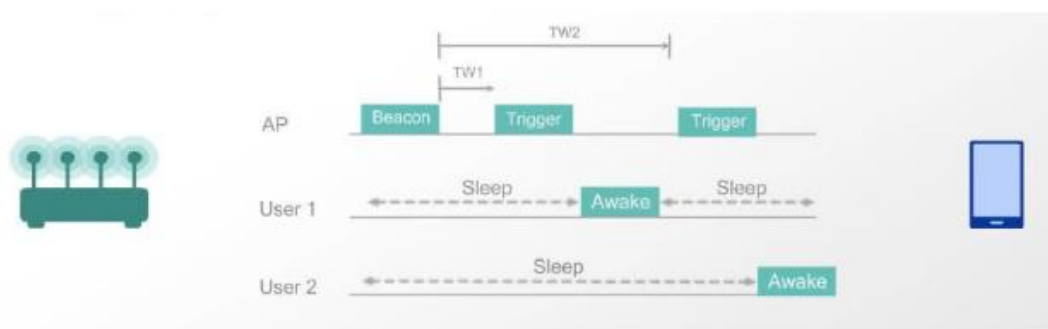
Esta es una función que se adopta del estándar 802.11ah con la diferencia que permite la transmisión con enlaces ascendentes, esta función permite a los dispositivos “dormir” por más

tiempo, y activarse previo a una negociación con el AP, este mecanismo permite ahorro de energía de los dispositivos (Mosquera Chica, 2019). Generalmente la estación solicita un horario para despertar en el futuro.

En la figura 29 se puede observar cómo es el proceso de TWT en una transmisión, se observa que el dispositivo se encuentra dormido mientras no se le envíe datos, y se activa al momento de recibir datos, una vez que recibe estos datos se vuelve a dormir, todo este proceso ya está previamente negociado con el AP.

Figura 29

Proceso de TWT entre un AP y una estación.



Nota: Adaptado de ¿Qué es WiFi 6 y por qué va a mejorar tu red WiFi de casa?, J. Penalva, 2019, Xataka(<https://www.xataka.com/especiales/que-wifi-6-que-va-a-mejorar-tu-red-wifi-casa-cuando-te-conectes-a-publica>)

Además de reducir el consumo energético, con TWT de 802.11ax se reduce la sobrecarga e ineficacia del proceso normal de contención de las redes Wi-Fi.

El mecanismo de TWT comprende dos conceptos importantes: período de sesión (SP) que es el tiempo en el que una estación está despierta para recibir o enviar información, y el acuerdo TWT es el acuerdo entre el AP y la estación que define los detalles de SP a los que pertenecerá la estación (Mosquera Chica, 2019).

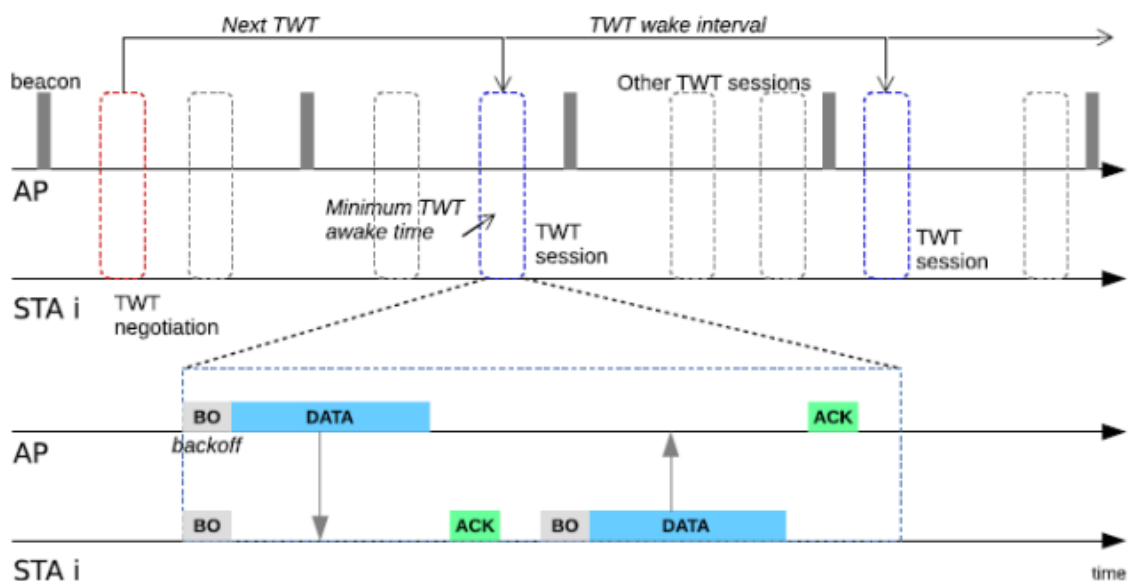
TWT tiene dos modos de operación:

- **TWT individual**

Es cuando la estación elige la programación después de negociar con el AP, una vez que se produce el acuerdo TWT se produce la secuencia escogida por la estación. En la figura 30 se presenta el proceso de acuerdo TWT individual, se observa que existe la negociación TWT y el dispositivo se encuentra en estado de reposo hasta que se inicia la sesión TWT en donde se procede al envío y recepción de datos para después reanudar el estado de reposo (Mosquera Chica, 2019).

Figura 30

Acuerdo TWT individual



Nota: Adaptado de Estudio Y Análisis de las nuevas tecnologías 802.11ax Y 5G para el desarrollo del Internet de las Cosas (p. 92), A. Mosquera, 2019, Universidad Católica de Santiago de Guayaquil.

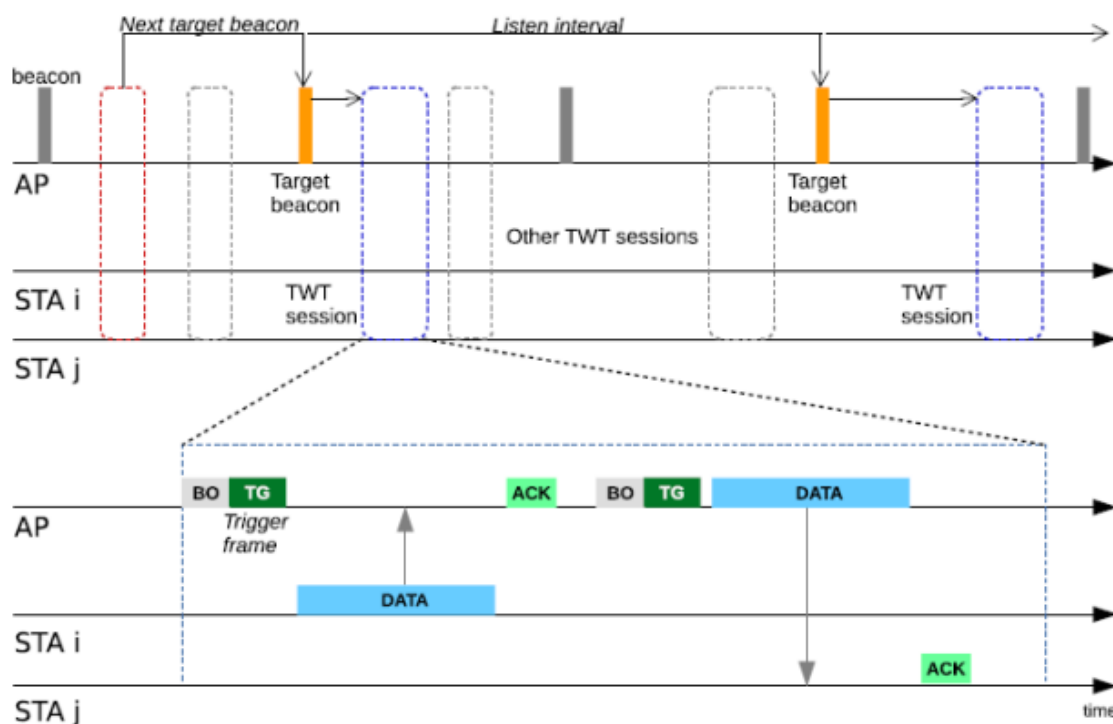
- **TWT broadcast**

Es cuando el AP decide la programación, envía parámetros en el Beacon utilizando el elemento TWT, aquí el AP proporciona a todas las estaciones el horario de cuando empieza a

transmitir o cuando entren en estado de reposo. En la figura 31 se puede apreciar que la negociación se realiza con dos estaciones, y de la misma forma cuando se le informa a la estación de una sesión TWT empieza el envío y recepción de datos, para después continuar en modo de reposo (Mosquera Chica, 2019).

Figura 31

Acuerdo TWT broadcast



Nota: Adaptado de Estudio Y Análisis de las nuevas tecnologías 802.11ax Y 5G para el desarrollo del Internet de las Cosas (p. 92), A. Mosquera, 2019, Universidad Católica de Santiago de Guayaquil.

3. Capítulo III: Requerimientos y Diseño

En este capítulo se realiza el diseño de los entornos inalámbricos para el estudio del rendimiento de 802.11ax basados en la metodología en cascada y etapas del tesbed, el cual incluye un análisis de la tecnología 802.11 ac y 802.11ax con la finalidad de definir las características, requerimientos de la tecnología y limitaciones del tesbed para posteriormente realizar el diseño de este, también seleccionar los componentes tanto en hardware como software que integran el sistema.

3.1. Análisis

3.1.1. Metodología en cascada

El proyecto estará basado en la metodología en cascada, este modelo sigue una secuencia lineal permitiendo identificar etapas específicas las cuales se deben dar cumplimiento (González González et al., 2019).

Para el desarrollo de la solución se debe recopilar información teórica que permitirá sustentar los objetivos de la investigación, es importante entender que es la tecnología, que características tiene, cuáles son sus ventajas y desventajas, cómo funciona la tecnología a nivel de capas, entender todos los parámetros necesarios para medir su rendimiento y por último como se lo implementaría en un banco de pruebas.

En la primera etapa (Análisis) se identifican y evalúan las necesidades y restricciones para el proyecto, con lo cual, si hay dudas en los requisitos, poder mitigarlos mediante el análisis de características y requerimientos planteados, para posteriormente determinar las mejores alternativas y darle viabilidad al proyecto.

En la segunda etapa (Diseño) se tiene el estudio de las alternativas y restricciones que puede generar el proyecto, aquí se identifican y especifican las condiciones para el desarrollo del proyecto como son: sistemas operativos de código abierto(Linux), entornos de desarrollo(Visual Studio, Pydev), lenguajes de programación(Phyton, Java, C), dispositivos necesarios para la infraestructura(concentradores, placas Raspberry, puntos de acceso entre otros), además permite identificar las características y requerimientos necesarios para la infraestructura inalámbrica en diferentes entornos, como son número de dispositivos, marcas, tipo de topología a utilizar para un correcto diseño del banco de pruebas.

En la tercera etapa (Implementación). En esta etapa se realiza la implementación del banco de pruebas, este estará compuesto de dispositivos basados en tecnología 802.11ax.

En la cuarta etapa (Verificación) se debe poner a prueba la red y verificar su funcionamiento, aquí en esta etapa se compara los resultados obtenidos con los resultados teóricos, se debe verificar si los objetivos del proyecto fueron cumplidos.

En la quinta etapa (Mantenimiento) se planifica al final del proyecto, si se producen errores, existen inconvenientes o los resultados no son los esperados, se busca soluciones en las alternativas planteadas, en donde si existe una mejor solución, se la aplicará hasta tener la solución terminada y con la calidad requerida.

3.1.2. Tesbed.

Un tesbed o banco de pruebas es una plataforma que permite experimentar proyectos, estos bancos de prueba proporcionan un medio de demostración que es riguroso sobre la comprobación o demostración de características de nuevas tecnologías en un ambiente real para probar la eficiencia de este(Chico et al., 2013).

3.1.2.1. Objetivo del tesbed

- Determinar los principales elementos para el desarrollo del banco de pruebas.
- Desarrollar de manera teórica los fundamentos y características de 802.11ax.
- Dimensionar los diferentes escenarios del tesbed.
- Implementar y realizar pruebas de funcionamiento y rendimiento de la tecnología.
- Analizar los datos reales vs los teóricos y determinar el rendimiento de este.

3.1.2.2. Etapas

El desarrollo del tesbed comprende las siguientes etapas:

La primera etapa denominada etapa de análisis, se realizará un sondeo de todos los elementos necesarios para poder demostrar las características esenciales de 802.11 ax., además de determinar los datos teóricos en un ambiente ideal de las funciones y mecanismos de 802.11ax.

La segunda etapa se denomina etapa de generación de los escenarios, aquí se realizará y dimensionará los diferentes escenarios para realizar las pruebas, se realizará las configuraciones y se obtendrá un entorno real, pero controlado de una red 802.11ax.

La tercera etapa corresponde a la etapa de implementación, esta tiene como objetivo generar un conjunto de datos que serán analizados posteriormente en la siguiente fase, se emplean diferentes situaciones, parámetros que permitan comprender el funcionamiento y rendimiento de la red.

La cuarta etapa se denomina etapa de análisis de datos, el propósito de esta etapa es analizar los datos obtenidos y compararlos con los teóricos, y demostrar cómo actúa la red en un entorno real, que parámetros podemos ajustar para obtener un mejor rendimiento de la red.

La quinta etapa es la etapa de mantenimiento, esta etapa consiste en modificar los parámetros para obtener los datos más correctos y de mejor rendimiento, repitiendo así las diferentes etapas hasta conseguirlo, además a partir de estos datos se realizará las guías de laboratorio que permitirán entender el funcionamiento de la tecnología.

3.1.3. Características de la tecnología

Para la definición de requerimientos se basa en la información bibliográfica de la tecnología, para lo cual se profundiza en características de 802.11 ac como su antecesor y 802.11ax como tecnología actual, dando a conocer que características se mantienen y cuáles son las nuevas implementaciones en 802.11ax. En la tabla 5 se enlista las principales características de las tecnologías.

Tabla 5

Características de 802.11 ac y ax

Característica	802.11 ac	802.11ax
Bandas de operación	5 GHz	2.4/5 GHz
Anchos de canal	20-40-80-80+80-160 MHz	20-40-80-80+80-160 MHz
Velocidad de datos	3.6 Gbps*	9.6 Gbps*
Multiplexación	OFDM	OFDMA
Espacio de subportadora	312.5 KHz	78.125 KHz
Tiempo de símbolo OFDM	3,2 us	12,8 us
Tiempo de símbolo	3.6/4.0 us	13.6/14.4/16.0 us
Rango de cobertura	200-250 metros	500-800 metros
Modulación	BPSK, QPSK, 16/64/256 QAM	BPSK, QPSK 16/64/256/1024 QAM

Flujos espaciales	4	8
Unidades de recursos (RU)	No soportado	Soportado
MU MIMO UL	No soportado	Soportado
MU MINO DL	Soportado	Soportado
Reutilización espacial (BSS)	No soportado	Soportado
TWT	No soportado	Soportado
Seguridad WPA 3	Soportado (Depende del dispositivo)	Soportado
Throughput	-	-

Nota 1: Tomado de (CWNA_Certified_Wireless_Network_Administ, n.d.)

Nota 2: La tabla muestra las principales características de 802.11 ac y ax a tomar en cuenta.

Nota 3: Los valores de la tabla son netamente teóricos.

* Depende del número de flujos y canales utilizados.

3.1.4. Requerimientos

El análisis y estudio que se realizó con anterioridad permite conocer los requisitos necesarios para realizar el proyecto, en donde se definirán requerimientos de Stakeholders, requerimiento de arquitectura y de sistema para diseñar el tesbed, estos requerimientos serán planteados acorde a la información bibliográfica de la tecnología, ya que esto permitirá elegir el software y hardware para el correcto funcionamiento y análisis de la tecnología.

3.1.5. Stakeholders

Los stakeholders son las personas que se involucran, supervisan y contribuyen en el proyecto de manera directa o indirecta, en la tabla 6 se detalla el listado de stakeholders.

Tabla 6
Lista de stakeholders

Lista de stakeholders
1. Msc. Carlos Vásquez Director de tesis
2. Sr. Adonis Narváez
3. Ing. Jaime Michilena Opositor de tesis
4. Ing. Henry Farinango
5. Ing. Santiago Meneses

Nota: Autoría propia

3.1.6. Requerimientos de stakeholders

Los requerimientos de los stakeholders vienen definidos por las características que se observan o son deseables por los interesados y especifican requisitos de manera general, estos requerimientos de detallan en la tabla 7, además se utiliza STSR como nomenclatura para una mejor comprensión y se los puede sintetizar como requerimientos operacionales.

Tabla 7
Requerimientos operacionales

STSR		Prioridad		
#	Requerimientos	Alta	Media	Baja
STSR1	Tamaño e integración de los dispositivos pequeño.		X	
STSR2	Flexibilidad de manejo.	X		
STSR3	Tesbed acorde al entorno de pruebas.	X		
STSR4	Dimensionamiento para varias arquitecturas	X		
STSR5	Sniffer para 802.11ax	X		

STSR6	Analizador de espectro		X
STSR7	Debe ser económicamente eficiente	X	

Nota: Autoría propia

Estos requerimientos son parte de la propuesta de desarrollo del tesbed, ya que para posteriores pruebas y manejos de este se debe cumplir con estos requisitos para poder cumplir los objetivos planteados.

3.1.7. Requerimientos de sistema

En la tabla 8 se puntualizan los requisitos del sistema que son los que comprenden el funcionamiento del tesbed, desde el software hasta el hardware ya que son factores importantes en el diseño de la red y permite entender que función cumplirán los dispositivos en el tesbed, y se los denota con la nomenclatura SYSR.

Tabla 8
Requerimientos del sistema

SYSR				
#	Requerimientos del sistema	Prioridad		
		Alta	Media	Baja
REQUERIMIENTOS DE USO				
SYSR1	Facilidad para crear escenarios y evaluar las redes		X	
SYSR2	Simplicidad de manejo		X	
SYSR3	Manual de configuración.		X	
SYSR4	Fácil conexión de dispositivos.	X		
REQUERIMIENTOS DE PERFORMANCE				
SYSR5	Sniffer compatible y funcional con cualquier computador		X	

SYSR6	Access Point debe tener todas las características 802.11ax		X
SYSR7	Los dispositivos del tesbed deben soportar 802.11 ax	X	
SYSR8	Integración de software para mapas de calor		X
SYSR9	Soporte para el sistema operativo		X
SYSR10	Conexión remota para configuración	X	
REQUERIMIENTOS DE INTERFACES			
SYSR11	Compatibilidad entre marcas de dispositivos 802.11ax		X
SYSR12	Dispositivos con acceso a internet		X
SYSR13	Conexión mediante HDMI		X
SYSR14	Conexión a periféricos (mouse, teclado)		X
REQUERIMIENTOS DE ESTADO			
SYSR10	Constantemente enviando información		X
SYSR11	Encendido y apagado de dispositivos	X	
REQUERIMIENTOS DE FÍSICOS			
SYSR12	Los nodos formaran diferentes arquitecturas		X
SYSR13	Tamaño reducido		X
SYSR14	Protección contra manipulación a las tarjetas		X
SYSR15	Protección contra el ambiente	X	

Nota: Autoría propia

3.1.8. Requerimientos de arquitectura

Estos requerimientos examinan los requisitos de hardware como software. Se realiza un análisis de los principales requerimientos y a partir de aquí seleccionar el hardware y software que se adapte de mejor manera al proyecto, la nomenclatura utilizada es SRSR.

Tabla 9
Requerimientos de arquitectura

SYSR				
#	Requerimientos	Prioridad		
		Alta	Media	Baja
REQUERIMIENTOS DE DISEÑO				
SRSH1	El tesbed debe contar con un AP principal, un sniffer y nodos clientes	X		
SRSH2	Los dispositivos deben ser de fácil acceso y conexión.	X		
SRSH3	Manipulable para diferentes arquitecturas		X	
SRSH4	Tesbed escalable		X	
REQUERIMIENTOS DE HARDWARE				
SRSH5	Deben estar disponibles en el mercado	X		
SRSH6	Se debe poder integrar nodos al sistema	X		
SRSH7	Compatible con cualquier sistema operativo		X	
SRSH8	Tenga características propias de 802.11ax	X		
SRSH9	Los dispositivos deben ser de doble banda		X	
SRSH10	Deben soportar red mallada		X	
SRSH11	El AP debe contar con puertos ethernet		X	
SRSH12	Dispositivos compatibles con sistemas de código abierto		X	
SRSH13	Antena para sniffer debe soportar modo monitor	X		
SRSH14	Placa SBC de hasta 4 GB de RAM, con entrada HDMI		X	
SRSH15	Placas y dispositivos de tamaño reducido		X	
REQUERIMIENTOS DE SOFTWARE				

SRSH16	Compatible con software libre		X
SRSH17	Lenguajes de programación versátiles		X
SRSH18	Acople de librerías y firmware de antenas	X	
SRSH19	Menores requerimientos para procesamiento		X
SRSH20	IDE para configuración		X
SRSH21	Licencias gratuitas		X
REQUERIMIENTOS LÓGICOS			
SRSH22	Vinculación de todos los nodos a la red	X	
SRSH23	Transmisión de datos de varios tamaños		X
SRSH24	Funcionamiento con WPA3	X	
SRSH25	Captura de diferentes tramas		X
SRSH26	Herramientas para compilar		X
REQUERIMIENTOS ELÉCTRICOS			
SRSH27	Alimentación de entre 5 y 12 voltios hasta 2 amperios		X

Nota: Autoría propia

3.2. Alcance de la propuesta

En esta sección se enlistan las restricciones y los riesgos presentes en el proyecto, esto de manera general, con la finalidad de mostrar temas que no se consideran en el desarrollo del proyecto.

3.2.1. Restricciones

- El estudio se limita a características propias de 802.11ax
- El estudio se limita a evaluar el rendimiento de la tecnología, más no a compararla con versiones anteriores.

3.2.2. Riesgos

- Tiempo de envío y recepción de los dispositivos desde el exterior.
- Dispositivos no cuentan con todas las características necesarias para un despliegue completo de 802.11ax.
- Incompatibilidad entre dispositivos.
- No poder demostrar todas las características de la tecnología por falta de recursos.
- Falta de nodos clientes para algunas pruebas.

3.3. Desarrollo de la propuesta

3.3.1. Selección de hardware

La selección del hardware está sujeta a los requerimientos antes mencionados, entre más características sean acertadas habrá un mejor resultado que cumpla con los objetivos.

La selección de hardware es importante para dar cumplimiento a las características de los dispositivos a utilizar, los dispositivos primordiales son el AP, los nodos clientes, el sniffer y las antenas, para esto se realizará una tabla comparativa con valoración de 1 y 0 como se indica en la tabla 10.

Tabla 10

Nomenclatura para selección de hardware y software

Descripción	Nomenclatura
Si cumple	1
No cumple	0

Nota: Autoría propia

- **Selección del AP**

Para seleccionar el AP se comparará dos marcas al fin de seleccionar el mejor acorde a los requerimientos, esto se aprecia en la tabla 11.

Tabla 11
Análisis comparativo de APs

Hardware	SRSH3	SRSH6	SRSH7	SRSH8	SRSH9	SRSH13	SRSH7	Total
Huawei AX3	1	1	1	1	1	1	1	7
Tp-link AX1800	0	1	1	1	1	1	0	5

Nota: Autoría propia

Figura 32
Huawei AX3 Quad Core



Acorde a los resultados de la tabla 11, el AP que mejor se adapta a los requerimientos es el Huawei AX3, cuya imagen se ilustra en la figura 32, cuya principal ventaja en comparación a otras marcas es su costo y fácil adquisición.

- **Selección de la placa SBC**

Para la selección de la placa SBC, se tomará en cuenta dos marcas, de las cuales se seleccionará una acorde a la comparación realizada en la tabla 12.

Tabla 12
Análisis comparativo de placas SBC

Hardware	SRSH3	SRSH5	SRSH10	SRSH12	SRSH13	SRST7	Total
Raspberry CM4	1	1	1	1	1	1	6
ASUS Tinker	1	1	1	1	1	0	5

Board

Nota: Autoría propia

Figura 33
Placa Raspberry Pi



Acorde a los resultados de la tabla 12, la mejor opción es la Raspberry Pi, cuya imagen se ilustra en la figura 33, y su principal ventaja es el costo y facilidad de adquisición.

- **Selección de Antenas**

Para seleccionar las antenas a utilizar se comparará antenas tipo mini PCIe, tomando en cuenta que para las raspberry se necesitan PCIe, estas comparaciones se pueden apreciar en la tabla 13.

Tabla 13
Análisis comparativo de antenas PCIe

Hardware	SRSH3	SRSH4	SRSH5	SRSH6	SRSH7	SRSH10	SRSH11	SRST7	Total
Intel ax200 y ax210	1	1	1	1	1	1	1	1	7
Netely	1	1	0	1	1	1	0	1	6

Nota: Autoría propia

Figura 34
Antena Intel AX200



En base a los resultados de la tabla 14, la mejor opción para el sniffer es la antena de Intel ax200 y ax210, ya que su mayor característica es que soporta modo monitor, indispensable para la captura de paquetes, se puede observar este dispositivo en la figura 34.

3.3.2. Selección de software

Una parte importante es el software que permitirá la conexión entre los dispositivos mediante instrucciones, estructuras y programas. A continuación, se realiza la selección del software en base a sus requerimientos para el desarrollo del proyecto.

- **Software para la placa SBC**

Este software es con el que trabajara la placa Raspberry, este software debe cumplir con la mayoría de las características de software, además de ser compatible con la placa, en la tabla 14 se observa la comparación entre dos sistemas operativos libres.

Tabla 14
Análisis comparativo de SO

S.O.	SRSH14	SRSH15	SRSH16	SRSH17	SRST7	Total
Ubuntu	1	1	1	0	1	4

Raspberry Pi OS	1	1	1	1	1	5
-----------------	---	---	---	---	---	---

Nota: Autoría propia

En base a los resultados de la tabla comparativa el sistema que más se ajusta a las necesidades del proyecto es Raspberry Pi OS, su principal ventaja es los requerimientos que necesita para operar.

- **Software para el sniffer**

Para el sniffer se considerará una laptop, a la cual se le instalará el sniffer, para determinar el mejor se realiza una comparación entre dos principales sniffer como se indica en la tabla 15.

Tabla 15

Análisis comparativo de sniffers

Software	SYSR2	SRSR14	SRSR21	SRSR16	SRST7	Total
Wireshark	1	1	1	1	1	5
Acrylic	1	1	1	1	0	4

Nota: Autoría propia

Como se observa en la tabla 16, los dos sniffer tienen las mismas condiciones, para el estudio se utilizará Wireshark, ya que la única ventaja es su costo, este software es gratuito.

- **Software y hardware para análisis de señal y frecuencia.**

Para el análisis de la señal y la frecuencia se utilizará una estación de monitoreo del espectro Radioeléctrico, realizada por Wilman Suarez en su tesis de postgrado “Observatorio de radio comunicaciones para el análisis del espectro radio eléctrico en la zona 1 del Ecuador”(Suarez, 2022). En su tesis realiza una estación capas de monitorear el espectro radioeléctrico mediante placa Raspberry, permitiendo así mostrar cómo se comporta el espectro en diferentes ámbitos.

Uno de los principales es la frecuencia de 2,4 Ghz, que es la banda utilizada por wifi y el software utilizado es mediante Linux.

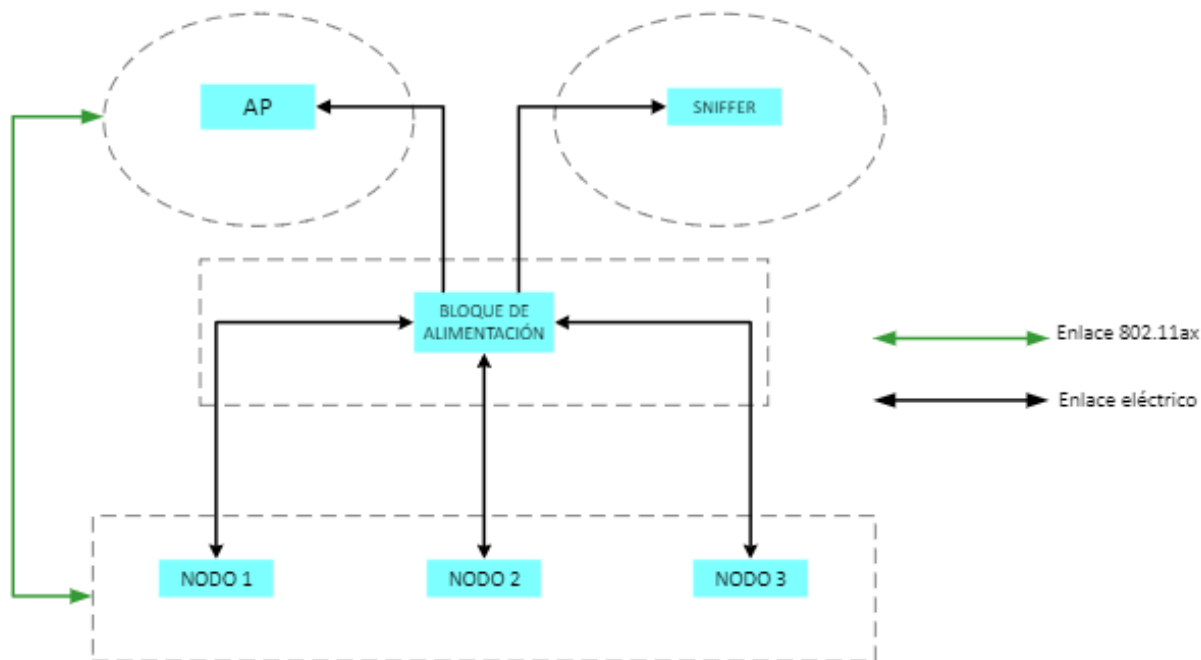
3.3.3. Bloques del sistema

A continuación, se presenta cada uno de los diagramas de bloques que conformaran el sistema, esto permitirá entender cómo funcionará cada elemento del tesbed y como se interconectaran cada uno de ellos.

3.3.3.1. Diagrama de bloque de todo el sistema.

A continuación, en la figura 35 se detalla el diagrama de bloque del sistema de manera general para posteriormente detallar cada uno de los bloques y procesos del tesbed.

Figura 35
Diagrama de bloques del tesbed.

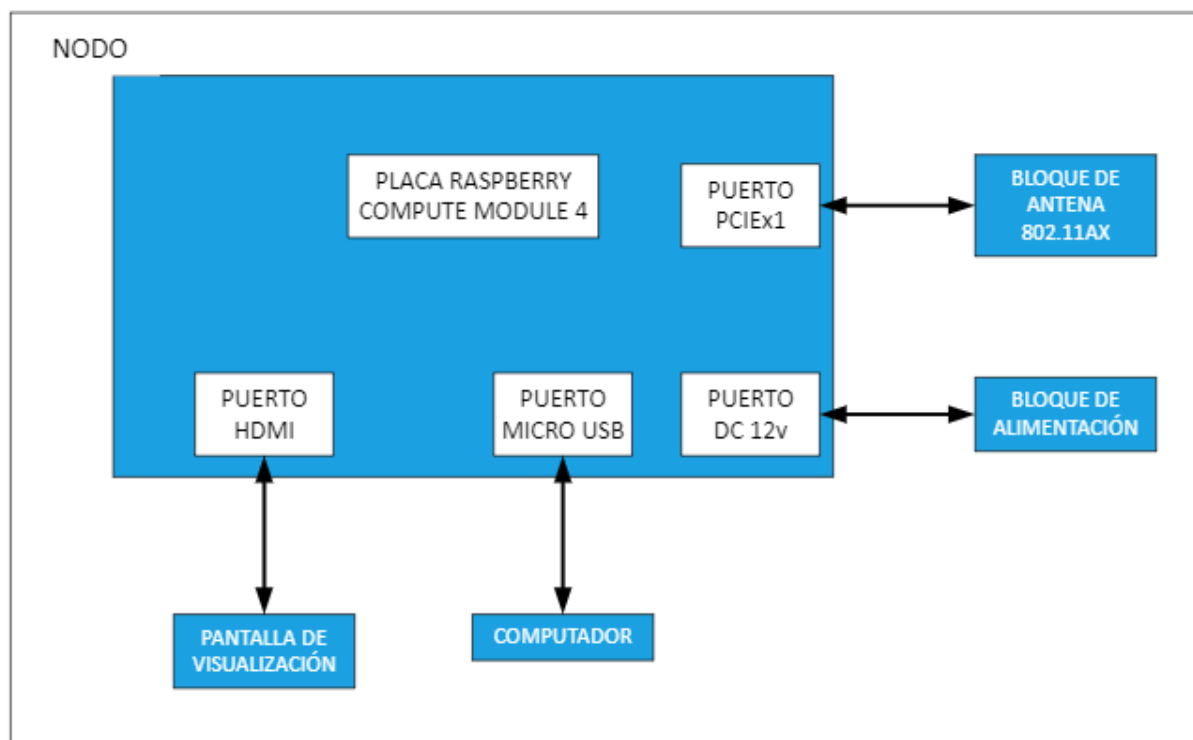


3.3.3.2. Diagrama de bloque de los nodos

En la figura 36, se observa el diagrama de bloques de los nodos, cada nodo estará compuesto por una antena, una placa Raspberry Pi, su alimentación y una pantalla para su visualización.

