



**REESTRUCTURACIÓN DE LA RED WI-FI DEL CAMPUS BARCELONA DE LA
UNIVERSIDAD DE LOS LLANOS**

JULY STEFANNY SALAZAR SIERRA

160003237

BAYRON DANILO ORTIZ FORONDA

160002925

**UNIVERSIDAD DE LOS LLANOS
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
VILLAVICENCIO, COLOMBIA**

2019

**REESTRUCTURACIÓN DE LA RED WI-FI DEL CAMPUS BARCELONA DE LA
UNIVERSIDAD DE LOS LLANOS**

JULY STEFANNY SALAZAR SIERRA

160003237

BAYRON DANILO ORTIZ FORONDA

160002925

Trabajo de grado presentado como requisito parcial para optar al título de
Ingeniero de Sistemas

Director

HECTOR IVAN REYES MONCAYO

Ingeniero Electrónico, MSc. en Teleinformática, Ph. D. en Ingeniería

Supervisor

JAIME ELIECER ROA GARCÍA

Ingeniero de Sistemas

**UNIVERSIDAD DE LOS LLANOS
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
VILLAVICENCIO, COLOMBIA**

2019

NOTAS DE ACEPTACIÓN:

Hector Ivan Reyes Moncayo
Director

Jaime Eliecer Roa Garcia
Supervisor

Cesar Augusto Diaz Celis
Jurado

Fecha

AGRADECIMIENTOS

En primer lugar quiero dar gracias a Dios, pues soy un fiel testigo de que en la vida los sueños se cumplen con paz en tu alma, fortaleza y esperanza. Ello te permite perseverar para enfrentar la vida con alegría y confianza, requiriendo siempre de esfuerzo para que las cosas sean posibles. Vale la pena creer.

A mi familia especialmente a mi madre, pues siempre ha sido ese pilar de amor fundamental del cual he recibido una muy buena formación. Su apoyo me anima a perseguir cada día aquellas cosas con las que sueño y me apasionan, a ir contracorriente sin nunca olvidar la humildad y la sencillez que se deben mantener en cada momento de la vida.

Al ingeniero Hector Ivan Reyes, director de este trabajo. Gracias por esta oportunidad y la confianza que permitieron que hiciera parte en este proyecto; ya que se logró poner en práctica y profundizar muchos conocimientos adquiridos, durante mis últimos semestres de carrera de los cursos referentes al área de las telecomunicaciones. De alguna manera el tenerlo como profesor en estos, amplió mi perspectiva del campo de acción que puede tener un ingeniero de sistemas, no solo dentro de los límites del desarrollo de software, sino también en el vasto mundo de las telecomunicaciones, en donde quiero crecer y espero contar con su mentoría.

A la ingeniera Olga Lucía Balaguera, jefe de la Oficina de Sistemas de la Universidad de los Llanos. Agradecerle por ese gran trabajo y compromiso que esta llevando a cabo dentro de la dependencia; pues este ha permitido empoderar a los estudiantes a que participen en la resolución de los problemas que aquejan a la Universidad, en los aspectos relacionados con TI a través de los proyectos en modalidad de pasantía.

Al ingeniero Jaime Roa, supervisor dentro de la pasantía. Aunque creo que le salieron algunas canas ante dificultades presentadas a medida que se iban aplicando cambios en el avance del proyecto, le doy gracias por su disposición, empatía y confianza brindadas; pues finalmente se pudo llevar a buen término la mayoría de actividades planteadas en este trabajo. Finalmente dar gracias a todas aquellas personas que de manera directa o indirecta hicieron parte, contribuyeron e influenciaron, para que la realización de este trabajo fuera posible.

Bayron Danilo Ortiz Foronda

AGRADECIMIENTOS

Durante todo mi proceso académico y más que eso, mi proceso de crecimiento personal tanto físico como espiritual, siempre he estado acompañado de dos grandes seres humanos que Dios designo como mis padres, agradezco a Dios y a ellos por cada uno de los esfuerzos que han hecho por darme lo mejor posible, más que algo material, su amor incondicional y su apoyo total en todos los aspectos del transcurso de mi vida.

Agradezco al Ingeniero Héctor Iván Reyes Moncayo por confiar en mis capacidades e integrarse a este gran proyecto, siendo así mi guía de aprendizaje continuo tanto en el proceso de la pasantía como en las clases que me impartió, en cursos que hasta el día de hoy me han proporcionado infinidad de conocimientos que deseo seguir implementando a lo largo de mi carrera profesional. A la Ingeniera Olga Balaguera jefe de la Oficina de Sistemas, agradezco también la confianza que brinda a todos los estudiantes que desarrollamos y afianzamos nuestros conocimientos en los proyectos que imparte la Oficina de Sistemas, proporcionándonos así un medio de crecimiento personal y profesional.

Por último y no menos importantes agradezco a cada uno de mis compañeros y amigos que fueron parte de mi proceso académico en esa etapa tan importante de mi vida, a esas personas que a lo largo de estos años contribuyeron de cierta forma en mi crecimiento personal y académico continuamente.

July Stefanny Salazar Sierra

TABLA DE CONTENIDO

1. RESUMEN Y PALABRAS CLAVE	19
2. PLANTEAMIENTO DEL PROBLEMA	19
3. OBJETIVOS	20
3.1 Objetivo general	20
3.2 Objetivos específicos	20
4 JUSTIFICACIÓN	21
5 MARCO DE REFERENCIA, TEÓRICO O CONCEPTUAL	22
5.1 Wi-Fi	23
5.2 Red	23
5.2.1 Clasificación de redes	23
5.2.1.1 Redes de área local (LAN)	23
5.2.1.2 Redes de área metropolitana (MAN)	24
5.2.1.3 Redes de área amplia (WAN)	24
5.3 Red inalámbrica	25
5.3.1 Red de área personal inalámbrica (WPAN)	25
5.3.2 Red de área local inalámbrica (WLAN)	25
5.3.3 Red de área metropolitana inalámbrica (WMAN)	26
5.4 División de canales y frecuencias en redes inalámbricas Wi-Fi (802.11)	26
5.5 Segmentación de tráfico red de área local virtual (VLAN)	28
5.5.1 Definición de VLAN	28
5.5.2 Ventajas de las VLANs	29
5.5.2.1 Incrementan el desempeño de la red	29
5.5.2.2 Facilidad en la administración	29
5.5.2.3 Mejoran la seguridad de la red	29

5.5.2.4 Facilitan el control de flujo de tráfico	30
5.5.3 Tipos de VLANs	30
5.5.3.1 VLAN de nivel 1	30
5.5.3.2 VLAN de nivel 2	30
5.6 Gestión de la red protocolo SNMP	31
6. METODOLOGÍA	33
6.1 Fase I: Analizar requisitos	34
6.2 Fase II: Diseño de la red	34
6.3 Fase III: Fase de implementación, prueba, optimización y documentación del diseño de la red.	34
7. DESARROLLO DE LA PASANTÍA	35
7.1 Fase I: Analizar requisitos	35
7.1.1 Identificación necesidades usuarios	35
7.1.2 Identificación características técnicas red existente	40
7.2 Fase II: Diseño de la red	43
7.2.1 Diseño lógico de la red	43
7.2.1.1 Direccionamiento IP	43
7.2.1.2 Segmentación de la red en VLANs	44
7.2.2 Plan de frecuencias y potencias de los dispositivos de red Wi-Fi	46
7.2.2.1 Plan elaborado puntos de acceso oficinas	47
7.2.2.1.1 Plan Zona Determinada Coliseo	47
7.2.2.1.2 Plan zona determinada edificios Einstein, Da Vinci y Bunker	48
7.2.2.2 Plan elaborado puntos de acceso HP ARUBA	49
7.2.3 Planificación puntos de acceso en nuevas zonas del campus Barcelona	52
7.3 Fase III: Fase de implementación, prueba,	

optimización	53
y documentación del diseño de la red.	
7.3.1 Implementación	53
7.3.1.1 Configuración de access points dependencias	53
7.3.1.2 Configuración de access points HP Aruba	54
7.3.1.3 Configuración de switches	54
7.3.1.4 Instalación e implementación de la plataforma LibreNMS	55
7.3.1.5 Implementación diseño de la red	55
7.3.1.5.1 Segmentación de tráfico	56
7.3.1.5.2 Direcccionamiento IP	56
7.3.2 Pruebas	56
8. RESULTADOS	59
8.1 Consolidado encuestas	60
8.1.1 Zonas estudiantiles frecuentadas del campus Barcelona, que requieren de cobertura Wi-Fi	60
8.1.2 Servicios más utilizados ya sean de aplicaciones o sitios web, tanto académicos como de ocio	61
8.1.3 Tipos de dispositivos usados (smartphones o computadores)	61
para el acceso a los servicios de red dentro del campus	
8.2 Consolidado Características Routers.	62
8.2.1 Ecosistema de marcas de dispositivos en la red.	63
8.2.2 Compatibilidad cambio de firmware DD-WRT	63
8.2.3 Soporte de protocolo RADIUS (802.1x)	64
8.2.4 Disponibilidad de antena externa	64
8.2.4 Estado físico de dispositivos	65
8.3 Consolidado switches	66
8.3.1 Ecosistema de marcas de dispositivos en la red	66
8.3.2 Cantidad de switches por número de puertos	67
8.3.3. Switches administrables y no administrables	67

8.4 Consolidado configuración	68
8.4.1 Configuración access points	68
8.4.2 Configuración switches	69
8.4.2.1 Cantidad de switches por cada rack	70
8.5 Frecuencias y potencias de los access points	72
8.5.1 Zona torre administrativa	72
8.5.2. Zona de la Facultad FCARN	73
8.5.3. Zona del programa de Matemáticas	73
8.5.4. Zona de la cafetería Nestea	74
8.5.5. Zona de la clínica Veterinaria	74
8.5.6. Zona de los laboratorios de Electrónica	75
8.5.7. Zona de los laboratorios de Química	75
8.8.8. Zona de la facultad FCBI	76
8.8.9. Zona del edificio Albert Einstein	76
8.8.10. Zona del Coliseo	77
8.8.11. Zona del IALL	77
8.8.12. Zona de la sede Posgrados	78
8.6 VLANs y direccionamiento	78
8.7 Plataforma LibreNMS	81
8.7.1 Adición de dispositivos de red a la plataforma	81
8.7.2 Visualización de información de puertos	82
8.7.3 Visualización del tráfico total de red	82
8.7.4 Visualización de monitoreo de recursos	83
8.7.5 Creación de alertas	84
8.7.6 Notificaciones de alertas	84
8.8 Pruebas de rendimiento previas	85
8.8.1 Punto de acceso zona IDEAD	86
8.8.2 Punto de acceso zona Biblioteca/Torre Administrativa	87
8.8.3 Punto de acceso zona Cooperativa/Counillanos	88
8.8.4 Punto de acceso zona Coliseo	90
8.8.5 Punto de acceso zona edif. Albert Einstein	90

8.8.6 Punto de acceso zona Corocora/Plaza Garza	91
8.9 Puntos de acceso en nuevas zonas del campus Barcelona	92
9. CONCLUSIONES	102
10. RECOMENDACIONES	103
10.1 Oficina de Sistemas	103
10.1.1 Características técnicas de nuevos equipos	103
10.1.2 Personal capacitado dedicado a la gestión de la red	104
10.2 Programa Ingeniería de Sistemas	105
10.2.1 Fortalecimiento de la línea de profundización de Teleinformática	105
10.3 Trabajos futuros	106
11.IMPACTO	106
12. GLOSARIO	107
12.1 Generalidades de la empresa	107
12.1.1 Ubicación y contacto	108
12.1.2 Misión	108
12.1.3 Visión	109
12.2 Acrónimos y siglas	109
13. ANEXOS	110
13.1 Caso Rogue DHCP en la red campus Barcelona	110
13.2 Acuerdos de confidencialidad	122
14 BIBLIOGRAFÍA	126

ÍNDICE DE FIGURAS, GRÁFICAS Y TABLAS

FIGURAS

Figura 1. Ejemplo de red de área local.	23
Figura 2. Ejemplo de red de área metropolitana basada en la TV por cable.	24
Figura 3. Ejemplo de red de área amplia en el continente oceánico.	25
Figura 4. Ejemplo de red de área local inalámbrica.	26
Figura 5. Distribución de canales y sus frecuencias banda 2.4GHz.	27
Figura 6. Distribución de canales con múltiples puntos de acceso en una zona.	27
Figura 7. Distribución canales y sus frecuencias banda 5 GHz.	28
Figura 8. Ejemplo topología de VLANs.	29
Figura 9. VLAN basada en puertos.	30
Figura 10. VLAN basada en direcciones MAC.	31
Figura 11. Ejemplo de configuración gestión de red.	33
Figura 12. Formato de encuesta aplicada a los estudiantes.	36
Figura 13. Sección 1, formato de encuesta Google Forms.	37
Figura 14. Sección 2, formato de encuesta Google Forms.	38
Figura 15. Sección 3, formato de encuesta Google Forms.	39
Figura 16. Formato de recolección de información routers.	40
Figura 17. Formato de recolección de información switches.	41
Figura 18. Esquema general del nuevo direccionamiento IP, para el campus Barcelona.	44
Figura 19. Distribución de VLANs proyectadas a implementar en el	46

campus Barcelona.

Figura 20. Plan de frecuencias en routers zona Coliseo.	48
Figura 21. Plan de frecuencias en routers zona Einstein/Da Vinci.	49
Figura 22. Frecuencias en la banda de 2.4 GHz puntos de acceso estudiantes, campus Barcelona.	51
Figura 23. Frecuencias en la banda de 5 GHz puntos de acceso estudiantes, campus Barcelona.	52
Figura 24. Puntos de acceso estudiantes campus Barcelona.	57
Figura 25. Diagrama funcionamiento <i>iPerf 3</i> .	59
Figura 26. Ubicación Switches configurados en el campus Barcelona.	71
Figura 27. VLANs implementadas en el campus Barcelona.	81
Figura 28. Lista de algunos de los switches agregados a la plataforma piloto.	82
Figura 29. Detalles de información de tráfico de red de los puertos de todos los switches.	83
Figura 30. Gráfico del tráfico de red de un dispositivo.	83
Figura 31. Representación del estado del procesador y memoria de un switch.	84
Figura 32. Representación del estado de la temperatura y de los sensores de un switch.	84
Figura 33. Alertas creadas por el usuario en la plataforma piloto.	85
Figura 34. Notificaciones de alertas de diferentes switches.	86
Figura 35. Ubicación zonas, donde se hace necesario cobertura de red Wi-Fi, campus Barcelona.	95
Anexo. Figura 36. Formato de mensaje protocolo DHCP.	112
Anexo. Figura 37. Intercambio de mensajes asignación IP, protocolo DHCP.	114

Anexo. Figura 38. Intercambio de mensajes DHCP, red no segmentada con Rogue DHCP.	117
Anexo. Figura 39. Puerto de WAN, indicación router D-Link.	118
Anexo. Figura 40. Captura tráfico usando la aplicación <i>Wireshark</i> , en busca de un Rogue DHCP.	119
Anexo. Figura 41. Paquetes análisis con <i>Wireshark</i> .	119
Anexo. Figura 42. Mensaje de tipo <i>Request</i> , análisis con <i>Wireshark</i> .	120
Anexo. Figura 43. Mensaje de tipo <i>Request</i> , análisis con <i>Wireshark</i> .	121

GRÁFICAS

Gráfica 1. Representación de zonas que requieren mayor cobertura según estudiantes.	60
Gráfica 2. Representación de las aplicaciones y/o páginas web más visitadas.	61
Gráfica 3. Representación del uso de dispositivos para acceder a la red.	62
Gráfica 4. Cantidad de dispositivos inalámbricos por marca.	63
Gráfica 5. Representación de la cantidad de dispositivos que soportan DD-WRT.	63
Gráfica 6. Representación de la cantidad de dispositivos que soportan RADIUS.	64
Gráfica 7. Representación de los dispositivos que disponen antenas.	65
Gráfica 8. Cantidad de dispositivos inalámbricos por marca.	66
Gráfica 9. Cantidad de Switches por número de puertos en el campus Barcelona.	67
Gráfica 10. Cantidad de switches Administrables/No administrables.	68
Gráfica 11. Access points operando en nuevo direccionamiento IP.	69
Gráfica 12. Switches los cuales se les aplicó el nuevo	69

direccionamiento IP.

Gráfica 13. Estado inicial, frecuencias redes Wi-Fi torre administrativa.	72
Gráfica 14. Estado final, frecuencias redes Wi-Fi torre administrativa.	72
Gráfica 15. Estado inicial, frecuencias redes Wi-Fi facultad FCARN.	73
Gráfica 16. Estado final, frecuencias redes Wi-Fi facultad FCARN.	73
Gráfica 17. Estado inicial, frecuencias redes Wi-Fi programa de matemáticas.	73
Gráfica 18. Estado final, frecuencias redes Wi-Fi programa de matemáticas.	73
Gráfica 19. Estado inicial, frecuencias redes Wi-Fi cafetería Nестea.	74
Gráfica 20. Estado final, frecuencias redes Wi-Fi cafetería Nестea.	74
Gráfica 21. Estado inicial, frecuencias redes Wi-Fi clínica veterinaria.	74
Gráfica 22. Estado final, frecuencias redes Wi-Fi clínica veterinaria.	74
Gráfica 23. Estado inicial, frecuencias redes Wi-Fi laboratorios de electrónica.	75
Gráfica 24. Estado final, frecuencias redes Wi-Fi laboratorios de electrónica.	75
Gráfica 25. Estado inicial, frecuencias redes Wi-Fi laboratorios de química.	75
Gráfica 26. Estado final, frecuencias redes Wi-Fi laboratorios de química.	75
Gráfica 27. Estado inicial, frecuencias redes Wi-Fi facultad FCBI	76
Gráfica 28. Estado final, frecuencias redes Wi-Fi facultad FCBI.	76
Gráfica 29. Estado inicial, frecuencias redes Wi-Fi edif. Albert Einstein.	76
Gráfica 30. Estado final, frecuencias redes Wi-Fi edif. Albert Einstein.	76
Gráfica 31. Estado inicial, frecuencias redes Wi-Fi coliseo.	77
Gráfica 32. Estado final, frecuencias redes Wi-Fi coliseo.	77

Gráfica 33. Estado inicial, frecuencias redes Wi-Fi IALL.	77
Gráfica 34. Estado final, frecuencias redes Wi-Fi IALL.	77
Gráfica 35. Estado inicial, frecuencias redes Wi-Fi Posgrados.	78
Gráfica 36. Estado final, frecuencias redes Wi-Fi Posgrados.	78

TABLAS

Tabla 1. Descripción de direccionamiento IP campus Barcelona.	42
Tabla 2. Distribución de VLANs por dependencia campus Barcelona.	45
Tabla 3. Frecuencias y potencias, diseñadas para puntos de acceso ubicados en oficinas Coliseo.	47
Tabla 4. Frecuencias y potencias, diseñadas para puntos de acceso ubicados en oficinas Edificios Einstein, Da Vinci y Bunker.	48
Tabla 5. Frecuencias y potencias, diseñadas para puntos de acceso estudiantes.	49
Tabla 6. Zonas mapa, cobertura de puntos de acceso estudiantes campus Barcelona.	58
Tabla 7. Access Points del campus Barcelona en mal estado.	65
Tabla 8. Access Points Aruba del campus Barcelona en mal estado.	66
Tabla 9. Cantidad y marcas de switches por rack.	70
Tabla 10. VLANs configuradas e implementadas en el switch principal.	79
Tabla 11. Gráficos pruebas de rendimiento, generados por kentnetmon IDEAD.	86
Tabla 12. Valores obtenidos de las pruebas de rendimiento, IDEAD	86
Tabla 13. Gráficos pruebas de rendimiento, generados por kentnetmon Biblioteca.	87
Tabla 14. Valores obtenidos de las pruebas de rendimiento, Biblioteca.	87

Tabla 15. Gráficos pruebas de rendimiento, generados por kentnetmon Cooperativa.	88
Tabla 16. Valores obtenidos de las pruebas de rendimiento, Cooperativa.	88
Tabla 17. Gráficos pruebas de rendimiento, generados por kentnetmon Coliseo.	89
Tabla 18. Valores obtenidos de las pruebas de rendimiento, Coliseo.	89
Tabla 19. Gráficos pruebas de rendimiento, generados por kentnetmon Einstein.	90
Tabla 20. Valores obtenidos de las pruebas de rendimiento, Einstein.	90
Tabla 21. Gráficos pruebas de rendimiento, generados por kentnetmon Corocora.	91
Tabla 22. Valores obtenidos de las pruebas de rendimiento, Corocora.	91
Tabla 23. Zonas donde se hace necesario cobertura de red Wi-Fi, campus Barcelona.	93
Tabla 24. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Da Vinci.	95
Tabla 25. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Einstein - Da Vinci 1.	95
Tabla 26. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Einstein - Da Vinci 2.	96
Tabla 27. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Clínica Veterinaria.	96
Tabla 28. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Biblioteca	97
Tabla 29. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Auditorio Eduardo Carranza.	98
Tabla 30. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Bienestar Institucional.	99
Tabla 31. Detalle y ubicación de dispositivos mejoramiento de cobertura,	99

zona Facultad de Matemáticas.

Tabla 32. Detalle y ubicación de dispositivos mejoramiento de cobertura,
zona Ovinos y Caprinos. **100**

Tabla 33. Detalle y ubicación de dispositivos mejoramiento de cobertura,
zona Laboratorios de Química. **100**

Tabla 34. Detalle y ubicación de dispositivos mejoramiento de cobertura,
otras zonas. **101**

ACUERDO DE CONFIDENCIALIDAD

Debido a lineamientos de protección de propiedad intelectual, la Oficina de Sistemas se guarda el derecho de reservar los secretos corporativos detrás de este proyecto. Para garantizar la discreción de la información relevante a los proyectos de la Oficina de Sistemas se realizó un acuerdo de confidencialidad, al final del presente libro se anexa una copia del formato en donde se explican todos los términos y condiciones de la cláusula.

1. RESUMEN Y PALABRAS CLAVE

Actualmente la Universidad de los Llanos cuenta con una red inalámbrica con acceso a internet el cual ha sido altamente criticada y ha traído consigo muchas opiniones y comentarios de inconformismo. De acuerdo a un estudio realizado por el Ingeniero Héctor Iván Reyes Moncayo, integrante de la Escuela de Ingeniería, con la colaboración de los estudiantes del programa de Ingeniería de sistemas, Juan David Baez, Kevin Nieves, Jorge Reina, Cristian Rojas, y Alexis Sierra, miembros del Grupo de estudio de Redes y Aplicaciones- GERA, la red Wi-Fi del campus Barcelona no se encuentra diseñada adecuadamente y por esta razón actualmente padece de problemas cobertura y soporte. Es por esto que el propósito del presente proyecto es realizar una reestructuración de la red de Wi-Fi de la Universidad de los Llanos en este campus, para así brindar un servicio eficiente y de calidad a la comunidad Unillanista, conformada por docentes, administrativos y estudiantes.

Palabras claves: red, Wi-Fi, Universidad de los Llanos, inalámbrico, Internet, campus.

2. PLANTEAMIENTO DEL PROBLEMA

Procesos académicos y administrativos se apoyan cada vez más en recursos informáticos que dependen de un acceso estable a Internet; por tanto, se presenta la necesidad de mejorar la infraestructura de la red inalámbrica con la que cuenta la Universidad de los Llanos en el campus Barcelona.

Actualmente el ecosistema de la red inalámbrica, posee diferentes inconvenientes, tanto en el campo de usabilidad para los usuarios finales (comunidad académica y administrativos) como para los entes encargados del control y administración de la red. En cuanto a usabilidad se dificulta en gran medida el acceso al medio inalámbrico, lentitud en la navegación, inestabilidad de las conexiones; provocado por una incorrecta planificación de frecuencias y potencias de los puntos de acceso, algunas zonas se encuentran saturadas de redes inalámbricas y otras zonas sin cobertura. No hay segmentación del tráfico de red entre estudiantes y administrativos, lo que representa una amenaza para

la seguridad de la red; no se posee un conocimiento profundo de la infraestructura de TI de la red, ya que no se cuenta con un inventario de los dispositivos, ni una plataforma que permita la gestión de los mismos de una forma centralizada, sino que actualmente se configura cada dispositivo de manera independiente, lo que no es óptimo en los casos de redes corporativas como la que se requiere en la Universidad. La información anterior se obtiene de un pequeño estudio de campo realizado por el Ingeniero Héctor Iván Reyes Moncayo, en conjunto con el grupo de estudio GERA.

3. OBJETIVOS

3.1 Objetivo general

Apoyar a la Oficina de Sistemas en la reestructuración de la red de acceso inalámbrico del campus Barcelona de la Universidad de los Llanos.

3.2 Objetivos específicos

- Apoyar las labores relacionadas en la identificación de los requerimientos de conectividad de los usuarios de la red inalámbrica del campus Barcelona de la Universidad de los Llanos, en cuanto a cubrimiento y capacidad.
- Asistir en las tareas de identificación de las características técnicas de los equipos de acceso inalámbrico de propiedad de la Universidad de los Llanos instalados en el campus Barcelona, con el fin de establecer la posibilidad de usarlos en la nueva red.
- Apoyar en las tareas de diseño del nuevo sistema de acceso inalámbrico, en base a los requerimientos de cubrimiento y capacidad identificados en el estudio de campo; lo que implica nueva planificación de canales de frecuencia y potencias de los puntos de acceso.

- Asistir en la identificación de la necesidad de compra de nuevos equipos y componentes de acceso: access points, switches, enrutadores, antenas, etc.
- Apoyar a la Oficina de Sistemas en la implementación del nuevo diseño realizado, lo cual incluye reconfigurar y reubicar aquellos puntos de acceso existentes, como también instalar y configurar nuevos puntos; condicionado esto último a la adquisición de nuevos dispositivos y a la renovación de las líneas de fibra óptica, por parte de la Universidad, dentro del tiempo propuesto para el desarrollo del proyecto.
- Asistir en las tareas de segmentación de tráfico de la red de datos en cuestión, según el diseño establecido. El cumplimiento de este objetivo está condicionado a que la Universidad proporcione el equipo necesario: switch capa 3 o enrutador; dentro del tiempo propuesto para el desarrollo de este proyecto y a la renovación de las líneas de fibra óptica con las que se cuenta actualmente.
- Apoyar a la Oficina de Sistemas en la implementación de un módulo piloto de una plataforma de gestión de red basado en el protocolo SNMP.
- Apoyar actividades de capacitación para el personal técnico de la Oficina de Sistemas en la gestión de la red.

4 JUSTIFICACIÓN

La red inalámbrica del campus Barcelona de la Universidad de los Llanos, presenta actualmente diferentes inconvenientes, como lo son la falta de un plan de frecuencias adecuado, desconocimiento de los dispositivos con los que cuenta la red; método de autenticación personal, inadecuado para un ambiente de alta densidad de tráfico, zonas del campus sin cobertura y la inexistencia de un diseño o esquema lógico de la red; no permiten brindar a los usuarios un servicio eficiente de conectividad para el desarrollo de las diferentes actividades académicas. Es por ello que este trabajo se presenta como una oportunidad, para realizar cambios significativos en el mejoramiento de la red, atacando los inconvenientes con una reestructuración que permita aprovechar en lo posible los

dispositivos instalados con los que cuenta la red y la implementación de equipos nuevos correctamente configurados, basados en un diseño lógico y un plan de frecuencias para la red inalámbrica; condicionado este punto a la gestión realizada por parte de la Oficina de Sistemas, para la adquisición de nuevos equipos, dentro del tiempo del desarrollo del proyecto; según los objetivos planteados dentro de esta propuesta, mejorando el acceso y la cobertura según las necesidades de conectividad de los usuarios. Otros de los cambios significativos a realizar es la segmentación del tráfico de la red, implementando redes locales virtuales (VLANs); pues actualmente esta funciona como un único segmento, lo que conlleva a problemas no sólo de seguridad, sino también de congestión ya que todos los equipos comparten un mismo dominio de difusión, haciendo que el acceso a los servicios de la red sean inestables. Por último mencionar que este proyecto, también incluirá la puesta en marcha de algunos servicios inexistentes en la red actual, como lo es una plataforma piloto para la gestión de la red la cual permitirá la detección de fallas, el monitoreo continuo del funcionamiento de los equipos y el constante seguimiento a la red para la corrección de fallas futuras.

Cada una de las diferentes problemáticas y las soluciones posibles brindadas anteriormente, permitirán poner en práctica los conocimientos adquiridos en los cursos aprobados del plan de estudios de la carrera Ingeniería de Sistemas, especialmente aquellos de las líneas de profundización correspondientes a Teleinformática e Ingeniería de Software; junto con el acompañamiento de un profesional en el área como lo es el Ph.D. Héctor Iván Reyes Moncayo, quien posee una amplia experiencia y conocimiento en el campo, para la implementación de este tipo de soluciones telemáticas.

5 MARCO DE REFERENCIA, TEÓRICO O CONCEPTUAL

En el proceso de diseño e implementación de una red inalámbrica se hace necesario un aporte teórico a este proyecto, se hace referencia al tema “Redes inalámbricas de área local (WLAN) y su estándar 802.11” más conocido como Wi-Fi y el uso de diferentes conceptos que se ven involucrados en este campo de estudio y que se verán a continuación:

5.1 Wi-Fi

Sus siglas significan Wireless Fidelity, en español fidelidad inalámbrica, es un conjunto de redes no cableadas interconectadas que funcionan inalámbricamente y a base de diferentes protocolos. En la figura 1 se ilustra el modelo de una red Wi-Fi, donde los diferentes dispositivos se conectan a la red por medio del router.

5.2 Red

El comité IEEE 802 establece que “Una red es un sistema de comunicaciones que permite que un número de dispositivos independientes se comuniquen entre sí” [10], su comunicación se hace a partir de la compartición de recursos entre ellas, capacidad que da a las redes potencial y atraktividad.

5.2.1 Clasificación de redes

Existen diferentes tipos de redes inalámbricas que se clasifican según la cobertura que ofrecen.

5.2.1.1 Redes de área local (LAN)

Una red de área local que se muestra en la Figura 1, es una red privada limitada físicamente a un edificio o un entorno de hasta 200 metros, muy usadas en espacios de trabajo e interconexión de computadores personales. Se caracteriza por tener un tamaño restringido, alta velocidad y baja tasa de errores.

