

# 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:**

**DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN WI-FI  
CENTRALIZADO, EN LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS,  
MEDIANTE ROUTEROS, PARA MEJORAR LA CALIDAD DE SERVICIO**

**AUTOR:**

**LÓPEZ ROSERO JHERMAN FREDDY**

**DIRECTOR:**

**ING. DANIEL JARAMILLO**

**IBARRA – ECUADOR**



**UNIVERSIDAD TÉCNICA DEL NORTE**  
**BIBLIOTECA UNIVERSITARIA**

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

### 1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

<b>DATOS DE CONTACTO</b>			
<b>CÉDULA DE IDENTIDAD:</b>	1002912390		
<b>APELLIDOS Y NOMBRES:</b>	LÓPEZ ROSERO JHERMAN FREDDY		
<b>DIRECCIÓN:</b>	AV. ELOY ALFARO 3-30 Y JULIO ZALDUMBIDE		
<b>EMAIL:</b>	jhermanlopez@hotmail.com		
<b>TELÉFONO FIJO:</b>	062642207	<b>TELÉFONO MÓVIL:</b>	0982291892
<b>DATOS DE LA OBRA</b>			
<b>TÍTULO:</b>	DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN WI-FI CENTRALIZADO, EN LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, MEDIANTE ROUTEROS, PARA MEJORAR LA CALIDAD DE SERVICIO.		
<b>AUTOR (ES):</b>	LÓPEZ ROSERO JHERMAN FREDDY		
<b>FECHA: AAAAMMDD</b>	2017/05/30		
SOLO PARA TRABAJOS DE GRADO			
<b>PROGRAMA:</b>	<input checked="" type="checkbox"/>	<b>PREGRADO</b>	<input type="checkbox"/> <b>POSGRADO</b>
<b>TÍTULO POR EL QUE OPTA:</b>	INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN		
<b>ASESOR /DIRECTOR:</b>	ING. DANIEL JARAMILLO		

## **2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD**

Yo, López Rosero Jherman Freddy, con cédula de identidad Nro. 1002912390, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

## **3. 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 30 días del mes de mayo de 2017

**EL AUTOR:**



Nombre: Jherman López



## UNIVERSIDAD TÉCNICA DEL NORTE

### **CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO**

#### **A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE**

Yo, López Rosero Jherman Freddy, con cédula de identidad Nro. 1002912390, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor (es) de la obra o trabajo de grado denominado: DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN WI-FI CENTRALIZADO, EN LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, MEDIANTE ROUTEROS, PARA MEJORAR LA CALIDAD DE SERVICIO, que ha sido desarrollado para optar por el título de: INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, a los 30 días del mes de mayo de 2017

Nombre: Jherman López

Cédula: 1002912390

## DECLARATORIA DE AUTENTICIDAD

Yo, López Rosero Jherman Freddy, con cedula de identidad 1002912390, declaro que los resultados obtenidos en esta investigación que presento, previo la obtención del título de Ingeniero en Electrónica y Redes de Comunicación son originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones, los efectos legales y académicos que se desprenden del trabajo de investigación y luego de la redacción de este documento son y serán de mi sola y exclusiva responsabilidad legal y académica.



López Rosero, Jherman Freddy

C.I. 1002912390



**UNIVERSIDAD TÉCNICA DEL NORTE**  
**FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS**

**CERTIFICACIÓN**

Ing. Daniel Jaramillo Director de Trabajo de Grado desarrollado por el señor Estudiante

**JHERMAN FREDDY LÓPEZ ROSERO**

**CERTIFICA**

Que, el Proyecto de Trabajo de grado titulado “Diseño e implementación de un sistema de gestión wi-fi centralizado, en la facultad de ingeniería en ciencias aplicadas, mediante routers, para mejorar la calidad de servicio.” Ha sido elaborado en su totalidad por el señor estudiante Jherman Freddy López Rosero bajo mi dirección para la obtención del título de Ingeniero en Electrónica y Redes de Comunicación. Luego de ser revisada, considerando que se encuentra concluido y cumple con las exigencias y requisitos académicos de la Facultad de Ingeniería en Ciencias Aplicadas, Carrera de Ingeniería en Electrónica y Redes de Comunicación, autorizo su presentación y defensa para que pueda ser juzgado por el tribunal correspondiente.

A handwritten signature in blue ink, which appears to read "D. Jaramillo". The signature is written over a horizontal line that has a decorative, wavy pattern.

**ING. DANIEL JARAMILLO**  
**DIRECTOR DE TESIS**

**DEDICATORIA**

Este proyecto está dedicado principalmente a mis padres que, gracias a su esfuerzo, perseverancia y disciplina diaria, me han permitido llegar a la culminación de mi carrera.

Jherman López

## **AGRADECIMIENTO**

En primer lugar, quiero agradecer a Dios, porque gracias a su bendición he podido llegar a este logro.

Mediante la presente, quiero extender mis más sinceros agradecimientos a mis padres, hermanos, docentes y todas aquellas personas que directa o indirectamente, han hecho posible terminar este proyecto y a la vez mi carrera.

También debo agradecer a los ingenieros Daniel Jaramillo, Fernando Garrido, Mauricio Domínguez, Carlos Vásquez y Fabián Cuzme que, gracias a su apoyo incondicional y a sus críticas constructivas, he podido llegar a la culminación de este proyecto.

Jherman López



## RESUMEN

En este proyecto se detalla la implementación de un sistema de red Wi-Fi centralizada, mediante una topología de red tipo estrella y basada en RouterOS, en los interiores del edificio de la FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS (FICA), de la UNIVERSIDAD TECNICA DEL NORTE, ciudad de Ibarra, provincia de Imbabura, esta red permite acceso a sitios web y contenidos de la internet a estudiantes, docentes, administrativos, autoridades e invitados, a través de dispositivos móviles como: laptops, celulares y computadores con interfaces inalámbricas que soporten los estándares IEEE 802.11 b/g/n.

Este sistema está basado en las prestaciones del sistema operativo RouterOS, mediante un servidor hotspot, el mismo que permite ejecutar administración centralizada y personalizada, para la asignación de recursos como: usuario, contraseña, ancho de banda y tiempo de conexión, según el tipo de usuario.

También, se hace uso de un portal cautivo personalizado, que brinda la interface de visual y de acceso a todos los usuarios que requieren acceder desde la red local hacia la red pública.

Finalmente, se implementa políticas de QoS estático, que permiten brindar prioridades y control de ancho de banda según el tipo de servicio requerido desde los usuarios dentro de la red interna.

Permitiendo de esta manera, solucionar el problema de congestión en el acceso a internet, que tenía la FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS (FICA).

## ABSTRACT

This project detailed the implementation of a system of network centralized Wi-Fi, using star topology and based on RouterOS, in the indoors of the FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS (FICA), in the city Ibarra, Imbabura province, this network allow access to websites and Internet contents to students, teachers, administrators, authorities and guests, through mobile devices as: laptops, mobile phones and computers with wireless interfaces IEEE 802.11 b / g / n.

This system is based on the performance of the RouterOS operating system, through the hotspot server; it allows running a centralized and personal administration, for assignment of resources such as: username, password, and bandwidth and connection time, depending on the type of user.

Also, it used a personalized captive portal that provides a visual interface and access to all users, who require access from the local network to the public network.

Finally, is implemented policy of static QoS, allowing priorities and bandwidth control depending on the type of service required by users within the internal network.

Allowing thus solve the problem of congestion in access to internet, in the indoors of FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS (FICA).

## INDICE GENERAL

AUTORIZACIÓN DE USO Y PUBLICACIÓN.....	ii
DECLARATORIA DE AUTENTICIDAD .....	v
DEDICATORIA.....	vii
AGRADECIMIENTO.....	viii
RESUMEN.....	ix
ABSTRACT .....	x
INDICE GENERAL.....	xi
ÍNDICE DE FIGURAS .....	xvii
ÍNDICE DE TABLAS .....	xxi
ÍNDICE DE ECUACIONES.....	xxii
<b>CAPITULO I.....</b>	<b>1</b>
1      Antecedentes.....	1
1.1    Tema .....	1
1.2    Definición del problema .....	1
1.3    Delimitación del problema .....	2
1.4    Objetivos.....	3
1.4.1  Objetivo general .....	3
1.4.2  Objetivos específicos .....	3
1.5    Justificación del proyecto .....	3
1.6    Alcance .....	4
<b>CAPITULO II .....</b>	<b>7</b>
2      Marco teórico.....	7

2.1	Tecnologías inalámbricas .....	7
2.1.1	Redes WPAN.....	8
2.1.2	Redes WMAN .....	9
2.1.3	Redes WWAN .....	10
2.1.4	Redes WLAN .....	10
2.1.4.1	Ventajas de una red WLAN.....	11
2.1.4.2	Desventajas de las redes WLAN.....	12
2.1.5	Redes Wi-Fi.....	12
2.1.6	Elementos de una red Wi-Fi .....	13
2.1.6.1	Punto de acceso.....	13
2.1.6.2	Controlador de puntos de acceso .....	14
2.1.6.3	Estación o CPE .....	14
2.1.6.4	Potencia y sensibilidad de recepción .....	15
2.1.6.5	Cobertura.....	17
2.1.6.6	Canales y frecuencias.....	18
2.2	Estándar IEEE 802.11 .....	20
2.2.1	Variantes de IEEE 802.11 .....	21
2.2.1.1	IEEE 802.11a .....	22
2.2.1.2	IEEE 802.11b.....	23
2.2.1.3	IEEE 802.11g.....	26
2.2.1.4	IEEE 802.11n.....	27
2.2.1.5	IEEE 802.11ac .....	30
2.3	Topologías de red .....	32

2.3.1	Topología de redes LAN .....	32
2.3.1.1	Topología tipo bus .....	33
2.3.1.2	Topología tipo estrella .....	34
2.3.1.3	Topología tipo anillo.....	35
2.3.1.4	Topología tipo árbol.....	36
2.3.2	Topología de redes WLAN.....	37
2.3.2.1	Red AD-HOC.....	37
2.3.2.2	Infraestructura .....	38
2.4	RouterOS Mikrotik .....	39
2.4.1	Introducción a Mikrotik.....	39
2.4.2	RouterOS .....	40
2.4.3	Configuración de RouterOS .....	41
2.5	Centralización de redes Wi-Fi .....	41
2.6	Gestión centralizada de redes Wi-Fi con CAPsMAN .....	44
2.6.1	Requerimientos de funcionamiento .....	45
2.7	Gestión de usuarios mediante Hotspot .....	45
2.7.1	Hotspot de Mikrotik.....	46
2.8	Calidad de servicio .....	47
2.8.1	Calidad de servicio con encolamiento PCQ .....	48
2.9	Criterios de diseño .....	49
2.9.1	Criterio de selección de canales.....	49
2.9.2	Adaptar el diseño a las instalaciones .....	51

2.9.3	Capacidad adecuada .....	51
2.9.4	Roaming WiFi (Movilidad) .....	52
CAPITULO III .....		55
3	Propuesta del proyecto.....	55
3.1	Situación actual de la red Wi-Fi de la FICA .....	55
3.1.1	Descripción geográfica .....	55
3.1.2	Situación tecnológica actual .....	56
3.1.2.1	Topología física y lógica de la red existente.....	56
3.1.2.2	Ubicación de los equipos de la red existente .....	57
3.1.2.3	Dispositivos de la red existente.....	60
3.1.3	Justificación de pruebas a la red existente.....	61
3.1.3.1	Prueba de velocidad con herramientas web .....	61
3.1.3.2	Descarga y reproducción de un video en el formato más básico de 144p .....	63
3.1.3.3	Prueba de envío y recepción de paquetes ICMP .....	63
3.1.3.4	Búsqueda del punto crítico de degradación de la red .....	64
3.2	Diseño del sistema de gestión Wi-Fi .....	66
3.2.1	Ubicación de equipos de la nueva red WiFi .....	66
3.2.2	Topologías física y lógica de la nueva red Wi-Fi.....	66
3.2.2.1	Topología física de la nueva red WiFi .....	67
3.2.2.2	Topología lógica de la nueva red WiFi.....	68
3.2.3	Gestión centralizada de los puntos de acceso .....	68
3.2.3.1	Routerboard RB1100AHx2 .....	68
3.2.3.2	Qpcom QP-1240R.....	70

3.2.4	Distribución de puntos de acceso .....	71
3.2.5	Cálculo de cobertura .....	75
3.2.5.1	Nivel de señal que llega al equipo receptor .....	75
3.2.6	Distribución de frecuencias de la nueva red WiFi.....	77
3.2.7	Análisis y selección de canales para la nueva red WiFi FICA.....	78
3.2.7.1	Selección de canales para la nueva red WiFi.....	78
3.2.8	Alternativas de diseño .....	82
3.2.8.1	Plataforma Mikrotik.....	82
3.2.8.2	Plataforma UNIFI de UBIQUITI.....	84
3.2.8.3	Plataforma D-Link .....	87
3.2.9	Comparativa de selección de la mejor tecnología .....	90
3.2.9.1	Sumario de resultados a la comparativa de selección.....	93
3.2.10	Selección la tecnología más adecuada.....	94
3.2.11	Análisis costo beneficio .....	97
3.3	Implementación del sistema de gestión Wi-Fi .....	101
3.3.1	Implementación .....	101
3.3.2	Configuración del servidor central, el RB1100AHx2 .....	102
3.3.3	Configuración de los puntos de acceso, los RBcAP2n.....	114
3.3.4	Implementación del CAPsMAN.....	121
3.3.5	Gestión y privilegios de usuarios.....	126
3.3.5.1	Activación del servidor hotspot .....	126
3.3.5.2	Configuración de los parámetros generales de hotspot.....	127
3.3.5.3	Configuración del método de autenticación al hotspot.....	128

3.3.5.4	Asignación de usuarios y privilegios mediante hotspot.....	129
3.3.6	Pruebas de funcionamiento nueva red WiFi.....	130
3.3.6.1	Prueba de funcionamiento con herramientas de la web.....	130
3.3.6.2	Prueba de con la herramienta ping.....	132
3.3.6.3	Prueba de reproducción de un video en 360p.....	134
3.3.6.4	Prueba de reproducción de un video en 480p.....	134
3.3.6.5	Prueba de reproducción de un video en HD (720p).....	135
3.3.6.6	Prueba de descarga de un paquete de datos de 372 MB.....	136
CAPITULO IV.....		137
4	Análisis de resultados.....	137
4.1	Calidad del servicio a nivel de usuarios finales.....	137
4.1.1	Historias de usuario.....	137
4.1.2	Pruebas de aceptación.....	140
CAPÍTULO V.....		143
5	Conclusiones y recomendaciones.....	143
5.1	Conclusiones.....	143
5.2	Recomendaciones.....	144
Glosario de Términos.....		145
Bibliografía.....		148
ANEXOS.....		153



## ÍNDICE DE FIGURAS

Figura 1. Tecnologías de redes inalámbricas. ....	7
Figura 2. Red inalámbrica de área local .....	10
Figura 3. Antenas, patrones y omnidireccional dipolo de radiación. Hardesty, G.....	17
Figura 4. Evolución y variantes de redes Wi-Fi.....	21
Figura 5. Lista de canales de radio frecuencia para 802.11b. ....	24
Figura 6. Esquema comparativo de velocidades 802.11n con tecnología MIMO. ....	28
Figura 7. Esquema de un sistema típico de transmisión MIMO 2x2. ....	29
Figura 8. Velocidad de estándar 802.11ac. ....	30
Figura 9. Topología de red tipo bus. Diseñado en GNS3. ....	33
Figura 10. Topología de red tipo estrella. ....	34
Figura 11. Topología de red tipo anillo.....	35
Figura 12. Topología de red tipo árbol.....	36
Figura 13. Topología de red tipo ad-hoc. ....	37
Figura 14. Topología de red tipo infraestructura.....	38
Figura 15. Esquema de Calidad de servicio usando encolamiento PCQ. ....	48
Figura 16. Relación de canales en el espectro de 2.4 GHz .....	49
Figura 17. Velocidad de datos vs. rango de cobertura .....	50
Figura 18. Interferencia co-canal .....	50
Figura 19. Diseño de rangos de cobertura.....	51
Figura 20. Roaming.....	53
Figura 21. Topología física de la red existente en la FICA.....	56
Figura 22. Topología lógica de la red existente en la FICA .....	57
Figura 23. Dispositivos de la red actual en la planta baja de la FICA .....	58
Figura 24. Dispositivos de la red actual en el segundo piso de la FICA.....	58

Figura 25. Dispositivos de la red actual en el tercer piso de la FICA .....	59
Figura 26. Dispositivos de la red actual en el tercer piso de la FICA .....	59
Figura 27. Medición de velocidad de transmisión con la herramienta speedof.me. ....	61
Figura 28. Test de velocidad en la red existente con AEPROVI. ....	62
Figura 29. Prueba de la red Wi-Fi reproduciendo de un video en 144p. ....	63
Figura 30. Estadística de tiempos y envió de paquetes ICMP sin saturación de canal. ....	64
Figura 31. Trazado de ruta al servidor DNS de Google. ....	65
Figura 32. Distribución de los puntos de acceso por cada piso de la FICA. ....	66
Figura 33. Topología física para la nueva red FICA. ....	67
Figura 34. Topología lógica para la nueva red FICA. ....	68
Figura 35. Vista frontal del router RB1100AHx2. ....	69
Figura 36. Switch QPCOM QP-1240R. ....	71
Figura 37. Plano bidimensional de planta baja FICA, con la distribución de APs. ....	72
Figura 38. Plano bidimensional del primer piso del edificio de la FICA. ....	72
Figura 39. Vista superior del segundo piso del Edificio FICA. ....	73
Figura 40. Vista superior del tercer piso con los tres APs instalados en el pasillo. ....	74
Figura 41. Vista superior del cuarto piso del edificio FICA. ....	74
Figura 42. Nivel de intensidad de la señal en la red ficawifi .....	77
Figura 43. Distribución de APs por piso, con canales y zonas de cobertura. ....	79
Figura 44. Escaneo de canales en el ambiente planta baja. ....	80
Figura 45. Escaneo de canales en el ambiente primer piso .....	80
Figura 46. Escaneo de canales en el ambiente segundo piso .....	81
Figura 47. Escaneo de canales en el ambiente tercer piso .....	81
Figura 48. Escaneo de canales en el ambiente cuarto piso. ....	82
Figura 49. Monitoreo de APs desde una plataforma UniFi. ....	86

Figura 50. Plataforma centralizada para redes Wi-Fi en la marca D-Link. ....	90
Figura 51. Sumario de la comparativa .....	93
Figura 52. Vista frontal de un cAP2n.....	94
Figura 53.Herramienta WinBox de Mikrotik.....	102
Figura 54. Ingreso a la interface de configuración con WinBox. ....	103
Figura 55. Pantalla de configuración principal de un equipo Mikrotik. ....	104
Figura 56. Etiquetado de interfaces según su funcionalidad.....	105
Figura 57. Asignación de IP a las interfaces ether13-WAN y ether6- LAN.....	106
Figura 58. Activación y configuración del servidor DHCP.....	107
Figura 59. Rango de direcciones disponibles para la red LAN.....	108
Figura 60. Dirección y mascara de red asignada al servidor DHCP.....	108
Figura 61. Configuración de rutas estáticas y dinámicas.....	109
Figura 62. Configuración de rutas DNS principal y alternativo. ....	110
Figura 63. Traducción de direcciones de red (NAT). ....	111
Figura 64. Enmascaramiento de direcciones de red.....	111
Figura 65. Implementación de seguridad en el equipo de gestión central. ....	112
Figura 66. Activación y configuración de graficas de monitoreo de recursos.....	113
Figura 67. Etiquetado y asignación de direcciones a las interfaces del AP1. ....	114
Figura 68. Etiquetado de la interface wireless del AP1. ....	115
Figura 69. Configuración de parámetros en la interface wireless del AP1.....	116
Figura 70. Fijación de velocidades en la interface Wireless del AP1.....	117
Figura 71. Límite de estaciones que permite registrar simultáneamente el AP1. ....	118
Figura 72. Rango de potencias permitido en el AP1 para estaciones registras.....	119
Figura 73. Bridge entre interfaces ether1 y Wlan. ....	120
Figura 74. Activación del CAP en el AP1. ....	121

Figura 75. Activación del CAPsMAN en el equipo de gestión central.....	122
Figura 76. Asignación de canales en el CAPsMAN .....	123
Figura 77. Agregación de perfiles de configuración .....	124
Figura 78. Visualización de los perfiles de configuración .....	125
Figura 79. Implementación del hotspot.....	126
Figura 80. Configuración de parámetros generales del hotspot.....	127
Figura 81. Configuración del método de autenticación al hotspot.....	128
Figura 82. Creación de perfiles de usuario en el gestor hotspot .....	129
Figura 83. Usuarios autenticados a través del hotspot.....	129
Figura 84. Test de velocidad con la herramienta speedof.me.....	130
Figura 85. Test de velocidad con herramienta de AEPROVI. ....	131
Figura 86. Test de velocidad con herramienta de speedtest. ....	131
Figura 87. Estadística de paquetes ICMP con la herramienta ping de Windows.....	132
Figura 88. Reproducción de un Video a 360p.....	134
Figura 89. Reproducción de un Video a 480p.....	134
Figura 90. Reproducción de un Video HD a 720p.....	135
Figura 91. Prueba de descarga de un archivo.....	136

## ÍNDICE DE TABLAS

Tabla 1. Conversión de potencias para sistemas de transmisión de Dbm a Watts.....	15
Tabla 2. Descripción y características de los equipos de la red existente en la FICA .....	60
Tabla 3. Prueba de velocidad con herramientas web .....	62
Tabla 4. Prueba de envío y recepción de paquetes ICMP .....	64
Tabla 5. Características técnicas de router RB1100AHx2.....	68
Tabla 6. Características técnicas de Switch QP-1240R .....	70
Tabla 7. Distribución de frecuencias para los cAP2n. ....	78
Tabla 8. Características técnicas de APs UniFi.....	86
Tabla 9. Definición de métricas para el cumplimiento de selección.....	91
Tabla 10. Comparativa de selección de la tecnología más adecuada.....	91
Tabla 11. Sumario de resultados a la comparativa de selección .....	93
Tabla 12. Características técnicas de un RBcAP2n .....	95
Tabla 13. Análisis comparativo de marcas con precios .....	97
Tabla 14. Costos adicionales para la construcción de la infraestructura nueva de red .....	98
Tabla 15. Costo invertido en la red antigua. ....	98
Tabla 16. Comparativa de precios unitarios del AP nuevo vs antiguo .....	99
Tabla 17. Prueba de velocidad con herramientas web para la nueva red.....	132
Tabla 18. Prueba de envío y recepción de paquetes ICMP para la nueva red .....	133
Tabla 19. Historia de un usuario docente .....	137
Tabla 20. Historia de un usuario docente .....	138
Tabla 21. Historia de un usuario estudiante .....	139
Tabla 22. Caso de prueba para la navegación web con rol docente.....	140
Tabla 23. caso de prueba para la carga y descarga de información rol docente .....	141
Tabla 24. caso de visualización de videos rol estudiante.....	142

**ÍNDICE DE ECUACIONES**

Ecuación 1. Cálculo de puntos de acceso necesarios .....	52
Ecuación 2. Cálculo de pérdida de propagación .....	75
Ecuación 3. Cálculo de ganancia de salidad del equipo transmisor.....	76
Ecuación 4. Cálculo de nivel de señal que le llega al equipo receptor .....	77

## CAPITULO I

### 1 Antecedentes

#### 1.1 Tema

Diseño e implementación de un sistema de gestión Wi-Fi centralizado, en Facultad de Ingeniería en Ciencias Aplicadas, mediante RouterOS, para mejorar la calidad de servicio.

#### 1.2 Definición del problema

La Facultad de Ingeniería en Ciencias Aplicadas (FICA), es una institución educativa de nivel superior, perteneciente a la Universidad Técnica del Norte, ubicada en la ciudad de Ibarra, la misma que hoy en día con el avance tecnológico se ha convertido en una facultad pionera en la formación del estudiante universitario.

En el desarrollo de las actividades académicas y con la creciente demanda de acceso inalámbrico a redes Wi-Fi, y específicamente por las facilidades que este tipo de redes prestan en campus universitarios, se presenta el inconveniente de saturación de conexiones en la red, que puede darse en: la red acceso, la red de transporte, la red core, en salida pública o en todas las anteriores.

Según datos obtenidos del departamento de sistemas de la UTN, la red Wi-Fi implementada dentro de la FICA cuenta con 300 usuarios aproximadamente, que se conectan de manera simultánea, por lo que la tecnología implementada actualmente no abátese todo el tráfico de peticiones de acceso a internet, provocando esto una baja calidad de servicio en el usuario final.

En vista de esta problemática se plantea la implementación de un sistema de gestión de red centralizada, el mismo que me permita ejecutar una mejor administración centralizada de usuarios, pero descentralizando la red de acceso Wi-Fi, en las: aulas, pasillos y oficinas, para poder de esta manera ejecutar un mejor sistema de gestión Wi-Fi, y poder brindar mejor calidad de servicio a nivel de usuarios finales.

### 1.3 Delimitación del problema

Este proyecto se lo llevará a cabo en las instalaciones de la Universidad Técnica del Norte, específicamente en la Facultad de Ingeniería en Ciencias Aplicadas (FICA).

Mediante el presente proyecto se realizará la implementación de un sistema de gestión Wi-Fi centralizado que permita monitorear y controlar el desempeño de la red Wi-Fi. El sistema se implementará sobre RouterOS y con hardware Mikrotik; para el correcto funcionamiento del sistema, se debe considerar, que la red de acceso inalámbrica cumpla las especificaciones técnicas para soportar los estándares 802.11b/g/n, la red de transporte debe cumplir especificaciones 10/100/1000 BASE-T, para evitar congestión en este tramo de red, la red core se montará sobre un RouterBoard con características Gigabit, que se encargará de gestionar toda las conexiones de la red Wi-Fi, bajo una topología de red tipo estrella y finalmente se debe considerar que el acceso WAN debe tener la capacidad suficiente para transportar todo el tráfico generado dentro de la red.

El sistema de gestión de red Wi-Fi centralizado es el encargado de monitorear el tráfico de la red Wi-Fi a nivel de cada piso y a nivel de cada punto de acceso, para determinar quién se conecta, cuánto tiempo y que tipo de privilegios o restricciones se le da a cada usuario, para que de esta manera se haga un uso eficiente del ancho de banda que se entrega en el acceso WAN.

Una vez implementado el sistema de gestión Wi-Fi, se realizará las pruebas de funcionamiento, mediante el uso del protocolo ICMP, con trazado de rutas y tiempos de respuesta en cada tramo de la red. También utilizará herramientas como, Bandwidthplace y Speedof.me, que me permitan obtener parámetros como ancho de banda y latencia de acceso a sitios web. Es importante indicar que estas pruebas se van a realizar en distintos horarios para determinar el rendimiento de la red Wi-Fi, en diferentes condiciones de tráfico.



Con toda esta información obtenida, finalmente se realizará las conclusiones y recomendaciones para determinar la funcional y alcance del sistema y a la vez definir futuros estudios que pudieran complementar a este proyecto inicial.

## **1.4 Objetivos**

### **1.4.1 Objetivo general**

Implementar un sistema de gestión Wi-Fi centralizado, en la Facultad de Ingeniería en Ciencias Aplicadas, mediante RouterOS, para mejorar la calidad de servicio a nivel de usuarios finales.

### **1.4.2 Objetivos específicos**

- Analizar la situación actual de la Facultad de Ingeniería en Ciencias Aplicadas (FICA), para determinar la problemática a nivel de usuario final.
- Recopilar la información que sustenta el proyecto para fundamentar su desarrollo.
- Diseñar el sistema considerando: la red de acceso, la red de transporte, la red core y el acceso WAN, para que su implementación brinde las mejores prestaciones.
- Implementar sistema de gestión Wi-Fi centralizado con todas las especificaciones técnicas del proyecto.
- Realizar las pruebas de funcionamiento del sistema, para evaluar los resultados obtenidos.

## **1.5 Justificación del proyecto**

La Facultad de Ingeniería en Ciencias Aplicadas (FICA), en el desempeño de sus actividades académicas, necesita tener una red Wi-Fi, con las mejores prestaciones de calidad de servicio, en acceso a contenidos a nivel de usuarios finales: en pasillos, aulas y oficinas.

Por tal razón surge la necesidad de implementar un sistema de gestión centralizado que pueda administrar: quien se conecta a la red Wi-Fi, tiempos de conexión, concesión de ancho

de banda, reglas de firewall y restricción de contenidos. Todo esto con el fin de garantizar la calidad de servicio a nivel de usuarios finales, los mismos que pueden ser: estudiantes, docentes y administrativos, que se encuentren dentro de las instalaciones de Facultad de Ingeniería en Ciencias Aplicadas (FICA).

Además de mejoramiento del acceso a contenidos, este proyecto también está enfocado a la optimización de recursos económicos para la Universidad Técnica del Norte, sin dejar de lado la calidad de prestaciones que se debe ofrecer a los usuarios finales de la Facultad de Ingeniería en Ciencias Aplicadas (FICA).

## **1.6 Alcance**

Este proyecto se lo llevara a cabo en las instalaciones de la Universidad Técnica del Norte, específicamente en la Facultad de Ingeniería en Ciencias Aplicadas (FICA).

Mediante el presente proyecto se realizará la implementación de un sistema de gestión Wi-Fi centralizado, que permita monitorear y controlar el desempeño de la red Wi-Fi. El sistema se implementara sobre RouterOS y con hardware Mikrotik; para el correcto funcionamiento del sistema, se debe considerar, que la red de acceso inalámbrica cumpla las especificaciones técnicas para soportar los estándares 802.11b/g/n, la red de transporte debe cumplir especificaciones 10/100/1000 BASE-T, para evitar congestión en este tramo de red, la red core se montara sobre un RouterBoard con características Gigabit, que se encargará de gestionar toda las conexiones de la red Wi-Fi, bajo una topología de red tipo estrella y finalmente se debe considerar que el acceso WAN debe tener la capacidad suficiente para transportar todo el tráfico generado dentro de la red.

El sistema de gestión de red Wi-Fi centralizado, es el encargado de monitorear el tráfico de: toda la red red Wi-Fi, a nivel de cada piso y a nivel de cada punto de acceso, para determinar quién se conecta, cuánto tiempo y que tipo de privilegios o restricciones se le da a cada usuario,

para que de esta manera se haga un uso eficiente del ancho de banda que se entrega en el acceso WAN.

Una vez implementado el sistema de gestión Wi-Fi, se realizará las pruebas de funcionamiento, mediante el uso del protocolo ICMP, con trazado de rutas y tiempos de respuesta en cada salto de la red. También utilizara herramientas como, Bandwidthplace y Speedof.me, que me permitan obtener parámetros como, ancho de banda y latencia de acceso a sitios web. Es importante indicar que estas pruebas se van a realizar en distintos horarios para determinar el rendimiento de la red Wi-Fi, en diferentes condiciones de tráfico.

Con toda esta información obtenida, finalmente se realizará las conclusiones y recomendaciones para determinar la funcional y alcance del sistema, y a le vez definir futuros estudios que pudieran complementar a este proyecto inicial.



## CAPITULO II

### 2 Marco teórico

#### 2.1 Tecnologías inalámbricas

Una red inalámbrica permite la comunicación de dos más terminales sin la necesidad de una conexión por cable. En una red inalámbrica un usuario puede permanecer conectado dentro de un área geográfica determinada, por tal razón a veces a esto suele llamarse movilidad.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya sea que se encuentren a unos metros de distancia o a varios kilómetros. La instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente a diferencia de las redes cableadas, en donde hay necesidad de agujerear las paredes para pasar cables. Esto ha hecho que el uso de esta tecnología se extienda con rapidez (Tanenbaum & Wetherall, 2011).

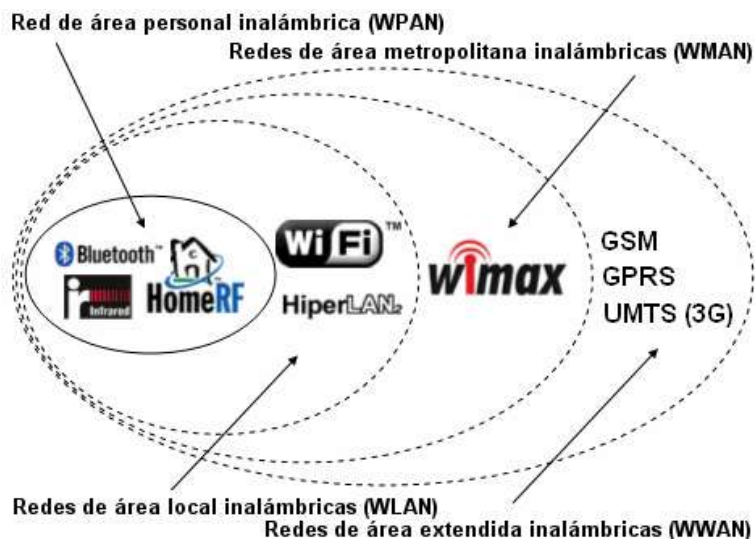


Figura 1. Tecnologías de redes inalámbricas.

Fuente: (Kioskea, 2014)

La figura anterior muestra las diferentes tecnologías inalámbricas, que según el área geográfica de cobertura se las puede clasificar en:

- Redes WPAN
- Redes WMAN
- Redes WWAN
- Redes WLAN

### 2.1.1 Redes WPAN

Las redes WPAN por sus siglas en inglés Wireless Personal Area Network, son redes inalámbricas de área personal y de corto alcance que abarcan un área de algunas decenas de metros. Este tipo de red se usa generalmente para conectar dispositivos periféricos, por ejemplo, impresoras, teléfonos móviles y electrodomésticos, asistente personal digital (PDA) y ordenadores sin el uso de cables. También se pueden conectar de forma inalámbrica dos ordenadores cercanos. Este tipo de redes se subdividen en redes Bluetooth, redes HomeRF, tecnologías Zigbee y redes infrarrojas.

La tecnología principal WPAN es Bluetooth, fue lanzado por Ericsson en 1994. Ofrece una velocidad máxima de 1 Mbps con un alcance máximo de hasta treinta metros. La tecnología Bluetooth, también conocida como IEEE 802.15.1 tiene la ventaja de tener un bajo consumo de energía, algo que resulta muy práctico para usarla en periféricos de pequeño tamaño.

HomeRF (Home Radio Frequency), fue lanzada en 1998 por **HomeRF Working Group**, que incluye a los fabricantes Compaq, HP, Intel, Siemens, Motorola y Microsoft, entre otros. Esta ofrece una velocidad máxima de 10 Mbps con un alcance de 50 a 100 metros sin amplificador. A pesar de estar respaldado por Intel, el estándar HomeRF se abandonó en enero de 2003, porque los fabricantes de procesadores empezaron a usar la tecnología Wi-Fi, integrando de esta manera un microprocesador y un adaptador Wi-Fi en un solo componente.

La tecnología Zigbee normada el estándar IEEE 802.15.4, también se puede utilizar para conectar dispositivos en forma inalámbrica a un coste muy bajo y con bajo consumo de energía. Particularmente resulta adecuada porque se integra directamente en pequeños aparatos electrónicos como: electrodomésticos, sistemas estéreos y juguetes. Zigbee funciona en la banda de frecuencia de 2,4 GHz y en 16 canales, logrando alcanzar una velocidad de transferencia de hasta 250 Kbps, con distancias de hasta 100 metros.

Por último, las redes infrarrojas se utilizan para crear conexiones inalámbricas de corto alcance, pudiendo alcanzar velocidades de unos pocos megabits por segundo. Esta tecnología se usa ampliamente en aparatos electrónicos del hogar como los controles remotos, pero puede sufrir interferencias debidas a las ondas de luz.

Los enlaces infrarrojos se encuentran limitados por el espacio y los obstáculos. El hecho de que la longitud de onda de los rayos infrarrojos sea tan pequeña (850-900 nm), hace que no pueda propagarse de la misma forma en que lo hacen las señales de radio.

Es por eso que las redes infrarrojas suelen estar dirigidas a oficinas o plantas de oficinas de reducido tamaño. Algunas empresas van un poco más allá, transmitiendo datos de un edificio a otro mediante la colocación de antenas en las ventanas de cada edificio.

Por otro lado, las transmisiones infrarrojas presentan la ventaja, frente a las de radio, de no transmitir a frecuencias bajas, donde el espectro está más limitado, y así no se restringe su ancho de banda por el uso de frecuencias libres (Tanenbaum & Wetherall, 2011).

### **2.1.2 Redes WMAN**

Las redes inalámbricas de área metropolitana o **WMAN** (Wireless Metropolitan Area Network), son también conocidas como bucle local inalámbrico (WLL, Wireless Local Loop). Las WMAN se basan en el estándar IEEE 802.16<sup>1</sup>. Los bucles locales inalámbricos ofrecen

---

<sup>1</sup> IEEE 802.16. Especificaciones para redes inalámbricas de acceso metropolitano, de banda ancha fijas.

una velocidad total efectiva de 1 a 10 Mbps con un alcance de 4 a 10 kilómetros, algo muy útil para compañías de telecomunicaciones.

La mejor red inalámbrica de área metropolitana es WiMAX<sup>2</sup>, que puede alcanzar una velocidad aproximada de 70 Mbps en un radio de varios kilómetros (Stallings, 2014).

### 2.1.3 Redes WWAN

Las redes inalámbricas de área extensa o **WWAN** (Wireless Wide Area Network), tienen el alcance más amplio de todas las redes inalámbricas (Stallings, 2014). Básicamente difiere de una **WLAN** en que utiliza tecnologías de red celular para comunicaciones móviles como:

- GSM (Global System for Mobile Communication)
- GPRS (General Packet Radio Service)
- UMTS (Universal Mobile Telecommunication System)

### 2.1.4 Redes WLAN



*Figura 2. Red inalámbrica de área local  
Fuente: (Sifra consultores, S.A. de C.V., 2009)*

---

<sup>2</sup> WiMaX. Conocida como tecnología de última milla, que transmite de datos mediante ondas de radio en las frecuencias de 2,5 a 5,8 GHz.



Una red inalámbrica de área local o WLAN (Wireless Local Area Network), es un sistema de comunicación inalámbrica flexible que tiene similar cobertura que una red LAN. Se utiliza como alternativa a las redes cableadas o como una extensión de las mismas. Usa tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios sobre todo por la tendencia al uso de equipos Smart como celulares y tablets. Estas redes van adquiriendo importancia en muchos campos pues permiten transmitir información desde diversos dispositivos a una terminal central. Actualmente su uso está muy extendido en la industria, la educación y el gobierno.

Una WLAN es un tipo de red, utilizada como alternativa de LAN cableada, que usa ondas de radiofrecuencia de transmisión de datos y brinda conectividad a internet, sin la necesidad de usar los tradicionales cables para conectar dispositivos, permitiendo también a los usuarios tener mayor movilidad en un área de trabajo (Stallings, 2014).

#### **2.1.4.1 Ventajas de una red WLAN**

- **Movilidad:** Estas redes pueden proveer acceso a la información los usuarios en tiempo real en cualquier lugar dentro de un área geográfica de cobertura (Stallings, 2014).
- **Escalabilidad:** Tienen la facilidad de expansión de la red después de su instalación inicial (Stallings, 2014).
- **Flexibilidad:** Permite la colocación de dispositivos en cualquier lugar sin tener que cambiar la configuración de la red (Stallings, 2014).
- **Ventajas de instalación:** Las redes WLAN pueden ser utilizadas para proporcionar conectividad entre sitios que están separados por barreras físicas que dificultan la instalación de una red cableada (Stallings, 2014).

#### 2.1.4.2 Desventajas de las redes WLAN

- La velocidad que alcanzan es baja en comparación con la de un cable de red (Stallings, 2014).
- La señal puede obstruirse o presentar interferencias por otros dispositivos inalámbricos (Stallings, 2014).
- Es muy vulnerable a los ataques a usuarios por intersección el medio de transmisión (Stallings, 2014).