Figura
Diagrama de bloques de los nodos

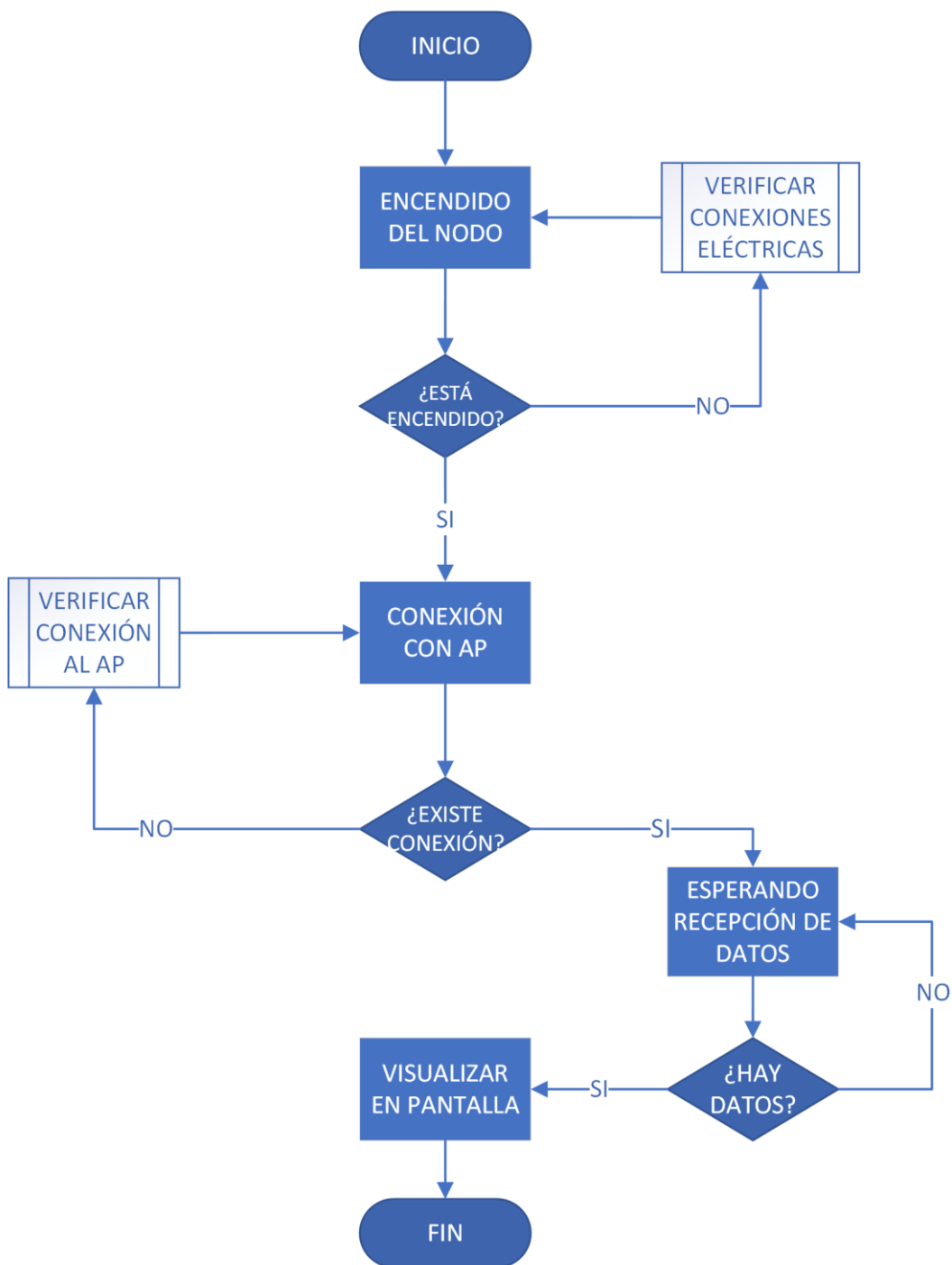
36



Se puede observar que el nodo está compuesto de un bloque con la antena 802.11ax conectada al puerto PCIe x1 del board, un puerto HDMI que permitirá la conexión a una pantalla para la visualización del sistema operativo y de los datos, un puerto micro usb esclavo que permitirá la conexión hacia el computador para cargar el sistema y el kernel, un puerto DC a 12v para energizar la placa, y lo más importante el módulo CM4 de raspberry que es la fuente de cada nodo.

A continuación, en la figura 37 se detalla el proceso mediante un diagrama de flujos del funcionamiento de este.

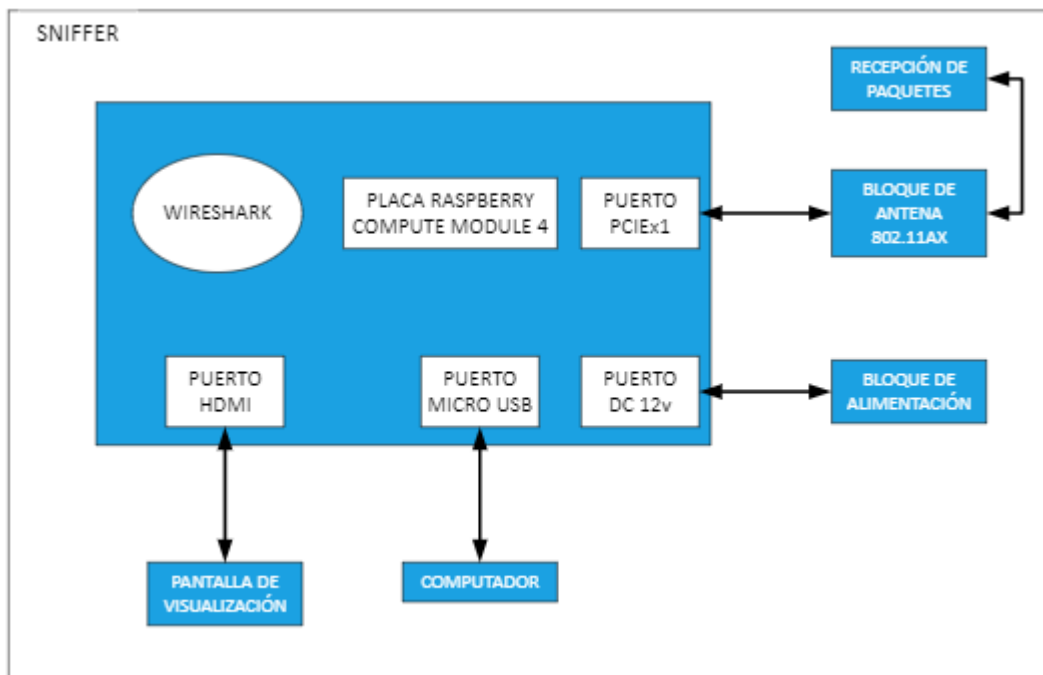
Figura 37
Flujograma de los nodos



3.3.3.3. Diagrama de bloque del sniffer

Figura 38

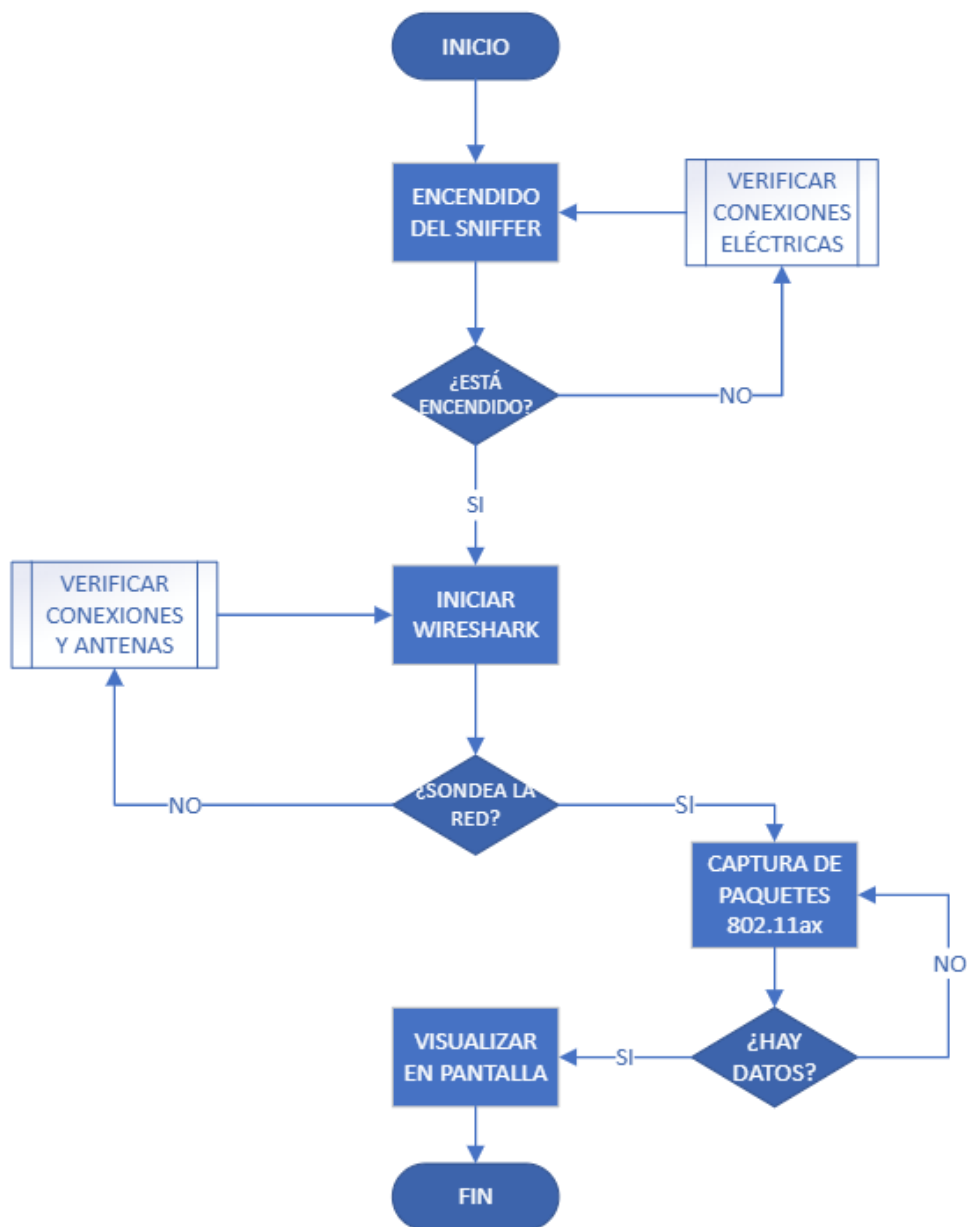
Diagrama de bloques del sniffer



El diagrama de la figura 38, corresponde al funcionamiento del sniffer, como se puede observar este estará constituido por una antena conectada a la placa, el programa wireshark instalado en este y se lo podrá visualizar en pantalla.

En la figura 39 se puede observar el funcionamiento mediante su diagrama de flujos.

Figura 39
Diagrama de flujo del sniffer



3.3.4. Flujogramas de funcionamiento

En este apartado se realiza el flujograma del funcionamiento del sistema, se indica como será el proceso para la configuración y conexión de los nodos a la red.

3.3.5. Diseño y configuración de los nodos

El proyecto necesitará de nodos para las correspondientes conexiones, para esto se utilizará una Raspberry Pi como se muestra en la figura 40 como placa SBC de acuerdo con los requerimientos de hardware antes mencionados.

Figura 40
Placa Raspberry



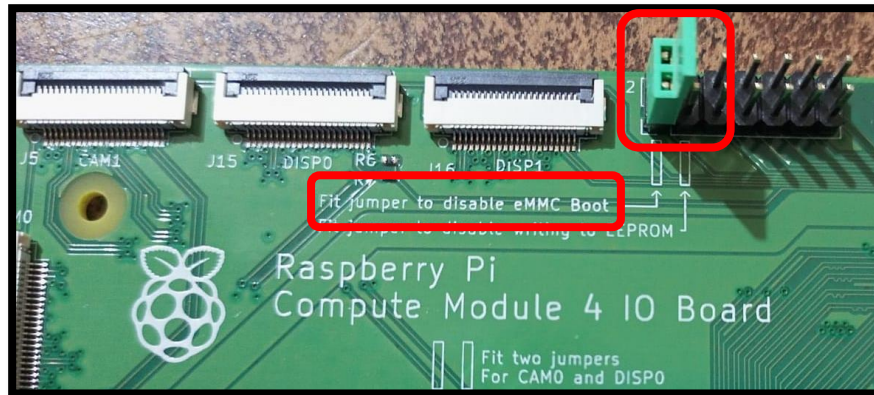
En la figura 40, se indica la conexión física de los elementos que componen los nodos, está conformado por la placa, la alimentación y su antena.

3.3.5.1. Configuración del nodo

Instalación del sistema operativo

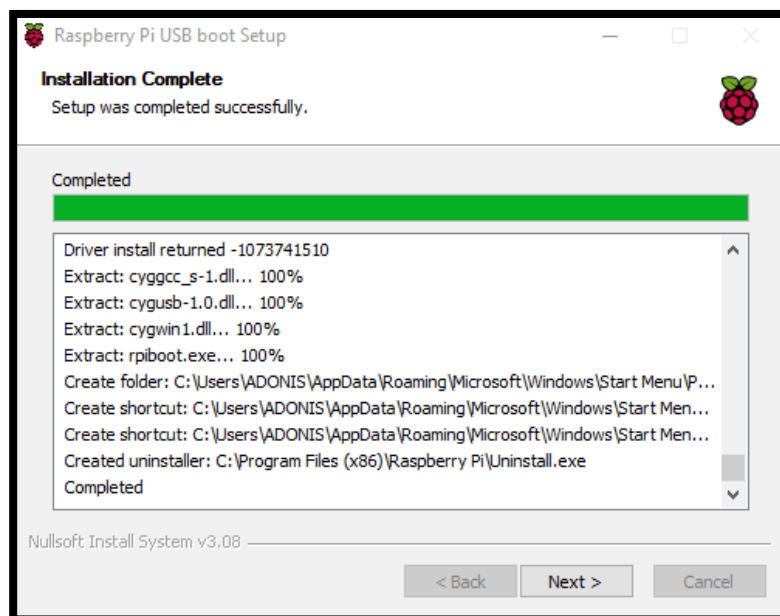
Antes de instalar el sistema operativo se debe preparar la raspberry para que instale en la memoria eMMC, para que posteriormente el sistema arranque desde esa unidad. Para esto se debe realizar un puente entre dos pines de la raspberry como se indica en la figura 41 para deshabilitar el arranque desde esa unidad.

Figura 41
Deshabilitar eMMC boot



A continuación, es necesario que la PC detecte la raspberry como una unidad de almacenamiento, para esto se descarga un ejecutable para Windows desde el siguiente enlace https://github.com/raspberrypi/usbboot/raw/master/win32/rpiboot_setup.exe, y se procede a instalarlo como se indica en la figura 42, una vez instalado se conecta la raspberry al computador y lo detectara como unidad de almacenamiento.

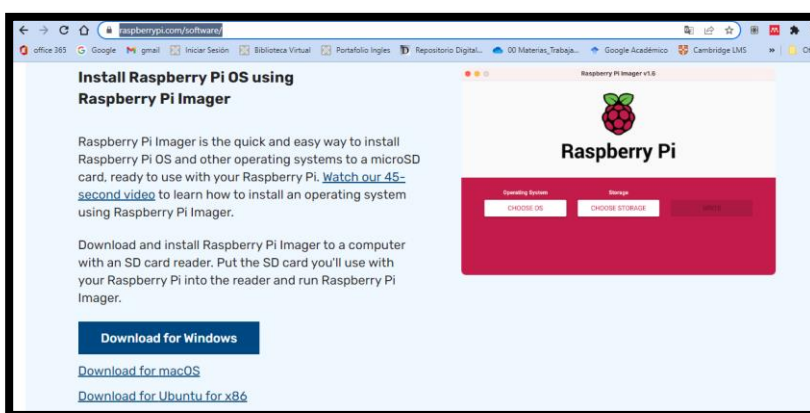
Figura 42
Instalación de rpiboot



Cada nodo debe tener un sistema operativo y un lugar para almacenarlo. Raspberry en la actualidad tiene una herramienta denominada Raspberry Pi Imager, esta permite una instalación del sistema operativo sencilla en una tarjeta SD, para el caso en la memoria eMMC, a continuación, se indica el proceso de instalación.

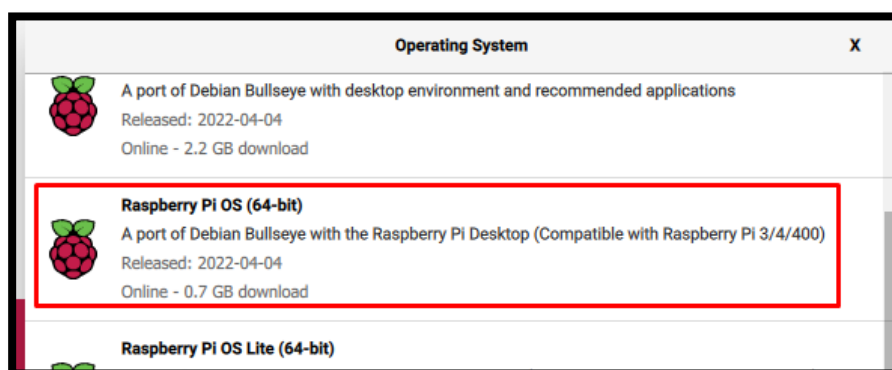
- Descargar Raspberry Pi Imager del siguiente enlace <https://www.raspberrypi.com/software/>, e instalarlo.

Figura 43
Página oficial de Raspberry



- Seleccionar el sistema operativo a instalar (Raspberry Pi OS de 64 bits)

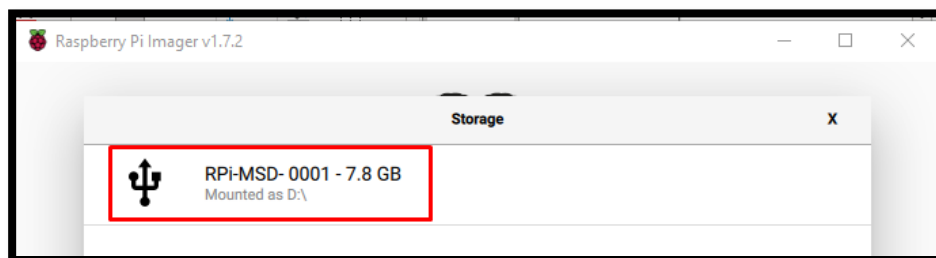
Figura 44
Selección del Sistema Operativo



- Seleccionar la tarjeta de memoria

Figura 45

Selección del almacenamiento



- Dar clic en el botón Write

Una vez finalizada la instalación se procede a quitar el jumper y a energizar la placa, el sistema operativo comenzara a cargar, se configura y en la figura 46 se observa la pantalla principal del SO.

Figura 46

Escritorio de Raspberry Pi OS



Instalación de la antena en la Raspberry CM4

Antes de iniciar con la instalación hay que tener en cuenta que la tarjeta tiene un puerto PCIe x1, en el cual se conectara el adaptador con la tarjeta inalámbrica ax200 o ax210.

Una vez iniciada la Raspberry se procede a verificar si la tarjeta es reconocida en el puerto, mediante el comando “**sudo lspci -vvv**”, mostrando la salida que se indica en la figura 47.

Figura 47

Reconocimiento del puerto PCIe



```

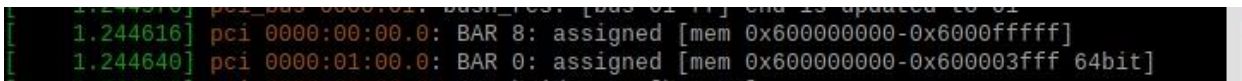
pi2@raspberrypi: ~
Archivo  Editar  Pestañas  Ayuda
pi2@raspberrypi:~ $ sudo lspci
00:00.0 PCI bridge: Broadcom Inc. and subsidiaries BCM2711 PCIe Bridge (rev 20)
01:00.0 Network controller: Intel Corporation Device 2725 (rev 1a)
pi2@raspberrypi:~ $

```

A continuación, hay que verificar que no exista problemas de asignación de BAR, mediante el comando “**dmesg**”, mostrando la siguiente salida que se muestra en la figura 48.

Figura 48

Asignación de espacio



```

[ 1.244616] pci 0000:00:00.0: BAR 8: assigned [mem 0x600000000-0x6000ffff]
[ 1.244640] pci 0000:01:00.0: BAR 0: assigned [mem 0x600000000-0x600003fff 64bit]

```

Las tarjetas 802.11ax en los entornos actuales no son reconocidas de manera directa, por tal motivo es indispensable realizar una compilación cruzada, para realizar este proceso es importante realizar la compilación en un entorno Linux, ya que el proceso es mucho más rápido.

Para realizar la compilación cruzada se realiza el siguiente procedimiento.

1. Se copia el siguiente repositorio con el comando:

```

sudo apt install git bc bison flex libssl-dev make
git clone --depth=1 https://github.com/raspberrypi/linux

```

2. Se crea un archivo de configuración .config.

```

cd linux
make ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu- bcm2711_defconfig

```

3. A continuación, se edita el archivo `.config` mediante el menú, con el siguiente comando.

```
make ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu- menuconfig
```

4. Una vez ingresado al menú, se procede a habilitar las siguientes opciones, y se guarda la configuración.

- Controladores de dispositivos > Compatibilidad con dispositivos de red > LAN inalámbrica > Intel > "Intel Wireless WiFi Next Gen AGN (iwlwifi)"
- "Intel Wireless WiFi MVM Firmware support" (en la opción `iwlwifi`, una vez seleccionada)

5. Por último, se debe compilar el núcleo con el siguiente comando.

```
make -j8 ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu- Image modules dtbs
```

6. Una vez terminada la compilación se debe copiar el nuevo kernel a la raspberry para lo cual es importante montar la unidad de la siguiente manera.

```
sudo mkdir -p mnt/fat32  
sudo mkdir -p mnt/ext4  
sudo mount /dev/sda1 mnt/fat32  
sudo mount /dev/sda2 mnt/ext4
```

7. Ahora se procede a copiar los archivos necesarios.

```
sudo cp arch/arm64/boot/Image mnt/fat32/kernel8.img  
sudo cp arch/arm64/boot/dts/broadcom/*.dtb mnt/fat32/  
sudo cp arch/arm64/boot/dts/overlays/*.dtb* mnt/fat32/overlays/  
sudo cp arch/arm64/boot/dts/overlays/README mnt/fat32/overlays/
```

8. Se instala los módulos del kernel en la unidad y se los copia también.

```
sudo env PATH=$PATH make ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu-  
INSTALL_MOD_PATH=mnt/ext4 modules_install  
sudo cp arch/arm64/boot/Image mnt/fat32/kernel8.img  
sudo cp arch/arm64/boot/dts/broadcom/*.dtb mnt/fat32/  
sudo cp arch/arm64/boot/dts/overlays/*.dtb* mnt/fat32/overlays/  
sudo cp arch/arm64/boot/dts/overlays/README mnt/fat32/overlays/
```

9. Por último, se desmonta la unidad.

```
sudo umount mnt/fat32  
sudo umount mnt/ext4
```

10. Una vez iniciada la raspberry con el nuevo kernel, se procede a instalar el firmware de la interfaz inalámbrica de la siguiente manera.

```
$ wget https://wireless.wiki.kernel.org/_media/en/users/drivers/iwlwifi/iwlwifi-cc-46.3cfab8da.0.tgz  
$ tar -xvzf iwlwifi-cc-46.3cfab8da.0.tgz  
$ cd iwlwifi-cc-46.3cfab8da.0/  
$ sudo cp iwlwifi-*.ucode /lib/firmware
```

11. Una vez realizado este procedimiento se reinicia la raspberry y se verifica la conexión mediante la interfaz.

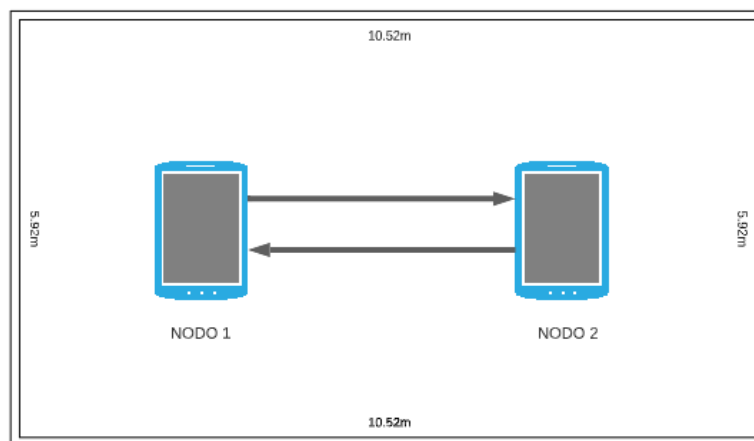
3.3.6. Escenarios para pruebas

Los escenarios de pruebas estarán determinados por los modos de funcionamiento de la red, y las características de 802.11ax.

- **Escenario 1: Modo ad-hoc sin interferencia**

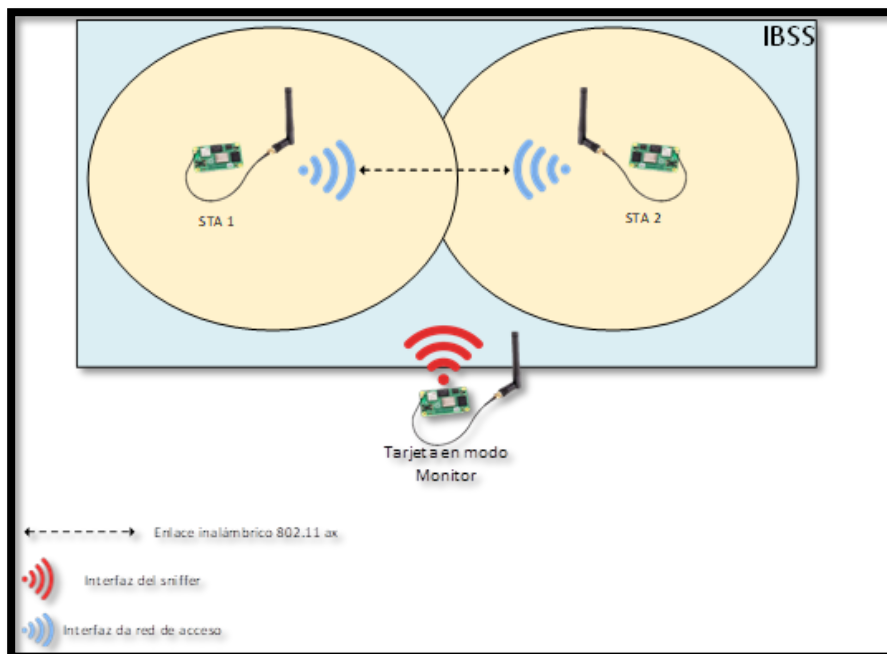
Figura 49

Escenario 1 Modo Ad-hoc



Este escenario permitirá ver la conexión entre dos dispositivos 802.11ax, sin la necesidad de una infraestructura para operar, el medio estará libre sin interferencia de ningún tipo, tendrán línea de vista directa como se observa en la figura 49.

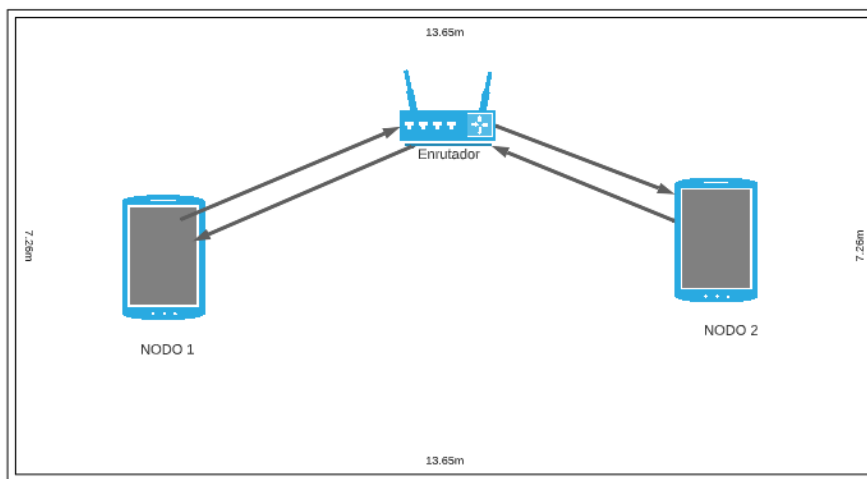
Figura 50
 Topología de la red Ad-hoc



La red estará formada por dos dispositivos Raspberry con sus correspondientes antenas, y establecerán una comunicación directa. La topología de la red se puede observar en la figura 50.

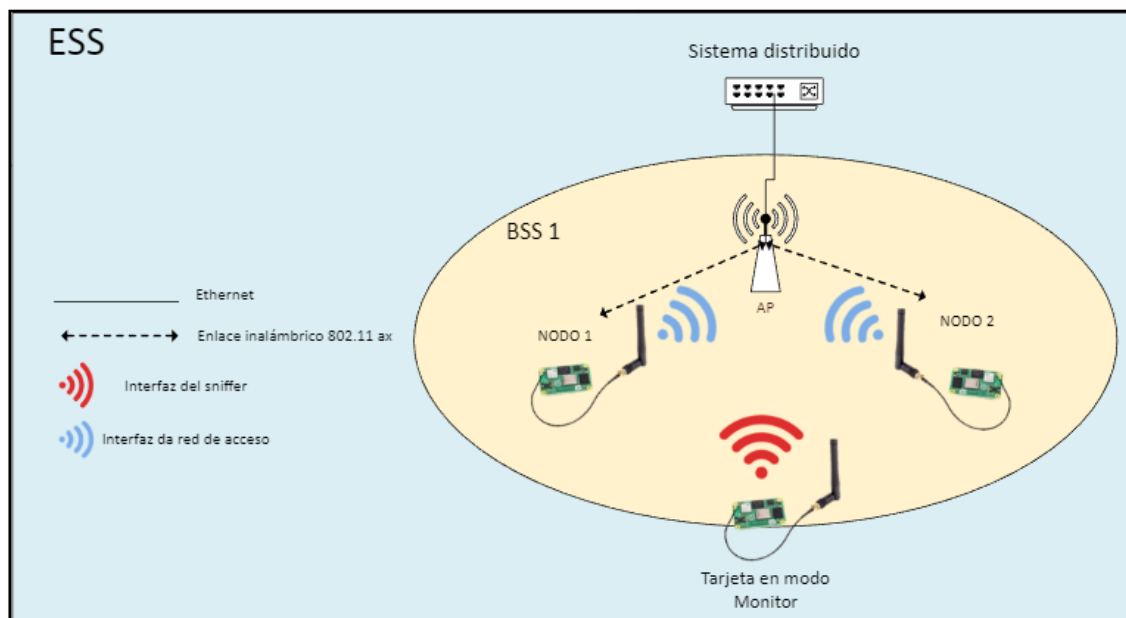
- **Escenario 2: Modo infraestructura sin interferencia**

Figura 51
 Escenario 2 Modo Infraestructura sin interferencia



Este escenario permitirá la conexión de dos dispositivos 802.11 ax, mediante un enrutador que también operará con este protocolo, el medio para esta comunicación también será un medio sin interferencias de ningún tipo, como se observa en la figura 51.

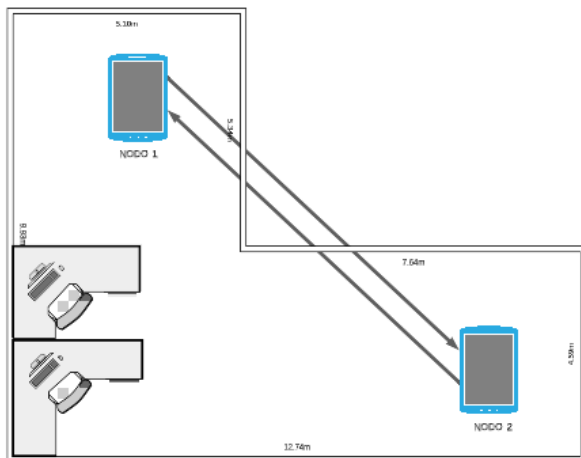
Figura 52
Topología de la red en modo infraestructura



Esta red estará conformada de dos nodos Raspberry, conectados a un router mediante sus interfaces wifi, como se observa en la figura 52.

- **Escenario 3: Modo ad-hoc con interferencia**

Figura 53
Escenario 3 Modo ad-hoc con interferencia

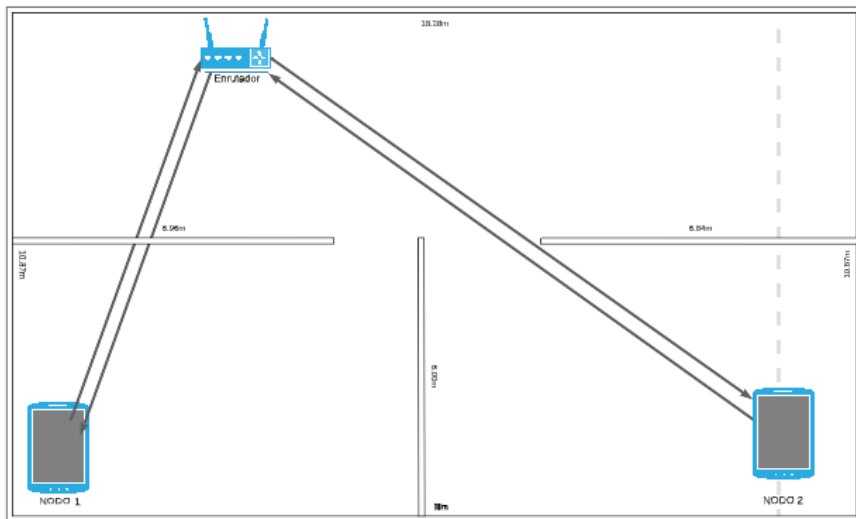


En este escenario se tiene la red en modo ad-hoc con la diferencia que estará en un ambiente con interferencia, como se indica en la figura 53.

La topología para este escenario corresponde a la figura 50, con la única diferencia que estará implementada en un ambiente con interferencias.

- **Escenario 4: Modo infraestructura con interferencia.**

Figura 54
Escenario 4 Modo Infraestructura con interferencia



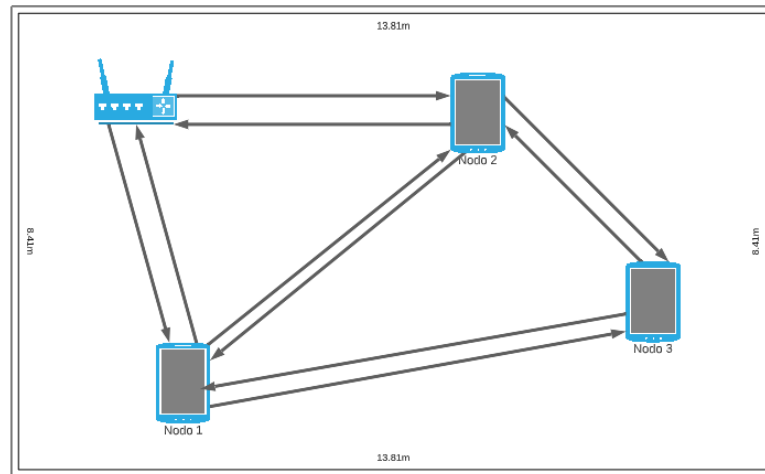
En este escenario la red en modo infraestructura estará en un ambiente con interferencias, como se indica en la figura 54.