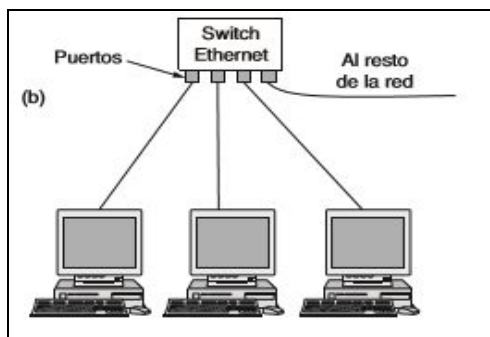


Figura 1. Ejemplo de red de área local [2]

5.2.1.2 Redes de área metropolitana (MAN)

Una red de área metropolitana es una red de alta velocidad, cuya cobertura alcanza un área geográfica extensa. Se caracteriza por proporcionar capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y video, sobre medio de transmisión tales como la fibra óptica y el par trenzado [13], (ver Figura 2)

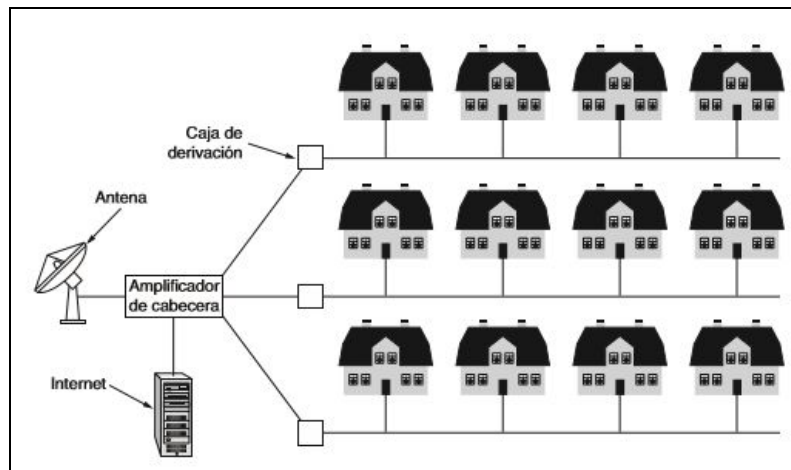


Figura 2. Ejemplo de red de área metropolitana basada en la TV por cable. [2]

5.2.1.3 Redes de área amplia (WAN)

Una red de área amplia, es un tipo de red con una capacidad de cobertura entre los 100 km hasta los 1000km, prestando así el servicio a un país o a un continente, el cual funciona a través de la unión de varias redes LAN (ver Figura 3).

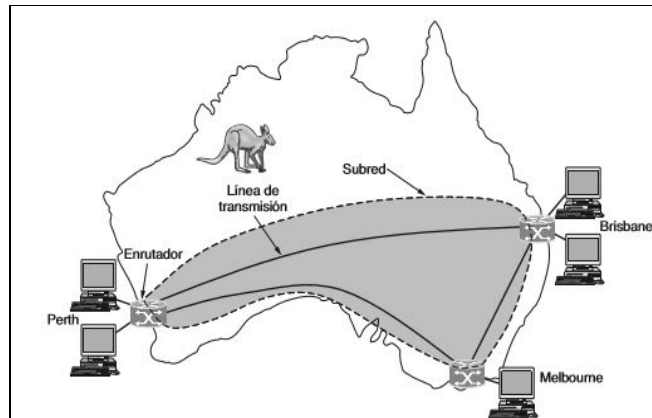


Figura 3. Ejemplo de red de área amplia en el continente oceánico. [2]

5.3 Red inalámbrica

Las redes inalámbricas funcionan mediante ondas de radio que permiten que los dispositivos móviles de un área determinada se conecten y comuniquen entre sí, sin necesidad de cableado. Las redes de área local (LAN) es muy habitual encontrarlas principalmente en áreas de oficinas, aunque la tecnología inalámbrica también es usada en redes de área amplia, de voz y de datos [6].

5.3.1 Red de área personal inalámbrica (WPAN)

Wireless Personal Area Network, esta red se reconoce porque su cobertura es más personalizada por ello tiene un alcance máximo de 10 metros, un claro ejemplo de esta red es el Bluetooth.

5.3.2 Red de área local inalámbrica (WLAN)

Wireless Local Area Network, es una red inalámbrica donde se conectan una serie de dispositivos (PCs, estaciones de trabajo, impresoras, servidores, laptop, celulares, etc.), que se conectan entre sí sin necesidad de estar conectado por medio de cables. La tecnología WLAN es aquella con área de cobertura en entorno local. Algunos ejemplos de áreas de cobertura que se considera locales o de área no extensa son: oficinas, empresas, universidades, hoteles, centros de congreso, aeropuertos, etc. [1]. En la figura 4 se ilustra el modelo de una red WLAN.

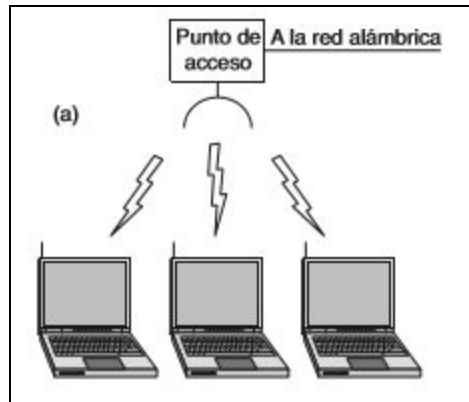


Figura 4. Ejemplo de red de área local inalámbrica. [2]

5.3.3 Red de área metropolitana inalámbrica (WMAN)

Esta red es la versión inalámbrica de MAN, sus principales ventajas son la disminución de costos, ya que se elimina el cableado ethernet entre cada uno de los dispositivos existentes, a su vez enfrenta una desventaja al ser más propensa a intrusos, por el cual la seguridad y la robustez de esta debe ser mayor.

5.4 División de canales y frecuencias en redes inalámbricas Wi-Fi (802.11)

Las redes inalámbricas trabajan bajo ciertas frecuencias dentro del espectro electromagnético considerado sin licenciamiento, estas son la banda de los 2.4GHz y la banda de los 5 GHz. Cada una de ellas ofrece una distribución de canales diferentes, sobre los cuales deben operar los dispositivos inalámbricos (Access Point) dentro de la red.

Un punto muy importante que se debe tener en cuenta, es que entre estos canales existe un solapamiento que puede conllevar a interferencia entre los dispositivos. A continuación, en la Figura 5 se puede apreciar los canales para la banda de 2.4GHz.

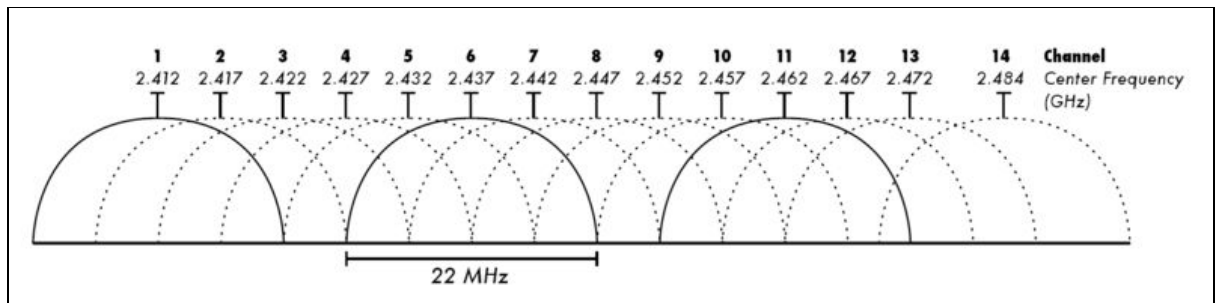


Figura 5. Distribución de canales y sus frecuencias banda 2.4GHz. [8]

En la banda de 2.4GHz existen 3 canales que no se traslapan, los cuales son el 1, el 6 y el 11 con sus respectivas frecuencias 2.412GHz, 2.437GHz y 2.462GHz. Las configuraciones para los puntos de acceso que deseen trabajar en esta banda, deben operar sobre estos canales. En el caso de que existan más de un punto de acceso operando en la misma zona, debe procurarse una distribución de las frecuencias para que un mismo canal no se solape sobre otro. Por ejemplo, Canal 11 con canal 11, o canal 6 con canal 6; estas deben quedar distribuidas de manera similar a la Figura 6.

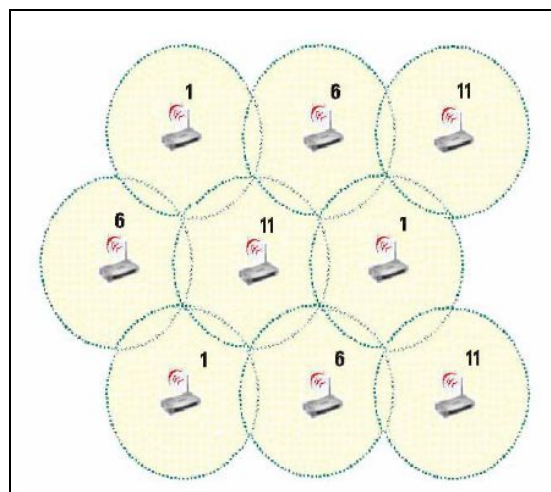


Figura 6. Distribución de canales con múltiples puntos de acceso en una zona. [9]

En el caso de las redes que trabajan en la banda de los 5 GHz existe la posibilidad de tener 25 canales no traslapados, aumentando las posibilidades de

crecimiento de la red inalámbrica. En la figura 7 pueden observarse los canales disponibles.

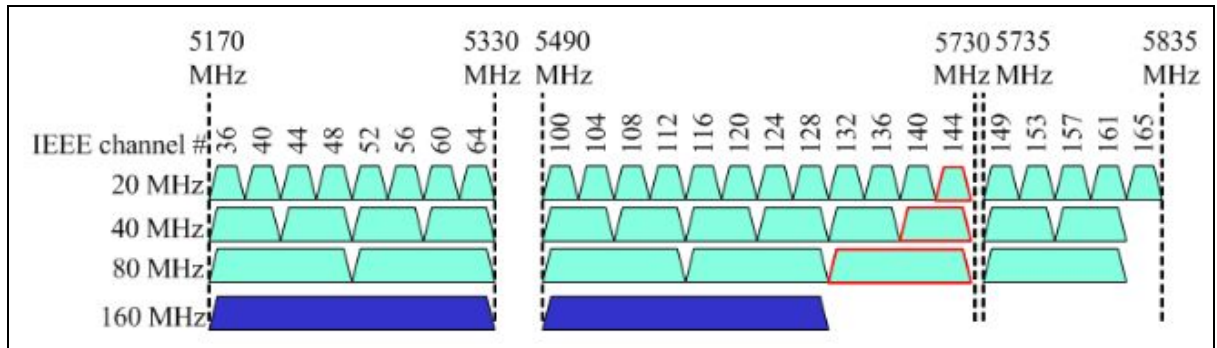


Figura 7. Distribución canales y sus frecuencias banda 5 GHz. [12]

Finalmente destacar que ambas bandas brindan buenas prestaciones, para la red que se quiera implementar; pero si se desea mayor cobertura la banda de 2.4GHz posee menor atenuación (pérdida de potencia) en el aire; en cuanto a la banda de 5GHz esta ofrece mejor velocidad y posibilidad de menos interferencia dado al buen número de canales que posee para operar.

5.5 Segmentación de tráfico red de área local virtual (VLAN)

Dentro del diseño de las redes es importante el tema de la segmentación, ya que permite dividir y aislar ciertas partes de la red, según las necesidades de la organización, generalmente enfocado a las diferentes dependencias que lo componen; mejorando la seguridad ya que el usuario de una dependencia A, no tendrá ningún tipo de oportunidad de intentar establecer conexiones a otras dependencias y equipos que no pertenezcan a su Área Local Virtual A.

A continuación se hablará un poco acerca de las Redes de Área Local Virtual (VLANs), para entender un poco mejor su funcionamiento.

5.5.1 Definición de VLAN

Una VLAN (Virtual Local Area Network) se define como un agrupamiento tanto de dispositivos como de servicios de red de manera lógica, basado en funciones,

aplicaciones, departamentos, entidades o equipos de trabajo; sin necesidad de que estos compartan una ubicación física [14], (ver Figura 8)

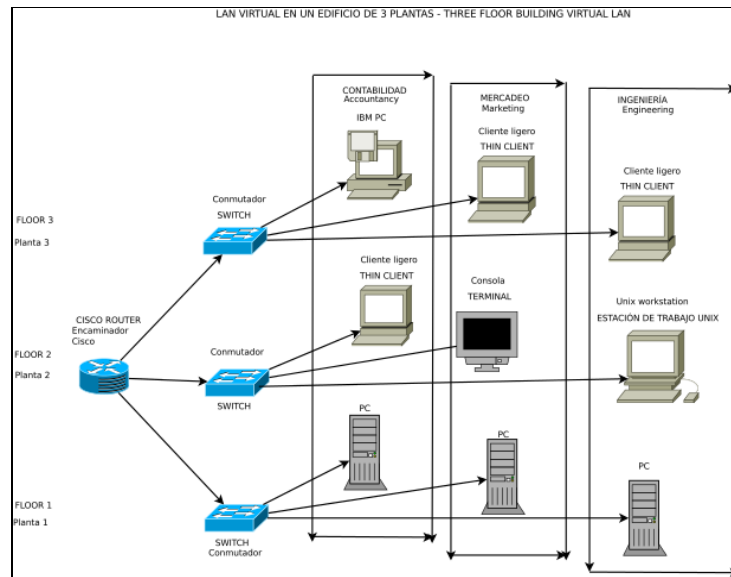


Figura 8. Ejemplo topología de VLANs. [15]

5.5.2 Ventajas de las VLANs

5.5.2.1 Incrementan el desempeño de la red

Permite la agrupación de equipos, recursos y servidores según la función que desempeñen, sin importar si estos se encuentran en el mismo segmento de la red LAN. [14]

5.5.2.2 Facilidad en la administración

Facilita la adición, movimiento y cambio de los equipos de la red, permitiendo flexibilidad y escalabilidad; además las configuraciones son realizadas por medio de software en los dispositivos de red (Switch). [14]

5.5.2.3 Mejoran la seguridad de la red

Dado que sólo los equipos de la red, pueden comunicarse directamente a otros equipos que pertenezcan a su misma VLAN, sin necesidad de utilizar enrutamiento. [14]

5.5.2.4 Facilitan el control de flujo de tráfico

Permitiendo el control de la cantidad y tamaño de los dominios de broadcast, que al ser más pequeños evita que la red sufra de congestión. [14]

5.5.3 Tipos de VLANs

5.5.3.1 VLAN de nivel 1

Denominada como VLAN basada en puerto, ya que define la red virtual según los puertos de conexión del Switch, por medio de configuración en el software de este dispositivo (ver Figura 9).

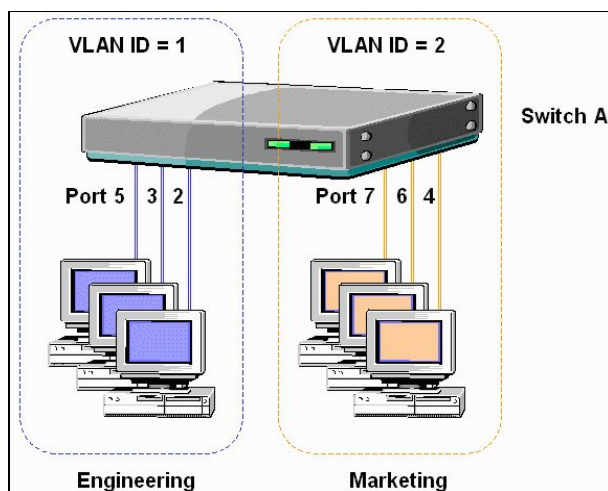


Figura 9. VLAN basada en puertos. [16]

5.5.3.2 VLAN de nivel 2

Denominada como VLAN basada en direcciones MAC. Este tipo de red virtual se administra de forma similar a la de Nivel 1, pero asociando y agrupando a los dispositivos en base a su dirección física (MAC); para ello se hace necesario un servidor de administración de VLANs, el cual posee una base de datos, que

determina cuáles direcciones MAC de los equipos conectados a la red, pertenecen a una VLAN específica (ver Figura 10).

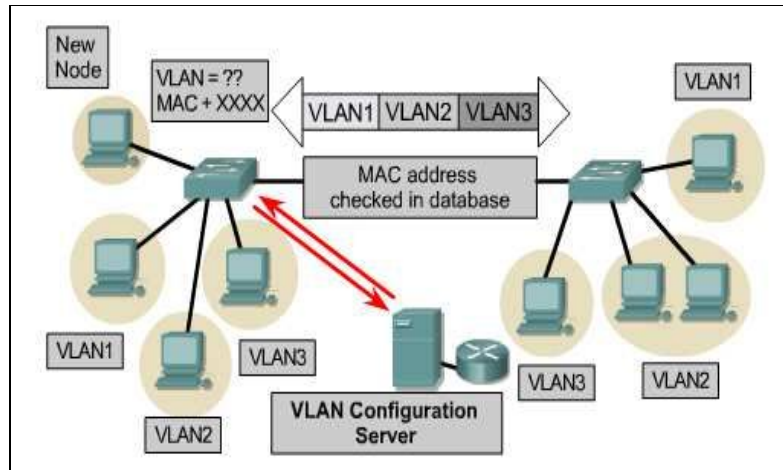


Figura 10. VLAN basada en direcciones MAC. [14]

5.6 Gestión de la red protocolo SNMP

Las redes en los ambientes corporativos, comerciales o educativos, cada vez toman más fuerza e importancia, ya que el uso de recursos compartidos dentro de estas y la velocidad de comunicación entre diferentes entidades permiten el trabajo colaborativo y la centralización de la información, como recurso más valioso. Pero qué pasa si la red necesita ampliar sus servicios a nuevas oficinas, ofrecer otro tipo de aplicaciones, despliegue de algún servicio necesario; esto hace que crezca la complejidad de la misma y se pueden evidenciar dos cosas importantes:

- La red se convierte de algún modo, en una herramienta o servicio indispensable dentro de la organización.
- Al convertirse la red en algo indispensable, la falla de algún dispositivo o nodo, puede afectar el funcionamiento de la misma, disminuyendo el rendimiento o dejándola totalmente inoperativa.

Una red fiable y extensa no se puede instalar y gestionar sólo con esfuerzo humano (Stallings, 2004), es por ello que se hace necesario el uso de herramientas que faciliten esta tarea, claramente en las redes conviven gran

cantidad de dispositivos de fabricantes distintos, brindando cada uno una función específica; sin embargo, aquí es donde vienen los protocolos como es el caso de SNMP para proveer una forma estandarizada de llevar a cabo esta gestión.

SNMP (Simple Network Management Protocol) protocolo simple de gestión de red, usa un conjunto de especificaciones para gestionar la red, la definición de base de datos y otros conceptos importantes. SNMP incluye cuatro elementos importantes, que definen el modelo para la gestión de la red:

1. **Estación de gestión o gestor:** Dispositivo generalmente autónomo que actúa como interfaz entre el administrador de la red y el sistema o plataforma de gestión de la misma. Este gestor debe incluir como mínimo:
 - a. Aplicaciones para la gestión y análisis de datos.
 - b. Interfaz por medio de la cual se pueda monitorizar y controlar la red.
 - c. Capacidad de controlar parámetros y requisitos del administrador, hacia los elementos o dispositivos de la red de forma remota.
 - d. Base de datos de los dispositivos interconectados en la red.
2. **Agente:** Es un elemento activo dentro del sistema y es equipado en los dispositivos de la red, sean computadoras, switches, hubs etc. y responde con información a las solicitudes realizadas por la estación de gestión.
3. **Base de datos información de gestión:** Es utilizada por la estación de gestión, funciona como una colección de los puntos de acceso de la red, los cuales son tratados cada uno como un objeto, con diferentes variables que permiten establecer los parámetros deseados de la red por parte del administrador.
4. **Protocolo de gestión de red:** Para enlazar todos los agentes y la estación de gestión se utiliza el protocolo SNMP, antes mencionado; que posee capacidades para obtener información de los objetos del agente, establecer ciertos parámetros a los objetos del agente y generar notificaciones a la estación acerca de eventos importantes de la red.

A continuación, puede apreciarse en la Figura 11 un ejemplo de una red gestionada por SNMP, con lo elementos básicos mencionados.

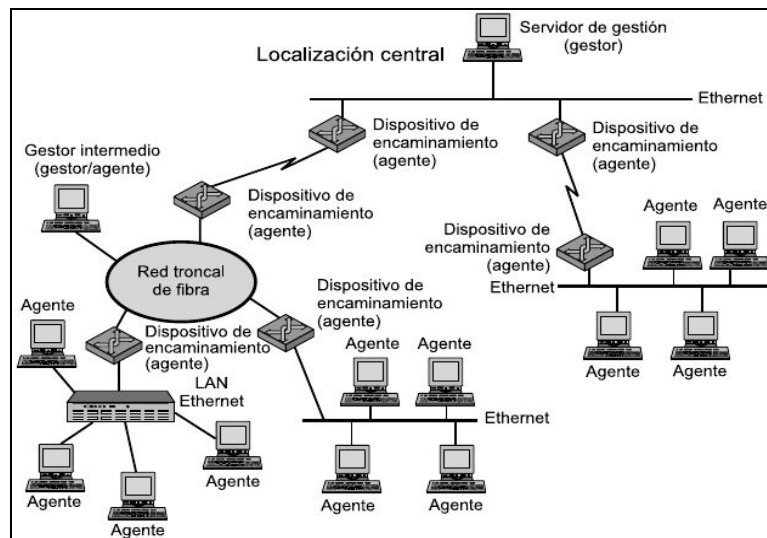


Figura 11. Ejemplo de configuración gestión de red. [6]

Actualmente una muy buena opción a la hora de elegir una plataforma para la gestión de la red es openNMS, un software libre implementado totalmente en el lenguaje Java que cumple con las características antes mencionadas y que permitiría un ahorro a la hora del licenciamiento, con grandes opciones a la hora de escalar la arquitectura de la red.

6. METODOLOGÍA

Para el desarrollo de este proyecto se utilizará la metodología Top Down Network Design, la cual propone cuatro fases, de las cuales se tomarán tres para el diseño de la red, las cuales son:

6.1 Fase I: Analizar requisitos

En la Primera fase se deben identificar y evaluar los problemas existentes en la red de Wi-Fi de la Universidad de los Llanos, campus Barcelona. Para poder analizar los requisitos se debe:

- Hacer entrevistas con usuarios y personal técnico.
- Conocer las características de la red existente (Topología lógica y física, el rendimiento actual), lo que conlleva a realizar un levantamiento de requerimientos con visitas a cada una de las oficinas de las diferentes facultades , identificando los puntos de acceso con que cuenta el campus universitario.
- Caracterizar el tráfico de la red (Flujos y carga de tráfico, comportamiento de los protocolos).
- Identificar los puertos y direccionamiento IP actual de la red no segmentada, en el dispositivo (switch) que funciona actualmente en la Oficina de Sistemas.
- Identificar aquellos servicios comunes, utilizados por las diferentes facultades del campus a tener en cuenta para el diseño de la segmentación de la red.

6.2 Fase II: Diseño de la red

En esta fase se diseñará la topología de red, el direccionamiento IP y la segmentación usando VLANs; así como también se hará el plan de frecuencias y se definirá las potencias de funcionamiento correspondientes a los puntos de acceso Wi-Fi.

6.3 Fase III: Fase de implementación, prueba, optimización y documentación del diseño de la red.

En esta fase se intervendrán los puntos de acceso de la red, según el diseño establecido; como resultado de la identificación de requerimientos. Se realizarán pruebas de rendimiento de la red por medio de una plataforma de gestión basada

en el protocolo SNMP realizando pruebas de servidor, análisis y monitoreo de la red, aplicando las correcciones necesarias para lograr tiempos de latencia aceptables en la red. Finalmente se procederá a documentar el diseño de la red y a capacitar al personal técnico el cual quedará encargado del mantenimiento de la red. [7]

7. DESARROLLO DE LA PASANTÍA

7.1 Fase I: Analizar requisitos

En esta fase se llevaron a cabo tareas en dos frentes importantes, como fueron la encuesta a los estudiantes y la identificación de las características de la red existente, tanto física (dispositivos) como lógica (direccionamiento IP).

7.1.1 Identificación necesidades usuarios

En la primera tarea, referente a la encuesta aplicada a los estudiantes, esta permitió conocer tres aspectos fundamentales de estos como usuarios de la red, los cuales son:

1. Zonas o puntos de conexión dentro del campus Barcelona, frecuentados y donde hace falta cobertura.
2. Servicios utilizados ya sean de aplicaciones o sitios web, tanto académicos como de ocio.
3. Tipos de dispositivos usados (smartphones o computadores) para el acceso a los servicios de red dentro del campus

Para esto se diseñó un formato de encuesta (ver Figura 12, 13, 14 y 15) que permitió obtener la información de los aspectos ya mencionados anteriormente. Este formato fue socializado con los representantes de los estudiantes, los cuales propusieron que fuera llevado a formato digital, para facilitar la aplicación de la misma. La Oficina de Sistemas se encargó de publicarla en la página web de la Universidad, utilizando para ello la herramienta Google Forms y los representantes estudiantiles mediante redes sociales hicieron difusión a la comunidad estudiantil. La encuesta estuvo disponible durante alrededor de un

mes, buscando obtener una participación lo más significativa posible por parte de los estudiantes.

	UNIVERSIDAD DE LOS LLANOS Reestructuración De La Red Wi-Fi De La Universidad De Los Llanos
---	---

Con el fin de conocer las necesidades de los estudiantes respecto al servicio de la red Wi-Fi, requerimos de su colaboración respondiendo la siguiente encuesta.

Programa académico al que pertenece: _____

1. ¿Qué aplicaciones y/o páginas web utiliza con frecuencia en las instalaciones de la universidad?

Redes Sociales en general:	Redes Sociales de audio y/o video:	Correo Electrónico:	Plataformas Educativas:
☐ Facebook	☐ YouTube	☐ Gmail	☐ EDX, Coursera, Udemmy (Tipo MOOC)
☐ Whatsapp	☐ Spotify	☐ Outlook	☐ Sena SofiaPlus
☐ Messenger	☐ Netflix	☐ Yahoo	☐ Virtual Unillanos
☐ Instagram			☐ Duolingo
☐ Twitter			

Otras: _____

2. De acuerdo a los espacios académicos correspondientes a su programa, ¿Cuáles son aquellos que más frecuentan los estudiantes y que considera deberían tener cobertura de red Wi-Fi?

Respuesta:

3. ¿En qué otras zonas, considera usted que se hace necesario la cobertura de Wi-Fi?

Respuesta: _____

4. ¿Qué dispositivos electrónicos utiliza para conectarse a la red Wi-Fi?

☐ Computador Portátil | Cantidad: ____ ☐ Smartphone | Cantidad: ____

Figura 12. Formato de encuesta aplicada a los estudiantes.

A continuación algunas capturas de la encuesta publicada mediante Google Forms, en el sitio web de la Universidad.

Reestructuración de la red Wi-Fi de la Universidad de los Llanos

Con el fin de conocer las necesidades de los estudiantes respecto al servicio de la red Wi-Fi, requerimos de su colaboración respondiendo la siguiente encuesta.

Your username will be recorded when you submit this form.

*Required



1. Programa académico al que pertenece *

Mark only one oval.

- ☐ Ingeniería Agronómica
- ☐ Licenciatura en Educación Infantil
- ☐ Medicina Veterinaria y Zootecnia
- ☐ Ingeniería Agroindustrial
- ☐ Economía
- ☐ Biología
- ☐ Ingeniería de Sistemas
- ☐ Ingeniería Electrónica
- ☐ Administración de Empresas
- ☐ Contaduría Pública
- ☐ Enfermería
- ☐ Licenciatura en Matemáticas
- ☐ Licenciatura en Educación Física y Deporte
- ☐ Mercadeo
- ☐ Licenciatura en Producción Agropecuaria

Figura 13. Sección 1, formato de encuesta Google Forms.

1. ¿Que aplicaciones y/o paginas web utiliza con frecuencia en las instalaciones de la universidad?

2. Redes sociales en general: *
Tick all that apply.

- ☐ Facebook
- ☐ Whatsapp
- ☐ Messenger
- ☐ Instagram
- ☐ Twitter

3. Redes sociales de audio y/o video *
Tick all that apply.

- ☐ Youtube
- ☐ Spotify
- ☐ Netflix

4. Correo Electrónico *
Tick all that apply.

- ☐ Gmail
- ☐ Outlook
- ☐ Yahoo

5. Plataformas educativas *
Tick all that apply.

- ☐ EDX, Coursera, Udemy (Tipo MOOC)
- ☐ Sena SofiaPlus
- ☐ Virtual Unillanos
- ☐ Duolingo

6. Otras

Figura 14. Sección 2, formato de encuesta Google Forms.

Sección sin título

7. 2. De acuerdo a los espacios académicos correspondientes a su programa, ¿Cuales son aquellos que mas frecuentan los estudiantes y que consideran deberían tener cobertura de red Wi-Fi? *

3. ¿En que zonas, considera usted que se hace necesaria la cobertura de Wi-Fi?

8.

9. 4. ¿Que dispositivos electrónicos utiliza para conectarse a la red Wi-Fi? *

Mark only one oval.

☐ Computador Portátil

☐ Smartphone

☐ Ambos

10. Cuales son las marcas y modelos de los dispositivos que utiliza para conectarse a la red Wi-Fi *

Powered by

 Google Forms

Figura 15. Sección 3, formato de encuesta Google Forms.

7.1.2 Identificación características técnicas red existente

En la segunda tarea, referente a la identificación de las características de la red existente; se realizaron visitas a cada una de las oficinas y dependencias dentro del campus, para realizar un levantamiento de información de los dispositivos de acceso inalámbrico AP (Access Points) y de conmutación de paquetes (Switches). Para ello se diseñó un formato con los siguientes campos relevantes de AP (ver Figura 16):

- Marca
- Modelo
- Versión
- Serial
- Número Antenas
- SSID (Nombre de la Red)
- Canal de Frecuencia
- Ubicación

A continuación se puede observar el formato utilizado para los AP.

REESTRUCTURACIÓN DE LA RED WI-FI DE LA UNIVERSIDAD DE LOS LLANOS FORMATO DE IDENTIFICACIÓN CARACTERÍSTICAS TÉCNICAS ACCESS POINTS									
N°	Fecha	Marca	Modelo	Ver.	Serial	# Ant.	SSID	Canal Frec.	Ubicación
1									
2									
3									
4									
5									
6									
7									

Figura 16. Formato de recolección de información routers..
Fuente: Los autores.

En el caso de los dispositivos de conmutación de paquetes (switches), se hizo el previo levantamiento de información y a su vez también se diseñó un formato con los siguientes campos:

- Marca
- Modelo
- Número de puertos
- Sistema Operativo
- Ubicación
- Tipo de Switch
- Rack (Ubicación)

Esto permitió contabilizar e identificar aspectos técnicos a tener en cuenta para tareas posteriores, principalmente el cambio de firmware en los AP y en los Switches para conocer la forma de gestión y soporte de Virtual LAN (VLAN) (ver Figura 17).

A continuación se puede observar el formato utilizado para los Switches.