#### 2.1.5 Redes Wi-Fi

En los inicios, las redes inalámbricas no se encontraban estandarizadas por ningún estándar. El principal problema que existía hasta entonces era la falta de compatibilidad entre distintos fabricantes, pues aun cumpliendo todos ellos la norma 802.11<sup>3</sup>, dicha norma dejaba abierta a la interpretación de suficientes puntos como que los sistemas de distintos fabricantes no trabajaran entre sí. Así pues, se crea la Wi-Fi Alliance, permitiendo homogeneizar productos y hacer posible que se asentaran en el mercado de consumo, hasta el punto de que hoy en día las redes inalámbricas se conocen popularmente como redes Wi-Fi en referencia a este organismo.

En el estándar original también se define el protocolo de acceso múltiple por detección de portadora sin colisiones, CSMA/CA<sup>4</sup> (carrier sense multiple access with collision avoidance).

Wi-Fi o WiFi es una tecnología que permite que los dispositivos electrónicos que se conectan a una red LAN inalámbrica (WLAN), usando principalmente las bandas de radio ISM<sup>5</sup> de 2.4 GHz (12 cm) y de 5 GHz (6 cm). El acceso a una red Wi-Fi es generalmente

---

<sup>3</sup> 802.11. Define el uso de los dos niveles inferiores del modelo OSI, capa física y capa de enlace de datos.

<sup>4</sup> CSMA/CD. Acceso Múltiple con escucha de portadora y detección de colisiones, es un protocolo de acceso al medio compartido que evita colisiones.

<sup>5</sup> ISM (Industrial, Scientific and Medical). son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica.

protegido por contraseña, pero puede ser abierto, lo que permite que cualquier dispositivo dentro de su rango para acceder a los recursos de dicha red.

La Wi-Fi Alliance posee y controla el logotipo "Wi-Fi Certified", como una marca registrada, lo cual se permiten sólo los equipos que hayan superado la prueba. Los consumidores que dependen de esta marca tendrán mayores posibilidades de interoperabilidad con otras marcas. Las pruebas no sólo involucran a los protocolos de radio y formatos de interoperabilidad datos, sino también seguridad, así como la prueba opcional para la calidad de los protocolos de servicio y administración de energía. Un enfoque en la experiencia del usuario ha dado forma al enfoque general del programa de certificación de Wi-Fi Alliance. Los productos certificados por Wi-Fi tienen que demostrar que tienen un buen desempeño con otros productos certificados, en la ejecución de aplicaciones comunes (Stallings, 2014).

### **2.1.6 Elementos de una red Wi-Fi**

Al montar y configurar una red Wi-Fi, que permita la comunicación de dos o más estaciones móviles, generalmente se necesitan los siguientes elementos de red:

- Punto de acceso
- Controlador de puntos de acceso
- Estación o CPE
- Potencia y sensibilidad de recepción
- Cobertura
- Canales y frecuencias

#### **2.1.6.1 Punto de acceso**

Un punto de acceso inalámbrico WAP o AP (Wireless Access Point o Access Point), en una red de computadoras, es un dispositivo de red que interconecta equipos de comunicación

inalámbrica, para formar una red que interconecta dispositivos móviles o con tarjetas de red inalámbricas.

Los AP son dispositivos que permiten la conexión inalámbrica de un dispositivo móvil de cómputo (computadora, tableta, smartphone), con una red. Normalmente, un AP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos, tienen asignadas direcciones IP, para poder ser configurados, pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar roaming o itinerancia (Rojas Villegas & Rivera Paredes, 2010).

#### **2.1.6.2 Controlador de puntos de acceso**

Son soluciones de hardware o software que permiten el manejo centralizado de puntos de acceso, esto permite a pequeñas y medianas empresas, sucursales y puntos de venta controlar sus redes inalámbricas mediante un sistema ampliable, seguro y de gestión centralizada.

Ofrecen administración LAN inalámbrica de varios puntos de acceso, capacidades de agrupación de controladores, organización automática, optimización automática, reparación automática y mecanismos de seguridad avanzados para facilitar el despliegue, la administración y las operaciones de la red. Los controladores de puntos de acceso son la solución perfecta para los administradores de redes que buscan una forma fiable, segura y sencilla de administrar una red Wireless (Rojas Villegas & Rivera Paredes, 2010).

#### **2.1.6.3 Estación o CPE**

La estación o CPE (Equipo Local del Cliente - Customer Premises Equipment)

El CPE es usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación. El equipo puede proveer una combinación de servicios incluyendo datos, voz, video y un host de aplicaciones multimedia interactivos.

Son unidades terminales localizadas en el lado del suscriptor y que se encuentran conectadas con el canal de comunicaciones del proveedor o ISP, prácticamente cualquier equipo de usuario final se puede denominar Customer Premises Equipment, y puede ser propiedad tanto del usuario como del proveedor. Pero, aunque puede ser propiedad cualquiera de los dos, el CPE suele ser del usuario y se sitúa en la conexión eléctrica del mismo o directamente en un enchufe. Los datos enviados por el usuario son transmitidos desde el CPE al punto de acceso WAP o AP. El CPE está conectado al ordenador a través de un puerto Ethernet, un concentrador/conmutador u otros medios como interfaces USB, etc (Rojas Villegas & Rivera Paredes, 2010).

#### 2.1.6.4 Potencia y sensibilidad de recepción

*Tabla 1. Conversión de potencias para sistemas de transmisión de Dbm a Watts.*

<b>dBm</b>	<b>Watts</b>	<b>dBm</b>	<b>Watts</b>	<b>dBm</b>	<b>Watts</b>
0	1.0 mw	16	40 mw	32	1.6 w
1	1.3 mw	17	50 mw	33	2 w
2	1.6 mw	18	63 mw	34	2.5 w
3	2.0 mw	19	79 mw	35	3.2 w
4	2.5 mw	20	100 mw	36	4.0 w
5	3.2 mw	21	126 mw	37	5.0 w
6	4 mw	22	158 mw	38	6.3 w
7	5 mw	23	200 mw	39	8.0 w
8	6 mw	24	250 mw	40	10 w
9	8 mw	25	316 mw	41	13 w
10	10 mw	26	398 mw	42	16 w
11	13 mw	27	500 mw	43	20 w
12	16 mw	28	630 mw	44	25 w

13	20 mw	29	800 mw	45	32 w
14	25 mw	30	1 w	46	40 w
15	32 mw	31	1.3 w	47	50 w

---

*Fuente: Propia*

Las principales características a tener en cuenta en las transmisiones inalámbricas son la potencia de transmisión (dbm o mW), sensibilidad de recepción (-dbm) y ganancia de la antena (dbi)<sup>6</sup>.

La potencia, en este caso de transmisión, se mide en Vatios o Watt (W), pero en las telecomunicaciones y sobre todo en wifi, se trabaja con valores de potencia muy pequeños y estos se expresan en mW (milivatios; 1000mW=1W). Normalmente veremos en las fichas técnicas la potencia expresada en dBm, que es una medida basada en los decibelios y tiene su equivalencia en mW. En este caso, como se especifica a que unidades está referida, el dBm<sup>7</sup> mide un valor absoluto, no relativo (Ariganello & Barrientos Savilla, 2010).

La sensibilidad de recepción indica qué cantidad de señal (dBm) debe recibir un dispositivo Wi-Fi para trabajar correctamente a una determinada velocidad de transmisión (Mbps). Cuanto menor es la sensibilidad mejor será un dispositivo ya que necesitará que le llegue menos potencia para trabajar correctamente (a una velocidad dada). El rango de señal válido para enlaces WiFi está alrededor de los -70 dBm. Una diferencia de 3 dBm significa que la potencia que se necesita es dos veces menor. Por ejemplo, un dispositivo que tenga una sensibilidad de recepción (a 11 Mbps) de -70 dBm significa que necesita recibir una potencia de 0,0000001mW para que funcione correctamente. (Ariganello & Barrientos Savilla, 2010)

---

<sup>6</sup> Dbi. Relación logarítmica entre la potencia de emisión de una antena en relación a un radiador isotrópico.

<sup>7</sup> Dbm. Unidad de medida de potencia expresada en decibelios (dB) relativa a un mili vatio (mW).

Debemos entender que las unidades medidas son relativas. De ahí que muchos equipos que vemos a la venta marquen alcances kilométricos. Esto es real a medias, ya que son mediciones y magnitudes calculadas en lo que se denomina “condiciones de laboratorio”, es decir, sin ningún tipo de obstáculo o interferencia. Podríamos decir que es un valor máximo teórico (Ariganello & Barrientos Savilla, 2010).

### 2.1.6.5 Cobertura

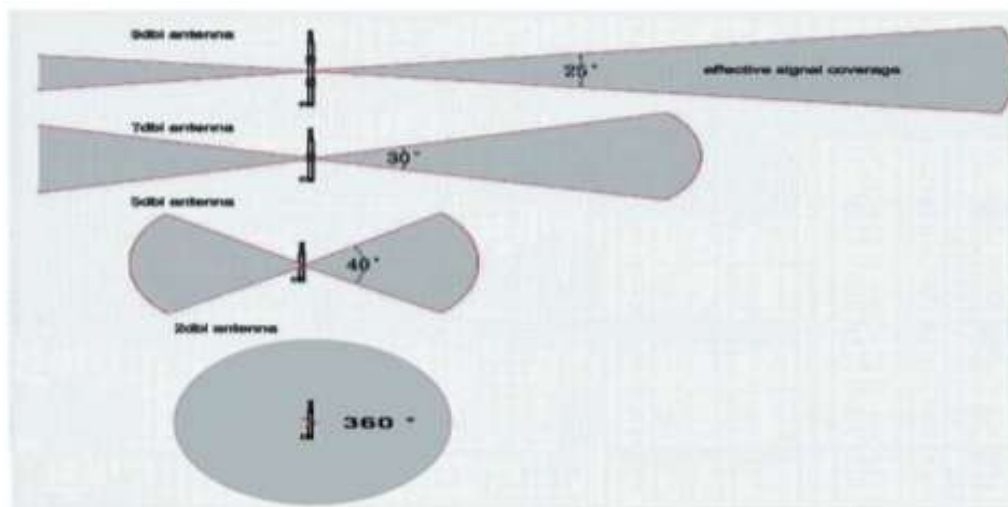


Figura 3. Antenas, patrones y omnidireccional dipolo de radiación. Hardesty, G.  
Fuente: (DATA ALLIANCE, 2016)

Las ondas de radio tienen dificultades para atravesar obstáculos. Las antenas de alta ganancia tienen un patrón plano de radiación, así que una antena más grande solo le ayudará a aumentar la cobertura, pero nos servirá de mucho si se tiene diferentes niveles, esta información es útil para entender por qué un AP no es útil para proveer señal a un edificio de varios pisos. Las antenas de alto poder se deben utilizar para enviar la señal a largas distancias a través de un punto específico y muy enfocado. Cuanto más se incremente la ganancia de la antena, la señal se aplanará más. Las antenas de bajo poder enviarán sus señales a elevaciones altas y bajas de un área local. La ganancia de la antena se incrementa tanto en el poder de transmisión como en la sensibilidad del receptor, por lo que no sólo se enviará la señal más lejos, sino que

se podría recibir señales más débiles dentro del área de cobertura. La ganancia de una antena es un indicador de una mejora en la fuerza de la señal, dicha ganancia se mide en dBi (Ortega Gallegos, 2012).

Las antenas generalmente tienen una gran cobertura a expensas del alcance, a más alto sea el alcance, habrá menos ancho de cobertura en el área, la mitad de la potencia del ancho del haz (Ortega Gallegos, 2012).

Como regla general a mayor sea la ganancia más estrecha será el ancho del haz (en el área de cobertura)

#### **2.1.6.6 Canales y frecuencias**

El acceso a la información a través de los medios de comunicación y la asignación de frecuencias para el uso del espectro radioeléctrico en el Ecuador esta normado y regulado por la Constitución de la República, dicho texto elaborado en el 2008 describe lo siguiente:

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos (Asamblea Constituyente del Ecuador, 2008).
2. El acceso universal a las tecnologías de información y comunicación (Asamblea Constituyente del Ecuador, 2008).
3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas (Asamblea Constituyente del Ecuador, 2008).
4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad (Asamblea Constituyente del Ecuador, 2008).



5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.

Art. 17.- El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto:

1. Garantizará la asignación, a través de métodos transparentes y en igualdad de condiciones, de las frecuencias del espectro radioeléctrico, para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, así como el acceso a bandas libres para la explotación de redes inalámbricas, y precautelará que en su utilización prevalezca el interés colectivo (Asamblea Constituyente del Ecuador, 2008).
2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada (Asamblea Constituyente del Ecuador, 2008).
3. No permitirá el oligopolio o monopolio, directo ni indirecto, de la propiedad de los medios de comunicación y del uso de las frecuencias (Asamblea Constituyente del Ecuador, 2008).

De la misma manera el estado ha establecido un Plan Nacional de asignación de frecuencias al cual se deben regir todos los proyectos y desarrollos inalámbricos que hagan uso de la banda de frecuencias no licenciadas, tanto empresariales como institucionales.

En este plan se define que:

Las bandas:

13 553-13 567 kHz

(Frecuencia central 13 560 kHz),

26 957-27 283 kHz

(Frecuencia central 27 120 kHz),

40,66-40,70 MHz

(Frecuencia central 40,68 MHz),

902-928 MHz en la Región 2

(Frecuencia central 915 MHz),

2 400-2 500 MHz

(Frecuencia central 2 450 MHz),

5 725-5 875 MHz y

(Frecuencia central 5 800 MHz) y

24-24,25 GHz

(Frecuencia central 24.125 GHz)

Están designadas para aplicaciones industriales, científicas y médicas (ICM). Los servicios de radiocomunicación que funcionan en estas bandas deben aceptar la interferencia perjudicial resultante de estas aplicaciones (Conatel, 2011).

## **2.2 Estándar IEEE 802.11**

IEEE 802.11 describe el conjunto de especificaciones técnicas para las capas inferiores del modelo OSI, la capa física (Physical Layer) y la capa MAC (Media Access Control), en la implementación redes WLAN, que trabajan sobre las bandas 2.4, 3.6, 5 y 60 Ghz. La versión original del estándar fue publicada en 1997, la misma que trabajaba con velocidades de hasta 1 y 2 Mbps, sobre un medio de transmisión infrarrojo (Tanenbaum & Wetherall, 2011).

La familia 802.11 consiste en una serie de técnicas de modulación half-dúplex sobre el aire que utilizan el mismo protocolo básico. 802.11 de 1997 fue el primer estándar para redes inalámbricas, pero 802.11b fue el primero en ser ampliamente aceptado, seguido por 802.11a, 802.11g, 802.11n y 802.11ac. Otras normas como la c, f, h, j son reformas de servicios que se

utilizan para ampliar el alcance actual de la norma existente, también pueden incluir correcciones a una especificación anterior (Tanenbaum & Wetherall, 2011).

Los estándares 802.11b y 802.11g utilizan la banda ISM de 2.4 GHz, que operan en Ecuador según el Plan Nacional de Asignación de Frecuencias, emitido por el estado en año 2011. Debido a esta elección de esta banda de frecuencia no licenciada, los equipos 802.11b y 802.11g pueden sufrir de vez en cuando interferencia de hornos microondas, teléfonos inalámbricos y dispositivos Bluetooth. 802.11b y 802.11g controlan su interferencia y la susceptibilidad a la misma, mediante el uso de métodos como el espectro ensanchado por secuencia directa (DSSS-Direct Sequence Spread Spectrum) y multiplexación por división de frecuencias ortogonales (OFDM-Orthogonal Frequency Division Multiplexing) (Tanenbaum & Wetherall, 2011).

### 2.2.1 Variantes de IEEE 802.11



Figura 4. Evolución y variantes de redes Wi-Fi.  
Fuente: (De Luz, 2012).

Como se puede ver en la figura anterior, las redes inalámbricas se reparten entre dos clases principales subdivididas por la banda de frecuencia. Las primeras tecnologías usaban la banda de 2.4 GHz mientras que las más modernas usan la de 5 GHz (más ancha). La primera incluye los estándares del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.11b a 11 Mbps y es compatible con su sucesor 802.11g a 54 Mbps. Esta primera opción es la más común actualmente (Paz, 2012).

Por otro lado, tanto 802.11a como 802.11h, que operan en la banda de 5 GHz, consiguen un rendimiento nominal de 54 Mbps. 802.11h, referida en Estados Unidos como la de compatibilidad en Europa, es la variante europea del estándar americano. Sus dos características más importantes son la selección dinámica de frecuencias y la potencia de transmisión variable, obligatorias para el mercado europeo según el Instituto Europeo de Estándares de Comunicación (ETSI)<sup>8</sup> con el fin de asegurar que los sistemas tengan una capacidad de transmisión razonable (Paz, 2012).

Desde la publicación del estándar inicial de estándar IEEE 802.11 y en base a las necesidades del mercado, surgieron algunas variantes como:

- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11ac

#### **2.2.1.1 IEEE 802.11a**

La revisión 802.11a fue aprobada en 1999. Este estándar utiliza los mismos protocolos de base que el original, opera en la banda de 5 GHz y utiliza 52 subportadoras y trabaja con la tecnología OFDM<sup>9</sup>. Con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. Maneja dinámicamente velocidades de 48, 36, 24, 18, 12, 9 o 6 Mbit/s en de que caso necesario (Paz, 2012).

---

<sup>8</sup> ETSI. European Telecommunications Standards Institute. Organización europea de estandarización independiente sin fines de lucro.

<sup>9</sup> OFDM. Orthogonal Frequency-Division Multiplexing. Acceso múltiple por división de frecuencias ortogonales. Técnica que se basa en la multiplexación por división de frecuencias equiespaciadas.

Fuente: (Codejobs, 2014)

802.11a tiene 12 canales sin solapamiento, 8 para red inalámbrica y 4 para conexiones punto a punto. No es compatible con equipos del estándar 802.11b, excepto si el equipo maneja los dos estándares mutuamente. Recientemente, en muchos países del mundo están permitiendo el funcionamiento en la banda de 5.47 a 5.725 GHz como usuarios secundarios utilizando un método de intercambio derivado del 802.11h. Esto añadirá otros 12 canales a la banda de 5GHz global, permitiendo significativamente incrementar la capacidad de red inalámbrica global (Paz, 2012).

El uso de la banda de 5 GHz 802.11a da una ventaja significativa, ya que la banda de 2,4 GHz es muy utilizada hasta el punto de estar llena. La degradación causada en redes que trabajan a 2.4Ghz puede causar conflictos en las conexiones con caídas frecuentes. Sin embargo, la alta frecuencia de portadora también trae una ligera desventaja: El rango total efectivo de 802.11a es ligeramente menor que la de 802.11b y 802.11g, ya que las señales 802.11a no puede penetrar en la medida que lo hace una 802.11b porque son absorbidos más fácilmente por las paredes y otros objetos sólidos en su camino, siendo la pérdida de trayectoria en la intensidad de la señal proporcional al cuadrado de la frecuencia de dicha señal (Paz, 2012).

Por otro lado, OFDM tiene ventajas de propagación fundamental cuando están en un entorno de trayectos múltiples, tales como una oficina cubierta, y las frecuencias más altas permiten la construcción de antenas más pequeñas y con una mayor ganancia en el sistema. El aumento del número de canales utilizables de 4 a 8 veces más y la casi ausencia de otros sistemas de interferencia como microondas, teléfonos inalámbricos, monitores de bebés, le dan a 802.11a ventajas de ancho de banda y fiabilidad significativas sobre 802.11b/g (Paz, 2012).

### **2.2.1.2 IEEE 802.11b**

La revisión 802.11b del estándar original fue ratificada en 1999. Tiene una velocidad máxima de transmisión de 11 Mbps y utiliza el mismo método de acceso definido en el estándar original CSMA/CA. El estándar 802.11b funciona en la banda de 2,4 GHz. Debido al espacio



La figura anterior permite visualizar el espectro de radio frecuencias disponibles a nivel mundial, sin embargo, es necesario recalcar que en algunos países como Estados Unidos y Ecuador solo se puede hacer uso hasta el canal 11 (Paz, 2012).

- **Interferencia en 802.11b**

En vista que el protocolo requiere de 16,25 a 22 MHz de separación entre canales, los canales adyacentes se superponen y se interfieren entre sí. Se recomienda dejar 3 o 4 canales claros entre los canales utilizados para evitar interferencias. La separación exacta requerida depende del tipo de protocolo y de dato seleccionado, así como también del entorno electromagnético donde se utiliza el equipo (Paz, 2012).

Cuando dos o más transmisores 802.11b operan en el mismo espacio aéreo, sus señales deben ser atenuadas por -50dBm y/o separados por 22 MHz para evitar interferencias. Esto es porque el algoritmo de DSSS<sup>12</sup> transmite datos logarítmicamente a lo largo de un ancho de banda de 20 MHz. La brecha restante 2 MHz se utiliza como una banda de guarda para permitir suficiente atenuación a lo largo de los canales de borde (Paz, 2012).

- **Rango de cobertura de 802.11b**

802.11b normalmente se utiliza en una configuración punto a multipunto, en donde un punto de acceso se comunica a través de una antena omnidireccional con clientes móviles dentro del alcance de dicho punto de acceso. El rango típico de cobertura depende del espectro de radiofrecuencias, la potencia de salida y la sensibilidad del receptor. El ancho de banda permitido es compartido a través de clientes en canales discretos. Una antena direccional concentra la potencia de salida en un campo más pequeño, pero aumenta el alcance de un enlace

---

<sup>12</sup> DSSS. es una técnica de codificación que utiliza un código de pseudoruido para "modular" digitalmente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral.

punto a punto. Sin embargo, los diseñadores de este tipo de instalaciones que desean permanecer dentro de la ley deben tener cuidado con las limitaciones legales de la potencia radiada efectiva (Correa, Godoy, Grote, & Orellana, 2005).

Algunas tarjetas 802.11b operan a 11 Mbit/s, pero pueden ir escalando en orden a 5.5, luego a 2, y finalmente a 1 Mbit/s, a esto se conoce como selección de tasa adaptable, de con el fin de disminuir la tasa de retrasmisiones que resultan errores en la comunicación (Correa, Godoy, Grote, & Orellana, 2005).

### **2.2.1.3 IEEE 802.11g**

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, que es la evolución de 802.11b. Este utiliza la banda de 2,4 Ghz al igual que 802.11b, pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar 802.11 b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del nuevo estándar lo tomó el hacer compatible ambos modelos. Sin embargo, en redes bajo el estándar 802.11g, la presencia de estaciones bajo el estándar 802.11b reduce significativamente la velocidad de transmisión, debido a que el Access Point en 800.11g, debe garantizar la interconexión con equipos que soporten velocidades de 800.11b.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente. Esto se debió, a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar 802.11b.

Actualmente se consiguen equipos con potencias de este estándar con hasta un vatio, que permite hacer comunicaciones de más de 50 km con antenas parabólicas o equipos de radio apropiados.



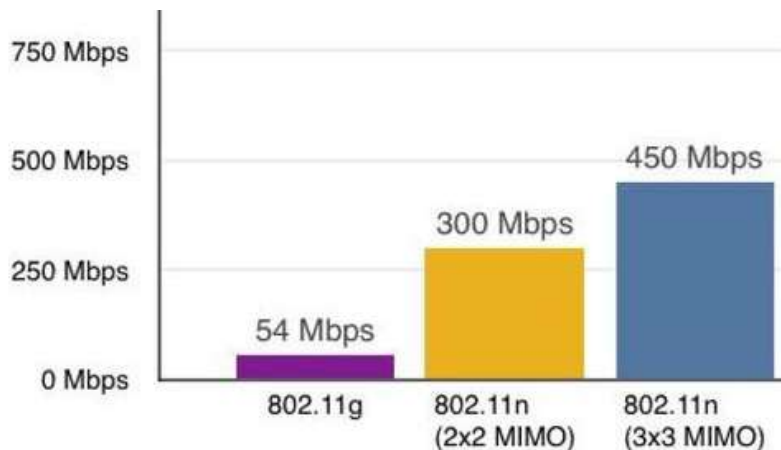
Existe una variante llamada 802.11g+ o 802.11g turbo capaz de alcanzar los 108Mbps de tasa de transferencia. Generalmente sólo funciona en equipos del mismo fabricante pues utiliza protocolos propietarios (Grote, Ávila, & Molina, 2007).

#### **2.2.1.4 IEEE 802.11n**

Fue aprobado 11 de septiembre del 2009. Su alcance de operación en redes es mayor con la nueva tecnología MIMO, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas (hasta 3). Existen también otras propuestas alternativas que podrán ser consideradas. El estándar ya está redactado y se viene implantando desde 2008. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento con una velocidad de 600 Mbps en capacidad física (80-100 estables)

El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5 Ghz. Lo que la hace compatible con las redes que trabajan bajo los estándares 802.11b y 802.11g. Todas las versiones de 802.11xx, aportan la ventaja de ser compatibles entre sí, de forma que el usuario no necesitará nada más que su adaptador Wi-Fi integrado, para poder conectarse a la red (Oliva, 2005).

- **Velocidades de transferencia de datos en 802.11n**



*Figura 6. Esquema comparativo de velocidades 802.11n con tecnología MIMO.  
Fuente: (Belt, 2016).*

La figura anterior muestra un análisis comparativo de cómo mejora la tasa de transferencia de datos en el estándar 802.11n al hacer uso de la tecnología MIMO.

Suponiendo que los parámetros de funcionamiento son iguales, una red 802.11g puede alcanzar 54 Mbps en un solo canal 20 MHz con una antena, entonces una red 802.11n puede alcanzar 72 Mbps en un solo canal 20 MHz con una antena y 400ns intervalo guarda. La velocidad de 802.11n puede ir hasta 150 Mbps si no hay otras transmisiones como Bluetooth, microondas o Wi-Fi en la zona y hace uso de dos canales de 20 MHz en el modo de 40 MHz. Si se usan más antenas, 802.11n puede ir hasta 288 Mbps en el modo de 20 MHz con cuatro antenas, o 600 Mbps en el modo de 40 MHz con cuatro antenas y 400ns como intervalo de guarda (Oliva, 2005).

Debido a que la banda de 2,4 GHz está gravemente congestionada en la mayoría de las áreas urbanas, las redes 802.11n por lo general tienen más éxito en el aumento de velocidad de datos mediante la utilización de más antenas en 20 MHz en lugar de al operar en 40 MHz, ya que el modo de 40 MHz requiere más espectro de radio libre, y este sólo está disponible en las zonas rurales alejadas de las ciudades. Por lo tanto, los ingenieros que instalan una red en

802.11n deben esforzarse para seleccionar los routers y los clientes inalámbricos con la mayor cantidad de antenas posibles y tratar de asegurarse de que el ancho de banda de la red será satisfactorio incluso en 20MHz (Oliva, 2005).

- **Tecnología MIMO**

El estandar IEEE 802.11n se basa en el estandar inicial 802.11, pero agrega algunas mejoras como: la adición de múltiples entradas - múltiples salidas (MIMO- multiple-input multiple-output), la creación de canales de 40 MHz a la capa física y la agregación de tramas a la capa MAC (L. Marcelo, 2009).

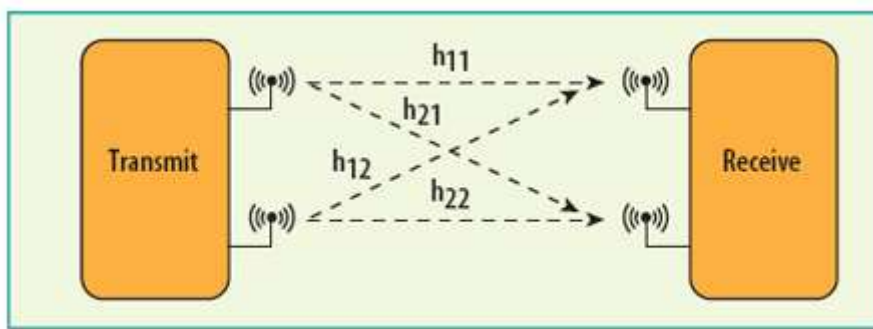


Figura 7. Esquema de un sistema típico de transmisión MIMO 2x2.  
Fuente: (Hall, 2009).

La figura anterior muestra un esquema típico de transmisión de un sistema de antenas 2x2 con múltiples entradas – múltiples salidas.

MIMO es un método utilizado para la multiplicación de la capacidad de un enlace de radio, utilizando múltiples antenas de transmisión y recepción, que a su vez explota el fenómeno físico de la multitrayectoria. Convirtiéndose en un elemento esencial en los estándares de comunicación inalámbrica IEEE 802.11n, IEEE 802.11ac y WiMAX (L. Marcelo, 2009).

En un tiempo, el término "MIMO" en redes inalámbricas, se refería principalmente a la teoría del uso de múltiples antenas en el transmisor y el receptor. Hoy en día "MIMO" se refiere específicamente a una técnica práctica para enviar y recibir más de una señal de datos

con el mismo canal de radio simultáneamente a través de la propagación multitrayecto. MIMO es fundamentalmente diferente de las técnicas de antenas inteligentes desarrolladas para mejorar el rendimiento de una única señal de datos (L. Marcelo, 2009).

El método usado es a través de multiplexación por división espacial (SDM), que espacialmente establece múltiples flujos de datos independientes, transferidos simultáneamente dentro de un canal de ancho de banda espectral. MIMO a través de SDM puede aumentar significativamente el rendimiento de datos y como el número de flujos de datos espaciales resueltos se incrementa, cada flujo espacial requiere una antena discreta tanto en el transmisor y el receptor. Además, la tecnología MIMO requiere una cadena de radiofrecuencia separado, y un convertidor independiente de analógico a digital para cada antena MIMO, por lo que implementarla es más costoso que los sistemas no-MIMO (L. Marcelo, 2009).

#### 2.2.1.5 IEEE 802.11ac

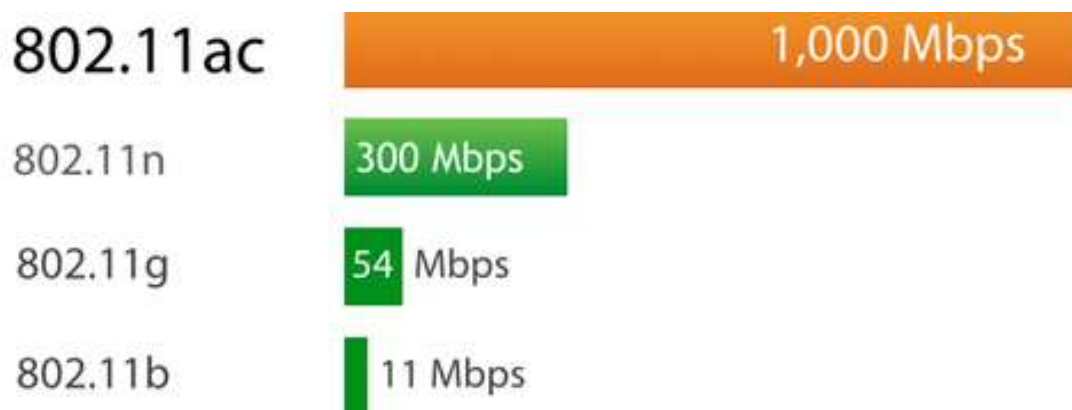


Figura 8. Velocidad de estándar 802.11ac.  
Fuente: (Bear Extender, 2014)

IEEE 802.11ac (también conocido como WiFi 5G o WiFi Gigabit), es una mejora a la norma IEEE 802.11n, que se ha desarrollado entre el año 2011 y el 2013, y finalmente aprobada en enero de 2014.

El ancho de canal para la transmisión en el estándar 802.11n tiene un máximo de 40MHz, y ahora el estándar 802.11ac lo incrementa hasta 80MHz o incluso hasta 160MHz, aumentando aún más la velocidad de datos por cada radio.

El estándar 802.11ac ahora emplea QAM<sup>13</sup>, Modulación de amplitud en cuadratura, lo que significa altas tasas de transferencia de datos.

Multi-user MIMO (MU-MIMO): Soporte de transmisiones simultáneas a múltiples clientes, maximizando la utilización de la banda RF.

El estándar 802.11ac opera únicamente en la banda de los 5GHz donde hay menos ruido e interferencia de tecnologías competidoras. Además, en esta banda hay mucho espacio disponible, lo que permite aumentar el número de canales de flujo en esta banda, a diferencia de los tres existentes en el 802.11n.

Debido a que se utilizará la banda de los 5GHz, 802.11ac tiene menos alcance que la banda de 2.4GHz en las mismas condiciones por un principio físico. Este nuevo estándar incluye **Beamforming** para transmisión y recepción.

Beamforming es un tipo de categoría MIMO que consiste en la formación de una onda de señal reforzada mediante el desfase en distintas antenas y es capaz de superar obstáculos llegando hasta al cliente por el mejor camino. Beamforming reconoce los elementos que causan un bajo rendimiento como muros y paredes e intenta evitarlos (Meden Peralta, 2013).

---

<sup>13</sup> Quadrature Amplitude Modulation. Modulación de amplitud en cuadratura es una técnica que transporta dos señales independientes mediante la modulación de una señal portadora.

## **2.3 Topologías de red**

Es el mapa físico o lógico de una red de datos, que permite intercambiar información entre dos o varios nodos interconectados. La topología de red es la que determina la distribución geométrica de los elementos de red, como: hubs, switches, routers, access point, estaciones fijas y estaciones móviles. La topología también es encargada de la configuración de los elementos interconectados entre nodos, las distancias y las tasas de transmisión, según el tipo de red, las topologías pueden ser clasificadas en topologías de redes LAN y topologías de redes WLAN (Cabeza, 2009).

### **2.3.1 Topología de redes LAN**

Las topologías más conocidas para la interconexión de nodos en Redes de Área Local, según la distribución física pueden ser clasificadas en:

- Red tipo bus
- Red tipo estrella
- Red tipo anillo
- Red tipo árbol

### 2.3.1.1 Topología tipo bus

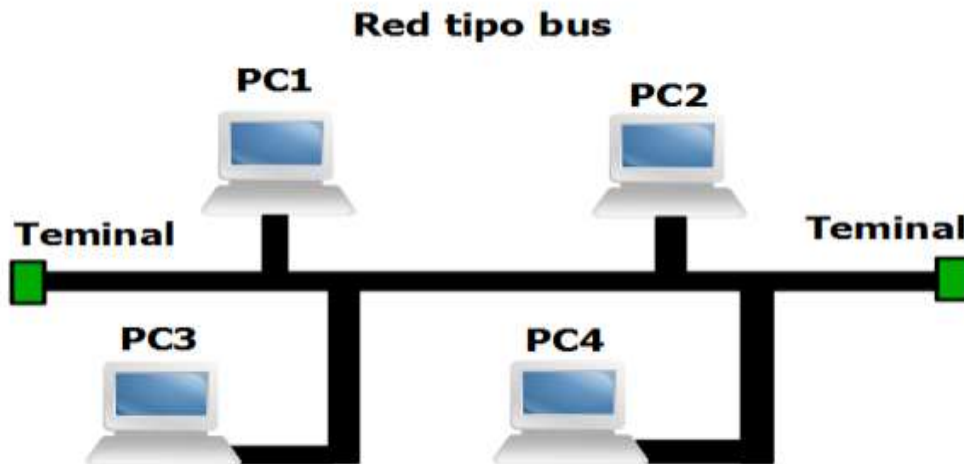


Figura 9. Topología de red tipo bus. Diseñado en GNS314.  
Fuente: Propia

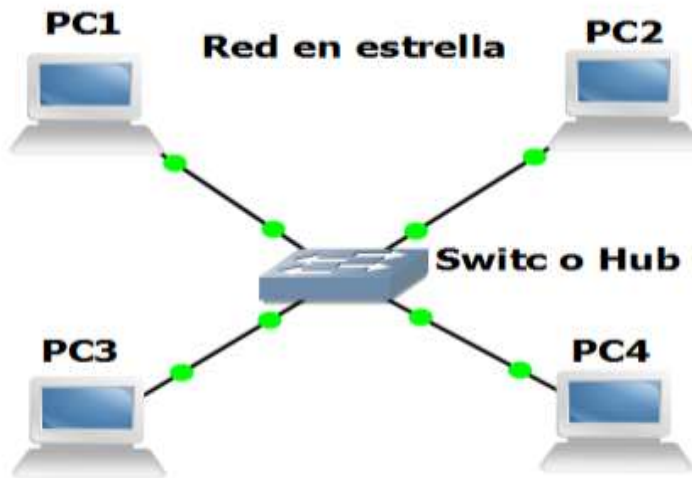
En este tipo de topología de red todas las computadoras están conectadas a un circuito común, también llamado backbone, en este tipo de conexión se comparte la información de manera directa o indirecta a través de un medio físico que puede ser: cable coaxial, par trenzado o fibra óptica. La comunicación en esta topología tiene la ventaja de que, al haber una falla de un host, el enlace de datos de los demás hosts, sigue arriba, pero la desventaja es que, si falla el circuito común, toda la red cae.

Se pueden conectar una gran cantidad de computadoras al mismo bus, ya que comparten el mismo segmento de red, siendo como un cable largo que va de extremo a extremo conectando cada nodo (Cabeza, 2009).

---

<sup>14</sup> GNS3. Es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos.

### 2.3.1.2 Topología tipo estrella



*Figura 10. Topología de red tipo estrella.  
Fuente: Propia*

Una red estrella es una red de computadores donde las estaciones están conectadas directamente a un nodo central activo, que normalmente es capaz establecer las comunicaciones entre estaciones y prevenir problemas relacionados con el eco. Esta red es normalmente usada en redes de área local, en las que se tiene un router, un switch, y a veces un hub, entonces el nodo central activo sería el switch o el hub, ya que por el pasan todo el paquete desde y hacia las estaciones finales de la red (Cabeza, 2009).

#### **Ventajas:**

- El nodo central tiene medios para prevenir problemas en toda la red.
- Si una estación se desconecta o es roto su medio de trasmisión, solo queda fuera dicha estación.
- Su facilidad para prevenir caídas.
- Permite que la comunicación entre nodos sea de manera coordinada.
- La administración de esta red más fácil, que otras topologías de red.



### Desventajas:

- Si el nodo central falla, toda la red falla.
- Es más costosa en comparación a una topología tipo bus o anillo, ya que, en esta, se requiere más cable.

#### 2.3.1.3 Topología tipo anillo

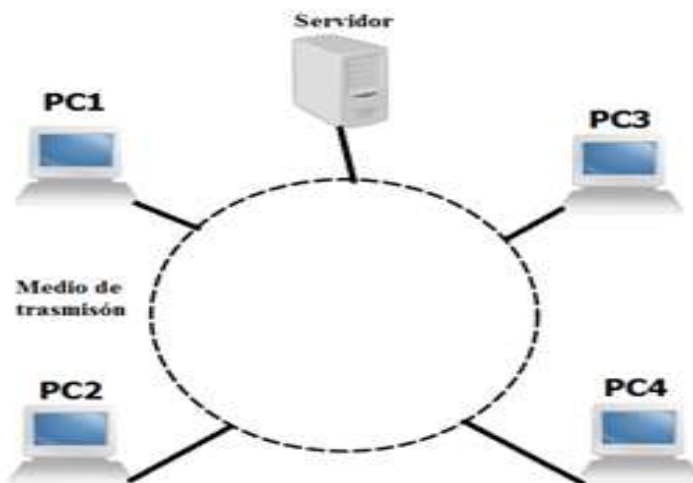


Figura 11. Topología de red tipo anillo.

Fuente: Propia

En una topología tipo anillo, cada estación tiene una conexión de entrada y otra de salida, cada estación hace una retransmisión, para pasar la señal a la siguiente estación.

La topología anillo, como su nombre lo indica, consiste en conectar linealmente entre sí el total de computadores, en un bucle cerrado. La información en esta topología se transmite de en un solo sentido de a través del anillo, mediante un paquete especial de datos llamado token, o testigo, que se asemeja, a un mensajero que pasa recogiendo y entregando información, evitando de esta manera eventuales pérdidas de la información.