La topología para este escenario corresponde a la figura 52, con la única diferencia que estará implementada en un ambiente con interferencias.

- **Escenario 5: Modo mesh sin interferencia**

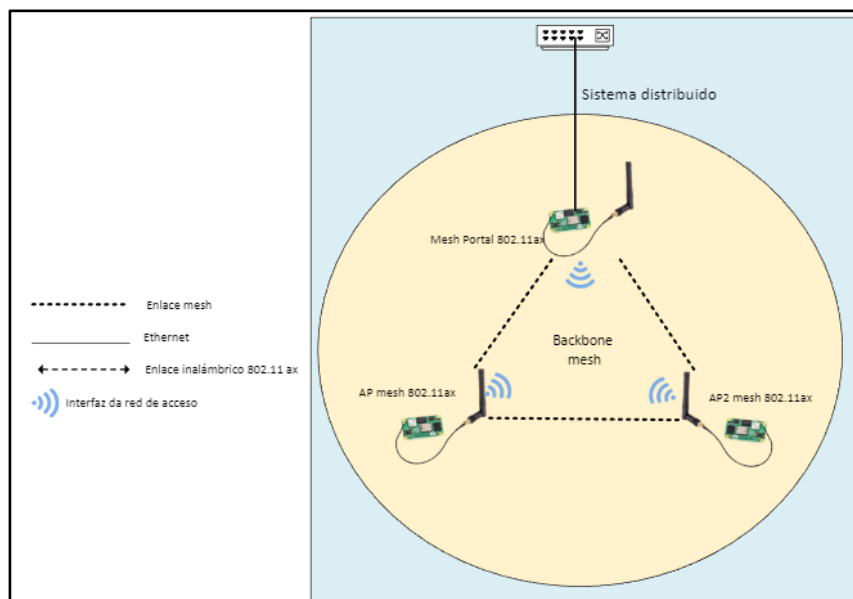
Figura 55

Escenario 5 Red mesh sin interferencia



En la figura 55 se observa el escenario de una red mesh, pero sin interferencia, estos nodos se comunicarán entre ellos hasta llegar al enrutador.

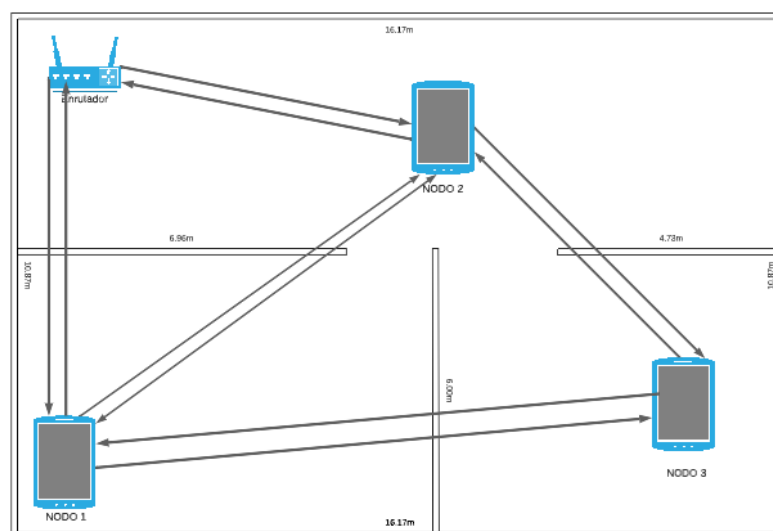
Figura 56
Topología de la red mesh



Esta red está formada por tres nodos, los cuales se comunicarán entre sí para poder comunicarse con el router principal, de tal forma se puede tener una mayor cobertura, la topología de esta red se puede observar en la figura 56.

- **Escenario 6: Modo mesh con interferencia**

Figura 57
Escenario 6 Red mesh con interferencia



En este escenario la red operará en modo mesh, pero se encontrará en un ambiente con interferencia, se comunicarán entre dispositivos hasta poder salir por el enrutador principal, como se observa en la figura 57.

La topología para este escenario corresponde a la figura 56, con la única diferencia que estará implementada en un ambiente con interferencias

3.4. Dimensionamiento

Para el dimensionamiento de los diferentes escenarios se toma en consideración los siguientes parámetros.

- **Eficiencia del canal.** - Este parámetro permitirá determinar cuanta información buena y valida fue transmitida por el canal.
- **Potencia recibida.** - Este parámetro está vinculado al área de cobertura, permitiendo obtener la cantidad de potencia recibida, además de encontrar el SNR (Relación señal a ruido).
- **Existencia de interferencia.** - Permite determinar si existe perdida de paquetes, retransmisiones, permitiendo saber si la eficiencia de la red cae.
- **Velocidad de transferencia.** - Es un parámetro que permitirá conocer la velocidad a la que se envía la información.
- **Seguridad.** - Determinará la seguridad del nuevo estándar WPA3.
- **Ahorro de energía.** - Este parámetro se utiliza para verificar el funcionamiento de la nueva característica de 802.11ax, el TWT.

Para determinar estos parámetros se toma también en cuenta las siguientes métricas, que permitirán verificar el rendimiento de la red.

- **Link Budget (Balance del enlace).** - El balance de enlace permite calcular el valor total de las ganancias y pérdidas en una comunicación entre transmisor y receptor.
- **BER (Bit Error Ratio).**- Tasa de error bit media, es la relación que existe entre el número de bits recibidos errados sobre el número total de bits recibidos.
- **SNR (Signal to Noise Ratio).** - La relación señal a ruido, es una métrica que permite determinar si la cantidad de ruido existente en la comunicación afecta o no a la transmisión.
- **Latencia.** - Es el tiempo que tarde un paquete en transmitirse por la red, entre menor tiempo mejor será la comunicación.
- **Packetloss.** - Son paquetes que se pierden durante una transmisión, las causas son varias, pero las principales se deben a congestión de la red y al medio de transmisión.
- **Througput.** - Tasa de transferencia efectiva, es la cantidad neta que atraviesa en la red.
- **Jitter.** - Variaciones de latencia, este parámetro permite determinar las variaciones que existe en la comunicación de tal manera que interrumpa en varias ocasiones a la transmisión.
- **Cobertura.** - La cobertura permite determinar el rango en el cual las transmisiones son posibles sin que existan desconexiones.

Todos estos parámetros y métricas están involucrados en cada uno de los escenarios, a partir de aquí se verificará el rendimiento de la red y a su vez las nuevas características de 802.11ax.

3.5. Direccionamiento

A continuación, se presenta el direccionamiento de cada dispositivo involucrado en cada una de las redes 802.11ax. En la tabla 16 se presenta el direccionamiento para la red ad-hoc, En la tabla 17 se presenta el direccionamiento para la red de infraestructura, y en la tabla 18 para la red mesh.

Tabla 16

Direccionamiento para la red ad-hoc

Dispositivo	Interfaz	Dirección IP	Gateway predeterminado
NODO 1	802.11ax	192.168.50.1 /24	-
NODO 2	802.11ax	192.168.50.2 /24	-

Tabla 17

Direccionamiento para la red de infraestructura

Dispositivo	Interfaz	Dirección IP	Gateway predeterminado
Router	802.11ax	192.168.101.1 /24	-
NODO 1	802.11ax	192.168.101.2 /24	192.168.101.1
NODO 2	802.11ax	192.168.101.3 /24	192.168.101.1
NODO 3	802.11ax	192.168.101.4 /24	192.168.101.1

Tabla 18

Direccionamiento para la red mesh

Dispositivo	Interfaz	Dirección IP	Gateway predeterminado
NODO GW	802.11ax	192.168.100.1 /24	192.168.100.1
NODO 2	802.11ax	192.168.100.2 /24	192.168.100.1
NODO 3	802.11ax	192.168.100.3 /24	192.168.100.1

4. Capítulo IV: Implementación y pruebas

En el presente capítulo se realiza la implementación de cada parte del tesbed, juntamente con la fase de pruebas que validaran el funcionamiento del tesbed, se probara cada uno de los escenarios, métricas y parámetros determinados con anterioridad, y se analizara cada uno de los resultados obtenidos y así poder generar las prácticas de laboratorio.

4.1. Implementación de la red Ad-hoc

Para levantar la red se utiliza dos nodos, en cada uno se configurará el modo ad-hoc para que se comuniquen entre ellos, el procedimiento se detalla a continuación.

Para los dos nodos es la misma configuración con la diferencia que a cada uno se le asignará una dirección ip diferente, pero en la misma red, para el nodo1 192.168.100.1 y para el nodo 2 192.168.100.2, además se debe asignar el nombre de la red “RED”, el modo de operación y la contraseña.

```
sudo nano /etc/network/interfaces
```

```
auto wlan0
iface wlan0 inet static
address 192.168.100.1
netmask 255.255.255.0
network 192.168.100.0
wireless-channel 1
wireless-essid RED
wireless-mode ad-hoc
wireless-key 1234567890
```

```
sudo wpa_cli terminate
```

```
sudo service networking restart
```

Una vez se ha configurado los dos nodos, se observa en la figura 58 que se ha realizado la conexión ad-hoc, además de la comunicación entre nodos mediante el comando ping.

Figura 58
Conexión Ad-Hoc

```

pi@raspberrypi:~$ iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0      IEEE 802.11  ESSID:"RED"
           Mode:Ad-Hoc  Frequency:2.412 GHz  Cell: D6:65:F8:F5:35:E0
           TX-Power=22 dBm
           Retry short limit:7   RTS thr:off   Fragment thr:off
           Power Management:on

pi@raspberrypi:~$ ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data:
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.997 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.868 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.814 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=0.868 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=64 time=0.889 ms

```

4.2. Implementación de la red de infraestructura

Para levantar la red en modo infraestructura se utiliza un AP conectado a la red principal, además de dos nodos clientes que serán las raspberry, estos nodos se conectarán al AP tanto en 2.4 y 5 GHz, para esto se configura el AP de la siguiente manera:

1. Se configura el AP tanto en la banda de 2.4 GHz y 5GHz, asignando el canal, el modo que será 802.11 ax y el ancho de banda permitido que va desde 20 hasta 160 en 5Ghz, como se indica en la figura 59.

Figura 59
Configuración del AP

The image shows a configuration interface for an Access Point (AP) with two sections: "Wi-Fi de 2.4 GHz" and "Wi-Fi de 5 GHz".

- Wi-Fi de 2.4 GHz:**
 - Canal: 6
 - Modo: 802.11b/g/n/ax
 - Ancho de banda: 20/40 MHz
 - Intervalo de guarda 11ax: Corto
 - Wi-Fi invisible: Deshabilitado
 - WMM: Habilitar
- Wi-Fi de 5 GHz:**
 - Canal: 44
 - Modo: 802.11a/n/ac/ax
 - Ancho de banda: 20/40/80/160 MHz
 - Intervalo de guarda 11ax: Corto

2. También se debe configurar la red Wifi, es decir asignarle el SSID y escoger el tipo de seguridad en este caso WPA3, como se muestra en la figura 60.

Figura 60
Configuración de la red Wifi.

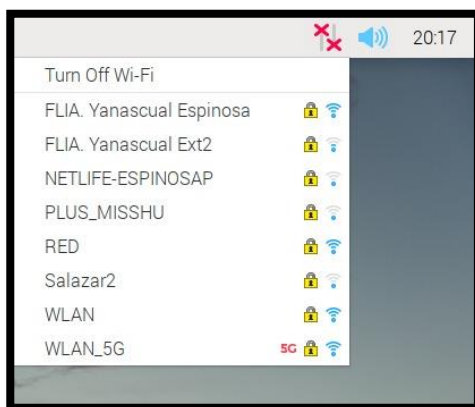
The image shows a configuration interface for Wi-Fi networks with two sections: "Wi-Fi de 2.4 GHz" and "Wi-Fi de 5 GHz".

- Wi-Fi de 2.4 GHz:**
 - Nombre de la red Wi-Fi: WLAN
 - Seguridad: WPA2 PSK / WPA3 SAE
 - Contraseña de la red Wi-Fi: [oculto]
- Wi-Fi de 5 GHz:**
 - Nombre de la red Wi-Fi: WLAN_5G
 - Seguridad: WPA2 PSK / WPA3 SAE
 - Contraseña de la red Wi-Fi: [oculto]

Nota: Asegúrese de que el modo WPA2-PSK/WPA3-SAE se admita en todos los dispositivos conectados. Si los dispositivos detectan problemas de conexión durante su uso, vuelva al modo WPA2-PSK.

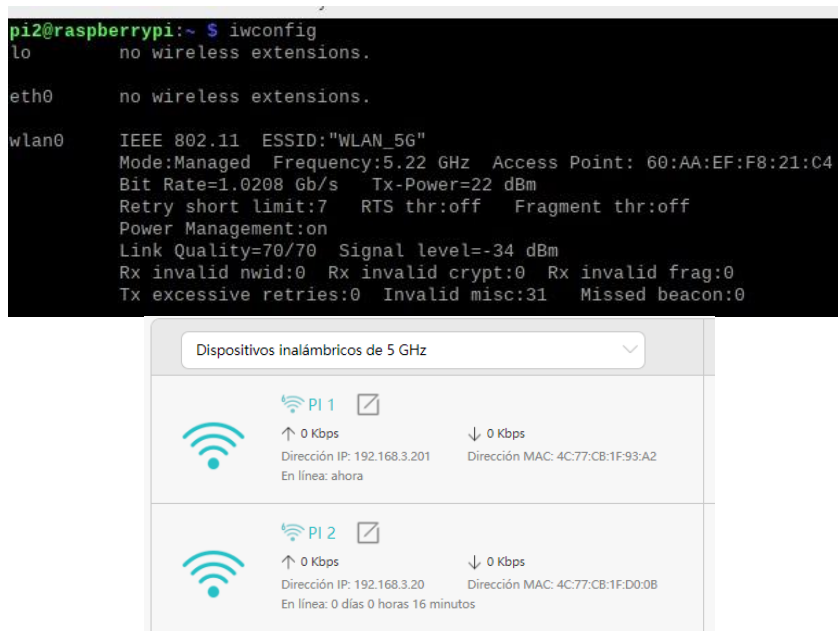
3. Una vez realizada estas configuraciones se puede apreciar que en las raspberry ya aparecen las dos redes WLAN y WLAN_5G, esto se observa en la figura 61.

Figura 61
Redes disponibles



4. Para conectarse solo es necesario ingresar la contraseña, además se verifico las ip y la conexión de los dos raspberry al AP, como se indica en la figura 62.

Figura 62
Conexión de clientes al AP



4.3. Implementación de la red mesh

Para la creación de la red mallada se utilizará el protocolo BATMAN, con la herramienta para Linux batman-adv, este protocolo de enrutamiento permite la creación de una red ad-hoc avanzada, la cual a través de los diferentes nodos realiza la comunicación.

Para implementar la red se realiza el siguiente procedimiento en cada uno de los nodos que conformarán la red mallada.

1. Primero, se debe instalar la herramienta con el comando **“sudo apt-get install -y batctl”**.
2. Se crea un archivo con el siguiente comando y nombre **“sudo nano batman-adv-conf.sh”**
3. Dentro del archivo se debe ingresar la siguiente información, tomando en cuenta que si son nodos que no son Gateway el modo es cliente.

```
#!/bin/bash
#Selección de la interfaz a usar con el protocolo batman-adv
sudo batctl if add wlan0
sudo ifconfig bat0 mtu 1468
#Indicar que el dispositivo ejercera de nodo en la red mesh
sudo batctl gw_mode client
#Habilitar y activar las interfaces empleadas por el protocolo batman-adv
sudo ifconfig wlan0 up
sudo ifconfig bat0 up
#Asignar una ip estática al nodo
sudo ifconfig bat0 192.168.100.1/24
```

4. Ahora para que el archivo se pueda ejecutar se asigna permisos con el comando **“sudo chmod +x batman-adv-conf.sh”**

5. A continuación, se debe crear un archivo con el comando **“sudo nano /etc/network/interfaces.d/wlan0”**
6. Dentro del archivo se coloca la siguiente información en donde se especifica el canal de operación de la red, el nombre de la red y el modo de operación.

```

auto wlan0

iface wlan0 inet manual

wireless-channel 1

wireless-ssid MESH

wireless-mode ad-hoc

```

7. Ahora, para que se inicie el archivo al encenderse la raspberry se debe configurar el siguiente archivo **“sudo nano /etc/rc.local”**, ubicando la siguiente instrucción al final del archivo.

```

/home/pi/batman-adv-conf.sh &

```

8. Una vez finalizada esta configuración, se debe reiniciar la raspberry.

Si la raspberry va a ser Gateway, se debe realizar la siguiente configuración extra.

1. Se descarga el paquete dnsmasq con el comando **“sudo apt-get install -y dnsmasq”**
2. Una vez instalado se ingresa en la siguiente ruta **“sudo nano /etc/dnsmasq.conf”**, y al final del archivo se coloca las siguientes líneas de código, indicando el rango de direcciones IP, y la interfaz en la que va a operar.

```

interface=bat0

dhcp-range=192.168.100.2,192.168.100.10,255.255.255.0,12h

```

3. Ahora, se vuelve a ingresar al archivo de batman-adv, y se actualiza la información con las siguientes líneas de código, esto permitirá indicar que el nodo será Gateway, además se

ingresa reglas iptables para que el tráfico pueda ingresar y salir de la red, mediante este nodo.

```
#!/bin/bash

#Selección de la interfaz a usar con el protocolo batman-adv

sudo batctl if add wlan0

sudo ifconfig bat0 mtu 1468

#Indicar que el dispositivo ejercerá de nodo en la red mesh

sudo batctl gw_mode server

#Habilitar el reenvío de puertos

sudo sysctl -w net.ipv4.ip_forward=1

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -A FORWARD -i eth0 -o bat0 -m conntrack --ctstate RELATED,ESTABLISHED -j
ACCEPT

sudo iptables -A FORWARD -i bat0 -o eth0 -j ACCEPT

#Habilitar y activar las interfaces empleadas por el protocolo batman-adv

sudo ifconfig wlan0 up

sudo ifconfig bat0 up

#Asignar una IP estática al nodo

sudo ifconfig bat0 192.168.100.1/24
```

Se verifica mediante el comando **iwconfig**, se observa que la configuración realizada fue implementada, como se indica en la figura 63 el ESSID es MESH1, el modo es ad-hoc y la frecuencia corresponde al canal 36, además que se formó una celda con un ID aleatorio.

Figura 63
Configuración de MESH

```

pi@raspberrypi:~$ iwconfig
lo          no wireless extensions.

eth0       no wireless extensions.

wlan0      IEEE 802.11  ESSID:"MESH1"
           Mode:Ad-Hoc  Frequency:5.18 GHz  Cell: 92:F1:BA:AE:2B:31
           Tx-Power=22 dBm
           Retry short limit:7   RTS thr:off   Fragment thr:off
           Power Management:on

bat0       no wireless extensions.

```

Con el comando **ifconfig**, se puede observar en la figura 64 como se asignó la IP a la interfaz **bat0**, con la cual trabaja la red mesh.

Figura 64
Asignación de IP a la interfaz **bat0**

```

pi@raspberrypi:~$ ifconfig
bat0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
      inet 192.168.100.1 netmask 255.255.255.0 broadcast 192.168.100.255
      inet6 fe80::af1:3b2a:aaa9:cab2 prefixlen 64 scopeid 0x20<link>
      ether 56:e9:e4:bb:f3:99 txqueuelen 1000 (Ethernet)
      RX packets 3065 bytes 134052 (130.9 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 179 bytes 15676 (15.3 KiB)
      TX errors 0 dropped 225 overruns 0 carrier 0 collisions 0

```

Para observar los vecinos que se forman en la red mesh, se utiliza un comando propio de **batctl**, que es “**sudo batctl n**”, como se observa en la figura 65 existen dos nodos conectados entre ellos.

Figura 65
Vecinos de la red mesh

```

pi@raspberrypi:~$ sudo batctl n
[B.A.T.M.A.N. adv 2021.3, MainIF/MAC: wlan0/4c:77:cb:1f:d0:0b]
IF          Neighbor          last-seen
wlan0       4c:77:cb:1f:d0:0b  0.640s
wlan0       48:68:4a:ea:27:fc  0.792s

```


Por último, se verifica la comunicación entre los nodos mediante el comando ping, como se observa en la figura 66.

Figura 66

Verificación de la comunicación entre nodos

```

pi@raspberrypi:~$ ping 192.168.100.3
PING 192.168.100.3 (192.168.100.3) 56(84) bytes of data.
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=0.714 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.717 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.765 ms
^C
--- 192.168.100.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.714/0.732/0.765/0.023 ms
pi@raspberrypi:~$ ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=45.3 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.644 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.646 ms
^C
--- 192.168.100.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.644/15.518/45.265/21.034 ms

```

4.4. Instalación y configuración de las herramientas.

Para realizar las pruebas en los diferentes escenarios se utilizará varias herramientas como son: D-ITG, iperf, jperf, analizador de espectro y wireshark, que permitirán obtener datos para el posterior análisis de los parámetros y métricas. El proceso de instalación de estas herramientas se puede encontrar detallado en los Anexos B.

4.5. Implementación de pruebas

4.5.1. Red ad-hoc sin interferencia

Para implementar las pruebas se considerará las siguientes condiciones que se muestran en la tabla 19.

Tabla 19
Condiciones para la red ad-hoc

Condición	Valor
Banda de operación	2,4
Ancho de canal	20 MHz
Flujos espaciales	2
Canal	11
Número de nodos	2
Distancia	5 metros.

- **Verificar conexión**

Para verificar la conexión entra las dos redes, se observa las ip de cada uno de los nodos, además el ID de la celda a la cual estan conectadas verificando que son iguales como se ve en la figura 67 y 68, y por último se realiza un ping para verificar la conexión entre los dos nodos, este procedimiento se observa en la figura 70.

Figura 67
Configuración del nodo 1

```

pi@raspberrypi:~$ iwconfig
lo        no wireless extensions.

eth0     no wireless extensions.

wlan0    IEEE 802.11  ESSID:"RED"
          Mode:Ad-Hoc  Frequency:2.462 GHz  Cell: D2:71:EA:67:8D:AF
          TX-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

bat0     no wireless extensions.

pi@raspberrypi:~$ ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
          inet 192.168.50.1  netmask 255.255.255.0  broadcast 192.168.50.255
          inet6 fe80::e001:d2bf:ca29:bd8c  prefixlen 64  scopeid 0x20<link>
          ether 4c:77:cb:1f:93:a2  txqueuelen 1000  (Ethernet)
          RX packets 368977  bytes 161425712 (153.9 MiB)
          RX errors 0  dropped 0  overruns 0  frame 0
          TX packets 813002  bytes 698788928 (666.4 MiB)
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

```

Figura 68
Configuración del nodo 3

```

pi3@raspberrypi:~$ iwconfig wlan0
wlan0 IEEE 802.11 ESSID:"RED"
Mode:Ad-Hoc Frequency:2.462 GHz Cell: D2:71:EA:67:8D:AF
TX-Power=22 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on

pi3@raspberrypi:~$ ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.50.3 netmask 255.255.255.0 broadcast 192.168.5
inet6 fe80::17c4:4b75:107a:e82e prefixlen 64 scopeid 0x20<1
ether 48:68:4a:ea:27:fc txqueuelen 1000 (Ethernet)
RX packets 813654 bytes 682675794 (651.0 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 371801 bytes 169020273 (161.1 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura 69
Ping del nodo 1 al nodo 3

```

pi@raspberrypi:~$ ping 192.168.50.3
PING 192.168.50.3 (192.168.50.3) 56(84) bytes of data.
64 bytes from 192.168.50.3: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.50.3: icmp_seq=2 ttl=64 time=0.920 ms
64 bytes from 192.168.50.3: icmp_seq=3 ttl=64 time=1.40 ms
64 bytes from 192.168.50.3: icmp_seq=4 ttl=64 time=0.693 ms
^C
--- 192.168.50.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.693/1.017/1.400/0.256 ms

```

- **Ancho de banda**

Para medir los siguientes valores hay que tomar en cuenta la conexión que tienen los nodos, con un ancho de canal máximo de 20 MHz como se indica en la figura 70.

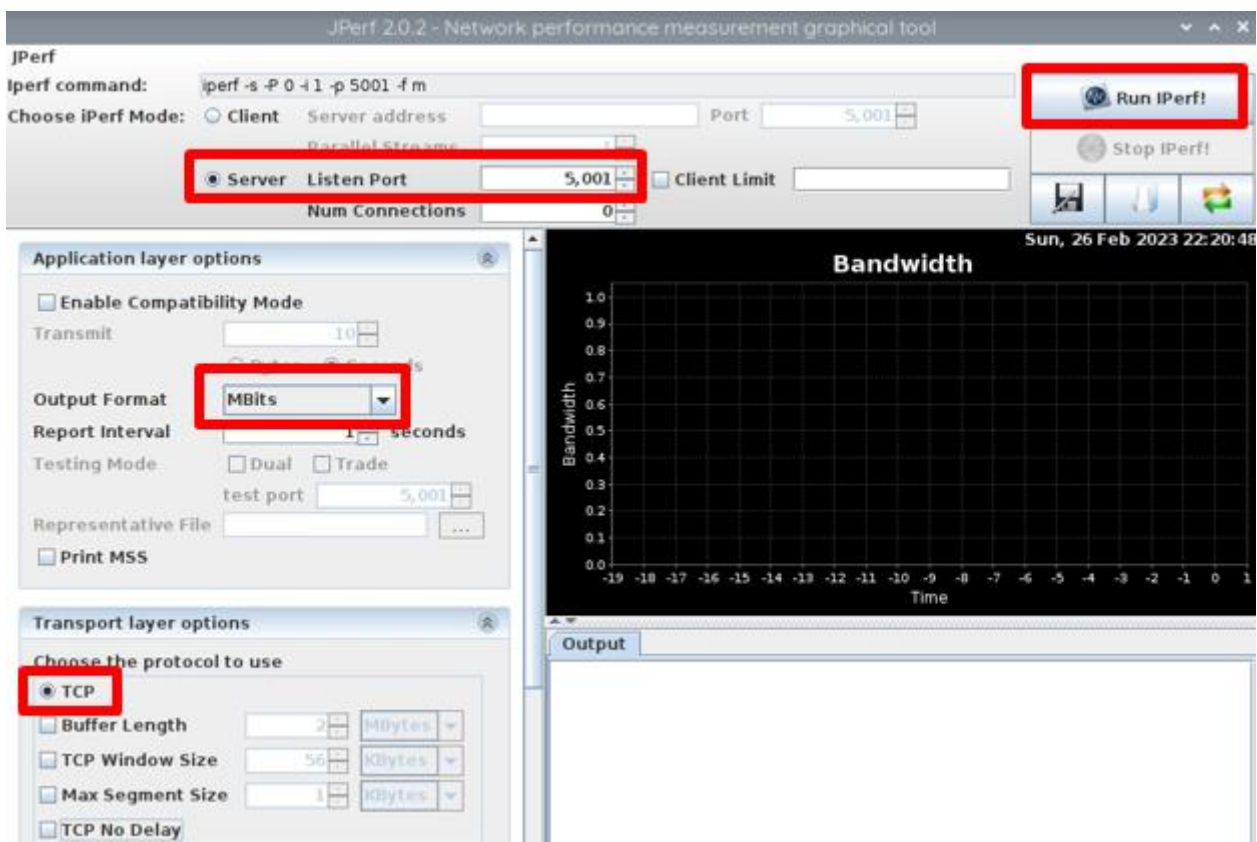
Figura 70
Información de la interfaz wlan0