UNIVERSIDAD DE LOS LLANOS		REESTRUCTURACIÓN DE LA RED WI-FI DE LA UNIVERSIDAD DE LOS LLANOS FORMATO DE IDENTIFICACIÓN CARACTERÍSTICAS TÉCNICAS SWITCHES						
N°	N° Rack	Fecha	Marca	Modelo	N° Puertos	Sistema Operativo	Ubicación	Estado ☐
1								
2								
3								
4								
5								
6								
7								

Figura 17. Formato de recolección de información switches.

Fuente: Los autores

Finalmente se llevaron a cabo reuniones con el personal encargado de la Oficina de Sistemas, quienes explicaron y proporcionaron documentación del direccionamiento IP de la red y su distribución en las diferentes dependencias del campus. Se logró determinar lo siguiente:

Direccionamiento IP Encontrado Campus Barcelona				
Red	Máscara	Rango Asignable		Broadcast
		Inicial	Final	
172.17.0.0	255.255.0.0	172.17.0.1	172.17.255.254	172.17.255.255

Tabla 1. Descripción de direccionamiento IP campus Barcelona.

Como se puede observar en la Tabla 1, se usaba una dirección IP clase B. La red local funcionaba bajo un único segmento, el cual contenía y compartía entre todos los equipos el mismo dominio de *Broadcast*; lo que generaba mayor congestión de la red y problemas de seguridad, con un riesgo muy alto en el caso de que un usuario malintencionado con conocimientos, generarse un ataque a la infraestructura de red, servidores, equipos de otros usuarios; llegando a ocasionar una denegación de servicios que afecte el funcionamiento de la Universidad.

Un caso particular lo puede encontrar en el **Anexo 13.1** al final de este libro, dónde se puede entender como un equipo mal conectado, perteneciente a una red no segmentada, como era el caso en el campus Barcelona, llega a generar una afectación grave en la prestación del servicio de Internet en las oficinas y dependencias.

Para los rangos asignados de direcciones **IPs** de la red clase B mencionada con anterioridad, se encontró que se seguía la siguiente convención para cada una de las dependencias de la Universidad:

- Routers: tienen reservado desde la IP **1** hasta la **5** inclusive.
- Impresoras: tienen reservado desde la IP **6** hasta la **10** inclusive.
- Equipos de cómputo: tienen reservadas direcciones a partir de la IP **11**.

7.2 Fase II: Diseño de la red

En esta segunda fase se realizaron las actividades correspondientes a la reestructuración lógica de la red Wi-Fi actual y las configuraciones correctas que debe tener una red teniendo en cuenta las buenas prácticas de configuración del Wi-Fi en la banda 2.4 GHz.

7.2.1 Diseño lógico de la red

7.2.1.1 Direccionamiento IP

Primeramente se realizó el diseño del nuevo esquema de direccionamiento IP y la segmentación por VLANs de la red de la Universidad de los Llanos, campus Barcelona, mejorando así la seguridad y el flujo de tráfico a través de la misma. En el nuevo esquema de direccionamiento se utilizó una red clase A: **10.X.X.X /12** para las dependencias y oficinas del campus. Esta se dividió en subredes mediante el siguiente proceso:

Se tomaron **7 bits** más para subred y los **13 bits** restantes asignados para hosts. De esta manera se obtuvo el número de subredes y la cantidad de equipos en total por cada subred.

$$2^7 = 128 \text{ Subredes.} \qquad 2^{13} - 2 = 8190 \text{ Hosts.}$$

Entonces finalmente se pasó de una red con máscara de subred **/12** a una con máscara de subred **/19**. Al tener disponibilidad de **128** subredes, se seleccionaron algunas para operar sobre una VLAN asignada. Por otro lado se conservó algo de la red clase B: **172.17.0.0 /16** usando la VLAN 2, permitiendo la comunicación entre el switch capa 3 y el equipo del proveedor de internet que da salida a Internet a través de la IP pública **190.X.X.X**. Además se estableció inicialmente, dejar los servidores que se encuentran ubicados en la Oficina de Sistemas, sobre la red antigua, para evitar cualquier tipo de inconveniente durante la transición hacia el nuevo esquema de direccionamiento (ver Figura 18).

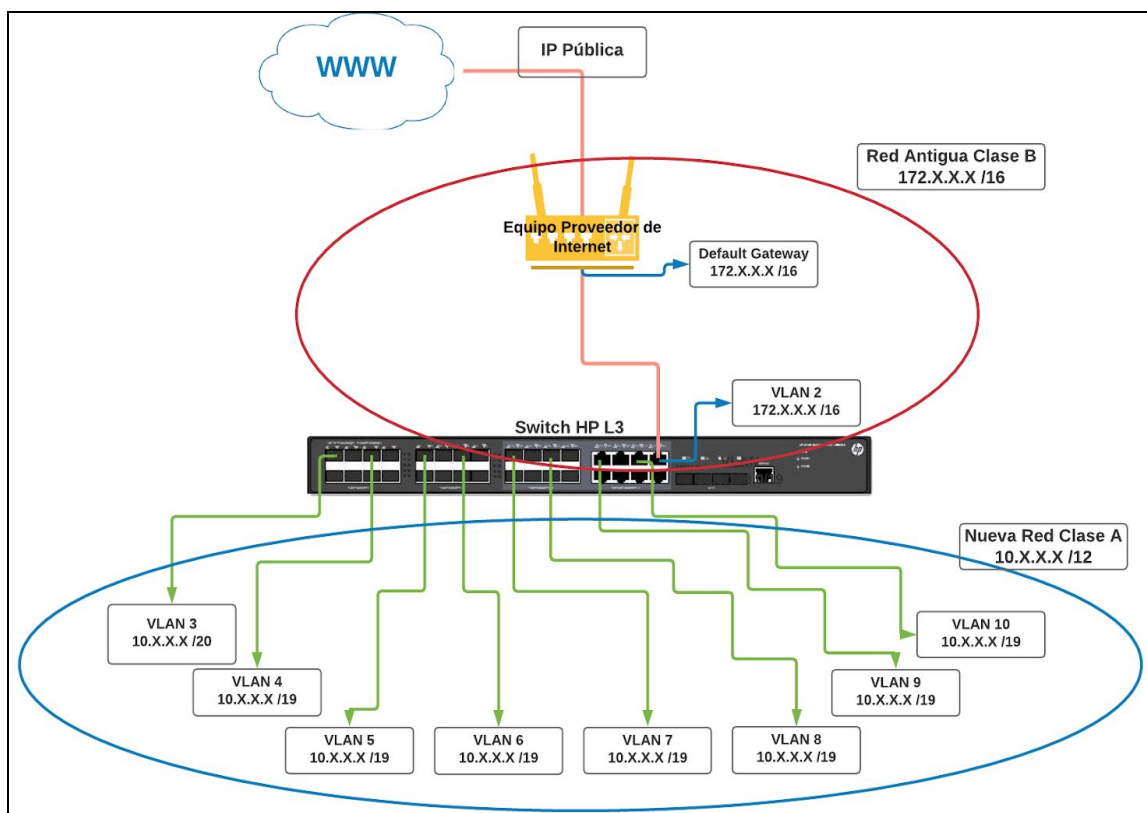


Figura 18. Esquema general del nuevo direccionamiento IP, para el campus Barcelona.

7.2.1.2 Segmentación de la red en VLANs

Como parte de la fase de diseño se proyectó también la asignación de las diferentes VLANs a cada una de las dependencias del campus Barcelona. Puede observarse en la siguiente tabla la distribución de las mismas.

VLAN ID	DEPENDENCIAS
---------	--------------

VLAN # 1	VLAN de administración switches.
VLAN # 2	VLAN de respaldo y comunicación, antiguo esquema de direccionamiento IP.
VLAN # 3	VLAN de servidores.
VLAN # 30	VLAN puntos de acceso campus, plataforma Aruba .
VLAN # 4	Torre Administrativa.
VLAN # 5	Auditorio IALL.
VLAN # 6	Zona Rack Agronomía.
VLAN # 7	Zona Bienestar Institucional.
VLAN # 8	IALL - Granja
VLAN # 9	FCBI (Facultad de Ciencias Básicas e Ingeniería)
VLAN # 10	FCH (Facultad de Ciencias Humanas)
VLAN # 11	Edif. Leonardo Da Vinci
VLAN # 12	Coliseo.
VLAN # 13	IDEAD.
VLAN # 14	Electrónica.
VLAN # 15	Zona FCARN, Agroforestería, Counillanos.
VLAN # 16	Zona Matemáticas y Clínica Veterinaria.
VLAN # 17	Sede de Posgrados.

Tabla 2. Distribución de VLANs por dependencia campus Barcelona.

A continuación también se puede observar la distribución de las VLANs en el plano en perspectiva del campus Barcelona (ver Figura 19).

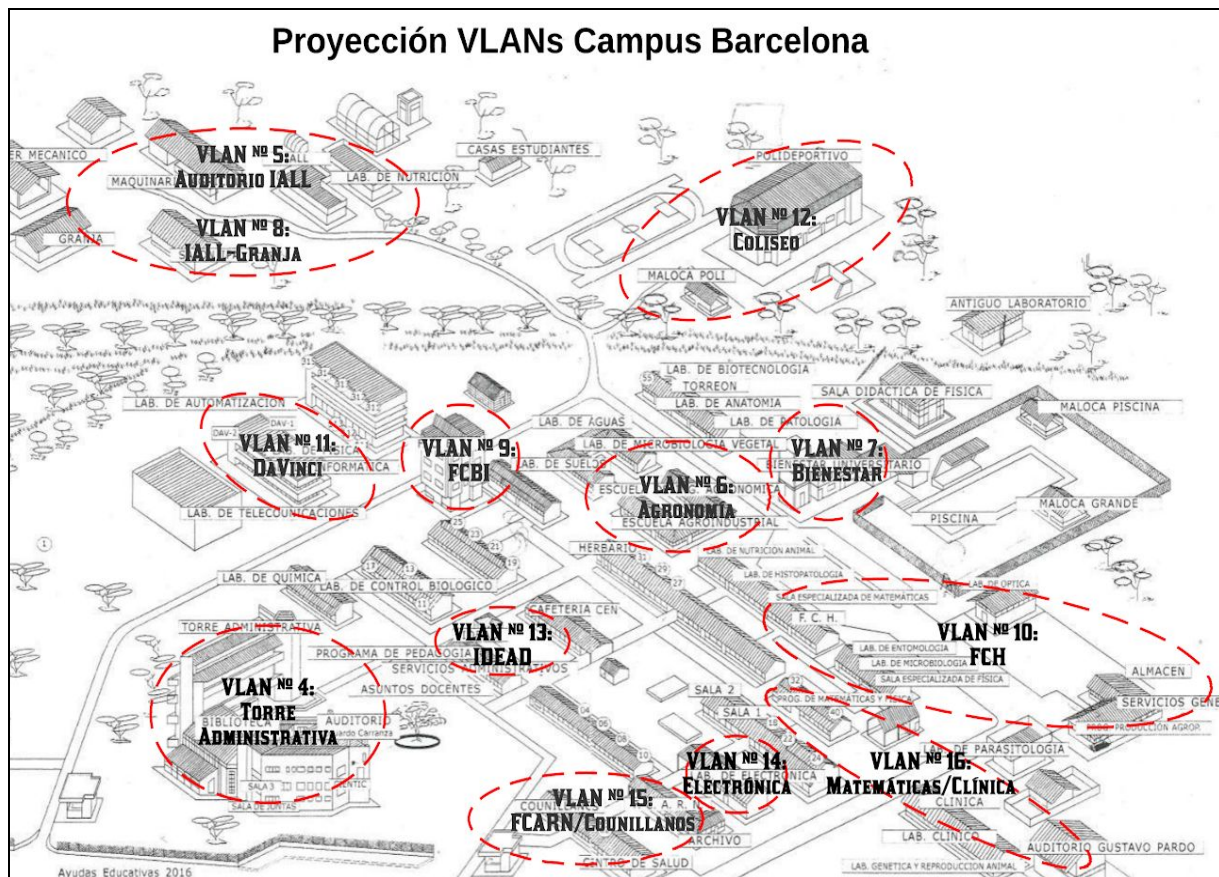


Figura 19. Distribución de VLANs proyectadas a implementar en el campus Barcelona.

Fuente: Los autores

En la **sección 8.6** de resultados, podrá encontrar la información correspondiente a las VLANs que se lograron implementar, dentro de las fechas de ejecución del proyecto.

7.2.2 Plan de frecuencias y potencias de los dispositivos de red Wi-Fi

Se realizó un plan de frecuencias y potencias, tomando en cuenta la ubicación de los diferentes dispositivos de red Wi-Fi en el campus Barcelona, con el fin de que los canales no se interfirieran entre sí, puesto que en la banda 2.4 GHz la más usual en la que operan los dispositivos inalámbricos del campus, dispone de 14

canales de los cuales en Colombia se usan únicamente 11, en donde solo el 1, 6 y 11 no se solapan.

Dentro del plan de frecuencias mencionado anteriormente, se incluyeron todos los puntos de acceso ubicados en las oficinas y dependencias del campus; como también aquellos externos que brindan el acceso a los estudiantes, los cuales pertenecen a la marca **HP Aruba** siendo estos últimos los únicos dispositivos que soportaban doble banda (2.4 GHz y 5 GHz).

7.2.2.1 Plan elaborado puntos de acceso oficinas

A continuación se puede observar en las siguientes tablas 3, 4 y figura 19, la planificación de las frecuencias y potencias para los puntos de acceso ubicados en las oficinas y dependencias del campus Barcelona. En este caso se han tomado dos zonas específicas como ejemplo, para describir el patrón de distribución usado, que evite la interferencia entre canales vecinos y que fue aplicado en todas las dependencias visitadas durante el desarrollo del proyecto; esto con el fin de facilitar la visualización de los datos, debido a la gran cantidad de routers que se encontraron en el campus, lo que dificulta su presentación dentro de una imagen en este documento.

7.2.2.1.1 Plan Zona Determinada Coliseo

ID	Marca	Canal	Potencia
55	CISCO	1	10 mW 10 dBm
56	CISCO	1	10 mW 10 dBm
57	CISCO	11	10 mW 10 dBm
79	CISCO	6	10 mW 10 dBm

Tabla 3. Frecuencias y potencias, diseñadas para puntos de acceso ubicados en oficinas Coliseo.

En la Figura 20, podrá encontrar la ubicación de los dispositivos de la tabla anterior, tomando como referencia su ID.

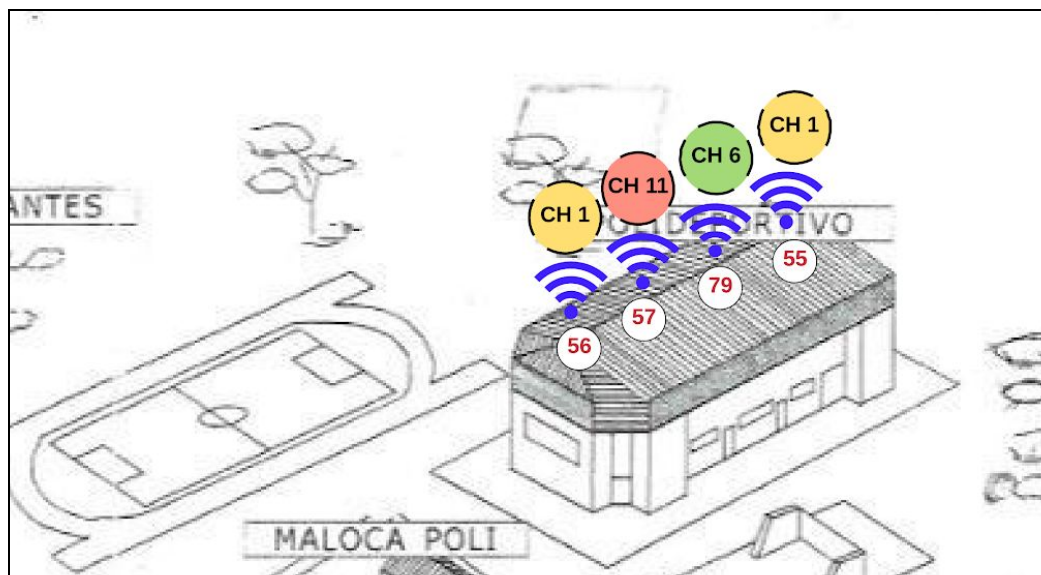


Figura 20. Plan de frecuencias en routers zona Coliseo.
Fuente: Los autores.

7.2.2.1.2 Plan zona determinada edificios Einstein, Da Vinci y Bunker

ID	Marca	Canal	Potencia
1	TP-LINK	6	50 %
2	CISCO	1	15 mW
3	D-Link	11	Low
4	TP-LINK	1	50 %
5	TP-LINK	6	
6	Linksys	6	10 mW
7	TP-LINK	11	Low
58	QPCOM	1	

Tabla 4. Frecuencias y potencias, diseñadas para puntos de acceso ubicados en oficinas Edificios Einstein, Da Vinci y Bunker.

En la Figura 21, podrá encontrar la ubicación de los dispositivos de la tabla anterior, tomando como referencia su ID.

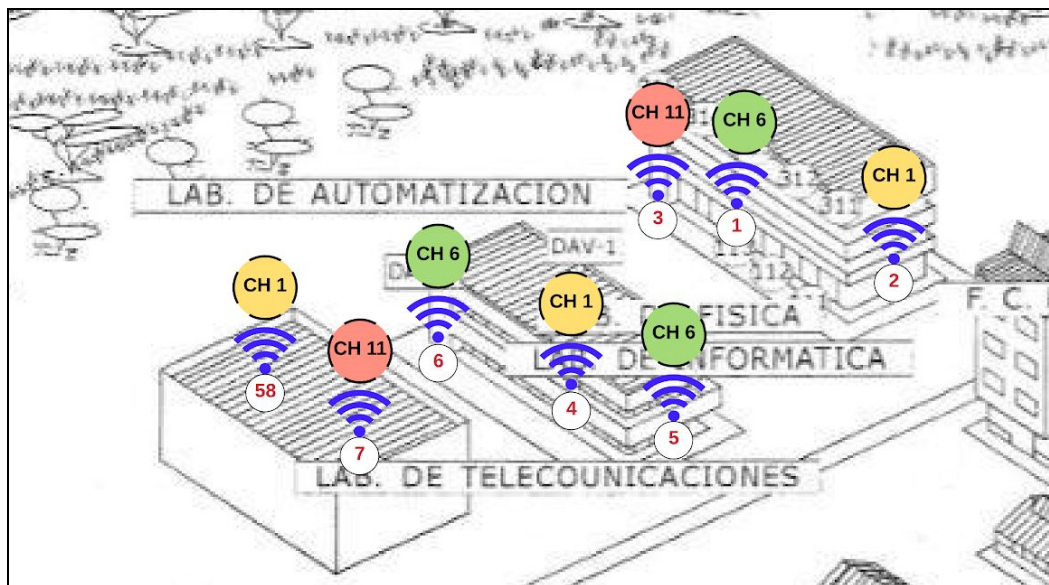


Figura 21. Plan de frecuencias en routers zona Einstein/Da Vinci.
Fuente: Los autores.

7.2.2.2 Plan elaborado puntos de acceso HP ARUBA

A continuación se puede observar en la tabla 5, la planificación de las frecuencias y potencias para los puntos de acceso de los estudiantes (**HP Aruba**).

ID	Nombre AP	Modelo	Tipo	Canal Potencia (dBm)	
				2.4 GHz	5 GHz
APC1	BIBLIOTECA	275	Outdoor	CH 1 13 dBm	CH 149 18 dBm
APC2	IDEAD	275	Outdoor	CH 11 12 dBm	CH 153 18 dBm
APC3	COOPERATIVA	275	Outdoor	CH 6 13 dBm	CH 157 18 dBm

APC4		275	Outdoor	CH 6	CH 161 18 dBm
APC5		275	Outdoor	CH 1	CH 165 18 dBm
APC6	PLAZA_GARZA	275	Outdoor	CH 1 12 dBm	CH 157 18 dBm
APC7	COLISEO	275	Outdoor	CH 11 18 dBm	CH 149 18 dBm
APC8	LAB_FISIOVEGETAL	205	Indoor	CH 11 5 dBm	CH 36 18 dBm
APC9	LAB_MICROVEGETAL	205	Indoor	CH 6 5 dBm	CH 40 18 dBm
APC10	AULA_315A	205	Indoor	CH 11 5 dBm	CH 40 18 dBm
APC11	AULA_313A	205	Indoor	CH 1 5 dBm	CH 165 18 dBm
APC12	AULA_311A	205	Indoor	CH 6 5 dBm	CH 48 18 dBm
APC13	AULA_113A	205	Indoor	CH 6 5 dBm	CH 36 18 dBm
APC14	AULA_111A	205	Indoor	CH 11 5 dBm	CH 44 18 dBm

Tabla 5. Frecuencias y potencias, diseñadas para puntos de acceso estudiantes.

A continuación en las Figuras 22 y 23 podrá observar la distribución de las frecuencias (canales) en los puntos de acceso de los estudiantes, tanto en la banda de 2.4 GHz como de 5 GHz; de esta manera se logra aplicar una buena práctica en la configuración de las redes Wi-Fi, que mejora el uso del espectro electromagnético principalmente en una banda tan saturada como la de 2.4 GHz.

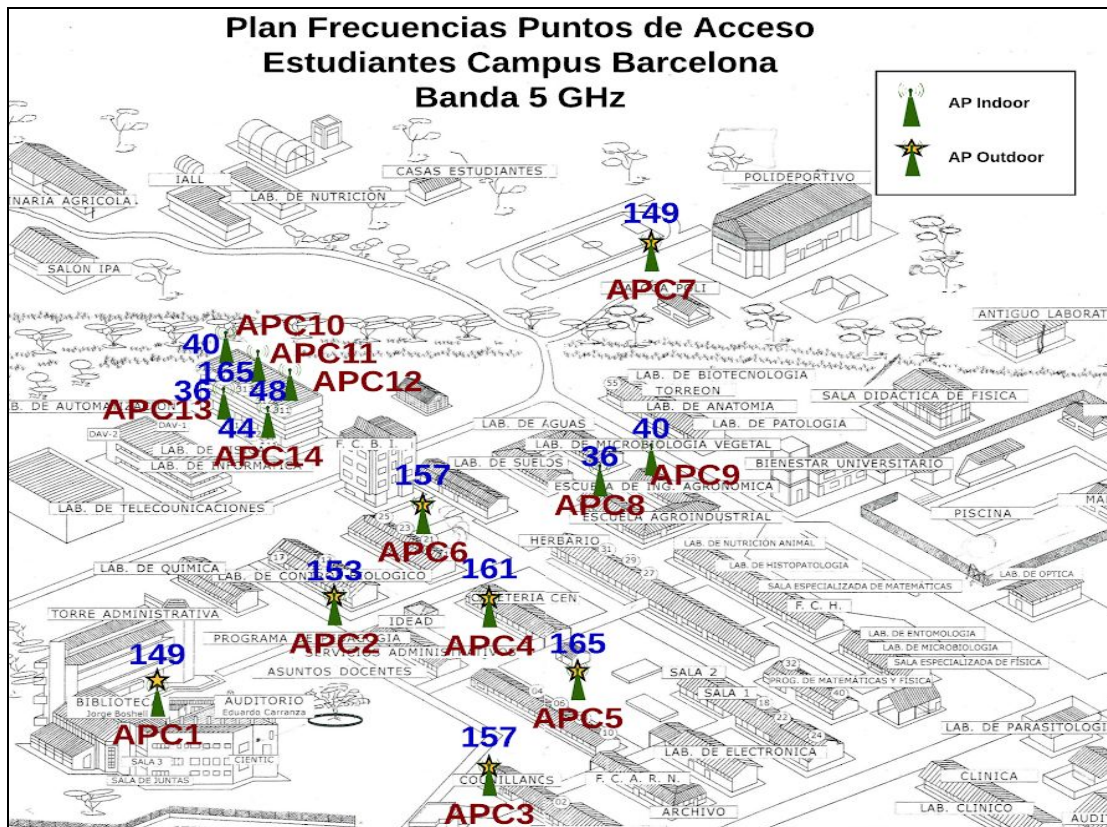


Figura 23. Frecuencias en la banda de 5 GHz puntos de acceso estudiantes, campus Barcelona.
Fuente: Los autores.

7.2.3 Planificación puntos de acceso en nuevas zonas del campus Barcelona

A partir de los resultados de la encuesta realizada, de algunas visitas y diálogo con los estudiantes en las diferentes zonas del campus Barcelona, se lograron identificar aquellas en las cuales se hace necesario cobertura o corregir la ubicación de los puntos de acceso existentes.

Como resultado de la búsqueda de mejorar el acceso de los estudiantes a la red Wi-Fi del campus, se entregó a la Oficina de Sistemas un informe en el cual se establecen las nuevas zonas, ubicación de puntos de acceso y recomendación de las características técnicas, que deben tener los nuevos dispositivos a adquirir por parte de la Universidad, los cuales contribuirían a ofrecer un mejor servicio de Wi-Fi a los estudiantes.

Puede dirigirse a la **sección 8.9** de resultados, allí encontrará las tablas correspondientes a la planificación de las nuevas zonas y la ubicación de dispositivos, igualmente en la **sección 10.1** de recomendaciones, podrá encontrar los aspectos técnicos referentes a las características que deben tener los nuevos equipos para mejorar el servicio de Wi-Fi.

7.3 Fase III: Fase de implementación, prueba, optimización y documentación del diseño de la red.

7.3.1 Implementación

7.3.1.1 Configuración de access points dependencias

Se realizó la configuración de cada uno de los routers y access points de las diferentes oficinas y dependencias de la universidad, con el fin de mejorar significativamente el uso del espectro electromagnético en el campus Barcelona, de las redes Wi-Fi que coexisten en el mismo, a partir de importantes ajustes técnicos como lo son:

- 1. Rango de la potencia:** se configuró de acuerdo al espacio físico de la oficina donde se hacía uso de la red o se proveía el servicio, usando para ello una app móvil de análisis de Wi-Fi llamada Wi-Fi Analyzer, que nos permitió realizar las mediciones de la potencia mínima necesaria para cada espacio.
- 2. Ancho de banda:** se redujo el ancho de banda del canal a 20 Mhz, evitando de esta manera la interferencia hacia otros canales adyacentes.
- 3. Canal de frecuencia:** a partir del plan frecuencias elaborado con anterioridad, se configuró su canal respectivo.
- 4. Cambio de IP:** se les asignó una IP fija y una máscara de red a cada dispositivo de red.
- 5. Administración remota:** se habilitó la administración remota a cada dispositivo.
- 6. Seguridad de acceso:** se modificaron las credenciales de acceso a la configuración de los dispositivos inalámbricos, ya que la mayoría se encontraban con los valores de acceso por defecto.

Para los routers y access points que soportaban el cambio de firmware, se les instaló **DD-WRT** un firmware libre con buena compatibilidad para los dispositivos y un gran soporte por parte de la comunidad de desarrollo, lo que permitió en algunos dispositivos ampliar las opciones de configuración, específicamente en el control de potencia, acceso remoto y ancho de banda; los cuales son limitados por el firmware original del fabricante.

7.3.1.2 Configuración de access points HP Aruba

Al igual que los dispositivos inalámbricos de las diferentes dependencias anteriormente nombrados, se configuraron aspectos técnicos en la totalidad de los access points marca **HP Aruba Serie 270 y Serie 205**, los cuales también hacen parte de la red Wi-Fi de la Universidad y proveen el servicio de internet a los estudiantes del campus Barcelona; las configuraciones modificadas de estos dispositivos se pueden observar a continuación:

- 1. Actualización de firmware:** se actualizó el firmware de cada uno de los dispositivos inalámbricos, al más reciente respecto a su modelo.
- 2. Rango de potencia:** al igual que los dispositivos de red de las dependencias, se ajustó el rango de potencia del Wi-Fi de acuerdo al espacio físico del cual se quisiera cubrir.
- 3. Canal de frecuencia:** los dispositivos **HP Aruba** disponen de la capacidad de doble banda (2.4 GHz - 5 GHz), por lo cual se configuraron los canales de frecuencia de cada una de ellas, con el mismo fin de evitar la interceptación de canales con los dispositivos de red vecinos.

7.3.1.3 Configuración de switches

Se realizaron configuraciones en cada uno de los switches ubicados en los diferentes puntos del campus Barcelona, con el fin de monitorearlos a través de la plataforma de SNMP **LibreNMS**. Los ajustes realizados comprendieron los siguientes aspectos:

- Dirección IP.
- Credenciales de acceso (usuario y contraseña).
- Habilitación del protocolo SNMP

- Localización
- Comunidad
- Configuración de traps
- Versión protocolo SNMP

Se configuraron switches en su mayoría de las marcas **HP**, modelos 1920 y V1910, **3Com** modelos 4900 y 4400 y el switch principal anteriormente mencionado el **HP FlexNetwork 5130**. Esto permitió agregarlos a la plataforma de monitoreo, instalada de manera previa en un servidor de la Oficina de Sistemas, logrando tener un control y acceso al estado de los equipos de manera remota y centralizada.

7.3.1.4 Instalación e implementación de la plataforma LibreNMS

Se instaló la plataforma piloto **LibreNMS** en uno de los servidores de la Oficina de Sistemas sobre el sistema operativo Ubuntu y el servidor web Apache con dirección IP 172.X.X.X, el software trabaja con el sistema de gestión de base de datos **MySQL**, el cual se implementó con el fin de monitorear aspectos técnicos y de red de los diferentes switches de la Universidad de los Llanos, campus Barcelona.

Para hacer uso de la herramienta de monitoreo de red, se agregaron todos los switches por medio de su IP a la plataforma, de esta forma por medio de mensajes SNMP se pudo obtener toda la información de las características técnicas, el rendimiento de la red y el estado activo o inactivo de cada uno de los dispositivos constantemente, con el fin de accionar oportunamente ante cualquier problema que se presente.

7.3.1.5 Implementación diseño de la red

En esta actividad se realizaron las actividades relacionadas a la implementación del nuevo diseño lógico de red, como lo son la segmentación de tráfico por medio de la creación de VLANs en los switches administrables de la red del campus

Barcelona y la reconfiguración del nuevo direccionamiento IP de cada uno de los dispositivos de la red.

7.3.1.5.1 Segmentación de tráfico

Inicialmente se instaló el switch **HP** capa 3 modelo **FlexNetwork 5130** de 24 puertos, el cual se implementó con el fin de segmentar el tráfico de la red, haciendo uso de VLANs. Se configuraron en este 12 de ellas, de las cuales se implementaron 10 de un total de 18 proyectadas en la fase de diseño, esto dado por motivos de escasez de cables de conexión tipo LC. Este switch actúa sobre la capa de distribución de la red, al cual se conectaron 3 cables de fibra óptica, que permiten conectar los switches de la capa de acceso, distribuidos en las diferentes zonas del campus Barcelona.