Se puede formar un anillo doble o también llamado token ring, la formación de estos dos anillos, permiten enviar datos en las dos direcciones, para brindar redundancia y evitar colisiones (Cabeza, 2009).

#### 2.3.1.4 Topología tipo árbol

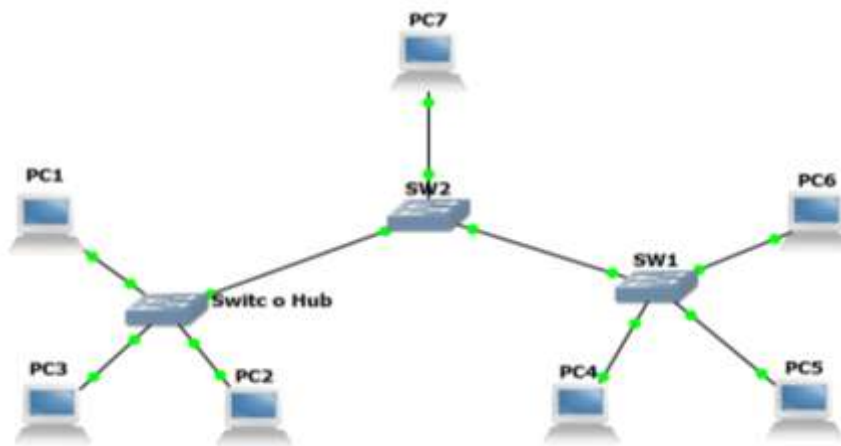


Figura 12. Topología de red tipo árbol.  
Fuente: Propia

Es una topología que interconecta varias, redes en topología tipo estrella, pero tiene un nodo central, pero en cambio tiene un nodo de enlace troncal, que generalmente puede ser un switch o hub, desde donde se ramifican los demás nodos. En realidad, es la variación de una red tipo bus, en donde la falla de un nodo no implica la interrupción de los demás.

La topología tipo árbol, podría verse como una combinación de varias topologías tipo estrella, en donde tanto el árbol como la estrella son similares de un bus, cuando el nodo de interconexión trabaja en modo difusión.

La información se propaga a todas las ramificaciones del árbol desde un punto raíz, según sus características de transmisión. La mayoría de problemas en este tipo de redes es que comparten un mismo medio de transmisión y la información debe pasar por todas las estaciones sin importar cuál es el destino de la misma, para esto es necesario usar mecanismos que permitan identificar el destino que tienen los paquetes (Cabeza, 2009).

### 2.3.2 Topología de redes WLAN

Una topología de redes inalámbricas está basada en una arquitectura celular, donde, el sistema está dividida celdas llamadas conjunto de servicios básicos (BSS)<sup>15</sup>, y cada una de estas celdas es controlada por una estación base denominada punto de acceso (AP). Aunque una red inalámbrica puede estar formada por una sola celda, normalmente se usan varias celdas, donde los puntos de acceso están conectados, por medio de un sistema de distribución (DS), que puede ser Ethernet o sin cables.

En base a lo descrito anteriormente existen dos tipos de topologías, bien conocidas, en redes inalámbricas (Cabeza, 2009).

#### 2.3.2.1 Red AD-HOC



*Figura 13. Topología de red tipo ad-hoc.  
Fuente: Propia*

Una red Ad-hoc es una red de conexión simple, entre dos o más estaciones por un tiempo ilimitado que no están conectados a través de un punto de acceso (AP), a una red cableada. Este tipo de red es también llamada red entre pares, en donde se conectan varios dispositivos para

<sup>15</sup> BSS. Es un modo de red inalámbrica, también denominado modo infraestructura. En esta configuración se conectan un determinado número de puntos de acceso a una red cableada.

intercambiar información, sin la necesidad de elementos auxiliares como APs. Estas son redes punto a punto, fácil de configurar, para un conjunto básico de servicios independientes (Cabeza, 2009).

### 2.3.2.2 Infraestructura

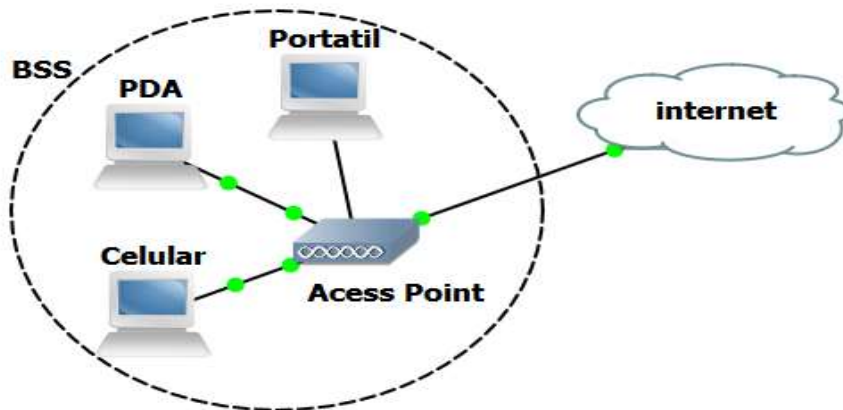


Figura 14. Topología de red tipo infraestructura.  
Fuente: Propia

Es esta topología los dispositivos o estaciones, se conectan a través de un equipo central que trabaja como elemento coordinador, el mismo que puede ser, punto de acceso (AP), o estación base, cada AP irradia una zona de cobertura que se denomina célula. Si el punto de acceso se conecta a una red Ethernet cableada, entonces las estaciones finales, pueden compartir información a través de dicho punto de acceso.

Se puede interconectar varios puntos de acceso, para maximizar la zona de cobertura, entonces se debe configurar el mismo SSID<sup>16</sup>, en todos los APs, pero no se debe usar el mismo canal en todos los APs, que se encuentren en la misma área física de cobertura, ya que los clientes se encargan de identificar el canal de transmisión. En redes IEEE 802.11, el modo

<sup>16</sup> SSID. Nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. A menudo al SSID se le conoce como “nombre de la red”.

infraestructura, es conocido como conjunto de servicios básicos (BSS – BASIC SERVICE SET) (Cabeza, 2009).

## **2.4 RouterOS Mikrotik**

### **2.4.1 Introducción a Mikrotik**

Cuando Arnis Riekstins y John Tully, dueños y fundadores de Mikrotik, tuvieron que hacer su tesis de universidad pensaron en un router basado en Linux que tenga las mismas funcionalidades de los routers del mercado. Luego en 1995 lanzaron las soluciones para proveedores de Internet, en el año 1996 se ingresa al mundo de WISPs<sup>17</sup> alrededor del mundo. Rápidamente fue creciendo y tomando mercado en un mundo de las telecomunicaciones cada vez más próspero.

En 1997 diseñaron su propio software para PC Intel brindando soluciones de ruteo, a medida que fueron pasando los años se le agregaron muchas funcionalidades, como la parte inalámbrica, un mejor control de ancho de banda y calidad de servicio.

En el año 2002 iniciaron el proyecto de hardware y crearon el primer RouterBoard 230, luego se agregaron una amplia gama de RouterBoards RB, como los de la serie RB500, RB100, RB300, RB600 y los poderosos RB400 y RB1000.

Hoy es una empresa que tiene más de 70 empleados y que está ubicada en Riga, capital de Latvia, un país ex integrante la Unión Soviética en el este de Europa. Es una empresa muy prometedora, que ha crecido notablemente, imponiéndose en un mercado emergente como el del wireless.

Mikrotikls Ltd., conocida internacionalmente como MikroTik, es una compañía letona proveedora de tecnología disruptiva de hardware y software para la creación de redes.

---

<sup>17</sup> WISP. Es un proveedor de Servicio de Internet Inalámbrico.

MikroTik se dedica principalmente a la venta de productos de hardware de red como routers denominados routerboards y switches también conocidos por el software que los integra, denominado RouterOS y SwOS (Pugliese, 2014).

#### **2.4.2 RouterOS**

Mikrotik RouterOS o simplemente RouterOS es un software que funciona como un Sistema Operativo para convertir una PC o una placa Mikrotik RouterBoard<sup>18</sup> en un router dedicado.

RouterOS es un sistema operativo basado en GNU/Linux que implementa funcionalidades que los NSP e ISP tienden a usar, como enrutamiento, cortafuegos, gestión de ancho banda, punto de acceso inalámbrico, BGP, IPv6, OSPF y MPLS.

RouterOS es un sistema versátil, con un soporte muy avanzado por parte de MikroTik, tanto a través de foros como a través de su wiki, proporcionando una amplia variedad de ejemplos de configuración.

La venta de RouterOS, combinado con su línea de productos hardware conocida como MikroTik RouterBoard, está enfocada a pequeños y medianos proveedores de acceso a Internet, que normalmente proporcionan acceso de banda ancha en áreas remotas.

RouterOS es un sistema operativo independiente basado en el núcleo Linux v2.6, y el objetivo de Mikrotik es proporcionar todas estas funciones con un rápido acceso, instalación sencilla

y una interfaz fácil de usar.

---

<sup>18</sup> RouterBoard. son miniCPU con avanzadas prestaciones para redes de datos.

## Fechas de lanzamiento de RouterOS

- v6 - Mayo de 2013
- v5 - Marzo de 2010
- v4 - Octubre de 2009
- v3 - Enero de 2008

Routerboard es el hardware de MikroTik caracterizado por incluir su sistema operativo RouterOS por defecto y actualizaciones de por vida. Estos dispositivos tienen la ventaja de tener una buena relación calidad/precio (Pugliese, 2014).

### 2.4.3 Configuración de RouterOS

RouterOS admite varios métodos de configuración de acceso locales: con teclado y monitor, vía consola con una aplicación terminal, Telnet y acceso seguro a través de SSH, una herramienta de configuración GUI personalizada llamada Winbox, mediante una sencilla interfaz de configuración basada en web. En caso de que no haya acceso local y hay un problema con el nivel de comunicaciones IP, también RouterOS es compatible con una conexión basada en el nivel MAC a través de la herramienta WinBox (Pugliese, 2014).

## 2.5 Centralización de redes Wi-Fi

Originalmente en los sistemas Wi-Fi autónomos. Cada punto de acceso tenía toda la capacidad para crear la celda y gestionar los clientes asociados a ella, incluso las comunicaciones hacia la red cableada.

Cuando las redes Wi-Fi pasaron de ser una solución puntual a solventar problemas de instalaciones complejas y de gran escala, se vio la necesidad de disponer de sistemas de gestión centralizados que faciliten su administración.

En inicios, la aparición de estos sistemas se vio limitada por el alto precio de los puntos de acceso. Para abaratar las grandes instalaciones, se tomó la decisión de hacer puntos de accesos

menos inteligentes, y se transfirió la inteligencia a un sistema de gestión centralizado. Es cierto que este sistema de control suele tener un costo elevado, pero al ser la red muy extensa, la reducción en el precio de cada punto de acceso compensa el costo total del sistema central (SlideShare, 2015).

Con el tiempo, las redes Wi-Fi fueron soportando más servicios y se demandó cada vez más de ella, teniendo que aportar más opciones de configuración y funcionalidades que las hicieran aptas para las aplicaciones y servicios que demande el usuario final. En instalaciones con un elevado número de puntos de acceso, la configuración manual de cada uno de ellos y su mantenimiento, así como la detección y corrección de errores se tornó compleja y el coste en tiempo y personal demasiado elevado (Simal, Observatorio Tecnológico, 2011).

Los sistemas de gestión centralizados tienen como objetivo disminuir estos problemas y ofrecer funcionalidades añadidas.

Es cierto que no se pueden enumerar las funcionalidades de estos sistemas, puesto que no existe un modelo y cada fabricante toma la aproximación que le parece más conveniente, pero suele tener algunas características y funcionalidades básicas comunes.

Habitualmente el controlador se vende como un sistema independiente cerrado, pero internamente es siempre un ordenador con un software asociado y pre instalado, al cual el usuario no tiene acceso más que por la consola de configuración. En cualquier caso, los controladores se conectarán en la red Ethernet del cliente desde la que detectarán a los puntos de acceso con los que sea compatible. Una vez detectados, realizará una configuración previa de estos y permitirá su gestión centralizada desde un solo punto (Simal, Observatorio Tecnológico, 2011).

Dependiendo el fabricante, se implementarán distintas medidas para elegir los puntos de acceso que han de ser gestionado, ya sea mediante una pre configuración de la dirección IP en el punto de acceso, o mediante algún tipo de filtrado y/o clave en el controlador. Una vez



añadido el punto de acceso se le cargara automáticamente una configuración base, lo cual reduce los tiempos de instalación y minimiza los errores de configuración.

El objetivo general de esta fase es que la instalación de nuevos sistemas se simplifique.

Una vez realizado el despliegue inicial el controlador permitirá desde una sola consola configurar los distintos puntos de acceso, individualmente, por grupos o globalmente, así como recibir alarmas asociadas al funcionamiento de ellos (Butler, Pietrosevoli, Zennaro, & Fonda, 2013).

Como se ha comentado, la funcionalidad depende de cada fabricante, pero estas son algunas de las funciones ofrecidas:

- **Gestión centralizada:** Una sola consola para gestionar los distintos puntos de acceso.
- **Centralización de eventos:** En instalaciones amplias, con un elevado número de puntos de acceso, resulta inviable acceder a cada uno de ellos para tener conocimiento de los eventos acontecidos y posteriormente relacionar los datos obtenidos de cada uno de ellos. El controlador permite automatizar este proceso con un ahorro en costes y un aumento en la fiabilidad de la red.
- **Servicios de localización de clientes Wi-Fi:** Puesto que el sistema de gestión centralizada controla todos los puntos de acceso, es capaz de obtener los datos de potencia de recepción que cada uno de ellos obtiene de cada uno de los clientes. Gracias a estos datos, relacionando los que distintos puntos de acceso obtienen de un mismo cliente, por triangulación y conociendo previamente la localización de los puntos de acceso (datos que deberán ser introducidos manualmente previamente) el gestor será capaz de obtener la localización de los terminales.
- **Respuesta automatizada ante fallos.** Es posible, por ejemplo, que ante el fallo de un punto de acceso, el controlador, de forma automática active alguno que estuviera de reemplazo,

o aumente la potencia de los circundantes para aumente su cobertura y cubrir el área que se quedó sin servicio.

- **Gestión de la calidad de servicio:** Puede priorizar, penar o controlar el tráfico de ciertas aplicaciones, servicios o usuarios.
- **Tunelización:** Es posible ofrecer el servicio de que los datos de la red Wi-Fi no sean inyectados a la red cableada directamente por el punto de acceso, si no que se genere un túnel entre este y el gestor centralizado. De esta manera se permite que el gestor pueda controlar los datos del cliente realizando sobre ellos funciones como priorización, filtrado y monitorización.
- **Gestión de estructuras de red “mesh”:** La incorporación de un gestor permitirá la elección de forma automática de los enlaces atendiendo a la calidad de estos de manera que se optimicen los caminos y por tanto el rendimiento y fiabilidad. Además, es posible que el gestor, ante el fallo de un punto de acceso o un enlace, recomponga de forma automática la arquitectura de la malla de forma que la comunicación se mantenga (Kleinrock, 2011).

## **2.6 Gestión centralizada de redes Wi-Fi con CAPsMAN**

El administrador de sistema de punto de acceso controlado (CAPsMAN - Controlled Access Point system Manager) permite la centralización de la gestión de redes inalámbricas y si es necesario el procesamiento de datos. Al utilizar la función CAPsMAN, la red consistirá en una serie de puntos de acceso controlados (CAP) que proporcionan conectividad inalámbrica y un Administrador del sistema (CAPsMAN) que gestiona la configuración de los puntos de acceso, se encarga de la autenticación del cliente y opcionalmente del reenvío de datos (Mikrotik, 2015).

Cuando un CAP es controlado por CAPsMAN que sólo requiere la configuración mínima requerida para permitir que se establezca la conexión. Las funciones que tradicionalmente fueron ejecutados por un punto de acceso como el control de acceso y autenticación de clientes,

ahora están ejecutados por CAPsMAN. El dispositivo CAP ahora solamente tiene que proporcionar a la capa de enlace inalámbrico datos de cifrado y descifrado (Mikrotik, 2015).

Para que el sistema CAPsMAN pueda funcionar y proporcionar conectividad inalámbrica, a un CAP se debe establecer la conexión con gestor CAPsMAN. Una conexión de gestión se puede establecer a través de protocolos de capa MAC o IP.

Un CAP también puede pasar la conexión de datos del cliente al administrador, pero la conexión de datos no siempre está asegurada. Es necesario considerar otros medios de seguridad para los datos, por ejemplo, IPSec o túneles cifrados.

Una conexión del CAP al CAPsMAN puede establecerse por medio de 2 mecanismos de transporte, a través de la Capa 2 o capa 3 (Mikrotik, 2015).

### **2.6.1 Requerimientos de funcionamiento**

- CAPsMAN funciona en cualquier dispositivo de RouterOS a partir de la versión 6.11.
- No se requieren interfaces inalámbricas ya que gestiona las interfaces inalámbricas en el CAP.
- CAPsMAN v2 está trabajando a partir de RouterOS v6.22rc7.
- El dispositivo CAP debe tener una licencia RouterOS al menos Nivel 4 y al menos una interfaz inalámbrica.

### **2.7 Gestión de usuarios mediante Hotspot**

Un Hotspot es un lugar físico donde las personas pueden obtener acceso a Internet, normalmente utilizando tecnología Wi-Fi, a través de una red inalámbrica de área local (WLAN), que a su vez está conectado a un proveedor de servicios de Internet por medio de un router.

Los hotspot públicos pueden encontrarse en un creciente número de empresas para uso de los clientes principalmente en áreas urbanas desarrolladas a través de todo el mundo. Muchos

hoteles ofrecen acceso Wi-Fi a sus clientes, ya sea en las habitaciones o en los pasillos a través de hotspot.

Normalmente, los hotspots son zonas de alta demanda de tráfico que por tanto el dimensionamiento de su cobertura está condicionado a cubrir esta demanda por parte de uno o varios puntos de acceso, y de este modo proporcionar servicios de red a través de un proveedor de servicios de Internet Inalámbrico (WISP). Los hotspots se encuentran en lugares públicos, como aeropuertos, bibliotecas, centros de convenciones, cafeterías, hoteles, universidades, etcétera. Este servicio puede hacer uso de la red Wi-Fi y permite mantenerse conectado a Internet en lugares públicos. Puede brindarse de manera gratuita o pagando una suma que depende del proveedor. Cuando un usuario intenta acceder a internet a través del navegador a este se le presenta una pantalla de inicio de sesión, en donde una vez que registra usuario y contraseña inmediatamente puede hacer uso de los servicios de la red (Wifi Safe, 2015).

### **2.7.1 Hotspot de Mikrotik**

HotSpot es una manera de autorizar a los usuarios y tener acceso a algunos recursos de la red, pero no proporciona cifrado del tráfico. Para iniciar la sesión, los usuarios pueden utilizar casi cualquier navegador web (HTTP o HTTPS), por lo que no es necesario instalar software adicional. El gateway hotspot es el encargado de la contabilidad del tiempo de actividad y la cantidad de tráfico utilizado por cada cliente, y también se puede enviar esta información a un servidor RADIUS. El sistema HotSpot puede limitar la tasa de transferencia de datos de cada usuario en particular, cantidad total de tráfico, el tiempo de actividad permitida, entre otros parámetros.

El sistema de HotSpot está dirigido a proporcionar autenticación en una red local, pero también puede ser utilizado para autorizar el acceso a redes externas. Es posible permitir a los usuarios acceder a algunas páginas web sin autenticación utilizando la función de Walled Garden.

En primer lugar, un cliente tiene que obtener una dirección IP. Esta puede establecerse en el cliente de forma estática, o desde un servidor DHCP. Al sistema de HotSpot no le importa cómo el cliente obtiene su dirección antes de que el obtenga acceso a la página de acceso público.

Al activar el HotSpot en una interfaz, el sistema configura automáticamente todo lo necesario para mostrar la página de inicio de sesión para todos los clientes no identificados. Esto se hace mediante la adición de reglas dinámicas de NAT de destino, que se pueden observar en un sistema de trabajo del HotSpot. Estas normas son necesarias para redirigir todas las peticiones HTTP y HTTPS de usuarios no autorizados a la página de autenticación (Mikrotik, 2015).

## **2.8 Calidad de servicio**

El entorno inalámbrico es muy hostil para medidas de Calidad de Servicio debido a su variabilidad con el tiempo, ya que puede mostrar una calidad nula en un cierto instante de tiempo. Esto implica que satisfacer la QoS resulta imposible para el 100% de los casos, lo que representa un serio desafío para la implementación de restricciones de máximo retardo y máxima varianza en el retardo (jitter)<sup>19</sup> en sistemas inalámbricos.

Los sistemas de comunicaciones ya estandarizados con restricciones QoS de retardo y jitter en entornos inalámbricos (por ejemplo, en GSM y UMTS) sólo pueden garantizar los requisitos para un porcentaje (<100%) de los casos. Esto implica una caída del servicio (Outage o downtime en inglés), generando los cortes de llamadas y/o los mensajes de “red ocupada”. Por otro lado, algunas aplicaciones de datos (por ejemplo, WiFi) no requieren de restricciones de máximo retardo y jitter, por lo que su transmisión sólo necesita de la calidad media del canal, evitando la existencia de caídas del servicio.

---

<sup>19</sup> JITTER. Variabilidad temporal durante el envío de señales digitales. Suele considerarse una señal de ruido no deseada que provoca un cambio abrupto e indeseado de la amplitud, frecuencia o fase de la señal.

También se puede asignar prioridad a los paquetes, a las conexiones, tiempos específicos, ráfagas de ancho de banda, control de ancho de banda de subida, el ancho de banda de bajada, ancho de banda mínimo garantizado, entre otros.

Logrando con esta herramienta hacer que, los usuarios utilicen el ancho de banda adecuado, sin que perjudique a los otros usuarios, permitiendo que todos los usuarios naveguen de una forma racionalizada, optimizando de esta forma los recursos tanto de hardware como de software, y el ancho de banda, consiguiendo con esto que todos los usuarios tengan la percepción, de tener una navegación rápida (Simal, Observatorio Tecnológico, 2011).

### 2.8.1 Calidad de servicio con encolamiento PCQ

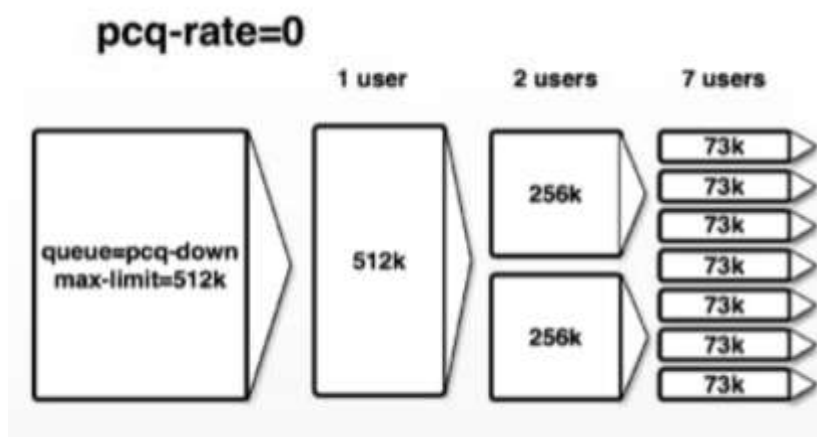


Figura 15. Esquema de Calidad de servicio usando encolamiento PCQ.  
Fuente: (Mikrotik, 2010)

El encolamiento simple PCQ (Por cada cola de conexión- Per Connection Queue) se introdujo para optimizar los sistemas de calidad de servicio masivos, donde la mayoría de las colas son exactamente los mismos para diferentes flujos de datos. Por ejemplo, un sub-flujo de datos se puede descargar o cargar para un cliente en particular hacia el servidor.

El Algoritmo PCQ es muy simple, en un primer momento se utiliza clasificadores seleccionados para distinguir una sub-corriente de otra, entonces se aplica tamaño de la cola

FIFO<sup>20</sup> individual y limitación en todos los sub-corriente, luego grupos de todas las sub-corrientes juntos y aplica tamaño de la cola global y limitación.

El sistema de colas PCQ, es un sistema de control de ancho de banda dinámico, que permite asignación de recurso ancho de banda de manera simétrico, según el número de conexiones establecidas en una misma interfaz, el mismo que permite controlar tanto el tráfico de carga como el de descarga (Mikrotik, 2010).

## 2.9 Criterios de diseño

### 2.9.1 Criterio de selección de canales

La diferencia de la cantidad de espectro si licencia es significativo y para la banda de 2.4GHz se compone por 3 canales “1, 6 y 11” de 20 MHz que no se solapan. En Japón existen 4 canales que no se solapan, pero el uso del canal 14 está restringido para DSSS/CCK<sup>21</sup> (Homotech, 2016).

En la siguiente imagen se puede observar claramente cómo se encuentra distribuido el espectro de canales.

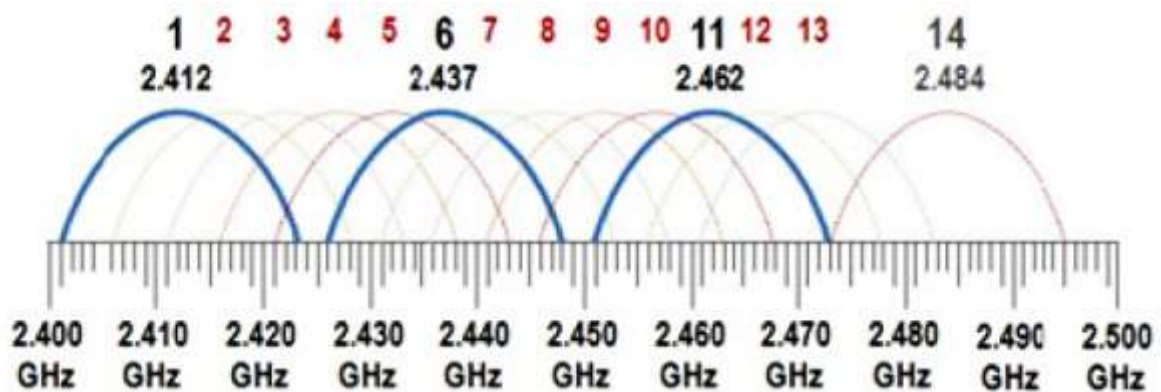


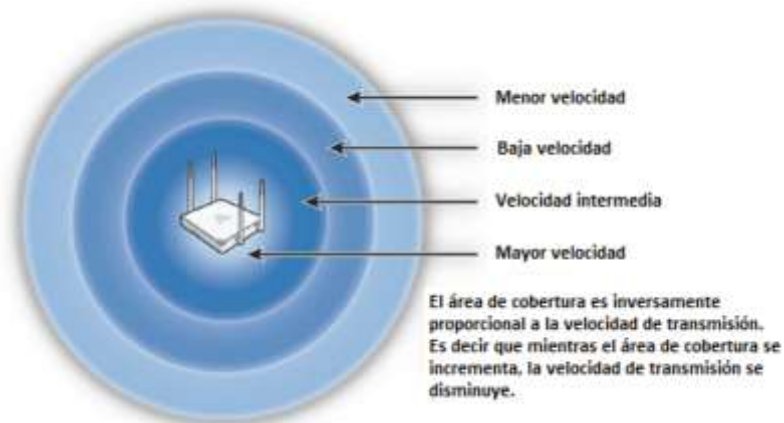
Figura 16. Relación de canales en el espectro de 2.4 GHz

Fuente: (Homotech, 2016)

<sup>20</sup> FIFO. Primero en entrar, primero en salir (First In First Out) es un concepto utilizado en estructura de datos y teoría de colas.

<sup>21</sup> DSSS/CCK. Direct Sequence Spread-Spectrum Complementary Code Keying (Codificación de código complementario de espectro de dispersión de secuencia directa)

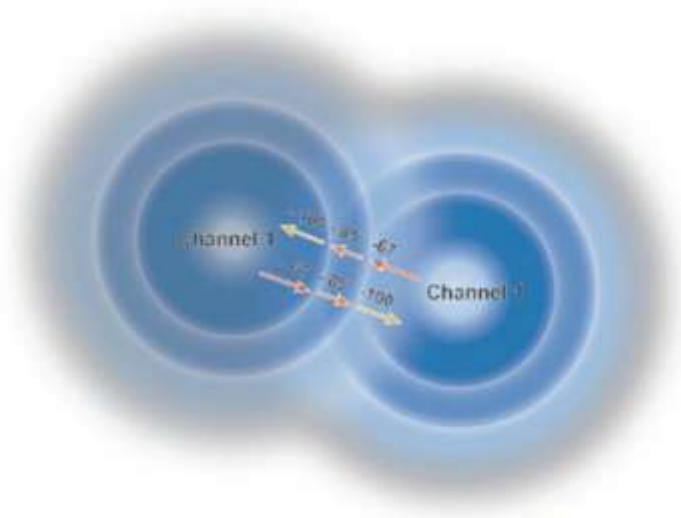
Para minimizar la interferencia co-canal se mide en base a la distancia a la que los usuarios pueden asociarse y la distancia a la que la señal del AP crea interferencia de canales con los otros APs creándose así una significativa reducción del rendimiento y la capacidad de la red (Homotech, 2016).



*Figura 17. Velocidad de datos vs. rango de cobertura*

*Fuente: (Homotech, 2016)*

Por esta razón el administrador de la red debe diseñar celdas con solapamiento entre los diferentes APs de la red e implementar un plan de canales que reduzca la interferencia entre los Access Points (Homotech, 2016).



*Figura 18. Interferencia co-canal*

*Fuente: (Homotech, 2016)*



## 2.9.2 Adaptar el diseño a las instalaciones

Para el diseño de la red wifi se debe tener en cuenta el diseño y las características de la infraestructura física donde será instalado el servicio, los materiales utilizados para la construcción pueden llegar a tener un fuerte impacto en la atenuación de la intensidad de señal, en algunos casos es necesario utilizar varios APs en las zonas de mayor interferencia (Homotech, 2016).

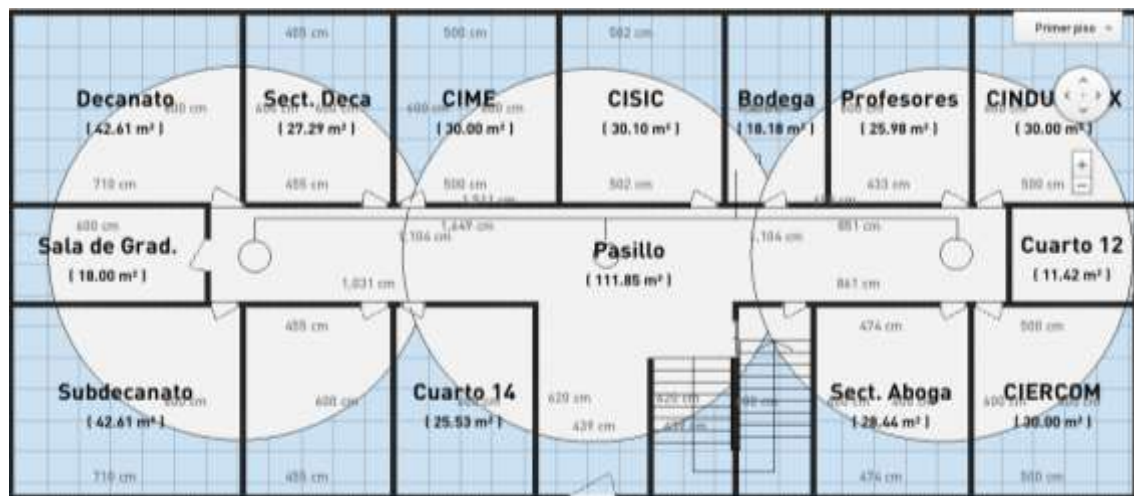


Figura 19. Diseño de rangos de cobertura  
Fuente:

## 2.9.3 Capacidad adecuada

“Al realizar un diseño con una cobertura básica dentro del área de cobertura, puede satisfacer las necesidades del usuario, pero puede generar una capacidad reducida de usuarios, pero existen ciertas diferencias entre las capacidades de las redes wifi y crear un diseño de cobertura orientado a satisfacer las necesidades de rendimiento puede resumirse bajo los siguientes métodos:

- Reducción de la interferencia entre canales vecinos.
- Maximización de la capacidad espectral a través del uso de diferentes frecuencias.
- Optimizar el ancho de banda para mejorar el uso de la capacidad espectral disponible.

- Equilibrar el número de clientes por cada AP.
- Realizar un diseño en base a la calidad del servicio.” (Hometech, 2016).

Fórmula para calcular los puntos de acceso necesarios por cada piso

$$\#AP = \frac{\text{Anchodebanda} \times N^{\circ}\text{Usuarios} \times \%Uso}{\text{VelocidadProgramada}}$$

- Ancho de banda deseado para cada usuario: 1Mbps
- Número de usuarios: 75
- Uso promedio de la red: 25%
- Velocidad estimada por AP: 6Mbps

$$3,125 = \frac{1 \text{ Mbps} \times 75 \text{ Usuarios} \times 0.25}{6}$$

*Ecuación 1. Cálculo de puntos de acceso necesarios  
Fuente: Propia*

#### **2.9.4 Roaming WiFi (Movilidad)**

En los puntos de acceso inalámbricos aproximadamente se dispone de 100 metros de cobertura, pero varía entre modelos y marcas de fabricantes de los dispositivos. Lo que interesa es permitir la (intinerancia o roaming) movilidad de los usuarios, colocando los puntos de acceso de tal forma que exista una superposición entre el perímetro de cobertura.

Se puede observar en la siguiente figura el solapamiento indicado por la marca de color rojo y la flecha verde el sentido de desplazamiento del usuario que pasa de recibir la señal A hacia la señal B (López Barnés, 2008).

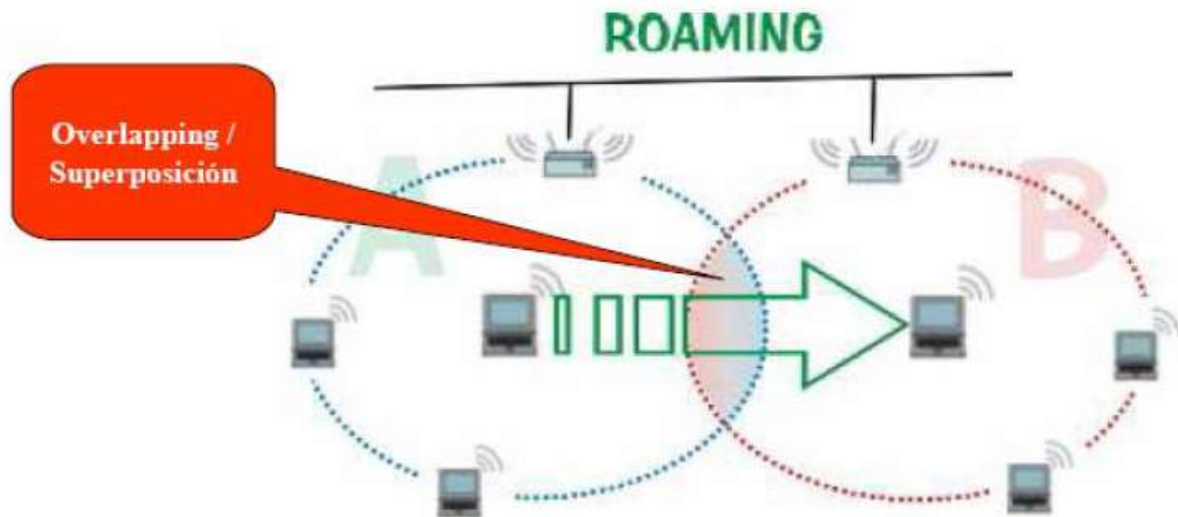


Figura 20. Roaming  
Fuente: (López Barnés, 2008)

El proceso de roaming puede funcionar por medio de paquetes Beacons y de paquetes ACK (López Barnés, 2008).

- **Paquetes beacons**

Los puntos de acceso inalámbricos intermitentemente emiten unos paquetes llamados beacons y cuando una estación se aleja demasiado del AP deja de emitir beacons que son aquellos que indican la presencia de señal; cuando existe el solapamiento o superposición cuando se aleja del AP que emite los beacons se empiezan a captar los beacons del siguiente AP al que se está dirigiendo para realizar el nuevo enlace (López Barnés, 2008).

- **Paquetes ACK**

En la transición de información en WiFi cuando se envían paquetes de datos dentro de la red inalámbrica la estación receptora emite un OK llamado ACK; cuando la estación emisora se aleja deja de captar los ACK enviados, gracias a que los dispositivos WiFi poseen un algoritmo que determinan el momento en que se desconecta del punto A y se conecta al punto B (López Barnés, 2008).



## CAPITULO III

### 3 Propuesta del proyecto

#### 3.1 Situación actual de la red Wi-Fi de la FICA

##### 3.1.1 Descripción geográfica

La UNIVERSIDAD TECNICA DEL NORTE se encuentra ubicada la ciudad de Ibarra, situada al Norte del país, a 115 Km al suroeste de Quito y 125 Km de Tulcán, con una altitud de 2192 metros sobre el nivel del mar, una población de 153.256 habitantes aproximadamente según el censo del año 2001, Población Urbana 108535, Población Rural 44721, su latitud bordea los 00° 21' N y su longitud 078° 07' O siendo parte de la provincia de Imbabura país Ecuador, es actualmente una de las referentes instituciones educativas de nivel superior, del norte del país, la cual se ha destacado por su valioso aporte, dentro de la sociedad, a nivel nacional e internacional, siendo la cuna de valiosos profesionales, quien han aportado soluciones a innumerables problemas que surgen en la sociedad.

Dentro de la UNIVERSIDAD TECNICA DEL NORTE, tenemos la Facultad de Ingeniería en Ciencias Aplicadas (FICA), ubicada en sector norte del campus universitario, y siendo una de las facultades más destacadas, en el desarrollo tecnológico que actualmente aporta la universidad.

La FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS FICA, es un edificio de consta de cinco pisos incluyendo la planta baja, cada piso tiene un pasillo central a lo largo del cual, se facilita el acceso a las aulas de sus alrededores.

### 3.1.2 Situación tecnológica actual

#### 3.1.2.1 Topología física y lógica de la red existente

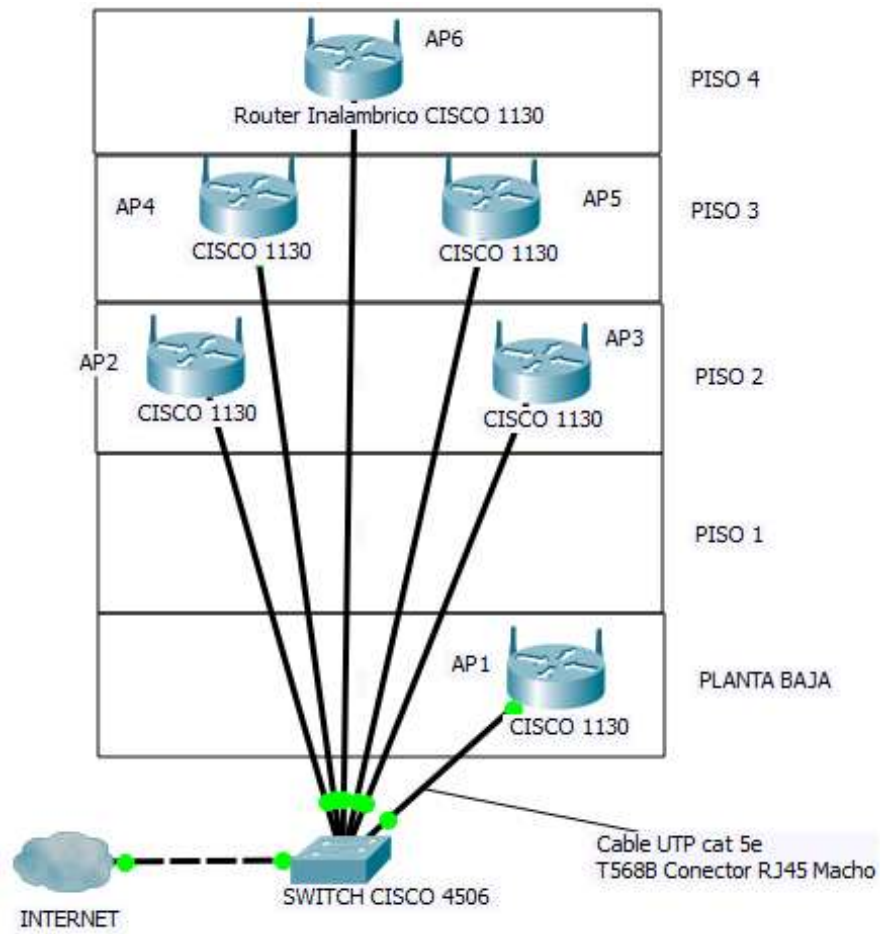


Figura 21. Topología física de la red existente en la FICA  
Fuente: Propia

La figura anterior muestra la topología física de cómo se encuentra estructurada la red existente en la FICA.