```
ACpi3@raspberrypi:~$ iw dev wlan0 info
Interface wlan0
  ifindex 3
  wdev 0x1
  addr 48:68:4a:ea:27:fc
  ssid RED
  type IBSS
  wiphy 0
  channel 11 (2462 MHz) width: 20 MHz (no HT), center1: 2462 MHz
  txpower 22.00 dbm
  multicast TXQ:
    qsz-byt qsz-pkt flows drops marks overlmt hashcol tx-bytes
    0 0 46876 0 0 0 0 4759062
```

Para verificar el ancho de banda se utiliza la herramienta iperf, en donde se configura el nodo 1 como servidor, y el nodo 3 como cliente.

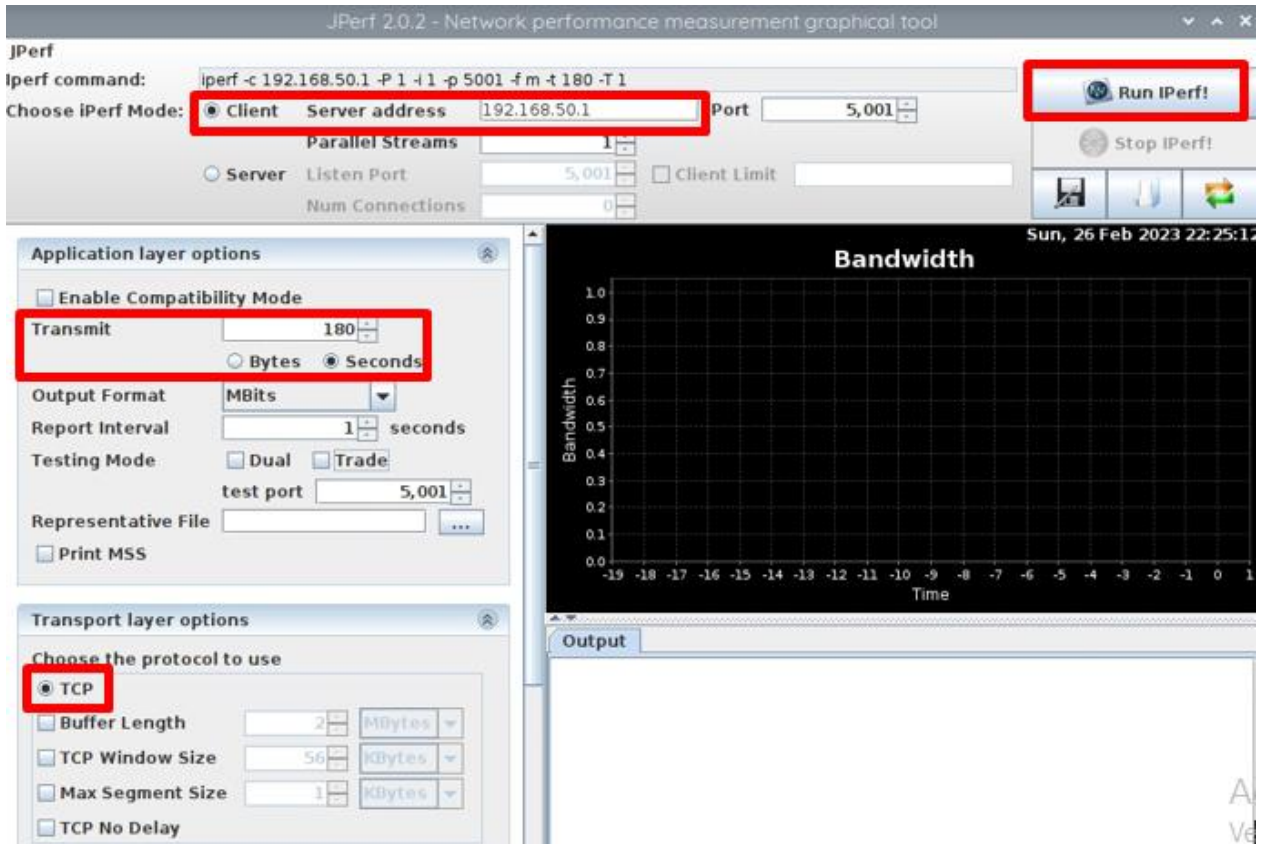
Para el servidor se configura con los siguientes parámetros como se indica en la figura 71.

Figura 71
Configuración del servidor con iperf



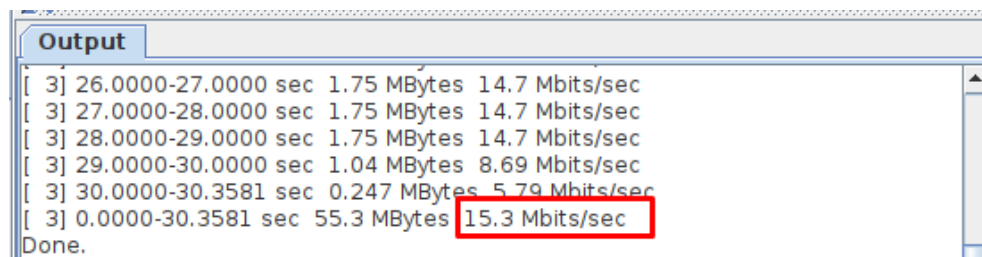
Y para el cliente se configura como se indica en la figura 72, se establece la ip del servidor, el tiempo de transmisión, en este caso 180 segundos, y se especifica el protocolo TCP.

Figura 72
Configuración del cliente con iperf



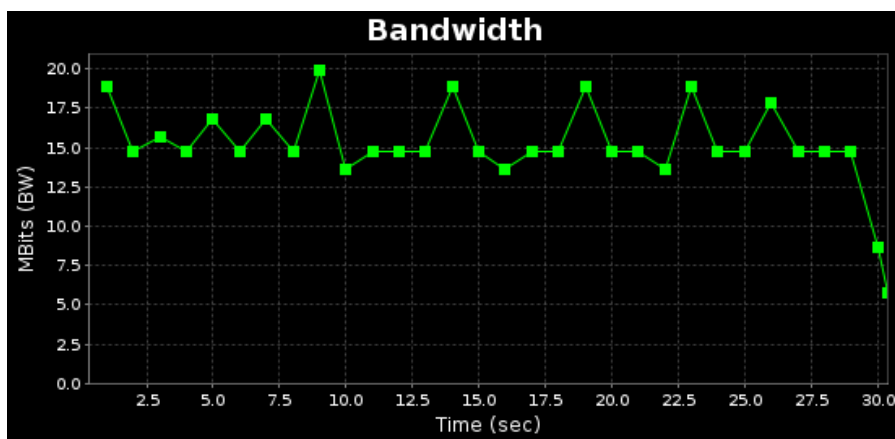
Con la configuración de los nodos en modo ad-hoc, se tiene los siguientes valores de ancho de banda. Hay que tomar en cuenta que la herramienta envía paquetes de diferentes tamaños a cierto ancho de banda, y para determinar este valor se lo obtiene con la media de los valores obtenidos. En la figura 73 se puede observar el total de paquetes transferidos y el ancho de banda total utilizado.

Figura 73
Informe de ancho de banda



Y, en la figura 74 se observa como varia el ancho de banda en todo el tiempo de transmisión, teniendo un promedio de ancho de banda de 15.3 mbps.

Figura 74
Gráfico de ancho de banda

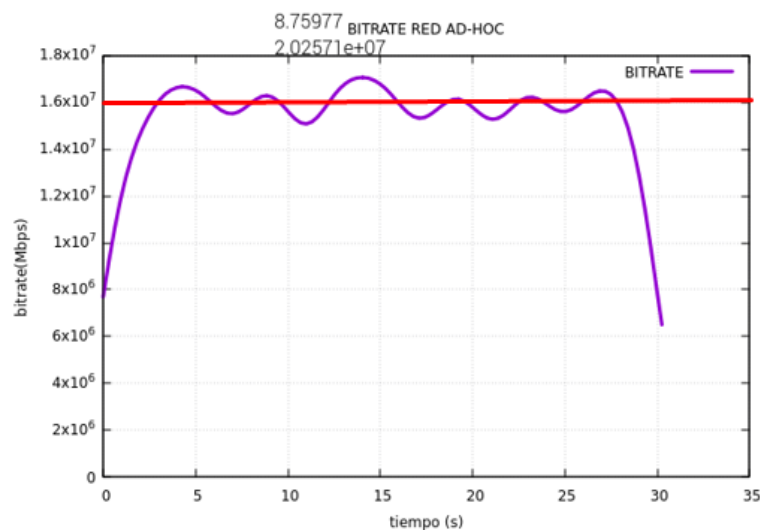


Para los siguientes parámetros se utiliza el software D-ITG, en el cual se envía tráfico por 30 segundos, de un nodo a otro, este tráfico corresponde a 2000 paquetes por segundo con un tamaño de 2500 bytes, mediante el protocolo UDP.

- **Bitrate**

El primer parámetro para analizar es el bitrate, entendiendo como la velocidad de transferencia de datos en un sistema. Una vez realizado el proceso de inyección de tráfico se obtiene los siguientes resultados que se indican en la figura 75.

Figura 75
Bitrate modo ad-hoc sin interferencia

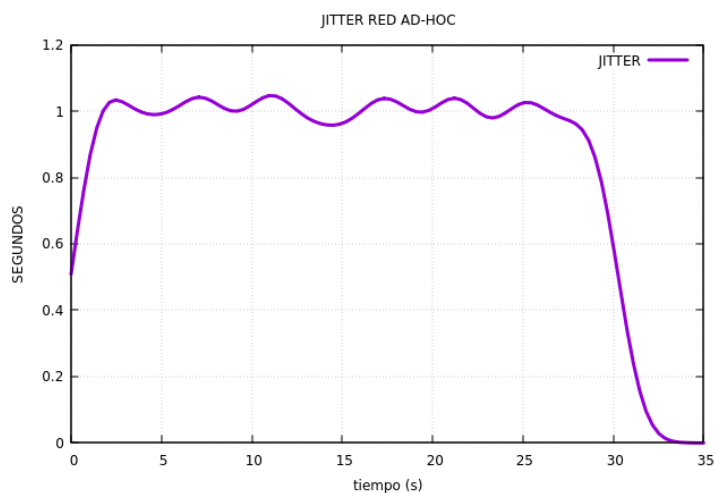


Se puede observar que en todo el tiempo de inyección de tráfico el promedio de la velocidad de transferencia esta aproximadamente en los 16 Mbps.

- **Jitter**

A continuación, se analiza el jitter de la transmisión, entendiendo el jitter como la fluctuación en el retardo en una transmisión los resultados se observan en la figura 76.

Figura 76
Jitter en modo ad-hoc sin interferencia

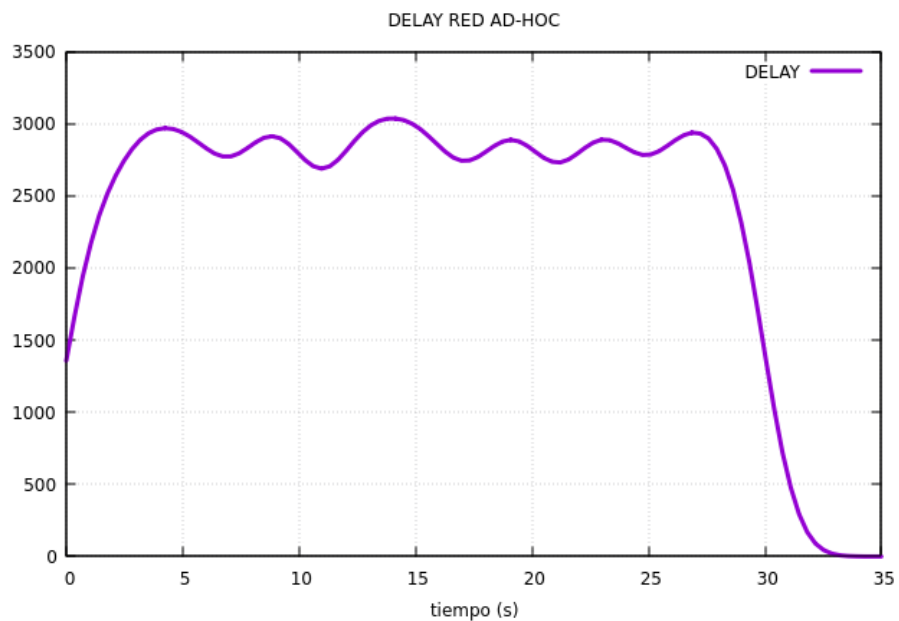


Se observa que el jitter está en una media de 0,001 segundos, concluyendo que el jitter es bajo en esta transmisión.

- **Delay**

El delay es el retardo total de la transmisión, es el tiempo que se demora un bit en ser transmitido de un nodo a otro.

Figura 77
Delay en modo ad-hoc son interferencia

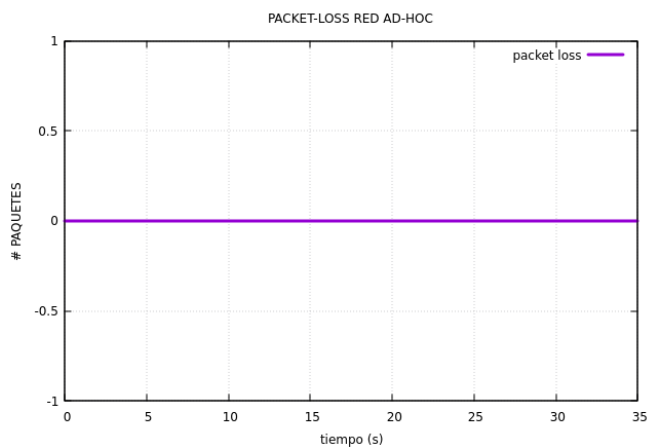


En la figura 77 se observa que el delay varía entre 2,5 y 3 segundos, siendo un tiempo bastante bueno para la transmisión.

- **Packet Loss**

Como se observa en la figura 78, no existió perdidas de paquetes en esta transmisión.

Figura 78
Paquetes perdidos en modo ad-hoc



En la tabla 20 se observa todos los valores de la prueba realizada.

Tabla 20
Resultados en modo ad-hoc

Resultados	
Total de paquetes	23922
Delay mínimo	3.710775 s
Delay máximo	4.030196 s
Promedio delay	3.754750 s
Promedio de jitter	0.001334 s
Promedio de bitrate	15817.187117 Kbit/s
Paquetes perdidos	0

4.5.2. Ad-hoc con interferencia

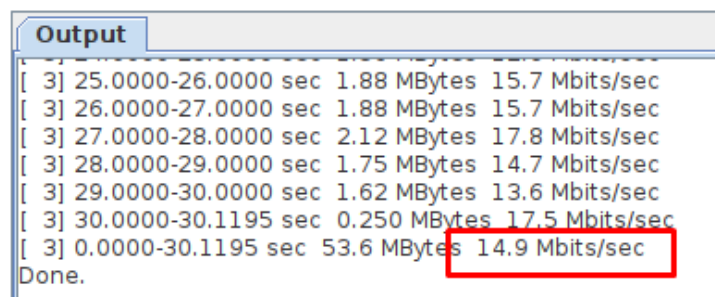
Bajo los mismos parámetros que el anterior a diferencia que la comunicación entre ellas no tiene línea de vista directa, ya existe obstáculos que interfieren en la comunicación.

- **Ancho de banda**

Después de enviar un flujo de datos por 30 segundos, se obtiene que el ancho de banda es de 14.9 Mbps, como se ve en la figura 79.

Figura 79

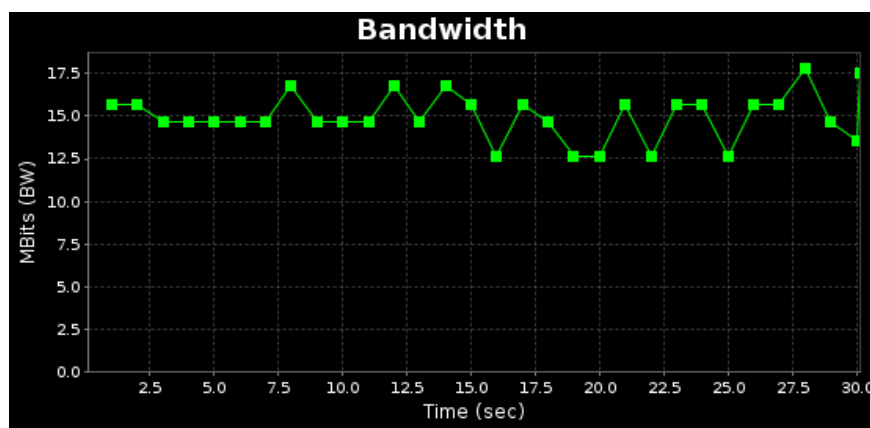
Ancho de banda modo ad-hoc con interferencia



Además, en la figura 80 se puede ver como varía este ancho de banda en el tiempo.

Figura 80

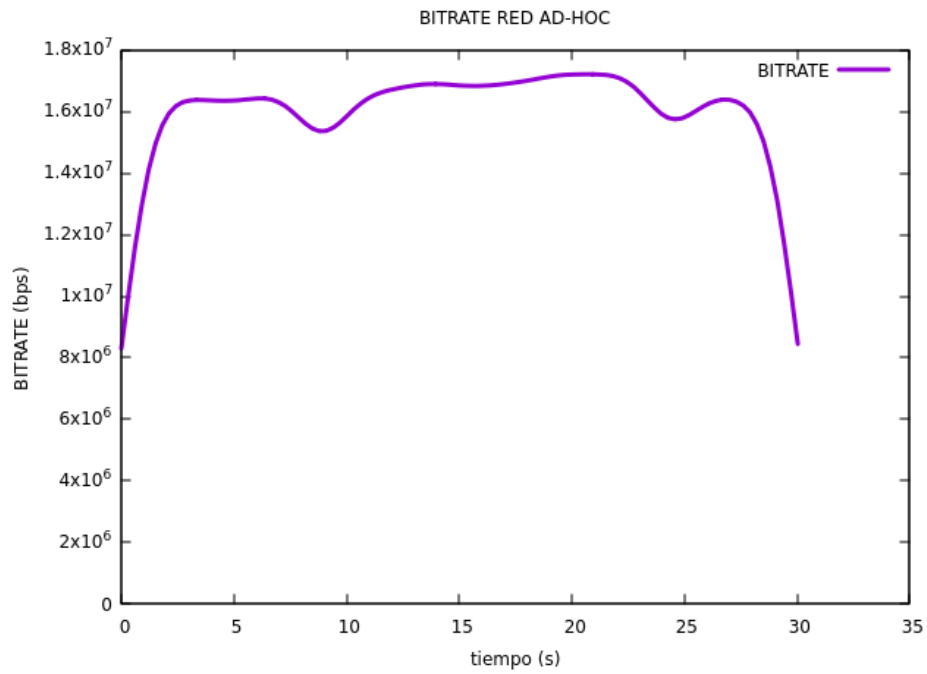
Variaciones del ancho de banda



- **Bitrate**

El bitrate para esta transmisión de la red en modo ad-hoc con interferencia es el siguiente que se muestra en la gráfica de la figura 81, se puede observar que hay punto en donde el bitrate es inestable, esto debido a las interferencias y obstáculos que existen.

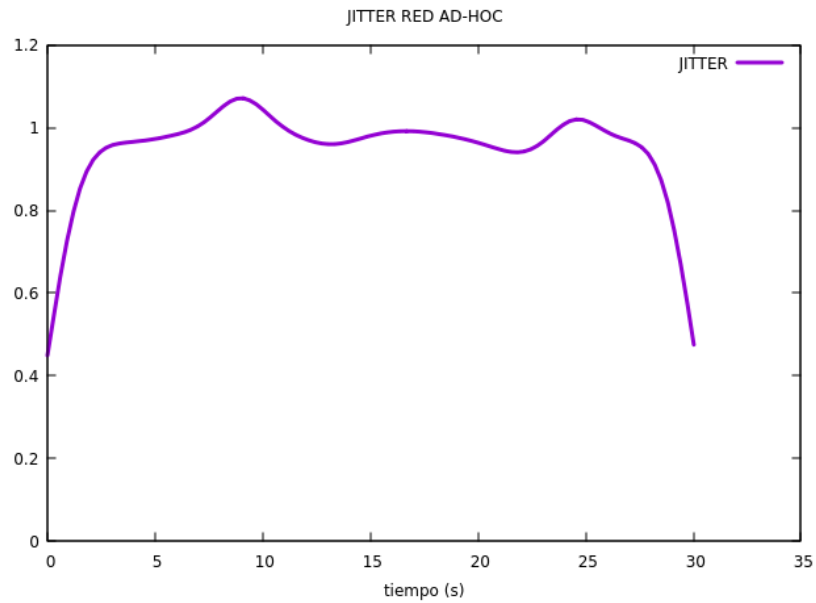
Figura 81
Bitrate en un entorno con interferencia



- **Jitter**

El jitter en esta transmisión aumento e inclusive es más inestable, se puede observar que los valores aumentaron en comparación a un ambiente sin obstáculos.

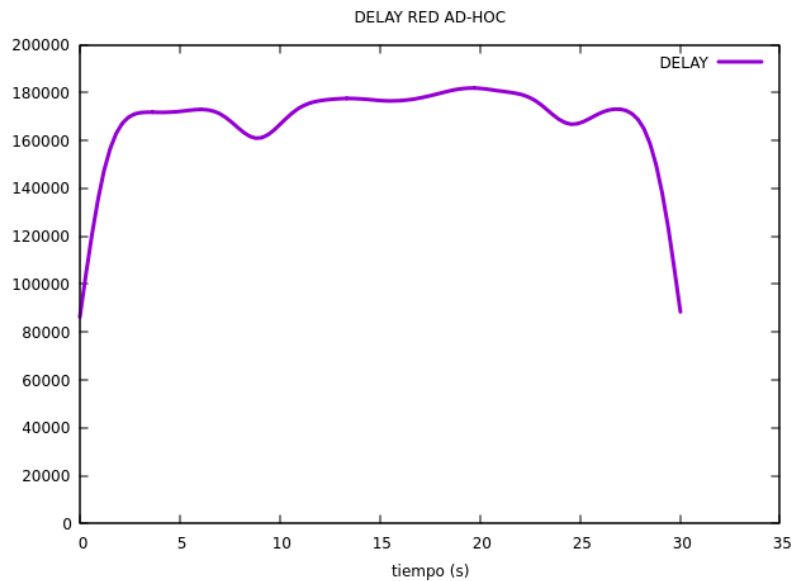
Figura 82
Jitter en modo ad-hoc con interferencia



- **Delay**

De la misma manera se tiene un delay mayor, los tiempos de retardo son mayores, estas variaciones se pueden ver en la figura 83.

Figura 83
Delay en modo ad-hoc con interferencia



Los valores de la prueba realizada se pueden observar en la tabla 21.

Tabla 21

Resultados modo ad-hoc con interferencia

Resultados	
Total de paquetes	24824
Delay mínimo	222.508509 s
Delay máximo	222.663816 s
Promedio delay	222.548747 s
Promedio de jitter	0.001245 s
Promedio de bitrate	16533.546001 Kbit/s
Paquetes perdidos	0

4.5.3. Infraestructura sin interferencia

Para las pruebas en este modo se utiliza las condiciones que se muestran en la tabla 22.

Tabla 22

Condiciones para la red

Condición	Valor
Banda de operación	5 Ghz
Ancho de canal	160 MHz
Flujos espaciales	2
Canal	36
Número de nodos	2
Distancia	5 metros.

- **Conectividad**

Se verifica la conectividad observando que los dos nodos están conectados al mismo AP, además que está trabajando en modo infraestructura.

Figura 84

Conexión en modo infraestructura

```
wlan0 IEEE 802.11 ESSID:"WLAN_5G"
Mode:Managed Frequency:5.18 GHz Access Point: 60:AA:EF:F8:21:C4
Bit Rate=245 Mb/s Tx-Power=22 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:on
Link Quality=70/70 Signal level=-37 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:10 Missed beacon:0
```

También se realiza un ping tanto al AP como al nodo, verificando la comunicación como se indica en la figura 85.

Figura 85

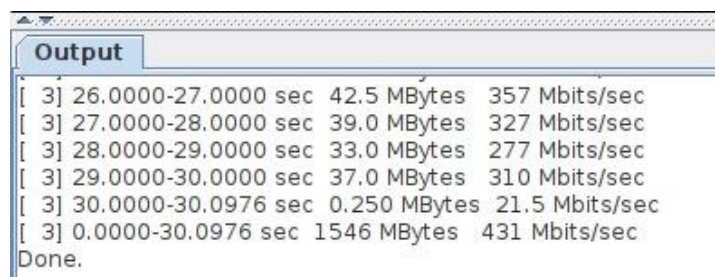
Verificación de la comunicación