La implementación del dispositivo mencionado anteriormente, también incluyó el cambio de direcciones IP de los equipos (computadores, routers, impresoras) ubicados en las zonas intervenidas; del antiguo al nuevo esquema de direccionamiento propuesto en la **sección 7.2.1** de la fase de diseño lógico de la red. En la **sección 8.6** de resultados, podrá encontrar la tabla con la información de las VLANs implementadas y el plano en perspectiva con la ubicación de las mismas.

7.3.1.5.2 Direccionamiento IP

Para la implementación de un nuevo direccionamiento IP, inicialmente se le informó y solicitó al proveedor de internet de la Universidad de los Llanos, generar la ruta de salida a internet de la nueva red **10.X.X.X/12** lo que permite que sus subredes también lo accedan. Se reconfiguraron las nuevas IPs de todos los dispositivos interconectados a la red del campus Barcelona de acuerdo a la VLAN que correspondían, como los son equipos de cómputo, impresoras y routers. Por cada segmento de red de las diferentes VLANs se dispusieron de 8190 IPs de las cuales las primeras 100 son IPs fijas y las demás son DHCP.

7.3.2 Pruebas

Para medir la velocidad del tráfico tanto de bajada como de subida, retardo y porcentaje de pérdida de paquetes, sobre los APs (Access Point) ubicados en las diferentes áreas del campus Barcelona; se realizaron pruebas de rendimiento de

manera previa a la aplicación de la configuración, relacionada con el nuevo direccionamiento e inclusión de los dispositivos sobre la VLAN 30; según el plan definido en la etapa anterior de diseño. Estos dispositivos de marca **HP Aruba Serie 270 (Outdoor)** y **205 (Indoor)** brindan el servicio de Wi-Fi a los estudiantes y cuentan con capacidad de doble banda (2.4 GHz - 5 GHz) y son administrados de forma centralizada bajo una plataforma que corre sobre un dispositivo designado como controlador.

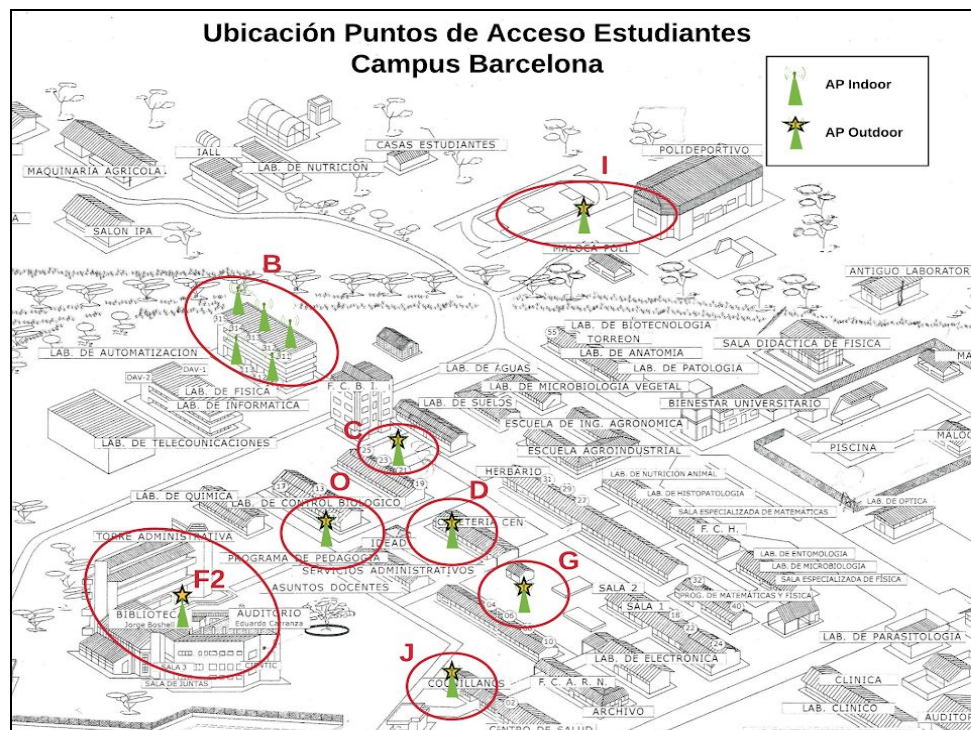


Figura 24. Puntos de acceso estudiantes campus Barcelona.

Fuente: Los autores.

En la la Figura 24 se pueden observar las zonas en las cuales se realizaron las pruebas. Estas se efectuaron simulando el comportamiento normal de un estudiante a la hora de conectarse y se llevaron a cabo durante una semana (entre el 8 y 12 Octubre 2018); excepto para el punto de acceso ubicado cerca del monumento de la Corocora, en frente del edificio FCBI, dado por inconvenientes que el dispositivo presentaba. Se pensaba que estaba quemado, pudo recuperarse luego de una revisión que se hizo más adelante. Se ejecutó una prueba por día procurando el mismo horario y con el dispositivo sobre producción, quiere decir con usuarios (estudiantes) conectados en jornada académica normal.

En la siguiente tabla se describen las zonas en las cuales existía cobertura para los estudiantes con puntos de acceso **HP Aruba** hasta la fecha de la terminación de la pasantía y que puede relacionarse con el mapa presentado anteriormente, usando el identificador de la zona.

Identificador	Nombre Zona	# APs	Tipo AP
B	Edif. Albert Einstein	5	Indoor
C	Plaza Corocora frente FCBI	1	Outdoor
D**	Zona común cafetería Nestea-Comedor universitario	1	Outdoor
F2	Torre administrativa zona verde, frente auditorio	1	Outdoor
G**	Varado	1	Outdoor
I	Coliseo	1	Outdoor
J	Counillanos, zona entrada principal.	1	Outdoor
M	Prog. Agroindustrial Laboratorios	4	Indoor
O	IDEAD, zona externa laboratorios de química.	1	Outdoor

**Fuera de servicio.

Tabla 6. Zonas mapa, cobertura de puntos de acceso estudiantes campus Barcelona.

Las herramientas utilizadas para la realización de las pruebas consistieron claramente en un equipo de cómputo, bajo un sistema operativo Linux Ubuntu y un software para las mediciones de ancho de banda llamado **iPerf 3**, el cual es de uso libre y utiliza un modelo cliente/servidor para las pruebas.

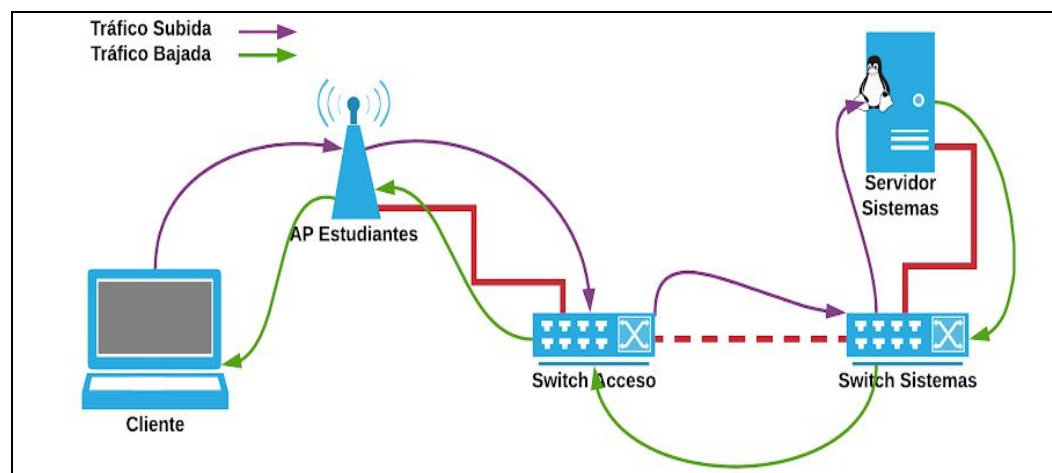


Figura 25. Diagrama funcionamiento *iPerf 3*.
Fuente: Los autores.

Como puede observarse en el diagrama de la Figura 25, además del equipo cliente, se dispuso de un servidor en la Oficina de Sistemas, también corriendo un sistema operativo Linux, sobre el cual se configuró el servicio de **iPerf 3**, mediante un script en bash que permitiera el arranque y ejecución como demonio dentro del sistema.

Finalmente para facilitar la lectura y el almacenamiento de los resultados de las pruebas de rendimiento, se utilizó en el equipo cliente el agente **kentnetmon**, el cual básicamente es un web frontend para **iPerf 3** de uso libre y desarrollado por la *Universidad de Kent*; puede encontrarse en GitHub siguiendo o escribiendo en el navegador el siguiente enlace <https://github.com/IceQubed/kentnetmon>.

En la **sección 8.8** de resultados, podrá encontrar las tablas y gráficas obtenidas de las pruebas realizadas en cada una de las zonas del campus.

8. RESULTADOS

En el desarrollo de la pasantía se llevaron a cabo diferentes actividades de acuerdo a los objetivos planteados inicialmente, estas fueron con anterioridad

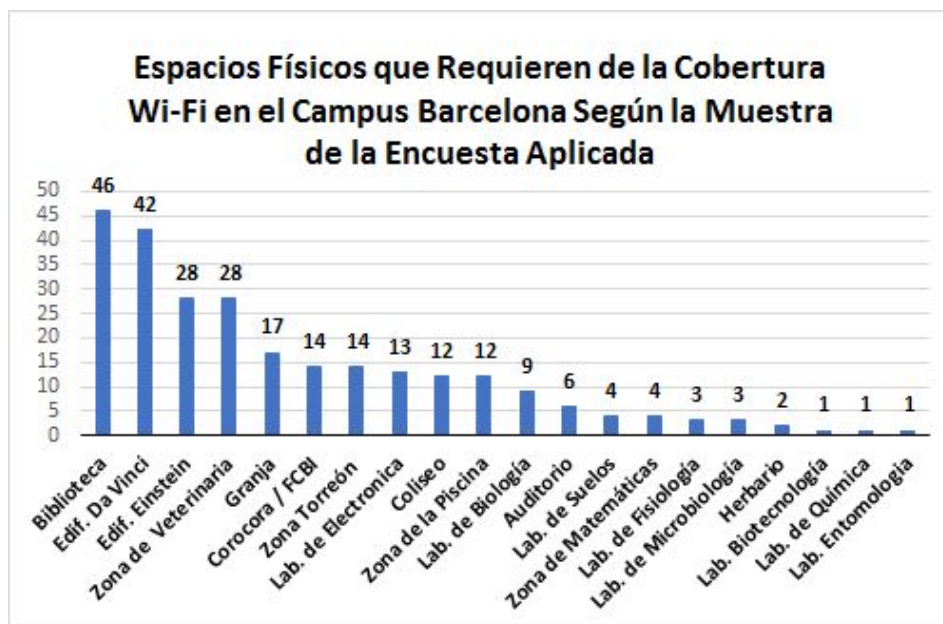
expuestas detalladamente las cuales conllevaron a la obtención de los siguientes resultados:

8.1 Consolidado encuestas

A partir de la encuesta aplicada a la comunidad estudiantil la cual fue mencionada con anterioridad y tuvo un total de participación de **160** estudiantes de todos los programas académicos de la Universidad de los Llanos, se realizaron sus respectivos consolidados y estadísticas de los siguientes aspectos:

8.1.1 Zonas estudiantiles frecuentadas del campus Barcelona, que requieren de cobertura Wi-Fi

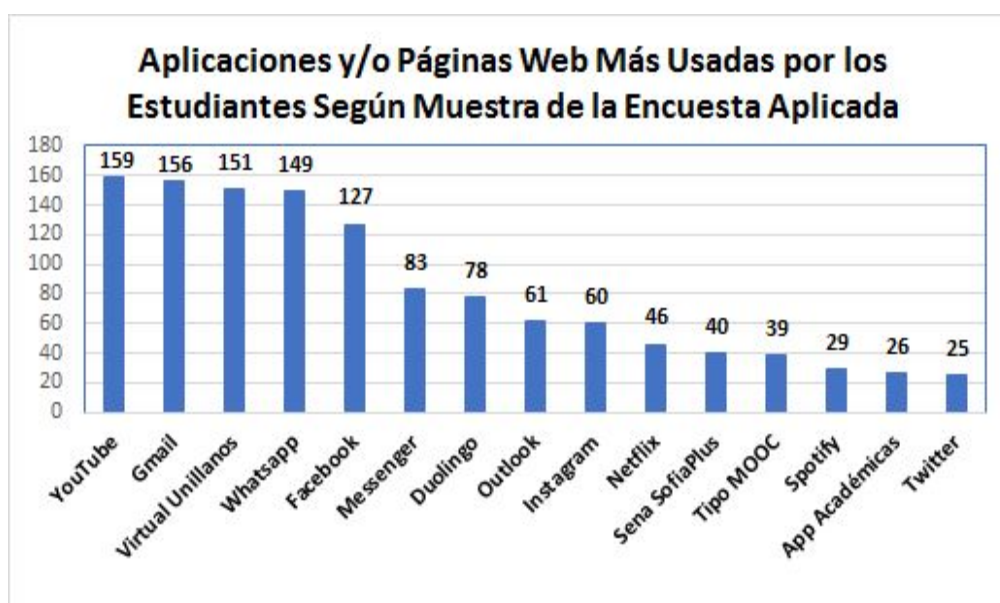
En la Gráfica 1 se pueden observar las diferentes zonas estudiantiles con mayor demanda respecto a las necesidades de cobertura Wi-Fi en la sede Barcelona, como es notorio en la gráfica se puede concluir que la zona con menor cobertura de red según el estudiantado, es la biblioteca, el edificio Da Vinci, la zona de veterinaria y aunque el edificio Einstein actualmente dispone de 5 routers **HP Aruba serie 205** al servicio estudiantil, la opinión de los estudiantes es que en su mayoría de veces, no cubre las zonas verdes de esparcimiento de los mismos u otras zonas cercanas a los salones de clases



Gráfica 1. Representación de zonas que requieren mayor cobertura según estudiantes.

8.1.2 Servicios más utilizados ya sean de aplicaciones o sitios web, tanto académicos como de ocio

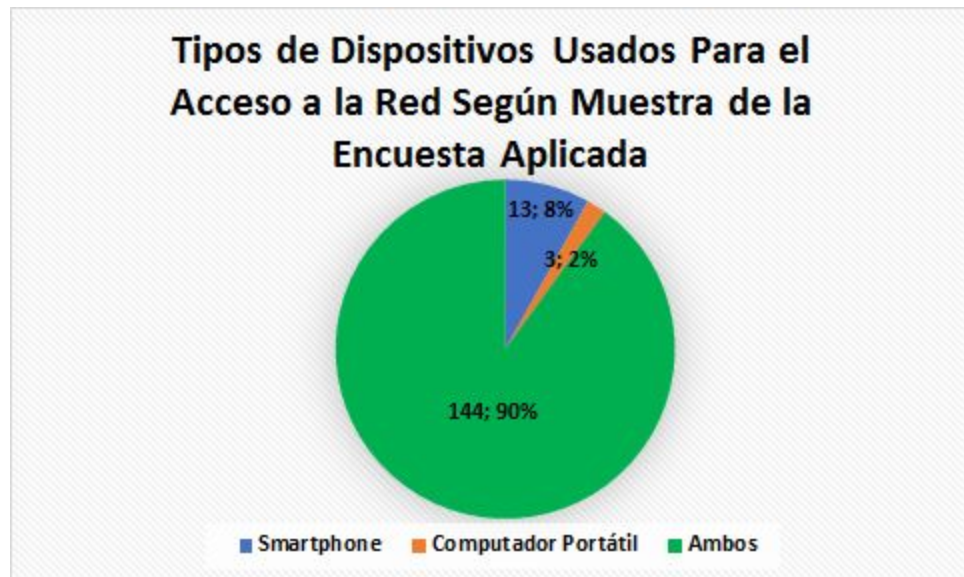
Según los consolidados de la encuesta aplicada con anterioridad, las aplicaciones y/o páginas web más visitadas por los estudiantes en el campus Barcelona, son las redes sociales, como lo son Whatsapp, Facebook y Youtube, al igual que plataformas de correo electrónico como Gmail y plataformas educativas como Virtual Unillanos, estos resultados se pueden apreciar a continuación en la Gráfica 2:



Gráfica 2. Representación de las aplicaciones y/o páginas web más visitadas.

8.1.3 Tipos de dispositivos usados (smartphones o computadores) para el acceso a los servicios de red dentro del campus

A continuación se pueden observar cuales son los porcentajes de los dispositivos más utilizados por los estudiantes para acceder a la red Wi-Fi del campus Barcelona, para un total de **160** respuestas de las cuales el **90%** de los estudiantes usan ambos dispositivos electrónicos, el **8%** solo usa smartphone y el **3%** computador portátil (ver Gráfica 3).



Gráfica 3. Representación del uso de dispositivos para acceder a la red.

8.2 Consolidado Características Routers.

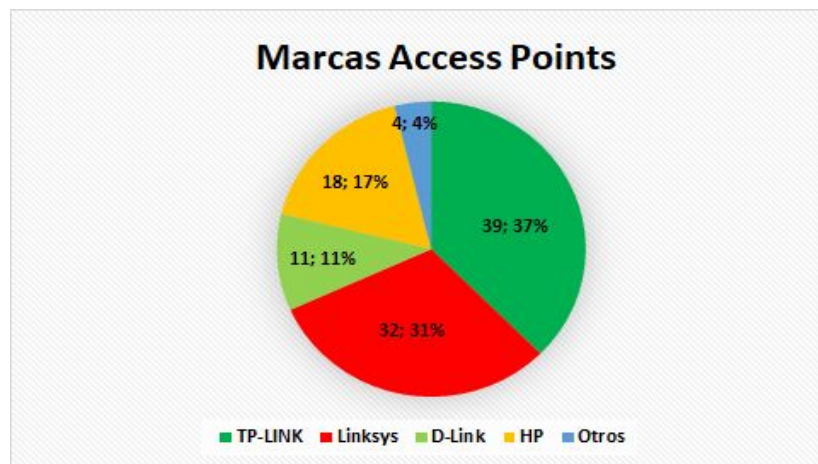
A continuación se presentan una serie de gráficas, que resumen los aspectos importantes tenidos en cuenta, obtenidos de la recolección de información de los access points en las diferentes oficinas y dependencias del campus Barcelona de la Universidad de los Llanos. Estos resultados son:

1. Ecosistema de marcas de dispositivos en la red.
2. Compatibilidad cambio de firmware **DD-WRT**.
3. Soporte de protocolo RADIUS (802.1x)
4. Disponibilidad de antena externa.
5. Estado físico dispositivos.

Se identificaron un total de **113** dispositivos de acceso inalámbrico (Access Points), en todo el campus Barcelona hasta la fecha de la terminación de la pasantía, incluidos **7** de marca **HP Aruba serie 205**, los cuales se excluyeron de las gráficas y tablas; pues estos no serán intervenidos y son controlados por la Oficina de Sistemas de forma remota. De esta manera se tendrá en cuenta un total de **106** dispositivos.

8.2.1 Ecosistema de marcas de dispositivos en la red

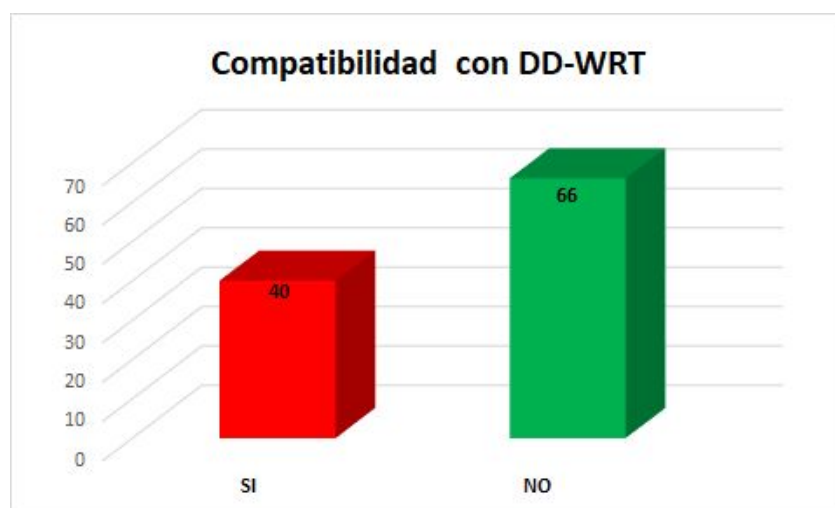
En la siguiente Gráfica 4 se pueden observar las diferentes marcas de los dispositivos de red localizados en las oficinas o dependencia, a su vez se puede apreciar cual marca domina más en el campus Barcelona:



Gráfica 4. Cantidad de dispositivos inalámbricos por marca.

8.2.2 Compatibilidad cambio de firmware DD-WRT

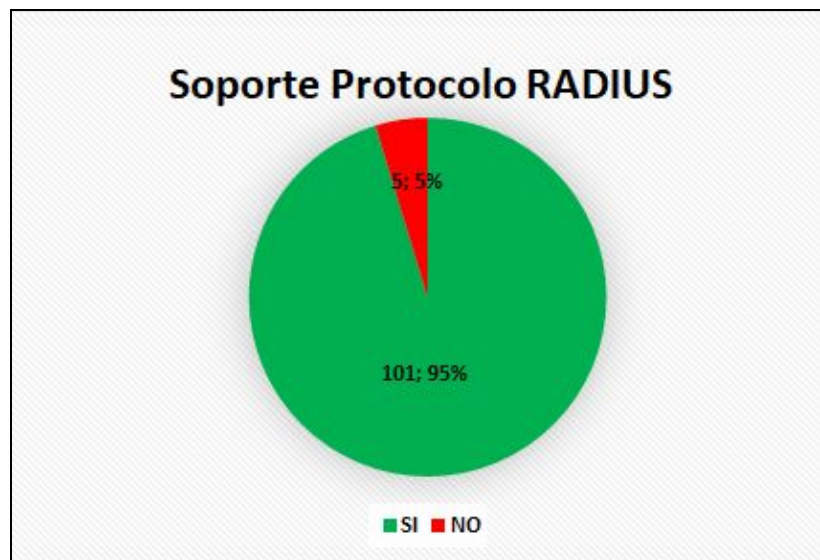
En la Gráfica 5 se puede visualizar la cantidad de access points del campus Barcelona, que son compatibles y que no lo son, con el firmware **DD-WRT**.



Gráfica 5. Representación de la cantidad de dispositivos que soportan **DD-WRT**.

8.2.3 Soporte de protocolo RADIUS (802.1x)

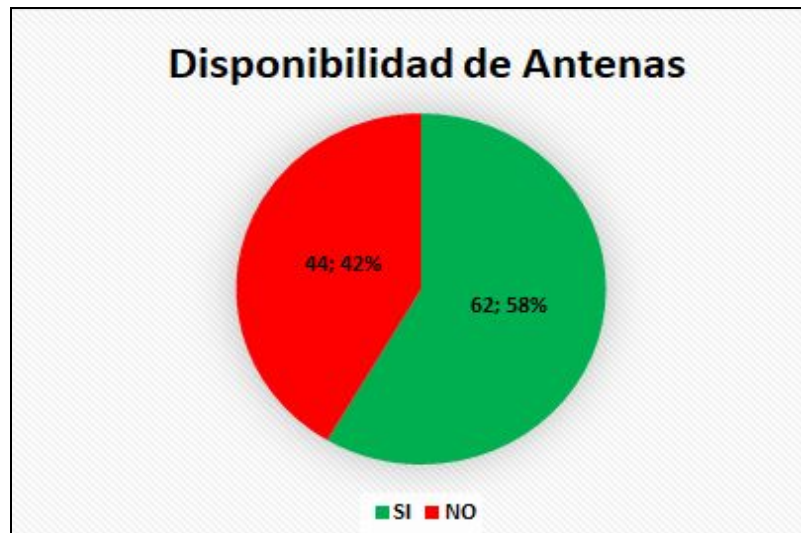
Un importante aspecto a tener en cuenta cuando se realizó el levantamiento de información, era el soporte del protocolo RADIUS en cada uno de los puntos de acceso, en la Gráfica 6 se pueden observar la cantidad de dispositivos que lo soportan y los que no lo hacen:



Gráfica 6. Representación de la cantidad de dispositivos que soportan RADIUS.

8.2.4 Disponibilidad de antena externa

Se tomó en cuenta el aspecto de la disponibilidad de antenas externas en los dispositivos, por motivos de mejor radiación y mejor cobertura que pueden tener los equipos con esta característica. En la Gráfica 7 se puede visualizar la proporción de la disponibilidad de antenas en los dispositivos de red del campus.



Gráfica 7. Representación de los dispositivos que disponen antenas.

8.2.4 Estado físico de dispositivos

Una anotación final y no menos importante que se debe mencionar, es el estado físico de algunos dispositivos de las oficinas o dependencias de la Universidad y Arubas del campus encontrados hasta la fecha de la terminación de la pasantía, que aunque se encontraban funcionando tienen algunas particularidades que requieren atención y son referidos en la siguiente tabla:

Dispositivos de las dependencias del campus Barcelona

Marca	Modelo	Ubicación	Estado Físico
HP M200	RSVLC-1001	Sala Circulación y Préstamo. Piso 1. Edif. Biblioteca	Router de 3 antenas, actualmente cuenta sólo con 2 antenas.
Linksys	WRT54GL	Ofic. Personal Advtvo.	Carcasa del router se encuentra suelta.
D-LINK	DIR-905L	Sala Profesores, Programa LPA	Router de 2 antenas, pero se encontraron partidas.

Tabla 7. Access Points del campus Barcelona en mal estado.

Dispositivos HP Aruba del campus Barcelona

Marca	Modelo	Tipo	Ubicación	Estado Físico
Aruba	Serie 270	Outdoor	Comedor Universitario	Su cable de alimentación se encuentra cortado.
Aruba	Serie 270	Outdoor	Diagonal a la Oficina Estudiantil	El inyector PoE al cual está conectado, no funciona.

Tabla 8. Access Points Aruba del campus Barcelona en mal estado.

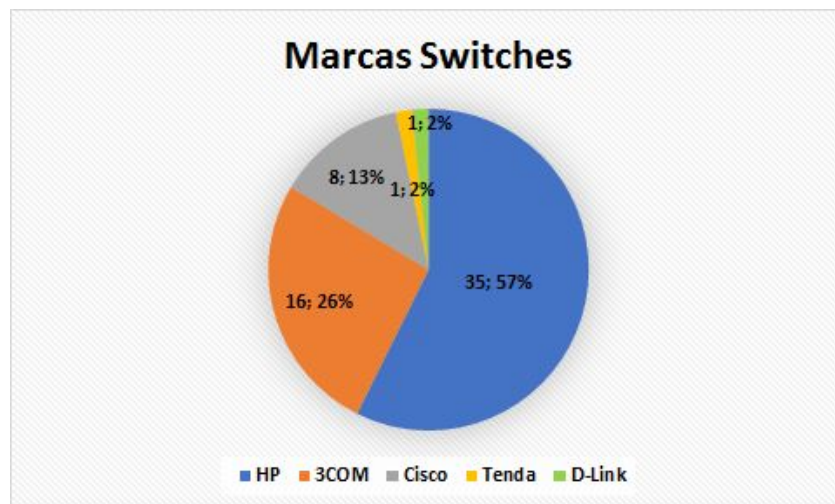
8.3 Consolidado switches

Al igual que los access points, se realizó el levantamiento de información de los Switches que el campus Barcelona disponía hasta la fecha de terminación de la pasantía se identificaron un total de 52 switches, a continuación se puede observar por medio de gráficas los resultados de los siguientes aspectos:

1. Ecosistema de marcas de dispositivos en la red.
2. Disponibilidad de puertos de conexión.
3. Switches Administrables y no administrables

8.3.1 Ecosistema de marcas de dispositivos en la red

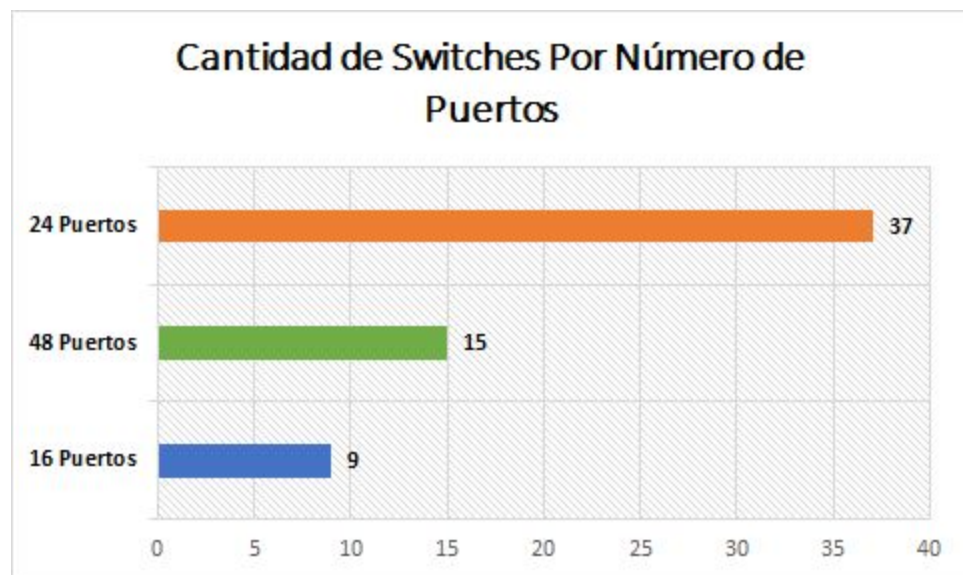
En la Gráfica 8 se puede observar las marcas de switches que predominan en todo el campus Barcelona, con gran notoriedad se puede deducir que su gran mayoría son Switches **HP**.



Gráfica 8. Cantidad de dispositivos inalámbricos por marca.