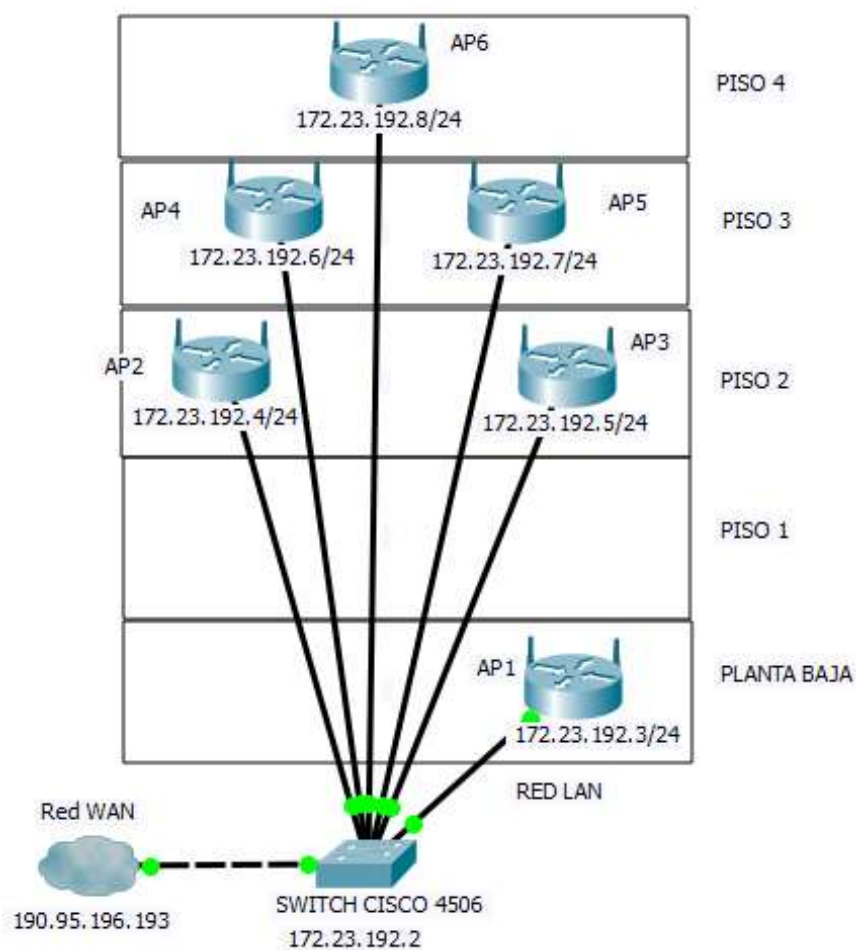


Figura 22. Topología lógica de la red existente en la FICA  
Fuente: Propia

De una forma resumida se puede observar la distribución lógica de la red existente en la FICA identificando las IPs asignadas a cada dispositivo.

### 3.1.2.2 Ubicación de los equipos de la red existente

La investigación de campo para ha permitido evaluar la situación tecnológica en funcionamiento donde se llegó a determinar que actualmente la red Wi-Fi de la facultad, estaba compuesta por 6 puntos de acceso marca CISCO de la serie 1130, los mismos que están

distribuidos uno en la planta baja, dos en el segundo piso, dos en el tercer piso y uno en el cuarto piso.

- Uno en la planta baja



Figura 23. Dispositivos de la red actual en la planta baja de la FICA  
Fuente: Propia

- Dos en el segundo piso

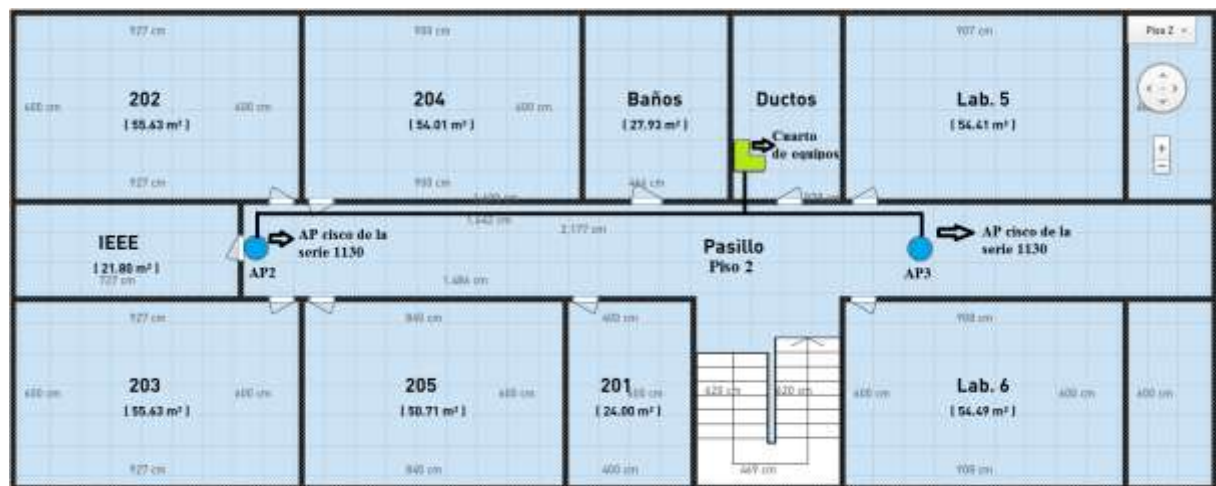


Figura 24. Dispositivos de la red actual en el segundo piso de la FICA  
Fuente: Propia



- Dos en el tercer piso

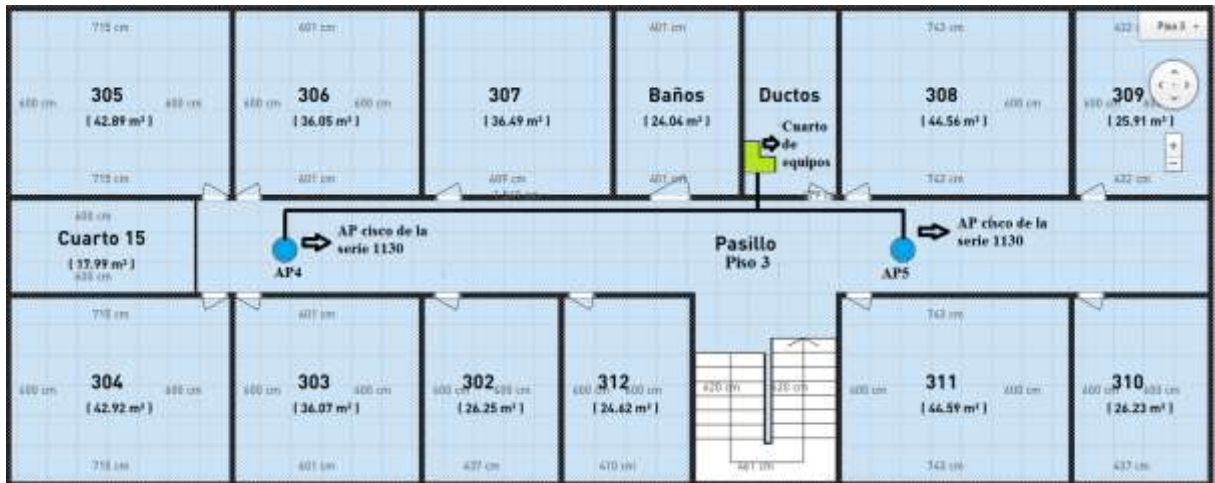


Figura 25. Dispositivos de la red actual en el tercer piso de la FICA  
Fuente: Propia

- Uno en el cuarto piso.

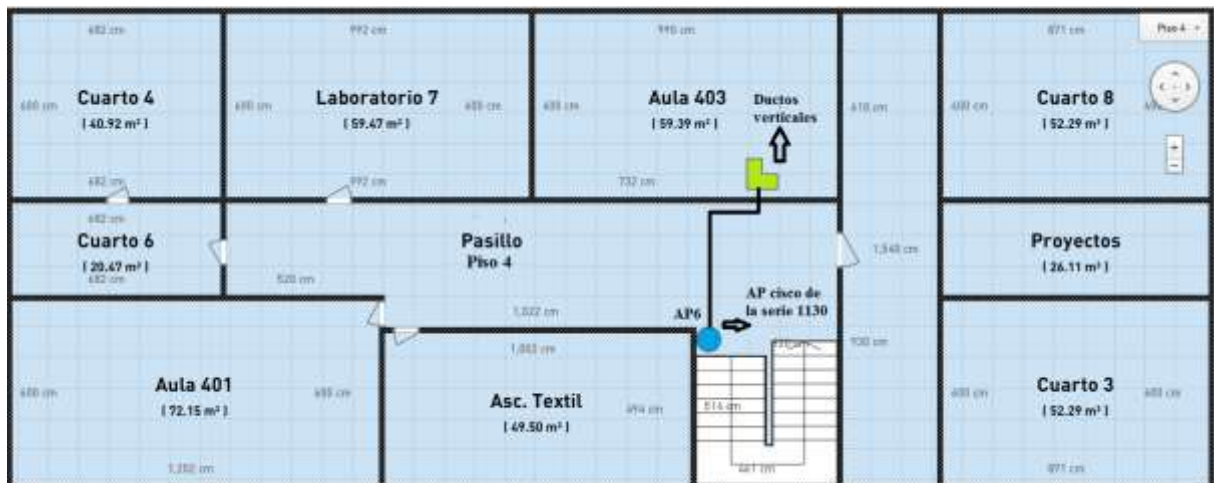


Figura 26. Dispositivos de la red actual en el tercer piso de la FICA  
Fuente: Propia

Los puntos de acceso estaban distribuidos e interconectados sin un diseño de topología conocido como: estrella, bus, o árbol. Por el contrario, estaban interconectados a través de puntos de red próximos al AP o a switch en cascada, provocándose de esta manera un cuello de botella, retransmisión y pérdida de paquetes por la existencia de un mayor número de puntos de falla en la red, sobre todo en los APs más alejados del cuarto de equipos.

También se encontró que las interfaces inalámbricas de cada AP estaban totalmente saturadas con un promedio de 60 estaciones por cada AP en horas pico y 45 estaciones en horarios normales, según datos obtenidos del centro de monitoreo del departamento de sistemas de la universidad Técnica del Norte. Esta saturación se producía debido que no se tenía implementado un control del número máximo estaciones permitidas por AP.

Una deficiencia muy importante que se encontró es que no tenía sistema gestión y administración de usuarios, que permita la asignación de recursos y control de ancho de banda, y al no tener control de cada usuario se produce una congestión en la red de acceso, dejando casi inutilizable la red Wi-Fi instalada para el acceso recursos locales y mucho menos al internet.

Del análisis realizado también se pudo determinar que no existía un sistema de administración centralizado que permita manejar algunos parámetros como seguridad, control de acceso, perfiles de usuarios, calidad de servicio y administración de ancho de banda, que es necesario ser implementarlos para poder administrar la red de una forma adecuada y tener un funcionamiento óptimo y cumpla con requerimientos mínimos necesarios de calidad en el acceso a contenidos locales y de acceso público.

### 3.1.2.3 Dispositivos de la red existente

*Tabla 2. Descripción y características de los equipos de la red existente en la FICA*

Equipo				Características	
	Cant	Marca	Serie		
Piso 1 – D1	1	CISCO	Serie 1130	Código del producto	1130AG IEEE 802.11
				Procesador	PowerPCElvis
				Velocidad CPU	262Mhz
				10/100 puertos Ethernet	1
				Tipo de almacenamiento	Flash
Piso 2 – D2 y D3	2	CISCO	Serie 1130	Rango de temperatura Operativo	0 to 40°C
				Network Standard	IEEE 802.11a, 802.11b, and 802.11g
Piso 3 – D4 y D5	2	CISCO	Serie 1130	Sistema Operativo	Cisco IOS Software Release 12.3
				Memoria Ram	32 MB

Piso 4 D6	1	CISCO	Serie 1130	Voltaje	12.2W máximo
				Numero de antenas	2
				Ganancia de Antena en DBI	2.4 Ghz, Gain 3.0 dBi
				Dimensiones	5 Ghz, Gain 4.5 dBi 7.5 in. x 7.5 in. x 1.3 in. (19.1 x 19.1 x 3.3 cm)
				Tamaño de almacenamiento	16 MB

*Fuente: Propia*

### 3.1.3 Justificación de pruebas a la red existente

Con el fin de determinar la calidad de red Wi-Fi existente que se encontraba funcionando inicialmente en la FICA para brindar acceso a internet en los interiores de la facultad, se preparó diferentes pruebas.

#### 3.1.3.1 Prueba de velocidad con herramientas web

Para establecer el rendimiento de la red Wi-Fi y el acceso a internet que es brindado actualmente en la FICA, se realiza la primera prueba con las herramientas web de medición speedOf.Me y test de APROVI disponibles en la web. Los datos tomados que presentan las siguientes figuras fueron tomados a las 11:25am, el día 15 de mayo del 2015.



*Figura 27. Medición de velocidad de transmisión con la herramienta speedof.me.*

*Fuente: Propia*

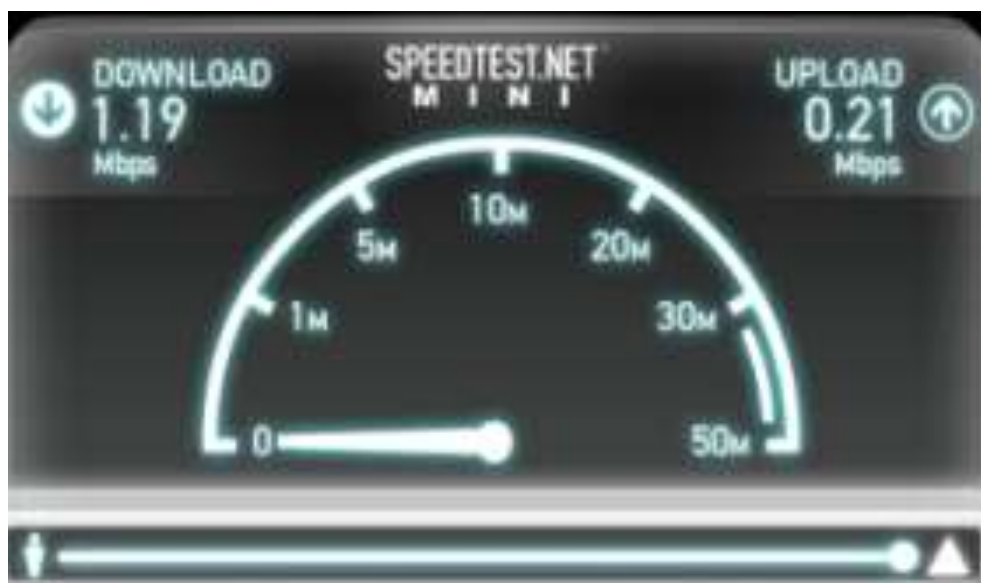


Figura 28. Test de velocidad en la red existente con AEPROVI.

Fuente: Propia

Se evidencia en las figuras anteriores que se hizo una prueba de velocidad con las herramientas de Spedof.me<sup>22</sup> y AEPROVI<sup>23</sup>, indistintamente en los interiores del edificio de la FICA.

Tabla 3. Prueba de velocidad con herramientas web

Herramienta/Detalle	Descarga	Carga	Latencia
SPEDOF.ME	340 kbps	30 kbps	1315 ms
AEPROVI	1.19 Mbps	0.21 Mbps	1256 ms

Fuente: Propia

De dichas pruebas se obtuvo la información expresada en la anterior tabla y evaluando estos resultados se puede determinar claramente que en un comienzo el ancho de banda disponible para el usuario final es mínimo y al mismo tiempo es variable, siendo tan deficiente que no era posible realizar el envío de mensajes de texto y tampoco se disponía de acceso a contenidos en

<sup>22</sup> Spedofme. Herramienta para pruebas de velocidad de internet.

<sup>23</sup> AEPROVI. Asociación de empresas proveedoras de internet, valor agregado, portadores y tecnólogos de la información.

tiempo real; además, la latencia alta indica que es casi imposible el acceso a contenidos externos, como sitios web, o servidores remotos de interés para los usuarios.

### 3.1.3.2 Descarga y reproducción de un video en el formato más básico de 144p

La prueba de disponibilidad de ancho de banda se realizó mediante la visualización de un video a 144p en la plataforma YouTube, en donde se utilizó el formato de calidad más bajo de un video digital y se evidenció que no puede ser reproducido debido a la alta latencia y el escaso ancho de banda que se tiene disponible en la red Wi-Fi existente.



Figura 29. Prueba de la red Wi-Fi reproduciendo de un video en 144p.  
Fuente: Propia

### 3.1.3.3 Prueba de envío y recepción de paquetes ICMP

Se hace una prueba básica mediante el envío de paquetes ICMP<sup>24</sup> para medir el estado de comunicación desde el host local hacia un host remoto, mediante la ayuda de la herramienta ping y así diagnosticar el estado, velocidad y calidad de la red existente.

La siguiente figura permite ver la prueba realizada, donde se realiza el envío de paquetes desde la red interna hacia un host remoto con IP 181.198.80.18.

<sup>24</sup> ICMP. Protocolo de mensajes de control de Internet. Permite administrar información relacionada con errores de los equipos en red. Fuente: (Kioskea, 2014)

```

Símbolo del sistema
Respuesta desde 181.198.80.18: bytes=32 tiempo=9ms TTL=58
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 181.198.80.18: bytes=32 tiempo=70ms TTL=58
Respuesta desde 181.198.80.18: bytes=32 tiempo=45ms TTL=58
Tiempo de espera agotado para esta solicitud.
Respuesta desde 181.198.80.18: bytes=32 tiempo=66ms TTL=58
Respuesta desde 181.198.80.18: bytes=32 tiempo=64ms TTL=58
Respuesta desde 181.198.80.18: bytes=32 tiempo=99ms TTL=58
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 181.198.80.18: bytes=32 tiempo=711ms TTL=58
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 181.198.80.18:
    Paquetes: enviados = 151, recibidos = 113, perdidos = 38
              (25% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 4ms, Máximo = 3006ms, Media = 471ms
Control-C
^C
C:\Users\Soporte técnico>

```

Figura 30. Estadística de tiempos y envío de paquetes ICMP sin saturación de canal.

Fuente: Propia

La siguiente tabla indica con mayor claridad los resultados obtenidos con la herramienta ping.

Tabla 4. Prueba de envío y recepción de paquetes ICMP

	Enviados	Recibidos	Perdidos
Paquetes	151	113	38
	Mínimo	Máximo	Media
Tiempos (Latencia)	4 ms	3006 ms	471 ms

Fuente: Propia

Según la tabla anterior dichos parámetros indican que es casi imposible el acceso a sitios remotos debido al porcentaje de paquetes perdidos y a la muy alta latencia de la red instalada.

### 3.1.3.4 Búsqueda del punto crítico de degradación de la red

Una vez realizada la prueba de latencia y envío de paquetes hacia sitios remotos, era preciso determinar cuál es la parte crítica, o el tramo donde se produce el mayor retardo y retransmisión de paquetes, para ello se realizó un trazado de rutas desde el equipo local hasta el host remoto, el DNS del Google (181.198.80.173), como se indica en la siguiente figura, esto permite

determinar que el problema inicia en el primer salto, en el router con IP 172.23.192.2, cabe resaltar que si se está a nivel del primer salto, aún se está a nivel de la red local, entonces se determina que se debe empezar por la red acceso y estaciones finales para encontrar las posibles causas que provocan retardo en la transmisión de datos.

```

Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 39ms, Máximo = 44ms, Media = 41ms
Control-C
^C
C:\Users\Soporte técnico>tracert 181.198.80.173 -t

Uso: tracert [-d] [-h saltos_máximos] [-j lista_de_hosts] [-w tiempo_de_espera]
[-R] [-S srcaddr] [-4] [-6] nombre_destino

Opciones:
-d          No convierte direcciones en nombres de hosts.
-h saltos_máximos  Máxima cantidad de saltos en la búsqueda del objetivo.
-j lista-host      Enrutamiento relajado de origen a lo largo de la
                  lista de hosts (solo IPv4).
-w tiempo_espera  Tiempo de espera en milisegundos para esperar cada
                  respuesta.
-R            Seguir la ruta de retorno (solo IPv6).
-S srcaddr      Dirección de origen para utilizar (solo IPv6).
-4            Forzar usando IPv4.
-6            Forzar usando IPv6.

C:\Users\Soporte técnico>tracert 181.198.80.173

Traza a la dirección host-181-198-80-173.telconet.net [181.198.80.173]
sobre un máximo de 30 saltos:

  1  65 ms   34 ms   68 ms  172.23.192.2
  2   *     18 ms   28 ms  190.95.196.193
  3  18 ms   22 ms   19 ms  190.95.196.153
  4  52 ms   28 ms   39 ms  10.201.26.225
  5  23 ms   37 ms   49 ms  10.201.211.58
  6  56 ms   50 ms   40 ms  host-181-198-80-1.telconet.net [181.198.80.1]
  7  45 ms  182 ms   42 ms  host-181-198-80-173.telconet.net [181.198.80.173]
]

Traza completa.
C:\Users\Soporte técnico>

```

Figura 31. Trazado de ruta al servidor DNS de Google.

Fuente: Propia

La figura anterior mide la latencia y número de saltos que toma una solicitud de acceso externo e indica que el problema de la degradación de la calidad de la red Wi-Fi, inicia en la red de acceso, donde se encuentra distribuida la carga de usuarios que están conectados a los distintos puntos de acceso.

## 3.2 Diseño del sistema de gestión Wi-Fi

### 3.2.1 Ubicación de equipos de la nueva red WiFi

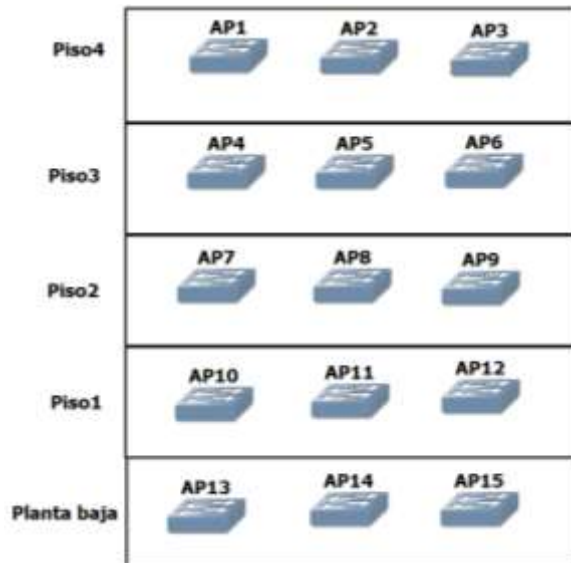


Figura 32. Distribución de los puntos de acceso por cada piso de la FICA.  
Fuente: Propia

La figura anterior es una vista frontal del edificio de la FICA, en donde los puntos de acceso o APs han sido distribuidos simétricamente de arriba hacia abajo y de izquierda a derecha.

El área que se va a cubrir consiste en un bloque constructivo de 5 pisos los cuales tienen una disposición particular y similar, particular porque las aulas y ambientes se encuentran distribuidos de manera circular y se accede a ellos a través de un pasillo central, desde este pasillo se tiene alcance hacia todos los ambientes a través de ventanas ubicadas en cada uno de ellos.

### 3.2.2 Topologías física y lógica de la nueva red Wi-Fi

La topología de red con todos los elementos que conforman la red Wi-Fi se muestra en la figura siguiente.



### 3.2.2.1 Topología física de la nueva red WiFi

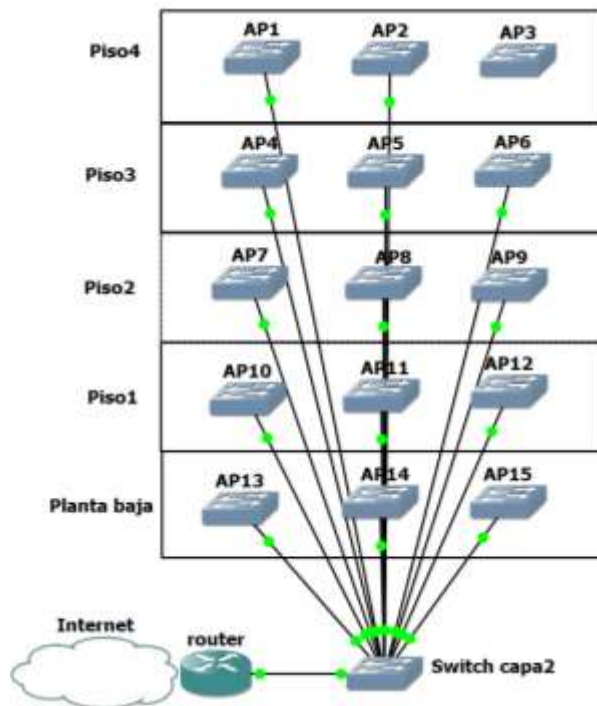


Figura 33. Topología física para la nueva red FICA.  
Fuente: Propia

En esta topología se puede visualizar el diagrama final de conexiones que tendría la red WiFi desde una vista frontal del edificio de la Facultad. También se puede apreciar como toda la red está totalmente centralizada en basada en una topología tipo estrella, permitiendo de esta manera disminuir cuellos de botella entre los puntos de acceso hasta el switch que funciona como equipo central.

### 3.2.2.2 Topología lógica de la nueva red WiFi

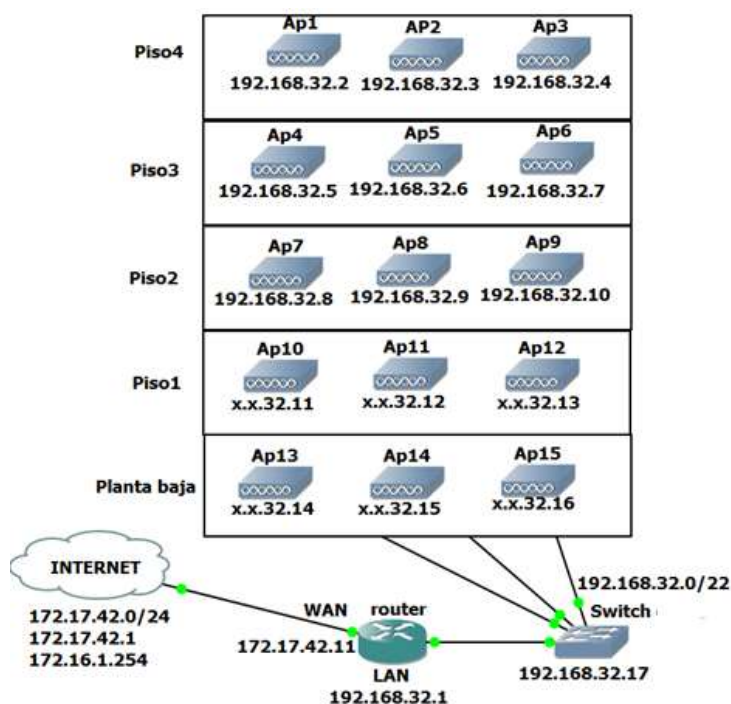


Figura 34. Topología lógica para la nueva red FICA.  
Fuente: Propia

La figura anterior proporciona información más detallada sobre el direccionamiento de la nueva red mediante la topología lógica.

### 3.2.3 Gestión centralizada de los puntos de acceso

Para la administración de los usuarios y la gestión centralizada de los puntos de acceso es necesario un equipo central de ruteo, para el caso de este proyecto se ha seleccionado el Routerboard RB1100AHx2 y el Qpcom qp-1240r, que poseen las siguientes características:

#### 3.2.3.1 Routerboard RB1100AHx2

Tabla 5. Características técnicas de router RB1100AHx2

Detalles	
Código del producto	RB1100AHx2
Frecuencia nominal del CPU	1 GHz
Numero de núcleos	2
Arquitectura	PPC

Memoria RAM	2 GB
Puertos Ethernet 10/100/1000	13
Número de puertos USB	1
Power Jack	1
PoE in	Yes
Voltaje de entrada soportado	10 V - 28 V
Monitor de Voltaje	Yes
Monitor de temperatura PCB	Yes
Dimensiones	1U case: 44 x 176 x 442 mm
Sistema Operativo	RouterOS
Rango de temperatura	-35C a +65C probado
Nivel de licencia	6
CPU	P202ASSE2KFB
Máxima potencia de consumo	15W
Puerto Serial	RS232
Tipo de almacenamiento	NAND
Memoria de almacenamiento	128 MB

---

*Fuente: Propia*



*Figura 35. Vista frontal del router RB1100AHx2.*

*Fuente: (Routerboard, 2016)*

El RB1100AHx2 es el equipo central de gestión que será el encargado de recibir el internet por parte del proveedor de servicios y retransmitir hacia los usuarios de la red interna a través a través de la red de acceso, mediante políticas de enmascaramiento IP. También será el equipo encargado de realizar el control de ancho de banda y asignación de recursos a las estaciones

finales a través de la herramienta Hotspot, para evita que el uso inadecuado del ancho de banda provoque deterioro en la calidad de la red (Routerboard, 2015).

Finamente este equipo, a través del gestor CAPsMAN se encarga administrar y gestionar los perfiles de configuración de todos los puntos de acceso que conforman la red Wi-Fi de la FICA.

### 3.2.3.2 Qpcom QP-1240R

*Tabla 6. Características técnicas de Switch QP-1240R*

<b>Detalles</b>	
Código del producto	QP-1240R
Tasa de transmisión	10/100 Mbps en modo Half Dúplex 10/100/1000 Mbps en modo Full Dúplex
Método de transmisión	Almacenar y enviar
Control de flujo	IEEE 802.3x (Full Dúplex)
Puertos	24 puertos RJ-45 con auto negociación de velocidad 10/100/1000 Mbps (Auto- MDI/MDIX)
Medio de red	10BASE-T: UTP Categoría 3 o superior. 100BASE-TX: UTP Categoría 5 o superior. 1000BASE-T: UTP Categoría 5 o superior.
Método de acceso	CSMA/CD
Indicadores LED	Power Link/Act.
Entorno	Temperatura de operación: 0°C ~ 40°C (32°F ~ 104°F)
Temperatura de almacenamiento	-40°C ~ 70°C (-40°F ~ 158°F) Humedad de operación: 10% ~ 90% no condensado
Humedad de almacenamiento	5% ~ 90% no condensado
Alimentación eléctrica	3.3V / 4A
Dimensiones	445mm x 120 mm x 45 mm
Emisiones y seguridad	FCC, CE
Estándares	IEEE 802.3 10Base-T, 802.3u 100Base-TX, 802.3ab 1000Base-T, 802.3x Flow Control

*Fuente: (QPCOM, 2016)*



*Figura 36. Switch QPCOM QP-1240R  
Fuente: (QPCOM, 2016)*

“El switch de 24 puertos 10/100/1000 Mbps es compatible con la función de auto-negociación y auto-crossing. Cumple con el estándar IEEE802.3x para el control de flujo de datos para el modo Full Dúplex. Ideal para el uso en oficinas. Fácil instalación Plug & Play. Bajo consumo de energía” (QPCOM, 2016).

### **3.2.4 Distribución de puntos de acceso**

A continuación, se muestra la distribución de los puntos de acceso con su respectiva área de cobertura, mediante el uso de planos bidimensionales, debe indicarse que estos mapas de cobertura son a máxima potencia, y las zonas de color blanco es en donde el usuario puede moverse si perder conectividad, además el nivel de señal de recepción es directamente proporcional a la distancia donde se encuentra el cliente.

- **Planta baja:**

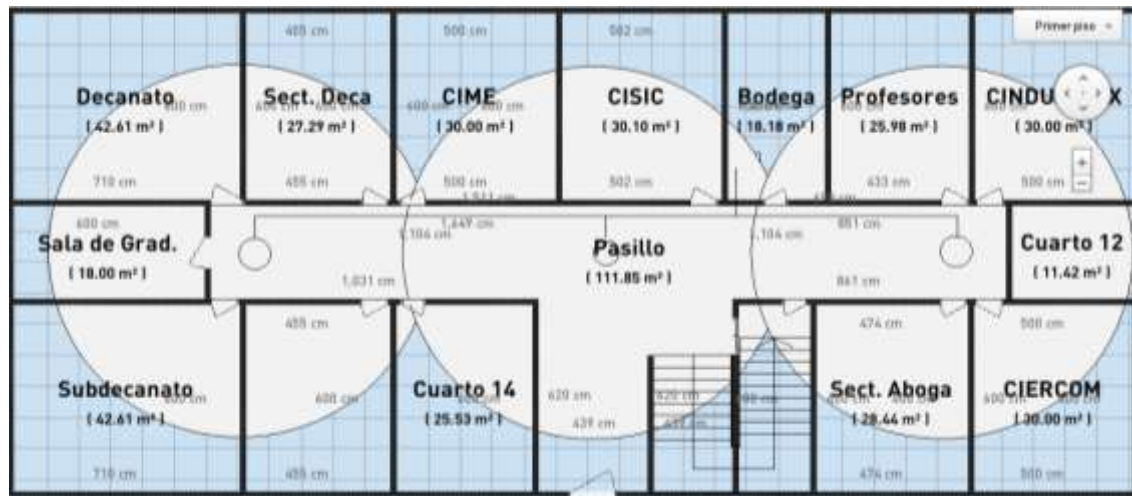


Figura 37. Plano bidimensional de planta baja FICA, con la distribución de APs.  
Fuente: Propia.

En la figura anterior se puede ver la distribución de los puntos de acceso correspondientes a la planta baja, los mismos que han sido denominados AP13, AP14 y AP15 en dirección de izquierda a derecha.

- **Primer piso:**

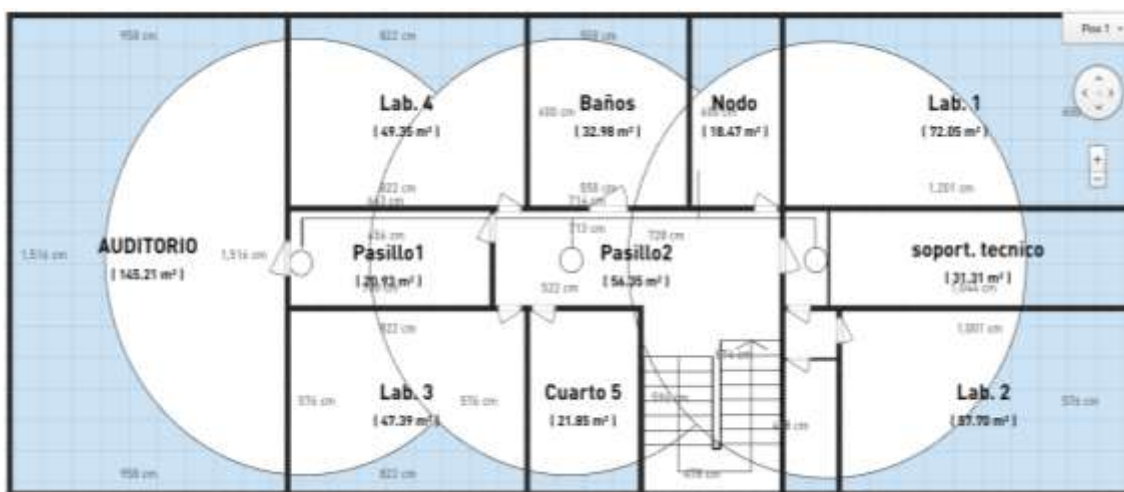
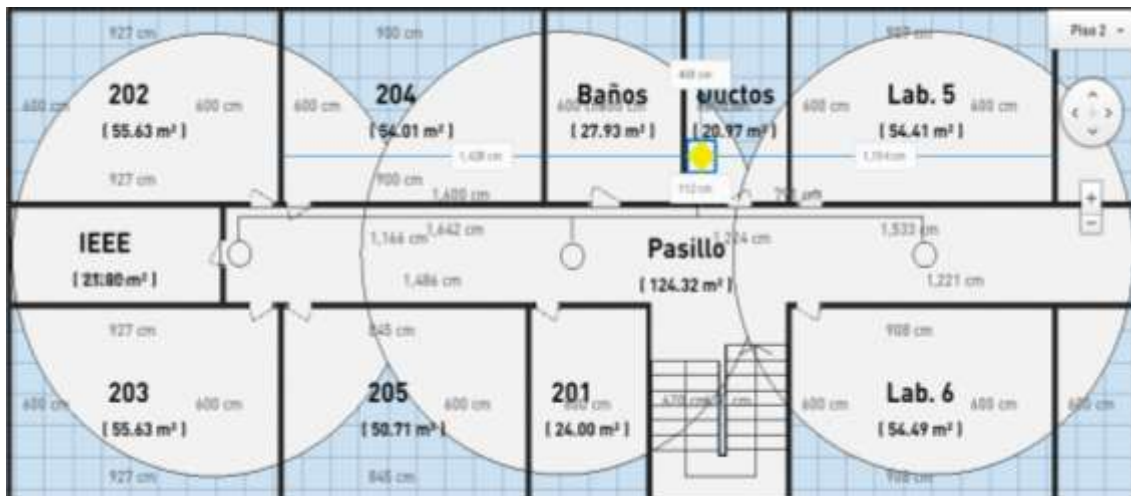


Figura 38. Plano bidimensional del primer piso del edificio de la FICA.  
Fuente: Propia

En el primer piso se designado los puntos de acceso AP10, AP11 Y A12, en dirección de izquierda a derecha, según se puede ver en la figura anterior. Además, debe indicarse que los tres puntos de acceso antes mencionados han sido distribuidos más próximos, para tener mayor cobertura a nivel de los pasillos, considerando que el piso uno es donde se encuentran la mayoría de laboratorios con disponibilidad de puntos de red.

- **Segundo piso:**



*Figura 39. Vista superior del segundo piso del Edificio FICA.*

*Fuente: Propia*

En el segundo piso se ha hecho la distribución de los puntos de acceso AP7, AP8 y AP9, a través de todo el pasillo en dirección de izquierda a derecha, como se puede ver en la figura anterior.