```
pi3@raspberrypi:~$ ping 192.168.101.1
PING 192.168.101.1 (192.168.101.1) 56(84) bytes of data.
64 bytes from 192.168.101.1: icmp_seq=1 ttl=64 time=5.49 ms
64 bytes from 192.168.101.1: icmp_seq=2 ttl=64 time=2.93 ms
64 bytes from 192.168.101.1: icmp_seq=3 ttl=64 time=3.45 ms
^C
--- 192.168.101.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.932/3.957/5.487/1.102 ms
pi3@raspberrypi:~$ ping 192.168.101.11
PING 192.168.101.11 (192.168.101.11) 56(84) bytes of data.
64 bytes from 192.168.101.11: icmp_seq=1 ttl=64 time=316 ms
64 bytes from 192.168.101.11: icmp_seq=2 ttl=64 time=237 ms
64 bytes from 192.168.101.11: icmp_seq=3 ttl=64 time=83.0 ms
64 bytes from 192.168.101.11: icmp_seq=4 ttl=64 time=286 ms
^C
--- 192.168.101.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 82.961/230.536/316.215/89.789 ms
```

- **Ancho de banda**

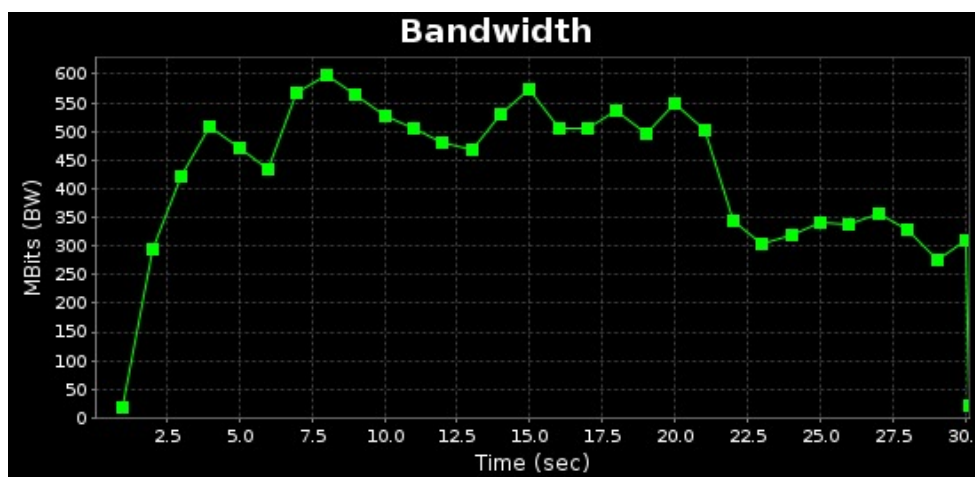
Para medir el ancho de banda en la red, se utiliza la herramienta jperf, permitiendo así enviar tráfico y poder determinar los valores que utiliza para enviar los paquetes. Se puede observar en la figura 86 que la media es de 431 Mbps, superando por mucho a la conexión ad-hoc.

Figura 86
Ancho de banda modo infraestructura



También en la siguiente figura se puede observar cómo varía el ancho de banda durante la comunicación teniendo valores muy cambiantes.

Figura 87
Variación del ancho de banda



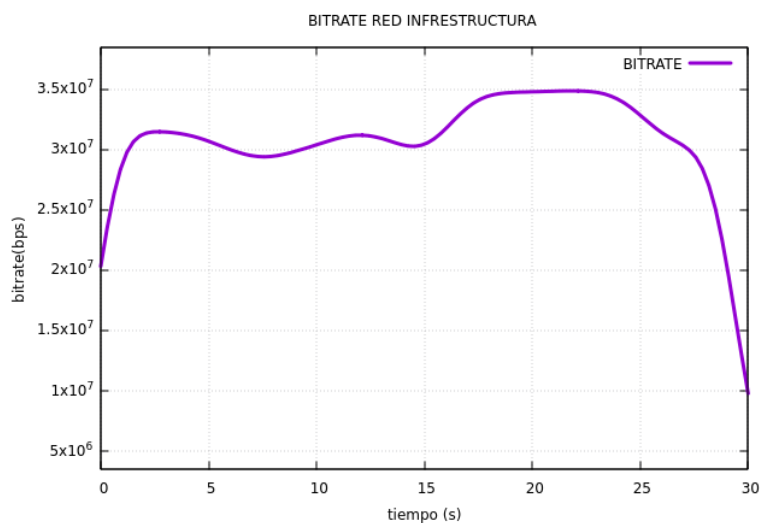
Para las siguientes pruebas se utilizó la herramienta DITG, configurada para un envío de 2000 paquetes por segundo, con un tamaño de 2500 bytes/s. Obtenido los resultados que se indican a continuación.

- **Bitrate**

En este modo de operación se tiene un promedio de 32,35 Mbps de bitrate, notándose un aumento del doble en comparación a los valores obtenidos en el anterior modo, ya que aumento el ancho del canal para las comunicaciones, además de existir menos interferencia al trabajar en la banda de 5GHz. Estos valores de bitrate se puede observar en la figura 88.

Figura 88

Bitrate en modo infraestructura sin interferencia

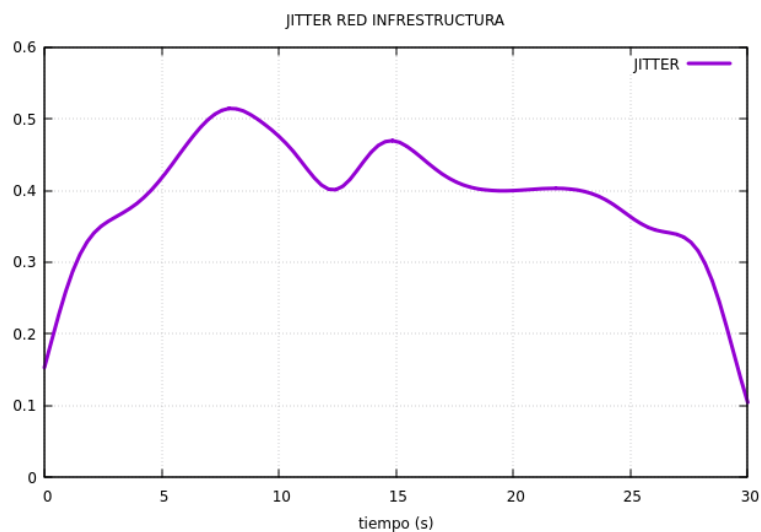


- **Jitter**

En cuanto a las variaciones de los retardos existe valores menores al anterior con una media de 0,7 ms., verificando que en la banda de 5Ghz existe una transferencia más efectiva.

Estas variaciones se observan en la siguiente figura 89.

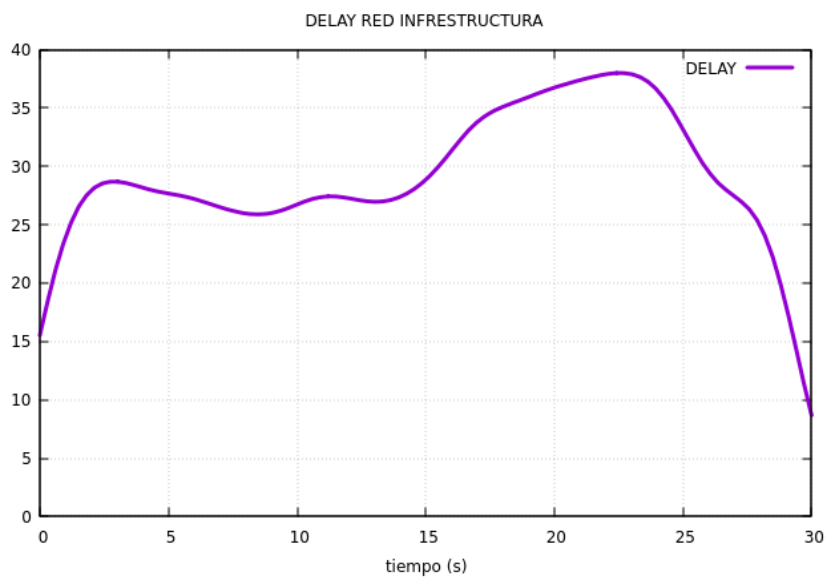
Figura 89
Jitter en modo infraestructura sin interferencia



- **Delay**

En la transmisión, los retardos totales se reducen debido a la comunicación que existe con el AP, además de la banda en la que está operando, permite que los envíos sean mucho más rápidos.

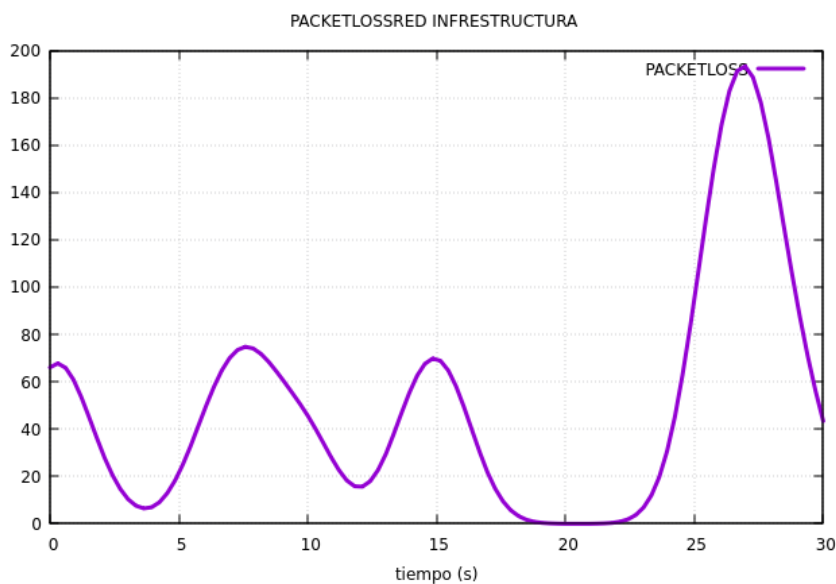
Figura 90
Delay en modo infraestructura sin interferencia



- **Packet Loss**

En esta transmisión al tener saltos para poder comunicarse entre los nodos, ya existe pérdida de paquetes, de un total de 47579 paquetes enviados se han perdido solo un 3,3%. Se puede observar en la figura 91 los momentos en los que se han perdido cantidad significativa de paquetes, hay que tomar en cuenta que no tienen retransmisión por haber utilizado el protocolo UDP.

Figura 91
Pérdida de paquetes



Los resultados de esta prueba se observan en la tabla 23.

Tabla 23
Resultados de la red en modo infraestructura sin interferencia

Resultados	
Total de paquetes	47579
Delay mínimo	0.047428 s
Delay máximo	0.550956 s

Promedio delay	0.058843 s
Promedio de jitter	0.000714 s
Promedio de bitrate	32351.601164 Kbit/s
Paquetes perdidos	1625 (3.30 %)

4.5.4. Infraestructura con interferencia

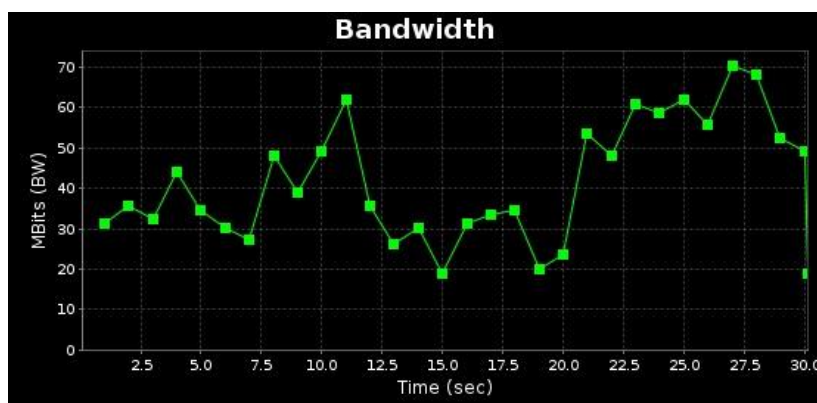
Para las pruebas en este escenario se toma en cuenta las mismas condiciones de la tabla 22.

- **Ancho de banda**

Se realiza la prueba utilizando jperf, se observa que la media del ancho de banda es de 42.2 Mbps, notándose una caída en comparación a un ambiente sin obstáculos, también considerando que se trabaja a 5GHz teniendo esta banda una menor cobertura. Se puede observar en la figura 92 como estos valores verían en el transcurso de la transmisión.

Figura 92

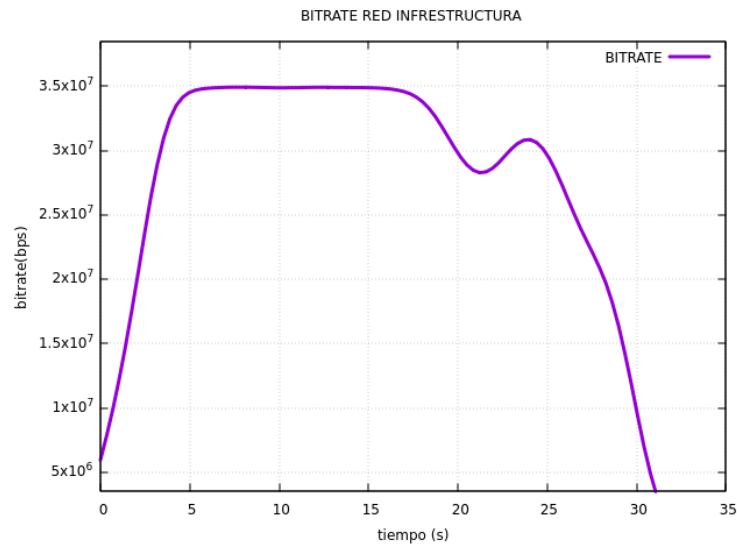
Ancho de banda en infraestructura con interferencia



- **Bitrate**

Utilizando la herramienta DITG, se realizó la inyección de tráfico obteniendo un promedio de bitrate de 29,8 Mbps, en la figura 93 se observa como varia estos valores en el transcurso de la transmisión.

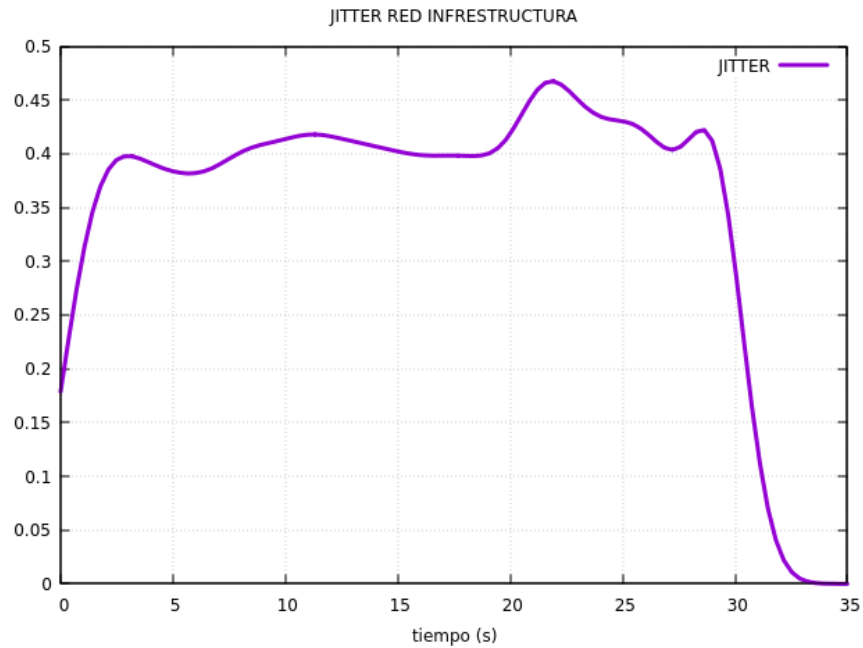
Figura 93
Bitrate en infraestructura con interferencia



- **Jitter**

En la variación del retardo se observa que hay un pequeño aumento en comparación al anterior, en la figura 94 se observa estas variaciones, tendiendo un promedio de 0,95ms.

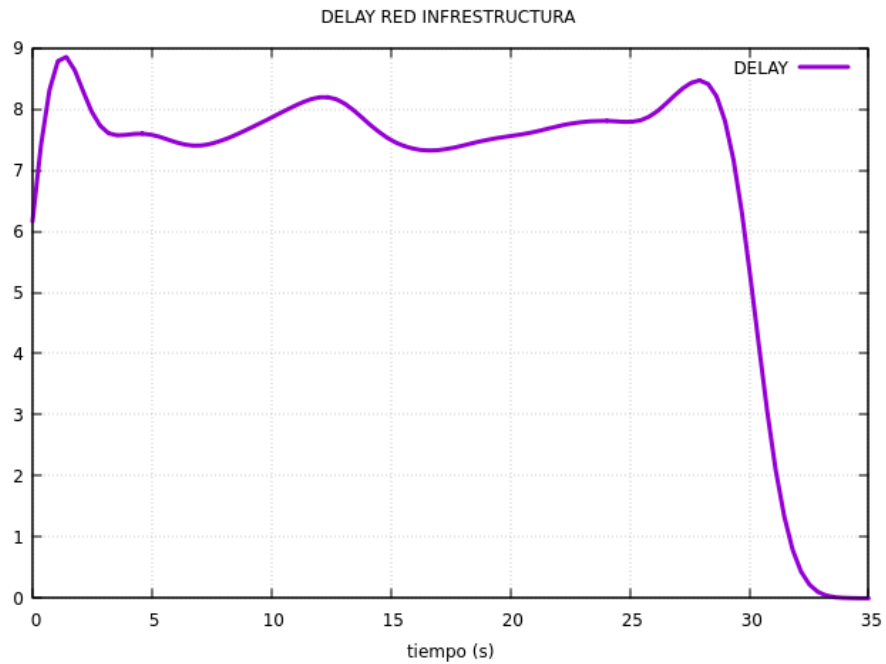
Figura 94
Jitter en infraestructura con interferencia



- **Delay**

El delay en este escenario aumento en comparación al anterior, esto debido a los obstáculos en la comunicación, pero es menor que una red ad-hoc., se puede ver en la figura 95 como varia el delay en la transmisión, pero siendo un delay bajo que no imposibilita la comunicación.

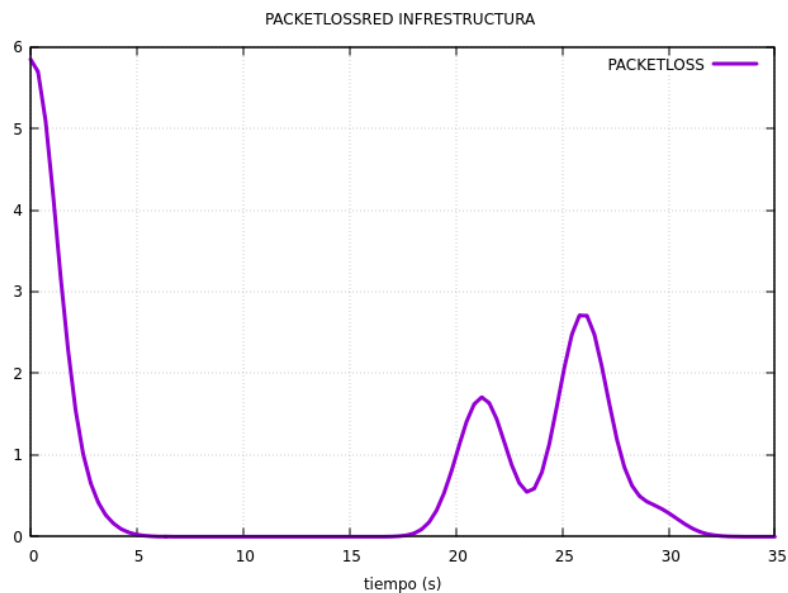
Figura 95
Delay en infraestructura con interferencia



- **Packet Loss**

En comparación al anterior existió una pérdida mucho menor de paquetes, estos paquetes no se vieron afectado por los obstáculos en la transmisión, esto es visible en la gráfica de la figura 96.

Figura 96
Pérdida de paquetes en infraestructura con interferencia



Todos los resultados obtenidos en esta prueba se pueden observar en la tabla 24.

Tabla 24
Resultados de la red en modo infraestructura con interferencia

Resultados	
Total de paquetes	44905
Delay mínimo	0.010061 s
Delay máximo	0.642940 s
Promedio delay	0.026408 s
Promedio de jitter	0.000950 s
Promedio de bitrate	29891.403111 Kbit/s
Paquetes perdidos	28 (0.06 %)

4.5.5. Mesh sin interferencia

Para las pruebas en este escenario se toma en cuenta las condiciones de la tabla 25.

Tabla 25
Condiciones para red Mesh

Condición	Valor
Banda de operación	5 Ghz
Ancho de canal	80 MHz
Flujos espaciales	2
Canal	36
Número de nodos	3
Distancia	5 metros.

Una vez los nodos estén configurados y en funcionamiento se realiza las siguientes pruebas.

- **Ancho de banda**

Para determinar el ancho de banda se utiliza la herramienta jperf, obtenido como media de ancho de banda un total de 42,2 Mbps, se puede observar en la figura 97 que durante la transmisión el ancho de banda no varía tanto como en los anteriores escenarios.

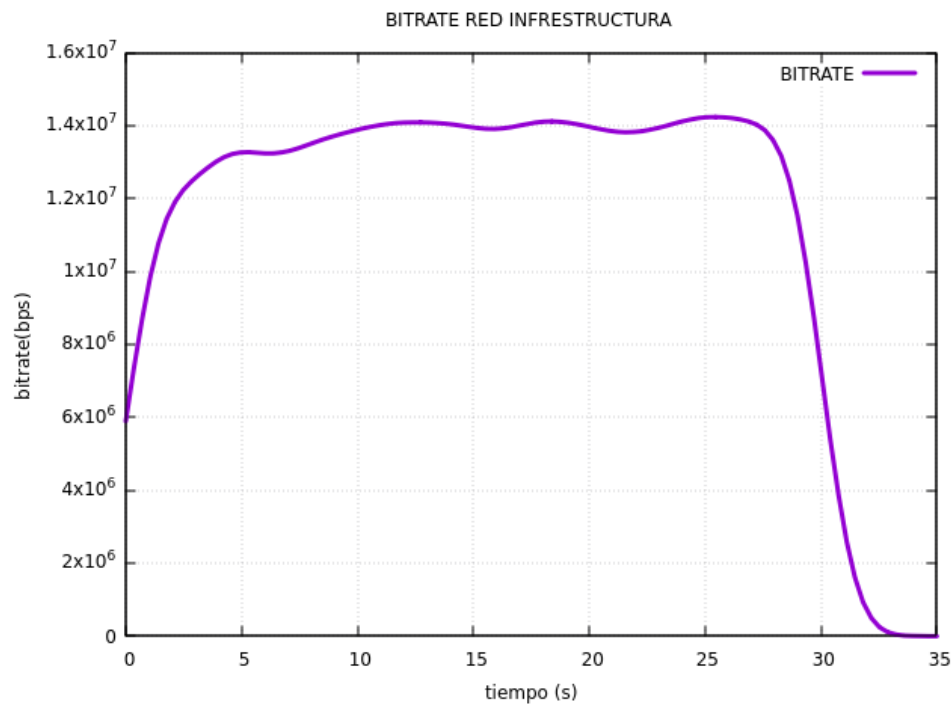
Figura 97
Variación del ancho de banda



- **Bitrate**

Para el bitrate se utiliza la herramienta DITG, con esta herramienta se inyecta tráfico entre los dos nodos, obteniendo un promedio de 13.68 Mbps, se observa en la figura 98 que este bitrate es más constante, tiene menos deficiencia.

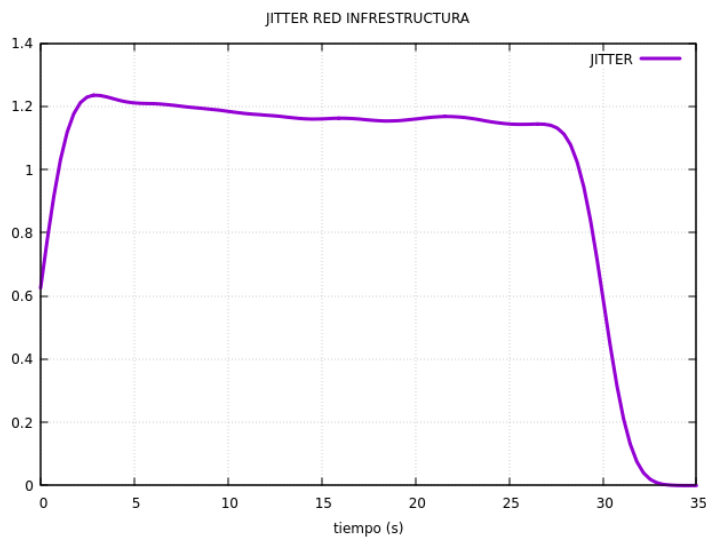
Figura 98
Bitrate en red mesh sin interferencia



- **Jitter**

En esta prueba se obtiene una media de 1,7 ms, en donde se puede observar que estos valores son constantes durante la transmisión, en la figura 99 se observa que no hay muchas fluctuaciones en el jitter.

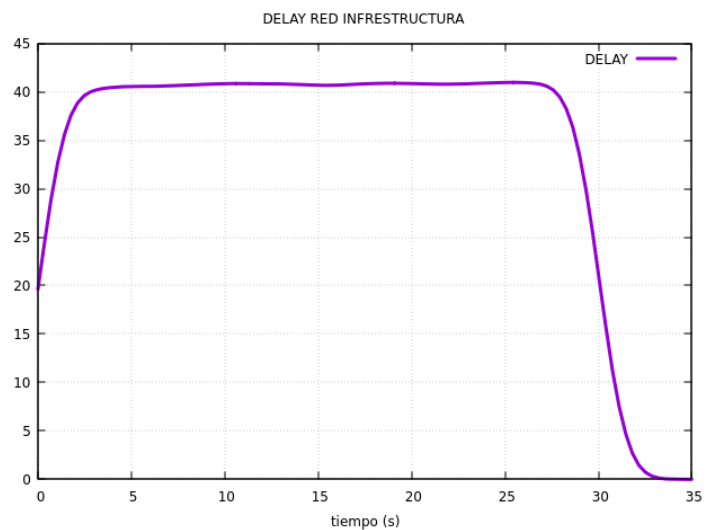
Figura 99
Jitter en una red mesh sin interferencia



- **Delay**

En cuanto al retardo en la transmisión o delay se observa en la figura 100 que es muy constante, el valor no sufre cambios significantes durante la transmisión.

Figura 100
Delay en una red mesh sin interferencia



Los resultados obtenidos en este escenario se los puede apreciar en la tabla 26.

Tabla 26
Resultados de la red mesh sin interferencia

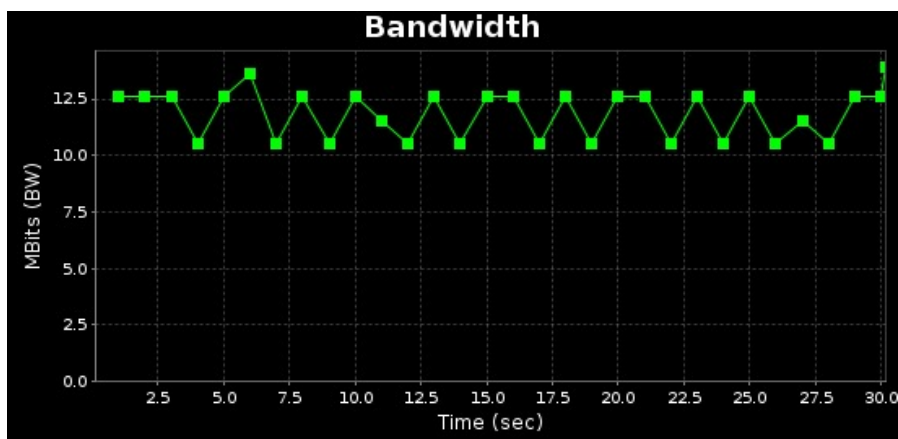
Resultados	
Total de paquetes	20561
Delay mínimo	0.008696 s
Delay máximo	0.110245 s
Promedio delay	0.059643 s
Promedio de jitter	0.001728 s
Promedio de bitrate	13680.354762 Kbit/s
Paquetes perdidos	0

4.5.6. Mesh con interferencia

- Ancho de banda

El ancho de banda a diferencia del anterior disminuyo debido a los obstáculos que existen entre los nodos, pero en la figura 101 se observa que la variación que existió en la transmisión es mínima.

Figura 101
Ancho de banda en red mesh con interferencia

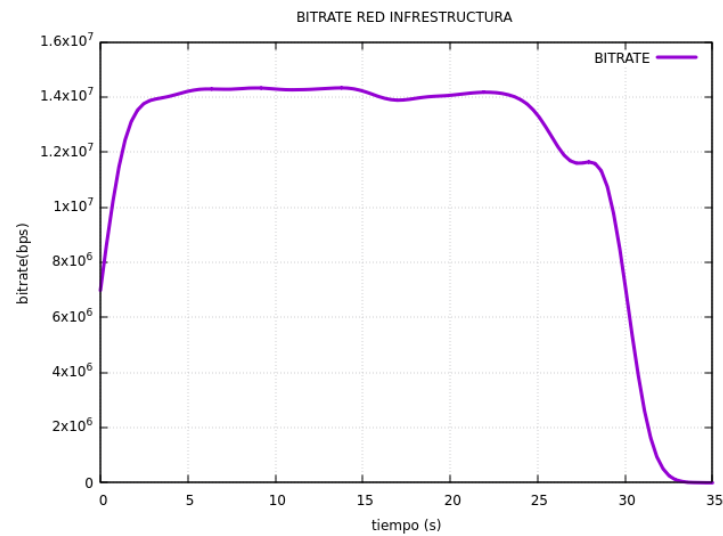


- **Bitrate**

El bitrate en este escenario tiene un promedio de 13,87 Mbps, este valor no varía mucho en comparación con el anterior escenario, además de que durante la transmisión el valor no varía mucho como se aprecia en la figura 102.

Figura 102

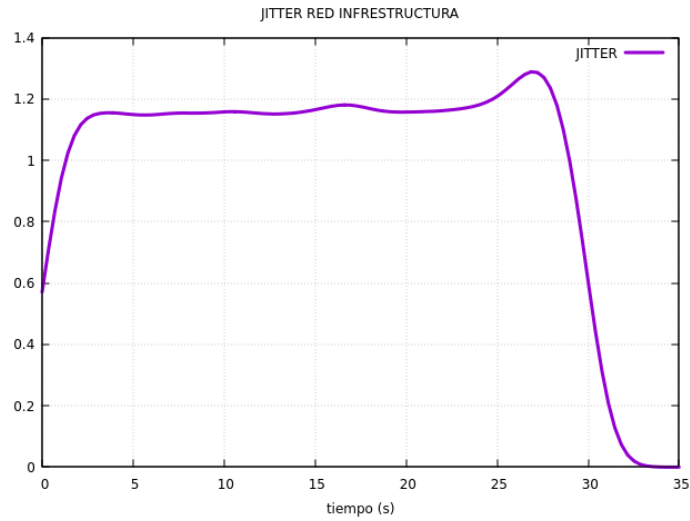
Bitrate en red mesh con interferencia



- **Jitter**

El valor promedio del jitter es de 1,6 ms, este valor es muy bajo con lo cual no afecta las transmisiones, además se observa en la figura 103 que los valores no fluctúan mucho durante el tiempo de transmisión.

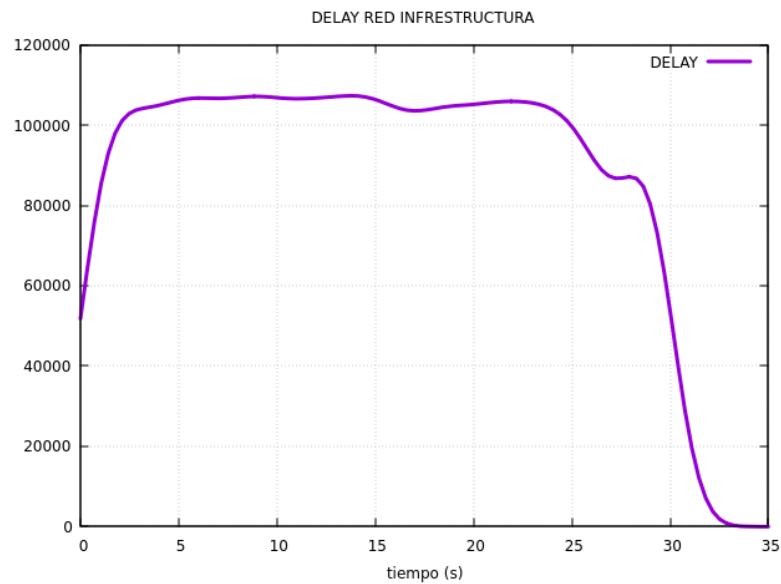
Figura 103
Jitter en red mesh con interferencia



- **Delay**

Los valores de delay en este escenario tienen un promedio de 149 ms, esto se debe a que existe obstáculos que no permiten que la transmisión sea fluida. Esto se observa en la figura 104.

Figura 104
Delay en red mesh con interferencia



Los resultados de esta prueba se pueden observar en la tabla 27.

Tabla 27
Resultados de la red mesh con interferencia

Resultados	
Total de paquetes	20847
Delay mínimo	149.814679 s
Delay máximo	149.980325 s
Promedio delay	149.862529 s
Promedio de jitter	0.001696 s
Promedio de bitrate	13871.930943 Kbit/s
Paquetes perdidos	0

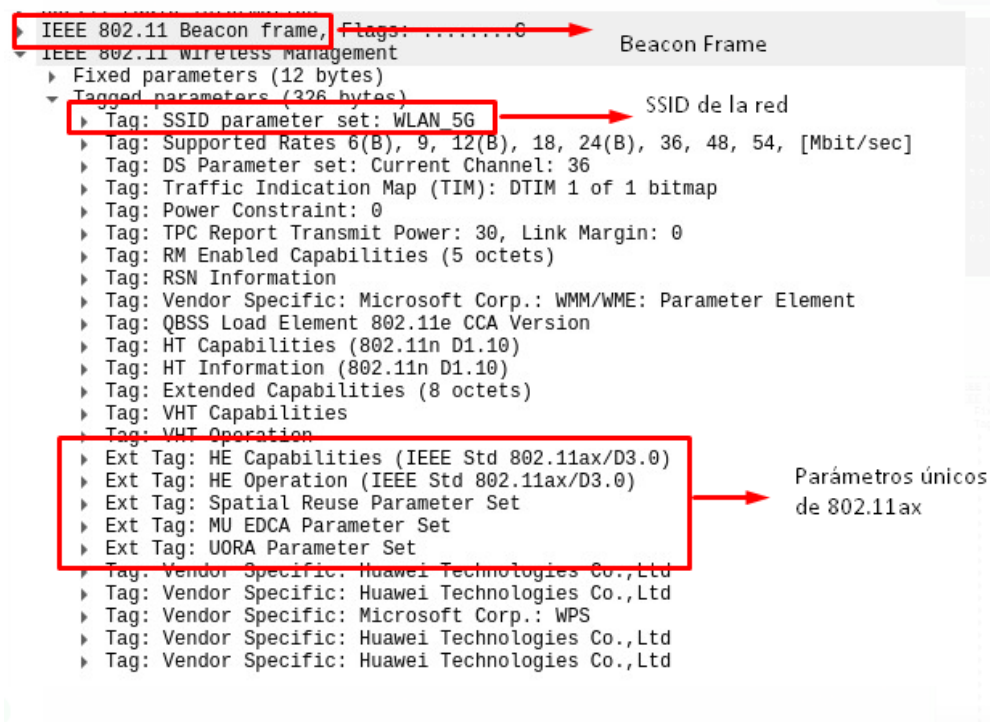
4.5.7. Captura de paquetes

- **Análisis de tramas 802.11ax**

Para el análisis de las tramas 802.11ax se utiliza la herramienta wireshark. Se analizará en el canal 36 que es en el que opera el AP.

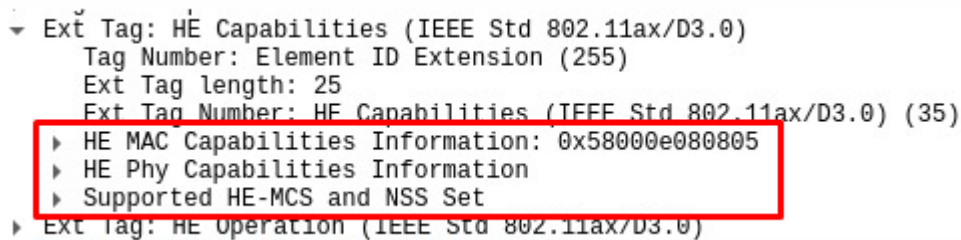
Primero se analiza los beacons enviados por la AP, estos contienen información necesaria para que una estación pueda conectarse, como son el SSID entre otros. En esta trama los campos que demuestran que opera bajo el protocolo 802.11ax son las que se muestran en la figura 105.

Figura 105
Beacon frame



Cada uno de estos campos contienen información propia de la tecnología, en la figura 106 se puede ver el campo HE Capabilities, el cual cuenta con tres subcampos, la HE MAC y la HE Phy y Supported HE-MCS and NSS Set.

Figura 106
HE Capabilities



El campo HE MAC Capabilities tienen varios campos que se indicada en la figura 107, estos campos determinan si el AP y las estaciones tienen ciertas características, como por ejemplo TWT, OFDMA, UL RU entre las más importantes.

Figura 107
HE MAC Capabilities

```

HE MAC Capabilities Information: 0x58000e080805
.....1 = +HTC HE Support: Supported
.....0. = TWT Requester Support: Not supported
.....1.. = TWT Responder Support: Supported
.....0 0... = Fragmentation Support: No support for dynamic frag
.....000. .... = Reserved: 0x0
.....000. .... = Reserved: 0x0
.....10.. .... = Trigger Frame MAC Padding Duration: 2
.....0000 .... = Multi-TID Aggregation Support: 0
.....0 0... = HE Link Adaptation Support: No feedback if the STA
.....0. .... = All Ack Support: Not supported
.....0.. .... = TRS Support: Not supported
.....1. .... = BSR Support: Supported
.....0. .... = Broadcast TWT Support: Not supported
.....0. .... = 32-bit BA Bitmap Support: Not supported
.....0. .... = MU Cascading Support: Not supported
.....0. .... = Ack-Enabled Aggregation Support: Not supported
.....0. .... = Reserved: 0x0
.....1. .... = OM Control Support: Supported
.....1. .... = OFDMA RA Support: Supported
.....0 1... = Maximum A-MPDU Length Exponent Extension: 1
.....0. .... = A-MSDU Fragmentation Support: Not supported
.....0. .... = Flexible TWT Schedule Support: Not supported
.....0. .... = Rx Control Frame to MultiBSS: Not supported
.....0. .... = BSRP BQRP A-MPDU Aggregation: Not supported
.....0. .... = QTP Support: Not supported
.....0. .... = BQR Support: Not supported
.....0. .... = SRP Responder Role: Not supported
.....0. .... = NDP Feedback Report Support: Not supported
.....0. .... = OPS Support: Not supported
.....0. .... = A-MSDU in A-MPDU Support: Not supported
.....00 0... = Multi-TID Aggregation TX Support: 0
.....0. .... = HE Subchannel Selective Transmission Support: Not
.....1. .... = UL 2x996-tone RU Support: Supported
.....1. .... = OM Control UL MU Data Disable RX Support: Supporte
.....0. .... = HE Dynamic SM Power Save: Not supported
.....1. .... = Punctured Sounding Support: Supported

```

En el siguiente subcampo de la figura 108 se tiene otras características más físicas como son el ancho del canal que soportan.

Figura 108*Ancho del canal soportado*

```

  ▾ HE Phy Capabilities Information
    ▶ .... ..0 = Reserved: 0x0
    ▾ 0000 110. = Channel Width Set: 0x06
      .... ..0. = 40MHz in 2.4GHz band: Not supported
      .... .1.. = 40 & 80MHz in the 5GHz band: Supported
      .... 1... = 160MHz in the 5GHz band: Supported
      ...0 .... = 160/80+80MHz in the 5GHz band: Not supported
      ..0. .... = 242 tone RUs in the 2.4GHz band: Not supported
      .0.. .... = 242 tone RUs in the 5GHz band: Not supported
      0... .... = Reserved: 0x0
    ▶ Bits 8 to 23: 0x4e2f
    ▶ Bits 24 to 39: 0x6fc9
    ▶ Bits 40 to 55: 0x27c9
    ▶ Bits 56 to 71: 0x01de
    ▶ Bits 72 to 87: 0x008f
  
```

En el campo HE Operation hay un subcampo muy importante para esta tecnología como es el BSS Color, se puede observar cómo está configurado.

Figura 109*HE Operation - BSS Color*

```

  ▾ Supported HE MCS and NSS Set
  ▾ Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
    Tag Number: Element ID Extension (255)
    Ext Tag length: 6
    Ext Tag Number: HE Operation (IEEE Std 802.11ax/D3.0) (36)
    ▶ HE Operation Parameters: 0x003fe4
    ▶ BSS Color Information: 0x01
    ▶ Basic HE-MCS and NSS Set: 0x11fc
  
```

A continuación, se obtendrá la velocidad de datos de un marco 802.11ax, para esto se basa en las tablas de los anexos C1 y C2. Estas tablas se obtuvieron en base a las siguientes formulas:

$$Data\ Rate = \frac{N_{SD} * N_{BPSCS} * R * N_{SS}}{T_{DFT} + T_{GI}} \quad (1)$$

En donde,

N_{SD} = Número de datos de la Subportadora

N_{BPSCS} = Número de bits codificados por subportadora por flujo

R = Codificación

N_{SS} = Numero de flujos espaciales

T_{DFT} = Duración del símbolo OFDM

T_{GI} = Duración del intervalo de guarda.

La fórmula 1 se utiliza cuando se trabaja con OFDM, y los valores que pueden tomar las variables se observan en la figura 110.

Figura 110

Variables para MSC con OFDM

PHY	Modulation		R	N_{SS}	N_{SD}				T_{DFT}	T_{GI}		
	Name	N_{BPSCS}			20MHz	40MHz	80MHz	160MHz		Long	Medium	Long
802.11ax (HE)	BPSK	1	1/2	1 to 8	234	468	980	1960	12.8 μ s	0.8 μ s	1.2 μ s	3.2 μ s
	QPSK	2	1/2 & 3/4									
	16-QAM	4	1/2 & 3/4									
	64-QAM	6	1/2 & 2/3 & 3/4									
	256-QAM	8	2/3 & 5/6									
1024-QAM	10	3/4 & 5/6										

Nota: Tomado de <https://semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates/>

Ahora, cuando se trabaja con OFDMA, es similar a la fórmula 1 con la diferencia que se define la cantidad de subportadora de datos por RU y no por canal.

$$Data\ Rate = \frac{N_{SD,U} * N_{BPSCS,U} * R * N_{SS}}{T_{DFT} + T_{GI}} \quad (2)$$

en donde,

$N_{SD,U}$ = Número de datos de la Subportadora por unidades de recurso

$N_{BPSCS,U}$ = Número de bits codificados por subportadora por unidades de recurso

R = Codificación

N_{SS} = Numero de flujos espaciales

T_{DFT} = Duración del símbolo OFDM

T_{GI} = Duración del intervalo de guarda.

Para la fórmula 2 los valores que pueden tomar se definen en la figura 111.

Figura 111

Variables para MSC con OFDMA

PHY	Modulation		R	N_{ss}	N_{SD}						T_{DFT}	T_{GI}		
	Name	N_{BPSCS}			26-tone	52-tone	106-tone	242-tone	484-tone	996-tone		Long	Medium	Long
802.11ax (HE)	BPSK	1	1/2	1 to 8	24	48	102	234	468	980	12.8 μ s	0.8 μ s	1.2 μ s	3.2 μ s
	QPSK	2	1/2 & 3/4											
	16-QAM	4	1/2 & 3/4											
	64-QAM	6	1/2 & 2/3 & 3/4											
	256-QAM	8	2/3 & 5/6											
1024-QAM	10	3/4 & 5/6												

Nota: Tomado de <https://semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates/>

Y debido a la implementación de la modulación 1024-QAM, se introduce dos nuevos MSC, la 10 y 11, correspondientes a una codificación de 3/4 y 5/6.

Los parámetros que se necesitan son los siguientes para poder obtener la velocidad de datos en la transmisión.

- Número de subportadoras de datos para un canal de 160 MHz de ancho
- Número de bits codificados por subportadora (Modulación): (Si se conoce)
- Codificación: (Si se conoce)
- Número de flujos espaciales
- Duración Símbolo OFDM
- Intervalo de Guardia

Además, se debe tomar en cuenta que 802.11ax utiliza una nueva duración de símbolo que es de 12,8 μ s, diferentes intervalos de guarda que son de 0,8 μ s, 1,6 μ s y 3,2 μ s, asimismo el tamaño y cantidad de subportadoras no es el mismo.

Para capturar los paquetes que necesitamos aplicamos el siguiente filtro en wireshark.

**wlan.fc.type == 2 && (radiotap.he.data_1.ppdpu_format == 0x0 ||
radiotap.he.data_1.ppdpu_format == 0x2)**

wlan.fc.type == 2 (Filtra trama de datos 802.11)

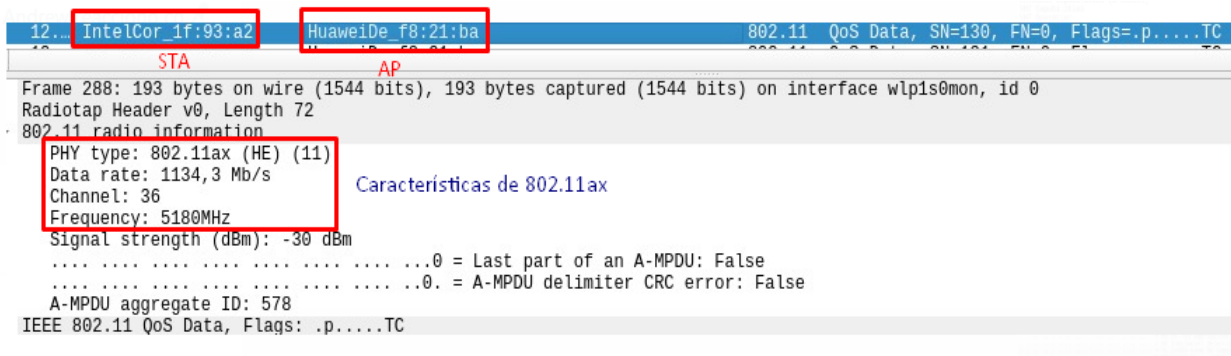
radiotap.he.data_1.ppdpu_format == 0x0 (Filtra HE PPDU de único usuario)

radiotap.he.data_1.ppdpu_format == 0x2 (Filtra HE PPDU multiusuario)

Una vez obtenidos los marcos, se selecciona uno y se verifica que se envió del nodo al AP, también se verifica la capa física si es 802.11ax, en que canal está trabajando y con que data rate, como se indica en la figura 112.

Figura 112

Información de marcos 802.11ax



Ara encontrar la información de la transmisión se debe ubicar en el campo radiotap, y buscar la siguiente información para encontrar la velocidad exacta de datos.

- Índice MCS
- Intervalo de guarda

- Ancho del canal o tamaño de la unidad de recursos
- Número de flujos espaciales

El índice MCS se encuentra en la sección "**HE Information/HE Data 3**". En esta transmisión se tiene un índice MCS de 11, mostrado por el código 0xb (b es 11 en formato hexadecimal), esto se muestra en la figura 113.

Figura 113 Índice MSC

```

Radiotap Header v0, Length 72
  Header revision: 0
  Header pad: 0
  Header length: 72
  Present flags
  Flags: 0x10
  Channel frequency: 5180 [A 36]
  Channel flags: 0x0140, Orthogonal Frequency-Division Multiplex
  Antenna signal: -26 dBm
  RX flags: 0x0000
  A-MPDU status
  timestamp information
  HE information
    HE Data 1: 0xc7fc, PPDU Format: HE_SU, BSS Color known, Bea
    HE Data 2: 0x007e, GI known, LTF symbols known, Pre-FEC Pad
    HE Data 3: 0xabc1, Coding: LDPC
      .... ..00 0001 = BSS Color: 0x01
      .... ..1.. .... = Beam Change: 0x1
      .... ..1.... .... = U/I/DI: 0x1
      .... 1011 .... = data MCS: 0xb
      .... ..0 .... .... = data DCM: 0x0
      ..1. .... .... = Coding: LDPC (0x1)
      .0.. .... .... = LDPC extra symbol segment: 0x0
      1... .... .... = STBC: 0x1
    HE Data 4: 0x0000
  
```

El intervalo de guarda GI y el ancho de canal de la RU, están en los campos "**HE Information/HE Data 5**". En este caso se tiene un GI de 1,6 μ s y un ancho de canal de 160 MHz, esta información se observa en la figura 114.

Figura 114

Intervalo de guarda y Ancho de canal

```

- Radiotap Header v0, Length 72
  Header revision: 0
  Header pad: 0
  Header length: 72
  ▶ Present flags
  ▶ Flags: 0x10
  Channel frequency: 5180 [A 36]
  ▶ Channel flags: 0x0140, Orthogonal Frequency-Division Multiplexing (OFDM),
  Antenna signal: -26 dBm
  ▶ RX flags: 0x0000
  ▶ A-MPDU status
  ▶ timestamp information
  - HE information
    ▶ HE Data 1: 0xc7fc, PPDU Format: HE_SU, BSS Color known, Beam Change kn
    ▶ HE Data 2: 0x007e, GI known, LTF symbols known, Pre-FEC Padding Factor
    ▶ HE Data 3: 0xabc1, Coding: LDPC
    ▶ HE Data 4: 0x0000
    - HE Data 5: 0x2093, data Bandwidth/RU allocation: 160/80+80, GI: 1.6us,
      .... 0011 = data Bandwidth/RU allocation: 160/80+80 (0x3)
      .... 0011 = GI: 1.6us (0x1)
      .... 10.. = LTF symbol size: 2x (0x2)
      .... 0000 = LTF symbols: 1x (0x0)
      .... 0... = reserved: 0x0
      ..10 = Pre-FEC Padding Factor: 0x2
      .0.. = TxBF: 0x0
      0... = PE Disambiguity: 0x0
    ▶ HE Data 6: 0x0e01, NSTS: 1 space-time stream
  
```

Ahora se encuentra el número de flujos espaciales que se utilizó, este se encuentra en los campos "HE Information/HE Data 6". Se observa que se utilizó un flujo espacial, esto se observa en la figura 115.

Figura 115
Número de flujos espaciales