8.3.2 Cantidad de switches por número de puertos

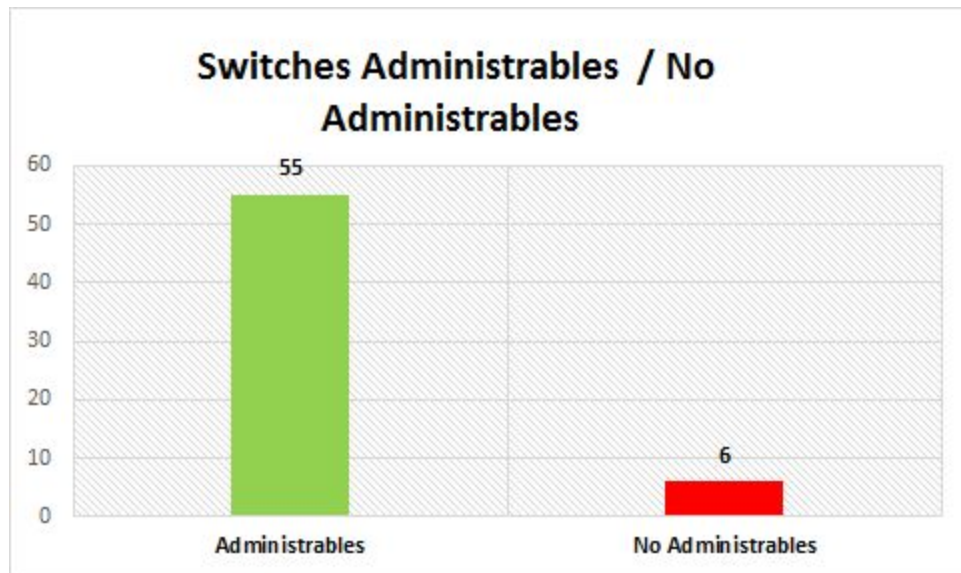
Se realizó un recuento de la disponibilidad de los puertos de conexión de cada uno de los dispositivos de conmutación de paquetes (Switches) en el campus Barcelona, obteniendo así la cantidad de switches por número de puertos disponibles, los cuales se pueden visualizar en la Gráfica 9.



Gráfica 9. Cantidad de Switches por número de puertos en el campus Barcelona.

8.3.3. Switches administrables y no administrables

Una de las características más importantes en el momento de levantar la información de los switches, era el conocer si eran dispositivos administrables o no administrables, puesto que debían ser configurados posteriormente para la implementación de la nueva red, por consiguiente se obtuvo los siguientes resultados (ver Gráfica 10):



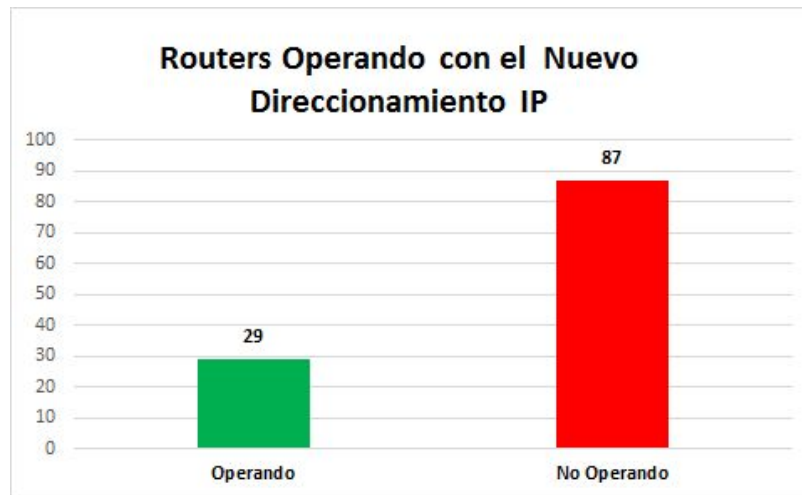
Gráfica 10. Cantidad de switches Administrables/No administrables.

Actualmente en la nueva implementación de red, estos 6 dispositivos no administrables no se han requerido, pues como se ha mencionado anteriormente, por razones externas no se han implementado los nuevos cables de fibra óptica; si llegasen a ser instaladas las fibras, es de carácter urgente realizar el cambio debido de los switches de red que no cumplen con el requerimiento de administración.

8.4 Consolidado configuración

8.4.1 Configuración access points

Se configuraron un total de 29 access points con el nuevo direccionamiento IP, a cada dispositivo se le asignó una IP fija respecto al rango de su correspondiente VLAN, en la Gráfica 11 se pueden observar los resultados anteriormente mencionados.



Gráfica 11. Access points operando en nuevo direccionamiento IP.

8.4.2 Configuración switches

Se obtuvo un total de 63 switches pertenecientes a la Universidad, de los cuales 30 han sido integrados a las VLANs configuradas con anterioridad en la nueva red implementada hasta la fecha de la terminación de la pasantía, por lo tanto estos hacen parte del nuevo direccionamiento IP, al contrario de los switches restantes que aún conservan el direccionamiento antiguo, estos equipos en su mayoría son administrados por la Oficina de Sistemas, en la Figura 26 se pueden observar las ubicaciones de cada uno de los dispositivos en el campus Barcelona (ver gráfica 12).



Gráfica 12. Switches los cuales se les aplicó el nuevo direccionamiento IP.

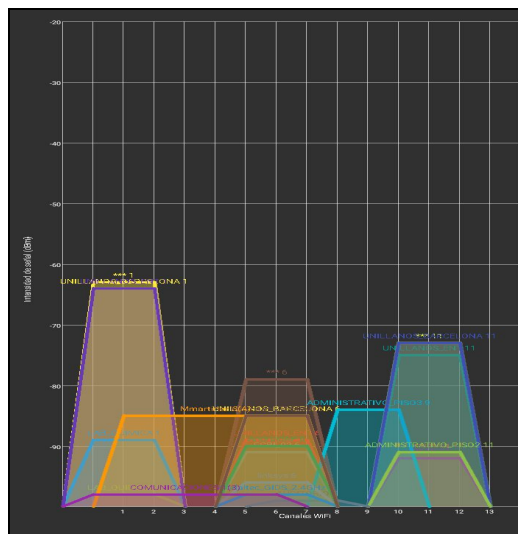
3	HP	1	24	HP	1
4	3COM	1	25	CISCO	1
5	HP	1	26	3COM	1
	3COM	1	27	3COM	1
6	HP	1	28	HP	1
	3COM	1	29	HP	1
7	TENDA	1		3COM	1
8	3COM	1	30		
9	HP	1	32	Cisco	1
10	3COM	1	33	Cisco	1
11	3COM	1	34	HP	1
12	HP	1	35	Cisco	2
	3COM	1	36	HP	1
13	HP	1	37	Cisco	1
14	HP	2	38	Cisco	1
15	HP	3	39	3COM	1
16	D-Link	1	40	HP	2
17	HP	2			

Tabla 9. Cantidad y marcas de switches por rack.

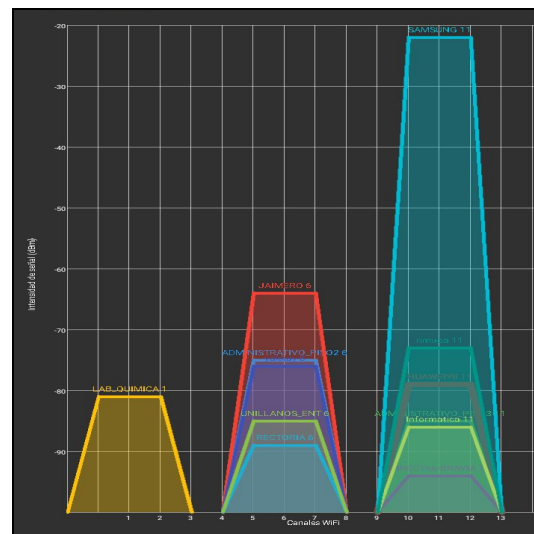
8.5 Frecuencias y potencias de los access points

En las siguientes capturas del espectro se puede observar el estado inicial y final de las redes inalámbricas en las diferentes dependencias u oficinas del campus Barcelona de la Universidad de los Llanos, respecto a sus canales de frecuencia y ancho de banda, en las cuales interfieren redes inalámbricas externas de los domicilios cercanos a la Universidad.

8.5.1 Zona torre administrativa

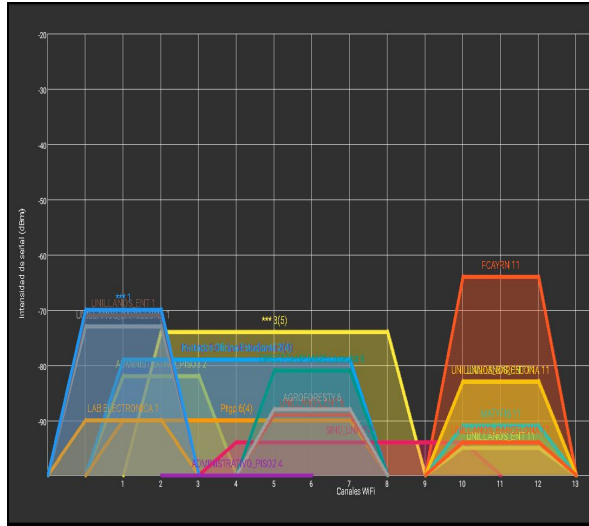


Gráfica 13. Estado inicial, frecuencias redes Wi-Fi torre administrativa.

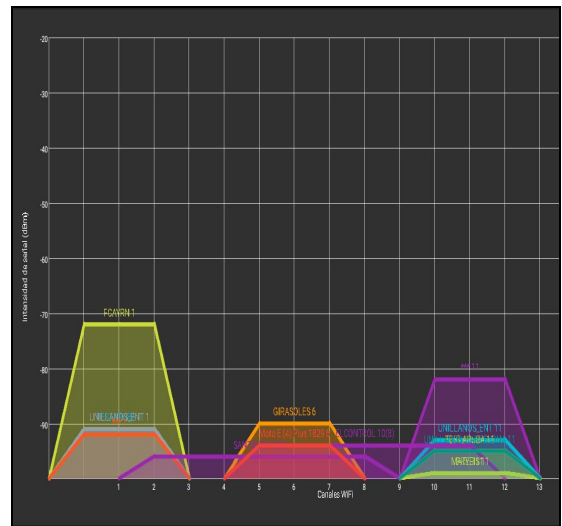


Gráfica 14. Estado final, frecuencias redes Wi-Fi torre administrativa.

8.5.2. Zona de la facultad FCARN

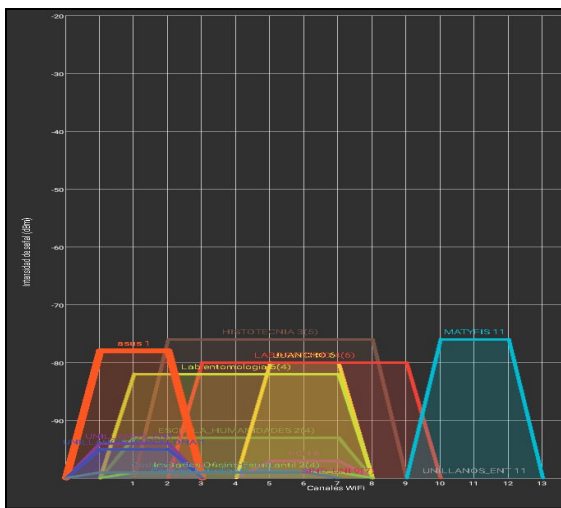


Gráfica 15. Estado inicial, frecuencias redes Wi-Fi facultad FCARN.

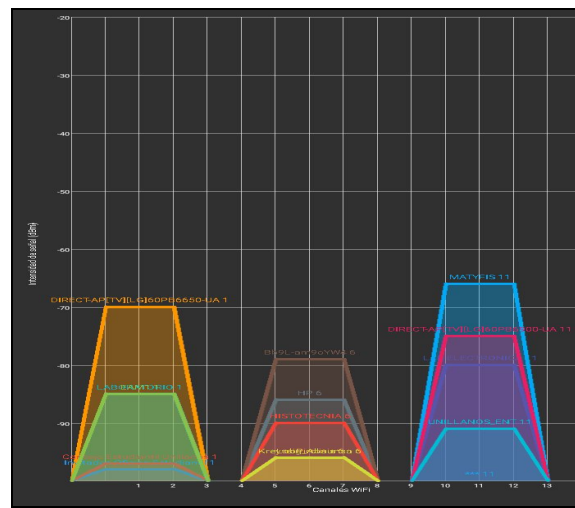


Gráfica 16. Estado final, frecuencias redes Wi-Fi facultad FCARN.

8.5.3. Zona del programa de Matemáticas

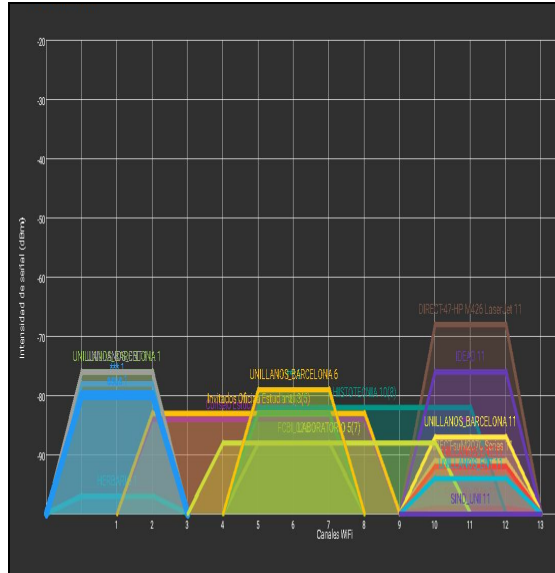


Gráfica 17. Estado inicial, frecuencias redes Wi-Fi programa de matemáticas.

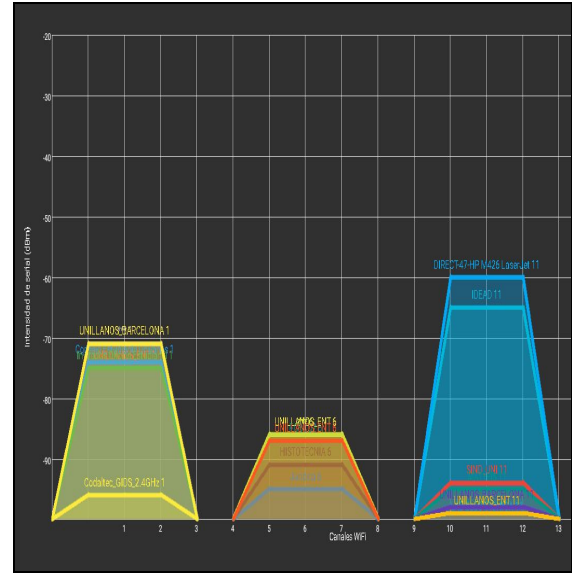


Gráfica 18. Estado final, frecuencias redes Wi-Fi programa de matemáticas.

8.5.4. Zona de la cafetería Nestea

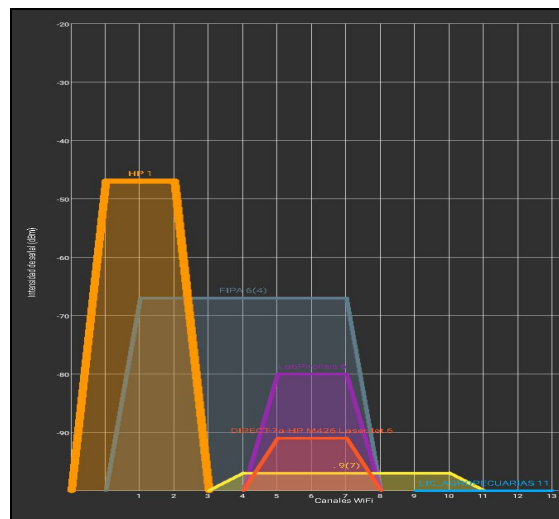


Gráfica 19. Estado inicial, frecuencias redes Wi-Fi cafetería Nестea.

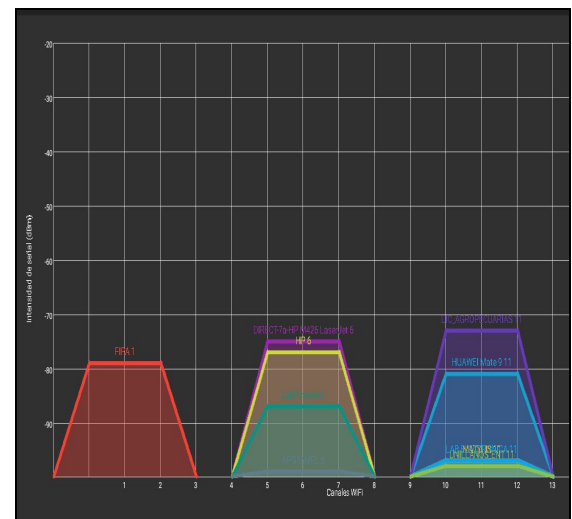


Gráfica 20. Estado final, frecuencias redes Wi-Fi cafetería Nестea.

8.5.5. Zona de la clínica Veterinaria

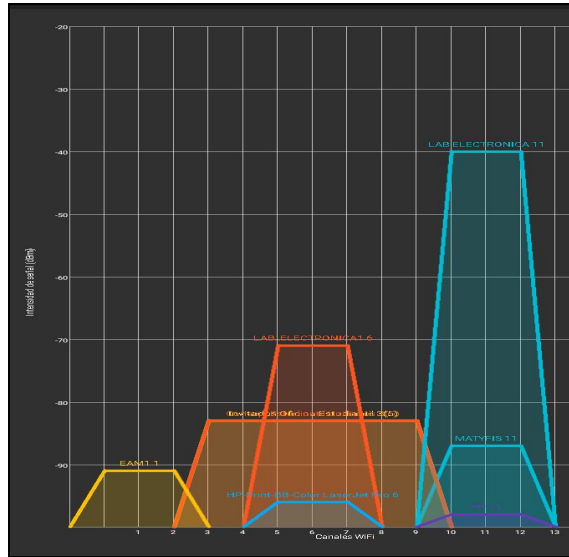


Gráfica 21. Estado inicial, frecuencias redes Wi-Fi clínica veterinaria.

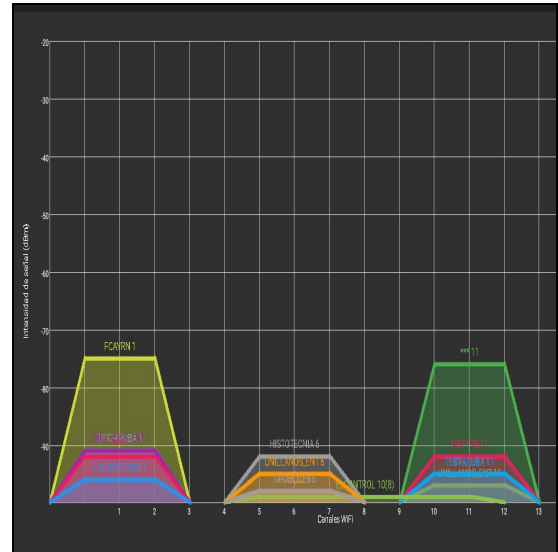


Gráfica 22. Estado final, frecuencias redes Wi-Fi clínica veterinaria.

8.5.6. Zona de los laboratorios de Electrónica

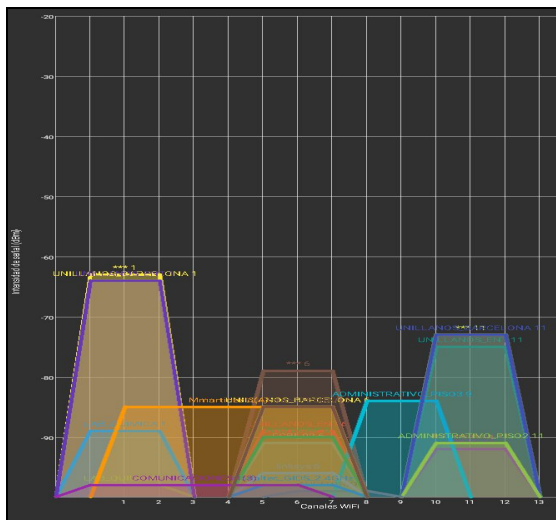


Gráfica 23. Estado inicial, frecuencias redes Wi-Fi laboratorios de electrónica.

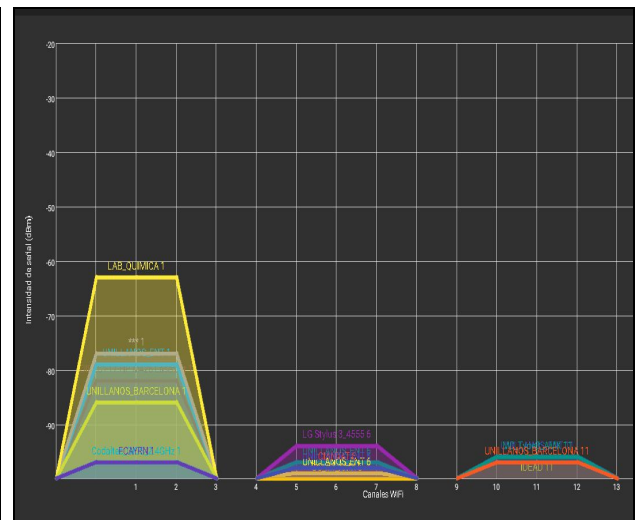


Gráfica 24. Estado final, frecuencias redes Wi-Fi laboratorios de electrónica.

8.5.7. Zona de los laboratorios de Química

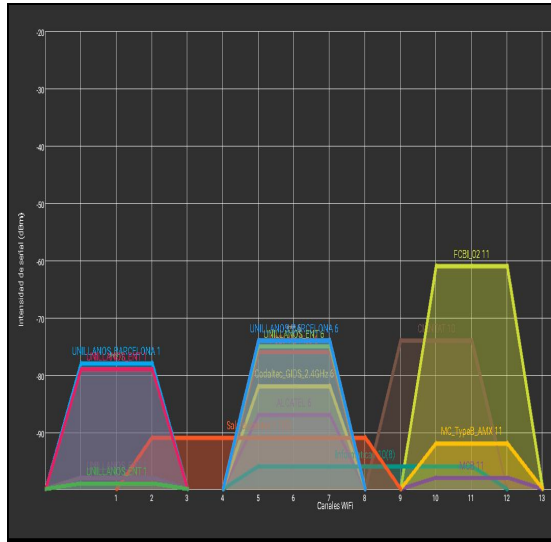


Gráfica 25. Estado inicial, frecuencias redes Wi-Fi laboratorios de química.

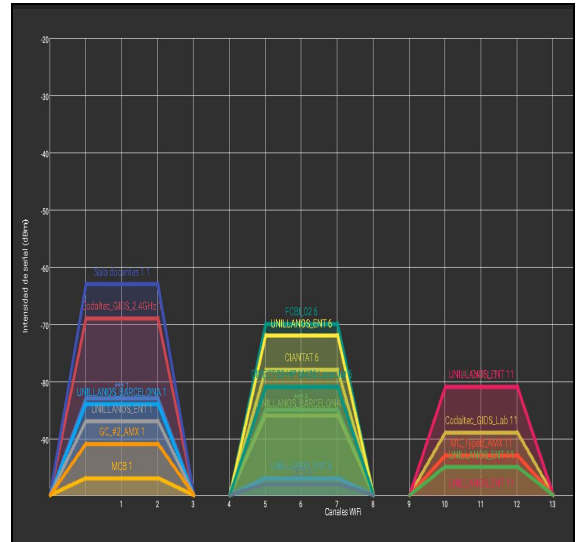


Gráfica 26. Estado final, frecuencias redes Wi-Fi laboratorios de química.

8.8.8. Zona de la facultad FCBI

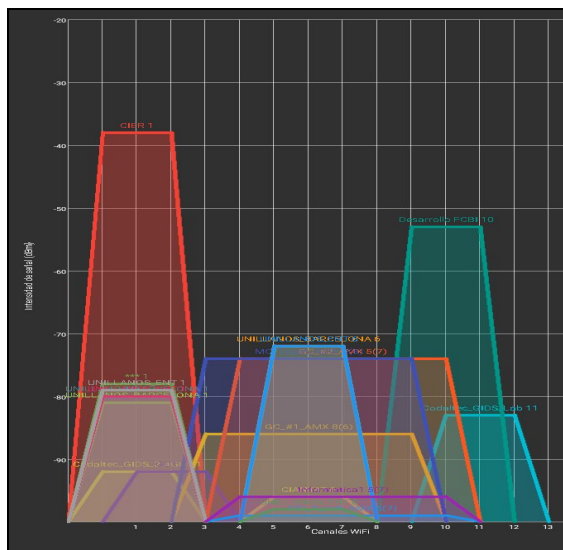


Gráfica 27. Estado inicial, frecuencias redes Wi-Fi facultad FCBI.

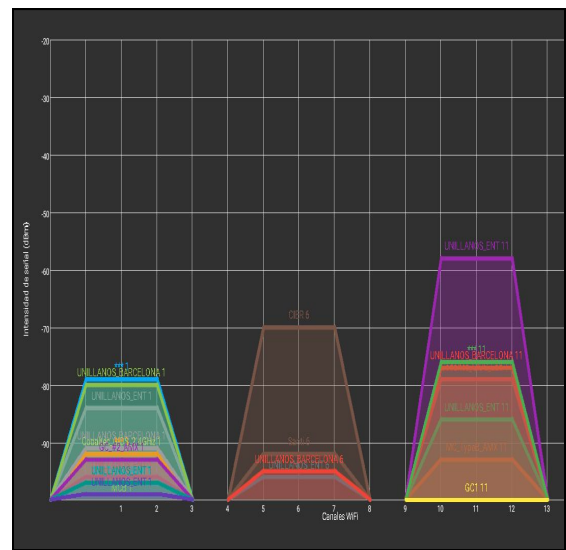


Gráfica 28. Estado final, frecuencias redes Wi-Fi facultad FCBI.

8.8.9. Zona del edificio Albert Einstein

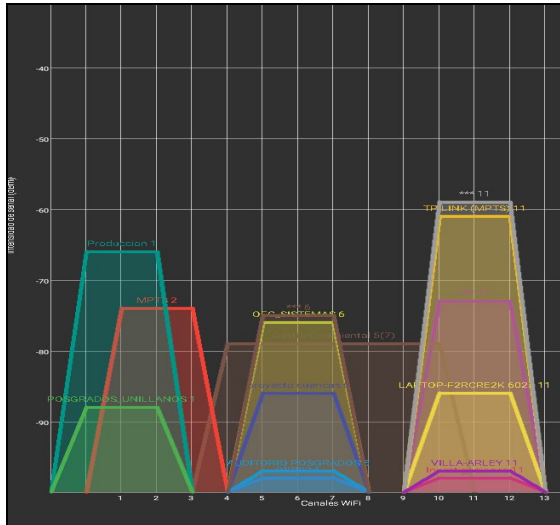


Gráfica 29. Estado inicial, frecuencias redes Wi-Fi edif. Albert Einstein.

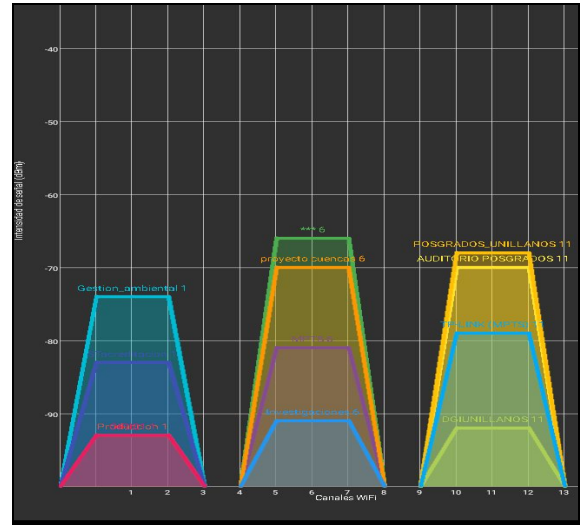


Gráfica 30. Estado final, frecuencias redes Wi-Fi edif. Albert Einstein.

8.8.12. Zona de la sede Posgrados



Gráfica 35. Estado inicial, frecuencias redes Wi-Fi Posgrados.



Gráfica 36. Estado final, frecuencias redes Wi-Fi Posgrados.

Resaltar que el proceso de mantenimiento y configuración en el ambiente Wi-Fi es iterativo, siendo necesario un constante monitoreo del espectro, para mantener las condiciones establecidas, aún cuando sea necesario instalar nuevos dispositivos.

8.6 VLANs y direccionamiento

A continuación en la Tabla 10 y en la Figura 27, podrá encontrar la información relacionada con las VLANs implementadas y su ubicación en el campus Barcelona, hasta la fecha de terminación de la pasantía.

VLAN	Ubicación
VLAN 1	Administración switches.
VLAN 2	Respaldo y comunicación, antiguo esquema de direccionamiento IP, routers HP Aruba (provisional)
VLAN 3	Servidores.
VLAN 4	Auditorio IALL.
VLAN 5	Zona Rack Agronomía.
VLAN 6	Zona Bienestar Institucional.
VLAN 7	IALL - Granja
VLAN 8	FCBI (Facultad de Ciencias Básicas e Ingeniería)
VLAN 9	FCH (Facultad de Ciencias Humanas)
VLAN 10	Edif. Leonardo Da Vinci.
VLAN 30	APs plataforma HP Aruba .

Tabla 10. VLANs configuradas e implementadas en el switch principal.

8.7 Plataforma LibreNMS

La plataforma **LibreNMS** brinda diferentes servicios de monitoreo de red y de otros recursos de los dispositivos, por medio del protocolo SNMP, los cuales se pueden observar a continuación por medio de la incorporación de los diferentes dispositivos de conmutación de paquetes (Switches) a la plataforma piloto.

8.7.1 Adición de dispositivos de red a la plataforma

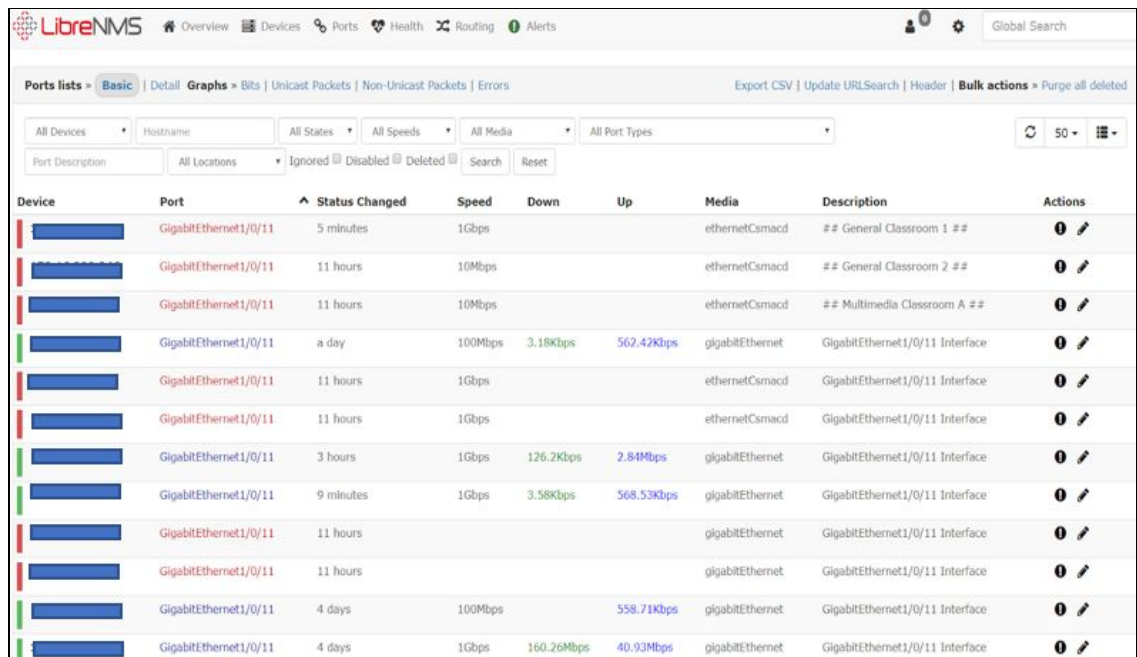
Inicialmente se agregaron los switches a la plataforma piloto a través de su IP asignada con anterioridad, a continuación se puede visualizar la lista de algunos de los dispositivos agregados, con su respectiva información de fabrica y de configuración (ver Figura 28).