- **Tercer piso:**

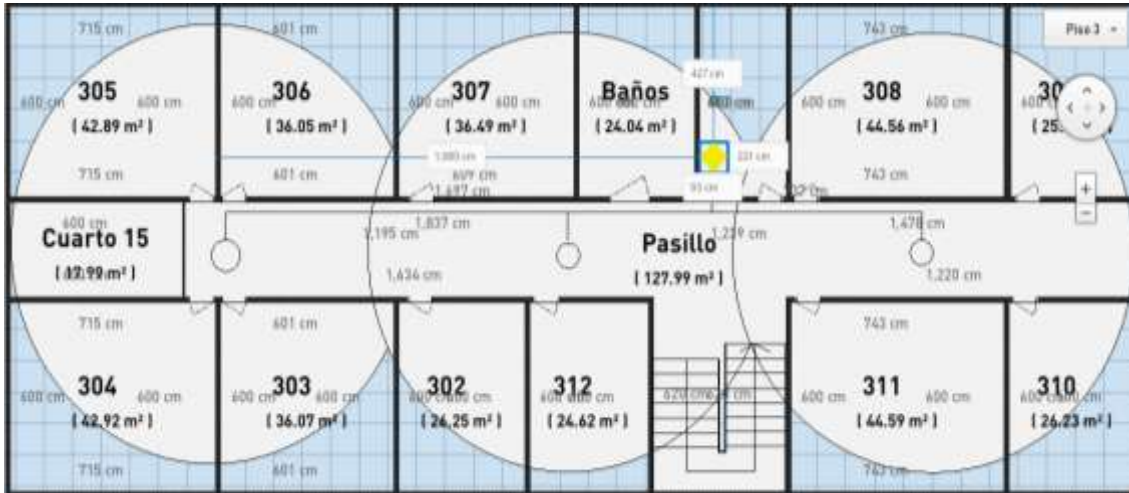


Figura 40. Vista superior del tercer piso con los tres APs instalados en el pasillo.  
Fuente: Propia

En el tercer piso se han asignado designado los puntos de acceso AP4, AP5 y AP6, a través de la extensión de todo el pasillo de izquierda a derecha

- **Cuarto piso**

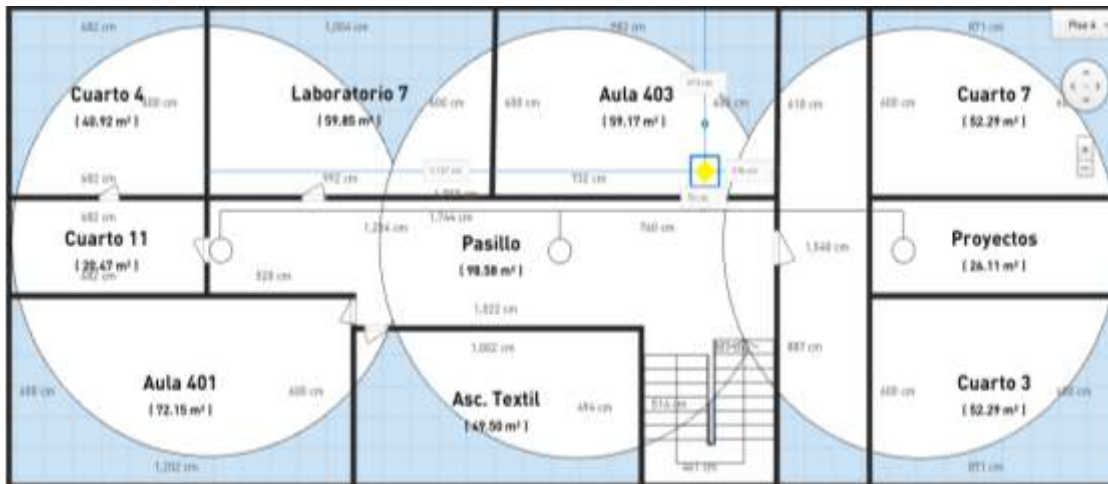


Figura 41. Vista superior del cuarto piso del edificio FICA.  
Fuente: Propia

En el cuarto y último piso se han asignado los puntos de acceso AP1, AP2 y AP3 de izquierda a derecha, como puede verse de mejor manera en la figura anterior



Se determinó entonces que el lugar adecuado para la ubicación de los equipos de transmisión es el pasillo pues desde ahí y en todos los pisos tenemos la facilidad de irradiar a través de las ventanas que se ubican en cada uno de los ambientes.

La distribución de los puntos de acceso a lo largo de los pasillos tiene como finalidad crear una mayor zona de cobertura que puede cubrir la mayor parte de cada piso, pero siempre garantizando la calidad de servicio dentro de dicha zona.

### 3.2.5 Cálculo de cobertura

#### 3.2.5.1 Nivel de señal que llega al equipo receptor

Se debe tomar en cuenta que el alcance es la distancia lineal y física que permite que la conexión inalámbrica sea exitosa y para determinar el nivel de señal que llega al equipo receptor es necesario realizar una serie de cálculos (HWAGM Seguridad Wireless, 2016).

- **Pérdida de propagación  $P_p$**

Es la conexión necesaria para llegar de un extremo de la conexión wireless a otro (HWAGM Seguridad Wireless, 2016).

$$P_p = 20 \log_{10}(d/1000) + 20 \log_{10}(f * 1000) + 32.4$$

Donde: d = Distancia en metros.

f = Frecuencia en GHz

32.4 = constante

Fórmula resumida:

$$P_p = 20 \log_{10}(d) + 100$$

$$P_p = 20 \log_{10}(0.013) + 100$$

$$P_p = 62.33 \text{ db}$$

*Ecuación 2. Cálculo de pérdida de propagación  
Fuente: (HWAGM Seguridad Wireless, 2016)*

- **Pérdidas y ganancias**

Además de las pérdidas de propagación existen también diferentes dispositivos que producen pérdidas o ganancias de señal.

Para los conectores y el cableado es difícil saber con qué calidad fueron fabricados, por esa razón se considera una pérdida de 0.5 db respectivamente, mientras que para considerar la pérdida por las condiciones ambientales se estima 20db (HWAGM Seguridad Wireless, 2016).

- **Ganancia de salida del equipo transmisor**

Potencia en db con la que sale la señal del equipo transmisor (HWAGM Seguridad Wireless, 2016).

$$Gse = 10 \log(Pem)$$

Donde:  $Gse$  = Ganancia de salida del equipo transmisor.

$Pem$  = Potencia de emisión en miliwatios.

$$Gse = 10 \log(250)$$

$$Gse = 23.98$$

*Ecuación 3. Cálculo de ganancia de salida del equipo transmisor*  
Fuente: (HWAGM Seguridad Wireless, 2016)

Por tanto, se tiene el nivel de señal  $Sr$

$$Sr = Gse - Pce - Pae + Gae - Pp + Gar - Pcr - Par - Pa$$

Donde:  $Sr$  = Nivel de señal que le llega al equipo receptor. Siempre será negativo (dB).

$Gse$  = Ganancia de salida del equipo transmisor.

$Gae$  = Ganancia de la antena del equipo transmisor.

$Pce$  = Pérdida cables equipo transmisor.

$Pae$  = Pérdida conectores equipo transmisor.

$Pp$  = Pérdida de propagación.

Gar = Ganancia de la antena del equipo receptor.

Pcr = Perdida cables equipo receptor.

Par = Perdida conectores equipo receptor.

Pa = Perdidas adicionales debido a las condiciones ambientales.

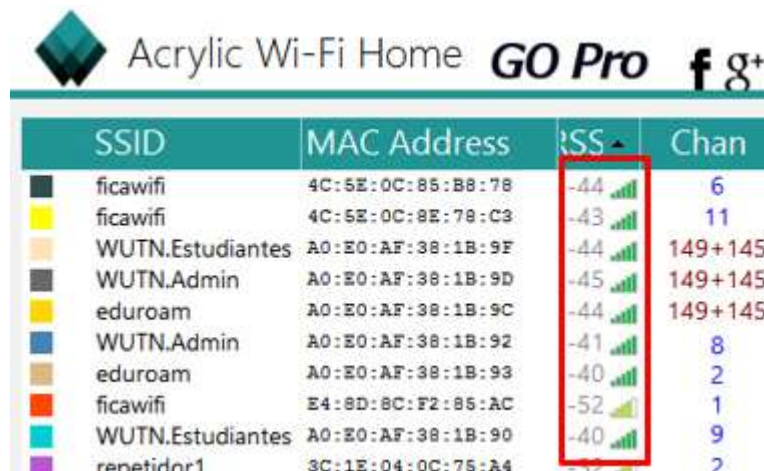
Resultado:

$$S_r = 23.98 - 0.5 - 0.5 + 2 - 62.33 + 2 - 0 - 0 - 20$$

$$S_r = -55.35 \text{ db}$$

*Ecuación 4. Cálculo de nivel de señal que le llega al equipo receptor*  
*Fuente: (HWAGM Seguridad Wireless, 2016)*

Los cálculos realizados permiten demostrar que el nivel de señal que emite cada AP cumple con el requerimiento pues cada dispositivo se encuentra ubicado cada 13 metros y el nivel de señal que se evidencia tiene un promedio de -46.33 db como se observa en la figura siguiente.



SSID	MAC Address	RSSI	Chan
ficawifi	4C:5E:0C:85:BB:78	-44	6
ficawifi	4C:5E:0C:8E:78:C3	-43	11
WUTN.Estudiantes	A0:E0:AF:38:1B:9F	-44	149+145
WUTN.Admin	A0:E0:AF:38:1B:9D	-45	149+145
eduroam	A0:E0:AF:38:1B:9C	-44	149+145
WUTN.Admin	A0:E0:AF:38:1B:92	-41	8
eduroam	A0:E0:AF:38:1B:93	-40	2
ficawifi	E4:8D:8C:F2:85:AC	-52	1
WUTN.Estudiantes	A0:E0:AF:38:1B:90	-40	9
repetidor1	3C:1E:04:0C:75:A4	-40	2

*Figura 42. Nivel de intensidad de la señal en la red ficawifi*  
*Fuente: Propia*

### 3.2.6 Distribución de frecuencias de la nueva red WiFi

Es necesario abordar el tema de solapamiento por piso, se debe considerar también que la implantación del edificio es de hormigón, entre pisos la señal podría alcanzar los pisos adyacentes ya sea por refracción o difracción. Para evitar esto se diseña una matriz para que los equipos que se encuentren uno sobre otro entre pisos no tengan solapamiento.

Tabla 7. Distribución de frecuencias para los cAP2n.

PISO 4	AP1 2412 Mhz	AP2 2437 Mhz	AP3 2462 Mhz
PISO 3	AP4 2462 Mhz	AP5 2412 Mhz	AP6 2437 Mhz
PISO 2	AP7 2412 Mhz	AP8 2437 Mhz	AP9 2462 Mhz
PISO 1	AP10 2437 Mhz	AP11 2462 Mhz	AP12 2412 Mhz
PLANTA	AP13 2412 Mhz	AP14 2437 Mhz	AP15 2462 Mhz
BAJA			

*Fuente: Propia*

La tabla anterior, indica la asignación de frecuencias por piso, para garantizar que al menos los puntos de acceso no se solapen con sus vecinos inmediatos tanto de manera horizontal como de manera vertical.

### 3.2.7 Análisis y selección de canales para la nueva red WiFi FICA

#### 3.2.7.1 Selección de canales para la nueva red WiFi

La selección de canales de una red wifi debe ser previamente analizada mediante herramientas que muestran la saturación de cada canal que se encuentra dentro del área de cobertura, tratando así de realizar una configuración más efectiva de los routers o Aps y evitar la saturación y la pérdida de velocidad de conexión.

Para su aplicación se configura los canales de tal forma que los equipos adyacentes verticalmente y horizontalmente posean un canal diferente impidiendo el solapamiento de los dispositivos vecinos como se muestra en la siguiente figura.

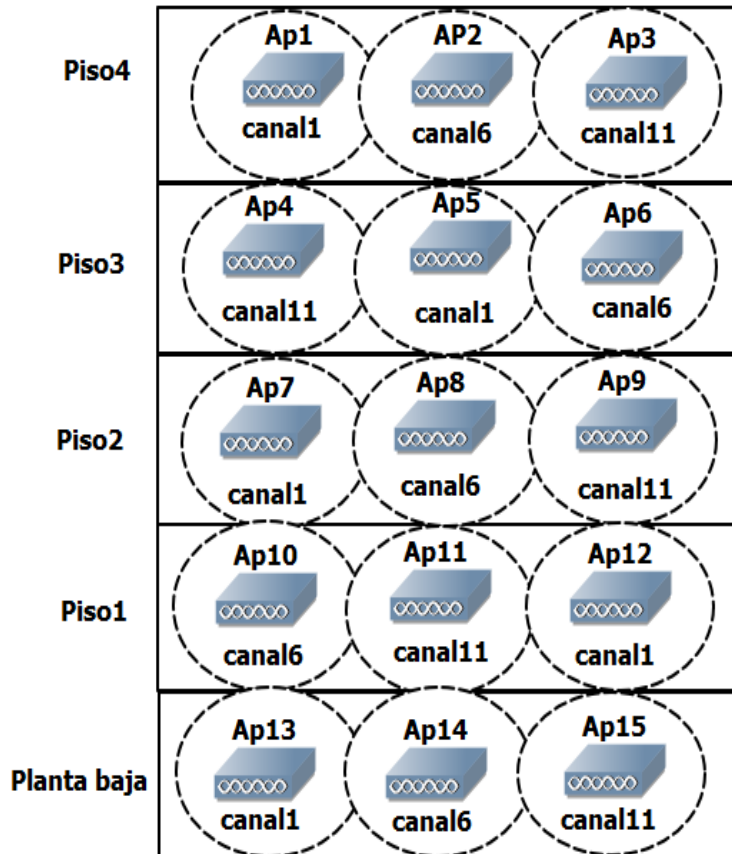
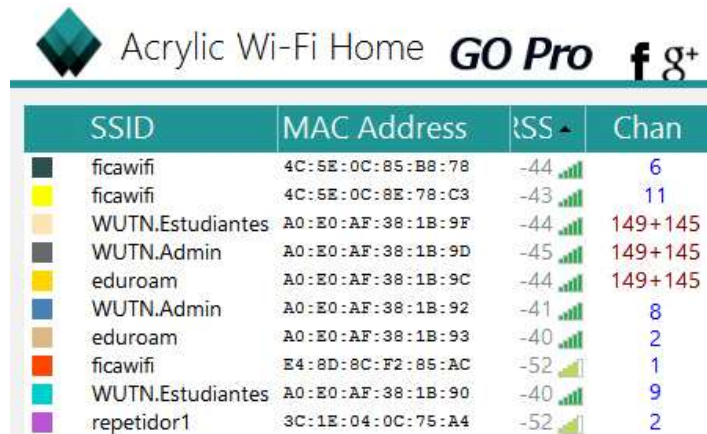


Figura 43. Distribución de APs por piso, con canales y zonas de cobertura.  
Fuente: Propia

Adicionalmente es necesario justificar que los canales seleccionados cumplen con el diseño planteado y el software Acrylic Wi-Fi Home permite escanear la red y visualizar el rango de canales utilizados.

- **Planta baja**



SSID	MAC Address	RSSI	Chan
ficawifi	4C:5E:0C:85:B8:78	-44	6
ficawifi	4C:5E:0C:8E:78:C3	-43	11
WUTN.Estudiantes	A0:E0:AF:38:1B:9F	-44	149+145
WUTN.Admin	A0:E0:AF:38:1B:9D	-45	149+145
eduroam	A0:E0:AF:38:1B:9C	-44	149+145
WUTN.Admin	A0:E0:AF:38:1B:92	-41	8
eduroam	A0:E0:AF:38:1B:93	-40	2
ficawifi	E4:8D:8C:F2:85:AC	-52	1
WUTN.Estudiantes	A0:E0:AF:38:1B:90	-40	9
repetidor1	3C:1E:04:0C:75:A4	-52	2

Figura 44. Escaneo de canales en el ambiente planta baja  
Fuente: Propia

En la figura anterior se puede evidenciar que las redes encontradas en el rango de una buena intensidad de señal cumplen con el diseño planteado para la planta baja con los canales 1, 6 y 11.

- **Primer Piso**

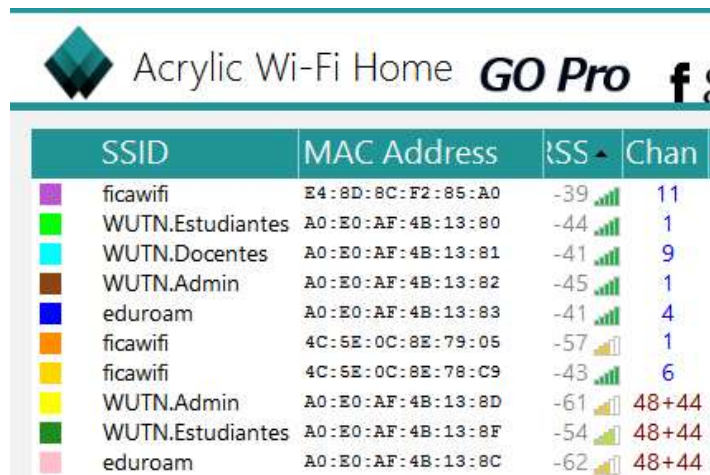


SSID	MAC Address	RSSI	Chan	802.11
ficawifi	4C:5E:0C:8E:79:05	-42	11	b, g, n
WUTN.Estudiantes	A0:E0:AF:38:1B:90	-54	1	b, g, n
ficawifi	4C:5E:0C:8E:78:C9	-53	6	b, g, n
repetidor1	3C:1E:04:0C:75:A4	-62	9	b, g, n
WUTN.Admin	A0:E0:AF:38:1B:92	-56	2	b, g, n
eduroam	A0:E0:AF:38:1B:93	-55	9	b, g, n
WUTN.Docentes	A0:E0:AF:38:1B:91	-56	9	b, g, n
ficawifi	E4:8D:8C:F2:85:AC	-56	1	b, g, n

Figura 45. Escaneo de canales en el ambiente primer piso  
Fuente: Propia

En la figura anterior muestra las redes encontradas en el rango de una buena intensidad de señal cumplen con los canales planteados 6, 11 y 1.

- **Segundo Piso**



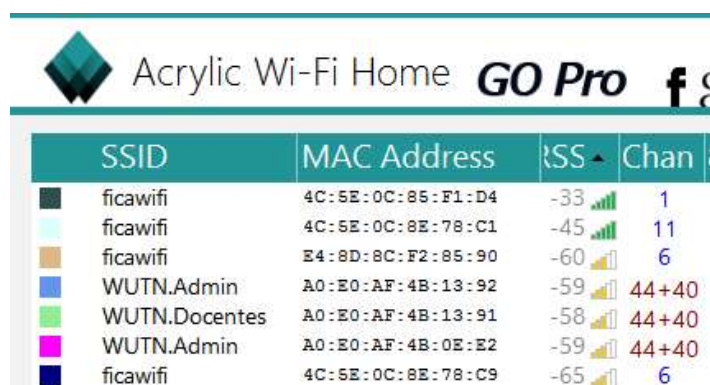
SSID	MAC Address	RSSI	Chan
ficawifi	E4:8D:8C:F2:85:A0	-39	11
WUTN.Estudiantes	A0:E0:AF:4B:13:80	-44	1
WUTN.Docentes	A0:E0:AF:4B:13:81	-41	9
WUTN.Admin	A0:E0:AF:4B:13:82	-45	1
eduroam	A0:E0:AF:4B:13:83	-41	4
ficawifi	4C:5E:0C:8E:79:05	-57	1
ficawifi	4C:5E:0C:8E:78:C9	-43	6
WUTN.Admin	A0:E0:AF:4B:13:8D	-61	48+44
WUTN.Estudiantes	A0:E0:AF:4B:13:8F	-54	48+44
eduroam	A0:E0:AF:4B:13:8C	-62	48+44

Figura 46. Escaneo de canales en el ambiente segundo piso

Fuente: Propia

La figura anterior muestra la distribución de canales en el ambiente para el piso 2 según lo planteado.

- **Tercer Piso**



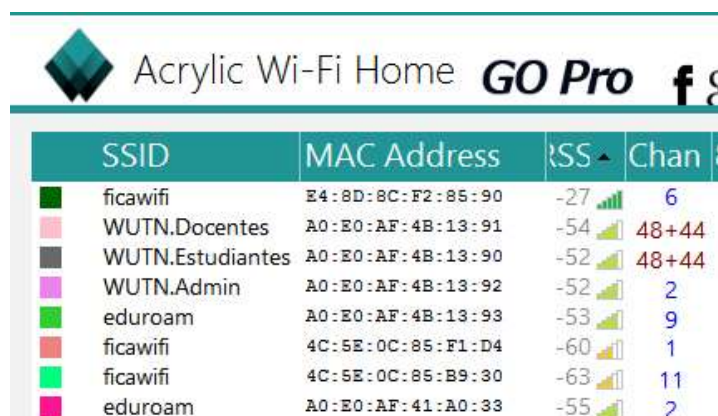
SSID	MAC Address	RSSI	Chan
ficawifi	4C:5E:0C:8E:F1:D4	-33	1
ficawifi	4C:5E:0C:8E:78:C1	-45	11
ficawifi	E4:8D:8C:F2:85:90	-60	6
WUTN.Admin	A0:E0:AF:4B:13:92	-59	44+40
WUTN.Docentes	A0:E0:AF:4B:13:91	-58	44+40
WUTN.Admin	A0:E0:AF:4B:0E:E2	-59	44+40
ficawifi	4C:5E:0C:8E:78:C9	-65	6

Figura 47. Escaneo de canales en el ambiente tercer piso

Fuente: Propia

La figura anterior muestra el escaneo de canales en el piso tres donde se evidencia que no existe solapamiento en ese sector para los canales 11, 1 y 6.

- **Cuarto Piso**



SSID	MAC Address	RSSI	Channel
ficawifi	E4:8D:8C:F2:85:90	-27	6
WUTN.Docentes	A0:E0:AF:4B:13:91	-54	48+44
WUTN.Estudiantes	A0:E0:AF:4B:13:90	-52	48+44
WUTN.Admin	A0:E0:AF:4B:13:92	-52	2
eduroam	A0:E0:AF:4B:13:93	-53	9
ficawifi	4C:5E:0C:85:F1:D4	-60	1
ficawifi	4C:5E:0C:85:B9:30	-63	11
eduroam	A0:E0:AF:41:A0:33	-55	2

Figura 48. Escaneo de canales en el ambiente cuarto piso  
Fuente: Propia.

La figura anterior muestra los canales encontrados en el ambiente del cuarto piso y evidencia el uso de los canales 1, 6 y 11.

### 3.2.8 Alternativas de diseño

Para determinar la mejor solución a implementarse en la red Wi-Fi de la FICA, se hace un análisis comparativo de las plataformas **Mikrotik**, **Ubiquiti** y **Dlink**, tomando como referencia las características técnicas. Además, debe indicarse que todas estas alternativas son plataformas propietarias que permiten hacer gestión centralizada de redes Wi-Fi, donde se necesita administrar en tiempo real varios puntos de acceso.

#### 3.2.8.1 Plataforma Mikrotik

Para facilitar la implementación y administración de ISP (Internet Service Providers), la compañía Mikrotik ha desarrollado un sistema operativo basado en Linux llamado RouterOS MikroTik. Permitiendo incluso que cualquier plataforma x86 se convierta en un potente router, que puede realizar funciones como: VPN, Proxy, Hotspot, Control de ancho de banda, QoS, Firewall, entre otros, que varían según el nivel de licencia adquirida.



Además, la compañía también produce tableros compactos SBC (Single Board Computer), llamados routerboards, estos equipos permiten tener routers en placas bases prensadas que suelen tener varios slots de expansión miniPCI. Por defecto, un routerBoard viene instalado un sistema operativo propietario de la compañía Mikrotik, llamado **RouterOS**, pero se puede cambiar reprogramando la memoria flash interna a través del **puerto serie**.

### **Características principales**

- Se utiliza en redes inalámbricas 802.11 a / b / g / n /ac
- WEP / WPA / WPA2
- Cliente DHCP o Servidor
- Firewall con el marcado de paquetes (Mangle)
- Enrutamiento simple (NAT)
- QoS con control de ancho de banda
- Hotspot y Administrador de usuarios
- Proxy web (páginas de caché y archivos)
- Acceso remoto (WinBox , SSH y Telnet )
- Balanceo de carga
- VPN
- Los protocolos de enrutamiento RIP, OSPF y BGP
- Enrutamiento MPLS
- Servidor Radius
- Servidor Dial-in y marcación de salida.

Mikrotik, ha desarrollado una herramienta de gestión centralizada llamada CAPsMAN, permite la centralización de la gestión de redes inalámbricas. Al utilizar la función CAPsMAN, la red consistirá en una serie de puntos de acceso controlados llamados CAP, que proporcionan

conectividad inalámbrica a usuarios finales que se encuentran distribuidos a través de la red. Un administrador de sistemas (CAPsMAN) es el que se encarga de: la configuración de los puntos de acceso remotos, la autenticación de clientes y opcionalmente el reenvío de datos. Cuando un CAP es controlado por el CAPsMAN, solo requiere la configuración mínima para que se pueda establecer la conexión con CAPsMAN, las funciones convencionalmente ejecutados por un AP como el control de acceso, autenticación del cliente ahora están ejecutados por CAPsMAN. El dispositivo CAP ahora solo tiene que proporcionar la capa de enlace de cifrado / descifrado inalámbrica.

Lo mejor de todo lo que se puede construir utilizando el hardware existente, en una red ya desplegada, con lo que el uso de software permite redefinir la red inalámbrica

El CAPsMAN es un paquete de Mikrotik, que luego de ser instalado, este hace que los dispositivos AP, se convierten en puntos de acceso controlados llamados CAP. El CAPsMAN al ser el sistema administrador, hace que cada CAP se convierte simplemente de una interfaz del router y funciona como una interfaz en modo Bridge.

### **3.2.8.2 Plataforma UNIFI de UBIQUITI**

Es un sistema Wi-Fi que permite la administración centralizada de dispositivos inalámbricos a través de un software intuitivo y gratuito. Esta solución puede ser usada tanto en redes empresariales como en pequeñas empresas, con Access Point para interiores y exteriores.

A diferencia de los sistemas de Wi-Fi que utilizan un hardware (Wireless Switch), Unifi utiliza un software que no tiene costo y los Access Point pueden ir conectados a los switch existentes en la red. Las principales características del sistema UNifi son:

Software intuitivo que permite instalar, configurar y gestionar todos sus puntos de acceso inalámbrico Unifi con una intuitiva y fácil herramienta.

Los puntos de acceso Unifi tienen lo último en tecnología Wi-Fi 802.11n MIMO, son capaces de trabajar a velocidades de 300 Mbps con un alcance de hasta 500 pies (esto depende del medio ambiente y de las tarjetas inalámbricas que posea el cliente).

Extensibilidad ilimitada que permite construir su conexión inalámbrica tan pequeña o grande como lo necesite. Se empieza con uno y se puede expandir a miles.

Unifi posee soluciones para interiores y exteriores, a diferencia de las soluciones tradicionales de sistemas de administración centralizada de equipos inalámbricos, basados en hardware, Unifi de Ubiquiti emplea una aplicación virtual, basada en cliente/servidor, sin ningún costo adicional. El software UniFi permite administrar de forma fácil e intuitiva todos los Access Point conectados a la red. Una vez instalado el UniFiController en su PC o Mac, se puede acceder a los APs conectados, usando un Web browser. UniFiController permite la administración de los equipos, tráfico de la red, mapas, etc (Condor Comunicaciones, 2013).

**El paquete permite:**

- Actualización remota de firmware.
- Guest Portal/Hotspot.
- Integración a Google Maps.
- Eventos y alertas.
- Administración centralizada.
- Administración Capa 3







Figura 49. Monitoreo de APs desde una plataforma UniFi.  
Fuente: (Richardson Comunicaciones, 2016)

La figura anterior permite visualizar la interface gráfica de monitoreo corriendo en una plataforma Unifi de Ubiquiti, esta herramienta es muy práctica y amigable para el administrador debido a que funciona a través de la web.

- **Modelos de APs Unifi**

Tabla 8. Características técnicas de APs UniFi

				
	<b>UAP</b>	<b>UAP-LR</b>	<b>UAP-PRO</b>	<b>UAP-AC</b>
Frecuencia	2.4 GHz	2.4 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz
2.4 GHz Throughput	300 Mbps	300 Mbps	450 Mbps	450 Mbps
5 GHz Throughput	N/A	N/A	300 Mbps	1300 Mbps
Alcance	122 m	183 m	122 m	122 m

Fuente: Propia

La tabla anterior muestra una comparativa de equipos disponibles en la plataforma UniFi. Descripción de frecuencia, rendimiento y alcance de cada equipo.

### 3.2.8.3 Plataforma D-Link

D-Link Central WiFiManager es una herramienta gratuita que permite a los administradores de redes racionalizar la gestión de los diferentes puntos de acceso en una infraestructura inalámbrica.

Pudiéndose implementar en un equipo local o como un servicio en una cloud pública, el software de gestión de puntos de acceso D-Link Central WiFiManager (CWM-100) puede integrarse con los elementos de la red y gestionar de una forma sencilla una red inalámbrica, independientemente de su tamaño.

Preparado para trabajar con diferentes puntos de acceso inalámbricos profesionales de D-Link, proporciona a la empresa un sistema sólido para el control de su red Wi-Fi de forma centralizada, tanto en local como en remoto. Se instala sobre plataforma Windows y puede gestionar hasta 500 puntos de acceso sin ningún tipo de coste ni licencia adicional. Una vez instalado el controlador software en un PC, la interfaz de gestión de CentralWiFi Manager está basada en web, por lo que es posible acceder a ella en remoto con cualquier navegador web desde ordenadores, móviles o tabletas (Ros, 2015).

El software D-Link Central WiFiManager (CWM-100) está orientado a empresas, hoteles o almacenes que necesiten gestionar y tener seguridad en el acceso inalámbrico de empleados y/o clientes de forma centralizada.

Otra posibilidad es que un proveedor de servicios quiera ofrecer a sus clientes, pequeñas o medianas empresas, gestión remota de su red Wi-Fi sin necesidad de contar con un administrador local en cada uno de sus clientes.

El software de gestión está basado en web, por lo que permite administrar y monitorizar redes desde cualquier punto del mundo con un Smartphone, tablet o PC. Ofrece gestión de los puntos de acceso, así como funciones de reportes y monitorización que pueden incorporarse a la red sin necesidad de una instalación adicional. Además, el control del ancho de banda y la

gestión automática de radiofrecuencia permiten optimizar el rendimiento de la red en todo momento (Ros, 2015).

Central WiFiManager es una herramienta de software para gestión de puntos de acceso que está disponible para su descarga gratuita. Ofrece soporte para un amplio rango de modelos de puntos de acceso de D-Link, desde dispositivos de banda única 802.11n a doble banda 802.11ac con velocidades combinadas de hasta 1.750 Mbps.

Central Wifi Manager está diseñado para entornos empresariales. Permite gestionar hasta 500 puntos de acceso sin ningún coste adicional, e incorpora funciones como optimización del ancho de banda, portal cautivo y gestión integrada de radiofrecuencia, que cubren las necesidades de cualquier red con independencia de su tamaño.

Ofrece control de acceso de los usuarios de la red, incluyendo invitados mediante un portal cautivo sencillo y personalizable que facilita la autenticación; permite disponer de cuentas dedicadas de usuario o códigos de acceso temporales para rentabilizar la inversión en su red wireless, proporcionando conexión a Internet Wi-Fi como un valor más de su negocio.

Cabe destacar que el Central WiFiManager ofrece escalabilidad y flexibilidad: no sólo por llegar a soportar hasta 500 puntos de acceso, sino porque puede utilizar estos AP como Stand Alone en el momento inicial, y poder terminar gestionándolos centralizadamente a través del CWM en caso necesario. Además, proporciona cobertura inalámbrica global, que abarca soluciones Wireless N y Wireless AC, con velocidades que van de los 300 Mbps a los 1.750Mbps, con puntos de acceso tanto de interior como de exterior (Ros, 2015).

### **Características fundamentales**

Las principales características de Central WiFiManager (CWM-100) son:

- Gestión basada en web. El controlador de software puede instalarse en un PC Windows y acceder a él desde cualquier dispositivo con un navegador web, incluyendo smartphones, tabletas y PC.

- Gestión multi sitio. Es posible gestionar puntos de acceso instalados en ubicaciones remotas.
- Gestión a través de NAT. Los controladores pueden manejar los puntos de acceso en localizaciones remotas incluso si están ubicados detrás de un dispositivo NAT (router o firewall), sin necesidad de disponer conexiones VPN.
- Incorpora soporte para autenticación WiFi mediante base de datos local, RADIUS, LDAP, POP3 así como control de acceso de usuarios.
- Gestión de auto-radiofrecuencia (RF) Gestiona de forma automática los canales y la potencia de emisión de los puntos de acceso.
- Optimización de ancho de banda.

Como se ha indicado, Central WiFiManager permite la gestión de puntos de acceso independientemente del tamaño de la red. Pero podemos indicar algunos posibles escenarios donde implementar esta solución.

- Uno de estos escenarios es la empresa, independientemente de su tamaño, donde un administrador de red puede gestionar desde su propio smart phone, tablet o PC todos puntos de acceso de la compañía, tanto en la sede central como en las diferentes oficinas remotas.
- Centros educativos, donde el administrador puede gestionar el acceso a la red de cada alumno o de cada profesor.
- Almacenes o tiendas, donde el administrador puede, además de controlar los puntos de acceso, ofrecer diferentes modalidades y permisos de conexión si se trata de un trabajador o de un cliente. En este caso, el sistema puede trabajar en modo Hot-Spot y proporcionar acceso temporal a usuarios invitados. Éste puede ser un formato similar al empleado en hoteles, donde el personal del mismo tiene unas posibilidades de acceso diferentes a las de los diferentes clientes.



*Figura 50. Plataforma centralizada para redes Wi-Fi en la marca D-Link.  
Fuente: (Conectónica, 2015)*

La figura anterior muestra los seis puntos de acceso compatibles con la herramienta CWM propietaria del fabricante Dlink. Se trata de los DAP-2695 y DAP-2660, ambos dispositivos son 802.11ac Dual-Band; DAP-2690 es un punto de acceso 802.11n, y dos dispositivos 802.11n Single-Band, DAP-2360, y DAP-2310. También hay que destacar un punto de acceso para exteriores, el DAP-3662, también 802.11ac Dual-Band.

En el análisis comparativo de marcas se ha dejado a grandes competidores de lado, entre los cuales obligatoriamente se debe mencionar a Cisco - Linksys, Motorola, Engenius, Trendnet, que son marcas con presencia y productos en el segmento Wi-Fi para interiores ya que muchos de ellos no poseen una plataforma de manejo integrado. Otros hasta la fecha de esta investigación no cuentan con productos que posean las características buscadas y más bien son de uso doméstico.

### **3.2.9 Comparativa de selección de la mejor tecnología**

Para realizar la comparación se establece un puntaje para cada una de las características que satisface cada producto seleccionado para la comparación.



Tabla 9. Definición de métricas para el cumplimiento de selección

<b>Métricas de cumplimiento</b>				
Cumplimiento	SI	NO		
Equivalente	1	0		
<b>Métricas para evaluación según valores</b>				
Consumo Energético		2 watts	4 watts	11 watts
Valoración		3	2	1
Cobertura en metros (Hasta)		150	125	100
Valoración		3	2	1

Fuente: Propia

La tabla anterior considera los valores que serán tomados en cuenta en la selección de la tecnología más adecuada para la aplicación de la nueva red en la FICA.

Tabla 10. Comparativa de selección de la tecnología más adecuada

	<b>D-link DAP-2660</b>	<b>Mikrotik Cap2n</b>	<b>Ubiquiti Unifi</b>
<b>Rango de frecuencia</b>			
2.4 GHz	1	1	1
5.0 GHz	1	0	0
<b>Seguridad Inalámbrica</b>			
WEP	1	1	1
WPA-PSK	1	1	1
WPA-TKIP	0	1	1
WPA2-PSK	1	1	0
WPA2 AES	0	1	1
WPS	1	0	0
MAC	1	1	1
FILTRO DE DIRECCIONES	1	1	0
802.11i	0	1	1
<b>Estándares de red</b>			
IEEE 802.11a	1	0	0
IEEE 802.11b	1	1	1
IEEE 802.11g	1	1	1
IEEE 802.11n	1	1	0

IEEE 802.11ac	1	0	0
IEEE 802.11n*	0	0	1
IEEE 802.3u	1	0	0
IEEE 802.3ab	0	0	0
IEEE 802.3af	0	0	0
<b>Velocidades máximas</b>			
Hasta 300 Mbps en 2.4 GHz	1	1	1
Hasta 900 Mbps en 5.0 GHz	1	0	0
<b>Indicador</b>			
LED (Encendido)	1	1	1
<b>Certificación</b>			
FCC	1	1	1
IC	1	1	1
CE	1	1	1
UL	1	1	0
Wi-Fi Certified	1	1	0
<b>Adaptador de corriente y consumo energético</b>			
12 V	1	1	1
24 V	0	1	1
57 V	0	1	0
PoE	1	1	1
Watts (Rango)	1	3	2
<b>Cobertura</b>			
Metros (Rango)	1	3	2
<b>Dimensiones y peso</b>			
Dimensiones	170 x 170 x 28 mm	185 x 31 mm	20 x 20 x 3.65 cm
Peso	316 g		290 g
Antenas	Dos internas 3 dBi para 2.4 GHz Dos internas 4 dBi para 5 GHz	Interna 2 dBi para 2.4 GHz	2 antenas Integradas (soporta modo MIMO 2x2 con diversidad espacial)

*Fuente: Sitios web del fabricante*

### 3.2.9.1 Sumario de resultados a la comparativa de selección

Tabla 11. Sumario de resultados a la comparativa de selección

CARACTERÍSTICAS	DAP-2660	Cap2n	Unifi
Rango de frecuencia	2	1	1
Seguridad Inalámbrica	6	8	6
Estándares de red	6	3	3
Velocidades máximas	2	1	1
Indicador	1	1	1
Certificación	5	5	3
Adaptador de corriente y consumo energético	3	7	5
Cobertura	1	3	2
Dimensiones y peso	No aplica	No aplica	No aplica
Suma / 35	26	29	22
Total %	76%	83%	63%

Fuente: Propia

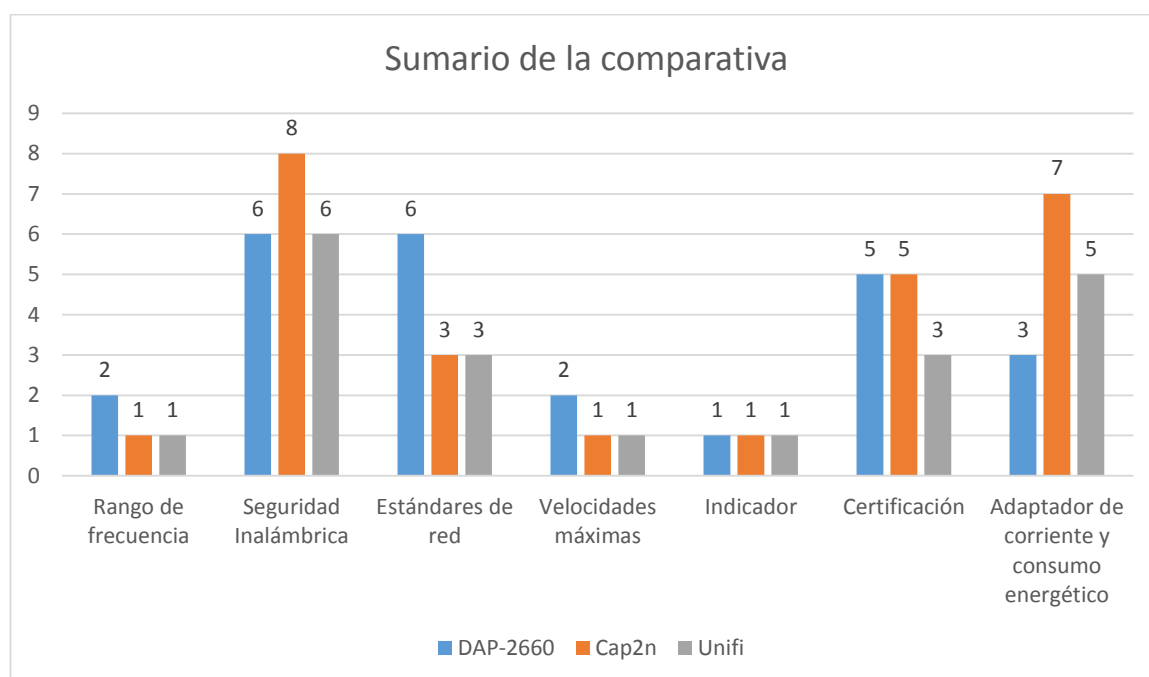


Figura 51. Sumario de la comparativa

Fuente: Propia

Una vez concluido con el proceso de evaluación de cada tecnología seleccionada se evidencia mediante el sumario de la comparativa que la más adecuada para ser utilizada en la

aplicación del nuevo sistema de gestión Wi-Fi es el Mikrotik Cap2n que satisface las características propuestas en un 83%.