```

Radiotap Header v0, Length 72
  Header revision: 0
  Header pad: 0
  Header length: 72
  Present flags
  Flags: 0x10
  Channel frequency: 5180 [A 36]
  Channel flags: 0x0140, Orthogonal Frequency-Division Multiplexing
  Antenna signal: -26 dBm
  RX flags: 0x0000
  A-MPDU status
  timestamp information
  HE information
    HE Data 1: 0xc7fc, PPDU Format: HE_SU, BSS Color known, Beam
    HE Data 2: 0x007e, GI known, LTF symbols known, Pre-FEC Paddi
    HE Data 3: 0xabc1, Coding: LDPC
    HE Data 4: 0x0000
    HE Data 5: 0x2093, data Bandwidth/RU allocation: 160/80+80, (
    HE Data 6: 0x0e01, NSTS: 1 space-time stream
      .... 0001 = NSTS: 1 space-time stream (0x1)
      .... 0000 = Doppler value: 0x0
      .... 0000 = Reserved: 0x0
      .000 1110 = TXOP value: 0x0e
      0.... = midamble periodicity unknown: 0x0
  
```

Por último se verifica que tipo de modulación está utilizando si OFDM o OFDMA, esta información se encuentra en el campo “**Channel Flags**”, como se indica en la figura 116.

Figura 116
Modulación en la transmisión

```

Radiotap Header v0, Length 72
  Header revision: 0
  Header pad: 0
  Header length: 72
  Present flags
  Flags: 0x10
  Channel frequency: 5180 [A 36]
  Channel flags: 0x0140, Orthogonal Frequency-Division Multiplexing (OFDM), 5 GHz spectrum
    .... 0000 = Turbo: False
    .... 0000 = Complementary Code Keying (CCK): False
    .... 0100 = Orthogonal Frequency-Division Multiplexing (OFDM): True
    .... 0000 = 2 GHz spectrum: False
    .... 0100 = 5 GHz spectrum: True
    .... 0000 = Passive: False
    .... 0000 = Dynamic CCK-OFDM: False
    .... 0000 = Gaussian Frequency Shift Keying (GFSK): False
    .... 0000 = GSM (900MHz): False
    ..0000 = Static Turbo: False
    .0000 = Half Rate Channel (10MHz Channel Width): False
    000000 = Quarter Rate Channel (5MHz Channel Width): False
  
```


En la tabla 28 se observa los valores que se obtuvo en la transmisión, mediante estos valores se determina la velocidad de datos en la tabla del anexo C1 que es para OFDM.

Tabla 28
Valores obtenidos en la captura de marcos 802.11ax

Característica	Valor
PHY	802.11ax
Índice MCS	11
Intervalo de guarda	1,6 μ s
Ancho del canal	160 MHz
Flujos espaciales	1
Modulación	OFDM

En base a esta información se obtuvo que la velocidad de datos es de 1134,3 Mbps, esto se observa en la figura 117.

Figura 117
Valor de la velocidad de datos.

MCS Index	Spatial Stream	Modulation	Coding	OFDM (802.11ax)											
				20MHz			40MHz			80MHz			160MHz		
				0.8 μ s GI	1.6 μ s GI	3.2 μ s GI	0.8 μ s GI	1.6 μ s GI	3.2 μ s GI	0.8 μ s GI	1.6 μ s GI	3.2 μ s GI	0.8 μ s GI	1.6 μ s GI	3.2 μ s GI
0	1	BPSK	1/2	8.6	8.1	7.3	17.2	16.3	14.6	36	34	30.6	72.1	68.1	61.3
1	1	QPSK	1/2	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	144.1	136.1	122.5
2	1	QPSK	3/4	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	216.2	204.2	183.8
3	1	16-QAM	1/2	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5	288.2	272.2	245
4	1	16-QAM	3/4	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
5	1	64-QAM	2/3	68.8	65	58.5	137.6	130	117	288.2	272.2	245	576.5	544.4	490
6	1	64-QAM	3/4	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	648.5	612.5	551.3
7	1	64-QAM	5/6	86	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3	720.6	680.6	612.5
8	1	256-QAM	3/4	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	864.7	816.7	735
9	1	256-QAM	5/6	114.7	108.3	97.5	229.4	216.7	195	480.4	453.7	408.3	960.8	907.4	816.7
10	1	1024-QAM	3/4	129	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4	1080.9	1020.8	918.8
11	1	1024-QAM	5/6	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4	1201	1134.3	1020.8

- **Análisis de WPA3**

Ahora se va a analizar el protocolo WPA3, que es el nuevo protocolo de seguridad para 802.11ax.

Primero se analiza los beacons enviado por el AP, para verificar si este puede utilizar este protocolo, en la figura 118 se observa en el campo RSN.

Figura 118
Información del beacon

```

IEEE 802.11 Beacon frame, Flags: .....C
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
  Tagged parameters (326 bytes)
    Tag: SSID parameter set: WLAN_5G
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 36
    Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    Tag: Power Constraint: 0
    Tag: TPC Report Transmit Power: 30, Link Margin: 0
    Tag: RM Enabled Capabilities (5 octets)
    Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 24
      RSN Version: 1
      Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
      Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Auth Key Management (AKM) Suite Count: 2
      Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256)
        Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
        Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
          Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
          Auth Key Management (AKM) type: SAE (SHA256) (8)
      RSN Capabilities: 0x0000
  
```

Se observa en la figura 119 en el campo Auth Key Management hay dos AKM SUITE , la primera corresponde a WPA 2, ya que su AKM es de tipo 2 y PSK, mientras que en el segundo su AKM es de tipo 8 y SAE, el cual identifica a WPA3.

Figura 119
Auth AKM Management

```

Auth Key Management (AKM) Suite Count: 2
Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256)
  Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
    Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) type: PSK (2)
  Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
    Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) type: SAE (SHA256) (8)

```

Una vez que el beacon llega a la estación esta intentara conectarse, enviando un probe request al AP, este se enviara solo si la estación es compatible con WPA3. Y de la misma manera el AP enviara un probe response indicando que puede conectarse.

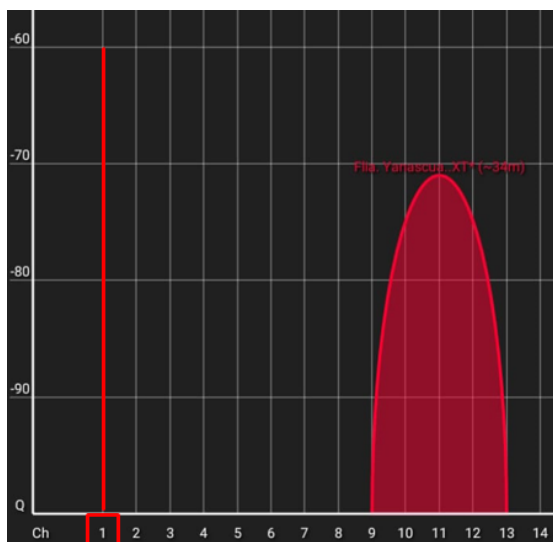
A continuación, la estación envía un authentication con los valores del escalar y elemento infinito, que son valores que permitirán establecer una PMK y de esta manera comprobar los valores para autenticarse. El AP también envía estos valores a la estación. La estación confirma que los valores son correctos y solicita la asociación al AP.

4.5.8. Análisis de espectro

Para analizar el espectro de wifi, se considera los canales 1, y 11 en la banda de 2,4 GHz, ya que el analizador soporta como máximo hasta 3,8GHz, y estos canales son los más utilizados ya que no tiene interferencia cocanal entre ellos.

En el primer caso del canal 1, será un canal libre de otras redes, como se observa en la figura 120, en donde no existe ni solapamiento, ni interferencia cocanal.

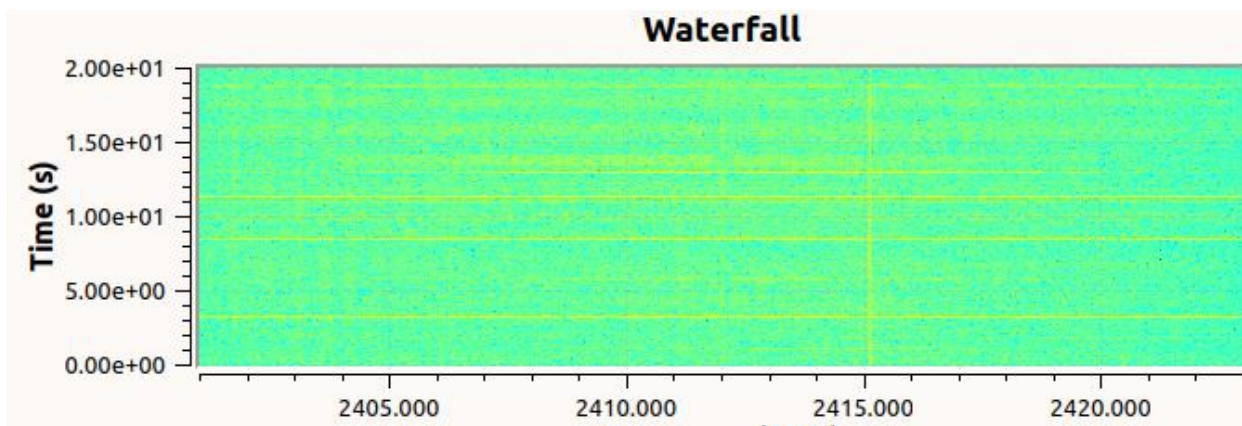
Figura 120 Análisis del espectro Wifi.



Una vez ingresado a la herramienta de análisis, se pone los parámetros como la frecuencia central (2412 MHz), al ancho de banda (22 MHz) y la tasa de muestreo de 20e6 sps.

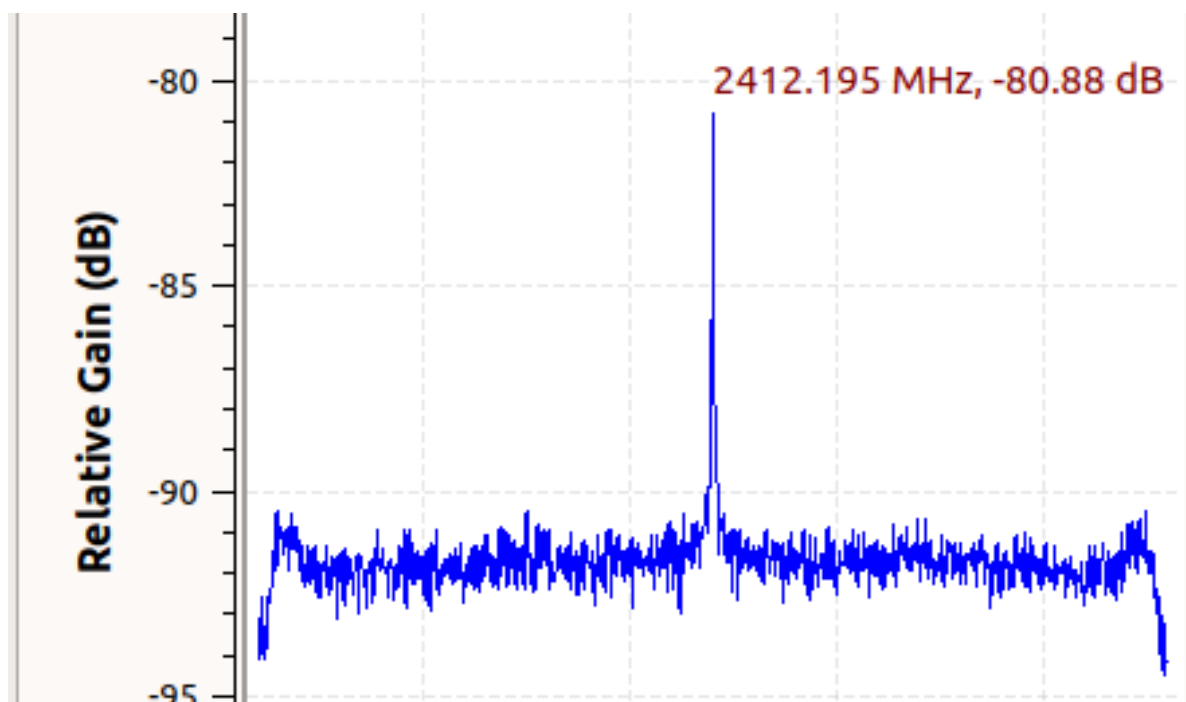
En la figura 121 se observa el espectro en el canal 1, esta figura es un mapa de calor, en donde la tonalidad más cálida determina la energía que pasa en esa frecuencia.

Figura 121
Mapa de calor



Y, en la figura 122 se observa la señal del canal 1, se puede apreciar que en la frecuencia de 2412 Mhz, existe un pulso, aquí es donde se concentra la mayor energía y es donde se transmite la mayoría de los datos.

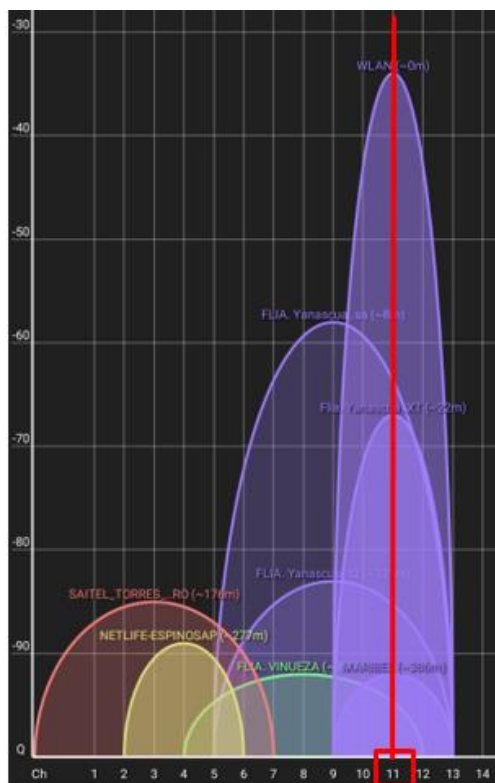
Figura 122
Señal del canal 1



También hay que tomar en cuenta que esta señal presenta un nivel muy bajo de ruido e interferencia de cualquier tipo, se puede decir es una señal limpia.

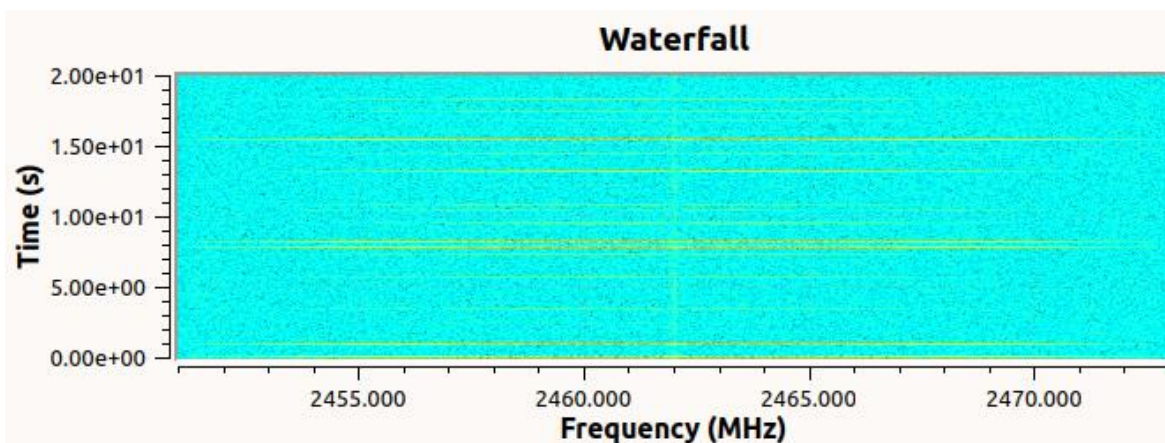
Para el segundo caso, el canal 11 presentara varias interferencias de solapamiento y de cocanal. En la figura 123 se observa que existen varias redes operando en el mismo canal causando así que este canal este congestionado.

Figura 123
Análisis del canal 11



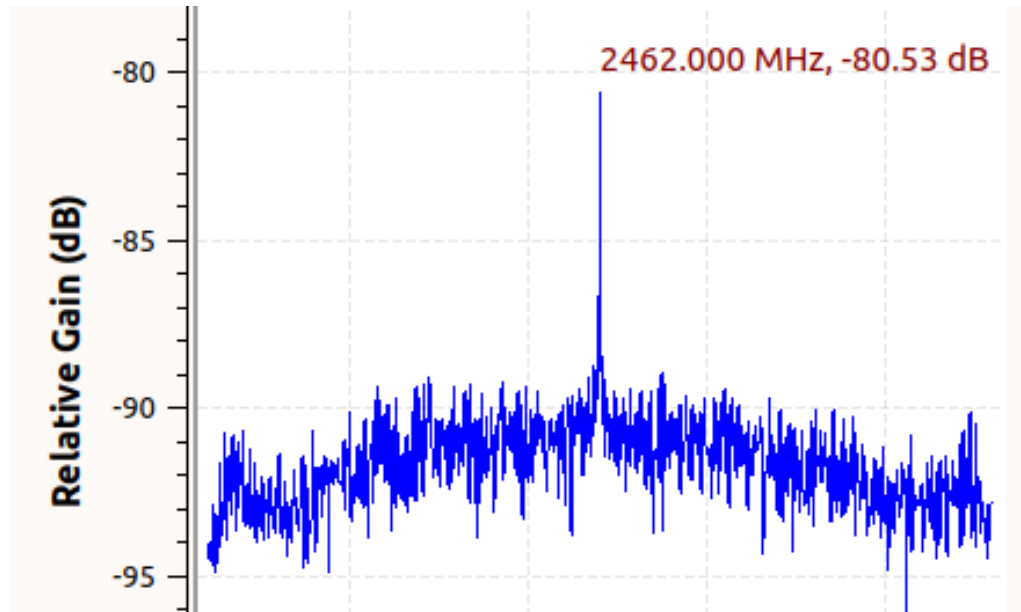
Una vez realizado el escaneo del canal 11, se determina que existe interferencia en ese canal, según la figura 124, un tono más frío significa que la señal está siendo alterada por agentes externos.

Figura 124
Mapa de calor canal 11



Y, de la misma forma en la figura 125 se observa que la señal si esta con ruido e interferencias.

Figura 125
Señal del canal 11




Por motivos de hardware analizar la banda de 5GHz resultado complicado, se dejará el análisis para trabajos futuros.

4.6. Guías de laboratorio

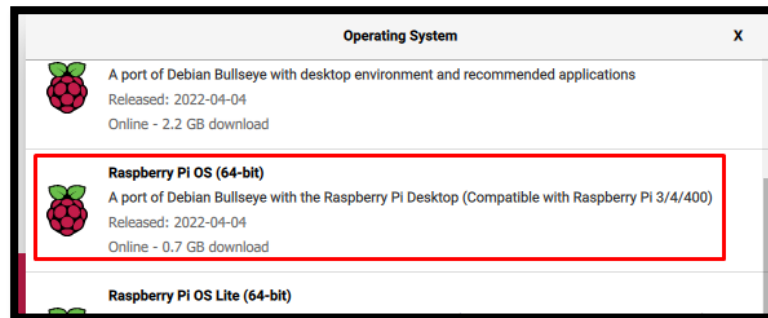
A continuación, se detallan las guías de laboratorio que se implementaran en la materia de comunicación inalámbrica.

4.6.1. Guía 1: “Instalación y configuración de Raspberry PI OS”

	UNIVERSIDAD TÉCNICA DEL NORTE FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CARRERA EN TELECOMUNICACIONES COMUNICACIÓN INALAMBRICA		
Guía de laboratorio			
Nombre y Apellido:		Guía #:	1
Docentes:			
Fecha:			
Nivel:			
Tema:	“Instalación y configuración de Raspberry PI OS”		
Objetivo general:	<ul style="list-style-type: none"> • Describir el procedimiento de instalación y configuración Raspberry PI OS, para comprender el funcionamiento de este. 		
Objetivos específicos:	<ul style="list-style-type: none"> • Instalar Raspberry Pi OS en la raspberry CM4 • Configurar la raspberry para comunicación mediante SSH. • Instalar y configurar las antenas Intel AX200 y AX210. • Demostrar conectividad inalámbrica. 		
Marco teórico:	Investigar los siguientes temas: <ul style="list-style-type: none"> • Raspberry Pi OS • Principales características de raspberry Pi. • Compilación cruzada. • Comandos para utilizar en la terminal de raspberry 		
Materiales y equipos:	Se debe listar los principales materiales, software y equipos a utilizar durante la práctica. <ul style="list-style-type: none"> • 1 raspberry pi CM4 • 1 antena Intel ax200 o ax210 • Adaptador de m.2 a PCIx1 • Cable micro usb • 1 computador • Rpiboot • Raspberry PI Imager • 1 AP 		
Procedimiento:	1. Preparar la raspberry para que instale el sistema operativo en la memoria eMMC, ubicando un jumper como se indica en la imagen. (evitar este paso si el sistema se instala en un SDcard)		



2. Descargar e instalar rpiboot para que reconozca la raspberry como unidad de almacenamiento.
(https://github.com/raspberrypi/usbboot/raw/master/win32/rpiboot_setup.exe)
3. Descargar raspberry pi Imager e instalarlo para posterior instalación del sistema operativo. (<https://www.raspberrypi.com/software/>), se debe instalar la versión de 64-bits.



4. Configurar SSH en la raspberry, ingresar a la terminal y digitar raspi-config, en interfaces habilitar SSH.
5. En un computador con sistema Linux, se procede a realizar la compilación cruzada para habilitar la tarjeta inalámbrica.
6. Se copia el siguiente repositorio con el comando:


```
sudo apt install git bc bison flex libssl-dev make
git clone --depth=1 https://github.com/raspberrypi/linux
```
7. Se crea un archivo de configuración .config.

```
cd linux
make ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu-
bcm2711_defconfig
```


8. A continuación, se edita el archivo .config mediante el menú, con el siguiente comando.

```
make ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu- menuconfig
```

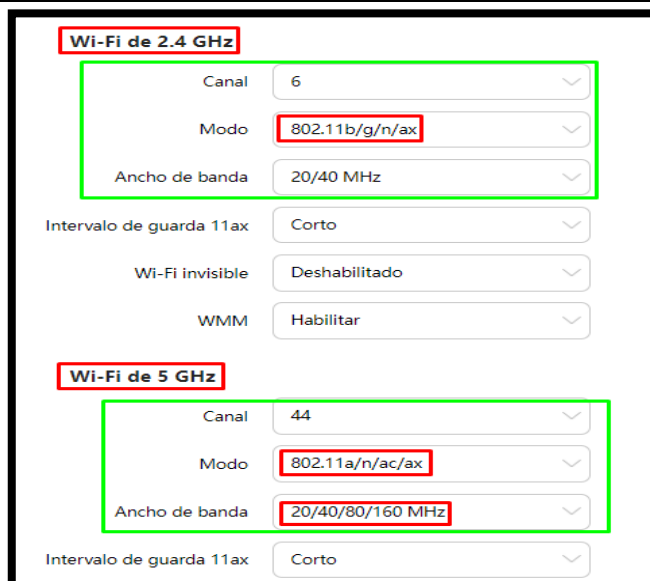
9. Una vez ingresado al menú, se procede a habilitar las siguientes opciones, y se guarda la configuración.
 - Controladores de dispositivos > Compatibilidad con dispositivos de red > LAN inalámbrica > Intel > "Intel Wireless WiFi Next Gen AGN

	<p>(iwlwifi)"</p> <ul style="list-style-type: none"> • "Intel Wireless WiFi MVM Firmware support" (en la opción iwlwifi, una vez seleccionada) <p>10. Por último, se debe compilar el núcleo con el siguiente comando.</p> <pre>make -j8 ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu- Image modules dtbs</pre> <p>11. Una vez terminada la compilación se debe copiar el nuevo kernel a la raspberry para lo cual es importante montar la unidad de la siguiente manera.</p> <pre>sudo mkdir -p mnt/fat32 sudo mkdir -p mnt/ext4 sudo mount /dev/sda1 mnt/fat32 sudo mount /dev/sda2 mnt/ext4</pre> <p>12. Ahora se procede a copiar los archivos necesarios.</p> <pre>sudo cp arch/arm64/boot/Image mnt/fat32/kernel8.img sudo cp arch/arm64/boot/dts/broadcom/*.dtb mnt/fat32/ sudo cp arch/arm64/boot/dts/overlays/*.dtb* mnt/fat32/overlays/ sudo cp arch/arm64/boot/dts/overlays/README mnt/fat32/overlays/</pre> <p>13. Se instala los módulos del kernel en la unidad y se los copia también.</p> <pre>sudo env PATH=\$PATH make ARCH=arm64 CROSS_COMPILE=aarch64-linux-gnu- INSTALL_MOD_PATH=mnt/ext4 modules_install sudo cp arch/arm64/boot/Image mnt/fat32/kernel8.img sudo cp arch/arm64/boot/dts/broadcom/*.dtb mnt/fat32/ sudo cp arch/arm64/boot/dts/overlays/*.dtb* mnt/fat32/overlays/ sudo cp arch/arm64/boot/dts/overlays/README mnt/fat32/overlays/</pre> <p>14. Por último, se desmonta la unidad.</p> <pre>sudo umount mnt/fat32 sudo umount mnt/ext4</pre> <p>15. Una vez iniciada la raspberry con el nuevo kernel, se procede a instalar el firmware de la interfaz inalámbrica de la siguiente manera.</p> <pre>\$ wget https://wireless.wiki.kernel.org/_media/en/users/drivers/iwlwifi/iwlwifi-cc-46.3fab8da.0.tgz \$ tar -xvzf iwlwifi-cc-46.3fab8da.0.tgz \$ cd iwlwifi-cc-46.3fab8da.0/ \$ sudo cp iwlwifi-*.ucode /lib/firmware</pre> <p>16. Una vez realizado este procedimiento se reinicia la raspberry y se verifica la conexión mediante la interfaz.</p>
Resultados:	<ul style="list-style-type: none"> • Verificar la conexión a una red mediante la tarjeta inalámbrica. • Verificar el acceso a internet.
Conclusiones:	Escribir 5 conclusiones sobre la práctica
Recomendaciones:	Escribir 5 recomendaciones sobre la práctica
Bibliografía:	Indicar la bibliografía utilizada para la práctica.

4.6.2. Guía 2: “Levantamiento red en modo ad-hoc e infraestructura”

	UNIVERSIDAD TÉCNICA DEL NORTE FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CARRERA EN TELECOMUNICACIONES COMUNICACIÓN INALAMBRICA														
Guía de laboratorio															
Nombre y Apellido:			Guía #: 2												
Docentes:															
Fecha:															
Nivel:															
Tema:	“Levantamiento red en modo ad-hoc e infraestructura”														
Objetivo general:	<ul style="list-style-type: none"> • Realizar el levantamiento de la red en modo ad-hoc e infraestructura con las raspberry Pi y entender cómo operan estas redes. 														
Objetivos específicos:	<ul style="list-style-type: none"> • Configurar dos nodos para la red ad-hoc • Configurar el AP y los nodos para la red de infraestructura. • Verificar comunicación entre los nodos en las dos redes. 														
Marco teórico:	Investigar los siguientes temas: <ul style="list-style-type: none"> • Red ad-hoc • Red de infraestructura • Características de 802.11ax (Capa física) 														
Materiales y equipos:	<p>Se debe listar los principales materiales, software y equipos a utilizar durante la práctica.</p> <ul style="list-style-type: none"> • 2 raspberry pi CM4 • 1 antena Intel ax200 o ax210 • Adaptador de m.2 a PCIx1 • 1 AP 802.11ax <p>Además, se debe incluir una tabla de direccionamiento para cada red.</p> <p>Red ad-hoc</p> <table border="1" data-bbox="443 1556 1430 1759" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Dispositivo</th> <th style="text-align: center;">Interfaz</th> <th style="text-align: center;">Dirección IP</th> <th style="text-align: center;">Gateway predeterminado</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">NODO 1</td> <td style="text-align: center;">802.11ax</td> <td style="text-align: center;">192.168.50.1 /24</td> <td style="text-align: center;">-</td> </tr> <tr> <td style="text-align: center;">NODO 2</td> <td style="text-align: center;">802.11ax</td> <td style="text-align: center;">192.168.50.2 /24</td> <td style="text-align: center;">-</td> </tr> </tbody> </table>			Dispositivo	Interfaz	Dirección IP	Gateway predeterminado	NODO 1	802.11ax	192.168.50.1 /24	-	NODO 2	802.11ax	192.168.50.2 /24	-
Dispositivo	Interfaz	Dirección IP	Gateway predeterminado												
NODO 1	802.11ax	192.168.50.1 /24	-												
NODO 2	802.11ax	192.168.50.2 /24	-												

	<p>Red de infraestructura</p> <table border="1" data-bbox="444 226 1430 527"> <thead> <tr> <th>Dispositivo</th> <th>Interfaz</th> <th>Dirección IP</th> <th>Gateway predeterminado</th> </tr> </thead> <tbody> <tr> <td>Router</td> <td>802.11ax</td> <td>192.168.101.1 /24</td> <td>-</td> </tr> <tr> <td>NODO 1</td> <td>802.11ax</td> <td>192.168.101.2 /24</td> <td>192.168.101.1</td> </tr> <tr> <td>NODO 2</td> <td>802.11ax</td> <td>192.168.101.3 /24</td> <td>192.168.101.1</td> </tr> <tr> <td>NODO 3</td> <td>802.11ax</td> <td>192.168.101.4 /24</td> <td>192.168.101.1</td> </tr> </tbody> </table>	Dispositivo	Interfaz	Dirección IP	Gateway predeterminado	Router	802.11ax	192.168.101.1 /24	-	NODO 1	802.11ax	192.168.101.2 /24	192.168.101.1	NODO 2	802.11ax	192.168.101.3 /24	192.168.101.1	NODO 3	802.11ax	192.168.101.4 /24	192.168.101.1
Dispositivo	Interfaz	Dirección IP	Gateway predeterminado																		
Router	802.11ax	192.168.101.1 /24	-																		
NODO 1	802.11ax	192.168.101.2 /24	192.168.101.1																		
NODO 2	802.11ax	192.168.101.3 /24	192.168.101.1																		
NODO 3	802.11ax	192.168.101.4 /24	192.168.101.1																		
<p>Procedimiento:</p>	<p>Red Ad-hoc</p> <p>Para levantar la red se utiliza dos nodos, en cada uno se configurará el modo ad-hoc para que se comuniquen entre ellos, el procedimiento se detalla a continuación. Para los dos nodos es la misma configuración con la diferencia que a cada uno se le asignará una dirección ip diferente, pero en la misma red, para el nodo1 192.168.50.1 y para el nodo 2 192.168.50.2, además se debe asignar el nombre de la red “RED”, el modo de operación y la contraseña.</p> <pre data-bbox="609 915 1268 1451"> sudo nano /etc/network/interface auto wlan0 iface wlan0 inet static address 192.168.50.1 netmask 255.255.255.0 network 192.168.50.0 wireless-channel 1 wireless-ssid RED wireless-mode ad-hoc wireless-key 1234567890 sudo wpa_cli terminate sudo service networking restart </pre> <p>Red Infraestructura</p> <ol style="list-style-type: none"> 1. Se configura el AP tanto en la banda de 2.4 GHz y 5GHz, asignando el canal, el modo que será 802.11 ax y el ancho de banda permitido que va desde 20 hasta 160 en 5Ghz 																				



Wi-Fi de 2.4 GHz

Canal: 6

Modo: 802.11b/g/n/ax

Ancho de banda: 20/40 MHz

Intervalo de guarda 11ax: Corto

Wi-Fi invisible: Deshabilitado

WMM: Habilitar

Wi-Fi de 5 GHz


Canal: 44

Modo: 802.11a/n/ac/ax

Ancho de banda: 20/40/80/160 MHz

Intervalo de guarda 11ax: Corto

2. También se debe configurar la red Wifi, es decir asignarle el SSID y escoger el tipo de seguridad en este caso WPA3.



Wi-Fi de 2.4 GHz

Nombre de la red Wi-Fi: WLAN

Seguridad: WPA2 PSK / WPA3 SAE

Contraseña de la red Wi-Fi:

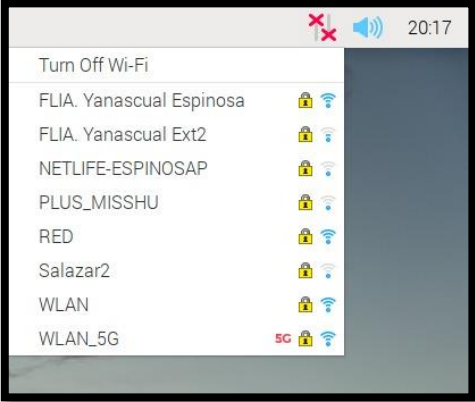
Wi-Fi de 5 GHz

Nombre de la red Wi-Fi: WLAN_5G


Seguridad: WPA2 PSK / WPA3 SAE

Contraseña de la red Wi-Fi:

3. Una vez realizada estas configuraciones se puede apreciar que en las raspberry ya aparecen las dos redes WLAN y WLAN_5G.

	 <p>Para conectarse solo es necesario ingresar la contraseña,</p>
Resultados:	<ul style="list-style-type: none"> • Verificar la conexión a la red mediante la tarjeta inalámbrica. • Verificar el acceso a internet en la red de infraestructura. • Verificar comunicación entre los nodos de la red.
Conclusiones:	Escribir 5 conclusiones sobre la práctica
Recomendaciones:	Escribir 5 recomendaciones sobre la práctica
Bibliografía:	Indicar la bibliografía utilizada para la práctica.

4.6.3. Guía 3: “Levantamiento red mesh”

	UNIVERSIDAD TÉCNICA DEL NORTE FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CARRERA EN TELECOMUNICACIONES COMUNICACIÓN INALAMBRICA																		
Guía de laboratorio																			
Nombre y Apellido:			Guía #: 3																
Docentes:																			
Fecha:																			
Nivel:																			
Tema:	“Levantamiento red mesh”																		
Objetivo general:	<ul style="list-style-type: none"> • Realizar el levantamiento de la red mesh con las raspberry Pi y el protocolo BATMAN y entender cómo operan estas redes. 																		
Objetivos específicos:	<ul style="list-style-type: none"> • Configurar los nodos en una red mesh • Configurar el protocolo batman en cada uno de los nodos. • Verificar comunicación entre los nodos en las dos redes. 																		
Marco teórico:	Investigar los siguientes temas: <ul style="list-style-type: none"> • Red mesh • Protocolo batman • Comando para la herramienta batctl. 																		
Materiales y equipos:	<p>Se debe listar los principales materiales, software y equipos a utilizar durante la práctica.</p> <ul style="list-style-type: none"> • 3 raspberry pi CM4 • 1 antena Intel ax200 o ax210 • Adaptador de m.2 a PCIx1 <p>Además, se debe incluir una tabla de direccionamiento de la red.</p> <table border="1" data-bbox="443 1480 1432 1732" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="width: 25%;">Dispositivo</th> <th style="width: 25%;">Interfaz</th> <th style="width: 25%;">Dirección IP</th> <th style="width: 25%;">Gateway predeterminado</th> </tr> </thead> <tbody> <tr> <td>NODO GW</td> <td>802.11ax</td> <td>192.168.100.1 /24</td> <td>192.168.100.1</td> </tr> <tr> <td>NODO 2</td> <td>802.11ax</td> <td>192.168.100.2 /24</td> <td>192.168.100.1</td> </tr> <tr> <td>NODO 3</td> <td>802.11ax</td> <td>192.168.100.3 /24</td> <td>192.168.100.1</td> </tr> </tbody> </table>			Dispositivo	Interfaz	Dirección IP	Gateway predeterminado	NODO GW	802.11ax	192.168.100.1 /24	192.168.100.1	NODO 2	802.11ax	192.168.100.2 /24	192.168.100.1	NODO 3	802.11ax	192.168.100.3 /24	192.168.100.1
Dispositivo	Interfaz	Dirección IP	Gateway predeterminado																
NODO GW	802.11ax	192.168.100.1 /24	192.168.100.1																
NODO 2	802.11ax	192.168.100.2 /24	192.168.100.1																
NODO 3	802.11ax	192.168.100.3 /24	192.168.100.1																
Procedimiento:	Para implementar la red se realiza el siguiente procedimiento en cada uno de los nodos que conformarán la red mallada.																		

1. Primero, se debe instalar la herramienta con el comando **“sudo apt-get install -y batctl”**.
2. Se crea un archivo con el siguiente comando y nombre **“sudo nano batman-adv-conf.sh”**
3. Dentro del archivo se debe ingresar la siguiente información, tomando en cuenta que si son nodos que no son Gateway el modo es cliente.