 Overview Devices Ports Health Routing Alerts 0 Settings Global Search							
Vendor	Device	Metrics	Platform	System	Uptime	Location	Actions
	hp	54 15	Copyright(c) 2010-2013 Hewlett-Packard Development Company, L.P. 1513P62	HPE Comware 5.20	1d 4h 31m 55s	Bloques de Agronomía y Agroidust	   
	est_2f_svr_l3_c2960_1.rtp.cisco.com	38 4	Catalyst 2960S UNIVERSALK9	Cisco IOS 12.2(55)SE7	11d 3h 56m 22s	Sala de Servidores	   
	est_2f_mca_c2960_1.rtp.cisco.com	37 4	Catalyst 2960S UNIVERSALK9	Cisco IOS 12.2(55)SE7	3d 9h 3m 36s	Sala MCA Cier	   
	est_2f_mca_c2960_2.rtp.cisco.com	37 4	Catalyst 2960S UNIVERSALK9	Cisco IOS 12.2(55)SE7	3d 9h 4m 24s	Sala MCA Cier	   
	est_2f_mcb_h2530_1	63 2	J9775A 2530-48G Switch	HP ProCurve YA.15.12.0007	27d 7h 53m 41s	Cier Sala MCB	   
	est_if_gc1_c2960_1.rtp.cisco.com	36 4	Catalyst 2960S UNIVERSALK9	Cisco IOS 12.2(55)SE7	27d 7h 53m 7s	Sala GC1 Cier	   
	est_if_gc2_c2960_1.rtp.cisco.com	36 4	Catalyst 2960S UNIVERSALK9	Cisco IOS 12.2(55)SE7	22d 5h 59m 57s	Sala GC2 Cier	   
	est_2f_opo_c2960_1.rtp.cisco.com	36 4	Catalyst 2960S UNIVERSALK9	Cisco IOS 12.2(55)SE7	11d 3h 57m 3s	Oficina de Operaciones Cier	   
	est_new1f_so_c2960_1.rtp.cisco.com	36 4	Catalyst 2960S UNIVERSALK9	Cisco IOS 12.2(55)SE7	11d 3h 57m 1s	Bunker Sala de Desarrollo Cier	   
	est_new1f_mms_h1910_1	24 5	Copyright (c) 2004-2012 Hewlett-Packard Development Company, L.P.	HPE Comware 5.20	3h 16m 52s	Estudio Audiovisuales	   

Figura 28. Lista de algunos de los switches agregados a la plataforma piloto.

8.7.2 Visualización de información de puertos

La plataforma **LibreNMS** brinda el servicio de monitoreo de puertos de red de cada uno de los dispositivos agregados a esta, en la Figura 29 se puede observar la información de puertos de diferentes switches, como lo es la velocidad de transmisión, el estado actual del puerto e información de tráfico de red en tiempo real.



Device	Port	Status Changed	Speed	Down	Up	Media	Description	Actions
	GigabitEthernet1/0/11	5 minutes	1Gbps			ethernetCsmacd	## General Classroom 1 ##	
	GigabitEthernet1/0/11	11 hours	10Mbps			ethernetCsmacd	## General Classroom 2 ##	
	GigabitEthernet1/0/11	11 hours	10Mbps			ethernetCsmacd	## Multimedia Classroom A ##	
	GigabitEthernet1/0/11	a day	100Mbps	3.18Kbps	562.42Kbps	gigabitEthernet	GigabitEthernet1/0/11 Interface	
	GigabitEthernet1/0/11	11 hours	1Gbps			ethernetCsmacd	GigabitEthernet1/0/11 Interface	
	GigabitEthernet1/0/11	11 hours	1Gbps			ethernetCsmacd	GigabitEthernet1/0/11 Interface	
	GigabitEthernet1/0/11	3 hours	1Gbps	126.2Kbps	2.84Mbps	gigabitEthernet	GigabitEthernet1/0/11 Interface	
	GigabitEthernet1/0/11	9 minutes	1Gbps	3.58Kbps	568.53Kbps	gigabitEthernet	GigabitEthernet1/0/11 Interface	
	GigabitEthernet1/0/11	11 hours				gigabitEthernet	GigabitEthernet1/0/11 Interface	
	GigabitEthernet1/0/11	11 hours				gigabitEthernet	GigabitEthernet1/0/11 Interface	
	GigabitEthernet1/0/11	4 days	100Mbps		558.71Kbps	gigabitEthernet	GigabitEthernet1/0/11 Interface	
	GigabitEthernet1/0/11	4 days	1Gbps	160.26Mbps	40.93Mbps	gigabitEthernet	GigabitEthernet1/0/11 Interface	

Figura 29. Detalles de información de tráfico de red de los puertos de todos los switches.

8.7.3 Visualización del tráfico total de red



Figura 30. Gráfico del tráfico de red de un dispositivo.

8.7.4 Visualización de monitoreo de recursos

Otro servicio importante y muy útil de la plataforma, es el monitoreo a los recursos del sistema de los dispositivos, los cuales son representados por medio de gráficas y estadísticas en tiempo real como se puede observar en las Figuras 31 y 32.



Figura 31. Representación del estado del procesador y memoria de un switch.



Figura 32. Representación del estado de la temperatura y de los sensores de un switch.

8.7.5 Creación de alertas

LibreNMS incluye un sistema de alertas el cual se encarga de notificar eventos de los dispositivos de los cuales se requiera estar al tanto, para ello el sistema requiere de la configuración de un conjunto de reglas definidas por el usuario para evaluar el estado de cada dispositivo (ver Figura 33).

#	Name	Rule	Severity	Status	Extra	Enabled	Action
+ Create new alert rule - OR - + Create rule from collection 50							
#148	Devices up/down	<code>macros.device_down = 1 AND devices.status_reason = "icmp"</code>	critical	!	Max: -1 Delay: 300 Interval: 300	ON	 
#149	Device rebooted	<code>devices.uptime < 300 AND macros.device = 1</code>	warning	✓	Max: 1 Delay: 300 Interval: 300	ON	 
#152	Port status up/down	<code>ports.ifOperStatus = "down" AND ports.ifOperStatus_prev = "up"</code>	warning	!	Max: 1 Delay: 300 Interval: 300	ON	 
#153	Port utilisation over threshold	<code>macros.port_usage_perc >= 80 AND macros.port_up = 1</code>	critical	✓	Max: -1 Delay: 300 Interval: 300	ON	 
#154	Sensor over limit - Check Device Health Settings	<code>sensors.sensor_current > sensors.sensor_limit AND sensors.sensor_alert = 1 AND macros.device_up = 1</code>	critical	!	Max: -1 Delay: 300 Interval: 300	ON	 
#155	Sensor under limit - Check Device Health Settings	<code>sensors.sensor_current < sensors.sensor_limit_low AND sensors.sensor_alert = 1 AND macros.device_up = 1</code>	critical	!	Max: -1 Delay: 300 Interval: 300	ON	 
#156	Service up/down	<code>services.service_status != 0 AND macros.device_up = 1</code>	critical	✓	Max: -1 Delay: 300 Interval: 300	ON	 

Figura 33. Alertas creadas por el usuario en la plataforma piloto.

8.7.6 Notificaciones de alertas

La plataforma informa por medio de notificaciones, eventos fuera de lo común de los dispositivos de red, las notificaciones pueden ser observadas en la plataforma o con una previa configuración en el correo electrónico u otro medio de transporte, en la Figura 34 se pueden visualizar algunas notificaciones de alerta de diferentes dispositivos.

Timestamp	Rule	Hostname	ACK	Notes
2019-02-15 13:52:11	Sensor over limit - Check Device Health Settings	[Redacted]	[Red]	[Icon]
2019-02-15 13:52:11	Sensor under limit - Check Device Health Settings	[Redacted]	[Red]	[Icon]
2019-02-15 12:02:09	Port status up/down	[Redacted]	[Red]	[Icon]
2019-02-15 12:01:26	Devices up/down	[Redacted]	[Red]	[Icon]
2019-02-15 09:59:02	Sensor over limit - Check Device Health Settings	[Redacted]	[Red]	[Icon]
2019-02-15 09:58:42	Sensor over limit - Check Device Health Settings	[Redacted]	[Red]	[Icon]
2019-02-15 09:32:11	Sensor over limit - Check Device Health Settings	[Redacted]	[Red]	[Icon]
2019-02-13 09:33:04	Sensor over limit - Check Device Health Settings	[Redacted]	[Red]	[Icon]
2018-12-10 11:00:12	Devices up/down	[Redacted]	[Red]	[Icon]

Figura 34. Notificaciones de alertas de diferentes switches.

8.8 Pruebas de rendimiento previas

A continuación se encuentran cada una de las gráficas y tablas, obtenidas de las pruebas de rendimiento realizadas en los puntos de acceso que ofrecen servicio de Wi-Fi a los estudiantes. Estos puntos de acceso se encuentran distribuidos en distintas zonas del campus, como puede apreciarse en el mapa de la Figura 18 de la **sección 7.3.2** concerniente a las pruebas.

En general se puede decir de los resultados obtenidos de las pruebas, que la red Wi-Fi que ofrece servicio a los estudiantes, tiene unos rendimientos en cuanto a transmisión y recepción de paquetes (Throughput), bastante baja e impredecible, ya que no sigue un patrón constante con excepción de algunas zonas como IDEAD, BIBLIOTECA y COROCORA. Pudo observarse también un alto porcentaje en el retardo y pérdida de paquetes, lo que lleva a la red a una alta retransmisión de los mismos; esto puede verse como una consecuencia clara de la falta de segmentación que presentaba y al limitado número de puntos de acceso disponibles para los estudiantes en las diferentes zonas, generando una sobrecarga en los dispositivos de red.

8.8.1 Punto de acceso zona IDEAD

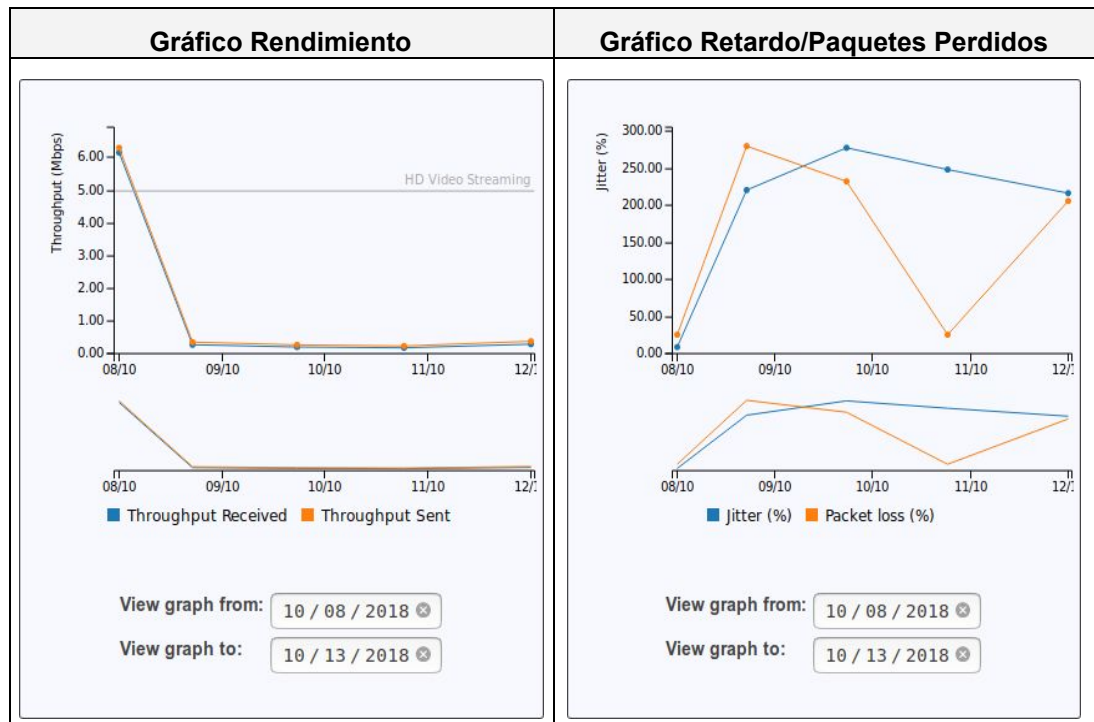


Tabla 11. Gráficos pruebas de rendimiento, generados por **kentnetmon** IDEAD.

N°	Fecha/Hora	Throughput (Enviado) Mbps	Throughput (Recibido) Mbps	Jitter %	Packet Loss %
1	08-10-2018	6,2772	6,1324	8,7399	0,0000
2	09-10-2018	0,3498	0,2687	219,9890	77,6978
3	10-10-2018	0,2664	0,2004	276,8640	63,1579
4	11-10-2018	0,2316	0,1749	247,5800	0,0000
5	12-10-2018	0,3753	0,2861	215,8590	55,0725
Promedio		1,5001	1,4125	193,8064	39,1856

Tabla 12. Valores obtenidos de las pruebas de rendimiento, IDEAD

8.8.2 Punto de acceso zona Biblioteca/Torre Administrativa

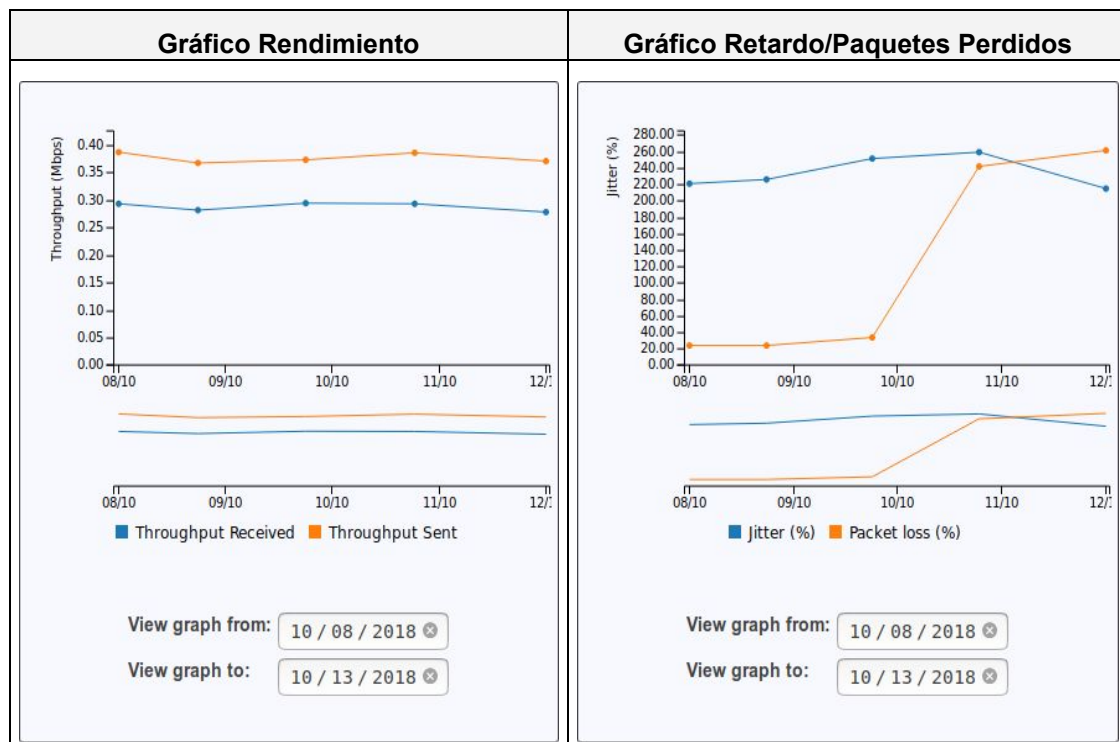


Tabla 13. Gráficos pruebas de rendimiento, generados por kentnetmon Biblioteca.

N°	Fecha/Hora	Throughput (Enviado) Mbps	Throughput (Recibido) Mbps	Jitter %	Packet Loss %
1	08-10-2018	0,3861	0,2930	220,6880	0,0000
2	09-10-2018	0,3672	0,2815	225,7890	0,0000
3	10-10-2018	0,3730	0,2942	251,2230	3,3333
4	11-10-2018	0,3857	0,2930	259,0060	74,5763
5	12-10-2018	0,3706	0,2780	214,7020	81,2500
Promedio		0,3765	0,2879	234,2816	31,8319

Tabla 14. Valores obtenidos de las pruebas de rendimiento, Biblioteca.

8.8.3 Punto de acceso zona Cooperativa/Counillanos

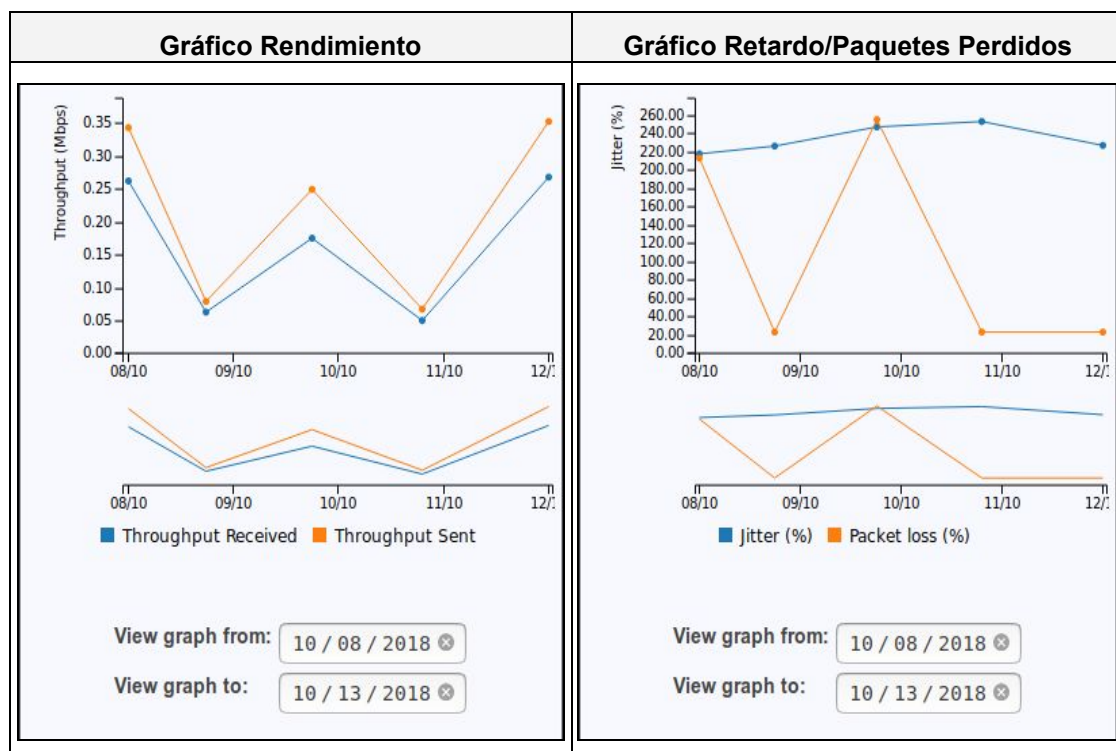


Tabla 15. Gráficos pruebas de rendimiento, generados por **kentnetmon** Cooperativa.

N°	Fecha/Hora	Throughput (Enviado) Mbps	Throughput (Recibido) Mbps	Jitter %	Packet Loss %
1	08-10-2018	0,3428	0,2618	217,2660	64,7727
2	09-10-2018	0,0788	0,0625	225,7390	0,0000
3	10-10-2018	0,2490	0,1749	246,6080	79,1139
4	11-10-2018	0,0672	0,0498	252,5030	0,0000
5	12-10-2018	0,3521	0,2676	226,4860	0,0000
Promedio		0,2180	0,1633	233,7204	28,7773

Tabla 16. Valores obtenidos de las pruebas de rendimiento, Cooperativa.

8.8.4 Punto de acceso zona Coliseo

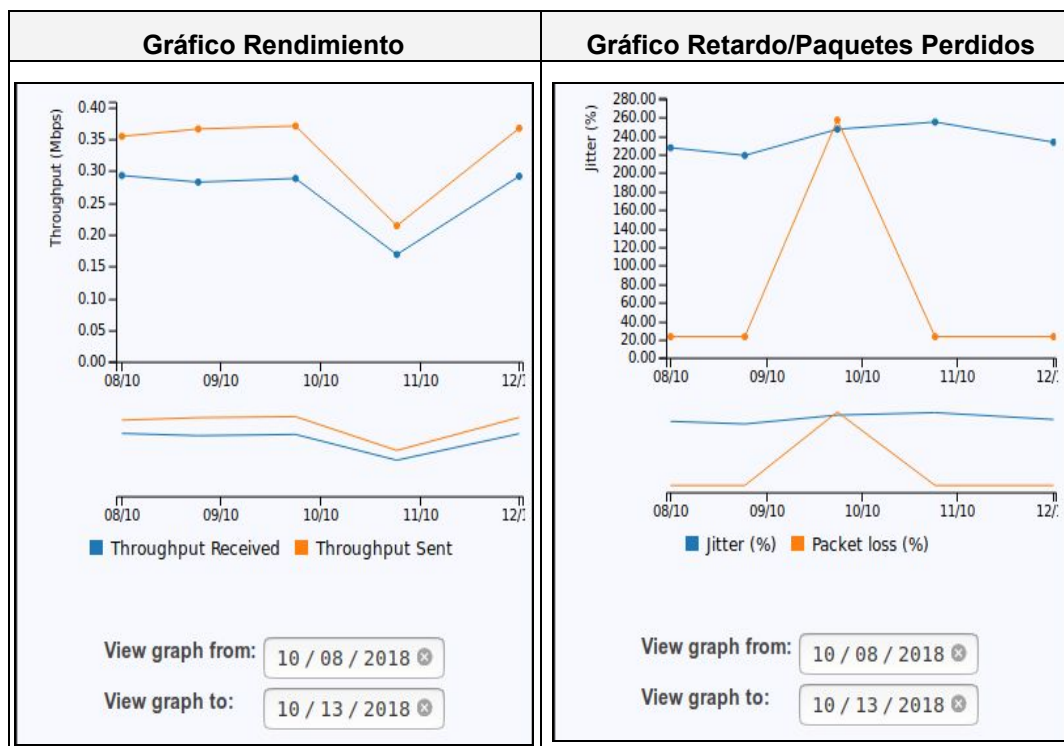


Tabla 17. Gráficos pruebas de rendimiento, generados por **kentnetmon** Coliseo.

N°	Fecha/Hora	Throughput (Enviado) Mbps	Throughput (Recibido) Mbps	Jitter %	Packet Loss %
1	08-10-2018	0,3544	0,2930	227,0850	0,0000
2	09-10-2018	0,3660	0,2826	218,7910	0,0000
3	10-10-2018	0,3706	0,2884	247,0440	3,4483
4	11-10-2018	0,2143	0,1691	254,8100	0,0000
5	12-10-2018	0,3672	0,2919	232,9960	0,0000
Promedio		0,3345	0,2650	236,1452	0,6897

Tabla 18. Valores obtenidos de las pruebas de rendimiento, Coliseo.

8.8.5 Punto de acceso zona edif. Albert Einstein

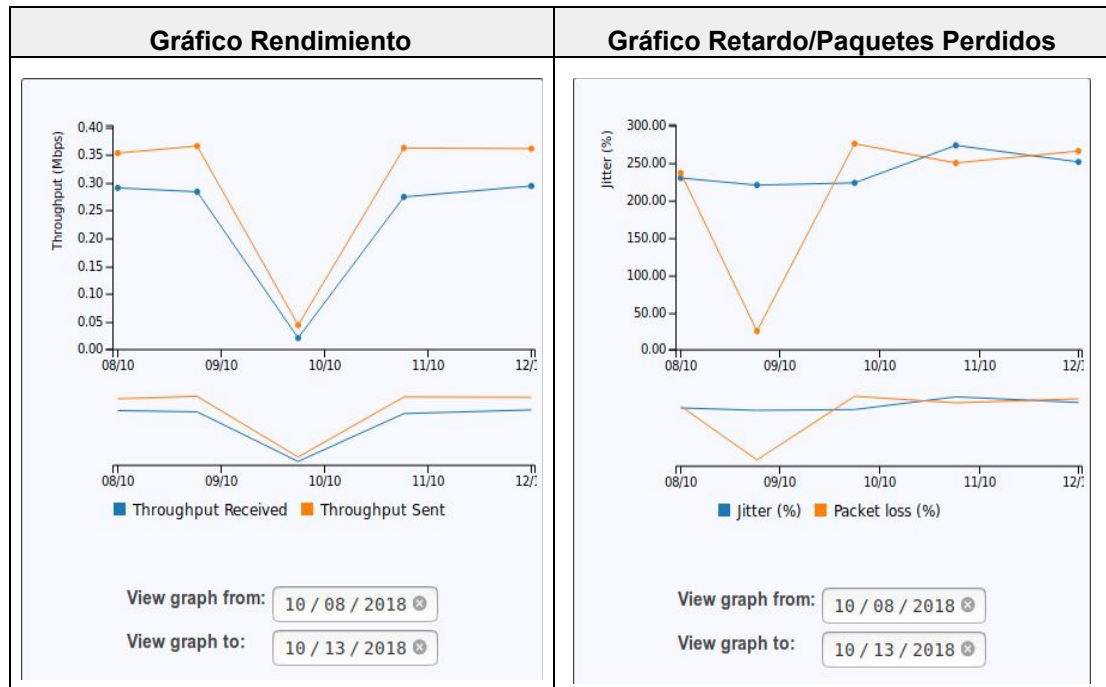


Tabla 19. Gráficos pruebas de rendimiento, generados por **kentnetmon** Einstein.

N°	Fecha/Hora	Throughput (Enviado) Mbps	Throughput (Recibido) Mbps	Jitter %	Packet Loss %
1	08-10-2018	0,3533	0,2907	229,7860	59,7561
2	09-10-2018	0,3660	0,2838	220,2070	0,0000
3	10-10-2018	0,0440	0,0208	223,2580	70,7965
4	11-10-2018	0,3626	0,2745	273,3810	53,6037
5	12-10-2018	0,3614	0,2942	251,2270	68,0000
Promedio		0,2975	0,2328	239,5718	50,4313

Tabla 20. Valores obtenidos de las pruebas de rendimiento, Einstein.

8.8.6 Punto de acceso zona Corocora/Plaza Garza

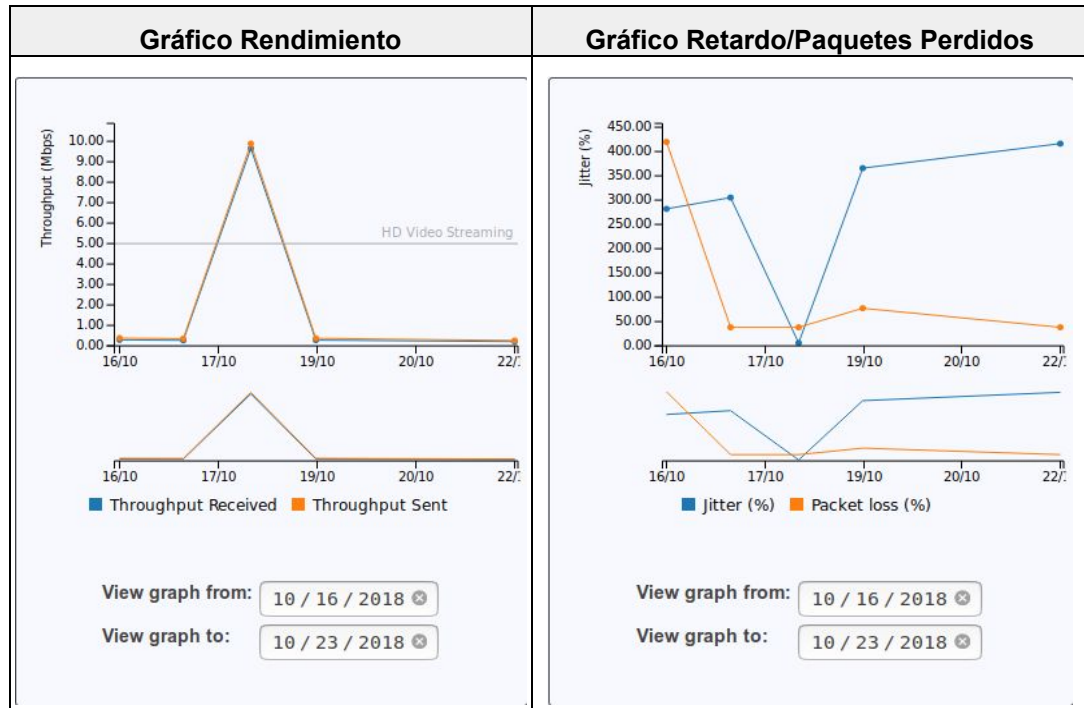


Tabla 21. Gráficos pruebas de rendimiento, generados por **kentnetmon** Corocora.

N°	Fecha/Hora	Throughput (Enviado) Mbps	Throughput (Recibido) Mbps	Jitter %	Packet Loss %
1	16-10-2018	0,3799	0,2942	281,4200	34,7826
2	17-10-2018	0,3521	0,2687	304,6370	0,0000
3	18-10-2018	9,8717	9,6435	5,9845	0,0000
4	19-10-2018	0,3695	0,2791	365,1280	3,5714
5	22-10-2018	0,2624	0,2099	415,4570	0,0000
Promedio		2,2471	2,1391	274,5253	7,6708

Tabla 22. Valores obtenidos de las pruebas de rendimiento, Corocora.

8.9 Puntos de acceso en nuevas zonas del campus Barcelona

Debido a la baja participación de los estudiantes en la encuesta propuesta al inicio de la pasantía; se hizo necesario por medio de observación y diálogo con la comunidad estudiantil, contabilizar la cantidad de personas que frecuentaban ciertas zonas del campus. A continuación se presentan los resultados obtenidos de esas visitas realizadas, donde se identificó la necesidad de puntos de acceso.

En la Tabla 23 se presentan las zonas de interés, ubicación y densidad de usuarios aproximada, también se hace referencia al número de puntos de acceso necesarios, para tener un mejor cubrimiento sobre el campus, en busca de mejorar el servicio de Wi-Fi a los estudiantes.