### 3.2.10 Selección la tecnología más adecuada

Como se justificó en las secciones anteriores la plataforma elegida para desarrollar nuestra solución fue del fabricante Mikrotik, con su sistema operativo integrado RouterOS, del mismo trabajamos con los equipos cAP2n, que como se había mencionado es el equipo que mejores prestaciones tiene para aplicaciones indoor<sup>25</sup> inalámbricas sobre todo en ambientes de concurrencia masiva, como es nuestro caso los interiores del edificio de la FICA.



*Figura 52. Vista frontal de un cAP2n.  
Fuente: (Routerboard, 2016)*

La figura anterior es una vista frontal de cómo se ve el routerboard de Mikrotik, llamado cAP2n, este equipo ha sido elegido gracias a sus prestaciones no solo técnicas sino también estéticas para ser ubicado el techo de los interiores de la facultad sin que se vea afectada la ornamentación del sitio.

<sup>25</sup> Indoor. Término usado en equipos de transmisión inalámbrica usados en interiores de hogares, hoteles, centros comerciales, etc.

A continuación, en la siguiente tabla se detalla las características técnicas más importantes que brinda el routerboard cAP2n:

*Tabla 12. Características técnicas de un RBcAP2n*

Código del producto	RBcAP2n
Velocidad CPU	400 MHz
Número de CPU	1
Memoria RAM	64 MB
10/100 puertos Ethernet	1
Modelo de chip wireless	AR9331
Estándares Wireless	802.11b/g/n
Voltaje de ingreso soportado	11 V - 57 V
Dimensiones	185mm diámetro, 31mm.
Sistema Operativo	RouterOS
Rango de temperatura Operativo	-30C a +70C
Nivel de licencia	4
Ganancia de Antena en DBI	2
CPU	AR9331
Máximo consumo de Poder	2W
Numero de antenas	1
Tipo de almacenamiento	FLASH
Tamaño del almacenamiento	16 MB

*Fuente: Propia*

En la tabla anterior se muestra las características técnicas del RBcAP2n. Equipo que será instalado en como punto de acceso en cada uno de los pasillos de edificio de la Facultad de Ingeniería en Ciencias Aplicadas.

En resumen, él RBcAP2n es un punto de acceso compacto que se puede instalar en el techo o pared. Opera en la banda de 2,4 Ghz 802.11b/g/n, permite su gestión conjunta con otros dispositivos Mikrotik mediante el controlador wireless por software, denominado CAPSMAN. El controlador CAPSMAN se puede instalar en cualquier routerboard Mikrotik que ya tengamos en la red, por lo que no hace falta un equipo dedicado externo (PC, controlador hardware) para instalarlo. Es el equipo perfecto para hoteles, aeropuertos, espacios públicos y en nuestro caso para ambientes universitarios.

Una de las grandes ventajas que tiene este equipo es que está diseñado para ser montado sobre techos y paredes y que además para su facilidad de instalación se energiza por POE<sup>26</sup> (Power Over Ethernet) es decir con el mismo cable de red. La ventaja del equipo al ser montado en el techo es que evita de mejor manera los obstáculos tradicionales de un ambiente de trabajo como son mobiliario, equipos e incluso las mismas personas transitando.

Sin embargo, que el fabricante indica que estos equipos funcionan de manera adecuada en un rango de hasta 100 metros a la redonda, en línea recta y sin obstáculos, el área en la que se ha suscrito es de 15m de alto por 33 m de ancho.

Se puede instalar un solo equipo por cada piso a cubrir, pero se debe tomar en cuenta que el número de usuarios concurrentes va a ser bastante alto por lo que más bien decidimos colocar 3 equipos por cada piso, esto porque es el número máximo de equipos que pueden coexistir en el mismo ambiente de irradiación en la frecuencia 2.4 Ghz, sin que sus frecuencias de trabajo se solapen. Sin embargo, que el equipo Cap2n es capaz de trabajar con anchos de banda de 5, 10, 20, 30 y 40 MHz, se decidió trabajar con 20 MHz pues este ancho de banda permite la

---

<sup>26</sup> POE. Permite la transmisión de electricidad y datos a través de cable UTP/STP.

asociación de estaciones que trabajan con los estándares b y g más antiguos, si se considera un ancho de banda del canal de 20 MHz más 5 MHz de separación, las frecuencias con las que se trabajó son: 2412, 2437 y 2462 MHz

Se debe mencionar que el equipo finalmente trabajará con una modulación TDMA<sup>27</sup> (Time Division Multiple Access) que permitirá entregar a cada estación la máxima velocidad posible, esto sobre todo a estaciones nuevas como laptops y celulares de última generación que tienen interfaces de hasta 150 Mbps de velocidad.

### 3.2.11 Análisis costo beneficio

En este punto se debe considerar que es imperiosa la optimización recursos para la implementación del proyecto, debido a eso se realiza un análisis comparativo de precios y marcas como puede verse en la tabla siguiente, Dando un valor agregado al análisis comparativo realizado para la selección de la tecnología más adecuada.

*Tabla 13. Análisis comparativo de marcas con precios*

	MODELO	CANTIDAD DE APs	P. UNITARIO	TOTAL
D-link	DAP-2660	15	200,00	3000,00
Mikrotik	Cap2n	15	70,00	1050,00
Ubiquiti	Unifi UAP	15	90,00	1350,00

*Fuente: Propia*

La tabla anterior muestra una comparativa de equipos de marcas y precios de las diferentes plataformas analizadas y los datos presentados fueron tomados de las páginas de cada

<sup>27</sup> TDMA. Es una tecnología inalámbrica de segunda generación, que distribuye las unidades de información en ranuras alternas de tiempo. Fuente: (Alegsa, 2010)

fabricante en el mes de agosto del 2015, cabe indicar que al precio de compra ha sido agregado costos de importación e impuestos de ingreso al país.

Adicional a los costos por dispositivo es necesario catalogar los costos generados por los materiales y dispositivos adicionales utilizados para la construcción de la infraestructura de red.

*Tabla 14. Costos adicionales para la construcción de la infraestructura nueva de red*

<b>Materiales y Dispositivos</b>				
	Modelo	Cantidad De Aps	P. Unitario	Total
Qpcom	qp-1240r	1	150.00	150.00
UTP	Cat. 6a	750 metros	0.57	427.5
Conectores	Rj45	30	0.25	7.50
Patch cord	Cat. 6a	2	8.00	16.00
Canaleta	Canaleta	60	2.50	150.00
Mikrotik	RB1100AHx2	1	650.00	650.00
			<b>Total</b>	<b>1401.00</b>

*Fuente: Propia*

Pero es necesario recordar el valor de los dispositivos utilizados en la red antigua dejando claro así que el reemplazo de un dispositivo averiado por uno de la nueva red es más económico.

*Tabla 15. Costo invertido en la red antigua.*

	<b>MODELO</b>	<b>CANTIDAD DE APs</b>	<b>P. UNITARIO</b>	<b>TOTAL</b>
<b>Dispositivo AP</b>				
Cisco	Aironet 1130 AG	6	399,00	2394,00



---

<b>Otros</b>				
UTP	Cat. 6a	240 metros	0,75	180,80
Conectores	Rj45	12	0.40	4.80
Patch cord	Cat. 6a	2	10.00	20.00
Canaleta	Canaleta	30	2.80	84.00
Cisco	Switch 4506	1	650,00	650,00
				3332.80

---

*Fuente: Propia*

Dichos datos permiten determinar que es factible la utilización del dispositivo base seleccionado mediante el análisis comparativo y bajo el análisis de costos debemos inclinarlos por la solución Mikrotik pues tiene el costo más bajo pues el costo de reemplazar un dispositivo de la red antigua muy elevado.

*Tabla 16. Comparativa de precios unitarios del AP nuevo vs antiguo*

	Mikrotik Cap2n (Nuevo)	Cisco Aironet 1130 AG (Antiguo)
Precio	70,00	399,00

---

*Fuente: Propia*

La tabla anterior muestra una comparativa del costo individual del dispositivo AP utilizado en la red nueva y en la red antigua dando una ventaja muy amplia en cuanto a su costo ante posibles reemplazos.

Ahora si se hace el análisis de la plataforma de manejo centralizado de cada uno se debe indicar que tanto el mercado ecuatoriano y latinoamericano se orienta a la solución Mikrotik, gracias su versatilidad, escalabilidad, actualizaciones ilimitadas por licenciamiento, todas estas buenas y amigables características han hecho que al menos en el tema de ruteo y manejo centralizado sigan siendo la marca de mayor crecimiento en nuestro medio.

La versatilidad en la administración y configuración que brindan los puntos de acceso de la marca Mikrotik, para el caso del presente proyecto se ha seleccionado el cAP2n, el mismo que permite establecer: el máximo número de estaciones que pueden conectarse a cada AP, el rango de sensibilidad de señal, la potencia de transmisión y finalmente este equipo permite convertirse en CAP y ser administrado de manera centralizada mediante el gestor CAPsMAN.

De las pruebas realizadas a la red Wi-Fi que venía funcionando previamente a la implementación del presente proyecto existente se determinó que el uso de los recursos es bastante bajo, del lado final (red de transporte e internet) y altísimo del lado inicial (red de acceso) esto genera que desde el inicio existe congestión en el sistema y que al final la experiencia que tiene el usuario es bastante mala. Se puede decir que, si se logra implementar una red de acceso más robusta y a menor costo, esta permite que el sistema pueda gestionar de mejor manera y así se pueda encontrar los siguientes beneficios:

- Optimización en cuanto al número de equipos (menor presupuesto)
- Administración inteligente en cuanto a la red de acceso, esto evitará la congestión de entrada.
- Mejor uso de la red de transporte al evitar retransmisiones.
- Uso eficiente y completo del ancho de banda.
- Menor tiempo necesario para realizar una tarea de navegación.

Dadas estas consideraciones se justifica la implementación de un sistema de gestión Wi-Fi centralizado en la FICA que tenga un costo accesible per a la vez brinde las mejores prestaciones y calidad de servicio en el usuario final

### **3.3 Implementación del sistema de gestión Wi-Fi**

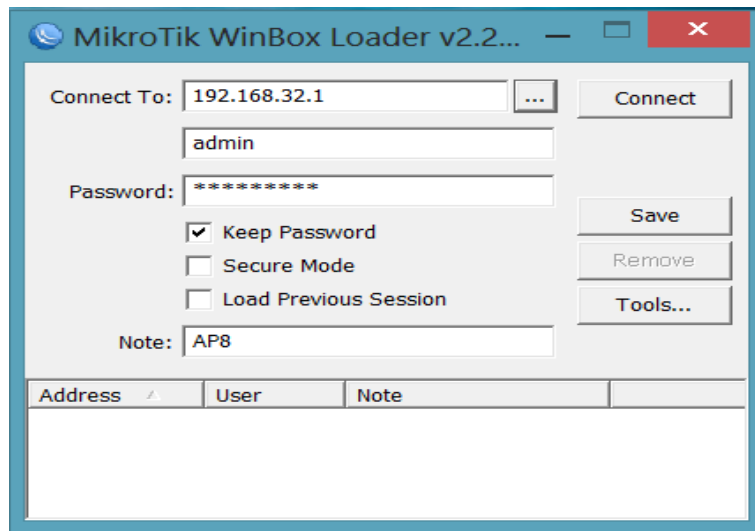
#### **3.3.1 Implementación**

Para la configuración del sistema de red Wi-Fi centralizado, se debe definir el direccionamiento IP y para eso se tomó como una subred clase C, que normalmente es utilizada para pequeñas y medianas empresas. El rango disponible de una red Clase C es: 192.168.0.0 a 192.168.255.255, teniendo disponibles 24 bits para red y 8 bits para host. Para el proyecto se tomó la red 192.168.32.0/22, con 1022 host disponibles en toda la red LAN.

Para la red de infraestructura, se ha reservado el rango desde la 192.168.32.2 que identifica al AP1 hasta la 192.168.32.16 que le correspondería al AP15.

La red WAN es dada por el proveedor del servicio, es la red 172.17.42.0/24. El Gateway y DNS asignados son 172.17.42.1 y 172.16.1.254, teniendo un total de 254 IPs, disponibles para acceso WAN.

Para la configuración de un Routerboard Mikrotik, existen varias opciones disponibles en el mercado, entre las más importantes tenemos la Web, ingresando la IP del routerboard a través de un navegador con su respectivo usuario y contraseña y como segunda opción se tiene la herramienta propietaria de Mikrotik, llamada Winbox. Siendo esta la más amigable con administrador, ya que permite visualizar el proceso de configuración y funcionamiento del equipo en tiempo real.



*Figura 53. Herramienta WinBox de Mikrotik  
Fuente: Propia*

La figura anterior muestra a Winbox que es una pequeña aplicación que nos permite la administración de Mikrotik RouterOS usando una interfaz gráfica de usuario fácil y simple. Es un binario Win32 nativo, pero se puede ejecutar en Linux y Mac usando Wine (Wine es una aplicación que permite usar programas de windows en linux).

Casi todas las funciones que podemos hacer por medio de la interfaz winbox se puede hacer por consola y viceversa.

### **3.3.2 Configuración del servidor central, el RB1100AHx2**

Una vez determinado la herramienta a utilizarse y el direccionamiento IP, se empezó con la configuración del equipo de gestión centralizada, es el routerboard RB1100AHx2 de la marca Mikrotik. Este equipo es el encargado gestionar de forma centralizada cada uno de los 15 APs que se colocaran en las 5 plantas del edificio de la FICA.

La configuración del equipo de gestión centralizada se detalla en los siguientes pasos:

- **Paso 1:** Ingreso a la pantalla de configuración inicial

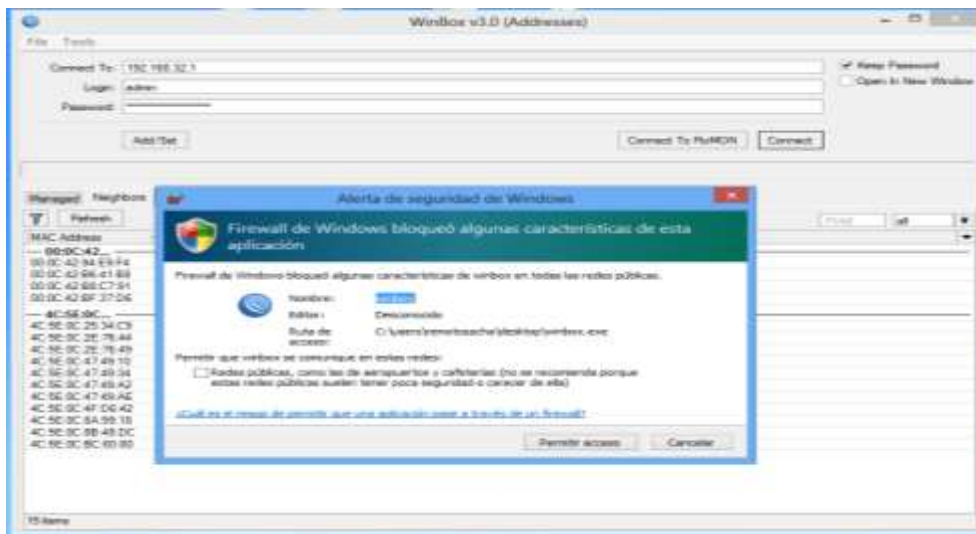


Figura 54. Ingreso a la interface de configuración con WinBox.  
Fuente: Propia

Como se puede ver en la figura anterior al ejecutar el WinBox, lo primero que se debe hacer es permitir la ejecución de esta herramienta a través del firewall del sistema operativo, una vez que se tiene acceso a la aplicación sin ninguna restricción, la ventana de WinBox permite acceder al equipo mediante IP o a través de MAC<sup>28</sup>. La ventaja de acceder a través de MAC es que no se necesita estar en el mismo segmento de red con el equipo a ser configurado, es decir que si se cambia la IP del equipo local de configuración la conexión con la interface de configuración no se pierde.

Entonces para nuestro caso se selecciona acceso mediante MAC debido a la fiabilidad que ofrece cuando se encuentra conectado al equipo administrable, sin embargo, se debe indicar que la IP de defecto del RB1100AHx2 es **192.168.88.1 /24** y el usuario es **admin** y la contraseña **espacio en blanco**.

<sup>28</sup> MAC. Identificador único asignado por el fabricante a una pieza de hardware de red.

Una vez dentro del routerboard Mikrotik, el fabricante muestra la configuración que viene dentro del mismo, se debe remover esta configuración para evitar complicaciones con la configuraciones que se van a realizar.

A continuación, se actualiza la última versión del firmware (routeros-mipsbe-6.35rc1.npk) disponible por el fabricante, para obtener el mejor rendimiento del RB1100AHx2.

- **Paso 2:** Pantalla de principal e identificación de interfaces

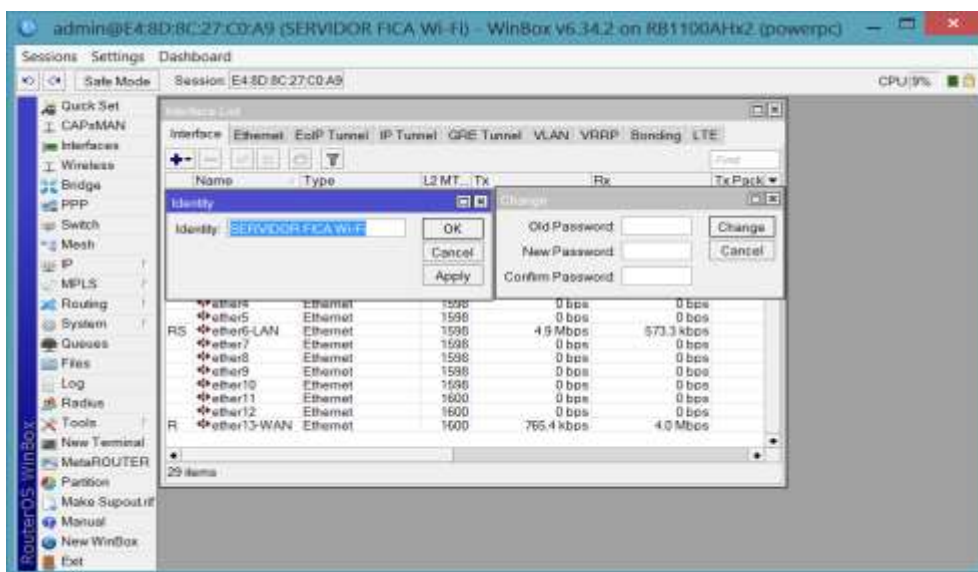


Figura 55. Pantalla de configuración principal de un equipo Mikrotik.  
Fuente: Propia

Una vez actualizado el firmware y adentro del equipo, lo primero que se configura es el nombre que identifique al equipo, para este caso se le denominó “SERVIDOR FICA Wi-Fi”.

Name	Type	L2 MT	Tx	Rx	Tx Packet (p/s)	Rx Pac
R	Bridge1	Bridge	1598	14.0 Mbps	998.1 kbps	1.842
RS	cap1-AP1	Interfaces	1600	85.6 kbps	85.2 kbps	45
RS	cap2-AP2	Interfaces	1600	0 bps	0 bps	0
RS	cap3-AP3	Interfaces	1600	71.3 kbps	11.2 kbps	44
RS	cap4-AP4	Interfaces	1600	3.4 Mbps	162.1 kbps	346
RS	cap5-AP5	Interfaces	1600	1298.1 kbps	83.4 kbps	156
RS	cap6-AP6	Interfaces	1600	14.3 kbps	0 bps	24
RS	cap7-AP7	Interfaces	1600	1146.1 kbps	54.9 kbps	132
RS	cap8-AP8	Interfaces	1600	15.3 kbps	1646 bps	26
RS	cap9-AP9	Interfaces	1600	852.3 kbps	29.3 kbps	91
SM	cap10-AP10	Interfaces	1600	0 bps	0 bps	0
SM	cap11-AP11	Interfaces	1600	0 bps	0 bps	0
SM	cap12-AP12	Interfaces	1600	0 bps	0 bps	0
SM	cap13-AP13	Interfaces	1600	0 bps	0 bps	0
SM	cap14-AP14	Interfaces	1600	0 bps	0 bps	0
SM	cap15-AP15	Interfaces	1600	0 bps	0 bps	0
	ether1	Ethernet	1598	0 bps	0 bps	0
	ether2	Ethernet	1598	0 bps	0 bps	0
	ether3	Ethernet	1598	0 bps	0 bps	0
	ether4	Ethernet	1598	0 bps	0 bps	0
	ether5	Ethernet	1598	0 bps	0 bps	0
RS	ether6-LAN	Ethernet	1598	5.4 Mbps	558.9 kbps	1.022
	ether7	Ethernet	1598	0 bps	0 bps	0
	ether8	Ethernet	1598	0 bps	0 bps	0
	ether9	Ethernet	1598	0 bps	0 bps	0
	ether10	Ethernet	1598	0 bps	0 bps	0

Figura 56. Etiquetado de interfaces según su funcionalidad.  
Fuente: Propia

En la figura anterior se asigna nombres a cada una de las interfaces para identificar y facilitar el trabajo al administrar el equipo. En el equipo de gestión centralizada, se han designado las interfaces ether13 como **ether13-WAN**, y la interface ether6 se la ha denominado **ether6-LAN**.

Antes de realizar el direccionamiento IP a cada interface, es necesario que estas sean claramente identificadas para no cometer errores al momento de realizar las configuraciones del equipo de gestión central.

- **Paso 3: Direccionamiento IP**

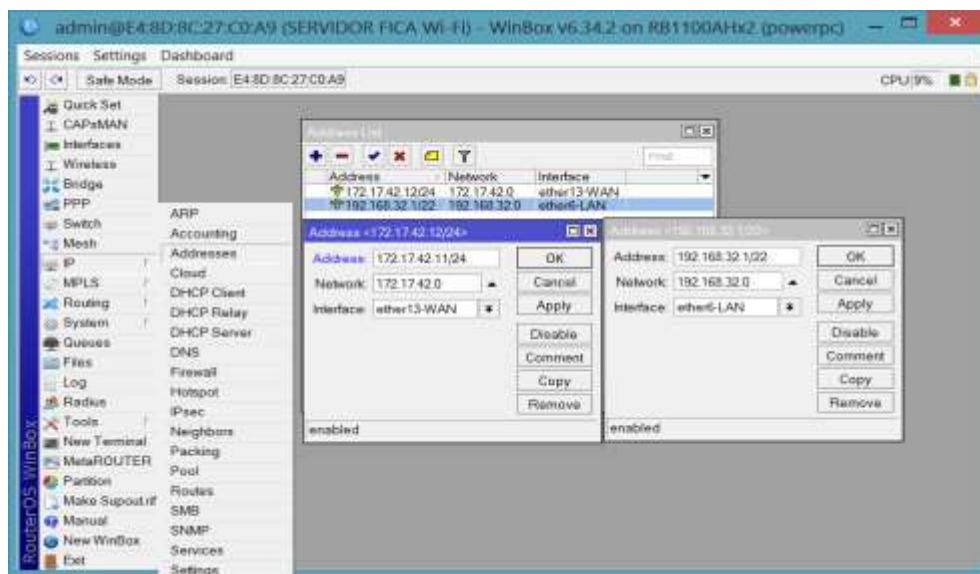


Figura 57. Asignación de IP a las interfaces ether13-WAN y ether6- LAN.  
Fuente: Propia

Ahora se asigna el direccionamiento IP a cada interface, según su funcionalidad. La dirección

172.17.42.11/24 ha sido asignada a la interface denominada **ether13-WAN**, mientras que la dirección 192.168.32.1/22 se asigna a la interface **ether6-LAN**.

La dirección IP de la interface WAN está dada por el proveedor de servicios mientras que la dirección IP asignada a la red LAN ha sido escogida una dirección privada clase C con mascara /22 para la asignación de IPs a usuarios finales.

Para configurar las direcciones IP de cada interface se debe hacer lo siguiente:

1. En la pantalla principal ir a **IP**, y luego clic **Addresses**
2. En la ventana **Adresses List**, clic el signo +
3. En Adresses escribimos la IP 172.17.42.11/24, seleccionar la interface **ether13-WAN**
4. Clic en **Apply** y clic en **Ok**.



5. Para la asignación de la IP a la interface **ether6-LAN**, se repiten los numerales 1 y 2 y en campo **Addresses** se ingresa la IP 192.168.32.1/22, luego clic en **Apply** y **Ok**.
- **Paso 4:** Asignación automática de direcciones IP mediante DHCP Server

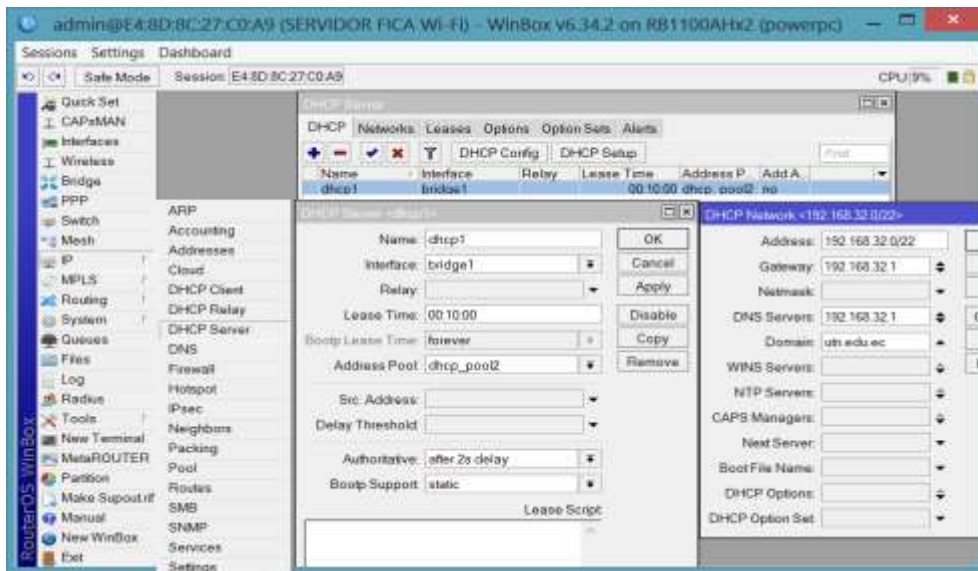


Figura 58. Activación y configuración del servidor DHCP.

Fuente: Propia

La figura anterior muestra la activación y configuración del servidor DHCP y la asignación del pool de IPs a la interface LAN.

Dentro de la pantalla principal:

1. Seleccionamos IP y activamos DHCP Server.
2. Una vez dentro, se agrega un nombre al nuevo servidor DHCP, se selecciona la interface **ether6-LAN**, la que se convertirá en la puerta de acceso a todos los usuarios finales, además de manera opcional se escoge un pool o rango disponible de direcciones IP que serán asignadas automáticamente a cada estación final.
3. Se selecciona la interface **bridge1**, esta será la puerta de enlace encargada de entregar automáticamente direcciones IP a toda la red LAN.

- En el campo **Lease Time** se ingresa 00:10:00, esto permite que el tiempo de arrendamiento de IPs a cada usuario de la red interna sea de hasta 10 horas.



Figura 59. Rango de direcciones disponibles para la red LAN.  
Fuente: Propia

- A continuación, en el **Address Pool** se selecciona **dhcp\_pool2**, esto establece el rango de asignación automática de IPs a la red interna. El mismo que va desde la 192.168.32.21–192.168.35.254. Luego para aplicar y guardamos los cambios haciendo clic en **Apply** y **Ok**.

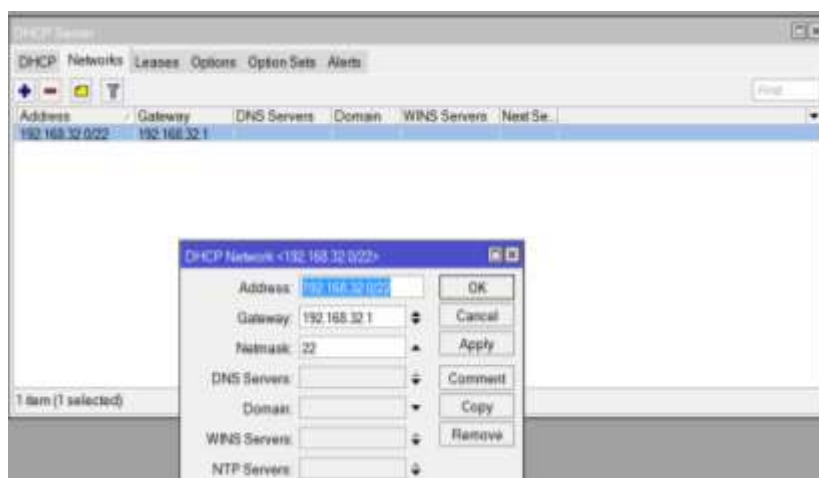


Figura 60. Dirección y máscara de red asignada al servidor DHCP.  
Fuente: Propia

La figura anterior muestra el servidor DHCP corriendo sobre el RB1100AHx2, en donde también puede verse que la máscara de red asignada es /22.

- **Paso 5:** Configuración de rutas en el servidor central

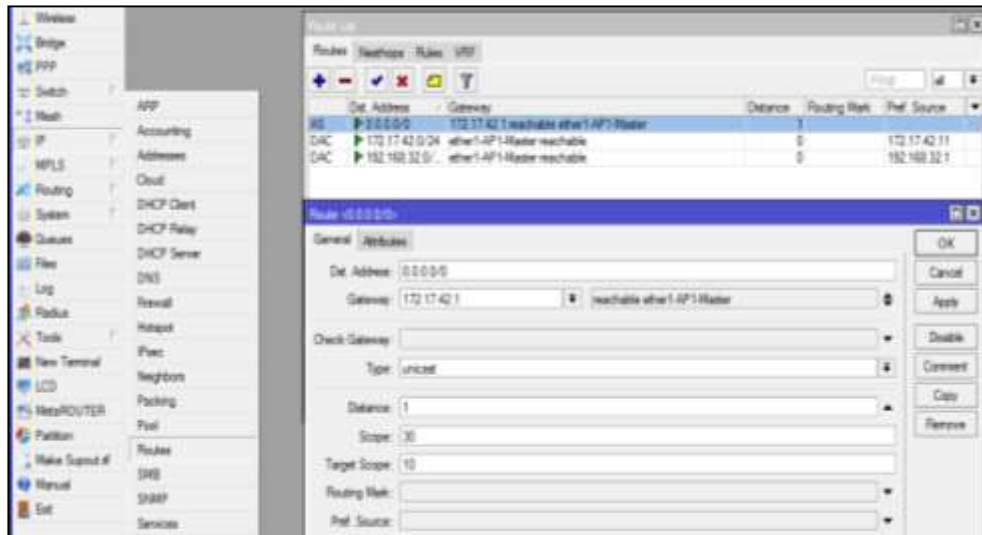


Figura 61. Configuración de rutas estáticas y dinámicas.  
Fuente: Propia

Como se ve en la figura anterior, se debe configurar las rutas de salida en el servidor central el RB1100AHx2 para lo cual se hace lo siguiente:

1. Desde la ventana principal, clic en **IP**, luego clic en **Routes**, una vez dentro puede verse las rutas 172.17.42.0/24 y 192.168.32.0/22 que se han creado automáticamente en el momento que se agregó IP a cada interface.
2. A continuación, se hace clic en el botón +, para agregar una nueva ruta.
3. Una vez dentro, en el campo Dst.Addresses se debe ingresar la dirección IP destino 0.0.0.0/0. Esta dirección destino es asignada dentro de la tabla de ruteo en el equipo local, para que las conexiones desde la red local nunca fallen en su salida a la red externa.
4. En el campo **Gateway** se ingresan la dirección 172.17.42.1.
5. Finalmente se hace clic en **Apply** y **Ok**, para aplicar y guardar los cambios efectuados.

- **Paso 6:** Configuración de Servidor de nombres de dominio (DNS)

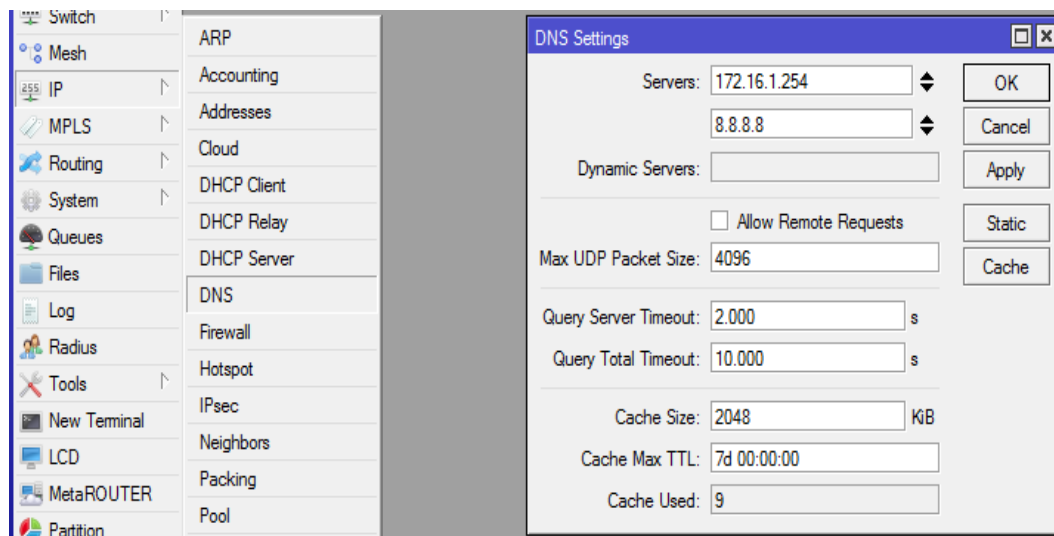


Figura 62. Configuración de rutas DNS principal y alternativo.  
Fuente: Propia

Para permitir el acceso a sitios web, el equipo central de ruteo debe ser configurado con la dirección del servidor de nombres de dominio, para conseguir esto se debe configurar lo siguiente:

1. En la pantalla principal de configuración, se hace clic en **IP** y luego en **DNS**.
2. Una vez dentro, en el campo **Servers** ingresamos la dirección 172.16.1.254, la cual es dada por el proveedor de servicios.
3. Adicionalmente en lado derecho del campo **Servers**, se hace clic en la flecha hacia abajo, y el nuevo campo en blanco se ingresa la dirección 8.8.8.8, siendo este un DNS alternativo de Google.
4. Finalmente se debe hacer clic en **Apply** y **Ok** para guardar los cambios.

Se debe considerar que, si se activa el **Allow Remote Requests**, el servidor central hace cache de DNS dentro del propio servidor, pero al habilitar esto significa mayor uso recursos de en el equipo, en este caso al disponer de un acceso WAN de alta velocidad se opta por optimizar recursos del hardware, por lo que este queda deshabilitado.

- **Paso 7:** Traducción de direcciones de red NAT (Network Address Translation)

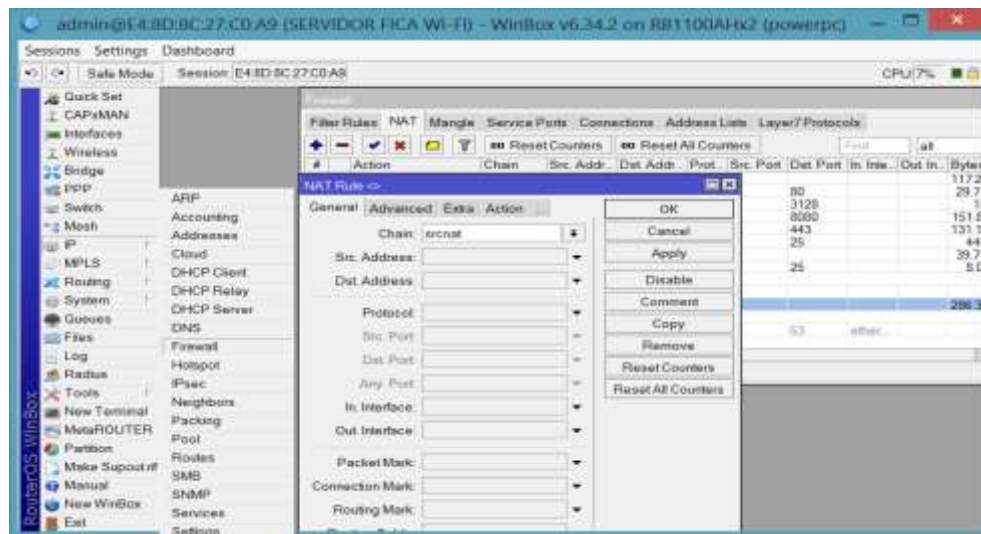


Figura 63. Traducción de direcciones de red (NAT).

Fuente: Propia

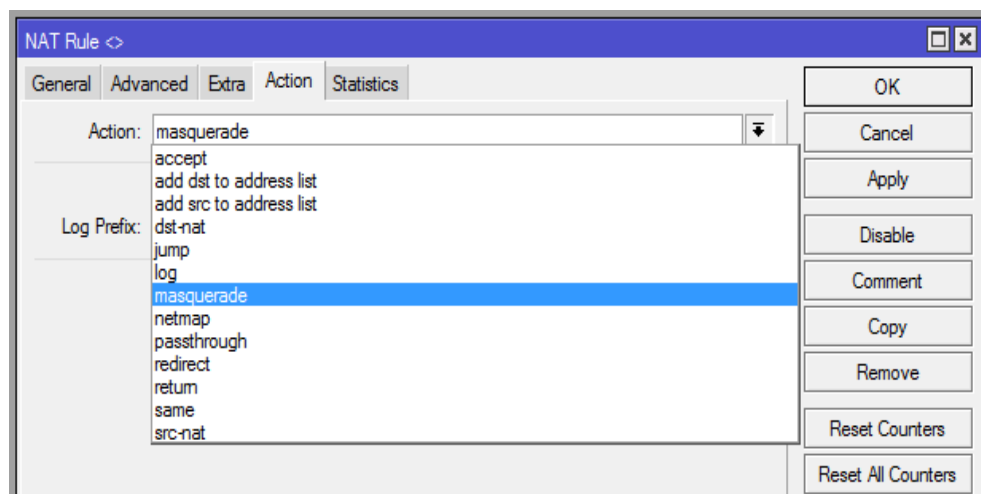


Figura 64. Enmascaramiento de direcciones de red.

Fuente: Propia

Ahora se debe configurar, el servidor de traducción de direcciones de redes NAT, para permitir que las estaciones finales identificadas con direcciones IP de clase C privada, puedan acceder hacia la red externa utilizando una misma IP pública asignada.