```
#!/bin/bash
#Selección de la interfaz a usar con el protocolo batman-adv
sudo batctl if add wlan0
sudo ifconfig bat0 mtu 1468
#Indicar que el dispositivo ejercerá de nodo en la red mesh
sudo batctl gw_mode client
#Habilitar y activar las interfaces empleadas por el protocolo batman-adv
sudo ifconfig wlan0 up
sudo ifconfig bat0 up
#Asignar una IP estática al nodo
sudo ifconfig bat0 192.168.100.1/24
```

4. Ahora para que el archivo se pueda ejecutar se asigna permisos con el comando **“sudo chmod +x batman-adv-conf.sh”**
5. A continuación, se debe crear un archivo con el comando **“sudo nano /etc/network/interfaces.d/wlan0”**
6. Dentro del archivo se coloca la siguiente información en donde se especifica el canal de operación de la red, el nombre de la red y el modo de operación.

```
auto wlan0
iface wlan0 inet manual
wireless-channel 1
wireless-essid MESH
wireless-mode ad-hoc
```

7. Ahora, para que se inicie el archivo al encenderse la Raspberry se debe configurar el siguiente archivo **“sudo nano /etc/rc.local”**, ubicando la siguiente instrucción al final del archivo.

```
/home/pi/batman-adv-conf.sh &
```

8. Una vez finalizada esta configuración, se debe reiniciar la Raspberry. Si la Raspberry va a ser Gateway, se debe realizar la siguiente configuración extra.
9. Se descarga el paquete dnsmasq con el comando **“sudo apt-get install -y dnsmasq”**
10. Una vez instalado se ingresa en la siguiente ruta **“sudo nano /etc/dnsmasq.conf”**, y al final del archivo se coloca las siguientes líneas de código, indicando el rango de direcciones IP, y la interfaz en la que va a operar.

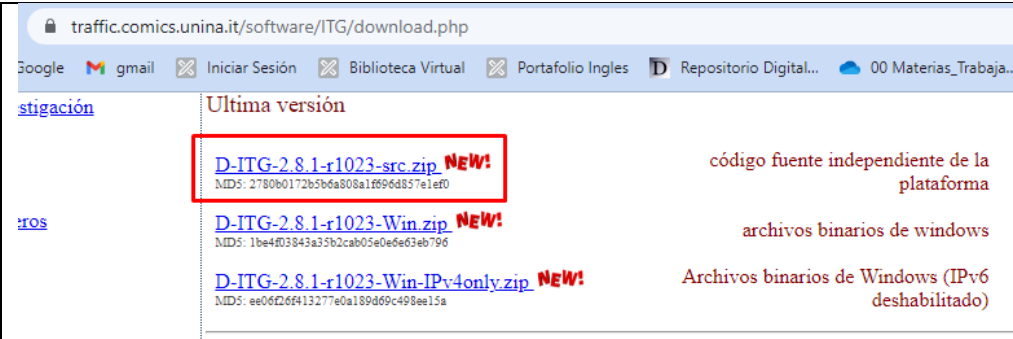
```
interface=bat0
dhcp-range=192.168.100.2,192.168.100.10,255.255.255.0,12h
```

11. Ahora, se vuelve a ingresar al archivo de batman-adv, y se actualiza la

	<p>información con las siguientes líneas de código, esto permitirá indicar que el nodo será Gateway, además se ingresa reglas iptables para que el tráfico pueda ingresar y salir de la red, mediante este nodo.</p> <pre data-bbox="448 310 1435 961">#!/bin/bash #Selecccion de la interfaz a usar con el protocolo batman-adv sudo batctl if add wlan0 sudo ifconfig bat0 mtu 1468 #Indicar que el dispositivo ejercera de nodo en la red mesh sudo batctl gw_mode server #Habilitar el reenvío de puertos sudo sysctl -w net.ipv4.ip_forward=1 sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE sudo iptables -A FORWARD -i eth0 -o bat0 -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT sudo iptables -A FORWARD -i bat0 -o eth0 -j ACCEPT #Habilitar y activar las interfaces empleadas por el protocolo batman-adv sudo ifconfig wlan0 up sudo ifconfig bat0 up #Asignar una ip estática al nodo sudo ifconfig bat0 192.168.100.1/24</pre>
Resultados:	<ul style="list-style-type: none"> • Verificar la conexión a la red mediante la tarjeta inalámbrica. • Verificar el acceso a internet en la red de mesh • Verificar comunicación entre los nodos de la red. • Verificar los vecinos de la red mallada
Conclusiones:	Escribir 5 conclusiones sobre la práctica
Recomendaciones:	Escribir 5 recomendaciones sobre la práctica
Bibliografía:	Indicar la bibliografía utilizada para la práctica.

4.6.4. Guía 4: “Instalación y configuración de D-ITG, jperf y wireshark.”

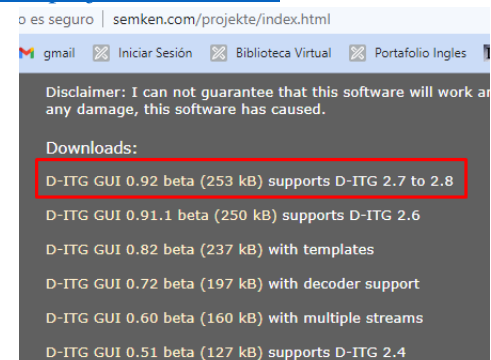
	UNIVERSIDAD TÉCNICA DEL NORTE FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CARRERA EN TELECOMUNICACIONES COMUNICACIÓN INALAMBRICA		
Guía de laboratorio			
Nombre y Apellido:		Guía #:	4
Docentes:			
Fecha:			
Nivel:			
Tema:	“Instalación y configuración de D-ITG, jperf y wireshark.”		
Objetivo general:	<ul style="list-style-type: none"> • Realizar la instalación y configuración de las herramientas D-ITG, jperf y wireshark, para el análisis de la tecnología 802.11. 		
Objetivos específicos:	<ul style="list-style-type: none"> • Instalar D-ITG, jperf y wireshark. • Configurar D-ITG, jperf y wireshark. • Verificar las herramientas mediante pruebas en las redes. 		
Marco teórico:	Investigar los siguientes temas: <ul style="list-style-type: none"> • D-ITG • Jperf • Wireshark • Modo monitor • Comandos para análisis de tramas en wireshark. 		
Materiales y equipos:	Se debe listar los principales materiales, software y equipos a utilizar durante la práctica. <ul style="list-style-type: none"> • 3 nodos raspberry • D-ITG • Jperf • Wireshark 		
Procedimiento:	Instalación y configuración de D-ITG. <ol style="list-style-type: none"> 1. Primero se ingresa al siguiente enlace y se descarga el archivo que se indica en la figura. https://traffic.comics.unina.it/software/ITG/download.php 		



2. Una vez descargado se descomprime en el directorio de su preferencia, se ingresa en la carpeta con el comando **“cd D-ITG-2.8.1-r1023/src”** y por último se construye el binario con el comando **“make”**.

3. Para poder trabajar de mejor manera se instala la GUI del programa, para esto se ingresa a la siguiente página y se descarga el archivo que se indica en la figura.

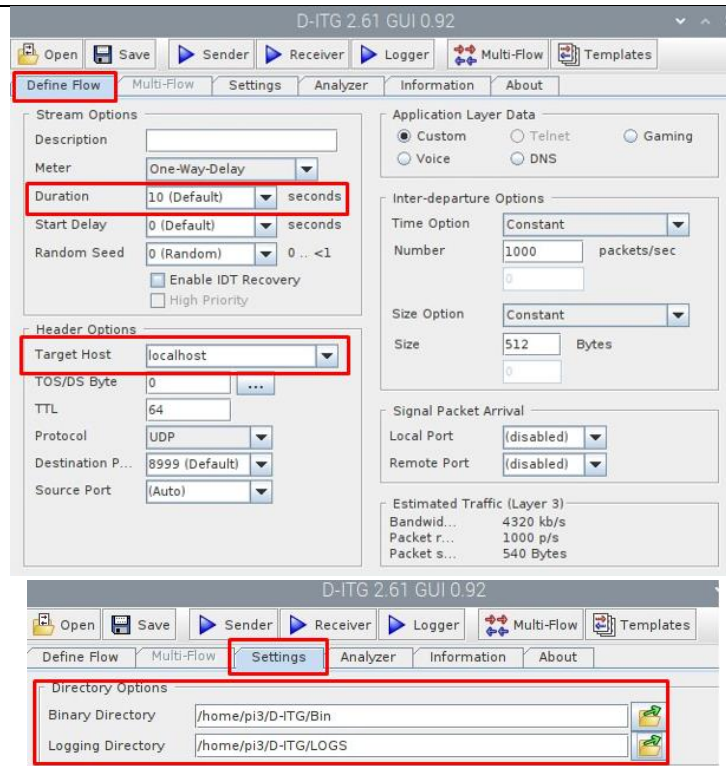
<http://www.semken.com/projekte/index.html>



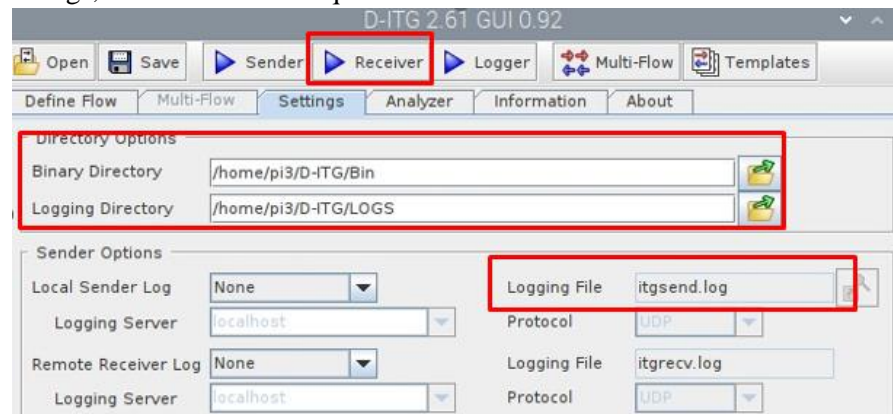
4. Se crea una carpeta que se llame D-ITG, y dentro de esta se descomprime el archivo.

5. Se ingresa a la carpeta con el comando **“cd D-ITG”**, dentro de este directorio se escribe el siguiente comando para ejecutar el programa **“sudo java -jar ITGGUI.jar”**.

6. Para la configuración del programa se debe configurar tanto en el transmisor como en el receptor, los principales parámetros a configurar en el transmisor son el host de destino, la duración, y la ubicación de los archivos binarios y de log.



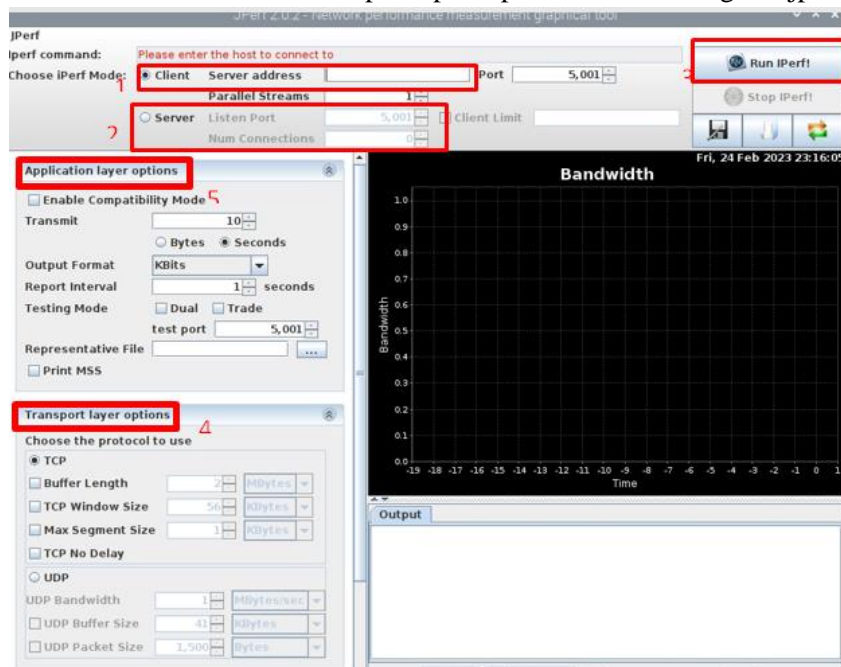
7. Y para el receptor hay que indicar la ubicación para los archivos binarios y logs, además de indicar que se va a recibir tráfico.



Instalación de iperf y jperf.

1. Primero, antes de instalar iperf y jperf es necesario que en el sistema tenga instalado java, para esto se utiliza el comando **“sudo apt install default-jdk”**
2. A continuación, se instala iperf, esto mediante los siguientes comandos **“sudo apt-get install iperf”**, **“sudo apt-get install iperf3”**.
3. Ahora, se debe descargar jperf, para esto se dirige a la página <https://www.telectronika.com/descargas/jperf/>
4. Una vez descargado se descomprime en el directorio de preferencia, se ingresa a la carpeta y mediante el siguiente comando se ejecuta el programa **“sh jperf.sh”**

5. A continuación, se detalla los principales parámetros a configurar jperf.



- 1) Client: se especifica que el nodo estará como cliente, además se especificará la ip del servidor.
- 2) Server: Especifica que el nodo estará como servidor.
- 3) Run iPerf: Permite correr el programa para que empiece a enviar o recibir datos.
- 4) Transport layer options: Determina el tipo de protocolo de transporte, ya sea TCP o UDP
- 5) Application layer options: Permite configurar parámetros como el tiempo de envío de datos, el intervalo y el formato de envío.

Instalación de wireshark.

Antes de instalar wireshark se necesita un sistema Operativo Linux, para el caso Raspbian, además que la tarjeta inalámbrica ax esté funcionando correctamente y además permita operar en modo monitor.

Primero se debe actualizar el sistema, para esto se utiliza los siguientes comandos:

```
$ sudo apt-get update -y
$ sudo apt-get upgrade -y
```


Una vez realizado este procedimiento, a continuación, se debe actualizar el kernel a una versión mayor a 5.1, para esto utilice el comando `$ uname -a` para verificar la versión, si la versión esta desactualizada actualícela.

Ahora, se debe configurar para que la tarjeta capture en modo monitor, permitiendo así tramas 802.11, para esto se debe seguir los siguientes comandos:

```
$ sudo apt-get install aircrack-ng
$ sudo airmon-ng start wlan0
$ monitor mode enabled on mon0
```

	<p>Una vez aplicado estos comandos si todo esta correcto deberá aparecer una interfaz con el nombre mon0. Esta interfaz es la que se utilizara para capturar.</p> <p>Por último, se debe instalar wireshark en su versión más reciente para que permita la especificación 802.11ax., para esto se sigue los siguientes comandos.</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo add-apt-repository ppa:wireshark-dev/stable \$ sudo apt update \$ sudo apt -y install wireshark \$ sudo apt -y install wireshark-qt</pre> <p>Para instalar una versión de desarrollo se procede con los siguientes comandos:</p> <pre style="border: 1px solid black; padding: 5px;">\$ sudo add-apt-repository ppa:dreibh/ppa \$ sudo apt update \$ sudo apt -y install wireshark</pre> <p>Finalmente abrimos wireshark con el comando \$sudo wireshark y se verifica si captura marcos 802.11ax.</p>
Resultados:	<ul style="list-style-type: none"> • Realizar inyección de tráfico con DITG • Verificar la comunicación mediante jperf • Verificar las tramas 802.11ax en wireshark. • Probar las herramientas en las diferentes redes.
Conclusiones:	Escribir 5 conclusiones sobre la práctica
Recomendaciones	Escribir 5 recomendaciones sobre la práctica
Bibliografía:	Indicar la bibliografía utilizada para la práctica.

4.6.5. Guía 5: “Métricas de rendimiento en red de infraestructura”

	UNIVERSIDAD TÉCNICA DEL NORTE FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CARRERA EN TELECOMUNICACIONES COMUNICACIÓN INALAMBRICA		
Guía de laboratorio			
Nombre y Apellido:			Guía #: 5
Docentes:			
Fecha:			
Nivel:			
Tema:	“Métricas de rendimiento en red de infraestructura”		
Objetivo general:	<ul style="list-style-type: none"> • Realizar la prueba de las métricas de rendimiento en una red de infraestructura, y verificar los valores de la tecnología. 		
Objetivos específicos:	<ul style="list-style-type: none"> • Probar las métricas mediante jperf • Analizar cada uno de los valores obtenidos. • Compararlos para diferentes bandas y anchos de canal. 		
Marco teórico:	Investigar los siguientes temas: <ul style="list-style-type: none"> • Ancho de banda • Jitter • Delay • Bitrate • Packetloss • Gnuplot 		
Materiales y equipos:	Se debe listar los principales materiales, software y equipos a utilizar durante la práctica. <ul style="list-style-type: none"> • 3 nodos • D-ITG • Jperf 		
Procedimiento:	Ancho de banda. <ol style="list-style-type: none"> 1. Primero se realiza la prueba del ancho de banda, para esto se enviará desde el cliente tráfico al servidor con la herramienta jperf. El tráfico que se enviará será TCP por un tiempo de 30 s. 2. Una vez finalizado el proceso se obtiene el valor del ancho de banda promedio para esa transmisión. 3. Probar el mismo método para tráfico UDP, diferentes tiempos. 4. Probar el ancho de banda para diferentes bandas, tanto 2,4 y 5 GHz. 5. Cambiar el ancho de canal en la banda de 5GHz y verificar el ancho de 		

	<p>banda.</p> <p>Jitter, delay, bitrate y Packetloss.</p> <ol style="list-style-type: none"> 1. Para estos parámetros se enviará tráfico por 30 segundos, de un nodo a otro, este tráfico corresponde a 2000 paquetes por segundo con un tamaño de 2500 bytes, mediante el protocolo UDP. 2. Una vez finalizada la prueba en la pestaña de análisis, se deberá generar los archivos .dat, estos permitirán obtener las diferentes gráficas de las métricas. <p>Estas pruebas se deben realizar en ambientes con y sin interferencias de todo tipo.</p>
Resultados:	<ul style="list-style-type: none"> • Verificar ancho de banda en diferentes condiciones • Verificar bitrate, jitter, delay y packetloss en la red. • Verificar los mismos parámetros en diferentes bandas. • Mostrar y analizar las gráficas obtenidas.
Conclusiones:	Escribir 5 conclusiones sobre la práctica
Recomendaciones:	Escribir 5 recomendaciones sobre la práctica
Bibliografía:	Indicar la bibliografía utilizada para la práctica.

4.6.6. Guía 6: “Captura de marcos 802.11ax”

	UNIVERSIDAD TÉCNICA DEL NORTE FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS CARRERA EN TELECOMUNICACIONES COMUNICACIÓN INALAMBRICA		
Guía de laboratorio			
Nombre y Apellido:		Guía #:	6
Docentes:			
Fecha:			
Nivel:			
Tema:	“Captura de marcos 802.11ax”		
Objetivo general:	<ul style="list-style-type: none"> • Capturar marcos 802.11ax en una red de infraestructura, y verificar las características de la tecnología. 		
Objetivos específicos:	<ul style="list-style-type: none"> • Realizar la captura de tráfico wifi 802.11ax mediante modo monitor. • Encontrar las características en los marcos capturados. • Analizar cada una de las características. 		
Marco teórico:	Investigar los siguientes temas: <ul style="list-style-type: none"> • OFDMA • 1024 QAM • MU-MIMO • BSS coloring • TWT • WPA3 • Índices MCS 		
Materiales y equipos:	Se debe listar los principales materiales, software y equipos a utilizar durante la práctica. <ul style="list-style-type: none"> • 2 nodos STA • 1 nodo en modo monitor • 1 AP • Wireshark 		
Procedimiento:	Generar tráfico de un nodo al otro, y capturarlo desde wireshark. Encontrar tramas que envía los nodos o el AP y buscar la siguiente información.		

IEEE 802.11 Beacon frame, Flags:0 → Beacon Frame

- IEEE 802.11 Wireless Management
 - Fixed parameters (12 bytes)
 - Tagged parameters (326 bytes)
 - Tag: SSID parameter set: WLAN 5G → SSID de la red
 - Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 - Tag: DS Parameter set: Current Channel: 36
 - Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
 - Tag: Power Constraint: 0
 - Tag: TPC Report Transmit Power: 30, Link Margin: 0
 - Tag: RM Enabled Capabilities (5 octets)
 - Tag: RSN Information
 - Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
 - Tag: QBSS Load Element 802.11e CCA Version
 - Tag: HT Capabilities (802.11n D1.10)
 - Tag: HT Information (802.11n D1.10)
 - Tag: Extended Capabilities (8 octets)
 - Tag: VHT Capabilities
 - Tag: VHT Operation
 - Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
 - Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0) → Parámetros únicos de 802.11ax
 - Ext Tag: Spatial Reuse Parameter Set
 - Ext Tag: MU EDCA Parameter Set
 - Ext Tag: UORA Parameter Set
 - Tag: Vendor Specific: Huawei Technologies Co.,Ltd
 - Tag: Vendor Specific: Huawei Technologies Co.,Ltd
 - Tag: Vendor Specific: Microsoft Corp.: WPS
 - Tag: Vendor Specific: Huawei Technologies Co.,Ltd
 - Tag: Vendor Specific: Huawei Technologies Co.,Ltd

Además, analizar las características presentes en los marcos.

HE MAC Capabilities Information: 0x58000e080805

-1 = +HTC HE Support: Supported
-0 = TWT Requester Support: Not supported
-1 = TWT Responder Support: Supported
-0 = Fragmentation Support: No support for dynamic frag
-000 = Reserved: 0x0
-100 = Reserved: 0x0
-10 = Trigger Frame MAC Padding Duration: 2
-000 = Multi-TID Aggregation Support: 0
-00 = HE Link Adaptation Support: No feedback if the STA
-0 = All Ack Support: Not supported
-0 = TRS Support: Not supported
-1 = BSR Support: Supported
-0 = Broadcast TWT Support: Not supported
-0 = 32-bit BA Bitmap Support: Not supported
-0 = MU Cascading Support: Not supported
-0 = Ack-Enabled Aggregation Support: Not supported
-0 = Reserved: 0x0
-1 = OM Control Support: Supported
-1 = OFDMA RA Support: Supported
-01 = Maximum A-MPDU Length Exponent Extension: 1
-0 = A-MSDU Fragmentation Support: Not supported
-0 = Flexible TWT Schedule Support: Not supported
-0 = Rx Control Frame to MultiBSS: Not supported
-0 = BSRP BQRP A-MPDU Aggregation: Not supported
-0 = QTP Support: Not supported
-0 = BQR Support: Not supported
-0 = SRP Responder Role: Not supported
-0 = NDP Feedback Report Support: Not supported
-0 = OPS Support: Not supported
-0 = A-MSDU in A-MPDU Support: Not supported
-000 = Multi-TID Aggregation TX Support: 0
-0 = HE Subchannel Selective Transmission Support: Not
-1 = UL 2x996-tone RU Support: Supported
-1 = OM Control UL MU Data Disable RX Support: Supporte
-0 = HE Dynamic SM Power Save: Not supported
-1 = Punctured Sounding Support: Supported

	<pre> ▼ HE Phy Capabilities Information ▶0 = Reserved: 0x0 ▼ 0000 110. = Channel Width Set: 0x06 0. = 40MHz in 2.4GHz band: Not supported 1.. = 40 & 80MHz in the 5GHz band: Supported 1... = 160MHz in the 5GHz band: Supported ...0 = 160/80+80MHz in the 5GHz band: Not supported ..0. = 242 tone RUs in the 2.4GHz band: Not supported .0... = 242 tone RUs in the 5GHz band: Not supported 0... = Reserved: 0x0 ▶ Bits 8 to 23: 0x4e2f ▶ Bits 24 to 39: 0x6fc9 ▶ Bits 40 to 55: 0x27c9 ▶ Bits 56 to 71: 0x01de ▶ Bits 72 to 87: 0x008f ... ▼ Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0) Tag Number: Element ID Extension (255) Ext Tag length: 6 Ext Tag Number: HE Operation (IEEE Std 802.11ax/D3.0) (36) ▶ HE Operation Parameters: 0x003fe4 ▶ BSS Color Information: 0x01 ▶ Basic HE-MCS and NSS Set: 0x1ffc </pre> <p>Tomar en cuenta los filtros para wlan.</p> <pre> Filter for all management frames: wlan.fc.type == 0 Filter for Association Requests: wlan.fc.type_subtype == 0 Filter for Association Responses: wlan.fc.type_subtype == 1 Filter for Reassociation Requests: wlan.fc.type_subtype == 2 Filter for Reassociation Responses: wlan.fc.type_subtype == 3 Filter for Probe Requests: wlan.fc.type_subtype == 4 Filter for Probe Responses: wlan.fc.type_subtype == 5 Filter for Beacons: wlan.fc.type_subtype == 8 Filter for ATIMs: wlan.fc.type_subtype == 9 Filter for Disassociations: wlan.fc.type_subtype == 10 Filter for Authentications: wlan.fc.type_subtype == 11 Filter for Deauthentications: wlan.fc.type_subtype == 12 Filter for Actions: wlan.fc.type_subtype == 13 </pre>
Resultados:	<ul style="list-style-type: none"> • Explicar en qué consiste cada una de las características presentes en las tramas 802.11ax • Verificar que son tramas 802.11ax • Realizar un sondeo de la red, encontrar todo el proceso de las tramas de gestión. • Analizar cada una de las tramas presentes en la comunicación.
Conclusiones:	Escribir 5 conclusiones sobre la práctica
Recomendaciones	Escribir 5 recomendaciones sobre la práctica
Bibliografía:	Indicar la bibliografía utilizada para la práctica.

CONCLUSIONES

La tecnología 802.11ax presenta importantes mejoras en términos de eficiencia y rendimiento respecto a 802.11ac. Entre las nuevas características de esta tecnología se encuentran la modulación OFDMA, TWT, 1024-QAM y WPA3, que permiten un mayor ancho de banda, una mayor capacidad de usuarios y una mayor eficiencia energética.

La tecnología 802.11ax es una de las tecnologías inalámbricas con mayor crecimiento en la actualidad, gracias a su capacidad de adaptación a diferentes modos de red (ad-hoc, infraestructura y mallada), su alta velocidad de transferencia de datos y su bajo consumo de energía.

La combinación de la tecnología 802.11ax con plataformas SBC como las Raspberry Pi en su versión CM4 permite crear redes en varios modos, lo que amplía las posibilidades de análisis en campos relacionados con el acceso, la gestión y la transmisión de datos.

La investigación realizada para esta tesis permite comprender en detalle las características y funcionamiento de la tecnología 802.11ax, así como los parámetros necesarios para medir su rendimiento y su implementación en un banco de pruebas. Estos conocimientos resultan fundamentales para el diseño y la implementación de redes inalámbricas eficientes y de alta calidad.

En conclusión, la tecnología 802.11ax representa un gran avance en el campo de las comunicaciones inalámbricas, gracias a sus mejoras en términos de eficiencia, velocidad y capacidad de usuarios. Su combinación con plataformas SBC como las Raspberry Pi permite una gran variedad de aplicaciones, y su investigación y análisis son fundamentales para el diseño de redes de alta calidad en diferentes entornos.

RECOMENDACIONES

A medida que la tecnología 802.11ax sigue evolucionando, es importante mantenerse actualizado con las últimas innovaciones y mejoras. Mantenerse informado sobre los desarrollos más recientes y sus aplicaciones potenciales puede ayudar a los ingenieros de redes y telecomunicaciones a mejorar su capacidad de diseño e implementación de redes inalámbricas.

Dado que la tecnología 802.11ax es compatible con múltiples modos de red, es importante evaluar cuidadosamente qué modo de red es el más adecuado para una aplicación determinada. Los modos de red ad-hoc, infraestructura y mallada tienen diferentes requisitos y beneficios, y seleccionar el modo adecuado puede ser crucial para el éxito de una implementación de red.

La tecnología 802.11ax se beneficia de una serie de características de hardware y software, incluyendo placas SBC como las Raspberry Pi. En el diseño de redes se debe evaluar cuidadosamente qué hardware y software son los más adecuados para su aplicación específica, con el fin de aprovechar al máximo las capacidades de la tecnología.

La seguridad sigue siendo un problema importante en las redes inalámbricas, y la tecnología 802.11ax no es una excepción. Hay que ser conscientes de los riesgos de seguridad asociados con la tecnología, y tomar medidas para proteger los datos y la infraestructura de red. La implementación de características de seguridad como WPA3 es esencial para proteger los datos de los usuarios y garantizar la privacidad de estos.

REFERENCIAS

- Bellalta, B., & Kosek-Szott, K. (2019). AP-initiated multi-user transmissions in IEEE 802.11ax WLANs. *Ad Hoc Networks*, 85, 145–159. <https://doi.org/https://doi.org/10.1016/j.adhoc.2018.10.021>
- Buy a Compute Module 4 IO Board – Raspberry Pi.* (n.d.). Retrieved August 10, 2021, from <https://www.raspberrypi.org/products/compute-module-4-io-board/>
- CAPÍTULO 1: INTRODUCCIÓN A LAS REDES INALÁMBRICAS 1.1 Introducción.* (n.d.).
- Chico, J. C., Mejía, D., & Bernal, I. (2013). Implementación de un prototipo de una Red Definida por Software (SDN) empleando una solución basada en hardware. *Escuela Politécnica Nacional, Quito, Ecuador.*
- CWNA_Certified_Wireless_Network_Administ.* (n.d.).
- Eduardo, I. J., & Rodriguez, C. (2018). *Implementación de un prototipo de sistema de comunicación inalámbrico OFD en SDR.*
- González González, F., Calero Castañeda, S. L., & others. (2019). *Comparación de las metodologías cascada y ágil para el aumento de la productividad en el desarrollo de software.* Universidad Santiago de Cali.
- Grupo de Nuevas Actividades Profesionales (NAP) del COIT. (2004). *La situación de las tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes (“Wi-Fi”).*
- Guayaquil, R. (2018). *Diseño de una GUI en MATLAB para evaluar técnicas de modulación de amplitud en cuadratura (QAM).*

Gutierrez, O. E. (2020). *Comunicaciones móviles y redes inalámbricas*. Jorge Sarmiento Editor - Universitos.

Horno Anguís, J. J. (2008). *Redes de Área Local Inalámbricas: Diseño de la WLAN de Wheelers Lane Technology College*.

IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2021). In *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)* (pp. 1–4379). <https://doi.org/10.1109/IEEESTD.2021.9363693>

IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Ame. (2021). In *IEEE Std 802.11ax-2021 (Amendment to IEEE Std 802.11-2020)* (pp. 1–767). <https://doi.org/10.1109/IEEESTD.2021.9442429>

IEEE Standard for Information technology--Telecommunications and information exchange between systems—Local and metropolitan area networks--Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--A. (2013). In *IEEE Std 802.11ac(TM)-2013 (Amendment to IEEE Std 802.11-2012, as amended by IEEE Std 802.11ae-2012, IEEE Std 802.11aa-2012, and IEEE Std 802.11ad-2012)* (pp. 1–425). <https://doi.org/10.1109/IEEESTD.2013.7797535>

- Islam, G. Z., & Kashem, M. A. (2018). An OFDMA-based New MAC Mechanism for IEEE 802.11ax. *2018 5th International Conference on Networking, Systems and Security (NSysS)*, 1–7. <https://doi.org/10.1109/NSysS.2018.8631367>
- Jiménez, L., Parrado, J., Quiza, C., & Suárez, C. (2001). Modulación multiportadora OFDM. In *Ingeniería, ISSN-e 0121-750X, Vol. 6, N°. 2, 2001, págs. 30-34* (Vol. 6, Issue 2). Universidad Distrital Francisco José de Caldas.
- José, J., & Torres, Y. (n.d.-a). *CAPÍTULO 4 LA CAPA FÍSICA 4.1 INTRODUCCIÓN*.
- José, J., & Torres, Y. (n.d.-b). *CAPÍTULO 5 LA CAPA MAC 5.1 INTRODUCCIÓN*.
- Lederkremer, M. (2019). *Redes Informáticas* (RedUsers, Ed.).
- Lee, K.-H. (2019). Using OFDMA for MU-MIMO User Selection in 802.11ax-Based Wi-Fi Networks. *IEEE Access*, 7, 186041–186055. <https://doi.org/10.1109/ACCESS.2019.2960555>
- Martínez, G., Dirigido, P., Luis Gómez, J., Codirigido, T., Carlos, J., & Aarnoutse Sánchez, J. (n.d.). *Punto de Acceso WiFi Inteligente con Antena de tipo Leaky-Wave y Esquema de Salto en Frecuencia*.
- Mosquera Chica, Á. L. (2019). *Estudio y análisis de las nuevas tecnologías 802.11 ax y 5G para el desarrollo del internet de las cosas*.
- Nayak, P. (2021). *Study of MU-MIMO Performance Under Variable Traffic*. <https://doi.org/10.13140/RG.2.2.21823.84648>
- NVIDIA Jetson Nano Developer Kit | NVIDIA Developer*. (n.d.). Retrieved August 10, 2021, from <https://developer.nvidia.com/embedded/jetson-nano-developer-kit>

¿Qué es Wi-Fi 6? [Básico] / Cuadrado Técnico / Marubun. (n.d.). Retrieved December 4, 2021, from <https://www.marubun.co.jp/service/technicalsquare/a7ijkd000000mzqv.html>

Quiénes somos / Alianza Wi-Fi. (n.d.). Retrieved June 17, 2021, from <https://www.wifi.org/who-we-are>

Ricardo, Y., & Jijón, P. S. (2002). *SOLUCIÓN SPREAD SPECTRUM PARA UNA RED MÓVIL DE DATOS EN LAS ÁREAS ABIERTAS DEL CAMPUS POLITÉCNICO*.

Salazar, J. (n.d.). REDES INALÁMBRICAS. *TechPedia*, 40.

Suárez Zambrano, W. R. (2022). Observatorio de radio comunicaciones para el análisis del espectro radio eléctrico en la zona 1 del Ecuador [Tesis de maestría, Universidad Técnica del Norte]. Recuperado de <http://repositorio.utn.edu.ec/handle/123456789/11917>

Torres, I. (2021). *Análisis y simulación del estándar 802.11 ax para evaluar el rendimiento de despliegues WLAN en escenarios con tráfico de red elevado*. Riobamba, Universidad Nacional de Chimborazo.

Unda, C., & Jaramillo, F. (2004). *Diseño e implementación de una red de comunicaciones tipo espectro ensanchado como solución de última milla para Andinanet*. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

What is BSS Color in 802.11ax? Background, Definition, Set-up. (n.d.). Retrieved August 10, 2021, from <https://www.extremenetworks.com/extreme-networks-blog/what-is-bss-color-in-802-11ax/>

Wi-Fi 6 Technology and Evolution White Paper. (2020a).

Wi-Fi 6 Technology and Evolution White Paper. (2020b).

ANEXOS

- **ANEXOS A:** Datasheets de los equipos utilizados en el desarrollo del proyecto.

Anexo A1: Raspberry CM4

El datasheet se lo puede encontrar en la página principal de raspberry o a través del siguiente enlace: <https://datasheets.raspberrypi.com/cm4/cm4-datasheet.pdf>

Anexo A2: Intel AX200

Las especificaciones del producto se pueden obtener en la página de Intel o en el siguiente enlace: <https://ark.intel.com/content/www/us/en/ark/products/189347/intel-wifi-6-ax200-gig.html>

- **ANEXOS B:** Configuración de las herramientas para el análisis de las redes.

Anexo B1: Instalación y configuración de D-ITG.

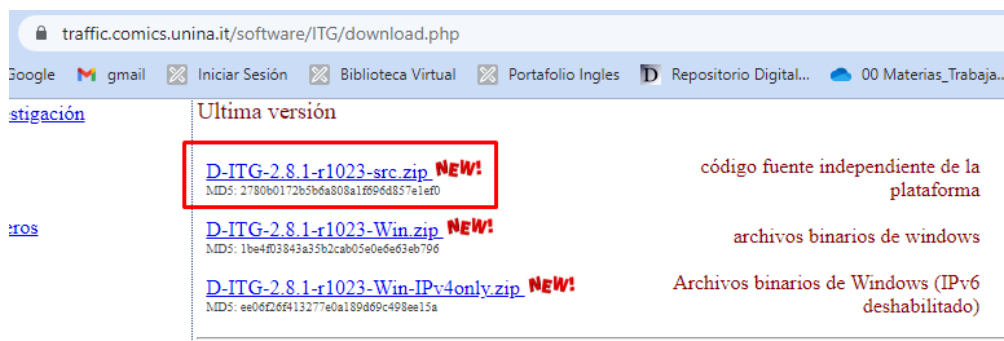
8. Primero se ingresa al siguiente enlace y se descarga el archivo que se indica en la figura

126

<https://traffic.comics.unina.it/software/ITG/download.php>

Figura 126

Página para descargar D-ITG

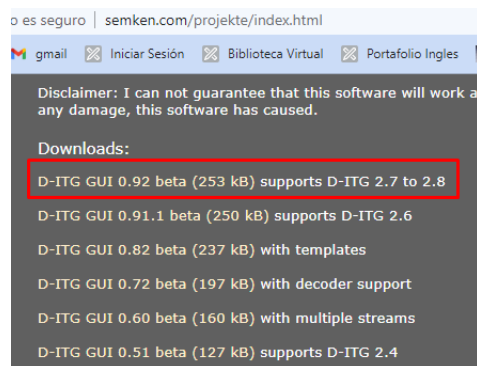


9. Una vez descargado se descomprime en el directorio de su preferencia, se ingresa en la carpeta con el comando **“cd D-ITG-2.8.1-r1023/src”** y por último se construye el binario con el comando **“make”**.
10. Para poder trabajar de mejor manera se instala la GUI del programa, para esto se ingresa a la siguiente página y se descarga el archivo que se indica en la figura 127

<http://www.semken.com/projekte/index.html>

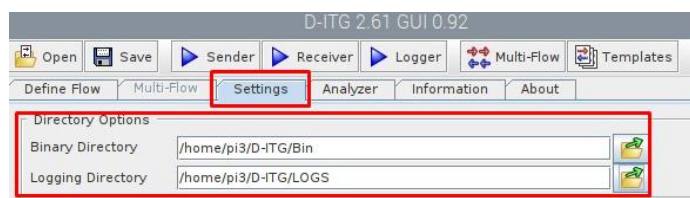
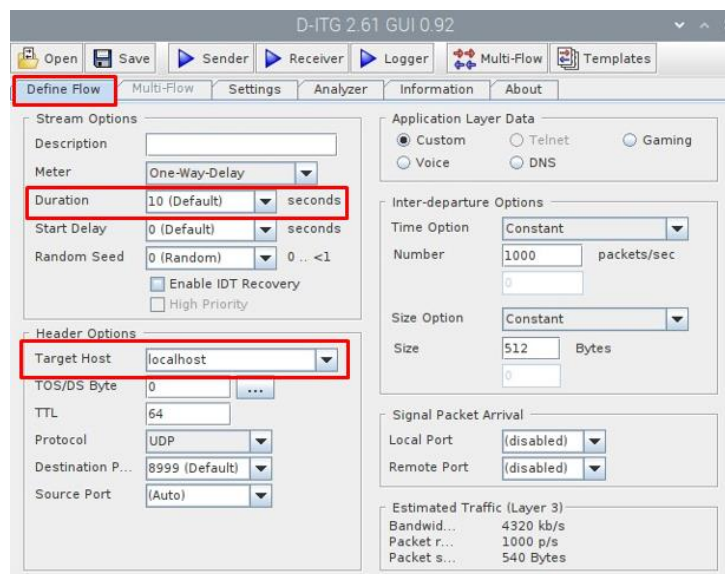
Figura 127

Descarga de la GUI de D-ITG



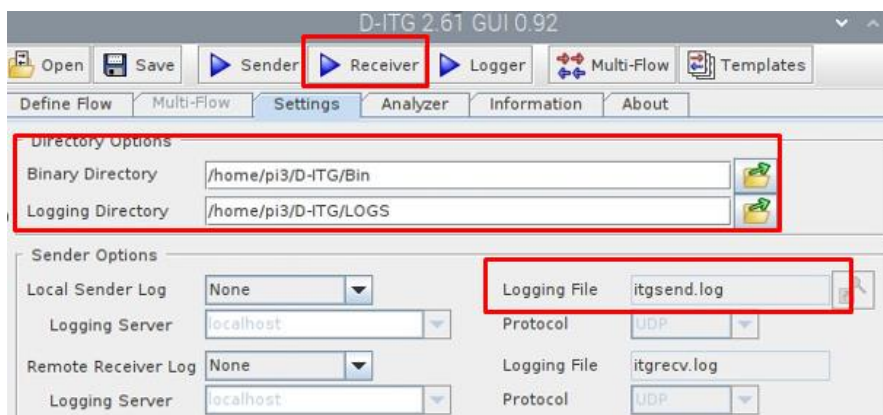
11. Se crea una carpeta que se llame D-ITG, y dentro de esta se descomprime el archivo.
12. Se ingresa a la carpeta con el comando **“cd D-ITG”**, dentro de este directorio se escribe el siguiente comando para ejecutar el programa **“sudo java -jar ITGGUI.jar”**.
13. Para la configuración del programa se debe configurar tanto en el transmisor como en el receptor, los principales parámetros a configurar en el transmisor son el host de destino, la duración, y la ubicación de los archivos binarios y de log.

Figura 128
Configuración de transmisor



14. Y para el receptor hay que indicar la ubicación para los archivos binarios y logs, además de indicar que se va a recibir tráfico.

Figura 129
Configuración del receptor

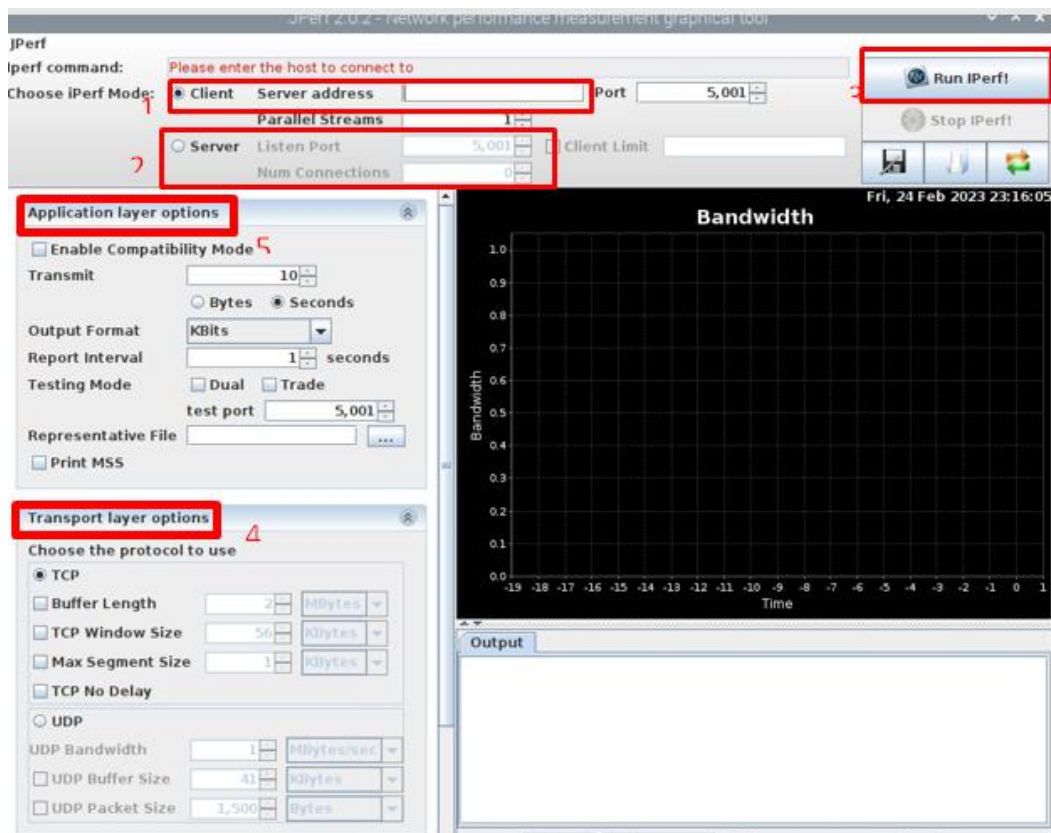


Anexo B2: Instalación de iperf y jperf.

6. Primero, antes de instalar iperf y jperf es necesario que en el sistema tenga instalado java, para esto se utiliza el comando **“sudo apt install default-jdk”**
7. A continuación, se instala iperf, esto mediante los siguientes comandos **“sudo apt-get install iperf”**, **“sudo apt-get install iperf3”**.
8. Ahora, se debe descargar jperf, para esto se dirige a la página <https://www.telectronika.com/descargas/jperf/>
9. Una vez descargado se descomprime en el directorio de preferencia, se ingresa a la carpeta y mediante el siguiente comando se ejecuta el programa **“sh jperf.sh”**
10. A continuación, se detalla los principales parámetros a configurar jperf.

Figura 130

Pantalla principal de jPerf



- 6) Client: se especifica que el nodo estará como cliente, además se especificará la ip del servidor.
- 7) Server: Especifica que el nodo estará como servidor.
- 8) Run iPerf: Permite correr el programa para que empiece a enviar o recibir datos.
- 9) Transport layer options: Determina el tipo de protocolo de transporte, ya sea TCP o UDP
- 10) Application layer options: Permite configurar parámetros como el tiempo de envío de datos, el intervalo y el formato de envío.

Anexo B3: Configuración del analizador de espectro.

1. Una vez conectado y encendido el dispositivo, se abre un terminal y se verifica la conexión con Adalm-pluto SDR, esto mediante el comando ping a la ip “192.168.2.10”.

Figura 131

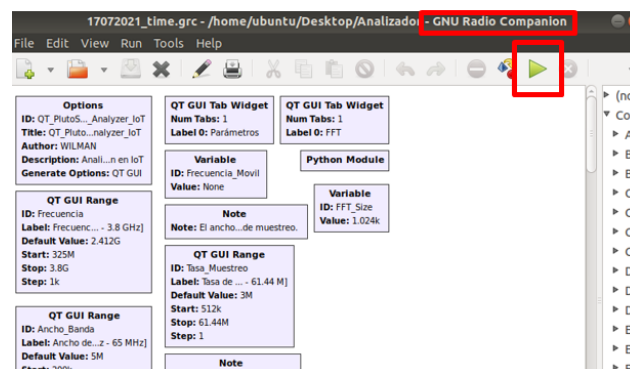
Verificar conexión a Adalm-Pluto SDR