ID	Nombre Zona	# Usuarios (aprox.)	# Access Points	Tipo AP
A	Edif. Leonardo Da Vinci	30	1	Indoor
B	Zona verde entre Einstein-DaVinci	60	1	Outdoor
C	Corocora.	30	1	Outdoor
D	Zona común cafetería Nестea-Comedor universitario.	25	1	Outdoor
E	Biblioteca salas de consulta.	100	4	Indoor
F1	Auditorio Eduardo Carranza	200	5	Indoor
F2	Torre administrativa zona verde, frente auditorio.	50	1	Outdoor
G	Varado.	30	1	Outdoor
H	Clínica veterinaria.	50	1	Outdoor
I	Coliseo	40	1	Outdoor
J	Zona verde entrada principal	40	1	Outdoor

K	Bienestar institucional y piscina	40	1	Indoor
L	Facultad Matemáticas y Física	35	1	Outdoor
M	Prog. Agroindustrial Laboratorios	40	4	Indoor
N	Auditorio Bertha Lucía, Posgrados.	40	2	Indoor
O	Zona externa laboratorios de química.	45	1	Outdoor
P	Granja	20	1	Indoor
Q	Laboratorio de Lácteos.	15	1	Indoor
R	Unidad de Ovinos y caprinos.	20	1	Indoor

****Zona cuenta con cobertura actualmente.**

Tabla 23. Zonas donde se hace necesario cobertura de red Wi-Fi, campus Barcelona.

En el Figura 35 se ubican los dispositivos en cada una de las zonas identificadas. Aquellos en color verde, indican dispositivos existentes, mientras que aquellos en color rojo, indican dispositivos necesarios.

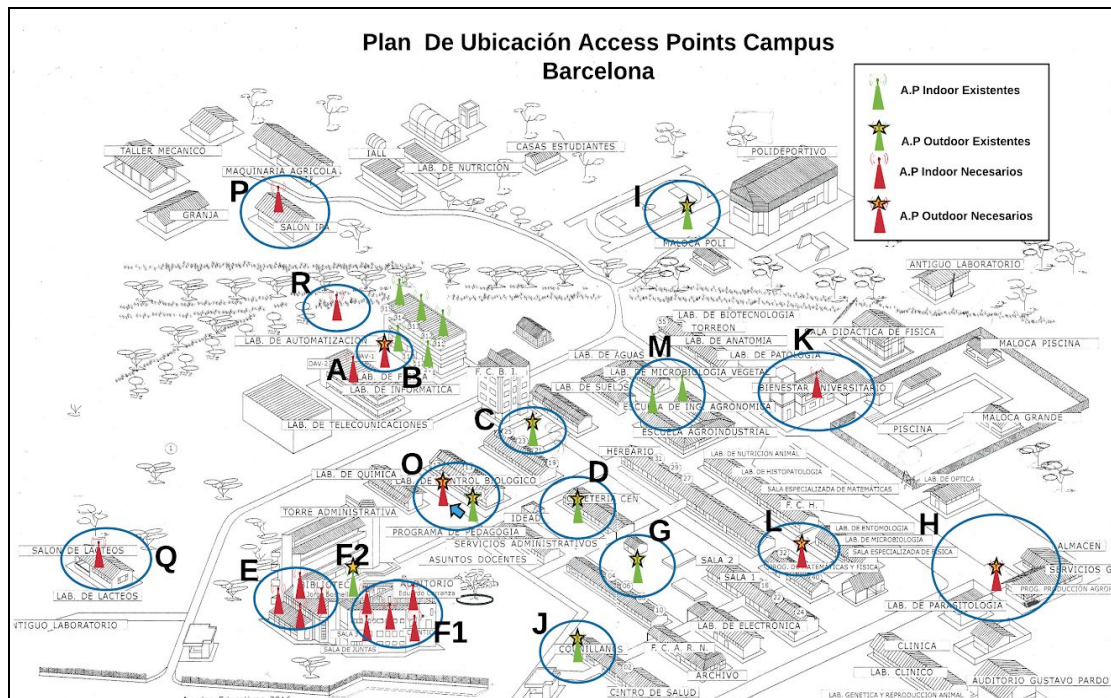


Figura 35. Ubicación zonas, donde se hace necesario cobertura de red Wi-Fi, campus Barcelona.
Fuente: Los autores.

Aquí se muestran por medio de las fotos, la ubicación recomendada de los dispositivos para un mejor aprovechamiento del patrón de radiación y una descripción acerca de algunas características de los mismos.

Zona A: Edif. Leonardo Da Vinci	
<u>Detalle Dispositivo</u> Tipo: Indoor AP de techo. Patrón Radiación: Omnidireccional. Ubicación: Parte central edif. en escaleras.	

Tabla 24. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Da Vinci.

Zona B: Área verde entre Einstein-DaVinci - Opción 1	
<u>Detalle Dispositivo</u> Tipo: Outdoor AP. Patrón Radiación: Omnidireccional. Ubicación: Parte central del área verde entre los edificios Einstein y Da Vinci.	

Tabla 25. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Einstein - Da Vinci 1.

Zona B: Área verde entre Einstein-DaVinci - Opción 2	
<u>Detalle Dispositivo</u> Tipo: Outdoor AP. Patrón Radiación: Directivo. Ubicación: En el costado del área verde entre los edificios Einstein y Da Vinci, frente al parqueadero sobre el paso peatonal.	

Tabla 26. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Einstein - Da Vinci 2.

Zona H: Clínica Veterinaria	
<u>Detalle Dispositivo</u> Tipo: Outdoor AP. Patrón Radiación: Directivo. Ubicación: Zona intermedia entre cafetería y área verde de descanso de la Clínica Veterinaria.	

Tabla 27. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Clínica Veterinaria.

Zona E: Biblioteca salas de consulta	
<u>Detalle Dispositivo</u> Tipo: 2 x Indoor AP de techo. Patrón Radiación: Directivo IEEE 802.11 ac Wave 2 Ubicación: Sala de consulta de la Biblioteca Jorge Boshell.	
<u>Detalle Dispositivo</u> Tipo: 2 x Indoor AP de techo. Patrón Radiación: Directivo. IEEE 802.11 ac Wave 2 Ubicación: Sala de consulta aire libre de la Biblioteca Jorge Boshell.	

Tabla 28. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Biblioteca.

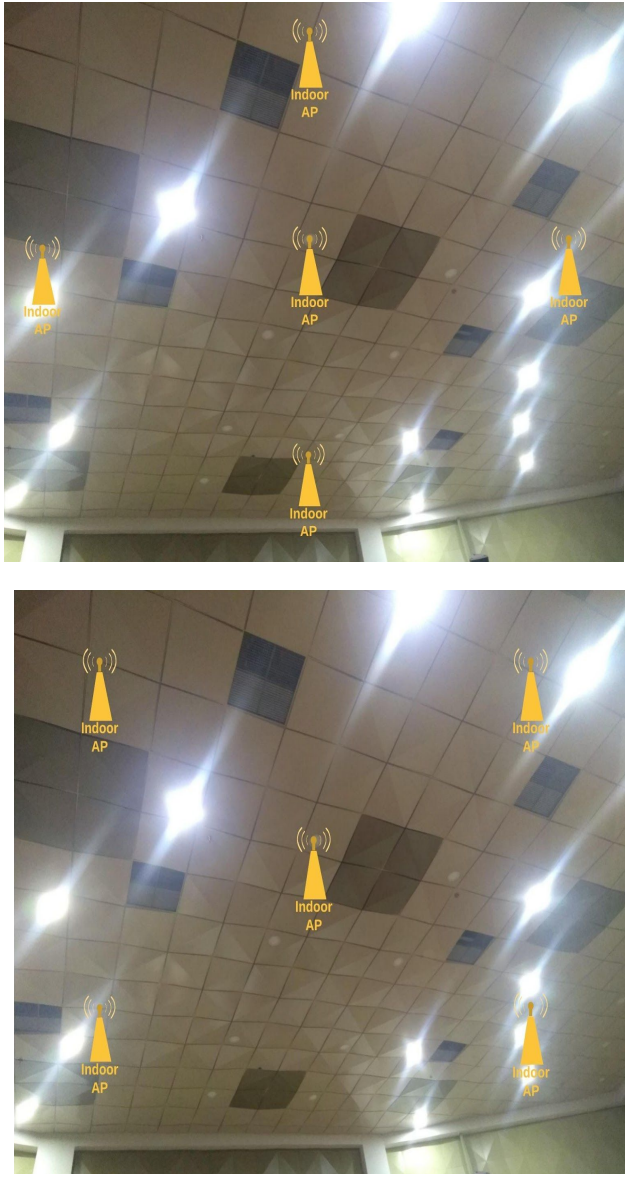
Zona F1: Auditorio Eduardo Carranza	
<u>Detalle Dispositivo</u> Tipo: 5 x Indoor AP de techo. Patrón Radiación: Directivo. IEEE 802.11 ac Wave 2 Ubicación: Auditorio Eduardo Carranza.	

Tabla 28. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Auditorio Eduardo Carranza.

Zona K: Bienestar institucional y piscina	
<u>Detalle Dispositivo</u> Tipo: Indoor AP de techo. Patrón Radiación: Omnidireccional. Ubicación: Primer piso en Bienestar Institucional.	

Tabla 30. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Bienestar Institucional.

Zona L: Facultad Matemáticas y Física	
<u>Detalle Dispositivo</u> Tipo: Outdoor AP. Patrón Radiación: Omnidireccional. Ubicación: En frente del pasillo de las salas de ayudas 1 y 2 de la facultad de Matemáticas y Física.	

Tabla 31. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Facultad de Matemáticas.

Zona R: Unidad de Ovinos y caprinos.	
<u>Detalle Dispositivo</u> Tipo: Indoor AP. Patrón Radiación: Omnidireccional. Ubicación: Oficina de estudiantes de la unidad de ovinos y caprinos.	

Tabla 32. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Ovinos y Caprinos.

Zona O: Zona externa laboratorios de química.	
<u>Detalle Dispositivo</u> Tipo: Outdoor AP. Patrón Radiación: Omnidireccional. Ubicación: Zona de laboratorios de química(Aruba IDEAD), cerca del sendero que lleva a la Torre Administrativa. Recomendación: Reubicación del dispositivo al poste contiguo, para un mejor aprovechamiento del patrón de radiación emitido.	

Tabla 33. Detalle y ubicación de dispositivos mejoramiento de cobertura, zona Laboratorios de Química.

Otras Zonas		
Zona N: Auditorio Bertha Lucía, Posgrados	<u>Detalle Dispositivo</u> Tipo: 2 x Indoor AP de techo. Patrón Radiación: Omnidireccional. Ubicación: Auditorio Bertha Lucía de posgrados.	
Zona P: Granja	<u>Detalle Dispositivo</u> Tipo: Indoor AP de techo. Patrón Radiación: Omnidireccional. Ubicación: Salón IPA en la zona de la granja, cerca al IALL.	
Zona Q: Laboratorio de Lácteos.	<u>Detalle Dispositivo</u> <u>Opción # 1</u> Tipo: Indoor AP de techo. Patrón Radiación: Omnidireccional. Ubicación: Oficina laboratorio de lácteos.	<u>Detalle Dispositivo</u> <u>Opción # 2</u> Tipo: Indoor AP de techo. Patrón Radiación: Directivo. Ubicación: Garita del vigilante, entrada # 2 campus Barcelona. Recomendación: La antena de patrón de radiación directivo, debe ubicarse de manera tal, que emita la señal en dirección al Lab. de Lácteos, ubicado alrededor de 20 m. de distancia.

Tabla 34. Detalle y ubicación de dispositivos mejoramiento de cobertura, otras zonas.

9. CONCLUSIONES

En las fases iniciales del proyecto, al identificar cada uno de los dispositivos que integran y brindan servicio en la red (APs y switches) del campus Barcelona, se logró entregar a la Oficina de Sistemas documentos con un inventario del 100% de los equipos hasta la fecha de la terminación de la pasantía, donde se pueden encontrar las características técnicas, ubicación y parámetros de configuración de los mismos. Posteriormente estos equipos fueron configurados, habilitando la opción para la administración de manera remota. Esto facilitó en gran medida el trabajo de los ingenieros del área de soporte de la Oficina de Sistemas, reduciendo tiempo a la hora de realizar ciertos tipos de configuraciones y detección de fallas; aunque se lleva un control de llegada y baja de estos dispositivos, no se contaba en esta dependencia con un consolidado real de la cantidad coexistente en la red.

La participación de la comunidad estudiantil como eje principal para la realización del proyecto, permitió a través de la encuesta aplicada, conocer las necesidades de conectividad de la misma; principalmente en el aspecto relacionado con la identificación de los espacios o áreas del campus Barcelona que requerían cobertura y la densidad de usuarios en cada una de estas. Aunque esta necesidad no fue suplida dentro del tiempo de la realización del proyecto, se logró dar un primer paso importante, ya que se determinaron las características técnicas de los equipos requeridos y la ubicación idónea en el campus Barcelona; entregando un documento con dicha información (véase **sección 8.9**) a la Oficina de Sistemas, en busca de mejorar el servicio de Wi-Fi en el campus en un mediano plazo.

Gracias a la correcta configuración realizada sobre los access points en aspectos relacionados con canales de frecuencia, potencias y ancho de banda; se logró mejorar el uso del espectro electromagnético en la banda de 2.4 GHz, reduciendo la interferencia co-canal que existía en las diferentes dependencias y oficinas del campus Barcelona, producto del alto número de APs existentes por área, como se pudo observar en las gráficas de la **sección 8.5** de este libro.

A pesar de las limitaciones encontradas a la hora de proporcionar algunos recursos de hardware (*Patch Cord* de fibra) por parte de la Oficina de Sistemas, necesarios para las actividades relacionadas con la segmentación de la red, se logró dejar en funcionamiento un poco más del 50% de las VLANs (10 de un total de 18 véase **sección 8.6**) proyectadas en la fase de diseño, lo cual también incluyó para estas el nuevo direccionamiento IP. Esto fue posible gracias a la instalación y puesta en marcha del Switch L3 proporcionado por la Oficina de Sistemas; reduciendo significativamente el gran dominio de broadcast que se tenía con el direccionamiento antiguo en dominios más pequeños, aliviando la sobrecarga de tráfico que se generaba y haciendo más sencilla la administración y detección de problemas en la red.

Se logró la instalación e implementación de una plataforma de monitoreo de red, como lo fue la plataforma LibreNMS en uno de los servidores principales de la Oficina de Sistemas, obteniendo así resultados en tiempo real del estado físico (sensores, memoria, procesador) y de red (velocidad de transmisión, tráfico de puertos) de cada uno de los switches del campus Barcelona integrados a dicha plataforma.

10. RECOMENDACIONES

10.1 Oficina de Sistemas

10.1.1 Características técnicas de nuevos equipos

En caso de adquisición de nuevos equipos, es recomendable que estos cumplan con ciertas características técnicas que implementen estándares y tecnologías recientes; en busca de mejorar el servicio a la comunidad universitaria del campus Barcelona.

En el caso de los puntos de acceso tanto de interiores (indoors) como de exteriores (outdoors), se recomienda que los dispositivos cuenten con las siguientes características:

- Soporte para el estándar IEEE 802.11ac Wave 2
- Soporte para la banda 2.4 GHz y 5 GHz

- Soporte para autenticación tipo Enterprise 802.1x
- Capacidad de Accounting.
- Potencia controlable en incrementos de 0.5 dBm
- Alimentación por PoE o adaptador.
- En caso de APs interiores, capacidad de antena externa preferiblemente.
- En caso de APs exteriores, antenas direccionales integradas o conectores para antenas externas (Min. 3)
- Capacidad de ser administrado por medio de controlador virtual

En el caso de los equipos de conmutación (switches) de la red, se recomiendan que estos dispositivos sean de tipo **Enterprise** (empresarial), lo que garantizará alta capacidad de procesamiento, soporte a grandes cargas de trabajo (tráfico de la red) y funcionamiento 24/7. Las características que deben poseer estos, son las siguientes:

- Administrable.
- Capa 2 o capa 3.
- Soporte para autenticación tipo Enterprise 802.1x
- Soporte SNMP v2c (Mínimo)
- Soporte IPV4 e IPV6
- Soporte de etiquetado de VLAN 802.1p/q
- Soporte puertos de fibra.
- Mínimo 48 puertos de conexión.

10.1.2 Personal capacitado dedicado a la gestión de la red

El capital humano es uno de los recursos, sino el más valioso que puede tener una organización. Es por ello que se hace necesario que la Oficina de Sistemas de la Universidad de los Llanos, integre dentro de su equipo de trabajo un **Administrador de Infraestructura de TI**, con los conocimientos y competencias necesarias para la planeación, montaje, gestión y soporte de este tipo de infraestructuras. Ya que ello permite fijar un norte en la proyección de estrategias

y crecimiento a futuro de la red; como se pudo evidenciar en el desarrollo del proyecto el área de soporte es la encargada de esta función.

10.2 Programa Ingeniería de Sistemas

10.2.1 Fortalecimiento de la línea de profundización de Teleinformática

El programa de Ingeniería de Sistemas, adscrito a la Facultad de Ciencias Básicas e Ingeniería (FCBI) ofrece actualmente tres líneas de profundización, en los siguientes campos:

1. Ingeniería de Software.
2. Teleinformática.
3. Ciencias de la Computación.

Como estudiantes se debe elegir una de ellas en los últimos semestres de la carrera de manera libre, según el enfoque que se quiera seguir en el desarrollo académico y profesional. El trabajo realizado y presentado en este libro, es netamente del área de las redes informáticas y las telecomunicaciones; en donde se logró aplicar y afianzar los conocimientos adquiridos en los cursos recibidos de la línea de profundización de Teleinformática.

Se valora el esfuerzo que ha llevado a cabo la Facultad en el fortalecimiento de las diferentes líneas de profundización, pero también se hace necesario inversión en la línea de Teleinformática, que en consecuencia es la más abandonada. Un laboratorio de telecomunicaciones, dotado de dispositivos de red (switches, routers, APs) y antenas, permitirán a los estudiantes la práctica necesaria en equipos reales afianzando los conocimientos en infraestructura y plasmando los diseños elaborados en los simuladores. Así como las líneas de Ingeniería de Software y Automatización cuentan sus laboratorios correspondientes, existe una deuda con la línea de Teleinformática ya que a la fecha de la elaboración de este libro, no se cuenta con un laboratorio adecuado para esta. Afortunadamente este trabajo permitió un fuerte contacto con infraestructura real en producción, que claramente no permite gran escala de experimentación, que si puede ser lograda en instancias académicas más tempranas con los espacios y equipos adecuados.

10.3 Trabajos futuros

Terminado el proyecto de pasantía en la Oficina de Sistemas, se pudo observar que muchas de las actividades implementadas durante el proceso de reestructuración de la red Wi-Fi del campus Barcelona, no fueron terminadas al 100% por cuestiones de presupuesto; así que estas pueden servir de guía a trabajos futuros para aquellos estudiantes que se encuentren en proceso de encontrar una opción de grado que permita continuar con su progreso y ajuste, mejorando el funcionamiento de la red.

Los trabajos futuros pueden surgir de actividades pendientes como lo son la terminación de implementación de las VLANs faltantes actualmente y la debida configuración del direccionamiento a los equipos de cómputo, impresoras y routers pertenecientes a su VLAN, la realización de pruebas de rendimiento a los dispositivos de acceso Aruba al finalizar la implementación total de las VLANs, la implementación completa de todas las funciones que proporcionan una gran cantidad de características y soporte para los dispositivos la plataforma LibrenNMS.

11. IMPACTO

Por medio del proyecto de grado en modalidad de pasantía “Reestructuración de la red Wi-Fi del campus Barcelona de la Universidad de los Llanos” se lograron importantes avances tanto desde el punto de vista de acceso inalámbrico (Wi-Fi) como de configuración lógica de la infraestructura de la red actual, en su mayoría llevados a cabo por medio de la implementación de buenas prácticas y de muchas otras actividades con resultados satisfactorios para la Universidad. El impacto generado es visible más desde un punto de vista técnico, que para el usuario final (comunidad universitaria). A continuación se mencionan algunas de esas actividades realizadas.

Una importante actividad que se llevó a cabo fue la correcta planeación y configuración de los canales de frecuencia de cada uno de los dispositivos de acceso inalámbrico en el campus Barcelona, resultados que pueden ser evidenciados en la **sección 8.5** donde se puede observar el mejoramiento en el uso del espectro.

Se elaboró e implementó un adecuado diseño lógico de red a través de la segmentación por medio de VLANs, lo cual generó significativamente la reducción de tráfico en la red, realizando una correcta configuración e implementación en cada uno de los segmentos, por lo tanto disminuyó el dominio de broadcast evidenciándose así la mejora de la congestión que era de gran notoriedad antiguamente.

Otra actividad involucra el inventario de los equipos que componen la red (routers y switches), en donde se reunieron cada una de las características técnicas y su ubicación dentro del Campus. Posteriormente estos equipos fueron configurados para permitir la administración remota y en el caso de los switches, agregados a una plataforma piloto de monitoreo que trabaja con el protocolo de SNMP (LibreNMS), la cual genera diferentes alertas que permiten una detección temprana y centralizada de problemas que pueden presentar estos; lo que impactó positivamente en el personal del área de soporte de la Oficina de Sistemas, reduciendo los tiempos de detección y atención a fallas de la red.

12. GLOSARIO

12.1 Generalidades de la empresa

La Universidad de los Llanos es una Institución del Orden Nacional que desarrolla el servicio público de la Educación Superior, sujeta a inspección y vigilancia por el Ministerio de Educación Nacional.

Creada mediante la Ley 8 de 1974 y el Decreto 2513 de noviembre 25 de 1974 expedido por el Ministerio de Educación Nacional; y reconocida como Universidad mediante la Resolución No. 03273 del 25 de junio de 1993 emanada del mismo

Ministerio. Es un ente universitario autónomo, con carácter estatal, régimen especial, personería jurídica; al igual que en su gobierno, en su ejercicio académico, administrativo, financiero y presupuestal; con rentas y patrimonio propios e independientes; además, se encuentra vinculada al Ministerio de Educación Nacional en lo referente a la política y a la planeación del sector educativo, al Sistema Nacional de Ciencia y Tecnología y al Sistema Nacional de Cultura; se rige por la Constitución Política, la Ley 30 de 1992, las demás disposiciones que le sean aplicables de acuerdo con su régimen especial y las normas internas emitidas en ejercicio de su autonomía.

La Universidad de los Llanos tiene domicilio principal en Villavicencio, capital del Departamento del Meta, República de Colombia. Sin embargo, con arreglo a la Ley y al Estatuto General, puede establecer seccionales y dependencias en cualquier lugar del territorio nacional, priorizando como área de influencia la Orinoquia Colombiana.

12.1.1 Ubicación y contacto

Universidad de los Llanos

Nit: 892.000.757-3

contacto@unillanos.edu.co,

Sedes:

Barcelona: Km. 12 Vía Puerto López - PBX. +57 (8) 6616800

San Antonio: Calle 37 No. 41-02 Barzal - PBX. +57 (8) 6616900

Emporio: Calle 40 A No. 28-32 Emporio - +57 (8) 6734700

Fax: +57 (8) 6616800 ext: 204

Horario de atención: Lunes a Viernes

7:30am a 11:45 am y 2:00 pm a 5:30 pm

12.1.2 Misión

La Universidad de los Llanos forma integralmente ciudadanos, profesionales y científicos con sensibilidad y aprecio por el patrimonio histórico, social, cultural y ecológico de la Humanidad, competentes y comprometidos en la solución de problemas de la Orinoquia y el país con visión universal, conservando su naturaleza como centro de generación, preservación, transmisión y difusión del conocimiento y la cultura.

12.1.3 Visión

La Universidad de los Llanos propende ser la mejor opción de Educación Superior de su área de influencia, dentro de un espíritu de pensamiento reflexivo, acción autónoma, creatividad e innovación. Al ser consciente de su relación con la región y la Nación es el punto de referencia en el dominio del campo del conocimiento y de las competencias profesionales en busca de la excelencia académica.

12.2 Acrónimos y siglas

AP	<i>Access Point</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
IP	<i>Internet Protocol</i>
LAN	<i>Local Area Network</i>
MAN	<i>Metropolitan Area Network</i>
PC	<i>Personal Computer</i>
RADIUS	<i>Remote Authentication Dial-In User Service</i>
SNMP	<i>Simple Network Management Protocol</i>
SSID	<i>Service Set Identifier</i>
VLAN	<i>Virtual Local Area Network</i>
WAN	<i>Wide Area Network</i>
WLAN	<i>Wireless Local Area Network</i>

WMAN *Wireless Metropolitan Area Network*

WPAN *Wireless Personal Area Network*

13. ANEXOS

13.1 Caso Rogue DHCP en la red campus Barcelona

En este anexo se hará referencia a un problema muy común, que se presentaba recurrentemente durante el tiempo en el que se desarrolló el proyecto de pasantía. De esta manera se busca visibilizar, la importancia de la segmentación de una red y cómo a partir de la aplicación de las bases teóricas y buenas prácticas, se logra mejorar la seguridad de la infraestructura de red, desde el punto de vista lógico.

Para entender mejor el proceso, se explicará de manera resumida el funcionamiento del protocolo DHCP (*Dynamic Host Configuration Protocol*), luego el concepto al que hace referencia **Rogue DHCP** y finalmente las capturas de pantalla del análisis de tráfico realizado con la aplicación *Wireshark*, durante el suceso de uno de los casos, en donde se afectó el servicio de Internet dentro del campus.

Protocolo DHCP

De sus siglas en inglés *Dynamic Host Configuration Protocol*, es un protocolo que tiene la capacidad de asignar dinámicamente las direcciones a los clientes o equipos conectados dentro de una red, facilitando la administración centralizada de las mismas. Actualmente es el estándar de configuración del protocolo IP más usado, tanto en redes domésticas/hogareñas como en empresariales.

DHCP utiliza UDP (*User Datagram Protocol*) como protocolo en la capa de transporte; ocupando el puerto **67** para la recepción de mensajes y el puerto **68** para el envío de los mismos, desde y hacia los clientes. Básicamente para la asignación de una dirección IP, un equipo cliente debe hacer una solicitud que es respondida por el servidor y en esta comunicación se produce un intercambio de mensajes, como puede observarse en la Figura 36. Estos mensajes siguen un

formato estándar, el cual contiene ciertos campos de interés que es necesario entender, para proceder a la descripción de las capturas del tráfico.

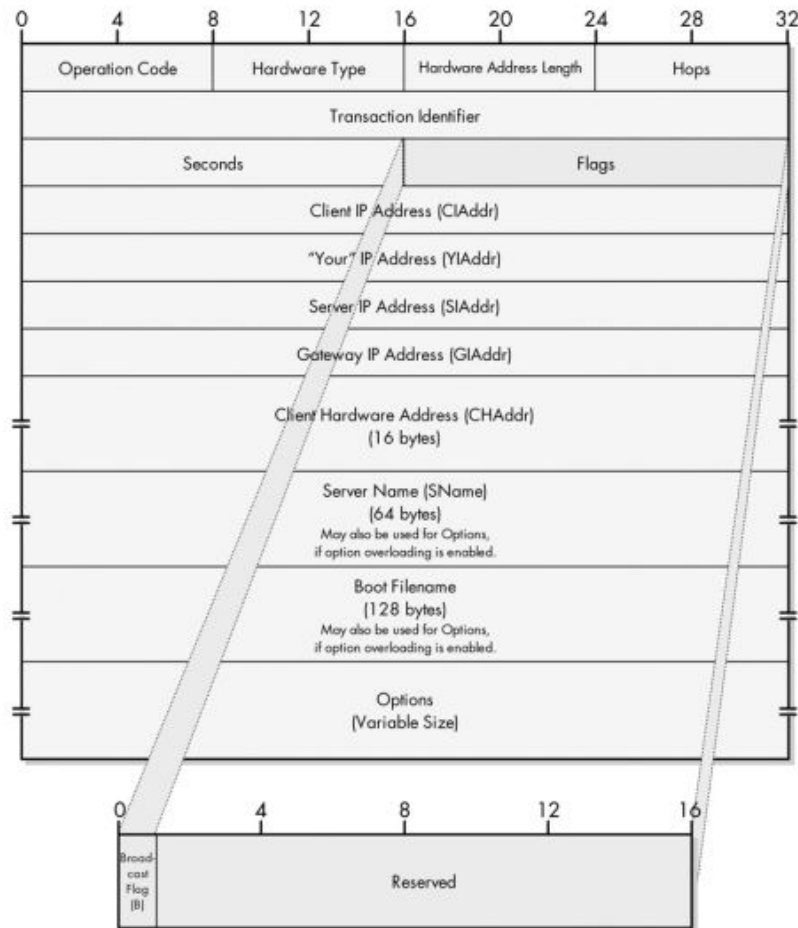


Figura 36. Formato de mensaje protocolo DHCP. [17]

Puede encontrar información más detallada en relación con cada uno de los campos en el **RFC 2131: Dynamic Host Configuration Protocol**, de la IETF (*Internet Engineering Task Force*). En este caso se explicarán los de interés que son los siguientes:

Hardware Type: en este campo se coloca información relacionada con el tipo de hardware utilizado en la red local. Puede tomar diferentes valores, siendo el más común el 1 (uno), que es Ethernet.

Transaction Identifier: número aleatorio elegido por el equipo cliente, usado para identificar la comunicación entre este y un equipo servidor.

Flags: contiene un subcampo llamado **broadcast flag** que toma el valor de 1 (uno), cuando un cliente no tiene dirección IP en el momento de realizar una petición. En caso contrario es 0 (cero).

Client IP Address (CIAddr): en este campo el cliente coloca la dirección IP, sólo si es válida y el servidor DHCP se la asigna. En caso contrario tendrá un valor de 0 (cero). No es usado en el proceso de solicitud de direcciones, hasta que el servidor responde con un mensaje **DHCP ACK** y el equipo pasa al estado de dirección asignada (*BOUND state*). Esto podrá verse más adelante.

Your IP Address (YIAddr): esta se refiere a la dirección que el servidor DHCP le esta asignando al equipo cliente.

Server IP Address (SIAddr): este campo le indica al equipo cliente la dirección IP del servidor DHCP que debe utilizar en el siguiente paso, durante el proceso de solicitud de IP. Las respuestas hechas por el servidor, siempre utilizan este campo y otro llamado **DHCP Server Identifier**, que es opcional; estableciendo la dirección IP del mismo.

Client Hardware Address (CHAddr): en este campo se coloca la dirección MAC (*Media Access Control*) de la interfaz de comunicación que posea el equipo cliente, permitiendo su identificación.

Options: en este existen una variedad de campos, que son requeridos para el funcionamiento básico del protocolo DHCP, cada uno con un código respectivo. Entre los que nos interesan para este caso particular se pueden encontrar:

- **Requested IP Address (50):** este campo es usado por el equipo cliente para solicitar una IP específica al servidor DHCP.
- **DHCP Message Type (53):** indica el tipo de mensaje DHCP.
- **DHCP Server Identifier (54):** indica la dirección del servidor DHCP.