Para esto, una vez en la pantalla principal de configuración se hace lo siguiente:

1. Selecciona IP, Firewall, NAT, una vez aquí se agrega una nueva regla de NAT.
  2. Al ingresar a la nueva regla, en la pestaña **General**, en el campo **Chain** se elige **srcnat**.
  3. Adicional se escoge en el campo **Out Interface** se escoge la interface de salida **ether13-WAN** para direccionar el tráfico de salida a través de esta.
  4. A continuación, en la pestaña **Action**, selecciona la opción **masquerade** para permitir que la red LAN pueda salir enmascarada a través de la IP pública asignada en la interface ether13-WAN.
- **Paso 8: Configuración de seguridad**

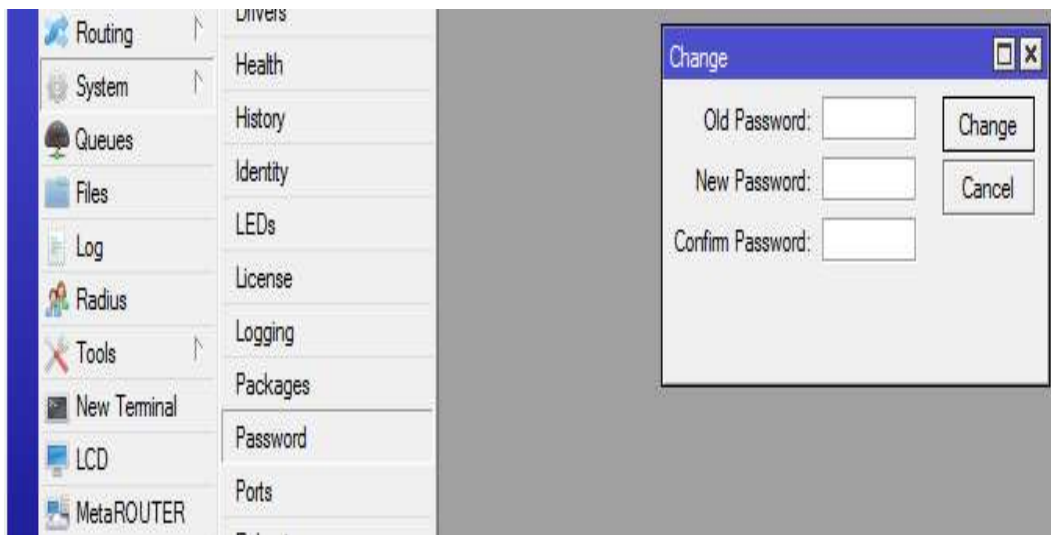


Figura 65. Implementación de seguridad en el equipo de gestión central.  
Fuente: Propia

Para garantizar, la seguridad e integridad de la información que cursa a través del equipo de gestión central, el RB1100AHx2 es configurado con usuario y contraseña adecuados para brindar mayor seguridad en el equipo, como puede verse en figura anterior. Para lograr esto se hace lo siguiente:

1. En la ventana principal, hacer Clic en **System** y luego en **Passwaord**.
2. En el campo **Old Password** se escribe la contraseña actual.

3. Luego en el campo New Password se escribe la nueva contraseña y seguido en el campo **Confirm Password** se confirma la nueva contraseña.
  4. Finalmente hacer clic en **Apply** y **Ok** para guardar los cambios.
- **Paso 9: Graficas de monitoreo**

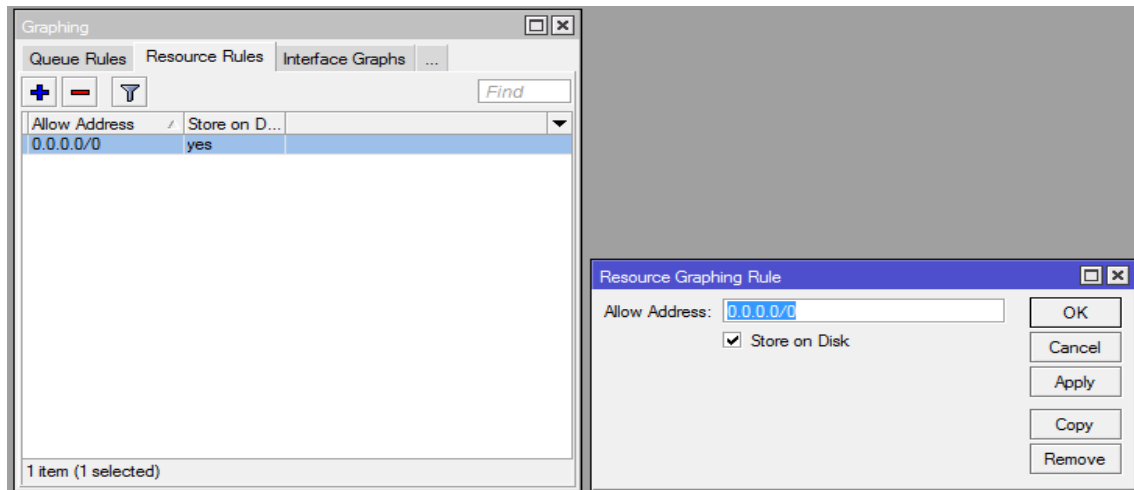


Figura 66. Activación y configuración de graficas de monitoreo de recursos.

Fuente: Propia

Finalmente, se debe habilitar las gráficas para monitoreo de recursos en servidor central, para esto hacemos lo siguiente:

1. En la ventana principal de configuración, se debe seleccionar **Tools**, luego **Graphing**, y luego clic en la pestaña **Resource Rules**, Una vez dentro hacer clic en el signo + para agregar una nueva regla de monitoreo.
2. En el campo **Allow Adresses** ingresar la IP 0.0.0.0/0, al hacer esto se permite que se puedan monitorear desde cualquier estación dentro de la red interna, al habilitar las gráficas en el servidor central se puede monitorear recursos como: tráfico de entrada y salida en todas interfaces, consumo de CPU y consumo de memoria y tiempo de funcionamiento del equipo.
3. Finalmente se hace clic en **Apply** y **Ok** para guardar los cambios efectuados.

### 3.3.3 Configuración de los puntos de acceso, los RBcAP2n

Determinado el direccionamiento IP, como se puede ver en la siguiente figura. Tanto para el equipo de gestión central, el RB1100AHx2 como para cada uno de APs, los RBcAP2n que se han instalado en cada piso.

Ahora se debe configurar cada uno de los APs, que se han distribuido desde el cuarto piso hasta la planta baja.

#### Configuración del AP1

- **Paso 1:** Identificación y direccionamiento del AP1

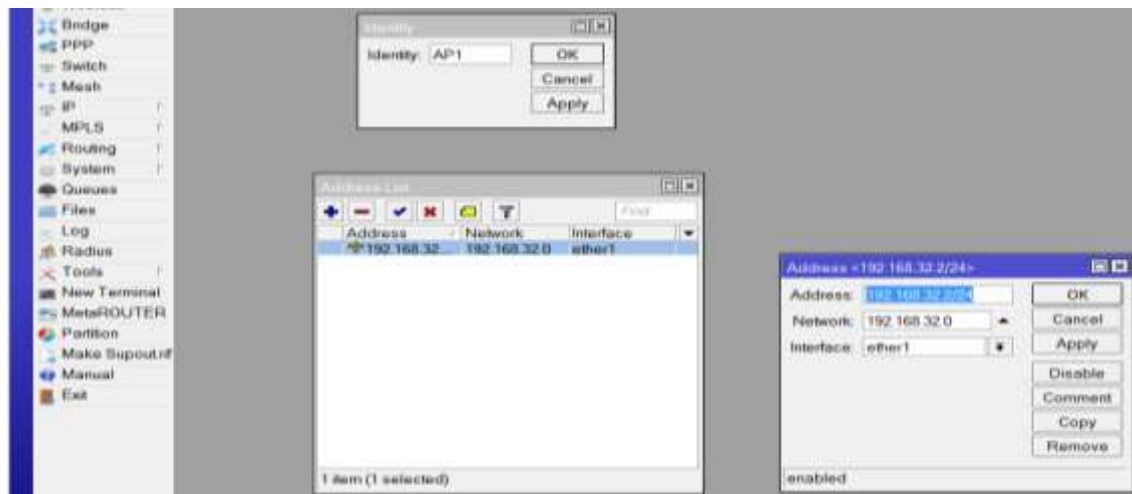


Figura 67. Etiquetado y asignación de direcciones a las interfaces del AP1.

Fuente: Propia

La figura anterior muestra la asignación de la dirección IP 192.168.32.2 a la interface ether1, que en adelante será denominada **AP1**, para conseguir esto se hace lo siguiente:

1. En la pantalla principal de configuración, hacer clic en **System** y luego clic en **Identity**.
2. Dentro de la venta en el campo en blanco se escribe **AP1**, este es el nombre que permite identificar en adelante al punto de acceso número uno. Para guardar los cambios, se hace clic en **Apply** y **Ok**.



3. A continuación, se debe asignar la dirección IP que permita identificar de manera lógica al AP1, para esto hacemos lo siguiente: clic en **IP**, luego entrar en **Addresses**, una vez dentro, hacer clic en el botón +, luego en el campo **Address** se ingresa la IP 192.168.32.2, luego se asigna la interface **ether1** (interface que posteriormente se la denominara AP1) y finalmente clic en a **Apply** y **Ok** para guardar los cambios.

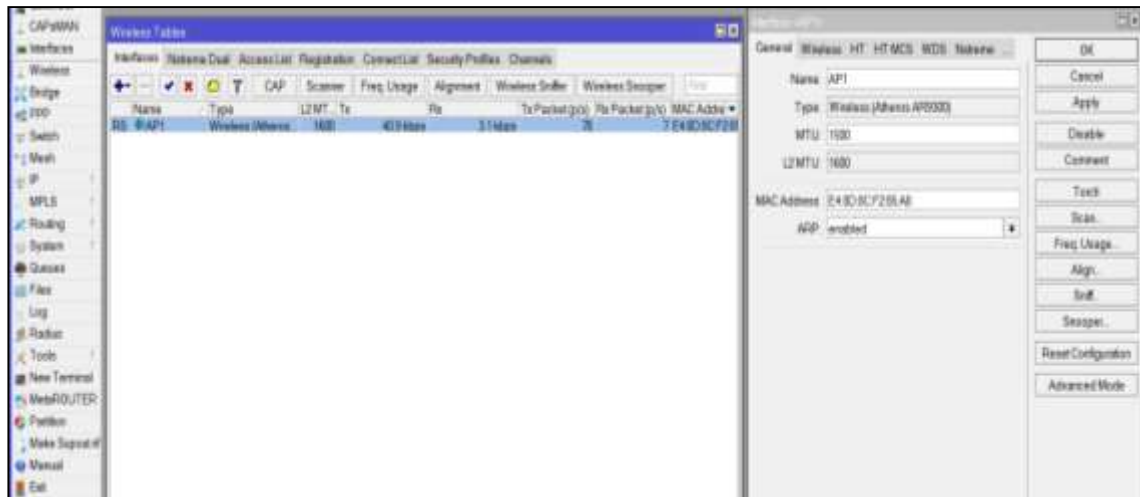


Figura 68. Etiquetado de la interface wireless del AP1.

Fuente: Propia

Al igual como se hizo con el equipo de gestión central (el RB1100AHx2), ahora la configuración del punto de acceso (El RBcAP2n) ahora llamado AP1, se inicia haciendo una identificación de tanto del equipo Access Point como también de cada una de las interfaces, tal como puede verse en la figura anterior. La interface wireless, del primer punto de acceso ahora se la denomina AP1, y así se sucesivamente se hace con las interfaces del resto de puntos de acceso hasta el AP15.

Para hacer esto se hace lo siguiente:

1. En pantalla principal de configuración, se hace clic en **Wireless**.
2. Una vez dentro, hacer clic en la pestaña interfaces, en la pestaña **General**, en el campo **Name** escribimos **AP1**.
3. Finalmente se guarda los cambios haciendo clic en **Apply** y **Ok**.

- **Paso 2:** Configuración de parámetros inalámbricos en el AP1



Figura 69. Configuración de parámetros en la interface wireless del AP1.

Fuente: Propia

Una vez que se ha identificado, el nombre del equipo, las direcciones IP y los nombres de las interfaces. Ahora se hace la configuración de los parámetros inalámbricos del AP1, para esto hacemos lo siguiente:

1. En la pantalla principal seleccionar el botón **Wireless** y luego clic en nuevamente en la pestaña **Wireless**.
2. Una vez dentro de la pestaña Wireless, en el campo **Modo** se escoge **ap bridge**, luego en el campo **Band** se escoge **2Ghz-B/G/N**, al seleccionar la banda de 2GHZ-B/G/N, se asegura que las estaciones basadas en estándares anteriores como 802.11b y 802.11g puedan inter operar con estaciones basadas en estándares de alta velocidad como 802.11n.
3. En **Channel Width** se escoge **20Mhz**, y en **Frequency** se escoge **2412**, con esto se establece que el ancho del canal de transmisión sea el mínimo y así evitar mayor interferencia en el medio.

4. A continuación, se configura el identificador del conjunto de servicios SSID, con el nombre de “**ficawifi**”, este será común para todos los puntos de acceso, debido a se necesita tener movilidad a través de todo el edificio de la Facultad. Para configurar esto se debe dirigir al campo **SSID**, en donde se ingresa **ficawifi**.
5. Al final un parámetro importante que se activa es el Default Authenticate, este permite que los dispositivos móviles se conecten de forma automática al encontrar el SSID, en caso contrario haría que las estaciones escaneen al AP, pero no se puedan registrar en el mismo.

Para la asignación de canales y frecuencias se determinó que el AP1 debe ser asignado el canal1 o la frecuencia 2412MHz.

- **Paso 3:** Fijación de Velocidades o Data Rates

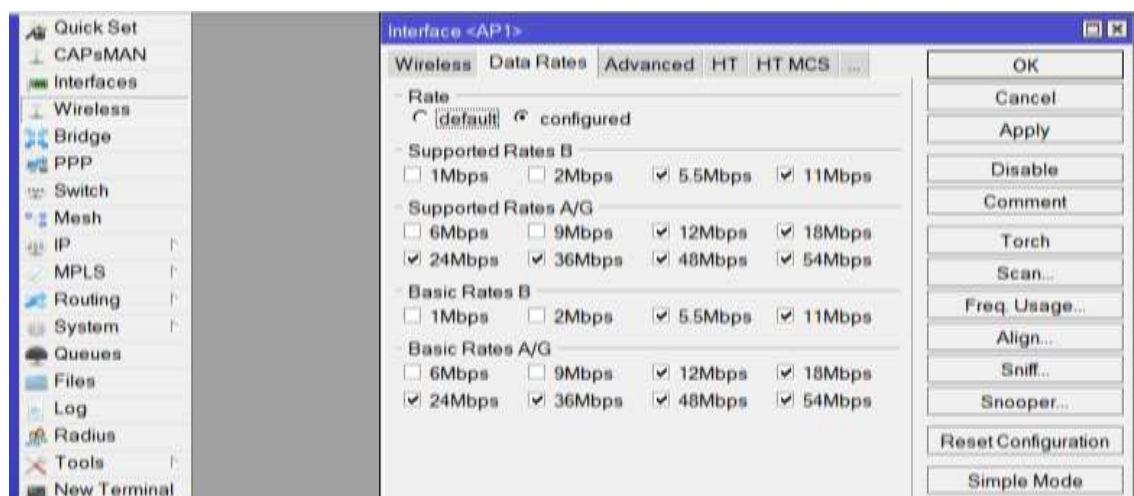


Figura 70. Fijación de velocidades en la interface Wireless del AP1.

Fuente: Propia

Ahora en el menú Data Rates, de la interface wireless se fijan las velocidades de 5.5Mbps y 11Mbps para 802.11b y las velocidades de 12, 18, 24, 36, 48 y 54Mbps para el estándar 802.11 A/G. Se deshabilita velocidades bajas como 1 y 2Mbps de cada uno de los estándares a fin de garantizar que las estaciones que se conectan en el AP operen a las mejores velocidades.

- **Paso 4:** Limite de estaciones



*Figura 71. Límite de estaciones que permite registrar simultáneamente el API.  
Fuente: Propia*

En la misma interface wireless, en la pestaña **advanced**, se configura el número máximo de 30 estaciones, ingresando el valor numérico **30** en el campo **<Max Station Count>**, se hace esto con el fin de garantizar que el Punto de Acceso no se sature con un número excesivo de estaciones conectadas.

En el campo **<Distance>**, seleccionamos la opción **<dynamic>**, para asegurar que el ACK de la comunicación entre origen y destino sea el menor posible.

- **Paso 5:** Rango de sensibilidad en el AP1

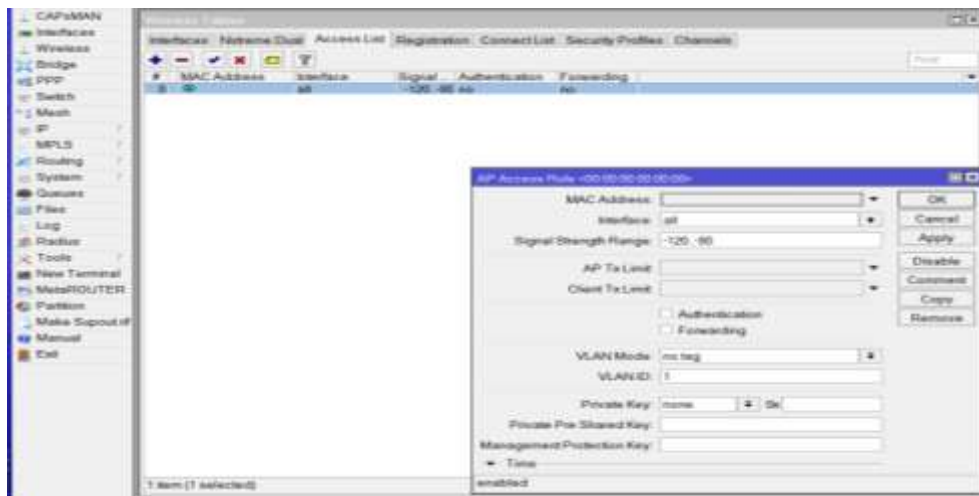


Figura 72. Rango de potencias permitido en el AP1 para estaciones registras  
Fuente: Propia

La figura anterior muestra el rango de potencias permitido en el AP1 para estaciones registras. Para evitar la degradación de los enlaces inalámbricos.

Una vez más en la interface wireless, en la ventana <Access List>, se agrega una nueva regla de control. En el campo <Interface>, seleccionamos <all>, y en campo <Signal Strength Range> agregamos lo siguiente <-120..-75>.

Se selecciona **all**, para que todas las interfaces entren en la nueva cola del **Access List**. Al ingresar el parámetro -12..-75 y dejar deshabilitado el botón de **Authentication**, se obliga a que el AP solo permita autenticar por defecto estaciones con niveles de señal menores a 75dBm, garantizando con esto que no se degrade la calidad del AP al tener estaciones con niveles muy altos de señal de recepción.

- **Paso 6:** Configuración del bridge

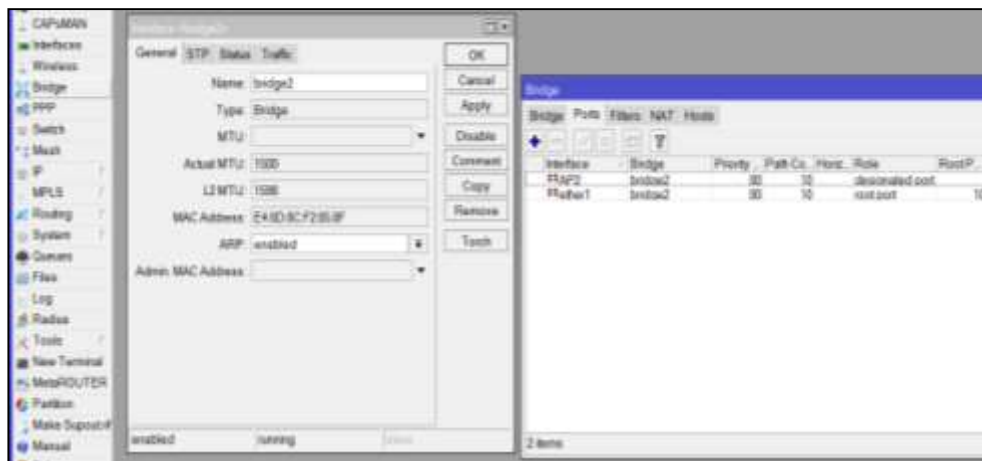


Figura 73. Bridge entre interfaces ether1 y wlan.  
Fuente: Propia

Una vez configurada la interface wireless, ahora se habilita el bridge que permita establecer la comunicación entre el puerto **ether1** del AP1, que está conectado al puerto uno de conmutación el RB1100AHx2 y la interface wireless llamada AP1.

Para esto se hace lo siguiente, desde la ventana principal de configuración se selecciona **<Bridge y nuevo Bridge>**, una vez dentro de interface bridge, se debe asignar un nombre a dicha interface. Siguiendo en la misma ventana en la pestaña **<Ports>** se agrega la interface wireless **AP1** y la interface **ethe1** al mismo Bridge, estableciendo de esta manera un puente entre dichas interfaces.

Desde el AP2 al AP15 se realizan las mismas configuraciones que se ha hecho para el AP1 en todos sus pasos. Únicamente cambia la frecuencia o canal asignado y el nombre del AP. Además, al final de la configuración de cada AP, se cambia el usuario y contraseña de administración de cada equipo RBcAP2n, para proteger seguridad de la información y garantizar un funcionamiento adecuado dentro de la red Wi-Fi.

### 3.3.4 Implementación del CAPsMAN

En la sección anterior los puntos de acceso llamados AP1, AP2..., Ap15, se hizo la configuración básica para cada uno, ahora mediante la implantación del CAPsMAN estos puntos de acceso, serán administrados mediante el servidor central.

La implementación del gestor CAPsMAN para el punto de acceso AP1 se detalla en los siguientes pasos:

- **Paso 1: Activación del CAP en la interface wireless del AP1**

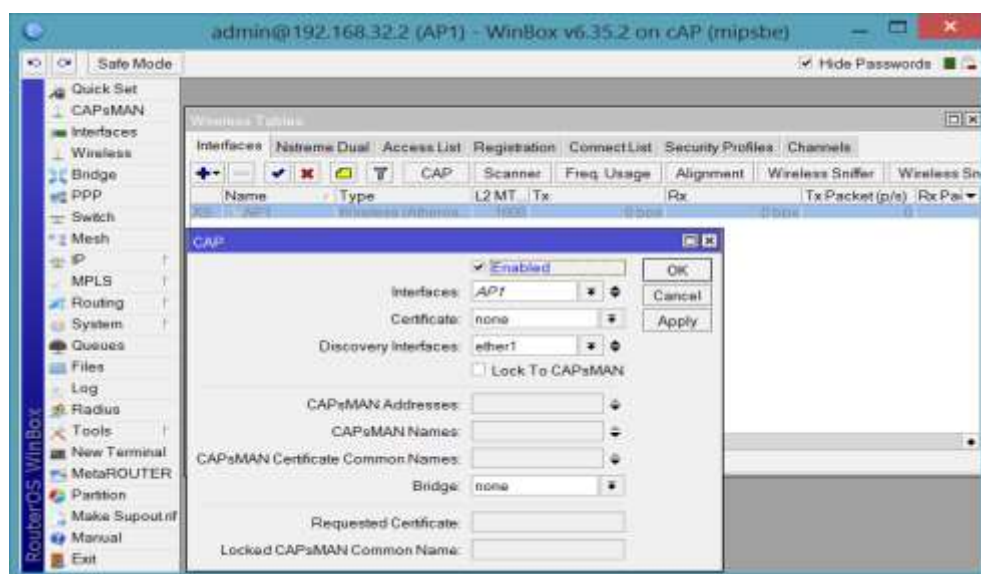


Figura 74. Activación del CAP en el AP1.

Fuente: Propia

La figura anterior permite evidenciar el proceso de convertir al punto de acceso AP1 en un CAP1, es decir ahora este será controlado remotamente y recibe parámetros de configuración desde el gestor central CAPsMAN, a continuación, se explica el proceso:

1. En la ventana de configuración principal del **AP1**, de debe dar clic en la pestaña **Wireless**, hacer clic en el botón **CAP**.

2. Una vez dentro, habilitar el botón **Enabled**, en el campo **Interfases** se escoge **AP1**, y a continuación habilitamos el descubriendo de interfaces y en los campos **Discovery Interfaces** se escoge **ether1**.
  3. Finalmente se guarden los cambios al hacer clic en **Apply** y **Ok**.
- **Paso 2: Activación de CAPsMAN en el equipo de gestión central el RB1100AHx2**

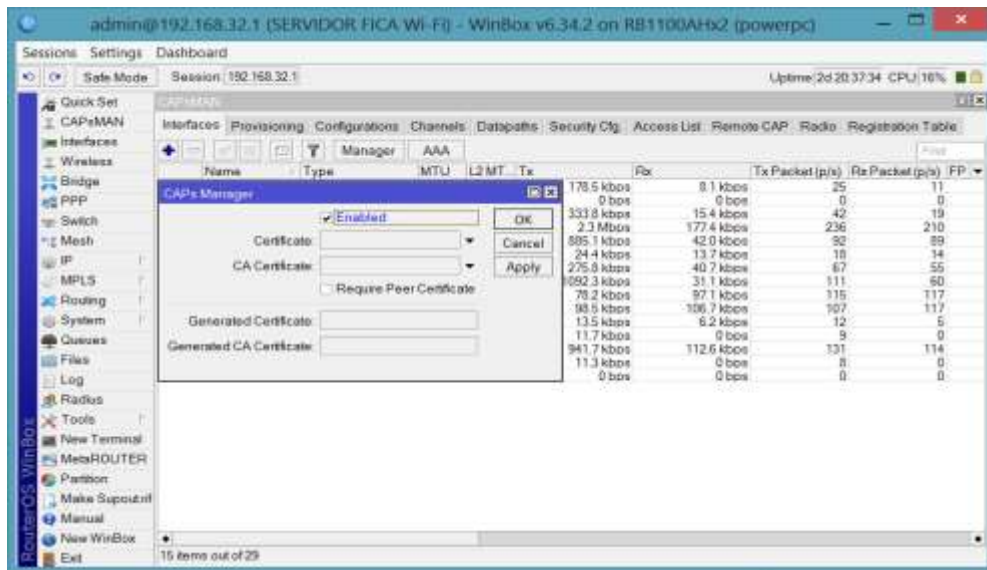


Figura 75. Activación del CAPsMAN en el equipo de gestión central.

A continuación, se activa el gestor CAPsMAN, en el RB1100AHx2 como se puede ver en la figura anterior y para lo cual se hace lo siguiente:

En la pantalla principal de configuración del RB1100AHx2, clic en el botón **CAPsMAN**, luego clic en el botón **Enabled**, finalmente presionamos **Apply** y **Ok** para se guarden los cambios.

El proceso de activación que hizo para que el punto de acceso AP1 se convierta en punto de acceso controlado (CAP) y lo repetimos para el AP2, hasta el AP15.

Una vez que cada punto de acceso ha sido convertido en un punto de acceso controlado (CAP), la interface wireless de cada AP se deshabilita y no permite realizar ninguna configuración de manera local, sino solo a través sistema gestion CAPsMAN.



Una vez terminada la activación de todos los puntos de acceso y la activación del gestor central CAPsMAN, ahora se debe establecer los perfiles de configuración que serán enviados desde el equipo gestor hacia cada uno de los CAPs ahora administrados de manera centralizada.

- **Paso 3: Agregación de los perfiles de configuración en el CAPsMAN para cada CAP**

Antes de crear los perfiles de configuración para cada CAP, primero se debe crear la lista de canales disponibles para esto se hace lo siguiente:

1. En la pantalla principal hacer clic en **CAPsMAN**, luego dentro, hacer clic en la pestaña **channels**. Seguido de esto se hace clic en el botón + para agregar un nuevo canal.
2. Una vez dentro la ventana, en el campo **Name** se escribe **channel1**, en **Frequency** se asigna **2412**, en **Width** se escoje **20Mhz**, en Band seleccione **2ghz-b/g/n**.
3. Finalmente, clic en **Apply** y **Ok** para guardar los cambios.
4. Igual como se creó el canal1 se repite el proceso hasta el canal11.

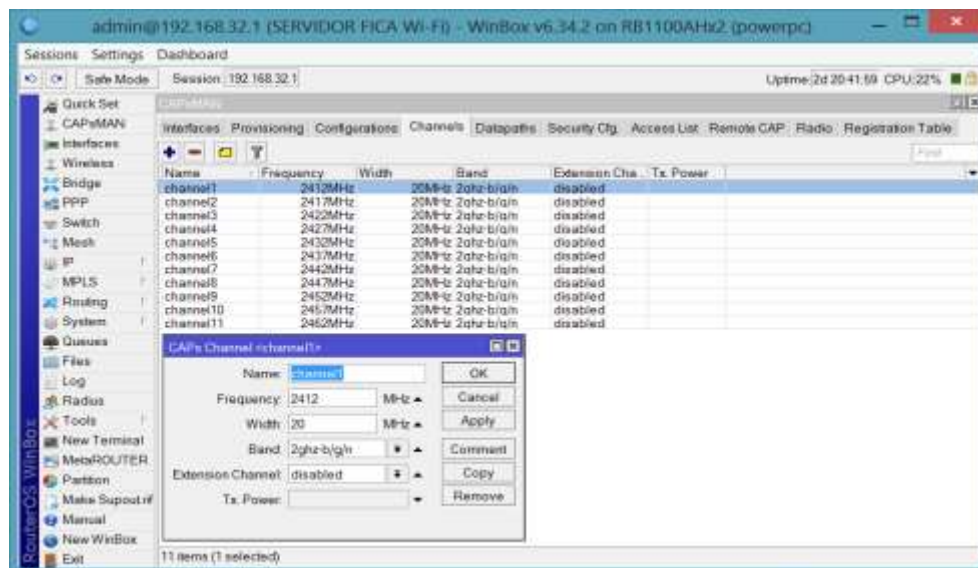


Figura 76. Asignación de canales en el CAPsMAN  
Fuente: Propia

La configuración y asignación de Canales puede ser entendida de mejor manera mediante la figura anterior.

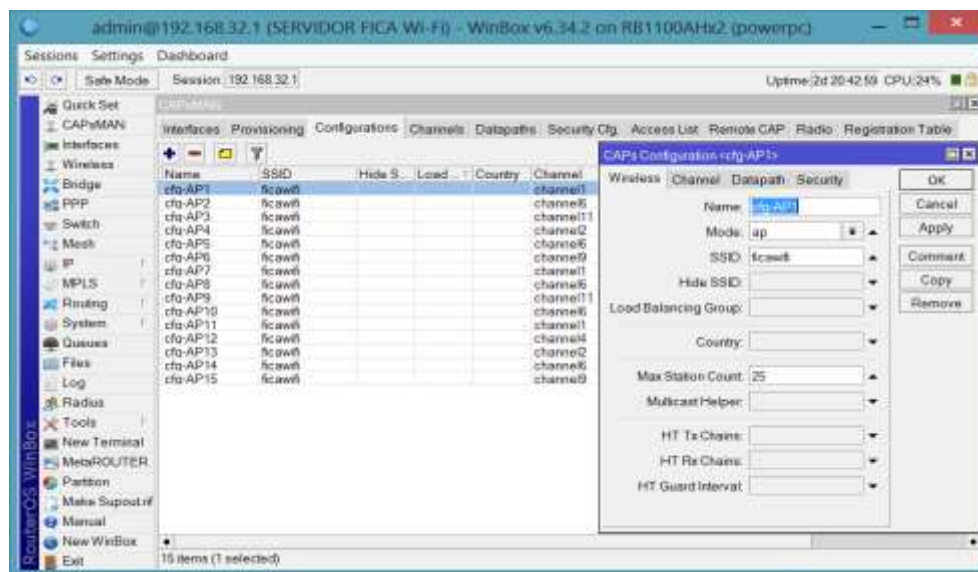


Figura 77. Agregación de perfiles de configuración  
Fuente: Propia

Una vez establecida la lista de canales estarán disponible, es momento de crearlos perfiles de configuración en el CAPsMAN, se debe agregar los perfiles de configuración para cada CAP, para que esto se procede de la siguiente manera:

1. Dentro de la pantalla principal de configuración, de CAPsMAN, escoger la pestaña **Configurations** y allí se hace clic en el botón +, para agregar un nuevo perfil de configuración.
2. Una vez dentro, en la pestaña **Wireless**, en **Name** se debe escribir **cfg-AP1**, para identificar el perfil de configuración correspondiente al AP1.
3. En el campo **Mode** se escoge **ap**, en **SSID** se escoge **ficawifi**, y en Max Station count ingrese **25**.

4. En la misma ventana de **Configurations**, se debe seleccionar la pestaña Channels, y ahí se asigna el **Channel1** al perfil de configuración **cfg-AP1**, con esto ya queda anexado el canal1 a su respectivo perfil de configuración.
  5. Finalmente se hace clic en **Apply** y **Ok**, para guardar los cambios.
- **Paso 4: Agregación del perfil de configuración al CAP1**

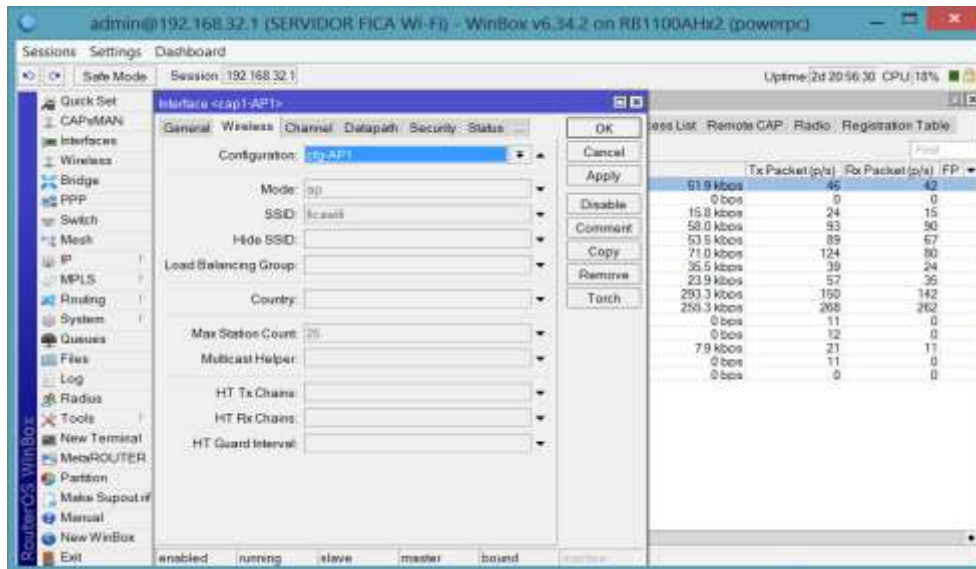


Figura 78. Visualización de los perfiles de configuración  
Fuente: Propia

Para terminar la configuración del CAPsMAN se necesita agregar los perfiles de configuración a cada punto de acceso ahora denominados CAPs, este proceso se puede ver en mediante la figura anterior y se lo hace de la siguiente manera:

1. En la ventana de configuración del **CAPsMAN**, se debe seleccionar la pestaña **Interfaces**, ahí en **Configuration** escoger **cfg-AP1**, se agrega el perfil previamente configurado a cada interface uno a uno según corresponde, es decir el perfil **cfg-AP1** a la interface **CAP1** y así sucesivamente hasta el **CAP15**.
2. Finalmente, clic en **Apply** y **Ok** para guardar los cambios efectuados.

### 3.3.5 Gestión y privilegios de usuarios

Para completar el sistema de gestión Wi-Fi centralizado, ahora se implementa la herramienta hotspot, la misma que permite facilitar la gestión de usuarios, asignación de privilegios, recursos y control de ancho de banda.

#### 3.3.5.1 Activación del servidor hotspot

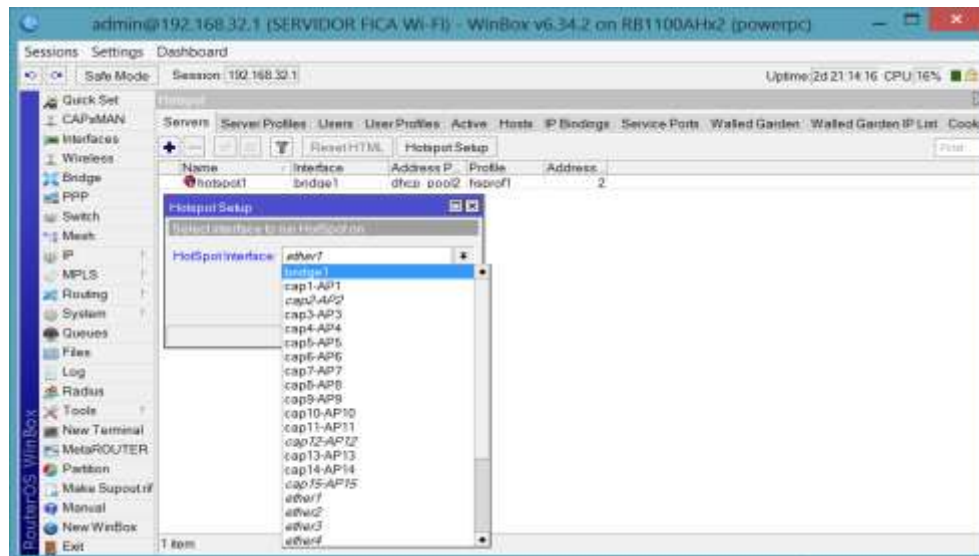


Figura 79. Implementación del hotspot

Fuente: Propia

En la ventana principal de configuración, clic en **IP**, seguido clic en **Hotspot**, luego en **Hotspot Setup**, se escoge la interface **bridge1**, se asigna la dirección IP 192.168.32.0/22, luego se establece el rango de IPs disponibles para navegación de usuarios, el mismo que va desde la IP 192.168.32.21 hasta la 192.168.35.254, luego se asigna el servidor DNS y finalmente el nombre del nuestro dominio el cual es **www.ficawifi.edu**.

Al ejecutar el asistente de Hotspot, este permite crear un usuario y la contraseña para que el administrador de la red pueda ingresar después que el hotspot entra en ejecución.

### 3.3.5.2 Configuración de los parámetros generales de hotspot

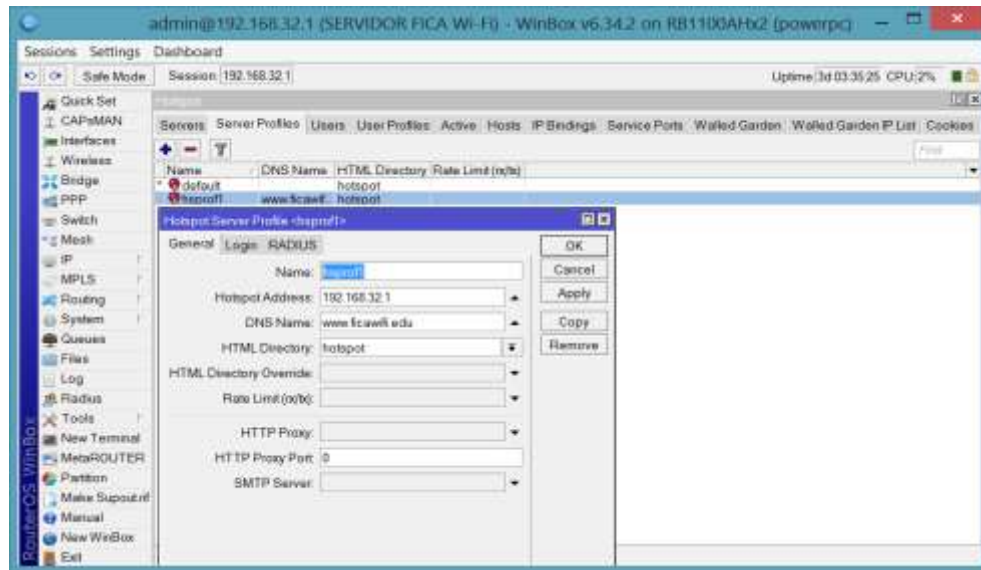


Figura 80. Configuración de parámetros generales del hotspot  
Fuente: Propia

En la ventana principal de configuración del hotspot, se debe seleccionar la pestaña **Server Profiles**, una vez dentro en la pestaña **General**, en el campo Name se escribe el nombre del Hotspot. Los datos de los campos **Hotspot Address**, **DNS Name** fueron creados en el momento que se activó el hotspot.

### 3.3.5.3 Configuración del método de autenticación al hotspot

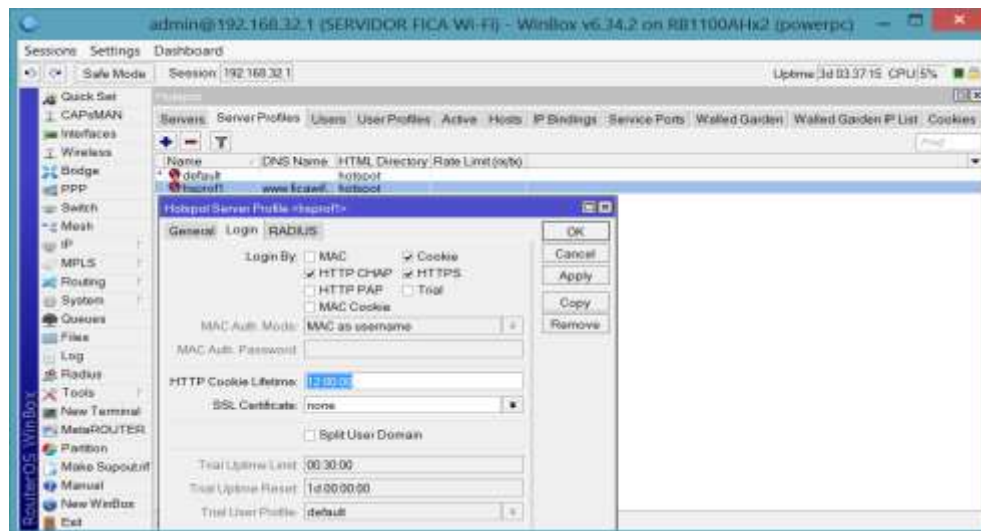


Figura 81. Configuración del método de autenticación al hotspot.