```
ubuntu@ubuntu:~$ ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data:
64 bytes from 192.168.2.10: icmp_seq=1 ttl=64 time=0.086 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=64 time=0.124 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=64 time=0.126 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=64 time=0.123 ms
```

2. A continuación, se abre el programa GNU Radio Companion, y se procede a ejecutar el analizador.

Figura 132

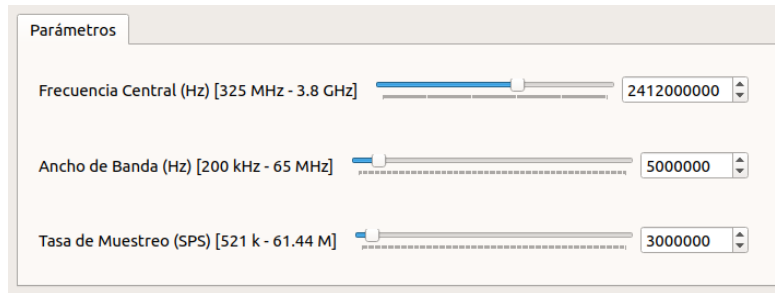
Pantalla de GNU Radio Companion



- Ahora, dependiendo de la aplicación se debe configurar la frecuencia central, el ancho de banda y la tasa de muestreo.

Figura 133

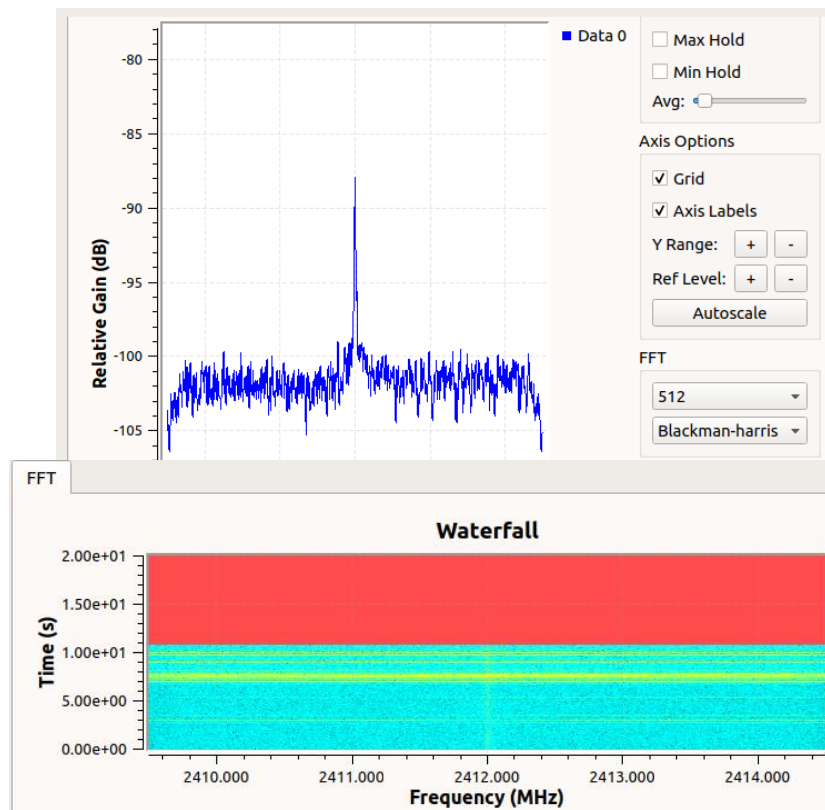
Parámetros para el análisis espectral



- Una vez realizado la configuración se puede observar las diferentes graficas que presenta el programa, para el posterior análisis.

Figura 134

Graficas de las señales obtenidas (FFT y mapa de calor)



Anexo B4: Instalación de wireshark.

Antes de instalar wireshark se necesita un sistema Operativo Linux, para el caso Raspbian, además que la tarjeta inalámbrica ax esté funcionando correctamente y además permita operar en modo monitor.

Primero se debe actualizar el sistema, para esto se utiliza los siguientes comandos:

```
$ sudo apt-get update -y  
$ sudo apt-get upgrade -y
```

Una vez realizado este procedimiento, a continuación, se debe actualizar el kernel a una versión mayor a 5.1, para esto utilice el comando **\$ uname -a** para verificar la versión, si la versión esta desactualizada actualícela.

Ahora, se debe configurar para que la tarjeta capture en modo monitor, permitiendo así tramas 802.11, para esto se debe seguir los siguientes comandos:

```
$ sudo apt-get install aircrack-ng  
$ sudo airmon-ng start wlan0  
$ monitor mode enabled on mon0
```

Una vez aplicado estos comandos si todo esta correcto deberá aparecer una interfaz con el nombre mon0. Esta interfaz es la que se utilizara para capturar.

Por último, se debe instalar wireshark en su versión más reciente para que permita la especificación 802.11ax., para esto se sigue los siguientes comandos.


```
$ sudo add-apt-repository ppa:wireshark-dev/stable  
$ sudo apt update  
$ sudo apt -y install wireshark  
$ sudo apt -y install wireshark-qt
```

Para instalar una versión de desarrollo se procede con los siguientes comandos:

```
$ sudo add-apt-repository ppa:dreibh/ppa  
$ sudo apt update  
$ sudo apt -y install wireshark
```

Finalmente abrimos wireshark con el comando **\$sudo wireshark** y se verifica si captura marcos 802.11ax.

- **ANEXOS C:** Tablas MCS de 802.11ax

MCS también denominada índice de esquema de codificación y modulación es el que define la transmisión máxima con la que los nodos pueden comunicarse. Para 802.11ax utiliza High Efficiency (HE).

Anexo C1: Tabla de MCS con OFDM

Figura 135
Tabla MCS con OFDM

MCS Index	Spatial Stream	Modulation	Coding	OFDM (802.11ax)											
				20MHz			40MHz			80MHz			160MHz		
				0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI
0	1	BPSQ	1/2	8.6	8.1	7.3	17.2	16.3	14.6	36.0	34.0	30.6	72.1	68.1	61.3
1	1	QPSK	1/2	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	144.1	136.1	122.5
2	1	QPSK	3/4	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	216.2	204.2	183.8
3	1	16-QAM	1/2	34.4	32.5	29.3	68.8	65.0	58.5	144.1	136.1	122.5	288.2	272.2	245.0
4	1	16-QAM	3/4	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
5	1	64-QAM	2/3	68.8	65.0	58.5	137.6	130.0	117.0	288.2	272.2	245.0	576.5	544.4	490.0
6	1	64-QAM	3/4	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	648.5	612.5	551.3
7	1	64-QAM	5/6	86.0	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3	720.6	680.6	612.5
8	1	256-QAM	3/4	103.2	97.5	87.8	206.5	195.0	175.5	432.4	408.3	367.5	864.7	816.7	735.0
9	1	256-QAM	5/6	114.7	108.3	97.5	229.4	216.7	195.0	480.4	453.7	408.3	960.8	907.4	816.7
10	1	1024-QAM	3/4	129.0	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4	1080.9	1020.8	918.8
11	1	1024-QAM	5/6	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4	1201.0	1134.3	1020.8
0	2	BPSQ	1/2	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	144.1	136.1	122.5
1	2	QPSK	1/2	34.4	32.5	29.3	68.8	65.0	58.5	144.1	136.1	122.5	288.2	272.2	245.0
2	2	QPSK	3/4	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
3	2	16-QAM	1/2	68.8	65.0	58.5	137.6	130.0	117.0	288.2	272.2	245.0	576.5	544.4	490.0
4	2	16-QAM	3/4	103.2	97.5	87.8	206.5	195.0	175.5	432.4	408.3	367.5	864.7	816.7	735.0
5	2	64-QAM	2/3	137.6	130.0	117.0	275.3	260.0	234.0	576.5	544.4	490.0	1152.9	1088.9	980.0
6	2	64-QAM	3/4	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3	1297.1	1225.0	1102.5
7	2	64-QAM	5/6	172.1	162.5	146.3	344.1	325.0	292.5	720.6	680.6	612.5	1441.2	1361.1	1225.0
8	2	256-QAM	3/4	206.5	195.0	175.5	412.9	390.0	351.0	864.7	816.7	735.0	1729.4	1633.3	1470.0
9	2	256-QAM	5/6	229.4	216.7	195.0	458.8	433.3	390.0	960.8	907.4	816.7	1921.6	1814.8	1633.3
10	2	1024-QAM	3/4	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8	2161.8	2041.7	1837.5
11	2	1024-QAM	5/6	286.8	270.8	243.8	573.5	541.7	487.5	1201.0	1134.3	1020.8	2402.0	2268.5	2041.7
0	3	BPSQ	1/2	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	216.2	204.2	183.8
1	3	QPSK	1/2	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
2	3	QPSK	3/4	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	648.5	612.5	551.3
3	3	16-QAM	1/2	103.2	97.5	87.8	206.5	195.0	175.5	432.4	408.3	367.5	864.7	816.7	735.0
4	3	16-QAM	3/4	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3	1297.1	1225.0	1102.5
5	3	64-QAM	2/3	206.5	195.0	175.5	412.9	390.0	351.0	864.7	816.7	735.0	1729.4	1633.3	1470.0
6	3	64-QAM	3/4	232.3	219.4	197.4	464.6	438.8	394.9	972.8	918.8	826.9	1945.6	1837.5	1653.8
7	3	64-QAM	5/6	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8	2161.8	2041.7	1837.5
8	3	256-QAM	3/4	309.7	292.5	263.3	619.4	585.0	526.5	1297.1	1225.0	1102.5	2594.1	2450.0	2205.0
9	3	256-QAM	5/6	344.1	325.0	292.5	688.2	650.0	585.0	1441.2	1361.1	1225.0	2882.4	2722.2	2450.0
10	3	1024-QAM	3/4	387.1	365.6	329.1	774.3	731.3	658.1	1621.3	1531.3	1378.1	3242.6	3062.5	2756.3
11	3	1024-QAM	5/6	430.1	406.3	365.6	860.3	812.5	731.3	1801.5	1701.4	1531.3	3602.9	3402.8	3062.5

Nota: Tomado de <https://semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates/>

Anexo C2: Tabla de MCS con OFDMA

MCS Index	Spatial Stream	Modulation	Coding	MU-OFDMA (802.11ax)																	
				26-tone RU			52-tone RU			106-tone RU			242-tone RU			484-tone RU			996-tone RU		
				0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI
0	1	BPSQ	1/2	0.9	0.8	0.8	1.8	1.7	1.5	3.8	3.5	3.2	8.6	8.1	7.3	17.2	16.3	14.6	36.0	34.0	30.6
1	1	QPSK	1/2	1.8	1.7	1.5	3.5	3.3	3.0	7.5	7.1	6.4	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
2	1	QPSK	3/4	2.6	2.5	2.3	5.3	5.0	4.5	11.3	10.6	9.6	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9
3	1	16-QAM	1/2	3.5	3.3	3.0	7.1	6.7	6.0	15.0	14.2	12.8	34.4	32.5	29.3	68.8	65.0	58.5	144.1	136.1	122.5
4	1	16-QAM	3/4	5.3	5.0	4.5	10.6	10.0	9.0	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
5	1	64-QAM	2/3	7.1	6.7	6.0	14.1	13.3	12.0	30.0	28.3	25.5	68.8	65.0	58.5	137.6	130.0	117.0	288.2	272.2	245.0
6	1	64-QAM	3/4	7.9	7.5	6.8	15.9	15.0	13.5	33.8	31.9	28.7	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6
7	1	64-QAM	5/6	8.8	8.3	7.5	17.6	16.7	15.0	37.5	35.4	31.9	86.0	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3
8	1	256-QAM	3/4	10.6	10.0	9.0	21.2	20.0	18.0	45.0	42.5	38.3	103.2	97.5	87.8	206.5	195.0	175.5	432.4	408.3	367.5
9	1	256-QAM	5/6	11.8	11.1	10.0	23.5	22.2	20.0	50.0	47.2	42.5	114.7	108.3	97.5	229.4	216.7	195.0	480.4	453.7	408.3
10	1	1024-QAM	3/4	13.2	12.5	11.3	26.5	25.0	22.5	56.3	53.1	47.8	129.0	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4
11	1	1024-QAM	5/6	14.7	13.9	12.5	29.4	27.8	25.0	62.5	59.0	53.1	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4
0	2	BPSQ	1/2	1.8	1.7	1.5	3.5	3.3	3.0	7.5	7.1	6.4	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
1	2	QPSK	1/2	3.5	3.3	3.0	7.1	6.7	6.0	15.0	14.2	12.8	34.4	32.5	29.3	68.8	65.0	58.5	144.1	136.1	122.5
2	2	QPSK	3/4	5.3	5.0	4.5	10.6	10.0	9.0	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
3	2	16-QAM	1/2	7.1	6.7	6.0	14.1	13.3	12.0	30.0	28.3	25.5	68.8	65.0	58.5	137.6	130.0	117.0	288.2	272.2	245.0
4	2	16-QAM	3/4	10.6	10.0	9.0	21.2	20.0	18.0	45.0	42.5	38.3	103.2	97.5	87.8	206.5	195.0	175.5	432.4	408.3	367.5
5	2	64-QAM	2/3	14.1	13.3	12.0	28.2	26.7	24.0	60.0	56.7	51.0	137.6	130.0	117.0	275.3	260.0	234.0	576.5	544.4	490.0
6	2	64-QAM	3/4	15.9	15.0	13.5	31.8	30.0	27.0	67.5	63.8	57.4	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3
7	2	64-QAM	5/6	17.6	16.7	15.0	35.3	33.3	30.0	75.0	70.8	63.8	172.1	162.5	146.3	344.1	325.0	292.5	720.6	680.6	612.5
8	2	256-QAM	3/4	21.2	20.0	18.0	42.4	40.0	36.0	90.0	85.0	76.5	206.5	195.0	175.5	412.9	390.0	351.0	864.7	816.7	735.0
9	2	256-QAM	5/6	23.5	22.2	20.0	47.1	44.4	40.0	100.0	94.4	85.0	229.4	216.7	195.0	458.8	433.3	390.0	960.8	907.4	816.7
10	2	1024-QAM	3/4	26.5	25.0	22.5	52.9	50.0	45.0	112.5	106.3	95.6	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8
11	2	1024-QAM	5/6	29.4	27.8	25.0	58.8	55.6	50.0	125.0	118.1	106.3	286.8	270.8	243.8	573.5	541.7	487.5	1201.0	1134.3	1020.8
0	3	BPSQ	1/2	2.6	2.5	2.3	5.3	5.0	4.5	11.3	10.6	9.6	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9
1	3	QPSK	1/2	5.3	5.0	4.5	10.6	10.0	9.0	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
2	3	QPSK	3/4	7.9	7.5	6.8	15.9	15.0	13.5	33.8	31.9	28.7	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6
3	3	16-QAM	1/2	10.6	10.0	9.0	21.2	20.0	18.0	45.0	42.5	38.3	103.2	97.5	87.8	206.5	195.0	175.5	432.4	408.3	367.5
4	3	16-QAM	3/4	15.9	15.0	13.5	31.8	30.0	27.0	67.5	63.8	57.4	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3
5	3	64-QAM	2/3	21.2	20.0	18.0	42.4	40.0	36.0	90.0	85.0	76.5	206.5	195.0	175.5	412.9	390.0	351.0	864.7	816.7	735.0
6	3	64-QAM	3/4	23.8	22.5	20.3	47.6	45.0	40.5	101.3	95.6	86.1	232.3	219.4	197.4	464.6	438.8	394.9	972.8	918.8	826.9
7	3	64-QAM	5/6	26.5	25.0	22.5	52.9	50.0	45.0	112.5	106.3	95.6	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8
8	3	256-QAM	3/4	31.8	30.0	27.0	63.5	60.0	54.0	135.0	127.5	114.8	309.7	292.5	263.3	619.4	585.0	526.5	1297.1	1225.0	1102.5
9	3	256-QAM	5/6	35.3	33.3	30.0	70.6	66.7	60.0	150.0	141.7	127.5	344.1	325.0	292.5	688.2	650.0	585.0	1441.2	1361.1	1225.0
10	3	1024-QAM	3/4	39.7	37.5	33.8	79.4	75.0	67.5	168.8	159.4	143.4	387.1	365.6	329.1	774.3	731.3	658.1	1621.3	1531.3	1378.1
11	3	1024-QAM	5/6	44.1	41.7	37.5	88.2	83.3	75.0	187.5	177.1	159.4	430.1	406.3	365.6	860.3	812.5	731.3	1801.5	1701.4	1531.3

Nota: Tomado de <https://semfionetworks.com/blog/mcs-table-updated-with-80211ax-data-rates/>

ANEXO D: Encuestas**Anexo D1: Encuesta dirigida a los docentes de la materia.**

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS
CARRERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

Encuesta dirigida a los docentes encargados de la materia de comunicación inalámbrica de la Carrera de Telecomunicaciones de la Universidad Técnica del Norte.

La siguiente encuesta tiene como objetivo recopilar información que permita establecer los principales requerimientos en cuanto al diseño del tesbed para la tecnología 802.11ax, estos requerimientos estarán enfocados en conocer la dimensión del tesbed, los equipos necesarios y las principales pruebas a realizar.

Por su tiempo y apoyo le estamos agradecidos.

1. ¿Cree usted que es necesario implementar en la materia de comunicación inalámbrica laboratorios prácticos de nuevas tecnologías como es 802.11ax?

	SI
	NO
	TALVEZ

2. 802.11ax al ser una nueva tecnología. ¿Cree usted que es importante que el manejo del tesbed sea flexible y sencillo?

	SI
	NO
	TALVEZ

3. ¿La integración y tamaño de los componentes del tesbed deben ser?

	PEQUEÑOS
	MEDIANOS
	GRANDES

4. El tesbed debe ser acorde al entorno de pruebas, es decir debe ser manejable en diferentes ámbitos.

	SI
--	----

<input type="checkbox"/>	NO
<input type="checkbox"/>	TALVEZ

5. Seleccione las arquitecturas en las que el tesbed debe operar.

<input type="checkbox"/>	AD-HOC
<input type="checkbox"/>	INFRAESTRUCTURA
<input type="checkbox"/>	MES

6. ¿Cree usted que es importante la implementación de un sniffer en el tesbed?

<input type="checkbox"/>	SI
<input type="checkbox"/>	NO
<input type="checkbox"/>	TALVEZ

7. 802.11ax al implementar nuevas tecnologías, cree usted que es importante que se estudie con un analizador de espectro.

<input type="checkbox"/>	SI
<input type="checkbox"/>	NO
<input type="checkbox"/>	TALVEZ

8. ¿Cree usted que el tesbed debe ser económicamente eficiente?

<input type="checkbox"/>	SI
<input type="checkbox"/>	NO
<input type="checkbox"/>	TAL VEZ

9. Indique que otras características podrían ser necesarias para añadir al tesbed.