- **Message (56):** indica información acerca de algún tipo de error. Es usado tanto por el equipo cliente, como por el servidor.
- **Client Identifier (60):** indica información del tipo y dirección de hardware (MAC) del equipo cliente, lo que permite al servidor identificarlo como un equipo único, entre todos los clientes DHCP.

Luego de este pequeño vistazo a los campos del formato de mensajes, utilizado en el protocolo DHCP; el diálogo que establece un equipo cliente con un servidor para obtener una dirección IP es el siguiente (ver Figura 37):

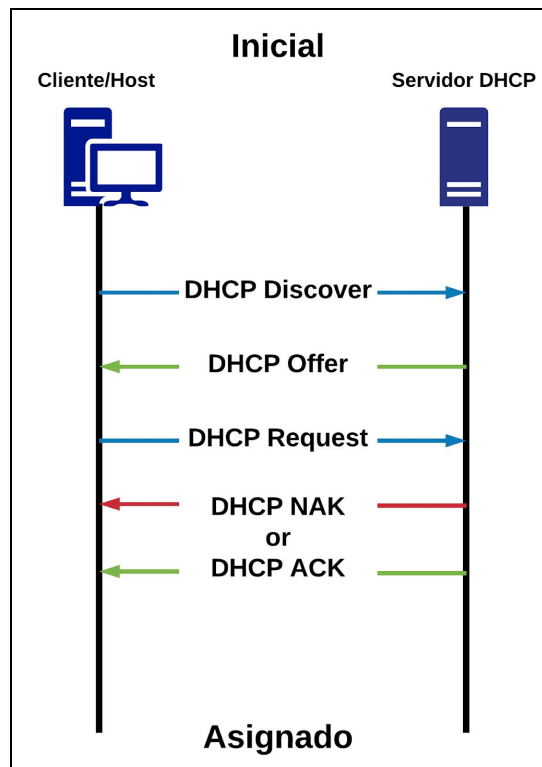


Figura 37. Intercambio de mensajes asignación IP, protocolo DHCP.
Adaptado de: *TCP/IP Guide*. (p.1096) [17]

1. Un equipo cliente comienza en un estado inicial, en donde necesita asociarse a una red, pero no tiene una dirección IP asignada, ni tampoco sabe si en esta, existe un servidor DHCP. El equipo entonces, envía un mensaje **DHCP DISCOVER** a la red, el cual es de tipo **broadcast**. En este mensaje se envía la MAC del equipo cliente, en el campo **CHAddr** y el

número de identificación de la transacción, en el campo **Transaction Identifier**, lo que permitirá al cliente reconocer los mensajes que pertenecen a una misma transacción o diálogo con un servidor. Finalmente se entra en un modo de espera, a la escucha de respuestas a su petición.

2. El servidor DHCP, recibe el mensaje **DHCP DISCOVER**. Este pasa a examinarlo y lee el campo **CHAddr**, para buscar si el equipo cliente esta en su base de datos y de esta manera determinar si puede ofrecerle, lo que se llama un arrendamiento bajo ciertas condiciones. También verifica si en el campo de **Options**, específicamente en **Requested IP Address**, el equipo cliente esta solicitando alguna dirección IP en particular. El servidor responde con un **DHCP OFFER** el cual es de tipo *broadcast*, usando el campo **YIAddr** para decirle al equipo cliente la dirección que le va a asignar, envía el mismo número de identificación de transacción, elegido por el cliente en el campo **Transaction Identifier** y en **Options** usa el campo **DHCP Server Identifier** estableciendo su dirección IP. En esta respuesta del servidor, viaja otro tipo de información adicional correspondiente a las condiciones de arrendamiento que ofrece al cliente.
3. El equipo cliente recibe los mensajes **DHCP OFFER** respondidos por el servidor o servidores DHCP que existan dentro de la red local. En este caso el comportamiento del cliente, depende de la implementación que tenga el sistema operativo de la máquina; ya que este puede elegir la primer respuesta o esperar más tiempo y decidir sobre cuales son las condiciones de arrendamiento ofrecidas más favorables. Una vez el equipo cliente ha decidido, envía un mensaje **DHCP REQUEST** el cual es de tipo *broadcast*, usando en **Options** los campos de **DHCP Server Identifier**, en donde establece la dirección IP del servidor DHCP elegido y **Requested IP Address**, en donde confirma al servidor que va a usar la dirección IP ofrecida. En esta solicitud también viajan algunos parámetros adicionales de configuración necesarios para establecer una conexión exitosa.

4. El servidor recibe los mensajes **DHCP REQUEST**, verifica que la dirección IP establecida en **Options**, en el campo **DHCP Server Identifier** corresponda a la suya; si es correcto procesa el mensaje de lo contrario simplemente lo descarta. En este punto el servidor puede responder de dos formas distintas dependiendo sea el caso. La primera forma, es enviando al cliente un mensaje **DHCP NAK** el cual es de tipo **broadcast**, en donde el servidor determina que no es posible usar la dirección IP solicitada u ofrecida, o simplemente en la negociación de arrendamiento no se cumplen ciertos parámetros; por tanto informa al cliente del rechazo de su petición. La segunda forma, es enviando al cliente un mensaje **DHCP ACK** el cual es de tipo **broadcast**, en donde el servidor le confirma al cliente la concesión del arrendamiento solicitado, pues los recursos están disponibles y se cumple con los parámetros requeridos para la conexión.
5. Finalmente el equipo cliente recibe la respuesta del servidor. En caso de que esta sea una respuesta negativa con un mensaje **DHCP NAK**, el equipo retorna al estado inicial para realizar nuevamente todo el proceso. Si la respuesta es positiva mediante un mensaje **DHCP ACK**, el equipo establece su configuración y se incorpora a la red, pasando al estado donde los recursos han sido asignados. En caso de que el cliente no reciba respuesta del servidor dentro de un tiempo determinado, generará nuevamente un mensaje **DHCP REQUEST**.

ROGUE DHCP

Una vez se ha comprendido el funcionamiento básico del protocolo DHCP y el proceso llevado a cabo entre un equipo cliente y un servidor, para la obtención de una dirección IP a fin de acceder a los recursos ofrecidos por una red; se describirá un poco uno de los problemas potenciales que se pueden presentar, respecto al uso de este protocolo.

Un **ROGUE DHCP** es un servidor DHCP no autorizado, el cual se encuentra por fuera del control de los administradores de la red, que ofrece información de configuración falsa a las solicitudes realizadas por los equipos cliente conectados o que buscan acceder a la misma, por medio de una dirección IP dinámica. Este

servicio puede ser ofrecido por un dispositivo de cómputo configurado para tal fin conectado a cualquier punto de red, ya sea un equipo de escritorio, portátil, raspberry o similares; también por dispositivos de red como los routers.

La puesta en marcha de un **ROGUE DHCP** dentro de una red, depende de los objetivos y conocimientos que posea el usuario atacante. Este simplemente puede sabotear la red y denegar el acceso a los equipos cliente de la misma; por otro lado y más grave, es que logre configurar este servicio para que los equipos cliente, accedan a través de una puerta de enlace maliciosa (router), lo que permitiría explotarlos en usos futuros.

En la Figura 38, se muestra un esquema de red donde existen 3 switches, uno principal que se encarga de la distribución de la red, al cual esta conectado el servidor DHCP Oficial, y dos switches de acceso que permiten conectar los equipos clientes. Puede observarse como el **ROGUE DHCP** esta conectado a uno de los switches de acceso.

Dado que la red denominada como **Red A** no se encuentra segmentada, el servicio no autorizado puede escuchar todas las solicitudes enviadas por los clientes mediante el mensaje **DHCP DISCOVER** y responderlas con un **DHCP OFFER**, ya que estos mensajes son de tipo **broadcast** y todos los equipos de la red comparten ese mismo dominio.

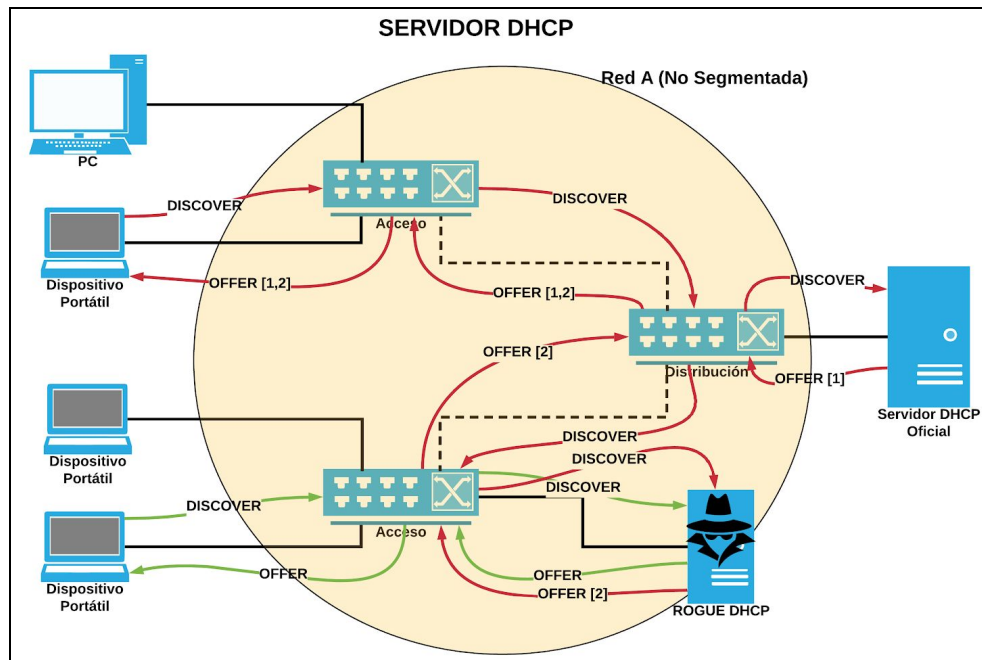


Figura 38. Intercambio de mensajes DHCP, red no segmentada con Rogue DHCP.
Fuente: Los autores.

Análisis caso campus Barcelona

En el apartado anterior se refleja lo que sucedía en el campus Barcelona. Afortunadamente aunque se afectaba el servicio de internet para algunos equipos cliente, el problema residía en un equipo mal conectado, en este caso un router manipulado por un usuario no técnico. Lo que realizaba el usuario era conectar el cable de WAN, que provenía de un switch de acceso a uno de los puertos de LAN de un router; provocando que ese router empezará a responder solicitudes de DHCP de equipos cliente en busca de una dirección IP (ver Figura 39).

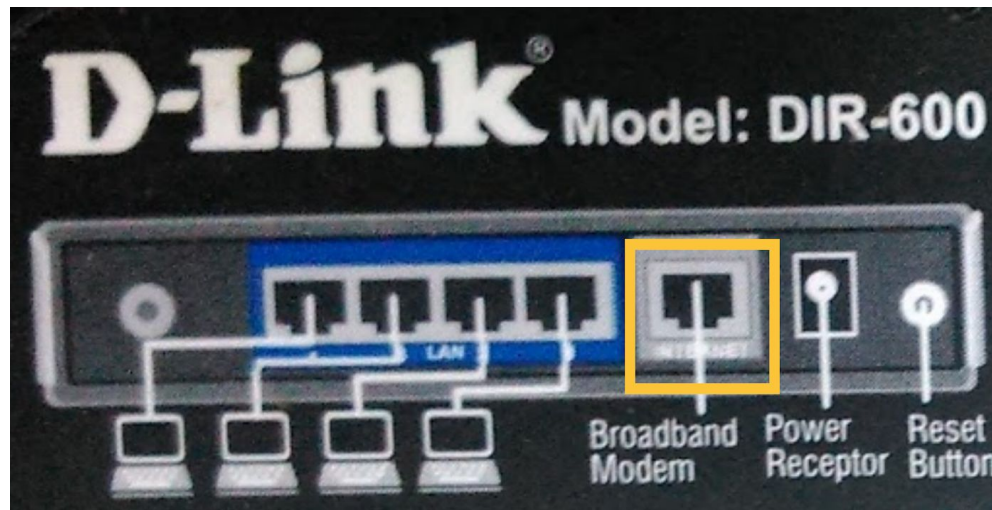


Figura 39. Puerto de WAN, indicación router D-Link.

Por tanto cuando se empezó a reportar el problema por parte del personal encargado de la Oficina de Sistemas, se procedió con el analizador de protocolos *Wireshark* a capturar el tráfico en un switch de la red. Conociendo el problema que ya se había presentado en ocasiones anteriores, se empezó a buscar mensajes de tipo **DHCP NAK** aplicando el filtro correspondiente, que permitiera visualizar el intercambio de mensajes del protocolo DHCP.

Filtro *Wireshark*:

udp.port==67 or udp.port==68

Claramente el filtro se aplica sobre los puertos de trabajo del protocolo DHCP, correspondientes al **67** y **68**. En la Figura 40 se puede observar el resultado de la captura.

udp.port==67 or udp.port==68						
Io.	Time	Source	Destination	Protocol	Length	Info
5209	8.086468510	0.0.0.0	255.255.255.255	DHCP	356	DHCP Request - Transaction ID 0xb5f0cf52
5210	8.088277360	192.168.1.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xb5f0cf52
5590	8.699974788	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x713c7334
5595	8.703708604	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x713c7334
5716	8.898404752	0.0.0.0	255.255.255.255	DHCP	366	DHCP Request - Transaction ID 0x749e648c
5928	9.220144549	0.0.0.0	255.255.255.255	DHCP	357	DHCP Request - Transaction ID 0xa3065b8a
5930	9.220841584	172.17.0.6	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xa3065b8a
5932	9.222433891	192.168.1.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xa3065b8a
5978	9.312878824	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0x73ab3e61
5984	9.338996070	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x73ab3e61
6964	10.82146574	0.0.0.0	255.255.255.255	DHCP	357	DHCP Request - Transaction ID 0xa3065b8a
6965	10.82187294	172.17.0.6	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xa3065b8a
6967	10.82441562	192.168.1.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xa3065b8a
7348	11.52409156	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6d9550a
8256	12.971608540	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x361a2495

Figura 40. Captura tráfico usando la aplicación *Wireshark*, en busca de un Rogue DHCP.

Para la fecha de esta captura, el campus contaba con la red bajo el direccionamiento antiguo usando la red **172.17.0.0/16**, en la cual se encontraban varios servidores DHCP con las direcciones **172.17.0.X - 172.17.0.X - 172.17.0.X**. Al observar con detalle la captura, existe un equipo bajo una IP privada **192.168.1.1** el cual esta generando mensajes **DHCP NAK**, lo que claramente indica que existe un **Rogue DHCP** dentro de la red.

Analizando con más profundidad se toman estos 2 paquetes, que poseen el mismo **Transaction Identifier 0x4fdc8d8b**, lo que quiere decir que pertenecen a una misma conversación o diálogo entre los equipos cliente y servidor (ver Figura 41).

0.0.0.0	255.255.255.255	DHCP	356 DHCP Request - Transaction ID 0x4fdc8d8b
192.168.1.1	255.255.255.255	DHCP	342 DHCP NAK - Transaction ID 0x4fdc8d8b

Figura 41. Paquetes análisis con *Wireshark*.

Se puede observar en la Figura 42, el contenido del formato de mensaje DHCP, para el *Request*.

1. El **Transaction Identifier** corresponde al **0x4fdc8db8b**.
2. Dentro del campo **Options**, utiliza el subcampo **DHCP Message Type** que corresponde a un **DHCP REQUEST**, lo que indica que el equipo cliente esta realizando una petición al servidor.
3. Dentro del campo **Options**, utiliza el subcampo **Requested IP Address**, que corresponde al valor de **172.17.226.123**, lo que indica que el equipo cliente está solicitando una IP específica, con la cual pudo estar asociado anteriormente.

```
Transaction ID: 0x4fdc8d8b 1
Seconds elapsed: 0
▶ Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: SamsungE_1c:17:3a (84:2e:27:1c:17:3a)
Client hardware address padding: 0000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
▼ Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3) 2
▶ Option: (61) Client identifier
▼ Option: (50) Requested IP Address
    Length: 4
    Requested IP Address: 172.17.226.123 3
▶ Option: (57) Maximum DHCP Message Size
▶ Option: (60) Vendor class identifier
```

Figura 42. Mensaje de tipo *Request*, análisis con *Wireshark*.

Ahora en la respuesta del servidor, se puede observar el contenido del mensaje DHCP con los siguientes valores.

1. El **Transaction Identifier** corresponde al **0x4fdc8db8b**. Esto indica que pertenece al mismo diálogo establecido, junto con la captura analizada anteriormente.
2. Dentro del campo **Options**, utiliza el subcampo **DHCP Message Type** que corresponde a un **DHCP NAK**, lo que indica que la petición realizada anteriormente por el equipo cliente, no cumple o no puede ser aplicada debido a que los parámetros de configuración solicitados (IP 172.17.226.123) no pueden ser brindados por el servidor.
3. Dentro del campo **Options**, utiliza el subcampo **DHCP Server Identifier** con el valor **192.168.1.1**, lo que indica que el servidor se está identificando con esa IP (**Rogue DHCP**).

4. Dentro del campo **Options**, utiliza el subcampo **Message** con el valor **wrong network** (red equivocada), lo que indica que el servidor no puede proveer al cliente, ese rango de IP (ver Figura 43).

```
nups. v
Transaction ID: 0x4fdc8d8b 1
Seconds elapsed: 0
▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: SamsungE_1c:17:3a (84:2e:27:1c:17:3a)
Client hardware address padding: 0000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
▼ Option: (53) DHCP Message Type (NAK)
    Length: 1
    DHCP: NAK (6) 2
▼ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.1.1 3
▼ Option: (56) Message
    Length: 13
    Message: wrong network 4
▶ Option: (255) End
```

Figura 43. Mensaje de tipo *Request*, análisis con *Wireshark*.

En este caso, al servidor responder con un **DHCP NAK**, hará que el equipo cliente regrese a su estado inicial, para luego nuevamente solicitar una dirección IP. En el caso inverso, otros equipos solicitaron direcciones IP en el rango ofrecido por el **Rogue DHCP** siendo estas concedidas, ocasionando que estos quedarán vinculados a la red con una dirección incorrecta y sin acceso a Internet.

Finalmente lo que se presentó en este anexo, representa uno de los peligros a los cuales se expone una red, donde el nivel de impacto que puede ocasionar este tipo de ataques, tanto a los servicios como a la información; pueden ser minimizados o evitados si se siguen los parámetros correctos y buenas prácticas a la hora del despliegue de una infraestructura de red (físico y lógico). Estos parámetros y buenas prácticas, se encuentran representados a lo largo del libro, en las actividades realizadas concernientes a la implementación del nuevo

direccionamiento IP, las VLANs para la segmentación y el uso de plataformas de monitoreo como por ejemplo **LibreNMS**. Resaltar que en este campo el trabajo debe ser siempre iterativo y de una constante supervisión, ya que una red, aunque se considera como una infraestructura de evolución o crecimiento lento dentro de la organización, es la encargada de ser la autopista sobre la que viaja toda la información (activo valioso) que allí se maneja. Por eso la proactividad que se cierna alrededor de la misma, hará posible la resolución y anticipación a posibles problemas y riesgos de seguridad que se puedan llegar a presentar, beneficiando a los usuarios con un mejor servicio y protección de la información.

13.2 Acuerdos de confidencialidad

**ACUERDO DE CONFIDENCIALIDAD
ENTRE UNIVERSIDAD DE LOS LLANOS – OFICINA DE SISTEMAS
Y BAYRON DANILO ORTIZ FORONDA**

Entre la oficina de sistemas de la Universidad de los Llanos y el estudiante **BAYRON DANILO ORTIZ FORONDA** con código 160002925 y cédula de ciudadanía N° 1121887045, se establece un acuerdo de confidencialidad sobre la información suministrada y desarrollada dentro del proyecto "REESTRUCTURACIÓN DE LA RED WI-FI DEL CAMPUS BARCELONA DE LA UNIVERSIDAD DE LOS LLANOS" como parte de la pasantía, la cual está regida por la resolución No. 018 DE 2006.

En atención a lo anterior, este Acuerdo de Confidencialidad consta de las siguientes cláusulas:

1. Obligaciones especiales del estudiante:

Guardar absoluta confidencialidad, incluso después de terminada la pasantía: procedimientos, procesos, actividades, proyectos que se adelanten de investigación, desarrollos, datos, diseños, fotografías, especificaciones de software, software, claves de seguridad, suministros, base de datos de cualquier índole, información técnica, manuales de uso, manuales técnicos y demás que la oficina de sistemas de la Universidad de los Llanos utilice en el desarrollo de sus actividades.

Parágrafo Uno: El incumplimiento de esta obligación no sólo es causal de terminación de la pasantía, sino que podría conllevar a iniciar acciones judiciales en contra del estudiante por los perjuicios materiales e inmateriales que cause.

- a) Garantizar la más estricta reserva respecto de la información técnica y bases de datos, entregada por la oficina de sistemas de la Universidad de los Llanos en el marco de la pasantía, y advertir de dicho deber de confidencialidad y secreto a cualquier persona que por su relación con él, deba tener acceso a dicha información para el correcto cumplimiento de sus obligaciones.



Universidad
de los Llanos

Oficina de Sistemas

- b) Abstenerse de reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente acuerdo, sin previa autorización escrita y expresa de la Oficina de sistemas de la Universidad de los Llanos.
- c) Adoptar todas las precauciones necesarias y apropiadas para la guarda de la confidencialidad de la información que tenga el estudiante de la oficina de sistemas, esto es, procedimientos, procesos, actividades, proyectos que se adelanten de investigación, desarrollos, datos, diseños, fotografías, especificaciones de software, software, claves de seguridad, suministros, base de datos de cualquier índole, información técnica, manuales de uso, manuales técnicos utilizados por Oficina de sistemas de la Universidad de los Llanos interna y externamente frente a terceros.

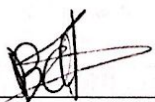
Parágrafo Dos: La omisión del estudiante en prevenir la fuga de información confidencial o exclusiva de la oficina de sistemas interna y externamente, es causal de terminación de pasantía, sin perjuicio de las acciones legales en su contra por los perjuicios causados y el cobro de las sanciones por incumplimiento, además de la cláusula penal por incumplimiento.

2. Sanciones por incumplimiento: El estudiante se sujetará a través de la suscripción del presente compromiso, a las acciones legales que la Universidad de los Llanos pueda ejercer frente al incumplimiento del mismo, de esta manera si la Universidad demuestra que con su actuación se vulneran los derechos, podrá ejercer las acciones civiles, penales y administrativas que le permitan restablecer su situación y la indemnización del daño causado según lo determinen las autoridades competentes que conozcan de las acciones legales que se adelanten.

3. Aspectos finales: Este Acuerdo de Confidencialidad se mantendrá en el tiempo, así la pasantía o de cualquier tipo haya terminado, pues su incumplimiento causará perjuicios a la oficina de sistemas de la Universidad de los Llanos y le dará derecho a cobrar la cláusula penal establecida por el sólo hecho de su incumplimiento y sin perjuicio de las acciones judiciales del caso por los perjuicios causados.

Se suscribe en Villavicencio, a los 04 del mes de abril de 2018


OLGA-LUCÍA BALAGUERA RIVERA
Jefe de la Oficina de sistemas


BAYRÓN D. ORTIZ FORONDA
Cód. 160002925

Tel. 6616800 Ext. 107 Sede Barcelona
6616900 Ext. 109 Sede San Antonio

sistemas@unillanos.edu.co
soporte@unillanos.edu.co

**ACUERDO DE CONFIDENCIALIDAD
ENTRE UNIVERSIDAD DE LOS LLANOS – OFICINA DE SISTEMAS
Y JULY STEFANNY SALAZAR SIERRA**

Entre la oficina de sistemas de la Universidad de los Llanos y el estudiante **JULY STEFANNY SALAZAR SIERRA** con código 160003237 y cédula de ciudadanía N° 1121929886, se establece un acuerdo de confidencialidad sobre la información suministrada y desarrollada dentro del proyecto "REESTRUCTURACIÓN DE LA RED WI-FI DEL CAMPUS BARCELONA DE LA UNIVERSIDAD DE LOS LLANOS" como parte de la pasantía, la cual está regida por la resolución No. 018 DE 2006.

En atención a lo anterior, este Acuerdo de Confidencialidad consta de las siguientes cláusulas:

1. Obligaciones especiales del estudiante:

Guardar absoluta confidencialidad, incluso después de terminada la pasantía: procedimientos, procesos, actividades, proyectos que se adelanten de investigación, desarrollos, datos, diseños, fotografías, especificaciones de software, software, claves de seguridad, suministros, base de datos de cualquier índole, información técnica, manuales de uso, manuales técnicos y demás que la oficina de sistemas de la Universidad de los Llanos utilice en el desarrollo de sus actividades.

Parágrafo Uno: El incumplimiento de esta obligación no sólo es causal de terminación de la pasantía, sino que podría conllevar a iniciar acciones judiciales en contra del estudiante por los perjuicios materiales e inmateriales que cause.

- a) Garantizar la más estricta reserva respecto de la información técnica y bases de datos, entregada por la oficina de sistemas de la Universidad de los Llanos en el marco de la pasantía, y advertir de dicho deber de confidencialidad y secreto a cualquier persona que por su relación con él, deba tener acceso a dicha información para el correcto cumplimiento de sus obligaciones.
- b) Abstenerse de reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente acuerdo, sin previa autorización escrita y expresa de la Oficina de sistemas de la Universidad de los Llanos.



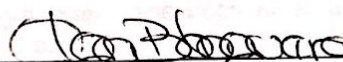
- c) Adoptar todas las precauciones necesarias y apropiadas para la guarda de la confidencialidad de la información que tenga el estudiante de la oficina de sistemas, esto es, procedimientos, procesos, actividades, proyectos que se adelanten de investigación, desarrollos, datos, diseños, fotografías, especificaciones de software, software, claves de seguridad, suministros, base de datos de cualquier índole, información técnica, manuales de uso, manuales técnicos utilizados por Oficina de sistemas de la Universidad de los Llanos interna y externamente frente a terceros.

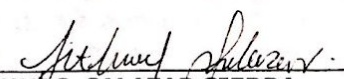
Parágrafo Dos: La omisión del estudiante en prevenir la fuga de información confidencial o exclusiva de la oficina de sistemas interna y externamente, es causal de terminación de pasantía, sin perjuicio de las acciones legales en su contra por los perjuicios causados y el cobro de las sanciones por incumplimiento, además de la cláusula penal por incumplimiento.

2. Sanciones por incumplimiento: El estudiante se sujetará a través de la suscripción del presente compromiso, a las acciones legales que la Universidad de los Llanos pueda ejercer frente al incumplimiento del mismo, de esta manera si la Universidad demuestra que con su actuación se vulneran los derechos, podrá ejercer las acciones civiles, penales y administrativas que le permitan restablecer su situación y la indemnización del daño causado según lo determinen las autoridades competentes que conozcan de las acciones legales que se adelanten.

3. Aspectos finales: Este Acuerdo de Confidencialidad se mantendrá en el tiempo, así la pasantía o de cualquier tipo haya terminado, pues su incumplimiento causará perjuicios a la oficina de sistemas de la Universidad de los Llanos y le dará derecho a cobrar la cláusula penal establecida por el sólo hecho de su incumplimiento y sin perjuicio de las acciones judiciales del caso por los perjuicios causados.

Se suscribe en Villavicencio, a los 04 del mes de abril de 2018


OLGA LUCIA BALAGUERA RIVERA
Jefe de la Oficina de sistemas


JULY S. SALAZAR SIERRA
Cód. 160003237

14 BIBLIOGRAFÍA

- [1] Pellejero, I., Andreu, F., Lesta, A., (2006), *Fundamentos y Aplicaciones de Seguridad en Redes WLAN*. Barcelona, España. Marcombo Ediciones Técnicas.
- [2] Tanenbaum, A., Wetherall, D., (2012), *Redes de Computadoras*. Naucalpan de Juárez, México, Editorial Pearson Educación.
- [3] Lammle, T., (2007), *CCNA: Cisco Certified Network Associate Study Guide*. Indianapolis, USA, Wiley Publishing, Inc.
- [4] Alonso, I., (2013), *Análisis Comparativo De Dos Protocolos Para Control De Acceso Y Administración De Equipos De Telecomunicaciones* (Tesis de Pregrado). Universidad Católica de Colombia, Bogotá.
- [5] Network RADIUS SARL. (2014), *The FreeRADIUS Technical Guide*. Recuperado de <http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf>
- [6] Stallings, W.,(2004), *Comunicaciones y Redes de Computadores*. Madrid, España. Editorial Pearson Educación S.A
- [7] Oppenheimer, P., & Press, C. (2012). *Top-Down Network Design Top-Down Network Design*, Third Edition Warning and Disclaimer Corporate and Government Sales. Recuperado de <http://ptgmedia.pearsoncmg.com/images/9781587202834/samplepages/1587202832.pdf>
- [8] Wireless Networking in the Developing World. (2007). *2.4 GHz Wi-Fi channels (802.11b,g WLAN)* [Figura 5], Recuperado de [https://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_\(802.11b,g_WLAN\).svg](https://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg)
- [9] Camargo, J., (2009), *Modelo De Cobertura Para Redes Inalámbricas De Interiores* (Tesis de Pregrado). Universidad de Sevilla. Sevilla, España.
- [10] López, J., (2007), *Redes Inalámbricas Wireless LAN* (Monografía de Pregrado). Universidad Autónoma Del Estado De Hidalgo, México.
- [11] Reyes, H., Grupo GERA. (2017). *Informe Diagnóstico Red Unillanos*. Universidad de los Llanos. Villavicencio, Colombia.

- [12] Rohde & Schwarz, (2012), White Paper: *802.11ac Technology Introduction*. Recuperado de http://www.rohde-schwarz-usa.com/rs/rohdeschwarz/images/1MA192_7e_80211ac_technology.pdf
- [13] Arguello, M., Mata, J., & Navarrete, I., (2009). *Propuesta de análisis y diseño de la red inalámbrica en la DCYC del instituto politécnico nacional* (Propuesta de Pregrado). Instituto Politécnico Nacional, México.
- [14] Molina, J.,(2012). *Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la empresa editora El Comercio planta norte*. (Tesis de Pregrado). Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú.
- [15] Rafax. (2012). *A Virtual Local Area Network Topology* [Figura 8], Recuperado de <https://commons.wikimedia.org/wiki/File:VLAN.svg>
- [16] Oyuhain. (2016). *Virtual LAN*. [Figura 9]. Recuperado de <https://commons.wikimedia.org/wiki/File:Vlan-fig1.gif>
- [17] Kozierok, Charles M., (2005), *The TCP/IP Guide*. San Francisco, USA, Editorial No Starch Press.