Fuente: Propia

La figura anterior permite visualizar el proceso de autenticación y logeo del servidor hotspot. En pestaña **Login** se deja habilitado **HTTP CHAP** como método de autenticación, **HTTPS** para ingresar a páginas con seguridad SSL, también se deja activado **Cookie**, para que se guarde las conexiones establecidas de cada usuario. El campo **HTTP Cookie Lifetime** seteado en 12 horas, establece el tiempo de vida que permanece al conexión activa en el usuario mediante el cookie.

Finalmente se hace clic en **Apply** y **Ok** para guardar los cambios efectuados.

### 3.3.5.4 Asignación de usuarios y privilegios mediante hotspot

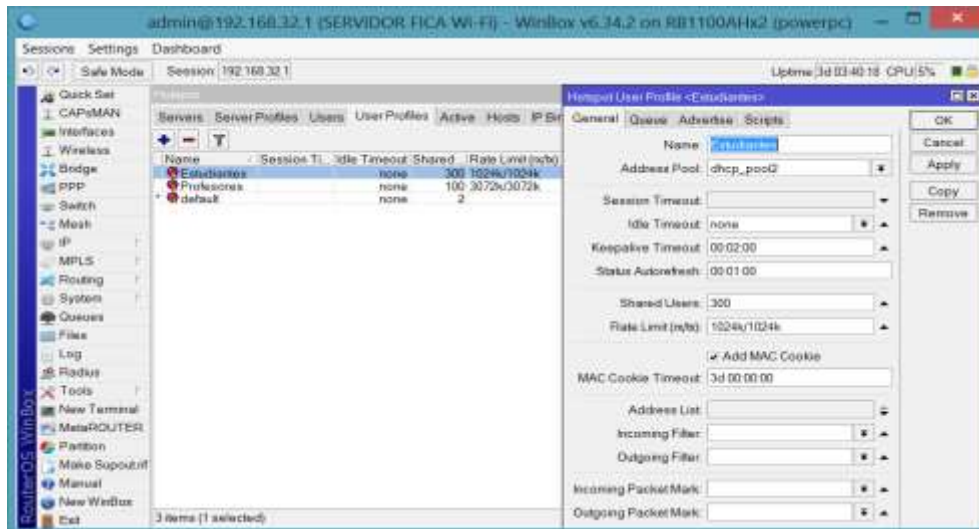


Figura 82. Creación de perfiles de usuario en el gestor hotspot  
Fuente: Propia

La figura anterior permite visualizar los perfiles de usuarios que se han creado, para estudiantes y para docentes, dejando reservado un total de 300 cuentas para estudiantes y 150 para profesores. Además, se asigna 3Mbps de ancho de banda para profesores y 1Mbps para cada estudiante registrado.

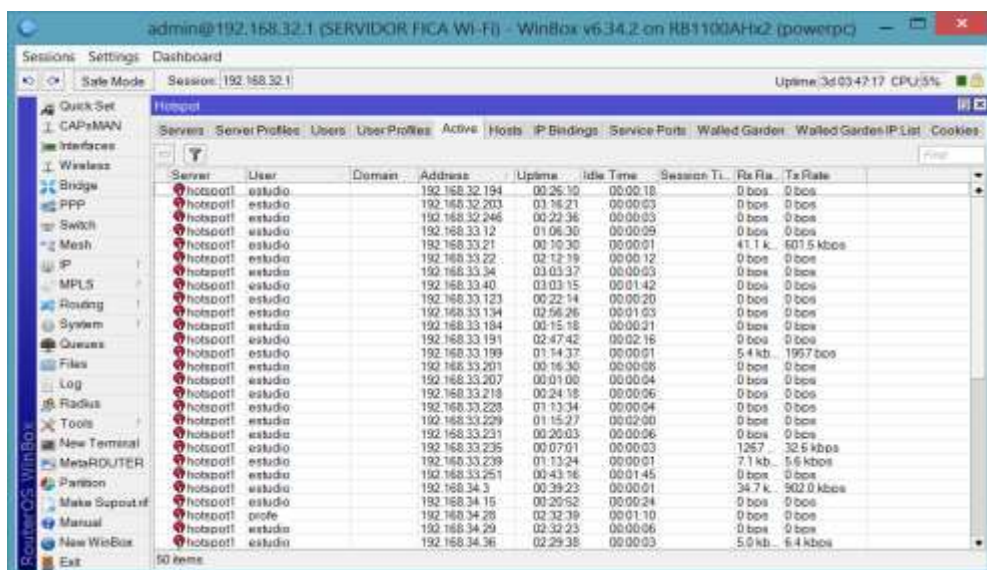


Figura 83. Usuarios autenticados a través del hotspot  
Fuente: Propia

Una vez que el usuario ha obtenido el usuario y password, este puede ya puede acceder a los recursos de la red Wi-Fi, ya sean estos locales o externos. Los usuarios que ya sido registrados se agrupan en la lista de usuarios activos, tal como se puede ver en la anterior figura.

### 3.3.6 Pruebas de funcionamiento nueva red WiFi

Para determinar el rendimiento de la red Wi-Fi implementada en la Facultad de Ingeniería en Ciencias Aplicadas (FICA), se realizó varias pruebas de funcionamiento, entre las más importantes tenemos, prueba de velocidad con diferentes con herramientas de la web, prueba de visualización de videos en diferentes formatos de calidad, envío de paquetes ICMP mediante la herramienta ping, descarga de contenidos, y trazado de rutas.

Datos tomados 19/01/2016 a 11:40 am

#### 3.3.6.1 Prueba de funcionamiento con herramientas de la web



Figura 84. Test de velocidad con la herramienta speedof.me.  
Fuente: Propia

Como primera herramienta de medición de rendimiento se utiliza la prueba de velocidad con la herramienta speedof.me, tal como se ve en la figura anterior. La medición indica que la



latencia máxima del sistema es 81ms, velocidad de descarga 4.27Mbps y velocidad de carga 3.73Mbps.

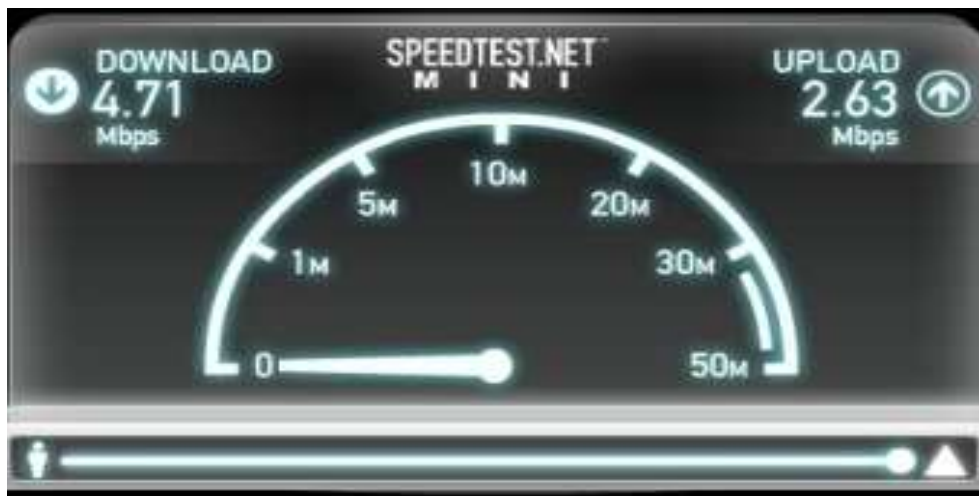


Figura 85. Test de velocidad con herramienta de AEPROVI.  
Fuente: Propia

Para obtener información desde otra fuente, se hace prueba la velocidad con la herramienta de AEPROVI, se obtiene 4,71Mbps de descarga y 2.63Mbps de carga. La velocidad de descarga es muy similar a la realizada con speeddof.me, pero la velocidad de carga es al menos 1Mbps menor.



Figura 86. Test de velocidad con herramienta de speedtest.  
Fuente: Propia

La tercera prueba de velocidad se hace con speedtest, esta medición se la hace desde el host local hasta host ubicado en Boca Ratón - Florida, a pesar de la distancia y que el número de saltos es mucho mayor, la latencia del sistema es 70ms, velocidad de descarga 11.99Mbps y velocidad de carga 7.67Mbps.

Tabla 17. Prueba de velocidad con herramientas web para la nueva red

Herramienta/Detalle	Descarga	Carga	Latencia
SPEDOF.ME	4.27 kbps	3.73 kbps	81 ms
AEPROVI	4.71 Mbps	2.63 Mbps	76 ms
SPEEDTEST	11.9 Mbps	7.67 Mbps	70 ms

Fuente: Propia.

Haciendo un análisis comparativo entre las tres herramientas utilizadas con sus respectivos resultados y las pruebas que se obtuvo en la red existente que funcionaba antes de iniciar el proyecto, se puede determinar claramente que la eficiencia de la red Wi-Fi que se ha instalada es al menos 5 veces más rápida.

### 3.3.6.2 Prueba de con la herramienta ping

```

Símbolo del sistema
Respuesta desde 192.168.32.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=12ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=45ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=9ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=17ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=10ms TTL=64
Respuesta desde 192.168.32.1: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.32.1:
    Paquetes: enviados = 31, recibidos = 31, perdidos = 0
              (0% perdidos)
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 8ms, Máximo = 147ms, Media = 13ms
Control-C
^C
C:\Users\Soporte técnico>

```

Figura 87. Estadística de paquetes ICMP con la herramienta ping de Windows.

Fuente: Propia

Continuando con las pruebas de funcionamiento, se envían paquetes ICMP con la ayuda de la herramienta ping para diagnosticar el estado de la comunicación desde el host local hacia la red de acceso.

*Tabla 18. Prueba de envío y recepción de paquetes ICMP para la nueva red*

	Enviados	Recibidos	Perdidos
Paquetes	31	31	0
	Mínimo	Máximo	Media
Tiempos (Latencia)	0 ms	174 ms	13 ms

*Fuente: Propia*

Como se puede ver en la figura anterior, del total de 31 paquetes enviados 31 paquetes son recibidos, teniendo 0 % de paquetes perdidos. Tiempo mínimo 0ms, tiempo máximo 147ms y tiempo promedio 13ms.

Esta información permite determinar la eficiencia en la red Wi-Fi, me indica que la latencia en la red de acceso y red de transporte es la adecuada para que la comunicación sea fluida desde y hacia los usuarios finales.

### 3.3.6.3 Prueba de reproducción de un video en 360p



Figura 88. Reproducción de un Video a 360p.  
Fuente: Propia

### 3.3.6.4 Prueba de reproducción de un video en 480p



Figura 89. Reproducción de un Video a 480p.  
Fuente: Propia

Para diagnosticar el rendimiento de la red Wi-Fi se agrega una prueba más, la visualización de videos en varios formatos 360p, 480p y 720p. Esta prueba en tiempo real hace que el canal de trasmisión se sature debido a la cantidad de información que se transfiere simultáneamente, al reproducir el video.

La variedad de formatos permite medir la fiabilidad del sistema, la descarga y visualización de los videos es muy fluida, incluso en el video HD a 720p, esto indica que la capacidad de trasmisión del sistema es bastante aceptable para el usuario final.

### 3.3.6.5 Prueba de reproducción de un video en HD (720p)

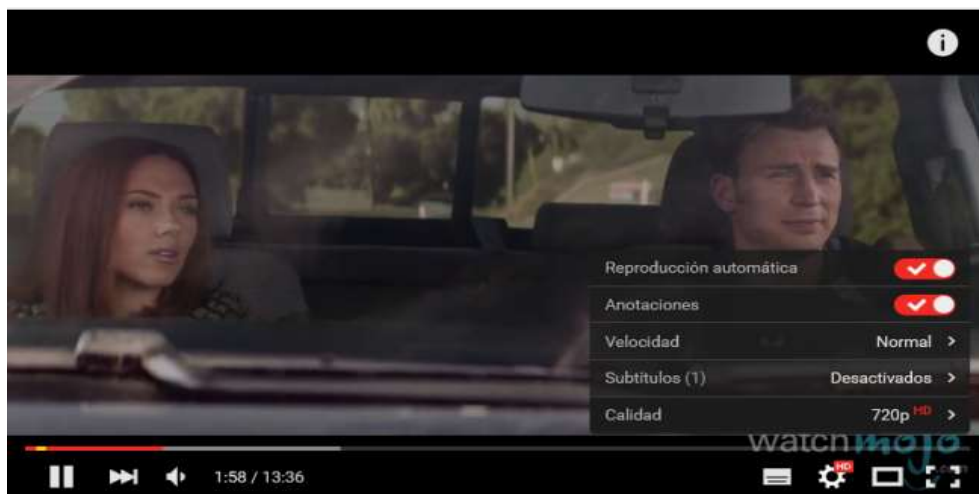


Figura 90. Reproducción de un Video HD a 720p.  
Fuente: Propia.

Un video en HD 720p necesita aproximadamente 3Mbps de capacidad en el canal de trasmisión para que la reproducción sea fluida, esto indica que la red de acceso Wi-Fi garantiza la trasmisión desde y hacia la red externa.

### 3.3.6.6 Prueba de descarga de un paquete de datos de 372 MB



Figura 91. Prueba de descarga de un archivo  
Fuente: Propia

Al final del conjunto de pruebas, se realiza una descarga de un archivo de 372MB alojado en un host remoto de red externa, mostrado en la figura anterior, donde la descarga media es de 1MB/seg. Siendo el MB/seg la unidad estándar de descarga de un archivo desde la web, es necesario hacer la conversión a Mbps para determinar la velocidad máxima de transmisión. 1MB/seg equivale a 8Mb/seg, lo que finalmente permite concluir que la capacidad de transmisión de la red Wi-Fi brinda las mejores prestaciones a las estaciones que demanden por acceso contenidos y sitios web.

## CAPITULO IV

### 4 Análisis de resultados

#### 4.1 Calidad del servicio a nivel de usuarios finales

Para cumplir con el resultado esperado mediante la implementación del nuevo sistema de gestión Wi-Fi es necesario evidenciar el proceso de pruebas a nivel de usuarios finales Estudiantes y Docentes, para quienes se establece las historias de usuario y pruebas de aceptación respectivamente.

##### 4.1.1 Historias de usuario

Se muestra la historia de usuario con rol Docente

*Tabla 19. Historia de un usuario docente*

Historia 1	
<b>Nombre de la historia</b>	Docente
<b>Fecha</b>	15 de abril del 2016
<b>Usuario</b>	Sandra Narváez
<b>Prioridad</b>	Alta
<b>Nivel de iteración</b>	1
<b>Responsable</b>	Jherman López
<b>Riesgo</b>	Conexión de red fallida
<b>Descripción</b>	El docente manifestó que para lograr el éxito en el proceso de gestión del wifi debe redirigirse a la página de login en cuanto se ejecute la conexión y los pasos para hacerlo no deben ser complejos.

*Fuente: Propia*

Se muestra la historia de otro usuario con rol Docente

*Tabla 20. Historia de un usuario docente*

<b>Historia 2</b>	
<b>Nombre de la historia</b>	Docente
<b>Fecha</b>	15 de abril del 2016
<b>Usuario</b>	Stefany Flores
<b>Prioridad</b>	Alta
<b>Nivel de iteración</b>	2
<b>Responsable</b>	Jherman López
<b>Riesgo</b>	Conexión de red fallida
<b>Descripción</b>	El docente pidió que la conexión no sea compleja y que la velocidad de red debe ser estable para poder realizar carga y descarga de información.

*Fuente: Propia*



Se muestra la historia de usuario con rol Administrador

*Tabla 21. Historia de un usuario estudiante*

<b>Historia 3</b>	
<b>Nombre de la historia</b>	Estudiante
<b>Fecha</b>	15 de abril del 2016
<b>Usuario</b>	Cristian Freire
<b>Prioridad</b>	Alta
<b>Nivel de iteración</b>	3
<b>Responsable</b>	Jherman López
<b>Riesgo</b>	Conexión de red fallida
<b>Descripción</b>	<p>El estudiante manifestó que espera una excelente calidad en la transmisión de datos, carga y descarga de archivos y visualización de videos.</p>

*Fuente: Propia*

### 4.1.2 Pruebas de aceptación

La siguiente tabla muestra el caso de prueba para la navegación web utilizando el rol de docente.

Tabla 22. Caso de prueba para la navegación web con rol docente

<b>Prueba de aceptación</b>			
<b>Caso de Prueba</b>	Test de la red FICA	Rol de usuario	Docente
<b>Nro. Caso de prueba</b>	1	Nro. De historia de usuario	1
<b>Descripción</b>	Navegación web		
<b>Condiciones de ejecución</b>	<ul style="list-style-type: none"> <li>• El usuario debe tener las credenciales para inicio de sesión en la red.</li> <li>• El usuario debe estar en el rango de conexión.</li> <li>• El usuario debe tener acceso a internet</li> </ul>		
<b>Datos de entrada</b>	<ul style="list-style-type: none"> <li>• Usuario: Indica el nombre de usuario otorgado según su función en la facultad (Docente).</li> <li>• Contraseña: Frase de acceso otorgada para el usuario (Docente).</li> </ul>		
<b>Pasos de ejecución</b>	<ol style="list-style-type: none"> <li>1. Se conecta a la red libre ficawifi</li> <li>2. Ingresa los datos de usuario y contraseña</li> <li>3. Navega en internet</li> </ol>		
<b>Resultado esperado</b>	Se conecta a la red ficawifi		SI
	Todos los datos a ingresar son validados.		SI
	Navega en internet		SI
<b>Evaluación</b>	Satisfactorio		

Fuente: Propia

La siguiente tabla muestra el caso de prueba para la carga y descarga de información utilizando el rol de docente.

Tabla 23. caso de prueba para la carga y descarga de información rol docente

<b>Prueba de aceptación</b>			
<b>Caso de Prueba</b>	Test de la red FICA	Rol de usuario	Docente
<b>Nro. Caso de prueba</b>	2	Nro. De historia de usuario	2
<b>Descripción</b>	Carga y descarga de información		
<b>Condiciones de ejecución</b>	<ul style="list-style-type: none"> <li>• El usuario debe tener las credenciales para inicio de sesión en la red.</li> <li>• El usuario debe estar en el rango de conexión.</li> <li>• El usuario debe tener acceso a internet</li> </ul>		
<b>Datos de entrada</b>	<ul style="list-style-type: none"> <li>• Usuario: Indica el nombre de usuario otorgado según su función en la facultad (Docente).</li> <li>• Contraseña: Frase de acceso otorgada para el usuario (Docente).</li> </ul>		
<b>Pasos de ejecución</b>	<ol style="list-style-type: none"> <li>1. Se conecta a la red libre ficawifi</li> <li>2. Ingresa los datos de usuario y contraseña</li> <li>3. Navega en internet</li> <li>4. Realiza la carga de información o archivos</li> <li>5. Realiza la descarga de información o archivos</li> </ol>		
<b>Resultado esperado</b>	Se conecta a la red ficawifi		SI
	Todos los datos a ingresar son validados.		SI
	Navega en internet		SI
	Carga información o archivos		SI
	Descarga información o archivos		SI
<b>Evaluación</b>	Satisfactorio		

Fuente: Propia

La siguiente tabla muestra el caso de visualización de videos utilizando el rol de estudiante.

Tabla 24. caso de visualización de videos rol estudiante

<b>Prueba de aceptación</b>			
<b>Caso de Prueba</b>	Test de la red FICA	Rol de usuario	Docente
<b>Nro. Caso de prueba</b>	3	Nro. De historia de usuario	3
<b>Descripción</b>	Visualización de videos		
<b>Condiciones de ejecución</b>	<ul style="list-style-type: none"> <li>• El usuario debe tener las credenciales para inicio de sesión en la red.</li> <li>• El usuario debe estar en el rango de conexión.</li> <li>• El usuario debe tener acceso a internet</li> </ul>		
<b>Datos de entrada</b>	<ul style="list-style-type: none"> <li>• Usuario: Indica el nombre de usuario otorgado según su función en la facultad (Estudiante).</li> <li>• Contraseña: Frase de acceso otorgada para el usuario (Estudiante).</li> </ul>		
<b>Pasos de ejecución</b>	<ol style="list-style-type: none"> <li>1. Se conecta a la red libre ficawifi</li> <li>2. Ingresa los datos de usuario y contraseña</li> <li>3. Navega en internet</li> <li>4. Realiza la carga de información o archivos</li> <li>5. Realiza la descarga de información o archivos</li> <li>6. Visualiza videos</li> </ol>		
<b>Resultado esperado</b>	Se conecta a la red ficawifi		SI
	Todos los datos a ingresar son validados.		SI
	Navega en internet		SI
	Carga información o archivos		SI
	Descarga información o archivos		SI
	Visualiza videos		SI
<b>Evaluación</b>	Satisfactorio		

Fuente: Propia

El análisis de las pruebas de aceptación permiten evidenciar que el sistema de gestión Wi-Fi centralizado, en la Facultad de Ingeniería en Ciencias Aplicadas, ha mejorado su calidad de servicio a nivel de usuarios finales dando satisfacción a los requerimientos planteados.

## CAPÍTULO V

### 5 Conclusiones y recomendaciones

#### 5.1 Conclusiones

- Luego de analizar la situación actual de la FICA se determinó que el sistema de red Wi-Fi que funcionaba previo al desarrollo del presente proyecto y tenía un mal diseño en la interconexión de los puntos de acceso a través de todo el edificio. Debido a que estos eran conectados indistintamente en cualquier punto de red inmediato, a pesar de que la geografía del edificio facilitaba hacer centralización de los APs, en base a una topología de red tipo estrella.
- Se recopiló información del departamento de sistemas y fue de mucha importancia, y gracias a eso se pudo determinar las causas específicas que provocaban la degradación de la red Wi-Fi.
- El diseño de red de acceso inalámbrica fue la parte más importante en el funcionamiento de todo el sistema implementado. Porque se logró establecer las políticas para cada punto de acceso y esto finalmente determinó el rendimiento y disponibilidad de la red Wi-Fi en su totalidad.
- La implementación de la red Wi-Fi tuvo algunas variantes, sobre todo en el cableado estructurado, debido al re ubicación del cuarto de equipos que hizo dentro de la FICA.
- La selección de la marca y las prestaciones que brindan los equipos a utilizarse es muy determinante en la solución final implementada. Ya que en nuestro caso. Mikrotik es una marca de costos accesibles, pero con muy altas prestaciones en cuanto a su rendimiento. Además, la administración de estos equipos es muy amigable con el usuario.
- El rendimiento de cada punto de acceso está directamente relacionado a la calidad de las estaciones registradas en el mismo, es decir si un AP tiene varias estaciones registradas

con señales de entre -90 y -60 dBm, la estación de menor señal hará que se degrade la calidad de todo el AP, incluyendo las estaciones con mejores parámetros de conexión.

- Se realizó pruebas de aceptación con evaluando las acciones de usuarios reales obteniendo resultados satisfactorios, también se realizó pruebas técnicas a la red para determinar que la calidad del servicio sería la ideal para las pruebas con los usuarios reales.

## **5.2 Recomendaciones**

- Siempre que se implemente una red mixta como es el caso del presente proyecto realizado, se recomienda certificar el cableado estructurado para evitar la degradación del sistema en algún segmento de red por el uso de cables defectuosos.
- Implementar una base de datos que permita llevar un registro de usuarios, contraseñas y asignación de recursos que funcione paralelo a la red de acceso Wi-Fi implementada para mejorar la administración de usuarios dentro de la red.
- Se recomienda crear zonas Wi-Fi de alta velocidad en donde las características de funcionamiento de la red tanto para el Punto de Acceso como para la Estación son totalmente personalizadas en base a estándares inalámbricos de alto rendimiento como, IEEE 802.11n y IEEE 802.11ac. En esta zona solo serán permitidas estaciones que cumplan con las características técnicas de interoperabilidad con la red de acceso disponible.
- Al estar transmitiendo en banda no licenciada dentro de la Facultad existe muchas redes que provocan interferencia a la red Wi-Fi implementada, por tal razón se recomienda establecer una campaña de control para suprimir todas aquellas redes que no sean necesarias.

## Glosario de Términos

**IEEE 802.16.** Especificaciones para redes inalámbricas de acceso metropolitano, de banda ancha fijas.

**WIMAX.** Conocida como tecnología de última milla, que transmite de datos mediante ondas de radio en las frecuencias de 2,5 a 5,8 GHz.

**802.11.** Define el uso de los dos niveles inferiores del modelo OSI, capa física y capa de enlace de datos.

**CSMA/CD.** Acceso Múltiple con escucha de portadora y detección de colisiones, es un protocolo de acceso al medio compartido que evita colisiones.

**ISM (INDUSTRIAL, SCIENTIFIC AND MEDICAL).** Son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica.

**DBI.** Relación logarítmica entre la potencia de emisión de una antena en relación a un radiador isotrópico.

**DBM.** Unidad de medida de potencia expresada en decibelios (dB) relativa a un mili vatio (mW).

**ETSI.** European Telecommunications Standards Institute. Organización europea de estandarización independiente sin fines de lucro.

**OFDM.** Orthogonal Frequency-Division Multiplexing. Acceso múltiple por división de frecuencias ortogonales. Técnica que se basa en la multiplexación por división de frecuencias equiespaciadas. Fuente: (Codejobs, 2014)

**UDP.** User Datagram Protocol. Protocolo no orientado a conexión del nivel de transporte basado en el intercambio de datagramas. Fuente: (Kioskea, 2014)

**CCK.** Provee un mecanismo para incrementar la eficiencia de ancho de banda en un sistema de espectro extendido.

**DSSS.** es una técnica de codificación que utiliza un código de pseudoruido para "modular" digitalmente una portadora, de tal forma que aumente el ancho de banda de la transmisión y reduzca la densidad de potencia espectral.

**QUADRATURE AMPLITUDE MODULATION.** Modulación de amplitud en cuadratura es una técnica que transporta dos señales independientes mediante la modulación de una señal portadora.

**GNS3.** Es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos.

**BSS.** Es un modo de red inalámbrica, también denominado modo infraestructura. En esta configuración se conectan un determinado número de puntos de acceso a una red cableada.

**SSID.** Nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. A menudo al SSID se le conoce como "nombre de la red".

**WISP.** Es un proveedor de Servicio de Internet Inalámbrico.

**ROUTERBOARD.** son miniCPU con avanzadas prestaciones para redes de datos.

**JITTER.** Variabilidad temporal durante el envío de señales digitales. Suele considerarse una señal de ruido no deseada que provoca un cambio abrupto e indeseado de la amplitud, frecuencia o fase de la señal.

**FIFO.** Primero en entrar, primero en salir (First In First Out) es un concepto utilizado en estructura de datos y teoría de colas.

**SPEDOFME.** Herramienta para pruebas de velocidad de internet.

**AEPROVI.** Asociación de empresas proveedoras de internet, valor agregado, portadores y tecnólogas de la información.

**ICMP.** Protocolo de mensajes de control de Internet. Permite administrar información relacionada con errores de los equipos en red. Fuente: (Kioskea, 2014).



**INDOOR.** Término usado en equipos de transmisión inalámbrica usados en interiores de hogares, hoteles, centros comerciales, etc.

**POE.** Permite la transmisión de electricidad y datos a través de cable UTP/STP.

**TDMA.** Es una tecnología inalámbrica de segunda generación, que distribuye las unidades de información en ranuras alternas de tiempo. Fuente: (Alegsa, 2010)

**MAC.** Identificador único asignado por el fabricante a una pieza de hardware de red.

**DSSS/CCK.** Direct Sequence Spread-Spectrum Complementary Code Keying (Codificación de código complementario de espectro de dispersión de secuencia directa).

## Bibliografía

- Alegsa, L. (12 de Diciembre de 2010). *www.alegsa.com.ar*. Obtenido de Definición de TDMA:  
<http://www.alegsa.com.ar/Dic/tdma.php>
- Araujo, G., Camacho, L., & Vera, J. (2011). *Redes inalámbricas para zonas rurales*. Lima, Perú. Obtenido de <http://gtr.telecom.pucp.edu.pe/system/files/1041.pdf>
- Ariganello, E., & Barrientos Savilla, E. (2010). *Redes Cisco*. México D.F.: Alfaomega Grupo Editor, S.A.
- Asamblea Constituyente del Ecuador. (2008). *Constitucion de la Republica del Ecuador*. Alfaro, Manabí, Ecuador.
- Bear Extender. (2014). <https://store.bearextender.com>. Obtenido de What is High Speed 802.11ac Wi-Fi?: <https://store.bearextender.com/pages/802-11ac>
- Belt. (15 de Enero de 2016). *www.belt.es*. Obtenido de Seguridad de la Información y Protección de Datos.: [http://www.belt.es/noticiasmdb/HOME2\\_notaprensa.asp?id=10043](http://www.belt.es/noticiasmdb/HOME2_notaprensa.asp?id=10043)
- Butler, J., Pietrosemoli, E., Zennaro, M., & Fonda, C. (Octubre de 2013). Obtenido de Redes inalámbricas en los países en desarrollo: <http://wndw.net/pdf/wndw3-es/wndw3-es-ebook.pdf>
- Cabeza, A. (11 de Noviembre de 2009). *Slideshare*. Obtenido de Tecnología de redes inalámbricas: [https://es.slideshare.net/amparocabeza/redes-inalambricas-2475196?qid=385509c4-523a-4f63-94a1-3ceef3f4766c&v=qf1&b=&from\\_search=2](https://es.slideshare.net/amparocabeza/redes-inalambricas-2475196?qid=385509c4-523a-4f63-94a1-3ceef3f4766c&v=qf1&b=&from_search=2)
- Codejobs. (16 de Febrero de 2014). *www.codejobs.biz*. Obtenido de ¿Qué es OFDM? - Telecomunicaciones: <https://www.codejobs.biz/es/blog/2014/02/16/que-es-ofdm-telecomunicaciones>
- Conatel. (2011). *Plan nacional de frecuencias*.

- Condor Comunicaciones. (30 de Abril de 2013). *www.condor.com.ni*. Obtenido de UniFi – Redes WiFi administrables: <http://www.condor.com.ni/blog/2013/04/30/unifi-redes-wifi-administrables/>
- Conectrónica. (10 de Junio de 2015). *www.conelectronica.com*. Obtenido de Software gratuito Central WiFi Manager para administrar redes inalámbricas de forma centralizada: <http://www.conelectronica.com/wireless/redes-wireless/software-gratuito-central-wifi-manager-para-administrar-redes-inalambricas-de-forma-centralizada>
- Correa, C., Godoy, R., Grote, W., & Orellana, M. (2005). Evaluación de enlaces inalámbricos urbanos usando protocolo IEEE 802.11 b. *Revista Facultad de Ingeniería-Universidad de Tarapacá*.
- DATA ALLIANCE. (2016). *www.data-alliance.net*. Obtenido de Omni-Directional Antennas: Dipole / Rubber Duck: <https://www.data-alliance.net/omni-directional-antennas-dipole/>
- De Luz, S. (29 de Marzo de 2012). <https://www.redeszone.net>. Obtenido de 802.11ac : Todo lo que debes saber sobre el nuevo estándar Wi-Fi - See more at: <https://www.redeszone.net/2012/03/29/802-11ac-todo-lo-que-debes-saber-sobre-el-nuevo-estandar-wi-fi/#sthash.e2CrTA2n.dpuf>: <https://www.redeszone.net/2012/03/29/802-11ac-todo-lo-que-debes-saber-sobre-el-nuevo-estandar-wi-fi/>
- Grote, W., Ávila, C., & Molina, A. (2007). Análisis de máximo desempeño para WLAN operando a tasas fijas o adaptivas usando el estándar IEEE 802.11 a/b/g. *Ingeniare. Revista chilena de ingeniería*.
- Hall, D. A. (20 de Mayo de 2009). *Microwaves & RF*. Obtenido de Understanding Benefits Of MIMO Technology: <http://mwrf.com/markets/understanding-benefits-mimo-technology>

Hometech. (2016). <http://www.hometechcolombia.com>. Obtenido de ¿Cómo diseñar una red wifi?: <http://www.hometechcolombia.com/boletines/PDF/DisenarRedWiFi.pdf>

HWAGM Seguridad Wireless. (2016). <http://hwagm.elhacker.net>. Obtenido de ¿Como se calcula el alcance en una conexión wireless?: <http://hwagm.elhacker.net/calculo/calcularalcance.htm>

Joskowicz, J. (03 de Febrero de 2009). *es.slideshare.net*. Obtenido de Redes de datos: <https://es.slideshare.net/guest8c095/presentacion-redes-984189>

Kioskea. (Junio de 2014). *es.kioskea.net*. Obtenido de Redes inalámbricas: <http://es.ccm.net/contents/818-redes-inalambricas>

Kioskea. (Junio de 2014). *es.kioskea.net*. Obtenido de Protocolo UDP: <http://es.ccm.net/contents/284-protocolo-udp>

Kioskea. (Junio de 2014). *es.kioskea.net*. Obtenido de El protocolo ICMP: <http://es.ccm.net/contents/265-el-protocolo-icmp>

Kleinrock, L. (Agosto de 2011). *es.slideshare.net*. Obtenido de Redes inalámbricas: [https://es.slideshare.net/ernestoespinozaramos/redes-inalambricas-2c2011?qid=5cb0fdb26e6-4e95-8805-8e398a1e4713&v=default&b=&from\\_search=19](https://es.slideshare.net/ernestoespinozaramos/redes-inalambricas-2c2011?qid=5cb0fdb26e6-4e95-8805-8e398a1e4713&v=default&b=&from_search=19)

L. Marcelo. (2009). *Redes Wireless–Tecnología MIMO–Análisis y performance de Estandar de Comunicaciones Inalambricas 802.11 n*. Buenos Aires, Argentina.

López Barnés, R. (Marzo de 2008). Red basada en acceso inalámbrico (WiFi & WiMAX).

Meden Peralta, J. A. (2013). *IEEE 802.11ac*. Asunción.

Mikrotik. (2010). Obtenido de Mikrotik RouterOS: [https://www.mikrotik.com/download/pdf/what\\_is\\_routeros.pdf](https://www.mikrotik.com/download/pdf/what_is_routeros.pdf)

Mikrotik. (Abril de 2015). *wiki.mikrotik.com*. Obtenido de Manual:CAPsMAN: <https://wiki.mikrotik.com/wiki/Manual:CAPsMAN>

- Mikrotik. (Febrero de 2015). *wiki.mikrotik.com*. Obtenido de Manual:IP/Hotspot:  
<https://wiki.mikrotik.com/wiki/Manual:IP/Hotspot>
- Oliva, P. (2005). *IEEE 802.11 n Next Generation WiFi*. 3er Seminario Mataró Wireless, España.
- Ortega Gallegos, D. (15 de Noviembre de 2012). *Slideshare*. Obtenido de Conceptos fundamentales de telecomunicaciones: <https://es.slideshare.net/davidortegag/capitulo-02-conceptos-fundamentales>
- Paz, M. A. (15 de Marzo de 2012). *Slideshare*. Obtenido de WLAN (Wireless Local Area Network): [https://es.slideshare.net/malepaz14/wlan-wireless?qid=8140059a-7e0d-463e-b9ab-f801158f1b13&v=qf1&b=&from\\_search=10](https://es.slideshare.net/malepaz14/wlan-wireless?qid=8140059a-7e0d-463e-b9ab-f801158f1b13&v=qf1&b=&from_search=10)
- Pugliese, F. (2014). Introducción a MikroTik. *Taller de Redes inalámbricas*. Obtenido de Introducción a Mikrotik:  
[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj0zd3u3L\\_TAhVDOiYKHTwPBsMQFggkMAA&url=http%3A%2F%2Feva.universidad.edu.uy%2Fmod%2Fresource%2Fview.php%3Fid%3D197479&usg=AFQjCNEM3uaZcJwV\\_5yJS0S7IIXHy86j4A&sig2=\\_vdwus-Gx7a1AzgVqvi\\_](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj0zd3u3L_TAhVDOiYKHTwPBsMQFggkMAA&url=http%3A%2F%2Feva.universidad.edu.uy%2Fmod%2Fresource%2Fview.php%3Fid%3D197479&usg=AFQjCNEM3uaZcJwV_5yJS0S7IIXHy86j4A&sig2=_vdwus-Gx7a1AzgVqvi_)
- QPCOM. (2016). *qpcom.com.co*. Obtenido de QP-1240R Ficha técnica:  
[http://qpcom.com.co/Portals/116/QP-1240R\\_espanol.pdf](http://qpcom.com.co/Portals/116/QP-1240R_espanol.pdf)
- Richartson Comunicaciones. (2016). *www.richartson.com*. Obtenido de Soluciones Wireless:  
<http://www.richartson.com/xtrem-ubiquiti.php>
- Rojas Villegas, R., & Rivera Paredes, R. (2010). *Internet y redes inalámbricas*. Arequipa, Perú: Clanar Internacional.
- Ros, I. (09 de Junio de 2015). *www.muycomputer.com*. Obtenido de D-Link Central WiFi Manager: <http://www.muycomputer.com/2015/06/09/d-link-central-wifi-manager/>

- Routerboard. (2015). *routerboard.com*. Obtenido de RB1100AHx2|:  
<https://routerboard.com/RB1100AHx2>
- Routerboard. (2016). *routerboard.com*. Obtenido de RB1100AHx2:  
<https://routerboard.com/RB1100AHx2>
- Sifra consultores, S.A. de C.V. (2009). *http://www.sifra.net.mx*. Obtenido de Redes inalámbricas: <http://www.sifra.net.mx/tecnologías/redes-inalámbricas.aspx>
- Simal, T. (12 de Febrero de 2011). *Observatorio Tecnológico*. Obtenido de Redes Wifi - Wi-Fi y QoS: <http://recursostic.educacion.es/observatorio/web/ca/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi?start=6>
- Simal, T. (12 de Febrero de 2011). *Observatorio Tecnológico*. Obtenido de Redes Wifi - Sistemas de gestión Wi-Fi centralizados: <http://recursostic.educacion.es/observatorio/web/ca/cajon-de-sastre/38-cajon-de-sastre/961-monografico-redes-wifi?start=3>
- SlideShare. (Abril de 2015). *es.slideshare.net*. Obtenido de Redes inalámbricas: [https://es.slideshare.net/guest0c6d6/redes-inalambricas-1?qid=385509c4-523a-4f63-94a1-3ceef3f4766c&v=qf1&b=&from\\_search=6](https://es.slideshare.net/guest0c6d6/redes-inalambricas-1?qid=385509c4-523a-4f63-94a1-3ceef3f4766c&v=qf1&b=&from_search=6)
- Stallings, W. (2014). *Data and Computer Communications* (Décima ed.). Ney Jersey, United States of America: Pearson.
- Tanenbaum, A. S., & Wetherall, D. J. (2011). *Redes de computadoras* (Quinta ed.). México: Pearson.
- Wifi Safe. (2015). *www.wifisafe.com*. Obtenido de CONTROLES DE ACCESO WIFI, ESCENARIOS HOTSPOT: <https://www.wifisafe.com/blog/controles-acceso-wifi-hotspot/>

## **ANEXOS**

**Anexo 1.** Evidencias fotografías de la instalación de los APs y el equipo de gestión central

**Anexo 2.** Encuestas

**Anexo 3.** Modelo de encuesta utilizado